

HP Business Service Management

for the Windows operating system

Software Version: 9.00

Data Flow Management

Document Release Date: July 2010

Software Release Date: July 2010



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 Notices

© Copyright 2005 - 2010 Hewlett-Packard Development Company, L.P

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

- This product includes software developed by Apache Software Foundation (<http://www.apache.org/licenses>).
- This product includes OpenLDAP code from OpenLDAP Foundation (<http://www.openldap.org/foundation/>).
- This product includes GNU code from Free Software Foundation, Inc. (<http://www.fsf.org/>).
- This product includes JiBX code from Dennis M. Sosnoski.
- This product includes the XPP3 XMLPull parser included in the distribution and used throughout JiBX, from Extreme! Lab, Indiana University.
- This product includes the Office Look and Feels License from Robert Futrell (<http://sourceforge.net/projects/officelnfs>).
- This product includes JEP - Java Expression Parser code from Netaphor Software, Inc. (<http://www.netaphor.com/home.asp>).

Documentation Updates

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

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

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

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link 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 web site at:

<http://www.hp.com/go/hpsoftwaresupport>

This web site 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 web site 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 sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

Welcome to This Guide	11
How This Guide Is Organized	11
Who Should Read This Guide	12
How Do I Find the Information That I Need?	13
Additional Online Resources.....	15
Documentation Updates	16

PART I: INTRODUCTION

Chapter 1: Introduction to Data Flow Management.....	19
Data Flow Management Overview	20
Data Flow Management Architecture	24
Data Flow Management Concepts	25
Naming Conventions	30
Receiving Bulk Data from SiteScope	30
Troubleshooting and Limitations	30
Chapter 2: Licensing Models for ODB	33
Licensing Models – Overview	34
Upgrade to the Integration or DDM Advanced License	37
Troubleshooting and Limitations	38
Chapter 3: Data Flow Probe Installation.....	39
Install the Data Flow Probe	40
Upgrade the Probe	51
Run Probe Manager and Probe Gateway on Separate Machines	51
Configure the Probe Manager and Probe Gateway Components.....	52
Connect a Data Flow Probe to a Non-Default Customer.....	53
Data Flow Probe Installation Requirements.....	54

PART II: DATA FLOW MANAGEMENT SETUP

Chapter 4: Data Flow Probe Setup 59
Job Execution Policies 60
Data Validation on the Data Flow Probe 62
Filtering Results 63
Get Started With the ODB Data Flow Probe 64
Add a Data Flow Probe 65
Delete Unsent Probe Results 67
Data Flow Probe Setup User Interface 68
Domain Credential References..... 83
Data Flow Probe Log Files 106
The DiscoveryProbe.properties File 110
Troubleshooting and Limitations 111

Chapter 5: Data Flow Probe Status 113
Data Flow Probe Status Overview 114
View Current Status of Discovered CIs 115
Data Flow Probe Status User Interface 116

Chapter 6: Adapter Management 123
Automatically Deleted CIs and Relationships and Candidates
for Deletion CIs..... 124
Discovering Running Software..... 126
Identifying Running Software by Processes 127
The portNumberToPortName.xml File 128
Configure the Data Flow Probe to Automatically Delete CIs –
Workflow 129
Discover Running Software – Scenario 130
Define a New Port 133
Use the cpVersion Attribute to Verify Content Update..... 135
Manage Adapter Configurations 135
Resource Files..... 138
Internal Configuration Files..... 141
Adapter Management User Interface 141

PART III: INTEGRATION

Chapter 7: Integration Studio	189
Integration Studio Overview	190
Work with Federated Data	194
Work with Population Jobs	195
Work with Data Push Jobs	197
Integration Studio User Interface	199
Out-of-the-Box Integrations	213
Troubleshooting and Limitations	214
Chapter 8: Integrating Multiple ODBs	217
Integrating Multiple ODBs Overview.....	218
Content Management System (CMS).....	218
Global ID	219
Use Cases – Multiple ODB Deployments	219
Multiple Deployments with Version 9.00 ODBs	220
Federation in Version 9.01 ODBs	224
Multiple Deployments with Version 8.0 ODBs	226
Set Up Integrations Between Multiple ODBs (ODB Version 9.0x)....	229
Set Up Integrations between CMS and ODB.....	230
Set Up Integrations Between Multiple ODBs (ODB Version 8.0x)....	232
Troubleshooting and Limitations	234

PART IV: DISCOVERY

Chapter 9: Discovery Control Panel	239
Discovery Control Panel Overview	240
Viewing Permissions While Running Jobs	242
Managing Problems With Error Reporting	243
The Permissions Document.....	244
Discovery Control Panel – Basic Mode Workflow	246
Discovery Control Panel – Advanced Mode Workflow	247
View Job Information on the ODB Data Flow Probe.....	251
Manually Activate a Job	263
Manage Errors.....	263
Find Errors	265
Discovery Control Panel User Interface	267

PART V: RECONCILIATION

Chapter 10: Reconciliation **339**
Reconciliation Overview 340
Stable ID 341
Reconciliation Configuration..... 341
Reconciliation Services 346
Add an Identification Rule to an Existing CIT..... 353
Add Reconciliation Priorities to an Existing CIT 353
Create XML Reconciliation Files 354
Identification Rule Schema 358
Reconciliation Priority Schema 366

PART VI: HARDENING

Chapter 11: Hardening Data Flow Management **371**
Hardening Data Flow Management Overview..... 372
Credentials Encryption With Confidential Manager 374
Manage the Storage of Credentials 376
Generate or Update the Encryption Key..... 377
Export and Import the domainScopeDocument (DSD) File in
 Encrypted Format 383
Chapter 12: Hardening the Data Flow Probe **385**
Set the MySQL Database Encrypted Password 386
Set the JMX Console Encrypted Password 388
Enable SSL Between BSM Server and Data Flow Probe with Mutual
 Authentication 389
Enable SSL on the Data Flow Probe with Basic Authentication 390
Connect the Data Flow Probe by Reverse Proxy 390
Control the Location of the domainScopeDocument File 392
Chapter 13: Using SSL with the Data Flow Probe **393**
Using SSL with the Data Flow Probe Overview..... 394
Enable SSL Between BSM Running an Internal UCMDDB and
 the Data Flow Probe with Mutual Authentication 395
Configure SSL from the Data Flow Probe to the Gateway Server 395
Index **397**

Welcome to This Guide

This guide describes the applications that enable data flow management. These applications include the Integration Studio and Discovery.

For details on working with DFM content, see the *ODB Discovery and Integration Content Guide* PDF.

This chapter includes:

- How This Guide Is Organized on page 11
- Who Should Read This Guide on page 12
- How Do I Find the Information That I Need? on page 13
- Additional Online Resources on page 15
- Documentation Updates on page 16

How This Guide Is Organized

The guide contains the following parts:

Part I Introduction

Describes the components of Data Flow Management, including the Integration Studio and discovery. Describes ODB licensing policies and Data Flow Probe installation.

Part II Data Flow Management Setup

Describes how to set up HP Business Service Management to discover components running in your environment.

Part III Integration

Explains how to define adapters to include data in the ODB from other sources.

Part IV Discovery

Describes how to activate jobs that discover the components of your system

Part V Reconciliation

Explains how to match and identify entities from different data repositories.

Part VI Hardening

Explains how to harden Discovery and the Data Flow Probe and how to configure SSL with your Business Service Management platform and Data Flow Probe.

Who Should Read This Guide

This guide is intended for the following users of HP Business Service Management:

- ▶ HP Business Service Management administrators
- ▶ HP Business Service Management platform administrators
- ▶ HP Business Service Management application administrators
- ▶ HP Business Service Management data collector administrators

Readers of this guide should be knowledgeable about enterprise system administration, have familiarity with ITIL concepts, and be knowledgeable about Business Service Management in general and the Operational Database technology specifically.

How Do I Find the Information That I Need?

This guide is part of the HP Business Service Management Documentation Library. This Documentation Library provides a single-point of access for all Business Service Management documentation.

You can access the Documentation Library by doing the following:



- In Business Service Management, select **Help > Documentation Library**.
- From a Business Service Management Gateway Server machine, select **Start > Programs > HP Business Service Management > Documentation**.



Topic Types

Within this guide, each subject area is organized into topics. A topic contains a distinct module of information for a subject. The topics are generally classified according to the type of information they contain.

This structure is designed to create easier access to specific information by dividing the documentation into the different types of information you may need at different times.

Three main topic types are in use: **Concepts**, **Tasks**, and **Reference**. The topic types are differentiated visually using icons.

Topic Type	Description	Usage
Concepts 	Background, descriptive, or conceptual information.	Learn general information about what a feature does.
Tasks 	<p>Instructional Tasks. Step-by-step guidance to help you work with the application and accomplish your goals. Some task steps include examples, using sample data.</p> <p>Task steps can be with or without numbering:</p> <ul style="list-style-type: none"> ▶ Numbered steps. Tasks that are performed by following each step in consecutive order. ▶ Non-numbered steps. A list of self-contained operations that you can perform in any order. 	<ul style="list-style-type: none"> ▶ Learn about the overall workflow of a task. ▶ Follow the steps listed in a numbered task to complete a task. ▶ Perform independent operations by completing steps in a non-numbered task.
	<p>Use-case Scenario Tasks. Examples of how to perform a task for a specific situation.</p>	Learn how a task could be performed in a realistic scenario.

Topic Type	Description	Usage
 Reference	General Reference. Detailed lists and explanations of reference-oriented material.	Look up a specific piece of reference information relevant to a particular context.
	User Interface Reference. Specialized reference topics that describe a particular user interface in detail. Selecting Help on this page from the Help menu in the product generally open the user interface topics.	Look up specific information about what to enter or how to use one or more specific user interface elements, such as a window, dialog box, or wizard.
 Troubleshooting and Limitations	Troubleshooting and Limitations. Specialized reference topics that describe commonly encountered problems and their solutions, and list limitations of a feature or product area.	Increase your awareness of important issues before working with a feature, or if you encounter usability problems in the software.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help > Troubleshooting & Knowledge Base**. The URL for this Web site is <http://h20230.www2.hp.com/troubleshooting.jsp>.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help > HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport user ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help > HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (<http://h20230.www2.hp.com/selfsolve/manuals>).

Part I

Introduction

1

Introduction to Data Flow Management

This chapter includes:

Concepts

- ▶ Data Flow Management Overview on page 20
- ▶ Data Flow Management Architecture on page 24
- ▶ Data Flow Management Concepts on page 25

Reference

- ▶ Naming Conventions on page 30
- ▶ Receiving Bulk Data from SiteScope on page 30

Troubleshooting and Limitations on page 30

Concepts

Data Flow Management Overview

This section includes the following topics:

- "ODB Integrations" on page 20
- "Discovery" on page 21
- "Reconciliation" on page 23

ODB Integrations

You use the Integration Studio to set up integrations with external data repositories.

An integration type can be:

- **Population.** Integration that populates the ODB with CI and relationship information.
- **Federation.** Integration that retrieves CIs and relationships from an external repository whenever the data is requested in an ad-hoc fashion.
- **Data Push.** Integration that pushes CIs and relationships from the ODB to an external data repository.

Each integration adapter supports certain types of integrations. For example, an Integration adapter that supports both Population and Federation types can retrieve data periodically for storage within the CMDB or upon query time; both these configurations can co-exist within a single integration.

For details, see "Integration Studio" on page 189.

Discovery

The Discovery process is the mechanism that enables you to collect information about your IT infrastructure resources and their interdependencies. Discovery automatically discovers and maps logical application assets in Layers 2 to 7 of the Open System Interconnection (OSI) Model.

Discovery discovers resources such as applications, databases, network devices, servers, and so on. Each discovered IT resource is delivered to, and stored in, the configuration management database (CMDB) where the resource is represented as a managed CI.

Discovery is an ongoing, automatic process that continuously detects changes that occur in the IT infrastructure and updates the CMDB accordingly. You do not need to install any agents on the devices to be discovered.

Following installation, the network on which the ODB Data Flow Probe is located, the host on which the Probe resides, and the host's IP address are automatically discovered and a CI is created for each of these objects. These discovered CIs populate the CMDB. They act as triggers that activate a Discovery job. Every time a job is activated, the job discovers more CIs, which in turn are used as triggers for other jobs. This process continues until the entire IT infrastructure is discovered and mapped.

Once you configure Discovery and activate the required discovery jobs, Discovery runs on the system, discovers system components, and saves them as CIs in the CMDB. You can discover new objects either manually or automatically. Objects that are outside the Probe's network require additional, manual configuration.

Note: This guide assumes that the ODB Data Flow Probe is installed in the default location, that is, **C:\hp\UCMDB\DataFlowProbe**.

Data Flow Management Modules

Data Flow Management (DFM) includes the following application modules:

- "Integration Studio" on page 22
- "Discovery Control Panel" on page 22
- "Data Flow Probe Setup" on page 22
- "Adapter Management" on page 23
- "DDM Community" on page 23
- "Data Flow Probe Status" on page 23

Integration Studio

The Integration Studio module enables you to set up BSM integrations to define and control data flows from external data repositories to the ODB, or from the ODB to external data repositories.

For details, see "Integration Studio" on page 189.

Discovery Control Panel

The Discovery Control Panel application module enables you to manage the Discovery process to discover the CIs and relationships of your IT Infrastructure. You control the process by activating discovery jobs. You can choose to activate all or some of the jobs in a module. You can also edit discovery jobs, and schedule a job to run at a certain time.

For details, see "Discovery Control Panel" on page 239.

Data Flow Probe Setup

The Data Flow Probe Setup module enables you to add Probes to the system and to edit existing Probes. You define the network range that each Probe covers. From the Data Flow Probe Setup you also manage credentials. The credentials are used for both Discovery and Integrations purposes.

For details, see "Data Flow Probe Setup" on page 59.

Adapter Management

The Adapter Management module enables you to edit adapters, scripts, and configuration files. You can also replace or remove external resources needed in either Discovery or Integration.

For details, see "Adapter Management" on page 123.

DDM Community

The DDM Community Web site provides you with a convenient way to obtain the latest Discovery and Integration Content Pack. You need an HP Passport user name and password to log in. The URL for this Web site is: <https://h20090.www2.hp.com/>.

For details, see "DDM Community" on page 135.

Data Flow Probe Status

The Data Flow Probe Status module enables you to view the current status of a particular Data Flow Probe: which discovery or integration job the Probe is currently running, execution statistics, and so on. You can also view the report results in a My BSM portlet.

For details, see "Data Flow Probe Status" on page 113.

Reconciliation

The Reconciliation process consists of two important steps:

- ▶ **Identification.** The process by which CIs and relationships within the ODB are identified against existing CIs within the ODB, other CIs within the same bulk, or CIs coming from various federated data sources.
- ▶ **Reconciliation Priority.** The process by which the ODB reconciliation engine decides how to deal with conflicting data. When conflicting values are given for the same CI attribute by different integrations, the ODB reconciliation engine resolves the conflict by looking at the reconciliation priority assigned to each integration.

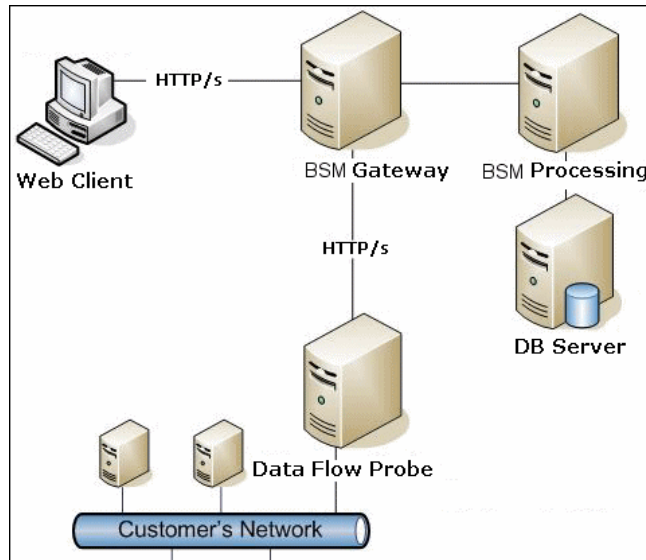
By default, unless you customize the reconciliation priorities within the Reconciliation Priority Manager, the ODB reconciliation engine uses the last reported value as the most accurate, that is, all integrations have exactly the same priority.

For details about reconciliation, see "Reconciliation" on page 339.

For details about the Reconciliation Priority Manager, see "Reconciliation Priority Manager Window" on page 211.

Data Flow Management Architecture

Data Flow Management architecture is deployed as follows:



- The Data Flow Probe is responsible for the data flow to and from external data repositories (data push or population) and for performing discovery. Federation is always run directly from the ODB Server and does not leverage the Probe infrastructure. Generally, data push runs from the ODB Server, but uses the Probe in cases where the adapter is based on the Data Push Adapter platform.

- The Data Flow Probe initiates communication with the ODB Server using http or https traffic, enabling the product to bypass possible firewalls.

Data Flow Management Concepts

This section describes the main topics of Data Flow Management:

- "Data Flow Probe" on page 25
- "Communication Protocols" on page 25
- "Discovery and Integration Adapters" on page 26
- "Discovery Modules" on page 27
- "Discovery and Integration Content Packs" on page 28
- "Integration Points" on page 28
- "Discovery Jobs" on page 28
- "Discovery Wizards" on page 28
- "Agentless Discovery" on page 29
- "Trigger CIs and Trigger Queries" on page 29

Data Flow Probe

The ODB Data Flow Probe is the main component responsible for requesting tasks from the server, scheduling tasks, executing them, and sending the results back to the BSM Server. You define a range of network addresses for a specific, installed Probe. Each Probe is identified by its name, chosen as part of the Data Flow Probe installation process.

Communication Protocols

Discovery of the IT infrastructure components uses protocols such as SNMP, WMI, JMX, Telnet, and so on. For details, see "Domain Credential References" on page 83.

Discovery and Integration Adapters

An adapter can be of one of the following types:

- ▶ **Jython Adapter.** An adapter based on a set of Jython scripts that are executed sequentially. For details, see "Create Jython Code" in the *ODB Developer Reference Guide*.
- ▶ **Java Adapter.** An adapter based on Java code that implements the various DFM interfaces and is wrapped in a JAR file. For details, see "Developing Java Adapters" in the *ODB Developer Reference Guide*.
- ▶ **Generic DB Adapter.** An adapter that uses SQL queries and maps database tables to CIs and relationships by using an ORM file. For details, see "Developing Generic Database Adapters" in the *ODB Developer Reference Guide*.
- ▶ **Generic Push Adapter.** An adapter that uses a mapping file and Jython scripts to push data to an external data repository. For details, see "Developing Push Adapters" in the *ODB Developer Reference Guide*.

The adapters themselves do not contain information about the target to which they are to connect and from which they are to retrieve information. For data flow to be configured and set up correctly, adapters require further context information, which can include an IP address, port information, credentials, and so on.

For discovery adapters (adapters used for performing Discovery), the additional information is brought from the Trigger CIs attached to the Discovery Jobs; for integration adapters, the information is either being manually fed when creating the integration or take from the selected Trigger CI.

For details on making adapter changes, see "Adapter Management Window" on page 157. For details on creating adapters, see "Adapter Development and Writing" in the *ODB Developer Reference Guide*.

Input Queries

Note: Input queries refer only to Discovery-based integrations.

Each adapter is assigned an Input query that is used for two functions:

- ▶ **The Input query defines a minimal set of requirements** for every Trigger CI included in a job or integration that triggers this adapter. (This is true even when no trigger query is associated with the job.)

For example, an input query can query for IPs related to hosts with an SNMP agent installed and discovered on them, that is, only IPs with installed SNMP agents can trigger this adapter. This prevents the case where a user could manually create a Trigger CI that adds all IPs as triggers to an adapter.

- ▶ **An Input query defines how to retrieve data information from the ODB.** Destination data information, even if it is not included in a Trigger CI, can be retrieved by the input query. The input query defines **how** to retrieve the information.

For example, you can define a relationship between a Trigger CI (a node with the node name of **SOURCE**) and the target CI and then can refer to the target CI according to this node name, in the Triggered CI Data pane. For details, see "Input Pane" on page 143.

For details on using input queries when writing adapters, see "Step 1: Create an Adapter" in the *ODB Developer Reference Guide*.

Discovery Modules

The module is a grouping of discovery jobs that logically belong together, can be operated and managed together, and so on. This helps to reduce clutter in the main view when many jobs need to be written, and can also offer better manageability.

When creating a job, you should choose a module for it or create a new module. If you are creating several jobs, the best practice is to split them into logical groups and assign them to modules accordingly.

Discovery Modules support a hierarchy of folders, to facilitate easy finding of the relevant discovery capability.

Discovery and Integration Content Packs

The latest Discovery and Integration content for ODB is delivered as a Content Pack available for download via the HP Live Network. For details on downloading and installing Content Packs, see "DDM Community" on page 135.

By downloading the latest Content Pack, you ensure that your system is up-to-date with the latest defect-fixes and content functionality. Content Packs are released in a separate release train and are installed on top of the current product platform.

Integration Points

Integration points are entities used to set up ODB integrations. Each integration point is created with a selected integration adapter and the additional configuration information required to set up the integration. For details on creating integration points, see "Integration Studio" on page 189.

Discovery Jobs

A job enables reuse of a discovery adapter for multiple Discovery process flows. Jobs enable scheduling the same adapter differently over different sets of triggered CIs and also supplying different parameters to each set. You launch Discovery by activating the relevant set of discovery jobs that must be run. Relevant trigger CIs are automatically added to the activated discovery jobs based on their Trigger Queries.

For details, see "Discovery Control Panel" on page 239.

Discovery Wizards

You use one of the Discovery wizards (to discover the infrastructure, databases, and J2EE applications) when you need to use the default values set for IP ranges, network credentials, and so on. For details on using a wizard, see "Basic Mode Window" on page 269.

Agentless Discovery

Discovery is an agentless technology that discovers IT environment components through a dedicated ODB Data Flow Probe residing on the customer's site.

Although Discovery is agentless, that is, it does not require the installation of dedicated agents on the servers that are to be discovered, it does depend on agents that are already installed such as SNMP, WMI, TELNET, SSH, NETBIOS, and others. Other discovery capabilities are based on application-specific protocols such as SQL, JMX, SAP, Siebel, and so on. For details, see "Domain Credential References" on page 83.

Trigger CIs and Trigger Queries

A Trigger CI is a CI in the CMDB that activates a discovery job. Every time a job is activated, the job may discover additional CIs, which in turn are used as triggers for other jobs. This process continues until the entire IT infrastructure is discovered and mapped.

For details on adding Trigger CIs to a job, see "Discovery Status Pane" on page 285.

A Trigger Query associated with a job is a subset of the Input Query, and defines which specific CIs should automatically trigger a job. That is, if an Input Query queries for IPs running SNMP, a Trigger Query queries for IPs running SNMP in the range 195.0.0.0-195.0.0.10.

Note: A Trigger Query must refer to the same objects as the Input Query. For example, if an Input Query of an adapter queries for IPs running SNMP, you cannot define a Trigger Query for an associated job to query for IPs connected to a node. This is because some of the IPs may not be connected to an SNMP object, as required by the Input Query.

Reference

Naming Conventions

When naming entities in Data Flow Management, you can use the following characters: a-z, A-Z, 0-9. When entering IP addresses, use only digits and asterisks (*).

Receiving Bulk Data from SiteScope

SiteScope results can be sent to BSM either zipped or unzipped. The request includes a parameter that indicates to BSM whether the results being sent are in zipped or unzipped format.

To send SiteScope results in a zipped format:

- 1 Open the following file:
`C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties`
- 2 Locate the line beginning `appilog.agent.probe.send.results.zipped`.
- 3 Change the value to **true**.
- 4 Restart the Probe so that it is updated with the changes.

SiteScope results are zipped before being sent to BSM.

Troubleshooting and Limitations

For details on using the log files to perform basic troubleshooting, see:

- ▶ "Data Flow Probe Log Files" on page 106.
- ▶ "Data Flow Management Log Files" in the *ODB Administration Guide*.

This section includes the following topics:

- ▶ "Discovery Results Do Not Appear in the Topology Map" on page 31

- "Networks and IPs" on page 31
- "TCP Ports" on page 31
- "Discover Resources on a Windows XP Machine" on page 32
- "Limitations" on page 32

Discovery Results Do Not Appear in the Topology Map

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

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

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

Networks and IPs

Problem. Not all networks or IPs have been discovered.

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

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

Solution. Change the scope of the Discovery range:

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

TCP Ports

Problem. Not all TCP ports have been discovered.

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

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

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

Discover Resources on a Windows XP Machine

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

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

Limitations

- ▶ When Discovery is installed on a non-English operating system, job and module names are still limited to English characters.
- ▶ Each Content Pack installation overrides all out-of-the-box resources with the contents of that Content Pack. This means that any changes you made to these resources are lost. This applies to the following resources: Queries, Views, Enrichments, Reports, Discovery Jython scripts, Discovery adapters, Discovery jobs, Discovery resources, Discovery configuration files, Discovery modules, CI Types, and Relationships. (Attributes added to CI Types and Relationships are not overridden).

In general, it is recommended to refrain from making changes to out-of-the-box resources. If you must do so, be sure to track your changes so that they can be re-applied after you install a Content Pack. Important general fixes (not specific to your environment) should be sent to CSO so that they can be analyzed and included as part of one of the next Content Packs.

2

Licensing Models for ODB

This chapter includes:

Concepts

- ▶ Licensing Models – Overview on page 34

Tasks

- ▶ Upgrade to the Integration or DDM Advanced License on page 37

Troubleshooting and Limitations on page 38

Concepts

Licensing Models – Overview

This section includes the following topics:

- ▶ “Licensing Levels” on page 34
- ▶ “Defined Terms and Definitions” on page 34
- ▶ “License for HP Software-as-a-Service” on page 35
- ▶ “License for HP ServiceCenter/Service Manager and Other Integrations” on page 35
- ▶ “Data Flow Probe Licensing” on page 36

Licensing Levels

- ▶ **UCMDB Foundation License.** The Foundation license includes UCMDB as the backbone component for BTO products. This version enables data flow between multiple instances of UCMDB, and integration with BTO products to enable solution deployment.
- ▶ **UCMDB Integration License.** The Integration license adds third party integrations on top of the UCMDB Foundation license.
- ▶ **UCMDB DDM Advanced License.** The DDM Advanced license includes all discovery capabilities to discover the IT infrastructure elements and feed that information as CIs and Relationships to the CMDB.

Defined Terms and Definitions

OS Instance. Each implementation of the bootable program that can be installed onto a physical system or a partition within the physical system. A physical system can contain multiple Operating System instances.

Managed Server. A computer system or computer system partition where a bootable program is installed. This does not include personal computers (or any computer primarily serving a single individual).

ODB uses a server OS instance-based licensing scheme for the DDM Advanced license with a minimum purchase requirement of 100 OS instances. An OS instance counts both physical and virtual systems including the physical system hosting one or more virtual systems. The DDM Advanced license entitles the licensee to integrate third party (non-HP) data sources to extend discovery. Server data integration requires one license for each Managed Server to extend discovery. The Licensee is entitled to one DDMi license for every DDM OS instance.

Example: A VMware ESX Server hosting one virtual machine requires two licenses to use (LTUs).

License for HP Software-as-a-Service

All packages.

License for HP ServiceCenter/Service Manager and Other Integrations

The following packages are available:

- UCMDB7-SCSM
- SAR_Integration
- DDMI_Integration
- NNM_Integration
- SE_Integration
- SM_Integration

Note:

- ▶ The name of the license file is `ucmdb_license.xml`.
 - ▶ You are asked for the location of the license file during installation. The default location of the Basic license is: **<Business Service Management root directory>\mam_lib\server** on the Data Processing server machine.
 - ▶ Two weeks before the license expires, a reminder message is displayed for you to renew the license.
-

Data Flow Probe Licensing

You should install the Data Flow Probe, no matter which license you are running. If you have the Foundation license, the Probe is needed to run the Integration jobs (NNMi, SE, and DDMi). For details, see “Data Flow Probe Installation” on page 39.

Tasks

Upgrade to the Integration or DDM Advanced License

When you install Business Service Management, you receive the Universal CMDB Foundation license. To obtain the file needed to upgrade to the Integration or DDM Advanced license, contact HP Software Support, then perform the following procedure:

To upgrade your license:

- 1** Obtain the appropriate file from HP Software Support.
- 2** Replace the `ucmdb_license.xml` file in the `<Business Service Management root directory>\mam_lib\server` folder on the Data Processing server machine.

If Business Service Management is installed in a distributed deployment, replace the file on the Gateway Server machine.

- 3** Use the JMX console to force a license change:
 - a** Launch the Web browser and enter the server address, as follows:
`http://<BSM Server Host Name or IP>:21212/jmx-console`.
 - b** When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
 - c** Under CMDB, click `service=UCMDB UI` to open the JMX MBEAN View page.
 - d** Locate `getLicenseForCustomer` and enter the following information:
In the force parameter box, select **True**.
In the ParamValue box for the parameter `customerId`, enter **1**.
Click **Invoke**.

Note: To verify the type of license that is installed, select **False** and enter the customer ID. Details about the license are displayed.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for ODB licensing.

- ▶ **Problem:** When integrating ODB with HP Storage Essentials, unable to run the **SE Integration by SQL** job with the Foundation license.

Solution: Perform the procedure in “Discover the SE Oracle Database” in *ODB Discovery and Integration Content Guide* PDF.

- ▶ **Problem:** When integrating ODB with HP Network Node Manager (NNMi), unable to run the **Layer2 by NNM** job with the Foundation license.

Solution: For details, see “Network Node Manager i (NNMi) Integration with HP Business Service Management” in *ODB Discovery and Integration Content Guide* PDF.

3

Data Flow Probe Installation

This chapter includes:

Tasks

- ▶ Install the Data Flow Probe on page 40
- ▶ Upgrade the Probe on page 51
- ▶ Run Probe Manager and Probe Gateway on Separate Machines on page 51
- ▶ Configure the Probe Manager and Probe Gateway Components on page 52
- ▶ Connect a Data Flow Probe to a Non-Default Customer on page 53

Reference

- ▶ Data Flow Probe Installation Requirements on page 54

Tasks

Install the Data Flow Probe

The following procedure explains how to install the Data Flow Probe on a Windows platform.

The Probe can be installed before or after you install the Business Service Management Gateway server. However, during Probe installation you must provide the server name, so it is preferable to install the server before installing the Probe.

Verify that you have enough hard disk space available before beginning installation. For details, see “Data Flow Probe Installation Requirements” on page 54.

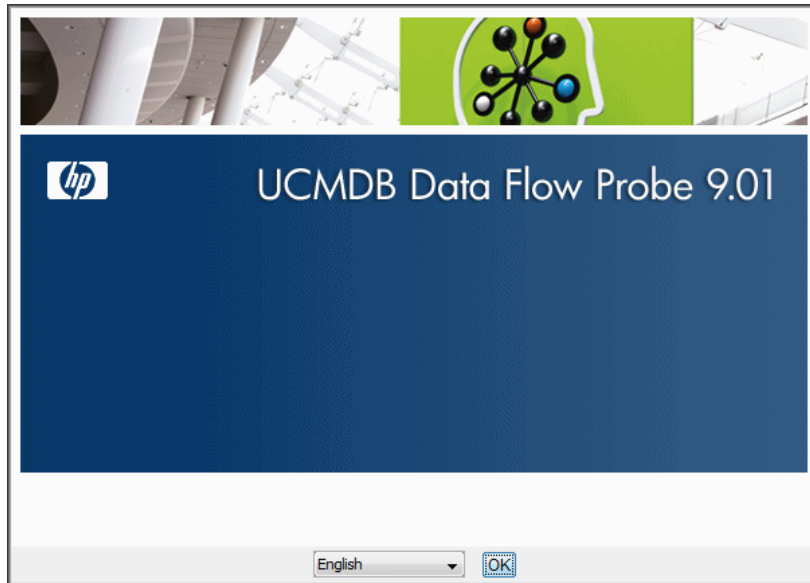
It is recommended to install the Probe on a separate server from the BSM servers, to distribute the overall system load.

To install the ODB Data Flow Probe:

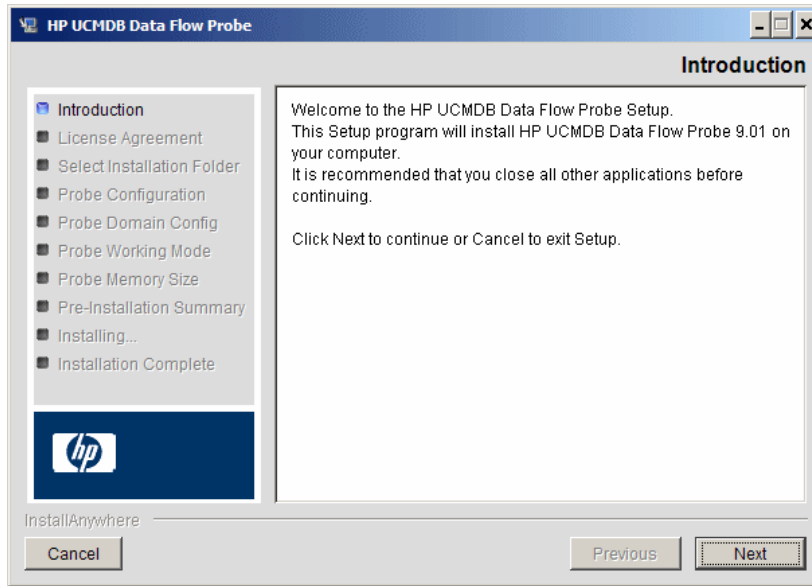
- 1 Select **Admin > Platform > Setup and Maintenance > Downloads**.

Note: The ODB Data Flow Probe link in the Downloads page is displayed only if you have purchased a license for Data Flow Management, and if the administrator has added the Probe link to the Downloads page. For details, see “Installing Component Setup Files” in the *HP Business Service Management Deployment Guide* PDF.

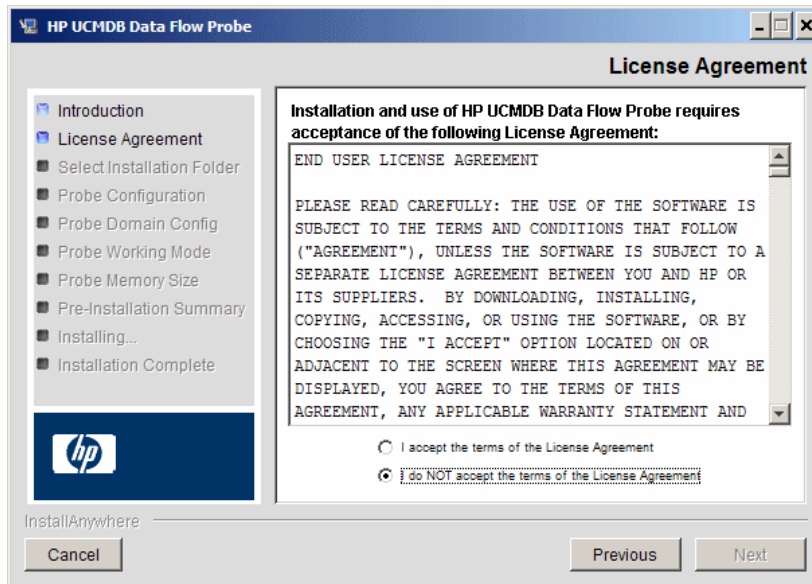
- 2 Click the **HPUCMDB_DataFlowProbe_901.exe** link. You can open the Setup file or save it to your computer:
 - If you choose to open the file, it is not saved to your computer, and the setup program starts immediately. In this case, depending on your browser security settings, a security warning dialog box may open. Confirm that you want to proceed.
 - If you choose to save the file to your computer, double-click the downloaded file to begin installation.



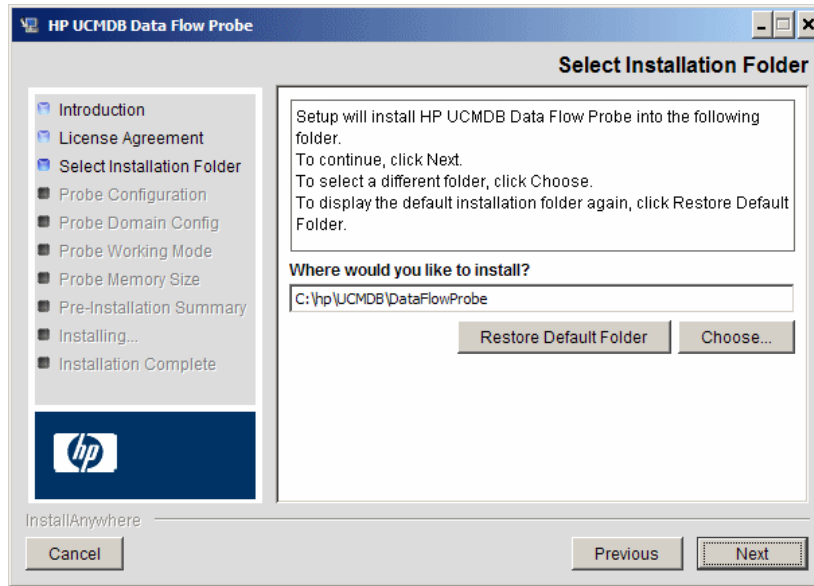
- 3 Choose the locale language and click **OK** to open the Introduction dialog box.



- 4 Click **Next** to continue to the License Agreement.



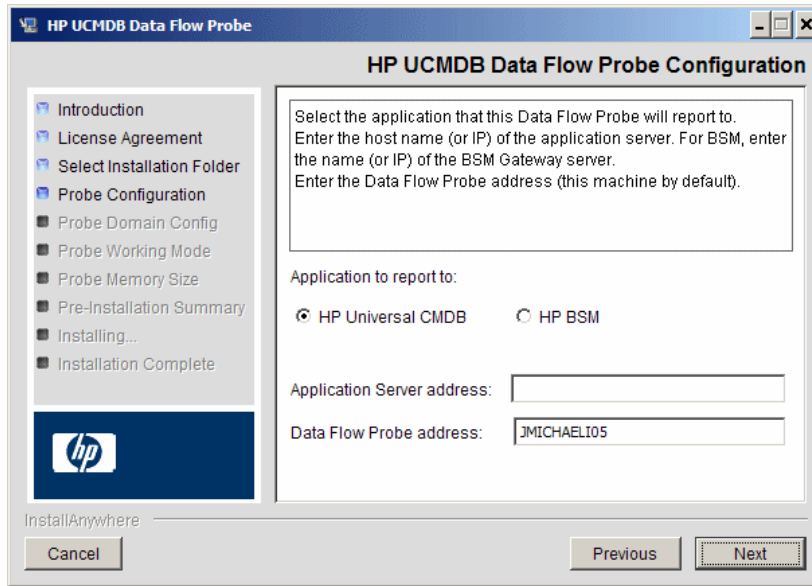
- 5 Accept the terms of the agreement and click **Next** to open the Select Installation Folder dialog box.



- 6 Accept the default entry or click **Choose** to display a standard Browse dialog box. To install to a different directory, browse to and select the installation folder.

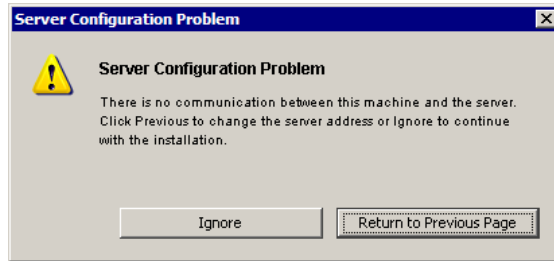
Note: To restore the default installation directory, after selecting a directory in the Browse dialog box, click **Restore Default Folder**.

- 7 Click **Next** to open the HP UCMDB Data Flow Probe Configuration dialog box.

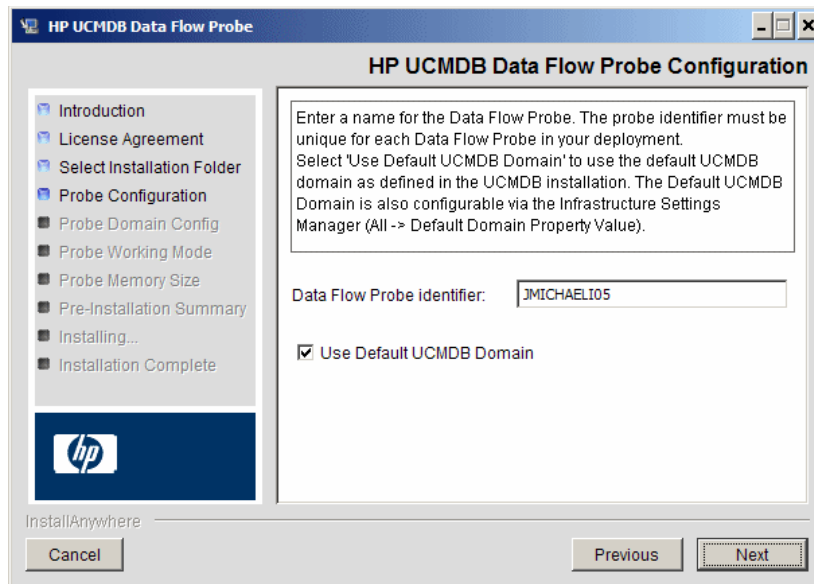


- **Application to report to.** Choose the application server with which you are working. You can use the Probe with either HP Universal CMDB or Business Service Management.
 - If you select **HP Universal CMDB**, in the **Application Server address** box, enter the name or the IP address of the HP Universal CMDB server to which the Probe is to be connected.
 - If you select **HP BSM**, in the **Application Server address** box, enter the IP or the DNS name of the Gateway Server.
- In the **Data Flow Probe address** box, enter the IP address or the DNS name of the machine on which you are currently installing the Probe, or accept the default.

- 8 If you do not enter the address of the application server, a message is displayed. You can choose to continue to install the Probe without entering the address, or to return to the previous page and add the address.



- 9 Click **Next** to open the HP UCMDB Data Flow Probe Configuration dialog box.



- In the **Data Flow Probe Identifier** box, enter a name for the Probe that will be used to identify it in your environment. This is the name that will appear in the user interface.

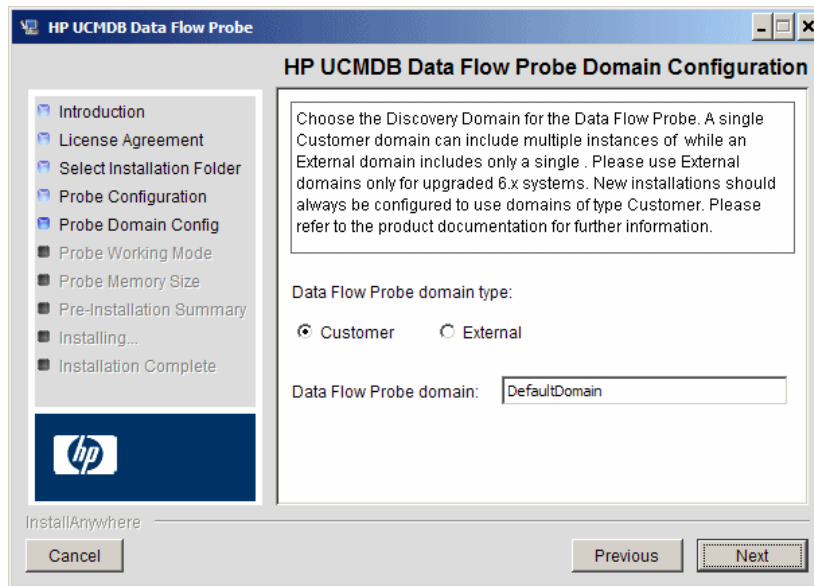
Important:

- ▶ The ODB Probe identifier must be unique for each Probe in your deployment.
 - ▶ When installing the Probe in separate mode, that is, the Probe Gateway and Probe Manager are installed on separate machines, you must give the same name to the Probe Gateway and all its Managers. This name appears in ODB as a single Probe node.
-

- ▶ Select **Use Default CMDB Domain** to use the default BSM IP address or machine name, as defined in the BSM Server installation.

The Default UCMDB Domain is also configurable via the Infrastructure Settings Manager, available after installing Business Service Management (**Admin > Platform > Setup and Maintenance > Infrastructure Settings > Foundations > ODB > Class Model Settings > Default Domain Property Value**).

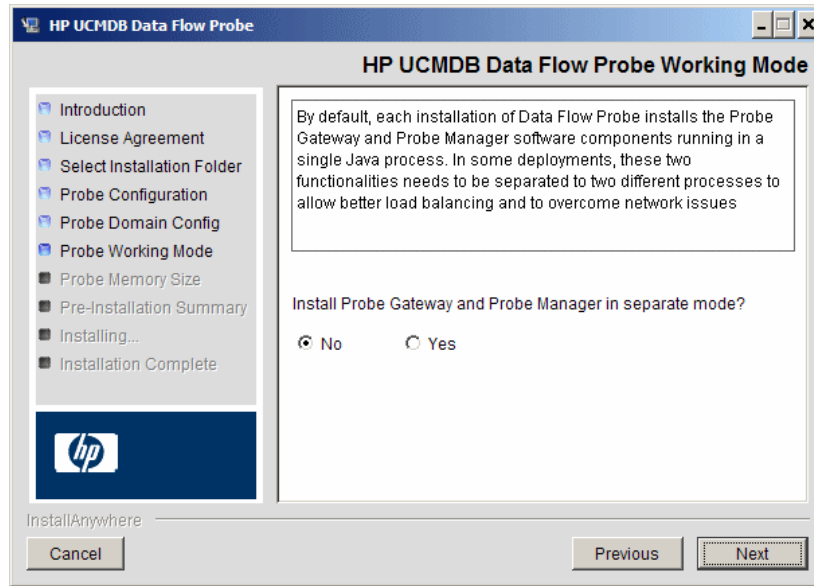
- 10** Click **Next**. If you cleared the **Use Default CMDB Domain** box in the HP UCMDB Data Flow Probe Configuration dialog box, the HP UCMDB Data Flow Probe Configuration Domain Configuration dialog box appears.



- **Data Flow Probe domain type.** Choose between **Customer** and **External**, depending on the type of domain on which the Probe is to be running:
 - **Customer.** Select if you are installing one or more Probes in your deployment.
 - **External.** Select if you are upgrading from version 6.x systems.

Important: For new installations, always select **Customer**.
- **Data Flow Probe domain:** If you are not using the default domain defined in ODB, enter the name of the domain here.

- 11 Click **Next** to open the HP UCMDB Data Flow Probe Working Mode dialog box.

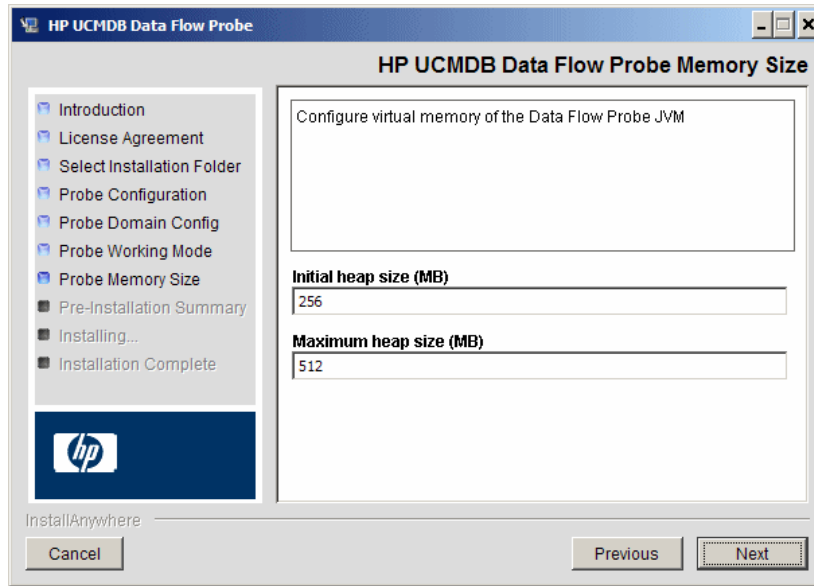


You can run the Probe Gateway and Manager as one Java process or as separate processes. You would probably run them as separate processes in deployments that need better load balancing and to overcome network issues.

Click **No** to run Probe Gateway and Probe Manager as one process.

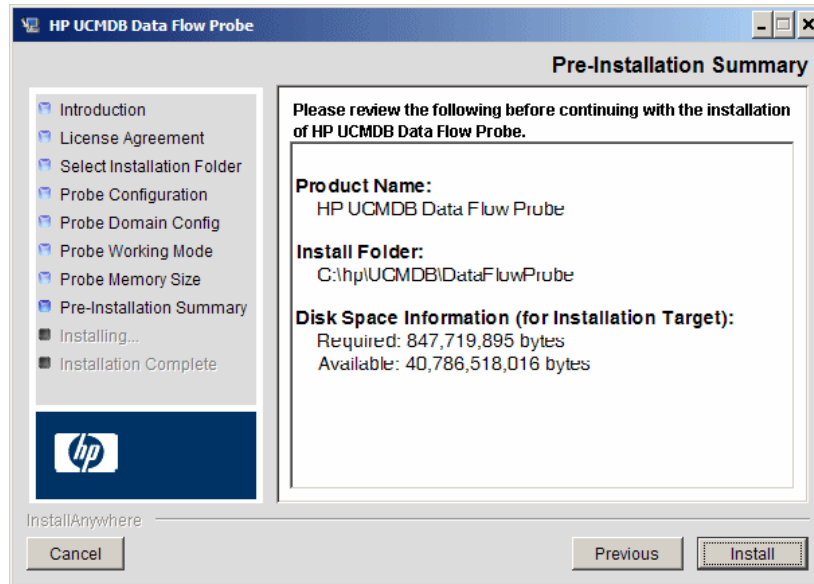
Click **Yes** to run Probe Gateway and Probe Manager as two processes. For details on the procedure, see “Run Probe Manager and Probe Gateway on Separate Machines” on page 51.

- Click **Next** to open the HP UCMDB Data Flow Probe Memory Size dialog box.



Define the minimum and maximum memory to be allocated to the Probe. The values are measured in megabytes.

- 13 Click **Next** to open the Pre-Installation Summary dialog box and review the selections you have made.



- 14 Click **Install** to complete the installation of the Probe. When the installation is complete the Install Complete page is displayed.

Any errors occurring during installation are written to the following file:
C:\hp\UCMDB\DataFlowProbe\HP_UCMDB_Data_Flow_Probe_Install Log.log.

- 15 Click **Done**. The following shortcut is added to the Windows **Start** menu:
Programs > HP UCMDB > Start Data Flow Probe

- 16 Activate the Probe by selecting the shortcut.

You can run the Probe in a console. For details, see “Launch the Probe in a Console” in the *ODB Data Flow Management Guide*.

The Probe is displayed in Business Service Management: access **Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup**. For details see “Data Flow Probe Installation Requirements” on page 54.

Upgrade the Probe

This task describes how to upgrade the ODB Data Flow Probe.

1 Uninstall the Old Probe

Uninstall all existing Probes. If a Probe is running, stop it before you uninstall it.

2 Install the New Probe

You should install the new Probe with the same configuration, that is, use the same Probe ID, domain name, and server name as for the previous Probe installation.

Run Probe Manager and Probe Gateway on Separate Machines

During installation, you can choose to separate the Probe Manager and Probe Gateway processes so that they run on separate machines. You must:

- 1 Install the Probe on both machines according to the procedure in “Install the Data Flow Probe” on page 40.

When installing the Probe in separate mode, that is, the Probe Gateway and Probe Manager are installed on separate machines, you must give the same name to the Probe Gateway and all its Managers. You name the Probe during installation in the **Data Flow Probe Identifier** box in the **HP UCMDB Data Flow Probe Configuration** dialog box. For details, see step 9 on page 45.

This name appears in ODB as a single Probe node. Failure to give the same name may prevent jobs from running.

- 2 Choose **Yes** in step 11 on page 48.
- 3 Perform the configuration in “Configure the Probe Manager and Probe Gateway Components” on page 52.

Configure the Probe Manager and Probe Gateway Components

This section explains how to set up the Probe when the Probe Manager and Probe Gateway run as separate processes on two machines.

This section includes the following topics:

- “Set Up the Probe Gateway Machine” on page 52
- “Set Up the Probe Manager Machine” on page 52
- “Start the Services” on page 53

1 Set Up the Probe Gateway Machine

Open the following file:

C:\hp\UCMDB\DataFlowProbe\conf\probeMgrList.xml.

- a** Locate the line beginning `<probeMgr ip=` and add the Manager machine name or IP address, for example:

```
<probeMgr ip="OLYMPICS08">
```

- b** Open the following file:

C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties

- c** Locate the lines beginning `appilog.collectors.local.ip =` and `appilog.collectors.probe.ip =` and enter the Gateway machine name or IP address, for example:

```
appilog.collectors.local.ip = STARS01  
appilog.collectors.probe.ip = STARS01
```

2 Set Up the Probe Manager Machine

- a** In **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties**, locate the line beginning `appilog.collectors.local.ip =` and enter the Manager machine name or IP address, for example:

```
appilog.collectors.local.ip = OLYMPICS08
```

- b** Locate the line beginning **appilog.collectors.probe.ip =** and enter the Gateway machine name in uppercase, for example:

```
appilog.collectors.probe.ip = STARS01
```

3 Start the Services

- a** On the Probe Manager machine start the Manager: **Start > Programs > UCMBDB > Start Data Flow Probe Manager.**
- b** On the Probe Gateway machine start the Gateway: **Start > Programs > UCMBDB > Start Data Flow Probe Gateway.**

Connect a Data Flow Probe to a Non-Default Customer

You can connect a Data Flow Probe to a customer that is not the default. The default customer ID is 1.

- 1** Open the following file in a text editor:
`C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties.`
- 2** Locate the **customerID** entry.
- 3** Update the value with the customer ID, for example, **customerID = 2.**
- 4** Restart the Probe so that it is updated with your changes.

Reference

Data Flow Probe Installation Requirements

Hardware Requirements

Computer/processor	Windows: Pentium IV 2.4 GHz or later processor
Memory	Windows: Minimum 1 GB RAM (Recommended: 2 GB RAM)
Virtual memory (for Windows deployment)	Minimum 2 GB Note: The virtual memory size should always be at least twice the physical memory size.
Free hard disk space	Windows: Minimum 4 GB (at least 4 GB for database software and data files) (Recommended: 20 GB hard disk)
Display	Windows: Color palette setting of at least 256 colors (32,000 colors recommended)

Software Requirements

Platform	OS Version and Edition	Supported	Recommended
32-bit x86/x64	Windows 2008 Standard/Enterprise editions, SP2 and R2	Yes	Yes
32-bit x86/x64	Windows 2003 Standard/Enterprise editions, SP2 and R2 SP2	Yes	
Any	Windows 7 Professional/Enterprise	No	
Any	Windows 2000	No	

Virtual Environment Requirements

Platform	OS Version and Edition	Supported	Recommended
VMware ESX 3.x	<ul style="list-style-type: none"> ▶ Windows 2003 Standard/Enterprise editions SP2 and R2 SP2 ▶ Windows 2008 Standard/Enterprise SP2 and R2 	Yes	
VMware ESX 4.0	<ul style="list-style-type: none"> ▶ Windows 2003 Standard/Enterprise editions SP2 and R2 SP2 ▶ Windows 2008 Standard/Enterprise SP2 and R2 	Yes	Yes
Pre ESX 3.5 (like 3.0.x versions)	<ul style="list-style-type: none"> ▶ May not provide adequate performance ▶ Does not support Windows 2008 or Windows 7 	No	
ESXi VMware	All platforms	No	
MS Hyper-V	Server 2008 v1 and R2	No	
Xen Hypervisor 3.x	All platforms	No	

Part II

Data Flow Management Setup

4

Data Flow Probe Setup

This chapter includes:

Concepts

- ▶ Job Execution Policies on page 60
- ▶ Data Validation on the Data Flow Probe on page 62
- ▶ Filtering Results on page 63

Tasks

- ▶ Get Started With the ODB Data Flow Probe on page 64
- ▶ Add a Data Flow Probe on page 65
- ▶ Delete Unsent Probe Results on page 67

Reference

- ▶ Data Flow Probe Setup User Interface on page 68
- ▶ Domain Credential References on page 83
- ▶ Data Flow Probe Log Files on page 106
- ▶ The DiscoveryProbe.properties File on page 110

Troubleshooting and Limitations on page 111

Concepts






Job Execution Policies

You can define periods of time when a Probe must not run. You can choose to disable specific jobs running on any Probe or all jobs running on a specific Probe. You can also exclude jobs from a job execution policy so that they continue running as usual.

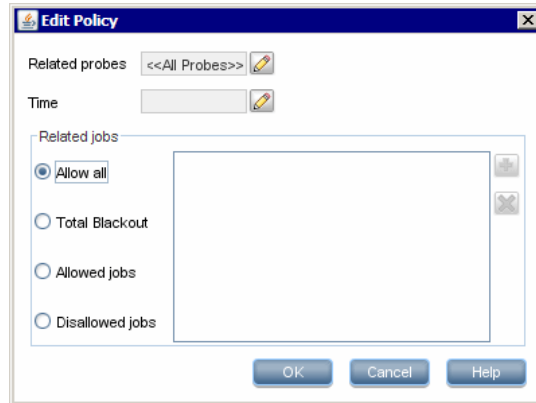
For details on defining a job execution policy, see "Add/Edit Policy Dialog Box" on page 71.

Example of Policy Ordering

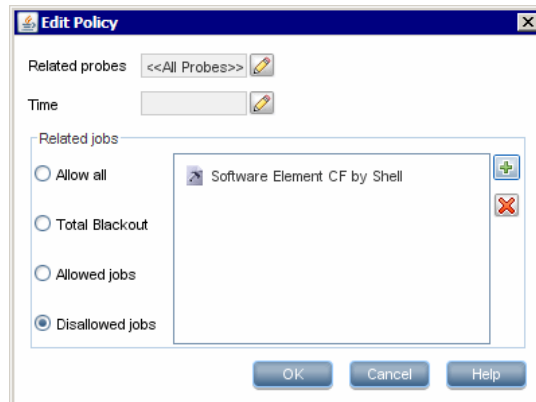
There are two policies, **Total TCP Blackout** and **Always**. **Total TCP Blackout** does not allow any TCP discovery jobs to run. The policies appear in the list as follows:

Job Execution Policy		
    		
Time	Probes	Jobs
Total TCP Blackout	All	[IP Traffic by Network Data, Col
Always	All	All

A job (Class C IPs by ICMP) starts running. It checks the policies in the policy list from top to bottom. It starts by checking **Total TCP Blackout**. The job does not appear in this policy, so it continues down the list and checks **Always**. The job does appear here (**Allow All** is selected in the Edit Policy dialog box) so the job runs:



The next job (Software Element CF by Shell) starts running. It checks the policies in the policy list from top to bottom. It starts by checking **Total TCP Blackout**. The job appears in this policy (**Disallowed Jobs** is selected in the Edit Policy dialog box), so the job does not run:



Caution: If a job is not connected to any policy, it does not run. To run these jobs, set the last policy in the list to **Allow All**.

Running Jobs When a Job Execution Policy Is Running

If a policy begins to operate while a Probe is executing a job, the job pauses. When the policy finishes, the job continues to run from where it ceased. For example, say a job contains 10,000 Trigger CIs. The job finishes working on 7,000 of them and then the policy starts to operate. When the job continues (after the policy finishes), it works on the remaining 3,000 Trigger CIs—the job does not start running from the beginning.

Data Validation on the Data Flow Probe

The CIT model resides on the Data Flow Probe (as well as in the CMDB). This enables data validation to take place on the Probe when receiving data from services. Problems are generated for a specific Trigger CI and displayed to the user.

The following validation takes place on the Probe:

- ▶ The CIT of the CI is compared to that in the CIT model.
- ▶ The CI is checked to verify that all key attributes are present (on condition that the `CmdbObjectId` attribute is not defined).
- ▶ The CI's attributes are checked to verify that they are all defined in the CIT.
- ▶ The CI's attributes of type `STRING` are checked to verify that they do not exceed the size limit. If an attribute is longer than the limit, DFM checks whether an `AUTO_TRUNCATE` qualifier is defined for the attribute. If there is a qualifier, the value is truncated and a warning message is written to the Probe `error.log` file.

All invalid attributes raise an error, which reports on a specific CI. When the Probe finds invalid data that is related to the CITs, all data that the Probe has collected on that CI is dropped by the Probe and is not sent to the server.

For details on attributes, see "CI Type Attributes" in the *Modeling Guide*.

Filtering Results

You can filter results sent by the Probe to the HP Business Service Management Gateway server. You would probably need to filter irrelevant data regularly during production runs and specifically when you are testing a limited environment.

There are two levels of filtering: adapter filtering and global filtering:

- ▶ **Adapter filtering.** The Data Flow Probe filters the results for a specific adapter and sends to the CMDB only those filtered CIs. You define an adapter filter in the Results Management Pane in the Adapter Management tab. For details, see "Adapter Management Tab" on page 150.
- ▶ **Global filtering.** DFM filters the results of all jobs running on a Probe. You define global filters in the `globalFiltering.xml` file. For details, see "globalFiltering.xml" on page 139.

The order of filtering is as follows: during a run, the Data Flow Probe first searches for an adapter filter and applies the filter to the results of the run. If there are no adapter filters, DFM searches for a global filter and applies that filter to the results. If DFM finds no filters, all results are sent to the server.

Tasks

Get Started With the ODB Data Flow Probe

This section explains how to install and launch the Data Flow Probe.

Note:

- The Probe link in the Downloads page is displayed only if you have purchased a license for the DFM application.
 - The managed environment is defined by the IP ranges of the domains. However, with some discovery adapters it is possible to override this behavior and discover CIs that are out of a Probe's range.
-

This task includes the following steps:

- "Install the Probe" on page 64
- "Launch the Probe from the Start Menu" on page 64
- "Launch the Probe in a Console" on page 65
- "Run Discovery" on page 65
- "Stop the Probe" on page 65

Install the Probe

For details, see "Data Flow Probe Installation" on page 39.

Launch the Probe from the Start Menu

On the machine on which the Probe is installed, select **Start > Programs > HP UCMDB > Start Data Flow Probe**. The Probe is started as a service.

To verify that the Probe has been launched successfully, in Business Service Management select **Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup**. Select the Probe and, in the Details pane, verify that the status is **connected**.

Launch the Probe in a Console

You can configure the Probe so that it opens in a console. In this case, the command prompt window is displayed. Execute the following script:
C:\hp\UCMDB\DataFlowProbe\bin\gateway.bat console.

Note: The user running the Probe service must be a member of the Administrators group.

Run Discovery

For details, see "Discovery Control Panel Overview" on page 240.

Stop the Probe

- To stop the Probe when it is running in a command prompt window (the console), press CTRL+C, then **y**.
- To stop the Probe when it is running as a service, select **Start > Programs > HP UCMDB > Stop Data Flow Probe**.

Add a Data Flow Probe

This task describes how to add a Probe to BSM.

This task includes the following steps:

- "Prerequisites" on page 66
- "Add a Domain to ODB" on page 66
- "Add a Probe to the New Domain" on page 66

- "Add Further Probes to the Domain – Optional" on page 66
- "Define Credentials" on page 67

1 Prerequisites

Verify that the Probe is installed and make a note of its IP address.

2 Add a Domain to ODB

In this step, you create the domain for the new Probe. When you start the Probe, it connects to ODB automatically. To verify, select **Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup**. Select the Probe and, in the Details pane, verify that the status is **connected**.

To define Probe ranges before the Probe has connected for the first time, you must define them manually. For details, see "Add/Edit IP Range Dialog Box" on page 69.

- a** Access the Probe configuration window: **Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup**.
- b** Select **Domains and Probes** and click the **Add Domain or Probe** button to open the Add New Domain dialog box. For details, see "Add New Domain Dialog Box" on page 72.

3 Add a Probe to the New Domain

In this step, you define the Probe and its range.

- a** Double-click the new domain and select the **Probes** folder.
- b** Click the **Add Domain or Probe** button to open the Add New Probe dialog box. For details, see "Add New Probe Dialog Box" on page 73.
- c** Select the new probe and define its IP range. For details, see "Add/Edit IP Range Dialog Box" on page 69.

4 Add Further Probes to the Domain – Optional

You can add more probes to this domain. For details, see the previous steps.

5 Define Credentials

You configure credentials depending on what must be discovered and which protocols are supported on your site's network.

For details, see "Details Pane" on page 76. For a list of protocols, see "Domain Credential References" on page 83.

Delete Unsent Probe Results

This task describes how to empty the Probe queue that contains results that have not yet been transmitted to the ODB Server.

- 1 Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: **http://<Probe Gateway machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

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

Note: If you have not created a user, use the default user name **admin** and the password **admin** to log in.

- 2 Locate the **Probe_<Probe Name> > type=MainProbe** service and click the link to open the JMX MBEAN View page.
- 3 Invoke the operation by clicking the **dropUnsentResults** button.

Reference

Data Flow Probe Setup User Interface

This section describes:




- ▶ Add/Edit IP Range Dialog Box on page 69
- ▶ Add/Edit Policy Dialog Box on page 71
- ▶ Add New Domain Dialog Box on page 72
- ▶ Add New Probe Dialog Box on page 73
- ▶ Choose Discovery Jobs Dialog Box on page 74
- ▶ Data Flow Probe Setup Window on page 74
- ▶ Details Tab on page 75
- ▶ Domains and Probes Pane on page 79
- ▶ Edit Related Probes Dialog Box on page 81
- ▶ Edit Timetable Dialog Box on page 81
- ▶ Protocol Parameters Dialog Box on page 82
- ▶ Scope Definition Dialog Box on page 82
- ▶ Selecting Probes on page 83

Add/Edit IP Range Dialog Box

Enables you to set the network range for discovery. The results are retrieved from the addresses in the range you define. You can also define IP addresses that must be excluded from a range.

To access	Select the required Probe in the Domains and Probes pane and then click the Add IP range button in the Ranges pane (Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup > Details pane).
Important information	If you define a range that is out of the scope of the network on which the Probe is installed, a warning message informs you that the Probe is not included in the range. Answer Yes to save the current range without including the Probe in the range. Answer No to continue editing without saving the current range.
Relevant tasks	"Discovery Control Panel – Advanced Mode Workflow" on page 247

User interface elements are described below:

GUI Element (A–Z)	Description
	To exclude an IP range from discovery, click the Add IP range button.
	To delete the excluded part of an IP range, select the excluded range and click the Remove IP range button.
	To edit the excluded part of an IP range, click the Edit IP range button. For details, see Exclude Ranges.

GUI Element (A-Z)	Description
<p>Exclude Ranges</p>	<p>Click the Add IP range or Edit IP range button to open the Add IP Pane Dialog box and then click Advanced to exclude part of a range. In the Exclude IP Range dialog box, enter the range to exclude.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ You must enter a range (in the Add/Edit IP Range dialog box) before you can enter the excluded range. ▶ The rules for entering an excluded range are the same as for entering a range. For details, see Range. ▶ Use this feature to divide a network range into several subranges. For example, say a range is 10.0.64.0 – 10.0.64.255. You define three excluded ranges: 10.0.64.45 – 10.0.64.50 10.0.64.65 – 10.0.64.70 10.0.64.89 – 10.0.64.95 Therefore, the ranges to be discovered are: 10.0.64.0 – 10.0.64.44 10.0.64.51 – 10.0.64.64 10.0.64.71 – 10.0.64.88 10.0.64.96 – 10.0.64.255



GUI Element (A–Z)	Description
Range	<p>The rules for defining an IP address range are as follows:</p> <ul style="list-style-type: none"> ▶ The IP address range must have the following format: start_ip_address – end_ip_address For example: 10.0.64.0 - 10.0.64.57 ▶ The range can include an asterisk (*), representing any number in the range of 0-255. ▶ If you use an asterisk, you do not need to enter a second IP address. For example, you can enter the range pattern 10.0.48.* to cover the range from 10.0.48.0 to 10.0.48.255. ▶ Use an asterisk in the lower bound IP address of the IP range pattern only. (If you use an asterisk in the lower bound IP address and also enter an upper bound IP address, the upper bound IP address is ignored.) ▶ You can use more than one asterisk (*) in an IP address as long as they are used consecutively. The asterisks cannot be situated between two numbers in the IP address, nor can they be substituted for the first digit in the number. For example, you can enter 10.0.*.* but not 10.*.64.*. ▶ Two Probes in the same domain cannot have the same IP address in their range.

Add/Edit Policy Dialog Box

Enables you to add a job execution policy, to disable jobs from running at specific times.

To access	Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup > Details pane > Job Execution Policy section. Select an existing policy and click Edit , or click the Add button.
See also	<p>"Job Execution Policies" on page 60</p> <p>"Job Execution Policy Pane" on page 77</p> <p>"Domain Credential References" on page 83</p>

User interface elements are described below:

GUI Element (A–Z)	Description
Related jobs	<ul style="list-style-type: none"> ➤ Allow all. Run the job execution policy on all jobs. ➤ Total blackout. The policy does not run on any jobs. ➤ Allowed jobs. Choose jobs to run even during the configured blackout time. ➤ Disallowed jobs. Choose jobs that do not run during the configured blackout time. <p>For allowed and disallowed jobs, click the Add job or Remove job button to choose specific jobs to be included in, or excluded from, the policy. If you click the Add job button, the Choose Discovery Jobs dialog box opens.</p>
Related Probes 	The Probes on which to run the policy. Click the button to open the Edit Related Probes dialog box to define which Probes are included in the policy.
Time 	The date and time during which the policy is active. Click the button to open the Edit Timetable dialog box.

Add New Domain Dialog Box

Enables you to add a domain.

To access	Click the Add Domain or Probe button in the Domains and Probes pane.
Important information	In a version 8.01 or later environment that has been upgraded from version 6.x, to enable data to be modelled similarly as in the previous version, you must define the Probes as belonging to the External domain and not to the Customer domain.

User interface elements are described below:

GUI Element (A–Z)	Description
Description	Enter a description to appear in the Details pane of the Data Flow Probe Setup window.
Domain Type	<ul style="list-style-type: none"> ▶ Customer. A private domain used for your site. You can define several domains and each domain can include multiple Probes. Each Probe can include IP ranges but the customer domain itself has no range definition. ▶ External. Internet/public domain. A domain that is defined with a range. The external domain can contain only one Probe whose name equals the domain name. However, you can define several external domains in your system.
Name	Enter a unique name for the domain.


Add New Probe Dialog Box

Enables you to add a Probe.

To access	Click the Add Domain or Probe button in the Domains and Probes pane.
Important information	<ul style="list-style-type: none"> ▶ To add a Probe to an existing domain, select Probes in the Domains and Probes pane and click the Add Domain or Probe button. ▶ To add a Probe to a new domain, create a domain, then add the Probe to the domain. ▶ Two Probes in the same domain cannot have the same IP address in their range. ▶ When a Probe is activated, it is added automatically and its status changes to connected. For details, see "Launch the Probe from the Start Menu" on page 64 or "Launch the Probe in a Console" on page 65.

Choose Discovery Jobs Dialog Box

Enables you to choose the jobs that are to be added to, or excluded from, the job execution policy.

To access	Select Allowed Jobs or Disallowed jobs in the Edit Policy dialog box and click the button  .
------------------	---

User interface elements are described below:

GUI Element (A–Z)	Description
<Installed packages>	Locate the job to be included in, or excluded from, the policy. (Use the SHIFT or CTRL key to select several packages.)

Data Flow Probe Setup Window

Enables you to define a new domain or to define a new Probe for an existing domain. Also enables you to define the connection data for each protocol.

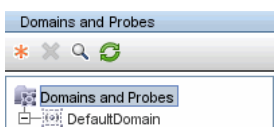
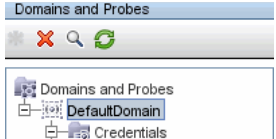
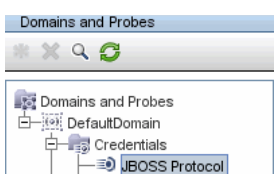
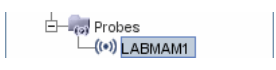
To access	Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup
Important information	<ul style="list-style-type: none"> ▶ For details on the Domains and Probes pane, see "Domains and Probes Pane" on page 79. ▶ For details on the Details pane, see "Details Tab" on page 75.
See also	"Domain Credential References" on page 83

Details Tab

Enables you to view the Probes running under all domains and to add an execution policy to jobs (that is, to schedule time periods when jobs should not run).





To access	Click an object in the Domains and Probes pane.
Important information	Depending on what you select in the Domains and Probes pane, different information is displayed in the Details tab. For details, see "Displayed Information" on page 75 in the next section.

Displayed Information

If You Select...	The Information Displayed Is...
 <p>The screenshot shows the "Domains and Probes" pane with a search icon and a refresh icon. The tree view shows "DefaultDomain" selected.</p>	<p>Domains and Probes. You can view details on all Probes and you can define and edit job execution policies. For details, see "Details Pane" on page 77 and "Job Execution Policy Pane" on page 77.</p>
 <p>The screenshot shows the "Domains and Probes" pane with a search icon and a refresh icon. The tree view shows "DefaultDomain" expanded, with "Credentials" selected.</p>	<p>A specific domain. You can add a description and view a list of Probes running in that domain. For details, see "Details Pane" on page 77 and "Description Pane" on page 76.</p>
 <p>The screenshot shows the "Domains and Probes" pane with a search icon and a refresh icon. The tree view shows "DefaultDomain" expanded, with "Credentials" expanded, and "JBOSS Protocol" selected.</p>	<p>A specific protocol. You can add protocol parameters and you can view details on the protocol, including user credentials. For details, see "Details Pane" on page 76 and "Domain Credential References" on page 83.</p>
 <p>The screenshot shows the "Probes" pane with a search icon and a refresh icon. The tree view shows "LABMAM1" selected.</p>	<p>A specific Probe. You can view details on the Probe, including range information. You can also add ranges to, or exclude ranges from, the Probe, and you can remove a Probe from ODB. For details, see "Ranges Pane" on page 78, "Details Pane" on page 77, and "Data Flow Probes Pane" on page 76.</p>

Details Pane

This pane is displayed if you select a specific protocol. User interface elements are described below:

GUI Element (A-Z)	Description
	Add new connection details for selected protocol type.
	Remove a protocol.
	Click to edit a protocol. For details, see "Protocol Parameters Dialog Box" on page 82.
	Click a button to move a protocol up or down to set the order in which credential sets are attempted. DFM executes all the protocols in the list with the first protocol taking priority.
Protocol	Click to view details on the protocol, including user credentials.

Description Pane

User interface elements are described below:

GUI Element (A-Z)	Description
Description	The description that was entered during domain creation.
Domain Type	For details, see Domain Type in "Add New Domain Dialog Box" on page 72.

Data Flow Probes Pane

Enables you to view a list of all Probes connected to the server.

To access	Click Domains and Probes or a domain.
------------------	--

User interface elements are described below:

GUI Element (A–Z)	Description
IP	The IP range defined during Probe creation.
Last Access Time	The last time that the Probe requested tasks from the server.
Name	The Probe name as it appears in DFM.
Status	<ul style="list-style-type: none"> ▶ Connected. The Probe has successfully connected to the server (the Probe connects every few seconds). ▶ Disconnected. The Probe is not connected to the server.

Details Pane

User interface elements are described below:





GUI Element (A–Z)	Description
Last time probe accessed	The last time that the Probe was accessed on the server machine.
Probe IPs	The IP of the Probe machine.
Status	<ul style="list-style-type: none"> ▶ Connected. The Probe has successfully connected to the server (the Probe connects every few seconds). ▶ Disconnected. The Probe is not connected to the server.

Job Execution Policy Pane

Enables you to configure the periods of time when jobs should not run.

To access	Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup. Select Domains and Probes.
Important information	Jobs that have a listening functionality (that is, they do not perform discovery, for example, they listen to SNMP traps) are not included in a policy.
See also	"Job Execution Policies" on page 60 "Domain Credential References" on page 83

User interface elements are described below:




GUI Element (A–Z)	Description
	Move the policy up or down. DFM executes all the policies in the list with the first policy taking priority. If a job is included in two policies, DFM executes the first policy only for that job.
	Add a policy.
	Remove a policy.
	Edit a policy. Click to open the Edit Policy dialog box.
Jobs	The jobs that are affected by the policy.
Probes	The Probes that are affected by the policy.
Time	The schedule of the policy.



Ranges Pane

Enables you to add and remove ranges that a Probe should work with.

To access	Click a Probe in the Domains and Probes pane.
Important Information	For details on searching for a specific range, locate the Find Probe Range by IP button in "Domains and Probes Pane" on page 79.

User interface elements are described below:


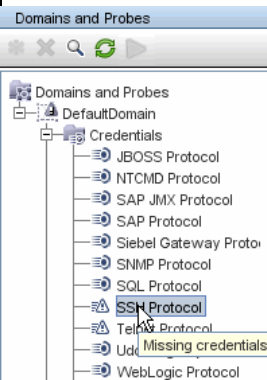
GUI Element (A–Z)	Description
	Click to open the Add IP Range dialog box.
	Click a range and click the button to remove a range from the list.
	Click to open the Edit IP Range dialog box.

GUI Element (A–Z)	Description
	Export a permission object in Excel, PDF, RTF, CSV, or XML format. For details, see "Browse Views Mode" in the <i>Modeling Guide</i> .
	Click to import ranges from a CSV file. Before using this feature, verify that the imported file is a valid CSV file, and that the ranges in the file do not conflict with existing ranges (that is, there are no duplicate or overriding ranges).
Excluded	Displays the IP addresses that have been excluded from the range that the Probe uses to discover CIs. For details, see "Add/Edit IP Range Dialog Box" on page 69.
Range	The network IP addresses that the Probe uses to discover CIs. For details, see "Add/Edit IP Range Dialog Box" on page 69.






Domains and Probes Pane

Enables you to view, define, or edit a domain, a Probe, or a Probe's credentials.

To access	Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup
------------------	---


<p>Important Information</p>	<p>A missing credential is represented by an icon , as shown in the following image:</p> 
<p>See also</p>	<p>"Job Execution Policies" on page 60</p>

User interface elements are described below:

GUI Element (A–Z)	Description
	<p>Adds a domain or Probe, depending on what is selected.</p>
	<p>Deletes a domain or Probe, depending on what is selected.</p>
	<p>Find Probe Range by IP button. If a Probe has many ranges defined for it, you can locate a specific range: select the Probe and click the button. In the Find Probe Range dialog box, enter the IP address and click the Find button. DFM highlights the range in the Ranges pane.</p>
	<p>Updates all domain and Probe information.</p>
	<p>Suspend probe. Click to disconnect the Probe from the BSM Server. The button changes to a Play button. To reconnect the Probe, click the button again.</p>


Edit Related Probes Dialog Box

Enables you to select specific Probes.

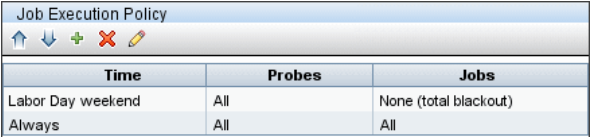
To access	 Click the Related Probes button in the Edit Policy dialog box.
See also	"Job Execution Policies" on page 60

Edit Timetable Dialog Box

Enables you to set the times when a Probe must run a job execution policy.

To access	 Click the Edit button in the Edit Policy dialog box.
See also	"Add/Edit Policy Dialog Box" on page 71

User interface elements are described below:

GUI Element (A–Z)	Description
Description	<p>Add a description of the specific policy. This field is mandatory.</p> <p>Tip: The text you enter here appears in the Time box in the Job Execution Policy pane, so it is recommended that the description be informative:</p> 
Time Definition	<p>Click a cell for a day and time to be included in the policy. To add more than one time unit, drag the pointer over the cells.</p> <p>Note: To clear a time unit, click the cell a second time.</p>

Protocol Parameters Dialog Box

Displays the attributes that can be defined for a protocol.

To access	Admin > ODB Administration > Data Flow Management > Data Flow Probe Setup > Domains and Probes > Domain > Credentials , select a protocol and click the Add or Edit button.
Important Information	For the description of each protocol, see "Domain Credential References" on page 83.

Scope Definition Dialog Box

Enables you to set the range that a protocol must discover.



To access	Click the Edit button in the Protocol Parameters dialog box.
------------------	---

User interface elements are described below:

GUI Element (A–Z)	Description
Selected Probes	To select specific Probes whose IP range must be changed, click Edit . For details, see "Choose Probe Dialog Box" on page 273.
Selected Ranges	<ul style="list-style-type: none"> ➤ All. The protocol runs discovery on all ranges for the domain. ➤ Selected Range. For the procedure to select a specific range on which the protocol runs discovery or to define an excluded range, see "Add/Edit IP Range Dialog Box" on page 69.

Selecting Probes

The Choose Probe to Filter, Edit Probe Limitations for Query Output, and Edit Related Probes dialog boxes include the following elements (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Add Selected Probe. Click to add a Probe to the Selected Probes column.
	Remove Selected Probe. Click to remove a Probe from the Selected Probes column.
All Data Flow Probes	<ul style="list-style-type: none"> ▶ Select to add all Probes in the Non-selected Probes list. ▶ Clear to add a specific Probe from the Non-selected Probes list.
Non-selected Probes	Probes that are not included in the policy/filter/limitations.
Selected Probes	Probes that are included in the policy/filter/limitations.

Domain Credential References

This section explains protocol credentials. You can edit credential attributes. For details, see "Protocol Parameters Dialog Box" on page 82.





Note: The following information can change from version to version: Changes in content implementation can cause protocol attributes to be updated.

This section includes the following topics:

- "Domains and Probes Pane GUI Elements" on page 84
- "Supported Agents" on page 86
- "Supported Protocols" on page 87

Domains and Probes Pane GUI Elements

When a protocol is selected in the Domains and Probes Pane, the following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to add new connection details, to open the Add Protocol Parameters dialog box.
	Select a protocol and click to remove connection details. Answer OK to the message.
	Select a protocol and click to edit connection details in the Protocol Parameters dialog box.
	<p>Select a protocol and click an arrow to move the protocol instance up or down.</p> <p>The order of the policies in the list defines which policy is checked first: a job starts running and checks the policy list from top to bottom. If the job name exists in a policy, the job runs. For details on adding jobs to a protocol, see "Add/Edit Policy Dialog Box" on page 71. For details on job execution policies, see "Example of Policy Ordering" on page 60.</p>

GUI Element (A-Z)	Description
<Right-click a credential>	<p>Choose from the following options:</p> <ul style="list-style-type: none"> ▶ Edit. Choose this option to enter protocol parameters, such as user name and password, that enable DFM to connect to an application on a remote machine. ▶ Edit using previous interface. Choose this option if: <ul style="list-style-type: none"> ▶ In a previous version of HP Business Service Management, you added parameters to this protocol that do not exist in this version. ▶ Values in this version cannot be deleted. For example, in this version you cannot configure SQL Protocol credentials with an empty port number. Select this option to open the previous Edit Protocol Parameter dialog box and delete the port number. ▶ Check credentials. In the box that opens, enter the IP address of the remote machine on which the protocol must run. The Probe attempts to connect to this IP and returns an answer as to whether the connection succeeded or not.
<Right-click a title>	<p>Choose from the following options:</p> <ul style="list-style-type: none"> ▶ Hide Column. Displayed when a column is shown. ▶ Show All Columns. Displayed when a column is hidden. ▶ Customize. Select to change the display order of the columns. ▶ Auto-resize Column. Select to change the column width to fit the contents.

All protocol credentials include the following parameters:

Parameter	Description
Index	Indicates the order in which protocol instances are used to make a connection attempt. The lower the index, the higher the priority. Default: 9999 . If you do not change the default, this protocol instance is used last.
Network Scope	To change the range that a protocol must discover or to select a Probe, click Edit . For details, see "Scope Definition Dialog Box" on page 82. Default: ALL .
User Label	Enter a label to help you identify a specific protocol credential, when you use it later. Enter a maximum of 50 characters.

Supported Agents

- ▶ **SNMP Agent.** Provides information about the operating systems, device types, installed software, and other system resources information. SNMP agents can usually be extended to support new MIBs, exposing more data for managerial purposes.
- ▶ **WMI Agent.** Microsoft's remote management agent, which is usually available for access by a remote administrator. The WMI agent is also extensible by adding WMI providers to the generic agent.
- ▶ **Telnet/SSH Agent (or daemon).** Used mostly on UNIX systems to connect remotely to a machine and to launch various commands to obtain data.
- ▶ **xCmd.** A remote administration technology similar in functionality to Telnet/SSH that enables launching any console command over Windows machines. xCmd relies on Administrative Shares & Remote Service Administration APIs to function correctly.

The **xCmd.exe** file is signed by an HP digital certificate. To validate that **xCmd.exe** is provided by HP, right-click the **xCmd.exe** file (or **xCmdSvc.exe** on a remote machine), select **Properties** and view the digital certificate.

- **Application specific.** This agent depends on the remote application to function as an agent and respond appropriately to the Probe's remote queries, for example, database discoveries, Web server discoveries, and SAP and Siebel discoveries.

Supported Protocols

This section includes the following topics:

- "Generic Protocol" on page 88
- "JBoss Protocol" on page 88
- "LDAP Protocol" on page 89
- "NNM Protocol" on page 89
- "NTCMD Protocol" on page 90
- "SAP JMX Protocol" on page 91
- "SAP Protocol" on page 91
- "Siebel Gateway Protocol" on page 92
- "SNMP Protocol" on page 93
- "SQL Protocol" on page 95
- "SSH Protocol" on page 96
- "Telnet Protocol" on page 99
- "UDDI Registry Protocol" on page 101
- "VMware Infrastructure Management (VIM) Protocol" on page 102
- "WebLogic Protocol" on page 103
- "WebSphere Protocol" on page 104
- "WMI Protocol" on page 105

Tip: If you use the SSH or Telnet credentials for discovery, we recommend that you add the following folders to the system path:

/sbin

/usr/sbin

/usr/local/sbin

Generic Protocol

This protocol is intended for integrations that do not need a specific protocol. It is recommended to use this protocol for all out-of-the-box integrations, as they require a user name and password only.

Parameter	Description
Description	Description of the credentials.
User Name	The name of the user needed for authentication.
User Password	The password of the user needed for authentication.

JBoss Protocol

Parameter	Description
Port Number	The port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the JBoss application server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.

 **LDAP Protocol**

Parameter	Description
Port Number	The port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the LDAP application server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.
Protocol	Choose which security model to use to access the service: LDAP . Discovery uses an unprotected connection. LDAPS . Discovery uses an SSL connection.
LDAP Authentication Method	Simple . The supported authentication method.
Trust Store File Path	The file containing trusted certificates. To import certificates into the Trust Store file: <ul style="list-style-type: none"> ▶ Create a new Trust Store or use the default Java Trust Store: <java-home>/lib/security/cacerts ▶ Enter the full path to the LDAP Trust Store file.
Trust Store Password	The LDAP Trust Store password used to access the Trust Store file. This password is set during the creation of a new Trust Store. If the password has not been changed from the default, use changeit to access the default Java Trust Store.

 **NNM Protocol**

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the NNM server.
NNM Password	The password for the NNM Web service (for example, Openview).

Parameter	Description
NNM User name	The user name of the NNM Web service (for example, system).
NNM Webservice Port	The Web service port number of the NNM server (for example, 80).
NNM Webservice Protocol	The protocol for the NNMi Web service (the default is http).
UMCBD Password	The password for the ODB Web service (the default is admin).
UCMDB Username	The user name of the ODB Web service (the default is admin).
UCMDB Webservice Port	The ODB Web service port number (the default is 8080).
UCMDB Webservice Protocol	The protocol for the ODB Web service (the default is http).

 **NTCMD Protocol**

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the NTCMD server.
User Name	The name of the user needed to connect to the host as administrator.
Password	The password of the user needed to connect to the host as administrator.
Windows Domain	The Windows domain in which the credentials are defined. If this field is left empty, the NTCMD protocol assumes the user is defined locally on the host.

SAP JMX Protocol

Parameter	Description
Port Number	<p>The SAP JMX port number. The SAP JMX Port structure is usually 5<System Number>04. For example, if the system number is 00, the port is 50004.</p> <p>Leave this field empty to try to connect to the discovered SAP JMX port; SAP JMX port numbers are defined in the portNumberToPortName.xml configuration file.</p>
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SAP JMX console.
User Name	The name of the user needed to connect to the application as administrator.
Password	The password of the user needed to connect to the application as administrator.

SAP Protocol

Parameter	Description	
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SAP console.	
User Name	The name of the user needed to log in to the SAP system. The user should have the following permissions:	
	Authorization Object	Authorization
	S_RFC	For the S_RFC object, obtain privileges: RFC1, SALX, SBDC, SDIF, SDIFRUNTIME, SDTX, SLST, SRFC, STUB, STUD, SUTL, SXMB, SXMI, SYST, SYSU, SEU_COMPONENT.
	S_XMI_PROD	EXTCOMPANY=MERCURY;EXTPRODUCT=DARM;INTERFACE=XAL
	S_TABU_DIS	DICBERCLS=SS; DICBERCLS=SC
Password	The password of the user needed to log in to the SAP system.	

Parameter	Description
SAP Client Number	It is recommended to use the default value (800).
SAP Instance Number	By default, set to 00 .
SAP Router String	A route string describes the connection required between two hosts using one or more SAProuter programs. Each of these SAProuter programs checks its Route Permission Table (http://help.sap.com/saphelp_nw04/helpdata/en/4f/992dfe446d11d189700000e8322d00/content.htm) to see whether the connection between its predecessor and successor is allowed. If it is, SAProuter sets it up.

Siebel Gateway Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the Siebel Gateway console
User Name	The name of the user needed to log on to the Siebel enterprise
Password	The password of the user needed to log on to the Siebel enterprise.
Siebel Site Name	The name of the Siebel Enterprise.
Path to Siebel Client	<p>The location on the Probe machine of the Siebel driver folder, where you copied <code>srvmgr</code>. For details, see "Prerequisites – Copy the driver Tool to the Data Flow Probe" in the <i>Discovery and Integration Content Guide</i>.</p> <p>Note: If there are several protocol entries with different <code>srvmgr</code> versions, the entry with the newer version should appear before the entry with the older version. For example, to discover Siebel 7.5.3. and Siebel 7.7, define the protocol parameters for Siebel 7.7 and then the protocol parameters for Siebel 7.5.3.</p>

 **SNMP Protocol**

Parameter	Description
Port Number	(For SNMP versions v1, v2, and v3) The port number on which the SNMP agent listens.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SNMP agent.
Retry Count	The number of times the Probe tries to connect to the SNMP agent. If the number is exceeded, the Probe stops attempting to make the connection.
Versions 1, 2	Community. Enter the authentication password you used when connecting to the SNMP service community (which you defined when configuring the SNMP service—for example, a community for read-only or read/write).

Parameter	Description
<p>Version 3</p>	<p>Authentication method: Select one of the following options for securing the access to management information:</p> <ul style="list-style-type: none"> ▶ NoAuthNoPriv. Using this option provides no security, confidentiality, or privacy at all. It can be useful for certain applications, such as development and debugging, to turn security off. This option requires only a user name for authentication (similar to requirements for v1 and v2). ▶ AuthNoPriv. The user logging on to the management application is authenticated by the SNMP v3 entity before the entity allows the user to access any of the values in the MIB objects on the agent. Using this option requires a user name, password, and the authentication algorithm (HMAC-MD5 or HMAC-SHA algorithms). ▶ AuthPriv. The user logging on to the management application is authenticated by the SNMP v3 entity before the entity allows the user to access any of the values in the MIB objects on the agent. In addition, all of the requests and responses from the management application to the SNMP v3 entity are encrypted, so that all the data is completely secure. This option requires a user name, password, and an authentication algorithm (either HMAC-MD5 or HMAC-SHA). <p>User Name: The name of the user authorized to log on to the management application.</p> <p>Password: The password used to log on to the management application.</p> <p>Authentication algorithm: The MD5 and SHA algorithms are supported.</p> <p>Privacy key: The secret key used to encrypt the scoped PDU portion in an SNMP v3 message.</p> <p>Privacy algorithm: The DES algorithm is supported.</p>

Troubleshooting

Problem. Failure to collect information from SNMP devices.

- **Solution 1.** Verify that you can actually access information from your Network Management station by using a utility that can verify the connectivity with the SNMP agent. An example of such a utility is **Getlft**.
- **Solution 2.** Verify that the connection data to the SNMP protocol has been defined correctly in the Add Protocol Parameters dialog box. For details, see "Protocol Parameters Dialog Box" on page 82.
- **Solution 3.** Verify that you have the necessary access rights to retrieve data from the MIB objects on the SNMP agent.



SQL Protocol

Parameter	Description
Database Type	The database type. Select the appropriate type from the box.
Port Number	<p>The port number on which the database server listens.</p> <ul style="list-style-type: none"> ➤ If you enter a port number, DFM tries to connect to a SQL database using this port number. ➤ For an Oracle database: If there are many Oracle databases in the environment and you do not want to have to create a new credential for each separate database port, you leave the Port Number field empty. When accessing an Oracle database, DFM refers to the <code>portNumberToPortName.xml</code> file and retrieves the correct port number for each specific Oracle database port. <p>Note: You can leave the port number empty on condition that:</p> <ul style="list-style-type: none"> ➤ All Oracle database instances are added to the <code>portNumberToPortName.xml</code> file. For details, see "The <code>portNumberToPortName.xml</code> File" on page 128. ➤ The same user name and password is needed to access all Oracle database instances.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the database.

Parameter	Description
User Name	The name of the user needed to connect to the database.
Password	The password of the user needed to connect to the database.
Instance Name	The name of the database instance, either the Oracle system identification or the DB2 database name. When connecting to any database, you can leave this field empty. In this case, DDM takes the SID from the Triggered CI data value: #{DB.name:NA} . For details, see "Trigger CIs and Trigger Queries" on page 29.

SSH Protocol

For details on configuring F-Secure when discovering Windows machines on which the F-Secure application is running on an SSH server, see "Host Connection by Shell: Discover Windows Running F-Secure" in the *Discovery and Integration Content Guide*.

Parameter	Description
Port Number	By default an SSH agent uses port 22. If you are using a different port for SSH, enter that port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the remote machine. For the UNIX platform: If your server is slow, it is recommended to change Timeout to 40000.
Version	SSH2 . Connect through SSH-2 only. SSH1 . Connect through SSH-1 only. SSH2 or SSH1 . Connect through SSH-2 and in case of error (if SSH-2 is not supported by the server), try to connect through SSH-1.

Parameter	Description
Shell Command Separator	<p>The character that separates different commands in a shell (to enable the execution of several commands in the same line).</p> <p>For example, in UNIX, the default shell command separator is a semicolon (;).</p> <p>In Windows, the shell command separator is an ampersand (&).</p>
Authentication Method	<p>Choose one of the following authentication options to access SSH:</p> <ul style="list-style-type: none"> ▶ password. Enter a user name and password. ▶ publickey. Enter the user name and path to the key file that authenticates the client. ▶ keyboard-interactive. Enter questions and answers. For details, see "Prompts and Responses" on page 98.
User Name	The name of the user needed to connect to the host through the SSH network protocol.
Password	The password of the user needed to connect to the host.
Key File Path	<p>(Enabled when the publickey authentication method is selected.) Location of the authentication key. (In certain environments, the full key path is required to connect to an SSH agent.)</p> <p>Note: Enter the full path to the key file on the Probe machine.</p>

Parameter	Description
<p>Prompts and Responses</p>	<p>(Enabled when the keyboard-interactive authentication method is selected.) A method whereby the server sends one or more prompts to enter information and the client displays them and sends back responses keyed-in by the user.</p> <p>The following is an example of prompts and expected responses:</p> <p>Prompt: Please enter your user name. Response: Shelly-Ann</p> <p>Prompt: What is your age? Response: 21</p> <p>Prompt: This computer is HP property. Press y to enter. Response: y</p> <p>To create these prompts and responses, enter the following strings in the fields, separated by commas:</p> <p>Prompts: user,age,enter Response: Shelly-Ann,21,y</p> <p>You can enter the full string as it appears in the SSH prompt, for example:</p> <div data-bbox="549 937 1039 1275" data-label="Form"> <p>The screenshot shows a configuration window with the following fields: <ul style="list-style-type: none"> Authentication Method: keyboard-interactive (dropdown) User Name: (empty text box) Password: (empty text box with a blue '...' button to its right) Key File Path: (empty text box) Prompts: Please enter your user name (text box) Responses: (empty text box with a blue '...' button to its right) Sudo paths: (empty text box) Sudo commands: (empty text box) At the bottom are three buttons: OK, Cancel, and Help. </p> </div> <p>or you can enter a key word, for example, user. DFM maps this word to the correct prompt.</p>

Parameter	Description
Sudo paths	The full paths to the sudo command. Paths are separated by commas.
Sudo commands	<p>A list of commands that can be executed with the sudo command. Commands are separated by commas. For all commands to be executed with sudo, add an asterisk (*) to this field.</p> <p>This field accepts a sudo command that prompts for the user's password.</p>

Troubleshooting

Problem. Failure to connect to the TTY (SSH/Telnet) agent.

Solution. To troubleshoot connectivity problems with the TTY (SSH/Telnet) agent, use a utility that can verify the connectivity with the TTY (SSH/Telnet) agent. An example of such a utility is the client tool PuTTY.

Telnet Protocol

Parameter	Description
Port Number	The port number. By default a Telnet agent uses port 23. If you are using a different port for Telnet in your environment, enter the required port number.
Connection Timeout	<p>Time-out in milliseconds after which the Probe stops trying to connect to the remote machine.</p> <p>For UNIX platforms: If your server is slow, it is recommended to change Connection Timeout to 40000.</p>
Authentication Method	<p>Choose one of the following authentication options to access Telnet:</p> <ul style="list-style-type: none"> ➤ password. Enter a user name and password. ➤ keyboard-interactive. Enter questions and answers. For details, see "Prompts and Responses" on page 98.
User Name	The name of the user needed to connect to the host.
Password	The password of the user needed to connect to the host.

Parameter	Description
<p>Prompts and Responses</p>	<p>(Enabled when the keyboard-interactive authentication method is selected.) A method whereby the server sends one or more prompts to enter information and the client displays them and sends back responses keyed-in by the user.</p> <p>The following is an example of prompts and expected responses:</p> <p>Prompt: Please enter your user name. Response: Shelly-Ann</p> <p>Prompt: What is your age? Response: 21</p> <p>Prompt: This computer is HP property. Press y to enter. Response: y</p> <p>To create these prompts and responses, enter the following strings in the fields, separated by commas:</p> <p>Prompts: user,age,enter Response: Shelly-Ann,21,y</p> <p>You can enter the full string as it appears in the Telnet prompt, for example:</p> <div data-bbox="545 939 1036 1211" data-label="Form"> </div> <p>or you can enter a key word, for example, user. DFM maps this word to the correct prompt.</p>

Parameter	Description
Sudo paths	The full paths to the sudo command. Paths are separated by commas.
Sudo commands	A list of commands that can be executed with the sudo command. Commands are separated by commas. For all commands to be executed with sudo, add an asterisk (*) to this field.

Troubleshooting

Problem. Failure to connect to the TTY (SSH/Telnet) agent.

Solution. To troubleshoot connectivity problems with the TTY (SSH/Telnet) agent, use a utility that can verify the connectivity with the TTY (SSH/Telnet) agent. An example of such a utility is the client tool PuTTY.

UDDI Registry Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the UDDI Registry.
UDDI Registry URL	The URL where the UDDI Registry is located.

VMware Infrastructure Management (VIM) Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to VMware Infrastructure.
Port Number	<p>DFM uses the number defined here when processing one of the Network – VMware jobs:</p> <p>If the port number is left empty, DFM performs a WMI query to extract the port number from the registry. DFM queries HKLM\SOFTWARE\VMware, Inc.\VMware VirtualCenter and searches for the HttpsProxyPort or HttpProxyPort attributes:</p> <ul style="list-style-type: none"> ▶ If the HttpsProxyPort attribute is found, DFM uses its value for the port and sets the prefix to HTTPS. ▶ If the HttpProxyPort attribute is found, DFM uses its value for the port and sets the prefix to HTTP.
Use SSL	<p>true: DFM uses a Secure Sockets Layer (SSL) protocol to access VMware Infrastructure, and the prefix is set to HTTPS.</p> <p>false: DFM uses the http protocol.</p>
User Name	The name of the user needed to connect to VMware Infrastructure.
User Password	The password of the user needed to connect to VMware Infrastructure.


WebLogic Protocol

Parameter	Description
Port Number	<p>If you enter a port number, DFM tries to connect to WebLogic using this port number.</p> <p>However, say you know that there are many WebLogic machines in the environment and do not want to have to create a new credential for each machine. You leave the Port Number field empty. When accessing a WebLogic machine, DFM refers to the WebLogic port (defined in <code>portNumberToPortName.xml</code>) already found on this machine (by TCP scanning, using the Network Connection – Active Discovery module).</p> <p>Note: You can leave the port number empty on condition that:</p> <ul style="list-style-type: none"> ▶ All WebLogic ports are added to the <code>portNumberToPortName.xml</code> file. For details, see "The <code>portNumberToPortName.xml</code> File" on page 128. ▶ The same user name and password is needed to access all WebLogic instances.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the WebLogic application server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.
Protocol	An application-level protocol that determines whether DFM should connect to the server securely. Enter either http or https .
Trust Store File Path	<p>Enter the full path to the SSL trust store file.</p> <p>To use the trust store file, do one of the following:</p> <ul style="list-style-type: none"> ▶ Enter the name (including the extension) and place the file in the following resources folder: C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\weblogic\ <WebLogic version>. ▶ Insert the trust store file full path.

Parameter	Description
Trust Store Password	The SSL trust store password.
Key Store File Path	<p>Enter the full path to the SSL keystore file.</p> <p>To use the keystore file, do one of the following:</p> <ul style="list-style-type: none"> ▶ Enter the name (including the extension) and place the file in the following resources folder: C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\weblogic\<WebLogic version>. ▶ Insert the keystore file full path.
Key Store Password	The password for the keystore file.

WebSphere Protocol

Parameter	Description
Port Number	<p>The protocol port number as provided by the WebSphere system administrator.</p> <p>You can also retrieve the protocol port number by connecting to the Administrative Console using the user name and password provided by the WebSphere system administrator.</p> <p>In your browser, enter the following URL: http://<host>:9060/admin, where:</p> <ul style="list-style-type: none"> ▶ <host> is the IP address of the host running the WebSphere protocol ▶ 9060 is the port used to connect to the WebSphere console <p>Access Servers > Application Servers > Ports > SOAP_CONNECTOR_ADDRESS to retrieve the required port number.</p>
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the WebSphere server.

Parameter	Description
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.
Trust Store File Name	The name of the SSL trust store file. To use the trust store file, do one of the following: <ul style="list-style-type: none"> ▶ Enter the name (including the extension) and place the file in the following resources folder: C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\websphere. ▶ Insert the trust store file full path.
Trust Store Password	The SSL trust store password.
Key Store File Name	The name of the SSL keystore file. To use the keystore file, do one of the following: <ul style="list-style-type: none"> ▶ Enter the name (including the extension) and place the file in the following resources folder: C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\websphere. ▶ Insert the keystore file full path.
Key Store Password	The password for the keystore file.

WMI Protocol

Parameter	Description
User Name	The name of the user needed to connect to the host.
Password	The password of the user needed to connect to the host.
Windows Domain	The Windows domain in which the credentials are defined. If this field is left empty, the NTCMD protocol assumes the user is defined locally on the host.

Data Flow Probe Log Files

Probe logs store information about job activation that occurs on the Probe Gateway and Probe Manager.

General Logs

wrapperProbeGW.log

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

Level	Description
Error	Any error that occurs within the Probe Gateway.
Information	Important information messages, such as the arrival or removal of a new task.
Debug	N/A

Basic Troubleshooting. Use this file for any Probe Gateway problems to verify what occurred with the Probe Gateway at any time as well as any important problems it encountered.

probe-error.log

Summary of the errors from the Probe.

Level	Description
Error	All errors in the Probe components.
Information	N/A
Debug	N/A

Basic Troubleshooting. Check this log to verify if errors occurred in the Probe components.

probe-infra.log

List of all infrastructure messages.

Level	Description
Error	All infrastructure errors.
Information	Information about infrastructure actions.
Debug	Messages mainly for debug purposes.

Basic Troubleshooting. Messages from the Probe's infrastructure only.

wrapperLocal.log

When running the Probe in separate mode (that is, the Probe Manager and Probe Gateway are installed on separate machines), a log file is also saved to the Probe Manager.

Level	Description
Error	Any error that occurs within the Probe Manager.
Information	Important information messages such as received tasks, task activation, and the transferring of results.
Debug	N/A

Basic Troubleshooting. Use this file for any Probe Manager problems to verify what occurred with the Probe Manager at any time as well as any important problems it encountered.

Probe Gateway Logs

probeGW-taskResults.log

This log records all the task results sent from the Probe Gateway to the server.

Level	Description
Error	N/A
Information	Result details: task ID, job ID, number of CIs to delete or update.
Debug	The ObjectStateHolderVector results that are sent to the server (in an XML string).

Basic Troubleshooting.

- ▶ If there is a problem with the results that reach the server, check this log to see which results were sent to the server by the Probe Gateway.
- ▶ The results in this log are written only after they are sent to the server. Before that, the results can be viewed through the Probe JMX console (use the **ProbeGW Results Sender** MBean). You may have to log in to the JMX console with a user name and password.

probeGW-tasks.log

This log records all the tasks received by the Probe Gateway.

Level	Description
Error	N/A
Information	N/A
Debug	The task's XML.

Basic Troubleshooting.

- If the Probe Gateway tasks are not synchronized with the server tasks, check this log to determine which tasks the Probe Gateway received.
- You can view the current task's state through the JMX console (use the **Discovery Scheduler** MBean).

Probe Manager Logs**probeMgr-performance.log**

Performance statistics dump, collected every predefined period of time, which includes memory information and thread pool statuses.

Level	Description
Error	N/A
Information	N/A
Debug	N/A

Basic Troubleshooting.

- Check this log to investigate memory issues over time.
- The statistics are logged every 1 minute, by default.

probeMgr-adaptersDebug.log

This log contains messages that are created following a job execution.

The **DiscoveryProbe.properties** File

A DFM process needs several parameters to be activated. These parameters specify the method to be used (for example, ping five times before declaring a failure) and against which CI a method should be run. If parameters have not been defined by the user, the DFM process uses the default parameters defined in the **DiscoveryProbe.properties** file. To edit the parameters, open **DiscoveryProbe.properties** in a text editor.

The **DiscoveryProbe.properties** file is located in the following folder:
C:\hp\UCMDB\DataFlowProbe\conf.

Caution: If you update the parameters in the **DiscoveryProbe.properties** file, you must restart the Probe so that it is updated with the changes.

The **DiscoveryProbe.properties** file is divided into the following sections:

- ▶ **Server Connection Definitions.** Contains parameters that are needed to set up the connection between the server and the Probe, such as the protocol to be used, machine names, default Probe and domain names, time-outs, and basic authentication.
- ▶ **Data Flow Probe Definitions.** Contains parameters that define the Probe, such as root folder location, ports, and Manager and Gateway addresses.
- ▶ **Probe Gateway Configurations.** Contains parameters that define time intervals for retrieving data.
- ▶ **Probe Manager Configurations.** Contains parameters that define Probe Manager functionality, such as scheduled intervals, result grouping, chunking, threading, time-outs, and filtering.
- ▶ **I18N Parameters.** Contains parameters that define language settings.
- ▶ **Internal Configurations.** (**Caution:** These parameters should not be changed without an advanced knowledge of Data Flow Management.) Contains parameters that enable DFM to function efficiently, such as thread pool size.

Troubleshooting and Limitations

Problem. You cannot transfer a Data Flow Probe from one domain to another. Once you have defined the domain of a Probe, you can change its ranges, but not the domain.

Solution. Install the Probe again:

- 1** (Optional) If you are going to use the same ranges for the Probe in the new domain, export the ranges before removing the Probe. For details, see "Ranges Pane" on page 78.
- 2** Remove the existing Probe from ODB. For details, see the **Remove Domain or Probe** button in "Domains and Probes Pane" on page 79.
- 3** Install the Probe. For details, see "Data Flow Probe Installation" on page 39.

During installation, make sure you give a different name to the Probe from the one used by the old Probe. For details, see step 7 in "Install the Data Flow Probe" in *ODB Data Flow Management Guide*.

Problem. Discovery shows a disconnected status for a Probe.

Solution. Check the following on the Probe machine:

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

Problem. You cannot transfer an ODB Data Flow Probe from one domain to another. Once you have defined the domain of a Probe, you can change its ranges, but not the domain.

Solution. Install the Probe again:

- 1** (Optional) If you are going to use the same ranges for the Probe in the new domain, export the ranges before removing the Probe. For details, see "Ranges Pane" on page 78.
- 2** Remove the existing Probe from ODB. For details, see the **Remove Domain or Probe** button in "Domains and Probes Pane" on page 79.
- 3** Install the Probe. For details, see "Data Flow Probe Installation" on page 39.

During installation, make sure you give a different name to the Probe from the one used by the old Probe. For details, see step 7.

Problem. The connection between the Business Service Management server and the Probe fails due to an HTTP exception.

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

Problem. The Discovery tab is not displayed in the main page of Business Service Management.

Solution. Install a license for the Probe. For details, see "Licensing Models for ODB" in *ODB Data Flow Management Guide*.

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

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

5

Data Flow Probe Status

This chapter includes:

Concepts

- ▶ Data Flow Probe Status Overview on page 114

Tasks

- ▶ View Current Status of Discovered CIs on page 115

Reference

- ▶ Data Flow Probe Status User Interface on page 116

Concepts

Data Flow Probe Status Overview

You use Data Flow Probe Status to view the current status of the discovered CIs in the Probes. Data Flow Probe Status retrieves the status from the Probes and displays the results in a view.

The view is not automatically updated; to refresh the status data, click the **Get snapshot** button.



Tasks

View Current Status of Discovered CIs

This task describes how to view the current status of discovered CIs.

This task includes the following steps:

- "Prerequisites" on page 115
- "Access Data Flow Probe Status" on page 115

1 Prerequisites

Verify that the Probe is enabled and is connected to the Business Service Management Gateway server. For details, see "Get Started With the ODB Data Flow Probe" on page 64.

2 Access Data Flow Probe Status

- a** Go to **Admin > ODB Administration > Data Flow Management > Data Flow Probe Status**.
- b** Select a connected Probe.

All current jobs in the Probe are listed, together with their status. For details, see "Data Flow Probe Status Window" on page 118.
- c** Click the **Get Snapshot** button.
- d** Select jobs from the Progress list and click the **View Job progress** button. The Job Progress window opens.

Reference


Data Flow Probe Status User Interface

This section includes (in alphabetical order):

- ▶ [Job Name] Dialog Box on page 116
- ▶ Data Flow Probe Status Window on page 118

[Job Name] Dialog Box

Enables you to view details about a job, including its scheduling, as well as job statistics.

To access	<ul style="list-style-type: none">▶ Select a job in the Progress pane of the Data Flow Probe Status window and click the View job progress  button.or▶ Double-click a job the Progress pane of the Data Flow Probe Status window.
------------------	---

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Job Details	<p>Status. Can be Scheduled (the job runs according to a defined schedule) or Running (the job is running now).</p> <p>Last updated. The last time that the job was updated.</p> <p>Threads. The number of threads currently allocated to this job.</p> <p>Progress. The number of Trigger CIs in the job and the number of Trigger CIs that the Probe has finished working on.</p>
Schedule	<p>Previous invocation. The last time that DFM ran the job.</p> <p>Next invocation. The next time that DFM is scheduled to run the job.</p> <p>Last duration. The length of time, in seconds, taken to run the job in the previous invocation.</p> <p>Average duration. The average duration, in seconds, of the time it took the Probe to run this job.</p> <p>Recurrence. The number of times a job is run in a week. For example, if a job is scheduled to run daily, it runs 7 times in a week. If a job is scheduled to run weekly, Recurrence = 1.</p>
Statistics Results	For details, see "Statistics Results Pane" on page 120.

Data Flow Probe Status Window

Enables you to view the current status of discovered CIs and all active jobs running on the Probes.

To access	Admin > ODB Administration > Data Flow Management > Data Flow Probe Status
Important Information	<p>Depending on what you select in the Domains Browser pane, different information is displayed in the viewing pane.</p> <p>If you select:</p> <ul style="list-style-type: none"> ▶ a domain, you can view details and CIT statistics for the domain. For details, see "Details Tab" on page 75 and "Statistics Results Pane" on page 120. ▶ a Probe, you can view details on the Probe (such as the Probe IP), the progress of a job and you can view CIT statistics. For details, see "Details Pane" on page 119, "Progress Pane" on page 120, "Statistics Results Pane" on page 120, and "Probe Snapshot Information" on page 122.
Relevant tasks	"View Current Status of Discovered CIs" on page 115
See also	"Data Flow Probe Status Overview" on page 114


Details Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
Domain Type	<p>Customer. A private domain used for your site. You can define several domains and each domain can include multiple Probes. Each Probe can include IP ranges but the customer domain itself has no range definition.</p> <p>External. Internet/public domain. A domain which is defined with a range. The external domain may contain only one Probe whose name equals the domain name. However, you can define several external domains in your system.</p> <p>For details on defining domains, see "Add New Domain Dialog Box" on page 72.</p>

Progress Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):



GUI Element (A-Z)	Description
	Select a CI and click View job progress to view details of a job. For details, see "[Job Name] Dialog Box" on page 116.
Job	The name of the job. Double click a job to open a dialog box displaying job details. For details, see "[Job Name] Dialog Box" on page 116.
Next invocation	The next time that the Probe is scheduled to run.
Previous invocation	The last time that the Probe ran.
Progress	Can be either Scheduled or Running. If a job is running, a progress bar displays the percentage finished.
Thread count	The number of threads currently allocated to this job.
Triggered CIs	The number of CIs triggered in the job.

Statistics Results Pane

Enables you to view details and CIT statistics.

To access	Click the Default Domain or Probe name in the Domains Browser pane.
------------------	---


The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to retrieve the latest data from the Probe (data is not automatically updated).
	<p>Set the time range for which to display statistics about the CITs.</p> <ul style="list-style-type: none"> ▶ All. Displays statistics for all job runs. ▶ Last Hour/Day/Week/Month. Choose a period of time for which to display statistics about the CITs. ▶ Custom Range. Click to open the Customize Statistics Time Range dialog box. Enter the date or click the arrow to choose a date and time from the calendar, for the To and From dates. To delete a date, click Reset.
<Column title>	Click a column title to change the order of the CITs from ascending to descending order, or vice versa.
<right-click a title>	<p>Choose from the following options:</p> <ul style="list-style-type: none"> ▶ Hide Column. Select to hide a specific column. ▶ Show All Columns. Displayed when a column is hidden. ▶ Customize. Select to display or hide columns and to change the order of the columns in the table. Opens the Columns dialog box. ▶ Auto-resize Column. Select to change a column width to fit the contents. <p>For details, see "Select Columns Dialog Box" in the <i>Modeling Guide</i>.</p>
CIT	The name of the discovered CIT.
Created	The number of CIT instances created by the Probe.
Deleted	The number of CIT instances deleted by the Probe.
Discovered CIs	The sum of all the CIs for all the invocations.

GUI Element (A–Z)	Description
Filter	The time range set with the Set Filter button.
Last updated	The date and time that the statistics table has been updated for a particular Probe.
Total	The total number of CIs in each column.
Updated	The number of CIT instances that have been updated.

Probe Snapshot Information

The following elements are included:

GUI Element (A–Z)	Description
	Click to view the current status of the discovered CIs and jobs on the selected Probe.
Last updated	The date and time at which the Get snapshot button was last pressed (that is, the date and time of the data displayed in Data Flow Probe Status).
Probe IPs	The IP addresses defined for the Probe.
Running jobs	The number of jobs running on the Probe.
Scheduled jobs	The number of jobs that are scheduled to run according to the settings in the Discovery Scheduler. For details, see "Discovery Scheduler Dialog Box" on page 301.
Status	The status of the Probe (either disconnected or connected).
Threads	The sum of all threads currently allocated to the running jobs.

6

Adapter Management

This chapter includes:

Concepts

- ▶ Automatically Deleted CIs and Relationships and Candidates for Deletion CIs on page 124
- ▶ Discovering Running Software on page 126
- ▶ Identifying Running Software by Processes on page 127
- ▶ The portNumberToPortName.xml File on page 128

Tasks

- ▶ Configure the Data Flow Probe to Automatically Delete CIs – Workflow on page 129
- ▶ Discover Running Software – Scenario on page 130
- ▶ Define a New Port on page 133
- ▶ Use the cpVersion Attribute to Verify Content Update on page 135
- ▶ Manage Adapter Configurations on page 135

Reference

- ▶ Resource Files on page 138
- ▶ Internal Configuration Files on page 141
- ▶ Adapter Management User Interface on page 141

Concepts

Automatically Deleted CIs and Relationships and Candidates for Deletion CIs

During discovery, the Data Flow Probe compares CIs found during the previous, successful invocation with those found during the current invocation. A missing component, such as a disk or software, is assumed to have been removed from the system, and its CI is deleted from the Probe's database.

The Data Flow Probe does not wait for the aging mechanism to perform the calculation but immediately sends a deletion request to the server. For details on aging, see "The Aging Mechanism Overview" in the *ODB Administration Guide*.

You can define that CI instances are to be deleted for specific jobs. For details, see "Configure the Data Flow Probe to Automatically Delete CIs – Workflow" on page 129.

By default, the Data Flow Probe deletes CI instances of certain CITs, for example, the current configuration for the Host Resources and Applications jobs (snmp: file system, installed software, osuser, service).

Candidates for Deletion

You can mark a CI instance as a candidate for deletion. This enables you to isolate CIs instead of them being automatically deleted when they are not discovered.

Discovery forces its aging status to change to **aged**, so that the CI appears in the Aged CIs box. Its time-to-deletion by the aging mechanism is shortened (to 20 days, by default).

Note:

- ▶ The change is defined on the job's adapter.
 - ▶ If discovery fails and errors occur, objects are sent for deletion according to how the results are managed. For details, see "Results Management Pane" on page 154.
 - ▶ Carefully choose the CIs that are to be candidates for deletion. For example, process CITs are not good candidates because they are often shutting down and starting up again and as a result may be deleted at every invocation.
 - ▶ You can use this procedure to delete relationships, too. For example, the contained relationship is used between a node and an IP address. A laptop machine is allocated a different IP address very often; by deleting the relationship, you prevent the accumulation of old IP addresses attached to this node.
-

Example of Automatic Deletion

During the previous invocation, the Data Flow Probe ran the **Host Resources and Applications by WMI** job and discovered a host with disks a, b, c, and d. During the current invocation, the Probe discovers disks a, b, and c, compares this result with the previous result, and deletes the CI for disk d.

More Information

- ▶ You can view deleted CIs in the Probe log and in the Deleted column in the Statistics Results pane. For details, see "Data Flow Probe Log Files" on page 106 and "Statistics Results Pane" on page 292.
- ▶ For details on setting automatic deletion, see "Automatic Deletion" on page 154.
- ▶ For details on aging, see "The Aging Mechanism Overview" in the *ODB Administration Guide*.

Discovering Running Software

You can discover software (for example, a specific Oracle database) running in your environment.

This section includes the following topics:

- ▶ "Discovery Process" on page 126
- ▶ "Running Software Default View" on page 126

Discovery Process

The discovery process runs as follows:

- ▶ The Host Resources and Applications jobs are activated.
- ▶ DFM searches for processes on the machines in your environment.
- ▶ DFM saves the process data (including open port and command line information) to the Probe database.
- ▶ The jobs run on this data in the Probe database, build the new RunningSoftware CIs according to the data in the database, and extract the key attributes from the process data. The jobs send the CIs to the ODB.

Running Software Default View

A default view displays the mapping of relationships between applications:

Admin > ODB Administration > Modeling > Modeling Studio > Resources pane > Root > Application > Deployed Software.

You can configure DFM to discover running software. For details, see "Discover Running Software – Scenario" on page 130.

Identifying Running Software by Processes

An application is identified by the existence of one or more running processes which are defined by their names and by command line (optional).

A process can be optionally marked as a key process or as a main process.

An application is identified if the following holds true:

- At least one process was found.
- All processes mark as key processes exist.

If an application is identified, a result RunningSoftware CI is created for the application obeying the following rules:

- If none of the processes mark as main process, a single RunningSoftware CI will be created, linked to all discovered processes by dependency links.
- If there are processes mark as main process, a RunningSoftware CI will be created for each instance of these main processes.

For example, assume that rules are defined for the identification of two applications, **application_a** and **application_b**:

- **application_a** is identified by **proc.exe** and **unique_proc_a.exe**.
- **application_b** is identified by **proc.exe** and **unique_proc_b.exe**.

Say that **proc.exe** is found but none of its processes are marked as key or main processes. In this case, **RunningSoftware** CIs are created for both **application_a** and **application_b**. These CIs are linked by a dependency link to the same process (that is, **proc.exe**).

Assume too that **unique_proc_a.exe** and **unique_proc_b.exe** are marked as key processes:

- If the **proc.exe** process only is discovered, a **RunningSoftware** CI is not created.
- If **unique_proc_a.exe** is discovered, **RunningSoftware** CIs are created for **application_a** linked by a dependency link to **unique_proc_a.exe**. If in addition, **proc.exe** is discovered, it is linked to the same CI. The same holds for **application_b**.

Assume that two instances of **unique_proc_a.exe** are discovered:

- ▶ If the process is not marked as a main process, a single **RunningSoftware** CI is created for **application_a** linked to both processes.
- ▶ If the process is marked as a main process, two separate **RunningSoftware** CIs are created for **application_a**.

For details on the key field in the Software Identification Rule Editor dialog box, see "Identifying Processes" on page 182.

The portNumberToPortName.xml File

The portNumberToPortName.xml file is used by DFM as a dictionary to create Port 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 Port CI with that name. If the port name does not appear in this file, the Probe uses the port number as the port name.

For details on adding new ports to be discovered, see "Define a New Port" on page 133.

Note: The results of running a **Network Connections – Active Discovery** job appear in the Topology Map with the port names instead of the port numbers (the port title is the value of the Port Name attribute, defined in the CIT). For details, see "Add/Edit Attribute Dialog Box" in the *Modeling Guide*.

Tasks

Configure the Data Flow Probe to Automatically Delete CIs – Workflow

This task explains how to configure a job so that CI instances of specific CITs are automatically deleted. For details on how the Data Flow Probe deletes CIs, see "Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 124.

This task includes the following steps:

- "Prerequisites" on page 129
- "Select the CIs to be Deleted" on page 129
- "Results" on page 129

1 Prerequisites

Verify that the **Filter unchanged results** check box is selected in the Results Management pane in the Adapter Management tab. For details, see "Results Management Pane" on page 154.

2 Select the CIs to be Deleted

- a** Select the **Enable Automatic Deletion** check box.
- b** Click the **Add** button to open the Choose Discovered Class dialog box. For details, see "Choose Discovered Class Dialog Box" on page 161.
- c** Select the deletion method for the CIT: either **Auto Delete** or **Candidate for Deletion**.
- d** Click the **Save** button at the bottom of the page.

3 Results

To view the deleted CIs, access the Deleted column in the Statistics Results pane. For details, see "Statistics Results Pane" on page 292.

Discover Running Software – Scenario

This scenario explains how to set up the discovery of Oracle databases so that there is no need to enter a specific set of credentials to discover each database instance. DFM runs an `extract` command that retrieves the database name attribute.

In this scenario, we assume that the following syntax is used in the Oracle command lines:

```
c:\ora10\bin\oracle.exe UCMDB
```

This task includes the following steps:

- ▶ "Prerequisites" on page 130
- ▶ "Create a Command Line Rule" on page 131
- ▶ "Define the Value of an Attribute" on page 132
- ▶ "Activate the Job" on page 133

1 Prerequisites

Display the Attribute Assignment Rules dialog box:

- a** Select **Admin > ODB Administration > Data Flow Management > Discovery Control Panel**. In the **Discovery Modules** pane, select the **Network** module > **Host Resources and Applications > Software Element CF by Shell**. In the **Properties** tab, select **Global Configuration Files > applicationSignature.xml**. For details, see "Global Configuration Files Pane" on page 148.

Tip: If the Global Configuration Files pane does not display, click the arrow below the Trigger Queries pane.

- b** Click the **Edit** button to open the Software Library dialog box. For details, see "Software Library Dialog Box" on page 184.

- c** Choose the signature to be edited. Click the **Edit** button to open the **Software Identification Rule Editor** dialog box. For details, see "Software Identification Rule Editor Dialog Box" on page 181.
- d** Click the **Set Attributes** button to open the **Attributes Assignment Editor** dialog box. For details, see "Attribute Assignment Editor Dialog Box" on page 159.

2 Create a Command Line Rule

The command line rule is text that identifies the process to be discovered, for example, `oracle.exe c:\ora10\bin\oracle.exe UCMDB`. You can substitute the text entry with a regular expression, so that discovery is more flexible. For example, you can set up a rule that discovers all Oracle databases, whatever their name.

Subsequently, DFM uses the information in the command lines discovered by the regular expression to populate a CI's name attribute with the database name.

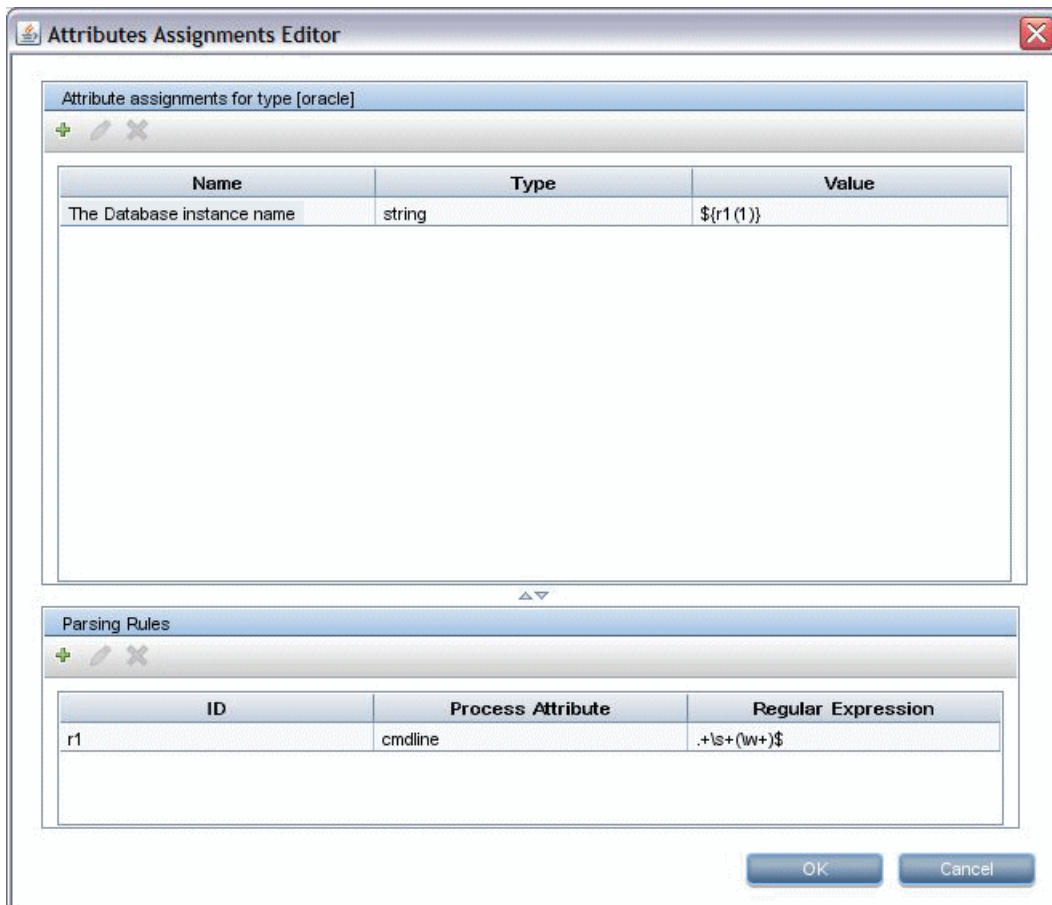
- a** To create a Command Line rule that includes a regular expression, in the Attributes Assignment Rules dialog box, click the **Add** button in the Parsing Rules pane. For details, see "Parse Rule Editor Dialog Box" on page 172.
- b** In the Parse Rules Editor dialog box, build the rule:
 - ▶ Enter a unique name in the Rule ID field: **r1**.
 - ▶ Choose **Command Line** in the Process Attribute field.
 - ▶ Enter the following regular expression in the Regular Expression field: `.\s+(\w+)\$`:

This expression searches for any character (`.`), followed by a space or spaces (`+\s+`), followed by a word or words (`(\w+)`) that appear at the end of the line (`$`). You can use the following characters: a-z, A-Z, or 0-9. The following command line fulfils this expression: `c:\ora10\bin\oracle.exe UCMDB`.

3 Define the Value of an Attribute

In this step, you define which attribute is used by DFM to discover the Oracle databases, and the value it should take.

- a** In the Attributes Assignment Rules dialog box, click the **Add** button in the Attribute Assignments pane, to select the attribute.
- b** In the Attribute Editor dialog box:
 - ▶ Choose the attribute that holds the database name, from the list of Oracle CIT attributes, in this case **The Database instance name**.
 - ▶ Enter a value, using the following syntax: **`${<rule ID name>(<group number>)}`**, in this case, **`$(r1(1))`**.



This dialog box is configured as follows: DFM enters the value of the first group (`(\w+)$`) in the command line regular expression (`(${r1(1)})`) in the name attribute of the Oracle database CI.

That is, during discovery, DFM searches through the process files for command lines with a word or words at the end of the line. For example, the following command line matches this regular expression: `c:\ora10\bin\oracle.exe UCMDB`.

4 Activate the Job

For details, see "Manually Activate a Job" on page 263 and "Discovery Modules Pane" on page 296.

Define a New Port

To define a new port by editing the `portNumberToPortName.xml` file:

- 1 In the Adapter Management window (**Admin > ODB Administration > 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 an explanation of the `portNumberToPortName.xml` file, see "The `portNumberToPortName.xml` File" on page 128.

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

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

- **portProtocol.** The network protocol used for discovery (udp or tcp).
- **portNumber.** The port number to be discovered.
- **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 ODB 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.cfg  
files.KnownPortsConfigFile" cpVersion="3">
```

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 "Use the cpVersion Attribute to Verify Content Update" on page 135.

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 5.00:

```
<portInfo portProtocol="tcp" portNumber="389" portName="ldap" discover="1"
cpVersion="5"/>
```

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 an explanation of the portNumberToPortName.xml file, see "The portNumberToPortName.xml File" on page 128.

To verify that a DFM Content Pack is successfully deployed:

- 1 Install the latest Service Pack release.
- 2 Start the BSM Server.
- 3 Verify that all services are running. For details, see "Viewing the Status of the Services" in the *HP Business Service Management Deployment Guide* PDF.
- 4 Install and deploy the latest Content Pack release. For details, refer to the Content Pack installation guide.
- 5 Access the portNumberToPortName.xml file (**Admin > ODB Administration > Data Flow Management > Adapter Management > Discovery Packages > Network > Configuration Files > portNumberToPortName.xml**).
- 6 Verify that any user-defined ports have not been deleted and any ports deleted by the user have not been added.

Manage Adapter Configurations

You should edit adapter and XML files in one of the following ways:

Use the Adapter Management module

This method is recommended.

- 1 Navigate to **Admin > ODB Administration > Data Flow Management > Adapter Management**.
- 2 In the Resources pane, select the adapter file: **Packages > <package name> > Adapters**.
- 3 Do one of the following:
 - ▶ To edit general adapter settings, use the Adapter Definition and Adapter Management tabs. For details, see "Adapter Definition Tab" on page 143 and "Adapter Management Tab" on page 150.
 - ▶ To define specific settings for the selected adapter, right-click the adapter and select **Edit Adapter Source** from the shortcut menu.

Use Package Manager

Edit the package and redeploy it. For details, see "Package Manager" in the *ODB Administration Guide*.

Use the JMX Console

- 1 Launch the Web browser and enter the server address, as follows: **http://BSM Server Host Name or IP>:21212/jmx-console**.

You may have to log in with a user name and password.
- 2 Under UCMDB, click **UCMDB:service=Packaging Services** to open the JMX MBEAN View page.
- 3 Locate the **listSubsystems** operation.
- 4 Enter the Customer ID value and click **Invoke**.
- 5 Click the **DiscoveryPatterns** or **DiscoveryConfigFiles** link.
- 6 Click the resource to edit.

Change the Full Population value

Because the ODB 9.0x adapter only synchronizes changes, **over time** CIs are not touched and are aged out; therefore, by default the ODB 9.0x adapter runs a full population job every seven days.

To change the full population value:

- 1** Access the Resources pane: **Data Flow Management > Adapter Management > Resources.**
- 2** Select the **CmdbAdapter** adapter file: **CmdbAdapter > Adapters > CmdbAdapter.**
- 3** Right-click the **CmdbAdapter** file and choose **Edit Adapter Source.**
- 4** In the source file, locate the following tag:
`<full-population-days-interval>7</full-population-days-interval>`.
- 5** Edit the value as follows:
 - **7** = run full population job every 7 days
 - **1** = run full population job each day
 - **0** = always run a full population job
 - **-1** = the option is disabled

Reference

Resource Files

The following files can be changed to enable DFM in non-default systems. The location of these files is: **Admin > ODB Administration > Data Flow Management > Adapter Management > Packages > Network > Configuration Files.**

This section includes the following topics:

- ▶ "oidToHostClass.xml" on page 138
- ▶ "globalFiltering.xml" on page 139

oidToHostClass.xml

The oidToHostClass.xml file contains a list of OID numbers, for all CIs in the system that have an ID. This list is required for mapping CIs to their correct CIT, and for converting the discovered OID number of an operating system or a device into string data.

To access the oidToHostClass.xml file, in Adapter Management, search for the file by clicking the **Find resource** button and entering **oidto** 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.

Note: If an OID is discovered and its details do not appear in the oidToHostClass.xml file, its CIT is registered in the CMDB as host.

The `oidToHostClass.xml` file includes the following parameters:

- ▶ **class.** The converted CIT name of the discovered OID. Under this name, the operating system or device appears in the CMDB and in HP Business Service Management.
- ▶ **vendor.** The vendor of the operating system or device.
- ▶ **os.** A specific operating system, for example, Linux. This parameter is optional.
- ▶ **model.** A specific model, for example, JETDIRECT,JD30. This parameter is optional.
- ▶ **oid.** The discovered OID.

globalFiltering.xml

This file enables you to filter Probe results for all adapters, so that only results of interest to you are sent to the HP Business Service Management server. (You can also filter specific adapters. For details, see "Adapter Management Tab" on page 150.)

To add a global filter:

- 1 Access the `globalFiltering.xml` file: in Adapter Management, open the Network folder and click the Configuration Files folder. Select the file to display the code in the View pane.
- 2 Locate the `<includeFilter>` and `<excludeFilter>` markers:
 - ▶ **<includeFilter>**. When a vector marker is added to this filter, all CIs that do not match the filter are removed. If this marker is left empty, all results are sent to the server:

```
<vector>
  <object class="ip_subnet">
  </object>
</vector>
```

- ▶ **<excludeFilter>**. When a vector marker is added to this filter, all CIs that match the filter are removed. If this marker is left empty, all results are sent to the server.

The following example shows an `ipAddress` CI that has address and domain attributes:

```
<vector>
  <object class="ipAddress">
    <attribute name="name" type="String">192.168.82.17.*</attribute>
    <attribute name="routing_domain" type="String">DefaultProbe</attribute>
  </object>
</vector>
```

If this vector is defined in `<includefilter>`, all results not matching the filter are removed. The results sent to the server are those where the `ip_address` matches the regular expression `192\.\168\.\82\.\17.*` and the `ip_domain` is **DefaultProbe**.

If this vector is defined in `<excludefilter>`, all results matching the filter are removed. The results sent to the server are those where the `ip_address` does not match the regular expression `192\.\168\.\82\.\17.*` and the `ip_domain` is not **DefaultProbe**.

The following example shows a `ip_subnet` CI that has no attributes.

- Attributes in the filter should be of type `string` only. For details on attribute types, see "Attributes Page" in the *Modeling Guide*.
 - A result is considered to be a match only if all filter attributes have the same values as those in the CI. (If one of a CI's attributes is not specified in the filter, all the results for this attribute match the filter.)
 - A CI can match more than one filter. The CI is removed or remains according to the filter in which it is included.
 - DFM filters first according to the `<includeFilter>` and then applies the `<excludeFilter>` on the results of `<includeFilter>`.
-

Internal Configuration Files

The following files are for internal use only and should be changed only by users with an advanced knowledge of content writing.

- ▶ **discoveryPolicy.xml**. Includes the schedule when the Probe does not execute tasks. For details, see "Add/Edit Policy Dialog Box" on page 71. Located in **Admin > ODB Administration > Data Flow Management > Adapter Management > Packages > AutoDiscoveryInfra > Configuration Files**.
- ▶ **jythonGlobalLibs.xml**. A list of default Jython global libraries that DFM loads before running scripts. Located in **Admin > ODB Administration > Data Flow Management > Adapter Management > Packages > AutoDiscoveryContent > Configuration Files**.

Adapter Management User Interface

This section describes:

- ▶ Adapter Definition Tab on page 143
- ▶ Adapter Management Tab on page 150
- ▶ Adapter Management Window on page 157
- ▶ Adapter Source Editor Window on page 158
- ▶ Attribute Assignment Editor Dialog Box on page 159
- ▶ Attribute Editor Dialog Box on page 160
- ▶ Choose Discovered Class Dialog Box on page 161
- ▶ Configuration File Pane on page 163
- ▶ Edit Process Dialog Box on page 164
- ▶ Find Resource/Jobs Dialog Box on page 165
- ▶ Find Text Dialog Box on page 166
- ▶ Input Query Editor Window on page 167
- ▶ Parse Rule Editor Dialog Box on page 172

Chapter 6 • Adapter Management

- ▶ Permission Editor Dialog Box on page 173
- ▶ Resources Pane on page 175
- ▶ Script Editor Window on page 178
- ▶ Script Pane on page 179
- ▶ Software Identification Rule Editor Dialog Box on page 181
- ▶ Software Library Dialog Box on page 184

Adapter Definition Tab

Enables you to define an adapter by specifying:

- which CITs the adapter should discover
- which protocols are needed to perform discovery


To access	Select a specific adapter in the Resources pane.
Relevant tasks	"Implement a Discovery Adapter" in the <i>ODB Developer Reference Guide</i>





The following elements are included (unlabeled GUI elements are shown in angle brackets>):




GUI Element (A–Z)	Description
Adapter Category	Used to arrange adapters by category.
Description	A detailed description of the adapter's purpose, including relevant comments.
Display Name	A display name to identify the adapter.
Type	For Discovery adapters: jython ; for Integration adapters: can be of various types.
Used as Integration Adapter	Select to define that this adapter is an integration adapter. These adapters cannot be used for defining Discovery jobs, and are accessible only through the Integration Studio.

Input Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):




GUI Element (A–Z)	Description
Input CI Type 	The input CIT is used as the adapter input. For details, see "Define Adapter Input (Trigger CIT and Input Query)" in the <i>ODB Developer Reference Guide</i> . Click the button to choose a CIT to use as the input.


GUI Element (A–Z)	Description
	Edit input query.
	Remove input query.
Input Query	<p>Defines a query for validation of the triggered CIs for jobs that run this adapter. (CIs matching the job's triggered query must match the Input query as well.)</p> <p>Note: Since this field is optional, not all adapters include an input query. None signifies this adapter does not have an input query definition.</p> <ul style="list-style-type: none"> ▶ Click the Edit Input Query button  to open the Input Query Editor window. ▶ Click the Remove Input query button  to remove the Input query from the adapter. <p>For details, see "Input Query Editor Window" on page 167. For an explanation, see "Trigger CIs and Trigger Queries" on page 29. For an example, see "Example of Input Query Definition" in the <i>ODB Developer Reference Guide</i>.</p>

GUI Element (A–Z)	Description
Triggered CI Data	 Add Trigger CI data to the adapter.  Remove Trigger CI data from the adapter.  Edit the Trigger CI data in the Parameter Editor dialog box. Name. The information that is needed to perform a task on a specific CI. This information is passed to the CI queried in the task. Value. The attribute value. Variables are written using the following syntax: <code>#{VARIABLE_NAME.attributeName}</code> where VARIABLE_NAME can be one of three predefined variables: <ul style="list-style-type: none"> ▶ SOURCE. The CI that functions as the task’s trigger. ▶ HOST. The node in which the triggered CI is contained. ▶ PARAMETERS. The parameter defined in the Parameter section. You can create a variable. For example, <code>#{SOURCE.network_netaddr}</code> indicates that the trigger CI is a network.

Used Scripts Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Change the order of the scripts. DFM runs the scripts in the order in which they appear here.
	Add a script to the adapter.
	Remove a script from the adapter.



GUI Element (A–Z)	Description
	Edit the selected script in the Script Editor that opens.
Scripts	A list of Jython scripts used by the adapter.




Required Permissions Pane

Enables you to view the permissions that you have configured for an adapter.

To access	Admin > ODB Administration > Data Flow Management > Adapter Management > select an adapter > Adapter Definition tab > Required Permissions pane.
Important Information	<ul style="list-style-type: none"> ▶ Workflow: <ul style="list-style-type: none"> ▶ Configure the permissions in the Permission Editor dialog box. ▶ View the permissions in this pane. ▶ When working with jobs in the Discovery Control Panel window, view these permissions for a specific job. ▶ For details on the fields in this pane, see "Permission Editor Dialog Box" on page 173.
See also	<ul style="list-style-type: none"> ▶ "Permission Editor Dialog Box" on page 173 ▶ "Discovery Permissions Window" on page 299 ▶ "Viewing Permissions While Running Jobs" on page 242



The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to add a permission object. The Permission Editor dialog box opens. For details, see "Permission Editor Dialog Box" on page 173.
	Select a permission object and click the button to edit. For details, see "Permission Editor Dialog Box" on page 173.

GUI Element (A–Z)	Description
	Select a permission object and click to delete it.
	Change the order of the permissions by selecting the permission object and clicking the up or down button. The order given here is the order in which the credentials are verified.
	Export a permission object in Excel, PDF, RTF, CSV, or XML format. For details, see "Browse Views Mode" in the <i>Modeling Guide</i> .




Required Discovery Protocols Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Opens the Add Required Protocol dialog box.
	Click to remove an existing protocol.
Protocols	List of protocols required by the adapter for the task. For example, the NTCmd protocol, together with its user name, password, and other parameters, is needed for DFM to access a Windows system.

Discovered CITs Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):




GUI Element (A–Z)	Description
	Click to open the Choose Discovered Class dialog box, to select a CIT that is to be discovered by the adapter. For details, see "Choose Discovered Class Dialog Box" on page 161.
	Click to remove the CIT from the list of CITs that the adapter discovers.
	You can choose to view a map of the CITs and links that are discovered by the adapter, instead of a list. Click the button to open the Discovered CITs Map window. The CIs and relationship links discovered by the adapter are shown.
CITs	List of CITs that the adapter discovers.

Global Configuration Files Pane

Enables you to add default configuration files to the adapter, as well as the specific configuration files that the adapter needs.




To access	<ul style="list-style-type: none"> ▶ In Adapter Management, select an adapter and the Adapter Definition tab. ▶ In Discovery Control Panel, select a job and the Properties tab.
Important Information	<p>The configuration file applicationsSignature.xml opens the Software Library dialog box. For details, see "Software Library Dialog Box" on page 184.</p> <p>The applicationsSignature.xml file contains a list of all applications that DFM attempts to find in the environment.</p>
Relevant tasks	"Discover Running Software – Scenario" on page 130

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to open the Global Configuration Files dialog box, to select configuration files that are needed by the adapter.
	Click to delete a selected configuration file.
	Select a configuration file and click to open the appropriate editor. For example, the file <code>msServerTypes.xml</code> opens the Script Editor.

Adapter Parameters Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to open the Parameter Editor. Enter details on the parameter. The value you enter here is assigned to the attribute.
	Click to remove a parameter.
	Select a parameter and click the button to open the Parameter Editor and make changes.
Name	Each row represents the definitions for one parameter.
Value	Separate values with commas.

Adapter Management Tab

Enables you to define additional options relevant to adapter execution and result filtering.

To access	Select a specific adapter in the Resources pane and click the Adapter Management tab.
Important Information	Click the Save button to save any changes you make.
See also	"The DiscoveryProbe.properties File" on page 110

Probe Selection Pane

Enables you to specify which Probe to use with an adapter.

To access	Select a specific adapter in the Resources pane and select the Adapter Management tab.
Important Information	<p>By default, DFM automatically chooses the Probe for the Trigger CI according to the CI's related node. After obtaining the CI's related node, DFM chooses one of the node's IPs and chooses the Probe according to the Probe's network scope definitions.</p> <p>This may fail in the following situations:</p> <ul style="list-style-type: none"> ▶ A Trigger CI does not have a related node (such as the network CIT). ▶ A triggered CI's node has multiple IPs, each belonging to a different Probe. <p>To resolve these issues, you can specify which Probe to use with the adapter by:</p> <ul style="list-style-type: none"> ▶ In the Probe Selection section, selecting Override default probe selection. ▶ In the Probe box, typing the Probe to use for the task.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
Override default probe selection	You can use calculated values such as: <code>\${Network.network_domain}</code> This value uses a syntax similar to that used by Triggered CI data in the Adapter Definition tab > Input pane. For details, see "Input Pane" on page 143.

Execution Options Pane

The following elements are included:

GUI Element (A–Z)	Description
<p>Create communication log</p>	<p>Choose to create a log file that logs the connection between the Probe and a remote machine.</p> <ul style="list-style-type: none"> ▶ Always. A communication log is created for this session. ▶ Never. A communication log is not created for this session. ▶ On Failure. A communication log is created for this session, only if the execution fails. <p>That is, DFM reports an error (report of a warning does not create a communication log). This is useful when you need to analyze which queries or operations take most of the time, send data for analysis from different locations, and so on.</p> <p>If the job completes successfully, no log is created.</p> <p>When requested (in the Discovery Status pane), DFM displays the log retrieved from the Probe (if a log has been created). For details, see "Discovery Status Pane" on page 285.</p> <p>Note: For debug purposes, you can always retrieve the communication logs for the last 10 executions, even if Create communication logs is set to On Failure.</p> <p>Communication log files are created on the Probe Manager under the C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog folder. For details on how the communication logs work, see "Record DFM Code" in the <i>ODB Developer Reference Guide</i>.</p>
<p>Include Results in Communication Log</p>	<p>Select to enable capturing the discovered results with the created communication log; these discovered results may help in investigating various discovery problems.</p>
<p>Max. Execution Time</p>	<p>The maximum time allowed for an adapter to run on one Trigger CI.</p>

GUI Element (A–Z)	Description
Max. Threads	<p>Each job is run using multiple threads. You can define a maximum number of threads that can be used concurrently when running a job. If you leave this box empty, the Probe's default threading value is used (8).</p> <p>The default value is defined in DiscoveryProbe.properties in the defaultMaxJobThreads parameter.</p> <p>Note: The jobs in the Network – Host Resources and Applications module require a permanent connection to the Probe's internal database. Therefore, these jobs are limited to a maximum number of 20 concurrent threads (which is the maximum number of concurrent connections permitted to the internal database). For details, see "Host Resources and Applications" in the <i>ODB Discovery and Integration Content Guide</i> PDF.</p>

Results Management Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Automatic Deletion	<p>Enables marking specific CITs for deletion or as candidates for deletion, if the Data Flow Probe does not find them during its next invocation.</p> <p>To add CITs to the list of CIs, click the Add button. In the Choose Discovered Class dialog box, choose the CITs that should be automatically deleted.</p> <p>The changes you make here are added to the adapter file, for example:</p> <pre data-bbox="592 664 1071 864"> <resultMechanism isEnabled="true"> <autoDeleteCITs isEnabled="true"> <CIT>shell</CIT> <candidateForDeletionCIT>node</ candidateForDeletionCIT> </autoDeleteCITs> </resultMechanism> </pre> <p>For details on how the Data Flow Probe handles CI deletion, see "Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 124.</p>
Enable aging	<p>Select this check box to run the aging mechanism that specifies how long a period must pass in which CIs are discovered, before DFM treats these CIs as no longer relevant and removes them. For details on aging, see "The Aging Mechanism Overview" in the <i>ODB Administration Guide</i>.</p>

GUI Element (A–Z)	Description
Enable Automatic Deletion	<p>Choose between:</p> <ul style="list-style-type: none"> ▶ Always. Automatic Deletion or Candidate for Deletion is always enabled, regardless of whether discovery succeeds or fails. ▶ On Success or Warnings. Automatic Deletion or Candidate for Deletion is enabled only when discovery finishes with a success or warning status. In the case of a discovery error, nothing is removed and CIs are not marked as a candidate for deletion. ▶ Only on Success. Automatic Deletion or Candidate for Deletion is enabled only when discovery finishes with a success status. In the case of a discovery error or warning, nothing is removed and CIs are not marked as a candidate for deletion (this is the default). <p>When this check box is selected, the Automatic Deletion pane is enabled. For details, see "Automatic Deletion" on page 154.</p> <p>For details on how the Data Flow Probe handles CI deletion, see "Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 124.</p>

GUI Element (A–Z)	Description
<p>Enable collecting 'Discovered by' data</p>	<ul style="list-style-type: none"> ▶ Selected. DFM collects data on the results of running the adapter. This data is then used to enable rediscovery of CIs. The data is necessary for the Discovery tab in IT Universe to function correctly. It is also used for the View Based Discovery Status functionality which leverages the data to aggregate the complete discovery status for certain views. ▶ Cleared. DFM does not collect this data. The check box needs to be cleared for adapters where rediscovery is not helpful. For example, the Range IPs by ICMP job has this check box cleared by default because its Trigger CI is the Probe Gateway and so all CIs discovered by this job have the same Trigger CI. If the check box was not cleared, a rediscovery attempt on any view containing any single IP would result in a ping sweep throughout the entire customer network, certainly not desirable behavior. <p>The job results of this adapter are displayed in the Discovery for View dialog box only if this check box is selected. For details, see "Check Status of Application Discovery (Rediscover a View)" and "Discovery and Changes Summary Dialog Box" in the <i>Modeling Guide</i>.</p>
<p>Fail entire bulks due to invalid CIs</p>	<p>If a set of objects (for example, 1,000 objects) includes even one invalid CI (for example, a node cannot be identified because of missing topological information), the reconciliation engine drops the entire set and does not send it to the CMDB. This is the default behavior.</p> <p>Clear the check box to have the results sent to the ODB with only the invalid CIs (and their topology) dropped from the results. In the above example, 999 objects would be processed. BSM displays an error message when you view the results.</p>

Result Grouping Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
Grouping Interval (Seconds)	To group results in the Probe before they are sent to the server, type the value that indicates how long results are stored in the Probe before being transferred to the server. The default value is 30 seconds. Note: If you enter a value in both boxes, DFM applies the value of whichever occurs first.
Max. CIs in group	Specify the number of CIs that should accumulate in the Probe before being transferred to the server. The default value is 5000.

Adapter Management Window

Enables you to view or edit default parameter values used for the DFM process.

To access	Admin > ODB Administration > Data Flow Management > Adapter Management or right-click a job in the Discovery Control Panel window and click Go to Adapter .
------------------	--




<p>Important Information</p>	<p>Note: An asterisk (*) next to a resource (adapter, script, or configuration file) signifies that the resource has changed since the package (in which it is included) was deployed. If the original package is redeployed, the changes are deleted from the resource. To save the changes, move the resource to a new package and deploy the package (the asterisk disappears).</p> <p>Caution: Only administrators with an expert knowledge of the DFM process should delete packages.</p>
<p>See also</p>	<ul style="list-style-type: none"> ➤ "Adapter Definition Tab" on page 143 ➤ "Global Configuration Files Pane" on page 148 ➤ "Adapter Management Tab" on page 150 ➤ "Script Pane" on page 179 ➤ "Resources Pane" on page 175 ➤ <i>ODB Discovery and Integration Content Guide PDF</i> ➤ "Configuration File Pane" on page 163


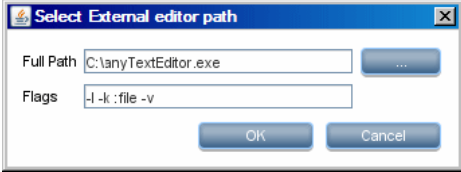



Adapter Source Editor Window

Enables you to edit an adapter script.

<p>To access</p>	<p>Right-click an adapter in the Resources pane and select Edit Adapter Source.</p>
<p>See also</p>	<p>"Resources Pane" on page 175</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	<p>Find specific text in the adapter script. For details, see "Find Text Dialog Box" on page 166.</p>
	<p>Click to go to a specific line in the adapter script. In the Go To Line dialog box, enter the line number.</p>
	<p>Click to open the adapter script in an external text editor.</p>




GUI Element (A–Z)	Description
	<p>Click to edit the external editor preferences. You can run the editor by adding flags to the path.</p> <p>In the following example:</p>  <p>:file sets the place of the file in relation to the flags. The user cannot set the file name.</p>
	<p>Click to toggle between the advanced editor and a simple text editor. You can use the simple editor when the advanced editor causes problems.</p>
	<p>Signifies that the code is valid.</p>
	<p>Signifies that the code is invalid.</p>

Attribute Assignment Editor Dialog Box

Enables you to define a regular expression that discovers specific running software according to a CIT's attribute value.

To access	Click Set Attributes in the Software Identification Rule Editor dialog box.
Relevant tasks	"Discover Running Software – Scenario" on page 130
See also	<ul style="list-style-type: none"> ▶ "Parse Rule Editor Dialog Box" on page 172 ▶ "Attribute Editor Dialog Box" on page 160 ▶ "Software Identification Rule Editor Dialog Box" on page 181

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to add a regular expression that determines the attribute of the CI to be discovered, or to add an attribute.
	Click to edit an existing regular expression or attribute.
	Click to delete the regular expression or the attribute.
Attribute assignments for type	For details, see "Attribute Editor Dialog Box" on page 160.
Parsing Rules	For details, see "Parse Rule Editor Dialog Box" on page 172.

Attribute Editor Dialog Box

Enables you to define a rule that discovers a CIT according to an attribute. The attribute is defined according to a regular expression.

To access	Software Identification Rule Editor > Set Attributes button > Attributes Assignment Editor. Click the Add button in the Attributes Assignment for Type pane.
Relevant tasks	"Discover Running Software – Scenario" on page 130
See also	"Parse Rule Editor Dialog Box" on page 172

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Name	Choose from the list of attributes of the CIT selected in the Editor. This attribute name is replaced by the value found by the regular expression. To find an attribute, start typing the name.


GUI Element (A–Z)	Description
Type	The type of operation defined for the attribute, for example, Boolean, string, date, and so on.
Value	<p>The value that replaces the name in the Rule ID field in the Parse Rule Editor dialog box.</p> <p>Use the following syntax for the value:</p> <pre>\${<rule ID name>(<group number>)}</pre> <p>For example, <code>\${DB_SID(1)}</code> means that DFM should search for the Rule ID with the name <code>DB_SID</code> and retrieve its regular expression.</p> <p>DFM should then retrieve the code for the first group (1). For example, in the regular expression <code>.\s+(\w+)\\$</code>, the first group is <code>(\w+)\\$</code>, that is, a word or words that appear at the end of the line.</p>

Choose Discovered Class Dialog Box

Enables you to choose CITs that are to be discovered by a selected adapter and to limit links so that they are mapped only when they connect specific CITs.

To access	<ul style="list-style-type: none"> ▶ Admin > ODB Administration > Data Flow Management > Adapter Management. In the Resources pane, select an adapter. In the Adapter Definition tab > Discovered CITs pane, click the Add Discovered CIT button. ▶ Admin > ODB Administration > Data Flow Management > Adapter Management. In the Resources pane, select an adapter. In the Adapter Management tab > Results Management pane, select the Enable Automatic deletion check box and click the Add button in the Automatic Deletion pane.
------------------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets>):





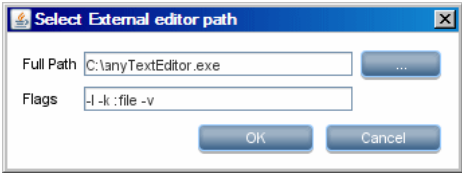
GUI Element (A-Z)	Description
<p>Link</p>	<p>Enables DFM to discover CITs only when they are linked by link types you choose in this box.</p> <p>Note: This section is relevant only when adding a discovered CIT, not for defining CITs for automatic deletion.</p> <p>Select a link type from the list and click the button  in the End 1 and End 2 boxes to open the Choose Configuration Item Type dialog box. Choose the CITs that DFM should map when they are linked by the selected link type.</p> <p>Note: DFM automatically recognizes the links between CIs and adds them to the map of discovered CITs. However, during adapter writing, you may need to exclude links between certain CITs. For example, both nodes and IPs and nodes and ports are linked by usage. You may need to receive results only for nodes and IPs that are connected by the usage link, and not nodes and ports. The End 1 and End 2 links determine the result received from the adapter, and this result is reflected in the map, as can be seen in the following example:</p> <div data-bbox="582 1020 1185 1357" data-label="Diagram"> <pre> graph TD ConfigDoc[Configuration Document] -- Usage_5 --> WebServer[WebServer] WebServer -- Usage_4 --> RunningSoftware[RunningSoftware] RunningSoftware -- Usage_3 --> IpAddress[IpAddress] RunningSoftware -- Usage_1 --> IpServiceEndpoint[IpServiceEndpoint] RunningSoftware -- Usage_2 --> NodeElement[NodeElement] NodeElement -- Usage --> TCP_IP_Port[TCP/IP Port] </pre> </div>
<p>Object</p>	<p>Select a CIT to be added to the list of CITs that an adapter is to discover. Save the changes by clicking the Save button at the bottom of the Adapter Definition pane.</p>




Configuration File Pane

Enables you to edit a specific configuration file that is part of a package. For example, you can edit the **portNumberToPortName.xml** file so that specific port numbers, names, or types are discovered.

To access	Click a specific configuration file in the Resources pane.
Important Information	<p>The following files are for internal use only and should only be changed by users with an advanced knowledge of adapter-writing:</p> <ul style="list-style-type: none"> ▶ discoveryPolicy.xml ▶ jythonGlobalLibs.xml <p>For details, see "Resource Files" on page 138 and "Internal Configuration Files" on page 141.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Find specific text in the configuration file. For details, see "Find Text Dialog Box" on page 166.
	Click to go to a specific line in the configuration file. In the Go To Line dialog box, enter the line number.
	Click to open the file in an external editor.
	<p>Click to edit the external editor preferences. You can run the editor by adding flags to the path.</p> <p>In the following example:</p> <div data-bbox="592 1241 1049 1414" data-label="Image">  </div> <p>:file sets the place of the file in relation to the flags. The user cannot set the file name.</p>

GUI Element (A–Z)	Description
	Click to toggle between the advanced editor and a simple text editor. You can use the simple editor when the advanced editor causes problems.
	For XML files, signifies that the code is valid.
	For XML files, signifies that the code is not valid.

Edit Process Dialog Box

Enables you to add a process that can identify specific running software.

To access	Click the Add button in the Identifying Processes pane in the Software Identification Rule Editor dialog box.
See also	"Software Identification Rule Editor Dialog Box" on page 181

The following elements are included:

GUI Element (A–Z)	Description
Attributes	Opens the Attributes Assignments Editor dialog box for the identifying process.
Command Line	The running software can also be mapped using the process name. In this case, you must add a process command line (or part of it) with which the process name uniquely identifies the software, for example, c:\ora10\bin\oracle.exe UCMDB.
Key Process	Select this check box if, during discovery, DFM must distinguish between applications that run similar processes (IP, port, command line, or owner). For an explanation of this box, see "Identifying Running Software by Processes" on page 127.


GUI Element (A–Z)	Description
Main process	Select this check box to mark this process as a unique and distinguishing process. For such processes there need to be several instances of the software CI.
Name	Enter the exact name of the process, for example, java.exe .
Port	<p>Add a port number or name, either by typing a number or by clicking the Add button then selecting the ports in the Global Ports List.</p> <ul style="list-style-type: none"> ▶ If the process has to listen at a specific port, the port should be listed. You can enter more than one port, separated by commas, for example, 8888,8081,8080,81,8000,82,80. ▶ If the process does not have to listen at a specific port (that is, the running software can use any port), select the All Ports option.
Port match is optional	<ul style="list-style-type: none"> ▶ Select this check box to enable discovery of processes that are not listening at any of the ports entered in the Port field (that is, identification is by process name only). ▶ Clear this check box to enable discovery of processes based on process name and the port number entered in the Port field.

Find Resource/Jobs Dialog Box

Enables you to build a search query to find a particular resource or job.

To access	<ul style="list-style-type: none"> ▶ Discovery Control Panel > Discovery Modules pane. Click the Search for Discovery Job button. ▶ Adapter Management > Resources pane. Click the Find resource button.
See also	"Resources Pane" on page 175

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element (A–Z)	Description
	Click to select a CIT from the dialog box that opens. Click OK to return to the Find Resource dialog box. Note: This button is not accessible when Name is selected.
Direction	Searches forwards or backwards through the packages.
Find Discovery resource by/ Find Discovery Job by	Choose between: <ul style="list-style-type: none"> ▶ Name. Enter the name, or part of it, of the resources. ▶ Adapter input type. CIs that trigger the job. Click the button to open the Choose Configuration Item Type dialog box. Locate the CI type that you are searching for. ▶ Adapter output type. CIs that are discovered as a result of the job or the adapter.
Find Next	The next resource meeting the search criteria is highlighted in the Resources pane.

Find Text Dialog Box

Enables you to find text in a script or configuration file.

To access	Select a script or configuration file and click the Find text button in the file pane.
------------------	---

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	<ul style="list-style-type: none"> ▶ Click Find to find one instance of the text you are searching for. ▶ Click Find All to find all instances of the text.
Direction	Search forwards or backwards through the script or configuration file.
Find what	Type the text to be found or click the down arrow to choose from previous searches. Click the adjacent arrow to display a list of symbols you can use in wildcard or regular expression searches. This arrow is enabled when you select the Use option.
Options	Select an option to narrow your search.
Origin	Enables a search of the entire scope or from the current cursor position.
Target	<ul style="list-style-type: none"> ▶ Global. Searches throughout the file. ▶ Selected Text. Searches through the selected text.

Input Query Editor Window

Enables you to define which CIs can be Trigger CIs for jobs that run a specific adapter.

To access	Admin > ODB Administration > Data Flow Management > Adapter Management > select an adapter > Adapter Definition tab > Input pane > click the Edit button next to the Input Query box.
See also	<ul style="list-style-type: none"> ▶ "Trigger CIs and Trigger Queries" on page 29 ▶ "Trigger Query Editor Window" on page 332

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Panes>	<ul style="list-style-type: none"> ▶ CI Type Selector Pane ▶ Editing Pane ▶ Information Pane
Query Name	The name of the adapter's input query.

CI Type Selector Pane

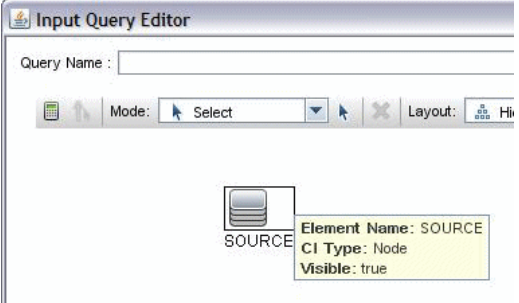
Displays a hierarchical tree structure of the CI Types found in the CMDB. For more details, see "CI Type Manager User Interface" in the *Modeling Guide*.

Note: The number of instances of each CIT in the CMDB is displayed to the right of each CIT.

To access	To create or modify a query, click and drag nodes to the Editing pane and define the relationship between them. Your changes are saved to the CMDB.
Relevant tasks	<ul style="list-style-type: none"> ▶ "Define a TQL Query" in the <i>Modeling Guide</i> ▶ "Create a Pattern View" in the <i>Modeling Guide</i>
See also	"Add Query Nodes and Relationships to a TQL Query" in the <i>Modeling Guide</i> .

Editing Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

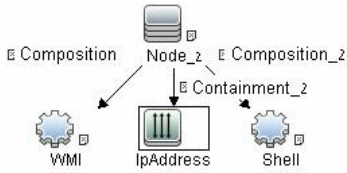
GUI Element (A–Z)	Description
<node>	Hold the cursor over a node to view information about the node:  <p>The screenshot shows a window titled "Input Query Editor" with a "Query Name:" field. Below the field is a toolbar with icons for "Mode:" (set to "Select"), "Layout:", and "Hi". In the center, a node labeled "SOURCE" is highlighted, and a tooltip displays the following information: "Element Name: SOURCE", "CI Type: Node", and "Visible: true".</p>
<right-click menu>	For details, see "Shortcut Menu Options" in the <i>Modeling Guide</i>
<Toolbar>	For details, see "Toolbar Options" in the <i>Modeling Guide</i>

Information Pane

Displays the properties, conditions, and cardinality for the selected node and relationship.

Important Information

Hold the pointer over a node to view information:




```

graph TD
    Node_2[Node_2] -- Composition --> WMI[WMI]
    Node_2 -- Containment_2 --> IpAddress[IpAddress]
    Node_2 -- Composition_2 --> Shell[Shell]
    
```

Element Name: WMI
 CI Type: WMI
 Visible: false
 Cardinality: Composition (Node_2, WMI) : 1..*

A small green indicator is displayed next to the tabs that include information:



```

graph TD
    Node[Node] -- Containment --> IpAddress_2[IpAddress_2]
    
```

Attributes	* Cardinality	Qualifiers
Containment (Node, IpAddress_2) : 1..*		

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Edit button	Select a node or relationship in the Editing pane and click the Edit button to open the Query Node Properties dialog box. For details, see "Query Node/Relationship Properties Dialog Box" in the <i>Modeling Guide</i> .
Attributes	Displays the attribute conditions defined for the node or the relationship. For details, see "Attribute Tab" in the <i>Modeling Guide</i> .
Cardinality	Cardinality defines how many nodes you expect to have at the other end of a relationship. For example, in a relationship between node and IP, if the cardinality is 1:3, the query retrieves only those nodes that are connected to between one and three IPs. For details, see "Cardinality Tab" in the <i>Modeling Guide</i> .
Details	<ul style="list-style-type: none"> ▶ CI Type. The CIT of the selected node/relationship. ▶ Visible. A tick signifies that the selected node/relationship is visible in the topology map. When the node/relationship is not visible, a box <input type="checkbox"/> is displayed to the right of the selected node/relationship in the Editing pane: <div data-bbox="591 1012 901 1263" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> </div> <ul style="list-style-type: none"> ▶ Include subtypes. Display both the selected CI and its descendants in the topology map. <p>Note: To change the visible and subtype settings, select a node in the Editing pane and click the Edit button. In the Query Node Properties dialog box, select or clear the boxes.</p>

GUI Element (A-Z)	Description
Qualifiers	Displays the qualifier conditions defined for the node or the relationship. For details, see "Qualifier Tab" in the <i>Modeling Guide</i> .
Selected Identities	Displays the element instances that are used to define what should be included in the query results. For details, see "Identity Tab" in the <i>Modeling Guide</i> .

Parse Rule Editor Dialog Box

Enables you to create a rule that matches an attribute to process-related information (IP, port, command line, and owner).

To access	Software Identification Rule Editor > Set Attributes > Attributes Assignment Editor > Parsing Rules > Add
Important Information	Only users with a knowledge of regular expressions should make changes to a rule.
Relevant tasks	"Discover Running Software – Scenario" on page 130
See also	<ul style="list-style-type: none"> ➤ "Attribute Editor Dialog Box" on page 160 ➤ "Software Identification Rule Editor Dialog Box" on page 181

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Process Attribute	Choose between the Port , IP , Command Line , Name , or Owner process-related information. The rule is invoked on the attribute you choose here.

GUI Element (A–Z)	Description
Regular Expression	<p>Enables you to create a dynamic expression that finds at least one process that defines this running software. The regular expression is invoked on the value in the Process Attribute field.</p> <p>For example, a command line process includes the following regular expression:</p> <pre>.\s+(\w+)\$</pre> <p>This expression searches for any character, followed by a space or spaces, followed by a word or words (a-z or A-Z or 0-9) that appear at the end of the line.</p> <p>The following command line matches this regular expression: <code>c:\ora10\bin\oracle.exe UC MDB</code></p>
Rule ID	<p>Enter a unique name for the rule. The Rule ID is needed to identify the rule in the Attributes Assignment Editor pane. For details, see "Additional Attributes" on page 182.</p>

Permission Editor Dialog Box




Enables you to configure an adapter you have written, so that users can view permissions for the job.

To access	Admin > ODB Administration > Data Flow Management > Adapter Management > select an adapter > Adapter Definition tab > Required Permissions pane > click the Add button.
Important Information	The information you define here is not dynamic, that is, if an adapter is changed, the information in this dialog box is not updated.
See also	<ul style="list-style-type: none"> ➤ "Discovery Permissions Window" on page 299 ➤ "Viewing Permissions While Running Jobs" on page 242 ➤ "Required Permissions Pane" on page 146 ➤ "Discovery Job Details Pane" on page 285

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
Operation	The action that is being run.
Permission	Enter a name for the permission, to appear in the Required Permissions pane.
Usage Description	Free text that you enter to describe the permission object and its parameters. This text is usually a general comment on the type of permission object, whereas the description is a more specific comment. For example, you could enter Permissions for host machines here, and Permissions for host machines running on Windows for a particular row.

Permission Objects and Parameters Dialog Box





GUI Element (A–Z)	Description
	Click to open the Permission Object and Parameter dialog box. You can enter more than one object or parameter for each permission. The information you enter in this dialog box appears in the Required Permissions pane, in the Objects and Parameters column.
	Click to delete a permission object.
	Click to edit an existing permission object.
Context	Specific information about the permission object's environment, for example, Windows or UNIX.
Parameter	The parameters that are needed during the job run. For example, the UNIX permission object <code>cat</code> needs the <code>/etc/passwd</code> parameter.
Permission Object	The name of the command, table, or other content of the Jython script.



Resources Pane

Enables you to locate a specific package, adapter, script, configuration file, or external resource. You can also create an adapter, Jython script, configuration file, or Discovery wizard, and you can import an external resource.

To access	Admin > ODB Administration > Data Flow Management > Adapter Management
Important Information	<p>Depending which level you select in the Resources pane, different information is displayed in the View pane.</p> <p>If you select:</p> <ul style="list-style-type: none"> ▶ One of the following folders: Discovery Packages root, a specific package, an adapter, script, configuration file, or external resource: a list of the resources in that folder is displayed. To access a resource directly, double-click the resource in the View pane. ▶ A specific adapter: The Adapter Definition and Adapter Management panes are displayed. For details, see "Adapter Definition Tab" on page 143 and "Adapter Management Tab" on page 150. ▶ A script or configuration file: The script editor is displayed. For details, see "Script Pane" on page 179. ▶ An external resource: Information about the file is displayed.
See also	"Package Manager User Interface" in the <i>ODB Administration Guide</i> .

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	<p>Click to:</p> <ul style="list-style-type: none"> ▶ Create an adapter. Enter the adapter name, choose whether it should be used as a discovery adapter or for integration. For integration adapters, choose the integration type from the list of available types. Click OK. The new adapter is added to the << No Package >> folder. Edit the adapter. For details, see "Adapter Definition Tab" on page 143 and "Adapter Management Tab" on page 150. For details on moving an adapter to a package, see "Create a Custom Package" in the <i>ODB Administration Guide</i>. For details on creating integration adapters, see "Discovery and Integration Adapters" on page 26. ▶ Create a Jython script. Enter the script name. For details, see "Script Pane" on page 179. ▶ Create a configuration file. Enter the configuration file name. By default, the file takes an .xml extension. To give the file another extension, for example, *.properties, name the file and include the extension. Add the appropriate XML code or other content. For XML files, you can save the file only if it is valid. For details, see "Configuration File Pane" on page 163. ▶ Import an external resource. In the browser that opens, locate the resource to be imported and click Open. ▶ Create a Discovery Wizard. Name the new wizard. By default, the file takes an .xml extension. A new file is added to the Discovery Wizard folder of the << No Package >> folder. The file is in template format.
	<p>Click to delete the resource.</p>
	<p>Click to open the Find Resource dialog box. For details on filtering, see "Filtering Results" on page 63.</p>
	<p>Click to refresh the list of packages.</p>

GUI Element (A–Z)	Description
	Packages tree. Displays a list of all packages.
	Package root. Displays a list of all resources included in the package. You can view any of these resources by clicking the resource in the Resources pane.
<Configuration files>	<p>Right-click a file to:</p> <ul style="list-style-type: none"> ▶ Save as. Saves the file under a new name. Use this option to clone an existing file. The new file includes all attributes of the existing file. Make any necessary changes to the file and save it. ▶ Delete. Deletes the configuration file. The resource is removed completely from the system. ▶ Open in Frame. Select to open the file in a new window.
<External resource files>	<p>An external resource is any file needed to perform discovery or integration by DFM. For example, the <code>nmap.exe</code> file is needed for credential-less discovery.</p> <ul style="list-style-type: none"> ▶ Right-click a file to: <ul style="list-style-type: none"> ▶ Save as. Save the resource under a new name. Use this option to clone an existing resource. The new resource includes all attributes of the existing resource and is saved to the same location in the file system. Make any necessary changes to the new resource and save it. ▶ Delete. Deletes the file. The file is removed completely from the system. ▶ Select the file to display information in the View pane. You can open an external resource or export it.

GUI Element (A–Z)	Description
<Adapter files>	<p>Right-click a file to:</p> <ul style="list-style-type: none"> ▶ Save as. Save the adapter under a new name. Use this option to clone an existing adapter. The new adapter includes all attributes of the existing adapter. Give a name to the new adapter, and change the necessary attributes. ▶ Delete. Deletes the adapter. The adapter is removed completely from the system. ▶ Go to Discovery job. When enabled, click to open the Discovery Control Panel window with the job selected. This option is enabled if the adapter is included in a job. ▶ Edit adapter source. Opens the adapter source editor where you can make changes to the adapter. For details, see "Adapter Source Editor Window" on page 158.
<Script files>	<p>Right-click a file to:</p> <ul style="list-style-type: none"> ▶ Save as. Save the script under a new name. Use this option to clone an existing script. The new script includes all attributes of the existing script. Make any necessary changes to the script and save it. ▶ Delete. Deletes the script. The script is removed completely from the system. ▶ Open in Frame. Select to open the script in a new window. For details on editing the script, see "Adapter Source Editor Window" on page 158.

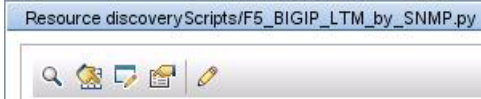
Script Editor Window

Enables you to edit a specific script that is part of a package.




To access	<ul style="list-style-type: none"> ▶ Right-click a script in the Resources pane and choose Open in Frame. ▶ Select a configuration file in the Global Configuration Files pane and click the Edit button. <p>For details, see "Script Pane" on page 179.</p>
------------------	--


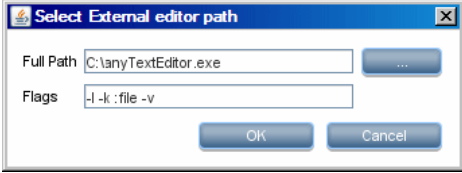




Script Pane

Enables you to edit a specific script that is part of a package.

To access	Click a specific script in the Resources pane.
Important Information	<p>The script pane title bar includes the actual physical location of the script. For example, the following script is located in C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryScripts (or probeGateway\discoveryScripts):</p> 
See also	"Adapter Development and Writing" in the <i>ODB Developer Reference Guide</i>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Find specific text in the script. For details, see "Find Text Dialog Box" on page 166.
	Click to go to a specific line in a script. In the Go To Line dialog box, enter the line number.
	Click to open the script in an external text editor.

GUI Element (A–Z)	Description
	<p>Click to edit the external editor preferences. You can run the editor by adding flags to the path.</p> <p>In the following example:</p>  <p>:file sets the place of the file in relation to the flags. The user cannot set the file name.</p>
	<p>Click to toggle between the advanced editor and a simple text editor. You can use the simple editor when the advanced editor causes problems.</p>
	<p>For Jython files, signifies that the code is valid.</p>
	<p>For Jython files, signifies that the code is not valid.</p>
	<p>See Validation Information below.</p> <p>Note: This button is displayed when a script contains Framework API errors.</p>






GUI Element (A–Z)	Description
<script>	The Jython script used by the package. For details on working with Jython, see "Create Jython Code" in the <i>ODB Developer Reference Guide</i> .
Validation Information	<p>If a script is not valid, Validation Information displays the errors in the script, for example:</p> <p>Script has failed validation. At line 48: Factory.getProtocolProperty() found. This is a problem - Usage of Factory is deprecated. Use Framework.getProtocolProperty instead.</p> <p>Click Fix validation errors then OK to update the script.</p> <p>The error may occur due to changes in the Framework object's API. For details, see "HP Universal CMDB Web Service API" in the <i>ODB Developer Reference Guide</i>.</p>

Software Identification Rule Editor Dialog Box

Enables you to define a new running software rule.

To access	Data Flow Management > Discovery Control Panel. In the Discovery Modules pane, select Network > Host Resources and Applications > Software Element CF by Shell . In the Properties tab, select Global Configuration Files > applicationSignature.xml . In the Software Library dialog box, click the Add button or select an existing element and click the Edit button.
Important Information	Each parse rule must be matched by at least one process.
Relevant tasks	"Discover Running Software – Scenario" on page 130
See also	"Global Configuration Files Pane" on page 148

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to add attributes to the component. For details, see "Attribute Assignment Editor Dialog Box" on page 159.
	Click to open the Optional Configuration Files dialog box.
	Click to add a process.
	Select a process and click to delete.
	Select a process and click to edit.
Additional Attributes	To add attributes, click the Set Attributes button. For details, see "Attribute Assignment Editor Dialog Box" on page 159.
Category	<p>You can:</p> <ul style="list-style-type: none"> ▶ Choose the category under which the new running software should appear. ▶ Change the category for an existing element. ▶ Add a new category by typing its name in this field. <p>The changes you make here are immediately displayed in the Software Library dialog box.</p>
CI Type	Select the CIT that is to be discovered.
Discovered Product Name	The name of the running software to be created by this signature.
Identifying Processes	To add a process that can identify specific running software, click the Add button. The Edit Process dialog box opens. For details, see "Edit Process Dialog Box" on page 164.





GUI Element (A–Z)	Description
Optional Configuration Files	<p>A list of configuration files</p> <p>Click the Set Configuration Files button to open the Optional Configuration Files dialog box.</p> <p>To add a configuration file, in the Optional Configuration Files dialog box, click the Add button and, in the Configuration File Names box, enter the full path to the running software's configuration file and the file name.</p>
Software Signature ID	<p>The name of the definition.</p> <p>Note: This is not the running software's name but a name you give to differentiate this discovery from similar discoveries.</p>
Supported versions	<p>Versions supported for this running software.</p>
Vendor	<p>The vendor of this running software.</p>

Software Library Dialog Box

Enables you to view the logical groups of running software.

To access	<ul style="list-style-type: none"> ▶ Discovery Control Panel window > Network Discovery > select one of the Host Resources and Applications module jobs. Locate the Global Configuration Files pane in the Properties tab. Select applicationsSignature.xml and click the Edit button. ▶ Adapter Management window > select one of the Host_Resources_By_SNMP/TTY/WMI adapters. Locate the Global Configuration Files pane in the Adapter Definition tab. Select applicationsSignature.xml and click the Edit button. ▶ In the Infrastructure Wizard Preferences page, open the Choose Software Element to be discovered box.
Important Information	<p>The software elements are organized in logical categories. You can change the names of these elements, you can move an element to another category, and you can define new elements and categories. For details, see the Category entry in "Software Identification Rule Editor Dialog Box" on page 181.</p> <p>The code you define in this dialog box and the Software Element Editor dialog box overwrites the code in applicationsSignature.xml.</p>
Relevant tasks	"Discover Running Software – Scenario" on page 130
See also	"Global Configuration Files Pane" on page 148

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	<p>Select a check box to include a category or software element in the discovery.</p> <p>Clear a check box to remove the category or element from the discovery.</p>
	<p>Click to define a new software element. For details, see "Software Identification Rule Editor Dialog Box" on page 181.</p>
	<p>Select a software element and click to delete the element.</p>
	<p>Select a software element and click to make changes to the element. For details, see "Software Identification Rule Editor Dialog Box" on page 181.</p>
<p><List of software elements></p>	<p>List of objects that are software elements.</p>

Part III

Integration

7

Integration Studio

This chapter includes:

Concepts

- ▶ Integration Studio Overview on page 190

Tasks

- ▶ Work with Federated Data on page 194
- ▶ Work with Population Jobs on page 195
- ▶ Work with Data Push Jobs on page 197

Reference

- ▶ Integration Studio User Interface on page 199
- ▶ Out-of-the-Box Integrations on page 213

Troubleshooting and Limitations on page 214

Concepts

Integration Studio Overview

The Integration Studio is where you manage your ODB integration points and connect and share information with external repositories, such as other ODBs, BTO Software products, or third party products.

Integration points in the ODB are based on adapters, which are entities that are capable of communicating with external data repositories. A basic set of adapters is provided with the ODB; however, you can create additional adapters using the Federation Framework SDK. For details, see "Add an Adapter for a New External Data Source" in the *ODB Developer Reference Guide*.

You can also create adapters in the Adapter Management module. For details, see "Resources Pane" on page 175.

For details about how to set up integration points for data integrations, see "Integration Studio Page" on page 208.

Integration points can be of one of the following types:

- "Population" on page 191
- "Federation" on page 191
- "Data Push" on page 193

Population

An integration of Population type copies data from an external data repository into the ODB, so that the ODB now controls the data.

You use population in one of the following scenarios:

- ▶ When you need to track changes made by the ODB at the CI level.
- ▶ When a remote repository is not reliable in terms of response time; for instance, a network delay prohibits you from setting up run-time federation with the repository.
- ▶ When a remote repository does not support federation capabilities (no appropriate adapter exists).

Federation

An integration of Federation type includes data in the ODB from other sources, in such a way that the source of the data still retains control of the data.

You use the ODB's federation capabilities to extend the scope of the existing topology query language (TQL) capabilities to encompass data that is stored and maintained in an external repository. The ability to include such information is important, as it prevents you from having to copy large amounts of data and instead bring it into your ODB only when it is really needed.

Federation also has the benefit that the federated data does not burden the ODB in terms of capacity; theoretically, you can set up an integration that federates trillions of CIs and relationships. Federated data is fetched at run time, as requested, which lessens the impact on system performance.

Note that the ODB does not offer change tracking on federated data, because the data does not reside within the ODB and the ODB is not notified when external data is modified.

Federated integration creates a federated integration point, which can then be used when defining TQL queries. For details on TQLs, see "Topology Query Language" in the *Modeling Guide*.

Retrieving Data from Multiple Federated Data Sources

During TQL calculation, you can retrieve data for the same CIT from several federated data sources. The data will be retrieved from the local ODB, as well as from other federated data sources, according to how you have configured integration points. As data arrives at the ODB, it is identified and reconciled, with the end result determined according to the configured reconciliation priority given to the various integrations.

Each CI that is retrieved from an external data repository includes an attribute (Created By) to show from which federated data source the CI has been retrieved.

For limitations, see "Limitations on Retrieving Data from Multiple Data Repositories" on page 214.

Retrieve Attributes from an External Data Repository

- ▶ You can retrieve the attributes of a CI from an external data repository, when the core CI data is stored in the ODB.
- ▶ The core data repository must be the ODB.
- ▶ The CIT must be located in a data repository for its attributes to be defined.
- ▶ The same attributes can be retrieved from multiple data repositories.
- ▶ For details on retrieval options, see the CI Type Retrieval Mode field on the "Federation Tab" on page 204.
- ▶ When you configure an integration point to include federated CIs, you must select either full federation of a CI, or the federation of an attribute alone. You cannot set up two integrations for the same CIT where one is mapped to an external CIT and the other is mapped to that same CIT with an external attribute.
- ▶ A CIT can support external attributes if the adapter (which is federating the CIT data) supports mapping information (reconciliation) for this CIT.

Reconciling Information

Federated queries should use the mapping engine to reconcile the CI from the ODB with the attributes from the external data repository.

For details on the Mapping Engine, see "Federation Framework Flow for FTQL" in the *ODB Developer Reference Guide*.

For details on selecting attributes to be included in the federation, see "Federation Tab" on page 204.

For details on how reconciliation is performed, see "Reconciliation" on page 339.

Use Cases

- ▶ You need to discover the SMS or Altiris desktops in your system. The desktop CIT is a core CIT and is already synchronized with the ODB. However, you do not want to store all the desktop data in the ODB as this is inefficient and unnecessary. It is enough to store core attributes such as name and MAC address in the ODB, and to define the other details of the desktops as external attributes in two data repositories: SMS and Altiris.
- ▶ VMware creates virtual machines that contain a virtual machine monitor (hypervisor) that allocates hardware resources dynamically and transparently. Multiple operating systems can run concurrently on a single physical computer. Since the allocation resources (for example, memory) are dynamic, DFM cannot discover these resources (DFM runs once every 24 hours and the resource data can change hourly). To enable Business Service Management to always be updated with real-time data, the solution is to divide the data into two: the core data of the virtual hosts should be discovered and placed in the ODB; the resource attributes should be retrieved from the external source. In this use case, the data for these attributes is retrieved from two data repositories: ODB and VMware.

Data Push

An integration of Data Push type copies data from the ODB to an external data repository, so that the ODB no longer retains control over this data.

You use data push integrations to feed important data from your ODB into an external system, in order to facilitate your necessary business processes. An example of this is pushing data discovered by DDM into HP Service Manager, where tickets may be opened that are connected to the actual CIs in your IT infrastructure.

Tasks

Work with Federated Data

This task explains how to set up and work with data that is federated from different CMDB sources.

This task includes the following steps:

- ▶ "Prerequisites" on page 194
- ▶ "Create an Integration Point" on page 194
- ▶ "Set Reconciliation Priority" on page 195
- ▶ "Select CITs and Attributes to be Federated" on page 195
- ▶ "Edit Adapter Configurations" on page 195
- ▶ "View Instances in IT Universe Manager" on page 195

1 Prerequisites

Set up the adapter. For details, see "Add an Adapter for a New External Data Source" in the *ODB Developer Reference Guide*.

For details on existing adapters, see "Out-of-the-Box Integrations" on page 213.

2 Create an Integration Point



Select **Admin > ODB Administration > Data Flow Management > Integration Studio**. Click the **Add** button to open the Create New Integration Point dialog box. For details, see "Create New Integration Point/Edit Integration Properties Dialog Box" on page 200.

3 Set Reconciliation Priority

For details, see "Reconciliation Priority Manager Window" on page 211.

4 Select CITs and Attributes to be Federated

For details, see "Federation Tab" on page 204.

5 Edit Adapter Configurations

Modify adapter configurations using the Adapter Management module.

Note: Since in ODB version 9.01 adapter files reside on both the Server and the Probe, manual editing of the adapter files is discouraged. Use the Adapter Management module of ODB to edit adapter files. For details, see "Manage Adapter Configurations" on page 135.

6 View Instances in IT Universe Manager

For details, see "IT Universe Manager Overview" in the *Modeling Guide*.

Work with Population Jobs

This task explains how to schedule population jobs and select the queries that will be used to populate the ODB with data.

This task includes the following steps:

- "Prerequisites" on page 196
- "Create an Integration Point" on page 196
- "Set Reconciliation Priority" on page 196
- "Edit Adapter Configurations" on page 196
- "Schedule the Population Job" on page 197
- "Build a View of the Population Results" on page 197

- ▶ "View Instances in IT Universe Manager" on page 197

1 Prerequisites

Set up the adapter. For details, see "Add an Adapter for a New External Data Source" in the *ODB Developer Reference Guide*.

For details on existing adapters, see "Out-of-the-Box Integrations" on page 213.

2 Create an Integration Point



Select **Admin > ODB Administration > Data Flow Management > Integration Studio**. Click the **Add** button to open the Create New Integration Point dialog box. For details, see "Create New Integration Point/Edit Integration Properties Dialog Box" on page 200.

3 Set Reconciliation Priority

For details, see "Reconciliation Priority Manager Window" on page 211.

4 Edit Adapter Configurations

Modify adapter configurations using the Adapter Management module.

Note: Since in ODB version 9.01 adapter files reside on both the Server and the Probe, manual editing of the adapter files is discouraged. Use the Adapter Management module of ODB to edit adapter files. For details, see "Manage Adapter Configurations" on page 135.

5 Schedule the Population Job

In this step you select queries that specify which CIs are copied to the ODB, and schedule these queries to run. For details, see "Population Tab" on page 210.

6 Build a View of the Population Results

For details, see "Modeling Studio Overview" in the *Modeling Guide*.

7 View Instances in IT Universe Manager

For details, see "IT Universe Manager Overview" in the *Modeling Guide*.

Work with Data Push Jobs

This task explains how to schedule data push jobs and select the queries that will be used to send data from the ODB to another data repository.

This task includes the following steps:

- "Prerequisites" on page 197
- "Create an Integration Point" on page 198
- "Set Reconciliation Priority" on page 198
- "Edit Adapter Configurations" on page 198
- "Schedule the Data Push Job" on page 198
- "Build a View of Data Push Results" on page 198
- "View Instances in IT Universe Manager" on page 198

1 Prerequisites

Set up the adapter. For details, see "Add an Adapter for a New External Data Source" in the *ODB Developer Reference Guide*.

For details on existing adapters, see "Out-of-the-Box Integrations" on page 213.

2 Create an Integration Point



Select **Admin > ODB Administration > Data Flow Management > Integration Studio**. Click the **Add** button to open the Create New Integration Point dialog box. For details, see "Create New Integration Point/Edit Integration Properties Dialog Box" on page 200.

3 Set Reconciliation Priority

For details, see "Reconciliation Priority Manager Window" on page 211.

4 Edit Adapter Configurations

Modify adapter configurations using the Adapter Management module.

Note: Since in ODB version 9.01 adapter files reside on both the Server and the Probe, manual editing of the adapter files is discouraged. Use the Adapter Management module of ODB to edit adapter files. For details, see "Manage Adapter Configurations" on page 135.

5 Schedule the Data Push Job

In this step you select queries that specify which CIs will be pushed to a remote repository from the ODB with CIs, and schedule these queries to run. For details, see "Data Push Tab" on page 204.

6 Build a View of Data Push Results

For details, see "Modeling Studio Overview" in the *Modeling Guide*.

7 View Instances in IT Universe Manager

For details, see "IT Universe Manager Overview" in the *Modeling Guide*.

Reference



Integration Studio User Interface

This section includes (in alphabetical order):

- "Create New Integration Point/Edit Integration Properties Dialog Box" on page 200
- "Create New Job Definition Dialog Box" on page 202
- "Credentials Dialog Box" on page 203
- "Data Push Tab" on page 204
- "Federation Tab" on page 204
- "Integration Points Pane" on page 206
- "Integration Studio Page" on page 208
- "Job Definition Pane" on page 209
- "Population Tab" on page 210
- "Reconciliation Priority Manager Window" on page 211

Create New Integration Point/Edit Integration Properties Dialog Box

This dialog box enables you to create a new integration point or edit the properties of an existing integration point.

To access	<p>Do one of the following:</p> <ul style="list-style-type: none"> ▶ Click the Create New Integration Point button  in the Integration Points pane. ▶ Click the Edit Integration Properties button  in the Integration Points pane.
Important information	<p>The list of fields contains all of the items that may be specified when you create an integration point. Not all of the fields are displayed for all adapters.</p> <p>Each required field is marked with an asterisk.</p>

User interface elements are described below:

UI Elements (A-Z)	Description
Adapter	<p>Select the adapter that your integration point will use. The following is the list of default adapters provided in the Integration Studio:</p> <ul style="list-style-type: none"> ➤ BACKPIsAdapter ➤ DDMi ➤ Local UCMDB History ➤ Microsoft SMS ➤ Service Center 6.2x ➤ Service Manager 7.0x ➤ Service Manager 7.1x ➤ UCMDB 8.x ➤ UCMDB 9.x ➤ UCMDB API Population <p>For details about each adapter, see "Out-of-the-Box Integrations" on page 213.</p>
Credentials	Allows you to set credentials for integration points. For details, see "Credentials Dialog Box" on page 203.
Integration Description	Enter a brief description of the integration point.
Integration Point Name	Enter a name for the integration point.
Is Integration Activated	Select this checkbox to create an active integration point. You clear the checkbox if you want to deactivate an integration, for instance, to set up an integration point without actually connecting to a remote machine.

UI Elements (A-Z)	Description
Probe Name	The name of the Data Flow Probe used to run population jobs.
Selected CI Instance	Enables you to select the trigger CI through which data is collected during integration. Note: The Selected CI Instance field is displayed only when you use an adapter that is based on a discovery resource. For details about Trigger CIs, see "Topology Map" in the <i>Modeling Guide</i> .



Note: Additional fields are available, depending on the adapter you select. Descriptions of each field may be viewed by hovering your mouse over that field on the screen. See the *ODB Developer Reference Guide* for details about specific adapters.


Create New Job Definition Dialog Box

This dialog box enables you to create and schedule population and data push jobs to be run at specific times.

To access	Click  on the Population or Data Push tabs.
------------------	--


User interface elements are described below:

UI Elements (A-Z)	Description
	Click to add an available integration query to the job definition.
	Click to delete the selected query from the job definition.

UI Elements (A-Z)	Description
Allow Delete	For population jobs: allows the deletion of CIs or links per job from the local ODB. For data push jobs: allows the deletion of CIs or links per query from the remote data repository.
Job Definition	Select integration queries for the job definition. Click  to add an available integration query to the job definition.
Name	Enter a name for the job.
Scheduler Definition	For details about scheduling jobs, see "Scheduler" in the <i>ODB Developer Reference Guide</i> .

Credentials Dialog Box

This dialog box enables you to add and manage credentials, or to select credentials for integration points.

To access	In the Connection Properties section of the Create New Integration Point/Edit Integration Properties Dialog Box, click  .
Important information	This option is relevant for all integration points for which the adapter requires you to specify credentials.

For details, see "Domain Credential References" on page 83.

Data Push Tab

This tab enables you to specify the queries that will be used to push data to external data repositories, and to schedule jobs that contain those queries. For details, see "Job Definition Pane" on page 209.

To access	Select the Data Push tab on the Integration Studio page.
Important information	This tab is enabled only when data push is supported by the adapter on which you are basing your integration point.
See also	"Create New Job Definition Dialog Box" on page 202



Federation Tab



This tab enables you to select which CITs or attributes are to be supported by the integration point. For example, if a TQL query includes a node that represents a specific CIT, the instances of this CIT are accepted from this external data repository.

For details about selecting CIs, see "CI Selector Overview" in the *Modeling Guide*.

To access	Select the Federation tab on the Integration Studio page.
Important information	This tab is enabled only when data federation is supported by the adapter on which you are basing your integration point.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click to clear all selected items.
	Click to invert the selections.

UI Elements (A-Z)	Description
	Click to expand the entire hierarchical tree structure.
	Click to collapse the hierarchical tree structure.
CI Type Retrieval Mode	<ul style="list-style-type: none"> ▶ Retrieve CIs of selected CI Type. All a CI's data, including all its attributes, are retrieved from the data repository. Retrieve CIs of the <CI Type name> CI Type from the UCMDDB too. The CI can be federated as well as physically retrieved from the ODB (if any CI instances exist in the database). ▶ Retrieve selected attributes. The selected attributes are retrieved from the data repository. The CIs must already exist in the ODB. Retrieve the attribute from the UCMDDB too. The attribute can be federated as well as physically retrieved from the ODB (if any attributes of CI instances exist in the database). <p>Note:</p> <ul style="list-style-type: none"> ▶ A parent CIT and all its child CITs included in an integration point definition must use the same retrieval mode. ▶ You cannot select both CITs and attributes for the same integration point.

UI Elements (A-Z)	Description
Select Attributes	<p>You can define which attributes of an external CIT are to be included in the federation:</p> <ul style="list-style-type: none"> ▶ In the CI Type Retrieval Mode pane, select Retrieve selected attributes. ▶ In the Select Attributes list, select the attributes that are to be included in the federation. ▶ Save the changes. <p>Note: Attributes are defined in the CIT Manager. For details, see "Add/Edit Attribute Dialog Box" in the <i>Modeling Guide</i>.</p>
Supported and Selected CI Types	<p>Displays a hierarchical tree containing the supported and selected CI Types and attributes.</p> <p>When queried by an TQL query, the CITs you select here are configured to retrieve the data from this external data repository.</p> <p>Select the CITs to be supported by this integration point.</p> <p>For BACKPIsAdapter, select Real Time KPI.</p>

Integration Points Pane









This pane enables you to define integration points, and schedule population and data push jobs.

Integration points are based on adapters, each of which is predefined to transmit information in specific ways. For example, the CMDbAdapter populates CIs and links from a remote ODB, in which case the ODB then has a local copy of these CIs (example of federation), while the ServiceManagerAdapter retrieves data from HP ServiceCenter and HP Service Manager, but HP ServiceCenter or HP Service Manager still retains control (example of data push).

For details about creating adapters based on Discovery, see "Adapter Management User Interface" on page 141.

To access	Located in the left pane of the Integration Studio.
See also	<ul style="list-style-type: none"> ▶ "Data Push Tab" on page 204 ▶ "Federation Tab" on page 204 ▶ "Population Tab" on page 210

User interface elements are described below (unlabeled elements are shown in angle brackets):


UI Elements (A-Z)	Description
	Click to create a new integration point. For details, see "Create New Integration Point/Edit Integration Properties Dialog Box" on page 200.
	Click to save the changes you made to the definition of an integration point.
	Click to delete the selected integration point.
	Click to edit a integration point's properties.
	Click to refresh the list of integration points and to fully refresh the selected integration point.
	Click to export the integration point's configuration in XML format.
	Click to import the integration point's configuration in XML format.
	Click to open the Reconciliation Priority Manager. For details, see "Reconciliation Priority Manager Window" on page 211.
<List of integration points>	Displays the list of previously defined integration points.
<Shortcut menu>	Open Reconciliation Priority Manager. For details, see "Reconciliation Priority Manager Window" on page 211.

Integration Studio Page

This page enables you to create and manage integration points.

To access	Select Admin > ODB Administration > Data Flow Management > Integration Studio .
------------------	---

User interface elements are described below:

UI Elements (A-Z)	Description
	Reconciliation Priority Manager. Opens the Reconciliation Priority Manager. For details, see "Reconciliation Priority Manager Window" on page 211.
Integration Points pane	Enables you to create integration points and edit their configuration. For details, see "Integration Points Pane" on page 206.
Right pane	Displays data transfer configuration options for an integration point. Depending on the adapter on which you base your integration point, one or more of the following tabs is enabled: <ul style="list-style-type: none"> ➤ "Data Push Tab" on page 204 ➤ "Federation Tab" on page 204 ➤ "Population Tab" on page 210








Job Definition Pane

This pane enables you to schedule integration jobs with external data repositories.

For additional details about scheduling jobs, see "Scheduler" in the *ODB Administration Guide*.

To access	Select the Population or Data Push tab on the Integration Studio page.
Important information	This tab is enabled only when population or data push is supported by the adapter on which you are basing your integration point.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click to create a new job definition. For details, see "Create New Job Definition Dialog Box" on page 202.
	Click to delete a job from the list.
	Click to edit a job's definition.
	Click to refresh the job definition list.
	Click to run a differential population or data push job. This job finds the differences in the ODB since the last job execution. By default, scheduled jobs are run as differential jobs, except for the first time a job runs. In that case, a full population or data push job runs.
	Click to run a full population or data push job. This job copies or pushes all data specified in the integration.
	Click to view statistics for a selected population or data push job, and to verify whether the job ran successfully.

UI Elements (A-Z)	Description
Job Name	Name given to the population or data push job.
Status	<p>Can be one of the following:</p> <ul style="list-style-type: none"> ▶ Job statuses <ul style="list-style-type: none"> ▶ Failed. The job did not run successfully. ▶ N/A. The job has not yet run since it was defined. ▶ Succeeded. The job ran successfully. ▶ Undefined. The job's status is not yet known. ▶ Query statuses <ul style="list-style-type: none"> ▶ Failed. The query did not run successfully. ▶ Finished. The query ran successfully ▶ Initializing. The query is in the process of starting. ▶ Not running. The query is not currently running. ▶ Running. The query is in the process of running.

Population Tab

This tab enables you to schedule jobs that push data to external data repositories. For details, see "Job Definition Pane" on page 209.


To access	Select the Population tab on the Integration Studio page.
Important information	This tab is enabled only when data population is supported by the adapter on which you are basing your integration point.
See also	"Create New Job Definition Dialog Box" on page 202

Reconciliation Priority Manager Window

This window enables you to specify the reconciliation priority for a particular integration point, CIT, or attribute.

The Reconciliation Priority Manager provides a centralized location where you can view and change the reconciliation priority for all integration points. In the Integration Points Pane, you can modify the reconciliation priority for the selected integration point only.

For more details, see "Reconciliation" on page 339

To access	Click  on the Integration Studio page.
Relevant tasks	<ul style="list-style-type: none"> ➤ "Work with Federated Data" on page 194 ➤ "Work with Population Jobs" on page 195 ➤ "Work with Data Push Jobs" on page 197

User interface elements are described below:

UI Elements (A-Z)	Description
Integration	Enables you to select a specific integration point for which to specify the reconciliation priority, or to set priorities for all integration points.

Authoritative Sources Pane

When you select a CI or attribute in the Reconciliation Priority Manager, the Authoritative Sources lists all integration points that contain the selected item.

User interface elements are described below:

UI Elements (A-Z)	Description
Integration Point Name	The name of the integration point that contains the selected attribute.
Inherited From	The name of the node from which the priority level is inherited.



UI Elements (A-Z)	Description
Overrides	<p>Displays the list of any priority overrides on a CI Type or attribute, in order from highest to lowest.</p> <p>Overrides are marked when a descendant overrides the priority of the specific integration point for a specific CIT.</p>
Priority	<p>Displays the priority that is assigned to a particular CI Type or attribute. The default priority level is for all items is 100. If you change the priority of a node, the new value propagates downwards to all descendants of that particular node.</p> <p>To change the priority of an item, do the following:</p> <ul style="list-style-type: none"> ▶ Click in the Priority field and enter a new value. ▶ Press Enter. ▶ Click Save to save the values you changed.

CI Types and Attributes Pane

The CI Types and Attributes pane displays the list of CI types and attributes that are supported by the selected integration point.

When you select a node in the CI Types and Attributes tree, all integration points that support the selected item are displayed in the right pane. If you have selected a specific integration point, its name is highlighted in the right pane. You can then change the reconciliation priority for that integration point only.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click to expand the entire hierarchical tree structure.
	Click to collapse the hierarchical tree structure.

Out-of-the-Box Integrations

You can use the following predefined adapters to integrate different ODB sources:

- ▶ **BACKPIsAdapter.** Select to define an adapter that enables a user to create a FTQL to retrieve, in an external application, the status and values of KPIs that are connected to CIs. For details, see "Viewing KPIs in External Applications" in the *ODB Developer Reference Guide*.
- ▶ **DDMi.** Select to define an adapter that is used for populating and federating data from DDMi. For details, see "Data Dependency and Mapping Inventory Integration with HP Business Service Management" in the *ODB Discovery and Integration Content Guide* PDF.
- ▶ **Local UCMDB History.** Select to define an adapter that is used for federating data from the local UCMDB History database.
- ▶ **Microsoft SMS.** Select to define an adapter that is used for populating and federating data from Microsoft SMS. For details, see "Data Dependency and Mapping Inventory Integration with HP Business Service Management" in the *ODB Discovery and Integration Content Guide* PDF.
- ▶ **Service Center 6.2x.** Select to define an adapter that is used for federating data from HP ServiceCenter version 6.2x. For details, see "HP ServiceCenter/Service Manager Integration" in the *ODB Discovery and Integration Content Guide* PDF.
- ▶ **Service Manager 7.0x.** Select to define an adapter that is used for federating data from HP Service Manager version 7.0x. For details, see "HP ServiceCenter/Service Manager Integration" in the *ODB Discovery and Integration Content Guide* PDF.
- ▶ **Service Manager 7.1x - 9.2x.** Select to define an adapter that is used for federating data from HP Service Manager versions 7.1x-9.2x and pushing data to HP Service Manager versions 7.1x-9.2x. For details, see "HP ServiceCenter/Service Manager Integration" in the *ODB Discovery and Integration Content Guide* PDF.
- ▶ **UCMDB 8.x.** Select to define an adapter that is used for populating data from ODB version 8.0x or pushing data to ODB version 8.0x. For details, see "Use Cases – Multiple ODB Deployments" on page 219.

- ▶ **UCMDB 9.x.** Select to define an adapter that is used for populating and federating data from ODB version 9.0x. For details, see "Multiple Deployments with Version 9.00 ODBs" on page 220.
- ▶ **UCMDB API Population.** Select to define an adapter that specifies the reconciliation priority for data that is added to the ODB using the ODB API. For details, see "HP Universal CMDB API" in the *ODB Developer Reference Guide*.

You also have the option of adding a custom adapter for a new external data repository. For details, see "Add an Adapter for a New External Data Source" in the *ODB Developer Reference Guide*.

Integration Framework SDK allows you to create new adapters that connect Business Service Management with external products and services. For details, see "Developing Java Adapters" in the *ODB Developer Reference Guide*.

For details about selecting an adapter when creating integrations, see "Create New Integration Point/Edit Integration Properties Dialog Box" on page 200.

Troubleshooting and Limitations

This section includes troubleshooting and limitations for the Integrations Studio functionality.

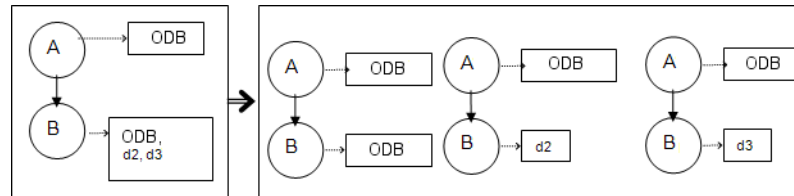
This section includes the following topics:

- ▶ "Limitations on Retrieving Data from Multiple Data Repositories" on page 214
- ▶ "Limitations on All Adapters" on page 215

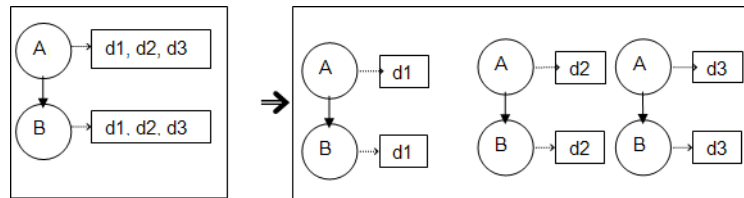
Limitations on Retrieving Data from Multiple Data Repositories

- ▶ When a virtual link exists between two data repositories, HP Business Service Management supports mapping in the following cases only:

- The BSM integration point lies at one end of the link and multiple data repositories lie at the other end. The Cartesian product is calculated for A's data repository (BSM) and B's data repositories (BSM, d2, d3).



- The same data repositories lie at both ends of the link. The link is an internal link of each data repository and no mapping is required.



Limitations on All Adapters

- When changes are made in the Modeling Studio and these changes affect the results of a TQL, federated CIs in the view are not updated. This is because federated TQLs are calculated ad-hoc only and are not updated when a view is recalculated. To update the federated CIs, select the view in the CI Selector and click the **Rebuild View** button. (Note that the recalculation may take a long time.) For details, see "Browse Views Mode" in the *Modeling Guide*.
- Do not choose a CIT to be supported by an external data repository if instances of this CIT exist in the local ODB, as this can lead to state inconsistency. For example, if there are instances of the CPU CIT in the local ODB, you must not choose the CPU when defining an external data repository, even if the selected adapter supports it.
- When configuring a population or data push job between two ODBs, verify that the class model is the same in the two ODBs.

8

Integrating Multiple ODBs

This chapter includes:

Concepts

- ▶ Integrating Multiple ODBs Overview on page 218
- ▶ Content Management System (CMS) on page 218
- ▶ Global ID on page 219
- ▶ Use Cases – Multiple ODB Deployments on page 219
- ▶ Multiple Deployments with Version 9.00 ODBs on page 220
- ▶ Federation in Version 9.01 ODBs on page 224
- ▶ Multiple Deployments with Version 8.0 ODBs on page 226

Tasks

- ▶ Set Up Integrations Between Multiple ODBs (ODB Version 9.0x) on page 229
- ▶ Set Up Integrations between CMS and ODB on page 230
- ▶ Set Up Integrations Between Multiple ODBs (ODB Version 8.0x) on page 232

Reference

Troubleshooting and Limitations on page 234

Concepts

Integrating Multiple ODBs Overview

Multiple ODBs is a solution that allows setting up a multiple number of ODBs for delegating the workload and responsibility of the solution to the different ODBs.

The usage of multiple ODBs enables increased performance, as the workload is split between different ODBs on different machines. It increases the capacity, as the data is split between the different ODBs.

The ODBs that are used during integration can all be version 9.01 ODBs, or can be split between version 8.04 or later and version 9.01 ODBs. When you integrate with a version 8.0x ODB, you can do the following:

- ▶ populate the version 9.01 ODB server with data from version 8.0x.
- ▶ push data from a version 9.0x ODB server to a version 8.0x server.

Content Management System (CMS)

The CMS is the central ODB Server and is the authority for configuration management in the multiple CMDBs solution. It is responsible for integrating between the different ODB Server instances and other services in the solution, as well as for generating global IDs. Most of the integrations are defined in the CMS, and other ODBs or services only access the CMS to access the data from these ODBs or services.

The CMS allows integration with other services using:

- ▶ Population
- ▶ Federation
- ▶ Data Push
- ▶ Data Flow Management Web Service API
- ▶ Soap Web Service

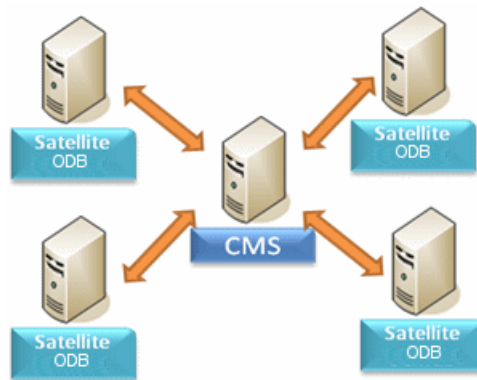
Global ID

The global ID is a unique CI ID, generated by the CMS, that identifies that CI across the entire portfolio, making it easier to work in multiple ODB environments.

Note: In the CMS, the ODB ID is identical to the global ID.

Use Cases – Multiple ODB Deployments

ODB–CMS Solution



The solution includes:

- ODB
- The central CMDB acting as the CMS
- Service Manager (SM)

The ODB is responsible for monitoring the authorized hosts and maintaining the business logic topology.

The CMS is responsible for Discovery and integration with SM.

The CMS populates all the business elements, CI collections and parties from the ODB using the ODB-to-CMS synchronization TQL. The ODB populates the infrastructure from the CMS. The ODB federates incidents from the CMS, which then federates them from SM. When a user requests incidents for a certain node, they are brought seamlessly from the CMS.

Multiple Deployments with Version 9.00 ODBs

This section includes:

- "Population from BSM 9.00 (CMS Synchronization)" on page 220
- "Query Support" on page 220
- "Global ID Synchronization" on page 221
- "Automatic Completion of Reconciliation Data" on page 223
- "Out-of-the-Box Synchronization Query" on page 224

Population from BSM 9.00 (CMS Synchronization)

When you use the UCMDb 9.0x adapter to create an integration point, you are able to synchronize data between different ODB instances using population. For details on population, see "Work with Population Jobs" on page 195.

During population, global IDs are synchronized. For details, see "Global ID Synchronization" on page 221.

Query Support

Two types of queries are supported for population jobs:

- Live queries—all non-federated TQL queries, when they are used for population with the UCMDb 9.0x adapter.

Live queries require less bandwidth, and cause less load on the source system. There may be a short delay from the time the change is made until the live query mechanism or the population job receives the change (this may take up to several minutes).

Subgraphs and compound relationships are supported in queries. When using compound relationships, you must select **Show full path between source and target CIs** in the Compound Relationship properties of the query.

- Federated Queries—queries that contain that contain at least one federated node or attribute.

When the UCMDB 9.0x adapter is used, federated queries may also be used for population.

Federated queries are calculated each time the integration is performed; the entire result set is retrieved and filtered by the Probe.

The deletion of CIs is not supported. The aging mechanism must be used, since no information about the deletion of CIs or links is populated.

Global ID Synchronization

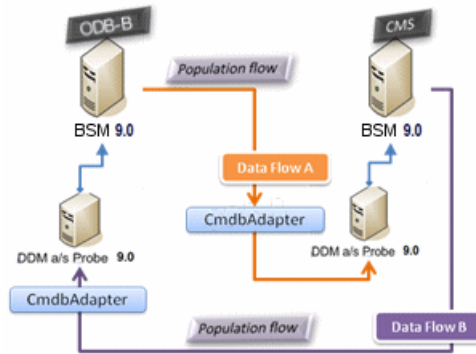
Two types of synchronization can be performed:

- Two-way ID synchronization

Synchronization of data occurs in both directions between two ODB instances.

The CMS uses the population flow to retrieve data from ODB-B, which may be any ODB. ODB-B uses the population flow to populate data from the CMS.

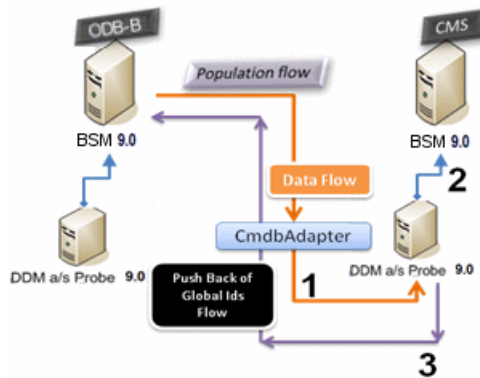
Because synchronization is performed in two directions, global IDs are also updated on ODB-B.



► Pushback of IDs

The CMS uses the population flow to retrieve data from ODB-B. CIs are reconciled with the data in the CMS.

The global-ID in the CMS for each CI received is pushed back to ODB-B.



The default state of this option is disabled.

For details about enabling the pushback of IDs, see "Set Up Integrations Between Multiple ODBs (ODB Version 9.0x)" on page 229.

Automatic Completion of Reconciliation Data

The UCMDB 9.0x adapter automatically retrieves data needed for the reconciliation process of the CIs brought by the population flow. The actual data retrieved is determined by the reconciliation rule defined for the CITs of the TQL.

For example, if your population TQL query includes a node but does not have any layout selected, the actual data that enters the ODB will be:

- ▶ Nodes, with layout
 - ▶ name
 - ▶ bios_uuid
 - ▶ serial_number
 - ▶ additional data, according to the defined reconciliation rule
- ▶ IP Addresses, with layout
 - ▶ name
 - ▶ routing_domain
- ▶ Interfaces, with layout
 - ▶ mac_address
 - ▶ interface_name

Note:

- ▶ The automatic completion feature may actually synchronize many more CIs or links than you intend.
 - ▶ The automatic completion feature always retrieves the Global ID.
 - ▶ "By default, if data required for the reconciliation of a particular CI cannot be retrieved (for example, if the data is missing in the source), that CI will be ignored without causing the entire job to fail. You can change this behavior in the CmdbAdapter configuration. For details, see "Results Management Pane" on page 154.
-

Out-of-the-Box Synchronization Query

The ODB to CMS synchronization query is used to:

- ▶ Populate data from the ODB to the CMS. Such data can include BusinessElements, CI collections, Parties and any infrastructure element connected to them and all the links between them.
- ▶ Populate locations connected to any of these CIs (that are defined as sub-graphs for each CI).

HP Software recommends that you schedule this query to run every 10 minutes, so that both the ODB and the CMS are continually updated with the most recent CIs. To define this schedule, do the following:

- 1** In the Job Definition window, select the **Scheduler Definition** checkbox.
- 2** Select the **Cron** repeat type.
- 3** In the **Cron Expression** field, enter *** 0/10 * * * ? *** and click **Validate**.

For details, see "Create New Job Definition Dialog Box" on page 202.

Federation in Version 9.01 ODBs

Federation allows the ODB to retrieve data in real time (on-the-fly) from any remote data repository, and combine it with ODB's internal data to show a complete picture of the configuration it manages, including multiple sources. For more information about federation, see "Work with Federated Data" on page 194.

Using the UCMDB 9.0x adapter to federate data from different ODBs, enables the federation of any CIT in the model. This means that only a small portion of data from the remote ODBs can be populated, and the rest of the data is federated on demand. This ability enables the delegation of the information to multiple ODBs, with the CMS always showing the most updated data available and at the same time not overloading its capacity.

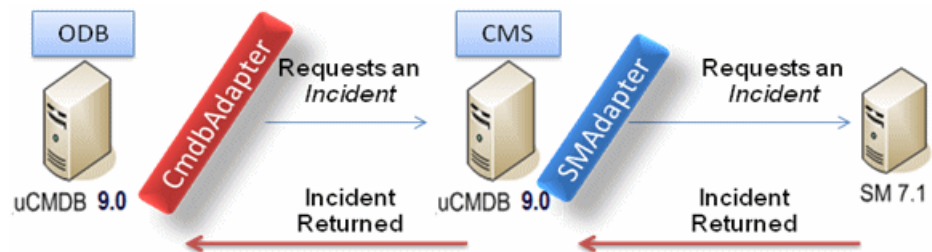
The following is an example of federation with multiple ODBs:

A CMS populates the Node, Interface, and IP from a Discovery ODB (a ODB whose role is to run Discovery), and defines the CPU, File System, OS, User, Printer, and Process CIs as federated from the same source. When a user runs a TQL query or view that has any federated CIs, these specific CIs are brought in real time from the Discovery ODB. They are therefore as updated as the Discovery ODB and do not depend on the population schedule to receive updated information. In addition, these CIs only reside on the Discovery CMDB, and do not burden the capacity of the CMS.

The ODB 9.0x adapter supports the delegation of the federation capabilities, providing the ability to set up a single point for data retrieval (usually the CMS). Any ODB or service that uses the ODB's ability to delegate federation uses the ODB as a virtual black box, and is unaware of whether data comes directly from the CMS or from an external integration.

Note: When you set up a federation flow, be careful not to cause an endless loop. For example, do not set up ODB-X to federate data from ODB-Y, and at the same time ODB-Y to federate data from ODB-X.

In the following example, the SM integration point is defined with **incidents** as federated CIs, and the ODB has **incidents** federated from the CMS. Whenever the ODB requests an **incident**, it requests it from the CMS, which in turn requests it from SM and returns the answer to the ODB.



Multiple Deployments with Version 8.0 ODBs

Note: The UCMDB 8.0x adapter uses the UCMDB version 8.0x API for both population and data push integrations.

This section includes:

- "Population from Version 8.0x UCMDBs" on page 226
- "Push to version 8.x ODBs " on page 227

Population from Version 8.0x UCMDBs

The population flow of integration points based on the UCMDB 8.0x adapter operates similarly to the way data is upgraded from version 8.0x to version 9.0x in BSM. Data is read from the version 8.0x UCMDB and is transformed using the upgrade XML documents. Since the version 8.0x adapter does not support all of the upgrade methods that are available in the upgrade process, not all CI types can be populated from version 8.0x to version 9.0x in BSM.

- Supported changes between version 8.x and version 9.x:
 - Name change for both CIs and attributes
 - Hierarchy change for CIs
 - Attributes deleted from version 8.x
 - Any updates to qualifiers
- Unsupported changes:
 - Attribute type changes
 - Attribute values, since in version 9.x they are calculated from existing values in version 8.x
 - Attributes in version 8.x that were merged to a single attribute in version 9.x are supported, but if all of the attributes hold a different value, one will be picked randomly to populate the merged attribute.

Note:

- ▶ There may be situations where the existing data in version 8.x is insufficient for the reconciliation engine to identify the data in 9.x. For example, if a CI in version 8.x has an optional attribute X, but attribute X is required in version 9.x in order to identify the CI, any CIs that have an empty X attribute will not be populated to version 9.x.
 - ▶ In order to populate any user-defined CI type, the CI type must have upgrade rules defined in one of the upgrade XML documents.
-

Push to version 8.x ODBs

The push flow provides the capability to push data from a ODB version 9.x Server to a ODB version 8.x Server, and the data is then downgraded to the version 8.x class model from version 9.x. CI types and attribute that exist in version 9.x but did not exist in version 8.x are ignored. The following lists changes to the class model between versions 8.x and 9.x that are not supported by the push flow:

- ▶ If a CI type has an attribute that was a key attribute in 8.x but is optional in 9.x, any CI with an empty value in that attribute is not pushed.
- ▶ Attributes that changed their type between versions are not supported.
- ▶ Attributes in version 8.x that were merged to a single attribute in version 9.x are supported, but all of the attributes in version 8.x contain the same value as the single attribute in version 9.x.
- ▶ Attributes whose values were calculated or transformed during the upgrade from version 8.x to version 9.x are not supported.

The UCMDB version 8.x adapter has two main parts:

- ▶ An XML document that maps the version 9.x class model to the version 8.x class model.
- ▶ A Jython script that updates data to a target version 8.x ODB server using the UCMDB version 8.x API.

In order to push user-defined CI types that exist both in the version 8.x and version 9.x ODB, the CI type and all its attributes must exist in the XML mapping file that comes with the UCMDB 8.x adapter. To do that, edit the **mappings_9x_to_8x.xml** file in BSM. For details, see "Resources Pane" on page 175.

Note: You can replace the **mappings_9x_to_8x.xml** file with a file of a different name, as long as you update the `mappingFile.default` key in the **push.properties** file.

Tasks

Set Up Integrations Between Multiple ODBs (ODB Version 9.0x)

The following steps describe how to create integration points and jobs to integrate between multiple ODBs.

- "Configure the ODBtoODBSync integration point" on page 229
- "Run the population job" on page 230

1 Configure the ODBtoODBSync integration point

- a Navigate to **Admin > ODB Administration > Data Flow Management > Integration Studio**.
- b Select the ODBtoODBSync integration point.
- c Click the **Edit Integration Properties** button.



Enter the following information:

Name	Recommended Value	Description
Hostname/IP	<user defined>	The name of the server on which the remote ODB resides.
Credentials	<user defined>	Use the credentials necessary for connecting to the remote ODB machine. For details, see "Domain Credential References" on page 83.
Probe Name	<user defined>	The name of the probe to be used for the synchronization.
Is Integration Activated	selected	Select this check box to create an active integration point.



- d Click **Save**.

2 Run the population job



Click the **Run Diff Job** button to make sure that the integration has been successfully configured.

Set Up Integrations between CMS and ODB

The following steps describe how to create an integration point for CMS-ODB synchronization. In this procedure, the CMS can be an ODB installation or a standalone UCMDB.

- "Deploy the CMStoODBSYNC.zip package" on page 230
- "Define an integration point" on page 230
- "Schedule the CMStoODBSync population jobs" on page 231
- "Run the population jobs" on page 231

1 Deploy the CMStoODBSYNC.zip package

- a** Browse to the `c:\HPBSM\odb\conf\factory_packages` directory on the BSM machine.
- b** Copy the `CMStoODBSync.zip` file to a temporary directory on the CMS machine.
- c** In the CMS, navigate to **Admin > ODB Administration > Administration > Package Manager**.



d Click the **Deploy Packages to Server (from local disk)** button.



e Click the **Add** button.

f Browse to the `CMStoODBSync.zip` file that you copied in step b.

g Click **Deploy**.

2 Define an integration point

- a** Navigate to **Admin > ODB Administration > Data Flow Management > Integration Studio**.
- b** Select the `CMStoODBSync` adapter.



- c** Click the **Edit Integration Properties** button.

Enter the following information:

Name	Recommended Value	Description
Credentials	<user defined>	Select the credentials that will be used to connect to the CMS. For details, see "Domain Credential References" on page 83.
Hostname/IP	<user defined>	The name of the server on which the CMS resides.
Is Integration Activated	selected	Select this check box to create an active integration point.
Probe Name	<user defined>	The name of the probe that will be used for synchronization.

- d** Click **Test Connection** and then click **OK**.

3 Schedule the CMStoODBSync population jobs

- a** Click the Population tab.
- b** Select each of the CMStoODBSync jobs for which you want to change the default scheduling.
- c** Set the required settings for each job in the Scheduler pane.

4 Run the population jobs



Click the **Run Diff Job** button for each job to make sure that the integration has been successfully configured.

Set Up Integrations Between Multiple ODBs (ODB Version 8.0x)

The following steps describe how to create integration points and jobs to integrate between multiple ODBs.

- "Define an integration point" on page 232
- "Define a population job (optional)" on page 233
- "Define a data push job (optional)" on page 233
- "Run the population or data push job" on page 233

1 Define an integration point

- a Navigate to **Admin > ODB Administration > Data Flow Management > Integration Studio**.



- b Click the **Create New Integration Point** button to open the New Integration Point Dialog Box. For details, see "Create New Integration Point/Edit Integration Properties Dialog Box" on page 200.

Enter the following information:

Name	Recommended Value	Description
Adapter	UCMDB 8.x	The adapter that will be used to integrate between multiple ODBs.
Credentials	Generic Protocol	If you must create a new credential protocol, use the Generic Protocol as a basis. For details, see "Domain Credential References" on page 83.
Customer ID	<user defined>	The numeric ID of the customer who owns the data on the remote machine.
Hostname/IP	<user defined>	The name or IP address of the remote ODB machine.
Integration Description	<user defined>	Free text that describes the integration point.

Name	Recommended Value	Description
Integration Name	<user defined>	The name you give to the integration point.
Port	<user defined>	The port listened to by the UCMDB version 8.x API.
Probe Name	<user defined>	The name of the probe with which the integration point communicates.

- c Click **Test Connection** to ensure that the integration point has been successfully created.

2 Define a population job (optional)

Select the Population tab to define a population job that uses the integration point you defined in step 1. For details, see "Create New Job Definition Dialog Box" on page 202.

All queries from the remote version 8.x ODB machine are displayed for selection, with no consideration as to the type of query.

The population flow will always extract the entire layout for every query node, without regard to any special layout that may exist (attributes that cannot be upgraded will be ignored). If the query contains a link or object that is not supported, it is ignored during population.

3 Define a data push job (optional)

Select the Data Push tab to define a data push job that uses the integration point you defined in step 1. For details, see "Create New Job Definition Dialog Box" on page 202.

4 Run the population or data push job



Click the **Run Diff Job** button to make sure that the integration has been successfully configured.

Reference

Troubleshooting and Limitations

Version 9.0x Troubleshooting and Limitations

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

- ▶ ODB server logs
 - ▶ fcldb.log
 - ▶ fcldb.adapters.log
 - ▶ error.log
- ▶ Probe logs
 - ▶ wrapperProbeGw.log
 - ▶ fcldb.log
 - ▶ fcldb.adapters.log
 - ▶ probe-infra.log

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

Problem. TQL not active/persistent error message.

The Query settings have been changed manually.

Solution. Run full population to reactivate/persist the query.

Problem. The number of CIs that is populated is much larger than the requested amount.

Solution. Since the automatic completion feature for reconciliation is turned on by default, it may populate the ODB with additional CIs or links, in order to contain sufficient information to insert the CIs into the ODB.

Problem. Changes are not populated immediately after a job is run.

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

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

Problem. CIs are not populated into the ODB.

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

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

Check the ODB reconciliation logs for more information.

Problem. Deletions are not populated.

Solution.

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

Problem. Queries that contain compound relationships fail.

Solution. Select **Show full path between source and target CIs** in the query's Compound Relationship properties.

Problem. Authentication fails.

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

Limitations

- The TQL query used for population (defined on the source) must not include any CI types or links that do not exist on the target ODB. For example, one way to prevent this is by blacklisting inheriting CITs from the query node by adding a condition: CI Type NOT EQUAL "myPrivateclass".

- ▶ If you are planning to synchronize between ODB and another data repository, it is recommended that you increase the Model capacity level on to the Server Deployment Page. After this, you must restart all BSM servers.

Version 8.0x Troubleshooting and Limitations

Logging

If objects or links are not pushed correctly to the remote version 8.x ODB machine, these log files may provide information about the reason:

- ▶ **fcmdb.adapters.log** – for any errors that were found while retrieving the data from the version 9.x ODB server, or while transforming it to the version 8.x class model.
- ▶ **wrapperProbeGw.log** (on the Probe) – for any errors that are raised by the UCMDB 8.x API while trying to add, update, or delete data.
- ▶ **cmdb.reconciliation.log** and **error.log** (on the remote version 8.x ODB machine) – use these logs to find out why data was not inserted.

Limitations

- ▶ The push flow does not support the delete operation; however, data may be deleted using the version 8.x aging mechanism. This means that if a certain CI is not pushed to the version 8.x server and is not updated on the version 8.x server by any other method, it will be deleted by the aging mechanism.
- ▶ Always supply all the necessary reconciliation data when you update data using differential synchronization. For example, if trying to update a node, the TQL should have any linked **ip_address** and **interface** attributes.

Part IV

Discovery

9

Discovery Control Panel

This chapter includes:

Concepts

- ▶ Discovery Control Panel Overview on page 240
- ▶ Viewing Permissions While Running Jobs on page 242
- ▶ Managing Problems With Error Reporting on page 243
- ▶ The Permissions Document on page 244

Tasks

- ▶ Discovery Control Panel – Basic Mode Workflow on page 246
- ▶ Discovery Control Panel – Advanced Mode Workflow on page 247
- ▶ View Job Information on the ODB Data Flow Probe on page 251
- ▶ Manually Activate a Job on page 263
- ▶ Manage Errors on page 263
- ▶ Find Errors on page 265

Reference

- ▶ Discovery Control Panel User Interface on page 267

Concepts

Discovery Control Panel Overview

The Discovery Control Panel pages enable you to activate jobs that discover the components of your system. You activate Discovery with one of the following methods:

- ▶ Use **Basic Mode** to run Discovery for a specific component (for example, the infrastructure, J2EE applications, or databases), using configurable, default preferences.

For details on the workflow, see "Discovery Control Panel – Basic Mode Workflow" on page 246.

For details on the Discovery wizard, see "Basic Mode Window" on page 269.

Note: Basic Mode is displayed by default when you access the Discovery Control Panel.

- ▶ Use **Advanced Mode** to run Discovery to customize a run by making changes to a job.

For details on the workflow, see "Discovery Control Panel – Advanced Mode Workflow" on page 247.

For details on the Discovery wizard, see "Advanced Mode Window" on page 268.

For details on running a specific module, see the *ODB Data Flow Management Guide*.

Jobs are organized in modules as follows:

- ▶ **Applications.** The modules discover Microsoft Exchange, Oracle E-Business Suite components, the SAP environment based on Computer Center Management System (CCMS), the Siebel environment (such as the Siebel topology and database), WebSphere MQ, and the UDDI registry Web services.
- ▶ **Cluster.** The modules discover Microsoft Cluster, ServiceGuard, Veritas, Alteon LB, Cisco CSS, F5 Big IP, and Microsoft NLB.
- ▶ **Database.** Discovery first finds instances of databases, then of the database resources (for example, users, tables, tablespaces) for each database instance. HP Business Service Management includes predefined default views of the DB2, Oracle, and Microsoft SQL Server databases.
- ▶ **Discovery Tools** This module holds the jobs necessary to discover document files and directories, discover hosts, import data from external sources, and serve as a template example.
- ▶ **Integration.** These modules are needed for integration between ODB and NNM Layer 2, Storage Essentials, and EMC Control Center.
- ▶ **J2EE.** The modules discover JBoss, Oracle Application Server, WebLogic, and WebSphere components.
- ▶ **Network.** The modules discover resources on Windows and UNIX hosts, for example, disk information, running processes or services, load balancing, and so on.
- ▶ **Virtualization.** The module discovers VMware components.
- ▶ **Web Servers.** The modules discover Apache and Microsoft IIS for Windows, SunOne for Solaris, and IBM HTTP Server.

Note: To view Help on Discovery Control Panel components:

- ▶ For details on the Discovery Modules pane, see "Discovery Modules Pane" on page 296.
 - ▶ For details on the Details tab, see "Details Tab" on page 284.
 - ▶ For details on the Properties tab, see "Properties Tab" on page 324.
 - ▶ For details on the Dependency Map tab, see "Dependency Map Tab" on page 282.
-

Discovery Wizards

As the creation of Discovery wizards entails a very advanced knowledge of Discovery, it is recommended that you contact HP Software Support before beginning the work.

Viewing Permissions While Running Jobs

During a job run, you often need to know which credentials are being used to connect to a component in the system. You also often need to know the effect of a run on network performance, for example, whether the job should be run at night instead of during the day. View Permissions enables you to view the objects and parameters of a job's Jython script commands, as can be seen in the following image:

Permission	Operation	Usage Description	Objects and Parameters
shellprotocol	exec	Basic login	uname ver
shellprotocol	exec	CPU Info	AIX: lsattr grep "proc" AIX: prtconf grep "proc" FreeBSD: dmesg grep "cpu Multiprocessor" FreeBSD: dmesg grep -A 1 "CPU:" FreeBSD: sysctl hw.model hw.ncpu hw.clockrate HPUX: model Linux: cat /proc/cpuinfo SunOS: /usr/sbin/psrinfo -v SunOS: prtconf Windows: reg query HKEY_LOCAL_MACHINE\HARDWARE\DESCRIP...

Note: The information you define here is not dynamic, that is, if an adapter is changed, the information in this dialog box is not updated.

For details, see "Discovery Permissions Window" on page 299.

Example of Using the Discovery Permissions Window:

You are running the Host Connection by Shell job to discover a host running on a UNIX system. An error message in the Discovery Status pane shows that Discovery could not access a host through SSH because permission was denied. You display the Discovery Permissions window and see that the command to access the host requires a user with a certain level of permissions. You check the SSH Protocol window and discover that the user defined there does not have that level of permissions.

To resolve the problem, either change the user in the SSH protocol or update the permissions for the existing user in the external system.

Managing Problems With Error Reporting

During discovery, many errors may be uncovered, for example, connection failures, hardware problems, exceptions, time-outs, and so on. DFM displays these errors in Discovery Control Panel, in both Basic and Advanced Mode. You can drill down from the Trigger CI that caused the problem to view the error message itself.

DFM differentiates between errors that can be ignored (for example, an unreachable host) and errors that must be dealt with (for example, credential problems or missing configuration or DLL files). Moreover, DFM reports errors once, even if the same error occurs on successive runs, and reports an error even if it occurs once only.

For details on severity levels, see "Error Severity Levels" in the *ODB Developer Reference Guide*.

Error Table in Database

All DFM errors are saved to the `discovery_problems` table in the Probe Manager database schema. (The error information is saved to the database—and is not handled in the Probe's memory—to guarantee delivery to the server.) The Probe holds the latest list of problems for each Trigger CI. After each run, the Probe checks for changes and reports them in the Discovery Status pane. For details, see "Discovery Status Pane" on page 285.

The Permissions Document

Note: This functionality is available as part of Content Pack 4.00 or later.

You can view a list of Discovery jobs together with the protocols and permissions needed to access the job components. For example, you can view information about what is needed to execute a basic login when running the Host Resources by Shell job.

The list is produced in a PDF document that is located in the following folder on the ODB machine: **C:\HPBSM\AppServer\webapps\site.war\amdocs\eng\pdfs\Permissions.pdf**.

The list is organized by module and consists of the following information:

- Module
- Job
- Protocol
- Operation, usage description, objects and parameters

Example of Permissions Document Contents

Database - Oracle. The module name.

Oracle RAC Topology by Shell. The job name.

Discovers Oracle RAC Topology by Shell. The job description. This section is omitted if no description is defined in the application.

Protocol: Shell. The protocol name: SQL, Shell, WMI, SNMP, and so on. For a full list, see "Domain Credential References" on page 83.

Operation	Usage Description	Objects and Parameters
file read	Parsing of listener and tnsnames configuration files	cat \$ORACLE_HOME\network\listener.ora cat \$ORACLE_HOME\network\admin\tnsnames.ora

Tasks

Discovery Control Panel – Basic Mode Workflow

This task describes how to begin mapping your system and its components, using the Discovery wizards. You run this workflow to use default values for the components in an infrastructure, database, or J2EE discovery.

Note: For details of running Discovery in Advanced Mode, see "Discovery Control Panel – Advanced Mode Workflow" on page 247.

This task includes the following steps:

- "Prerequisites" on page 246
- "Access the Discovery Wizard" on page 246

1 Prerequisites

Verify that the ODB Data Flow Probe is installed. For details on installing the Probe, see "Install the Data Flow Probe" on page 40.

For details on licensing, see "Licensing Models for ODB" on page 33.

2 Access the Discovery Wizard

For details, see the relevant wizard: "Infrastructure Wizard" on page 306, "J2EE Wizard" on page 314, or "Database Wizard" on page 275.

Discovery Control Panel – Advanced Mode Workflow

This task describes how to begin mapping your system and its components. You would use this workflow to customize the components of a module.

Note: For details of running discovery in Basic Mode, see "Discovery Control Panel – Basic Mode Workflow" on page 246.

This task includes the following steps:

- "Prerequisites" on page 247
- "Determine Network Range" on page 247
- "Set Relevant Credentials" on page 248
- "Activate Relevant Jobs" on page 248
- "Make Changes to Relevant Adapters" on page 249
- "Monitor the Discovery Process" on page 249
- "View Result Statistics" on page 250
- "Troubleshoot the Results" on page 251

1 Prerequisites

- a Verify that the ODB Data Flow Probe is installed. For details on installing the Probe, see "Install the Data Flow Probe" in *ODB Data Flow Management Guide*.

For details on licensing, see "Licensing Models for ODB" in *ODB Data Flow Management Guide*.

- b Verify that the relevant packages are deployed.

For details, see "Package Manager" in the *ODB Administration Guide*

2 Determine Network Range

You must define the network range of the network to be discovered. For details, see "Add/Edit IP Range Dialog Box" on page 69.

Note: Adapters try to connect to every IP in a range. Therefore, if a range is wide, network performance may be affected.

3 Set Relevant Credentials

To enable Discovery to connect to servers or applications using specific protocols, you must set the relevant credentials (for example, NTCmd, SNMP, TTY, or WMI). For details on protocol parameters, see "Domain Credential References" on page 83. For details on the Details pane in the Data Flow Probe Setup window, see "Details Tab" on page 75.

Note: Discovery tries to connect to a host by using each credential in turn. Discovery then saves the successful credential. The next time Discovery connects to this host, it first tries to connect using the successful credential.

4 Activate Relevant Jobs

Once you have defined the network range and set credentials, you can run discovery on specific jobs. For details, see the *Discovery and Dependency Mapping Content Guide*.

Tip: You can view a full description of a job. Select a module and locate the Description pane in the Properties tab.

Example – Finding SNMP Connections:

You can search for all jobs that discover SNMP connections: in the **Discovery Control Panel > Discovery Modules** pane, click the **Search for Discovery Job** icon. In the **Find Jobs** dialog box, enter **SNMP** in the **Name** box and click **Find All**. For details, see "Find Jobs Dialog Box" on page 305.

5 Make Changes to Relevant Adapters

You can customize adapters to discover infrequent system components. For details on adapter writing, see "Adapter Development and Writing" in the the *ODB Developer Reference Guide*.

Caution: Do not make changes to default adapters without consulting HP Software Support.

6 Monitor the Discovery Process

For details on monitoring the CIs that are discovered by the run, see "Statistics Results Pane" on page 292.

a Define a query

You create a query that retrieves information about CIs and CITs from the CMDB. For details, see "Define a TQL Query" in the *Modeling Guide*.

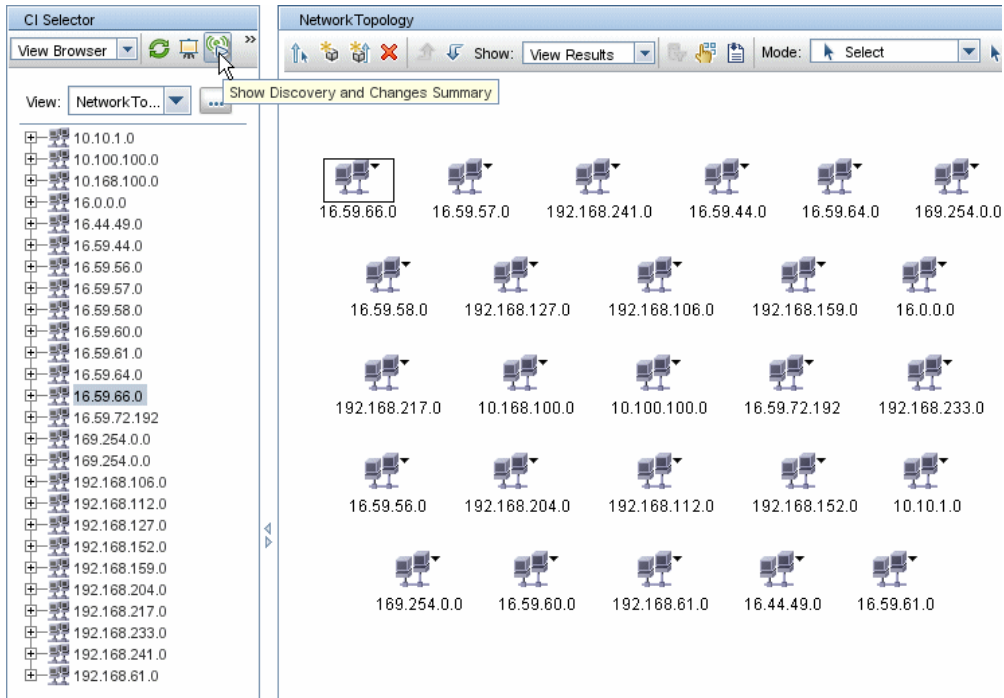
If necessary you can trigger queries to manually discover objects. For details, see "Trigger Queries Pane" on page 328.

b Build a View for each query

A view enables you to build a subset of the overall IT universe model, containing only those CIs in the CMDB that relate to a specific discovery. For details, see "Pattern View Editor" in the *Modeling Guide*.

Example – Creating a View to Display Discovered CI Instances:

To view the number of instances found by Business Service Management, select **Admin > ODB Administration > Modeling > IT Universe Manager**, and display the view you created, as seen in the following illustration:



7 View Result Statistics

You can display overall statistics for a job or you can filter the results by time range or by Probe. Each time you log in to HP Business Service Management and access Discovery Control Panel, the statistical data is updated so that the data displayed is the latest for the selected module or job.

For details on working with the statistical data, see "Statistics Results Pane" on page 292.

You can view discovered CIs also by accessing the Show Status Snapshot pane. For details, see "Data Flow Probe Status" on page 113.

8 Troubleshoot the Results

You can check Discovery results to see which errors are being reported. For details, see "Error-Writing Conventions" in the *ODB Developer Reference Guide*.

View Job Information on the ODB Data Flow Probe

This task describes how to invoke job information (for example, job threads and trigger CIs) saved to the Data Flow Probe's MySQL database. You work with the JMX console.

This task includes the following steps:

- "Access the MBean Operations" on page 251
- "Locate the Operation to Invoke" on page 251
- "Run the Operation" on page 252

1 Access the MBean Operations

Use the following procedure to access the JMX application on the Data Flow Probe and to invoke the JMX operations.

- a** Launch the Web browser and enter the following address:

```
http://<machine name or IP address>.<domain_name>:1977/
```

where **<machine name or IP address>** is the machine on which the Data Flow Probe is installed. You may have to log in with the user name and password.

- b** Click the **Local_<machine name or IP address> > type=JobsInformation** link.

2 Locate the Operation to Invoke

In the MBean View page, locate the operation. For details, see "Operations" on page 252 and "Job Operation Parameters" on page 261.

3 Run the Operation

Click the button to run the operation. A message is displayed with the results of the operation run.

Reload. The number of seconds between automatic reloads of the JMX interface. **0:** The interface is never reloaded. Click the **Reload** button to manually reload the current page (if more operations have been added or removed).

Unregister. Do not touch (the view becomes inaccessible to the application that is running).

Operations

activateJob

Enter the name of a job and click the button to activate the job immediately. This operation returns a message, for example, <job name> was triggered.

Note: The following message is displayed if the job has not been activated and there is no information about the job in the Probe's database:

Job '<job name>' does not exist in the Jobs Execution table (job was not activated!).

activateJobOnDestination

Enter the name of a job and a Trigger CI and click the button to activate the job immediately on a specific Trigger CI. This operation returns a message, for example, The operation returned with the value: Job <job name> was triggered on destination <CI name>.

Note: Both the **jobID** and **triggerCI** fields are mandatory.

start/stop

These operations start and stop the JobsInformation service. Do not use these operations; instead, restart the Probe itself.

viewJobErrorsSummary

Enter the name of a job to return a list of error messages reported on this job, together with the error severity, the last time that the error was reported, and the number of Trigger CIs that have the error.

For details on the job operation parameters, see "Job Operation Parameters" on page 261.

Click the entry in the **Number of trigger CIs** column to view a list of one job's trigger CIs with errors in the **viewJobTriggeredCIsWithErrorId** page.

viewJobExecHistory

Enter the name of a job to retrieve a history of job invocations. A message is displayed showing the job invocations (the last invocation is shown first).

For details on the job operation parameters, see "Job Operation Parameters" on page 261.

For each invocation the number of Triggered CIs and the total running time is shown. The Execution Details column shows at which times the job was executed. If the Probe shut down in the middle of a job execution and then resumed running or if there were blackout periods during the job execution, several time ranges are shown.

viewJobProblems

Enter the name of a job or the name of a trigger CI to retrieve a list of Trigger CIs that have problems.

Note: You must fill in at least one of the fields.

For details on the job operation parameters, see "Job Operation Parameters" on page 261.

viewJobResultCiInstances

Fill in one or more of the parameters to return a list of CIs that have been discovered by a job.

For details on the job operation parameters, see "Job Operation Parameters" on page 261.

The Object State Holder column displays the code for the CI or relationship defined in the CMDB. For details on creating object state holders for common CITs, see **modeling.py** in "Jython Libraries and Utilities" in the the *ODB Developer Reference Guide*. For details on the ObjectStateHolder method, see the *HP Universal CMDB Data Flow Management API Reference*.

viewJobResults

Fill in one or more of the parameters to return a list of CIs that have been discovered by a job.

For details on the job operation parameters, see "Job Operation Parameters" on page 261.

When **Hide Touched CIs Info** is set to **True**, the results page displays the following information:

Column	Description
Job Name	Displayed if the jobID field is left empty. The job name as it appears in Discovery. Click a job to go to its viewJobStatus page, to view its status and scheduling information.
CI Type	Click to filter the list to show results for one CIT only.
Total CIs	Click to go to the viewJobResultCiInstances page, to view a list of all CIs that have been discovered by a job.

Column	Description
Triggered CIs	Click to go to the viewJobTriggeredCIs page, to view a list of all Trigger CIs that have been discovered by a job.
Last Discover Time	The date and time that the job was invoked.

When **Hide Touched CIs Info** is set to **False**, the results page displays the following information:

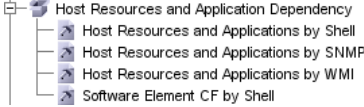
Column	Description
Job Name	Displayed if the jobID field is left empty. The job name as it appears in Discovery. Click a job to go to its viewJobStatus page, to view its status and scheduling information.
CI Type	Click to filter the list to show results for one CIT only.
Touched CIs	Click to go to the viewJobResultCiInstances page, to view a list of those CIs discovered by the job that are Touched CIs . For details, see "Job Operation Parameters" on page 261.
Non Touched CIs	Click to go to the viewJobResultCiInstances page, to view a list of those CIs discovered by the job that are not Touched CIs.
Triggered CIs for Touched CIs	Click to go to the viewJobTriggeredCIs page, to view a list of those Trigger CIs included in a job that are Touched CIs.
Triggered CIs for Non Touched CIs	Click to go to the viewJobTriggeredCIs page, to view a list of those Trigger CIs included in the job that are not Touched CIs.
Last Discover Time	The date and time that the job was invoked.

You can further filter results in the results page by entering text filters in one of the fields, and clicking the **Search** button.

viewJobsStatuses

Click the **viewJobsStatuses** button to return status and scheduling information for all jobs. You can choose to filter the results. For details, see "Job Operation Parameters" on page 261.

The results page displays the following information:

Column	Description
No.	The number of the job in the list.
Job Name	<p>The job name as it appears in Discovery, for example:</p>  <p>Click a job to go to its viewJobStatus page, to view its status and scheduling information.</p>
Status	<p>The severity of the job's status, as calculated by the Probe.</p> <p>Blocked. Not in use.</p> <p>Removed. The job is no longer active.</p> <p>Running. The job is currently running.</p> <p>Scheduled. The job is scheduled to run. For details on scheduling jobs, see "Discovery Scheduler Dialog Box" on page 301.</p> <p>A red background signifies that a thread has run longer than expected and may be stuck. A green background signifies that the job is running as expected.</p>
Errors	The number of errors for a specific job. Click to go to the viewJobErrorsSummary page, to view a list of error messages reported on this job.
Triggered CIs	The Trigger CIs that have been run by the job. Click to go to the viewJobTriggeredCIs page.
Last Invocation	The date and time that the job was last run.

Column	Description
Next Invocation	The date and time that the job is next scheduled to run.
Last Total run duration (seconds)	The total time that it took for the job to run in the last invocation. Compare this result with the average time taken for a job to run. The discrepancy is probably due to periods of time when a job waits for another job to finish.
Avg run duration (seconds)	The average time that the job ran, calculated from all previous invocations.
Recurrence	The number of times that the job was invoked. Click to go to the viewJobExecHistory page, to retrieve a history of job invocations.
Results	The number of CITs that have been discovered by the job. Click to go to the viewJobResults page to view the CITs.

viewJobStatus

Enter the name of a job to return its status and scheduling information.

For details on the job operation parameters, see "Job Operation Parameters" on page 261.

The results page displays the following information:

Column	Description
Threading info	The total number of worker threads created by the invocation, the free worker threads, and the stuck worker threads.
Total work time	The time that the Probe took to run this job.
Tasks waiting for execution	A list of jobs together with the number of Trigger CIs that are awaiting activation.
Max. threads	The number of threads that are serving this job.

Column	Description
<p>Progress</p>	<p>A summary of the current run, that is, since the specific run was activated.</p> <p>For example, Progress: 2017 / 6851 destinations (29%) means that out of 6851 CIs, 2017 CIs have already run.</p>
<p>Working Threads information</p>	<p>Thread Name. The thread that is now running this job. Click to go to the viewJobThreadDump page. You use this page when a thread is running for a long time, and you must verify that this is because the thread is working hard, and not because there is a problem.</p> <p>Curr Dest. ID. The name of the node on which the job is running.</p> <p>Curr Dest. IP. The IP for which the job is discovering information.</p> <p>Work Time (Sec). The length of time that this thread is running.</p> <p>Communication Log. Click to go to the viewCommunicationLog page, to view an XML file that logs the connection between the Probe and a remote machine. For details, see the Create communication logs field in the "Execution Options Pane" on page 152.</p>

Column	Description
Discovery Jobs Information table	<p>Status. The severity of the job's status, as calculated by the Probe. For details, see "Status" on page 256.</p> <p>Errors. Click to go to viewJobErrorsSummary page, to view a list of error messages reported on this job.</p> <p>Triggered CIs. Click to go to viewJobTriggeredCIs page, to view a list of Trigger CIs that are part of a job.</p> <p>Last invocation. The date and time that the job was last run.</p> <p>Next invocation. The date and time that the job is next scheduled to run.</p> <p>Last Total run duration (seconds). For details, see "Last Total run duration (seconds)" on page 257.</p> <p>Avg run duration (seconds). For details, see "Avg run duration (seconds)" on page 257.</p> <p>Recurrence. The number of times that the job was invoked. Click to go to viewJobExecHistory page, to view a history of job invocations.</p>
Results	<p>The number of CITs that have been discovered by the job. Click to go to the viewJobResults page to view the CITs.</p>

viewJobTriggeredCIs

Fill in one or more of the parameters to return a list of Trigger CIs that are part of a job.

For details on the job operation parameters, see "Job Operation Parameters" on page 261.

The results page displays the following information:

Column	Description
No.	The number of the job in the list.
Triggered CI ID	The CI instances that have been discovered by the job. Click to go to the viewJobResults page to view information about their CITs.
Last Execution	The date and time that the job was last run.
Service Exec. Duration (ms)	<p>The maximum time that it took for a job to run in the last invocation, not including periods when the job did not run. Compare this result with the total execution duration.</p> <p>For example, when several jobs run simultaneously, but there is only one CPU, a job might have to wait for another job to finish. The service duration does not include this waiting time, whereas the total duration does.</p>
Total Exec. Duration (ms)	The time that it took for a job to run in the last invocation, including the periods when the job did not run.
Last Run Status	The status of the last run, that is, whether the run succeeded or failed. In case of failure, click to go to the viewJobProblems page, to view a list of Trigger CIs with problems.
hostID	The name of the machine on which the job is running.
ip_address	<p>The IP address for which the job is collecting information.</p> <p>Note: If the Probe has not discovered the ID of the host (for example, because the job is given a range to discover and not a specific IP), information on the host may be missing. In this case, the hostID, ip_address, and ip_domain fields display the string (Empty).</p>
ip_domain	The Probe name as it appears in Discovery.

viewJobTriggeredCIsWithErrorId

Note: This operation is part of the inner interface and serves as a helper function. Do not use this page to view Trigger CIs information; instead, use the **viewJobTriggeredCIs** page.

Job Operation Parameters

The following list includes job operation parameters.

- ▶ **ciType.** The name of the CI type (for example, ip, host).
- ▶ **data.** A textual field in the DiscoveryResults table that contains information about the discovered object. For example:

```
<object class="ip">
  <attribute name="ip_probename" type="String">EBRUTER02</attribute>
  <attribute name="ip_address" type="String">16.59.58.200</attribute>
  <attribute name="ip_domain" type="String">DefaultDomain</attribute>
</object>
```

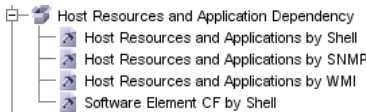
- ▶ **Error Id.** The error message hash string (error hash ID) that is displayed in the Jobs_Problems table.
- ▶ **HideRemovedJobs. True:** do not display jobs that have run previously and are not relevant to the current run.
- ▶ **Hide Touched CIs Info.** Touched CIs are CIs which were discovered in previous invocations. Discovery already has information about these CIs, so there is no need for the Probe to send the information to the server again. The server identifies that these CIs are relevant and that there is no need to enforce the aging mechanism on them. For details on aging, see "The Aging Mechanism Overview" in the *ODB Administration Guide*.

True: the table displays the total number of CIs and the total number of Trigger CIs for each CIT. **False:** The table displays the total number of CIs and Trigger CIs divided between touched CIs and non-touched CIs.

- **includeNonTouched.** Enables filtering the table to view non-touched CIs. Choose between viewing non-touched CIs only, all CIs (touched and non-touched), or none:

	Non-touched CIs	All CIs	No CIs
(boolean)includeTouchedCis	<input type="radio"/> True <input checked="" type="radio"/> False	<input checked="" type="radio"/> True <input type="radio"/> False	<input type="radio"/> True <input checked="" type="radio"/> False
(boolean)includeNonTouchedCis	<input checked="" type="radio"/> True <input type="radio"/> False	<input checked="" type="radio"/> True <input type="radio"/> False	<input type="radio"/> True <input checked="" type="radio"/> False

- **includeNonTouchedCIs.** See **includeNonTouched.**
- **includeTouched.** Enables filtering the table to view touched CIs. Choose between viewing touched CIs only, all CIs (touched and non-touched), or none.
- **includeTouchedCIs.** See **includeTouched.**
- **jobID.** The name of the job, for example, **Host Resources and Applications by SNMP:**



- **maxRows.** The maximum number of rows that should be displayed in the results table. The default is 100 or 1000.
- **maxTriggeredCIs.** See **maxRows.**
- **objectID.** The ODB object ID.
- **showRemovedJobs.** Shows information about jobs that are not currently scheduled to run, but that have run previously. These jobs take the state of **REMOVED.**
- **showResults.** Indicates whether to display the **Show Results** column. If the Show Results column is present, you can navigate from **viewJobsStatuses** to **viewJobResults.**
- **triggerCI.** The ODB object ID of the trigger for a job.
- **triggeredCiID.** See **triggerCI.**

Manually Activate a Job

You can activate a job by clicking the **Activate** button in the Discovery Modules pane. You can manually activate a CI by disabling the query and adding a CI. (You disable a query in the **Edit Probe Limitation for Queries Output** dialog box. You manually add a CI in the Choose CIs to Add dialog box.) The job runs using only the redispatched CIs. For details, see "Discovery Modules Pane" on page 296.

Manage Errors

This task describes how to investigate problems that arise during a run.

Note: For details about severity levels and so on, see "Managing Problems With Error Reporting" on page 243.

This task includes the following steps:

- "Prerequisites" on page 265
- "Run the Discovery Wizard or Select the Job" on page 265
- "Locate the Problem CI" on page 265
- "Troubleshoot the Problem" on page 264

1 Prerequisites

Set up Discovery. For details, see "Discovery Control Panel – Basic Mode Workflow" on page 246 or "Discovery Control Panel – Advanced Mode Workflow" on page 247.

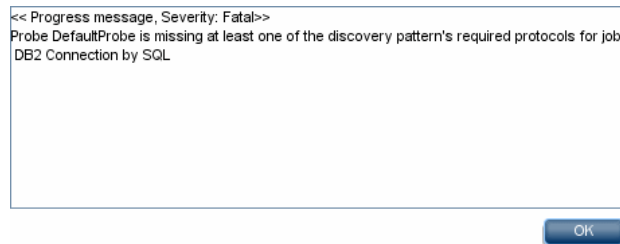
2 Run the Discovery Wizard or Select the Job

In Basic Mode, you can view error messages for a default job. In Advanced Mode, you can view error messages for one job, one module, or all modules. For details on running a wizard in Basic Mode, see "Discovery Control Panel – Basic Mode Workflow" on page 246. For details on running a job, see "Discovery Control Panel – Advanced Mode Workflow" on page 247.

3 Locate the Problem CI

Use the Discovery Status pane to drill down to the error messages. For details, see "Discovery Status Pane" on page 285. **Example:**

DFM displays the error message:



4 Troubleshoot the Problem

- For Fatal errors, you should contact HP Software Support.
- For other errors, check the CIs. For example, a Trigger CI that does not fall within the Probe's range may show an error.
- For details on setting communication logs, see "Execution Options Pane" on page 152.
- For details on managing problems, see "Managing Problems With Error Reporting" on page 243.

Find Errors

This task describes how to investigate problems that arise during a run.

Note: For details about severity levels and so on, see "Managing Problems With Error Reporting" on page 243.

This task includes the following steps:

- "Prerequisites" on page 265
- "Run the Discovery Wizard or Select the Job" on page 265
- "Locate the Problem CI" on page 265

1 Prerequisites

Set up DFM. For details, see Part II, "Data Flow Management Setup."

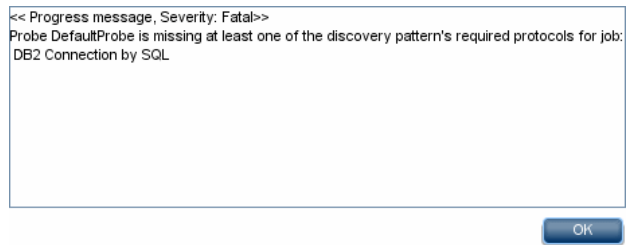
2 Run the Discovery Wizard or Select the Job

In Basic Mode, you can view error messages for a default job. In Advanced Mode, you can view error messages for one job, one module, or all modules. For details on running a wizard in Basic Mode, see "Discovery Control Panel – Basic Mode Workflow" on page 246. For details on running a job, see "Discovery Control Panel – Advanced Mode Workflow" on page 247.

3 Locate the Problem CI

Use the Discovery Status pane to drill down to the error messages. For details, see "Discovery Status Pane" on page 285.

Example of an error message:



Reference

Discovery Control Panel User Interface

This section describes:

- ▶ Advanced Mode Window on page 268
- ▶ Basic Mode Window on page 269
- ▶ Choose CIs to Add Dialog Box on page 271
- ▶ Choose Discovery Query Dialog Box on page 273
- ▶ Choose Probe Dialog Box on page 273
- ▶ Configuration Item Properties Dialog Box on page 273
- ▶ Create New Discovery Job Window on page 274
- ▶ Database Wizard on page 275
- ▶ Dependency Map Tab on page 282
- ▶ Details Tab on page 284
- ▶ Discovered CIs Dialog Box on page 295
- ▶ Discovery Modules Pane on page 296
- ▶ Discovery Permissions Window on page 299
- ▶ Discovery Scheduler Dialog Box on page 301
- ▶ Edit Probe Limitation for Query Output Dialog Box on page 304
- ▶ Edit Time Template Dialog Box on page 304
- ▶ Find Jobs Dialog Box on page 305
- ▶ Infrastructure Wizard on page 306
- ▶ J2EE Wizard on page 314
- ▶ Properties Tab on page 324
- ▶ Related CIs Window on page 329

- ▶ Show Results for Triggered CI Dialog Box on page 330
- ▶ Source CIs Dialog Box on page 331
- ▶ Time Templates Dialog Box on page 331
- ▶ Triggered CIs Window on page 332
- ▶ Trigger Query Editor Window on page 332

Advanced Mode Window

Enables you to view and manage modules and jobs, to activate jobs, and to follow job progress.

Advanced mode includes the following panes:

- ▶ **Discovery Modules pane.** Each module includes jobs. You activate a module or job to discover a specific group of CIs. For details, see "Discovery Modules Pane" on page 296.

Note: Basic Mode is displayed by default when accessing Discovery Control Panel.

- ▶ **Details tab.** Enables you to manage a module's CIs and view CI statistics. For details, see "Details Tab" on page 284.
- ▶ **Properties tab.** Enables you to view and administer the properties of modules and jobs. For details, see "Properties Tab" on page 324.

- **Dependency Map.** Displays a visual representation of the real-time progress of the process. For details, see "Dependency Map Tab" on page 282.

To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel
Important Information	<p>Each change you make in Discovery Control Panel is delivered to and stored in the ODB. From there, the changes are sent to the Probe. You can verify that changes have been sent to the Probe by opening the wrapperProbe.log file located in C:\hp\UCMDB\DataFlowProbe\runtime\logs\ and searching for the following lines:</p> <p>processing document domainScopeDocument.bin Processing document domainScopeDocument.bin is done.</p> <p>Note: Basic Mode is displayed by default when accessing Discovery Control Panel.</p>
Relevant tasks	"Discovery Control Panel – Advanced Mode Workflow" on page 247

Basic Mode Window

Enables you to use a Discovery wizard to discover infrastructure, databases, and J2EE applications.

Basic mode includes the following panes:




- **List of wizards.** Enables you to choose the wizard to run. For details, see "Infrastructure Wizard" on page 306, "Database Wizard" on page 275, or "J2EE Wizard" on page 314.
- **Summary pane.** Enables you to run the wizard and to stop Discovery running. For details, see "Summary Pane" on page 271.
- **Discovery Overview pane.** Enables you to:
 - View a brief run status and to drill down to problematic Trigger CIs. For details, see "Discovery Status Pane" on page 285.

- ▶ View statistics results. For details, see "Statistics Results Pane" on page 292.

This pane is displayed once discovery has been run for a component.

To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel
Important Information	Basic Mode is displayed by default when accessing Discovery Control Panel. For details on Advanced Mode, see "Advanced Mode Window" on page 268.
Relevant tasks	"Discovery Control Panel – Basic Mode Workflow" on page 246
See also	"Discovery Control Panel Overview" on page 240

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to refresh the list of wizards.
 Basic Mode	(Currently displayed) Click to run Discovery for a specific component (for example, the infrastructure, J2EE applications, or databases), using configurable, default preferences.
 Advanced Mode	Click to run Discovery when you need to customize a run by making changes to a job, adapter, and so on. For details, see "Advanced Mode Window" on page 268.

Summary Pane

Enables you to run a Discovery wizard.

To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel
Important Information	<p>Depending on whether a wizard has already run, the Summary pane displays the following information:</p> <ul style="list-style-type: none"> ▶ If a wizard has not yet run, the Summary pane displays the steps to be performed in the wizard and the Configure and Run button. ▶ If a wizard has run, the Summary pane displays a summary of the run parameters, the Configure and Stop Discovery buttons, and the results of the previous run in the Discovery Progress pane. <p>To run a discovery, select a wizard in the left pane and click Configure or Configure and Run to open the Discovery wizard.</p> <p>To stop a discovery run, click Stop Discovery.</p>
Relevant tasks	"Discovery Control Panel – Basic Mode Workflow" on page 246

Choose CIs to Add Dialog Box

Enables you to choose CIs to run with selected jobs.

To access	<ul style="list-style-type: none"> ▶ Admin > ODB Administration > Data Flow Management > Discovery Control Panel. In the Details tab, locate the Discovery Status pane. Click the Add CI button. ▶ In the Oracle TNSName File Location page of the Database Wizard, click the Add CI button.
------------------	---

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Add CI button	Note: If you choose CIs with an error status to add to the trigger list, a message is displayed when you click the Add button.
Search CIs	<p>Contains filters with which you can limit the number of CIs that appear in the Search Results pane.</p> <ul style="list-style-type: none"> ➤ By Discovery Query. Select a Discovery query to search for those CIs that match the query. ➤ Show only CIs containing. To search for CIs that include a certain text, enter the text here. ➤ Exact match. Select to search for CIs with the exact match of the text label. (By default, you search by entering part of a text. For example, searching for 10 within the IP CIs finds all the IPs that contain 10 in their address. Entering 10 then selecting Exact match finds no results.) ➤ Search. Click to display the search results.
Search Results	<p>Displays a list of triggered CIs answering to the criteria set in the filter. To add the CIs to the list in the triggered CIs pane, select the CIs. You can make multiple selections.</p> <ul style="list-style-type: none"> ➤ CIT. The CI type of the selected triggered CI. ➤ CI. The label of the triggered CI. ➤ Related Host. The label for the node related to the triggered CI. ➤ Related IPs. The IPs of the related node. <p>Page. The list of CIs is divided into pages. The number in the Page box indicates which page is currently displayed. To view other pages, use the up and down arrows, or type the page number, and press Enter.</p> <p>To determine the number of CIs that appear on a page, right-click either the up or down button and choose the required number. The default is 25.</p>

Choose Discovery Query Dialog Box

Enables you to add a trigger TQL to a job.

To access	Click the Add Query button in the Trigger Queries pane.
------------------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Discovery query name>	The query that queries the ODB for the selected CIT.
Query Preview	Hold the cursor over an element to view details.

Choose Probe Dialog Box

Enables you to filter the Probe list.

To access	Click a Filter button in the Discovery Control Panel > Details tab: <ul style="list-style-type: none"> ▶ Triggered CIs pane Filter button. For details on the menu options, see "Discovery Status Pane" on page 285. ▶ Statistics pane Filter button. For details on the menu options, see "Statistics Results Pane" on page 292.
------------------	---

Configuration Item Properties Dialog Box

Enables you to view CI properties.

To access	In the Discovered CIs dialog box, right-click a CI and choose Properties .
Important Information	For details, see "Configuration Item Properties Dialog Box" in the <i>Modeling Guide</i> .

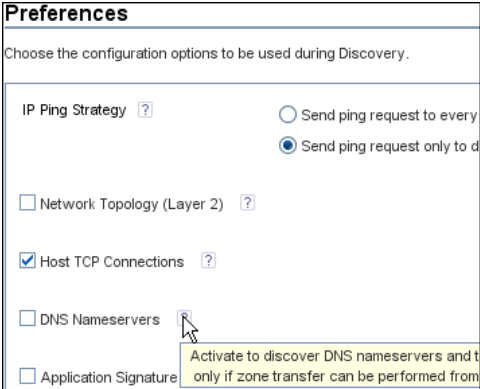
Create New Discovery Job Window

Enables you to create a job.

To access	Right-click a module in the Discovery Modules pane, and choose Create New Job .
Important Information	<ul style="list-style-type: none">➤ Job names must be limited to a length of 50 characters.➤ Job names must not start with a numeric value.
See also	For details on the panes in this window, see: <ul style="list-style-type: none">➤ "Discovery Job Details Pane" on page 285➤ "Parameters Pane" on page 327➤ "Trigger Queries Pane" on page 328➤ "Global Configuration Files Pane" on page 148➤ "Discovery Scheduler Pane" on page 324

Database Wizard

Enables you to discover databases such as DB2, Oracle, Microsoft SQL, and Sybase.




<p>To access</p>	<p>Admin > ODB Administration > Data Flow Management > Discovery Control Panel > Basic Mode. Select the Database wizard from the list in the left pane. Click Configure and Run.</p>
<p>Important Information</p>	<p>For more information, hold the pointer over a question mark icon:</p> 
<p>Wizard map</p>	<p>The Database Discovery wizard contains:</p> <p>Database Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary</p>



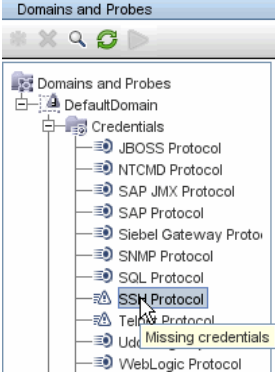
Define Credentials

Enables you to configure connection data for each protocol.

Important Information	<ul style="list-style-type: none"> ▶ You configure protocols depending on what must be discovered and which protocols are supported on your site's network. ▶ For a list of protocols, see "Domain Credential References" on page 83. ▶ General information about the wizard is available in "Database Wizard" on page 275.
Wizard Map	<p>The Database Discovery wizard contains:</p> <p>Database Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Add new connection details for selected protocol type.
	Remove a protocol.
	Edit a protocol. Click to open the Protocol Parameters dialog box.



GUI Element (A–Z)	Description
	Move a protocol up or down. Discovery executes all the protocols in the list with the first protocol taking priority.
Protocol	<p>Click to view details on the protocol, including user credentials.</p> <p>Note: A missing credential is represented by an icon , as shown in the following image:</p> 

Database Port Scanning

Enables you to discover the port itself and subsequently to discover the database.

Important Information	General information about the wizard is available in "Database Wizard" on page 275.
Wizard Map	<p>The Database Discovery wizard contains:</p> <p>Database Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	<p>Click to add a port to the port list. The Add New Port dialog box opens. Select the ports and click OK.</p> <p>To edit existing system ports, in the Add New Port dialog box, click Edit Known System Ports. The Edit Known System Ports dialog box opens. Select the port and click the Edit button. In the dialog box that opens, make changes to the entries and click OK.</p> <p>To add a port to the list, in the Edit Known System Ports dialog box, click the Add button. Enter details of the port name, number and type and click OK.</p>
	<p>Select a port and click the button to remove the port from the list.</p>

Custom JDBC Drivers

Enables you to select the JAR file for the DB2 and Sybase JDBC drivers.

<p>Important Information</p>	<p>General information about the wizard is available in "Database Wizard" on page 275.</p>
<p>Wizard Map</p>	<p>The Database Discovery wizard contains:</p> <p>Database Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
DB2 JDBC Driver	Select the check box and click Import file... to locate the appropriate JAR file in the DB2 JDBC installation, as follows: <ul style="list-style-type: none"> ➤ db2java.zip ➤ db2jcc.jar ➤ db2jcc_license_cu.jar ➤ db2jcc_license_cisuz.jar
Sybase JDBC Driver	Select the check box and click Import file... to locate the jconnectXXX.jar JAR file in the Sybase JDBC installation.



Oracle TNSName File Location

Enables the discovery of Oracle databases. You provide the location of the TNSNames.ora configuration file that contains database information needed to discover Oracle databases, such as port, node, SID, and so on.

Important Information	General information about the wizard is available in "Database Wizard" on page 275.
Wizard Map	The Database Discovery wizard contains: Database Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element (A-Z)	Description
Server Host	<p>Select the hosts on which the TNSNames.ora file is located. Click the Add CI button to choose the Trigger CIs that represent these hosts. For details, see "Choose CIs to Add Dialog Box" on page 271.</p> <ul style="list-style-type: none"> ▶ CIT. The CI type of the selected triggered CI. ▶ CI. The label of the triggered CI. ▶ Related Host. The label for the host related to the trigger CI. ▶ Related IPs. The IPs of the related host.
TNSNames.ora file location	<p>Enter the location of the TNSNames.ora file in the server host system. You can enter several locations (separate the locations by commas). If you terminate the path with a delimiter (for example, c:\temp\), Discovery assumes that the file name is tnsnames.ora.</p>

Schedule Discovery

Enables you to define a schedule for a specific job.

Important Information	<p>General information about the wizard is available in "Database Wizard" on page 275.</p>
Wizard Map	<p>The Database Discovery wizard contains:</p> <p>Database Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	You define a time template in the Discovery Scheduler pane of the Properties tab. For details, see "Discovery Scheduler Pane" on page 324.
Allow Discovery to run at	Choose the time at which the job should run.
Repeat Every	Select how often the job should run.

Summary

Enables you to review the wizard definitions before running a discovery.

Important Information	To make changes to the run, click the Back button. General information about the wizard is available in "Database Wizard" on page 275.
Wizard Map	The Database Discovery wizard contains: Database Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
Run	Click the button to run a discovery.

Dependency Map Tab

Displays a visual representation of the real-time progress of the discovery process. The map displays:

- CIs that were triggered by a job
- CIs that were discovered as a result of the activated job.

To access	Click the Dependency Map tab in the Discovery Control Panel window.
Important Information	<p>Depending which level you select in the Discovery Modules pane, different information is displayed in the Dependency Map tab.</p> <p>If you select:</p> <ul style="list-style-type: none"> ➤ The Discovery Modules root, and select the Show only active Discovery jobs check box, the Dependency Map displays only active jobs and their interdependencies. ➤ The Discovery Modules root, and clear the Show only active Discovery jobs check box, the Dependency Map displays all Discovery jobs and their interdependencies. ➤ A module, a topology map is displayed showing the module's active and inactive jobs. ➤ A job, the topology map highlights the job in the module's map.
See also	"Discovered CIs Dialog Box" on page 295

The following elements are included (unlabeled GUI elements are shown in angle brackets):

UI Elements (A-Z)	Description
<right-click menu>	<p>Use the right-click menu to view details for a job, CI, or link, for example, the number of CI instances (of a specific type) in the CMDB or the number of CI instances created by a specific job.</p> <p>Depending on which object is selected, the following menu options are displayed:</p> <ul style="list-style-type: none"> ▶ When a job is selected: <ul style="list-style-type: none"> Show discovered CIs. Click to view the CIs discovered by the job. To filter the query, select a CIT from the menu. Show trigger CIs. Click to view the CIs that triggered the job. ▶ When a CI is selected: <ul style="list-style-type: none"> Show all CIT instances. Click to view all CIs of this CI type. ▶ When a link from a CI to a job is selected: <ul style="list-style-type: none"> Show trigger CIs for job. Click to view CIs (of the selected type) that triggered the job. ▶ When a link from a job to a CI is selected: <ul style="list-style-type: none"> Show discovered instances. Click to view CIs (of the selected type) that were discovered by the job.
<Toolbar>	For details, see "Toolbar Options" in the <i>Modeling Guide</i> .
<Tooltip>	Hold the pointer over a CI or job to display a description.
Show only active Discovery jobs	When the Discovery Modules root is selected in the Discovery Modules pane, this check box is displayed. Select to display all active jobs (from any module).






Details Tab

Enables you to view and administer modules and jobs, to follow the progress of the Discovery process, and to manage errors during discovery.

To access	Click the Details tab in Discovery Control Panel .
Important Information	<p>Depending which level you select in the Discovery Modules pane, different information is displayed in the Details tab.</p> <p>If you select:</p> <ul style="list-style-type: none"> ▶ The Discovery Modules root or a Discovery module, the Discovery Status and Statistics Results panes are displayed with information and statistics about all active jobs and errors discovered during a run. For details, see "Discovery Status Pane" on page 285 and "Statistics Results Pane" on page 292. ▶ A job, the Discovery Job Details, Discovery Status, and Statistics Results panes are displayed. For details, see "Discovery Job Details Pane" on page 285, "Discovery Status Pane" on page 285, and "Statistics Results Pane" on page 292. ▶ Several jobs or modules, the Selected Items pane is displayed. For details, see "Selected Items Pane" on page 291.
Relevant tasks	"Error Messages Overview" in the <i>ODB Developer Reference Guide</i>

Discovery Job Details Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to go to the adapter in the Resources pane.
	You can choose to view a map of the CIs and links that are discovered by the adapter, instead of a list. Click the button to open the Discovered Classes Map window. The selected adapter is shown together with its CIs and relationships. Hold the cursor over a CIT to read a description in a tooltip.
	Click to view permissions that are defined for specific adapters. For details, see "Discovery Permissions Window" on page 299 For details on editing these permissions, see "Permission Editor Dialog Box" on page 173.
Adapter	The adapter needed by the job to discover the CIs.
Discovered CIs	The CIs that are discovered by this job.
Input CI Type	The CIT that triggers the CIs for this job.
Job Name	The name and description of the job. Important: Job names must not start with a numeric value.

Discovery Status Pane






Enables you to view a run status and to drill down to problematic Trigger CIs, to uncover specific problems that Discovery encountered during the run, for example, incorrect credentials.




In **Basic Mode**, enables you to view the results of the previous run for the selected job type (that is, infrastructure, database, or J2EE application).




In **Advanced Mode**, enables you to view the results of the previous run for a selected module or job, or for all modules.

To access	<ul style="list-style-type: none"> ▶ In Basic Mode, locate the Discovery Overview pane. ▶ In Advanced Mode, select a module or job, click the Details tab, and locate the Discovery Status pane.
Important Information	<ul style="list-style-type: none"> ▶ You can use the SHIFT and CTRL keys to select adjacent and non-adjacent CIs in a list. ▶ Depending which level you select in Advanced Mode in the Discovery Modules pane, information is displayed in the Discovery Status pane for all modules, for a specific module, or for a specific job. ▶ The information in this pane is automatically refreshed every thirty seconds.
Relevant tasks	"Check Status of Application Discovery (Rediscover a View)" in the <i>Modeling Guide</i>
See also	"Error Messages Overview" in the <i>ODB Developer Reference Guide</i>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to return to the upper pane.
	Click to drill down to the Trigger CI that includes the problem. Note: This icon is displayed only when you can drill down from error or warning links.
	Click to refresh the status view.
	Click to add a newly-discovered CI. For details, see "Choose CIs to Add Dialog Box" on page 271.
	Click to remove a CI from the list, if the CI is no longer of interest. The CI is deleted from the specific job.

GUI Element (A-Z)	Description
	<p>Click and choose an option from the menu:</p> <ul style="list-style-type: none"> ▶ By Status. Displays a list of Trigger CIs: <ul style="list-style-type: none"> ▶ All. Displays all the Trigger CIs. ▶ Waiting for Probe. Displays the Trigger CIs that are ready to be dispatched and are waiting for the Probe to retrieve them. ▶ In Progress. Displays the Trigger CIs that are active and are running on the Probe. ▶ In progress (being removed). Displays the Trigger CIs that are being removed from the Trigger CIs list. ▶ Success, Failed, Warning. Displays only those CIs that have the selected status. ▶ By Probe. Displays only the CIs triggered by a selected Probe. Click to open the Choose Probe dialog box. ▶ By Dispatch Type. Displays a list of CIs according to one of the following options: <ul style="list-style-type: none"> ▶ All. Displays both CIs that are used to manually activate the job and Discovery TQLs that are used to automatically activate the job. ▶ Manually added. Displays the CIs that are used to manually activate the job. ▶ By Discovery TQL. Displays the CIs that are used to automatically activate the job. ▶ Reset. Click to remove any filters.
	<p>Click to display a message box containing an explanation of the failure. (You can also view messages by right-clicking the CI and selecting Show error details.)</p>
	<p>Click to open the Triggered CIs dialog box with additional information about the CI. For details, see "Triggered CIs Window" on page 332.</p>

GUI Element (A-Z)	Description
	<p>► Show results for triggered CI. Discovery sends an ad-hoc request to the Probe and retrieves the latest results of the job (CIT name and number of discovered CIs) that is running on a specific trigger CI.</p> <p>This ad-hoc request does not run the job, but brings the results of the previous job run that are stored in the Probe's database. If the job has not yet run for this trigger CI, a message is displayed. See "Show Results for Triggered CI Dialog Box" on page 330.</p> <p>If no communication log exists in the Probe, a message is displayed. You can choose that Discovery always creates communication logs. For details, see "Execution Options Pane" on page 152.</p>
	<p>Click to rerun the discovery.</p>
	<p>Find a CI.</p>
<p><drill down></p>	<p>You can drill down from a job or a module.</p> <ul style="list-style-type: none"> ► Drill down from a job to view a list of Trigger CIs that are included in the job. ► Drill down from a module to view a list of the jobs in the module and the number of CIs returned by each job. Drill down from a job to its Trigger CIs. <p>Note: A Trigger CI can be present in more than one job.</p>

GUI Element (A-Z)	Description
<right-click CI menu>	<p>Right-click a CI to:</p> <ul style="list-style-type: none"> ▶ Show error details. Displays a list of the different types of errors returned by this CI. For details, see "Error Severity Levels" in the <i>ODB Developer Reference Guide</i>. ▶ Remove CI. Select to delete the CI from the job. The CI is removed from that job only, even if it appears in more than one job. ▶ Rerun Discovery. To run a specific CI or set of CIs, select the CIs. They are added to the list of CIs that the Probe is going to run (Waiting for Probe). ▶ Show results for triggered CI. Discovery sends an ad-hoc request to the Probe and retrieves the latest results of the job (CIT name and number of discovered CIs) that is running on a specific trigger CI. This ad-hoc request does not run the job, but brings the results of the previous job run that are stored in the Probe's database. If the job has not yet run for this trigger CI, a message is displayed. See "Show Results for Triggered CI Dialog Box" on page 330. If no communication log exists in the Probe, a message is displayed. You can choose that Discovery always creates communication logs. For details, see "Execution Options Pane" on page 152. ▶ Debug. Choose between: <ul style="list-style-type: none"> ▶ View communication log for triggered CI. Opens the log that includes information about the connection between the Probe and the remote machine. This is on condition that you have set the Create communication log to either Always or On failure. For details, see "Execution Options Pane" on page 152. ▶ Go to adapter. Displays the adapter that is included in the job in Adapter Management. ▶ Go to job. Displays the job in which the CI is included. ▶ Edit script. Select a script to open it in a script editor. ▶ Undispatch. Removes the Trigger CI.

GUI Element (A-Z)	Description
Failed	<p>Displays those CIs that returned a severity of type Error or Fatal.</p> <p>Right-click a job to rerun discovery.</p> <p>Double-click a job to display the error message.</p> <p>Right-click an error to deactivate or rerun a job.</p>
In progress	<p>Displays the number of Trigger CIs that are awaiting their turn to be run. Click to view the jobs that are waiting to be run.</p>
Look for	<p>To search for a specific Probe, related host, or related IP, enter part of its name in the box and click Search.</p>
Progress	<p>The indicator shows a summary of the current discovery run, that is, since the specific run was activated.</p>
Success	<p>Discovery displays the number of CIs that have been run successfully, that is, without errors.</p> <p>Click to view the jobs (and the number of CIs in each job) that completed successfully.</p> <p>Select a CI and use the right-click CI menu to view information.</p> <p>With warnings. Click to view a warning message for each job.</p> <p>Double-click a message to view the CIs that finished successfully with a warning.</p> <p>Right-click a message to view the right-click CI menu.</p>
Total	<p>Displays the status of all of a job's Trigger CIs. Double click a Warning or Error status to open the Message dialog box.</p>
Waiting for Probe	<p>The Trigger CIs that are either waiting for the Probe or are waiting to run.</p>

Selected Items Pane




The following elements are included (unlabeled GUI elements are shown in angle brackets):


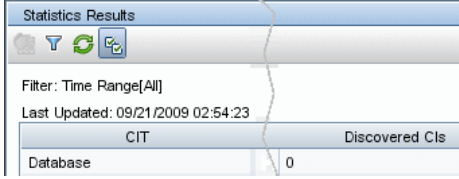
GUI Element (A–Z)	Description
<right-click menu>	Edit Scheduling. Click to open the Discovery Scheduler to define a schedule for a specific job. For details, see "Discovery Scheduler Pane" on page 324.
invoke immediately	<ul style="list-style-type: none"> ▶ A check mark signifies that the Discovery job runs as soon as the triggered CI reaches the Probe. In this case, the Invoke on new triggered CIs immediately check box is selected in the Properties tab. ▶ If this column does not contain a check mark, the job runs according to the schedule defined in the Schedule Manager.
Job name	The name of the job.
Schedule info	The scheduling information of the job as defined in the Discovery Scheduler.
Trigger Queries	The name of the query that activated the job. For details, see "Trigger Queries Pane" on page 328.

Statistics Results Pane

<p>Important Information</p>	<p>Version 9.01 includes a new purging mechanism for managing old Discovery result statistics. This mechanism enables faster display of the discovery results statuses. That is, the old statistics records are merged and therefore they are still available for the user. The new feature is controlled by two system parameters:</p> <ul style="list-style-type: none"> ▶ appilog.collectors.ResetDiscoveryStatisticsIntervalHours.name=Reset Discovery Statistics Interval by Hours. This property defines the interval of merging discovery statistics (the interval for running the purging mechanism). ▶ appilog.collectors.DiscoveryStatisticsArchiveDays.name=Discovery results statistics archive period. This property defines the number of days after which results statistics are being archived (the number of days after which the statistics are considered old). <p>For details on Infrastructure Settings, see "Infrastructure Settings Overview" in the <i>ODB Administration Guide</i>.</p>
-------------------------------------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	<p>Select a CI and click the View Instances button to view CI instances and their attributes. The Discovered CIs dialog box opens.</p> <p>Under the following conditions, a message is displayed:</p> <ul style="list-style-type: none"> ▶ All the CIs that were discovered by this job were already discovered by another job. ▶ All the CIs that this job discovered have been deleted. ▶ The CI instances were discovered in a previous version. (In version 7.0, you cannot view instances of CIs discovered in a previous version.) <p>Note:</p> <ul style="list-style-type: none"> ▶ You can also view CI instances by double-clicking a row. ▶ CITs with no instantiated instances are displayed.
	<p>Select the time range or Probe for which to display statistics about the CITs.</p> <ul style="list-style-type: none"> ▶ By Time Range: <ul style="list-style-type: none"> ▶ All. Displays statistics for all job runs. ▶ From Now/Last Minute/Hour/Day/Week. Choose a period of time for which to display statistics about the CITs. ▶ Custom Range. Click to open the Customize Statistics Time Range dialog box. Enter the date or click the arrow to choose a date and time from the calendar, for the To and From dates. To delete a date, click Reset. ▶ By Probe: To view statistics for a specific Probe, select to open the Choose Probe dialog box.
	<p>Click to retrieve the latest data from the server (job results are not automatically updated in the Statistics pane).</p>

GUI Element (A–Z)	Description
	<p>Show all declared CI Types. By default, only discovered CITs are listed in the table, that is, the Discovered CIs column includes CITs if the number of CIs found is greater than zero. Click the button to display every CI that can be discovered by the job, even if the Discovered CIs value is zero:</p> 
<Column title>	Click a column title to change the order of the CITs from ascending to descending order, or vice versa.
<right-click a title>	<p>Choose from the following options:</p> <ul style="list-style-type: none"> ▶ Hide Column. Select to hide a specific column. ▶ Show All Columns. Displayed when a column is hidden. ▶ Select Columns. Select to display or hide columns and to change the order of the columns in the table. Opens the Columns dialog box. ▶ Auto-resize Column. Select to change a column width to fit the contents. <p>For details, see "Select Columns Dialog Box" in the <i>Modeling Guide</i>.</p>
CIT	The name of the discovered CIT.
Created	The number of CIT instances created in the period selected or for the selected Probe.
Deleted	The number of CIT instances deleted in the period selected or for the selected Probe.
Discovered CIs	The number of CIs that were discovered for each CI type.
Filter	The time range set with the Set Time Range button.

GUI Element (A–Z)	Description
Last updated	The date and time that the statistics table was last updated for a particular job.
Total	The total number of CIs in each column.
Updated	The number of CIT instances that were updated in the period selected.

Discovered CIs Dialog Box

Enables you to view CI instances of a CIT discovered by a job.





To access	<ul style="list-style-type: none"> ➤ In the Statistics Results pane, select a CIT, and click the View instances button. ➤ In the Dependency Map tab, select Show Discovered CIs or Show all instances.
Important Information	<ul style="list-style-type: none"> ➤ The Discovered by <job name> window includes the same information as the Element Instances window. For details, see "Element Instances Dialog Box" in the <i>Modeling Guide</i>. ➤ Depending on whether you select Show discovered CIs or Show all instances in the Dependency Map, you can view either all CIs discovered by a selected job or all CIs of a selected type.





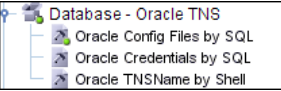

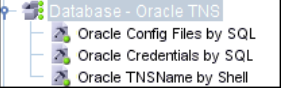
Discovery Modules Pane


Enables you to view and manage modules and jobs. Each module includes the jobs necessary to discover specific CIs.

To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel. The default view is called Basic Mode and displays the Discovery Wizard. You can run the J2EE, database, or infrastructure discovery. Click Advanced Mode to view all modules.
Important Information	<p>Caution: Only administrators with an expert knowledge of the Discovery process should delete modules.</p> <p>Obsolete. Contains several modules that are no longer relevant but remain for backward compatibility and upgrade purposes. Do not use these modules on new installations.</p> <p>No module. Contains jobs that are not included in any other module.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Refresh All. Updates the modules.
	Find Job. Click to open the Find Jobs dialog box. For example, to search for all jobs that discover SNMP connections, click the Filter icon. In the Find Jobs dialog box, enter SNMP in the Name box and click Find All . For details, see "Find Jobs Dialog Box" on page 305.
	Activate Selected Discovery Jobs. You can run one job or several jobs in a module, and one or several modules. Select either the jobs or modules and click Activate .
	Deactivate Selected Discovery Jobs. Select the jobs or modules to be stopped and click Deactivate .

GUI Element (A-Z)	Description
	<p>Represents the module root.</p> <p>To create a module, right-click to enter the name of the module you are creating.</p> <p>Note: A name is case sensitive. Names beginning with an upper case letter appear in the Discovery Modules list before names beginning with a lower case letter.</p>
	<p>Represents a module.</p>
	<p>Represents a job. Click to display information about the job. To view an adapter description, hold the pointer over a job.</p> <p>Jobs contain configuration information derived from adapters and other resources and are the entities controlled by users, for example, when activating or deactivating a module.</p> <p>For details on the right-click menu, see "Right-Click Menu" on page 298.</p>
	<p>One green dot signifies that some of a module's jobs are activated:</p> <div data-bbox="604 939 882 1029" style="border: 1px solid black; padding: 5px;">  <p>Database - Oracle TNS</p> <ul style="list-style-type: none"> Oracle Config Files by SQL Oracle Credentials by SQL Oracle TNSName by Shell </div>
	<p>Three green dots signify that all of a module's jobs are activated:</p> <div data-bbox="604 1138 882 1229" style="border: 1px solid black; padding: 5px;">  <p>Database - Oracle TNS</p> <ul style="list-style-type: none"> Oracle Config Files by SQL Oracle Credentials by SQL Oracle TNSName by Shell </div>

GUI Element (A–Z)	Description
	<p>An exclamation mark signifies that one or more of the jobs is experiencing a problem that could affect the Discovery process, for example, a protocol connection failure.</p> <p>To view the reason for the problem, click the (show errors) link in the Discovery Status pane. For details, see "Failed" on page 290.</p> <p>Note: If a problem is resolved by clicking the Refresh All button, the Problem Indicator disappears.</p>
Advanced Mode	(Currently displayed) Click to run Discovery to customize a run by making changes to a job, adapter, and so on.
Basic Mode	Click to run Discovery for a specific component (for example, the infrastructure, J2EE applications, or databases), using configurable, default preferences. For details, see "Basic Mode Window" on page 269.

Right-Click Menu

GUI Element (A–Z)	Description
Activate	<p>Click a module to run all its jobs. To run a specific job, select and activate it.</p> <p>The Discovery Module discovers CITs and relationships of the types that are described in each job, and places them in the CMDDB. For example, the Class C IPs by ICMP job discovers the Depend, IP, and Member CITs and relationships.</p>
Create New Job	Click to open the Create New Discovery Job. For details, see "Create New Discovery Job Window" on page 274.
Create New Module	<p>Click to define a new name for the module root.</p> <p>Note: Module names must be limited to a length of 50 characters.</p>
Deactivate	Stop the module or job from running.
Deactivate all jobs	Click Discovery Modules to display this option.
Delete	Click and answer Yes to the warning message.


GUI Element (A–Z)	Description
Delete job	Click and answer Yes to the warning message.
Go to adapter	Click to edit the adapter in the Adapter Management window.
Edit Scheduling	Click to open the Discovery Scheduler to define a schedule for a specific job.
Rename job	Click to open the Choose Name dialog box. Enter a new name for the job. Note: You cannot rename active jobs.
Run Now	Click to run the job again using the selected Trigger CIs.
Save as...	Click to clone the job.

Discovery Permissions Window

Enables you to view permissions data for jobs.

To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel > Advanced Mode. Select a job. Locate the Discovery Job Details pane in the Details tab. Click the View Permissions button.
See also	<ul style="list-style-type: none"> ➤ "Viewing Permissions While Running Jobs" on page 242 ➤ "Required Permissions Pane" on page 146 ➤ "Permission Editor Dialog Box" on page 173

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element (A-Z)	Description
	Export a permission object in Excel, PDF, RTE, CSV, or XML format. For details, see "Browse Views Mode" in the <i>Modeling Guide</i> .
Objects and Parameters	The commands that appear in the relevant Jython scripts.
Operation	The action that is being run.
Permission	The name of the protocol as defined for the job.
Usage Description	A description of how the protocol is used.

Discovery Scheduler Dialog Box

Enables you to define a schedule for a specific job, for example, every day Discovery starts running an IP ping sweep on class C networks at 6:00 AM.

<p>To access</p>	<ul style="list-style-type: none"> ▶ Right-click a job and choose Edit scheduling. ▶ Click the Edit Scheduler button in the Discovery Scheduler pane of the Properties tab in the Discovery Control Panel window.
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ The Discovery Scheduler defines the frequency of the discovery (daily, monthly) whereas the time template defines when the job should run (during the day, at night, at weekends only). You can run the same schedule with different time templates. For example, you can define a schedule that runs every day and you can define a time template that runs at night from 01:00 AM to 05:00 AM. A job defined in this way runs every day from 01:00 AM to 05:00 AM. You can define a second time template to run at a different time, and you can use this time template too with the same schedule. ▶ If you change a schedule for a job, Discovery next runs the job according to the following calculation: The current date and time plus the selected interval. For example, if you choose Once, the Invocation Time is in one hour. <p>For details on creating a time template, see "Edit Time Template Dialog Box" on page 304.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click to validate the Cron expression you entered.
<Frequency>	<ul style="list-style-type: none"> ➤ Once. Define the task to run only once. ➤ Interval. Defines the interval between successive runs. ➤ Daily. Run a task on a daily basis. ➤ Weekly. Run a task on a weekly basis. ➤ Monthly. Run a task on a monthly basis. ➤ Cron. Enter a Cron expression in the correct format.
Days of month	<p>(Displayed when you select Monthly.) Click the button to choose the days of the month on which the action must run. The Select Days dialog box opens. Choose the required days by selecting the check boxes. You can select multiple days.</p> <ul style="list-style-type: none"> ➤ Select all. Select all the days. ➤ Unselect all. Clear all the selected days.
Days of the week	(Displayed when you select Weekly .) Select the day or days on which the action should run.
End by	<p>Select the date and time when the action should stop running by selecting the End by check box, opening the calendar, selecting the date and time, and clicking OK.</p> <p>Note: This step is optional. If you do not need to specify an ending date, leave the End by check box cleared.</p>

GUI Element (A–Z)	Description
Invocation Hour	<p>(Displayed when you select Daily, Weekly, or Monthly.) Select the time to activate the action. Click the button to open the Select Hours dialog box. Choose the required time by selecting the check boxes. You can select multiple times.</p> <ul style="list-style-type: none"> ▶ Select all. Select all the times. ▶ Unselect all. Clear all the selected times. <p>Note: You can also enter the time manually in the Invocation hour box. Separate times by a comma and enter AM or PM after the hour. The manually entered action times are not restricted to the hour and half hour only: you can assign any hour and minute combination. Use the following format: HH:MM AM, for example, 8:15 AM, 11:59 PM.</p>
Invocation Time	<p>(Displayed when you select Once.) Choose the date and time the action should begin running by opening the calendar and choosing a date and time, or accept the default.</p>
Months of the year	<p>(Displayed when you select Monthly.) Select the month or months in which the action must run.</p>
Repeat every	<p>(Displayed when you select Interval.) Type a value for the interval between successive runs and choose the required unit of time (minutes, hours, or days).</p> <p>Note: After each change, the next time that the job runs is the current time plus the interval, that is, the job does not start immediately.</p>
Start at	<p>Choose the date and time when the action must begin running by selecting the Start at check box, opening the calendar, selecting the date and time, and clicking OK.</p>
Time Zone	<p>Select the time zone according to which the Probe must schedule jobs.</p> <p>The default is <<Data Flow Probe Time Zone>>: the Probe uses its own system-defined time zone. This enables scheduling to take place at different times in different geographical locations.</p> <p>For all Probes to start working at the same time, select a specific time zone. (This assumes that the Probes' system date and time and time zone are correctly configured.)</p>

Edit Probe Limitation for Query Output Dialog Box

Enables you to change the Probes on which a trigger TQL is running. For details on selecting the Probes, see "Selecting Probes" on page 83.

To access	Select a job and click the following button: Admin > ODB Administration > Data Flow Management > Discovery Control Panel > Properties tab > Trigger Queries pane > Probe Limit box.
------------------	--

Edit Time Template Dialog Box

Enables you to define a time template to use when scheduling jobs.

To access	Click the Add button in the Time Templates dialog box.
Important Information	The name of the time template must be unique.
See also	"Discovery Scheduler Dialog Box" on page 301

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Every day between	Define a daily schedule when a job must run. You can also type in times. You can assign any hour and minute combination.
Time Template	Enter a unique name.
Week Time	Define a weekly schedule when a job must run. Click to select a time. To select adjacent cells, click and drag the pointer over the table. To clear a time, click a cell a second time.

Find Jobs Dialog Box

Enables you to search for jobs answering to specific criteria. The results of the search are displayed in the Selected Items pane in the Details tab.

To access	Click the Search for Discovery Jobs button in the Discovery Modules pane.
------------------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
Direction	Searches forwards or backwards through the modules.
Find All	All jobs meeting the search criteria are highlighted.
Find Discovery job by	Choose between: <ul style="list-style-type: none"> ▶ Name. Enter the name, or part of it, of the job. ▶ Input type. CIs that triggered the job. Click the button to open the Choose Configuration Item Type dialog box. Locate the CI type that you are searching for. ▶ Output type. CIs that are discovered as a result of the activated job.
Find Next	The next job meeting the search criteria is highlighted.

Infrastructure Wizard

Enables you to run discovery on the networks in your system.



To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel > Basic Mode. Select Infrastructure Wizard from the list in the left pane. Click Configure and Run .
Wizard Map	The Infrastructure Discovery wizard contains: Infrastructure Wizard > Define IP Ranges > Define Credentials > Preferences > Schedule Discovery > Summary




Define IP Ranges

Enables you to set the network range for discovery for each Probe. The results are retrieved from the addresses in the range you define. You can also define IP addresses that must be excluded from a range.

Important Information	Any changes made here affect the global configuration. General information about the wizard is available in "Infrastructure Wizard" on page 306.
Wizard Map	The Infrastructure Discovery wizard contains: Infrastructure Wizard > Define IP Ranges > Define Credentials > Preferences > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	For details, see "Add/Edit IP Range Dialog Box" on page 69.
	Select a range and click the button to remove the range from the list.





GUI Element (A–Z)	Description
	Select a range and click the button to edit an existing range.
	Export a permission object in Excel, PDF, RTF, CSV, or XML format. For details, see "Browse Views Mode" in the <i>Modeling Guide</i> .
	Click to import ranges from a CSV file. Before using this feature, verify that the imported file is a valid CSV file, and that the ranges in the file do not conflict with existing ranges (that is, there are no duplicate or overriding ranges).
Address Ranges	<ul style="list-style-type: none"> ▶ Range. For details on the rules for defining ranges, see "Range" on page 71. ▶ Excluded. You can exclude part of a range. Select the range and click the Add button. In the dialog box, click the Advanced button. For details, see "Exclude Ranges" on page 70.
Data Flow Probes	<p>Enables you to view details on the Probe, including range information. You can also add ranges to, or exclude ranges from, the Probe.</p> <p>For details on defining a Probe, see "Domains and Probes Pane" on page 79.</p>

Define Credentials

Enables you to add, remove and edit a credentials set for protocols.

<p>Important Information</p>	<ul style="list-style-type: none"> ▶ You configure a credentials set depending on what must be discovered and which protocols are supported on your site's network. ▶ For a list of protocols, see "Domain Credential References" on page 83. ▶ General information about the wizard is available in "Infrastructure Wizard" on page 306.
<p>Wizard Map</p>	<p>The Infrastructure Discovery wizard contains: Infrastructure Wizard > Define IP Ranges > Define Credentials > Preferences > Schedule Discovery > Summary</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	<p>Add new connection details for selected protocol type.</p> <ul style="list-style-type: none"> ▶ For a list of protocols, see "Domain Credential References" on page 83.
	<p>Remove a protocol.</p>
	<p>Edit a protocol. Click to open the Protocol Parameters dialog box.</p>
	<p>Click a button to move a protocol up or down to set the order in which credential sets are attempted. Discovery executes all the protocols in the list with the first protocol taking priority.</p>
<p>Protocol</p>	<p>Click to view details on the protocol, including user credentials.</p>

Preferences

Enables you to choose the configuration options to be used during discovery that are activated by the Infrastructure Discovery wizard.

Important Information	General information about the wizard is available in "Infrastructure Wizard" on page 306.
Wizard Map	The Infrastructure Discovery wizard contains: Infrastructure Wizard > Define IP Ranges > Define Credentials > Preferences > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
DNS Nameservers	Discovers DNS nameserver machines and the IPs they hold names for. Choose to activate only if zone transfer can be performed from the Probe machine to the nameserver machines, that is, if the appropriate permissions exist on the DNS nameserver machines. Network implications. Discovery tries to connect to DNS nameserver servers.
Failover Cluster Discovery	Discovers failover clusters including HP Service Guard, Microsoft Cluster Service and Veritas Cluster.

GUI Element (A-Z)	Description
<p>Host Information</p>	<p>Select the host resources to be discovered. These resources can be either physically or logically part of a host.</p> <p>After Discovery connects to a host, it discovers the following resources:</p> <ul style="list-style-type: none"> ▶ For SNMP agents, the relevant Management Information Base (MIBs). ▶ For WMI agents, the relevant Windows Management Instrumentation Query Language (WQL) queries. <p>Discovery can also execute shell commands on a machine.</p> <p>Network implications. The Software and Services network resources, because of the large quantities of data that they transmit, may cause very high network traffic. For this reason, the default is not to discover them.</p>
<p>Host TCP Connections</p>	<p>Discover TCP communication channels to map dependency relationships between hosts.</p> <p>This discovery requires that at least one protocol has a defined set of credentials. For details, see the previous Define Credentials step.</p> <p>Network implications.</p> <p>Discovery executes Shell commands on a machine to find open ports.</p>

GUI Element (A-Z)	Description
IP Ping Strategy	<p>Choose the strategy for discovering IPs in your environment.</p> <p>This discovery requires that the SNMP protocol be configured in the previous Define Credentials step.</p> <ul style="list-style-type: none"> ▶ Send ping request to every address in defined IP range. Select this option when you know that most of the IP addresses will respond, the network range is small, and most of the IPs in the range are of interest to you (that is, they are part of your network). ▶ Send ping request only to discoverable IPs in a network. Select this option when you know that not all IP addresses will respond and the network range is large. In this case, Discovery first discovers a network, then sends a ping request to all discovered IPs in that network. <p>Versions and Limitations. Verify that you have the correct credentials set for all the machines between the Probe and one of the network's switches.</p>
Network Topology	<p>Activate to discover the connections, on a discovered switch (for example, a host), between a host and its physical port as well as between a host and its logical layout (VLANs, ELANs).</p> <p>This discovery requires that at least one protocol has a defined set of credentials. For details, see the previous Define Credentials step.</p>


GUI Element (A-Z)	Description
<p>Port Scanning</p>	<p>The TCP ports appearing in the Choose TCP ports for port scanning list are scanned to discover open server ports. The ports are scanned on every discovered host.</p> <p>You can add new ports to be scanned, and you can remove existing ports from the list.</p> <p>To choose a port that does not appear in the list:</p> <ol style="list-style-type: none"> 1 Click the Add port button to open the Add New Port dialog box. 2 Click the Add port button and enter the port name and number. 3 Click OK. <p>Network implications.</p> <p>Note that the scanning process may affect performance on the network. Furthermore, you may need to inform machine owners that Discovery will be trying to connect to their machines.</p>
<p>Software Element</p>	<p>Select to discover software elements running on the discovered hosts. As part of software element discovery, the processes and ports that are related to the software element are also discovered. The Software Library dialog box opens. For details, see "Software Library Dialog Box" on page 184.</p> <p>Network implications.</p> <p>A search pattern that is too general causes a toll on performance. For example, do not enter a process name that consists of an asterisk (*) only, as such a filter would try and retrieve all the processes running on all machines.</p>

Schedule Discovery

Enables you to define a schedule for a specific job.

Important Information	For details on scheduling Discovery, see "Discovery Scheduler Dialog Box" on page 301. General information about the wizard is available in "Infrastructure Wizard" on page 306.
Wizard Map	The Infrastructure Discovery wizard contains: Infrastructure Wizard > Define IP Ranges > Define Credentials > Preferences > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	You define a time template in the Discovery Scheduler pane of the Properties tab. For details, see "Discovery Scheduler Pane" on page 324.
Allow Discovery to run at	Choose the time at which the job should run.
Repeat Every	Select how often the job should run.

Summary

Enables you to review the definitions before running discovery.

Important Information	Click Run to begin Discovery. General information about the wizard is available in "Infrastructure Wizard" on page 306.
Wizard Map	The Infrastructure Discovery wizard contains: Infrastructure Wizard > Define IP Ranges > Define Credentials > Preferences > Schedule Discovery > Summary

J2EE Wizard

Enables you to run discovery on J2EE applications.






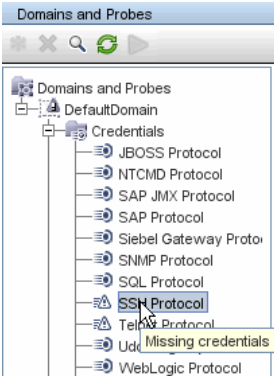
To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel > Basic Mode. Select the J2EE wizard from the list in the left pane. Click Configure and Run .
Important Information	For more information, hold the pointer over a question mark icon.
Wizard Map	The J2EE Discovery wizard contains: J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

Define Credentials

Enables you to configure connection data for each protocol.

Important Information	<ul style="list-style-type: none"> ▶ You configure protocols depending on what must be discovered and which protocols are supported on your site's network. ▶ For a list of protocols, see "Domain Credential References" on page 83. ▶ General information about the wizard is available in "J2EE Wizard" on page 314.
Wizard Map	The J2EE Discovery wizard contains: J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):



GUI Element (A–Z)	Description
	Add new connection details for selected protocol type.
	Remove a protocol.
	Edit a protocol. Click to open the Protocol Parameters dialog box.
	Move a protocol up or down. Discovery executes all the protocols in the list with the first protocol taking priority.
Protocol	<p>Click to view details on the protocol, including user credentials.</p> <p>Note: A missing credential is represented by an icon , as shown in the following image:</p>  <p>The screenshot shows a window titled "Domains and Probes" with a search bar and a list of protocols under "DefaultDomain > Credentials". The protocols listed are: JBOSS Protocol, NTCMD Protocol, SAP JMX Protocol, SAP Protocol, Siebel Gateway Proto, SNMP Protocol, SQL Protocol, SSH Protocol (highlighted with a tooltip "Missing credentials"), Telnet Protocol, Uddi, and WebLogic Protocol.</p>

J2EE Port Scanning

Enables you to choose the port number and port type through which to connect to the J2EE application.

Important Information	General information about the wizard is available in "J2EE Wizard" on page 314.
Wizard Map	The J2EE Discovery wizard contains: J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	<p>Click to add a port to the port list. The Add New Port dialog box opens. Select the ports and click OK.</p> <p>To edit existing system ports, in the Add New Port dialog box, click Edit Known System Ports. The Edit Known System Ports dialog box opens. Select the port and click the Edit button. In the dialog box that opens, make changes to the entries and click OK.</p> <p>To add a port to the list, in the Edit Known System Ports dialog box, click the Add button. Enter details of the port name, number and type and click OK.</p>
	Select a port and click the button to remove the port from the list.


WebLogic

Enables you to select the JAR files for specific WebLogic versions.

<p>Important Information</p>	<p>Discovery supports the following WebLogic versions: 6.x, 7.x, 8.x, 9.x, and 10.x.</p> <ol style="list-style-type: none"> 1 To discover WebLogic, obtain the following drivers: <ul style="list-style-type: none"> ➤ weblogic.jar (versions 6.x, 7.x, and 8.x only) ➤ wlcipher.jar (if WebLogic is running on SSL, for all versions) ➤ license.bea (if WebLogic is running on SSL but only for versions 6.x, 7.x, and 8.x) ➤ client trust store JKS file (for example, DemoTrust.jks, but only if WebLogic is running on SSL) ➤ wlclient.jar (versions 9.x and 10.x only) ➤ wljmxclient.jar (versions 9.x and 10.x only) 2 Place the driver under the correct version folder in the following location: C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\weblogic\ <version_folder>. For example, C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\weblogic\9.x. 3 On the WebLogic page in the J2EE wizard, select the check box for the versions to be discovered. Click Import file... to open a browse window. Browse to the appropriate WebLogic JAR file, as listed below. General information about the wizard is available in "J2EE Wizard" on page 314.
<p>Wizard Map</p>	<p>The J2EE Discovery wizard contains:</p> <p>J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Activate using default JAR files (version 8.x only)	Select to enable discovery without specifying version-specific JAR files. This is less recommended and works on some environments only.
WebLogic version 6.x	<ul style="list-style-type: none"> ➤ weblogic.jar ➤ For an SSL based discovery, select wlcipher.jar, license.bea, and the JKS file (for example, DemoTrust.jks)
WebLogic version 7.x	<ul style="list-style-type: none"> ➤ weblogic.jar ➤ For an SSL based discovery, select wlcipher.jar, license.bea, and the client trust store JKS file (for example, DemoTrust.jks)
WebLogic version 8.x	<ul style="list-style-type: none"> ➤ weblogic.jar ➤ For an SSL based discovery, select wlcipher.jar, license.bea, and the client trust store JKS file (for example, DemoTrust.jks)
WebLogic version 9.x	<ul style="list-style-type: none"> ➤ wlclient.jar ➤ wljmxclient.jar ➤ For an SSL based discovery, select wlcipher.jar and the client trust store JKS file (for example, DemoTrust.jks)
WebLogic version 10.x	<ul style="list-style-type: none"> ➤ wlclient.jar ➤ wljmxclient.jar ➤ For an SSL based discovery, select wlcipher.jar and the client trust store JKS file (for example, DemoTrust.jks)


WebSphere

Enables you to select the JAR files for specific WebSphere versions.

Important Information	<p>Discovery supports the following WebSphere versions: 5.x, 6.0, and 6.1.</p> <ul style="list-style-type: none"> ▶ To discover WebSphere, obtain the following certificates: <ul style="list-style-type: none"> ▶ client key store JKS file (DummyClientKeyFile.jks if WebSphere is running on SSL and the file is required) ▶ client trust JKS file (DummyClientTrustFile.jks if WebSphere is running on SSL) <p>Out-of-the-box drivers are located on the Probe machine at the following location: C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\websphere</p> <ul style="list-style-type: none"> ▶ Restart the Probe console before running the DDM jobs. <p>General information about the wizard is available in "J2EE Wizard" on page 314.</p>
Wizard Map	<p>The J2EE Discovery wizard contains:</p> <p>J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Activate using default JAR files (versions 5.x, 6.x only)	Select to enable discovery without specifying version-specific JAR files. This is less recommended and works on some environments only.
WebSphere	<p>Select the check box for the versions to be discovered. Click Import file... to open a browse window. Browse to the appropriate WebSphere JAR file, as follows:</p> <ul style="list-style-type: none"> ➤ admin.jar ➤ com.ibm.mq.pcf.jar ➤ ffdc.jar ➤ iwsorb.jar ➤ j2ee.jar ➤ jflt.jar ➤ jmx.jar ➤ jmxx.jar ➤ log.jar ➤ mail.jar ➤ ras.jar ➤ sas.jar ➤ security.jar ➤ soap.jar ➤ utils.jar ➤ wasjmx.jar ➤ websphere_arm_util.jar ➤ wlmclient.jar ➤ wsexception.jar ➤ wssec.jar


JBoss

Enables you to select the JAR files for specific JBoss versions.

Important Information	Discovery supports the following JBoss versions: 3.x, 4.x. General information about the wizard is available in "J2EE Wizard" on page 314.
Wizard Map	The J2EE Discovery wizard contains: J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
Activate using default JAR files (version 3.x, 4.x only)	Select to enable discovery without specifying version-specific JAR files. This is less recommended and works on some environments only.
JBoss version 3.x and 4.x	Select the check box for the versions to be discovered. Click Import file... to open a browse window. Browse to the jbossall-client.jar JBoss JAR file.


Oracle Application Server

Enables you to discover Oracle application servers.

Important Information	General information about the wizard is available in "J2EE Wizard" on page 314.
Wizard Map	The J2EE Discovery wizard contains: J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element (A-Z)	Description
Discover Oracle Application Server (version 10g)	Select to run Discovery for the Oracle Application Server, version 10g.

Schedule Discovery

Enables you to define a schedule for a specific job.

Important Information	General information about the wizard is available in "J2EE Wizard" on page 314.
Wizard Map	The J2EE Discovery wizard contains: J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	You define a time template in the Discovery Scheduler pane of the Properties tab. For details, see "Discovery Scheduler Pane" on page 324.
Allow Discovery to run at	Choose the time at which the job should run.
Repeat Every	Select how often the job should run.



Summary

Enables you to review the definitions before running discovery.

Important Information	To make changes to the run, click the Back button. General information about the wizard is available in "J2EE Wizard" on page 314.
Wizard Map	The J2EE Discovery wizard contains: J2EE Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
Run	Click to run Discovery.

Properties Tab

Enables you to view and administer the properties of modules and jobs.


To access	Click the Properties tab in Discovery Control Panel.
Important Information	<p>Depending which level you select in the Discovery Modules pane, different information is displayed in the Properties tab.</p> <p>If you select:</p> <ul style="list-style-type: none"> ▶ The Discovery Modules root, all active jobs are displayed with scheduling information. Click any of the columns to sort the list by that column. Right-click a job to edit its scheduling. For details, see "Discovery Scheduler Dialog Box" on page 301. ▶ A Discovery module, the Description and Module Jobs panes are displayed. To edit a description, make changes in the Description pane and click OK. See also "Module Jobs Pane" on page 325. ▶ A job, the Parameters, Trigger Queries, Global Configuration Files, and Discovery Scheduler panes are displayed. For details, see "Parameters Pane" on page 327, "Trigger Queries Pane" on page 328, "Global Configuration Files Pane" on page 148, and "Discovery Scheduler Pane" on page 324.

Discovery Scheduler Pane

Enables you to view information about the schedule set up for this job.

To access	Select a job in the Discovery Modules pane in the Discovery Control Panel window.
------------------	---

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to add times to the Enable Discovery to run at list. The Time Templates dialog box opens. To add a time template to the list, in the Time Templates dialog box, click the Add button to open the Edit Time Template dialog box. For details, see "Edit Time Template Dialog Box" on page 304.
Edit Scheduler	Click to open the Discovery Scheduler. For details, see "Discovery Scheduler Dialog Box" on page 301.
Invoke on New Trigger CIs Immediately	A check mark signifies that the job runs as soon as the Trigger CI reaches the Probe. If this column does not contain a check mark, the job runs according to the schedule defined in the Schedule Manager.
Time Template	Choose a template that includes the days and times when the job should run.

Global Configuration Files Pane




For details, see "Global Configuration Files Pane" on page 148.

Module Jobs Pane

Enables you to view the active jobs for a specific module.

To access	Select a module in the Discovery Modules pane in the Discovery Control Panel window.
------------------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Add Discovery Job to Module. Opens the Choose Discovery Jobs dialog box where you can select jobs from more than one zip file. (Use the SHIFT or CTRL key to select several jobs.)
	Remove Selected Discovery Job from Module. Select the job and click the button. (No message is displayed. To restore the job, click the Cancel button.)
	Show results as a map. You can choose to view a map of the CIs and links that are discovered by the adapter, instead of a list. Click the button to open the Discovered Classes Map window. The selected adapter is shown together with its CIs and relationships. Hold the cursor over a CIT to read a description in a tooltip.
<Column title>	Click a column title to change the order of the CITs from ascending to descending order, or vice versa.
<List of jobs>	All jobs included in the module. (Displayed when a specific module is selected in the Discovery Modules pane.)
<right-click menu>	Right-click a row to open the Discovery Scheduler for the selected job. For details, see "Discovery Scheduler Dialog Box" on page 301. Right-click a column title to customize the table. Choose from the following options: <ul style="list-style-type: none"> ➤ Hide Column. Select to hide a specific column. ➤ Show All Columns. Displayed when a column is hidden. ➤ Select Columns. Select to display or hide columns and to change the order of the columns in the table. Opens the Columns dialog box. ➤ Auto-resize Column. Select to change a column width to fit the contents. For details, see "Select Columns Dialog Box" in the <i>Modeling Guide</i>.

GUI Element (A–Z)	Description
Invoke Immediately	<ul style="list-style-type: none"> ▶ A check mark signifies that the Discovery job runs as soon as the triggered CI reaches the Probe. In this case, the Invoke on new triggered CIs immediately check box is selected in the Properties tab. ▶ If this column does not contain a check mark, the job runs according to the schedule defined in the Schedule Manager.
Job Name	<p>The name of the job and the package in which the job is included.</p> <p>(Displayed when a job is selected in the Discovery Modules pane.)</p>
Schedule Information	<p>The scheduling information of the job as defined in the Discovery Scheduler.</p>
Trigger Queries	<p>The name of the TQL that activated the job.</p>

Parameters Pane

Enables you to override adapter behavior.

To view a description, hold the pointer over the parameter.

To access	<p>Select a job in the Discovery Modules pane in the Discovery Control Panel window.</p>
Important Information	<p>You can override a default adapter parameter for a specific job, without affecting the default value.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):





GUI Element (A-Z)	Description									
Name	The name given to the adapter.									
Override	<p>Select to override the parameter value in the adapter.</p> <p>When this check box is selected, you can override the default value. For example, to change the <code>protocolType</code> parameter, select the Override check box and change <code>MicrosoftSQLServer</code> to the new value. Click OK in the Properties tab to save the change:</p> <table border="1" data-bbox="632 663 1212 788"> <thead> <tr> <th colspan="3">Parameters</th> </tr> <tr> <th>Override</th> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td><code>protocolType</code></td> <td><code>MicrosoftSQLServer</code></td> </tr> </tbody> </table> <p>For details on editing parameters in the Adapters Parameters pane, see "Adapter Parameters Pane" on page 149.</p>	Parameters			Override	Name	Value	<input checked="" type="checkbox"/>	<code>protocolType</code>	<code>MicrosoftSQLServer</code>
Parameters										
Override	Name	Value								
<input checked="" type="checkbox"/>	<code>protocolType</code>	<code>MicrosoftSQLServer</code>								
Value	The value defined in the adapter.									

Trigger Queries Pane

Enables you to define one or more queries to be used as triggers to activate the selected job.

To access	<ul style="list-style-type: none"> ▶ Select a job in the Discovery Modules pane in the Discovery Control Panel window. ▶ Create a job by right-clicking a module in the Discovery Modules pane, and choose Create New Job.
------------------	---

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Add Query. You can add one or more non-default TQL queries to be used as triggers to activate the selected job. Click to open the Choose Discovery Query dialog box.
	Remove Query. Select the TQL and click the button. (No message is displayed. To restore the query, click the Cancel button.) Note: If a query is removed for an active job, Discovery no longer receives new CIs coming from that query. Existing Trigger CIs that originally came from the query are not removed.
	Click to add or remove Probes for a specific query. For details, see "Edit Probe Limitation for Query Output Dialog Box" on page 304.
	Click to open the Trigger Query Editor. For details, see "Trigger Query Editor Window" on page 332.
Probe Limit	The Probes being used for the discovery process. To add or remove Probes, click the button.
Query Name	The name of the trigger query that activates the job.

Related CIs Window

Enables you to view, in map format, the CIs that are related to a selected CI.

To access	In the Discovered CIs dialog box, right-click a CIT and select Get Related CIs .
Important Information	Related CIs are CIs that are the parent, child, or sibling of an existing CI.

The following elements are included (unlabeled GUI elements are shown in angle brackets):



GUI Element (A-Z)	Description
<right-click menu>	For details, see "Shortcut Menu" in the <i>Modeling Guide</i> .
<menu>	For details, see "Toolbar Options" in the <i>Modeling Guide</i> .
<Topology Map>	For details, see "Topology Map Overview" in the <i>Modeling Guide</i> .

Show Results for Triggered CI Dialog Box

Enables you to view the results of running an ad-hoc request to the Probe. Discovery acquires the results by running the job on a selected trigger CI. In the case of an error, a message is displayed.

To access	Discovery Control Panel , select a module or job, select the Details tab. In the Discovery Status pane, drill down to a CI, right-click it, and choose Show Results for Triggered CI .
------------------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Select a CIT and click to display additional information in the Show Results for Triggered CI dialog box. For details, see "Show Results for Triggered CI Dialog Box" on page 330.
	Click to open a topology map showing a result map for the Triggered CI. Right-click a CIT to view its properties.

Source CIs Dialog Box




The Source CIs dialog box includes the same components as the **Discovered CIs** dialog box. For details, see "Discovered CIs Dialog Box" on page 295.

Time Templates Dialog Box

Enables you to define a daily or weekly schedule to run selected jobs.

To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel > Properties tab > Discovery Scheduler pane > Time Template icon
-----------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to add a time template. Opens the Edit Time Template dialog box.
	Select a time template and click to delete.
	Select a time template and click to edit it. Opens the Edit Time Template dialog box.

Triggered CIs Window

Enables you to view all CI instances found for a selected TQL node.

To access	<ul style="list-style-type: none"> ▶ Admin > ODB Administration > Data Flow Management > Discovery Control Panel > Dependency Map tab. Right-click a CIT and select Show Triggered CIs. ▶ In the Discovery Status pane, click the Show additional data button
Important Information	The Triggered CIs window includes the same information as the Element Instances window. For details, see "Element Instances Dialog Box" in the <i>Modeling Guide</i> .

Trigger Query Editor Window

Enables you to edit a TQL that has been defined to trigger jobs.

To access	Admin > ODB Administration > Data Flow Management > Discovery Control Panel > Properties tab > Trigger Queries pane > select a TQL and click the Open the Query Editor button
Important Information	A Trigger query associated with a job is a subset of the Input query, and defines which specific CIs should be the Trigger CIs for a job. That is, if an Input query queries for IPs running SNMP, a Trigger query queries for IPs running SNMP in the range 195.0.0.0-195.0.0.10.
See also	<ul style="list-style-type: none"> ▶ "Trigger CIs and Trigger Queries" on page 29 ▶ "Input Query Editor Window" on page 167

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Panels>	<ul style="list-style-type: none"> ➤ CI Type Selector Pane ➤ Editing Pane ➤ Information Pane
Query Name	The name of the trigger query that activates the job.

CI Type Selector Pane

Displays a hierarchical tree structure of the CI Types found in the CMDB. For more details, see "CI Type Manager User Interface" in the *Modeling Guide*.

Note: The number of instances of each CIT in the CMDB is displayed to the right of each CIT.

Important Information	To create or modify a TQL query, click and drag nodes to the Editing pane and define the relationship between them. Your changes are saved to the CMDB. For details, see "Add Query Nodes and Relationships to a TQL Query" in the <i>Modeling Guide</i> .
Relevant tasks	<ul style="list-style-type: none"> ➤ "Define a TQL Query" in the <i>Modeling Guide</i> ➤ "Create a Pattern View" in the <i>Modeling Guide</i>

Editing Pane

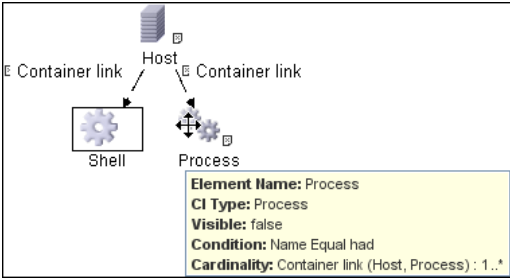
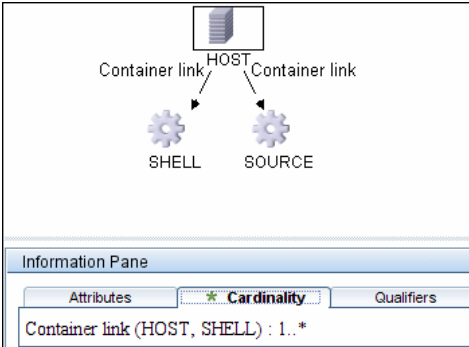
Enables you to edit the node selected in the Trigger Queries pane.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


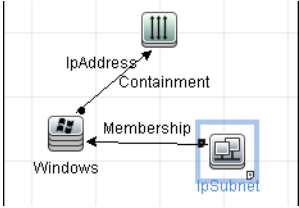
GUI Element (A-Z)	Description
<node>	Click to display information about the node in the information pane.
<right-click menu>	For details, see "Shortcut Menu Options" in the <i>Modeling Guide</i> .
<Toolbar>	For details, see "Toolbar Options" in the <i>Modeling Guide</i>

Information Pane

Displays the properties, conditions, and cardinality for the selected node and relationship.

<p>Important Information</p>	<p>Hold the pointer over a node to view information:</p>  <p>A small green indicator is displayed next to the tabs that include information:</p> 
-------------------------------------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	<p>To view information, select a node or relationship in the Editing pane, select the tab in the Information Pane, and click the Edit button. For details on the Node Condition dialog box, see "Query Node/Relationship Properties Dialog Box" in the <i>Modeling Guide</i>.</p>
Attributes	<p>Displays the attribute conditions defined for the node or the relationship. For details, see "Attribute Tab" in the <i>Modeling Guide</i>.</p>
Cardinality	<p>Cardinality defines how many nodes you expect to have at the other end of a relationship. For example, in a relationship between host and IP, if the cardinality is 1:3, the TQL retrieves only those hosts that are connected to between one and three IPs. For details, see "Cardinality Tab" in the <i>Modeling Guide</i>.</p>
Details	<ul style="list-style-type: none"> ▶ CI Type. The CIT of the selected node/relationship. ▶ Visible. A tick signifies that the selected node or relationship is visible in the topology map. When the node/relationship is not visible, a box <input type="checkbox"/> is displayed to the right of the selected node/relationship in the Editing pane: <div style="text-align: center; border: 1px solid gray; padding: 10px; width: fit-content; margin: 10px auto;">  </div> <ul style="list-style-type: none"> ▶ Include subtypes. Display both the selected CI and its descendants in the topology map.
Qualifiers	<p>Displays the qualifier conditions defined for the node or the relationship. For details, see "Qualifier Tab" in the <i>Modeling Guide</i>.</p>

GUI Element (A-Z)	Description
Selected Identities	Displays the element instances that are used to define what should be included in the TQL results. For details, see "Identity Tab" in the <i>Modeling Guide</i> .

Part V

Reconciliation

10

Reconciliation

This chapter includes:

Concepts

- ▶ Reconciliation Overview on page 340
- ▶ Stable ID on page 341
- ▶ Reconciliation Configuration on page 341
- ▶ Reconciliation Services on page 346

Tasks

- ▶ Add an Identification Rule to an Existing CIT on page 353
- ▶ Add Reconciliation Priorities to an Existing CIT on page 353
- ▶ Create XML Reconciliation Files on page 354

Reference

- ▶ Identification Rule Schema on page 358
- ▶ Reconciliation Priority Schema on page 366

Concepts

Reconciliation Overview

Reconciliation is the process of identifying and matching entities from different data repositories (for example, ODB Discovery, DDMi, ticketing, or BSM). This process is designed to avoid duplicate CIs in ODB.

Many different data collectors can send CIs to ODB. In actuality, each different source might be providing information about the same CI. The reconciliation engine is responsible for identifying and matching entities from different data collectors and storing them, without duplicating CIs, in ODB.

Three main services provide support for the reconciliation engine:

- ▶ **Data Identification.** Responsible for comparing input CIs, according to reconciliation rules. For details, see "Identification Service" on page 347.
- ▶ **Data In.** Responsible for inserting data into ODB. This service decides:
 - ▶ whether to merge data into existing CIs in ODB
 - ▶ whether to ignore input CIs in the case of multiple matchesFor details, see "Data In Service" on page 348.
- ▶ **Merge.** Responsible for merging CIs (used in Federation and Data In flows). Merging is done according to the reconciliation priority definitions.

These services operate during reconciliation for inserting data from different sources into ODB, and during federation for connecting or merging information from different data repositories during TQL calculations.

The reconciliation engine contains out-of-the-box identification and match criteria rules for most usable and problematic CITs, such as host, software element, and so on.

Stable ID

ODB now generates stable IDs during CI creation. This means that the ID of the CI is no longer calculated from the CI's properties. This stable ID therefore remains the same when the name, attribute name, or property values (during normalization) change.

Reconciliation Configuration

The reconciliation engine uses XML configuration files that contain identification and match criteria to determine how CIs are identified during federation or data insertion. Configuration files for out-of-the-box CI types are provided when packages are deployed, but you can modify the provided files or create additional files. For details, see "Create XML Reconciliation Files" on page 354.

The following rules are used during reconciliation:

1 Identification

- a** Identification criteria – These criteria locate a candidates list that may match to a newly introduced CI, either in the CMDB or from a different data repository.
- b** Match criteria – There are two types of match criteria:
 - ▶ Match verification criteria – a set of criteria that are applied to all candidates left over after performing step a (identification). Match verification ends successfully only when all applied criteria are true or NA (missing data).
 - ▶ Match validation criteria – an ordered set of criteria that are applied to all candidates left over after performing match verification. For each criterion, the following results are possible:
 - a true result implies a match
 - a false result implies no match
 - NA (missing data) causes reconciliation to proceed to the next criterion

- 2 Reconciliation Priority (conflict resolution) – configuration that specifies how matched CIs are merged. You set these priorities in the Reconciliation Priority Manager. For details, see "Reconciliation Priority Manager Window" on page 211.

This section also includes:

- "Identification and Match Criteria Configuration" on page 342
- "Reconciliation Priority Configuration" on page 344

Identification and Match Criteria Configuration

Due to the discovery method (local or remote), the available credentials (for example, remote access to SNMP or WMI), and specific system security settings (for example, the system responds to a ping), an integration point may have access to only a limited set of attributes when identifying a CI. For example, IP range discovery detects two IP addresses (10.12.123.101 and 16.45.77.145), and creates two nodes. However, detailed system discovery may detect that those two IP addresses are actually configured on two network interfaces in the same node.

This means that you cannot always rely on a single matching set of attributes for identification – other possible attributes that can potentially help to identify the CI should also be listed. In the previous example, the host identification attributes can be the IP address and the network interface. If you use the IP address to identify the CI, you see that all three discovered hosts are the same host.

However, suppose that detailed system discovery detects a host with IP address 10.12.123.101 and network interface MAC1. At some point, that host was shut down, and the the same IP address (10.12.123.101) was given to another host with network interface MAC2. These two hosts have the same IP address; however; it is obviously not the same CI. Performing match validation on the network interface data helps us to realize that it is not the same host.

The identification criteria are used to select candidates, and the match criteria are used to approve the identification result or dismiss it. For example, while handling input CI A, we may get identification candidates B and C, and the match criteria will dismiss B. In that case, we are left with C, which means that A is identified as B.

Identification Criteria

Data that the reconciliation engine receives from different data sources may contain different subsets of the attributes (topology) necessary for identifying a CI. The identification criteria should contain all potential attributes on which CI matching can be done.

Specifications

Each identification criterion defines a potential condition for CI matching. The criterion can be an attribute such as host name, or topology such as IP address. A criterion may contain two or more conditions, to create a more complex matching rule. It may also contain different condition operators such as equals or contains, or it may contain some master value that defines a value in the CI that will always allow a match.

During the identification process, all identification criteria are running to find all candidate CIs for matching.

Possible Host Identification Criteria

- HW ID
- Network interface (containing a condition operator)
- Host name
- IP address (containing a condition operator)

These host identification criteria show all possible host attributes that can be used for host matching. For example, if there are two hosts with the same HW ID or the same IP address, these hosts are candidates for matching.

Match Criteria

While identification criteria list all potential attributes for matching the data, match criteria contain the attributes that are essential for matching CIs, if any exist. This means that if two CIs are marked as candidates to be matched by the identification criteria, the match criteria will check if the data exists in both CIs in order to match the condition.

Match criteria are also used during the Data In process in case of multiple matches, to make the decision to merge CIs from the CMDB. The CIs are merged only if the match criteria are satisfied. If one of the CIs does not satisfy the match criteria, the merge is not performed.

Specifications

A match criterion is satisfied if two candidate CIs have the same essential data (as defined in the that criterion), the data matches the condition, or if at least one of the CIs has no essential data.

Match criteria can be divided into two categories:

- ▶ Match verification criteria – if the verification criterion is not satisfied on two candidate CIs, these CIs are not matched.
- ▶ Match validation criterion – if the criterion with higher priority is satisfied (without missing data) on two candidate CIs, the validation criterion with lower priority is even not checked and the CIs are marked as matched. Similarly, if the validation criterion with higher priority is refuted on two candidate CIs, the criterion with lower priority is even not checked and the CIs are marked as not matched.

Possible Host Match Criteria

- ▶ Match verification criteria uses the discovered OS data for verification. This means that if two hosts have discovered OS data and this data does not match, these two hosts are not matched.
- ▶ Match validation criteria (ordered from higher to lowest priority):
 - ▶ HW ID with an **equals** operator
 - ▶ Network interface with a **contains** operator
 - ▶ Host name with an **equals** operator

This means that if two hosts with the same HW ID are discovered, they are marked as matched even if they have different network interfaces or host names. On the other hand, if the discovered HW IDs on the hosts are not the same, the hosts are not marked as matched even if the network interfaces and host names are the same. The network interface rule is checked only if one of the hosts has no discovered HW ID.

Reconciliation Priority Configuration

When a CI is matched with another CI, they should be merged. This behavior becomes relevant in the following situations:

- ▶ During Data In service operation – to insert data to the ODB.

- During Federation – when multiple data repositories supply the same CI with different properties.

To solve this problem, you define priorities for each data repository to each CIT and attribute.

For details, see "Reconciliation Priority Manager Window" on page 211.

Examples of Identification Configuration

Sample "vlan" CI Type Identification Configuration

```
<identification-config type="vlan">
  <identification-criteria>
    <identification-criterion>
      <attribute-condition attributeName="vlan_id"/>
      <connected-ci-condition ciType="physical_port" linkType="membership">
        <overlap-fixed-operator number-of-matches="1"/>
      </connected-ci-condition>
    </identification-criterion>
  </identification-criteria>
</identification-config>
```

Sample "interface" CI Type Identification Configuration

```

<identification-config type="interface">
  <identification-criteria>
    <identification-criterion>
      <attribute-condition attributeName="root_container"/>
      <attribute-condition attributeName="mac_address"/>
    </identification-criterion>
    <identification-criterion>
      <attribute-condition attributeName="root_container"/>
      <attribute-condition attributeName="interface_name"/>
    </identification-criterion>
  </identification-criteria>
  <match>
    <verification-criteria>
      <verification-criterion>
        <attribute-condition attributeName="interface_type"/>
      </verification-criterion>
      <verification-criterion>
        <attribute-condition attributeName="interface_name"/>
      </verification-criterion>
      <verification-criterion>
        <attribute-condition attributeName="mac_address"/>
      </verification-criterion>
      <verification-criterion>
        <attribute-condition attributeName="interface_description"/>
      </verification-criterion>
      <verification-criterion numberOfConflictsToFailIdentification="2">
        <attribute-condition attributeName="interface_alias"/>
        <attribute-condition attributeName="interface_index"/>
        <attribute-condition attributeName="interface_speed"/>
      </verification-criterion>
    </verification-criteria>
  </match>
</identification-config>

```

Reconciliation Services

This section includes:

- ▶ "Identification Service" on page 347
- ▶ "Data In Service" on page 348

- "Merge Service" on page 352

Identification Service

The Identification service uses identification and match criteria to identify CIs. The process is as follows:

- 1** Finding matching candidates: Find all CIs that are matched with Input CI at least by one identification criterion.
- 2** For all candidate CIs from step 1, run match verification criteria. If one of the verification criteria is not satisfied for any CI, remove that CI from the candidates list.
- 3** For the remaining CIs from step 2, run match validation criteria one by one:
 - a** When the first validation criterion is satisfied, stop and mark the current candidate CI as matched.
 - b** When the first validation criterion is refuted (the data exists but does not match), mark the current candidate CI as unmatched.
 - c** If none of the validation criteria are satisfied or refuted, mark the current candidate CI as matched.

Identification Process Example

The following items are used in this example:

Input host host_name = h1, ip_address = ip1, MAC address = m1, os = nt

- CMDB hosts
- H1 = host_name=h2
 - H2 = ip_address=ip1,ip2
 - H3 = host_name=h3, MAC address = m1, hw_id = id1, os = unix)

1 For each CMDB host, run the identification criteria:

- If host H1 does not match any identification criteria, it will not be added to the candidates list.
- If host H2 matches the IP identification criterion of the input host, it will be added to the candidates list.
- If host H3 does not match the input host by the IP identification criterion, but does match by the MAC address identification criterion, it will be added to the candidates list.

The candidates list is: H2 and H3.

2 For each host in the candidates list, run OS match verification criteria. Host H3 does not satisfy this rule, since its OS is UNIX and the input host's OS is NT. Therefore, H3 will be removed from the candidates list.

The candidates list is: H2.

3 Run the match validation criteria one by one on host H2. Since host H2 has no data conflicts, the match validation criteria are approved and H2 is marked as matched.

The result of identification process is: H2.

Data In Service

After the Identification service runs, the identified data is merged and inserted into the CMDB by the Data In service.

One of the major problems that the Data In service solves is deciding what to do if the input CI matches multiple ODB CIs. There are three options:

- merge all matched CIs into one
- ignore the input CI

The Data In service uses match criteria to make the decision. The process is as follows:

1 Merge the input CI with each matching ODB CI.

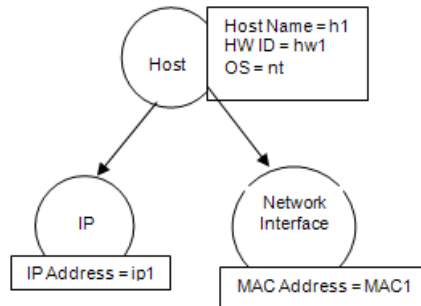
2 For each pair of CIs resulting from step 1, run match criteria (verification and validation criteria).

If at least one pair does not pass the match criteria check, the CIs are not merged. If all pairs pass the match criteria check, the CIs are merged.

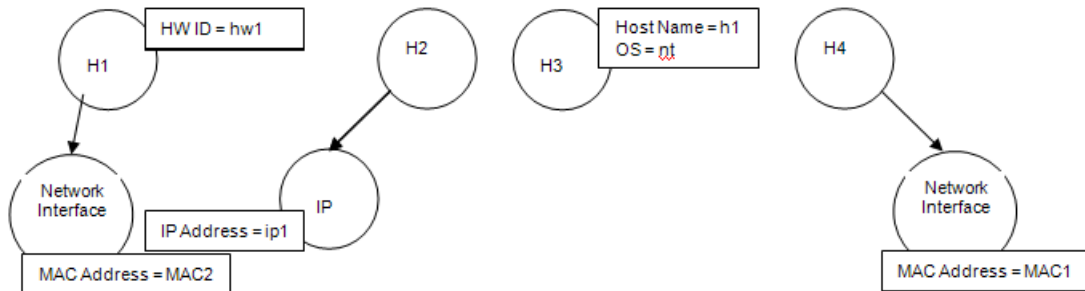
- 3 If the CIs are not merged, the Data In service decides to ignore the input CI. This occurs when the current match criterion causes a pair to fail the match criteria checking, and as a result the service does not merge the CIs.

Multiple Matching Examples

- Multiple matching by different identification criteria without conflicts
 - Input bulk data

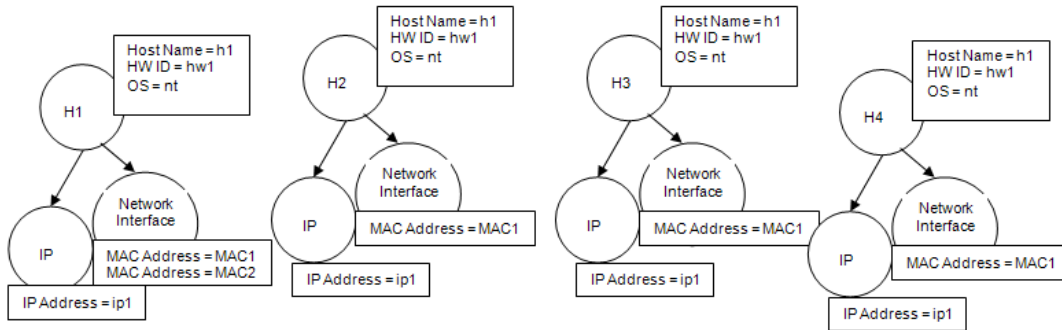


- Identified data in the ODB



In this example, the input host matches four hosts in the ODB having different identification criteria, and there are no conflicts with any of the ODB matched hosts. The process is as follows:

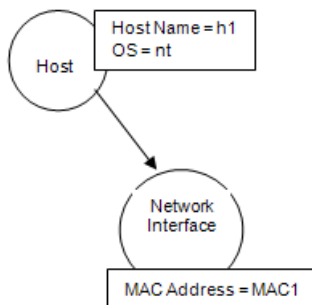
- Merge the input CI with each matched CI in the ODB.



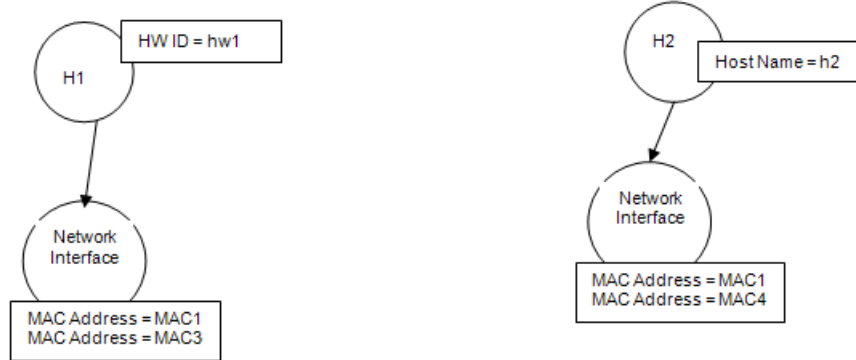
- Check for conflicts between the resulting merged CIs. In this example, there is no conflict between the merged CIs. Hosts H2, H3, and H4 are the same CI; therefore, it is obvious that there is no conflict between them. The only difference between hosts H1 and H2 is the additional MAC address in H1. Since the MAC address match validation criterion uses the **contains** operator, there is no conflict between hosts H1 and H2 either.

The decision here is to merge all CIs into one.

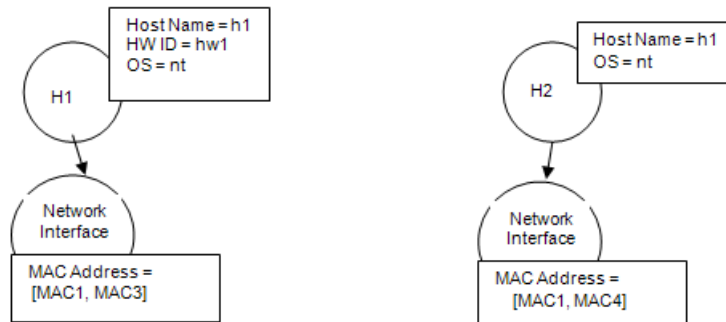
- Multiple matching by different identification criteria with conflicts
 - Input bulk data



► Identified data in the ODB



► Merge the input CI with each matched CI in the ODB.



In this example, the input host matches two hosts in the ODB having different identification criteria, and there are conflicts with the ODB matched hosts.

- Merge the input CI with each matched CI in the ODB.
- Check the conflicts between the resulting merged CIs. In this example, hosts H1 and H2 have conflicting MAC address match criteria.

The decision is to not merge all CIs to one.

The decision of whether to ignore data or pass it on for manual reconciliation depends on the flag setting for the MAC address match criterion.

Merge Service

The merge service is responsible for merging two or more CIs into one CI. This service is being used by the Data In service and the Federation service.

Tasks

Add an Identification Rule to an Existing CIT

- 1 Assign the CIT qualifier `RANDOM_GENERATED_ID` and make sure there are no key attributes in the CIT. For details, see "Qualifiers Page" in the *Modeling Guide*.
- 2 Create an XML reconciliation file that contains identification rules. For details, see "Create an identification rule document" on page 354.
- 3 Create a package that contains the XML identification file. The XML file should be located in a folder called **identification** at the root level in the package. For details, see "Create a Custom Package" in the *ODB Administration Guide*.
- 4 Deploy the package. For details, see "Deploy a Package" in the *ODB Administration Guide*.

Add Reconciliation Priorities to an Existing CIT

- 1 Create an XML reconciliation file that contains reconciliation priorities. For details, see "Create a reconciliation priority document" on page 356.
- 2 Create a package that contains the XML priorities file. The XML file should be located in a folder called **reconciliationPriority** at the root level in the package. For details, see "Create a Custom Package" in the *ODB Administration Guide*.
- 3 Deploy the package. For details, see "Deploy a Package" in the *ODB Administration Guide*.

Create XML Reconciliation Files

This task describes how to prepare the XML schema for a reconciliation information file. For details about the schema elements and attributes, see "Identification Rule Schema" on page 358 and "Reconciliation Priority Schema" on page 366.

This task assumes that the user has some basic knowledge of XML and XML schema. The schema permits XML document with different root elements; however, this task describes two recommended types of files: the identification rule document and reconciliation priority document.

This task includes the following steps:

- ▶ "Create an identification rule document" on page 354
- ▶ "Create a reconciliation priority document" on page 356

1 Create an identification rule document

The identification rule document is an XML file that describes the required reconciliation data for a specific CI type. This identification rule is applied to the CI type and each of its descendants, unless one of them has a identification rule of its own.

You can create an identification rule document from a blank document or use existing information as a basis. To do this:

- a** Navigate to **Admin > ODB Administration > Modeling > CI Type Manager**.
- b** Click on the Details tab.
- c** Select the information in the Identification field.

For details, see "Identification Rule Schema" on page 358.

Example of the identification section

```

<identification-criteria>
  <identification-criterion>
    <connected-ci-condition ciType="interface" linkType="composition">
      <overlap-operator match-percent="66"/>
      <attribute-condition attributeName="mac_address"/>
    </connected-ci-condition>
  </identification-criterion>
  <identification-criterion>
    <attribute-condition attributeName="name" operator="EqualIgnoreCase"/>
  </identification-criterion>
  <identification-criterion>
    <connected-ci-condition ciType="ip_address" linkType="containment">
      <overlap-operator match-percent="66"/>
      <attribute-condition attributeName="name"/>
      <attribute-condition attributeName="routing_domain"/>
    </connected-ci-condition>
  </identification-criterion>
  <identification-criterion>
    <attribute-condition attributeName="bios_uuid"/>
  </identification-criterion>
</identification-criteria>

```

In this example:

- ▶ A 66% match of the `mac_address` attribute from the connected interfaces CI types is required.
- ▶ The name attribute is not case sensitive.
- ▶ The rule requires both the `ip_address` name and `routing_domain` to be the same.
- ▶ Only one of the identification criteri needs to be fulfilled for the reconciliation engine to find a possible match.

Example of the match section

```

<match>
  <verification-criteria>
    <verification-criterion>
      <attribute-condition attributeName="os_family"/>
    </verification-criterion>
  </verification-criteria>
  <validation-criteria>
    <validation-criterion priority="1">
      <attribute-condition attributeName="bios_uuid"/>
    </validation-criterion>
    <validation-criterion priority="2">
      <connected-ci-condition ciType="interface" linkType="composition">
        <overlap-operator match-percent="66"/>
        <attribute-condition attributeName="mac_address"/>
      </connected-ci-condition>
    </validation-criterion>
    <validation-criterion priority="3">
      <attribute-condition attributeName="name"/>
    </validation-criterion>
  </validation-criteria>
</match>

```

In this example:

- ▶ The structure of the conditions is the same as those conditions in the Identification field.
- ▶ Only one priority criterion is given in this example, but there may be many criteria with the same priority.

2 Create a reconciliation priority document

The reconciliation priorities document is an XML file that describes the priorities of integration points in the Data In flow for a specific CI type. The priority is applied to the CI type and each of its descendants, unless one of them has a priority of its own for a given integration point.

For details, see "Reconciliation Priority Schema" on page 366.

You can create a reconciliation priority document from a blank XML document.

Example

```

<reconciliation-priority-config type="node">
  <reconciliation-priority dataStoreName="CMS_Sync" priority="80"/>
  <reconciliation-priority dataStoreName="DDMI_DS" priority="70"/>
  <attributes-reconciliation-priorities>
    <attribute-reconciliation-priorities attribute-name="name">
      <reconciliation-priority dataStoreName="DDMI_DS" priority="100"/>
    </attribute-reconciliation-priorities>
    <attribute-reconciliation-priorities attribute-name="snmp_sys_name">
      <reconciliation-priority dataStoreName="CMS_Sync" priority="50"/>
    </attribute-reconciliation-priorities>
  </attributes-reconciliation-priorities>
</reconciliation-priority-config>

```

In this example:

- ▶ The document handles only two data repositories: CMS_Sync and DDMI_DS. There may be other data repositories that already exist in the ODB or that will be created afterwards. This means that even though we could have given a data repository the highest priority (100) and the other the lowest priority (1), it is unwise to do so, since this leaves no room to integrate future or existing data repositories to the priority system.
- ▶ We first defined a priority value for all attributes for “node”. This is optional, and if omitted defaults to 100.
- ▶ For specific attributes we changed one of the data repositories. The other has the same value as the one defined at the top of the document.

Reference

 **Identification Rule Schema**

Element		Attributes
Name and Path	Description	
identification-config	The parent element for the identification rule document.	Name. description Description. A textual description of the identification rule. Is required. Optional Type. String
		Name. type Description. The CI type to which the identification rule will apply. Is required. Required Type. String
identification-criteria (Identification-config)	The parent element for all the possible identification criteria for the CI type. For details, see "Identification Criteria" on page 343. The identification criteria may contain many identification-criterion elements. Can appear at most once.	

Element		Attributes
Name and Path	Description	
match (Identification-config)	The parent element for all the possible match criteria for the CI type. For details, see "Match Criteria" on page 343. Can appear at most once.	
multiple-match-resolving (Identification-config)	When two or more CIs of the CI type are identified to one another, they may be of any descendant CI type as well. This element states that one of the descendant CI types is preferred over the others. Can appear at most once.	<p>Name. preferred-type</p> <p>Description. This value must have the value cluster_resource_group, which is a child CI type of node. Therefore, the element may only appear on a rule for the CI type node.</p> <p>Is required. Required</p> <p>Type. String</p>
identification-criterion (Identification-config identification-criteria)	This element defines a single identification criterion. The criterion may contain many conditions for identification, and for the criterion to return True , all of them must return True .	<p>Name. targetType</p> <p>Description. Indicates for which CI type this criterion is valid. If this attribute is omitted, then the criterion is applied to any derived type.</p> <p>Is required. Optional</p> <p>Type. String</p> <hr/> <p>Name. isTargetTypeDerived</p> <p>Description. Specifies whether the target type is a derived type of the current CI type.</p> <p>Is required. Optional</p> <p>Type. String</p>

Element		Attributes
Name and Path	Description	
key-attributes-condition (identification-config identification-criteria identification-criterion)	This special condition states that the CI type is identified by its key properties and CI type name, and not by any identification criteria. If this condition exists, it should be the only one in the criterion, as well the only criterion in the identification section. Can appear at most once.	

Element		Attributes
Name and Path	Description	
attribute-condition (identification-config)	Defines a condition based on an attribute.	Name. attributeName Description. The name of the attribute. Is required. Required Type. String
identification-criteria identification-criterion -OR- identification-config		Name. masterValue Description. For the purpose of fulfilling the condition, the value defined here is considered equal to any other value. Is required. Optional Type. String
identification-criteria identification-criterion connected-ci-condition -OR- identification-config		Name. operator Description. Specifies whether the equality of attribute values should be case sensitive or not. The default is case sensitive. Is required. Optional Type. One of the values: Equals or EqualsIgnoreCase
match		
validation-criteria)		Name. includeNullValue Description. Specifies whether a CI should still be considered as a valid value if it has a null (empty) value in the attribute, and the condition will process normally; or is the condition ignored and the reconciliation engine moves to the next criterion. Default value is False. Is required. Optional Type. Boolean

Element		Attributes
Name and Path	Description	
connected-ci-condition (Identification-config identification-criteria identification-criterion -OR- identification-config match verification-criteria -OR- identification-config match)	Defines a condition based on connected CIs. The connected condition may contain attribute conditions. If no attribute conditions exist, the condition matches the connected CI type using its own identification rule.	Name. ciType Description. The type of CI that is assumed to be connected to the CI type to which this rule belongs using the linkType attribute. Is required. Required Type. String
		Name. linkType Description. The type of link that the ciType attribute uses to connect to the CI type to which this rule belongs Is required. Required Type. String
		Name. isDirectionForward Description. The direction of the link. Default value is True (from the rule's CI type to ciType). Is required. Optional Type. Boolean
overlap-fixed-operator (Identification-config identification-criteria identification-criterion connected-ci-condition)	Defines the fixed number of matches to connected CIs that are needed to fulfill the condition for the connected-ci-condition element to return True . Either this or overlap-operator must exist.	Name. number-of-matches Description. The number of matches. Is required. Required Type. Integer

Element		Attributes
Name and Path	Description	
overlap-operator (Identification-config identification-criteria identification-criterion connected-ci-condition)	Defines the percent of connected CIs (from the total input number of connected CIs) that are needed to fulfill the condition for the connected-ci-condition element to return True . Either this or overlap-fixed-operator must exist.	Name. match-percent Description. The percent of matches. Is required. Required Type. Integer between 1 and 100
verification-criteria (Identification-config match)	The parent element for all the possible verification criteria for the CI type. For details, see "Match Criteria" on page 343. The verification criteria must contain at least one verification-criterion element. Can appear at most once.	

Element		Attributes
Name and Path	Description	
verification-criterion (Identification-config match verification-criteria)	This element defines a single verification criterion. The criterion may contain many conditions for verification.	Name. targetType Description. The derived CI type for which this criterion is valid. If this attribute is omitted, then the criterion is applied to any derived type. Is required. Optional Type. String
		Name. isTargetTypeDerived Description. Specifies whether the target type is a derived type of the current CI type. Is required. Optional Type. Boolean
		Name. numberOfConflictsToFailIdentification Description. The number of conflicting conditions that will cause the current criterion to fail. Default Value: 1. Is required. Optional Type. Integer
validation-criteria (Identification-config match)	The parent element for all possible validation criteria for the CI type. For details, see "Match Criteria" on page 343. The validation criteria must contain at least one validation-criterion element. Can appear at most once.	

Element		Attributes
Name and Path	Description	
validation-criterion (Identification-config match validation-criteria)	This element defines a single validation criterion. The criterion may contain many conditions for validation.	<p>Name. priority</p> <p>Description. The criterion's priority.</p> <p>Is required. Required</p> <p>Type. Integer</p>
		<p>Name. targetType</p> <p>Description. The derived CI type for which this criterion is valid. If this attribute is omitted, then the criterion is applied to any derived type.</p> <p>Is required. Optional</p> <p>Type. String</p>
		<p>Name. isTargetTypeDerived</p> <p>Description. Specifies whether the target type is a derived type of the current CI type.</p> <p>Is required. Optional</p> <p>Type. Boolean</p>
		<p>Name. numberOfConflictsToFailIdentification</p> <p>Description. The number of conflicting conditions that will cause the current criterion to fail. Default Value: 1.</p> <p>Is required. Optional</p> <p>Type. Integer</p>

 **Reconciliation Priority Schema**

Element		Attributes
Name and Path	Description	
reconciliation-priority-config	The parent element of a reconciliation priority section for a specific CI type.	<p>Name. type</p> <p>Description. The CI type to which the reconciliation priorities will apply.</p> <p>Is required. Required</p> <p>Type. String</p>
reconciliation-priority (reconciliation-priority-config -OR- reconciliation-priority-config attributes-reconciliation-priorities)	When this appears under the reconciliation-priority-config element, it defines priorities for all attributes in an integration point. When it appears under the attribute-reconciliation-priorities element, it defines a priority for a specific attribute. Must appear at least once when it is the child of the attributes-reconciliation-priorities element.	<p>Name. dataStoreName</p> <p>Description. The name of the integration point.</p> <p>Is required. Required</p> <p>Type. String</p> <hr/> <p>Name. priority</p> <p>Description. The priority of the dataStoreName attribute.</p> <p>Is required. Required</p> <p>Type. String</p>

Element		Attributes
Name and Path	Description	
attributes-reconciliation-priorities (reconciliation-priority-config)	The parent element for the section of the document that defines priorities for specific attributes. Can appear at most once.	
attribute-reconciliation-priorities reconciliation-priority-config attributes-reconciliation-priorities)	Defines the priorities of integration points for specific attributes of the current CI type.	<p>Name. attribute-name</p> <p>Description. The name of the attribute for which to define priorities.</p> <p>Is required. Required</p> <p>Type. String</p>

Part VI

Hardening

11

Hardening Data Flow Management

This chapter includes:

Concepts

- ▶ Hardening Data Flow Management Overview on page 372
- ▶ Credentials Encryption With Confidential Manager on page 374

Tasks

- ▶ Manage the Storage of Credentials on page 376
- ▶ Generate or Update the Encryption Key on page 377
- ▶ Export and Import the domainScopeDocument (DSD) File in Encrypted Format on page 383

Concepts

Hardening Data Flow Management Overview

Discovery credentials entered in the Data Flow Probe Setup window are saved in the ODB database, and managed by the Confidential Manager. On the Probe side, the credentials are saved in an encrypted file termed a domain scope document (DSD). This DSD contains discovery domain data. Each discovery domain entry in the document contains the network scope for the domain's Probes and the credentials the Probes may use when communicating with remote machines.

Note: Security features related to Business Service Management user management—for example, authentication and authorization—are not discussed here.

This section includes the following topics:

- “Basic Security Assumptions” on page 372
- “Credentials Encryption Management” on page 373
- “HTTPS\SSL Configuration” on page 374

Basic Security Assumptions

Note the following security assumptions:

- You have secured the Business Service Management Gateway Server and Probe file systems for authorized access only.
- You have secured the Gateway Server JMX console to enable access to BSM system administrators only, preferably through `localhost` access only.

Credentials Encryption Management

Note the following guidelines for managing credential encryption:

- ▶ The **domainScopeDocument** (DSD) file is encrypted using standard, symmetric encryption. The DSD file is encrypted during transfer and at its location (the key is stored on the server database and the Probe file system). The encryption uses an AES algorithm with a default key of 192 bytes (but you can decide the length of the encryption/decryption key and other security parameters). For details on changing the key size, see “Update an Encryption Key” on page 380.
- ▶ A default, symmetric key is distributed with the BSM installation. As all default keys are identical, you should replace this key with a locally-generated key.
- ▶ The DSD file is exportable and importable in encrypted file form. To import a file you should supply the matching key used for the encryption of the file. Perform the import and export operations through the server’s JMX console (the Discovery Manager service). For details, see “Export and Import the domainScopeDocument (DSD) File in Encrypted Format” on page 383.
- ▶ You can exchange the key while the system is up to keep the consistency of the system without losing any data. This is managed through the server’s JMX console. For details, see “Generate or Update the Encryption Key” on page 377.
- ▶ When a key is updated, you can automatically distribute the new key to the Probes. This option is easier to deploy but is considered less secure. The new key is encrypted using the old key. To achieve better security, you can change the key manually. For details, see “Generate a New Encryption Key” on page 378.
- ▶ The key for DSD encryption is itself encrypted using DPAPI and is stored on the Probe and BSM server file systems (in encrypted format—and not in clear text). DPAPI relies on the Windows user password in the encryption process. Therefore, to ensure that the Probe can read the key, the Probe should always run under the same Windows user that was used during the Probe’s installation (it is possible to change the user password). (DPAPI is a standard method to protect confidential data—such as certificates and private keys—on Windows.)

HTTPS\SSL Configuration

You can configure communication between the Business Service Management Gateway Server and the Data Flow Probe to use HTTPS\SSL. This enables better DSD security during transit.

For details on the procedure to configure Business Service Management to work with SSL, see “Enable SSL Between BSM Running an Internal UCMDB and the Data Flow Probe with Mutual Authentication” in the *HP Business Service Management Hardening Guide* PDF.

Note: As a result of using SSL, other aspects (for example, discovery tasks and gathered results) of the Business Service Management product may become more secure.

Credentials Encryption With Confidential Manager

Note the following guidelines for managing credential encryption:

- ▶ The **domainScopeDocument** (DSD) file on the BSM Server contains credentials IDs only. Credentials details are stored on Confidential Manager.
- ▶ The DSD file on the Data Flow Probe contains full credentials information. This copy is encrypted using standard symmetric encryption.

When the BSM Server updates the Probe with a new copy of the DSD, the following process occurs:

- 1 A new copy of DSD is created. This copy contains full credentials information that has been loaded from Confidential Manager.
- 2 The DSD copy is encrypted using standard symmetric encryption and transferred to the Data Flow Probe.

The encryption uses an AES algorithm with a default key of 192 bytes. However, you can decide the length of the encryption and decryption keys and other security parameters. For details on changing the key size, see “Update an Encryption Key” on page 380.

- ▶ A default, symmetric key is distributed with the BSM installation. As all default keys are identical, you should replace this key with a locally generated key.
- ▶ The DSD file is exportable and importable in encrypted file format. To import a file you should supply the matching key used for the encryption of the file. Perform the import and export operations through the Server's JMX console (the Discovery Manager service). For details, see “Export and Import the domainScopeDocument (DSD) File in Encrypted Format” on page 383.

Tasks

Manage the Storage of Credentials

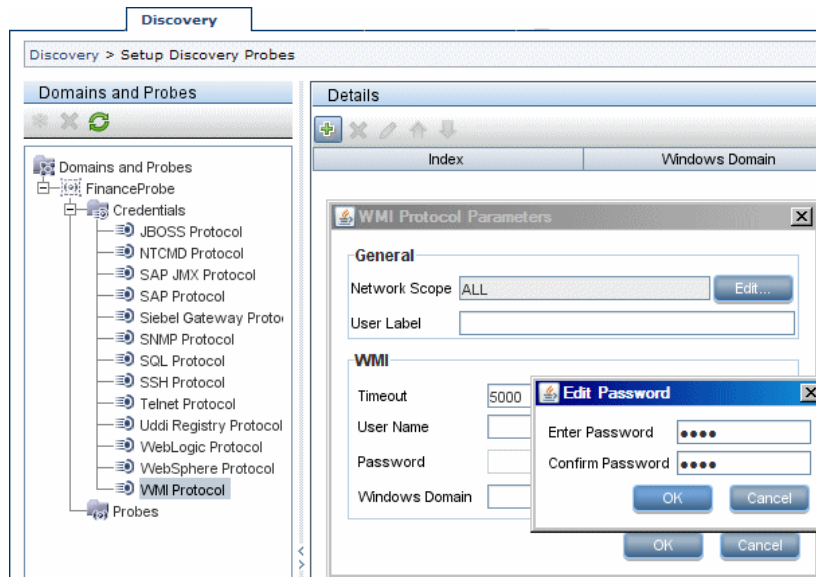
This section explains how to manage the DSD file.

This section includes the following tasks:

- ▶ “View Credentials Information (Data Direction: CMDB to Business Service Management)” on page 376
- ▶ “Update Credentials (Data Direction: Business Service Management to CMDB)” on page 377

1 View Credentials Information (Data Direction: CMDB to Business Service Management)

Passwords are not sent from the CMDB to the application. That is, Business Service Management displays asterisks (*) in the password field, regardless of content:



2 Update Credentials (Data Direction: Business Service Management to CMDB)

- The communication in this direction is not encrypted, therefore you should connect to the BSM Gateway Server using https\SSL, or ensure connection through a trusted network.

Although the communication is not encrypted, passwords are not being sent as clear text on the network. They are encrypted using a default key and, therefore, it is highly recommended to use SSL for effective confidentiality in transit.

- The password field is limited to 40 characters. The length of the password is not limited in other ways since it is saved only in a file.
- You can use special characters and non-English characters as passwords.

Generate or Update the Encryption Key

You can generate or update an encryption key for probe encryption and the transport of credentials from server to Probe. In each case DFM creates a new encryption key based on parameters that you supply (key length, extra PBE cycles, JCE provider). You can also disable DPAPI encryption.

The result of running the **generateEncryptionKey** method is a new generated encryption key. This key is stored only in the **secured_storage.bin** file and its name and details are not known. If you reinstall an existing Probe, or connect a new Probe to the BSM Server, this new generated key is not recognized by the new Probe.

In these cases, it is preferable to use the **changeEncryptionKey** method to change encryption keys. This way, when you reinstall a Probe or install a new Probe, you can import the existing key (whose name and location you know) by running the **importEncryptionKey** method on the Probe JMX console.

Note:

- ▶ The difference between the methods used to create a key (`generateEncryptionKey`) and to update a key (`changeEncryptionKey`) is that `generateEncryptionKey` creates a new, random encryption key, while `changeEncryptionKey` imports an encryption key whose name you provide.
 - ▶ Only one encryption key can exist on a system, no matter how many Probes are installed.
-

This section includes the following tasks:

- ▶ “Generate a New Encryption Key” on page 378
- ▶ “Update an Encryption Key” on page 380
- ▶ “Retrieve Encryption Key File Name” on page 381
- ▶ “Disable DPAPI Encryption” on page 381
- ▶ “Manually Change the Encryption Key When Probe Manager and Probe Gateway Installed on Separate Machines” on page 382
- ▶ “Define Several JCE Providers for the Server” on page 382

Generate a New Encryption Key

You can generate a new key to be used by the BSM Server and Data Flow Probe for encryption/decryption. DFM replaces the old key with the new generated key, and distributes this key among the Probes.

To generate a new encryption key through the JMX Console:

- 1** Launch the Web browser and enter the server address, as follows:
`http://<BSM Server Host Name or IP>:21212/jmx-console.`

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

- 2** Under UCMDB, click **UCMDB:service=Discovery Manager** to open the JMX MBEAN View page.

3 Locate the **generateEncryptionKey** operation.

- In the **customerId** parameter box, enter **1** (the default).
- **keySize**. The length of the encryption key (the length can be 128, 192, or 256).
- **usePBE**. **True**: use additional PBE hash cycles. **False**: do not use additional PBE hash cycles.
- **jceVendor**. You can choose to use a non-default JCE provider. If the box is empty, the default provider is used.
- **autoUpdateProbe**. **True**: The server distributes the new key to the Probes automatically. **False**: The new key should be placed on the Probes manually.
- **exportEncryptionKey**. **True**: In addition to creating the new password and storing it in secured storage, the Server exports the new password to the file system (**C:\HPBSM\obd\conf\discovery\key.bin**). This option enables you to update Probes manually with the new password. **False**: The new password is not exported to the file system.

To update Probes manually, set **autoUpdateProbe** to **False** and **exportEncryptionKey** to **True**.

Important:

Make sure that the Probe is up and connected to the server. If the Probe goes down, the key cannot reach the Probe.

If you have changed the key before the Probe goes down, once the Probe is up again, the key is sent again to the Probe. However, if you have changed the key more than once before the Probe goes down, you must change the key manually through the JMX console. (Select **False**).

4 Click **Invoke** to generate the encryption key.

Update an Encryption Key

You use the `changeEncryptionKey` method to import an encryption key.

To update an encryption key through the JMX Console:

- 1 Launch the Web browser and enter the server address, as follows:
http://<BSM Server Host Name or IP>:21212/jmx-console.

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

- 2 Under UCMDB, click **UCMDB:service=Discovery Manager** to open the JMX MBEAN View page.
- 3 Locate the `changeEncryptionKey()` operation.
 - ▶ In the **customerId** parameter box, enter **1** (the default).
 - ▶ **newKeyFileName**. Enter the name of the new key.
 - ▶ **keySizeInBits**. The length of the encryption key (the length can be 128, 192, or 256).
 - ▶ **usePBE**. **true**: use additional PBE hash cycles. **false**: do not use additional PBE hash cycles.
 - ▶ **jceVendor**. You can choose to use a non-default JCE provider. If the box is empty, the default provider is used.
 - ▶ **autoUpdateProbe**. Leave as **True** for the server to automatically distribute the changed key to the Probes.

Select **False** to distribute the changed key manually using the Probe JMX console.

Important:

Make sure that the Probe is up and connected to the server. If the Probe goes down, the key cannot reach the Probe.

If you have changed the key before the Probe goes down, once the Probe is up again, the key is sent again to the Probe. However, if you have changed the key more than once before the Probe goes down, you must change the key manually through the JMX console. (Select **False**).

- 4 Click **Invoke** to generate and update the encryption key.

Retrieve Encryption Key File Name

When you change an encryption key on the server (by using the **changeEncryptionKey** method), you may not want the new key to be downloaded automatically to the Probes because of security concerns. You can download the encryption key file to a Probe manually.

To prevent automatic download, run the `importEncryptionKey` method:

- 1 Place the encryption key file in the
C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\binaryData
 directory.
- 2 Launch the Web browser and enter the Probe address, as follows:
http://localhost.<domain_name>:1977/.
 You may have to log in with a user name and password.
- 3 Under the Probe domain, click **type=MainProbe** to open the MBean View page.
- 4 Locate the **importEncryptionKey** method.
- 5 Enter the name of the encryption key file that resides in the
C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\binaryData
 directory.
 This file contains the key to be imported.
- 6 Click the **importEncryptionKey** button.

Disable DPAPI Encryption

The key is encrypted with DPAPI on the file system. You can disable this encryption.

To disable encryption with DPAPI:

- 1 Launch the Web browser and enter the server address, as follows:
http://<BSM Server Host Name or IP>:21212/jmx-console.
 You may have to log in with a user name and password.

- 2 Under UCMDB, click **UCMDB:service=Discovery Manager** to open the JMX MBEAN View page.
- 3 Locate the **setDPApiUsage()** operation and enter the following properties:
 - In the **customerId** parameter box, enter **1** (the default).
 - **useDPAPI**. **true**: use DPAPI. **false**: do not use DPAPI.
- 4 Click **Invoke** to disable the DPAPI encryption.

Manually Change the Encryption Key When Probe Manager and Probe Gateway Installed on Separate Machines

- 1 On the Probe Manager machine, start the Probe Gateway service: **Start > Programs > HP UCMDB > Probe Gateway**.
- 2 Import the key from the server, using the Probe Gateway JMX. For details, see “Generate a New Encryption Key” on page 378.
- 3 After the encryption key is imported successfully, stop the Probe Gateway service.

Define Several JCE Providers for the Server

When generating an encryption key through the JMX Console, you can define several JCE providers with the **changeEncryptionKey** and **generateEncryptionKey** methods.

To change the default JCE provider:

- 1 Register the JCE provider jar files at the **\$JRE_HOME/lib/ext** directory.
- 2 Copy the jar files to the **\$JRE_HOME** directory:
 - For the **BSM Server**: **\$JRE_HOME** resides at:
 - **C:\HPBSM\odb\deploy\ucmdb-ui\static\JRE**
 - For the **Data Flow Probe**: **\$JRE_HOME** resides at:
 - **C:\hp\UCMDB\DataFlowProbe\bin\jre**
- 3 Add the provider class at the end of the provider list in the **\$JRE_HOME\lib\security\java.security** file.

- 4 Update the **local_policy.jar** and **US_export_policy.jar** files to include unlimited JCE policies. You can download these jar files from the Sun site.
- 5 Restart the BSM Server and the Data Flow Probe.
- 6 Locate the JCE vendor field for the **changeEncryptionKey** or **generateEncryptionKey** method, and add the name of the JCE provider.

Export and Import the domainScopeDocument (DSD) File in Encrypted Format

You can export and import DSD files in encrypted format. (You would probably import a DSD file during recovery following a system crash or during upgrade.)

- ▶ **When exporting the DSD file**, you must enter a password (of your choosing). The file is encrypted with this password. The encryption key used for storing the DSD file in the ODB database is no longer used.
- ▶ **When importing the DSD file**, you must use the same password that was defined when the DSD file was exported.

Important: If you exported the domainScopeDocument file from BSM version 8.02, to import the file to your present version, copy the password from the contents of the key.bin file located on the version 8.02 system.

To export or import a DSD file:

- 1 Launch the Web browser and enter the server address, as follows:
http://<BSM Server Host Name or IP>:21212/jmx-console.
You may have to log in with a user name and password.
- 2 Under UCMDB, click **UCMDB:service=Discovery Manager** to open the JMX MBEAN View page.
- 3 Locate the **ExportDomainScopeDocument** or **importDomainScopeDocument** operation and enter the existing file name and password.

- 4 Click **Invoke** to export or import the domainScopeDocument file.

The location of the saved domainScopeDocument file is the

C:\HPBSM\odb\conf\server\discovery\<customer_dir> directory.

12

Hardening the Data Flow Probe

This chapter includes:

Tasks

- ▶ Set the MySQL Database Encrypted Password on page 386
- ▶ Set the JMX Console Encrypted Password on page 388
- ▶ Enable SSL Between BSM Server and Data Flow Probe with Mutual Authentication on page 389
- ▶ Enable SSL on the Data Flow Probe with Basic Authentication on page 390
- ▶ Connect the Data Flow Probe by Reverse Proxy on page 390
- ▶ Control the Location of the domainScopeDocument File on page 392

Tasks

Set the MySQL Database Encrypted Password

This section explains how to encrypt the password for the MySQL database user.

1 Create the Encrypted Form of a Password (AES, 192-bit key)

- a Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

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

Note: If you have not created a user, use the default user name **admin** and the password **admin** to log in.

- b Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View page.
- c Locate the **getEncryptedDBPassword** operation.
- d In the **DB Password** field, enter the password to be encrypted.
- e Invoke the operation by clicking the **getEncryptedDBPassword** button.

The result of the invocation is an encrypted password string, for example:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```

2 Stop the Data Flow Probe

Start > Programs > HP UCMDB > Stop Data Flow Probe

3 Run the `set_dbuser_password.cmd` Script

This script is located in the following folder:

C:\hp\UCMDB\DataFlowProbe\tools\dbscripts
 \set_dbuser_password.cmd

Run the `set_dbuser_password.cmd` script with the new password as an argument, for example, `set_dbuser_password <my_password>`.

The password must be entered in its unencrypted form (as plain text).

4 Update the Password in the Data Flow Probe Configuration Files

- a The password must reside encrypted in the configuration files. To retrieve the password's encrypted form, use the `getEncryptedDBPassword` JMX method, as explained in page 386.
- b Add the encrypted password to the following properties in the `C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties` file.
 - `appilog.agent.probe.jdbc.pwd`

For example:

```
appilog.agent.probe.jdbc.user = mamprobe
appilog.agent.probe.jdbc.pwd =
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,6
1,61
```

- `appilog.agent.local.jdbc.pwd`

5 Start the Data Flow Probe

Start > Programs > HP UCMDB > Start Data Flow Probe

The `clearProbeData.bat` Script: Usage

The `clearProbeData.bat` script recreates the database user with a password that is provided as an argument to the script.

After you set a password, each time you execute the **clearProbeData.bat** script, it retrieves the database password as an argument.

After running the script:

- ▶ Review the following file for errors:
C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log
- ▶ Delete the following file, as it contains the database password:
C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log

Set the JMX Console Encrypted Password

This section explains how to encrypt the password for the JMX user. The encrypted password is stored in the `DiscoveryProbe.properties` file. Users must log in to access the JMX console.

1 Create the Encrypted Form of a Password (AES, 192-bit key)

- a** Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

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

Note: If you have not created a user, use the default user name **admin** and the password **admin** to log in.

- b** Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View page.
- c** Locate the **getEncryptedKeyPassword** operation.
- d** In the **Key Password** field, enter the password to be encrypted.
- e** Invoke the operation by clicking the **getEncryptedKeyPassword** button.

The result of the invocation is an encrypted password string, for example:

```
85,-9,-61,11,105,-93,-81,118
```

2 Stop the Data Flow Probe

3 Add the Encrypted Password

Add the encrypted password to the following property in the `C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties` file.

`appilog.agent.Probe.JMX.BasicAuth.Pwd`

For example:

```
appilog.agent.Probe.JMX.BasicAuth.User=admin
appilog.agent.Probe.JMX.BasicAuth.Pwd=-85,-9,-61,11,105,-93,-81,118
```

Note: To disable authentication, leaves these fields empty. If you do so, users can open the main page of the Probe's JMX console without entering authentication.

4 Start the Data Flow Probe

Test the result in a Web browser.

Enable SSL Between BSM Server and Data Flow Probe with Mutual Authentication

Note: In version 9.01, this functionality is not supported. Instead, you should use basic authentication. For details, see “Enable SSL on the Data Flow Probe with Basic Authentication” on page 390.

Enable SSL on the Data Flow Probe with Basic Authentication

To set basic authentication:

- 1 Locate the following file: `C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties`.
- 2 Remove the comment markers (#) from the following properties, and enter the relevant credentials:

```
appilog.agent.Probe.BasicAuth.Realm=  
appilog.agent.Probe.BasicAuth.User=  
appilog.agent.Probe.BasicAuth.Pwd=
```

The credentials should match those defined on the BSM server.

Connect the Data Flow Probe by Reverse Proxy

Perform the following procedure to connect the Data Flow Probe by reverse proxy.

Note: Enabling mutual authentication when using SSL between the BSM Server and the Data Flow Probe is not supported when the connection is made by reverse proxy.

To configure the Data Flow Probe to work against a reverse proxy:

- 1 Edit the `discoveryProbe.properties` file (located in `C:\hp\UCMDB\DataFlowProbe\conf`).
- 2 Set the `serverName` property to the reverse proxy server's IP or DNS name.
- 3 Save the file.

The following proxy server configuration is required if Data Flow Probes only are connected via a reverse proxy to Business Service Management:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam-collectors	http://[Business Service Management server]/mam-collectors

The following configuration is required if a SOAP adapter is used for replication via a reverse proxy to a secure (hardened) Business Service Management:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/axis2	http://[Business Service Management server]/axis2

Connecting the Data Flow Probe and Web Clients by Reverse Proxy

The following configuration is required if both Data Flow Probes and application users are connected via a reverse proxy to Business Service Management:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam	[Business Service Management server]/mam
/mam_images	[Business Service Management server]/mam_images
/mam-collectors	[Business Service Management server]/mam-collectors
/ucmdb	[Business Service Management server]/ucmdb
/site	[Business Service Management server]/site

Control the Location of the domainScopeDocument File

The Probe's file system holds (by default) both the encryption key and the domainScopeDocument file. Each time the Probe is started, the Probe retrieves the domainScopeDocument file from the server and stores it on its file system. To prevent unauthorized users from obtaining these credentials, you can configure the Probe so that the domainScopeDocument file is held in the Probe's memory and is not stored on the Probe file system.

To control the location of the domainScopeDocument file:

- 1** Open `C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties` and change:

```
appilog.collectors.storeDomainScopeDocument=true
```

to:

```
appilog.collectors.storeDomainScopeDocument=false
```

The Probe Gateway and Probe Manager `serverData` folders no longer contain the domainScopeDocument file.

For details on using the domainScopeDocument file to harden DFM, see “Manage the Storage of Credentials” on page 376.

- 2** Restart the Probe.

13

Using SSL with the Data Flow Probe

This chapter includes:

Concepts

- ▶ Using SSL with the Data Flow Probe Overview on page 394

Tasks

- ▶ Enable SSL Between BSM Running an Internal UCMDB and the Data Flow Probe with Mutual Authentication on page 395
- ▶ Configure SSL from the Data Flow Probe to the Gateway Server on page 395

Concepts

Using SSL with the Data Flow Probe Overview

This section describes how to configure your HP Business Service Management platform with the Data Flow Probe and Staging Data Replicator to support communication using the Secure Sockets Layer (SSL) channel.

For introductory and general information on configuring HP Business Service Management and its data collectors to support SSL, see "Introduction to Hardening the BSM Platform" in the *HP Business Service Management Hardening Guide* PDF.

Tasks

Enable SSL Between BSM Running an Internal UCMDB and the Data Flow Probe with Mutual Authentication

Note: In version 9.01, this functionality is not supported. Instead, you should use basic authentication. For details, see "Enable SSL on the Data Flow Probe with Basic Authentication" on page 390.

Configure SSL from the Data Flow Probe to the Gateway Server

When a session is started between the Data Flow Probe and the Gateway Server, the Gateway Server sends the Probe a server-side certificate that was issued by a Certification Authority (CA) recognized by the Gateway Server. The Data Flow Probe engine should be configured to trust the certificate or the CA that issued it, and to communicate via SSL.

To configure the Data Flow Probe to connect to the Gateway Server using SSL:

- 1** Prerequisite: Configure HP Business Service Management to use SSL.
- 2** Prerequisite: Install the Data Flow Probe. During installation, enter the name of the HP Business Service Management Gateway server to which the Probe must report results.
- 3** If you are working with the Certificate Authority, download the current Certificate Authority certificate to your Data Flow Probe server. Save it to a file, for example, C:\ca.cer.
- 4** Import this certificate into the Data Flow Probe JVM:
C:\hp\UCMDB\DataFlowProbe\jre\bin with the following values:

```
keytool -import -trustcacerts -alias <your alias> -keystore ../lib/security/cacerts  
-file <file path and name>
```

- 5 Enter the password and click **Yes** to confirm.
- 6 Set the connection parameters in the Data Flow Probe.
 - Open the file `%discovery root%\root\lib\collectors\DiscoveryProbe.properties`.
 - Configure the URL of the HP Business Service Management server:

```
serverName = <HP Business Service Management Gateway server domain name>
```

Note: The SSL connection may fail if an IP address is used instead of domain name.

- Configure the port number to use for HTTPS:

```
# Ports used for HTTP/s traffic  
#serverPort = 80  
serverPortHttps = 443
```

- Set the schema to be used by the Agent to HTTPS:

```
# Can be either HTTP or HTTPS  
appilog.agent.probe.protocol = HTTPS
```

- Set the name of the HP Business Service Management server:

```
# Name of the Server machine to which this probe reports  
serverName = <server name either of the reverse proxy or the Gateway server>
```

- 7 Restart the Data Flow Probe.

Index

A

- activateJob
 - JMX operations 252
- activateJobOnDestination
 - JMX operations 252
- Adapter Definition tab 143
- Adapter Management 23, 123
 - tab 150
 - user interface 141
 - window 157
- Adapter Parameters pane 149
- Adapter Source Editor window 158
- adapters 26
 - managing 123
 - managing configuration 135
- Add IP Range dialog box 69
- Add New Probe dialog box 72, 73
- Add Policy dialog box 71
- Advanced Edition Licensing 34
- Advanced Mode window
 - Discovery Control Panel 268
- agentless discovery 29
- applicationSignature.xml 130
- Attribute Assignment Editor dialog box 159
- attributes
 - retrieving from external data source 192
- automatic deletion 124

B

- basic authentication
 - enabling on ODB Data Flow Probe 390
- Basic Mode window
 - Discovery Control Panel 269

C

- candidates for deletion 124
- Choose CIs to Add dialog box 271
- Choose Discovered Class dialog box 161
- Choose Discovery Jobs dialog box 74
- Choose Discovery TQL dialog box 273
- Choose Probe to Filter dialog box 273
- CIs
 - and relationships, handling deleted 124
 - automatic deletion 124, 129
 - candidates for deletion 124
 - view current status of discovered 115
- Confidential Manager
 - credentials encryption 374
- Configuration File pane 163
- configuration files 141
 - discovery 130
- Configuration Item Properties dialog box 273
- cpVersion
 - use attribute to verify content update 135
- Create New Discovery Job window 274
- Create New Job Definition dialog box 202
- credentials
 - managing hardening 376
 - protocols 83
- Custom JDBC Drivers page
 - Database wizard 278
- customer ID
 - configure per Probe 53

D

- Data Flow Management
 - architecture 24

Index

- components 25
- hardening 371
- introduction 19
- job overview 28
- module overview 27
- wizards 28
- Data Flow Probe 25
 - automatic CIs deletion 129
 - configuring SSL support for 395
 - connect by reverse proxy to BSM server 390
 - connect to a non-default customer 53
 - data validation 62
 - delete results that have not yet been transmitted 67
 - Details pane 76
 - enabling SSL with basic authentication 390
 - enabling SSL with mutual authentication 389, 395
 - getting started 64
 - hardening 385
 - hardware requirements 54
 - installation requirements 54
 - installation, configuring Probe Manager and Probe Gateway as separate processes 52
 - launching as a service 65
 - launching from the Start menu 64
 - logs 106
 - selecting 83
 - set up 22
 - setting up 59
 - software requirements 54
 - using with SSL 393
 - viewing job information 251
 - virtual environment requirements 55
- Data Flow Probe Setup user interface 68
- Data Flow Probe Setup window 74
- Data Flow Probe Status 23, 113
 - (Job name) dialog box 116
 - user interface 116
 - window 118
- Data Flow Probes pane 77
- data push jobs 197
- Data Push tab 204
- data sources
 - retrieving data from multiple 192
- Database Port Scanning page
 - Database wizard 277
- Database wizard 275
 - Custom JDBC Drivers page 278
 - Database Port Scanning page 277
 - Define Credentials page 276
 - Oracle TNSName File Location page 279
 - Schedule Discovery page 280
 - Summary page 281
- DDM Community 23
- Define Credentials page
 - Database wizard 276
 - Infrastructure wizard 308
 - J2EE wizard 314
- Define IP Ranges page
 - Infrastructure wizard 306
- Dependency Map tab 282
- deployment
 - installation 39
- Description pane 76
- Details pane 76
- Details tab 75, 284
- Discovered CIs dialog box 295
- Discovered CITs pane 148
- discovery
 - running software 126
- Discovery Control Panel 22, 239
 - Advanced Mode window 268
 - advanced mode workflow 247
 - Basic Mode window 269
 - basic mode workflow 246
 - overview 240
 - user interface 267
 - view permissions 242
- Discovery Modules pane 296
- Discovery Permissions window 299
- Discovery Scheduler dialog box 301
- Discovery Status pane
 - problem management 243
- DiscoveryProbe.properties file 110
- documentation updates 16
- domain credentials 83
- Domains and Probes pane 79

- domainScopeDocument
 - controlling location of 392
 - export, import in encrypted format 383

E

- Edit IP Range dialog box 69
- Edit Policy dialog box 71
- Edit Probe Limitations for TQL Output dialog box 304
- Edit Process dialog box 164
- Edit Related Probes dialog box 81
- Edit Time Template dialog box 304
- Edit Timetable dialog box 81
- encryption keys
 - generating or updating 377
- errors
 - finding in messages 265
 - managing 263
- Execution Options pane 152

F

- federated data
 - working with 194
- federation
 - with multiple version 9.01 ODBs 224
- Federation tab 204
- Find Jobs dialog box 165, 305
- Find Resource dialog box 165
- Find Text dialog box 166

G

- Global Configuration Files pane 148
- global ID 219
- globalFiltering.xml 139

H

- hardening
 - enabling SSL on ODB Data Flow Probe 389, 390, 395
 - export, import
 - domainScopeDocument in encrypted format 383

- manage credentials storage 376
- HP Software Support Web site 15
- HP Software Web site 16

I

- identification criteria for reconciliation 342
- identifying processes 127
- Infrastructure wizard 306
 - Define Credentials page 308
 - Define IP Ranges page 306
 - Preferences page 309
 - Schedule Discovery page 313
 - Summary page 313
- Input pane 143
- input queries 26
- Input Query Editor window 167
- installation
 - on one machine 40
 - procedure 39
- integration
 - setting up between multiple version 8.0x ODBs 232
 - setting up between multiple version 9.0x ODBs 229, 230
- Integration Points pane 206
- Integration Studio 22, 190, 199
 - Data Push tab 204
 - Federation tab 204
 - Integration Points pane 206
 - Job Definition pane 209
 - Population tab 210
- Integration Studio page 208
- integrations
 - out-of-the-box 213

J

- J2EE Port Scanning page
 - J2EE wizard 316
- J2EE wizard 314
 - Define Credentials page 314
 - J2EE Port Scanning page 316
- JBoss page 321
- Oracle Application Server page 321
- Schedule Discovery page 322

Index

- Summary page 323
- WebLogic page 317
- WebSphere page 319
- JBoss
 - protocol 88
- JBoss page
 - J2EE wizard 321
- JMX console
 - set password to encrypt 388
- JMX operations
 - activateJob 252
 - activateJobOnDestination 252
 - start/stop 253
 - viewJobErrorsSummary 253
 - viewJobExecHistory 253
 - viewJobProblems 253
 - viewJobResultCiInstances 254
 - viewJobResults 254
 - viewJobsStatuses 256
 - viewJobStatus 257
 - viewJobTriggeredCIs 259
 - viewJobTriggeredCIsWithErrorId 261
- Job Definition pane 209
- Job Execution Policy pane 77
- jobs
 - execution policies 60
 - manually activating 263
 - running when job execution policy
 - running 62
 - viewing information through the JMX application 251
- K**
- keys
 - generating or updating encryption
 - key 377
- Knowledge Base 15
- L**
- LDAP
 - protocol 89
- licensing
 - Data Flow Probe installation 36
 - for HP ServiceCenter/Service Manager 35
- for HP Software-as-a-Service 35
- ODB 33
- overview 34
- troubleshooting and limitations 38
- upgrading to standard or advanced 37
- logs
 - Probe Gateway 108
 - Probe Manager 109
- LTU (license to use) 35
- M**
- managed server 34
- multiple CMDBs
 - for version 8.0 226
 - for version 9.0 220
 - integrating 218
 - use cases 219
- multiple ODBs 218
- mutual authentication
 - enabling on ODB Data Flow Probe 389, 395
- MySQL
 - set password to encrypt database 386
- N**
- naming conventions 30
- NNM protocol 89
- NTCMD protocol 90
- O**
- oidToHostClass.xml 138
- online resources 15
- Oracle Application Server page
 - J2EE wizard 321
- Oracle TNSName File Location page
 - Database wizard 279
- OS instance 34
- P**
- passwords
 - encrypt the JMX console 388
 - encrypt the MySQL database 386

- Permission Editor dialog box 173
- Permissions document 242, 244
- Permissions Objects and Parameters dialog box 174
- population jobs 195
- Population tab 210
- portNumberToPortName.xml 128
- ports
 - adding new attributes 133
 - defining 133
 - marking new entries 133
- Preferences page
 - Infrastructure wizard 309
- Probe Gateway
 - logs 108
- Probe Manager
 - logs 109
- Probe Selection pane 150
- problem management 243
- Properties tab 324
- Protocol Parameters dialog box 82
- protocols
 - definitions 25
 - domain credentials 83
 - JBoss 88
 - LDAP 89
 - NNM 89
 - NTCMD 90
 - SAP 91
 - SAP JMX 91
 - Siebel Gateway 92
 - SNMP 93
 - SQL 95
 - SSH 96
 - Telnet 99
 - UDDI registry 101
 - VMware Infrastructure 102
 - WebLogic 103
 - WebSphere 104
 - WMI 105

Q

- queries
 - building a view 249
 - defining 249

R

- Ranges pane 78
- reconciliation
 - adding priorities 353
 - configuration 341
 - conflict resolution 344
 - identification and match criteria 342
 - identification schema 358
 - overview 340
 - XML files 354
- Reconciliation Priority Manager window 211
- Related CIs window 329
- Required Discovery Protocols pane 147
- Required Permissions pane 146
- resource files 138
- Resources pane 175
- Result Grouping pane 157
- results
 - filtering 63
- reverse proxy
 - connect ODB Data Flow Probe to BSM server 390
- running software
 - discovery 126, 130
 - identifying processes 127

S

- SAP JMX protocol 91
- SAP protocol 91
- Schedule Discovery page
 - Database wizard 280
 - Infrastructure wizard 313
 - J2EE wizard 322
- Scope Definition dialog box 82
- Script Editor window 178
- Script pane 179
- Show Results for Triggered CI dialog box 330
- Siebel Gateway protocol 92
- SiteScope
 - sending zipped bulk data to ODB 30
- SNMP protocol 93
- Software Identification Rule Editor dialog box 181
- Software Library dialog box 184
- Source CIs dialog box 331

Index

SQL protocol 95

SSH protocol 96

SSL

 configuring ODB Data Flow Probe 395

 enabling on ODB Data Flow Probe
 389, 390, 395

 hardening the ODB Data Flow Probe
 393

stable ID 341

start/stop

 JMX operations 253

Statistics Results pane 120, 292

Summary page

 Database wizard 281

 Infrastructure wizard 313

 J2EE wizard 323

T

Telnet protocol 99

Time Templates dialog box 331

Trigger CIs 29

trigger queries 29

Trigger Query Editor window 332

Triggered CIs window 332

troubleshooting

 not all networks and IPs discovered 31

 not all TCP ports discovered 31

 results do not appear in map view 31

 transferring Probe from domain to
 domain 111

Troubleshooting and Knowledge Base 15

troubleshooting and limitations 30

U

Universal Description Discovery and
 Integration (UDDI) registry protocol
 101

update

 use cpVersion attribute to verify 135

updates, documentation 16

Used Scripts pane 145

V

view permissions 242

viewJobErrorsSummary

 JMX operations 253

viewJobExecHistory

 JMX operations 253

viewJobProblems

 JMX operations 253

viewJobResultCiInstances

 JMX operations 254

viewJobResults

 JMX operations 254

viewJobsStatuses

 JMX operations 256

viewJobStatus

 JMX operations 257

viewJobTriggeredCIs

 JMX operations 259

viewJobTriggeredCIsWithErrorId

 JMX operations 261

VMware

 protocol 102

W

WebLogic

 page in J2EE wizard 317

 protocol 103

WebSphere

 page in J2EE wizard 319

 protocol 104

wizard

 Database 275

 J2EE 314

WMI protocol 105

X

XML files

 reconciliation 354