OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Discovery Manager Administration

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Discovery Manager Administration

Version 6.5

Document Release Date: November 20, 2006

MERCURY™

Mercury Business Availability Center, Version 6.5
Discovery Manager Administration

Mercury provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. Mercury makes no representations or warranties whatsoever as to site content or availability.

Mercury Interactive Corporation
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Fax: (650) 603-5300
http://www.mercury.com

If you have any comments or suggestions regarding this document, please send them by e-mail to documentation@mercury.com.

AMLIB_DMAD6.5/01

Table of Contents

Welcome to Discovery Manager Administration................................ix
How This Guide Is Organized ix
Who Should Read This Guide x
Getting More Information x

PART I: INTRODUCTION

Chapter 1: Introduction to the Discovery Manager 3
About the Discovery Process 3
Discovery Process Architecture 4
About the Discovery Manager...6
Before You Begin 6

PART II: DISCOVERY PROBE INSTALLATION

Chapter 2: Installing the Discovery Probe 9
About Installing the Discovery Probe 9
Discovery Probe Hardware and Software Requirements.....................10
Discovery Probe Installation Procedure 10

PART III: PACKAGES

Chapter 3: Package Administration 15
Package Administration Overview 15
Deploying a Package...16
Removing a Package 17
Displaying Packages Currently Deployed 17
Dependencies Among Packages 18
XML File Naming Conventions 21
Troubleshooting Issues..21

PART IV: WORKING WITH THE DISCOVERY SYSTEM

Chapter 4: Running the Discovery Process..25
Understanding the Discovery Manager 26
Understanding the Module Manager Tab..27
Managing Modules...28
Adding a Discovery Probe 36
Configuring the Connection Data for a Protocol..............................40
Using Advanced Options in the Details View Pane...........................43
Discovery Process Configuration Files 59
Understanding the Discovery TQL Manager 63
Defining Discovery TQL Queries...64
Understanding the Pattern Editor...69
Editing a Pattern...70
Scheduling a Discovery Pattern to Run on a Periodic Basis................75
Defining Advanced Settings...80
Discovery Pattern Validation 81
Activating a Discovery Pattern...82
Deactivating a Discovery Pattern...82
Understanding the Discovery Manager Map View Tab......................83
Understanding the Schedule View Tab...90
Protocol Definitions 92

PART V: PERFORMING SPECIFIC DISCOVERIES

Chapter 5: Performing a SAP Discovery 109
Step 1 – Installing the Java Connectors 110
Step 2 – Preparing for a SAP Discovery 110
Step 3 – Adding a Network CI to Trigger the Discovery of
SAP System Networking..113
Step 4 – Accessing the Discovery Modules.......................................114
Step 5 – Running the Discovery Patterns...115
Step 6 – Checking that the Discovery Ran Correctly.......................124
Step 7 – Running SAP Solution Manager Discovery 125
CIs Created by the Discovery Process 126

Chapter 6: Performing a Siebel Discovery..137
About Performing a Siebel Discovery..138
Running Siebel Discovery...138
Step 1 – Preparing for a Siebel Discovery 139
Step 2 – Adding a Network CI to Trigger the Discovery of Siebel Enterprise Networking..143
Step 3 – Accessing the Discovery Modules..144
Step 4 – Discovering the Network 145
Step 5 – Running the Pre–Discovery Patterns for the Web Tier 146
Step 6 – Running the Siebel Discovery..147
Step 7 – Checking that Discovery Ran Correctly 148
Manual Configuration for Specific Siebel CIs 149
CIs Created by the Discovery Process 151

Chapter 7: Performing a Veritas Cluster Discovery 159
Step 1 – Preparing for a Veritas Cluster Discovery............................160
Step 2 – Running the Discovery Patterns..162
Step 3 – Checking that the Discovery Ran Correctly........................163
CIs Discovered by the Discovery Process 165
Troubleshooting 167

Chapter 8: Performing an SNMP Host Resources Discovery...........169
Step 1 – Preparing for an SNMP Discovery 170
Step 2 – Running the Discovery Patterns..173
Step 3 – Checking that the Discovery Ran Correctly........................174
CIs Discovered by the Discovery Process 175
Troubleshooting 176

Chapter 9: Performing an IIS Discovery 177
Step 1 – Preparing for an IIS Discovery 178
Step 2 – Running and Configuring the Discovery Patterns..............180
Step 3 – Checking that the Discovery Ran Correctly........................181
CIs Discovered by the Discovery Process 183

Chapter 10: Performing a WebLogic Discovery 185
Performing a WebLogic Discovery..186
Step 1 – Preparing for a WebLogic Discovery 186
Step 2 – Running the Discovery Patterns..188
Step 3 – Checking that the Discovery Ran Correctly........................189
CIs Discovered by the Discovery Process 190

Chapter 11: Performing a WebSphere Discovery............................193
Performing a WebSphere Discovery...194
Step 1 – Preparing for a WebSphere Discovery 194
Step 2 – Running the Discovery Patterns...197
Step 3 – Checking that the Discovery Ran Correctly.......................198
CIs Discovered by the Discovery Process 199

Chapter 12: Performing a UDDI Discovery.......................................201
Performing a UDDI Discovery...201
Step 1 – Preparing for a UDDI Discovery 202
Step 2 – Running the Discovery Patterns...204
Step 3 – Checking that the Discovery Ran Correctly.......................205
CIs Discovered by the Discovery Process 205

Chapter 13: Performing an SQL Discovery 209
Step 1 – Preparing for an SQL Discovery..209
Step 2 – Running the Pre-Discovery Pattern 212
Step 3 – Running the Discovery Patterns...212
Step 4 – Checking that the Discovery Ran Correctly.......................213
CIs Discovered by the Discovery Process 214

Chapter 14: Performing a Microsoft Cluster Server Discovery 217
Step 1 – Preparing for a Microsoft Cluster Server Discovery............218
Step 2 – Running the Pre-Discovery Patterns...................................220
Step 3 – Running the Discovery Pattern 221
Step 4 – Checking that the Discovery Ran Correctly.......................221
CIs Discovered by the Discovery Process 222
Troubleshooting 224

PART VI: APPENDIXES

Appendix A: Optional Variables in Discovery Patterns 227

Appendix B: Discovery Patterns 229
Application – Oracle E-Business Suite 231
Application – SAP 232
Application – Siebel 236
Application – Webservices 240
Database – DB2 240
Database – Oracle 242
Database – Oracle TNS 244
Database – SQL Server 246
Database – Sybase 248
Host Resources – NTCMD 249
Host Resources – SNMP 250
Host Resources – SSH/FD 252
Host Resources – WMI 253
J2EE – Weblogic 255
J2EE – Websphere 257
MS_Cluster 259
Mainframe 260
NetLinks – Passive Network Connections Discovery 261
Network – Advanced 263
Network – Basic 265
Network – Credential-Less Discovery 267
Network – Layer2 269
Network – Protocol Connections 271
Network – TCP Discovery 275
Veritas Cluster 279
Web Servers – Basic 280
Web Servers – IHS 281
Web Servers – IIS 282
Websphere_MQ 283
Others 285

Appendix C: Discovery Methods 293

Appendix D: Discovery Log Files 301
Understanding Discovery Log Files 301
Discovery Server Logs 302
Discovery Probe Logs 304

Index 309

Welcome to Discovery Manager Administration

This guide describes how to work with Discovery Manager.

How This Guide Is Organized

The guide contains the following chapters:

Part I **Introduction**

Contains an explanation of what the discovery process is and describes the Mercury Business Availability Center discovery process architecture.

Part II **Discovery Probe Installation**

Describes how to install the Discovery Probe.

Part III **Packages**

Describes how to create and deploy packages.

Part IV **Working with the Discovery System**

Describes how to run the discovery process by activating and editing discovery patterns.

Part V **Performing Specific Discoveries**

Contains a description of specific discoveries.

Part VI Appendixes

Describes how to add the attribute **optional="true"** to a variable tag in a discovery pattern. It also provides a list of discovery patterns, discovery methods and discovery log descriptions.

Who Should Read This Guide

This guide is intended for the following users of Mercury Business Availability Center:

- Mercury Business Availability Center administrators
- Mercury Business Availability Center platform administrators
- Mercury Business Availability Center application administrators
- Mercury Business Availability Center data collector administrators

Readers of this guide should be knowledgeable about enterprise system administration, have familiarity with ITIL concepts, and be knowledgeable about Mercury Business Availability Center in general and Mercury Application Mapping technology specifically.

Getting More Information

For information on using and updating the Mercury Business Availability Center Documentation Library, reference information on additional documentation resources, typographical conventions used in the Documentation Library, and quick reference information on deploying, administering, and using Mercury Business Availability Center, refer to *Getting Started with Mercury Business Availability Center*.

Part I

Introduction

1

Introduction to the Discovery Manager

This chapter introduces the Discovery Manager. The Discovery Manager enables you to manage the discovery process.

This chapter describes:	On page:
About the Discovery Process	3
Discovery Process Architecture	4
About the Discovery Manager	6
Before You Begin	6

About the Discovery Process

Mercury Business Availability Center's discovery system enables you to automatically discover and map logical application assets in Layers 2 through 7 of the Open System Interconnection (OSI) Model. It is an ongoing, automatic process that continuously detects changes that occur in your IT infrastructure and updates the CMDB accordingly. You do not need to install any agents on the discovered devices. The discovery process uses a spiral discovery model that has over 100 out-of-the-box discovery patterns.

The discovery process is a gradual uncovering of the elements in your system. Discovery is first done at the most basic level, and then at more in-depth ones. Every time a discovery pattern is activated, it discovers more CIs, which in turn are used as triggers for other discovery patterns. This process continues until your entire IT infrastructure is discovered and mapped.

The discovery process does the following:

- Sweeps the application domain
- Identifies application element details
- Determines which ports are being used
- Checks the operating system
- Communicates with Industry standard or Application APIs

Discovery Process Architecture

The architecture of the Mercury Business Availability Center discovery process consists of the following components:

- "Discovery Pattern" on page 4
- "Discovery Module" on page 5
- "Discovery Probe" on page 5
- "Mercury Business Availability Center Servers" on page 5
- "Discovery Protocol" on page 5

Discovery Pattern

The discovery process is run by activating discovery patterns. A discovery pattern is an XML template that contains definitions of one or more discovery tasks. It defines which data is discovered, through which protocol, when to pass the data on to the CMDB, and the executing schedule. A discovery pattern contains a description of the configuration items (CIs) and relationships that are created with each specific pattern. The CI and relationship definitions are taken from the CI Type Model, which contains the definitions of all the configuration item types (CITs) and relationships defined in the system.

Discovery Module

A discovery module contains one or more discovery patterns that together, allow a discovery of a specific technology/application. For example, discovery of the network includes patterns that discover: IPs, servers, switches, routers, and so forth.

Discovery Probe

The Discovery Probe is the main discovery component responsible for receiving discovery tasks from the Mercury Business Availability Center server, dispatching them to the IT components and sending the results back to the CMDB through the server. You define a range of network addresses to a specific installed Discovery Probe. The connection between the Discovery Probe ID to the physically installed Discovery Probe is made in the **appilog-remote.properties** file, which is located in: \<**Discovery Probe installation location**>**/root/lib/collectors**.

Mercury Business Availability Center Servers

The Mercury Business Availability Center Core Server hosts the servlets that deliver discovery requests to the Discovery Probe. The Processing Server receives the discovery results and stores the collected data in the CMDB.

If you install Mercury Business Availability Center using a single machine, that server functions as both a Processing and Core Server.

Discovery Protocol

Discovery of the different IT infrastructure components is performed by using various protocols such as SNMP, WMI, JMX, Telnet, and so forth.

About the Discovery Manager

The Discovery Manager contains discovery modules. Each module contains one or more discovery patterns required for discovering a specific group of CIs. You run the discovery process by activating discovery patterns in the Discovery Manager. You can choose to activate all the patterns in the module or only some of them.

The Discovery Manager also enables you to edit the discovery patterns. Only administrators with an advanced knowledge of how the discovery process works, should edit the discovery patterns. For details, see "Running the Discovery Process" on page 25.

Before You Begin

Before you run the discovery process, you must first do the following:

- **Obtain a license.** For more information, contact your Mercury representative.
- **Install the Discovery Probe.** For information on how to install the Discovery Probe, see "Installing the Discovery Probe" on page 9.

Note:

- To perform a DB2 discovery, copy the files **db2java.zip** and **db2jcc.jar** from the DB2 installation folder and place them in **Mercury Business Availability Center's\DiscoveryProbe\root\ext\jdbcdrivers\DB2**.
- When performing an Oracle RAC discovery, note that the discovery process cannot discover links to the remote machines (DB clients) in the following situation: The discovered database is reporting its clients by their host names and not the IP addresses and the host name cannot be resolved to an IP address. In this case, the remote client cannot be created.

Part II

Discovery Probe Installation

2

Installing the Discovery Probe

This chapter describes the hardware and software requirements and the procedures that are needed for the installation of the Discovery Probe on a Windows platform.

This chapter describes:	On page:
About Installing the Discovery Probe	9
Discovery Probe Hardware and Software Requirements	10
Discovery Probe Installation Procedure	10

About Installing the Discovery Probe

Before you run the discovery process, you first need to install the Discovery Probe. Read about the hardware and software requirements for installing the Discovery Probe below, and the Discovery Probe installation procedure in "Discovery Probe Installation Procedure" on page 10.

Discovery Probe Hardware and Software Requirements

The following table describes the hardware and software requirements for installing the Discovery Probe.

Supported Environments	Memory	Free Hard Disk Space
➤ Microsoft Windows 2000 ➤ Microsoft 2003 Server ➤ Microsoft Windows XP	Minimum: 256 MB RAM Recommended: 1024 MB RAM	Minimum: 2 GB Recommended: 4 GB

Discovery Probe Installation Procedure

It is recommended to install the Discovery Probe on a separate server with Windows 2000 or 2003 to distribute the overall system load. Solaris is not supported.

To install the Discovery Probe, follow the instructions of the Discovery Probe wizard.

To install the Discovery Probe:

1 In the **Admin** menu, select **Platform**, and then click **Downloads** to open the Downloads page.

2 Click the **Auto Discovery Probe** link. A dialog is displayed asking if you want to open the Setup file or save it to your computer.

- If you choose to open the file, it will not be saved to your computer, and the setup program will start immediately. In this case, depending on your browser security settings, you might receive a security warning dialog box. Confirm that you want to proceed.
- If you choose to save the file to your computer, double-click it to begin installation.

The Discovery Probe wizard opens the Introduction page.

3 Click **Next** to open the Choose Installation Folder page.

4. Click **Choose** to display a standard Browse dialog box. Browse to and select the installation folder.

   Note: If you change your mind after selecting a directory in the Browse dialog box, click **Restore Default Folder** to restore the default installation directory.

5. Click **Next** to display the Discovery Probe Configuration page.
6. In the Discovery Probe Configuration page, do the following:
   - ➤ In the **Core Server IP** box, enter the IP or the DNS name of the Core Server.
   - ➤ In the **Probe IP** box, enter the IP address of the machine on which you want to install the Discovery Probe.
   - ➤ In the **Probe Identifier** box, enter the name you want to give for the Discovery Probe to be used for the discovery process. The Discovery Probe identifier defined here appears as the default Discovery Probe in the Discovery Probes Manager tab in the Discovery Manager. For details, see “Adding a Discovery Probe” on page 36.
   - ➤ (For MMS environments only where a single server hosts multiple environments) In the **BAC Customer ID** box, enter the Customer ID for the environment to which the Discovery Probe reports.
7. Click **Next** to open the Server Communication Protocol page.
8. Select **Probe Server HTTPS** to secure the Discovery Probe/Server link.
9. Click **Next** to open the Memory Size page.
10. In the Memory Size page, define the minimum and maximum memory to be allocated to the Discovery Probe. The values are measured in megabytes.
    - ➤ In the **Discovery Probe Min Heap** box, enter a value that defines the minimum amount of memory to be allocated to the Discovery Probe.
    - ➤ In the **Discovery Probe Max Heap** box, enter a value that defines the maximum amount of memory to be allocated to the Discovery Probe.

Note: It is recommended not to change the defaults.

11 Click **Next** to open the Pre-Installation Summary page and review the selections you have made.

12 Click **Install** to complete the installation of the Discovery Probe. When the installation is complete the Install Complete page is displayed.

13 Click **Done**. The following shortcut is added to the Windows **Start** menu:

Programs > **Business Availability Center** > **Administration** > **Discovery Probe**

Part III

Packages

3

Package Administration

This chapter explains how to deploy packages. Packages contain definitions, resources, and tools that enable you to discover IT infrastructure resources such as network extensions, applications, and databases.

This chapter describes:	On page:
Package Administration Overview	15
Deploying a Package	16
Removing a Package	17
Displaying Packages Currently Deployed	17
Dependencies Among Packages	18
XML File Naming Conventions	21
Troubleshooting Issues	21

Package Administration Overview

Packages fulfill several functions:

- A package includes all resources needed for the discovery of a specific IT infrastructure asset. For example, Mercury Business Availability Center runs the SQL_Server package to discover Microsoft SQL Servers.

  For details on using the Discovery Manager, see Chapter 1, “Introduction to the Discovery Manager.”

- Mercury Business Availability Center extracts information from packages when building views, hierarchies, TQL queries, and so on.

- Packages enable you to copy resources from one environment to another, for example, from a test to a production environment.

  You can deploy and remove packages without the need to restart the server by using the JMX console. You can also display currently deployed packages.

Deploying a Package

This section explains how to deploy a package using the JMX console.

To deploy a package:

1. Launch the Web browser and enter the following address: http://<server_name>:8080/jmx-console, where <server_name> is the name of the machine on which the Data Processing Server is installed.
2. Under MAM, click **service=Package manager** to open the JMX MBEAN View page.
3. Locate deployPackages and enter the following information:
   - In the customerId box, enter **1**.
   - In the dir box, enter the name of the folder which contains the package's zip file.

     Include the full path to the folder.
   - In the packagesNames box, enter the name of the package.

     The rules for entering a package name are as follows:
     - The package name can contain a wildcard character (*).
     - The package name is case sensitive.
     - The package name must have a **.zip** extension.
4. Click **Invoke** to deploy the package.

Removing a Package

This section describes how to remove a package using the JMX console.

To remove (undeploy) a package:

1. Launch the Web browser and navigate to: http://<server_name>:8080/jmx-console, where <server_name> is the name of the machine on which the Data Processing Server is installed.
2. Under MAM, click **service=Package manager** to open the JMX MBEAN View page.
3. Enter the following to the right of the undeployPackages box:
   - ➤ In the customerId box, enter **1**.
   - ➤ In the packagesNames box, enter the name of the package you want to remove.

     The rules for entering a package name are as follows:

     - ➤ Wildcard characters (*) are not supported
     - ➤ The package name is case sensitive.
4. Click **Invoke** to remove the package.

Displaying Packages Currently Deployed

This section describes how to display packages that are currently deployed.

To display packages that are currently deployed:

1. Launch the Web browser and navigate to: http://<server_name>:8080/jmx-console, where <server_name> is the name of the machine on which the Data Processing Server is installed.
2. Under MAM, click **service=Package manager** to open the JMX MBEAN View page.
3. To the right of the displaydeployedPackages box, enter **1** in the customerId box.
4. Click **Invoke** to display the packages that are currently deployed.

Dependencies Among Packages

Certain packages are dependent for their functioning on the installation of other packages. This means that certain packages have to be deployed before deploying others. These dependencies are specified in the descriptor.xml file included in each package.

For example, the SQL_Server package is based on resources that are contained in the Database_Basic package. To view this dependency, open SQL_Server.zip and open descriptor.xml in a text editor:

```
<descriptor>
<dependency>Database_Basic.zip</dependency>
</descriptor>
```

The following table contains a list of the default packages in the package directory and their dependencies.

Package	Dependent On...
AutoDiscovery	None
Basic_Classes	None
BLE	➤ SLP ➤ Basic_Classes ➤ Database_Basic ➤ EUM ➤ Business
Business	Basic_Classes
BusinessService	None
Credential_Less_Discovery	➤ Basic_Classes ➤ AutoDiscovery
Database_Basic	➤ Host_Resources_Basic
DB2	Database_Basic
Default_View	views

Package	Dependent On...
diagnostics	➤ Network ➤ Business ➤ BLE ➤ views ➤ SLP
EMS	➤ Network ➤ Business ➤ BLE ➤ views
EUM	➤ Business ➤ views
EUM_61	➤ Business ➤ BLE ➤ EUM ➤ views
Host_Resources_Basic	Network
Host_Resources_By_NTCMD	Host_Resources_Basic
Host_Resources_By_SNMP	Host_Resource_Basic
Host_Resource_By_TTY	Host_Resources_Basic
Host_Resource_By_WMI	Host_Resource_Basic
IBM_HTTP_Server	➤ WebServer ➤ J2EE
ITU	➤ EUM ➤ sitescope ➤ views
J2EE	Database_Basic
Layer2	Network
Mainframe	Host_Resources_Basic

Package	**Dependent On...**
NetLinks	➤ Basic_Classes ➤ Network
Network	➤ Basic_Classes ➤ AutoDiscovery
Oracle	Database_Basic
OracleApps	➤ Database_Basic ➤ J2EE ➤ Oracle
SAP	➤ J2EE ➤ WebServer
SAP_discovery	➤ SAP
SAP_monitoring	➤ EUM ➤ sitescope ➤ BLE ➤ SAP
ServiceCatalog	view
Siebel	Database_Basic, WebServer
Siebel_discovery	Siebel
sitescope	Business
SLP	None
snapshot	None
SQL_Server	Database_Basic
Sybase	Database_Basic
TCP_discovery	Network
UDX	EMS
views	None
watchdog	➤ sitescope ➤ views

Package	Dependent On...
WebServer	Network
Websphere_MQ	Network

XML File Naming Conventions

Use the following naming conventions when naming the XML files:

- The names of the resources described in the XML file must be identical to the names of the XML files. For example, a correlation rule called MyCorrelation must be described in a file called MyCorrelation.xml.
- The XML file name is case sensitive.

Troubleshooting Issues

This section describes some of the troubleshooting issues that may arise when using the JMX console to deploy, display, or remove deployed packages.

This sections contains the following topics:

- "Verifying Dependency Among Packages" on page 21
- "Undeploying Packages" on page 22
- "Verifying Packaging Operations" on page 22

Verifying Dependency Among Packages

Certain packages are dependent for their functioning on the installation of other packages. These dependencies are specified in the descriptor.xml file included in each package. The success of package deployment or removal of a package may depend on the installation of other packages.

For example:

- If package A is dependent on package B, you cannot remove package B.
- If you want to deploy package A, which is dependent on package B, but package B does not exist, you cannot deploy package A.

Note: For a list of the packages and their dependencies, see "Dependencies Among Packages" on page 18.

Undeploying Packages

- You cannot remove (undeploy) a package that contains a CIT if an instance of that CIT appears in the CMDB.
- You cannot undeploy a package if one of its resources remains deployed.

Verifying Packaging Operations

It is recommended to check the packaging.log file after each operation to verify its success. If the operation was not successful, the log file contains detailed information on why the operation failed.

The packaging.log file is located in: **<Mercury Business Availability Center root directory>\log**.

Part IV

Working with the Discovery System

4

Running the Discovery Process

This chapter describes how to run the discovery process by activating and editing discovery patterns.

This chapter describes:	On page:
Understanding the Discovery Manager	26
Understanding the Module Manager Tab	27
Managing Modules	28
Adding a Discovery Probe	36
Configuring the Connection Data for a Protocol	40
Using Advanced Options in the Details View Pane	43
Discovery Process Configuration Files	59
Understanding the Discovery TQL Manager	63
Defining Discovery TQL Queries	64
Understanding the Pattern Editor	69
Editing a Pattern	70
Scheduling a Discovery Pattern to Run on a Periodic Basis	75
Defining Advanced Settings	80
Discovery Pattern Validation	81
Activating a Discovery Pattern	82
Deactivating a Discovery Pattern	82
Understanding the Discovery Manager Map View Tab	83

This chapter describes:	On page:
Understanding the Schedule View Tab	90
Protocol Definitions	92

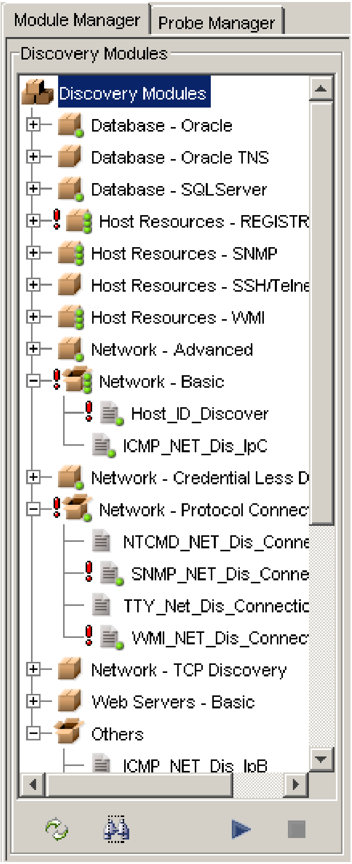
Understanding the Discovery Manager

The Discovery Manager is displayed by selecting **Admin** > **CMDB** and then clicking the **Discovery Manager** tab. The Discovery Manager contains the following tabs:

- **Module Manager.** Contains:
    - **Details View tab**. Enables you to activate discovery patterns. The Module Manager contains a list of discovery modules. Each discovery module includes a group of discovery patterns. Select the required discovery patterns from the various modules to discover a specific group of CIs. For details, see "Understanding the Module Manager Tab" on page 27.
    - **Map View tab**. Displays a visual representation of the real-time progress of the discovery process. For details, see "Understanding the Discovery Manager Map View Tab" on page 83.
    - **Schedule View tab**. Displays all discovery pattern scheduling information in one table. For details, see "Understanding the Schedule View Tab" on page 90.
- **Probe Manager.** Enables you to:
    - Define a new discovery probe and the range of the IP addresses to be discovered. For details, see "Adding a Discovery Probe" on page 36.
    - Define the connection data for each protocol. For details, see "Configuring the Connection Data for a Protocol" on page 40.

Understanding the Module Manager Tab

The Module Manager tab contains a list of discovery modules. Each module includes the discovery patterns necessary to discover a specific group of CIs.



From the Discovery Modules pane, you can select the module(s) you want to use for the discovery process. The discovery patterns contained in the modules you select are used in the discovery process. Each icon represents a module.

When you select a module, the Details View tab in the Module Manager is divided as follows:

Field	**Description**
Discovery Module Summary	Contains the following fields: ➤ **Discovery Module Name**. The name of the selected module. ➤ **Description**. A description of the selected module.
Statistics	Contains the following fields: ➤ **CIT**. The name of the CIT discovered by the module. ➤ **Created**. The number of CIT instances created by the module. ➤ **Updated**. The number of CIT instances updated by the module. ➤ **Deleted**. The number of CIT instances deleted by the module. **Note:** The last row of the Statistics table, the **Total** row, contains the total number of CIs in each column.

Note: For details on the Map View tab, see "Understanding the Discovery Manager Map View Tab" on page 83.

Managing Modules

This section contains the following topics:

- "Editing a Discovery Module" on page 29
- "Activating a Discovery Module" on page 30
- "Deactivating a Discovery Module" on page 31

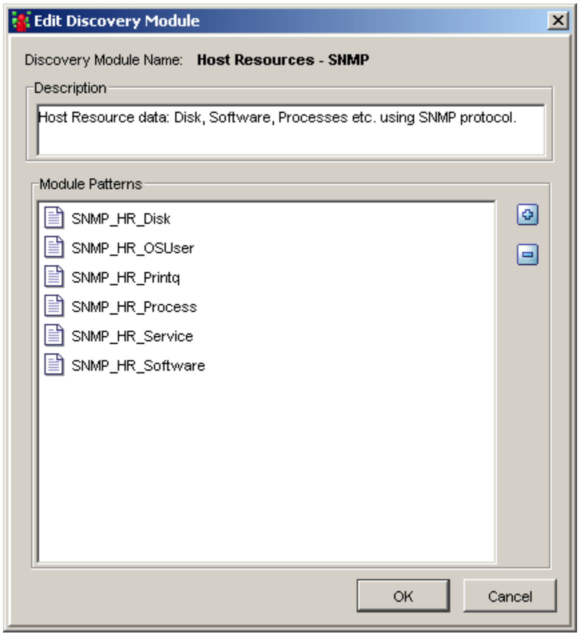
- “Creating a Discovery Module” on page 31
- “Deleting a Discovery Module” on page 32
- “Searching For a Discovery Pattern” on page 32
- “Updating the Statistics Table for the Selected Discovery Module” on page 33
- “Resetting the Statistics Table for the Selected Discovery Module” on page 33
- “Sorting and Customizing Tables” on page 34
- “Maximizing and Restoring the Statistics Table” on page 35

Editing a Discovery Module

You can edit each module to include the discovery patterns you want it to contain.

To edit a discovery module:

1 In the Discovery Modules pane, right-click the module you want to edit and select **Edit Module** to open the Edit Discovery Module dialog box.



Edit Discovery Module

Discovery Module Name: **Host Resources - SNMP**

Description

Host Resource data: Disk, Software, Processes etc. using SNMP protocol.

Module Patterns

SNMP_HR_Disk
SNMP_HR_OSUser
SNMP_HR_Printq
SNMP_HR_Process
SNMP_HR_Service
SNMP_HR_Software

The Edit Discovery Module dialog box has the following fields:

- **Description.** A description of the selected module.
- **Module Patterns.** A list of the discovery patterns in the selected module.

2. Click the **Add Discovery Pattern to Module** button to open the Choose Discovery Patterns dialog box.
3. Select the pattern(s) you want to add to the module. You can make multiple selections.
4. Click **OK**. The discovery patterns are added to the **Module Patterns** area in the Edit Discovery Module dialog box.
5. Click **OK** in the Edit Discovery Module dialog box to save the changes you have made.

Activating a Discovery Module

When you activate a discovery module, you activate all the patterns contained in the module.

To activate a discovery module:

In the Discovery Modules pane, right-click the module you want to activate and select **Activate**, or select the required module and click the **Activate** button in the bottom right corner of the Discovery Modules pane.

A module that is activated, as seen here, is marked with green dots.

Note: If only some of the module's patterns are activated, the module is marked with a single green dot. If all patterns of the module are activated, the module is marked with three green dots.

When the discovery module is activated, it discovers CITs and relationships of the types that are described in each pattern, and places them in the CMDB.

Deactivating a Discovery Module

This section explains how to deactivate a module that is activated.

To deactivate a discovery module:

In the Discovery Modules pane, right-click the module you want to deactivate and select **Deactivate**, or select the required module and click the **Deactivate** button in the bottom right corner of the Discovery Modules pane.

Creating a Discovery Module

This section describes how to create a discovery module.

To create a discovery module:

1. In the Discovery Modules pane, right-click **Discovery Modules** at the top of the hierarchy.
2. Select **Create new module.** The Choose new name for discovery module dialog box opens.
3. Enter a new name for the module.
4. Click **OK** to create the new module. The new discovery module appears in the Discovery Module pane.
5. To add discovery patterns to the module, right-click the module and select **Edit Module**. The Edit Discovery Module opens. For details, see “Editing a Discovery Module” on page 29. After you add one or more discovery patterns to the module, the module then appears in the Discovery Module pane.

Deleting a Discovery Module

This section describes how to delete a discovery module.

Note: Only administrators with an expert knowledge of the discovery process should delete discovery modules.

To delete a discovery module:

In the Discovery Modules pane, right-click the module you want to delete and select **Delete**.

Searching For a Discovery Pattern

Discovery Manager's searching capabilities enable you to find a specific discovery pattern in the Discovery Modules pane. These capabilities provide different search criteria through which you can search for discovery patterns. You can do a search according to their pattern name, input type, or output type.

To search for a discovery pattern in the Discovery Modules pane:

1. At the bottom of the Discovery Module pane, click the **Find Pattern** button to open the Find patterns dialog box.
2. To search for a pattern by name, do the following:
   - Select **Name**.
   - In the **Discovery Pattern Name** box, enter the name of the pattern you want to find. Mercury Business Availability Center searches for patterns whose names contain the entered text.
3. To search for patterns by CIs that triggered the discovery pattern (input CIs), do the following:
   - Select **Input type**.
   - In the **CI Type** area, click the **CI Type** button to open the Choose Configuration Item Type dialog box.
   - Select the required CIT and click **OK**.

4. To search for patterns by CIs that are discovered as a result of the activated discovery pattern (output CIs), do the following:
   - ➤ Select **Output type**.
   - ➤ In the **CI Type** area, click the **CI Type** button to open the Choose Configuration Item Type dialog box.
   - ➤ Select the required CIT and click **OK**.
5. In the **Direction** section, specify whether you want to do a forward or backward search.
6. To run the search do one of the following:
   - ➤ Click **Find Next**. If Mercury Business Availability Center finds a match, it highlights the next pattern that meets the search criteria you defined.
   - ➤ Click **Find All**. If Mercury Business Availability Center finds a match, it highlights all the patterns that meet the search criteria you defined.

Updating the Statistics Table for the Selected Discovery Module

The discovery process results in the **Statistics** table are not automatically updated.

To update the Statistics table:

In the **Module Manager** tab, click the **Refresh Statistics** button to the left of the Statistics table.

Resetting the Statistics Table for the Selected Discovery Module

You can delete all the statistics from the **Statistics** table and restart the counting from zero.

To reset the Statistics table:

In the **Module Manager** tab, click the **Reset Statistics** button to the left of the Statistics table.

Sorting and Customizing Tables

This section describes how to sort the content in the columns and set which columns you want to display and in what order.

➤ "Sorting the Statistics Table" on page 34

➤ "Hiding a Column in the Statistics Table" on page 34

➤ "Displaying Hidden Columns in the Statistics Table" on page 34

➤ "Customizing the Statistic Table" on page 35

Sorting the Statistics Table

You can sort the contents of the Statistics table to be displayed in either ascending or descending order.

To sort the contents of a Protocol Entry column:

1. Click a column header.
2. To change the sort order, click the column header again.

   Once a column has been sorted its header displays a pink triangle pointed upwards for ascending order or downwards for descending order.

Hiding a Column in the Statistics Table

You can hide a column in the Statistics table.

To hide a column in the Statistics table:

On the selected tab, right-click the header of the column you want to hide and select **Hide Column**.

Displaying Hidden Columns in the Statistics Table

You can display hidden columns in the Statistics table.

To display hidden columns:

Right-click one of the column headers and select **Show All Columns**.

Customizing the Statistic Table

You can customize the Statistics table.

To customize the Statistics table:

1 Right-click one of the column headers and select **Customize** to open the Columns dialog box.

< >

2 To remove column(s) from the tab, select the required column(s) in the **Visible Columns** area and click the **Remove Column** button. The selected column(s) moves to the **Hidden Columns** area. (To return a column to the **Visible Columns** area, select it and click the **Add Column** button.)

⇩ ⇧

3 To change the display order of the columns, use the up and down arrows.

4 Click **OK** to apply your customization to the table.

Maximizing and Restoring the Statistics Table

This section describes how to maximize and restore the Statistics table to its previous size.

To maximize and restore the Statistics table to its previous size:

1 Click the up arrow at the top left-hand corner of the Statistics table to maximize the table.

2 Click the down arrow at the top left-hand corner of the Statistics table to restore the table to its previous size.

Adding a Discovery Probe

This section explains how to add a Discovery Probe and define its discovery range using the Probe Manager tab.

This section contains the following topics:

- "Adding a Discovery Probe and Configuring the Discovery Range" on page 36
- "Deleting a Discovery Probe" on page 38
- "Editing the Probe Description" on page 38
- "Deleting an IP Range" on page 38
- "Editing an Existing IP Range" on page 39
- "Rules for Defining an IP Address Range" on page 39

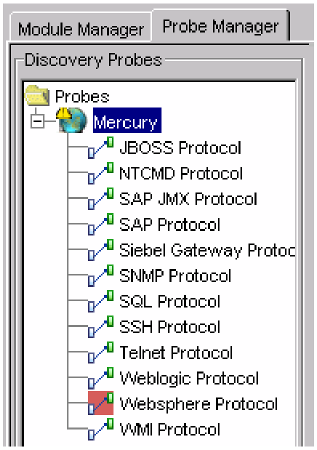
Adding a Discovery Probe and Configuring the Discovery Range

This section describes how to add a Discovery Probe and the range of the IP addresses to be discovered.

To add a new Discovery Probe and configure the discovery range:

1. Select **Admin** > **CMDB** and click the **Discovery Manager** tab.
2. Click the **Probe Manager** tab.

3 In the Discovery Probes pane, the Probe Identifier that is defined on the Discovery Probe Configuration page of the Discovery Probe wizard appears as the default Discovery Probe. (For details, see “Discovery Probe Installation Procedure” on page 10.)



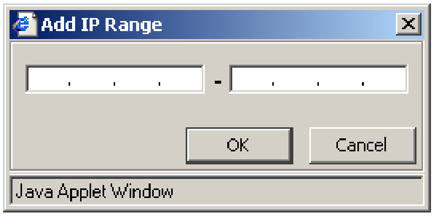
4 In the Discovery Probes pane, right-click the **Probes** folder or any empty space and select **Add probe** to open the Add New Probe dialog box.

5 In the **Name** box, type the new probe name.

6 In the **Description** box, type the probe description. This step is optional.

7 Click **OK** to add the new probe to the **Discovery Probes** list.

8 In the Ranges pane, click the **Add IP range** button to open the Add IP Range dialog box.



9 Enter an IP address range (for details, see “Rules for Defining an IP Address Range” on page 39).

10. Click **OK**. The range of net addresses you defined appears in the Ranges pane.
11. To enter another IP address range, click the **Add IP range** button again and repeat steps 9 and 10.
12. Click **Apply** to save the changes you have made.

Deleting a Discovery Probe

This section describes how to delete a Discovery Probe.

To delete a Discovery Probe:

1. From the **Discovery Probes** box, right-click the probe you want to delete and click **Remove probe**. A message appears asking you if you want to remove the Discovery Probe.
2. Click **Yes** to delete the probe.

Editing the Probe Description

This section describes how to edit the description of an existing probe.

To edit a probe's description:

1. From the Discovery Probes pane, select the Discovery Probe whose description you want to edit.
2. In the **Description** box in the Probe Details pane, make the required changes.

Deleting an IP Range

This section describes how to delete an IP range.

To delete an IP range:

In the **Ranges** box, select the IP range you want to delete and click the **Remove IP range** button.

Editing an Existing IP Range

This section describes how to edit an existing IP range:

To edit an existing IP range:

1 In the **Ranges** box, select the IP range you want to edit.

2 Click the **Edit IP range** button to open the Edit IP Range dialog box.

3 Make the required changes (for details, see "Adding a Discovery Probe and Configuring the Discovery Range" on page 36).

4 Click **OK** to save the changes you have made.

Rules for Defining an IP Address Range

The rules for defining an IP address range are as follows:

➤ 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 a wildcard character (*) so that Mercury Business Availability Center can match the range to more than one IP address. Mercury Business Availability Center scans the system to find the IP addresses matching the range pattern you defined.

➤ An asterisk (*) represents any number in the range of 0-255.

➤ You can use a wildcard character (*) in the lower bound IP address of the IP range pattern only.

For example:

Valid	Not Valid
10.0.64.* - 10.0.64.10	10.0.64.10 - 10.0.64.*

➤ If you do 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.

- You can use more than one asterisk (*) in an IP address as long as they are used consecutively. The asterisk(s) cannot be situated between two numbers in the IP address, nor can it substitute the first digit in the number.

  For example:

Valid	Not Valid
10.0.64.*	*0..60.10
10.0.*.*	10.*.64.*
10.*.*.*	10.*.*.1
	10.*.7.1

- 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. For example, if you enter the pattern 10.0.*.* - 10.0.20.30, the upper bound IP address is ignored. Since the asterisks (*) in the lower bound IP address cover a range wider than 20 and 30, 20 and 30 in the upper bound IP address are rendered irrelevant.

Configuring the Connection Data for a Protocol

You can add the connection data for each protocol included in the discovery process. The connection data can refer to a specific net address and/or to the entire net addresses range. When referring to the entire range, the net address value is DEFAULT. The default definitions relate to all IPs included in the defined range.

For a description of the connection data that needs to be defined for each protocol, see “Protocol Definitions” on page 92.

This section contains the following topics:

- “Defining the Connection Data For the Protocol” on page 41
- “Deleting the Connection Details for an Existing Protocol” on page 42
- “Editing the Connection Details for an Existing Protocol” on page 42
- “Sorting and Customizing the Protocol Entry Columns” on page 42

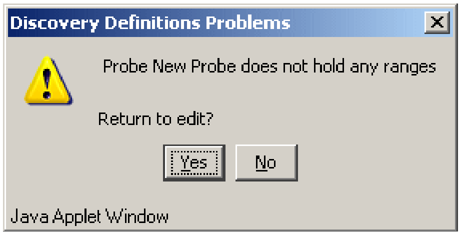
Defining the Connection Data For the Protocol

This section describes how to define the connection data for each protocol included in the discovery process.

To define the connection data for the required protocol:

1. Select **Admin** > **CMDB** and click the **Discovery Manager** tab.
2. Click the **Probe Manager** tab.
3. In the Discovery Probes pane, click the **Expand** button of the probe to which you want to add an instance of a protocol. A list of protocols is displayed.
4. Select the protocol whose connection data you want to define.
5. Click the **Add new connection details for selected protocol type** button to the right of the **Protocol Entries** area to add definitions to the protocol you have selected. The Add Protocol Parameter dialog box displays the list of attributes you need to define for the protocol.
6. Define the protocol parameters as required and then click **OK**. For information on protocol definitions, see **"Protocol Definitions" on page 92**. The parameter values you defined appear in the **Protocol entries** section.
7. Click **Apply** to save the changes you have made.

   If your Discovery Probe definitions are incorrect or incomplete, you get a message specifying what the problem is, as seen in the following example:



Discovery Definitions Problems

Probe New Probe does not hold any ranges

Return to edit?

Java Applet Window

8. Click:

   ➤ **Yes** to open the tab in which the issue has to be resolved.

   ➤ **No** to save the changes and close the Discovery Manager.

Note: If the Discovery Probe appears red, it indicates that not all the required protocols for the discovery pattern have been added as described in "Defining the Connection Data For the Protocol" on page 41.

9 Click the **Apply** button at the bottom of the screen to save the changes.

Deleting the Connection Details for an Existing Protocol

You can delete the connection details for an existing protocol.

To delete the connection details for an existing protocol:

1 In the **Probe Manager** tab, select the entry that you want to delete in the **Protocol entries** section, and click the **Remove selected connection details for selected protocol type** button.

2 Click the **Apply** button at the bottom of the screen to save the changes.

Editing the Connection Details for an Existing Protocol

You can edit the connection details for an existing protocol.

To edit the connection details for an existing protocol:

1 In the **Probe Manager** tab, select the entry that you want to edit in the **Protocol entries** area.

2 Click the **Edit selected connection details for selected protocol type** button.

3 Edit the details as required in the Edit Protocol Parameter dialog box that opens. For details, see "Protocol Definitions" on page 92.

4 Click the **Apply** button at the bottom of the screen to save the changes.

Sorting and Customizing the Protocol Entry Columns

For information on how to sort and customize the Protocol Entry table, see "Sorting and Customizing Tables" on page 34.

Using Advanced Options in the Details View Pane

You can view and edit the discovery patterns included in the modules.

Note: Only administrators with an expert knowledge of the discovery process should be allowed to delete discovery modules.

The following table describes the icons in the Discovery Modules pane.

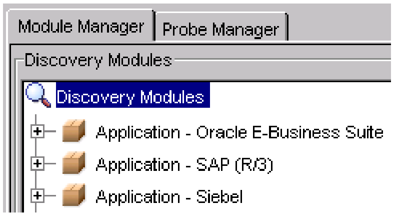
Icon	What it Represents
📦	A module
📄	A pattern

➤ When you select a pattern in the Discovery Modules pane, the Details View tab is divided as follows:

Field	Description
Discovery Pattern Name	The name of the selected discovery pattern and the package in which it is found.
Description	A description of the selected pattern.
Trigger TQLs	Define one or more TQL queries to be used as triggers to activate the selected discovery pattern. It contains the following fields: ➤ **TQL Name**. The name of the trigger TQL query that activates the discovery pattern. For details on TQL queries, see “Mercury Business Availability Center Topology Query System” in *View Manager Administration*. ➤ **Probe Limit**. The probes you want to use for the discovery process. For details, see “Defining a Trigger TQL Query” on page 47.

Field	Description
Triggered CIs	Display the CIs used by the discovery pattern for its discovery. For more information, see “Manually Activating a Discovery Pattern Using Specific CIs” on page 49.
Statistics	Display statistics on discovery results for the selected pattern. ➤ **CIT**. The name of the CIT discovered by the discovery pattern ➤ **Created**. The number of CIT instances created by the discovery pattern ➤ **Updated**. The number of CIT instances updated by the discovery pattern ➤ **Deleted**. The number of CIT instances deleted by the discovery pattern **Note:** The last row of the Statistics table, the **Total** row, contains the total number of CIs in each column.

- When you select the Discovery Modules root in the Discovery Modules pane (as in the picture below):



The Details View pane is divided as follows:

Field	**Description**
Configuration files	Contains configuration files with default parameter values that are used for the discovery process. For details, see "Discovery Process Configuration Files" on page 59.
Statistics	Displays statistics on discovery results for all the discovery modules. It contains the following fields: ➤ **CIT**. The name of the discovered CIT. ➤ **Created**. The number of CIT instances created. ➤ **Updated**. The number of CIT instances that were updated. ➤ **Deleted**. The number of CIT instances deleted. **Note:** The last row of the Statistics table, the **Total** row, contains the total number of CIs in each column.

This section contains the following topics:

- "Selecting a Pattern" on page 46
- "Defining a Trigger TQL Query" on page 47
- "Selecting the Probe(s) to Be Used in the Discovery Process" on page 48
- "Manually Activating a Discovery Pattern Using Specific CIs" on page 49
- "Filtering the Triggered CIs Table" on page 53
- "Updating the Triggered CIs Table" on page 54
- "Redispatching a Triggered CI to Manually Activate the Discovery Pattern Again" on page 55
- "Removing the Error Status of a Triggered CI" on page 55
- "Showing Error Details" on page 56
- "Sorting and Customizing the Triggered CI Table" on page 56
- "Maximizing and Restoring the Triggered CI Table" on page 56

- “Updating the Statistics Table for the Selected Discovery Pattern” on page 56
- “Resetting the Statistics Table for the Selected Discovery Pattern” on page 57
- “Sorting and Customizing the Statistic Table” on page 57
- “Maximizing and Restoring the Statistic Table” on page 57
- “Showing CI Instances” on page 57
- “Creating a Discovery Pattern” on page 58
- “Deleting a Discovery Pattern from a Module” on page 58
- “About Problem Indicators” on page 58

Selecting a Pattern

This section describes how to select a pattern in a module.

To select a pattern in a module:

✚ In the Discovery Modules pane, click the **Expand** button to the left of the required module to display the patterns contained in that module.

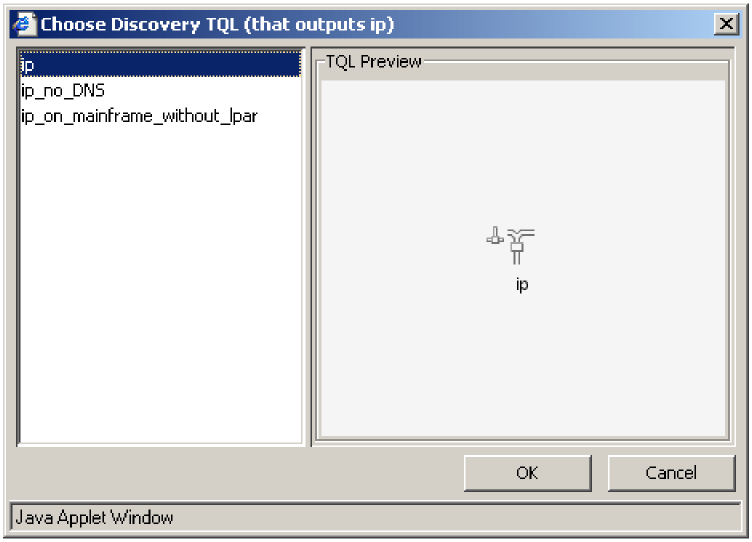
Defining a Trigger TQL Query

You can define one or more TQL queries to be used as triggers to activate the selected discovery pattern.

To define a trigger TQL query:

1 Select the required discovery pattern.

2 In the Trigger TQLs pane, click the **Add TQL** button to open the Choose Discovery TQL dialog box.


Choose Discovery TQL (that outputs ip)
ip
ip_no_DNS
ip_on_mainframe_without_lpar
TQL Preview
ip
OK
Cancel
Java Applet Window

The dialog box contains a list of discovery TQLs that match the discovery pattern's input CITs.

3 Select the TQL you want to serve as the trigger that invokes the discovery pattern's task, and click **OK**. The TQL query you selected appears in the Trigger TQLs pane.

Note: If necessary, you can create discovery TQLs from which to choose. For details, see "Defining Discovery TQL Queries" on page 64.

4 To remove a TQL query from the list, select the TQL you want to remove and click the **Delete TQL** button.

Note: If a TQL query is removed for an active discovery pattern, the Discovery Manager no longer receives new CIs coming from that TQL query. Existing triggered CIs that originally came from the TQL query are not removed.

---

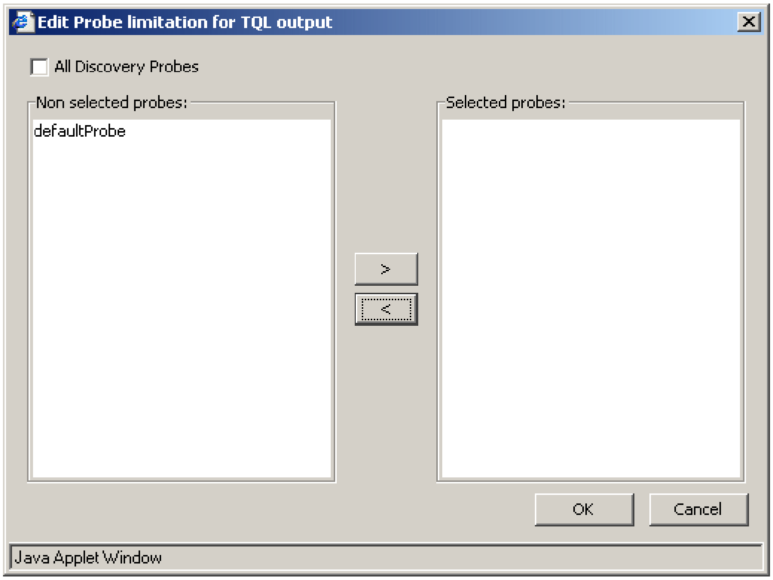
5 To add another TQL query, click the **New TQL** button again and repeat step 3.

Selecting the Probe(s) to Be Used in the Discovery Process

This section describes how to define the probe(s) to be used in the discovery process.

To select the probe(s) to be used in the discovery process:

1 From the Trigger TQLs pane, click the button to the right of the **Probe Limit** field to open the Edit probe limitation for TQL output dialog box.



defaultProbe

This screen displays a list of the Discovery Probes defined in the Probe Manager tab. For details, see “Adding a Discovery Probe and Configuring the Discovery Range” on page 36.

2 To activate all the probes, select the **All Discovery Probes** check box and click **OK**.

3 To activate a specific probe, do the following:

➤ Clear the **All Discovery Probes** check box.

➤ Select the required probes using the **Add** and **Remove** buttons to move them between the **Non selected probes** and **Selected probes** lists. You can also move multiple probes by making multiple selections.

4 Click **OK** to save the changes you have made.

Manually Activating a Discovery Pattern Using Specific CIs

Each discovery pattern contains the CIs that the pattern uses for the discovery process. After you have activated a discovery pattern, the CIs that are currently being used by the discovery pattern are displayed in the Triggered CIs pane.

When you can define one or more TQL queries to be used as triggers to activate the selected discovery pattern (for details, see “Defining a Trigger TQL Query” on page 47), the trigger TQL automatically triggers CIs that invoke the discovery pattern. You can choose to manually activate the discovery pattern so that it runs using only CIs that appear in the Triggered CIs pane instead of all the CIs triggered by the TQL. (For information on TQL queries, see Mercury Business Availability Center Topology Query System in *View Manager Administration*.)

The Triggered CIs pane has the following fields:

- **CI**. The triggered CI's label.
- **Status**. The current status of the triggered CI.

  Its status can be one of the following:

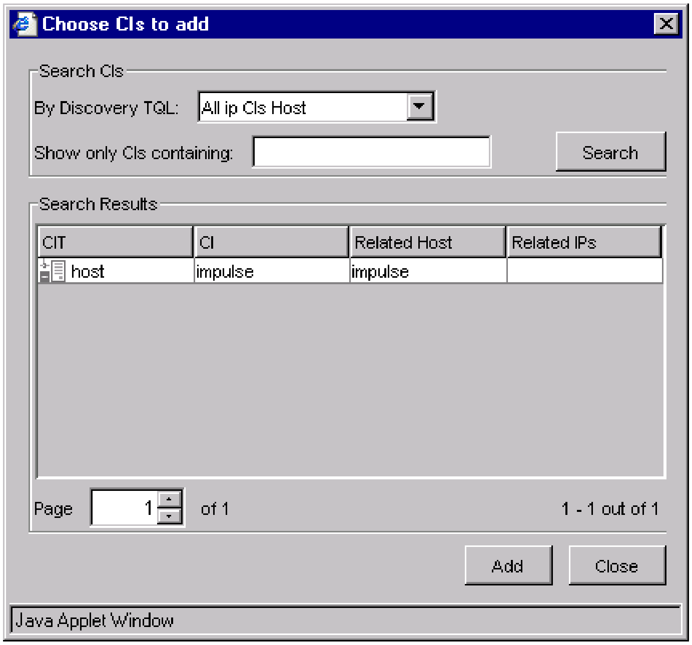
  - **Waiting for Probe**. The triggered CI is ready to be dispatched and is waiting for the Discovery Probe to retrieve it.
  - **Active**. The triggered CI is active and is running on the Discovery Probe.
  - **Discovery Errors**. Due to an error, the Mercury Business Availability Center server has failed to dispatch the discovery task.

    Following are the discovery error statuses:

    - **Server Processing Failure**. The server failed to add the CI to the list of triggered CIs.
    - **Active (Having error)**. An error occurred while running the discovery process (the discovery process continues running).
    - **Probe Fatal Error**. An error occurred while running the discovery process and the discovery pattern is no longer using this specific triggered CI for the discovery process.
  - **Active (being removed)**. The triggered CI is being removed from the Triggered CIs list.
- **Probe**. The discovery probe to which the triggered CI belongs.
- **Page**. The list of CIs are divided into pages. The number in the **Page** box indicates which page is currently being displayed.
  - To view other pages, use the up and down arrows, or type the page number, and click **Enter**.
  - To determine the number of CIs that appear on a page, right-click either the up or down button and select the required number. The default is 25.

To manually activate the discovery pattern using specific CIs:

1 In the Triggered CIs pane, click the **Add CI** button to open the Choose CIs to add dialog box.



By Discovery TQL: All ip CIs Host

Show only CIs containing:

CIT	CI	Related Host	Related IPs
host	impulse	impulse	

Page 1 of 1 1 - 1 out of 1

Note: The **Add CI** button is only enabled if the pattern is active. To activate the pattern, see “Activating a Discovery Pattern” on page 82.

The Choose CIs to add dialog box is divided as follows:

Field	Description
Search CIs	Contains two filters with which you can limit the number of CIs that appear in the Search Results pane. ➤ **By Discovery TQL** ➤ **Show only CIs containing** For details on how to use the filters, see step 3.
Search Results	Displays the list of triggered CIs from which you can choose. It has the following fields: ➤ **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 triggered CI ➤ **Related IPs**. The IPs of the related host

2 The list of CIs are divided into pages. The number in the **Page** box indicates which page is currently being displayed.

- To view other pages, use the up and down arrows, or type the page number, and press **Enter**.
- To determine the number of CIs that appear on a page, right-click either the up or down button and select the required number. The default is 25.

3 To limit the number of triggered CIs that are displayed in the **Search Results** list, use the following filters:

- (Required) In the **By Discovery TQL** box, choose one of the following:
  - **All CIs of the CI Type.** Display all CI instances of the CI type used by the discovery pattern.
  - **TQL**. Display only CI instances that are triggered by this TQL.
- In the **Show only CIs containing** box, enter the text defining what you want to appear in the list. Only the triggered CIs that contain the text in the **Show only CIs containing** box are displayed. This step is optional.

4 Click **Search** to display only the CIs that match the filter criteria.

5 Select the required CI or CIs. You can make multiple selections.

6 Click **Add**. The discovery pattern runs using only the CIs that appear in the Triggered CIs pane.

7 To remove a triggered CI from the list of triggered CIs on which the discovery pattern runs, select the source CI you want to remove from the Triggered CIs pane and click the **Remove CI** button. The discovery pattern no longer runs using the Triggered CI you deleted from the Triggered CIs pane.

Filtering the Triggered CIs Table

You can limit the number of CIs that appear in the Triggered CIs pane.

To limit the number of CIs that appear in the Triggered CIs pane:

1 Click the **Filter CIs** button.

2 Use one of the following filters:

Filter	Description
By Status	Display a list of triggered CIs according to status. Following are the options: ➤ **All.** Display all the triggered CIs. ➤ **Waiting for Probe.** The triggered CI is ready to be dispatched and is waiting for the Discovery Probe to retrieve it. ➤ **Active.** The triggered CI is active and is running on the Discovery Probe. ➤ **Active (being removed).** The triggered CI is being removed from the **Triggered CIs** list. ➤ **Discovery Errors.** Due to an error, the Mercury Business Availability Center server has failed to dispatch the discovery task. For more information on CI statuses, see “Manually Activating a Discovery Pattern Using Specific CIs” on page 49.
By Probe	Display only the CIs triggered by a selected probe. For details, see “Selecting the Probe(s) to Be Used in the Discovery Process”.

Filter	**Description**
By Dispatch Type	Display a list of CIs according to one of the following options: ➤ **All**. CIs that were used both to manually activate the discovery pattern as well as the CIs from the Discovery TQL(s) that were used to activate the discovery pattern. ➤ **Manually added.** Only the CIs that were used to manually activate the discovery pattern. For details, see “Manually Activating a Discovery Pattern Using Specific CIs”. ➤ **By Discovery TQL**. All the CIs from the Discovery TQL(s) used to activate the discovery pattern. For details, see “Defining a Trigger TQL Query”.
By Selected TQL	Display a list of only the triggered CIs that match the output of the selected TQL. **Note:** If none of the selected CIs in the Triggered CIs pane match the output of the selected TQL, the Triggered CIs pane is empty. For details, see “Defining a Trigger TQL Query”.

Updating the Triggered CIs Table

After you have activated a discovery pattern, the CIs that are currently being used by the discovery pattern are displayed in the **Triggered CIs** pane. The discovery results are not updated automatically.

To update the list of triggered CIs currently being used by the discovery pattern:

Click the **Refresh** button on the left side of the Triggered CIs pane.

Redispatching a Triggered CI to Manually Activate the Discovery Pattern Again

You can choose to manually activate a discovery pattern again by redispatching one or more selected triggered CIs. The discovery pattern runs using only the redispatched CIs.

To redispatch a triggered CI:

1. Select one or more required CIs in the Triggered CIs table.
2. Right-click and select **Redispatch**. The discovery pattern runs again using the triggered CIs you selected.

Removing the Error Status of a Triggered CI

You can remove the error status of one or more triggered CIs in the Triggered CIs pane.

To remove the error status of one or more triggered CIs:

1. In the Triggered CI pane, select the triggered CI(s) whose error status you want to remove. You can use multiple selections.
2. Right-click or click the **Handle errors** button and select **Acknowledge error**. The status of the selected CI(s) changes to **Active**.

Note: To acknowledge the errors of all the CIs in the Triggered CIs pane, select all the CIs, right-click and select **Acknowledge error** or click the **Handle errors** button and select **Acknowledge all CIs**. The status of the selected CIs changes to **Active**.

Showing Error Details

Mercury Business Availability Center allows you to view the details of the errors that appear for the triggered CIs.

To view the details of the triggered CI:

1. In the Triggered CI pane, select the required trigger CI.
2. Click the **Handle errors** button.
3. Select **Show Error Details** to open the Error dialog box.

Note: You can also double-click the required trigger CI to open the Error dialog box.

Sorting and Customizing the Triggered CI Table

For information on how to sort and customize the Triggered CI table, see “Sorting and Customizing Tables” on page 34.

Maximizing and Restoring the Triggered CI Table

For information of how to maximize and then restore the Triggered CI table to its previous size, see “Maximizing and Restoring the Statistics Table” on page 35.

Updating the Statistics Table for the Selected Discovery Pattern

The discovery pattern results in the **Statistics** table are not automatically updated.

To update the Statistics table:

Click the **Refresh Statistics** button to the left of the **Statistics** table.

Resetting the Statistics Table for the Selected Discovery Pattern

You can delete all the statistics from the **Statistics** table and restart the counting from zero.

To reset the Statistics table:

Click the **Reset Statistics** button to the left of the Statistics table.

Sorting and Customizing the Statistic Table

For information on how to sort and customize the Statistics table, see “Sorting and Customizing Tables” on page 34.

Maximizing and Restoring the Statistic Table

For information of how to maximize and then restore the Statistics table to its previous size, see “Maximizing and Restoring the Statistics Table” on page 35.

Showing CI Instances

You can display all of the CI instances created by the discovery pattern in a table.

To display all of the CI instances created by the discovery pattern in a table:

1. Click the **View Instances** button to the left of the **Statistics** table to open the CIs discovered by pattern window.

   The list of nodes are divided into pages. The number at the bottom of the screen indicates which page is currently being displayed. For example, 2/4 means that it is the second out of four pages.

2. To view other pages, use the left and right arrows.
3. To determine the number of node instances that appear on a page, do the following:

   ➤ Click the **Set bulk size** button to open the Set bulk size dialog box.

   ➤ Use the up and down arrows or type the number of node instances you want to appear on a page and click **OK**.

4 To update the table, click the **Refresh** button.

5 Click **OK** to save the settings you have defined.

Creating a Discovery Pattern

You can create a discovery pattern. The new discovery pattern you create is based on an existing pattern.

To create a discovery pattern:

1 In the Discovery Modules pane, right-click the pattern on which you want to base your new pattern and select **Save as** to open the Choose new name for discovery pattern dialog box.

2 Enter a new name for the pattern.

3 Click **OK** to create the new pattern. The new pattern appears in the Discovery Module pane.

4 To edit the pattern, right-click it and select **Edit Pattern**. For details on how to edit the pattern, see “Editing a Pattern” on page 70.

Deleting a Discovery Pattern from a Module

This section describes how to delete a discovery pattern from a module.

To remove a discovery pattern from a module:

In the Discovery Modules pane, right-click the module you want to delete and select **Delete pattern**.

About Problem Indicators

Problem Indicators appear to the left of a module in the Modules pane if one or more of its discovery patterns are experiencing a problem that could affect the discovery process, such as a protocol connection failure.

The **Refresh All** button at bottom of the Discovery Modules pane updates all the data within the Discovery Manager dialog box, such as the list of Discovery Probes, discovery patterns and protocol information.

If the problem for which the Problem Indicators appears is due to a problem that is resolved by clicking the **Refresh All** button, the Problem Indicator disappears.

If clicking the **Refresh All** button does not solve the problem, click the **Handle errors** icon in the Triggered CIs pane to view either a solution to the problem or show details regarding the specific problem.

Discovery Process Configuration Files

Mercury Business Availability Center configuration files define default parameter values that are used for the discovery process. For example, the **portNumberToPortName.xml** file contains known port numbers, names and types that are used for TCP discovery. You can view and edit existing configuration files as well as create new ones. You can also define which text editor you want to use to edit the configuration files.

This section contains the following topics:

- "Viewing and Editing Configuration Files" on page 59
- "Creating Configuration Files" on page 61
- "Deleting Configuration Files" on page 62

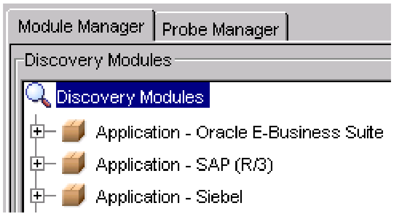
Viewing and Editing Configuration Files

This section describes how to view and edit a configuration file.

To view and edit a configuration file:

1 Click the **Module Manager** tab.

2 In the Discovery Modules pane, select the Discovery Modules root.



The Configuration Files pane is displayed.

3. Double-click the required configuration file or select it and click the **Edit Configuration File** button to open the Script Editor.
4. Make the required changes.
5. To find specific text in the Script Editor, do the following:
   - ➤ In the top left corner of the Script Editor, click the **find in text** button to open the Find dialog box.
   - ➤ In the **Text to Find** section, type the text you want to find.
   - ➤ In the **Direction** section, specify whether you want to do a forward or backward search.
   - ➤ In the **Options** section, select **Case Sensitive** if you want the matches to be case sensitive.
   - ➤ Click **Find**. If Mercury Business Availability Center finds a match, it selects the matching text.
6. To find a line in the Script Editor, do the following:
   - ➤ In the top left corner of the Script Editor, click **go to line** to open the Go to Line dialog box.
   - ➤ Type the required line number and then click **OK**. The insertion point appears to the left of the desired line.
7. Click **OK** to save the changes you have made.

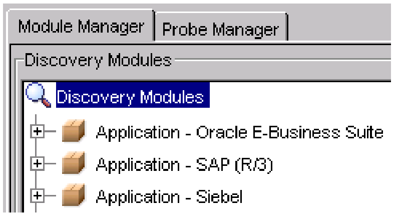
Creating Configuration Files

This section describes how to create a configuration file.

To create a configuration file:

1 Click the **Module Manager** tab.

2 In the Discovery Modules pane, select the Discovery Modules root.



The Configuration files pane is displayed.

3 Click the **Create configuration file** button to open the Choose new name for configuration file dialog box.

4 Type a name for the new configuration file and click **OK**. The new configuration file appears in the Configuration Files list with the extension **xml**.

5 Double-click the configuration file to open it.

6 Type the required text.

7 Click **OK** to save your changes.

Deleting Configuration Files

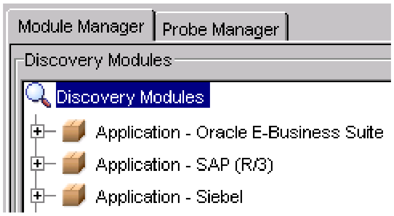
This section describes how to delete a configuration file.

Note: Only administrators with an expert knowledge of the discovery process should be allowed to delete discovery modules.

To delete a configuration file:

1 Click the **Module Manager** tab.

2 In the Discovery Modules pane, select the Discovery Modules root.

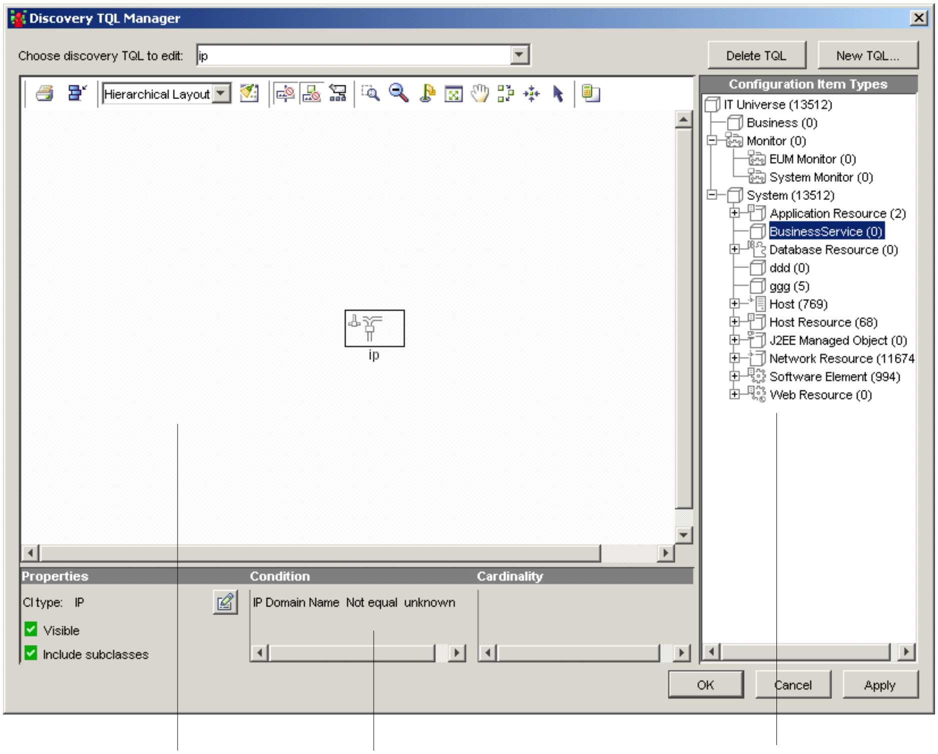


The Configuration Files pane is displayed.

3 Select the configuration file you want to delete and click the **Delete configuration file** button.

Understanding the Discovery TQL Manager

The Discovery TQL Manager allows you to define discovery TQL queries. These queries extract the information from the CMDB that is relevant to you. Once a discovery TQL query has been created, it persists in the system memory and generates updated results automatically.



Choose discovery TQL to edit: ip

Hierarchical Layout

Properties

CI type: IP

☑ Visible

☑ Include subclasses

Condition

IP Domain Name Not equal unknown

Cardinality

Editing Pane

Information Pane

Configuration Item Types

The Discovery TQL Manager is divided as follows:

- **Editing Pane.** Displays the currently selected TQL query, which consists of nodes and the relationships between them. For more information about the toolbar buttons, see “Toolbar Options” in *Working with the CMDB*.
- **Configuration Item Types.** Represents the Configuration Item Type model and contains icons for each CIT, as defined by the administrator (for details, see “Assigning an Icon to a CIT” in *CI Type Manager Administration*). By clicking and dragging CITs to the topology map and then defining the relationship between them, you can define a query and save it to the database. For example, you can drag the NT and IP CIT nodes to the topology map and then define the connection between them by adding relationships. For more information, see “Adding Nodes and Relationships to Discovery TQL Queries” on page 66.
- **Information pane.** Displays the attribute conditions you defined for the selected node/relationship. For details, see “Setting TQL Node and Relationship Definitions” on page 67.

Defining Discovery TQL Queries

You use the Discovery TQL Manager to define a new discovery TQL query. You select the nodes and relationships that are to be part of the query, and then define specific attribute conditions for each node, including the attributes of the relationships that define the connections between nodes. You can also edit or delete an existing discovery TQL.

This section has the following topics:

- “TQL Workflow” on page 65
- “Creating a Discovery TQL Query” on page 65
- “Adding Nodes and Relationships to Discovery TQL Queries” on page 66
- “Setting TQL Node and Relationship Definitions” on page 67
- “Creating a Dependency Graph” on page 68
- “Deleting a Node or Relationship” on page 68
- “Editing an Existing Discovery TQL” on page 68

- “Deleting a TQL” on page 69

TQL Workflow

You create discovery TQL queries according to the following workflow:

- Create a new discovery TQL query. For details, see “Creating a Discovery TQL Query” on page 65.
- Add nodes and relationships to the query. For details, see “Adding Nodes and Relationships to Discovery TQL Queries” on page 66.
- Define node and relationship attribute conditions. For details, see “Setting TQL Node and Relationship Definitions” on page 67.
- Create a graph that represents additional TQL query data related to a specific CI. This step is optional. For details, see “Creating a Dependency Graph” on page 68.

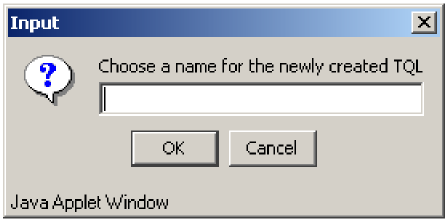
Creating a Discovery TQL Query

This section explains how to create a discovery TQL query.

To create a discovery TQL query:

1 In the Trigger TQLs pane, click the **Open Discovery TQL Manager** button to open the Discovery TQL Manager.

2 Click the **New TQL** button to open the Input dialog box.



Input

Choose a name for the newly created TQL

3 Type a unique name for the new TQL query and click **OK**. The new TQL name appears in the **Choose discovery TQL to edit** list.

Adding Nodes and Relationships to Discovery TQL Queries

Once you have created the discovery TQL query, the next step is to add the nodes and relationships that define the query. The nodes represent the CITs, as defined in the CI Type Model, and the relationships represent the connections between them. Relationships are defined one at a time for each pair of nodes in the query.

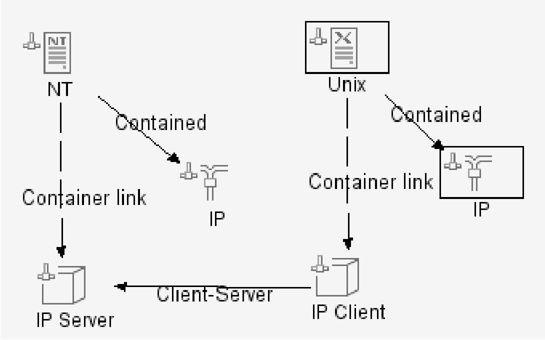
For a list of the existing relationships and their definitions, see "Relationship Definitions" in *CI Type Manager Administration*.

To add TQL nodes and relationships to a query:

1. From the **Choose discovery TQL to edit** list, select the TQL query to which you want to add TQL nodes and relationships.
2. From the tree displayed in the Configuration Item Types pane, click and drag one or more TQL nodes on to the topology map. These are the TQL nodes that are included in the query.
3. Select two TQL nodes by holding down CTRL and clicking the TQL nodes.
4. Right-click and select **Add Relationship** to open the Add Relationship dialog box.

   For details on how to add a relationship, see "Defining TQL Nodes and Relationships" in *View Manager Administration*.
5. Click **OK**. The selected nodes are linked by the relationship you have selected.

The direction of the relationship indicates which node is dependent on the other. The following example displays two hosts, an IP server, and an IP client that are linked to one another via a client/server connection.



Setting TQL Node and Relationship Definitions

After you have added the TQL nodes and relationships required for your query, you can define their specific attribute conditions.

- For details on how to define Discovery TQL nodes and relationships, see “Defining TQL Nodes and Relationships” in the *View Manager Administration*.
- For details on how to define attribute for nodes and relationships, see “Defining Attribute Conditions for Nodes and Relationships” on page 117 in the *View Manager Administration*.
- For details on how to define relationship cardinality, see “Defining Relationship Cardinality” in the *View Manager Administration*.
- For details on how to filter query results, see “Filtering Query Results in the Attribute Condition Tab” in the *View Manager Administration*.

Creating a Dependency Graph

You can create a graph that represents additional TQL query data related to a specific CI. The discovery pattern searches for the results from TQL query as well as the dependency graph definitions.

- For details on how to define a dependency graph, see "Defining a Dependency Graph" in *View Manager Administration*.
- For details on how to delete a dependency graph, see "Deleting a Dependency Definition" in *View Manager Administration*.
- For details on how to edit a dependency graph, see "Editing a Dependency Definition" in *View Manager Administration*.

Deleting a Node or Relationship

This section describes how to delete a node or relationship.

To delete a node or relationship:

1. In the Trigger TQLs pane, click the **Open Discovery TQL Manager** button to open the Discovery TQL Manager dialog box.
2. In the editing pane, right-click the TQL node or relationship you want to delete and select **Delete**.

Editing an Existing Discovery TQL

This section describes how to edit an existing TQL.

To edit an existing TQL:

1. In the Trigger TQLs pane, click the **Open Discovery TQL Manager** button to open the Discovery TQL Manager dialog box.
2. From the **Choose Discovery TQL to edit** list, choose the TQL you want to edit.
3. Make the required changes.
4. Click **OK** to save the changes you have made.

Deleting a TQL

This section describes how to delete a TQL.

To delete an existing TQL:

1. In the Trigger TQLs pane, click the **Open Discovery TQL Manager** button to open the Discovery TQL Manager dialog box.
2. From the **Choose Discovery TQL to edit** list, choose the TQL you want to delete.
3. Click the **Delete TQL** button.

Understanding the Pattern Editor

The Pattern Editor dialog box contains the following tabs and features:

- **Design View tab**. Enables you to define the following:
  - The CITs that are discovered during the discovery process.
  - The protocols that are required to perform the discovery process. For details, see "Protocol Definitions" on page 92.
- **Pattern Parameters tab**. Enables you to design and edit a discovery pattern. For details, see "Configuring a Discovery Pattern" on page 71.
- **Source View Tab**. Displays the discovery pattern in XML format, which can be edited. For details, see "Editing the Discovery Pattern" on page 74.
- **Advanced Settings**. Allows you to define advanced settings for your discovery pattern. For details, see "Defining Advanced Settings" on page 80.
- **Pattern Validation Indicator**. Indicates whether the discovery pattern is valid or not. For details, see "Discovery Pattern Validation" on page 81.

Editing a Pattern

You can edit a pattern in the Module Manager tab by accessing the Pattern Editor. The Pattern Editor allows you to either edit the pattern in XML format in the Source View tab or in the Pattern Parameters tab.

This section contains the following topics:

- "Defining the Discovery Pattern" on page 70
- "Configuring a Discovery Pattern" on page 71
- "Editing the Discovery Pattern" on page 74

Defining the Discovery Pattern

You define a discovery pattern by specifying the CITs the pattern will discover and the protocols needed to perform the discovery.

To define a discovery pattern:

1. Right-click the pattern you want to edit in the **Module Manager** tab and click **Edit Pattern**, or click the **Edit** button in the top right corner of the Discovery Pattern Summary pane to open the Pattern Editor.
2. Click the **Design View** tab.
3. In the **Discovery Pattern Version** box, enter the version of the discovery pattern you are using. This step is optional.
4. In the **Description** box, type a description of the discovery pattern.
5. In the **Trigger CIT** box, select the CIT you want to use as the trigger that activates the selected discovery pattern.
6. To define which CITs the pattern discovers, do the following:
   - In the **Discovered CITs** box, click the **Add discovered CIT** button to display the CITs in the CI Type Model pane.
   - Select the CIT or CITs you want the pattern to discover.
   - Click **OK** to save the changes you have made.
   - To delete an existing CIT from the **Discovered CITs** box, select the CIT you want to delete and click the **Remove discovered CIT** button.

7 To define which protocols the pattern requires for the discovery task, do the following:

- ➤ In the **Required Discovery Protocols** box, click the **Add required protocol** button to open the Add Required Protocol dialog box.
- ➤ From the **Choose Protocol Type** list, select the required protocol.
- ➤ Click **OK** to save the changes you have made.
- ➤ To delete an existing protocol from the **Required Discovery Protocols** box, select the protocol you want to delete and click the **Remove required protocol** button.

8 In the **Discovery Scheduler** section, you can schedule a discovery pattern to run on a periodic basis. Select the **Invoke on New Triggered CIs immediately** check box to run the discovery pattern as soon as the triggered CI reaches the Discovery Probe.

For details on how to schedule a discovery pattern to run on a periodic basis, see “Scheduling a Discovery Pattern to Run on a Periodic Basis” on page 75.

Configuring a Discovery Pattern

This section describes how to configure parameters for a discovery pattern.

To configure a discovery pattern:

1 Right-click the pattern you want to configure in the **Module Manager** tab and click **Edit Pattern**, or click the **Edit** button in the top right corner of the Discovery Pattern Summary pane.

2 Click the **Pattern Parameters** tab.

3 In the **Discovery Pattern Parameters** section, define the following parameter values:

- **Parameter name.** The name of the parameter.
- **Value.** The value you want to assign to the attribute.
- **Description.** Description of the parameter (optional).

Note: Each row represents the definitions for one parameter.

- To define another pattern parameter, click the **Add Parameter** button. Another row of parameter attribute definitions appears. Configure the parameters according to the list above.
- To delete a pattern parameter, select the parameter you want to delete and click the **Remove Parameter** button.

4 In the **Triggered CI Data** section, define the information that is needed to perform a discovery task on a specific CI. That information is passed to the CI queried in the discovery task.

To configure the triggered CI, do the following:

➤ Define the triggered CI's attributes according to the following table:

Attribute	**Description**
Attribute name	The name of the attribute.
Value	The attribute value. Variables are written using the following syntax: ${VARIABLE_NAME.attributeName} where <**VARIABLE_NAME** > can either be one of three predefined variables: ➤ **Source**. Refers to the CI that functions as the task's trigger. ➤ **Host**. Host in which the triggered CI is contained. ➤ **Parameters**. This variable refers to the parameter defined in the **Parameter** section as described above. or a variable that you have created. For example: ${SOURCE.network_netaddr} indicates that the triggered CI is a network.
Encrypted	Select this check box if the field is defined as a Password type in the CMDB.

➤ To define another attribute, click the **Add Triggered CI Data** button, and modify the attribute according to the table above.

➤ To delete an existing attribute, select the attribute you want to delete and click the **Remove Triggered CI Data** button.

Editing the Discovery Pattern

The **Source View** tab displays the discovery pattern in XML format, which can be edited.

To edit the discovery pattern in the Source View tab:

1. Right-click the pattern you want to edit in the **Module Manager** tab and click **Edit Pattern**, or double-click the pattern to open the Pattern Editor.
2. Click the **Source View** tab.
3. Make the required changes.
4. To find specific text in the Script Editor, click the **find in text** button. For details, see “Viewing and Editing Configuration Files” on page 59.
5. To find a line in the Script Editor, click the **go to line** button. For details, see “Viewing and Editing Configuration Files” on page 59.
6. Click **Save** to save the changes you have made.
7. The **Discovery Scripts** pane at the bottom contains a list of Jython scripts used by the discovery patterns. Jython is a Java implementation of the Python language, allowing python code to access Java classes. The Jython scripts that appear in bold are the scripts that the currently selected pattern is using. To edit the Jython scripts, do the following:
   - ➤ Select the Jython script you want to edit.
   - ➤ Click the **Edit Script** button to open the Script Editor window.
   - ➤ To find specific text, find a specific line, see “Viewing and Editing Configuration Files” on page 59.
   - ➤ Edit the script as required.
   - ➤ Click **OK** to save the changes you have made.

Scheduling a Discovery Pattern to Run on a Periodic Basis

This section explains how to set the schedule for activating a discovery pattern. It has the following topics:

- "Setting the Date for Starting and Stopping a Discovery Pattern" on page 75
- "Running a Discovery Pattern on a Periodic Basis" on page 76
- "Running a Discovery Pattern at Set Time Intervals" on page 77
- "Running a Discovery Pattern on a Daily Basis" on page 77
- "Running a Discovery Pattern on a Weekly Basis" on page 78
- "Running a Discovery Pattern on a Monthly Basis" on page 78

Setting the Date for Starting and Stopping a Discovery Pattern

This section describes how to set the date for starting and stopping a discovery pattern.

To set the date for starting and stopping a discovery pattern:

1 In the **Module Manager** tab, right-click the pattern or patterns you want to run on a periodic basis and click **Edit Pattern**, or click the **Edit** button in the top right corner of the Discovery Pattern Summary pane to open the Pattern Editor.

Note: You can set the date for more than one pattern at a time by holding the CTRL key down to make multiple time selections.

---

2 Click the **Design View** tab.

3 In the **Discovery Scheduler** section, click **Edit Scheduler** to open the Schedule dialog box.

4 To set the date for activating the discovery pattern, click the down button in the **Start on** box to display a calendar.

5 Use the diagonal arrow buttons to choose the month and year, and then click the required day.

6 Click anywhere outside the calendar to close it.

7 To delete the date you entered in the **Start on** box, click **Reset**.

Running a Discovery Pattern on a Periodic Basis

This section describes how to run a discovery pattern on a periodic basis.

To run a discovery pattern on a periodic basis:

1 Right-click the pattern you want to run on a periodic basis in the **Module Manager** tab and click **Edit Pattern**, or click the **Edit** button in the top right corner of the Discovery Pattern Summary pane to open the Pattern Editor.

2 Click the **Design View** tab.

3 In the **Discovery Scheduler** section, click **Edit Scheduler** to open the Schedule dialog box.

4 Select one of the following options:

- ➤ **Interval.** Activates the discovery pattern at a predefined time interval. For details, see “Running a Discovery Pattern at Set Time Intervals” on page 77.
- ➤ **Daily**. Activates the discovery pattern on a daily basis. For details, see “Running a Discovery Pattern on a Daily Basis” on page 77.
- ➤ **Weekly**. Activates the discovery pattern on a weekly basis. For details, see see “Running a Discovery Pattern on a Weekly Basis” on page 78.
- ➤ **Monthly**. Activates the discovery pattern on a monthly basis. For details, see “Running a Discovery Pattern on a Monthly Basis” on page 78.

5 Click **OK** to save the settings you have defined. The discovery schedule you have defined appears in the **Discovery Scheduler** section.

Running a Discovery Pattern at Set Time Intervals

This section describes how to run a discovery pattern at a predefined time interval.

To run a discovery pattern at a predefined time interval:

1. Select **Interval** in the Discovery Scheduler dialog box (see step 4 in "Running a Discovery Pattern on a Periodic Basis" on page 76), and then select the date on which you want to activate the pattern. For details, see "Setting the Date for Starting and Stopping a Discovery Pattern" on page 75.
2. In the **Repeat Every** boxes, do the following:
   - ➤ Type or select a value for the interval between successive runs.
   - ➤ Choose the required unit of time measurement (**seconds**, **minutes**, **hours**).
3. Choose the time and date for the task to end (for details, see "Setting the Date for Starting and Stopping a Discovery Pattern" on page 75).
4. Click **OK** to save the settings you have defined.

Running a Discovery Pattern on a Daily Basis

This section describes how to run a discovery pattern on a daily basis.

To run a discovery pattern on a daily basis:

1. Select **Daily** in the Discovery Scheduler dialog box (see step 4 in "Running a Discovery Pattern on a Periodic Basis" on page 76), and then select the date on which you want to activate the pattern. For details, see "Setting the Date for Starting and Stopping a Discovery Pattern" on page 75.
2. From the **Every day at hour** list, select the required time or times.

Note: Hold the CTRL key down to make multiple time selections.

3. In the **Discovery Time Limitations** section, choose the date and time you want the task to stop running. For details, see "Setting the Date for Starting and Stopping a Discovery Pattern" on page 75.

4 Click **OK** to save the settings you have defined.

Running a Discovery Pattern on a Weekly Basis

This section describes how to run a discovery pattern on a weekly basis.

To run a discovery pattern on a weekly basis:

1 Select **Weekly** in the Discovery Scheduler dialog box (see step 4 in “Running a Discovery Pattern on a Periodic Basis” on page 76), and then select the date on which you want to activate the pattern. For details, see “Setting the Date for Starting and Stopping a Discovery Pattern” on page 75.

2 From the **Start hour** list, select the hour or hours at which you want the task to run.

Note: You can hold the CTRL key down to make multiple time selections.

3 In the **Days of week** section, select the day or days of the week on which you want the task to run.

4 In the **Discovery Time Limitations** section, choose the date and time you want the task to stop running. For details, see “Setting the Date for Starting and Stopping a Discovery Pattern” on page 75.

5 Click **OK** to save the settings you have defined.

Running a Discovery Pattern on a Monthly Basis

This section describes how to run a discovery pattern on a monthly basis.

To run a discovery pattern on a monthly basis:

1 Select **Monthly** in the Discovery Scheduler dialog box (see step 4 in “Running a Discovery Pattern on a Periodic Basis” on page 76), and then select the date on which you want to activate the pattern. For details, see “Setting the Date for Starting and Stopping a Discovery Pattern” on page 75.

2 From the **Start hour** list, select the hour or hours at which you want the task to run.

Note: You can hold the CTRL key down to make multiple time selections.

---

3. In the **Days of month** box, click the **Add the required day of the month** button to specify the day or days of the month on which you want the pattern to run. The Add Required Day dialog box opens.
4. From the **Choose a day** list, select required day in the month and click **OK**. The day you selected appears in the **Days of the month** box. You can repeat this step to select as many days as you want.
5. To delete a day from the **Days of month** box, select the required day and click the **Delete the required day of the month** button.
6. In the **Discovery Time Limitations** section, choose the date and time you want the task to stop running. For details, see “Setting the Date for Starting and Stopping a Discovery Pattern” on page 75.
7. Click **OK** to save the settings you have defined.
8. To choose when you want the discovery pattern to stop, do one of the following:
    - If you do not want to specify an ending date, select **No time limitations**.
    - To set the pattern to stop after it has been activated a specific number of times, select **End after** and then enter or choose the required number from the **recurrences** list (maximum is 1000).
    - To choose the date and time for when you want the discovery task to stop, select **End by**, and do the following:
        - Click the down button to display a calendar.
        - In the **Date** and **Time** tabs, use the diagonal arrow buttons to choose the date and time.
        - Click anywhere outside the calendar to close it.

Defining Advanced Settings

You can define advanced settings for your discovery pattern.

To define advanced settings for the discovery pattern:

1. In the Discovery Modules pane, right-click the required pattern and select **Edit Pattern** to open the Pattern Editor.
2. Click the **Design View** tab.
3. Click **Advanced Settings** to open the Advanced Settings dialog box.
4. In the Task Management section, do the following:

   ➤ Select **Merge** if you want a task to include several Triggered CIs rather than only one triggered CI per task. The default is selected.

   ➤ Select **Enforce Dispatch** if you want to invoke a task for CIs whose Discovery Probe is not included in the discovery scope you define in the Probe Manager tab (see "Adding a Discovery Probe" on page 36). The default is not selected.

   ➤ If a CI that acted as a trigger for a discovery pattern was deleted from the database, select **Deletable** if you want the discovery task it activated to be deleted as well. The default is not selected.

5. By default, the Discovery Manager chooses the Discovery Probe for the triggered CI automatically according to the CI's related host. After obtaining the CI's related host, the system chooses one of the host's IPs and chooses the Discovery Probe according to the probe's network scope definitions (see "Adding a Discovery Probe" on page 36).

   This might fail in the following situations:

   ➤ A triggered CI does not have a related host (such as the **network** CIT).

   ➤ A triggered CI's host has multiple IPs, each belonging to different Discovery Probe.

   To resolve these issues, you can specify which Discovery Probe to use with the discovery pattern by doing the following:

   ➤ In the Probe Selection section, select **Override default probe selection**.

   ➤ In the Probe box, enter the Discovery Probe you want to use for the discovery task.

6 In the Result Grouping section:

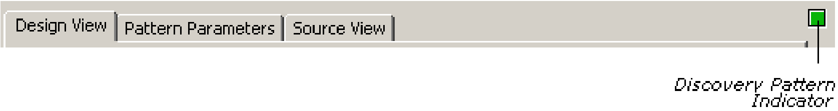
- Select **Group Results** if you want to group discovery results in the Discovery Probe before being sent to the Mercury Business Availability Center server.
  - In the Grouping Interval (Seconds) box, type the value that indicates how long discovery results are stored in the Discovery Probe before being transferred to the Mercury Business Availability Center server.
  - In the Group Max CIs box, specify the number of CIs that should accumulate in the Discovery Probe before being transferred to the Mercury Business Availability Center server.

Note: If you entered a value in both fields, Mercury Business Availability Center applies whichever occurs first.

- If you do not select Group Results, all discovery results are immediately sent to the Mercury Business Availability Center server.
- Click **OK** to save the changes you have made.

Discovery Pattern Validation

The Discovery Pattern Indicator indicates whether the selected discovery pattern is valid or not. It can be either green or red.



- Green indicates that the pattern is valid.
- Red indicates that the pattern is not valid. To display a description of the problem, move the pointer over the **Discovery Pattern** Indicator.

Activating a Discovery Pattern

You can choose to activate either all the discovery patterns in a discovery module or some of them.

To activate discovery patterns in a module:

1. Select **Admin** > **CMDB** and select the **Discovery Manager** tab.
2. In the Discovery Modules area, click the **Expand** button of the module whose discovery pattern you want to activate.
3. Right-click the module you want to activate and click the **Activate** button, or select the required module and click the **Activate** button in the bottom right corner of the Discovery Modules pane.

   A pattern that is activated, as seen here, is marked with a green dot.

Note: If only some of the module's patterns are activated, the module is marked with a single, green dot. If all patterns of the module are activated, the module is marked with three green dots.

Deactivating a Discovery Pattern

This section describes how to deactivate a discovery pattern that is being used in the discovery process.

To deactivate a discovery pattern that is being used in the discovery process:

1. Select **Admin** > **CMDB** and click the **Discovery Manager** tab.
2. Click the **Expand** button of the module whose discovery pattern you want to deactivate.
3. In the **Discovery Modules** area, right-click the pattern you want to deactivate and click the **Deactivate** button, or select the required pattern and click the **Deactivate** button in the bottom right corner of the Discovery Modules pane.

Understanding the Discovery Manager Map View Tab

The Mercury Business Availability Center discovery process is run by activating discovery patterns.

Each pattern contains a description of the CITs and relationships that are created with each discovery pattern. The definitions of the CITs and relationships are taken from the CI Type Manager (for details, see *CI Type Manager Administration* which contains the definitions of all CITs and relationships). When the discovery module is activated, it discovers CITs and relationships of the types that are described in each pattern, and places them in the CMDB.

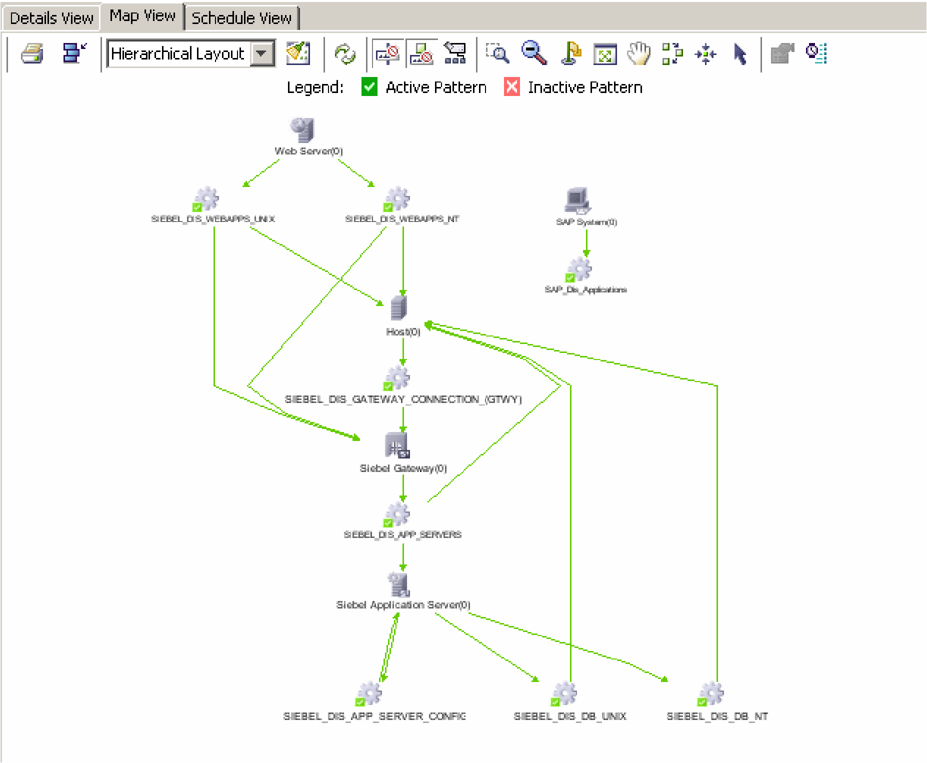
The discovered CIs act as triggers that activate another discovery pattern. Every time a discovery pattern is activated, it discovers more CIs, which in turn are used as triggers for other discovery patterns.

The Map View tab displays a visual representation of the real-time progress of the discovery process. It displays which CIs triggered which discovery pattern (trigger or input CIs), as well as which CIs that were discovered as a result of the activated discovery pattern (triggered or output CIs).

The Map View tab also displays other information, such as how many instances of a specific CI are contained in the CMDB and how many instances were created by a specific discovery pattern.

To display the Map View:

Click the **Module Manager** tab and then click the **Map View** tab.



Map View displays the real-time progress of a discovery pattern. Selecting a discovery pattern, either in the Discovery Modules pane or the Map View, simultaneously selects that pattern in both places.

This section includes the following topics:

- “Using the Map View Tab Toolbar” on page 85
- “Displaying Data in the Discovery Map View” on page 85
- “Understanding Items in the Discovery Map View” on page 87
- “Understanding Statistics in the Map View” on page 88
- “Understanding Map View Tooltips” on page 90

- “Using the Toolbar Options” on page 90
- “Printing the Contents of the Map View Tab” on page 90
- “Understanding Layout Options” on page 90

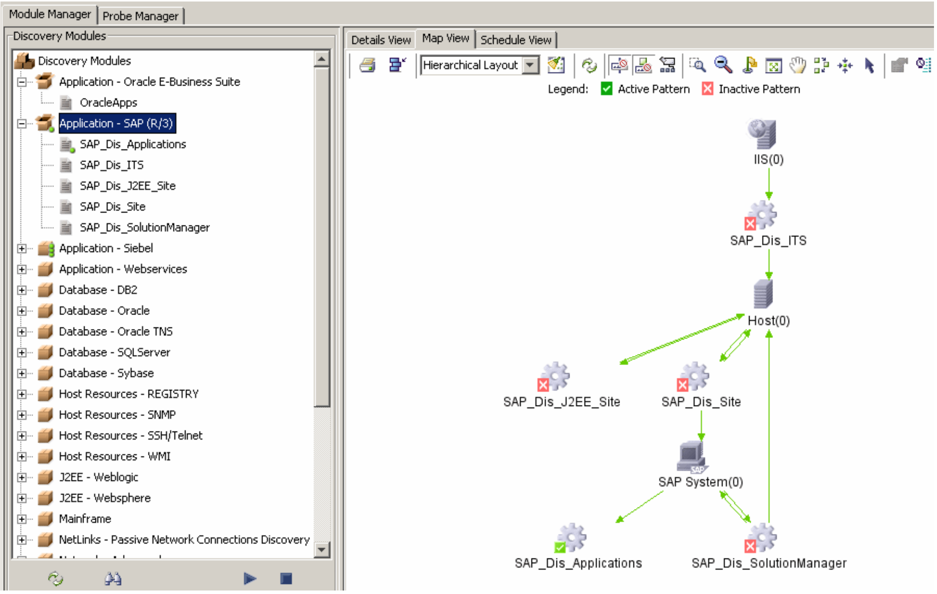
Using the Map View Tab Toolbar

For a description of the toolbar options in the Map View tab, see “Toolbar Options” in *Working with the CMDB*.

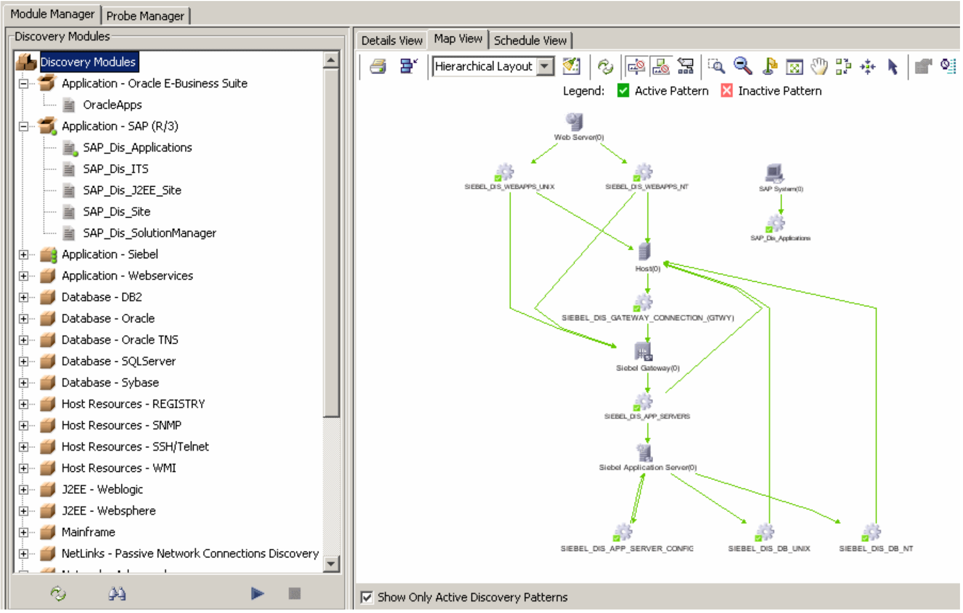
Displaying Data in the Discovery Map View

The Discovery Map View displays data according to the selection in the Discovery Modules pane.

- When you select a module in the Discovery Modules pane, the map view displays the module’s active and inactive patterns, as displayed by the following illustration:



➤ When you select the Discovery Modules root at the top of the Modules pane, and select the **Show only active discovery patterns** check box at the bottom, the map view displays only the active discovery patterns from the modules and the input/output CITs, as seen in the illustration below:

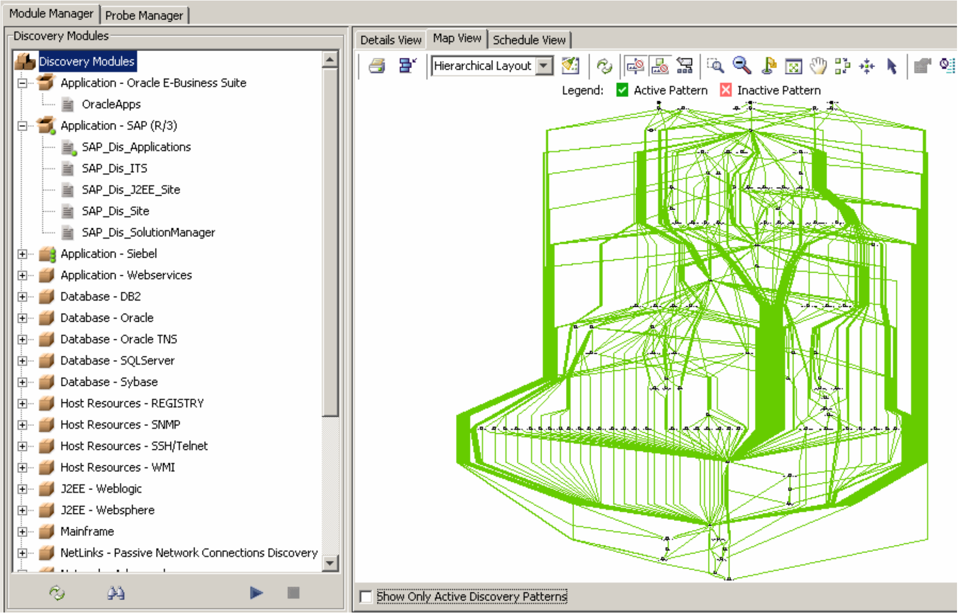


- Discovery Modules
  - Application - Oracle E-Business Suite
    - OracleApps
  - Application - SAP (R/3)
    - SAP_Dis_Applications
    - SAP_Dis_ITS
    - SAP_Dis_J2EE_Site
    - SAP_Dis_Site
    - SAP_Dis_SolutionManager
  - Application - Siebel
  - Application - Webservices
  - Database - DB2
  - Database - Oracle
  - Database - Oracle TNS
  - Database - SQLServer
  - Database - Sybase
  - Host Resources - REGISTRY
  - Host Resources - SNMP
  - Host Resources - SSH/Telnet
  - Host Resources - WMI
  - J2EE - Weblogic
  - J2EE - Websphere
  - Mainframe
  - NetLinks - Passive Network Connections Discovery

☑ Show Only Active Discovery Patterns

Note: If there are no active patterns, the Map View tab is empty.

➤ When you select the Discovery Modules root at the top of the Modules pane, and clear the **Show only active discovery patterns** check box at the bottom, the map view displays all discovery patterns from the modules and their interdependencies, as seen in the illustration below:



Legend: ✓ Active Pattern ☒ Inactive Pattern

□ Show Only Active Discovery Patterns

Understanding Items in the Discovery Map View

The following table describes the items in the Map View and what they represent:

Item	Description
☒	An inactive pattern.
✓	An active pattern.

Note: You can edit a discovery pattern by double-clicking it to open the Pattern Editor. For details, see "Understanding the Pattern Editor" on page 69.

Understanding Statistics in the Map View

The Map View tab displays the following statistics on discovery results for the selected pattern:

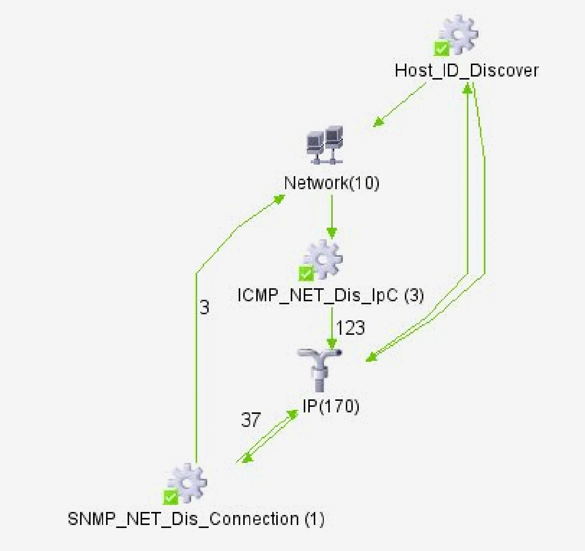
- The number of instances of a specific CI in the CMDB.

Note: You can also find the same statistical number in the Created column in the Statistics table in the Details View pane. For details, see "Using Advanced Options in the Details View Pane" on page 43.

- The number of CI instances that were created by a specific pattern.
- The number of triggered CIs currently being used by a discovery pattern to run the discovery pattern.

Note: You can also find the same statistical number at the bottom right corner of the Triggered CI pane. For example 25 out of 90 means that 90 triggered CIs are being used for the discovery pattern.

The following example displays the following statistics:



- The discovery pattern **SNMP_NET_Dis_Connection** created 37 instances of **IP** CIs.
- The discovery pattern **SNMP_NET_Dis_Connection** created 3 instances of **Network** CIs.
- There are 10 instances of **Network** CIs in the CMDB.
- There are 170 instances of **IP** CIs in the CMDB.
- The discovery pattern **ICMP_NET_Dis_IpC** is using 3 triggered CI to run the discovery pattern.
- The discovery pattern **SNMP_NET_Dis_Connection** is using 1 triggered CI to run the discovery pattern.

Note: To update the statistics in the Map View, click the **Refresh** button (for details, see “Using the Map View Tab Toolbar” on page 85).

Understanding Map View Tooltips

When the pointer is moved over either a CI or discovery pattern, a tooltip displays the description.

Using the Toolbar Options

For a description of each toolbar option in the Map View tab, see "Toolbar Options" in *Working with the CMDB*.

Printing the Contents of the Map View Tab

You can print the contents of the Map View tab. The result is similar to a screen capture. Therefore, it is recommended to arrange the contents of the map view according to your requirements before printing. For details, see "Printing the Topology Map" in *Working with the CMDB*.

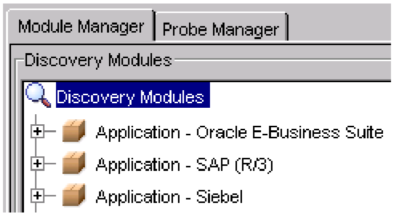
Understanding Layout Options

For a description of how you can display the contents of the topology map in the Map View tab using different layout options, see "Defining a View's Layout" in *Working with the CMDB*.

Understanding the Schedule View Tab

The Schedule View tab displays all discovery pattern scheduling information in one table.

➤ When you select the Discovery Modules root in the Discovery Modules pane (see the picture below), the Schedule View tab displays scheduling information for only the active patterns.

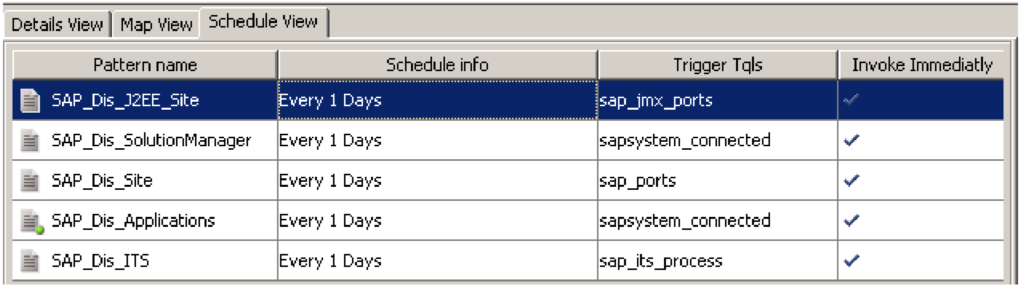


- When you select a module or a pattern in a module, the Schedule View tab displays scheduling information for the patterns in the selected module.

To view the Schedule View tab:

1 Click the **Module Manager** tab.

2 Click the **Schedule View** tab to view the **Schedule View** table.



Pattern name	Schedule info	Trigger Tqls	Invoke Immediatly
SAP_Dis_J2EE_Site	Every 1 Days	sap_jmx_ports	✓
SAP_Dis_SolutionManager	Every 1 Days	sapsystem_connected	✓
SAP_Dis_Site	Every 1 Days	sap_ports	✓
SAP_Dis_Applications	Every 1 Days	sapsystem_connected	✓
SAP_Dis_ITS	Every 1 Days	sap_its_process	✓

The **Schedule View** table is divided as follows:

Field	Description
Pattern Name	The name of the discovery pattern.
Schedule info	The scheduling information of the discovery pattern as defined in Discovery Scheduler. For details, see “Setting the Date for Starting and Stopping a Discovery Pattern” on page 75.
Trigger Tqls	The name of the TQL that activated the discovery pattern.
Invoke Immediately	The options for this field are as follows: ➤ If this column contains a check, the discovery pattern runs as soon as the triggered CI reaches the Discovery Probe. In this case, the **Invoke on new triggered CIs immediately** check box is selected in the Design View tab of the Pattern Editor. For details, see “Defining the Discovery Pattern” on page 70. ➤ If this column does not contain a check, the pattern runs according to the patterns schedule as defined in the Pattern Editor. For details, see “Defining the Discovery Pattern” on page 70.

Protocol Definitions

This section contains the definitions that are needed for Mercury Business Availability Center protocols.

Protocol	Parameter	Description
JBOSS Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the JBoss application server.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Port Number	The port number.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	User Name	The user name.
	User Password	The user password.

Protocol	**Parameter**	**Description**
NTCMD Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the NTCMD server.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	NT Domain	The Microsoft domain.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	User Name	The user name.
	User Password	The user password.

Protocol	Parameter	Description
SAP JMX Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the SAP JMX console.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Port Number	The port number of JMX.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	User Name	The user name.
	User Password	The user password.

Protocol	**Parameter**	**Description**
SAP Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the SAP server.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	Sap Client	An independent unit within the R/3 system, which is identified by a three-digit number.
	Sap Router String	A string that contains the host and port of the SAP router.
	Sap System Number	An unique identifier of SAP system.

Protocol	**Parameter**	**Description**
Siebel Gateway Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the Siebel gateway.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	Siebel Site Name	The name of the Siebel site.
	srvrmgr path	The directory in which the **srvr.exe** file is located.
	User Name	The user name.

Protocol	Parameter	Description
SNMP Protocol	Community	(For SNMP v1 and SNMP v2 only) Enter the password you used when connecting to the SNMP service community you defined while configuring the SNMP service (for example, a community for read-only or read/write).
	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the SNMP agent.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Port Number	(For SNMP versions v1, v2, and v3) The port number on which the SNMP agent listens.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	Retry	The number of times the Discovery Probe tries to connect to the SNMP agent. If the number is exceeded, the Discovery Probe stops attempting to make the connection.
	SNMP version	The options are: ➤ version 1 or 2 ➤ version 3
	User Name	(For SNMP v3 only) The name of the user authorized to log on to the management application.

Protocol	Parameter	Description
	User Password	(For SNMP v3 only) The password used to log on to the management application.
	V3 – Authentication algorithm	(For SNMP v3 only) Two algorithms are supported: ➤ MD5 ➤ SHA

Protocol	Parameter	Description
	V3 – Authentication method	(For SNMP v3 only) Select one of the following options for securing the access to management information: ➤ **NoAuthNoPriv.** Using this option provides no security, confidentiality, or privacy at all. It might 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).

Protocol	Parameter	Description
	V3 – Privacy algorithm	(For SNMP v3 only) The following algorithm is supported: DES.
	V3 – Privacy key	(For SNMP v3 only) The secrete key used to encrypt the scoped PDU portion in an SNMP v3 message.
SQL Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the database.
	Database Name	The database name.
	Database SID (Oracle, DB2)	The database SID.
	Database Type	The database type, such as Oracle and Microsoft SQL Server.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Port Number	The port number on which the database listens.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	User Name	The user name.
	User Password	The user password.

Protocol	**Parameter**	**Description**
SSH Protocol	Authentication Mode	These are the following authentication options: ➤ Password ➤ Key ➤ Keyboard Interactive
	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the remote machine.
	Key Path	Location of the authentication key.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Port Number	The port number.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	User Name	The user name.
	User Password	The user password.

Protocol	Parameter	Description
Telnet Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the remote machine.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Port Number	The port number.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	User Name	The user name.
	User Password	The user password.

Protocol	**Parameter**	**Description**
Uddi Registry Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the UDDI Registry.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	Publishing Organization	The name of the service publisher whose services you want to publish.
	UDDI inquiry URL	The URL where the UDDI Registry is located.

Protocol	**Parameter**	**Description**
WebLogic Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the WebLogic application server.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Port Number	The port number.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	User Name	The user name.
	User Password	The user password.

Protocol	Parameter	Description
Websphere Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the WebSphere server.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	Port Number	The port number.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	Trust Store	The location of SSL trust store file.
	Trust Store Password	The SSL trust store password.
	User Name	The user name.
	User Password	The user password.

Protocol	Parameter	Description
WMI Protocol	Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the WMI agent.
	Network Address	The discovered IP net address or the net address range.
	Note	A textual message.
	NT Domain	Microsoft domain.
	Protocol Index	Indicates the order in which protocol instances will be used to make a connection attempt. The lower the index is the higher the priority it has. The default is 9999. If you do not change the default, this protocol instance will be used last.
	User Name	The user name.
	User Password	The user password.

Part V

Performing Specific Discoveries

5

Performing a SAP Discovery

The SAP discovery process enables you to discover SAP elements and SAP topology.

This chapter describes:	On page:
Step 1 – Installing the Java Connectors	110
Step 2 – Preparing for a SAP Discovery	110
Step 3 – Adding a Network CI to Trigger the Discovery of SAP System Networking	113
Step 4 – Accessing the Discovery Modules	113
Step 5 – Running the Discovery Patterns	115
Step 6 – Checking that the Discovery Ran Correctly	124
Step 7 – Running SAP Solution Manager Discovery	125
CIs Created by the Discovery Process	126

Note: For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

Step 1 – Installing the Java Connectors

Step 1 is a prerequisite to the other steps. Steps 2 to 5 discover different SAP elements and different parts of SAP topology.

Before you run a SAP discovery, you install the Java connectors, if you have not already done so. For details, see "Step 3 – Performing the Discovery Probe Post-Installation Procedure" on page 275.

Step 2 – Preparing for a SAP Discovery

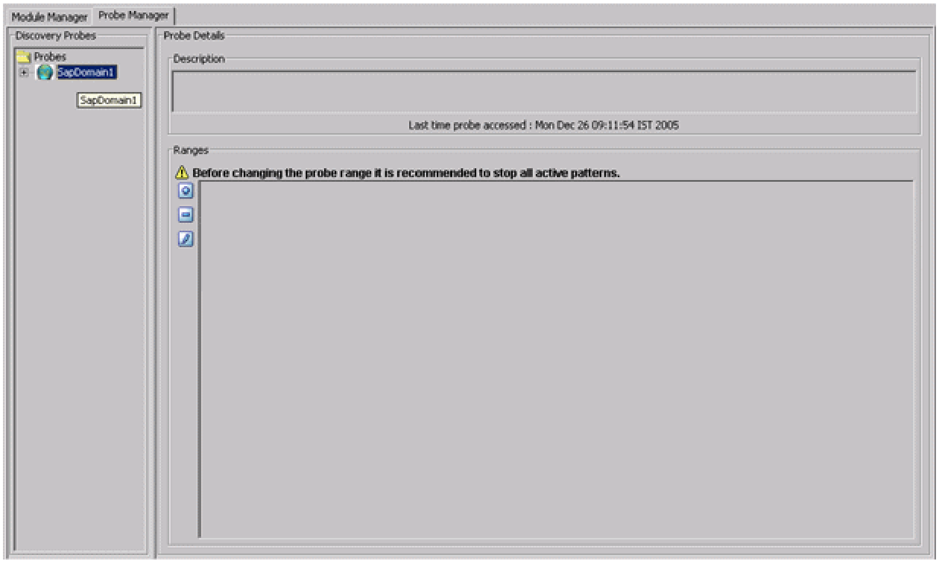
Before you run a SAP discovery, you must add a discovery probe and define the protocols as indicated in this section.

Note: Ensure that the Discovery Probe is running.

To prepare for a SAP discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the Probe Manager pane.

4 In the Discovery Probes pane, select the relevant Discovery Probe.



Last time probe accessed : Mon Dec 26 09:11:54 IST 2005

⚠ **Before changing the probe range it is recommended to stop all active patterns.**

5 Click the **Add IP Range** button to open the Add IP Range window.

6 Enter the range of IP addresses that includes the IP address of the probe you want to discover. If there is only one address, enter its value in both boxes.

7 Click **OK**.

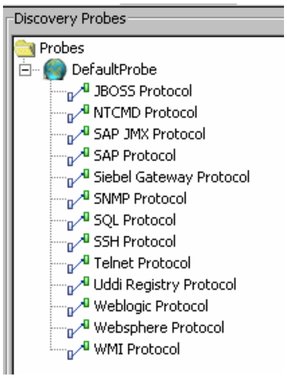
8 Click the **Add IP Range** button to open the Add Range window once more.

9 Enter the range of IP addresses that includes the IP address of the SAP system you want to discover. If there is only one address, enter its value in both boxes.

10 Click **OK**.

11 Click **Apply** to save the changes you have made.

12 Expand the appropriate Discovery Probe:



Discovery Probes

- Probes
- DefaultProbe
  - JBOSS Protocol
  - NTCMD Protocol
  - SAP JMX Protocol
  - SAP Protocol
  - Siebel Gateway Protocol
  - SNMP Protocol
  - SQL Protocol
  - SSH Protocol
  - Telnet Protocol
  - Uddi Registry Protocol
  - Weblogic Protocol
  - Websphere Protocol
  - WMI Protocol

13 Define the following protocols:

- ➤ Select **SNMP Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following field:
  - ➤ **Community.** Enter the password you used when connecting to the SNMP service community you defined while configuring the SNMP service (for example, a community for read-only or read/write).
- ➤ Select **WMI Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:
  - ➤ **NT Domain.** The name of the host where the Discovery Probe is installed.
  - ➤ **User Name.** The name of the user you use to connect to the host as administrator.
  - ➤ **User Password.** The password of the user you use to connect to the host as administrator.
- ➤ Select **NTCMD Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:
  - ➤ **NT Domain.** The name of the host where the Discovery Probe is installed.
  - ➤ **User Name.** The name of the user you use to connect to the host as administrator.

- **User Password.** The password of the user you use to connect to the host as administrator.

- Select **SAP Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:

  - **SAP Client.** The default value is 800. It is recommended to use the default value.

  - **SAP System Number.** The default value is 00. It is recommended to use the default value.

  - **User Name.** The name of the user you use to log on to the SAP system.

  - **User Password.** The password of the user you use to log on to the SAP system.

Note: If you want to discover more than one SAP System, it is recommended to create a SAP Protocol for each SAP system with different users and passwords.

---

14 Click **Apply** to save the changes.

Step 3 – Adding a Network CI to Trigger the Discovery of SAP System Networking

To trigger the discovery of SAP System networking features, you must add a Network CI to the CMDB.

To add a Network CI to trigger a discovery of SAP System networking:

1. To add the **Network** CI, access the New CI Wizard.
2. Select **Display all possible CITs**.
3. Expand **System**, expand **Network Resource**, and select **Network.**
4. Click **OK** to open the Define General Properties page, and then click **Next** to open the Define CIT-Specific Properties page.

5 Enter the following information:

- ➤ In the **Network Domain Name** box, enter the name of the domain that was specified during SAP installation.
- ➤ In the **Network Mask** box, enter the mask for the IP address of the SAP System network.
- ➤ In the **Network Address** box, enter the IP address of the SAP System network.

If the Network CI was added successfully, you get the following message: Network CI was added successfully.

6 Click **Finish**:

For details about this procedure, see "Using the New CI Wizard" in *IT Universe Manager Administration*.

Step 4 – Accessing the Discovery Modules

Access the discovery modules and activate the appropriate discovery patterns.

For details on how to activate a discovery pattern, see *Discovery Manager Administration*.

To access the discovery modules:

1 Click the **Discovery Manager** tab in CMDB Administration.

2 Click the **Module Manager** tab.

Step 5 – Running the Discovery Patterns

To run the discovery patterns, you must trigger them in the order described in this section. Each discovery pattern discovers different components. For details on the components and their hierarchy structure, see "CIs Created by the Discovery Process" on page 126.

This section includes the following topics:

- "Running the Discovery" on page 115
- "Selecting the Discovery Modes for Discovering Application Components, SAP Transactions, and Transports" on page 118

Running the Discovery

This section describes how to run the discovery.

To run the discovery:

In the Module Manager tab, expand the modules, select the patterns, and activate them:

Expand Module	Activate Pattern	Description
Network – Basic	**ICMP_NET_Dis_IpC**	Discover which machines are active by pinging the machines within the range of given IP addresses that you provided in "Step 2 – Preparing for a SAP Discovery" on page 110.

Expand Module	Activate Pattern	Description
Network – Protocol Connections	**SNMP_NET_Dis_ Connection**	Discovers, in the range of given IP addresses, the hosts that communicate using the SNMP protocol.
	NTCMD_NET_Dis_ Connection	Discovers, in the range of given IP addresses, the hosts that communicate using the NTCMD protocol.
	WMI_NET_Dis_Connection	Discovers, in the range of given IP addresses, the hosts that communicate using the WMI protocol.
Host Resources – WMI	**WMI_HR_Process**	Discovers the processes that are running on the server. If the SAP system you are discovering has an ITS configuration and you want to discover the ITS entities of the SAP system, run this pattern as a prerequisite to the SAP discovery that discovers ITS entities.
Network – Advanced	**TCP_NET_Dis_Port**	Discovers the server's open active ports.
Web Servers – Basic	**TCP_Webserver_Detection**	Discovers the Web servers running on this host. If the SAP system you are discovering has an ITS configuration and you want to discover the ITS entities of the SAP system, run this pattern as a pre requisite to the SAP discovery that discovers ITS entities.

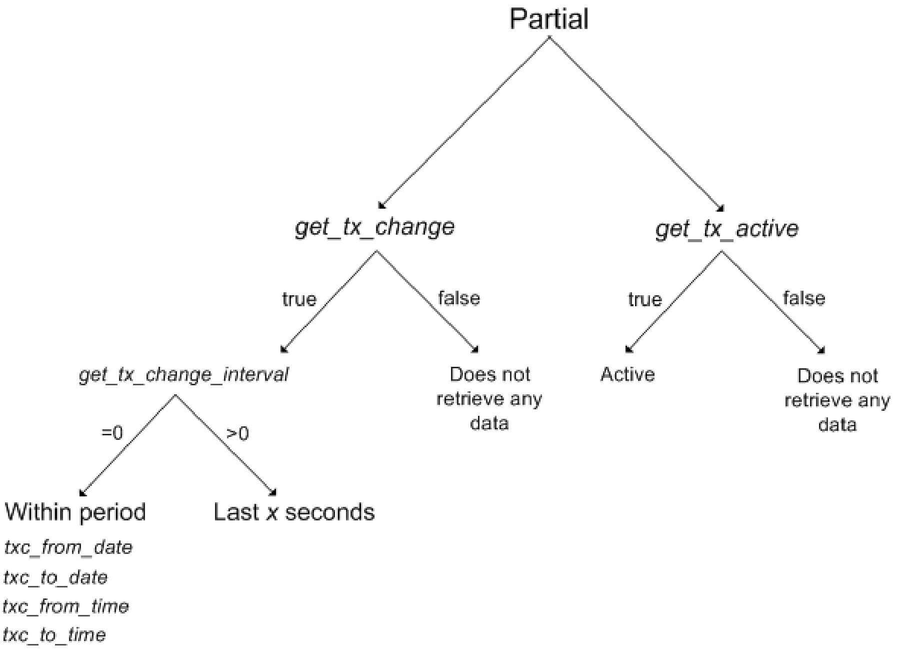
Expand Module	Activate Pattern	Description
Application – SAP (R/3)	**SAP_Dis_Site**	Discovers infrastructure entities in the SAP System: Hosts, R/3 Application server/s, Work Processes, databases, SAP clients, Configuration files, software components (discovered as a configuration file), and support packages (discovered as a configuration file).
	SAP_Dis_ITS	Discovers Internet Transaction Server (ITS) entities (Application Gateway and Web Gateway).
	SAP_Dis_Solution Manager	Run this discovery pattern if you are using SAP Solution Manager and you want to discover the SAP Solution Manager components. For details on the SAP Solution Manager components, see "CIs Created by the Discovery Process" on page 126. **Note:** Before you run this discovery pattern to discover application components, SAP transactions, and SAP transports, you must set the discovery mode. If you want to discover changed SAP transactions you must determine the appropriate range of dates. For details, see "Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery" on page 122.

Selecting the Discovery Modes for Discovering Application Components, SAP Transactions, and Transports

Before you run the SAP_Dis_Applications discovery pattern to discover application components, SAP transactions, and SAP transports, you must set the discovery mode.

If you want to discover changed SAP transactions you must determine the appropriate range of dates. For details, see “Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery” on page 122.

You can use the following parameter’s structure to run the required discovery pattern.



Depending on the combination of parameters and their values you can discover all SAP transactions, active SAP transactions, the SAP transactions that were modified by a SAP transport, or both the active and modified SAP transactions.

Once you have selected what you want to discover, run the appropriate discovery.

This section includes the following topics:

- "Discover Active SAP Transactions" on page 119
- "Discover Changed SAP Transactions" on page 120
- "Discover Active and Changed SAP Transactions" on page 121
- "Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery" on page 122

Discover Active SAP Transactions

You can discover active SAP transactions.

To discover active SAP Transactions:

1. Double-click **SAP_Dis_Application** discovery pattern to open the Pattern Editor page.
2. Set **get_tx_all** to **false**.
3. Set **get_tx_active** to **true**.
4. Click **OK** to save the changes.
5. Go to the next procedure. For details, see "Step 7 – Running SAP Solution Manager Discovery" on page 125.

Discover Changed SAP Transactions

You can discover the SAP transactions that have been changed by discovered transports.

To run changed SAP Transactions:

1. Double-click **SAP_Dis_Application** discovery pattern to open the Pattern Editor page.
2. Set **get_tx_all** to **false**.
3. Set **get_tx_active** to **false**.
4. Set **get_tx_change** to **true**.
5. Set **get_tx_change_interval** to one of the following:
   - ➤ **0.** To discover the changes to transactions in the period of time specified in the **txc_from_date, txc_from_time**, **txc_to_date,** and **txc_to_time** parameters. For details about the range to specify, see “Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery” on page 122.
   - ➤ **x.** To discover (where x > 0) the changes to transactions in the last **x** seconds.
6. Click **OK** to save the changes.
7. Go to the next procedure. For details, see “Step 7 – Running SAP Solution Manager Discovery” on page 125.

Discover Active and Changed SAP Transactions

You can discover the SAP transactions that are active and have changed since the last discovery.

To discover active and changed SAP Transactions:

1. Double-click **SAP_Dis_Application** discovery pattern to open the Pattern Editor page.
2. Set **get_tx_all** to **false**.
3. Set **get_tx_active** to **true**.
4. Set **get_tx_change** to **true**.
5. Set **get_tx_change_interval** to one of the following:
   - ➤ **0**. To discover the changes to transactions in the period of time specified in the **txc_from_date, txc_from_time**, **txc_to_date,** and **txc_to_time** parameters. For details about the range to specify, see “Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery” on page 122.
   - ➤ **x.** (where x > 0) to discover the changes to transactions in the last **x** seconds
6. Click **OK** to save the changes.
7. Go to the next procedure. For details, see “Step 7 – Running SAP Solution Manager Discovery” on page 125.

Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery

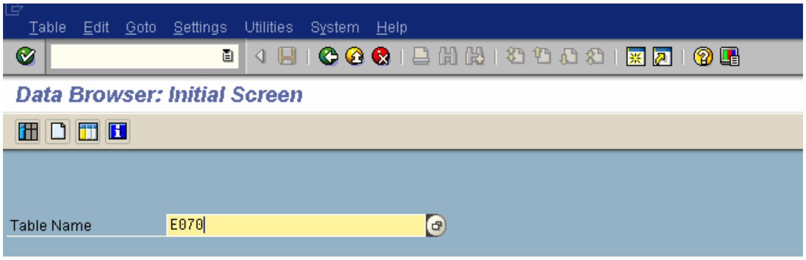
Note: This procedure is only required if the parameter **get_tx_change_interval** = 0. For details, see "Selecting the Discovery Modes for Discovering Application Components, SAP Transactions, and Transports" on page 118.

To discover the SAP transactions that have changed, you must determine the appropriate range of dates before entering them in the appropriate discovery pattern. For details, see "Selecting the Discovery Modes for Discovering Application Components, SAP Transactions, and Transports" on page 118.

To determine the appropriate range of dates for changed SAP transactions discovery:

1 Click the SAP Logon icon to log in to SAP.

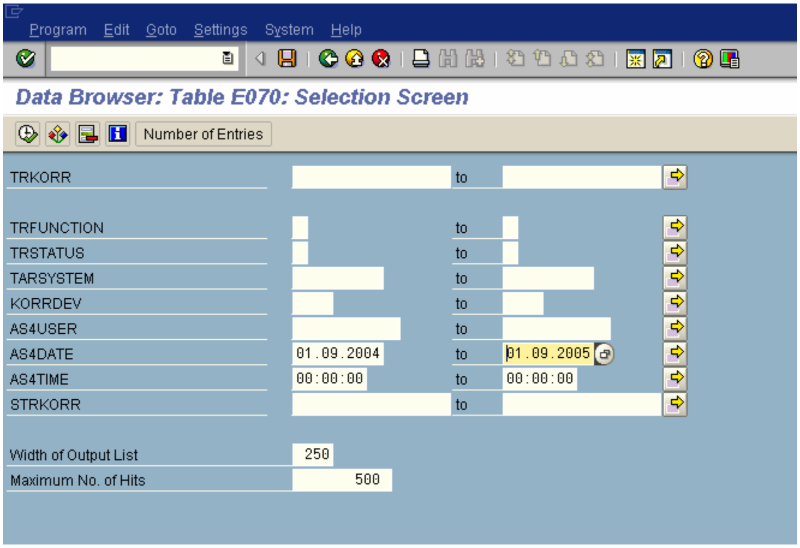
2 Activate SE16 in SAPGUI to open table E070.



Data Browser: Initial Screen

Table Name E070

3 Enter the range of dates for which you want to display the transports deployed.

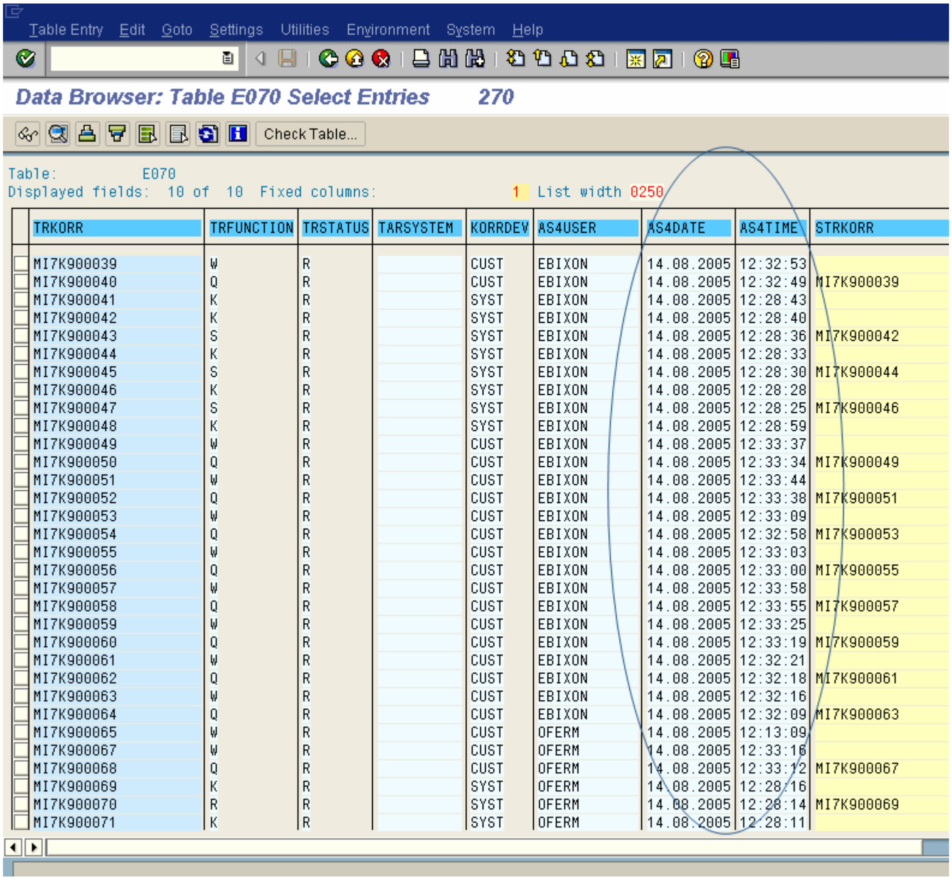


Data Browser: Table E070: Selection Screen

TRKORR		to	
TRFUNCTION		to	
TRSTATUS		to	
TARSYSTEM		to	
KORRDEV		to	
AS4USER		to	
AS4DATE	01.09.2004	to	01.09.2005
AS4TIME	00:00:00	to	00:00:00
STRKORR		to	
Width of Output List	250		
Maximum No. of Hits	500		

4 Press the **Execute** button, in the top left corner.

The outcome is the result of the query you just defined in SAP. The time range is indicated in the AS4DATE and AS4TIME columns.



Data Browser: Table E070 Select Entries 270

Table: E070
Displayed fields: 10 of 10 Fixed columns: 1 List width 0250

TRKORR	TRFUNCTION	TRSTATUS	TARSYSTEM	KORRDEV	AS4USER	AS4DATE	AS4TIME	STRKORR
MI7K900039	W	R		CUST	EBIXON	14.08.2005	12:32:53	
MI7K900040	Q	R		CUST	EBIXON	14.08.2005	12:32:49	MI7K900039
MI7K900041	K	R		SYST	EBIXON	14.08.2005	12:28:43	
MI7K900042	K	R		SYST	EBIXON	14.08.2005	12:28:40	
MI7K900043	S	R		SYST	EBIXON	14.08.2005	12:28:36	MI7K900042
MI7K900044	K	R		SYST	EBIXON	14.08.2005	12:28:33	
MI7K900045	S	R		SYST	EBIXON	14.08.2005	12:28:30	MI7K900044
MI7K900046	K	R		SYST	EBIXON	14.08.2005	12:28:28	
MI7K900047	S	R		SYST	EBIXON	14.08.2005	12:28:25	MI7K900046
MI7K900048	K	R		SYST	EBIXON	14.08.2005	12:28:59	
MI7K900049	W	R		CUST	EBIXON	14.08.2005	12:33:37	
MI7K900050	Q	R		CUST	EBIXON	14.08.2005	12:33:34	MI7K900049
MI7K900051	W	R		CUST	EBIXON	14.08.2005	12:33:44	
MI7K900052	Q	R		CUST	EBIXON	14.08.2005	12:33:38	MI7K900051
MI7K900053	W	R		CUST	EBIXON	14.08.2005	12:33:09	
MI7K900054	Q	R		CUST	EBIXON	14.08.2005	12:32:58	MI7K900053
MI7K900055	W	R		CUST	EBIXON	14.08.2005	12:33:03	
MI7K900056	Q	R		CUST	EBIXON	14.08.2005	12:33:00	MI7K900055
MI7K900057	W	R		CUST	EBIXON	14.08.2005	12:33:58	
MI7K900058	Q	R		CUST	EBIXON	14.08.2005	12:33:55	MI7K900057
MI7K900059	W	R		CUST	EBIXON	14.08.2005	12:33:25	
MI7K900060	Q	R		CUST	EBIXON	14.08.2005	12:33:19	MI7K900059
MI7K900061	W	R		CUST	EBIXON	14.08.2005	12:32:21	
MI7K900062	Q	R		CUST	EBIXON	14.08.2005	12:32:18	MI7K900061
MI7K900063	W	R		CUST	EBIXON	14.08.2005	12:32:16	
MI7K900064	Q	R		CUST	EBIXON	14.08.2005	12:32:09	MI7K900063
MI7K900065	W	R		CUST	OFERM	14.08.2005	12:13:09	
MI7K900067	W	R		CUST	OFERM	14.08.2005	12:33:16	
MI7K900068	Q	R		CUST	OFERM	14.08.2005	12:33:12	MI7K900067
MI7K900069	K	R		SYST	OFERM	14.08.2005	12:28:16	
MI7K900070	R	R		SYST	OFERM	14.08.2005	12:28:14	MI7K900069
MI7K900071	K	R		SYST	OFERM	14.08.2005	12:28:11	

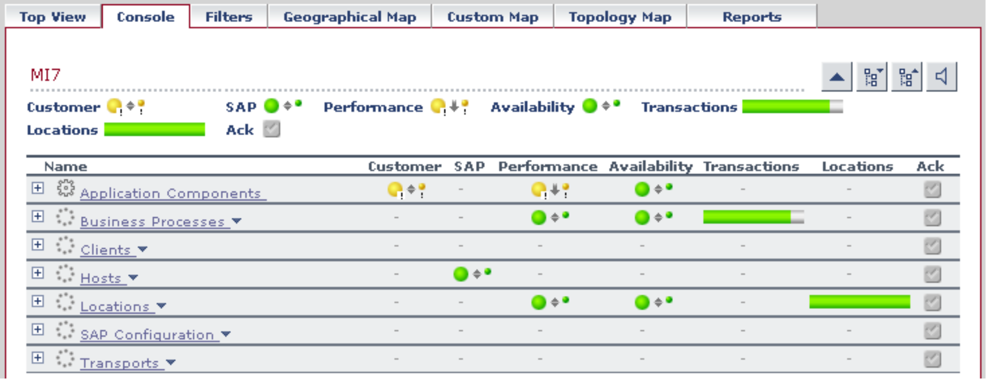
Step 6 – Checking that the Discovery Ran Correctly

After running all the discoveries, check that all the information is displayed correctly.

To check that the discovery ran correctly:

Select **Application** > **Dashboard**, click the **Console** tab, and open the SAP Systems view or select **Admin** > **CMDB**, and click the **IT Universe Manager** tab.

The view is as follows if Business Process Monitor profiles and CCMS monitors were configured before running discovery. Otherwise, the view is similar but the status indicators are grey:



MI7

Customer ● SAP ● Performance ● Availability ● Transactions 🟩
Locations 🟩 Ack ☑

Name	Customer	SAP	Performance	Availability	Transactions	Locations	Ack
⊞ Application Components	●	-	●	●	-	-	☑
⊞ Business Processes ▾	-	-	●	●	🟩	-	☑
⊞ Clients ▾	-	-	-	-	-	-	☑
⊞ Hosts ▾	-	●	-	-	-	-	☑
⊞ Locations ▾	-	-	●	●	-	🟩	☑
⊞ SAP Configuration ▾	-	-	-	-	-	-	☑
⊞ Transports ▾	-	-	-	-	-	-	☑

Step 7 – Running SAP Solution Manager Discovery

You run the SAP Solution Manager discovery to discover the business process hierarchy.

To run SAP Solution Manager Discovery:

1. Select **Admin** > **CMDB** and click the **Discovery Manager** tab to open the Discovery Management page.
2. Click the **Module Manager** tab.
3. In the Discovery Modules pane, expand **Application – SAP (R/3)**.
4. Select the **SAP_Dis_SolutionManager** discovery pattern.
5. ▶ Click the **Activate** button to start the discovery.

   The outcome is the business process hierarchy. For details, see “CIs Created by the Discovery Process” on page 126.

CIs Created by the Discovery Process

During discovery, specific SAP CIs and a hierarchy of CIs are entered in the CMDB.

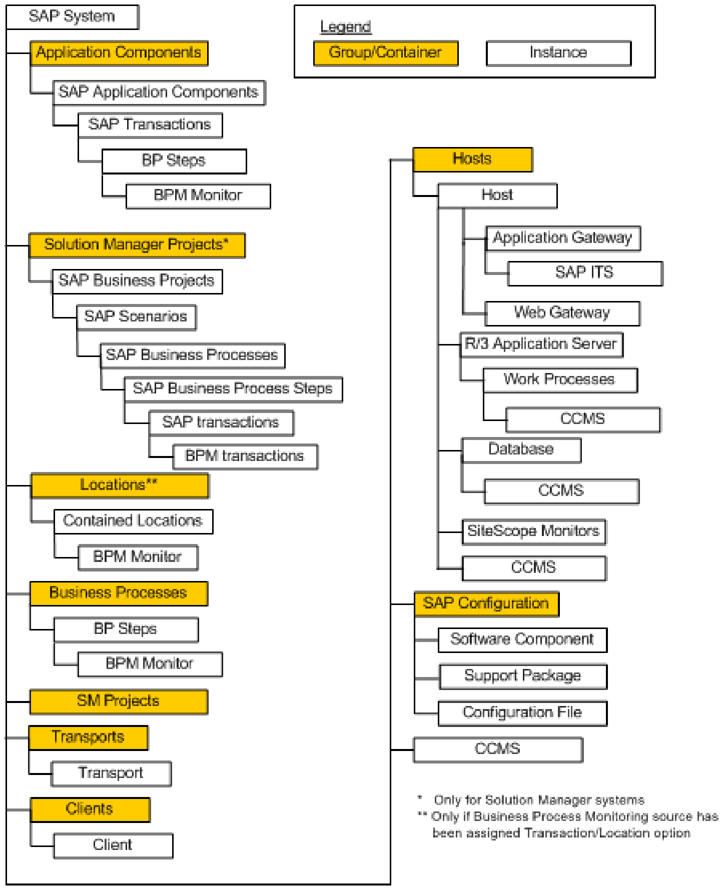
This section includes the following topics:

- "Hierarchy" on page 127
- "SAP System" on page 128
- "SAP Applications" on page 128
- "SAP Application Component" on page 128
- "SAP Transaction" on page 129
- "Business Process Step" on page 129
- "BPM Monitor" on page 129
- "Solution Manager Projects" on page 130
- "Locations" on page 130
- "Contained Location" on page 130
- "Business Processes" on page 131
- "Transports" on page 131
- "Client" on page 131
- "Hosts" on page 132
- "Application Gateway" on page 132
- "Web Gateway" on page 132
- "R/3 Application Server" on page 132
- "Work Processes" on page 133
- "Database" on page 133
- "Software Component" on page 134
- "Support Package" on page 134
- "Configuration File" on page 134

- ➤ "CCMS Counters" on page 134
- ➤ "Monitor" on page 135

Hierarchy

The CIs hierarchy is as follows:



SAP System

SAP System is a logical unit, grouping together SAP-related CIs (and possibly other CIs as well) into one homogenous SAP deployment.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Performance”
- “Availability”
- “System”
- “SAP”
- “Transactions”
- “Locations”

SAP Applications

SAP Applications is a logical unit, grouping together Application Components.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Performance”
- “Availability”

SAP Application Component

A SAP Application Component may include other SAP Application Components and some SAP transactions with some common denominator.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Performance”
- “Availability”

SAP Transaction

A SAP Transaction CI is part of a business process defined in the SAP System. It is comprised of request-response couples called dialog steps. The end user uses SAP transactions to carry out actions on the SAP System.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Performance”
- “Availability”

Business Process Step

Business Process Steps (BPM transactions inside a script) are emulated SAP transactions executed on a Business Process Monitor machine. They are used to supply proactive monitoring of end user experience.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Performance”
- “Availability”

BPM Monitor

The BPM Monitor CIs represent Business Process Monitor entities used to monitor user experience.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Performance”
- “Availability”

Solution Manager Projects

The Solution Manager Projects CI type includes SAP Business Project CIs, SAP Scenario CIs, SAP Business Process CIs, and SAP Business Process Step CIs.

The Solution Manager Projects hierarchy is specified by the user in SAP Solution Manager.

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPIs for this CI are:

- "Performance"
- "Availability"

Locations

The Contained Group Locations is a logical unit, grouping together Contained Locations CIs.

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPIs for this CI are:

- "Performance"
- "Availability"

Contained Location

Location CIs are created as part of the Business Process Monitor hierarchy when working with the **Transactions/locations** option.

To separate the SAP Business Process steps location status from the Location CI (from the Business Process Monitor), the Contained Location CIs are created by the SAP solution and are connected to the SAP Business Process steps (identified by following the naming convention or by manually linking them).

The regular Location CI is connected to all Business Process steps both regular and SAP, but the Contained Location CI is connected only to the SAP Business Process steps.

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPIs for this CI are:

- "Performance"
- "Availability"

Business Processes

The Contained Group called Business Processes is a logical container that contains all the Business Process steps attached to all the SAP transactions.

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPIs for this CI are:

- "Performance"
- "Availability"

Transports

A Transport represents packaged change requests that include the changes that are to be deployed onto the system.

This CI does not have KPIs.

Client

A client is an organizational and legal CI in the SAP system. The main objective of the client is to keep the data isolated: the data in a client can only be visible within that client; it cannot be displayed or changed from another client. Each client on a system can represent a unique working environment.

This CI does not have KPIs.

Hosts

Hosts is a logical unit, grouping together Host CIs.

A Host CI represents the physical machine on which a server is installed. This is not a SAP-specific element.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “System”
- “SAP”

Application Gateway

An Internet Transaction Server (ITS) component. Establishes the connection to the R/3 System and performs the processing of tasks that are required to move data between R/3 applications and the Internet.

This CI does not have KPIs.

Web Gateway

An ITS component. A web server extension that establishes the connection between ITS and the Web server and forwards user requests to the Application Gateway.

This CI does not have KPIs.

R/3 Application Server

SAP R/3 Application Server is SAP's integrated software solution for client/server and distributed open systems.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPI for this CI is:

- “SAP”

Work Processes

Each work process CI is a logical, single-instance representation of all the work processes of the same type existing on the R/3 server.

There are several available types of work processes:

- **Dialog Work Process.** Executes dialog programs (ABAP).
- **Update Work Process.** Responsible for asynchronous database changes (controlled by a COMMIT WORK statement in a dialog work process).
- **Update2 Work Process.** Used for statistical, non-critical updates (for example, result calculations).
- **Background Work Process.** Executes time-dependent or event-controlled background jobs.
- **Enqueue Work Process.** Executes locking operations (if SAP transactions have to synchronize themselves).
- **Spool Work Process.** Performs print formatting (to printer, file, or database).

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPI for this CI is:

- "SAP"

Database

A database management system holding the data tier, including all the SAP elements: SAP transactions, programs, work processes, and so forth. This is not a SAP-specific CI.

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPIs for this CI are:

- "System"
- "SAP"

Software Component

A software component installed on the SAP System, for example: SAP_ABA (cross-application component), SAP_HR (human resources), and so forth.

This CI does not have KPIs.

Support Package

A Support Package contains quality improvements for the SAP system, or adjustments due to legal changes.

This CI does not have KPIs.

Configuration File

Configuration files are used to enter configuration parameters into the system/servers.

This CI does not have KPIs.

CCMS Counters

CCMS Counters (also called Measurements) are pieces of information elements, relevant to SAP, retrieved from SAP CCMS (Computer Center Management System).

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPI for this CI is:

➤ “SAP”

Monitor

The monitors are SiteScope entities used to monitor the various CIs that exist in the CMDB. The monitors that are most likely to appear in the SAP view are host monitors: CPU, memory, disk space, and so forth. These monitors appear in the SAP view only if they are manually attached to the Host CI.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPI for this CI is:

- “System”

6

Performing a Siebel Discovery

This chapter includes the steps involved in discovering Siebel topology in your organization.

This chapter describes:	On page:
About Performing a Siebel Discovery	138
Running Siebel Discovery	138
Step 1 – Preparing for a Siebel Discovery	139
Step 2 – Adding a Network CI to Trigger the Discovery of Siebel Enterprise Networking	143
Step 3 – Accessing the Discovery Modules	144
Step 4 – Discovering the Network	145
Step 5 – Running the Pre–Discovery Patterns for the Web Tier	146
Step 6 – Running the Siebel Discovery	147
Step 7 – Checking that Discovery Ran Correctly	148
Manual Configuration for Specific Siebel CIs	149
CIs Created by the Discovery Process	151

Note: For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

About Performing a Siebel Discovery

Using the Siebel patterns, you can run an automatic Siebel discovery to create the Siebel world, with all its components inside Mercury Business Availability Center.

During the discovery process:

- All Siebel-related IT entities that reside in the organization are discovered and corresponding configuration items (CIs) are entered into the CMDB.
- When a new Siebel Application CI is created, two KPIs are created under it: Transactions and Locations.
- The relationships between the elements are created and saved in the CMDB.
- The newly generated CIs appear when the Siebel Enterprises view is selected in View Explorer under the Siebel Enterprises root CI.
- In addition, four logical containers: Applications, Business Processes, Hosts and Locations are also created under the Siebel Enterprises root CI.
- After the discovery has been performed, you must manually update some of the discovered CI's properties. For details, see "Matching Connection Parameters to SiteScope" on page 370.

Running Siebel Discovery

The Siebel discovery process enables you to discover Siebel elements and Siebel topology. The Siebel discovery process consists of the following steps:

- "Step 1 – Preparing for a Siebel Discovery" on page 139
- "Step 2 – Adding a Network CI to Trigger the Discovery of Siebel Enterprise Networking" on page 143
- "Step 3 – Accessing the Discovery Modules" on page 144
- "Step 4 – Discovering the Network" on page 145
- "Step 5 – Running the Pre–Discovery Patterns for the Web Tier" on page 146
- "Step 6 – Running the Siebel Discovery" on page 147
- "Step 7 – Checking that Discovery Ran Correctly" on page 148

Steps 1 to 4 are a prerequisite to the following steps. Steps 5 to 7 discover different parts of Siebel topology.

Step 1 – Preparing for a Siebel Discovery

Before you run a Siebel discovery, you must define the protocols as indicated in this section.

Note: Ensure that the Discovery Probe is running.

To define Siebel protocols, ask the Siebel enterprise administrator for the following information:

➤ Siebel Enterprise name

➤ Gateway host

➤ User name

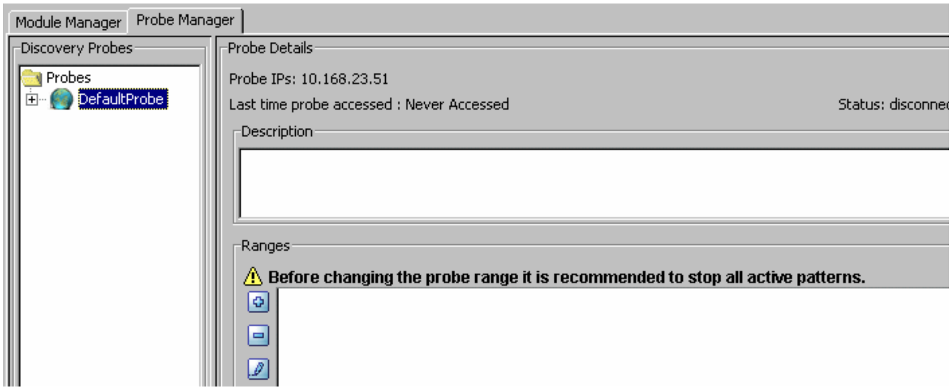
➤ Password

➤ The path to the srvrmgr directory on the Discovery Probe server. For details, see “Copying the srvrmgr Tool to the Discovery Probe Server” on page 327.

To prepare for a Siebel discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the **Probe Manager** tab.

4 In the Discovery Probes pane, select the relevant Discovery Probe.



Probe IPs: 10.168.23.51

Last time probe accessed : Never Accessed

Status: disconne

Before changing the probe range it is recommended to stop all active patterns.

5 Click the **Add IP Range** button to open the Add IP Range dialog box.

6 Enter the range of IP addresses that includes the IP address of the discovery probe. If there is only one address, enter its value in both boxes.

7 Click **OK**.

8 Click the **Add IP Range** button to open the Add IP Range dialog box once more.

9 Enter the range of IP addresses that includes the IP address of the Siebel server(s) you want to discover. If there is only one address, enter its value in both boxes.

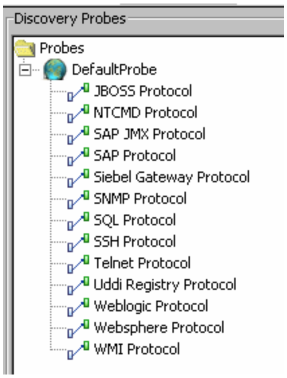
Note: Make sure that all the Siebel servers IP addresses are included in the range. If you do not want to cover all servers with one IP range, you may split it into a few ranges.

---

10 Click **OK**.

11 Click **Apply**.

12 Expand the appropriate Discovery Probe:



Discovery Probes

- Probes
  - DefaultProbe
    - JBOSS Protocol
    - NTCMD Protocol
    - SAP JMX Protocol
    - SAP Protocol
    - Siebel Gateway Protocol
    - SNMP Protocol
    - SQL Protocol
    - SSH Protocol
    - Telnet Protocol
    - Uddi Registry Protocol
    - Weblogic Protocol
    - Websphere Protocol
    - WMI Protocol

13 Define the appropriate protocols.

To define the protocols for the NT platform:

1. Select **WMI Protocol**, click the **Add new connection details for the selected protocol type** button, and populate the following fields:

   ➤ **Windows Domain.** The name of the domain that includes the host where discovery probe is installed.

   ➤ **User Name.** The name of the user you use to connect to the host as administrator.

   ➤ **User Password.** The password of the user you use to connect to the host as administrator.

2. Select **NTCMD Protocol**, click the **Add new connection details for the selected protocol type** button, and populate the following fields:

   ➤ **NT Domain.** The name of the domain that includes the host where discovery probe is installed.

   ➤ **User Name.** The name of the user you use to connect to the host as administrator.

   ➤ **User Password.** The password of the user you use to connect to the host as administrator.

3. Select **Siebel Gateway Protocol**, click the **Add new connection details for the selected protocol type** button, and populate the following fields:

- **Siebel Enterprise Name.** The name of the Siebel Enterprise.
- **srvrmgr path.** The location where you copied **srvrmgr** on the Probe server. For details, see "Copying the srvrmgr Tool to the Discovery Probe Server" on page 327.
- **User Name.** The name of the user you use to log on to the Siebel enterprise.
- **User Password.** The password of the user you use to log on to the Siebel enterprise.

Note: If you have several protocol entries with different srvrmgr versions, the entry with the newer version should appear before the entry with the older version. For example, if you want 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.

---

4 Click **Apply** to save the changes.

To define the protocols for the UNIX platform:

1 Select **SSH Protocol**, click the **Add new connection details for the selected protocol type** button, and populate the following fields:

- **User Name.** The name of the user you use to connect to the host as administrator.
- **User Password.** The password of the user you use to connect to the host as administrator.

  If your server is slow, it is recommended to change the Connection Timeout to 40000.

2 Select **Telnet Protocol**, click the **Add new connection details for the selected protocol type** button, and populate the following fields:

- **User Name.** The name of the user you use to connect to the host as administrator.

- **User Password.** The password of the user you use to connect to the host as administrator.

  If your server is slow, it is recommended to change the Connection Timeout to 40000.

3. Select **Siebel Gateway Protocol**, click the **Add new connection details for the selected protocol type** button, and populate the following fields:

   - **Siebel Enterprise Name.** The name of the Siebel Enterprise.
   - **srvrmgr path.** The location where you copied **srvrmgr** on the Probe server. "Copying the srvrmgr Tool to the Discovery Probe Server" on page 327.
   - **User Name.** The name of the user you use to log on to the Siebel enterprise.
   - **User Password.** The password of the user you use to log on to the Siebel enterprise.

Note: If you have several protocol entries with different srvrmgr versions, the client with the newer version should appear before the client with the older version. For example, if you want 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.

---

4. Click **Apply** to save the changes.

Step 2 – Adding a Network CI to Trigger the Discovery of Siebel Enterprise Networking

To trigger the discovery of Siebel enterprise networking features, you must add a Network CI to the CMDB.

To add a Network CI to trigger the discovery of Siebel Enterprise networking:

1. To add the **Network** CI, access the New CI Wizard.

2 Select **Display all possible CITs**.

3 Expand **System**, expand **Network Resource**, and select **Network.**

4 Click **OK** to open the Define General Properties page, and then click **Next** to open the Define CIT-Specific Properties page.

5 Enter the following information:

- In the **Network Domain Name** box, enter the name of the domain that was specified during the Discovery Probe's installation.
- In the **Network Mask** box, enter the mask for the IP address of the Siebel enterprise network. For example: 255.255.255.0
- In the **Network Address** box, enter the IP address of the Siebel enterprise network. For example: 10.168.11.0.

6 Click **Finish**.

For details about this procedure, see “Using the New CI Wizard” in *IT Universe Manager Administration*.

Step 3 – Accessing the Discovery Modules

Access the discovery modules and activate the appropriate discovery patterns.

For details on how to activate a discovery pattern, see “Running the Discovery Process” on page 25.

To access the discovery modules:

1 Click the **Discovery Manager** tab in CMDB Administration.

2 Click the **Module Manager** tab.

Step 4 – Discovering the Network

To discover the network, run the discovery patterns, select them and activate them as indicated in the procedure.

You can select all the discovery patterns and activate them at once. Each discovery pattern discovers different components. For details on the components and their hierarchy structure, see "CIs Created by the Discovery Process" on page 151.

To discover the network:

In the **Module Manager** tab, expand the modules, select the patterns, and activate them:

Expand Module	Activate Pattern	Description
Network – Basic	**ICMP_NET_Dis_ IpC**	Discovers which machines are active in the range of given IP addresses by pinging the machines in the IP address range that you provided in "Step 1 – Preparing for a Siebel Discovery" on page 139.
Network – Protocol Connections	**NTCMD_NET_Dis_ Connection**	Discovers, in the range of given IP addresses, the hosts that communicate using the NTCMD protocol when working with the NT platform.
Network – Protocol Connections	**WMI_NET_Dis_ Connection**	Discovers, in the range of given IP addresses, the hosts that communicate using the WMI protocol when working with the NT platform.
Network – Protocol Connections	**TTY_NET_Dis_ Connection**	Discovers, in the range of given IP addresses, the hosts that communicate using the SSH/Telnet protocol when working with the UNIX platform.

Step 5 – Running the Pre–Discovery Patterns for the Web Tier

To discover the Web tier, run the discovery patterns, select them and activate them as indicated in the procedure.

You can select all the discovery patterns and activate them at once. Each discovery pattern discovers different components. For details on the components and their hierarchy structure, see "CIs Created by the Discovery Process" on page 151.

To run the discovery:

In the **Module Manager** tab, expand the modules, select the patterns, and activate them:

Expand Module	Activate Pattern	Description
Network – Advanced	**TCP_NET_Dis_Port**	Discovers the http_80 port server's open active ports. If the port is not 80, the discovery procedure updates the **portNumberToPortName.xml** file.
Others	**NTCMD_HR_Reg_ Software**	Discovers the installation path of the Siebel Web Server Extension for the NT platform.
Others	**TTY_HR_ Software**	Discovers the installation path of the Siebel Web Server Extension for the UNIX platform.
Others	**WMI_HR_Software**	Discovers installed software using WMI.
Web Server – Basic	**TCP_Webserver_ Detection**	Discovers the Web Servers running on the host. This pattern is one of the pre-discovery steps needed to discover the Siebel Web Server Extension.

Step 6 – Running the Siebel Discovery

To discover Siebel, activate all the patterns in the Siebel module. The patterns are scheduled to run every 24 hours, by default.

You can select all the discovery patterns and activate them at once. Each discovery pattern discovers different components. For details on the components and their hierarchy structure, see "CIs Created by the Discovery Process" on page 151.

To run the discovery:

1 In the **Module Manager** tab, expand the modules, select the patterns, and activate them:

Expand Module	Activate Pattern	Description
Application – Siebel	**SIEBEL_DIS_ WEBAPPS_NT** (for Windows platform) **or SIEBEL_DIS_ WEBAPPS_UNIX** (for UNIX platform)	Discovers the appropriate IT entities and creates the corresponding Siebel Web Server Extensions, Siebel Web Application, and Siebel Gateway CIs in the CMDB. Currently, Siebel discovery discovers IIS and SunOne (Planet). Siebel Gateway CIs are discovered by the **SIEBEL_DIS_WEBAPPS_NT** discovery pattern when the Web requests load balancing is performed by the gateway.
Application – Siebel	**SIEBEL_DIS_ GATEWAY_ CONNECTION (GTWY)**	Select this pattern if the Web requests load balancing is not performed by the gateway but by an external load balancer. Discovers the appropriate IT entities and creates the corresponding Siebel Gateway CIs.
Application – Siebel	**SIEBEL_DIS_APP_ SERVERS**	Discovers the appropriate IT entities and creates the Siebel Application Server, Component Group, and Component CIs.

Expand Module	Activate Pattern	Description
Application – Siebel	**SIEBEL_DIS_APP_ SERVER_CONFIG**	Discovers the appropriate IT entities and creates the Siebel configuration files.
Application – Siebel	**SIEBEL_DIS_DB_NT** (for the Windows platform) or **SIEBEL_DIS_DB_ UNIX** (for the UNIX platform)	Discovers the appropriate IT entities and creates the Siebel Database CIs.

2 Note that the following enrichment patterns are automatically running in the background while discovery is taking place:

- **Siebel_Route_WebApp_To_Component.** Builds the route between Siebel Web Application CIs and Siebel Component CIs.
- **Siebel_Web_To_Middle_Tier.** Builds the route between the Web tier and the middle tier when the Siebel enterprise uses a Resonate server for load balancing.

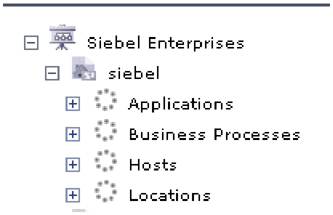
Step 7 – Checking that Discovery Ran Correctly

After running all the discovery patterns, check that all the information in the Siebel view is displayed correctly For information on which CIs are created, see “CIs Created by the Discovery Process” on page 151.

To check that the discovery ran correctly:

Select **Application** > **Dashboard**, and click the **Console** tab or select **Admin** > **CMDB** and click the **IT Universe Manager** tab.

The Siebel Enterprises view opens:



Note: Some of the properties of some of the CIs must be entered manually in order for data to be inserted properly in the Siebel Enterprises view. For details, see "Deploying the SiteScope Siebel Monitors" on page 344.

Manual Configuration for Specific Siebel CIs

When you run the Siebel discovery, the process creates CIs for the discovered components in the CMDB. In addition to the CI's properties that are automatically defined by the discovery process, you must manually define some properties so the Monitor Deployment Wizard and the Siebel diagnostics tools can run correctly.

You manually define properties in IT Universe Manager. For details on defining properties for a CI, see "CIT-Specific Properties" in *IT Universe Manager Administration*.

The following properties remain empty and must be entered manually.

CI Type	Properties	Description
Siebel Enterprise	**Admin user name**	The name of the user used to login to the Server Manager.
	Admin password	The password of the user used to login to the Server Manager.
	SARM Script Path	The path to the location of the Siebel Application Response Measurement (SARM) Analyzer package on the SiteScope server. The path is relative to the SiteScope server.
	Server Manager Script Path	The path to the location of the Server Manager package on the SiteScope server. The path is relative to the SiteScope server. For details, see "Copying the srvrmgr Tool and the SARM Analyzer Tool to the SiteScope Server" on page 328.
Siebel Application	**Emulated Transaction User Name**	The name of the user used in the script that analyzes the application. It is the default user name that appears when configuring the Database Breakdown tool.
Siebel Web Server Extension	**SARM Log Folder**	The log folder to which SARM log files are written on the Web Server Extension's machine. The path is relative to the SiteScope server. The folder should be shared. The format should be: \\<**siebel_web_server_extension_name**>\ <**log_directory**>
Siebel Application Server	**SARM Log Folder**	The log folder to which SARM files are written on the Application Server machine. The path is relative to the SiteScope server. The folder should be shared. The format should be: \\<**siebel_app_server_name**>\<**log_directory**>
	Log Folder	The log folder to which Siebel general log files are written on the Application Server machine. The path is relative to the SiteScope server. The folder should be shared. The format should be: \\<**siebel_app_server_name**>\<**log_directory**>

Note: In addition, you must make sure that the connection parameters used to connect to SiteScope monitors are the ones that exist in the various relevant CIs (Enterprise, Application Server, and so forth). For details, see "Matching Connection Parameters to SiteScope" on page 370.

CIs Created by the Discovery Process

During the discovery process, specific Siebel CIs and a hierarchy of CIs are entered in the CMDB.

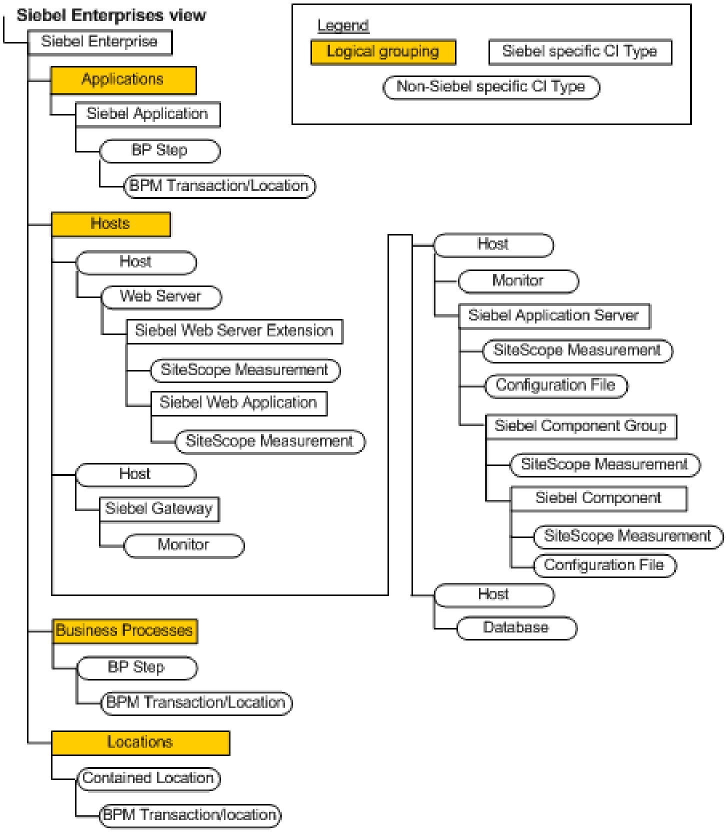
This section includes the following topics:

- "Hierarchy" on page 152
- "Siebel Enterprise" on page 153
- "Contained Group" on page 153
- "Siebel Application" on page 154
- "Business Process Step" on page 154
- "Contained Location" on page 154
- "BPM Transaction/Location" on page 155
- "Host" on page 155
- "Web Server" on page 155
- "Siebel Web Server Extension" on page 156
- "Siebel Web Application" on page 156
- "Siebel Gateway" on page 156
- "Siebel Application Server" on page 156
- "Siebel Component Group" on page 157
- "Siebel Component" on page 157
- "Database" on page 157

- ➤ "SiteScope Measurement" on page 158
- ➤ "Configuration File" on page 158

Hierarchy

The CIs hierarchy is as follows:



Siebel Enterprise

The Siebel Enterprise CI represents the logical grouping of Siebel Application Servers that support the same group of users accessing a common database server.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Availability”
- “Locations”
- “Performance”
- “Sessions”
- “Siebel”
- “System”
- “Transactions”

Contained Group

The Group CI is a logical container. This is not a Siebel-specific CI. The Siebel Enterprises view includes the following groups: Applications, Business Processes, Hosts, and Locations.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Availability”
- “Locations”
- “Performance”
- “Sessions”
- “Siebel”
- “System”
- “Transactions”

Siebel Application

The Siebel Application CI represents the Siebel complete solution for an organization's needs in a certain area. For example: marketing, call center, and so forth.

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPIs for this CI are:

- "Availability"
- "Performance"
- "Sessions"

Business Process Step

The Business Process Steps (BPM transactions inside a script) CIs are emulated Siebel transactions executed on a Business Process Monitor machine. They are used to supply proactive monitoring of end user experience.

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPIs for this CI are:

- "Availability"
- "Performance"

Contained Location

The Contained Location CIs are created as part of the Business Process Monitor hierarchy when working with the **Transactions/locations** option. They represent the locations from which the BP Steps monitoring Siebel are run.

The default KPIs are described in "Dashboard KPIs Detailed Description" in *Repositories Administration*. The default KPIs for this CI are:

- "Availability"
- "Performance"

BPM Transaction/Location

The BPM Transaction/Location CIs represent a BP Step/Location intersection (a specific transaction running at a specific location).

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Availability”
- “Performance”

Host

A Host CI represents the physical machine on which a server is installed. This is not a Siebel-specific element.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Sessions”
- “Siebel”
- “System”

Web Server

The Web Server CI represents the Web server that forwards requests to the Siebel enterprise.

This is not a Siebel-specific element.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Siebel”
- “System”

Siebel Web Server Extension

The Siebel Web Server Extension CI represents the Siebel Web Server Extension installed on the Web server.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPI for this CI is:

- “Siebel”

Siebel Web Application

The Siebel Web Application CI represents the application URL as it exists on the Siebel Web Server Extension.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPI for this CI is:

- “Siebel”

Siebel Gateway

The Siebel Gateway server is a coordinating server that routes requests to the correct component and provides enhanced scalability, load balancing, and high availability across the Siebel Enterprise.

This CI does not have KPIs.

Siebel Application Server

The Siebel Application Server CI represents a server running the business logic tier that supports both back-end and interactive processes for every Siebel client.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Sessions”
- “Siebel”
- “Tasks in Error”

Siebel Component Group

The Component Group CI represents an administrative grouping of components comprising an application running on the Siebel Application Server.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPI for this CI is:

- “Siebel”

Siebel Component

The Component CI represents a process running on the Siebel Application Server, which encapsulates some Siebel application functionality.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPIs for this CI are:

- “Sessions”
- “Siebel”
- “Tasks in Error”

Database

The Database CI represents the database that is holding the data tier. This is not a Siebel-specific CI.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPI for this CI is:

- “System”

SiteScope Measurement

The SiteScope Measurement CI is not a Siebel-specific CI. However, in the Siebel Enterprises view, it usually represents a metric of a Siebel monitor; for example, the Siebel Application Server monitor.

The default KPIs are described in “Dashboard KPIs Detailed Description” in *Repositories Administration*. The default KPI for this CI is:

- “Siebel”

Configuration File

The Configuration File CIs represent the **siebel.cfg** configuration file that includes information from the application server installation or the **parameters.cfg** that includes the output of the list parameters for component command using srvrmgr.

The Configuration File CIs do not have KPIs.

7

Performing a Veritas Cluster Discovery

The Veritas Cluster discovery process enables you to discover Veritas Cluster Servers (VCS), and their member machines (also referred to as nodes), that activate the discovered resources provided by the cluster.

This chapter describes:	On page:
Step 1 – Preparing for a Veritas Cluster Discovery	160
Step 2 – Running the Discovery Patterns	162
Step 3 – Checking that the Discovery Ran Correctly	163
CIs Discovered by the Discovery Process	165
Troubleshooting	167

Note: For details about how to perform a discovery, see "Running the Discovery Process" on page 25.

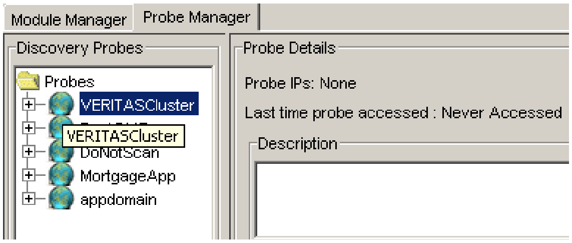
Step 1 – Preparing for a Veritas Cluster Discovery

Before you run a Veritas Cluster discovery, you must add a Discovery Probe and then define the protocols as indicated in this section.

Note: Ensure that the Discovery Probe is running.

To prepare for a Veritas discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the Probe Manager pane.
4. In the Discovery Probes pane, select the relevant Discovery Probe.

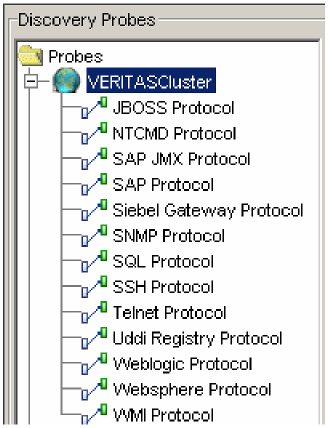


Probe IPs: None

Last time probe accessed : Never Accessed

5. Click the **Add IP Range** button to open the Add IP Range window.
6. Enter the range of IP addresses that includes the IP address of the Discovery Probe you want to discover. If there is only one address, enter its value in both boxes.
7. Click **OK**.
8. Click **Apply** to save the changes you have made.

9 Expand the Discovery Probe:



Discovery Probes

- Probes
  - VERITASCluster
    - JBOSS Protocol
    - NTCMD Protocol
    - SAP JMX Protocol
    - SAP Protocol
    - Siebel Gateway Protocol
    - SNMP Protocol
    - SQL Protocol
    - SSH Protocol
    - Telnet Protocol
    - Uddi Registry Protocol
    - Weblogic Protocol
    - Websphere Protocol
    - WMI Protocol

10 Define the following protocols:

➤ Select **SSH Protocol**, and click the **Add new connection details for the selected protocol type** button. Enter values for the following fields:

➤ **User Name.** The name of the user you use to connect to the host as administrator.

➤ **User Password.** The password of the user you use to connect to the host as administrator.

➤ **Key Path.** In certain environments, the Key Path is required to connect to an SSH agent.

➤ **Port Number.** By default a an SSH agent uses port 22. If you are using a different port for SSH in your environment, enter the required port number.

➤ Select **Telnet Protocol**, and click the **Add new connection details for the selected protocol type** button. Enter values for the following fields:

➤ **User Name.** The name of the user you use to connect to the host as administrator.

➤ **User Password.** The password of the user you use to connect to the host as administrator.

- ➤ **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.

11 Click **Apply** to save the changes.

Step 2 – Running the Discovery Patterns

To run the discovery process, you must activate the discovery patterns described in the table below. Each discovery pattern discovers different components. For details on the components that are discovered by the patterns, see “CIs Discovered by the Discovery Process” on page 165.

Note: For details on how to activate a discovery pattern, see “Running the Discovery Process” on page 25.

To run the Veritas Cluster discovery:

Click the Module Manager tab. Expand the modules, select the following patterns, and activate them:

Expand Module	Activate Pattern	Description
Network – Protocol Connections	**TTY_NET_Dis_ Connection**	Discovers, in the range of given IP addresses, the hosts that communicate using the SSH/Telnet protocol when working with the UNIX platform.
Host Resources – SSH/Telnet	**TTY_HR_Process**	Discovers the HAD processes that are running on the cluster’s nodes.
Veritas Cluster	**Veritas_Cluster_Topology**	Discovers Veritas Cluster server architecture by TTY.

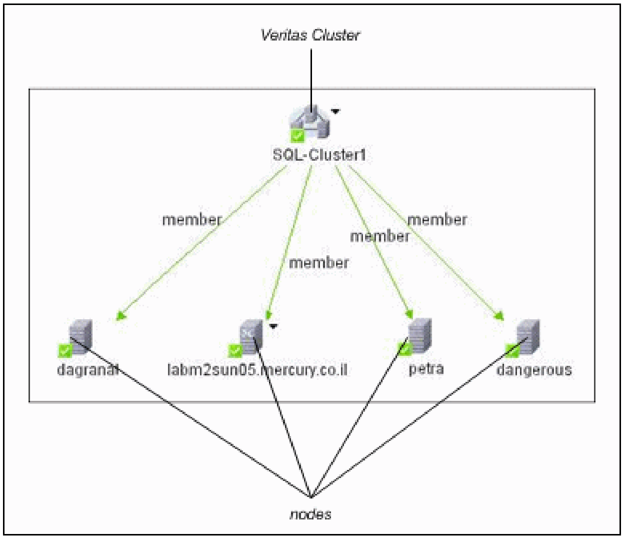
Step 3 – Checking that the Discovery Ran Correctly

After running all the discoveries, check that all the information is displayed correctly.

To check that the discovery ran correctly:

1. Select **Admin** > **CMDB**.
2. Click the **IT Universe** tab.
3. In the Folders pane, select the view called **Veritas cluster server.**

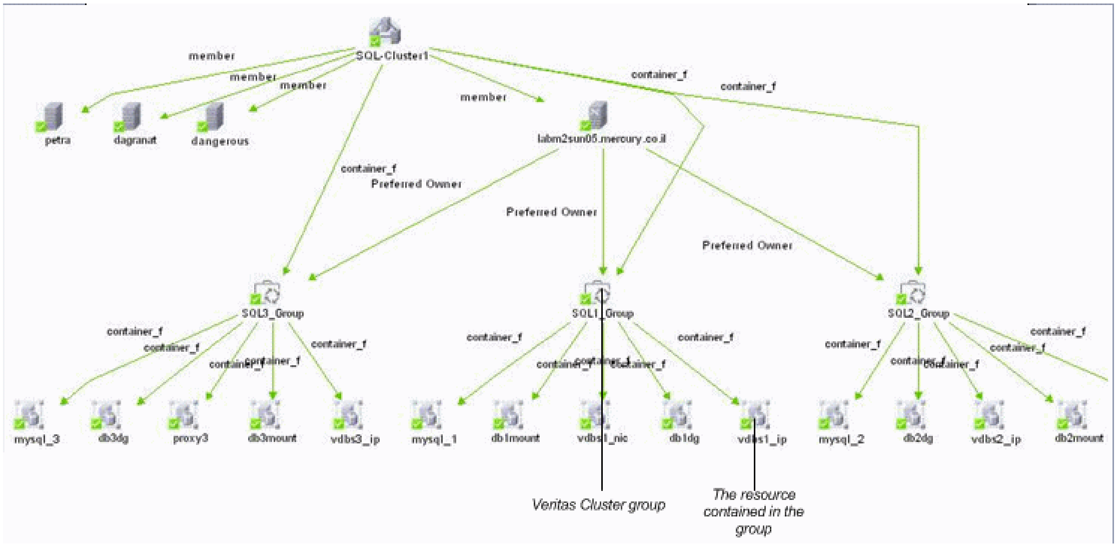
   The following view depicts the Veritas Cluster Server topology.



This view shows the top layer of the Veritas Cluster topology. It displays the discovered Veritas Cluster and the nodes that are members of that cluster. Each member node is linked by a **member** relationship to the Veritas Cluster.

Veritas Clusters contain multiple nodes. Each node is responsible for running certain services and applications. The nodes are used as backups for one another. When a system components fails, another node takes over to provide the necessary service.

Double-click the required node to drill down to the CIs folded underneath.



Veritas Cluster group

The resource contained in the group

This view displays the Veritas Cluster groups and the resources contained in each group.

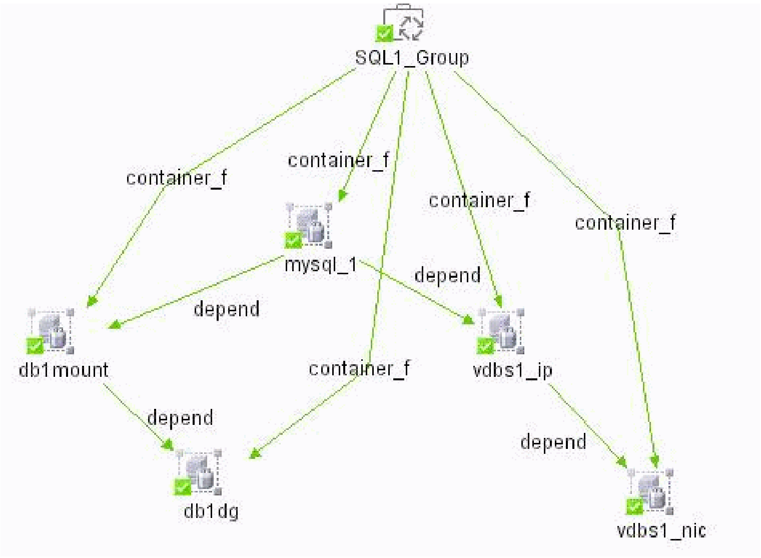
A Veritas Cluster group is a collection of dependent or related resources that is managed as a single unit. Each Veritas Cluster group is linked to a designated node, which is responsible for activating the resources contained in the group. The node is linked to the group by a **Preferred Owner** relationship. If a failure occurs in the designated node, then the responsibility for activating the resources is switched over to a different node.

Certain resources in each group are dependent on one another. Resources that are dependent on one another are linked by a **Dependent** relationship.

The figure below shows the following dependencies:

- **db1dg** is dependent on **db1mount**
- **db1mount** is dependent on **mysql_1**
- **vdbs1_nic** is dependent on **vdbs1_ip**

- **vdbs1_ip** is dependent on **mysql_1**



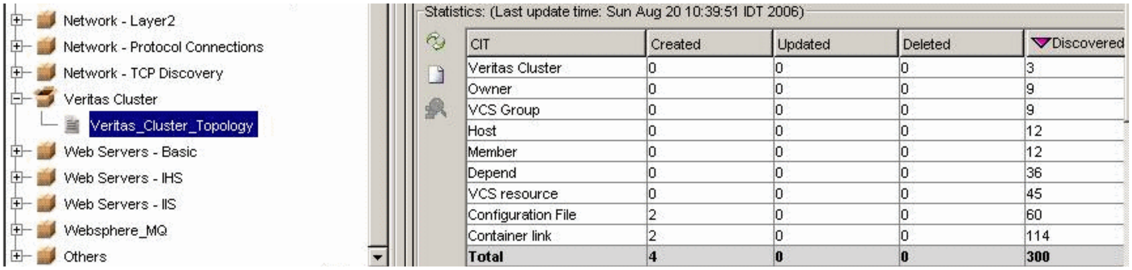
CIs Discovered by the Discovery Process

You can view the CIs discovered by the Veritas Cluster discovery.

To view the CIs discovered by the Veritas Cluster discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the **Module Manager** tab.
4. In the **Discovery Modules** pane, expand the **Veritas Cluster** module.
5. Select the **Veritas_Cluster_Topology** pattern.

In the **Details View** tab, the **Statistics** table at the bottom displays the CIs discovered by the Veritas Cluster discovery.



Statistics: (Last update time: Sun Aug 20 10:39:51 IDT 2006)

CIT	Created	Updated	Deleted	Discovered
Veritas Cluster	0	0	0	3
Owner	0	0	0	9
VCS Group	0	0	0	9
Host	0	0	0	12
Member	0	0	0	12
Depend	0	0	0	36
VCS resource	0	0	0	45
Configuration File	2	0	0	60
Container link	2	0	0	114
Total	**4**	**0**	**0**	**300**

The following table contains a description of the discovered CIs.

Display Name	CI Type	Description
Container link	contained	The relationship that links the discovered resource to the group to which it belongs.
Configuration File	configfile	The configuration files for the nodes, groups and resources.
Host	host	The Veritas Cluster nodes.
IP	ip	
Veritas Cluster	veritascluster	The discovered Veritas Cluster instance.
VCS Group	vcsgroup	Veritas Cluster groups.
VCS Resource	vcsresource	Veritas Cluster resources.
Member	member	The relationship that links the Veritas Cluster to its nodes.
Owner	owner	The relationship that links the nodes to its groups.
Depend	depend	The relationship that links the dependent resources within their group.
Oracle	oracle	

Troubleshooting

This section provides information that can help troubleshooting some of the problems that can occur when performing a Veritas Cluster discovery.

➤ **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.

➤ **Problem**. Failure to access the requested **main.cf** file.

Solution. The location of the **main.cf** file is defined in the discovery pattern. If the **main.cf** file is not found at the defined location, then you can set the location in the **Pattern Parameters** tab in the Pattern Editor of the Discovery Manager.

To set the location of the main.cf file:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the **Module Manager** tab.
4. In the **Discovery Modules** pane, expand the **Veritas Cluster** module.
5. Double-click the **Veritas_Cluster_Topology** pattern to open the Pattern Editor.
6. Click the **Pattern Parameters** tab.
7. For the parameter **main_cf_path**, enter the location of the **main.cf** file in the **Value** field if you do not want to use the default value in the **Description** field.
8. Click **OK** to save your changes.

8

Performing an SNMP Host Resources Discovery

This chapter explains how to discover hosts in your network that contain an SNMP agent.

This chapter describes:	On page:
Step 1 – Preparing for an SNMP Discovery	170
Step 2 – Running the Discovery Patterns	173
Step 3 – Checking that the Discovery Ran Correctly	174
CIs Discovered by the Discovery Process	175
Troubleshooting	176

Note: For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

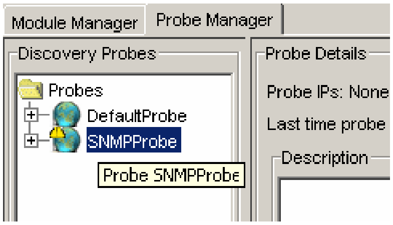
Step 1 – Preparing for an SNMP Discovery

Before you run an SNMP discovery, you must add a discovery probe and define the protocols as indicated in this section.

Note: Ensure that the Discovery Probe is running.

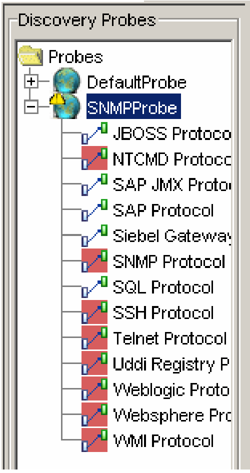
To prepare for an SNMP discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the Probe Manager pane.
4. In the Discovery Probes pane, select the relevant Discovery Probe.



5. Click the **Add IP Range** button to open the Add IP Range window.
6. Enter the range of IP addresses that includes the IP address of the probe you want to discover.
7. Click **OK**.
8. Click the **Add IP Range** button to open the Add Range window once more.
9. Enter the range of IP addresses that includes the system with the SNMP agent you want to discover. If there is only one address, enter its value in both boxes.
10. Click **OK**.
11. Click **Apply** to save the changes you have made.

12 Expand the Discovery Probe:



Discovery Probes

- Probes
  - DefaultProbe
  - SNMPProbe
    - JBOSS Protoco
    - NTCMD Protocc
    - SAP JMX Proto
    - SAP Protocol
    - Siebel Gatewa
    - SNMP Protocol
    - SQL Protocol
    - SSH Protocol
    - Telnet Protocol
    - Uddi Registry P
    - Weblogic Proto
    - Websphere Prc
    - WMI Protocol

Note: Mercury Business Availability Center supports SNMP versions v1, v2, and v3.

13 Select **SNMP Protocol**, and click the **Add new connection details for the selected protocol type** button. The Add Protocol Parameters dialog box opens.

14 Populate the following fields:

- (For SNMP v1 and SNMP v2 only) **Community.** Enter the password you used when connecting to the SNMP service community you defined while configuring the SNMP service (for example, a community for read-only or read/write).
- (For SNMP versions v1, v2, and v3) **Port Number**. The port number on which the SNMP agent listens.
- (For SNMP v3 only) **User Name.** The name of the user authorized to log on to the management application.
- (For SNMP v3 only) **User Password**. The password used to log on to the management application.

- (For SNMP v3 only) **V3 – Authentication method**. Select one of the following options for securing the access to management information:
    - **NoAuthNoPriv**. Using this option provides no security, confidentiality, or privacy at all. It might 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).
- (For SNMP v3 only) **V3 Authentication algorithm**. Two algorithms are supported: MD5 and SHA.
- (For SNMP v3 only) **V3 Privacy algorithm**. The following algorithm is supported: DES.
- (For SNMP v3 only) **V3 Privacy key**. The secrete key used to encrypt the scoped PDU portion in an SNMP v3 message.

15 Click **OK** to save the changes.

Step 2 – Running the Discovery Patterns

To run the discovery patterns, you must trigger them in the order described in this section. Each discovery pattern discovers different components. For details on the components, see "CIs Discovered by the Discovery Process" on page 175.

To run the discovery patterns:

Click the Module Manager tab. Expand the modules, select the patterns, and activate them.

Important: You must first activate the **SNMP_NET_Dis_Connection** pattern before activating the other patterns on this list.

Expand Module	Activate Pattern	Description
Network – Protocol Connections	**SNMP_NET_Dis_Connection**	Discovers the elements or devices in the network on which SNMP is running.
Host Resources – SNMP	**SNMP_HR_OSUser**	Discovers the users on the discovered machine.
	SNMP_HR_Printq	Discovers the print queue on the discovered machine.
	SNMP_HR_Process	Discovers the processes running on the discovered machine.
	SNMP_HR_Software	Discovers the installed software on the discovered machine.
	SNMP_HR_Service	Discovers the services running on the discovered machine.
	SNMP_HR_Disk	Discovers the disks on the discovered machine.

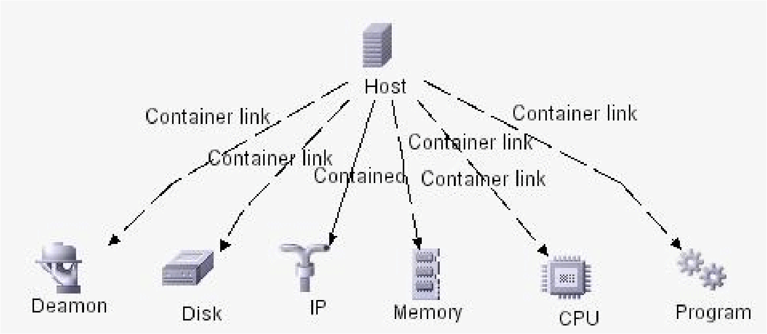
Step 3 – Checking that the Discovery Ran Correctly

After running all the discoveries, check that all the information is displayed correctly.

To check that the discovery ran correctly:

1. Select **Admin** > **CMDB**.
2. Click the **IT Universe** tab.
3. In the Folders pane, select the view called **Host Resources.**

The following figure depicts the topology of the Host Resources view:



This Host Resources view shows the hosts that were discovered in the system. The host contains the discovered Services, Disks, Print Queues, Processes and Programs discovered in the system.

Important: The IP CI is folded underneath the Host icon. In the Host Resource view, only the IP icon must appear in the view. All the other CIs, such as Disks, Services, and so forth, are optional.

CIs Discovered by the Discovery Process

You can view the CIs discovered by the SNMP HR discovery.

To view the CIs discovered by the SNMP HR discovery:

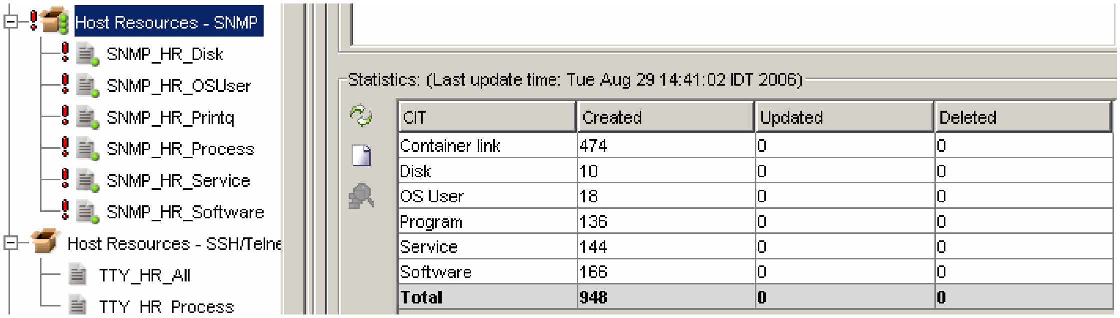
1 In Mercury Business Availability Center, select **Admin** > **CMDB**.

2 Click the **Discovery Manager** tab.

3 Click the **Module Manager** tab.

4 In the **Discovery Modules** pane, select the **Host Resources SNMP** module.

In the **Details View** tab, the **Statistics** table displays the CIs discovered by the SNMP HR discovery.



Statistics: (Last update time: Tue Aug 29 14:41:02 IDT 2006)

CIT	Created	Updated	Deleted
Container link	474	0	0
Disk	10	0	0
OS User	18	0	0
Program	136	0	0
Service	144	0	0
Software	166	0	0
Total	**948**	**0**	**0**

The following table contains a description of the discovered CIs.

Display Name	CI Type	Description
Container link	**container_f**	The relationship that links the discovered resource to the group to which it belongs.
OS User	**osuser**	(Discovered by the SNMP_HR_OSUser pattern) The OS users defined on the discovered machine.
Print Queue	**printq**	(Discovered by the SNMP_HR_Printq pattern) The print queue on the discovered machine.
Program	**program**	(Discovered by the SNMP_HR_Process pattern) The programs running on the discovered machine.

Display Name	CI Type	Description
Software	**software**	(Discovered by the SNMP_HR_Software pattern) The installed software on the discovered machine.
Service	**service**	(Discovered by the SNMP_HR_Service pattern) The running services on the discovered machine.
Disk	**disk**	(Discovered by the SNMP_HR_Disk pattern) The disks on the discovered machine.

Troubleshooting

This section provides information that can help troubleshooting some of the problems that can occur when performing an SNMP HR discovery.

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 GetIf.

➤ **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 “Step 1 – Preparing for an SNMP Discovery” on page 170.

➤ **Solution 3**. Verify that you have the necessary access rights to retrieve data from the MIB objects on the SNMP agent.

9

Performing an IIS Discovery

This chapter describes the steps involved in discovering (Internet Information Services) IIS elements and topology in your organization.

This chapter describes:	On page:
Step 1 – Preparing for an IIS Discovery	178
Step 2 – Running and Configuring the Discovery Patterns	180
Step 3 – Checking that the Discovery Ran Correctly	181
CIs Discovered by the Discovery Process	183

Note: Mercury Business Availability Center supports IIS versions 5 and 6.

Step 1 – Preparing for an IIS Discovery

Before you run an IIS discovery, you must add a discovery probe and then define the NTCMD protocol as described in this section. For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

Note: Ensure that the Discovery Probe is running.

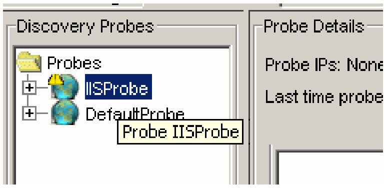
To prepare for an IIS discovery:

1 In Mercury Business Availability Center, select **Admin** > **CMDB**.

2 Click the **Discovery Manager** tab.

3 Click the Probe Manager pane.

4 In the Discovery Probes pane, select the relevant Discovery Probe.



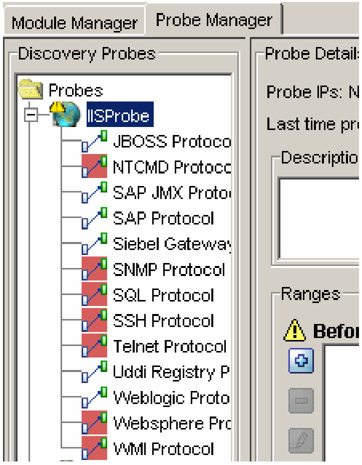
5 Click the **Add IP Range** button to open the Add IP Range window.

6 Enter the range of IP addresses that includes the IP address of the probe you want to discover. If there is only one address, enter its value in both boxes. For details, see “Rules for Defining an IP Address Range” on page 39.

7 Click **OK**.

8 Click **Apply** to save the changes you have made.

9 Expand the Discovery Probe:



10 Select **NTCMD Protocol**, and click the **Add new connection details for the selected protocol type** button. The Add Protocol Parameters dialog box opens.

11 Populate the following fields:

- **Windows Domain.** The name of the domain that includes the host where discovery probe is installed.
- **User Name.** The name of the user you use to connect to the host as administrator.
- **User Password.** The password of the user you use to connect to the host as administrator.

12 Click **OK** to save the changes.

Step 2 – Running and Configuring the Discovery Patterns

Each discovery pattern discovers different elements. For details on the discovered elements, see “CIs Discovered by the Discovery Process” on page 183.

This section contains the following topics:

- “Configuring the NTCMD_APP_Dis_IIS Pattern” on page 180
- “Running the Discovery Patterns” on page 180

Configuring the NTCMD_APP_Dis_IIS Pattern

You can set the configuration of the **NTCMD_APP_Dis_IIS** pattern to define whether web services are discovered or not.

To define whether web services are discovered:

1 Click the Module Manager tab. Double-click the **NTCMD_APP_Dis_IIS** pattern to open the Pattern Editor.

2 Click the **Pattern Parameters** tab.

3 In the **Discovery Pattern Parameters** area, enter one of the following in the **Value** column of the **do_web_service** parameter:

   - True if you want the **NTCMD_APP_Dis_IIS** pattern to discover web services.
   - False if you do not want the **NTCMD_APP_Dis_IIS** pattern to discover web services.

Note: The default is True.

4 Click **OK**.

Running the Discovery Patterns

This section describes the patterns you need to run for an IIS discovery.

To run the discovery patterns:

In the Module Manager tab, expand the modules, select the following patterns, and activate them.

1 Verify that the following patterns are already running:

Expand Module	Activate Pattern	Description
Network – Protocol Connections	**NTCMD_ NET_Dis_Connection**	Discovers NTCMD connections to the remote machine.
Network – Advanced	**TCP_NET_Dis_port**	Discovers the HTTP ports defined in the **portNumberToPortName.xml** file. If there are ports that need to be discovered that are not defined in the **portNumberToPortName.xml** file, they must be added.
Web Servers – Basic	**TCP_Webserver_Detection**	Discovers the CIs on which IIS is running and the IIS version.

2 Activate the following pattern:

Expand Module	Activate Pattern	Description
Web Servers – IIS	**NTCMD_APP_Dis_IIS**	Discovers IIS topology by connecting to the remote machine using NTCMD and running the IIS administration Adsutil.vbs utility.

Step 3 – Checking that the Discovery Ran Correctly

After running all the discoveries, check that all the information is displayed correctly.

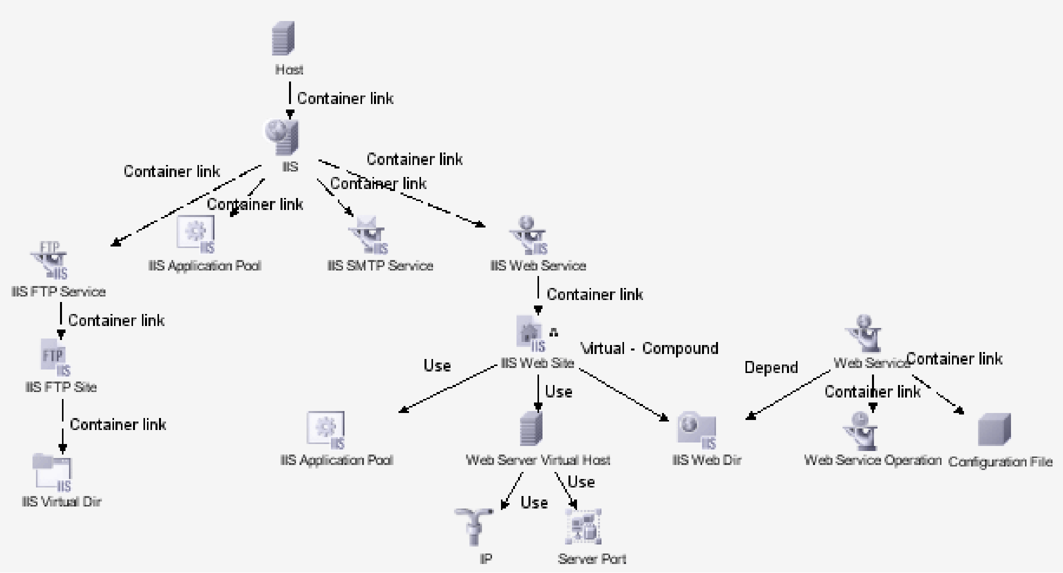
To check that the discovery ran correctly:

1 Select **Admin** > **CMDB**.

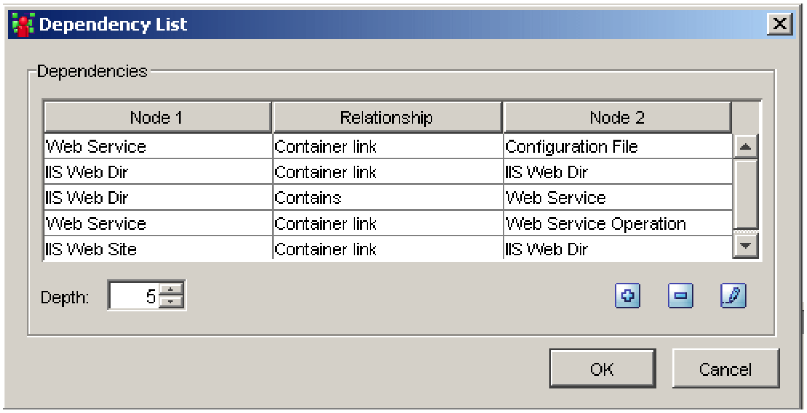
2 Click the **IT Universe Manager** tab.

3 In the Folders pane, select the view called **IIS_Topology.**

The following depicts the topology of the **IIS_Topology** view:



The dependency graph for the IIS Web Site node is defined as follows:



Node 1	Relationship	Node 2
Web Service	Container link	Configuration File
IIS Web Dir	Container link	IIS Web Dir
IIS Web Dir	Contains	Web Service
Web Service	Container link	Web Service Operation
IIS Web Site	Container link	IIS Web Dir

Depth: 5

CIs Discovered by the Discovery Process

You can view the CIs discovered by the IIS discovery.

To view the CIs discovered by the IIS discovery:

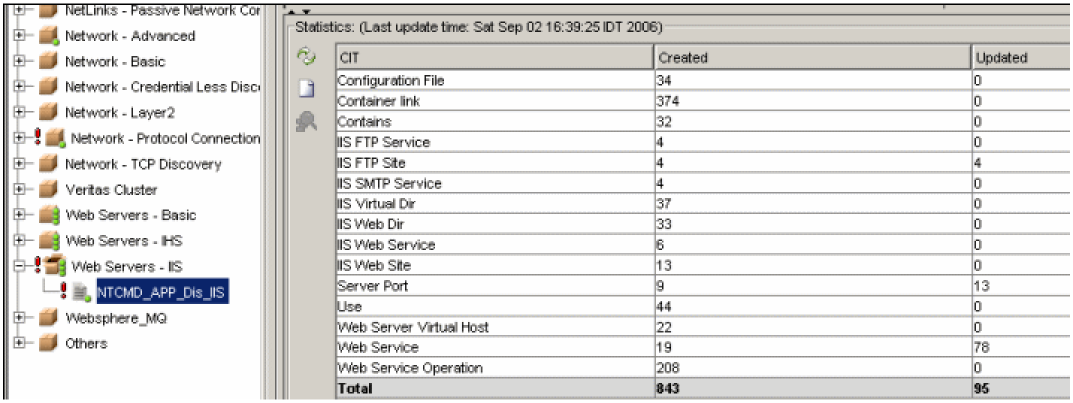
1 In Mercury Business Availability Center, select **Admin** > **CMDB**.

2 Click the **Discovery Manager** tab.

3 Click the **Module Manager** tab.

4 In the **Discovery Modules** pane, select the **NTCMD_APP_Dis_IIS** pattern.

In the **Details View** tab, the **Statistics** table displays the CIs discovered by the IIS discovery.



Statistics: (Last update time: Sat Sep 02 16:39:25 IDT 2006)

CIT	Created	Updated
Configuration File	34	0
Container link	374	0
Contains	32	0
IIS FTP Service	4	0
IIS FTP Site	4	4
IIS SMTP Service	4	0
IIS Virtual Dir	37	0
IIS Web Dir	33	0
IIS Web Service	6	0
IIS Web Site	13	0
Server Port	9	13
Use	44	0
Web Server Virtual Host	22	0
Web Service	19	78
Web Service Operation	208	0
Total	**843**	**95**

The following table contains a description of the CIs discovered by the **NTCMD_APP_Dis_IIS** discovery pattern.

Display Name	CI Type	Description
IIS Resource	**iisresource**	An abstract CIT from which all IIS resources inherit.
IIS Service	**iisservice**	An abstract CIT from which all IIS services inherit.
IIS Web Service	**iiswebservice**	The World Wide Web Publishing Service for hosting Internet and intranet content.

Display Name	CI Type	Description
IIS FTP Service	**iisftpservice**	The File Transfer Protocol (FTP) service for hosting sites where you can upload and download files.
IIS SMTP Service	**iissmtpservice**	The Simple Mail Transfer Protocol (SMTP) service for sending and receiving e-mail messages.
IIS Application Pool	**issapppool**	A group that contains specific Web applications and Web sites. For example, if you want to separate Web sites running in the same computer, you create a separate application pool for every Web site and place them in their corresponding application pool. **Note:** This is relevant for IIS 6.0 only.
IIS Web Site	**iiswebsite**	A Web site that represents a web application in IIS.
IIS FTP Site	**iisftpsite**	A Web site in which you can upload or download files.
IIS Web Dir	**iiswebdir**	A local or home directory that contains the published Internet content.
IIS Virtual Dir	**iisvirtualdir**	A directory that is not contained in the home directory but appears to client browsers as though it were. It allows you to publish from any directory not contained within your home or root directory.
Web Service	**webservice**	Web Service.
Web Service Operation	**webservice_operation**	Web Service operation.

10

Performing a WebLogic Discovery

This chapter includes the steps involved in performing a WebLogic discovery.

This chapter describes:	On page:
Performing a WebLogic Discovery	186
Step 1 – Preparing for a WebLogic Discovery	186
Step 2 – Running the Discovery Patterns	188
Step 3 – Checking that the Discovery Ran Correctly	189
CIs Discovered by the Discovery Process	190

Note: For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

Performing a WebLogic Discovery

The WebLogic discovery process discovers all the deployed web services and operations deployed on the WebLogic server. Mercury Business Availability Center supports WebLogic versions 8 and 9.

Note: If you are using WebLogic version 7, do the following:

- ➤ Take the **webserviceclient.jar** and **weblogic.jar** files from the following location: **<BEA Installation root folder>\<WebLogic version number>\server\lib**.
- ➤ Place both jar files in the following location: **<Discovery Probe Installation root folder>\root\lib\collectors\probeManager\userExt**.
- ➤ Rename the jar files by adding a suffix that includes the WebLogic version number, as follows: **webserviceclient70.jar**, **weblogic70.jar**.

Step 1 – Preparing for a WebLogic Discovery

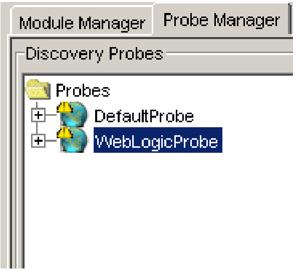
Before you run a WebLogic discovery, you must add a discovery probe and then define the WebLogic protocol as described in this section.

Note: Ensure that the Discovery Probe is running.

To prepare for a WebLogic discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the Probe Manager pane.

4 In the Discovery Probes pane, select the relevant Discovery Probe.



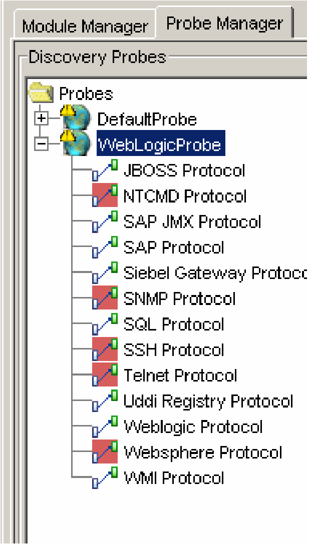
5 Click the **Add IP Range** button to open the Add IP Range window.

6 Enter the range of IP addresses that includes the IP address of the WebLogic servers you want to discover. If there is only one address, enter its value in both boxes. For details, see “Rules for Defining an IP Address Range” on page 39.

7 Click **OK**.

8 Click **Apply** to save the changes you have made.

9 Expand the Discovery Probe:



10. Select **WebLogic Protocol**, and click the **Add new connection details for the selected protocol type** button. The Add Protocol Parameters dialog box opens.

11. Populate the following fields:

    - **User Name.** The name of the user you use to connect to the host as administrator.

    - **User Password.** The password of the user you use to connect to the host as administrator.

12. Click **OK** to save the changes.

Step 2 – Running the Discovery Patterns

To run the discovery patterns, activate the following discovery patterns. Each discovery pattern discovers different elements. For details on the CIs that are discovered, see “CIs Discovered by the Discovery Process” on page 190.

To run the discovery:

Click the Module Manager tab. Expand the modules, select the patterns, and activate them in the following order.

Note: Before activating the following patterns, verify that you have already run the following patterns:

- Host_ID_Discover
- ICMP_NET_Dis_IpC

Both of these patterns are under the module **Network-Basic**.

---

1 First activate this pattern.

Expand Module	Activate Pattern	Description
J2EE WebLogic	**JMX_J2EE_Weblogic_Connection**	Discovers WebLogic servers based on the JMX protocol.

2 Then activate this pattern.

Expand Module	Activate Pattern	Description
J2EE WebLogic	**JMX_J2EE_Weblogic**	Discovers a WebLogic J2EE environment and its components.

Step 3 – Checking that the Discovery Ran Correctly

After running all the discovery patterns, check that all the information in the **WebLogic_Topology** view is displayed correctly.

For information on which CIs are discovered, see "CIs Discovered by the Discovery Process" on page 190.

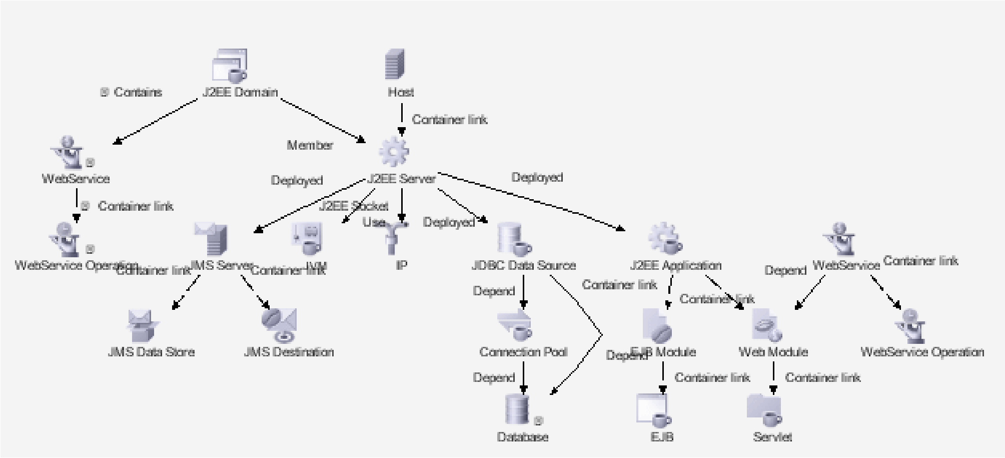
To check that the discovery ran correctly:

1 Select **Admin** > **CMDB**.

2 Click the **Topology Map** tab.

3 In the Folders pane, select the view called **WebLogic_Topology View.**

The following depicts the topology of the **WebLogic_Topology** view:



CIs Discovered by the Discovery Process

You can view the CIs discovered by the WebLogic discovery process.

To view the CIs discovered by the WebLogic discovery:

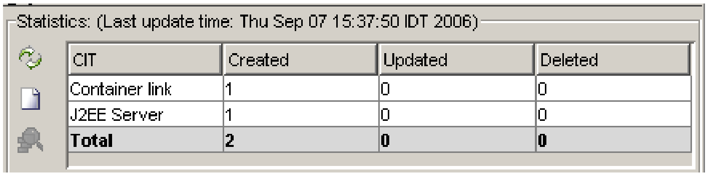
1 In Mercury Business Availability Center, select **Admin** > **CMDB**.

2 Click the **Discovery Manager** tab.

3 Click the **Module Manager** tab.

4 In the **Discovery Modules** pane, select the **JMX_J2EE_WebLogic_Connection** pattern.

In the **Details View** tab, the **Statistics** table displays the CIs discovered by the WebLogic discovery.



Statistics: (Last update time: Thu Sep 07 15:37:50 IDT 2006)

CIT	Created	Updated	Deleted
Container link	1	0	0
J2EE Server	1	0	0
Total	**2**	**0**	**0**

The following table contains a description of the CIs discovered by the WebLogic discovery process.

Display Name	CI Type	Description
Configuration File	**configfile**	Holds data regarding a configuration file of an application.
Connection Pool	**connectionpool**	
Contained	**contained**	The relationship between two CIs whereby a second CI is included in the first CI. This relationship is found only between IP and host.
Container link	**container_f**	The functional relationship between a parent and a child. The child does not inherit any properties.
Contains	**contains**	The relationship between two CIs whereby a second CI is included in the first CI.
Database	**database**	A collection of data that is organized so that its content can be easily accessed, managed and updated.
Depend	**depend**	The relationship wherein one CI needs a functionality of another CI.
Deployed	**deployed**	The relationship wherein one CI is put into action by another CI.
Document	**document**	Holds data regarding a document in the application.
EJB Module	**ejbmodule**	A module containing an EJB system.
Entity Bean	**entitybean**	An EJB entity.
J2EE Execute Queue	**executequeue**	
Host	**host**	Represents a network element that has a unique IP address.

Display Name	CI Type	Description
IP	**ip**	Represents an IP address that identifies the sender to receiver of information that is sent across the internet.
J2EE Application	**j2eeapplication**	An application inside the application server.
J2EE Cluster	**j2eecluster**	
J2EE Domain	**j2eedomain**	An application server domain.
J2EE Server	**j2eeserver**	A server within a J2EE application server.
J2EE Socket	**j2eesocket**	
JDBC Data Source	**jdbcdatasource**	A JDBC data source.
JMS Destination	**jmsdestination**	JMS destination.
JMS Server	**jmsserver**	A JMS server.
JVM	**jvm**	JVM.
Member	**member**	The relationship between two CIs whereby one CI is included in another CI.
Message Driven Bean	**messagedrivenbean**	
Servlet	**servlet**	
SQL Database	**sqldatabase**	An SQL database from Microsoft.
Statefull Session Bean	**statefulsessionbean**	
Stateless Session Bean	**statelesssessionbean**	
Use	**use**	
Web Module	**webmodule**	A J2EE deployed CI.
Web Service	**webservice**	A web service.
Web Service Operation	**webservice_operation**	A web service operation.

11

Performing a WebSphere Discovery

This chapter describes the steps involved in performing a WebSphere discovery.

This chapter describes:	On page:
Performing a WebSphere Discovery	194
Step 1 – Preparing for a WebSphere Discovery	194
Step 2 – Running the Discovery Patterns	197
Step 3 – Checking that the Discovery Ran Correctly	198
CIs Discovered by the Discovery Process	199

Note: For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

Performing a WebSphere Discovery

The WebSphere discovery discovers the Web services that are deployed on an IBM WebSphere server. The discovered Web services are represented by a **webservice** CI in the CMDB.

Note: Mercury Business Availability Center supports WebSphere versions 5 and 6.

Step 1 – Preparing for a WebSphere Discovery

Before you run a WebSphere discovery, you must define the protocols as indicated in this section.

Note: Ensure that the Discovery Probe is running.

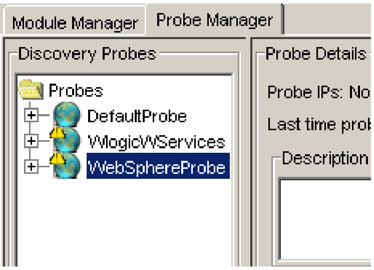
To prepare for a WebSphere discovery:

1 In Mercury Business Availability Center, select **Admin** > **CMDB**.

2 Click the **Discovery Manager** tab.

3 Click the **Probe Manager** tab.

4 In the Discovery Probes pane, select the relevant Discovery Probe.



5 Click the **Add IP Range** button to open the Add IP Range dialog box.

6 Enter the range of IP addresses that includes the IP address of the discovery probe. If there is only one address, enter its value in both boxes. For details, see “Rules for Defining an IP Address Range” on page 39.

7 Click **OK**.

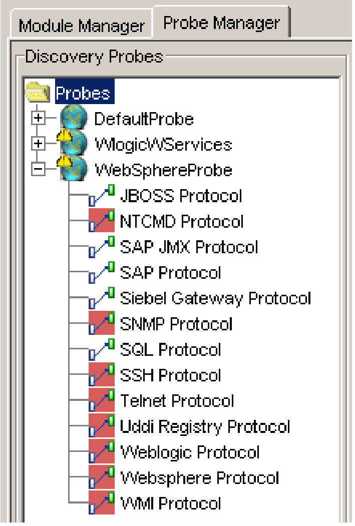
8 Click the **Add IP Range** button to open the Add IP Range dialog box once more.

9 Enter the range of IP addresses that includes the IP address of the WebSphere server(s) you want to discover. If there is only one address, enter its value in both boxes.

10 Click **OK**.

11 Click **Apply**.

12 Expand the Discovery Probe:



13 Select **WebSphere Protocol**, and click the **Add new connection details for the selected protocol type** button.

14 Ask the WebSphere system administrator for the following:

- **Username.** The name of the user you use to connect to the host as administrator.

- **Password.** The password of the user you use to connect to the host as administrator.
- **Truststore file**. The name of the SSL truststore file.

  Mercury Business Availability Centercontains a default truststore file called **DummyClientTrustFile**. It is located in the **userEXT** folder contained in the J2EE package. If you want to use a file other than the default truststore file provided by the system, enter the name of your own truststore file and place it in the **userEXT** folder. When the package is updated, the truststore file is copied to the relevant location.
- **Truststore password**. The SSL truststore password.

Note: The default password for the default truststore file in Mercury Business Availability Center is WebAs. If you are not using the default truststore file provided by the system, enter the password for the file you are using.

- **Port Number**. The protocol port number as provided by the WebSphere system administrator.

  You can also retrieve the protocol port number by connecting to the Administrative Console using the username and password provided by the WebSphere system administrator.

  In your browser, enter the following URL: **http:/<host>:9090/admin**, where:

  - **<host>** is the IP address of the host running the WebSphere protocol
  - **9090** is the port used to connect to the WebSphere console

  Then go to **System Administration** > **Deployment Manager** to retrieve the required port number.

Step 2 – Running the Discovery Patterns

To run the discovery patterns, activate the following discovery patterns. Each discovery pattern discovers different elements. For details on the CIs that are discovered, see “CIs Discovered by the Discovery Process” on page 199.

Note: For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

To run the discovery patterns:

Click the Module Manager tab. Expand the modules, select the patterns, and activate them in the following order.

Note: Before activating the following patterns, verify that you have already run the following patterns:

➤ Host_ID_Discover

➤ ICMP_NET_Dis_IpC

Both of these patterns are under the module **Network-Basic**.

---

1 First activate this pattern.

Expand Module	Activate Pattern	Description
JMX_J2EE	**JMX_J2EE_WebSphere_ Connection**	Discovers WebSphere servers based on either SOAP or RMI authentication.

2 Then activate this pattern.

Expand Module	Activate Pattern	Description
JMX_J2EE	**JMX_J2EE_WebSphere**	Discovers the WebSphere J2EE environment and components.

Step 3 – Checking that the Discovery Ran Correctly

After running all the discovery patterns, check that all the information in the **WebSphere_Topology** view is displayed correctly.

For information on which CIs are discovered, see "CIs Discovered by the Discovery Process" on page 199.

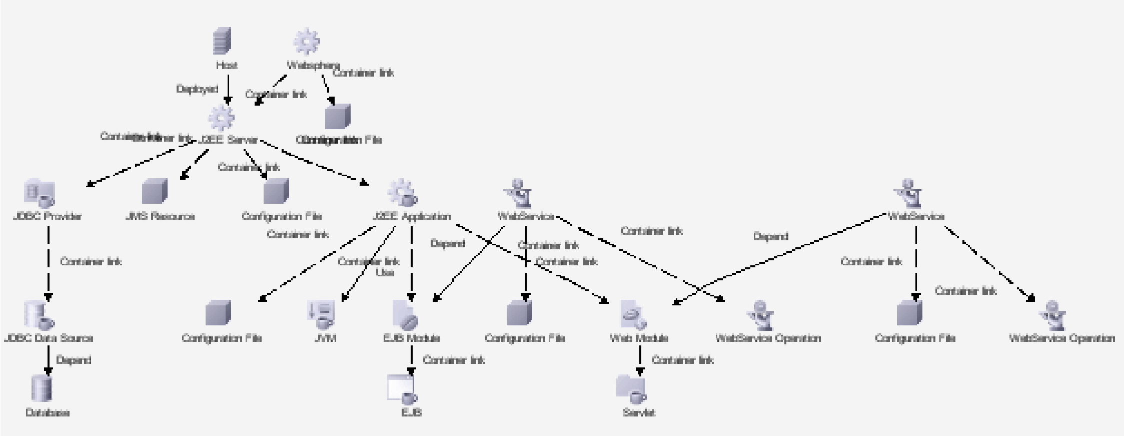
To check that the discovery ran correctly:

1 Select **Applications** > **Dashboard**.

2 Click the **Topology Map** tab.

3 In the Folders pane, select **WebSphere_Topology View.**

The following depicts the topology of the **WebSphere_Topology** view:



CIs Discovered by the Discovery Process

You can view the CIs discovered by the WebSphere discovery process.

To view the CIs discovered by the WebSphere discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the **Module Manager** tab.
4. In the **Discovery Modules** pane, select the **JMX_J2EE_WebSphere_ Connection** pattern.

   The following table contains a description of the CIs discovered by the **WebSphere** discovery process.

Display Name	CI Type	Description
Configuration File	**configfile**	Holds data regarding a configuration file of an application.
Container link	**container _f**	Represents a containment relationship between two CIs.
Contains	**container_f**	The relationship between two CIs whereby a second CI is included in the first CI.
Database	**database**	A collection of data that is organized so that its content can be easily accessed, managed and updated.
Depend	**depend**	
Deployed	**deployed**	
Document	**document**	Holds data regarding a document in the application.
EJB Module	**ejbmodule**	A module containing an EJB system.
Entity Bean	**entitybean**	An EJB entity.
Host	**host**	Represents a network element that has a unique IP address.

Display Name	CI Type	Description
J2EE Application	**j2eeapplication**	An application inside the application server.
J2EE Cluster	**j2eecluster**	J2EE cluster.
J2EE Server	**j2eeserver**	A server within a J2EE application server.
JDBC Data Source	**jdbcdatasource**	A JDBC data source.
JDBC Provider	**jdbcprovider**	A provider for JDBC.
JMS Server	**jmsserver**	A JMS server.
JVM	**jvm**	JVM.
Member	**member**	
Message Driven Bean	**messagedrivenbean**	
Servlet	**servlet**	
SQL Database	**sqldatabase**	An SQL database from Microsoft.
Statefull Session Bean	**staefulsessionbean**	
Use	**use**	
Web Module	**webmodule**	A J2EE deployed CI.
Web Service	**webservice**	A Web service.
Web Service Operation	**webservice_operation**	A Web service operation.
WebSphere	**websphere**	An application server of WebSphere based on the Java 2 platform.

12

Performing a UDDI Discovery

This chapter includes the steps involved in discovering Web services from a UDDI registry.

This chapter describes:	On page:
Performing a UDDI Discovery	201
Step 1 – Preparing for a UDDI Discovery	202
Step 2 – Running the Discovery Patterns	204
Step 3 – Checking that the Discovery Ran Correctly	205
CIs Discovered by the Discovery Process	205

Note: For details about how to perform a discovery, see "Running the Discovery Process" on page 25.

Performing a UDDI Discovery

The discovery process queries the Universal Description, Discovery and Integration (UDDI) registry for all its Web services, including non-SOAP services, or for a specific publisher service (if defined in the UDDI Registry protocol). The Web services found in the UDDI registry are represented by a **webservice** CI in the CMDB and the registry is created as a **uddiregistry** CI.

Note: Mercury Business Availability Center supports UDDI versions 2 and 3.

Step 1 – Preparing for a UDDI Discovery

Before you run a UDDI discovery, you must add a discovery probe and define the NTCMD protocol as described in this section.

Note: Ensure that the Discovery Probe is running.

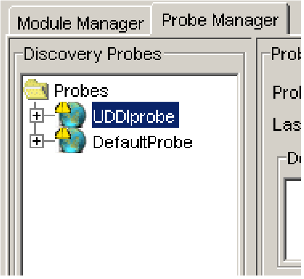
To prepare for a UDDI discovery:

1 In Mercury Business Availability Center, select **Admin** > **CMDB**.

2 Click the **Discovery Manager** tab.

3 Click the Probe Manager tab.

4 In the Discovery Probes pane, select the relevant Discovery Probe.



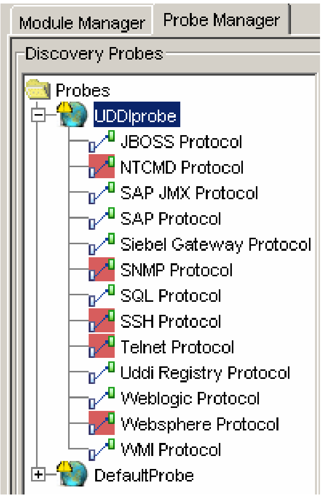
5 Click the **Add IP Range** button to open the Add IP Range window.

6 Enter the range of IP addresses that includes the IP address of the Discovery Probe you want to discover. If there is only one address, enter its value in both boxes. For details, see “Rules for Defining an IP Address Range” on page 39.

7 Click **OK**.

8 Click **Apply** to save the changes you have made.

9 Expand the Discovery Probe:



10 Select **UDDI Registry Protocol**, and click the **Add new connection details for the selected protocol type** button. The Add Protocol Parameters dialog box opens.

11 Populate the following field:

UDDI inquiry URL. The URL where the UDDI Registry is located.

12 Click **OK** to save the changes.

13 **(Optional)** To enter the name of the service publisher whose services you want to publish, do the following:

a Click the **Module Manager** tab.

b Expand the **Application – Webservices** module.

c Double-click the **UDDI_Registry** pattern to open the Pattern Editor.

d Click the **Pattern Parameters** tab.

e In the **Discovery Pattern Parameters** area, enter the name of the service publisher whose services you want to publish in the **Value** field of the **organization** parameter.

f In the **Description** field, enter the required description of the organization.

g Click **OK** to save your changes.

Step 2 – Running the Discovery Patterns

To run the discovery patterns, activate the following discovery patterns. Each discovery pattern discovers different elements. For details on the discovered elements, see "CIs Discovered by the Discovery Process" on page 205.

To run the discovery patterns:

Click the Module Manager tab. Expand the module, select the patterns, and activate them in the following order.

1 First activate this pattern.

Expand Module	Activate Pattern	Description
Application _ Webservices	**UDDI_Registry_Connection**	Discovers a UDDI registry using a given URL.

2 Then activate this pattern.

Expand Module	Activate Pattern	Description
Application _ Webservices	**UDDI_Registry**	Discovers business units and web services based on the UDDI registry.

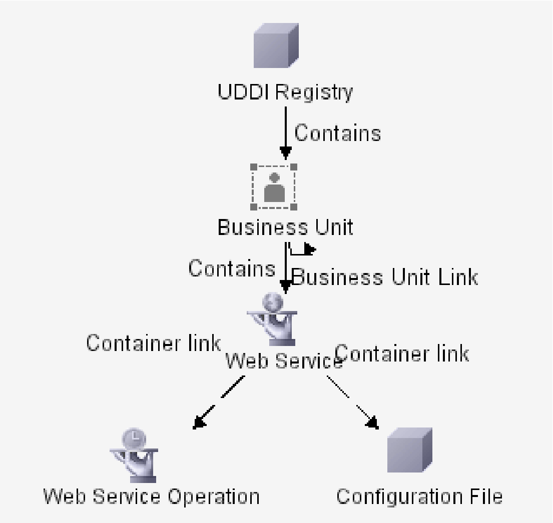
Step 3 – Checking that the Discovery Ran Correctly

After running all the discovery patterns, check that all the information in the SOA UDDI view is displayed correctly. For information on which CIs are discovered, see "CIs Discovered by the Discovery Process" on page 205.

To check that the discovery ran correctly:

1. Select **Admin** > **CMDB**.
2. Click the **Topology Map** tab.
3. In the Folders pane, select **SOA UDDI View**.

   The following depicts the topology of the **SOA_UDDI_View**:



CIs Discovered by the Discovery Process

You can view the CIs discovered by the UDDI discovery.

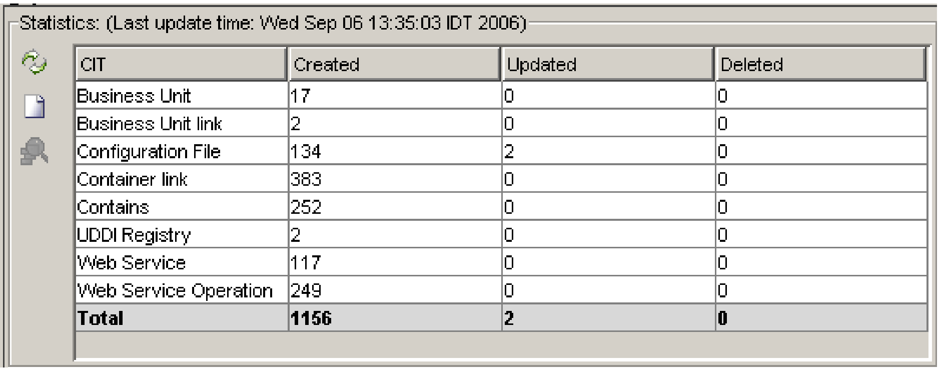
To view the CIs discovered by the UDDI discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.

3 Click the **Module Manager** tab.

4 In the **Discovery Modules** pane, select the **UDDI_Registry** pattern.

In the **Details View** tab, the **Statistics** table displays the CIs discovered by the UDDI discovery.



Statistics: (Last update time: Wed Sep 06 13:35:03 IDT 2006)

CIT	Created	Updated	Deleted
Business Unit	17	0	0
Business Unit link	2	0	0
Configuration File	134	2	0
Container link	383	0	0
Contains	252	0	0
UDDI Registry	2	0	0
Web Service	117	0	0
Web Service Operation	249	0	0
Total	**1156**	**2**	**0**

The following table contains a description of the CIs discovered by the **UDDI_Registry** discovery pattern.

Display Name	CI Type	Description
Business Unit	**business_unit**	A business entity, such as a customer or a provider.
Business Unit link	**business_unitlink**	A relationship that links between related business entities.
Configuration File	**configfile**	A WSDL (Web Service Description Language) file that holds data regarding the web services. For example, which protocols are supported and the location of the service and the operations.
Container link	**container _f**	Represents a containment relationship between two CIs.
Contains	**contains**	The relationship between two CIs whereby a second CI is included in the first CI.

Display Name	CI Type	Description
UDDI Registry	**uddiregistry**	Provides a standards-based foundation for locating services, invoking services and managing metadata about services (security, transport, or quality of service). This is similar to the traditional phone book's yellow and white pages.
Web Service	**webservice**	Represents a web service.
Web Service Operation	**webservice_operation**	Represents a web service operation.

13

Performing an SQL Discovery

This chapter explains how to discover SQL servers and their components on your network.

This chapter describes:	On page:
Step 1 – Preparing for an SQL Discovery	209
Step 2 – Running the Pre-Discovery Pattern	212
Step 3 – Running the Discovery Patterns	212
Step 4 – Checking that the Discovery Ran Correctly	213
CIs Discovered by the Discovery Process	214

Note: For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

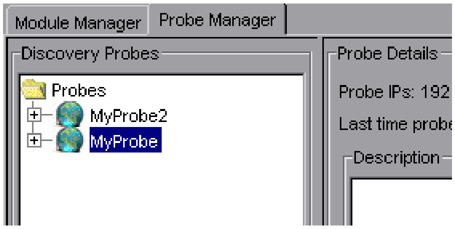
Step 1 – Preparing for an SQL Discovery

Before you run an SQL discovery, you must add a discovery probe and define the protocols.

Note: Ensure that the Discovery Probe is running.

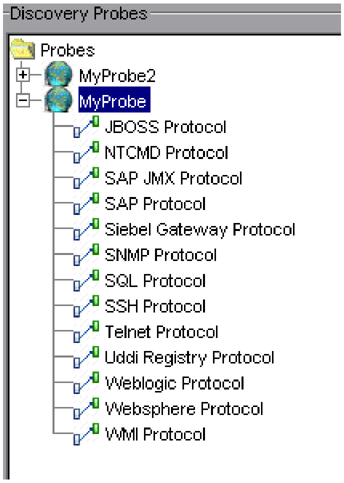
To prepare for an SQL discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the Probe Manager pane.
4. In the Discovery Probes pane, select the relevant Discovery Probe.



5. Click the **Add IP Range** button to open the Add IP Range window.
6. Enter the range of IP addresses that includes the IP address of the probe you want to discover.
7. Click **OK**.
8. Click the **Add IP Range** button to open the Add Range window once more.
9. Enter the range of IP addresses that includes the system with the SQL agent you want to discover.
10. Click **OK**.
11. Click **Apply** to save the changes you have made.

12 Expand the Discovery Probe:



13 Select **SQL Protocol**, and click the **Add new connection details for the selected protocol type** button. The Add Protocol Parameters dialog box opens.

14 Populate the following fields:

- **User Name**. The name of the user you use to connect to the host as administrator.
- **User Password**. The password of the user you use to connect to the host as administrator.
- **Port Number**. The default port which is used by Microsoft SQL is 1433.
- **Database Type**. Select **Microsoft SQL Server**.
- **Database Name**. The name assigned to the SQL database.

15 Click **OK** to save the changes.

Step 2 – Running the Pre-Discovery Pattern

Click the Module Manager tab. Expand the module, select the pattern, and activate it.

Expand Module	Activate Pattern	Description
Network Advanced	**TCP_NET_Dis_Port**	Discovers open TCP ports on a host of known server ports.

Step 3 – Running the Discovery Patterns

To run the discovery patterns, you must trigger them in the order described in this section. Each discovery pattern discovers different components. For details on the components, see “CIs Discovered by the Discovery Process” on page 214.

To run the discovery patterns:

Note: Before running the discovery patterns, verify that the machine where the SQL server is installed is using port 1433.

Click the Module Manager tab. Expand the modules, select the patterns, and activate them.

Expand Module	Activate Pattern	Description
Database - SQL Server	**SQL_NET_Dis_Connection**	Try to connect to host with known database port using JDBC and SQL protocol credentials
Database - SQL Server	**SQL_APP_Dis_SqlServer**	Discover Microsoft SQL Server in detail (SQL_NET_Dis_Connection is a prerequisite)

Step 4 – Checking that the Discovery Ran Correctly

After running all the discoveries, check that all the information is displayed correctly.

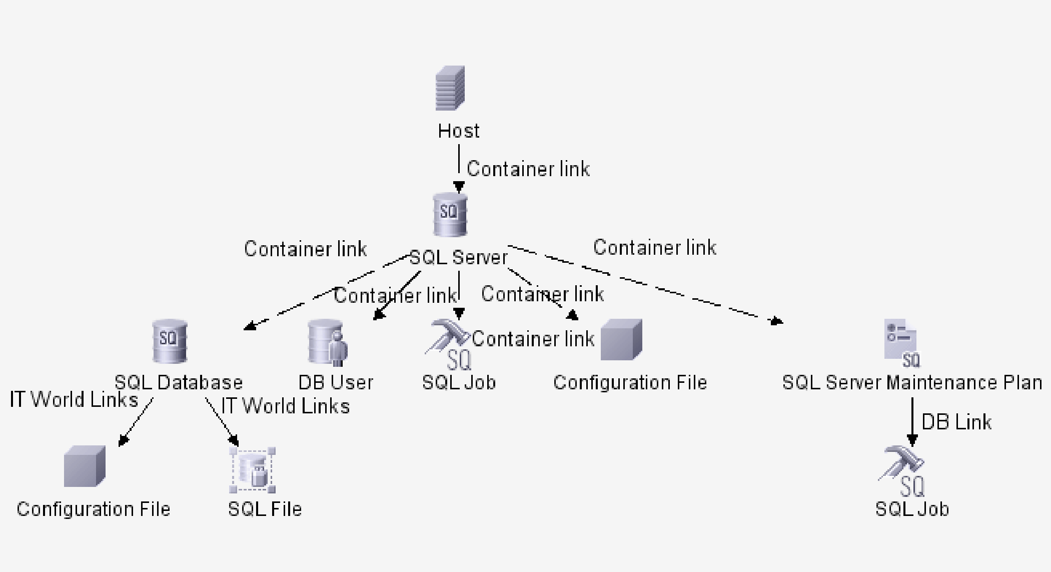
To check that the discovery ran correctly:

1 Select **Admin** > **CMDB**.

2 Click the **IT Universe** tab.

3 In the Folders pane, select the view called **SQL Server.**

The following depicts the topology of the SQL Server view:



This SQL Server view shows the hosts on which an SQL server is installed. The SQL server contains the SQL server databases, users, SQL jobs, and configuration files of this server and maintenance plans.

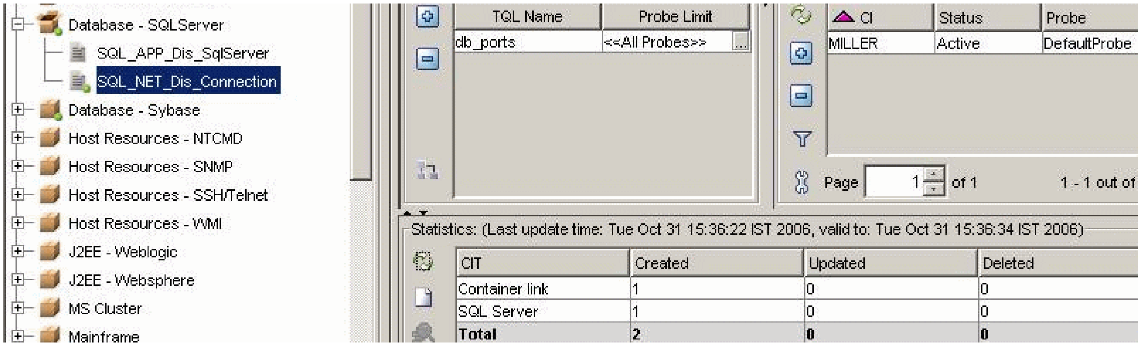
CIs Discovered by the Discovery Process

You can view the CIs discovered by the SQL discovery.

To view the CIs discovered by the SQL discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the **Module Manager** tab.
4. In the **Discovery Modules** pane, expand the **SQL Server** module and select the **SQL_NET_Dis_Connection** pattern.

   ➤ In the **Details View** tab, the **Statistics** table displays the CIs discovered by the **SQL_NET_Dis_Connection** pattern.



TQL Name	Probe Limit
db_ports	<<All Probes>>

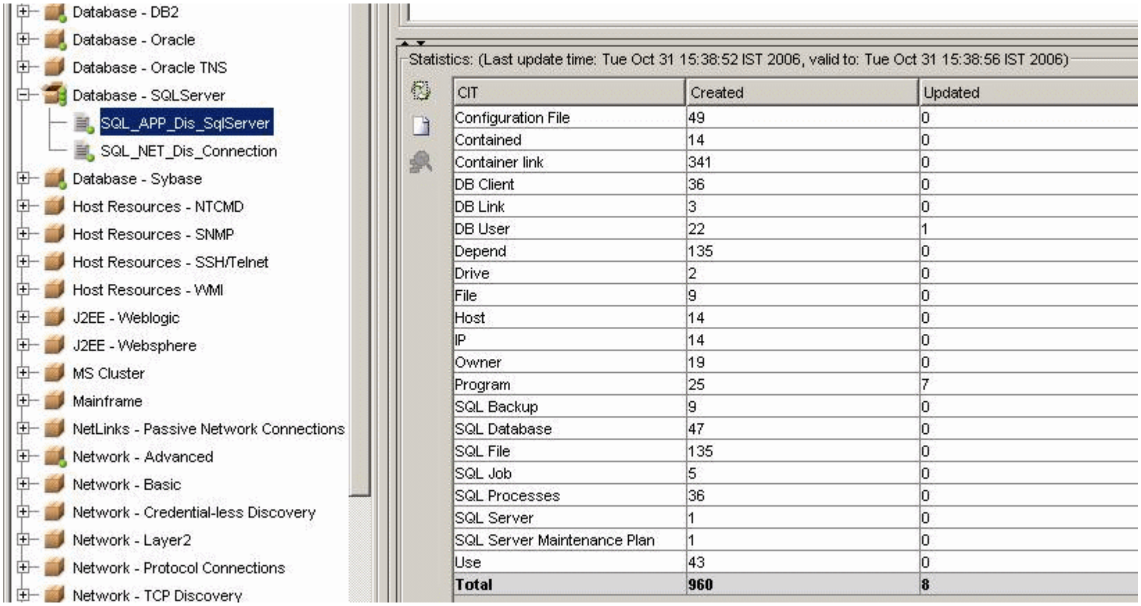
CI	Status	Probe
MILLER	Active	DefaultProbe

Page 1 of 1 1 - 1 out of

Statistics: (Last update time: Tue Oct 31 15:36:22 IST 2006, valid to: Tue Oct 31 15:36:34 IST 2006)

CIT	Created	Updated	Deleted
Container link	1	0	0
SQL Server	1	0	0
Total	**2**	**0**	**0**

➤ Select the **SQL_APP_Dis_SqlServer** pattern. In the **Details View** tab, the **Statistics** table displays the CIs discovered by the **SQL_APP_Dis_SqlServer** pattern.



Statistics: (Last update time: Tue Oct 31 15:38:52 IST 2006, valid to: Tue Oct 31 15:38:56 IST 2006)

CIT	Created	Updated
Configuration File	49	0
Contained	14	0
Container link	341	0
DB Client	36	0
DB Link	3	0
DB User	22	1
Depend	135	0
Drive	2	0
File	9	0
Host	14	0
IP	14	0
Owner	19	0
Program	25	7
SQL Backup	9	0
SQL Database	47	0
SQL File	135	0
SQL Job	5	0
SQL Processes	36	0
SQL Server	1	0
SQL Server Maintenance Plan	1	0
Use	43	0
Total	**960**	**8**

The following table contains a description of the discovered CIs.

Display Name	CI Type	Description
Configuration File	**configfile**	Holds data regarding a configuration file of the SQL server.
Contained	**contained**	The relationship that links the nodes and IPs.
Container Link	**container_f**	The relationship that links the discovered resource to the group to which it belongs.
DB Client	**dbclient**	
DB Link	**dblink**	
DB User	**dbuser**	Contains all the defined users in the database.

Display Name	CI Type	Description
Depend	**depend**	The link between resources.
Drive	**drive**	A hard disk drive.
File	**file**	An entity of data.
Host	**host**	The host represents a network element which has a unique IP address.
IP	**ip**	Represents an IP address which identifies the sender or receiver of information that is sent over the internet.
Owner	**owner**	The link between a node and its groups.
Program	**program**	The name of the installed software or application.
SQL Backup	**sqlbackup**	A backup file which was generated by the system by or by user requests.
SQL Database	**sqldatabase**	SQL database from Microsoft.
SQL File	**sqlfile**	SQL file.
SQL Job	**sqljob**	A job is a specified series of operations performed sequentially by SQL Server Agent. A job can perform a wide range of activities including running Transact-SQL scripts, command line applications, and Microsoft ActiveX scripts.
SQL Processes	**sqlprocesses**	SQL processes.
SQL Server	**sqlserver**	SQL server.
SQL Server Maintenance Plan	**sqlservermaintenanceplan**	
Use	**use**	Use link.

14

Performing a Microsoft Cluster Server Discovery

This chapter explains how to discover the topology of a Microsoft Cluster Server on your network.

This chapter describes:	On page:
Step 1 – Preparing for a Microsoft Cluster Server Discovery	218
Step 2 – Running the Pre-Discovery Patterns	220
Step 3 – Running the Discovery Pattern	221
Step 4 – Checking that the Discovery Ran Correctly	221
CIs Discovered by the Discovery Process	222
Troubleshooting	224

Note: For details about how to perform a discovery, see “Running the Discovery Process” on page 25.

Step 1 – Preparing for a Microsoft Cluster Server Discovery

Before you run an Microsoft Cluster Server discovery, you must add a discovery probe and define the protocols as indicated in this section.

Note: Ensure that the Discovery Probe is running.

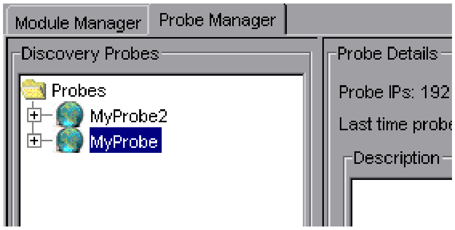
To prepare for an Microsoft Cluster Server discovery:

1 In Mercury Business Availability Center, select **Admin** > **CMDB**.

2 Click the **Discovery Manager** tab.

3 Click the Probe Manager pane.

4 In the Discovery Probes pane, select the relevant Discovery Probe.



5 Click the **Add IP Range** button to open the Add IP Range window.

6 Enter the range of IP addresses that includes the IP address of the probe you want to discover.

7 Click **OK**.

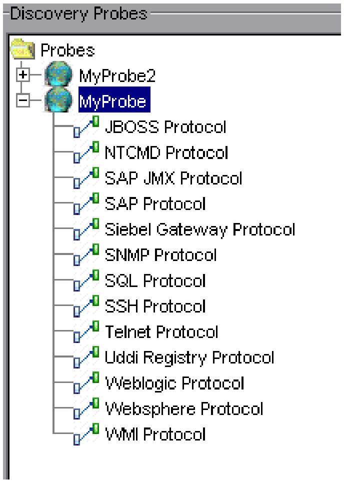
8 Click the **Add IP Range** button to open the Add Range window once more.

9 Enter the range of IP addresses that includes the system with the SQL agent you want to discover. If there is only one address, enter its value in both boxes.

10 Click **OK**.

11 Click **Apply** to save the changes you have made.

12 Expand the Discovery Probe:



Discovery Probes

Probes
- MyProbe2
- MyProbe
  - JBOSS Protocol
  - NTCMD Protocol
  - SAP JMX Protocol
  - SAP Protocol
  - Siebel Gateway Protocol
  - SNMP Protocol
  - SQL Protocol
  - SSH Protocol
  - Telnet Protocol
  - Uddi Registry Protocol
  - Weblogic Protocol
  - Websphere Protocol
  - WMI Protocol

13 Select **WMI Protocol**, and click the **Add new connection details for the selected protocol type** button. The Add Protocol Parameters dialog box opens.

14 Populate the following fields:

- **User Name**. The name of the user you use to connect to the host as administrator.
- **User Password**. The password of the user you use to connect to the host as administrator
- **NT Domain**. The name of the domain that includes the host where discovery probe is installed.

15 Click **OK** to save the changes.

16 Select **NTCMD Protocol**, and click the **Add new connection details for the selected protocol type** button. The Add Protocol Parameters dialog box opens.

17 Populate the following fields:

- **User Name**. The name of the user you use to connect to the host as administrator.
- **User Password**. The password of the user you use to connect to the host as administrator
- **Windows Domain**. The name of the domain that includes the host where discovery probe is installed.

18 Click **OK** to save the changes.

Step 2 – Running the Pre-Discovery Patterns

To run the discovery patterns, you must trigger them with pre-discovery patterns in the order described in this section. Each discovery pattern discovers different components. For details on the components, see “CIs Discovered by the Discovery Process” on page 222.

To run the pre-discovery patterns:

Click the Module Manager tab. Expand the modules, select the patterns, and activate them.

Expand Module	Activate Pattern	Description
Network - Protocol Connections	**WMI_NET_Dis_Connection**	Try to connect to a WIN server using WMI protocol
Network - Protocol Connections	**NTCMD_NET_Dis_Connection**	Try to connect to a WIN server using xCmd (NetBIOS)
Host Resources - WMI	**WMI_HR_Service**	DIscover services on host using WMI

Step 3 – Running the Discovery Pattern

This section describes the pattern you need to activate to run the Microsoft Cluster Server discovery.

To run the discovery pattern:

In the Module Manager tab, expand the module, select the pattern, and activate it.

Expand Module	Activate Pattern	Description
MS Cluster	**MS_Cluster_Topology**	Discover Microsoft Cluster Server architecture by NTCMD

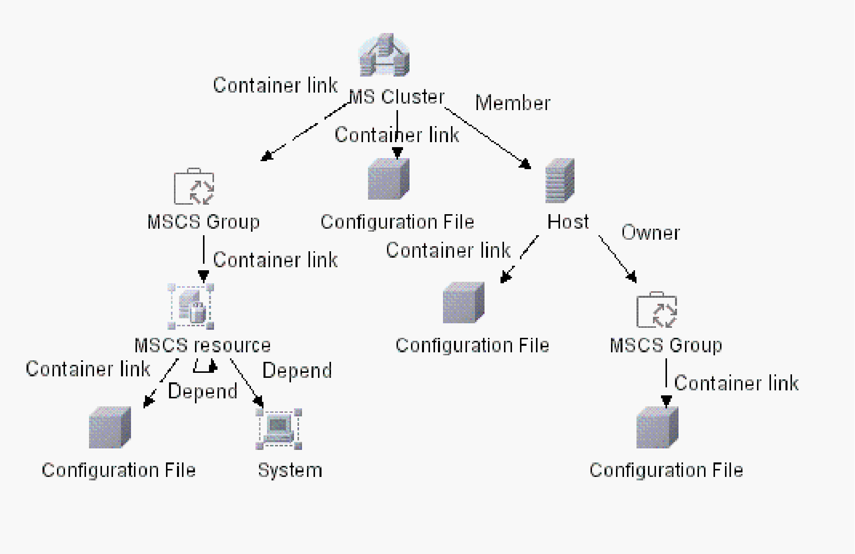
Step 4 – Checking that the Discovery Ran Correctly

After running all the discoveries, check that all the information is displayed correctly.

To check that the discovery ran correctly:

1. Select **Admin** > **CMDB**.
2. Click the **IT Universe** tab.
3. In the Folders pane, select the view called **Microsoft Cluster Server.**

The following depicts the topology of the Microsoft Cluster Server view:



This Microsoft Cluster Server view shows the clusters discovered in the system. The clusters contains Microsoft Cluster groups. Each of the groups contains Microsoft Cluster resources.

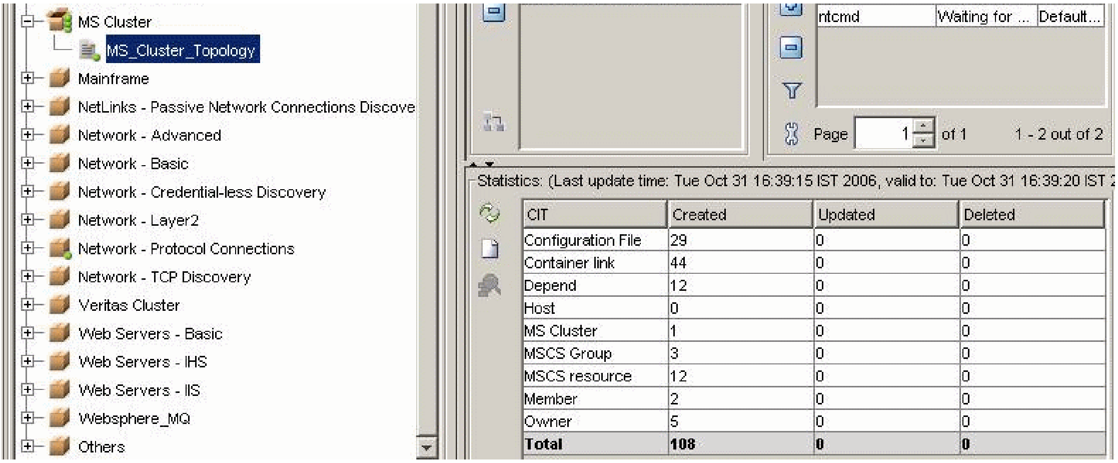
CIs Discovered by the Discovery Process

You can view the CIs discovered by the Microsoft Cluster Server discovery.

To view the CIs discovered by the Microsoft Cluster Server discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the **Module Manager** tab.
4. In the **Discovery Modules** pane, expand the **MS Cluster** module and select the MS_Cluster_Topology pattern.

In the **Details View** tab, the **Statistics** table displays the CIs discovered by the Microsoft Cluster Server discovery.



MS Cluster
MS_Cluster_Topology
Mainframe
NetLinks - Passive Network Connections Discove
Network - Advanced
Network - Basic
Network - Credential-less Discovery
Network - Layer2
Network - Protocol Connections
Network - TCP Discovery
Veritas Cluster
Web Servers - Basic
Web Servers - IHS
Web Servers - IIS
Websphere_MQ
Others

ntcmd	Waiting for ...	Default...

Page 1 of 1 1 - 2 out of 2

Statistics: (Last update time: Tue Oct 31 16:39:15 IST 2006, valid to: Tue Oct 31 16:39:20 IST 2

CIT	Created	Updated	Deleted
Configuration File	29	0	0
Container link	44	0	0
Depend	12	0	0
Host	0	0	0
MS Cluster	1	0	0
MSCS Group	3	0	0
MSCS resource	12	0	0
Member	2	0	0
Owner	5	0	0
Total	**108**	**0**	**0**

The following table contains a description of the discovered CIs.

Display Name	CI Type	Description
Contained	**contained**	The relationship that links the nodes and IPs.
Configuration File	**configfile**	Holds data regarding a configuration file of an application.
Host	**host**	The host represents a network element which has a unique IP address.
IP	**ip**	Represents an IP address which identifies the sender or receiver of information that is sent over the internet.
MS Cluster	**mscluster**	The Microsoft cluster server.
MSCS Group	**mscsgroup**	Collection of dependent or related resources to be manages as a single unit.
MSCS Resource	**mscsresource**	Physical or logical entity managed by a cluster node. A resource provides a service to clients in a client/server environment.
Member	**member**	The link between a cluster and its nodes.

Display Name	CI Type	Description
Owner	**owner**	The link between a node and its groups.
Depend	**depend**	The link between resources.

Troubleshooting

This section provides information that can help troubleshooting some of the problems that can occur when performing an Microsoft Cluster Server discovery.

Problem 1. You do not have access to the requested cluster command.

Solution 1. Contact your administrator.

Problem 2. Clus_Svc was not discovered.

Solution 2. The discovered host is not a cluster node.

Part VI

Appendixes

A

Optional Variables in Discovery Patterns

To ensure that a discovery pattern does not fail if a specific variable is missing, add the attribute **optional="true"** to a variable tag in a discovery pattern.

If the **optional="true"** attribute is added, every reference to the missing variable is replaced by either:

- An empty string " " as a value
- A default value if it is provided for the attribute

Use the following syntax to define the default value. The default value appears in bold:

<destinationData name="retry">${SNMP.snmp_retry:**5**}</destinationData>

In the following example, the **optional="true"**attribute was added to the variable tag and $SNMP was not found. The retry value is replaced by **5** since the value that is put after the colon (:) becomes the default value if the attribute does not exist.

```
<variables>
        <variable name="SNMP" getObjectBy="condition" optional="true">
                <condition>
                        <object id="-1" class="snmp" subsystem="6" container_name="host_applicationlist">
                                <attribute name="snmp_port" type="java.lang.Integer" list="false"
operator="EQ">161</attribute>
                                <attribute name="root_container" type="host" list="false" operator="EQ">
                                        <object id="${HOST.root_id}" class="host" subsystem="6" />
                                </attribute>
                         </object>
                </condition>
        </variable>
</variables>
```

Note: Discovery patterns that do not use optional variables fail if the specified variables are not found.

B

Discovery Patterns

This appendix contains details on the following discovery patterns.

This chapter describes:	On page:
Application – Oracle E-Business Suite	231
Application – SAP	232
Application – Siebel	236
Application – Webservices	240
Database – DB2	240
Database – Oracle	240
Database – Oracle TNS	244
Database – SQL Server	246
Database – Sybase	248
Host Resources – NTCMD	249
Host Resources – SNMP	250
Host Resources – SSH/FD	252
Host Resources – WMI	253
J2EE – Weblogic	255
J2EE – Websphere	257
MS_Cluster	259
Mainframe	260
NetLinks – Passive Network Connections Discovery	261

This chapter describes:	On page:
Network – Advanced	263
Network – Basic	265
Network – Credential-Less Discovery	267
Network – Layer2	269
Network – Protocol Connections	271
Network – TCP Discovery	275
Veritas Cluster	279
Web Servers – Basic	280
Web Servers – IHS	281
Web Servers – IIS	282
Websphere_MQ	283
Others	285

Application – Oracle E-Business Suite

Pattern		
OracleApps	Package	OracleApps
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ DB Tablespace ➤ Depend ➤ Deployed ➤ Host ➤ IP ➤ Member ➤ Oracle ➤ Oracle Application ➤ Service ➤ Service Manager ➤ Oracle iAS ➤ Oracle E-Business Suite ➤ Web Component ➤ Process ➤ Resource ➤ Use
	TQL	oracle_database
	Schedule	Once a day
	Notes	

Application – SAP

Pattern		
SAP_Dis_Applications	Package	SAP_discovery
	Parse Method	
	Protocol	SAP Protocol
	Discovered CIs/Relationships	➤ Container link ➤ Contains ➤ SAP Application Component ➤ SAP Transaction ➤ SAP Transport ➤ SAP Transport Charge ➤ Use
	TQL	sapsystem_connected
	Schedule	Once a day
	Notes	

Pattern		
SAP_Dis_ITS	Package	SAP_discovery
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ Depend ➤ Host ➤ IP ➤ SAP ITS AGate ➤ SAP ITS WGate ➤ SAP R/3 Application Server
	TQL	sap_its_process
	Schedule	Once a day
	Notes	
SAP_Dis_J2EE_Site	Package	SAP_discovery
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ Depend ➤ Host ➤ IP ➤ SAP ITS AGate ➤ SAP ITS WGate ➤ SAP R/3 Application Server
	TQL	sap_jmx_ports
	Schedule	Once a day
	Notes	

Pattern		
SAP_Dis_Site	Package	SAP_discovery
	Parse Method	
	Protocol	SAP_Protocol
	Discovered CIs/Relationships	➤ Configuration File ➤ Contained ➤ Container link ➤ Database ➤ Depend ➤ Host ➤ IP ➤ Member ➤ SAP Client ➤ SAP Gateway ➤ SAP R\3 Application Server ➤ RFC Connection ➤ sap_software_component ➤ sap_support_package ➤ SAP System ➤ SAP Work Process ➤ Use
	TQL	sap_ports
	Schedule	Once a day
	Notes	

Pattern		
SAP_Dis_SolutionManager	Package	SAP_discovery
	Parse Method	
	Protocol	SAP Protocol
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ Execute ➤ Host ➤ IP ➤ SAP Project ➤ SAP Business Process ➤ SAP Business Scenario ➤ SAP Process Step ➤ SAP Transaction
	TQL	sapsystem_connected
	Schedule	Once a day
	Notes	
WMI_APP_Lis_IIS_Down.xml	Package	IIS_Resources_By_WMI
	Parse Method	Dynamic
	Protocol	WMI (DCOM)
	Discovered CIs/Relationships	
	Monitored CIs/Relationships	iis
	TQL	iis_server
	Schedule	Once
	Notes	destination oriented DCOM listener, pulling

Application – Siebel

Pattern		
SIEBEL_DIS_APP SERVERS	Package	Siebel_discovery
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration file ➤ Contained ➤ Container link ➤ Contains ➤ Depend ➤ Host ➤ IP ➤ Member ➤ Siebel Application Server ➤ Siebel Application ➤ Siebel Component Group ➤ Siebel Component
	TQL	siebel_gtwy_connected
	Schedule	Once a day
	Notes	

Pattern		
SIEBEL_DIS_APP_SERVER_CONFIG	Package	Siebel_discovery
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration file ➤ Container link ➤ Siebel Application Server
	TQL	siebel_appserver_shell
	Schedule	Once a day
	Notes	
SIEBEL_DIS_DB_NT	Package	Siebel_discovery
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Database ➤ Depend ➤ Host ➤ Use
	TQL	siebel_appserver_nt
	Schedule	Once a day
	Notes	

Pattern		
SIEBEL_DIS_DB_UNIX	Package	Siebel_discovery
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Database ➤ Depend ➤ Host ➤ Use
	TQL	siebel_appserver_shell
	Schedule	Once a day
	Notes	
SIEBEL_DIS_GATEWAY_ CONNECTION_(GTWY)	Package	Siebel_discovery
	Parse Method	
	Protocol	Siebel Gateway Protocol
	Discovered CIs/Relationships	➤ Container link ➤ Member ➤ Siebel Gateway ➤ Siebel Enterprise
	TQL	siebel_ports_or_gtwy
	Schedule	Once a day
	Notes	

Pattern		
SIEBEL_DIS_WEBAPPS_NT	Package	Siebel_discovery
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration file ➤ Container link ➤ Contains ➤ Depend ➤ Host
	TQL	siebel_webserver_nt
	Schedule	Once a day
	Notes	
SIEBEL_DIS_WEBAPPS_UNIX	Package	Siebel_discovery
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration File ➤ Container link ➤ Contains ➤ Depend ➤ Host
	TQL	siebel_webshell_server
	Schedule	Once a day
	Notes	

Application – Webservices

Pattern		
UDDI_Registry	Package	Webservice_discovery
	Parse Method	
	Protocol	Uddi Registry Protocol
	Discovered CIs/Relationships	➤ Business Unit ➤ Business Unit link ➤ Configuration File ➤ Container link ➤ Contains
	TQL	local
	Schedule	Once a day
	Notes	

Database – DB2

Pattern		
SQL_APP_Dis_Db2	Package	DB2
	Parse Method	
	Protocol	SQL Protocol
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ DB2 ➤ DB2 Client ➤ DB2 Data File
	TQL	db2withuser
	Schedule	Every 1410 minutes
	Notes	

Pattern		
SQL_APP_Dis_Db2_Conn	Package	Database_Basic
	Parse Method	
	Protocol	SQL Protocol
	Discovered CIs/Relationships	➤ Container link ➤ DB2 ➤ Host
	TQL	db2_db_port
	Schedule	Every 1410 minutes
	Notes	
TCP_NET_Dis_Port	Package	Network
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Server Port ➤ User
	TQL	host
	Schedule	Once a day
	Notes	

Database – Oracle

Pattern		
CF_Oracle	Package	Oracle
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration File ➤ Container link
	TQL	oracle_database
	Schedule	Once a day
	Notes	

Pattern		
SQL_Dis_Oracle	Package	Oracle
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ DB_Archive File ➤ DB_Control-File ➤ DB_Re-do File ➤ DB_Re-do File group ➤ FBA Object ➤ DB Client ➤ DB Data File ➤ DB Job ➤ DB Link Object ➤ DB Scheduler Job ➤ DB Snapshot ➤ DB Tablespace ➤ DB User ➤ Depend ➤ Dependency ➤ Host ➤ IP ➤ Member ➤ Oracle ➤ Owner ➤ Program ➤ Oracle RAC ➤ Resource ➤ Service
	TQL	oracle_database
	Schedule	Once a day
	Notes	

Pattern		
SQL_NET_Dis_Connection	Package	Database Basic
	Parse Method	
	Protocol	SQL Protocol
	Discovered CIs/Relationships	➤ Container link ➤ Oracle ➤ SQL Server
	TQL	db_ports
	Schedule	Once a day
	Notes	

Database – Oracle TNS

Pattern		
CF_Oracle	Package	Oracle
	Parse Method	
	Protocol	TCP
	Discovered CIs/Relationships	➤ Configuration File ➤ Container link
	TQL	oracle_database
	Schedule	Once a Day
	Notes	

Pattern		
SQL_Oracle_Connection	Package	Oracle
	Parse Method	
	Protocol	SQL Protocol
	Discovered CIs/Relationships	➤ Container Link ➤ Oracle
	TQL	oracle_database
	Schedule	Once a Day
	Notes	
TNSNamesParser	Package	Oracle
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration File ➤ Contained ➤ Container Link ➤ Host ➤ IP ➤ Oracle
	TQL	host_tnsnames_shell
	Schedule	Once a Day
	Notes	

Database – SQL Server

Pattern		
SQL_APP_Dis_SqlServer	Package	SQL_Server
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration File ➤ Contained ➤ Container link ➤ DB Client ➤ DB Link ➤ DB User ➤ Depend ➤ Drive ➤ File ➤ Host ➤ IP ➤ Owner ➤ Program ➤ Replicated ➤ SQL Backup ➤ SQL Database ➤ SQL File ➤ SQL Job ➤ SQL Processes ➤ SQL Server ➤ Sql Server Distributor ➤ SQL Server Maintenance Plan ➤ SQL Server Publication ➤ SQL Server Publisher ➤ SQL Server Subscription ➤ Use

Pattern		
SQL_APP_Dis_SqlServer	TQL	sqlServer
	Schedule	Once a Day
	Notes	
SQL_NET_Dis_Connection	Package	Database_Basic
	Parse Method	
	Protocol	SQL Protocol
	Discovered CIs/Relationships	➤ Container link ➤ Oracle ➤ SQL Server
	TQL	sqlServer
	Schedule	Once a Day
	Notes	

Database – Sybase

Pattern		
SQL_APP_Dis_Sybase	Package	Sybase
	Parse Method	
	Protocol	SQL Protocol
	Discovered CIs/Relationships	➤ Container link ➤ DB Client ➤ DB Data File ➤ DB Tablespace ➤ Host ➤ Process ➤ Resource ➤ Sybase
	TQL	sybase_db
	Schedule	Once a Day
	Notes	
SQL_NET_Dis_sybase_Conn	Package	Database_Basic
	Parse Method	
	Protocol	SQL Protocol
	Discovered CIs/Relationships	➤ Container link ➤ Host ➤ Sybase
	TQL	sybase_db_port
	Schedule	Every1410 minutes
	Notes	

Pattern		
TCP_NET_Dis_Port	Package	Network
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Server Port ➤ Use
	TQL	host
	Schedule	Once a Day
	Notes	

Host Resources – NTCMD

Pattern		
NTCMD_HR_All	Package	Host_Resources_By_NTCM D
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ CPU ➤ Disk ➤ Memory ➤ Program ➤ Service ➤ Software
	TQL	ntcmd
	Schedule	Once a Day
	Notes	

Host Resources – SNMP

Pattern		
SNMP_HR_Disk	Package	Host_Resources_By_SNMP
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Disk
	TQL	snmp
	Schedule	Once a Day
	Notes	
SNMP_HR_OSUser	Package	Host_Resources_By_SNMP
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Disk
	TQL	snmp
	Schedule	Once a Day
	Notes	
SNMP_HR_Printq	Package	Host_Resources_By_SNMP
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container Link ➤ Print Queue
	TQL	snmp
	Schedule	Once a Day
	Notes	

Pattern		
SNMP_HR_Process	Package	Host_Resources_By_SNMP
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Process
	TQL	snmp
	Schedule	Once a Day
	Notes	
SNMP_HR_Service	Package	Host_Resources_By_SNMP
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Service
	TQL	snmp
	Schedule	Once a Day
	Notes	
SNMP_HR_Software	Package	Host_Resources_By_SNMP
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Software
	TQL	snmp
	Schedule	Once a Day
	Notes	

Host Resources – SSH/FD

Pattern		
TTY_HR_All	Package	Host_Resources_By_TTY
	Parse Method	
	Protocol	XCMD (NetBIOS)
	Discovered CIs/Relationships	Container link CPU Dir Disk Memory OS User Software
	TQL	shell_on_unix
	Schedule	Once a Day
	Notes	
TTY_HR_Process	Package	Host_Resources_By_TTY
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	Container link Process
	TQL	shell_on_unix
	Schedule	Once a Day
	Notes	

Host Resources – WMI

Pattern		
WMI_HR_CPU	Package	Host_Resources_By_WMI
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ CPU
	TQL	wmi
	Schedule	Once on Arrival
	Notes	
WMI_HR_Disk	Package	Host_Resources_By_WMI
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Disk
	TQL	wmi
	Schedule	Once on Arrival
	Notes	
WMI_HR_Memory	Package	Host_Resources_By_WMI
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Memory
	TQL	wmi
	Schedule	Once on Arrival
	Notes	

Pattern		
WMI_HR_Process	Package	Host_Resources_By_WMI
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Program
	TQL	wmi
	Schedule	Once on Arrival
	Notes	
WMI_HR_Service	Package	Host_Resources_By_WMI
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Container link ➤ Service
	TQL	wmi
	Schedule	Once on Arrival
	Notes	

J2EE – Weblogic

Pattern		
JMX_J2EE_Weblogic	Package	J2EE
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration File ➤ Connection Pool ➤ Contained ➤ Container link ➤ Contains ➤ Database ➤ Depend ➤ Deployed ➤ Document ➤ EJB Module ➤ Entity Bean ➤ J2EE Execute Queue ➤ Host ➤ IP ➤ J2EE Application ➤ J2EE Cluster ➤ J2EE Domain ➤ J2EE Server ➤ J2EE Socket ➤ JDBC Datasource ➤ JMS Data Store ➤ JMS Destination ➤ JMS Server ➤ JVM ➤ Member ➤ Message Driven Bean

Pattern		
JMX_J2EE_Weblogic (cont'd)	Discovered CIs/Relationships	➤ Servlet ➤ SQL Database ➤ Statefull Session Bean ➤ Stateless Session Bean ➤ Use ➤ Web Module) ➤ Web Service ➤ Web Service Operation
	TQL	sqlServer
	Schedule	Once a Day
	Notes	
JMX_J2EE_Weblogic_Connection	Package	J2EE
	Parse Method	
	Protocol	Weblogic Protocol
	Discovered CIs/Relationships	➤ Container link ➤ J2EE Server
	TQL	weblogic_ports
	Schedule	Once a Day
	Notes	

J2EE – Websphere

Pattern		
JMX_J2EE_Websphere	Package	J2EE
	Parse Method	
	Protocol	Websphere Protocol
	Discovered CIs/Relationships	➤ Configuration File ➤ Container link ➤ Contains ➤ Database ➤ Depend ➤ Deployed ➤ Document ➤ EJB Module ➤ Entity Bean ➤ Host ➤ J2EE Application ➤ J2EE Cluster ➤ J2EE Server ➤ JDBC Data Source ➤ JDBC Provider ➤ JMS Provider ➤ JMS Server ➤ JVM ➤ Member ➤ Message Driven Bean ➤ Servlet ➤ SQL Database ➤ Statefull Session Bean ➤ Stateless Session Bean ➤ Use ➤ Web Module ➤ Web Service ➤ Web Service Operation

Pattern		
JMX_J2EE_Websphere	TQL	websphere
	Schedule	Once a Day
	Notes	
JMX_J2EE_Websphere_Connection	Package	J2EE
	Parse Method	
	Protocol	Websphere Protocol
	Discovered CIs/Relationships	➤ Container link ➤ Websphere
	TQL	websphere_ports
	Schedule	Once a Day
	Notes	

MS_Cluster

Pattern		
MS_Cluster_Topology	Package	MS_Cluster
	Parse Method	
	Protocol	
	Discovered CIs/Relationships	➤ Configuration File ➤ Contained ➤ Container link ➤ Depend ➤ Host ➤ IP ➤ Member ➤ MS Cluster ➤ MSCS Group ➤ MSCS resource ➤ Owner
	TQL	ntcmd_on_mscs
	Schedule	Once a day
	Notes	

Mainframe

Pattern		
SNMP_IBM_Mainframe_lpar_discovery	Package	Mainframe
	Parse Method	
	Protocols	clientserver & tcp relationships for ipserver /ipclient
	Discovered CIs/Relationships	➤ Client-Server ➤ Contained ➤ Container link ➤ Dependency ➤ Host ➤ IP ➤ Client Port ➤ Server Port ➤ Logical Partition ➤ Member ➤ Service ➤ Sysplex ➤ Use
	TQL	ip_on_mainframe_without_lpar
	Schedule	Once a Day
	Notes	

NetLinks – Passive Network Connections Discovery

Pattern		
NetFlow_StartCollector	Package	NetLinks
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	
	TQL	local
	Schedule	Once on Arrival
	Notes	
Netlinks_Potential_Services	Package	NetLinks
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Client Server ➤ Contained ➤ Container link ➤ Host ➤ IP ➤ Server Port
	TQL	
	Schedule	Once a Day
	Notes	

Pattern		
Netlinks_Services	Package	NetLinks
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Client-Server ➤ Contained ➤ Container link ➤ Dependency ➤ Host ➤ IP ➤ Server Port ➤ Use
	TQL	local
	Schedule	Every 10 Minutes
	Notes	
Netlinks_ServicesConnectivity	Package	NetLinks
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Contained ➤ Host ➤ IP ➤ Traffic
	TQL	server ip
	Schedule	Once a Day
	Notes	

Network – Advanced

Pattern		
SNMP_NET_Dis_HostBase	Package	Network
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ ATM Switch ➤ Bridge ➤ Contained ➤ Container link ➤ Firewall ➤ Host ➤ Interface ➤ Interface Index ➤ IP ➤ LB ➤ Member ➤ Net Device ➤ Net Printer ➤ Network ➤ Windows ➤ Parent ➤ RAS ➤ Route ➤ Router ➤ SNMP ➤ Switch ➤ trminalserver ➤ Unix ➤ Unnumbered ➤ VAX ➤ X Terminal

Pattern		
SNMP_NET_Dis_HostBase	TQL	snmp
	Schedule	Once a Day
	Notes	
SNMP_NET_Dis_Router_Arp	Package	Network
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ Host ➤ Interface ➤ IP ➤ Member ➤ Network ➤ Parent
	TQL	snmp_router
	Schedule	Once a Day
	Notes	
TCP_NET_Dis_Port	Package	Network
	Parse Method	
	Protocols	SSH
	Discovered CIs/Relationships	clientserver & tcp relationships for ipserver /ipclient
	TQL	host
	Schedule	
	Notes	

Network – Basic

Pattern		
Host_ID_Discover	Package	Network
	Parse Method	
	Protocols	NTCMD Protocol SNMP Protocol SSH Protocol Telnet Protocol WMI Protocol
	Discovered CIs/Relationships	➤ ATM Switch ➤ Contained ➤ Container link ➤ Firewall ➤ Host ➤ Interface ➤ IP ➤ LB ➤ Mainframe ➤ Member ➤ Net Device ➤ Net Printer ➤ Network ➤ novell ➤ Windows ➤ NTCMD ➤ Parent ➤ RAS ➤ Router ➤ SNMP

Pattern		
Host_ID_Discover (cont'd)	Discovered CIs/Relationships	➤ SSH ➤ Switch ➤ Telnet ➤ trminalserver ➤ Unix ➤ VAX ➤ WMI ➤ X Terminal
	TQL	➤ ip
	Schedule	➤ Once a Day
	Notes	
ICMP_NET_Dis_IpC	Package	Network
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Depend ➤ IP ➤ Member
	TQL	network_C
	Schedule	Once a Day
	Notes	

Network – Credential-Less Discovery

Pattern		
MS_NET_Dis_Domain	Package	Network
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Contained ➤ Host ➤ IP ➤ Member ➤ MS Domain ➤ Windows
	TQL	probe
	Schedule	Once a Day
	Notes	
NSLOOKUP_on_Probe	Package	Network
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Contained ➤ Host ➤ IP ➤ Net Printer ➤ Windows ➤ Unix
	TQL	probe
	Schedule	Once a Day
	Notes	

Pattern		
OS_Fingerprint	Package	Credential_Less_Discovery
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Software Element ➤ Contained ➤ Container link ➤ Host ➤ Interface ➤ IP ➤ Server Port ➤ Member ➤ Use
	TQL	network_C
	Schedule	Once a Day
	Notes	

Network – Layer2

Pattern		
SNMP_Dis_L2_Bridge	Package	Layer2
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Bridge ➤ Concentrator ➤ Container link ➤ Physical Port
	TQL	catalyst_bridge_no_vlan
	Schedule	Once on Arrival
	Notes	
SNMP_Dis_L2_Vlan	Package	Network
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Bridge ➤ Concentrator ➤ Container link ➤ Physical Port
	TQL	catalyst_vlan_with_bridge
	Schedule	Once on Arrival
	Notes	

Pattern		
SNMP_NET_Dis_Catalyst_Vlans	Package	Layer2
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ VLAN
	TQL	snmp_of_catalyst_switch
	Schedule	Once on Arrival
	Notes	
SNMP_NET_Dis_VMS_catalyst	Package	Layer2
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Bridge ➤ Container link ➤ Contains ➤ Physical Port ➤ VLAN ➤ VLAN Membership ➤ Vlan ToBridge
	TQL	catalyst_vlan
	Schedule	Once on Arrival
	Notes	

Network – Protocol Connections

Pattern		
NTCMD_NET_Dis_Connection	Package	Network
	Parse Method	
	Protocols	NTCMD Protocol
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ Host ➤ Interface ➤ IP ➤ Member ➤ Network ➤ Windows ➤ NTCMD ➤ Parent
	TQL	ip
	Schedule	Once a Day
	Notes	

Pattern		
SNMP_NET_Dis_Connection	Package	Network
	Parse Method	
	Protocols	SNMP Protocol
	Discovered CIs/Relationships	➤ ATM Switch ➤ Contained ➤ Container link ➤ Firewall ➤ Host ➤ Interface ➤ IP ➤ LB ➤ Mainframe ➤ Member ➤ Net Device ➤ Net Printer ➤ Network ➤ novell ➤ Windows ➤ RAS ➤ Router ➤ SNMP ➤ Switch ➤ trminalserver ➤ Unix ➤ VAX ➤ X Terminal
	TQL	ip
	Schedule	Once a Day
	Notes	

Pattern		
TTY_Net_Dis_Connection	Package	Network
	Parse Method	
	Protocols	SSH Protocol Telnet Protocol
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ Host ➤ Interface ➤ IP ➤ Member ➤ Network ➤ Parent ➤ SSH ➤ Telnet
	TQL	ip
	Schedule	Once a Day
	Notes	

Pattern		
WMI_NET_Dis_Connection	Package	Network
	Parse Method	
	Protocols	WMI Protocol
	Discovered CIs/Relationships	Contained Container link Host Interface IP Member Network Windows WMI
	TQL	ip
	Schedule	Once a Day
	Notes	

Network – TCP Discovery

Pattern		
Dis_TCP	Package	TCP_discovery
	Parse Method	
	Protocols	NTCMD Protocol
	Discovered CIs/Relationships	➤ Client-Server ➤ Contained ➤ Container link ➤ Dependency ➤ Host ➤ IP ➤ Server Port ➤ IP Unknown ➤ Traffic ➤ Use
	TQL	snmp_and_shell
	Schedule	Once a Day
	Notes	

Pattern		
SNMP_NET_Dis_Connection	Package	Network
	Parse Method	
	Protocols	SNMP Protocol
	Discovered CIs/Relationships	➤ ATM Switch ➤ Contained ➤ Container link ➤ Firewall ➤ Host ➤ Interface ➤ IP ➤ LB ➤ Mainframe ➤ Member ➤ Net Device ➤ Net Printer ➤ Network ➤ novell ➤ Windows ➤ RAS ➤ Router ➤ SNMP ➤ Switch ➤ trminalserver ➤ Unix ➤ VAX ➤ X Terminal
	TQL	ip
	Schedule	Once a Day
	Notes	

Pattern		
TTY_Net_Dis_Connection	Package	Network
	Parse Method	
	Protocols	SSH Protocol Telnet Protocol
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ Host ➤ Interface ➤ IP ➤ Member ➤ Network ➤ Parent ➤ SSH ➤ Telnet
	TQL	ip
	Schedule	Once a Day
	Notes	

Pattern		
WMI_NET_Dis_Connection	Package	Network
	Parse Method	
	Protocols	WMI Protocol
	Discovered CIs/Relationships	➤ Contained ➤ Container link ➤ Host ➤ Interface ➤ IP ➤ Member ➤ Network ➤ Windows ➤ WMI
	TQL	ip
	Schedule	Once a Day
	Notes	

Veritas Cluster

Pattern		
Veritas_Cluster_Topology	Package	Vertias_cluster
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Configuration File ➤ Contained ➤ Container link ➤ Depend ➤ Host ➤ IP ➤ Member ➤ Owner ➤ VCS Group ➤ VCS resource ➤ Veritas Cluster
	TQL	shell_of_veritas_cs
	Schedule	Once a Day
	Notes	
	TQL	ip
	Schedule	Once a Day
	Notes	

Web Servers – Basic

Pattern		
Apache	Package	WebServer
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Configuration File ➤ Contained ➤ Container link ➤ Host ➤ IP ➤ Server Port ➤ Use ➤ Web Server ➤ Web Server Virtual Host
	TQL	shell_on_unix
	Schedule	Once a Day
	Notes	
TCP_Webserver_Detection	Package	WebServer
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Web Server
	TQL	http_ports
	Schedule	Once a Day
	Notes	

Web Servers – IHS

Pattern		
IHS_Dis_WebspherePlugin	Package	IBM_HTTP_Server
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Configuration File ➤ Contained ➤ Container link ➤ Host ➤ HTTP Context ➤ IBM HTTP Server ➤ IP ➤ Server Port ➤ Route
	TQL	unix_ihs_shell
	Schedule	Once on Arrival
	Notes	

Web Servers – IIS

Pattern		
NTCMD_APP_Dis_IIS	Package	IIS
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Configuration File ➤ Container link ➤ Contains ➤ IIS Resource ➤ Server Port ➤ Use ➤ Web Service ➤ Web Service Operation ➤ Web Server Virtual Host
	TQL	host_ntcmd_iis
	Schedule	Once a Day
	Notes	

Websphere_MQ

Pattern		
MQ_Topology	Package	Websphere_MQ
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Host ➤ IP ➤ Server Port ➤ Member ➤ IBM MQ Alias ➤ IBM MQ Alias Queue ➤ IBM MQ Channel ➤ IBM MQ Channel Of ➤ IBM MQ Client Connection Channel ➤ IBM MQ Cluster Reciever Channel ➤ IBM MQ Cluster Sender Channel ➤ IBM MQ Requester Channel ➤ IBM MQ Sender Channel ➤ IBM MQ Sender Channel ➤ IBM MQ Cluster ➤ IBM MQ Queue ➤ IBM MQ Queue Local ➤ IBM MQ Queue Manager

Pattern		
MQ_Topology (cont'd)	Discovered CIs/Relationships	➤ IBM MQ Queue Remote ➤ IBM MQ Repository ➤ IBM MQ Transmission Q ➤ Raw Event ➤ Use ➤ IBM Websphere MQ
	TQL	shell_on_mq_host
	Schedule	Once a Day
	Notes	

Others

Pattern		
FILE_Mon	Package	FileMonitoring
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Configuration File ➤ Container link ➤ Dir ➤ Document
	TQL	host_shell
	Schedule	Once a Day
	Notes	
ICPM_NET_Dis_IpB	Package	Network
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Depend ➤ IP ➤ Member
	TQL	network_B
	Schedule	Once a Day
	Notes	

Pattern		
JMX_J2EE_JBoss	Package	J2EE
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Connection Pool ➤ Container link ➤ EJB Module ➤ Entity Bean ➤ J2EE Server ➤ JMS Destination ➤ JMS Server ➤ JVM ➤ Message Driven Bean ➤ Servlet ➤ Statefull Session Bean ➤ Stateless Session Bean ➤ Web Application
	TQL	jboss_server
	Schedule	Once a Day
	Notes	
JMX_J2EE_JBoss_Connection	Package	J2EE
	Parse Method	
	Protocols	JBOSS Protocol
	Discovered CIs/Relationships	➤ Container link ➤ J2EE Server
	TQL	rmi_ports
	Schedule	Once a Day
	Notes	

Pattern		
NSLOOKUP_on_DNS_Server	Package	Network
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Contained ➤ Host ➤ IP ➤ Net Printer ➤ Windows ➤ Unix
	TQL	dns_server_shell
	Schedule	Once a Day
	Notes	
NTCMD_HR_Dis_Disk	Package	Host_Resources_By_NTCMD
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Disk
	TQL	ntcmd
	Schedule	Once a Day
	Notes	

Pattern		
NTCMD_HR_Dis_Memory	Package	Host_Resources_By_NTCMD
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Memory
	TQL	ntcmd
	Schedule	Once a Day
	Notes	
NTCMD_HR_Dis_Process	Package	Host_Resources_By_NTCMD
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Program
	TQL	ntcmd
	Schedule	Once a Day
	Notes	
NTCMD_HR_REG_CPU	Package	Host_Resources_By_NTCMD
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ CPU
	TQL	ntcmd
	Schedule	Once a Day
	Notes	

Pattern		
NTCMD_HR_REG_Service	Package	Host_Resources_By_NTCMD
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Service
	TQL	ntcmd
	Schedule	Once a Day
	Notes	
NTCMD_HR_REG_Software	Package	Host_Resources_By_NTCMD
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Software
	TQL	ntcmd
	Schedule	Once a Day
	Notes	
SQL_NET_Dis_db2_from_db2	Package	Database_Basic
	Parse Method	
	Protocols	SQL Protocol
	Discovered CIs/Relationships	DB2
	TQL	db2_no_user
	Schedule	Every 7 Days
	Notes	

Pattern		
SQL_NET_Dis_informix_Conn	Package	Database_Basic
	Parse Method	
	Protocols	SQL Protocol
	Discovered CIs/Relationships	Container link informix
	TQL	informixdb_port
	Schedule	Every 7 Days
	Notes	
TTY_HR_CPU	Package	Host_Resources_By_TTY
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ CPU
	TQL	shell_on_unix
	Schedule	Once a Day
	Notes	
TTY_HR_Disk	Package	Host_Resources_By_TTY
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Disk
	TQL	shell_on_unix
	Schedule	Once a Day
	Notes	

Pattern		
TTY_HR_Memory	Package	Host_Resources_By_TTY
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Memory
	TQL	shell_on_unix
	Schedule	Once a Day
	Notes	
TTY_HR_Software	Package	Host_Resources_By_TTY
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Software
	TQL	shell_on_unix
	Schedule	Once a Day
	Notes	
TTY_HR_User	Package	Host_Resources_By_TTY
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Dir ➤ OS User
	TQL	shell_on_unix
	Schedule	Once a Day
	Notes	

Pattern		
WMI_HR_Software	Package	Host_Resources_By_WMI
	Parse Method	
	Protocols	
	Discovered CIs/Relationships	➤ Container link ➤ Software
	TQL	
	Schedule	Once on Arrival
	Notes	

C

Discovery Methods

This chapter describes the list of supported discovery methods, the protocol type that is used to communicate with the device or application, the data that can be discovered, and the required permissions or prerequisites for each type of protocol and operating system.

Mercury Business Availability Center discovery methods hold the logic for the discovery of IT infrastructure components for OSI layers 2 to 7. For details, refer to http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#xtocid5.

Discovered Domain	Through Protocol	Permissions/ Prerequisites	Discovered Data	Notes
Layer 2	SNMP	SNMP community string with GET permission.	➤ concentrator (switch) ➤ port	
IP sweep	ICMP	N/A	IP	

Discovered Domain	Through Protocol	Permissions/ Prerequisites	Discovered Data	Notes
Network infrastructure	SNMP	SNMP community string with GET permission.	➤ host ➤ IP ➤ interface ➤ SNMP ➤ network ➤ bridge ➤ port ➤ layertwo relationships ➤ backbone relationships ➤ route relationships ➤ bridge relationships	
	Telnet	Regular (non-root) operating system user.	➤ host ➤ IP ➤ interface ➤ Telnet ➤ network	
	SSH	Regular (non-root) operating system user	➤ host ➤ IP ➤ interface ➤ SSH ➤ network	
	WMI	Non-admin account with only “Enable Account” and “Remote Enable”.	➤ host ➤ IP ➤ interface ➤ wmi ➤ network	

Discovered Domain	Through Protocol	Permissions/ Prerequisites	Discovered Data	Notes
	NTCMD	Admin user	➤ host ➤ IP ➤ interface ➤ ntcmd ➤ network	
	Java	Etc/hosts	DNS name for IP.	
Server inventory	SNMP	SNMP community string with GET permission	➤ disk ➤ printq ➤ program ➤ service ➤ software ➤ operating ➤ system user	Server inventory can be discovered by: ➤ SNMP ➤ Telnet ➤ WMI ➤ NetBios ➤ BB
	TTY (Telnet or SSH)	Regular (non-root) operating system user	➤ disk ➤ daemon ➤ software ➤ program.	
	NetBIOS	Admin User	➤ service ➤ software ➤ disk ➤ program	
	WMI	Admin User	➤ CPU ➤ disk ➤ memory ➤ program ➤ service	
TCP connections	SNMP	SNMP community string with GET permission	➤ IPserver ➤ IPclient ➤ TCP relationships	

Discovered Domain	Through Protocol	Permissions/ Prerequisites	Discovered Data	Notes
	NetBIOS	Administrator Windows User/Password	➤ IPserver, ➤ IPclient ➤ TCP relationships	
	Telnet	Local Admin User	➤ IPserver ➤ IPclient ➤ TCP relationships	
	SSH	Regular (non-root) operating system user	➤ IPserver ➤ IPclient ➤ TCP relationships	
Microsoft domains	WIN API	N/A	➤ msdomain ➤ nt	
DB2	SQL	DB user with select permissions for sysproc, sysibm and sysproc table functions	➤ DB2 ➤ DB Tablespace ➤ DB Datafile ➤ DB Client ➤ Host ➤ IP ➤ Process	

Discovered Domain	Through Protocol	Permissions/ Prerequisites	Discovered Data	Notes
Oracle	SQL	DB user with READ permission from V$ and DBA_ tables	➤ dbaobjects ➤ dbarchivefile ➤ dbclient ➤ dbcontrolfile ➤ dbdatafile ➤ dbjob ➤ dblinkobj ➤ dbredofile ➤ dbsnapshot ➤ dbtablespace ➤ dbuser ➤ owner ➤ program	Data sources: dba_data_files, dba_db_links, dba_jobs, dba_objects, dba_snapshots, dba_tablespaces, dba_users, v$backup, v$controlfile, v$database, v$datafile, vlog, vlogfile, v$parameter, v$recover_file, v$session Versions 8.x, 9i
SQL Server	SQL	Access to master tables	➤ sqldatabase ➤ sqlbackup ➤ sqlalert ➤ sqljob ➤ sqljobstep ➤ sqlperformance ➤ monitor ➤ sqlprocesses ➤ program ➤ dbclient ➤ sqlfile ➤ disk	Data sources: ➤ sysprocesses ➤ sysdatabases ➤ backupset ➤ sysalerts ➤ sysjobs ➤ sysloginsysjobhistory ➤ sysjobschedules ➤ sysperfinfo Versions 7, 8
Sybase	SQL		sybasedb	Data source: sysdatabases Versions 11, 12

Discovered Domain	Through Protocol	Permissions/ Prerequisites	Discovered Data	Notes
WebSphere_ MQ	Telnet	UNIX Operating System Account on an MQ server that allows SUDO access to : ➤ clusqmgr ➤ dspmq ➤ runmqlsr	➤ mqqueuemanager ➤ mqcluster ➤ mqxmitq ➤ mqqueuelocal ➤ mqqueueremote ➤ mqaliasq ➤ mqqueue ➤ mqalias ➤ mqchsdr ➤ mqchsvr ➤ mqchannel ➤ mqchannelof ➤ mqchrqstr ➤ mqchclntconn ➤ mqchclusrcvr ➤ mqchclussdr ➤ webspheremq	Version 5.3
	NetBIOS	Administrator Windows User/Password		
Weblogic	JMX	JMX MBean Server User/Password	➤ Jboss ➤ jmsdestination ➤ jmsserver ➤ ejbcomponent ➤ webapplication ➤ servlet ➤ connectionpool ➤ j2eecluster	Versions 6.1, 7.0, 8.1

Discovered Domain	Through Protocol	Permissions/ Prerequisites	Discovered Data	Notes
JBoss	JMX	JMX MBean Server User/Password	➤ Jboss ➤ jmsdestination ➤ jmsserver ➤ ejbcomponent ➤ webapplication ➤ servlet ➤ connectionpool ➤ j2eecluster	Versions 2.3, 3.2, 4
WebSphere Application Server	JMX	JMX MBean Server User/Password		Versions 5.0, 5.1
SAP	BAPI	SAP user/password for SAPGUI	➤ SAP server ➤ SAP site ➤ SAP service ➤ SAP support package ➤ SAP component	Versions 3, 4
Siebel	Siebel protocol	Siebel user/password for the Server Manager utility	➤ Siebel appserver ➤ Siebel compgrp ➤ Siebel component ➤ Siebel gateway ➤ Siebel site ➤ Siebel wse ➤ Siebel webapp ➤ Siebel webserver	Versions 7.5, 7.7
	WMI	Admin User	➤ database ➤ dbconnector	

Discovered Domain	Through Protocol	Permissions/ Prerequisites	Discovered Data	Notes
	Telnet	Regular (non-root) operating system user	➤ database ➤ Siebel application server ➤ siebelwse ➤ siebelgateway ➤ siebelsite ➤ siebelwebapp ➤ webserver	
	SSH	Regular (non-root) operating system user	➤ database ➤ Siebel App server ➤ siebelwse ➤ siebelgateway ➤ siebelsite ➤ siebelwebapp ➤ webserver	
	NTCMD	Admin User	➤ Siebelwse ➤ Siebel gateway ➤ Siebel site ➤ Siebel webapp ➤ Siebel webserver	

D

Discovery Log Files

This chapter describes various discovery log files and how you can use them to perform basic troubleshooting.

This chapter describes:	On page:
Understanding Discovery Log Files	301
Discovery Server Logs	302
Discovery Probe Logs	304

Understanding Discovery Log Files

The Discovery Probe is composed of two components: the Probe Gateway and the Probe Manager. The Probe Gateway is responsible for communication with the Mercury Business Availability Center server, such as downloading tasks and sending task results. The Probe Manager is responsible for running the discovery process itself. By default, they run as a single process.

Discovery log files store messages relating to the activation of discovery patterns. This includes a record of errors that may have occurred when trying to activate a discovery pattern.

Discovery Server Logs

Discovery Server log files reside on the Mercury Business Availability Center server. They store information about discovery server activity, including error messages that occur on the server side.

The logs in this section are located in <**Mercury Business Availability Center root directory**>**\log**.

- "Management Log" on page 302
- "User Servlet Log" on page 303
- "Probe Servlet Logs" on page 303

Management Log

- The log name is **collectorsManagement.log**. In a distributed environment, the **collectorsManagement.log** file resides on the Data Processing server.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
Contains information about tasks running on the server. The server provides services to the Mercury Business Availability Center user interface or the Probe Gateway, such as: activating patterns, processing results from the Discovery Probe, or creating tasks for the Discovery Probe.	All discovery process errors on the server side.	Information about requests being processed.	Logs mainly for debugging purposes.	Check this log when you have invalid user interface responses or errors you want to explore. This log provides information to enable you to analyze the problems.

User Servlet Log

➤ The log name is **collectorsUtilitiesServlet.log**.In a distributed environment, the **collectorsUtilitiesServlet.log** file resides on the Center server.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
This log receives all the messages from the Collectors Utilities Servlet. The user interface connects to the server through this servlet.	All errors in the servlet.	Information about user requests.	Record of any user request.	1. Look at this log mostly to see user User Interface-Server communication problems. 2. Some processing problems might be written to this log instead of the **collectorsManagement.log**.

Probe Servlet Logs

➤ The log name is **collectorsServlet.log**.In a distributed environment, the **collectorsServlet.log** file resides on the Core server.

Purpose	Informati on Level	Error Level	Debug Level	Basic Troubleshooting
This log receives all the messages from the Collectors Servlet. The Discovery Probe requests new tasks from the server through this servlet.	All errors in the servlet.	Information about Discovery Probe task requests.	Record of every Discovery Probe request to read discovery tasks.	1. Check this log to see Discovery Probe-Server communication problems. 2. Some processing problems might be written to this log instead of the **collectorsManagement.log**

- The log name is **collectorsResultsServlet.log.**In a distributed environment, the **collectorsResultsServlet.log** file resides on the Core server.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
This log receives all the messages from the **Collectors Results Servlet**. The Discovery Probe sends new results through this servlet.	All errors in the servlet.	Information about Discovery Probe Tasks requests.	N/A	1. Look at this log mostly to see Discovery Probe-Server communication problems. 2. Some processing problems might appear in this log instead of the **collectorsManagement.log**.

- The log name is **collectorsDownloadServlet.log.**In a distributed environment, the **collectorsDownloadServlet.log** file resides on the Core server.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
This log receives all the messages from collectors Download Servlet. The Discovery Probe downloads new server data through this servlet.	All errors in the servlet.	Information about Discovery Probe task requests.	Record of every Discovery Probe access of the servlet.	1. Look at this log mainly to see Probe-Server communication problems. 2. Some processing problems might appear in this log instead of the **collectorsManagement.log**.

Discovery Probe Logs

Discovery Probe logs store information involving discovery pattern activation that occurs in the Probe Gateway and Probe Manager.

The logs in this section are located in <**Mercury Business Availability Center root directory**>\<**Discovery Probe installation location**>**\root\logs.**

- "General Logs" on page 305
- "Probe Gateway Logs" on page 306

- "Probe Manager Logs" on page 307

General Logs

- The log name is **wrapperProbe.log**.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
Records all the Discovery Probe's console output in a single log file.	Any discovery error that occurs within the Probe Gateway.	Important information messages, such as the arrival or removal of a new task.	Record of every probe access of the servlet	This is the first place to look for any Probe Gateway problem. This log file shows what the Probe Gateway was doing at what time and any important problems it encountered.

- The log name is **probe-error.log**.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
Summary of the errors from the Discovery Probe.	All errors in the Discovery Probe components.	N/A	N/A	Check this log to see if errors occurred in the Discovery Probe components.

- The log name is **probe-infra.log**.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
This log lists all the infrastructure messages.	All infrastructure errors.	Information about infrastructure actions.	Messages mainly for debug purpose.	Open this log to see messages from the Discovery Probe's infrastructure only.

➤ The log name is **wrapperLocal.log.**

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
	Any discovery error that occurs within the Probe Manager.	Important information messages such as, received tasks, task activation, and the transferring of results.		This is the first place to look for any Probe Manager problem. This log file shows what the Probe Manager was doing at what time and any important problems it encountered.

Probe Gateway Logs

➤ The log name is **probeGW-taskResults.log.**

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
This log records all the tasks results sent from the Probe Gateway to the server.	N/A	Result details: task ID, pattern ID, number of CIs to delete/update.	The **ObjectState HolderVecto**r results that are sent to the server (in an XML string).	1. 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. 2. 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).

➤ The log name is **probeGW-tasks.log.**

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
This log records all the tasks received by the Probe Gateway.	N/A	N/A	The task's XML.	1. If the Probe Gateway tasks are not synchronized with the server tasks, check this log to determine which tasks the Probe Gateway received. 2. You can view the current task's state through the JMX console (Use the Discovery Scheduler MBean).

Probe Manager Logs

➤ The log name is **probeMgr-services.log**.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
Java services debug messages.	N/A	N/A	N/A	Check this log to view Java services debug messages.

➤ The log name is **probeMgr-performance.log**.

Description	Error Level	Information Level	Debug Level	Basic Troubleshooting
Performance statistics dump, collected every predefined period of time, which includes memory information and thread pool statuses.	N/A	N/A	N/A	1. Check this log to investigate memory issues over time. 2. The statistics are logged every 1 minute, by default.

- The log name is **probeMgr-patternsDebug.log**.

Description	**Error Level**	**Information Level**	**Debug Level**	**Basic Troubleshooting**
This log contains messages used to debug discovery pattern issues.	N/A	N/A	N/A	Use this log file for debugging discovery patterns.

Index

A

active and changed SAP transactions
  discover 121
active SAP transactions
  discover 119
Application CI 154
Application Component CI 128
Application Gateway CI 132
Application Server CI 156

B

Background Work Process CI 133
before you begin 6
BPM Monitor CI 129
BPM steps CI 129, 154
BPM Transaction/Location CI 155
Business Process CI 131

C

CCMS Counters CIs 134
changed SAP transactions
  discover 120
CI
  showing instances 57
CIs
  discovered by discovery process 126, 151
  discovered by the IDDI discovery process 190
  discovered by the IIS discovery process 183, 205
  discovered by the UDDI discovery process 199
  discovered by Veritas Cluster discovery process 165, 175, 214, 222
  Mercury Business Availability Center for SAP 126
CIs discovered by
  Internet Information Services (IIS) discovery 183
CITs (configuration item types) 64
Client CI 131, 134
columns in Event tabs
  hiding 34
Configuration File CI 134, 158
configuration files
  creating 61
  deleting 62
  viewing and editing 59
connection data
  configuring for protocol 40
  defining for protocol 41
  deleting for existing protocol 42
connection data for the protocol
  defining 41
Contained Group CI 153
Contained Location CI 130, 154

D

Database CI 133, 157
dependency graph
  creating 68
design view tab 69
Details View pane
  using advanced options 43
Dialog Work Process CI 133
Discovery
  SNMP 169
  SQL 209, 217
discovery

- checking it ran correctly 124, 148, 163, 174, 181, 189, 198, 205, 213, 221
- IBM WebSphere 194
- Internet Information Services (IIS) 178
- network 145
- Siebel 137, 185, 193, 201
- Veritas Cluster 159

Discovery Log Files 301
discovery log files 301
Discovery Manager 25
- Details View tab 26
- introduction 3
- Map View tab 26
- Schedule View tab 26
- understanding 26

discovery manager 26
- map view 83

discovery map view
- displaying data in 85

discovery methods 293
discovery modes
- application components 118
- SAP Transactions 118
- Transports 118

Discovery Module
- resetting statistics table 33

discovery module 5
- activating 30
- creating 31
- deactivating 31
- deleting 32
- editing 29
- updating statistics table 33

discovery modules
- accessing 114, 144

Discovery Pattern
- manually activating using specific CIs 49

discovery pattern
- creating 58
- deleting from module 58
- running 115, 146, 162, 173, 180, 188, 204, 212, 220
- running on a periodic basis 76
- updating statistics table 56

discovery patterns 4
- activating 82
- deactivating 82
- defining 70
- deleting 58
- designing 71
- editing 74
- manually activation using only specific CIs 49
- running at set time intervals 77
- running on a daily basis 77
- running on a monthly basis 78
- running on a weekly basis 78
- scheduling to run on periodic basis 75
- starting and stopping, setting date for 75
- validating 81

Discovery Probe
- installing 10

discovery probe 5
- adding 36
- configuring 36
- deleting 38
- hardware requirements 10
- installation procedure 10
- installing 9
- software requirements 10

discovery process 3
- architecture 4
- configuration files 59
- running 25

discovery protocol definitions 5
discovery range
- configuring 36

discovery TQL queries
- adding nodes and relationships 66
- creating 65
- defining domains 48
- editing 68

discovery TQL query
- creating 65

domain description, editing 38

E

Enqueue Work Process CI 133
existing discovery TQL
    editing 68

G

getting more information x

H

hierarchy 127, 152
Host CI 155
Hosts CI 132
how this guide is organized ix

I

IBM WebSphere discovery 193
IIS discovery
    preparing for 186, 202
Internet Information Services (IIS) discovery 177
IP address range
    rule definition 39
IP range
    deleting 38
    editing 39
    rules 39

J

Java Connectors
    installing 110

L

Locations CI 130

M

map view
    statistics 88
    tooltips 90
Map View tab
    printing contents of 90
Map View tab toolbar
    using 85
Mercury Business Availability Center for SAP
    CIs 126
    performing discovery 109, 159, 169, 177, 209, 217
Mercury Business Availability Center servers 5
module manager 26
Module Manager tab 27
module manager, understanding 27
modules
    managing 28
modules, managing 28
Monitor CIs 135

N

naming conventions
    XML files 21
network
    discovering 145
Network CI
    adding to trigger discovery of system networking 113, 143
node or relationship
    deleting 68
nodes, deleting 68

O

optional_variables_in_discovery_patterns 227

P

packages
    administration 15
    dependencies 18
    removing with JMX console 17
    undeploying 22
    verifying dependency 21
    verifying operations 22
pattern editor 69
pattern editor, understanding 69
pattern parameters tab 69
pattern validation indicator 69
patterns

editing 70
selecting 46
probe
selecting in discovery process 48
probe description
editing 38
protocol
editing connection details 42
protocol definitions 92
SNMP 97
SQL 100
Telnet 102
WebLogic 104
WMI 106
protocols
configuring connection data 40
deleting connection data 42

R

R/3 Application Server CI 132
range of dates
changed transactions 122
relationships, deleting 68

S

SAP Applications CI 128
SAP discovery
preparing for 110, 139, 160, 170, 178, 194, 209, 218
running 138
SAP Solution Manager discovery 125
running 125
SAP system CI 128
SAP transactions CI 129
SAP_Dis_SolutionManager 125
Siebel
discovery 137, 185, 193, 201
Siebel CIs
manual configuration 149
Siebel Component CI 157
Siebel Component Group CI 157
Siebel discovery
running 147
Siebel Enterprises CI 153
Siebel Gateway CI 156
Siebel Web Server Application CI 156
Siebel Web Server Extension CI 156
SiteScope Measurement CIs 158
SNMP Discovery 169
Software Component CI 134
Solution Manager Projects CI 130
source view tab 69
Spool Work Process CI 133
SQL Discovery 209, 217
statistics table
resetting for the selected discovery pattern 57
resetting for the selected module 33
updating for the selected discovery pattern 56
updating for the selected module 33
Support Package CI 134

T

the connection details
deleting for an existing protocol 42
toolbars
for View Manager 90
TQL
deleting 69
node and relationship definitions
setting 67
workflow 65
TQL node
setting relationship definitions 67
TQLs
deleting 69
Transport CI 131
trigger TQL queries, defining 47
trigger TQL query
defining 47
triggered CIs table
filtering 53
updating 54
triggered CIs table, updating 54
troubleshooting 21

U

Update Work Process CI 133
Update2 Work Process CI 133

V

Veritas Cluster
    CIs discovered by 165
Veritas Cluster discovery 159
View Manager
    using toolbar options 90

W

Web Gateway CI 132
Web Server CI 155
WebSphere discovery 193
who should read this guide x
Work Process
    Background Work Process CI 133
    Dialog Work Process CI 133
    Enqueue Work Process CI 133
    Spool Work Process CI 133
    Update Work Process CI 133
    Update2 Work Process CI 133

X

XML files
    naming conventions 21