HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.0

Discovery

hp ®

i n v e n t

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Third-Party Web Sites

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

Copyright Notices

Trademark Notices

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

Intel®, Pentium®, and Intel® Xeon^{TM} are trademarks of Intel Corporation in the U.S. and other countries.

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

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

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

This manual's title page contains the following identifying information:

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

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

http://ovweb.external.hp.com/lpe/doc_serv/

Support

Mercury Product Support

You can obtain support information for products formerly produced by Mercury as follows:

- If you work with an HP Software Services Integrator (SVI) partner (**http://h20230.www2.hp.com/svi_partner_list.jsp**), contact your SVI agent.

- If you have an active HP Software support contract, visit the HP Software Support Web site and use the Self-Solve Knowledge Search to find answers to technical questions.

- For the latest information about support processes and tools available for products formerly produced by Mercury, we encourage you to visit the Mercury Customer Support Web site at: **http://support.mercury.com**.

- If you have additional questions, contact your HP Sales Representative.

HP Software Support

You can visit the HP Software Support Web site at: **www.hp.com/go/hpsoftwaresupport**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest

- Submit and track support cases and enhancement requests

- Download software patches

- Manage support contracts

- Look up HP support contacts

- Review information about available services

- Enter into discussions with other software customers

- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To find more information about access levels, go to:
http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:
http://h20229.www2.hp.com/passport-registration.html

Table of Contents

PART III: DISCOVERY USER INTERFACE

Table of Contents

Welcome to This Guide

This guide describes how to install the Discovery Probe, how to manage the Discovery process and to automatically discover and map IT infrastructure resources and their interdependencies. Discovery can discover such resources as applications, databases, network devices, different types of servers, and so on.

This chapter describes:	On page:
How This Guide Is Organized	9
Who Should Read This Guide	10
Getting More Information	10

How This Guide Is Organized

The guide contains the following chapters:

Part I   **Discovery Probe Installation**

Explains how to install the Discovery Probe.

Part II   **Discovery Reference**

Describes the main Discovery concepts, tasks, and references.

Part III   **Discovery User Interface**

Describes the pages and dialog boxes that are part of the Discovery user interface.

Who Should Read This Guide

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

➤ HP Business Availability Center administrators

➤ HP Business Availability Center platform administrators

➤ HP Business Availability Center application administrators

➤ HP 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 HP Business Availability Center in general and HP Universal CMDB technology specifically.

Getting More Information

For a complete list of all online documentation included with HP Business Availability Center, additional online resources, information on acquiring documentation updates, and typographical conventions used in this guide, see the *HP Business Availability Center Deployment Guide* PDF.

Part I

Discovery Probe Installation

1

Installing the Discovery Probe

This chapter describes the procedures that are needed for the installation of the Discovery Probe on a Windows platform. Installation on a Solaris machine is not supported.

This chapter describes:	On page:
Installation Procedure	14

Installation Procedure

The following procedure explains how to install the Discovery probe.

It is recommended to install the Discovery Probe on a separate server from the Business Availability Center server, to distribute the overall system load.

To install the Discovery Probe:

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

Note: The Discovery Probe link in the Downloads page is displayed only if you have purchased a standard or advanced license for the Discovery application, and if the administrator has added the Discovery Probe link to the Downloads page. For details, see "Licensing Models" on page 23 and "Installing Component Setup Files" in the *HP Business Availability Center Deployment Guide* PDF.

---

2 Click **Discovery Probe for Windows 2000/2003/XP**. You can open the Setup file or save it to your computer:

➤ If you choose to open the file, it is not saved to your computer, and the setup program starts immediately. In this case, depending on your browser security settings, a security warning dialog box may open. Confirm that you want to proceed.

➤ If you choose to save the file to your computer, double-click the downloaded file to begin installation.

A progress bar is displayed. Once the initial process is complete, the
Introduction dialog box opens.
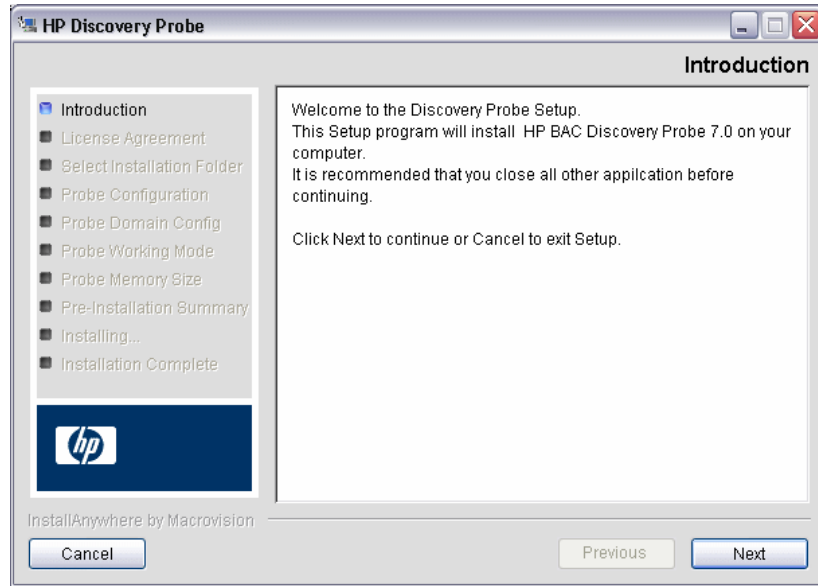
3 Click **Next** to open the License Agreement dialog box.
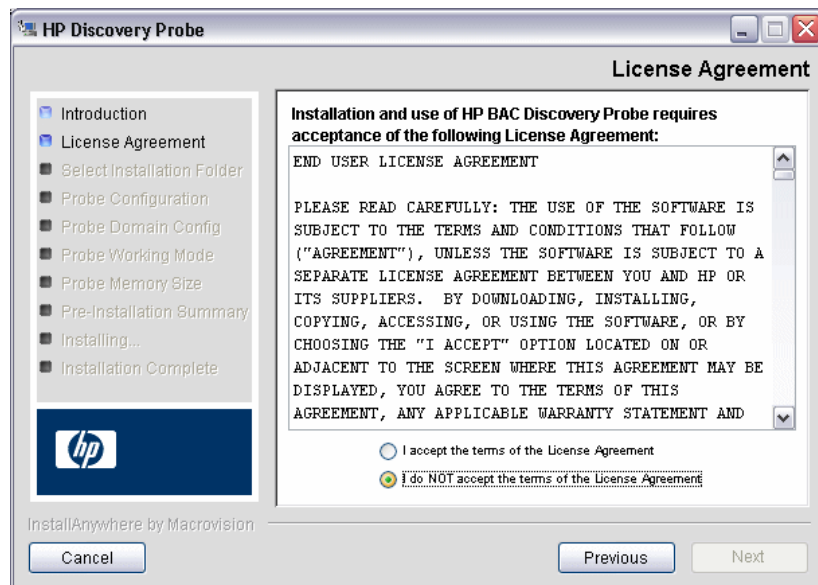
4 Accept the terms of the agreement and click **Next** to open the Select Installation Folder dialog box.
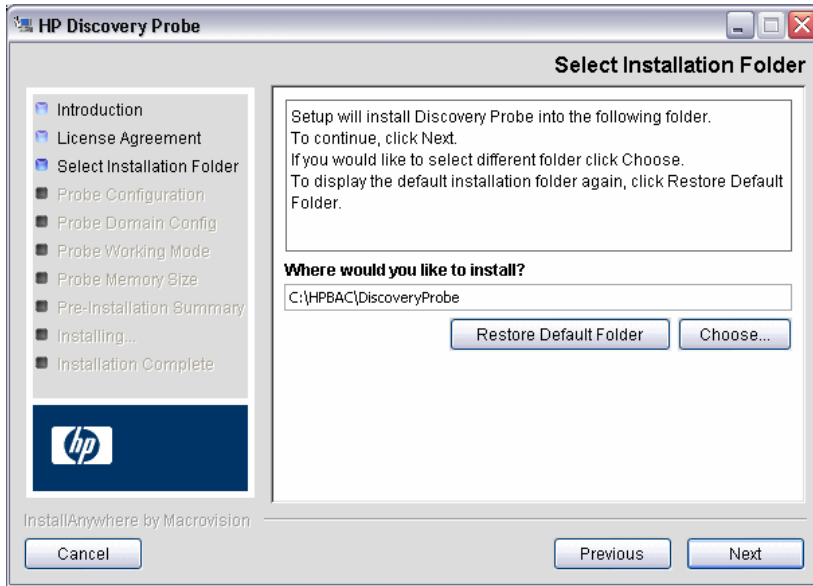
Accept the default entry or click **Choose** to display a standard Browse dialog box. To install to a different directory, browse to and select the installation folder.

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

5 Click **Next** to open the HP BAC Discovery Probe Configuration dialog box.
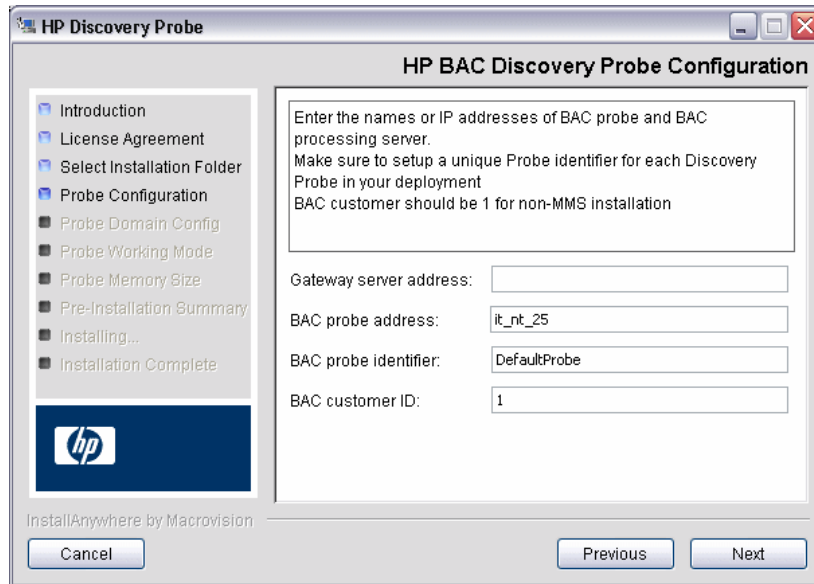
Accept the default values or make changes to the following fields:

➤ In the **Gateway Server Address** box, enter the IP or the DNS name of the Gateway Server.

➤ In the **BAC Probe Address** box, enter the IP address or the DNS name of the machine on which you are currently installing the Discovery Probe, or accept the default.

➤ In the **BAC Probe Identifier** box, enter a name for the Discovery Probe to be used for the discovery process. The Discovery Probe identifier defined here appears as the default Discovery Probe in Job Configuration. The probe identifier is taken from the **DiscoveryProbe.properties** file. If you change this entry, the new value is written to the file.

Important: The UCMDB probe identifier must be unique for each Discovery Probe in your deployment.

➤ (For HP Managed Software Solutions 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.

6 Click **Next** to open the HP BAC Discovery Probe Domain Configuration dialog box.
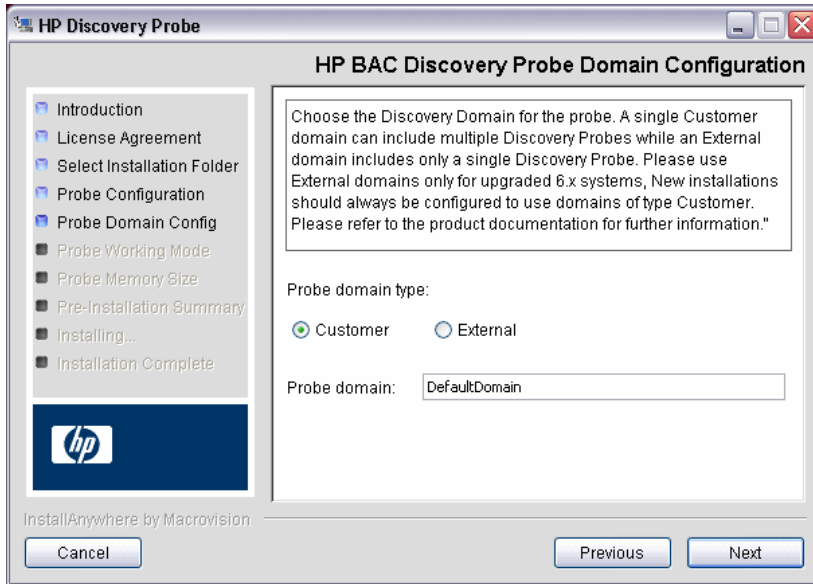
Choose between **Customer** and **External**, depending on the type of domain on which the Probe is to be running:

➤ **Customer.** Select if you are installing one or more Discovery Probes in your deployment.

Important: For new installations, always select **Customer**.

➤ **External.** Select if you are installing a single Discovery Probe in your deployment.

Important: When upgrading from version 6.x systems, select **External**.

➤ **Probe domain.** Accept the default domain name or enter another domain name. The default value is taken from the DiscoveryProbe.properties file. If you change this value, the new value is written to the file.

7 Click **Next** to open the HP BAC Discovery Probe Working Mode dialog box.
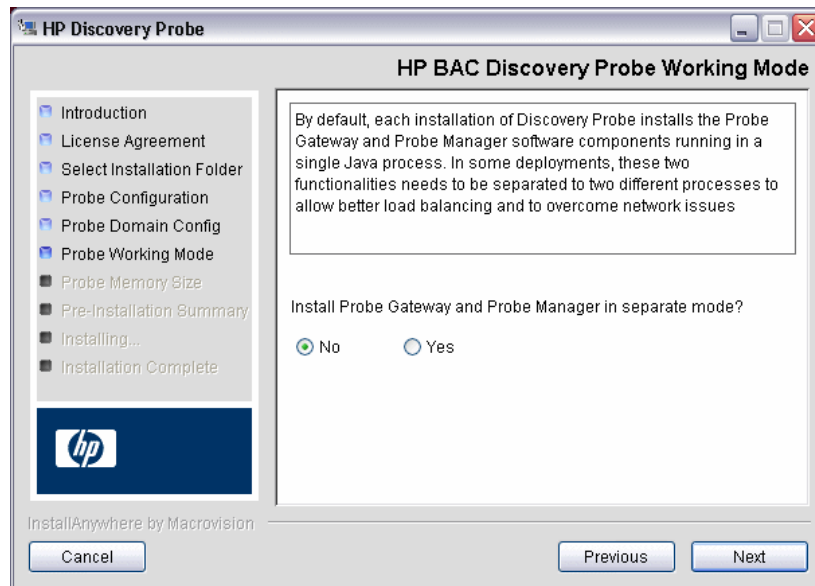
You can run the Probe Gateway and Manager as one Java process or as separate processes. You would probably run them as separate processes in deployments that need better load balancing and to overcome network issues.

For details about running Probe Gateway and Probe Manager, see "Discovery Probe Workflow – Handling Tasks" on page 39.

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

 8 Click **Next** to open the HP BAC Discovery Probe Memory Size dialog box.
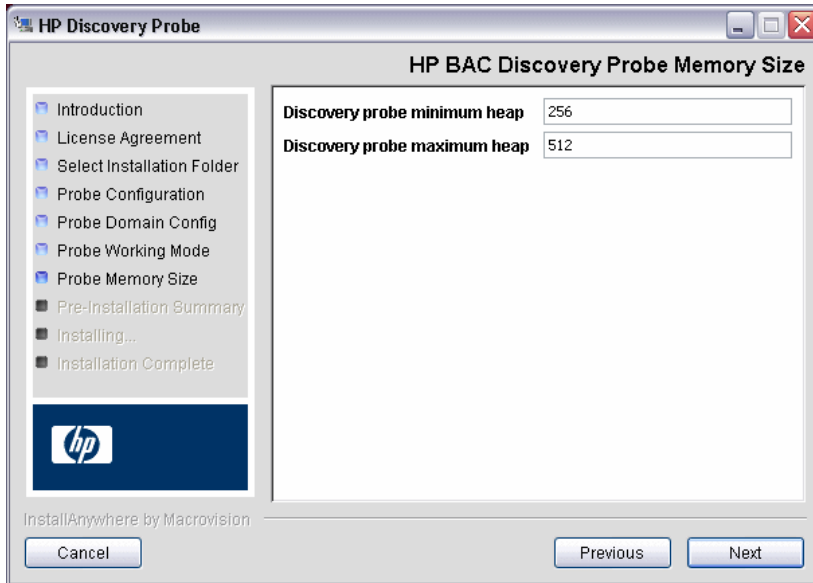
 Define the minimum and maximum memory to be allocated to the
 Discovery Probe. The values are measured in megabytes.

 For large systems (more than one hundred thousand CIs), it is
 recommended to enlarge the minimum and maximum heaps to 1 GB.
 Increase your memory max heap size for the Probe Manager. Also, separate
 the Probe Gateway and Manager to run as individual processes.

 9 Click **Next** to open the Pre-Installation Summary dialog box and review the selections you have made.
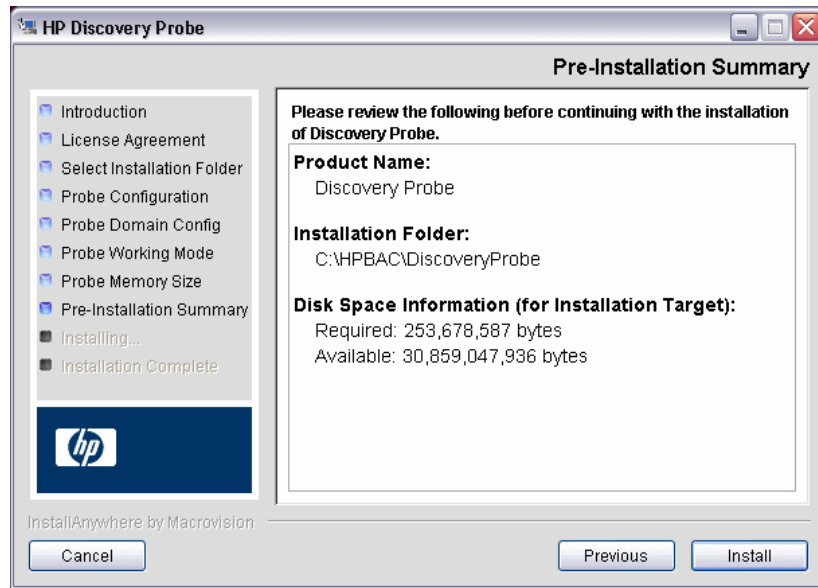
 10 Click **Install** to complete the installation of the Discovery Probe. When the installation is complete the Install Complete page is displayed.

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

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

 12 Activate the Probe by selecting the shortcut.

2

Licensing Models

This chapter describes the licensing models.

This chapter describes:	On page:
Licensing Models Overview	23
License Models	25

Licensing Models Overview

There are three levels of licensing:

➤ **Basic Edition.** Business Availability Center includes the complete class model (all CITs) and all packages. (You populate the UCMDB either manually or using integration.) Business Availability Center is provided without the Discovery or Federation features. This is the default edition.

➤ **Standard Edition.** This edition enables Discovery of the infrastructure and network.

➤ **Advanced Edition.** This edition enables Discovery of all components at your site and the ability to federate with other data sources and reconcile CIs.

For a complete list of features that are supported by each edition, see "License Models" on page 25.

Upgrading to Standard or Advanced Edition

When you install Business Availability Center you receive the Basic Edition. To obtain the file needed to upgrade to the Standard or Advanced Edition, contact Customer Support.

To upgrade Business Availability Center:

1 Obtain the appropriate file from Customer Support:
standard_ucmdb_license.xml or **advanced_ucmdb_license.xml**.

2 Stop the Business Availability Center server.

3 Place the file in the **<Business Availability Center root directory>\
mam_lib\server** folder on the Processing server machine.

If Business Availability Center is installed in a distributed deployment, on
the Gateway Server machine, use the JMX console to force the license
change:

a Launch the Web browser and navigate to:
http://<server_name>:8080/jmx-console, where <server_name> is the
name of the machine on which Business Availability Center is installed.

b Under MAM, click **service=UCMDB UI** to open the JMX MBEAN View
page.

c Locate **java.lang.String getLicenseForCustomer()** and enter the following
information:

In the force parameter box, select **True**.

In the ParamValue box for the parameter **customerId**, enter **1**.

Click **Invoke**.

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

---

4 Start the Business Availability Center server.

License Models

The following tables include the features that are available with each edition.

This section includes the following topics:

License Models

	Description	Basic Edition	Standard Edition	Advanced Edition
License Model	Per number of hosts	50 to X	50 to Y	50 to Z

Discovery

	Description	Basic Edition	Standard Edition	Advanced Edition
Discovery Methodology				
Credential-less	Support credential-less Discovery for rapid mapping of applications.	N	Y	Y
Discovery Coverage (Infrastructure)				
Layer 2	Discover and uniquely identify MAC addresses, VLANs and Layer 2 network topologies.	Y	Y	Y
Layer 3	Discover and uniquely identify IP addresses including physical and virtual IP addresses.	N	Y	Y

	Description	Basic Edition	Standard Edition	Advanced Edition
Network Discovery	**Switches and Routers**: Discovery of any SNMP V1, V2, V3 networking device, including mapping physical devices to ports, interfaces, VLANs, routing and routing protocols, and IP network topologies.	N	Y	Y
	Firewalls: Discovery of Firewall and reverse proxy devices, IP network boundaries, and devices in a redundant/HA configuration (for example, Cisco, Checkpoint, Gauntlet).	N	Y	Y
	Load Balancers: Discovery of the mapping of Virtual IPs to real IP addresses of servers configured for load balancing. Discovery of configuration files, load balancing algorithms, and end user IP addresses (for example, F5, Cisco, Nortel, Foundry, Radware).	N	Y	Y
Hosts	Discover and differentiate all flavors of Windows, Windows clustering, all flavors of UNIX, Solaris clustering and Zones, Novell, Regatta, and mainframe hosts and their resources.	N	Y	Y
Host Resources	Discovery of resources such as CPUs, disks, memory, services, daemons, event logs, and so on.	N	Y	Y

	Description	Basic Edition	Standard Edition	Advanced Edition
Mainframes	Discovery through SNMP and federation with vendor. Discovery of installed components, DB2 services and IP addresses, TCP/UDP connections, LPAR processes and Sysplexes (mainframe clustering), CICS, CICS groups and lists, CICS transactions, programs and subroutines, DB2 services, mainframe jobs, MQ series, MQ manager and individual queues, VASM, Control-M tasks and batch jobs, and JCL jobs.	N	N	Y
Virtual Machines	Discovery of VMWare virtual machines, their relationship to the physical machine (CPU, memory, disk, network) and relationship to services or components that use VMWare virtual machines.	N	N	Y
Storage	Discovery of storage arrays and configuration including number of physical drives, RAID configuration, and mapping of logical drives to physical spindles (EMC, Network Appliance).	N	N	Y

	Description	Basic Edition	Standard Edition	Advanced Edition
Discovery Coverage (Native, agentless Discovery of software)				
	LDAP: LDAP and LDAP services, dependencies on LDAP and LDAP configurations.	N	N	Y
	MS Active Directory: Discovery of Microsoft's Active Directory, to include AD servers and dependencies.	N	N	Y
	FTP: Discovery of the FTP application including the mount points of the FTP service, and the ability to execute any FTP command.	N	N	Y
	DNS: Discovery of DNS infrastructure and dependencies including DNS configuration, zone transfers, CNAMES and aliases.	N	N	Y
	MQ Series: Discovery of IBM MQ Series messaging including IBM MQ Message Channels, MQ Clusters, Queue Manager, individual message Queues and Queue services.	N	N	Y
	Web Servers: Discovery of individual Web servers that include ports and services, home directories, virtual directories and user connections (IIS, Apache, IBM, SunOne, and Tomcat).	N	N	Y
	Web Services: Discovery through the UDDI standard to retrieve Web services registry information, categories of Web services, service descriptions and compliance, business identification, Web services policy, provisioning status for all registered services, security ,and notifications.	N	N	Y

	Description	Basic Edition	Standard Edition	Advanced Edition
	J2EE: Discovery of J2EE applications, JVMs, servlets, JDBC instances (providers and connection pools), EJBs (including entity beans, message beans, session beans that are state or stateless), and JMS resources.	N	N	Y
	JBoss: Discovery of the JBoss J2EE application, including JVMs, JDBC instances (providers and connection pools), EJBs (including entity beans, message beans, session beans that are state or stateless), and JMS resources.	N	N	Y
	WebSphere: Discovery of Websphere application servers including Web services, J2EE applications, and WebSphere clustering.	N	N	Y
	WebLogic: Discovery of WebLogic application and Web servers including Web services, J2EE applications, WebLogic clustering and containers.	N	N	Y
	MS Exchange: Discovery of MS Exchange to include MS Exchange servers, MTS processes, mail stores, mail routing processes, mail proxy services, MTA agents, information stores, exchange management system, and system attendant components.	N	N	Y
	Lotus Notes: Discovery of Lotus Notes mail system, databases, application servers, collaboration services, and messaging services.	N	N	Y

	Description	Basic Edition	Standard Edition	Advanced Edition
	Citrix: Discovery of Citrix application servers, ICA client server communication, thin clients, and applications served by Citrix servers.	N	N	Y
	MS SQL: Discovery of MS SQL databases, including instances, tablespaces, users, processes, jobs (backup routines, log routines, and so on), any database objects, MS SQL clustering, and log file shipping tasks.	N	N	Y
	Oracle: Discovery of Oracle databases, including SIDs, TNS names, instances, tablespaces, users, processes, jobs (backup routines, ONP jobs, log routines, and so on), and any database objects.	N	N	Y
	Oracle RAC: Discovery of Real Application Clustering for Oracle databases and the relations to physical Oracle databases and the RAC configuration.	N	N	Y
	Informix: Discovery of Informix databases, including instances, tablespaces, users, processes, jobs (backup routines, log routines, and so on), and any database object.	N	N	Y
	Sybase: Discovery of Sybase databases, including instances, tablespaces, users, processes, jobs (backup routines, log routines, and so on), and any database objects.	N	N	Y

	Description	Basic Edition	Standard Edition	Advanced Edition
Discovery Coverage (native, agentless Discovery of ERP/CRM applications)				
	SAP: Discovery of SAP Enterprise, including SAP applications (MRP, Financial, and so on), SAP infrastructure components, SAP Web servers, application servers, gateway servers, individual SAP components, messages, brokers, and configuration files.	N	N	Y
	Siebel: Discovery of Siebel Enterprise, including Siebel applications (Call Center, Financial, and so on), Siebel infrastructure components, Siebel Web servers, application servers, gateway servers, individual Siebel components and configuration files.	N	N	Y
	Oracle E-Business: Discovery of Oracle E-Business applications, such as Oracle Financials. Discovery of infrastructure components, Web servers, application servers, individual components, and configuration files.	N	N	Y
Discovery Customization	➤ Ability to edit and extend out of the box Discovery patterns. ➤ Ability to add new Discovery patterns to product installation without requiring product reboot or product upgrade. ➤ Ability to Discover and capture additional configuration files.	N	N	Y

CMDB Management

	Description	Basic Edition	Standard Edition	Advanced Edition
Schema Extensibility	Ability to extend the CMDB schema via the UI. However, the default schema must support most commonly discovered items.	N	N	Y
Business Service Definition	Ability to define business services and keep business services automatically updated.	Y	Y	Y
	Note: All editions enable the manual and automatic creation of Business CIs. The Advanced Edition also enables the manual and automatic creation of enrichment rules.			
Access Controls	Access controls by user or groups of users to update, visualize ,and manipulate the CMDB. Ability to restrict CMDB views by groups (that is, only network groups can view detailed network views).	Y	Y	Y
SDK	Web services based APIs to integrate CMDB with other repositories.	Y	Y	Y
Federation & Reconciliation	Ability to federate with other data sources and reconcile CIs.	N	N	Y
User Interface				
Web based	All other users should be able to use Web-based GUI, which includes ability to visualize maps.	Y	Y	Y
Thick client	Thick client for administrative users.	Obsolete	Obsolete	Obsolete
Scalability	Supports 10mm+ CIs.	Y	Y	Y

Transform Data into Actionable Information

	Description	Basic Edition	Standard Edition	Advanced Edition
Impact Analysis	Native ability to analyze impact of change. Ability to inject/simulate event and study impact based on application maps.	Y	Y	Y
Visualization	Customizable views: Create customizable view that consists of a user defined set of CI types. View updates: Dynamic updating of views without requiring a Discovery refresh	Y	Y	Y
Information Enrichment	Enable CIs within the CMDB to be created, updated, enriched with additional data, or removed automatically depending on pre-defined business rules.	N	Y	Y
Reporting	Pre-built reports: for most common actions such as asset, change, host dependency, and so on.	Y – Minimal set	Y – Minimal set	Y – Full set
	Customizable reports: Native ability to customize reports without need for additional development or coding.	N	N	Y
Change Tracking	Track configuration changes and create change reports.	Y	Y	Y
CI Comparisons	Compare one CI to another and highlight differences.	N	N	Y
Gold Master Support	Store Gold copies of individual CIs (for example, Oracle database). Run comparisons of the Gold copy against other instances.	N	N	Y

	Description	Basic Edition	Standard Edition	Advanced Edition
Notifications	Automatic creation of reports and e-mail notification.	N	N	Y
Navigation	Easy and speedy navigation from one view to another when views have more than 50 elements.	Y	Y	Y

Part II

Discovery Reference

3

Discovery Concepts

This chapter includes the Discovery concepts.

Discovery Overview

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

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

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

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

For a description of a typical Discovery workflow, see "Run Discovery" on page 57.

Discovery Probe Workflow – Handling Tasks

This section describes the Discovery Probe workflow.

The Discovery Probe comprises two components: the Probe Gateway and the Probe Manager.

➤ The Probe Gateway provides communication (http or https) between the Probe Manager and the Business Availability Center server, for processes such as downloading tasks and returning task results.

➤ The Probe Manager runs the Discovery process itself.

The Probe Gateway communicates with the Probe Manager using RMI.

By default, the Gateway and Manager run as a single process but they can be configured (during installation) to reside on separate processes. Moreover, several Probe Managers can be configured to connect to a single Probe Gateway. This can be useful if you want a specific Probe Manager to deal with certain Discovery jobs.

This section includes the following topics:

➤ "Stage 1. Probe Gateway" on page 39
➤ "Stage 2. Business Availability Center Server" on page 40
➤ "Stage 3. Probe Gateway" on page 40
➤ "Stage 4. Probe Manager" on page 41
➤ "Stage 5. Probe Gateway" on page 41
➤ "Stage 6. Probe and Server" on page 42
➤ "Probe Configuration Update" on page 42

Stage 1. Probe Gateway

The Business Availability Center server does not initiate tasks on the Probe; it is the Probe's responsibility to request relevant tasks to run.

Stage 2. Business Availability Center Server

At the same time as the Probe requests tasks from the server, it also sends to the server the last update time of its configuration and the last task ID received. The server returns to the Probe one of the following:

➤ Updated server data (in the case that the configuration on the Probe is not current). The server data includes: Python scripts, patterns, the Domain Scope Document dictionary file, and so on. For details, see "Probe Configuration Update" on page 42.

➤ The last task sent (if there is a mismatch between the Probe and the server last task ID).

➤ New tasks to run (if any exist):

  ➤ if a job has been deactivated, the server sends a **delete job** message to the Probe.

  ➤ If a job has been activated, the server sends a **run new job** message to the Probe.

➤ The Business Availability Center server sends the Probe a response (in XML format) with the new task data. Each task contains the job and pattern names, and the relevant trigger CI data.

  The number of trigger CIs for a task is limited (100 by default). For example, if an active job includes 1000 destinations, the job is sent to the Probe in 10 tasks with 100 trigger CIs in each task.

Stage 3. Probe Gateway

➤ When the Probe Gateway receives tasks from the Business Availability Center server, it saves them to its local database (MySQL).

➤ Periodically, a thread on the Probe Gateway scans the database for tasks and sends them to the Probe Manager. This process enables load balancing in Discovery when there are multiple Probe Managers for each Probe Gateway.

Stage 4. Probe Manager

➤ The tasks on the Probe Manager are scheduled using the Quartz third-party library. When tasks are completed, the Probe Manager sends the results (in XML format) to the Probe Gateway. (For details on Quartz, refer to the documentation at http://www.opensymphony.com/quartz/.)

➤ The Probe Manager receives a set of result objects. The Probe first performs processing on the results (for example, filters results, runs the result redundant mechanism), and only then prepares the results for sending to the Probe Gateway.

➤ The results are stored in the Probe Manager database.

➤ A thread seeks the database for results that are ready to be sent to the Probe Gateway. These results are merged into a single result, whose size does not exceed Max Result Size (currently 20,000). When results reach the Gateway, it immediately responds with a success or failure reply. Based on this acknowledgement from the Gateway, the Probe Manager marks the results as **ack** in the database, so that they are not sent again during the next cycle.

➤ The task results which have been acknowledged by the Gateway remain in the Probe Manager database till they are deleted, once a week.

➤ When results reach the Probe Gateway, they are not sent directly to the server, but are stored in the Gateway database, to avoid flooding the server with data.

Stage 5. Probe Gateway

➤ A dedicated thread on the Probe Gateway scans the database and searches for task results that are ready to be sent to the server. These results are sent to the server by the Probe Gateway, using the **sendResultsToServer()** API.

➤ If the size of data that needs to be sent is too large, it is sent in chunks (max. 50,000). The information is then updated in the CMDB (using create, update, or remove).

➤ Finally, the Probe Gateway verifies that the server has finished handling the results, deletes those results from its database (so they will not be sent again to the server), and continues sending results to the server, if any more results exist.

Stage 6. Probe and Server

In Business Availability Center version 7.0, a new synchronization process is implemented. After reading a predefined number of tasks, the Probe confirms these tasks with the server. (This process prevents the need for manually reactivating patterns or jobs.)

The following synchronization steps take place:

1 The Probe sends to the server the names of all activated jobs and the number of trigger CIs for each job.

2 The server checks that the number matches that in the CMDB:

➤ If a job is missing from the Probe, the server redispatches the job to the Probe.

➤ If the Probe has less or more than the number of CIs on the server, the server returns the names of the problematic jobs and their CIs to the Probe.

3 The Probe checks the problematic jobs list. If the Probe has a job that is not on the server, the Probe sends a **remove job** remote method call to all Probe Managers.

4 If the Probe has a CI that is not on the server, the Probe sends a **remove CI** remote method call to all Probe Managers.

5 If the server has a trigger CI that is not on the Probe, the Probe requests this CI from the server. The server returns the tasks (in XML format) and the Probe distributes this task.

Probe Configuration Update

➤ To perform Discovery, the Probe needs resource data, such as the Domain Scope Document dictionary file, scripts, and so on. The Probe is updated automatically with these resources. Along with each task request from the Probe Gateway to the server, the Probe Gateway sends the last (server) update time of its latest updated resources.

➤ The server, before returning any new tasks, validates that there are no more recently updated resources. If there are, instead of returning the regular queued tasks for the Discovery Probe, the server returns a special crafted task for updating the Probe's resources.

➤ When the Probe receives this task, it sends a **GetResouces()** request to the server, which returns a list of resources which have not been updated to the Probe. In that way the Probe is always updated with the latest system configuration files.

Discovery Job Overview

A Discovery job is a new entity in Business Availability Center version 7.0 that enables reuse of the same pattern for different discoveries, without the need to change the pattern itself. (To activate Discovery, you now activate jobs—organized in modules—and not patterns.)

Each pattern includes default configuration parameters and scheduling information that define how to perform Discovery. A Discovery job can either override the default configuration (by associating a specific set of trigger CIs with each pattern) or can run what is declared in the pattern.

Packages now contain default Discovery job definitions as well as the appropriate Discovery patterns. For details, see "Package Manager" in *IT World Model Management.*

For details on defining a new job, see "Job Editor Dialog Box" on page 145.

For details on a Discovery workflow example, see "Run Discovery" on page 57.

Discovery Agentless Technology

Discovery is an agentless technology that discovers IT environment components through a dedicated Discovery Probe residing on the customer's site. The Discovery Probe connects to HP Business Availability Center via http or https traffic to receive new tasks, send task results, and so on. For details on the Discovery Probe workflow, see "Discovery Probe Workflow – Handling Tasks" on page 39.

Although the Auto Discovery is agentless, that is, it does not require the installation of any agent on a customer's machine, Discovery depends on agents that are already installed such as:

➤ **SNMP Agent.** Provides information about the operating systems, device types, installed software and other system resources information. SNMP agents can usually be extended to support new MIBs, exposing more data for managerial purposes.

➤ **WMI Agent.** Microsoft's remote management agent, which is usually available for access by a remote administrator. The WMI agent is also extensible by adding WMI providers to the generic agent.

➤ **Telnet/SSH Agent (or daemon).** Used mostly on UNIX systems to connect remotely to a machine and to launch various commands to obtain data.

➤ **xCmd.** A remote administration technology similar in functionality to Telnet/SSH that enables launching any console command over Windows machines. xCmd relies on Administrative Shares & Remove Service Administration APIs to function correctly.

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

Discovery Process Architecture

Discovery architecture is deployed as follows:
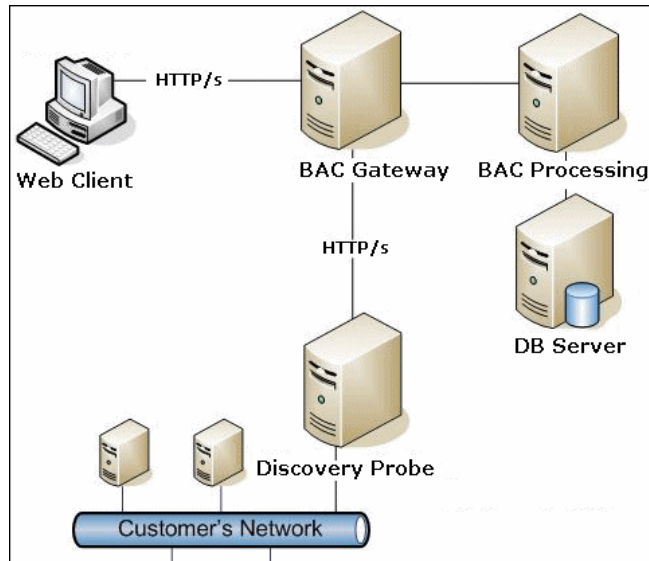
➤ Discovery User Interface

➤ The user interface servlet (collectorsUtilities) and the Discovery Probe servlets (collectorsServlet, collectorsResultsServlet, and collectorsDownloadServlet) reside on the HP Business Availability Center Gateway Server machine.

➤ To process clients' requests, these components interact with the HP Business Availability Center Data Processing Server running the Discovery components, the viewing system, and the CMDB.

Discovery Components

This section includes the following topics:

➤ "Discovery Probe" on page 46

➤ "HP Business Availability Center Servers" on page 46

➤ "Discovery Jobs" on page 46

➤ "Discovery Protocol" on page 47

➤ "Jython Scripts" on page 47

Discovery Probe

The Discovery Probe is the main Discovery component responsible for receiving Discovery tasks from the server, dispatching them, and sending the results back to the CMDB through the server. You define a range of network addresses to a specific, installed Discovery Probe. Each Probe is identified by its name. The Probe's name is set in the DiscoveryProbe.properties file, which is located in: **<Discovery Probe root folder>\root\lib\collectors**. For details, see "The DiscoveryProbe.properties File" on page 97.

HP Business Availability Center Servers

The HP Business Availability Center Gateway 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.

Discovery Jobs

A Discovery job is a new entity in Business Availability Center version 7.0 that enables reuse of a pattern for different Discovery processes. Jobs enable scheduling the same pattern differently over different sets of triggered CIs and also supplying different parameters to each set.

To activate Discovery, you now activate jobs—organized in modules—and not patterns.

For details on adding trigger CIs to a job, see "Trigger CIs Pane" on page 136. For details on job configuration, see "Job Configuration Window" on page 145.

Discovery Protocol

Discovery of the IT infrastructure components uses protocols such as SNMP, WMI, JMX, Telnet, and so on. For details, see "Domain Credential References" on page 99.

Jython Scripts

Business Availability Center uses Jython scripts for pattern writing. Jython is a language based on Python and powered by Java. For details on how to work in Jython, you can refer to these Web sites:

➤ http://www.jython.org

➤ http://www.python.org

Discovery Applications

Discovery includes the following applications:

Job Configuration

Job Configuration enables you to manage the Discovery modules and jobs (required for discovering a specific group of CIs). You run the Discovery process by activating Discovery jobs. You can choose to activate all or some of the jobs in a module. You can also edit Discovery jobs.

For details, see Chapter 6, "Job Configuration User Interface."

Domain Configuration

Domain Configuration enables you to add Probes to the system, and to edit existing Probes. You can also define periods of time when a job should not run.

For details, see Chapter 7, "Domain Configuration User Interface."

Resource Configuration

Note: Only users with an advanced knowledge of Discovery should make changes to the resources here.

Resource Configuration enables you to view the resources that are needed to perform Discovery. You can edit patterns, scripts, configuration files, and you can replace or remove external resources needed in Discovery.

For details, see Chapter 8, "Resource Configuration User Interface."

Status Snapshot

Status Snapshot enables you to view the progress of jobs that have been activated for each installed Probe and to view errors. You can also view the report results in a My BAC portlet.

For details, see Chapter 9, "Status Snapshot User Interface."

Reports

You can view reports on job statistics and job errors.

For details, see Chapter 10, "Discovery Job Statistics Report" and Chapter 11, "Discovery Job Errors Report."

Input TQLs, Trigger TQLs, and Trigger CIs

An input TQL is associated with a pattern and defines which CIs can be trigger CIs for jobs that run this pattern. For example, an input TQL can query for IPs running SNMP, that is, only IPs with SNMP can trigger this pattern.

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

Note: A trigger TQL must refer to the same objects as the input TQL. For example, if an input TQL of a pattern queries for IPs running SNMP, you cannot define a trigger TQL for an associated job to query for IPs connected to a host, because some of the IPs may not be connected to an SNMP object, as required by the input TQL.

A trigger CI is a CI in the CMDB that activates a Discovery job. Every time a Discovery job is activated, the job discovers more CIs, which in turn are used as triggers for other Discovery jobs. This process continues until the entire IT infrastructure is discovered and mapped.

For details on adding an input TQL to a pattern, see "Pattern Signature Tab" on page 188.

For details on adding trigger CIs to a job, see "Trigger CIs Pane" on page 136.

Data Validation on the Discovery Probe

From version 7.0, the CIT model also resides on the Discovery Probe. This enables data validation to take place on the Probe when receiving data from services. Problems are generated for a specific trigger CI and displayed to the user. For details, see "Trigger CIs Pane" on page 136.

The following validation takes place on the Probe:

➤ The CIT of the CI is compared to that in the CIT model.

➤ The CI is checked to verify that all key attributes are present (on condition that the CmdbObjectId attribute is not defined).

➤ The CI's attributes are checked to verify that they are all defined in the CIT.

➤ The CI's attributes of type STRING are checked to verify that they do not exceed the size limit. If an attribute is longer than the limit, Discovery checks whether an AUTO_TRUNCATE qualifier is defined for the attribute. If there is a qualifier, the value is truncated and a warning message is written to the Probe error.log file.

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

Blocking the Domain Scope Document Credentials

The Discovery Probe's file system holds (by default) both the encryption key and the Domain Scope Document. Each time the Probe is started, the Probe retrieves the Domain Scope Document from the server and stores it on the file system. To prevent unauthorized users from obtaining these credentials, you can configure the Probe so that the Domain Scope Document is held in the Probe's memory and is not stored on the Probe file system.

To change the configuration, access **DiscoveryProbe.properties** and change:

```
appilog.collectors.storeDomainScopeDocument=true
```

to

```
appilog.collectors.storeDomainScopeDocument=false
```

The Probe Gateway and Probe Manager serverData folders no longer contain the domainScopeDocument.bin file.

Job Execution Policies

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

For details on defining a job execution policy, see "Add/Edit Policy Dialog Box" on page 158.

Running Jobs When a Job Execution Policy Is Running

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

The Resource Configuration Structure

This section describes the resources that are needed to perform Discovery: jobs, patterns, scripts, configuration files, external resources, and packages.

Jobs

A Discovery job is a new entity in version 7.0 that enables reuse of the same pattern for different discoveries, without the need to change the pattern itself. For details, see "Discovery Job Overview" on page 43.

Patterns

A Discovery pattern includes parameters and an input TQL that describes the potential input CIs. Discovery patterns are one of the resources of a Discovery job. A pattern also includes scripts and other code needed for Discovery.

Note: From version 7.0, you no longer have to edit pattern XML files. To make pattern changes, use Resource Configuration. For details, see "Resource Configuration Window" on page 190.

Scripts

Discovery scripts are Jython scripts that can be executed as part of the Discovery pattern execution. For example, the SNMP_Connection.py script is used by the SNMP_NET_Dis_Connection pattern to try and connect to machines using SNMP.

Configuration Files

Configuration files include properties and parameters that are relevant for the Discovery patterns. For example, the portNumberToPortName.xml file (that maps a discovered port's number to a port name) includes a list of ports used by Discovery when discovering networks. For details on user-definable files, see "Resource Configuration Files" on page 91.

External Resources

External resources include all resources external to Business Availability Center that are needed in Discovery, for example, a Visual Basic file, a credentials file, and so on.

Packages

Packages contain definitions, resources, and tools that enable you to discover IT infrastructure resources such as network extensions, applications, and databases. For details, see "Package Manager" in *IT World Model Management.*

Handling Deleted CIs

Discovery can automatically delete CIs that have been removed from a system. This is useful in cases where Discovery can calculate directly that a CI has been removed (and does not have to rely on the aging mechanism to perform the calculation).

For example, when discovering installed software, Discovery can compare the pattern result to the software that was previously discovered. Software that no longer exists on the machine is considered as removed and the software CIs that were previously discovered are automatically deleted.

You can choose to automatically delete removed CIs in Resource Configuration. For details, see "Relevant CITs" on page 185.

For details on aging, see the Results Management pane in "Pattern Management Tab" on page 183.

Status Snapshot Overview

You use Status Snapshot to view the current status of the discovered CIs in the Discovery Probes. Status Snapshot retrieves the status from the Probes and displays the results in a view. For details on the view, see Chapter 9, "Status Snapshot User Interface."

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

4

Discovery Tasks

This chapter includes the main Discovery tasks.

Install the Discovery Probe

This section describes the Discovery Probe installation procedure.

Note:

➤ The Discovery Probe link in the Downloads page is displayed only if you have purchased a license for the Discovery application.

➤ The managed environment is defined by the IP ranges of the domains. However, with some Discovery patterns it is possible to override this behavior and discover CIs that are out of a probe's range.

➤ Install the Discovery Probe. For details, see Chapter 1, "Installing the Discovery Probe."

Launch the Discovery Probe

On the machine on which the Discovery Probe is installed, select **Start > Programs > UCMDB > UCMDB Discovery Probe** to start the Discovery Probe. To verify that the Discovery Probe has been launched successfully, in Business Availability Center select **Admin > Universal CMDB > Discovery > Domain Configuration**. Select the probe and, in the Details pane, verify that status is connected.

For details on how the Discovery Probe works, see "Discovery Probe Workflow – Handling Tasks" on page 39.

Run Discovery

This section describes a typical workflow that enables Discovery to begin mapping your system and its components.

Set Up the Credentials for the Probe

For each Discovery Probe, you must:

➤ Define the Discovery scope of the range of IP addresses to be discovered. For details, see "Add/Edit IP Range Dialog Box" on page 156.

➤ Configure the connection data for each protocol included in a Discovery process. To begin to discover the network, you should configure any of the following protocols: Telnet, SSH, WMI, SNMP, and NTCMD.

Note: You configure protocols depending on what you want to discover and on which protocols are supported on your site's network.

For a list of protocols, see "Domain Credential References" on page 99.

Activate the Network – Basic Module

The first stage in Discovery is to discover the network on which the Discovery Probe is installed.

Note: The following procedure is an example of one way of working with Discovery, by discovering the whole Probe's network. In your case, however, you may need to discover another network or not to discover a network at all. In these cases, the workflow is different, and may require manually adding a network CI or adding the IPs of the required Discovery targets. For details, see "Manually Create a Network CI" on page 88 and "Add/Edit IP Range Dialog Box" on page 156.

---

1 Select **Job Configuration** > **Discovery Modules pane**, right-click **Network – Basic**. For details, see "Discovery Modules Pane" on page 139.

2 Display the jobs that are included in the module. For details on jobs, see "Discovery Job Overview" on page 43.

3 Select the **Class C IPs by ICMP** job. This is the job that pings the IP addresses that fall within the IP address range defined for the Probe.

The ICMP_NET_Dis_IpC pattern performs the IP ping sweep for the job. The job runs this pattern with a trigger TQL that searches for network addresses that answer a specific query. For details on TQLs, see "Input TQLs, Trigger TQLs, and Trigger CIs" on page 49.

To view the TQL's conditions: In Job Configuration, select the **Properties** tab and locate the Trigger TQLs pane. The TQL used by this job is network_C. Select the TQL and click the **Edit** button to open the Trigger TQL Editor.
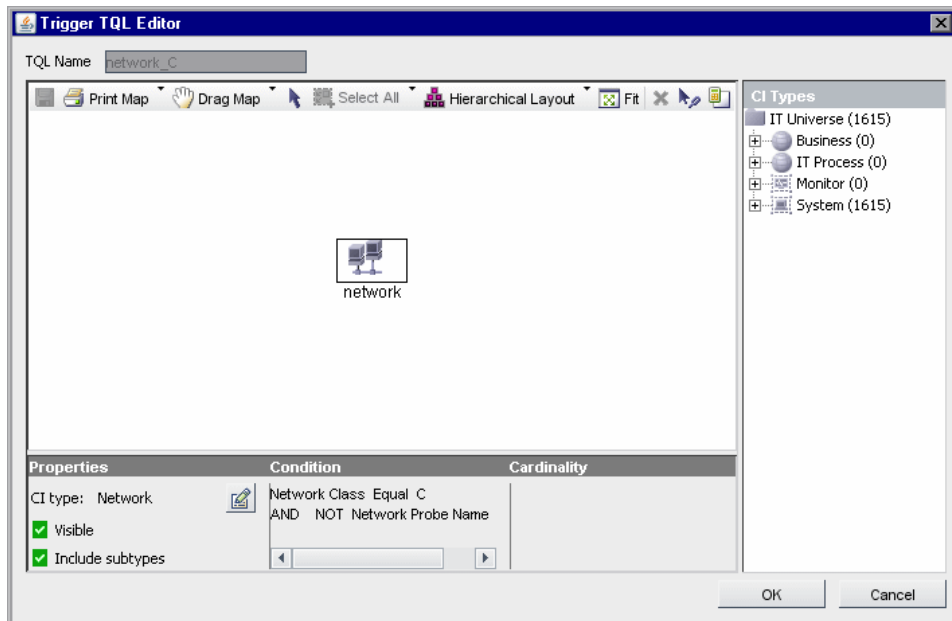
The Editor displays the network CIT. Select the CIT to display its conditions. These signify that when the TQL is run on the network, Discovery should look for networks with a class C address, where the name of the Probe is not null.

For details, see "Trigger TQL Editor" on page 150.

4 Return to the Job Configuration window and activate the **Class C IPs by ICMP** job.

Discovery activates a task which pings the IPs on the Probe's default network. When all the IP addresses in the Probe's range that answer the ping request are received by the Probe, Discovery creates a CI for each IP in the CMDB.

To display the number of networks found by the job, access the Statistics pane for the **Class C IPs by ICMP** job. You can also view statistics in the Status Snapshot window. For details, see Chapter 9, "Status Snapshot User Interface."

5 Return to the Job Configuration window and activate the **Host Connection by SNMP or WMI or SHELL** job.

Discovery activates a task which searches for agents running on the IP addresses found by the Class C IPs by ICMP job.

6 To verify the number of IPs found by the job, access the Statistics pane for the job and locate the IP row. The Statistics pane displays the number of discovered CIs as well as the total number of discovered CIs.

You can display overall statistics for a job or you can filter the results by time range or by probe. Each time you log in to Business Availability Center and access Job Configuration, the statistical data is updated so that the data displayed is the latest for the selected module or job. To work with the statistical data, see "Statistics Pane" on page 133.

You can also view statistics in the Status Snapshot window. For details, see Chapter 9, "Status Snapshot User Interface."

The pattern used to discover the host connections is Host_ID_Discover. To view pattern parameters, select **Properties tab** > **Parameters pane**. To override a default pattern parameter, select a check box and change the value. Save the changes.

The pattern parameters define the scope of the Discovery. Any changes to the pattern are saved in the job and not in the pattern itself, thus enabling the pattern to be reused in other jobs with other parameters.

Note:

➤ You can view these pattern parameters: in Job Configuration, select the Properties tab. Click the **Edit** button next to the Discovery Pattern name. In Resource Configuration, the pattern is selected. Select the Pattern Signature tab. Locate the Discovery Pattern Parameters pane. These parameters should not be changed.

➤ The Pattern Signature tab also displays the CITs that are created from the discovered objects. For example, for the ICMP_NET_Dis_IpC pattern, the CITs are Depend link, IP, and Member link.

For examples of viewing discovered CIs, see:

➤ "Example – Creating a View to Display Discovered Hosts" on page 61.

➤ "Example – Creating a View to Display Network and IP" on page 62.

➤ "Example – Creating a View to Display Discovered CI Instances" on page 63.

You can now confirm that Discovery has found all networks and IPs in the Probe's range.

7 Return to the Job Configuration window and activate the **DNS Resolver** job.

This job discovers the domain name system (DNS) protocol residing on IPs and hosts.

Once Discovery has finished running the DNS Resolver job, all of the basic network should be visible in the IT Universe Manager.

8 Activate the jobs in the Network – Protocol Connections module to try to connect to servers using the NTCmd, SNMP, TTY, and WMI protocols.

Note: Depending on what you need to discover, at this stage you may decide to activate other jobs.

The next stage in Discovery is to expand the network. For details, see the next section.

Example – Creating a View to Display Discovered Hosts

This example shows how to create a view to display all the hosts that Discovery finds.

You use the created view to see the network topology and to view changes to the topology. Select **Admin** > **Universal CMDB** > **Modeling** > **View Explorer**. For details, see "Create New View/View Properties Dialog Box" in *IT World Model Management*.

The following image shows View Manager displaying the created view.
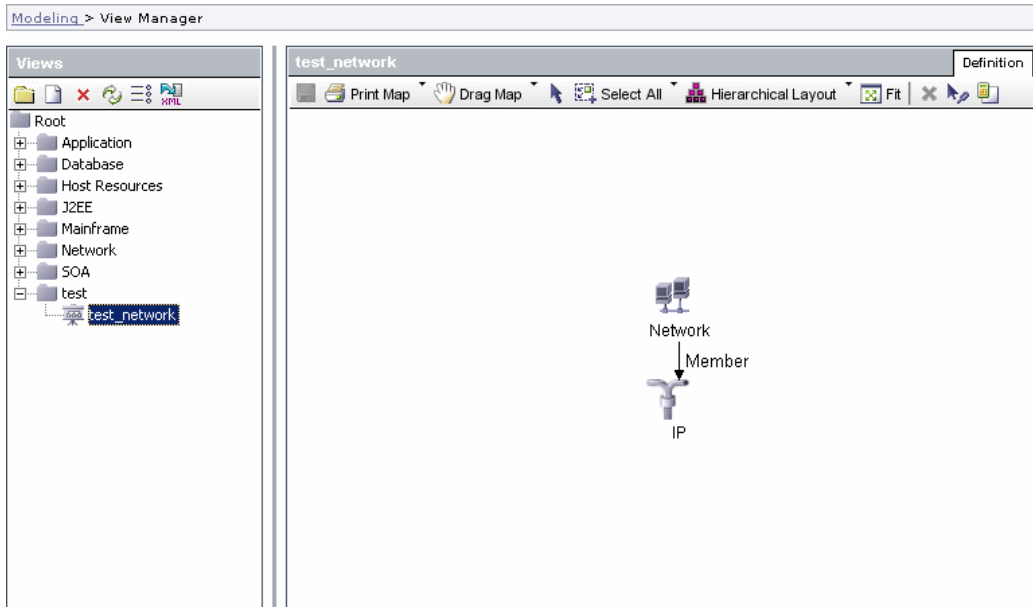
Example – Creating a View to Display Network and IP

The following image shows a network and IP connected by a Member connection.
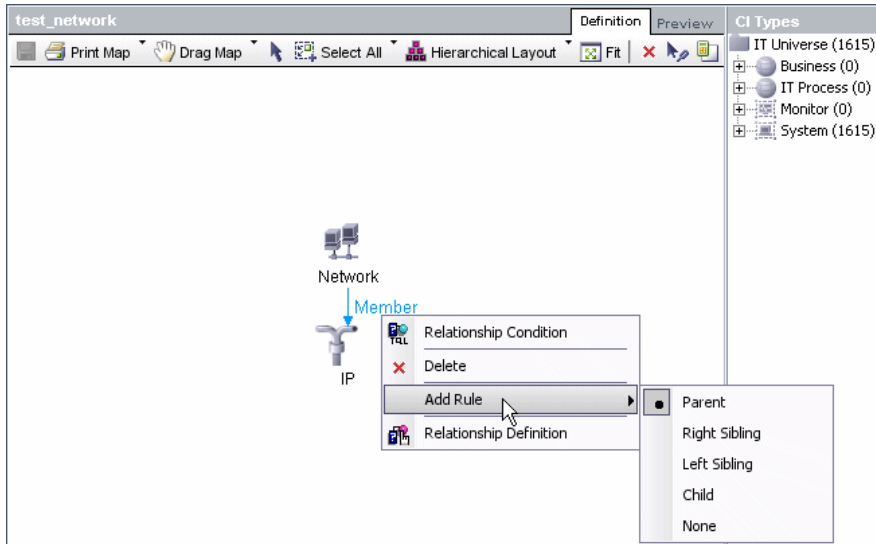
You can add a folding rule so that less CIs are displayed in the IT Universe Manager. For details, see Add Rule in "Topology Query Language Context Menu Options" in *Reference Information*.

Example – Creating a View to Display Discovered CI Instances

To view the number of instances found by Business Availability Center, select **Admin > Universal CMDB > Modeling > IT Universe Manager**, and display the view you created.
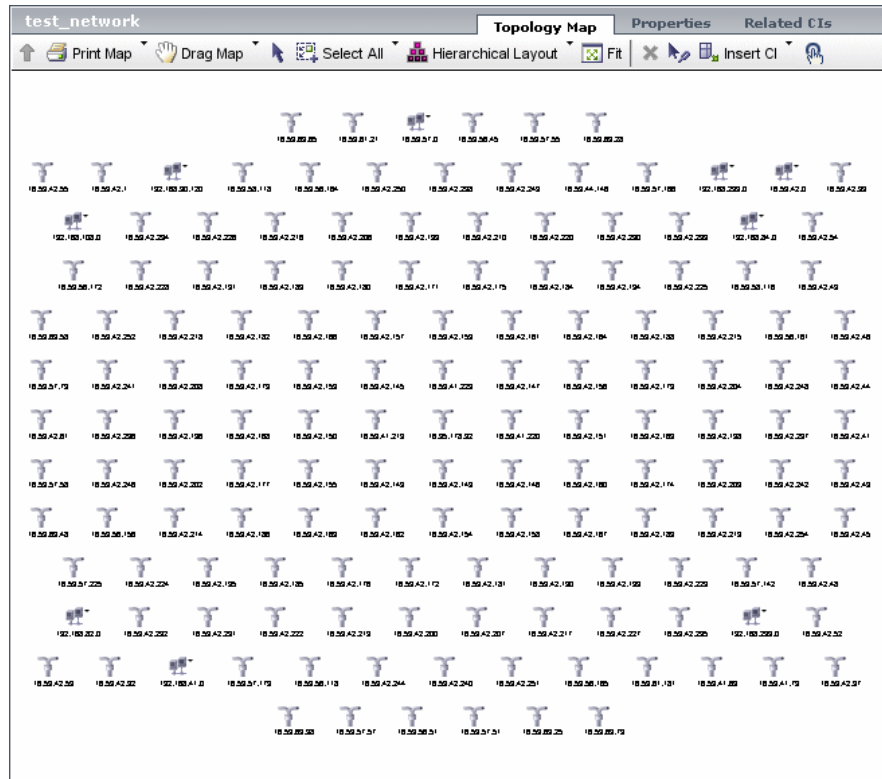
Expand Network Discovery

Continue to activate modules in the same way as explained in the previous section ("Activate the Network – Basic Module" on page 57), performing the procedures in the following order, according to the applications or components to be discovered.

Note: You can read a full description of a job in the Job Configuration Properties tab, under the Discovery pattern name.

➤ Network – Advanced module.

You activate the jobs in this module to discover information about host components, for example, which hosts have open TCP/UDP ports, the ARP table of a router that is using the SNMP protocol, and so on.

➤ Host Resources.

You activate these modules that use the NTCmd, SNMP, SSH/Telnet, and WMI protocols to discover resources on Windows and UNIX hosts, for example, disk information, running processes or services, and so on.

➤ Database modules (Oracle, DB2, Sybase, SQL Server).

Discovery first finds instances of databases, then of the database resources (for example, users, tables, tablespaces) for each database instance. Business Availability Center includes predefined default views of the DB2, Oracle and Microsoft SQL Server databases.

➤ J2EE resources (WebLogic, WebSphere).

WebLogic. Discovery first finds WebLogic servers based on the JMX protocol, then the WebLogic J2EE environment and components.

WebSphere. Discovery first finds WebSphere servers based on either SOAP or RMI authentication, then the WebSphere J2EE environment and components.

➤ Web servers.

The Web Servers modules discover the Apache Web server, Web servers that use a TCP port, and the Microsoft Internet Information Server (IIS).

➤ Applications.

The Application modules discover Oracle E-Business Suite components, the SAP environment based on Computer Center Management System (CCMS), the Siebel environment (such as the Siebel topology and database), and Web services such as the UDDI registry.

Example – Discovering SNMP Connections

You can search for all jobs that discover SNMP connections: in Job Configuration > Discovery Modules pane, click the **Search Discovery Job** icon. In the Find Jobs dialog box, enter **SNMP** in the Name field and click **Find All**. For details, see Add Rule in "Discovery Modules Pane" on page 139 and "Find Jobs Dialog Box" on page 144 in *Reference Information*.

Define a TQL

You create a TQL query that retrieves information about CIs and CITs from the CMDB. For details, see "Define a TQL Query" in *IT World Model Management*.

If necessary you can trigger TQLs to manually discover objects. For details, see "Trigger TQLs Pane" on page 149.

Build a View for Each TQL

A view enables you to build a subset of the overall IT universe model, containing only those CIs in the UCMDB that relate to a specific area of interest. For details, see "View Manager Window" in *IT World Model Management*.

Discover Specific System Components

The following examples explain how to discover specific components of the system.

Before setting up Discovery for these components, verify that the Discovery Probe is installed, is configured with relevant IP ranges, and the correct credentials have been added. For details, see "Set Up the Credentials for the Probe" on page 57. For a list of protocols, see "Domain Credential References" on page 99.

This section includes the following topics:

➤ "Internet Information Services (IIS)" on page 67

➤ "Microsoft Cluster Server" on page 68

➤ "Microsoft SQL Server" on page 69

➤ "SAP" on page 71

➤ "Siebel" on page 75

➤ "Universal Description Discovery and Integration (UDDI)" on page 80

➤ "Veritas Cluster Server" on page 81

➤ "VMWare" on page 84

➤ "WebLogic" on page 86

➤ "WebSphere" on page 87

Internet Information Services (IIS)

Note: Discovery supports IIS versions 5 and 6.

1 Set up the **NTCMD protocol** and verify that the target machine running IIS lies in the probe range. For details, see "NTCMD Protocol" on page 100.

Note: This pattern tries to connect to every IP in a range. Therefore, if a range is wide, network performance may be affected.

2 In the Job Configuration window, activate the jobs in the following order:

> ➤ Host Connection by NTCMD in the Network - Protocol Connections module

> ➤ TCP Ports in the Network - Advanced module

> ➤ Web Server Detection using TCP Ports in the Web Servers – Basic module

> ➤ IIS Applications by NTCMD in the Web Servers – IIS module

3 For details on the CIs that are discovered, see the Statistics table in the Details tab.

Note: You can follow the progress and view the discovered CIs also by accessing the Status Snapshot pane. For details, see Chapter 9, "Status Snapshot User Interface."

The dependency list for the IIS Web Site node is defined as follows:
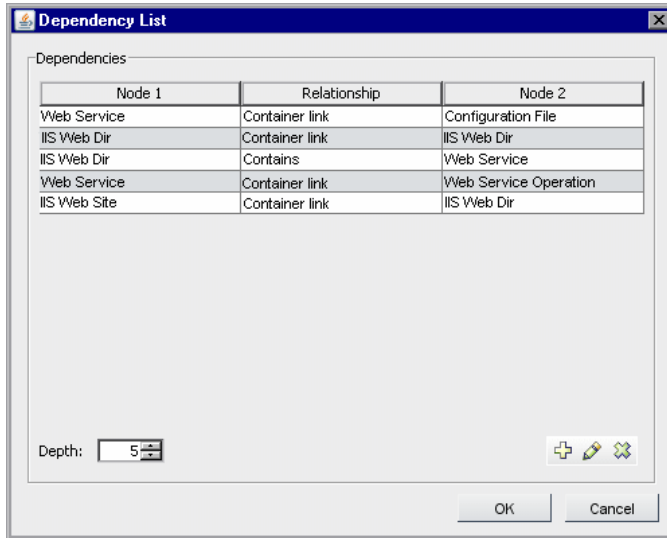
Microsoft Cluster Server

The MS Cluster discovery process enables you to discover the topology of a
Microsoft Cluster Server on the network.

1 Set up the following protocols:

➤ **WMI Protocol.** For details, see "WMI Protocol" on page 108.

➤ **NTCMD Protocol.** For details, see "NTCMD Protocol" on page 100.

2 In the Job Configuration window, activate the modules in the following
order:

➤ Network - Protocol Connections (Host Connection by WMI, then Host
Connection by NTCMD)

➤ Host Resources - WMI (Services by WMI)

➤ MS Cluster

3 For details on the CIs that are discovered, see the Statistics table in the
Details tab.

The following depicts the topology of the Microsoft Cluster Server view:
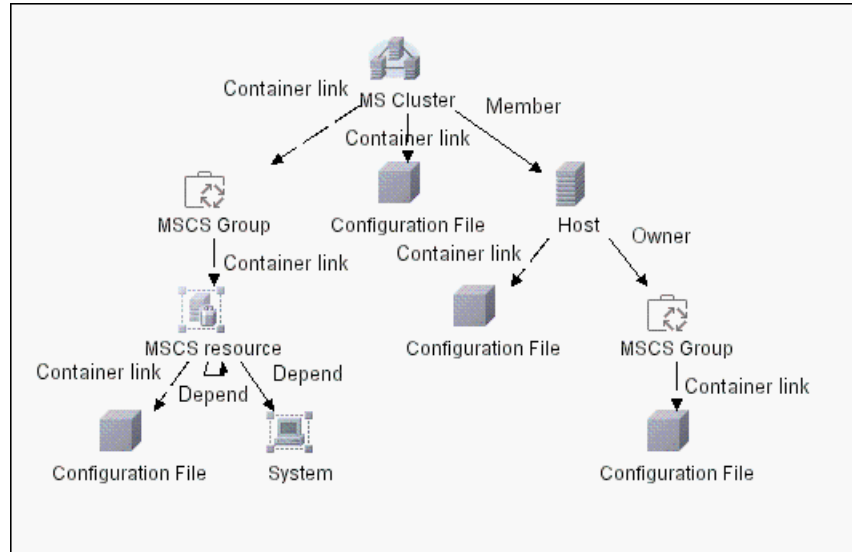
This Microsoft Cluster Server view shows the clusters discovered in the system. The clusters contains Microsoft Cluster groups. Each of the groups contains Microsoft Cluster resources.

Microsoft SQL Server

The SQL discovery process enables you to discover Microsoft SQL servers and their components on your network.

1 Verify the user name, password, and port used by the Microsoft SQL server.

2 Set up the **SQL protocol**. For details, see "SQL Protocol" on page 104.

3 In the Job Configuration window, activate the jobs in the Database – MS-SQL module in the following order:

➤ TCP Ports

➤ MSSQL Connection by SQL

➤ MSSQL Topology by SQL

4 For details on the CIs that are discovered, see the Statistics table in the Details tab.

The following image depicts the topology of the SQL Server view:
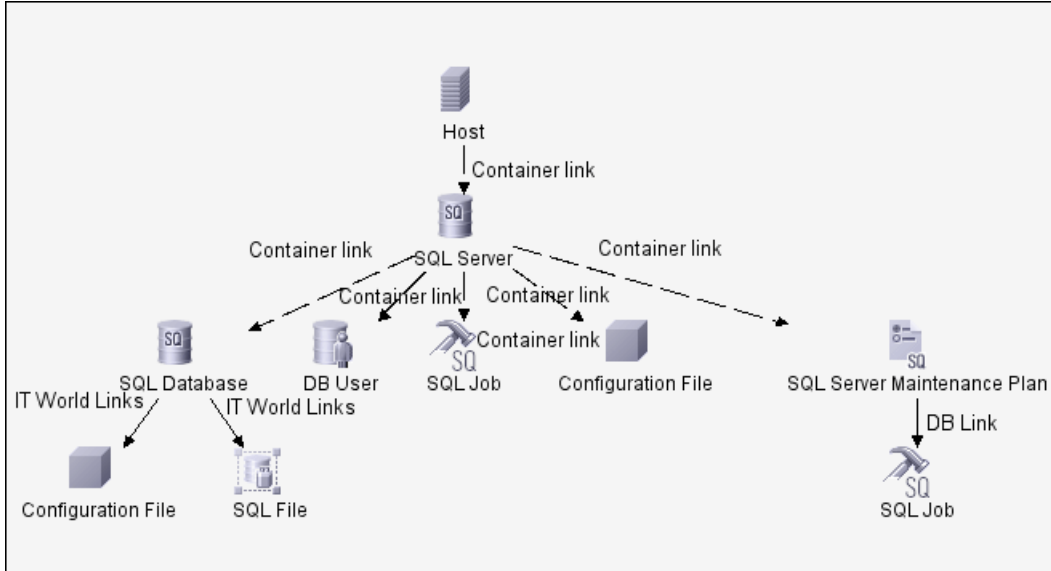
This SQL Server view shows the hosts on which an SQL server is installed. The SQL server contains the SQL server databases, users, SQL jobs, configuration files of this server, and maintenance plans.

SAP

The SAP discovery process enables you to discover application components, SAP transactions and transports, and SAP topology.

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

---

1 Install Java connectors:

➤ Download the SAP JCo package from the Tools & Services window of SAP JCo in SAP Service Marketplace:

https://websmp101.sap-ag.de/~form/ sapnet?_SHORTKEY=01100035870000463649

➤ Extract **sapjco-ntintel-2.0.8.zip** to a temporary directory (for example: C:\temp) on the Business Availability Center machine.

➤ Create a **sap** directory (in lowercase) in the **<Discovery Probe root directory>\Discovery Probe\root\ext** directory on the machine where the Discovery Probe is installed.

➤ Copy **sapjco.jar** from the temporary directory to the **<Discovery Probe root directory>\DiscoveryProbe\root\ext\sap** directory on the machine where the Discovery Probe is installed.

➤ Copy **sapjcorfc.dll** from the temporary directory to the **<Discovery Probe root directory>\DiscoveryProbe\root\ext\sap** directory on the machine where the Discovery Probe is installed.

➤ Copy **librfc32.dll** from the temporary directory to the **%winnt%\system32** directory.

➤ Verify that the **MSVCR71.dll** and **MSVCP71.dll** files are located in the **%winnt%\system32** directory.

2 Set up the following protocols:

> ➤ **SNMP Protocol.** For details, see "SNMP Protocol" on page 102.

> ➤ **WMI Protocol.** For details, see "WMI Protocol" on page 108.

> ➤ **NTCMD Protocol.** For details, see "NTCMD Protocol" on page 100.

> ➤ **SAP Protocol.** For details, see "SAP Protocol" on page 101.

3 To trigger the discovery of SAP System networking features, add a Network CI to the CMDB. For details, see "New CI Wizard" in *IT World Model Management*.

4 In the Job Configuration window, activate the modules in the following order:

> ➤ Network – Basic (Class C IPs by ICMP)

> ➤ Network – Protocol Connections (Host Connection by SNMP, Host Connection by NTCMD, and Host Connection by WMI)

> ➤ Host Resources – WMI (Processes by WMI)

> If the SAP system has an ITS configuration, 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 Ports)

> ➤ Web Servers – Basic (Web server detection using TCP Ports)

> If the SAP system has an ITS configuration, to discover the ITS entities of the SAP system, run this pattern as a prerequisite to the SAP Discovery that discovers ITS entities.

➤ Application – SAP (R/3)

SAP Site. Discovers infrastructure entities in the SAP System: hosts, R/3 Application servers, Work Processes, databases, SAP clients, configuration files, software components (discovered as configuration files), and support packages (discovered as configuration files).

SAP ITS by NTCMD. Discovers Internet Transaction Server (ITS) entities (Application Gateway and Web Gateway).

SAP Solution Manager. Discovers SAP Solution Manager components. **Note:** Before you run this Discovery pattern to discover application components, SAP transactions, and SAP transports, you must set the discovery mode. For details, see step 6.

5 For details on the CIs that are discovered, see the Statistics table in the Details tab.

6 Set the Discovery mode. According to the type of Discovery you are running, you set the pattern parameters as follows:

➤ Access the SAP pattern: **Resource Configuration** > **SAP_Discovery package** > **SAP_Dis_Applications**.

➤ Select the Pattern Signature tab and locate the Discovery Pattern Parameters pane.

➤ Set one of the following parameters, and click **OK** to save the changes.

To discover all SAP transactions: Set **get_tx_all** to **false**.

To discover active SAP transactions: Set **get_tx_active** to **true**.

To discover SAP transactions that have been changed by discovered transports: Set **get_tx_change** to **true**.

7 Verify that Discovery discovered the appropriate components. Access the SAP_Topology view in View Manager and verify that the map displays all components.

8 To view the CIs discovered by the SAP Discovery, select **Job Configuration** > **Application SAP (R/3)**, select a job and access the Dependency Map tab. Right click the selected job and choose **Show discovered CIs**.
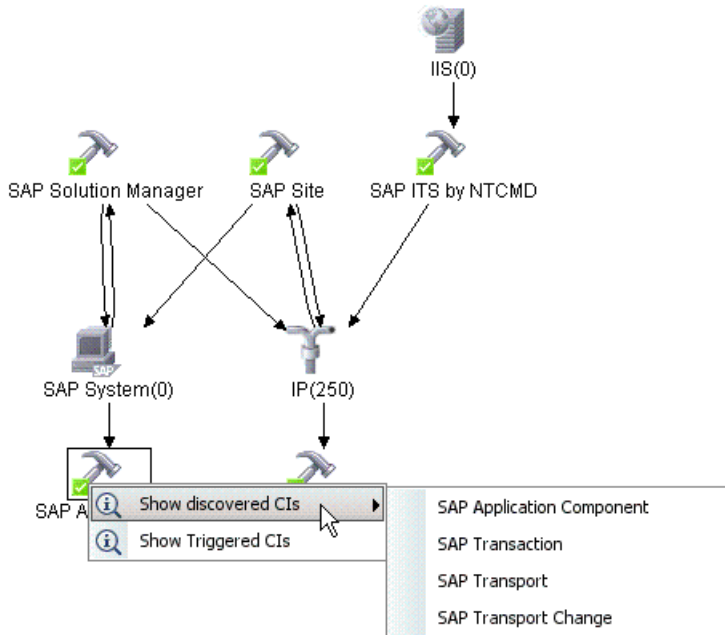
9 To view the SAP CITs, access the CI Type Manager and select **IT Universe** > **System** > **Application Resource** > **SAP Resource**. Hold the cursor over a CIT to view a description.

For details on KPIs created together with the CIs, see the SAP and SAP Alerts KPIs in "KPI Repository Reference" in *CI Attribute Customization*.

10 SAP Solution Manager Discovery enables you to discover the business process hierarchy. To run this Discovery, in the Job Configuration window, activate the SAP Solution Manager job.

Siebel

The Siebel Discovery process enables you to discover Siebel topology in the system.

About Performing a Siebel Discovery

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

During Discovery:

➤ All Siebel-related IT entities that reside in the organization are discovered and configuration items (CIs) are written to 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 are displayed when the Siebel Enterprises view is selected in View Explorer under the Siebel Enterprises root CI.

➤ Four logical containers—Applications, Business Processes, Hosts and Locations—are created under the Siebel Enterprises root CI.

➤ After Discovery has run, you must manually update some of the discovered CI's properties. For details, see "Configure HP Business Availability Center for Siebel Applications–Details" in *Solutions and Integrations*.

Note: Verify that all Siebel server IP addresses are included in the range. If you do not want to cover all servers with one IP range, you can split the range into several ranges.

---

1 Set up the following protocols for the Windows platform and continue to step 3:

➤ **WMI Protocol.** For details, see "WMI Protocol" on page 108.

➤ **NTCMD Protocol.** For details, see "NTCMD Protocol" on page 100.

➤ **Siebel Gateway Protocol.** For details, see "Siebel Gateway Protocol" on page 102.

2 Set up the following protocols for the UNIX platform and continue to step 3:

➤ **SSH Protocol.** For details, see "SSH Protocol" on page 104.

➤ **Telnet Protocol.** For details, see "Telnet Protocol" on page 105.

➤ **Siebel Gateway Protocol.** For details, see "Siebel Gateway Protocol" on page 102.

3 For Siebel discovery to run, you must copy the driver tool to the Discovery Probe server. For details, see "Copy the driver Tool to the Discovery Probe Server" on page 78.

4 For the SiteScope Siebel monitors to work correctly, copy the driver tool and the SARM Analyzer tool to the SiteScope server. On SiteScope, the driver tool is launched by the Siebel Application Server monitor to retrieve the metrics. For details, see "Copy the driver Tool and the SARM Analyzer Tool to the SiteScope Server" on page 79.

5 To trigger the discovery of Siebel networking features, add a Network CI to the CMDB. For details, see "New CI Wizard" on page 203.

6 In the Job Configuration window, activate the modules in the following order:

➤ Network – Basic (Class C IPs by ICMP)

➤ Network – Protocol Connections (Host Connection by NTCMD, Host Connection by WMI, Host Connection by TTY)

7 To discover the Web tier, activate the following modules:

➤ Network - Advanced (TCP Ports)

➤ Application - Siebel (Siebel Web Applications by NTCMD, Siebel Web Applications by TTY, Siebel DB by WMI and NTCMD)

➤ Web Server - Basic (WebServer Detection using TCP Ports)

8 To discover Siebel, activate all the patterns in the Application – Siebel module.

Note:

The following enrichment patterns automatically run in the background during Discovery:

➤ **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.

9 For details on the CIs that are discovered, see the Statistics table in the Details tab.
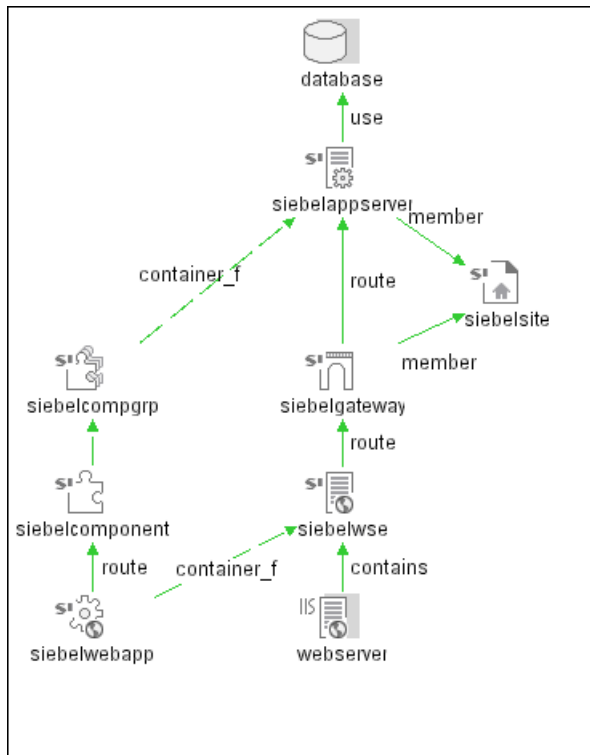
Copy the driver Tool to the Discovery Probe Server

The driver tool is used to extract data about the enterprise structure from Siebel.

Note: If you are working with different versions of Siebel in your organization, make sure you use a driver tool with a version that is appropriate for the Siebel server.

To copy the driver tool to the Discovery Probe server:

1 Copy the driver Command Line Interface (CLI) tool from the Siebel server to any folder on the Discovery Probe server.

2 It is recommended to run the Siebel connection test to validate the driver installation. To run the connection test, open the command line on the Discovery Probe server and change directory to the location of the driver.exe file.

3 Run from the command line:

```
>driver /e [site_name] /g [gateway_host] /u [username] /p [password]
```

If the connection is established successfully, the DOS window displays the driver prompt and a status message about the number of connected servers.

Copy the driver Tool and the SARM Analyzer Tool to the SiteScope Server

Note:

➤ The SARM Analyzer is used for analyzing SARM data, so that it can be displayed in the Business Availability Center for Siebel SARM – User Trace Breakdown tab.

➤ If you are working with different versions of Siebel in your organization, make sure you use a driver and a SARM Analyzer with a version that is appropriate for the SiteScope server.

➤ It is recommended to run the Siebel connection test to validate the driver installation.

➤ SiteScope should run under a domain user name which has permissions to run server manager and SARM Analyzer and also has read access to the log folders on the Siebel servers (Web servers and application servers).

➤ All Siebel servers (Windows and UNIX) must be defined as remote servers on the SiteScope server. For details, refer to the *SiteScope Reference Guide*.

To copy the driver tool to the SiteScope server:

1 Copy the driver Command Line Interface (CLI) tool from the Siebel server to any folder on the SiteScope server.

2 To run a connection test, open the command line on the SiteScope server and change directory to the location of the driver.exe file.

3 Run from the command line:

```
>driver /e [site_name] /g [gateway_host] /u [username] /p [password]
```

For the connection to work properly, verify that the user and password have the correct permissions for a remote connection.

If the connection is established successfully, you should see the driver prompt and the status message about the number of connected servers.

To copy the SARM Analyzer tool to the SiteScope server:

 1 Copy the SARM Analyzer tool from the Siebel server to a folder on the SiteScope server.

 2 If your site includes a large number of Web servers, it is preferable to use multiple SiteScopes to distribute the work done by the SARM Analyzer tool between those SiteScopes. In such a case, copy SARM Analyzer to each SiteScope.

Universal Description Discovery and Integration (UDDI)

The UDDI discovery process enables you to discover Web services from a UDDI registry.

Discovery queries the UDDI registry for 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: Business Availability Center supports UDDI versions 2 and 3.

---

 1 Set up the **UDDI protocol**. For details, see "UDDI Registry Protocol" on page 106.

 2 In the Job Configuration window, activate the **Application – Webservices** module.

 3 For details on the CIs that are discovered, see the Statistics table in the Details tab.

The following depicts the topology of the **SOA_UDDI_View**:
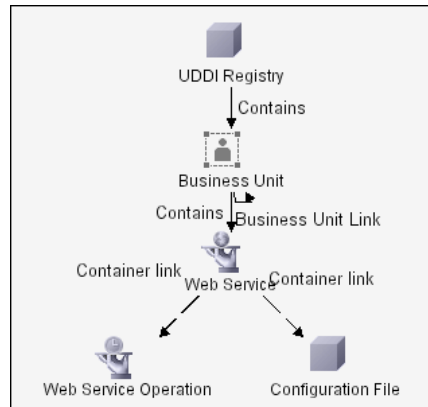
4 **(Optional)** To enter the name of the service publisher whose services you want to publish:

a Access the Resource Configuration window.

b In the Discovery Resources pane, locate the Webservices package and select the **UDDI_Registry** pattern.

c In the Pattern Signature tab, in the Discovery Pattern Parameters pane, select the **organization** parameter and click the **Edit** button.

d In the Parameter Editor:

➤ In the Value field, enter the name of the service publisher.

➤ In the **Description** field, enter the required description of the organization.

e Save the changes.

Veritas Cluster Server

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.

1 Set up the **SSH protocol**. For details, see "SSH Protocol" on page 104.

2 Set up the **Telnet protocol**. For details, see "Telnet Protocol" on page 105.

3 In the Job Configuration window, activate the following modules:

> ➤ Network - Protocol Connections

> ➤ Host Resources - SSH/Telnet

> ➤ Veritas Cluster

4 For details on the CIs that are discovered, see the Statistics table in the Details tab.

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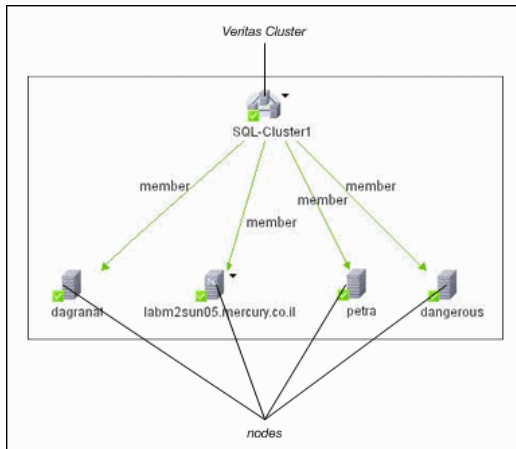
This view shows the top layer of the Veritas Cluster topology. It displays the discovered Veritas Cluster and the nodes that are members of that cluster. Each member node is linked by a **member** relationship to the Veritas Cluster.

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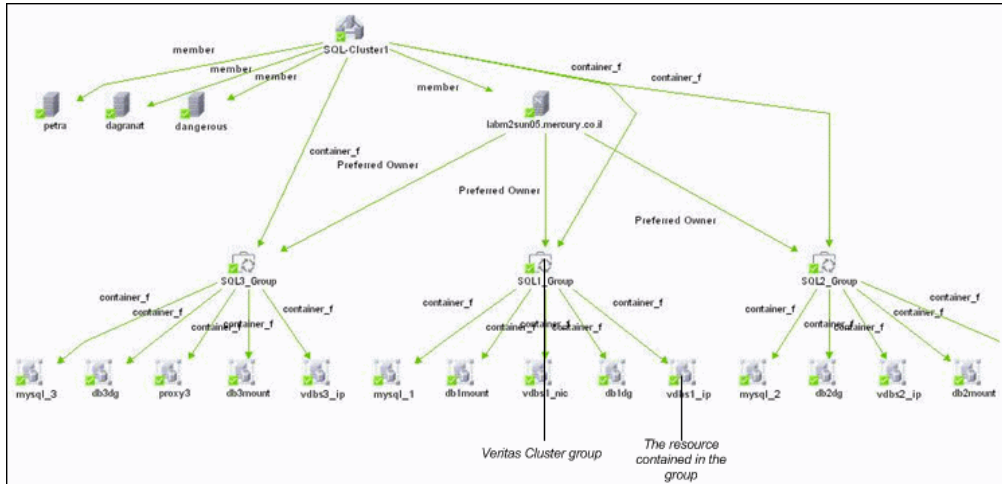
This view displays the Veritas Cluster groups and the resources contained in each group.

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, 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 following figure shows these 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**
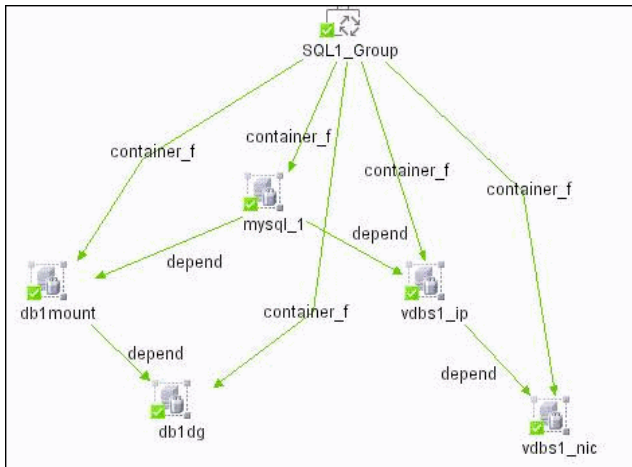
VMWare

The VMWare discovery process enables you to discover virtual machines, processors, memory, storage, and network resources that are running on VMWare version 2.5 ESX servers.

1 Set up the **SSH protocol**. For details, see "SSH Protocol" on page 104.

2 Set up the **Telnet protocol**. For details, see "Telnet Protocol" on page 105.

3 In the Job Configuration window, activate the following modules:

➤ Network - Protocol Connections

➤ Host Resources - SSH/Telnet

➤ Network - VMWare

4 For details on the CIs that are discovered, see the Statistics table in the Details tab.

The **VM Server** CIT inherits the base attributes from the system CIT. The data_name attribute contains the VM server type (for example, VMWare Server). The vmserver_version attribute contains version information (for example, ESX 2.5.2). The root_container attribute enables multiple VM servers with the same data_name attribute to remain unique.

The **Interface** CIT represents a virtual interface on condition that the isvirtual attribute is set to **true** (the default value is false). Since the virtual interface is linked to the physical interface on the VM server, the depend link joins the CIT to itself. The only difference between the virtual and physical interface CITs is that the virtual interface includes the isvirtual attribute. This CIT is part of the network resource CIT.

WebLogic

The WebLogic discovery process enables you to discover all the deployed Web services and operations deployed on a WebLogic server. Business Availability Center supports WebLogic versions 8 and 9.

Note: If you are using WebLogic version 7, perform the following procedure to enable Discovery to discover this Weblogic version:

➤ 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 root folder>\root\lib\collectors\probeManager\discoveryResources**. (This folder is created when the Discovery Probe connects to the WebLogic server. However, if you have not yet run Discovery, you must manually create the folder.)

➤ Rename the jar files by adding a suffix that includes the WebLogic version number, as follows: **webserviceclient70.jar**, **weblogic70.jar**.

---

1 Set up the **WebLogic protocol**. For details, see "WebLogic Protocol" on page 106.

2 In the Job Configuration window, activate the job in the J2EE – WebLogic module.

3 For details on the CIs that are discovered, see the Statistics table in the Details tab.

WebSphere

The WebSphere discovery discovers Web services that are deployed on an IBM WebSphere server. The discovered Web services are represented by the webservice CIT in the CMDB.

Note: Business Availability Center supports WebSphere versions 5 and 6.

---

1 Set up the **WebSphere protocol**. For details, see "WebSphere Protocol" on page 107.

2 In the Job Configuration window, activate the J2EE – WebSphere job.

3 For details on the CIs that are discovered, see the Statistics table in the Details tab.

Advanced Usage

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

The following sections include examples of tasks you may need to perform.

Manually Activate a Job

You can activate a job by clicking the **Activate** button in the Discovery Modules pane. You can manually activate a CI by disabling the TQL and clicking the **Add TQL** button. (You disable a TQL in the **Edit Probe Limitation for TQL Output** dialog box.) The Discovery job runs using only the redispatched CIs. For details, see "Discovery Modules Pane" on page 139.

Manually Create a Network CI

A Probe starts by discovering the network on which it is running, so usually there is no need for you to create a network CI. However, if you installed the Probe on a certain network, but configured the Probe to discover objects on another network, Discovery is not able to discover the network. You must manually create a network CI for the network that the Probe must discover.

To verify that a network CI exists, access the View Manager (**Admin > Universal CMDB > Modeling > View Manager**). Locate the Network folder and verify that the folder contains a Network Topology view.

For details on manually creating a network CI, see "Activate the Network – Basic Module" on page 57 and "New CI Wizard" in *IT World Model Management*.

Schedule Modules to Run

You can set a schedule for a Discovery job or a module so that it runs at a certain time. For details, see "Discovery Scheduler Dialog Box" on page 142.

Edit Resources

You can edit patterns, scripts, configuration files, and you can replace or remove external resources needed in Discovery. For details, see "Resource Configuration Window" on page 190.

Define Job Execution Policies

You can configure time periods when jobs should not run. For details, see "Add/Edit Policy Dialog Box" on page 158.

Run an Ad-Hoc Discovery to Rediscover CIs

You use the View Discovery wizard to perform an ad-hoc Discovery of a view. The ad-hoc Discovery runs the Discovery jobs relevant for the CIs in the selected view, to find recent changes to the configuration.

Business Availability Center processes an ad-hoc Discovery as follows:

Step 1: Access View

In IT Universe Manager, you access the view to be checked in the View Explorer. For details, see "View Explorer User Interface" in *Reference Information*.

Step 2: Display View Discovery Wizard

You click the Rediscover button to display the View Discovery Wizard. For details, see "View Discovery Wizard" in *IT World Model Management*.

A list of the jobs related to the discovered CIs in the view is displayed.

Step 3: Choose Jobs to Run

Business Availability Center displays the Choose Jobs for View dialog box and you choose which jobs should be run. For details, see "Choose Jobs for View Dialog Box" in *IT World Model Management*.

The Discovery Probe immediately runs the jobs that originally discovered the CIs and sends the results back to the server.

Business Availability Center displays statistics about the CIs (for example, how many new CIs have been discovered) in a table. For details, see "Discovered Changes Details Dialog Box" in *IT World Model Management*.

Business Availability Center rebuilds the view and displays updated information.

Filter Discovery Results

You can filter Discovery results sent by the Discovery Probe to the Business Availability Center server. You would probably want to filter irrelevant data regularly during production runs and specifically when you are testing a limited environment.

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

➤ **Pattern filtering.** Discovery filters the results for a specific pattern and sends to the CMDB only those CIs that are either updated or new. You define a pattern filter in the Pattern Management pane. For details, see "Pattern Management Tab" on page 183.

➤ **Global filtering.** Discovery filters the results of all jobs running on a Discovery Probe. You define global filters in the globalFiltering.xml file. For details, see "globalFiltering.xml" on page 93.

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

View Job Statistics

You can display overall statistics for a job or you can filter the results by time range or by probe. Each time you log in to Business Availability Center and access Job Configuration, the statistical data is updated so that the data displayed is the latest for the selected module or job.

For details on working with the statistical data, see "Statistics Pane" on page 133.

5

Discovery Reference

This chapter includes the main reference for Discovery.

This chapter describes:	On page:
Resource Configuration Files	91
Discovery System Directory Structure	95
The DiscoveryProbe.properties File	97
Domain Credential References	99
Discovery Log Files	108
Troubleshooting and Limitations	113

Resource Configuration Files

The following files can be changed to enable Discovery in non-default systems. The location of these files is: **Resource Configuration** > **Network** > **Configuration Files**.

This section includes the following topics:

➤ "portNumberToPortName.xml" on page 92

➤ "oidToHostClass.xml" on page 93

➤ "globalFiltering.xml" on page 93

➤ "Configuration Files for Internal Use Only" on page 95

portNumberToPortName.xml

The portNumberToPortName.xml file is used by Discovery as a dictionary to create Port CIs. When a port is discovered, the Discovery Probe extracts the port's name from this file, and creates the Port CI accordingly. If the port number does not appear in this file, the port name is used as the port number.

You edit this file when adding new ports to be discovered.

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

To define a new port:

1 In Resource Configuration, access portNumberToPortName.xml and search for the file by clicking the **Find resource** button and entering **portNumber** in the Name field. Click **Find Next**, then click **Close**.

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

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

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

➤ **portProtocol.** The network protocol used for Discovery (udp or tcp).

➤ **portNumber.** The port number to be discovered.

➤ **portName.** The name that is to be displayed for this port.

➤ **discover.** 1. This port must be discovered. 0: This port should not be discovered.

oidToHostClass.xml

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

To access the oidToHostClass.xml file, in Resource Configuration, search for the file by clicking the **Find resource** button and entering **oidto** in the Name field. Click **Find Next**, then click **Close**.

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

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

---

oidToHostClass.xml includes the following parameters:

➤ **class.** The converted CIT name of the discovered OID. Under this name, the operating system or device appears in the CMDB and in Business Availability Center.

➤ **vendor.** The vendor of the operating system or device.

➤ **os.** A specific operating system, for example, Linux. This parameter is optional.

➤ **model.** A specific model, for example, JETDIRECT,JD30. This parameter is optional.

➤ **oid.** The discovered OID.

globalFiltering.xml

This file enables you to filter Discovery Probe results for all patterns, so that only results of interest to you are sent to the Business Availability Center server. (You can also filter specific patterns. For details, see "Filter Discovery Results" on page 90 and "Pattern Management Tab" on page 183.)

To add a global filter:

1 Access the globalFiltering.xml file: in Resource Configuration, open the Network folder and click the Configuration Files folder. Select the file to display the code in the View pane.

2 Locate the <includeFilter> and <excludeFilter> markers:

➤ **<includeFilter>.** When a vector marker is added to this filter, all CIs that do not match the filter are removed. If this marker is left empty, all results are sent to the server.

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

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

```
<vector>
    <object class="ip">
        <attribute name="ip_address" type="String">192\.168\.82\.17.*</attribute>
        <attribute name="ip_domain" type="String">DefaultProbe</attribute>
    </object>
</vector>
```

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

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

The following example shows a network CI that has no attributes. All network results are sent to the server:

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

Note:

➤ Attributes in the filter should be of type string only. For details on attribute types, see "Attributes Page" in *CI Attribute Customization*.

➤ A result is considered to be a match only if all filter attributes have the same values as those in the CI. (If one of a CI's attributes is not specified in the filter, all the results for this attribute match the filter.)

➤ A CI can match more than one filter. The CI is removed or remains according to the filter in which it is included.

➤ Discovery filters first according to the <includeFilter> and then applies the <excludeFilter> on the results of <includeFilter>.

Configuration Files for Internal Use Only

The following files are for internal use only and should not be changed:

➤ **discoveryPolicy.xml.** Includes the schedule when the Probe does not execute tasks. For details, see "Add/Edit Policy Dialog Box" on page 158.

➤ **jythonGlobalLibs.xml.** A list of default Jython libraries that Discovery loads before running scripts.

➤ **interfaceType.xml.**

Discovery System Directory Structure

This section describes the folders and files that you may need to view or monitor.

The files and folders are located in the following path: <**Business Availability Center server root directory**>**root****lib****collectors**.

Note:

➤ When Discovery components are installed on different workstations, files and folders may be copied and stored on more than one workstation to provide data locally for each component.

➤ The files that are intended for internal HP use only do not appear in this section.

This section includes the following topics:

The collectors Folder

➤ **DiscoveryProbe.properties.** The Discovery Probe configuration file that includes the default parameters used in the Discovery processes. For details, see "The DiscoveryProbe.properties File" on page 97.

➤ **delCollectors.bat.** A command file that deletes Discovery task data from the Discovery Probe, including all tables, repositories, and pending tasks, and builds the data from scratch.

➤ **versions.properties.** Contains the version and build details on the installed Probe.

The probeGateway Folder

➤ create_probeGW_db.sql.

➤ create_probeGW_tables.sql

➤ drop_probeGW_db.sql

➤ probeGwLog4j.properties

➤ probeMgrList.xml

➤ probeTables.xml. Contains a definition set of the Probe Gateway repository tables.

➤ recreate_probeGW_DB.cmd

The probeManager Folder

➤ create_probemgr_db.sql

➤ create_probemgr_tables.sql

➤ drop_probemgr_db.sql

➤ ip2location.csv

➤ probeMgrLog4j.properties

➤ probeMgr-quartz.properties

➤ quartzTables.xml

➤ recreate_probeMgr_DB.cmd

The probeManager folder includes the following subfolders:

➤ **The binaryData folder.** For internal use only.

➤ **netlinks.**

The DiscoveryProbe.properties File

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

The DiscoveryProbe.properties file is located in <**Business Availability Center root directory**>**DiscoveryProbe****root****lib****collectors**.

Note: If you update the **DiscoveryProbe.properties** parameters, you must restart the Discovery Probe.

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

Server Connection Definitions. Contains parameters that are needed to set up the connection between the server and the Discovery Probe, such as the protocol to be used, machine names, default probe and domain names, timeouts, and basic authentication.

Discovery Probe Definitions. Contains parameters that define the Probe, such as root folder location, ports, and Manager and Gateway addresses.

Probe Gateway Configurations. Contains parameters that define time intervals for retrieving data.

Probe Manager Configurations. Contains parameters that define Probe Manager functionality, such as scheduled intervals, result grouping, chunking, threading, timeouts, and filtering.

I18N Parameters. Contains parameters that define language settings.

Internal Configurations. (Caution: These parameters should not be changed without an advanced knowledge of Discovery.) Contains parameters that enable Discovery to function efficiently, such as thread pool size.

Domain Credential References

This section explains protocol credentials. You can edit credential attributes. For details, see "Protocol Parameters Dialog Box" on page 167.

All protocol credentials include the following parameters:

Parameter	Description
Network Scope	To change the range that a protocol must discover or to select a Discovery Probe, click **Edit**. For details, see "Scope Definition Dialog Box" on page 168. The default is ALL.
Protocol Index	Indicates the order in which protocol instances are used to make a connection attempt. The lower the index, the higher the priority. The default is 9999. If you do not change the default, this protocol instance is used last.
User Label	Enter a label to help you identify a specific protocol credential, when you use it later. Enter a maximum of 50 characters.

This section includes the following topics:

➤ "JBoss Protocol" on page 100

➤ "NTCMD Protocol" on page 100

➤ "SAP JMX Protocol" on page 100

➤ "SAP Protocol" on page 101

➤ "Siebel Gateway Protocol" on page 102

➤ "SNMP Protocol" on page 102

➤ "SQL Protocol" on page 104

➤ "SSH Protocol" on page 104

➤ "Telnet Protocol" on page 105

➤ "UDDI Registry Protocol" on page 106

➤ "WebLogic Protocol" on page 106

JBoss Protocol

Parameter	Description
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the JBOSS application server.
Port Number	The port number.
User Name	The name of the user needed to connect to the application as administrator.
User Password	The password of the user needed to connect to the application as administrator.

NTCMD Protocol

Parameter	Description
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the NTCMD server.
User Name	The name of the user needed to connect to the host as administrator.
User Password	The password of the user needed to connect to the host as administrator.
Windows Domain	The name of the domain that includes the host where the Discovery Probe is installed.

SAP JMX Protocol

Parameter	Description
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the SAP JMX console.
Port Number	The SAP JMX port number.

Parameter	Description
User Name	The name of the user needed to connect to the application as administrator.
User Password	The password of the user needed to connect to the application as administrator.

SAP Protocol

Parameter	Description
SAP Client	It is recommended to use the default value (800).
SAP Router String	A route string describes the connection required between two hosts using one or more SAProuters. Each of these SAProuters checks its Route Permission Table (http://help.sap.com/saphelp_nw04/helpdata/en/4f/992 dfe446d11d189700000e8322d00/content.htm) to see whether the connection between its predecessor and successor is allowed. If it is, the SAProuter sets it up.
SAP System Number	It is recommended to use the default value (00).
Timeout/Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the SAP console.
User Name	The name of the user needed to log in to the SAP system.
User Password/Password	The password of the user needed to log in to the SAP system.

Siebel Gateway Protocol

Parameter	Description
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the Siebel Gateway console
Path of srvrmgr	The location on the Probe server to where you copied srvrmgr. For details, see "Copy the driver Tool to the Discovery Probe Server" on page 78. **Note:** If there are several protocol entries with different srvrmgr versions, the entry with the newer version should appear before the entry with the older version. For example, to discover Siebel 7.5.3. and Siebel 7.7, define the protocol parameters for Siebel 7.7 and then the protocol parameters for Siebel 7.5.3.
Siebel Site Name	The name of the Siebel Enterprise.
User Name	The name of the user needed to log on to the Siebel enterprise
User Password	The password of the user needed to log on to the Siebel enterprise.

SNMP Protocol

Parameter	Description
Community	(For SNMP v1 and SNMP v2 only) Enter the password you used when connecting to the SNMP service community (which you defined when configuring the SNMP service—for example, a community for read-only or read/write).
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the SNMP agent.
Port Number	(For SNMP versions v1, v2, and v3) The port number on which the SNMP agent listens.
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.

Parameter	Description
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.
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
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 may 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).

Parameter	Description
V3 – Privacy algorithm	(For SNMP v3 only) The following algorithm is supported: DES.
V3 – Privacy key	(For SNMP v3 only) The secret key used to encrypt the scoped PDU portion in an SNMP v3 message.

SQL Protocol

Parameter	Description
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the database.
Database Name	The database name.
Database SID	The database SID (Oracle, DB2).
Database Type	The database type. Select the appropriate type from the box.
Port Number	The port number on which the database listens.
User Name	The name of the user needed to connect to the database as administrator.
User Password	The password of the user needed to connect to the database as administrator.

SSH Protocol

Parameter	Description
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. For UNIX platforms: If your server is slow, it is recommended to change Connection Timeout to 40000.

Parameter	Description
Key Path	Location of the authentication key. (In certain environments, the key path is required to connect to an SSH agent.)
Network Address	The discovered IP network address or the network address range.
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.
User Name	The name of the user needed to connect to the host as administrator.
User Password	The password of the user needed to connect to the host as administrator.

Telnet Protocol

Parameter	Description
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the remote machine. For UNIX platforms: If your server is slow, it is recommended to change Connection Timeout to 40000.
Port Number	The port number. By default a Telnet agent uses port 23. If you are using a different port for Telnet in your environment, enter the required port number.
User Name	The name of the user needed to connect to the host as administrator.
User Password	The password of the user needed to connect to the host as administrator.

UDDI Registry Protocol

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

WebLogic Protocol

Parameter	Description
Certificate PEM File Path	Enables the WebLogic gateway to verify the user who is connecting to it. Enter the path to the certificate file.
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the WebLogic application server.
Key PEM File Path	Enables the WebLogic gateway to verify the user who is connecting to it. Enter the path to the key file.
Port Number	The port number.
Protocol	An application-level protocol that determines whether Discovery should connect to the server securely. Enter either **http** or **https**.
Trust File Name	Enables the WebLogic server to verify the user who is connecting to it. Enter the name of the Trust File, including the jks extension. For example, **Demotrust.jks**.
User Name	The name of the user needed to connect to the application as administrator.
User Password	The password of the user needed to connect to the application as administrator.

WebSphere Protocol

Parameter	Description
Password	The password of the user needed to connect to the application as administrator.
Port	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 user name 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
	Access **System Administration** > **Deployment Manager** to retrieve the required port number.
Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the WebSphere server.
Trust Store File Name	The name of the SSL trust store file.
	Business Availability Center contains a default trust store file called **DummyClientTrustFile.jks**. It is located in the External resources folder in the J2EE package. To use a file other than the default trust store file provided by the system, enter the name of your trust store file and place it in the External resources folder. When the package is updated, the trust store file is copied to the relevant location.

Parameter	Description
Trust Store Password	The SSL trust store password.
	The default password for the default trust store file in Business Availability Center is WebAs. If you are not using the default trust store file provided by the system, enter the password for the file you are using.
User Name	The name of the user needed to connect to the application as administrator.

WMI Protocol

Parameter	Description
Connection Timeout	Timeout in milliseconds after which the Discovery Probe stops trying to connect to the WMI agent.
User Name	The name of the user needed to connect to the host as administrator.
User Password	The password of the user needed to connect to the host as administrator.
Windows Domain	The name of the domain that includes the host where the Discovery Probe is installed.

Discovery Log Files

This section describes the Discovery log files and explains how to perform basic troubleshooting. Discovery log files store messages, including errors, relating to the activation of Discovery jobs.

Discovery Server Logs

Discovery Server log files reside on the HP Business Availability Center server. They store information about Discovery server activity, including error messages, that occurs on the server side.

The following logs are located in **<HP Business Availability Center root directory>\log**.

mamAutoDiscovery.log

Contains information about tasks running on the server. The server provides services to the user interface, such as: activating jobs, processing results from the Discovery Probe, or creating tasks for the Discovery Probe. In a distributed environment, the file resides on the Data Processing server.

Error Level. All Discovery process errors on the server side.

Information Level. Information about requests being processed.

Debug Level. Logs mainly for debugging purposes.

Basic Troubleshooting. 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.

mamWebAutoDiscovery.log

This log receives messages from:

➤ the Collectors Utilities Servlet. The user interface connects to the server through this servlet.

➤ the Collectors Servlet. The Discovery Probe requests new tasks from the server through this servlet.

➤ the Collectors Results Servlet. The Discovery Probe sends new results through this servlet.

➤ the Collectors Download Servlet. The Discovery Probe downloads new server data through this servlet.

In a distributed environment, the file resides on the Gateway server.

Error Level. All errors in the servlet.

Information Level. Information about user requests and Discovery Probe task requests.

Debug Level.

➤ User requests

➤ Discovery Probe requests to read Discovery tasks.

➤ Discovery Probe access of the servlet.

Basic Troubleshooting.

➤ User Interface–Server communication problems.

➤ Discovery Probe–Server communication problems.

Some processing problems may be written to this log instead of to mamAutoDiscovery.log.

mamAutoDiscoveryUpgrade.log

Contains information about the upgrade process.

mamAutoDiscoveryResultsStat.log

Contains the statistics of the results received from the Probe.

Discovery Probe Logs

Discovery Probe logs store information involving Discovery job activation that occurs in the Probe Gateway and Probe Manager.

The logs in this section are located in **<HP Business Availability Center root directory>\<Discovery Probe installation location>\root\logs**.

General Logs

wrapperProbe.log

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

Error Level. Any Discovery error that occurs within the Probe Gateway.

Information Level. Important information messages, such as the arrival or removal of a new task.

Debug Level. Record of every Probe access of the servlet.

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

probe-error.log

Summary of the errors from the Discovery Probe.

Error Level. All errors in the Discovery Probe components.

Information Level. N/A

Debug Level. N/A

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

probe-infra.log

List of all infrastructure messages.

Error Level. All infrastructure errors.

Information Level. Information about infrastructure actions.

Debug Level. Messages mainly for debug purposes.

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

wrapperLocal.log

Error Level. Any Discovery error that occurs within the Probe Manager.

Information Level. Important information messages such as, received tasks, task activation, and the transferring of results.

Debug Level.

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

Probe Gateway Logs

probeGW-taskResults.log

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

Error Level. N/A

Information Level. Result details: task ID, job ID, number of CIs to delete or update.

Debug Level. The **ObjectState HolderVecto**r results that are sent to the server (in an XML string).

Basic Troubleshooting.

➤ If there is a problem with the results that reach the server, check this log to see which results were sent to the server by the Probe Gateway.

➤ The results in this log are written only after they are sent to the server. Before that, the results can be viewed through the Probe JMX console (use the ProbeGW Results Sender MBean).

probeGW-tasks.log

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

Error Level. N/A

Information Level. N/A

Debug Level. The task's XML.

Basic Troubleshooting.

➤ If the Probe Gateway tasks are not synchronized with the server tasks, check this log to determine which tasks the Probe Gateway received.

➤ You can view the current task's state through the JMX console (use the Discovery Scheduler MBean).

Probe Manager Logs

probeMgr-services.log

Java services debug messages.

Error Level. N/A

Information Level. N/A

Debug Level. N/A

Basic Troubleshooting. Check this log to view Java services debug messages.

probeMgr-performance.log

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

Error Level. N/A

Information Level. N/A

Debug Level. N/A

Basic Troubleshooting.

➤ Check this log to investigate memory issues over time.

➤ The statistics are logged every 1 minute, by default.

probeMgr-patternsDebug.log

This log contains messages used to debug Discovery pattern issues.

Error Level. N/A

Information Level. N/A

Debug Level. N/A

Basic Troubleshooting. Use this log file for debugging Discovery patterns.

Troubleshooting and Limitations

For details on using the log files to perform basic troubleshooting, see "Discovery Log Files" on page 108.

This section includes the following topics:

➤ "The Probe Gateway and Probe Manager Activation" on page 115

➤ "The Probe Gateway and Probe Manager Connection" on page 116

The Probe Gateway and Probe Manager Activation

Problem. The Probe Gateway or Probe Manager cannot be activated.

Indication. When trying to activate the Probe Gateway or Probe Manager, the console opens and immediately closes.

Verification. To view the exception message, open the following files located in **<Business Availability Center root directory>\root\logs**:

➤ For the Probe Gateway: **wrapperProbe.log**

➤ For the Probe Manager: **wrapperLocal.log**

A message is displayed. If one of the following messages appears, the problem lies in the memory size definition:

```
Initial heap too small for new size specified.
Incompatible initial and maximum heap sizes specified.
The port number is being used.
```

To solve this problem, see the following Solution section. If another message appears and you cannot fix the problem, contact Customer Support.

Solution. There can be several reasons for the activation problem, for example:

➤ **Inappropriate memory size.** Minimum and maximum memory sizes are allocated for each CMDB component. These definitions are set in the batch.cmd file, under the set memory sizes section. If memory sizes are too high for your workstation, are illegal, or incompatible with one another, you must change them, save the file, and restart the component whose values you changed.

➤ **Installation path is too long.** If you installed Business Availability Center to a directory with a long path, the operating system or JVM may have problems running the Business Availability Center execution commands. Reinstall Business Availability Center to a different directory that creates a shorter path.

The Probe Gateway and Probe Manager Connection

Problem. The connection between the Probe Gateway and Probe Manager cannot be established.

Indication. The Discovery process is not working properly.

Verification. For the Probe Gateway: An error message is displayed in the Probe Gateway log (**wrapperProbe.log**, located in **<Business Availability Center root directory>\root\logs**), as shown in the following example:

```
Failed to connect to probe manager at <server>. Will retry later
```

For the Probe Manager: An error message is displayed in the Probe Manager log (**probe-infra.log**, located in **<Business Availability Center root directory>\root\logs**), as shown in the following example:

```
Connection attempt to service:jmx:rmi:///jndi/rmi://<Probe GW HOST>:1742/jmxrmi
failed, probe GW may be down
```

Solution. Check the following:

➤ Verify that the correct port—1742—is defined. The RMI connection port parameter is called appilog.collectors.rmi.port. It is defined in the **appilog-remote.properties** file, located in **<Business Availability Center root directory>\root\lib\collectors**.

➤ Verify whether the Probe Manager port is being used by another application. To verify this, in the Windows command interpreter (cmd.exe) type: netstat -na. A list of ports that are currently in use is displayed. If the port is in use, either close the other application or change the port number in the appilog-remote.properties file.

Host Name Cannot Be Resolved to IP Address

Problem. A host name cannot be resolved to its IP address. If this happens, the host cannot be discovered, and Discovery patterns do not run.

Solution. Add the host machine name to the Windows HOSTS file on the Discovery Probe machine.

Discovery Tab Missing from Tabs

Problem. The Discovery tab is not displayed in the main page of Business Availability Center.

Solution. Install a license for the Discovery Probe. For details, see Chapter 2, "Licensing Models."

Discovery Results Do Not Appear in the Topology Map

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

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

Solution. Check the error messages in the **probeMgr-services.log** file located in **<Business Availability Center root directory>\root\logs**.

Networks and IPs

Problem. Not all networks or IPs have been discovered.

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

Verification. The IP address range in the Domain Configuration window does not encompass the scope of the networks or IPs that should have been discovered.

Solution. Change the scope of the Discovery range:

1 Select **Admin > Discovery > Domain Configuration** to open the Domain Configuration window.

2 Select the Probe and the range.

3 Change the IP address range in the Ranges box as required.

TCP Ports

Problem. Not all TCP ports have been discovered.

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

Verification. Open the **portNumberToPortName.xml** file (**Admin** > **Universal CMDB** > **Resource Configuration** > **Network** > **Configuration Files** > **portNumberToPortName.xml**), and search for the missing TCP ports.

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

Resolving DNS Names

Problem. The Probe Manager cannot resolve DNS names.

Indication. The Host's label in the topology map contains only the CIT to which it belongs.

Verification. In the topology map, right-click the host whose DNS name has not been resolved. Select **Show CI Attributes** to open the CI Attributes dialog box. Check the **host_dnsname** field. If it is empty, the DNS name has not been resolved.

Solution.

Verify that:

➤ The protocol agent is installed on the remote machine.

➤ Business Availability Center can communicate with the protocol agent.

➤ You have the correct permissions to access the protocol agent.

Resolve the DNS name using any of the following protocols:

➤ SNMP

➤ Telnet

➤ SSH

➤ WMI

Status 'Disconnected' for Probe

Problem. Discovery shows a disconnected status for a Probe.

Solution. Check the following on the Probe machine:

➤ That the Probe is running.

➤ That there are no network problems.

SSH/Telnet Credentials

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.

SNMP Credentials

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 "Protocol Parameters Dialog Box" on page 167.

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

SAP Discovery Fails

Problem. The SAP Discovery fails and a java.exe message is displayed

This application has failed to start because MSVCR71.dll was not found.

Solution. Two .dll files are missing. For the solution, read Note #684106 in https://websmp205.sap-ag.de/~form/sapnet?_FRAME=CONTAINER&_ OBJECT=012003146900000245872003.

Host Fingerprinting in Nmap Cannot Run on Probe

Problem. When running the Host Fingerprinting feature in Nmap on a Probe that is installed on a Windows 2003 Server, you see an error message.

Solution. You cannot run Host Fingerprinting in Nmap when the Discovery Probe is installed on a Windows 2003 Server. Install the Probe on a different operating system, for example, Windows 2000.

Limitations

➤ To perform a DB2 Discovery, copy the files **db2java.zip** and **db2jcc.jar** from the DB2 installation folder and place them in **HP Business Availability Center's\DiscoveryProbe\root\ext\jdbcdrivers\DB2**.

➤ When performing an Oracle RAC Discovery, note that Discovery cannot discover links to the remote machines (the database clients) in the following situation: The discovered database reports its clients by their host names and not by their IP addresses, and the host name cannot be resolved to an IP address. In this case, the remote client cannot be created.

Part III

Discovery User Interface

6

Job Configuration User Interface

This chapter includes the pages and dialog boxes that are part of the Job Configuration user interface.

This chapter describes:	On page:
Choose CIs to Add Dialog Box	124
Choose Discovery TQL Dialog Box	125
Choose Probe Dialog Box	126
CIs Discovered by [Module or Job Name] Dialog Box	126
Dependency Map Tab	128
Details Tab	130
Discovery Modules Pane	139
Discovery Scheduler Dialog Box	142
Edit Probe Limitation for TQL Output Dialog Box	139
Find Jobs Dialog Box	144
Job Configuration Window	145
Job Editor Dialog Box	145
Properties Tab	146
Source CIs Dialog Box	150
Trigger TQL Editor	150

Choose CIs to Add Dialog Box

Description	Enables you to choose CIs to run with selected jobs.
	✚ **To access:** Click the **Add CI** button in the Trigger CIs pane.

The Choose CIs to Add dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Add button	**Note:** If you choose CIs with an error status to add to the trigger list, a message is displayed when you click the Add button.
Search CIs	Contains filters with which you can limit the number of CIs that appear in the Search Results pane.
	➤ **By Discovery TQL**. Select a Discovery TQL to search for those CIs that match the TQL.
	➤ **Show only CIs containing.** To search for CIs that include a certain text, enter the text here.
	➤ **Exact match.** Select to search for CIs with the exact match of the text label. (By default, you search by entering part of a text. For example, searching for **10** within the IP CIs finds all the IPs that contain 10 in their address. Entering **10** then selecting **Exact match** finds no results.)
	➤ **Search.** Click to display the search results.

GUI Element	Description
Search Results	Displays a list of triggered CIs answering to the criteria set in the filter. To add the CIs to the list in the triggered CIs pane, select the CIs. You can make multiple selections. ➤ **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. **Page.** The list of CIs is divided into pages. The number in the Page box indicates which page is currently displayed. To view other pages, use the up and down arrows, or type the page number, and press **Enter.** To determine the number of CIs that appear on a page, right-click either the up or down button and choose the required number. The default is 25.

Choose Discovery TQL Dialog Box

Description	Enables you to add a trigger TQL to a job. **To access:** Click the **Add TQL** button in the Trigger TQLs pane.

The Choose Discovery TQL dialog box includes the following elements (listed alphabetically):

GUI Element	Description
<Discovery TQL name>	The TQLs that can query the CMDB for the selected CIT.
TQL Preview	Hold the cursor over an element to view details.

Choose Probe Dialog Box
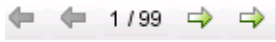
Description	Enables you to filter the Probe list.
	To access: Click a Filter button in the **Job Configuration** > **Details** tab:
	➤ **Triggered CIs** pane Filter button. For details on the menu options, see "Trigger CIs Pane" on page 136.
	➤ **Statistics** pane Filter button. For details on the menu options, see "Statistics Pane" on page 133.

CIs Discovered by [Module or Job Name] Dialog Box

Description	Enables you to view CI instances for a CIT.
	To access:
	➤ Click the **View instances** button in the Statistics pane.
	➤ Select **Show discovered CIs** or **Show all CI instances** in the Dependency Map.
Important Information	Depending on whether you select **Show discovered CIs** or **Show all CI instances** in the Dependency Map, you can view either all CIs discovered by a selected job or all CIs of a selected type. The number of displayed CIs appears at the top of the dialog box:
	CIs discovered by [Host Connection by SNMP or WMI or SHELL] - CIs
	CI Instances Last update at Thu Apr 26 2007 05:18 PM IDT Total CIs: 170

The CIs Discovered by [Module Name] dialog box includes the following elements (listed alphabetically):

GUI Element	Description
	Click to define a filter to shorten the list of results. For details, see "Filter CI Instances Dialog Box" in *Reference Information*.
	Clears the filter. All results are displayed in the list.

GUI Element	Description
	Click to select the columns to be displayed. For details, see "Columns Dialog Box" in *Reference Information*.
	Click to refresh the list of CI instances.
	Set rows per page.
⬅ ⬅ 1 / 99 ⮕ ⮕	Display another page.

<right click a row>	➤ **View Sublayer.** Displays a window showing the CIs in the layer beneath the selected CI. **Note:** This option is only active for CIs with children.
	➤ **Properties.** Displays the Properties page for the selected CI.
	➤ **CI History.** Displays the CI History dialog box.
	➤ **Label.** Select one of the following options:
	  ➤ **Edit Label.** Opens the Edit Label dialog box which enables you to edit the name of the CI.
	  ➤ **Reset Label.** Resets the CI name to its default value taken from the CMDB.
	➤ **Note.** Select one of the following options:
	  ➤ **Add Note.** Opens an editing box where you can type a note to be attached to the CI.
	  ➤ **Delete Note.** Deletes all text saved in a note.
	➤ **Delete.** Enables you to delete the selected CI from the view and from the CMDB. **Note:** When you delete a parent CI, the CI and its children are removed from the view, but only the CI is removed from the CMDB.
	➤ **New Related CI.**
	➤ **Attach Related CI.** Click to open the CI Wizard.
	➤ **Actions.** Select one of the following options:
	  ➤ **Add CI to Discovery Job.**
	  ➤ **Remove CI from Discovery Job.**

GUI Element	Description
Display Hidden Columns button	Click to display all CI attributes. Click **Show Filtered Attributes** to display the CI attributes selected in the Columns dialog box.
Show Filtered Attributes	Click to hide attributes.

Dependency Map Tab

Description	Displays a visual representation of the real-time progress of the Discovery process. The map displays:
	➤ CIs that were triggered by a Discovery job
	➤ CIs that were discovered as a result of the activated Discovery job.
	To access: Click the **Dependency Map** tab in the Job Configuration window.
Important Information	Depending which level you select in the Discovery Modules pane, different information is displayed in the Dependency Map tab.
	If you select:
	➤ **The Discovery Modules root**, and select the **Show only active Discovery jobs** check box, the Dependency Map displays only active jobs and their interdependencies.
	➤ **The Discovery Modules root**, and clear the **Show only active Discovery jobs** check box, the Dependency Map displays all Discovery jobs and their interdependencies.
	➤ **A module**, a topology map is displayed showing the module's active and inactive jobs.
	➤ **A job**, the topology map highlights the job in the module's map.
Useful Links	"CIs Discovered by [Module or Job Name] Dialog Box" on page 126

The Dependency Map tab includes the following elements (listed alphabetically):

GUI Element	Description
<Right-click menu>	Use the right-click menu to view details for a job, CI, or link, for example, the number of CI instances (of a specific type) in the CMDB or the number of CI instances created by a specific Discovery job.
	Depending on which object is selected, the following menu options are displayed:
	➤ When a job is selected:
	Show discovered CIs. Click to view the CIs discovered by the Discovery job. To filter the query, select a CIT from the menu.
	Show trigger CIs. Click to view the CIs that triggered the Discovery job.
	➤ When a CI is selected:
	Show all CIT instances. Click to view all CIs of this CI type.
	➤ When a link from a CI to a job is selected:
	Show trigger CIs for job. Click to view CIs (of the selected type) that triggered the Discovery job.
	➤ When a link from a job to a CI is selected:
	Show discovered instances. Click to view CIs (of the selected type) that were discovered by the Discovery job.
<Toolbar>	For details, see Chapter 7, "Toolbar Options" in *Reference Information*.
<Tooltip>	Hold the pointer over a CI or Discovery job to display a description.
Show only active Discovery jobs	When the Discovery Modules root is selected in the Discovery Modules pane, this check box is displayed.
	Select to display all active jobs (from any module).

Details Tab

Description	Enables you to view and administer modules and jobs.
	To access: Click the Discovery Modules root, a module, or a job in the Discovery Modules pane.
Important Information	Depending which level you select in the Discovery Modules pane, different information is displayed in the Details tab.
	If you select:
	➤ **The Discovery Modules root**, the Active Jobs and Statistics panes are displayed with information and statistics about all active jobs. For details, see "Active Jobs Pane" on page 131 and "Statistics Pane" on page 133.
	➤ **A Discovery module**, all the module's jobs are displayed and statistics about the module's CITs. For details, see "Module Jobs Pane" on page 132 and "Statistics Pane" on page 133.
	➤ **A job**, Discovery job details and the Trigger CIs and Statistics panes are displayed. For details, see "Discovery Job Details Pane" on page 135, "Trigger CIs Pane" on page 136 and "Statistics Pane" on page 133.

Active Jobs Pane

The Active Jobs pane includes the following elements (listed alphabetically):

GUI Element	Description
<Column title>	Click a column title to sort by that column. The arrow indicates whether the result is displayed in ascending or descending order.
<Right-click menu>	Right click a row to open the Discovery Scheduler for the selected job. For details, see "Discovery Scheduler Dialog Box" on page 142. Right-click a column title to customize the table. Choose from the following options: ➤ **Hide Column.** Select to hide a specific column. ➤ **Show All Columns.** Displayed when a column is hidden. ➤ **Customize.** Select to display or hide columns and to change the order of the columns in the table. Opens the Columns dialog box. ➤ **Auto-resize Column.** Select to change a column width to fit the contents. For details, see "Columns Dialog Box" in *Reference Information*.
Invoke Immediately	➤ A check mark ✔ signifies that the Discovery job 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 Properties tab. ➤ A hyphen (-) signifies that the job runs according to the schedule defined in the Schedule Manager.
Job Name	The job name.
Schedule Information	The scheduling information of the Discovery job as defined in the Scheduler Manager.
Trigger TQLs	The name of the TQL that activated the Discovery job.

Module Jobs Pane

The Module Jobs pane includes the following elements (listed alphabetically):

GUI Element	Description
<Column title>	Click a column title to sort by that column. The arrow indicates whether the result is displayed in ascending or descending order.
<Right-click menu>	Right click a row to open the Discovery Scheduler for the selected job. For details, see "Discovery Scheduler Dialog Box" on page 142.
	Right-click a column title to customize the table. Choose from the following options:
	➤ **Hide Column.** Select to hide a specific column.
	➤ **Show All Columns.** Displayed when a column is hidden.
	➤ **Customize.** Select to display or hide columns and to change the order of the columns in the table. Opens the Columns dialog box.
	➤ **Auto-resize Column.** Select to change a column width to fit the contents.
	For details, see "Columns Dialog Box" in *Reference Information*.
Invoke Immediately	➤ A check mark signifies that the Discovery job 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 Properties tab.
	➤ If this column does not contain a check mark, the job runs according to the schedule defined in the Schedule Manager.
Job Name	The job name.
Schedule Information	The scheduling information of the Discovery job as defined in the Discovery Scheduler.
Trigger TQLs	The name of the TQL that activated the Discovery job.

Statistics Pane

The Statistics pane includes the following elements (listed alphabetically):

GUI Element	Description
  <View instances>	Select a CI and click this icon to view CI instances and their attributes. The CIs Discovered by [Module or Job Name] Dialog Box opens. Under the following conditions, a message is displayed: ➤ All the CIs that were discovered by this job were already discovered by another job. ➤ All the CIs that this job discovered have been deleted. ➤ The CI instances were discovered in a previous version. (In version 7.0, you cannot view instances of CIs discovered in a previous version.) **Note**: You can also view CI instances by double-clicking a row.

	Select the time range or probe for which to display statistics about the CITs.
	
	➤ **By Time Range**:
	    ➤ **All.** Displays statistics for all Discovery job runs.
	    ➤ **Last Hour/Day/Week/Month.** Choose a period of time for which to display statistics about the CITs.
	    ➤ **Custom Range.** Click to open the Customize Statistics Time Range dialog box. Enter the date or click the arrow to choose a date and time from the calendar, for the **To** and **From** dates. To delete a date, click **Reset**.
	➤ **By Probe**: To view statistics for a specific Probe, select to open the Choose Probe dialog box.

	Click to retrieve the latest data from the server (Discovery job results are not automatically updated in the Statistics pane).

GUI Element	Description
▼	Click a column title to sort by that column. The arrow indicates whether the result is displayed in ascending or descending order.
<right-click a title>	Choose from the following options: ➤ **Hide Column.** Select to hide a specific column. ➤ **Show All Columns.** Displayed when a column is hidden. ➤ **Customize.** Select to display or hide columns and to change the order of the columns in the table. Opens the Columns dialog box. ➤ **Auto-resize Column.** Select to change a column width to fit the contents. For details, see "Columns Dialog Box" in *Reference Information*.
CIT	The name of the discovered CIT.
Created	The number of CIT instances created in the period selected or for the selected probe.
Deleted	The number of CIT instances deleted in the period selected or for the selected probe.
Discovered CIs	The number of CIs that were discovered for each CI type.
Filter	The time range set with the Set Time Range button.
Last updated	The date and time that the statistics table was updated for a particular job.
Total	The total number of CIs in each column.
Updated	The number of CIT instances that were updated in the period selected.

Discovery Job Details Pane

The Discovery Job Details pane includes the following elements (listed alphabetically):

GUI Element	Description
Discovered CIs	The CIs that are discovered by this job.
Input CI Type	The CIT that triggers the CIs for this job.
Job Name	The name and description of the Discovery job and the package in which it is located.

Trigger CIs Pane

The Discovery job runs using only the CIs that appear in the Trigger CIs pane. The Triggered CIs pane includes the following elements (listed alphabetically):

GUI Element	Description
	Refresh. To update the list of trigger CIs currently being used by the Discovery job.

Filter CIs
	Click and choose an option from the menu:
	➤ **By Status.** Displays a list of trigger CIs:
	  ➤ **All.** Displays all the trigger CIs.
	  ➤ **Waiting for Probe.** Displays the trigger CIs that are ready to be dispatched and are waiting for the Discovery Probe to retrieve them.
	  ➤ **Active.** Displays the trigger CIs that are active and are running on the Discovery Probe.
	  ➤ **Active (being removed).** Displays the trigger CIs that are being removed from the **Trigger CIs** list.
	  ➤ **Discovery Errors.** Displays CIs with an error status.
	➤ **By Probe.** Displays only the CIs triggered by a selected Probe. Click to open the Choose Probe to Filter dialog box.
	➤ **By Dispatch Type.** Displays a list of CIs according to one of the following options:
	  ➤ **All.** Displays both CIs that are used to manually activate the Discovery job and Discovery TQLs that are used to automatically activate the Discovery job.
	  ➤ **Manually added.** Displays the CIs that are used to manually activate the Discovery job.
	  ➤ **By Discovery TQL.** Displays the Discovery TQLs that are used to automatically activate the Discovery job.
	➤ **Reset.** Click to remove any filters.

GUI Element	Description
	Enables you to view details of a problem that is preventing Discovery from running, for example, a protocol connection failure.
	Click and choose an option from the menu:
	➤ **Show error details.** Opens the Error dialog box that includes details of the problem.
	➤ **Acknowledge error.** Select to remove an error from the CI. Once selected, this option and **Show error details** are disabled.
	➤ **Acknowledge all CIs.** Acknowledges the errors for all the CIs in the Discovery job.
	➤ **Remove.** Once selected, this option and the two previous options are disabled.
	➤ **Run now.** The Discovery job runs again using the selected trigger CIs.
	Note: Some of these options are also available when you right-click a CI row.
	You can also double-click the required trigger CI to open the Error dialog box.
	View instances. Click to open the Source CIs dialog box.

GUI Element	Description
+	**Add CI.** For details, see "Choose CIs to Add Dialog Box" on page 124. You would add CIs in the following cases: ➤ To restore CIs which were previously removed from the list (with the Delete button). ➤ To enable the trigger TQL (accessed in the Job Properties tab) that was disabled, preventing Discovery from automatically finding trigger CIs. ➤ To add a CI that is not included in the trigger TQL. (Not recommended. It is preferable to configure the trigger TQL to include all necessary triggers. For details, see "Trigger TQL Editor" on page 150.) **Note:** ➤ This button is enabled for active jobs only. ➤ If there is an error in a CI's status, the CI is added to the trigger list and a message is displayed.
✕	**Remove CI.** Select the CI to remove and click the button. The Discovery job runs without that CI.
CI	The triggered CIs that are currently being used by the Discovery job.
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.
Probe	The Discovery Probe on which the job is running.
Search	To filter the list of trigger CIs or to display only specific CIs, type a string in the Search box and click **Search**.
Status	The current status of the triggered CI. For details, see the Filter CIs section in this table.

Discovery Modules Pane

Description	Enables you to view and manage the Discovery modules and jobs. Each module includes the Discovery jobs necessary to discover specific CIs.
	To access: Admin > **Universal CMDB** > **Discovery** > **Job Configuration**.
Important Information	**Note:** Only administrators with an expert knowledge of the Discovery process should delete Discovery modules.

The Discovery Modules pane includes the following elements:

GUI Element	Description
	Refresh All. Updates the Discovery modules.
	Find Job. Click to open the Find Jobs dialog box. For example, to search for all jobs that discover SNMP connections, click the Filter icon. In the Find Jobs dialog box, enter **SNMP** in the Name field and click **Find All**. For details, see "Find Jobs Dialog Box" on page 144.
Activate	**Activate.** Click to run a Discovery module or job. You can choose to activate all Discovery jobs in a Discovery module or some of them: ➤ To activate all jobs in a module, right-click the module and select **Activate**. ➤ To activate specific jobs in a module, right-click the job and select **Activate**.
Deactivate	**Deactivate.** Select the jobs or modules to be stopped and click **Deactivate**.
	Represents the Discovery module root. To create a module, right-click to enter the name of the module you are creating. **Note:** A name is case sensitive. Names beginning with an upper case letter appear in the Discovery Modules list before names beginning with a lower case letter.

GUI Element	Description
	Represents a module. Click to display information about the modules being used for the Discovery process.
	For details on the right-click menu, see "Right-Click Menu" on page 141.
	Represents a Discovery job. Click to display information about the job. To view a pattern description, hold the pointer over a job.
	Discovery jobs contain configuration information derived from patterns and other resources and are the entities controlled by users, for example, when activating or deactivating a module.
	For details on the right-click menu, see "Right-Click Menu" on page 141.
⊞	Click to display a module's jobs.
	One green dot signifies that some of a module's jobs are activated.
	Three green dots signify that all of a module's jobs are activated.
	An exclamation mark signifies that one or more of the Discovery jobs is experiencing a problem that could affect the Discovery process, for example, a protocol connection failure.
	To view the reason for the problem, click the Handle errors button in the Triggered CI pane. For details, see "Trigger CIs Pane" on page 136.
	Note: If a problem is resolved by clicking the **Refresh All** button, the Problem Indicator disappears.

Right-Click Menu

Right-Click Menu	Description
Activate	Click a module to run all its jobs. To run a specific job, select and activate it.
	The Discovery Module discovers CITs and relationships of the types that are described in each job, and places them in the CMDB. For example, the Class C IPs by ICMP job discovers the Depend, IP, and Member CITs and relationships.
Create New Job	Click to open the Job Editor dialog box. For details, see "Job Editor Dialog Box" on page 145.
Create New Module	Click to define a new name for the module root.
Deactivate	Stop the module or job from running.
Delete	Click and answer **Yes** to the warning message.
Delete job	Click and answer **Yes** to the warning message.
Edit Pattern	Click to edit the pattern in the Resource Configuration window.
Edit Scheduling	Click to open the Discovery Scheduler to define a schedule for a specific job.
Rename job	Click to open the Choose Name dialog box. Enter a new name for the job.
	Note: You cannot rename active jobs.
Run Now	Click to run the Discovery job again using the selected trigger CIs.
Save as...	Click to clone the job.

Discovery Scheduler Dialog Box

Description	Enables you to define a schedule for a specific job.
	To access:
	➤ Right-click a job and choose **Edit scheduling**.
	➤ Click the **Edit Scheduling** button in the Properties tab of the Job Configuration window.

The Discovery Scheduler dialog box includes the following elements (listed alphabetically):

GUI Element	Description
🔧	Opens a calendar. Select the required date and time.
Validate Expression	Click to validate the Cron expression you entered.
<Frequency>	➤ **Once.** Define the task to run only once.
	➤ **Interval.** Defines the interval between successive runs.
	➤ **Daily.** Run a task on a daily basis.
	➤ **Weekly.** Run a task on a weekly basis
	➤ **Monthly.** Run a task on a monthly basis.
	➤ **Cron.** Enter a Cron expression in the correct format.
Days of month	(Appears when you select **Monthly**) Click the button ⏵⏵ to choose the days of the month on which the action must run. The Select Days dialog box opens. Choose the required days by selecting the check boxes. You can select multiple days.
	➤ **Select all**. Select all the days.
	➤ **Unselect all**. Clear all the selected days.
Days of the week	(Appears when you select **Weekly**) Select the day or days on which you want the action to run.

GUI Element	Description
End by	Select the date and time when you want the action to stop running by selecting the **End by** check box and clicking the **Open Calendar** [image] button. **Note**: This step is optional. If you do not want to specify an ending date, leave the **End by** check box unselected.
Invocation Hour	(Appears when you select **Daily**, **Weekly**, or **Monthly**) Select the time to activate the action. Click the button [image] to open the Select Hours dialog box. Choose the required time by selecting the check boxes. You can select multiple times. ➤ **Select all**. Select all the times. ➤ **Unselect all**. Clear all the selected times. **Note**: You can also enter the time manually in the **Invocation hour** box. Separate times by a comma and enter AM or PM after the hour. The manually entered action times are not restricted to the hour and half hour only: you can assign any hour and minute combination. Use the following format: HH:MM AM, for example, 8:15 AM, 11:59 PM.
Invocation Time	(Appears when you select **Once**) Choose the date and time you want the action to begin running by clicking the **Open Calendar** [image] button.
Months of the year	(Appears when you select **Monthly**). Select the month or months in which you want the action to run.
Repeat every	(Appears when you select **Interval**) Type a value for the interval between successive runs and choose the required unit of time (seconds, minutes, hours, or days).
Start at	Choose the date and time when you want the action to begin running by selecting the **Start at** check box and then clicking the **Open Calendar** [image] button to the right.
Time Zone	Set the time zone to the server time zone by clicking the **Set server time zone** button.

Edit Probe Limitation for TQL Output Dialog Box

Description	Enables you to change the Probes on which a trigger TQL is running.
	To access: Select a job and click the following button: **Job Configuration** > **Properties tab** > **Trigger TQLs pane** > **Probe Limit field**.
Useful Links	For details, see "Selecting Probes" on page 168.

Find Jobs Dialog Box

Description	Enables you to search for jobs answering to specific criteria.
	To access: Click the **Filter** button in the Discovery Modules pane.

The Find Jobs/Resources dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Direction	Searches forwards or backwards through the Discovery modules.
Find All	All jobs meeting the search criteria are highlighted.
Find Discovery job by	Choose between: ➤ **Name.** Enter the name, or part of it, of the job. ➤ **Input type.** CIs that triggered the Discovery job. Click the button ⋯ to open the Choose Configuration Item Type dialog box. Locate the CI type that you are searching for. ➤ **Output type.** CIs that are discovered as a result of the activated Discovery job.
Find Next	The next job meeting the search criteria is highlighted.

Job Configuration Window

Description	Enables you to view and manage Discovery modules and jobs, and to follow job progress.
	The Discovery Manager includes:
	➤ Discovery Modules pane. Each Discovery module includes Discovery jobs. You activate a module or job to discover a specific group of CIs. For details, see "Discovery Modules Pane" on page 139.
	➤ Details tab. Enables you to manage a module's CIs and view CI statistics. For details, see "Details Tab" on page 130.
	➤ Properties tab. Enables you to view and administer the properties of modules and jobs. For details, see "Properties Tab" on page 146.
	➤ Dependency Map. Displays a visual representation of the real-time progress of the Discovery process. For details, see "Dependency Map Tab" on page 128.
	To access: Admin > **Universal CMDB** > **Discovery** > **Job Configuration**.

Job Editor Dialog Box

Description	Enables you to create a Discovery job.
	To access: Right-click a module in the Discovery Modules pane, and choose **Create New Job**.

The Job Editor dialog box includes the following elements (listed alphabetically):

GUI Element	Description
✚	Add TQL.
✕	Delete TQL.

GUI Element	Description
	Open the TQL Editor to make changes to TQLs on the fly and add the changes to the job.
Description	A description of the job.
Discovery Pattern	Click the **Select** button to open the Choose Discovery Patterns dialog box. Use the SHIFT or CTRL keys to select several patterns.
Discovery Scheduler	Click the **Edit Scheduler** button to open the Discovery Scheduler dialog box.
Invoke on new triggered CIs immediately	A check mark signifies that the Discovery job runs as soon as the triggered CI reaches the Discovery Probe. If this column does not contain a check mark, the job runs according to the schedule defined in the Schedule Manager.
Job Name	Enter a name for the job.
Parameters	**Override.** Select to override the parameter value in the pattern. **Name.** The name given to the pattern. **Value.** The value defined in the pattern.
Trigger TQLs	**TQL Name.** The name defined for the TQL. **Probe Limit.** The Probes being used for the Discovery process. To add or remove Probes, click the button.

Properties Tab

Description	Enables you to view and administer the properties of modules and jobs. **To access:** Click the Properties tab in the Discovery Manager.
Important Information	Depending which level you select in the Discovery Modules pane, different information is displayed in the Properties tab.

The Properties tab includes the following elements (listed alphabetically):

GUI Element	Description
	Refreshes the list of CIT statistics.
	(Displayed when **Discovery Modules** is selected in the Discovery Modules pane.)
	➤ **By Time Range.**
	➤ **All.** Displays statistics for all Discovery job runs.
	➤ **Last Hour/Day/Week/Month.** Choose a period of time for which to display statistics about the CITs.
	➤ **Custom Range.** Click to open the Customize Statistics Time Range dialog box. Enter the date or click the arrow to choose a date and time from the calendar, for the **To** and **From** dates. To delete a date, click **Reset**.
	➤ **By Probe.** Displays only the CIs triggered by a selected Probe. Click to open the Choose Probe to Filter dialog box.
	(Displayed when **Discovery Modules** is selected in the Discovery Modules pane.)
	Click to open the CIs Discovered dialog box.
	(Displayed when **Discovery Modules** is selected in the Discovery Modules pane.)
Description	To edit the description, make changes and click **OK**.
	(Displayed when a specific module or job is selected in the Discovery Modules pane.)
Discovery Module Name	(Displayed when a module is selected in the Discovery Modules pane.)
Discovery Pattern	Displays the name of the pattern that is run by the job. Click the Edit button to open the Resource Configuration window. For details, see Chapter 8, "Resource Configuration User Interface."
Discovery Scheduler	Information about the schedule set up for this job.
Edit Scheduler	Click to open the Discovery Scheduler.

GUI Element	Description
Filter	The time range for which the statistics have been calculated. (Displayed when **Discovery Modules** is selected in the Discovery Modules pane.)
Invoke on New Trigger CIs Immediately	A check mark signifies that the Discovery job runs as soon as the trigger CI reaches the Discovery Probe. If this column does not contain a check mark, the job runs according to the schedule defined in the Schedule Manager.
Job Name	The name of the job and the package in which the job is included. (Displayed when a job is selected in the Discovery Modules pane.)
Last updated	The time when the Discovery job was last run. (Displayed when **Discovery Modules** is selected in the Discovery Modules pane.)
Module Jobs	✚ **Add Discovery Job to Module.** Opens the Choose Discovery Jobs dialog box where you can select jobs from more than one zip file. (Use the SHIFT or CTRL key to select several jobs.) ✖ **Remove Selected Discovery Job from Module.** Select the job and click the button. (No message is displayed. To restore the job, click the **Cancel** button.) **<List of jobs>.** All jobs included in the module. (Displayed when a specific module is selected in the Discovery Modules pane.)
Parameters	Use this pane to override pattern behavior. For example, to change timeout, select the **Override** check box and change the value of the parameter. Click **OK** to save the change. To view a description, hold the pointer over the parameter.

GUI Element	Description
Statistics	For details, see "Statistics Pane" on page 133.
	(Displayed when **Discovery Modules** is selected in the Discovery Modules pane.)
Trigger TQLs	Define one or more TQL queries to be used as triggers to activate the selected Discovery job.
	For details, see "Trigger TQLs Pane" on page 149.

Trigger TQLs Pane

The Trigger TQLs pane includes the following elements (listed alphabetically):

GUI Element	Description
+	**Add TQL.** You can add one or more non-default TQL queries to be used as triggers to activate the selected Discovery job. Click to open the Choose Discovery TQL dialog box.
✕	**Remove TQL.** Select the TQL and click the button.
	(No message is displayed. To restore the TQL, click the **Cancel** button.)
	Note: If a TQL query is removed for an active job, Discovery no longer receives new CIs coming from that TQL query. Existing trigger CIs that originally came from the TQL query are not removed.
...	Click to add or remove Probes for a specific TQL. For details, see "Edit Probe Limitation for TQL Output Dialog Box" on page 144.
✏	Click to open the Trigger TQL Editor. For details, see "Trigger TQL Editor" on page 150.
⊡	Click to open the Query Manager. For details, see Chapter 30, "Query Manager User Interface."

GUI Element	Description
Probe Limit	The Probes being used for the Discovery process. To add or remove Probes, click the button.
TQL Name	The name of the trigger TQL query that activates the Discovery job.

Source CIs Dialog Box

The Source CIs dialog box includes the same components as the CIs Discovered by [Module Name] dialog box. For details, see "CIs Discovered by [Module or Job Name] Dialog Box" on page 126.

Trigger TQL Editor

Description	Enables you to edit a TQL that has been defined to trigger Discovery jobs. **To access: Job Configuration > Properties tab > Trigger TQLs pane > select a TQL and click the Open the TQL Editor** button.

The Trigger TQL Editor includes the following elements (listed alphabetically):

GUI Element	Description
<Panes>	➤ CI Types Pane ➤ Editing Pane ➤ Information Pane
TQL Name	The name of the trigger TQL query that activates the Discovery job.

CI Types Pane

Description	Displays a hierarchical tree structure of the CI Types found in the CMDB. For more details, see "CI Type Manager User Interface" in *CI Attribute Customization*.
	Note: The number of instances of each CIT in the CMDB is displayed to the right of each CIT.
	To create or modify a TQL query, click and drag nodes to the Editing pane and define the relationship between them. Your changes are saved to the CMDB. For details, see "Adding Nodes and Relationships to a TQL Query" in *Reference Information*.
Important Information	The CI Types pane is part of the following managers: View Manager, Enrichment Manager, Query Manager, Correlation Manager, Report Manager, and Trigger TQL Editor.
Included in Tasks	➤ "Create a Correlation Rule" on page 81
	➤ "Define an Enrichment Rule" on page 108
	➤ "Define a TQL Query" on page 101
	➤ "Pattern View Workflow" on page 79
	➤ "Define a Report Rule" on page 86

Editing Pane

Description	Enables you to edit the node selected in the Trigger TQLs pane.

The Editing pane includes the following elements (listed alphabetically):

GUI Element	Description
<node>	Click to display information about the node in the information pane.
<Right-click menu>	For details, see Chapter 17, "Topology Query Language Context Menu Options."
<Toolbar>	For details, see Chapter 7, "Toolbar Options."

Information Pane

Description	Displays the properties, conditions, and cardinality for the selected node and relationship.
Important Information	The Information pane is part of the following managers and user interfaces: View Manager, Correlation Manager, Report Manager, Enrichment Manager, and Trigger TQL Editor.
Included in Tasks	➤ "Create a Correlation Rule" on page 81 ➤ "Define an Enrichment Rule" on page 108 ➤ "Define a TQL Query" on page 101 ➤ "Pattern View Workflow" on page 79 ➤ "Define a Report Rule" on page 86

The Information pane includes the following elements (listed alphabetically):

GUI Element	Description
Cardinality	Cardinality defines how many nodes you expect to have at the other end of a relationship. For example, in a relationship between host and IP, if the cardinality is 1:3, the TQL retrieves only those hosts that are connected to between one and three IPs. For details, see "Cardinality Tab" in *Reference Information*.
Condition	The attribute conditions defined for the node or the relationship. For details, see "Attribute Tab" in *Reference Information*.
Folding Rule	Displays the folding rule defined for the selected relationship. For details about folding rules, see "Adding Folding Rules to Relationships" in *IT World Model Management*.
	Note: This pane appears only when a relationship is selected in View Manager.

GUI Element	Description
Properties	➤ To open the Node/Relationship Condition dialog box, select a node or relationship in the Editing pane and click the **Edit Condition** 🖉 button. For details, see "Node/Relationship Condition Dialog Box" in *Reference Information*.
	➤ **CI Type.** The CIT of the selected node/relationship.
	➤ **Visible.** A tick signifies that the selected node/relationship is visible in the topology map. When the node/relationship is not visible, a box 🔲 appears to the right of the selected node/relationship in the Editing pane:
	➤ **Include subtypes.** Display both the selected CI and its descendents in the topology map.

7

Domain Configuration User Interface

This chapter includes the pages and dialog boxes that are part of the Domain Configuration user interface.

This chapter describes:	On page:
Add/Edit IP Range Dialog Box	156
Add/Edit Policy Dialog Box	158
Add New Domain Dialog Box	159
Add New Probe Dialog Box	160
Choose Discovery Jobs Dialog Box	161
Details Pane	161
Domain Configuration Window	165
Domains Browser Pane	166
Edit Related Probes Dialog Box	166
Edit Timetable Dialog Box	167
Protocol Parameters Dialog Box	167
Scope Definition Dialog Box	168
Selecting Probes	168

Add/Edit IP Range Dialog Box

Description	Enables you to set the network range for Discovery. The Discovery results are retrieved from the addresses in the range you define. You can also define IP addresses that must be excluded from a range.
	To access: Click the **Add IP range** button in the Details pane.
Important Information	If you define a Discovery range that is out of the scope of the network on which the Discovery Probe is installed, HP Business Availability Center automatically defines the range of the IP on which the Discovery Probe is running. The following message appears:
	Click **Yes** to add the Probe IP to the range.
Included in Tasks	Run Discovery

The Add IP Range dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Advanced	Click to enter ranges to be excluded from Discovery:
	✚ To exclude an IP range, click the **Add IP range** button.
	✖ To delete the excluded part of an IP range, select the excluded range and click the button.
	✐ To edit the excluded part of an IP range, click the button.
	For details, see Exclude Ranges.

GUI Element	Description
Exclude Ranges	Click the **Add IP range** or **Edit IP range** button to exclude part of a range. In the Exclude IP Range dialog box, enter the range to exclude. **Note:** ➤ You must enter a range (in the Add/Edit IP Range dialog box) before you can enter the excluded range. ➤ The rules for entering an excluded range are the same as for entering a range. For details, see Range. ➤ Use this feature to divide a network range into several subranges. For example, say a range is 10.0.64.0 – 10.0.64.255. You define three excluded ranges: 10.0.64.45 – 10.0.64.50 10.0.64.65 – 10.0.64.70 10.0.64.89 – 10.0.64.95 Therefore, the ranges to be discovered are: 10.0.64.0 – 10.0.64.44 10.0.64.51 – 10.0.64.64 10.0.64.71 – 10.0.64.88 10.0.64.96 – 10.0.64.255

GUI Element	Description
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 an asterisk (*****), representing any number in the range of 0-255. ➤ If you use an asterisk, you do not need to enter a second IP address. For example, you can enter the range pattern 10.0.48.* to cover the range from 10.0.48.0 to 10.0.48.255. ➤ Use an asterisk in the lower bound IP address of the IP range pattern only. (If you use an asterisk in the lower bound IP address and also enter an upper bound IP address, the upper bound IP address is ignored.) ➤ You can use more than one asterisk (*****) in an IP address as long as they are used consecutively. The asterisks cannot be situated between two numbers in the IP address, nor can they be substituted for the first digit in the number. For example, you can enter 10.0.*.* but not 10.*.64.*. ➤ Two probes in the same domain cannot have the same IP address in their range.

Add/Edit Policy Dialog Box

Description	Enables you to add a job execution policy, to disable jobs from running at specific times. **To access: Admin** > **Universal CMDB** > **Discovery** > **Domain Configuration** > **Details pane** > **Job Execution Policy** section. Select an existing policy and click **Edit**, or click the **Add** button.
Useful Links	"Job Execution Policies" on page 51

The Edit Policy dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Related jobs	➤ **Allow all.** Run the job execution policy on all jobs. ➤ **Total blackout.** The policy does not run on any jobs. ➤ **Allowed jobs.** Choose jobs to run even during the configured blackout time. ➤ **Disallowed jobs.** Choose jobs that do not run during the configured blackout time. For allowed and disallowed jobs, click the **Add job** or **Remove job** button to choose specific jobs to be included in, or excluded from, the policy. If you click the **Add job** button, the Choose Discovery Jobs dialog box opens.
Related Probes	The Probes on which to run the policy. Click the button to open the **Edit Related Probes** dialog box to define which Probes are included in the policy.
Time	The date and time during which the policy is active. Click the button to open the **Edit Timetable** dialog box.

Add New Domain Dialog Box

Description	Enables you to add a Discovery domain. **To access:** Click the **Add Domain or Probe** button in the Domains Browser pane.
Important Information	In an upgraded 6.x environment, to enable data to be modelled similarly as in the previous version, you must define the Discovery Probes as belonging to the **External** domain and not to the **Customer** domain.

The Add New Domain dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Description	Enter a description to appear in the Details pane of Domain Configuration.
Domain Type	➤ **Customer.** A private domain used for your site. You can define several domains and each domain can include multiple Probes. Each Probe can include IP ranges but the customer domain itself has no range definition. ➤ **External.** Internet/public domain. A domain that is defined with a range. The external domain can contain only one Probe whose name equals the domain name. However, you can define several external domains in your system.
Name	Enter a unique name for the domain.

Add New Probe Dialog Box

Description	Enables you to add a Discovery probe. **To access:** Click the **Add Domain or Probe** button in the Domains Browser pane.
Important Information	➤ To add a Probe to an existing domain, select **Probes** in the Discovery Domains pane and click the **Add Domain or Probe** button╬. ➤ To add a Probe to a new domain, create a domain, then add the Probe to the domain. ➤ Two probes in the same domain cannot have the same IP address in their range. ➤ When a probe is activated, it is added automatically and its status changes to connected. For details, see "Launch the Discovery Probe" on page 56.

Choose Discovery Jobs Dialog Box

Description	Enables you to choose the jobs that are to be added to, or excluded from, the job execution policy.
	To access: Select **Allowed Jobs** or **Disallowed jobs** in the Edit Policy dialog box and click the button ✚.

The Choose Discovery Jobs dialog box includes the following elements (listed alphabetically):

GUI Element	Description
<Installed packages>	Locate the job to be included in, or excluded from, the policy. To select jobs from several packages, hold down the CTRL key and make the selection.

Details Pane

Description	Enables you to view the Probes running under all domains and to add an execution policy to jobs (that is, to schedule time periods when jobs should not run).
	To access: Click an object in the Domains Browser pane.
Important Information	Depending on what you select in the Domains Browser pane, different information is displayed in the Details tab.
	If you select:
	➤ Discovery Domains, you can view details on all Probes and you can define and edit job execution policies.
	➤ A Specific Domain, you can add a description.
	➤ A Specific Protocol, you can add protocol parameters and you can view details on the protocol, including user credentials.
	➤ A Specific Probe, you can view details on the Probe, including range information. You can also add ranges to, or exclude ranges from, the Probe.

Discovery Domains

When Discovery Domains is selected in the Domains Browser pane, the Details tab includes the following elements (listed alphabetically):

GUI Element	Description
Discovery Probes	Includes a list of all probes connected to the server. ➤ **Name.** The Probe name as it appears in Discovery. ➤ **IP.** The IP range defined during Probe creation. ➤ **Status.** Can be Connected or Disconnected. ➤ **Last Access Time.** The last time that the Probe requested tasks from the server.
Jobs Execution Policy	The execution policy enables you to configure the periods of time when jobs in a Discovery should not run. ➤ Moves the policy up or down. Discovery executes all the policies in the list with the first policy taking priority. If a job is included in two policies, Discovery executes the first policy only for that job. ➤ Adds a policy. ➤Removes a policy. ➤Enables you to edit a policy. Click to open the Edit Policy dialog box. ➤ **Time.** The schedule of the policy. ➤ **Probes.** The Probes that are affected by the policy. ➤ **Jobs.** The jobs that are affected by the policy. **Note:** Jobs which have a listening functionality (that is, they do not perform Discovery) are not included in a policy.

A Specific Domain

When a specific domain is selected in the Domains Browser pane, the
Details tab includes the following elements (listed alphabetically):

GUI Element	Description
Description	The description that was entered during domain creation.
Domain Type	For details, see Domain Type in "Add New Domain Dialog Box" on page 159.

A Specific Protocol

When a specific protocol is selected in the Domains Browser pane, the
Details tab includes the following elements (listed alphabetically):

GUI Element	Description
✚	Click to add new connection details, to open the Add Protocol Parameters dialog box.
✖	Select a protocol and click to remove connection details. Answer **OK** to the message.
✐	Select a protocol and click to edit connection details in the Edit Protocol Parameters dialog box.
◆	Select a protocol and click to move the protocol instance up or down. **Note:** The lower the Protocol Index number, the higher the priority.
▼	Click a column title to sort by that column. The arrow indicates whether the result is displayed in ascending or descending order.

GUI Element	Description
<Right-click a credential>	Choose from the following options: ➤ **Edit.** Choose this option to enter protocol parameters, such as user name and password, that enable Discovery to connect to an application on a remote machine. ➤ **Edit using previous interface.** Choose this option if, in a previous version, you added parameters to this protocol that do not exist in this version. ➤ **Check credentials.** In the box that opens, enter the IP address of the remote machine on which the protocol must run. The Probe attempts to connect to this IP and returns an answer whether the connection succeeded or not.
<Right-click a title>	Choose from the following options: ➤ **Hide Column.** ➤ **Show All Columns.** Displayed when a column is hidden. ➤ **Customize.** Select to change the display order of the columns. ➤ **Auto-resize Column.** Select to change the column width to fit the contents.

A Specific Probe

When a specific Probe is selected in the Domains Browser pane, the Details tab includes the following elements (listed alphabetically):
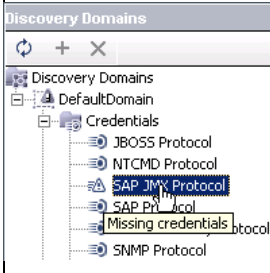
GUI Element	Description
Description	Enter a description to appear in this pane.
Last time Probe accessed	The last time that the probe was accessed on the server machine.
Probe IPs	The IP of the Probe machine.

GUI Element	Description
Ranges	Details on the range in which the Probe performs Discovery: ✚ ➤**Add IP range.** Click to open the Add IP Range dialog box. ✖ ➤**Remove IP range.** Click a range and click the button to remove a range from the list. ✐ ➤**Edit IP range.** Click to open the Edit IP Range dialog box. ➤ **Excluded.** Displays the IP addresses that have been excluded from the range that the Probe uses to discover CIs. ➤ **Range.** The network IP addresses that the Probe uses to discover CIs.
Status	➤ **Connected.** The Probe has successfully connected to the server (the Probe connects every few seconds). ➤ **Disconnected.** The Probe is not connected to the server.

Domain Configuration Window

Description	Enables you to define a new Discovery domain or to define a new Probe for an existing domain. Also, to define the connection data for each protocol. **To access: Admin** > **Universal CMDB** > **Discovery** > **Domain Configuration**.
Important Information	➤ For details on the Domains Browser pane, see "Domains Browser Pane" on page 166. ➤ For details on the Details pane, see "Details Pane" on page 161.
Included in Tasks	"Set Up the Credentials for the Probe" on page 57
Useful Links	"Domain Credential References" on page 99

Domains Browser Pane

Description	Enables you to view, define, or edit a domain, a Probe or a Probe's credentials.
	To access: Admin > **Universal CMDB** > **Discovery** > **Domain Configuration**.
Important Information	A missing credential is symbolized by the following icon:

The Domains Browser pane includes the following elements (listed alphabetically):

GUI Element	Description
+	Adds a domain or Probe, depending on what is selected.
✕	Deletes a domain or Probe, depending on what is selected.
↻	Updates all domain and Probe information.
⊞	Opens a domain to view credentials and Probes.

Edit Related Probes Dialog Box

Description	Enables you to select specific Probes.
	⌀ **To access:** Click the Related probes button in the Edit Policy dialog box.
Useful Links	"Define Job Execution Policies" on page 88

Edit Timetable Dialog Box

Description	Enables you to set the times when a Probe must run a job execution policy. *To access:* Click the **Edit** button in the Edit Policy dialog box.
Useful Links	"Add/Edit Policy Dialog Box" on page 158

The Edit Timetable dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Description	Add a description of the specific policy. This field is mandatory.
Time Definition	Click a cell for a day and time to be included in the policy. To add more than one time unit, drag the pointer over the cells. **Note:** To clear a time unit, click the cell a second time.

Protocol Parameters Dialog Box

Description	Displays the attributes that can be defined for a protocol. **To access: Domain Configuration** > **Discovery Domains** > **Probe** > **Credentials**, select a protocol and click the **Add** or **Edit** button.
Important Information	For the description of each protocol, see "Domain Credential References" on page 99.
Included in Tasks	"Set Up the Credentials for the Probe" on page 57

Scope Definition Dialog Box
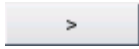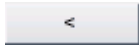
Description	Enables you to set the range that a protocol must discover.
	To access: Click the **Edit** button in the Protocol Parameters dialog box.

The Scope Definition dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Selected Probes	To select specific Probes whose IP range must be changed, click **Edit**. For details, see "Choose Probe Dialog Box" on page 126.
Selected Ranges	➤ **All.** The protocol runs Discovery on all ranges for the domain. ➤ **Selected Range.** For the procedure to select a specific range on which the protocol runs Discovery or to define an excluded range, see "Add/Edit IP Range Dialog Box" on page 156.

Selecting Probes

The Choose Probe to Filter, Edit Probe Limitations for TQL Output, and Edit Related Probes dialog boxes include the following elements (listed alphabetically):

GUI Element	Description
>	**Add Selected Probe.** Click to add a Probe to the Selected Probes column.
<	**Remove Selected Probe.** Click to remove a Probe from the Selected Probes column.
All Discovery Probes	➤ Select to add all Probes in the Non-selected probes list. ➤ Clear to add a specific Probe from the Non-selected probes list.

GUI Element	Description
Non-selected probes	Probes that are not included in the policy/filter/limitations.
Selected probes	Probes that are included in the policy/filter/limitations.

8

Resource Configuration User Interface

This chapter includes the pages and dialog boxes that are part of the Resource Configuration user interface.

Choose Configuration Item Type Dialog Box

Description	Enables you to select CITs to search for in the Discovery packages.
	To access: Click the button [...] in the Find Discovery Resources dialog box, when **Pattern input type** or **Pattern output type** is selected.

The Choose Configuration Item Type dialog box includes the following elements (listed alphabetically):

GUI Element	Description
<Configuration item types>	The CITs are organized in folders according to the CIT hierarchy.

Configuration File Pane

Description	Enables you to edit a specific configuration file that is part of a Discovery package. For example, you can edit the **portNumberToPortName.xml** file so that specific port numbers, names, or types are discovered.
	To access: Click a specific configuration file in the Discovery Resources pane.
Important Information	The following files are for internal use only and should not be changed:
	➤ discoveryPolicy.xml
	➤ interfaceType.xml
	➤ jythonGlobalLibs.xml
	For details, see "Resource Configuration Files" on page 91.
Included in Tasks	"Filter Discovery Results" on page 90

The Configuration File pane includes the following elements (listed alphabetically):

GUI Element	Description
🔍	Find specific text in the configuration file. For details, see "Find Text Dialog Box" on page 178.
📑	Click to go to a specific line in the configuration file. In the Go To Line dialog box, enter the line number.
📝	Click to open the file in an external editor.
XML (green)	For XML files, signifies that the code is valid.
XML (red)	For XML files, signifies that the code is not valid.

Discovery Pattern Source Editor

Description	Enables you to edit a pattern script.
	To access: Right-click a pattern in the Discovery Resources pane and select **Edit Pattern Source**.

The Discovery Pattern Source Editor window includes the following elements (listed alphabetically):

GUI Element	Description
🔍	Find specific text in the pattern script. For details, see "Find Text Dialog Box" on page 178.
📑	Click to go to a specific line in the pattern script. In the Go To Line dialog box, enter the line number.
📝	Click to open the pattern script in an external text editor.

GUI Element	Description
	Signifies that the code is valid.
	Signifies that the code is invalid.

Discovery Resources Pane

Description	Enables you to locate a specific package, pattern, script, configuration file, or external resource.
	To access: Admin > **Universal CMDB** > **Discovery** > **Resource Configuration**
Important Information	Depending which level you select in the Discovery Resources pane, different information is displayed in the View pane.
	If you select:
	➤ One of the following folders: Discovery Packages root, a specific package, a pattern, script, configuration file, or external resource: a list of the resources in that folder is displayed. To access a resource directly, double-click the resource in the View pane.
	➤ A specific pattern: The Pattern Signature and Pattern Management panes. For details, see "Pattern Signature Tab" on page 188 and "Pattern Management Tab" on page 183.
	➤ A script or configuration file: The script editor. For details, see "Script Pane" on page 193.
	➤ An external resource: Information about the file.
Useful Links	"Package Manager User Interface" in *IT World Model Management*.

The Discovery Resources pane includes the following elements (listed alphabetically):

GUI Element	Description
⟳	Click to refresh the list of packages.
🔍	Click to open the Find Discovery Resource dialog box. For details on filtering, see "Filter Discovery Results" on page 90.
🗎	Click to: ➤ **Create a Discovery pattern.** Enter the pattern name and click **OK**. The new pattern is added to the <<No Package>> folder. Edit the pattern. For details, see "Pattern Signature Tab" on page 188 and "Pattern Management Tab" on page 183. For details on moving a pattern to a package, see "Move Resource Dialog Box" in *IT World Model Management*. ➤ **Create a Jython script.** Enter the script name. For details, see "Script Pane" on page 193. ➤ **Create a configuration file.** Enter the configuration file name. By default, the file takes an .xml extension. To give the file another extension, for example, *.properties, name the file and include the extension. Add the appropriate XML code or other content. For XML files, you can save the file only if it is valid. For details, see "Configuration File Pane" on page 172. ➤ **Import an external resource.** In the browser that opens, locate the resource to be imported and click **Open**.
🗃	Discovery packages root. Displays a list of all resources included in all packages.
📦	Package root. Displays a list of all resources included in the package. You can view any of these resources by double-clicking the resource in the Discovery Resources pane.

GUI Element	Description
<Configuration files>	Right-click a file to: ➤ **Save as.** Save the file under a new name. Use this option to clone an existing file. The new file includes all attributes of the existing file. Make any necessary changes to the file and save it. ➤ **Delete.**

<External resource files>	➤ Right-click a file to:
	   ➤ **Save as.** Save the resource under a new name. Use this option to clone an existing resource. The new resource includes all attributes of the existing resource and is saved to the same location in the file system. Make any necessary changes to the new resource and save it.
	   ➤ **Delete.** Delete the file.
	➤ Select the file to display information in the View pane. You can open an external resource or export it.

<Pattern files>	Right-click a file to: ➤ **Save as.** Save the pattern under a new name. Use this option to clone an existing pattern. The new pattern includes all attributes of the existing pattern. Give a name to the new pattern, and change the necessary attributes. ➤ **Delete the pattern.** ➤ **Go to Discovery job.** When enabled, click to open the Job Configuration window. This option is enabled if the pattern is included in a job. For example, the ICMP_NET_DIS_IpC pattern is included in the Class C IPs by ICMP job. ➤ **Edit pattern source.** Opens the pattern source editor where you can make changes to the pattern. For details, see "Discovery Pattern Source Editor" on page 173.
<Script files>	Right-click a file to: ➤ **Save as.** Save the script under a new name. Use this option to clone an existing script. The new script includes all attributes of the existing script. Make any necessary changes to the script and save it. ➤ **Delete.**

Find Discovery Resource Dialog Box

Description	Enables you to build a search query to find a particular resource. **To access:** Click the **Find Job** filter button in the Discovery Resources pane.

The Find Discovery Resource dialog box includes the following elements (listed alphabetically):

GUI Element	Description
...	Click to open the Choose Configuration Item Type dialog box.
Direction	Searches forwards or backwards through the Discovery packages.
Find All	All resources meeting the search criteria are highlighted in the Discovery Resources pane.
Find Discovery resource by	Choose between: ➤ **Name.** Enter the name, or part of it, of the resources. ➤ **Pattern input type.** CIs that trigger the Discovery job. Click the button to open the Choose Configuration Item Type dialog box. Locate the CI type that you are searching for. ➤ **Pattern output type.** CIs that are discovered as a result of the activated Discovery job.
Find Next	The next resource meeting the search criteria is highlighted in the Discovery Resources pane.

Find Text Dialog Box

Description	Enables you to find text in a script or configuration file.
	To access: Click the **Find in text** button.

The Find in text dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Direction	Search up or down the script.
Options	Select **Case Sensitive** to narrow your search.
Text to find	Enter the text you are searching for.

Input TQL Editor Window

Description	Enables you to define which CIs can be trigger CIs for jobs that run a specific pattern.
	To access: Resource Configuration > select a pattern > **Pattern Signature** tab > click the **Edit** button next to the Input TQL box.

The Input TQL Editor window includes the following elements (listed alphabetically):

GUI Element	Description
<Panes>	➤ CI Types Pane ➤ Editing Pane ➤ Information Pane
TQL Name	The name of the trigger TQL query that activates the Discovery job.

CI Types Pane

Description	Displays a hierarchical tree structure of the CI Types found in the CMDB. For more details, see "CI Type Manager User Interface" in *CI Attribute Customization*.
	Note: The number of instances of each CIT in the CMDB is displayed to the right of each CIT.
	To create or modify a TQL query, click and drag nodes to the Editing pane and define the relationship between them. Your changes are saved to the CMDB. For details, see "Adding Nodes and Relationships to a TQL Query" in *Reference Information*.
Important Information	The CI Types pane is part of the following managers: View Manager, Enrichment Manager, Query Manager, Correlation Manager, Report Manager, and Trigger TQL Editor.
Included in Tasks	➤ "Create a Correlation Rule" on page 81
	➤ "Define an Enrichment Rule" on page 108
	➤ "Define a TQL Query" on page 101
	➤ "Pattern View Workflow" on page 79
	➤ "Define a Report Rule" on page 86

Editing Pane

Description	Enables you to edit the node selected in the Trigger TQLs pane.

The Editing pane includes the following elements (listed alphabetically):

GUI Element	Description
<node>	Click to display information about the node in the information pane.
<Right-click menu>	For details, see Chapter 17, "Topology Query Language Context Menu Options."
<Toolbar>	For details, see Chapter 7, "Toolbar Options."

Information Pane

Description	Displays the properties, conditions, and cardinality for the selected node and relationship.
Important Information	The Information pane is part of the following managers and user interfaces: View Manager, Correlation Manager, Report Manager, Enrichment Manager, and Trigger TQL Editor.
Included in Tasks	➤ "Create a Correlation Rule" on page 81 ➤ "Define an Enrichment Rule" on page 108 ➤ "Define a TQL Query" on page 101 ➤ "Pattern View Workflow" on page 79 ➤ "Define a Report Rule" on page 86

The Information pane includes the following elements (listed alphabetically):

GUI Element	Description
Cardinality	Cardinality defines how many nodes you expect to have at the other end of a relationship. For example, in a relationship between host and IP, if the cardinality is 1:3, the TQL retrieves only those hosts that are connected to between one and three IPs. For details, see "Cardinality Tab" in *Reference Information*.
Condition	The attribute conditions defined for the node or the relationship. For details, see "Attribute Tab" in *Reference Information*.
Folding Rule	Displays the folding rule defined for the selected relationship. For details about folding rules, see "Adding Folding Rules to Relationships" in *IT World Model Management*. **Note:** This pane appears only when a relationship is selected in View Manager.

GUI Element	Description
Properties	➤ To open the Node/Relationship Condition dialog box, select a node or relationship in the Editing pane and click the **Edit Condition** button. For details, see "Node/Relationship Condition Dialog Box" in *Reference Information*. ➤ **CI Type.** The CIT of the selected node/relationship. ➤ **Visible.** A tick signifies that the selected node/relationship is visible in the topology map. When the node/relationship is not visible, a box appears to the right of the selected node/relationship in the Editing pane: ➤ **Include subtypes.** Display both the selected CI and its descendents in the topology map.

Pattern Management Tab

Description	Enables you to define a Discovery pattern by specifying which CITs the pattern should discover and the protocols needed to perform Discovery. **To access:** Select a specific pattern in the Discovery Resources pane.
Important Information	The following files are for internal use only and should not be changed: ➤ discoveryPolicy.xml ➤ interfaceType.xml ➤ jythonGlobalLibs.xml
Useful Links	"The DiscoveryProbe.properties File" on page 97.

The Pattern Management pane includes the following elements (listed alphabetically):

GUI Element	Description

Execution Options	➤ **Enable Recording.** Records pattern execution to a file.
	➤ **Extended debug information.** Enables adding more debug points.
	➤ **Maximum Threads.** Each Discovery job is run using multiple threads. You can define a maximum number of threads that can be used concurrently when running a job. If you leave this box empty, the Probe's default threading value is used (8).
	The default value is defined in DiscoveryProbe.properties in the defaultMaxJobThreads parameter.
	   ➤ **regularPoolThreads.** The maximum number of worker threads allocated to the multi-threaded activity (the default is 50).
	   ➤ **priorityPoolThreads.** The maximum number of priority worker threads (the default is 20).
	Note: The number of actual threads should never be higher than regularPoolThreads + priorityPoolThreads.
	➤ **Max. Execution Time.** The maximum time allowed for a pattern to run on one Trigger CI.

Probe Selection	By default, Discovery automatically chooses the Discovery Probe for the trigger CI according to the CI's related host. After obtaining the CI's related host, HP Business Availability Center chooses one of the host's IPs and chooses the Discovery Probe according to the Probe's network scope definitions. This may fail in the following situations: ➤ A trigger CI does not have a related host (such as the **network** CIT). ➤ A triggered CI's host has multiple IPs, each belonging to a different Discovery Probe. To resolve these issues, you can specify which Discovery Probe to use with the Discovery pattern by: ➤ In the Probe Selection section, selecting **Override default probe selection**. ➤ In the Probe box, typing the Discovery Probe to use for the Discovery task.

GUI Element	Description

Relevant CITs	**Automatically delete removed CIs.** Select this check box to automatically delete CIs that should be removed.
	
	To add CITs to the list, click the **Add** button. In the Choose Configuration Item Type dialog box, choose the CITs.
	
	The changes you make here are added to the pattern file, for example:
	
	`<resultMechanism isEnabled="true">`
	`    <autoDeleteCITs isEnabled="true">`
	`        <CIT>networkshare</CIT>`
	`    </autoDeleteCITs>`
	`</resultMechanism>`
	
	For details on handling CI deletion, see "Handling Deleted CIs" on page 53.

Result Grouping	To group Discovery results in the Discovery Probe before they are sent to the 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 server. ➤ In the **Max. CIs in Group** box, specify the number of CIs that should accumulate in the Discovery Probe before being transferred to the server. If you enter a value in both fields, Discovery applies whichever occurs first.

GUI Element	Description

Results Management	➤ **Enable aging.** Select this check box to run the aging mechanism that specifies how long a period must pass in which CIs are discovered, before Discovery treats these CIs as no longer relevant and removes them.
	
	Aging parameters are defined in the Infrastructure Settings Manager (**Admin > Universal CMDB > Settings > Infrastructure Settings Manager**):
	
	  ➤ **Aging Scheduler Hour of the First Run.** Defines at what time aging will first run after server startup (for example, 02=2 AM).
	
	  ➤ **Aging Scheduler Interval.** Defines the interval between runs. If Aging Time Unit = days, the interval value is days; if Aging Time Unit = hours, the interval value is hours.
	
	  ➤ **Aging Time Unit.** The default is days. The hours option is provided to enable convenient verification checks of specific CIs.
	
	➤ **Filter unchanged results.** Select this check box for the Discovery Probe to send to the CMDB only those CIs that are unchanged since the last time Discovery results were sent to the server and that answer to the filter criteria. For details on filtering, see "Filter Discovery Results" on page 90.

GUI Element	Description

Triggered CI Data	✚ Add trigger CI data to the pattern.
	
	✖ Remove trigger CI data from the pattern.
	
	✎ Edit the trigger CI data in the Parameter Editor dialog box.
	
	➤ **Name.** The information that is needed to perform a Discovery task on a specific CI. This information is passed to the CI queried in the Discovery task.
	
	➤ **Value.** The attribute value. Variables are written using the following syntax:
	
	${VARIABLE_NAME.attributeName}
	
	where **VARIABLE_NAME** can be one of three predefined variables:
	
	  ➤ **SOURCE**. The CI that functions as the task's trigger.
	  ➤ **HOST**. The host in which the triggered CI is contained.
	  ➤ **PARAMETERS**. The parameter defined in the **Parameter** section.
	
	You can create a variable. For example, ${SOURCE.network_netaddr} indicates that the trigger CI is a network.

Used Scripts	A list of Jython scripts used by the Discovery pattern. The Jython scripts that appear in bold are the scripts that the currently selected pattern is using. 🔺🔻 Change the order of the scripts. Discovery runs the scripts in the order in which they appear here. ✚ Add a script to the pattern. ✖ Remove a script from the pattern. ✎ Edit the selected script in the Script Editor that opens.

Pattern Signature Tab

Description	Enables you to define a Discovery pattern by specifying which CITs the pattern should discover and the protocols needed to perform Discovery. **To access:** Select a specific pattern in the Discovery Resources pane.
Important Information	The following files are for internal use only and should not be changed: ➤ discoveryPolicy.xml ➤ interfaceType.xml ➤ jythonGlobalLibs.xml

The Pattern Signature pane includes the following elements (listed alphabetically):

GUI Element	Description
Description	The description of the Discovery pattern.
Discovered CITs	A list of CITs that the pattern should discover. ✚ Add a CIT. Click to open the Choose Configuration Item Type dialog box. Select the CIT that is to be included in the Discovery. ✖ Remove a CIT.
Discovery Pattern Parameters	Each row represents the definitions for one parameter. ✚ Add a parameter. Click to open the Parameter Editor. Enter details on the parameter. The value you enter here is assigned to the attribute. ✖ Remove a parameter. ✎ Edit a parameter. Click to open the Parameter Editor and make changes.

GUI Element	Description
Input TQL	Defines which CIs can be trigger CIs for jobs that run this pattern. This field is optional. Click the button to open the Input TQL Editor window. For details, see "Input TQL Editor Window" on page 178. For an explanation, see "Input TQLs, Trigger TQLs, and Trigger CIs" on page 49.
Required Discovery Protocols	List of protocols required by the pattern for the Discovery task. For example, the NTCmd protocol, together with its user name, password, and other parameters, is needed for Discovery to access a Windows system. ✛ Add a protocol. ✖ Remove an existing protocol.
Trigger CIT	The CIT used as the trigger that activates the selected Discovery pattern. Click the button to open the Choose Configuration Item Type dialog box and to choose a CIT to use as the trigger. (Use the SHIFT and CONTROL keys to select more than one CIT.)

Resource Configuration Window

Description	Enables you to view or edit default parameter values used for the Discovery process.
	To access: Administration > **Discovery** > **Resource Configuration** or right-click a job in the Job Configuration window.
Important Information	➤ An asterisk (*****) next to a resource (pattern, script, or configuration file) signifies that the resource has changed since the package (in which it is included) was deployed. If the original package is redeployed, the changes are deleted from the resource. To save the changes, move the resource to a new package and deploy the package (the asterisk disappears).
	➤ Only administrators with an expert knowledge of the Discovery process should delete Discovery packages.
Useful Links	"Pattern Signature Tab" on page 188
	"Pattern Management Tab" on page 183
	"Script Pane" on page 193
	"Configuration File Pane" on page 172

Important: The following examples include steps that modify resource files. Modification is considered a more advanced configuration and should be performed by users with an advanced knowledge of Business Availability Center only, for site-specific customization.

Example – Set Up Discovery of Microsoft Domains

On a network, you want to discover specific Microsoft domains:

1 In Resource Configuration, search for the msDomainNames.xml file by clicking the **Find resource** button and entering **domain** in the Name field:
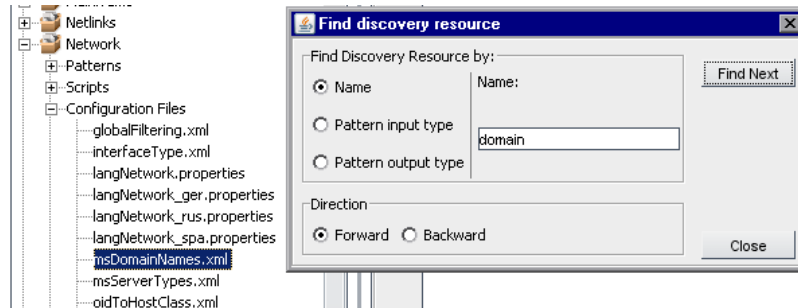
Discovery highlights the resource that includes this string.

2 Click **Find Next** until Discovery highlights msDomainNames.xml in the Network package. Click **Close**.

Discovery displays the file in the View pane with the results of the XML validation.

3 Locate the **<MsDomainNames all="true">** marker and change **true** to **false**.

false: Discovery finds only those Microsoft domain types specified in the <MsDomain> list.

true: Discovery finds all existing Microsoft domain types and not only the types listed in <MsDomain>.

4 Locate the **<MsDomain>** marker and replace DISCOVERED-MS-DOMAIN with the name of the Microsoft domain.

(To add more domains to be discovered, add a <MsDomain>Domain to be discovered<MsDomain> marker for each domain.)

Example:

```
<MsDomainNames all="false">
    <MsDomain>Business Availability Center Lab</MsDomain>
    <MsDomain>Finance_servers</MsDomain>
</MsDomainNames>
```

191

5 Save the file. Verify that the file is valid XML by checking the Validation info.

Example – Set Up Discovery of Novell Servers

On a network, you want to discover the host attributes of a Novell server:

1 In Resource Configuration, search for the msServerTypes.xml file by clicking the **Find resource** button and entering **msser** in the Name field:

2 Click **Find Next** until Discovery highlights msServerTypes.xml in the Network package. Click **Close**.

Discovery displays the file in the View pane with the results of the XML validation.

3 Locate the **<MsServerType value="80" name="NOVELL" calc="false"/>** marker and change **false** to **true**.

false: Discovery does not save data about this server to the database.

true: Discovery saves the CIs to the CMDB (as attributes of their host).

(**value** is the discovered number of the server type. **name** is the converted name of the discovered server type. The server type appears under this name in the CMDB and in Business Availability Center.)

Example – Configure Resources for a New Package

You need to define a package for a pattern and configuration file that you have written for a non-default Discovery:

1 To create a pattern, you can either define a new pattern or copy an existing pattern.

To define a new pattern, in Resource Configuration, click the icon in the Discovery Resources toolbar and select **New Discovery Pattern**. For details, see "Discovery Resources Pane" on page 174.

To copy an existing pattern, select the pattern, and save the file under a new name. The new pattern is located under the << No Packages >> folder.

2 Define the configuration file in the same way, either by defining a new file or by copying an existing file.

3 In Package Manager, define a new package and add the new resources to the package. For details, see "Package Manager User Interface" in *IT World Model Management.*

Script Pane

Description	Enables you to edit a specific script that is part of a Discovery package.
	To access: Click a specific script in the Discovery Resources pane.

The Script pane includes the following elements (listed alphabetically):

GUI Element	Description
🔍	Find specific text in the script. For details, see "Find Text Dialog Box" on page 178.
📄	Click to go to a specific line in a script. In the Go To Line dialog box, enter the line number.
📝	Click to open the script in an external text editor.
<script>	The Jython script used by the package.

9

Status Snapshot User Interface

This chapter includes the pages and dialog boxes that are part of the Status Snapshot user interface.

This chapter describes:	On page:
[Job Name] Dialog Box	195
Status Snapshot Window	196

[Job Name] Dialog Box

Description	Enables you to view details about the scheduling of a particular job as well as job statistics.
	To access: Double-click a job in the Progress pane of the Status Snapshot window.

The [Job Name] dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Average duration	The average duration, in seconds, of the time it took the Probe to run this job.
Last duration	The length of time, in seconds, taken to run the job in the previous invocation.
Last updated	The last time that the job was updated.
Next invocation	The next time that Discovery is scheduled to run the job.

GUI Element	Description
Previous invocation	The last time that Discovery ran the job.
Progress	The number of Trigger CIs in the job and the number of Trigger CIs that the Probe has finished working on.
Recurrence	The number of times a job is run in a week. For example, if a job is scheduled to run daily, it runs 7 times in a week. If a job is scheduled to run weekly, Recurrence = 1.
Schedule	The schedule defined in the Discovery Scheduler dialog box.
Statistics	For details, see "Statistics Pane" on page 198.
Status	Can be **Scheduled** (the job runs according to a defined schedule) or **Running** (the job is running now).
Threads	The number of threads currently allocated to this job.

Status Snapshot Window

Description	Enables you to view the current status of discovered CIs and all active jobs running on the Discovery Probes.
	To access: Admin > Universal CMDB > Discovery > Status Snapshot
Important Information	Depending on what you select in the Domains Browser pane, different information is displayed in the View pane.
	If you select:
	➤ a domain, you can view details and CIT statistics for the domain. For details, see "Details Pane" on page 161 and "Statistics Pane" on page 198.
	➤ a Probe, you can view details on the Probe (such as the Probe IP), the progress of a job and you can view CIT statistics. For details, see "Details Pane" on page 197, "Progress Pane" on page 197, "Statistics Pane" on page 198, and "View Pane" on page 200.
Useful Links	Status Snapshot Overview

Details Pane

The Details pane includes the following elements (listed alphabetically):

GUI Element	Description
Domain Type	**Customer.** A private domain used for your site. You can define several domains and each domain can include multiple Probes. Each Probe can include IP ranges but the customer domain itself has no range definition. **External.** Internet/public domain. A domain which is defined with a range. The external domain may contain only one Probe whose name equals the domain name. However, you can define several external domains in your system. For details on defining domains, see "Add New Domain Dialog Box" on page 159.

Progress Pane

The Progress pane includes the following elements (listed alphabetically):

GUI Element	Description
CIs	The number of CIs discovered by the job.
Job	The name of the job and an icon showing whether the job is active. Double click a job to open a dialog box displaying job details. For details, see "[Job Name] Dialog Box" on page 195.
Next invocation	The next time that the Discovery Probe is scheduled to run.
Previous invocation	The last time that the Discovery Probe ran.
Progress	Can be either Scheduled or Running.

Statistics Pane

The Statistics pane includes the following elements (listed alphabetically):

GUI Element	Description
	Click to retrieve the latest data from the Probe (Discovery data is not automatically updated).
	Set the time range for which to display statistics about the CITs. ➤ **All.** Displays statistics for all Discovery job runs. ➤ **Last Hour/Day/Week/Month.** Choose a period of time for which to display statistics about the CITs. ➤ **Custom Range.** Click to open the Customize Statistics Time Range dialog box. Enter the date or click the arrow to choose a date and time from the calendar, for the **To** and **From** dates. To delete a date, click **Reset**.
	Select a CI and click this icon to view CI instances and their attributes. Opens the CIs Discovered by [Module or Job Name] Dialog Box. In the following conditions, a message is displayed: ➤ All the CIs that were discovered by this job were already discovered by another job. ➤ All the CIs that this job discovered have been deleted. ➤ The CI instances were discovered in a previous version. (In version 7.0, you cannot view instances of CIs discovered in a previous version.)
	Click a column title to sort by that column. The arrow indicates whether the result is displayed in ascending or descending order.
<double-click a row>	For details, see "CIs Discovered by [Module or Job Name] Dialog Box" on page 126. **Note:** Not available for all CITs.

GUI Element	Description
<right-click a title>	Choose from the following options: ➤ **Hide Column.** Select to hide a specific column. ➤ **Show All Columns.** Displayed when a column is hidden. ➤ **Customize.** Select to display or hide columns and to change the order of the columns in the table. Opens the Columns dialog box. ➤ **Auto-resize Column.** Select to change a column width to fit the contents. For details, see "Columns Dialog Box" in *Reference Information*.
CIT	The name of the discovered CIT.
Created	The number of CIT instances created by the Probe.
Deleted	The number of CIT instances deleted by the Probe.
Discovered CIs	The number of CIs that have been discovered by the Discovery Probe for each CI type.
Filter	The time range set with the Set Time Range button.
Last updated	The date and time that the statistics table has been updated for a particular Probe.
Total	The total number of CIs in each column.
Updated	The number of CIT instances that have been updated.

View Pane

The View pane includes the following elements (listed alphabetically):

GUI Element	Description
	Click to view the current status of the discovered CIs and jobs on the selected Probe.
Last updated	The date and time at which the Get snapshot button was last pressed (that is, the date and time of the data displayed in Status Snapshot).
Probe IPs	The IP addresses defined for the Probe.
Running jobs	The number of jobs running on the Probe.
Scheduled jobs	The number of jobs that are scheduled to run according to the settings in the Discovery Scheduler. For details, see "Discovery Scheduler Dialog Box" on page 142.
Status	The status of the Probe (either disconnected or connected).
Threads	The sum of all threads currently allocated to the running Discovery jobs.

10

Discovery Job Statistics Report

The Discovery Job Statistics report enables you to view statistics for the ten most active Discovery jobs (that is, those with the most created, removed, or updated operations). Click a job to drill down to view statistics for a job's CIT.

For details on working with the report, see "Choosing the Time Range and Granularity" and "Sharing and Storing Reports" in *Reference Information*.

11
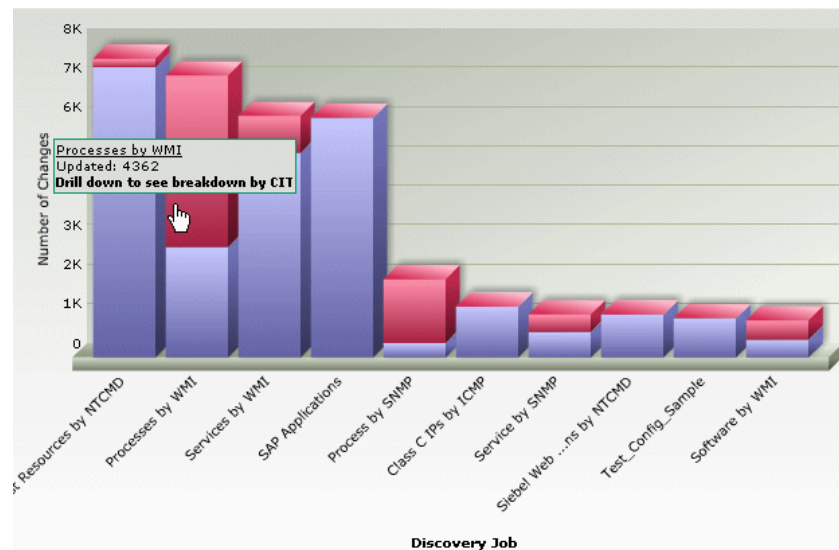
Discovery Job Errors Report

The Discovery Job Errors report enables you to view the ten Discovery jobs that have the highest number of errors.

For details on working with the report, see "Choosing the Time Range and Granularity" and "Sharing and Storing Reports" in *Reference Information*.

Index

Index