



HP Universal CMDB

Software Version: 10.22

DDMI to Universal Discovery Migration Walkthrough Guide

Document Release Date: December 2015
Software Release Date: December 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

Support

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

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

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

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

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

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

Contents

Chapter 1: DDMI to Universal Discovery Migration Overview	6
Migration Considerations	6
Architectural Changes	7
Chapter 2: Before Migration	11
DDMI to Universal Discovery Migration Options Overview	11
Check the DDMI Environment	15
Configure DDMI	16
Choose an Inventory Discovery Mode	19
Inventory Discovery Mode Concepts	19
Inventory Discovery Mode Types	20
Agent-Only Mode	21
Agentless Mode	22
Combined Mode	24
Agent-Driven Mode	26
SNMP-Agent Mode	28
SNMP-Combined Mode	30
SNMP-Agentless Mode	32
No-SNMP Agent Mode	34
Chapter 3: Migration Procedure	36
How to Migrate DDMI Server Configuration Data to Universal Discovery	36
How to Configure Universal Discovery	40
Change of the Migrated Configuration	41
Configure Data Flow Probe	42
Configure Inventory Discovery	44
Modify the UCMDB Environment	44
Configure Agent-Only Mode	47
Configure Agentless Mode	49
Configure Combined Mode	51
Configure Agent-Driven Mode	54
Configure SNMP-Agent Mode	56
Configure SNMP-Agentless Mode	59
Configure SNMP-Combined Mode	62

Configure No-SNMP Mode	65
Step-by-Step Configuration for Experienced Users	68
How to Migrate DDMI Agents to Universal Discovery Agents	71
Check the Migration Status	72
How to Configure DDMI and Universal Discovery for Interoperability	72
Chapter 4: After Migration	75
How to Run the Device Inventory Report	75
How to Import DDMI SAs to UCMDB	76
Chapter 5: Reference Information	80
How to Clean Up Legacy DDMI Agent Start-Up Scripts	80
Server Configuration Data Export Script Resources	82
Universal Discovery Resources for UNIX	83
Universal Discovery Resources for Windows	87
Server Configuration Data Import Troubleshooting	89
Terminology Changes from DDMI to Universal Discovery	90
Migrated Reports from DDMI to Universal Discovery	96
Mapping Attributes from DDMI to UCMDB	97
Java Viewer Mapping from DDMI to Universal Discovery	106
Chapter 6: Inventory Discovery Troubleshooting	108
How to view all information related to a device in a centralized view?	109
How to troubleshoot network availability and latency issue related to a device?	111
IP Ping and Agent Ping	111
SNMP Ping	114
Tracert and DNS Query	116
How to check the key indexes of the discovery history information for a discovered device?	117
How to check device related logs for a discovered device?	123
Agent deployment log	123
Scanner deployment log	124
Virtualization log	125
How to invoke discovery job relevant to the discovered device manually and check status to identify potential discovery errors?	126
Install UD Agent	126
Update UD Agent	129
Upgrade Scanner / Run Scanner / Download Scan File / Parse Enriched Scan File / Run Agentless Scanner	130

Uninstall Agent 132

Rerun Discovery 134

VMware Discovery Jobs 134

How to check which pattern (management zone) is used in the discovery for a discovered device? 136

How to check detailed discovery settings used in the discovery for a discovered device? ...138

How to check the SNMP credentials used in the discovery for a discovered device?142

Send Documentation Feedback144

Chapter 1: DDMI to Universal Discovery Migration

Overview

This guide describes how to migrate from DDMI versions 7.6x- 9.32 to Universal Discovery. In addition, it provides upgrade information for DDMA users.

This guide covers the following:

- Migrating DDMI server configuration data to Universal Discovery
- Migrating DDMI agents to Universal Discovery agents
- Configuring Universal Discovery agents to work with both DDMI and Universal Discovery

After you perform the migration, review the other documents in this guide to help you to make the transition to Universal Discovery.

Migration Considerations

Consider the following when selecting migration options:

- Migration Preferences
 - **Partial or phased.** You can continue using DDMI for inventory discovery while simultaneously utilizing discovery features of Universal Discovery. In this way, you can implement a parallel environment while gradually making the transition to Universal Discovery.
 - **Complete cutover.** You can migrate all configurations to Universal Discovery and then retire DDMI services.
- Upgrading DDMA (DDMA users only)
 - If DDMA is also running in your environment, upgrade to Universal Discovery as follows:
 - Locate the UCMDB installation media and perform the following:
 - Install UCMDB on the server where you want to run the UCMDB server. On the **Installation Type** page of the setup wizard, select **Upgrade from <VersionNumber>**.

where **<VersionNumber>** is the version of DDMA that is currently installed.

- Install the Data Flow Probe on the server where you want to run the Data Flow Probe server.

For complete details on installing UCMDB, see the interactive *HP Universal CMDB Deployment Guide*.

- Interoperating DDMI and Universal Discovery
 - In a partial or phased migration approach, the Universal Discovery agent can be utilized by both the DDMI server and the UCMDB Data Flow Probe for discovery and inventory. This functionality lets you upgrade from DDMI to Universal Discovery in a gradual way—running DDMI until the full migration from DDMI to Universal Discovery is completed.

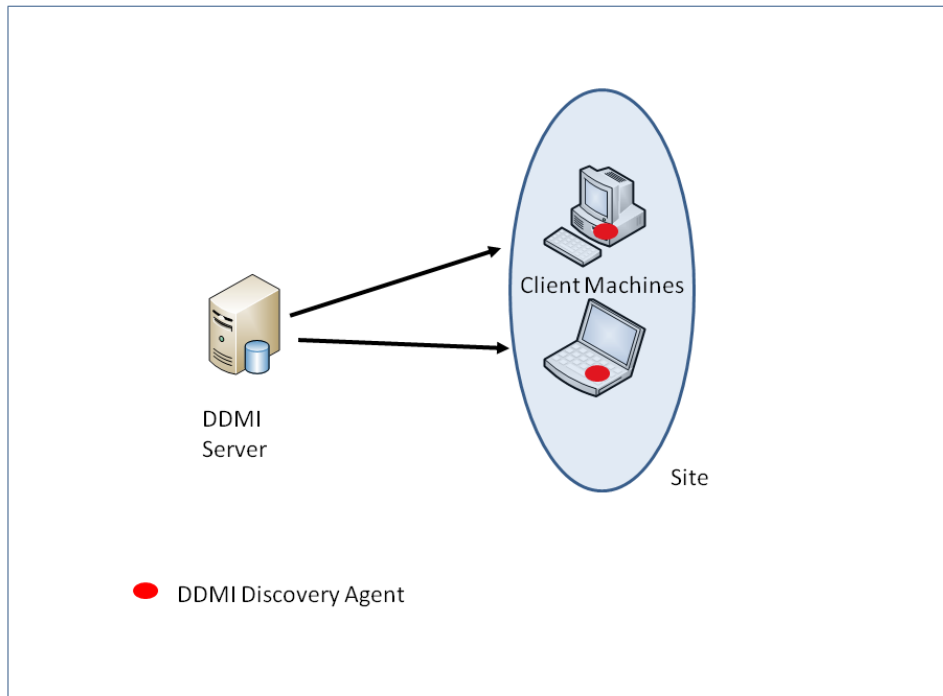
Architectural Changes

From a physical perspective, the DDMI and Universal Discovery architectures look similar. Most of the differences are from a logical perspective.

DDMI Deployment Scenarios

- DDMI Deployment Scenario 1

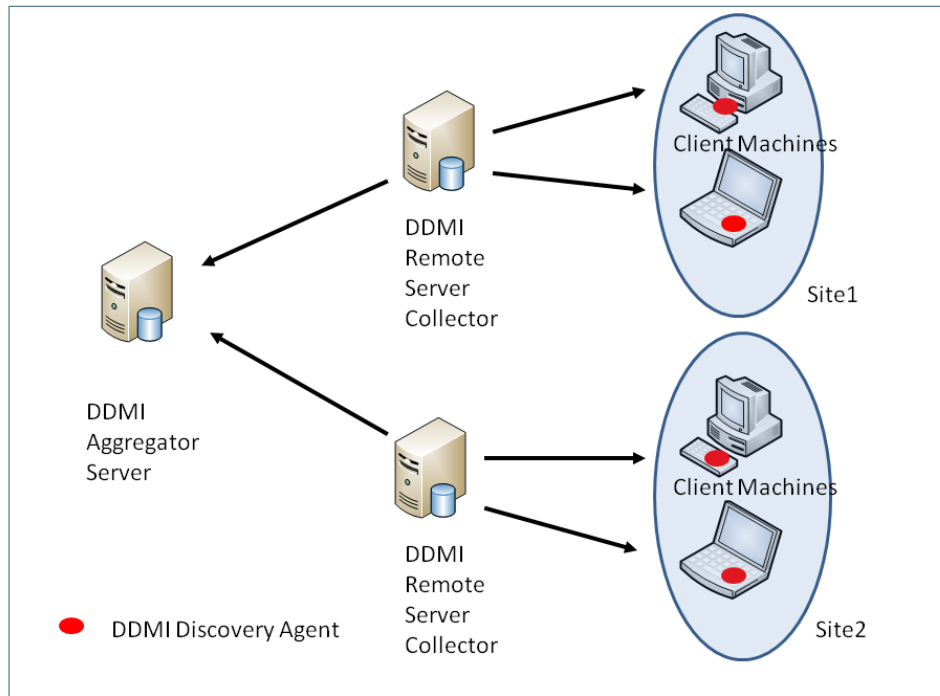
A DDMI server acts as both an aggregator and a collector for a site or region.



Comparing this deployment scenario to the Universal Discovery deployment scenario below, the DDMI server role is split into two distinct roles—UCMDB Server and Data Flow Probe.

- **DDMI Deployment Scenario 2**

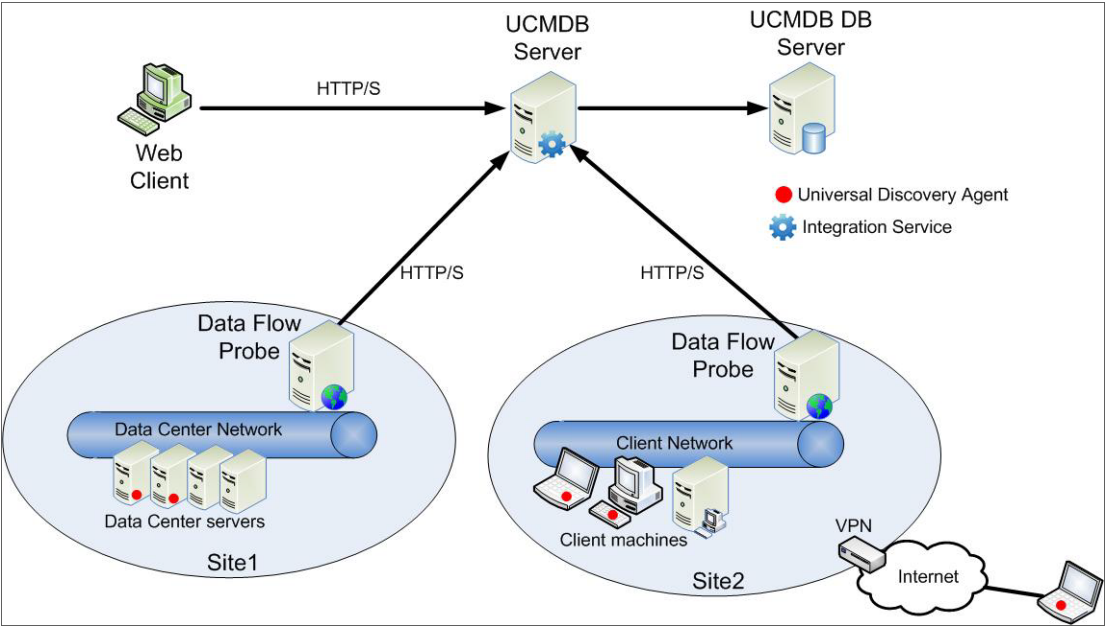
Multiple DDMI servers act in a collector server role (also called “remote” servers) for each of their respective sites or regions and then write results to local, built-in MySQL databases. Aggregator servers pull data from collector servers and then write the results to local, built-in MySQL databases and aggregate the data. Results are displayed in the Aggregator Health Panel. Each DDMI Remote Server Collector can independently display results for its respective sites.



Comparing this deployment scenario to the Universal Discovery deployment scenario below, the physical architecture looks similar. One prominent difference is the functionality of the DDMI Remote Server Collector and the UCMDB Data Flow Probe. The DDMI Remote Server Collector acts independently—able to report data for its respective site or region. The UCMDB Data Flow Probe has no reporting capabilities and serves only to execute jobs and maintain communication with UD Agents on remote discovery nodes.

Universal Discovery Deployment Scenario

The Data Flow Probe acts as the collector server for each of its respective sites. The Data Flow Probe converts collected data to Configuration Items (CIs) and reports the data to UCMDB which acts as an Aggregator Server. UCMDB uses an Oracle or SQL Server database system. The data is displayed using reports or modeling tools.



Chapter 2: Before Migration

This chapter includes:

DDMI to Universal Discovery Migration Options Overview	11
Check the DDMI Environment	15
Configure DDMI	16
Choose an Inventory Discovery Mode	19

DDMI to Universal Discovery Migration Options Overview

Tip: Read this entire section to ensure that you choose the migration options that are appropriate for your environment and migration preferences.

The migration options that you select depend on your migration preferences, and whether DDMA is also installed in your environment.

The following table lists all of the options that are available when migrating to Universal Discovery:

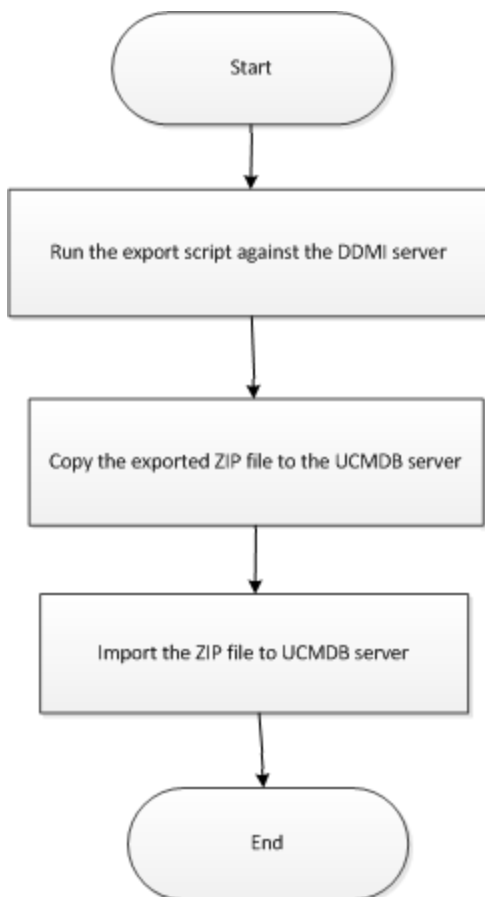
Option	Description
Migrate DDMI Server Configuration Data	Export DDMI server configurations, such as User SAs, certificates, and IP ranges to Universal Discovery
Migrate DDMI Agents	Migrate DDMI agents to Universal Discovery agents.
Configure Agents for Interoperability	(Optional) After DDMI agents are migrated to Universal Discovery agents, configure the DDMI server and Universal Discovery to interoperate in a partial/phased migration strategy.

The following matrix suggests the best options for your migration preferences. It also takes into account whether DDMA is installed.

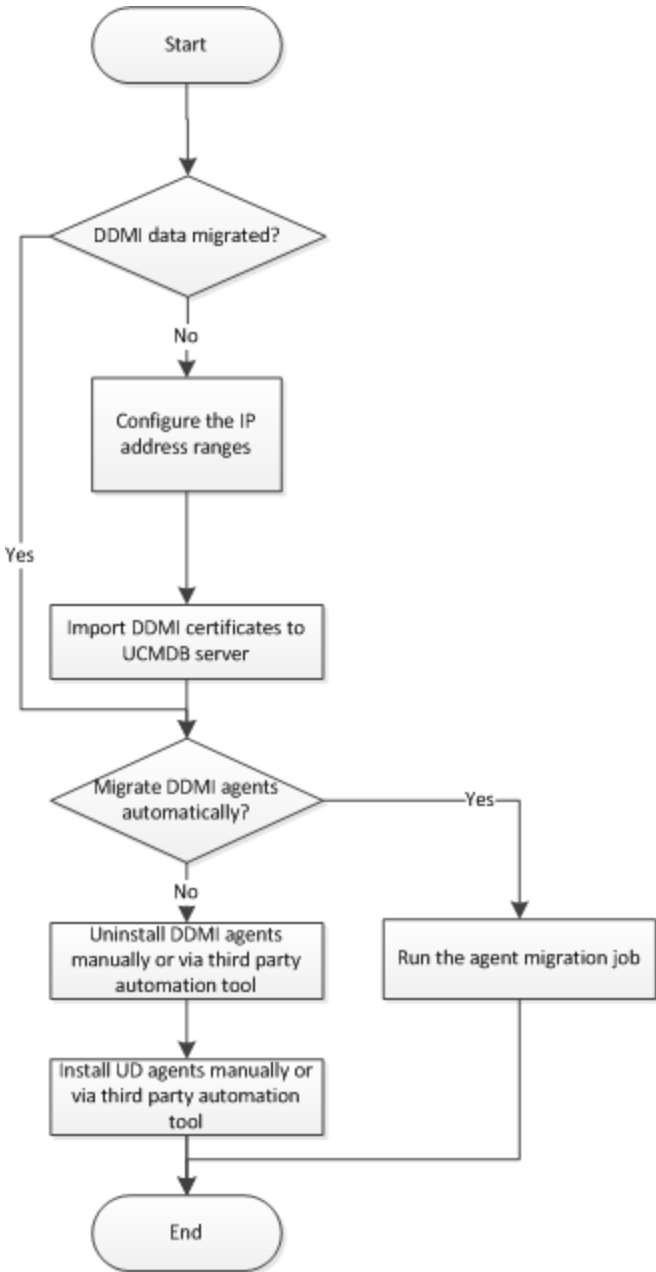
Retire DDMI?	DDMI and DDMA Installed	Only DDMI Installed
Yes, I want a complete cutover to Universal Discovery.	Migrate Agents	<ul style="list-style-type: none"> • Migrate DDMI Server Configuration Data • Migrate Agents
No, I want a partial/phased migration; migrate DDMI agents to Universal Discovery agents and run both systems in parallel.	<ul style="list-style-type: none"> • Migrate Agents • Agent Interoperability 	<ul style="list-style-type: none"> • Migrate DDMI Server Configuration Data • Migrate Agents • Agent Interoperability

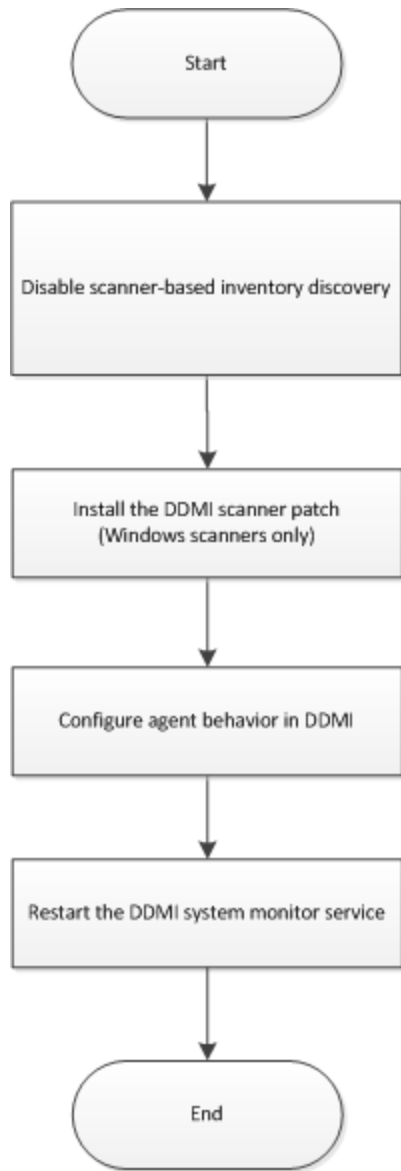
The following diagrams show each process step which corresponds to a step in the documentation.

Migrate DDMI Server Configuration Data



Migrate Agents



Agent Interoperability

The following table provides links to documentation for each option.

Option Name	Documentation Link
Migrate DDMI Server Configuration Data	"How to Migrate DDMI Server Configuration Data to Universal Discovery" on page 36
Migrate DDMI Agents	"How to Migrate DDMI Agents to Universal Discovery Agents" on page 71
Configure Agents for Interoperability	"How to Configure DDMI and Universal Discovery for Interoperability" on page 72

Check the DDMI Environment

Before Migrating DDMI to Universal Discovery (UD), check the following information with your DDMI administrator:

DDMI server

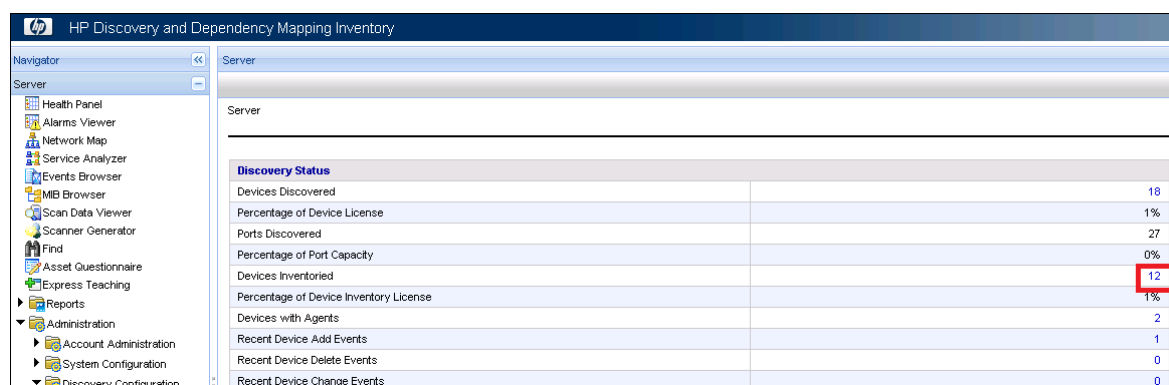
Each DDMI server will be mapped to a UD probe. However, the DDMI aggregator is not required to be migrated if it is not used to discover any devices.

To smoothly migrate, it is recommended to use a duplicate device of the DDMI server to install the UD probe. The duplicate device means the device with the same security configuration and the same position in the network as the DDMI server.

The DDMI server can be removed after the whole migration.

The number of devices that you have on each probe

Devices Inventoried that is shown below means devices that are discovered and managed by UD.



Discovery Status	
Devices Discovered	18
Percentage of Device License	1%
Ports Discovered	27
Percentage of Port Capacity	0%
Devices Inventoried	12
Percentage of Device Inventory License	1%
Devices with Agents	2
Recent Device Add Events	1
Recent Device Delete Events	0
Recent Device Change Events	0

In DDMI, the maximum number of **Devices Inventoried** that is allowed is 50,000. However, each UD probe cannot handle this number.

If this number is larger than 10,000, contact HP Software Support for further suggestion. It is recommended to split the DDMI server on several UD probes.

The number of device groups that you have on each probe

Each device group will be mapped to a management zone. DDMI can handle thousands of device groups; however, the maximum number of device groups that UD management zone can handle is 20.

Caution: Creating too many management zones may cause performance issues.

It is recommended to reconfigure the management zone. For details on how to configure the management zone, see the relevant section in ["Configure Inventory Discovery" on page 44](#).

Note: Do not create a device group with the passive discovery profile including 0.0.0.0 - 255.255.255.255. Although this is a valid configuration in DDMI, it can cause serious issues for UD.

DDMI credential

The UD agent requires absolute root privilege (or sudo) during installation.

Configure DDMI

The DDMI configuration here is the preparation for DDMI and UD Interoperability.

To configure DDMI, do the following:

1. Forbid the agent or scanner upgrade.
 - Go to **DDMI > Server > Administration > Discovery Configuration > Configuration Profiles > Agent Configuration Profiles > Settings** tab.

Ensure that **Allow agent communication** is selected. In the **Agent deployment actions** drop-down list box, select **No action**.

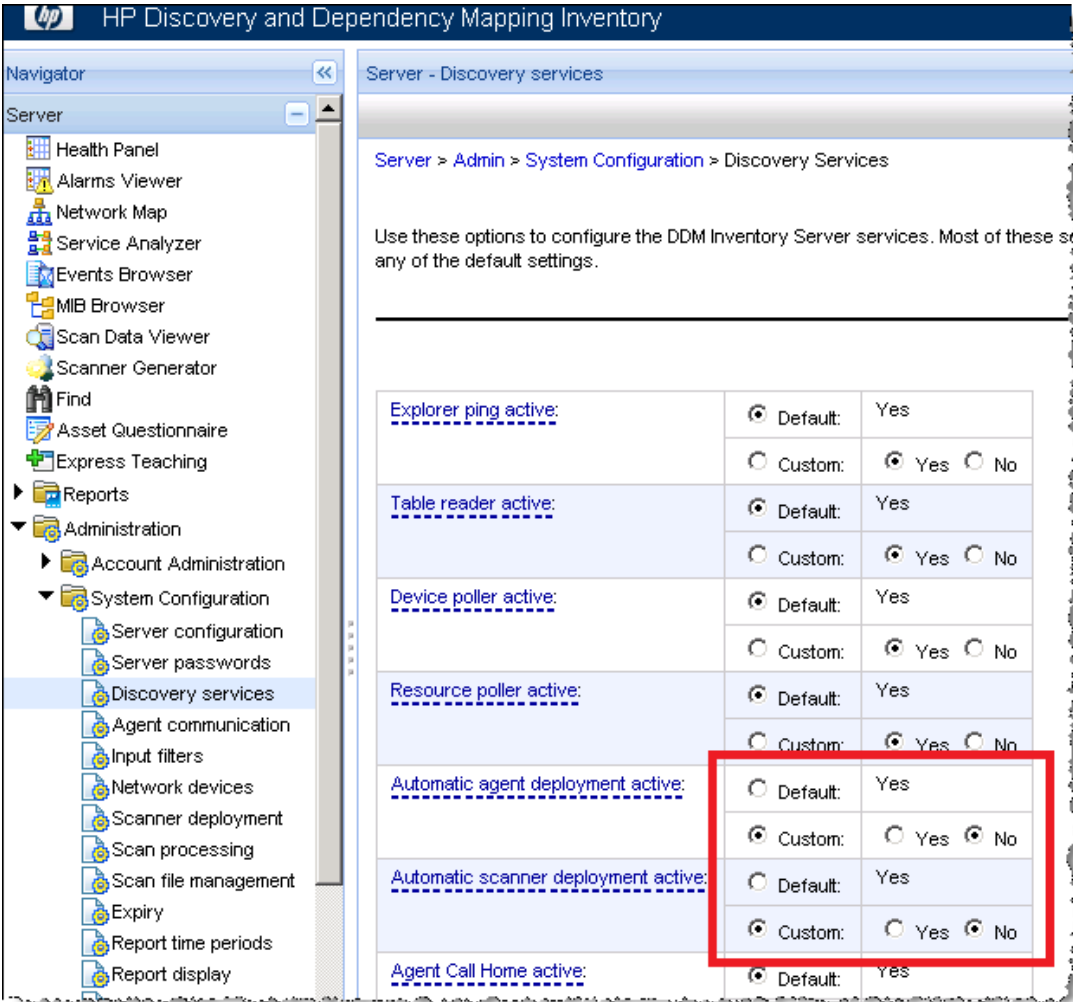
The screenshot shows the HP Discovery and Dependency Mapping Inventory (DDMI) interface. The left sidebar contains a Navigator pane with a tree view. The 'Server' node is expanded, and the 'Discovery Configuration' folder is selected, showing 'Configuration Profiles'. The main pane displays 'Server - Configuration Profile Details - Agent'. The breadcrumb trail is 'Server > Admin > Discovery Configuration > Configuration Profiles'. Below the breadcrumb are 'Save and Close' and 'Cancel' buttons. The 'Name' field is 'cls agent' and the 'Description' field is empty. There are two tabs: 'Settings' (selected) and 'Associated Groups'. Under the 'Settings' tab, the following options are visible:

- ☒ Allow agent communication
 - Agent deployment action: **No action** (highlighted with a red box)
- ☒ Allow agent upgrade
 - Agent automatic upgrade schedule: <All the time>
- ☐ Collect utilization data
- ☐ Allow agentless scanner execution
 - ☐ Remove scan data
 - ☐ Accept new public client key
 - ☐ Accept changed public client key
- ☐ Limit bandwidth for data transfers: 0 Kb/s

- Go to **DDMI > Server > Administration > System Configuration > Discovery services**.

For **Automatic agent deployment active**, click **Custom > No**.

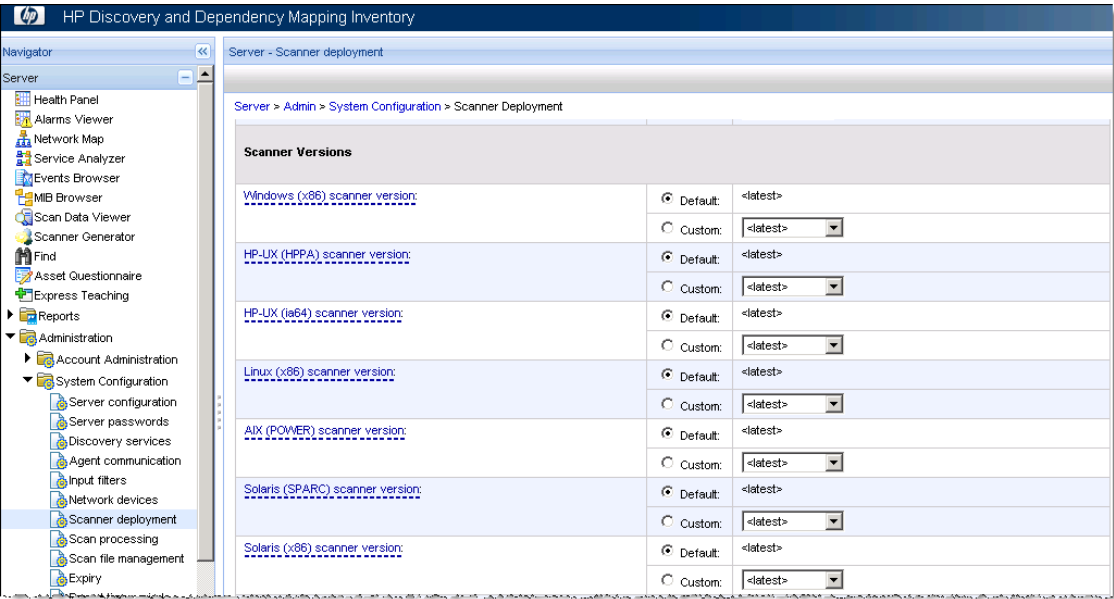
For **Automatic scanner deployment active**, click **Custom > No**.



2. Confirm that no specific scanner is selected.

Go to **DDMI > Server > Administration > System Configuration > Scanner deployment**.

Ensure that **Scanner Deployment** is configured as follows:



Note: For Interoperability issues before DDMI 9.32 Update2, contact HP Software Support if your DDMI is not updated.

Choose an Inventory Discovery Mode

This section includes:

Inventory Discovery Mode Concepts	19
Inventory Discovery Mode Types	20

Inventory Discovery Mode Concepts

This section describes the main concepts of Inventory Discovery Mode:

Inventory Discovery Mode

Inventory Discovery Mode is the way to obtain inventory data of devices.

Client

Client means devices without a bound IP address.

This kind of device usually requests a dynamic IP address to the DHCP (Dynamic Host Configuration Protocol) server when the device is connected to the network.

Data Center

Data Center means devices with relatively stable IP addresses, such as a server, database, and so on.

Note: You must be able to know if any IP address changes in the environment and you can manipulate the IP address manually in UCMDB.

Active discovery

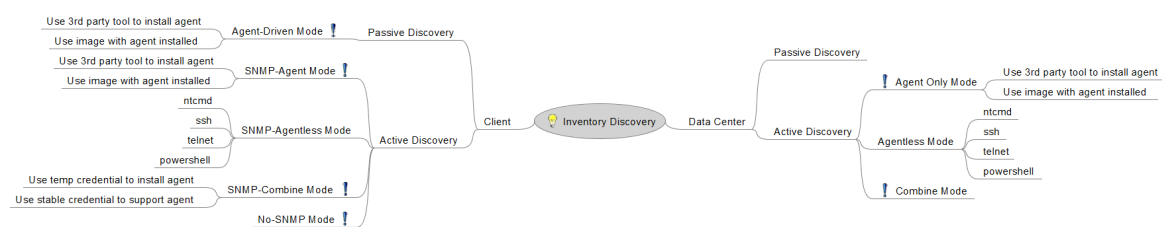
Data Flow Probe actively searches for devices. The whole discovery workflow is started by Universal Discovery.

Passive Discovery

Data Flow Probe just waits for devices to call home.

For details on Call Home, see the *HP Universal CMDB Data Flow Management Guide*.

Inventory Discovery Mode Types



This section includes:

Agent-Only Mode 21

Agentless Mode 22

Combined Mode 24

Agent-Driven Mode 26

SNMP-Agent Mode28

SNMP-Combined Mode30

SNMP-Agentless Mode32

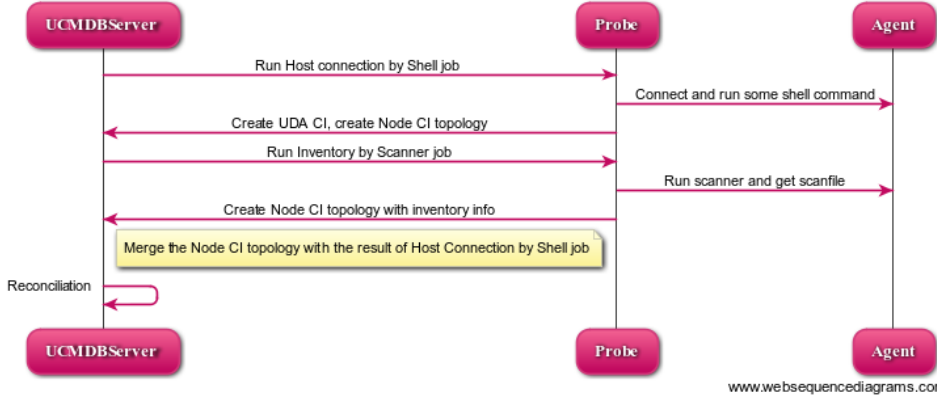
No-SNMP Agent Mode34

Agent-Only Mode

In this mode, an agent is preinstalled on devices. Data Flow Probe only has the Universal Discovery Protocol. When a device is in the network, the probe will ping it and create an IpAddress CI, and a series of jobs can be triggered to discover Node and NodeElement CI.

This mode is a recommended mode for the Data Center environment. Each agent has its own UUID that is saved in the agent configuration file. If the agent is preinstalled in an image, pay attention to the UUID. Contact HP Software Support for advice.

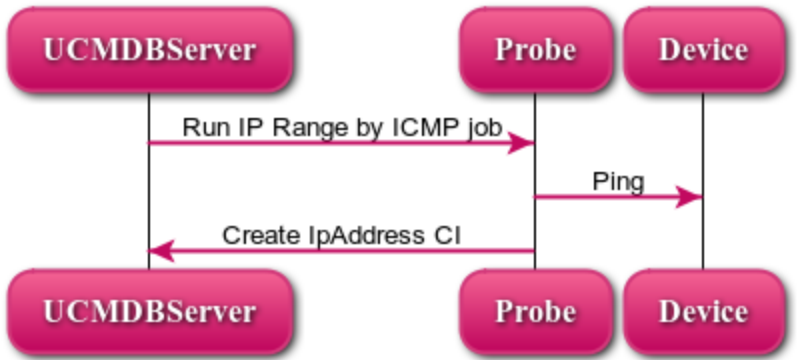
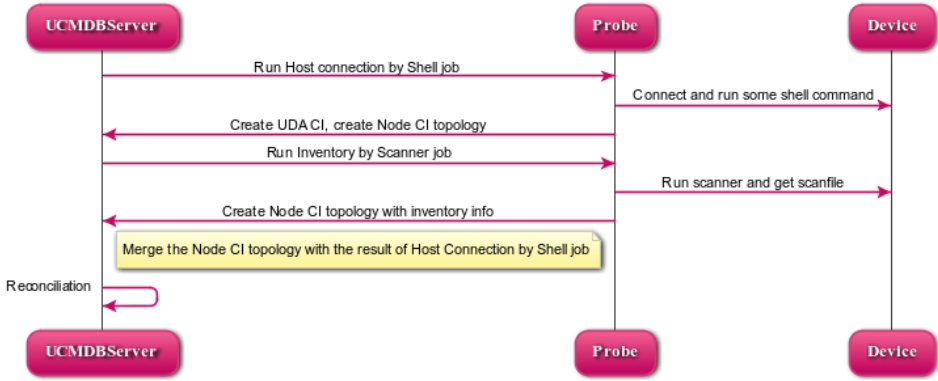
Agent-Only Mode	Description
Basic discovery	<div>Describes how UCMDB knows that the device exists in the environment.</div> <div>The basic discovery workflow of this mode is as follows:</div> <div><p>Ping the device</p><pre>sequenceDiagram participant UCMDBServer participant Probe participant Device UCMDBServer->>Probe: Run IP Range by ICMP job Note over Probe: Ping Probe->>Device: Ping Device-->>Probe: Probe-->>UCMDBServer: Create IpAddress CI</pre><p>www.websequencediagrams.com</p></div>
Inventory discovery	<div>Describes how UCMDB obtains the detailed Inventory data of a device.</div> <div>The inventory discovery workflow of this mode is as follows:</div>

Agent-Only Mode	Description
	<p style="text-align: center;">Inventory with agent workflow</p>  <p style="text-align: right; font-size: small;">www.websequencediagrams.com</p>
Advantages	<ul style="list-style-type: none"> • Simple and clear scenario without Call Home in it. • Secure because UCMDB do not need any other credentials but the Universal Discovery Protocol.
Disadvantages	<ul style="list-style-type: none"> • Need a preinstalled agent on every device. • No remedy if the agent fails because the agent is the only connection channel. • Difficult to troubleshoot if there is no remote access to the device.
Prerequisite	To apply this mode, you must have a method to install and upgrade an agent without UCMDB.
Related jobs	<ul style="list-style-type: none"> • Range IPs by ICMP • Host Connection by Shell • Inventory Discovery by Scanner
Attention	9. A score (1 - 10) to evaluate the mode. The higher the score is, the more recommended the mode is for you.
Other information	You must disable Call Home in this mode.

Agentless Mode

No Universal Discovery agent is installed in the whole environment. Data Flow Probe manages credentials of different protocols (NTCMD, SSH, and so on) to connect to the target device and discover.

The scanner is copied and run by the remote control.

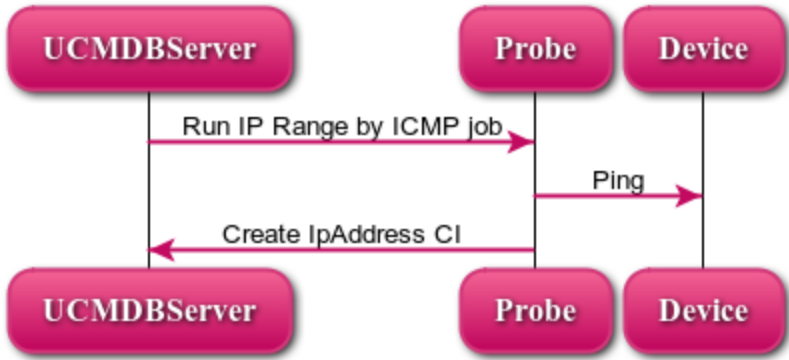
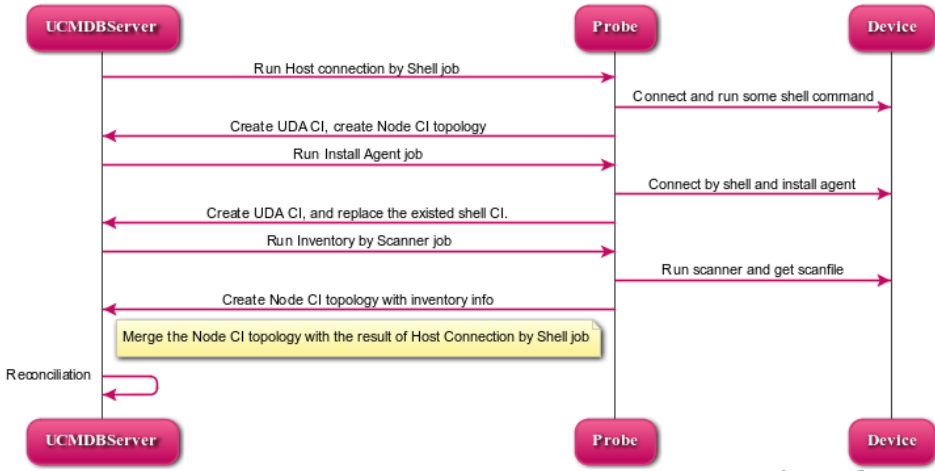
Agentless Mode	Description
<p>Basic discovery</p>	<p>Describes how UCMDB knows that the device exists in the environment.</p> <p>The basic discovery workflow of this mode is as follows:</p> <p style="text-align: center;">Ping the device</p>  <pre> sequenceDiagram participant UCMDBServer participant Probe participant Device UCMDBServer->>Probe: Run IP Range by ICMP job Probe->>Device: Ping Device-->>UCMDBServer: Create IpAddress CI </pre> <p style="text-align: right;">www.websequencediagrams.com</p>
<p>Inventory discovery</p>	<p>Describes how UCMDB obtains the detailed Inventory data of a device.</p> <p>The inventory discovery workflow of this mode is as follows:</p> <p style="text-align: center;">Inventory with agent workflow</p>  <pre> sequenceDiagram participant UCMDBServer participant Probe participant Device UCMDBServer->>Probe: Run Host connection by Shell job Probe->>Device: Connect and run some shell command Device-->>Probe: Run scanner and get scanfile Probe-->>UCMDBServer: Create Node CI topology with inventory info UCMDBServer->>Probe: Create UDA CI, create Node CI topology Probe->>Device: Run Inventory by Scanner job Device-->>UCMDBServer: Merge the Node CI topology with the result of Host Connection by Shell job Note over UCMDBServer: Reconciliation </pre> <p style="text-align: right;">www.websequencediagrams.com</p>
<p>Advantages</p>	<ul style="list-style-type: none"> • Simple and clear workflow. • No need to install an agent.
<p>Disadvantages</p>	<ul style="list-style-type: none"> • Lower security level than that of Agent-Only Mode. You must allow Universal Discovery to manage the credentials to access all devices. • Rely on third-party tools. Defects of xCmd and MindTerm can affect the product.

Agentless Mode	Description
	<ul style="list-style-type: none"> • Lower success ratio to obtain the scan file than that of Agent-Only Mode. • Difficult to troubleshoot.
Prerequisite	To apply this mode, you must configure all needed credentials in UCMDB.
Related jobs	<ul style="list-style-type: none"> • Range IPs by ICMP • Host Connection by Shell • Inventory Discovery by Scanner
Attention	5. A score (1 - 10) to evaluate the mode. The higher the score is, the more recommended the mode is for you.
Other information	If the scan file is important to you, use the agent.

Combined Mode

In this mode, you must provide all credentials to access devices. Universal Discovery can perform all tasks for the inventory discovery. You do not need to use the third-party tool to install the agent. Compared with the previous two modes, this mode charges the probe more.

Combined Mode	Description
Basic discovery	<p>Describes how UCMDB knows that the device exists in the environment.</p> <p>The basic discovery workflow of this mode is as follows:</p>

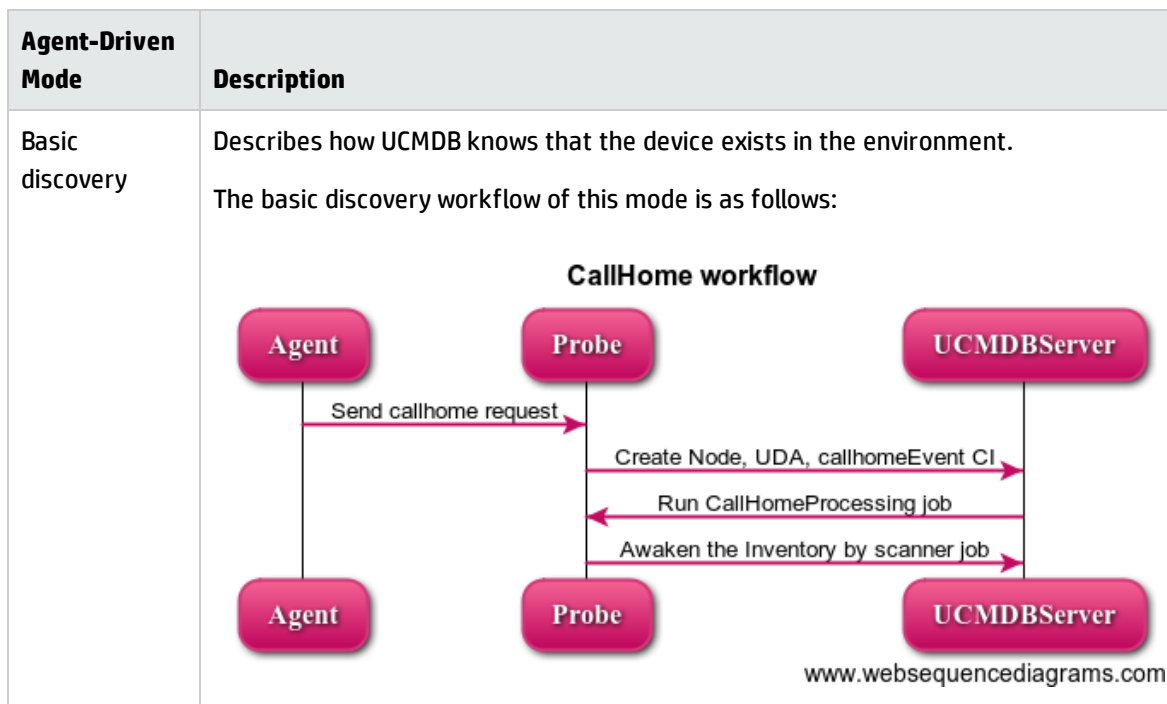
Combined Mode	Description
	<p style="text-align: center;">Ping the device</p>  <p style="text-align: center;">www.websequencediagrams.com</p>
Inventory discovery	<p>Describes how UCMDB obtains the detailed Inventory data of a device.</p> <p>The inventory discovery workflow of this mode is as follows:</p> <p style="text-align: center;">Inventory with agent workflow</p>  <p style="text-align: center;">www.websequencediagrams.com</p>
Advantages	<ul style="list-style-type: none"> • Robust agent. If the agent fails, it can be recovered by other shell commands.
Disadvantages	<ul style="list-style-type: none"> • Complicated workflow, especially the mechanism of Shell CI. Make it difficult to troubleshoot. • Lower security level than that of Agent-Only Mode. You must allow Universal Discovery to manage the credentials to access all devices.
Prerequisite	To apply this mode, you must configure all needed credentials in UCMDB.
Related jobs	<ul style="list-style-type: none"> • Range IPs by ICMP

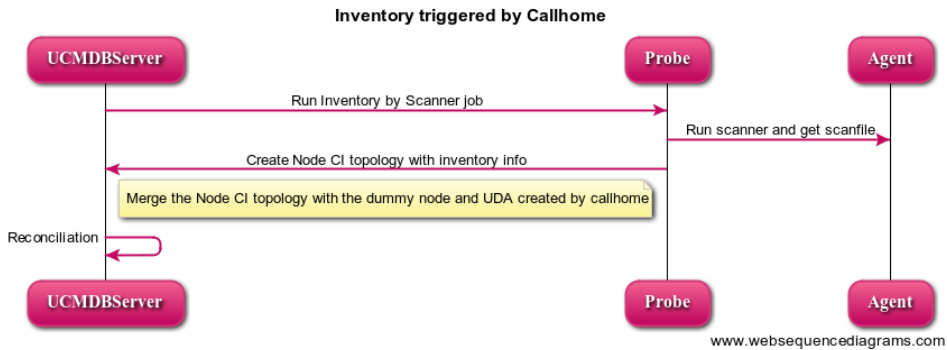
Combined Mode	Description
	<ul style="list-style-type: none"> • Host Connection by Shell • Install UD Agent • Update UD Agent • Inventory Discovery by Scanner
Attention	8. A score (1 - 10) to evaluate the mode. The higher the score is, the more recommended the mode is for you.
Other information	The customer base is large in this mode.

Agent-Driven Mode

In this mode, an agent is preinstalled on devices. Data Flow Probe only has the Universal Discovery Protocol. The probe is waiting for the agent to call home. When Call Home is finished, the probe will create a dummy node and Universal Discovery Agent (UDA) CI, and then trigger the **Inventory Discovery by Scanner** job.

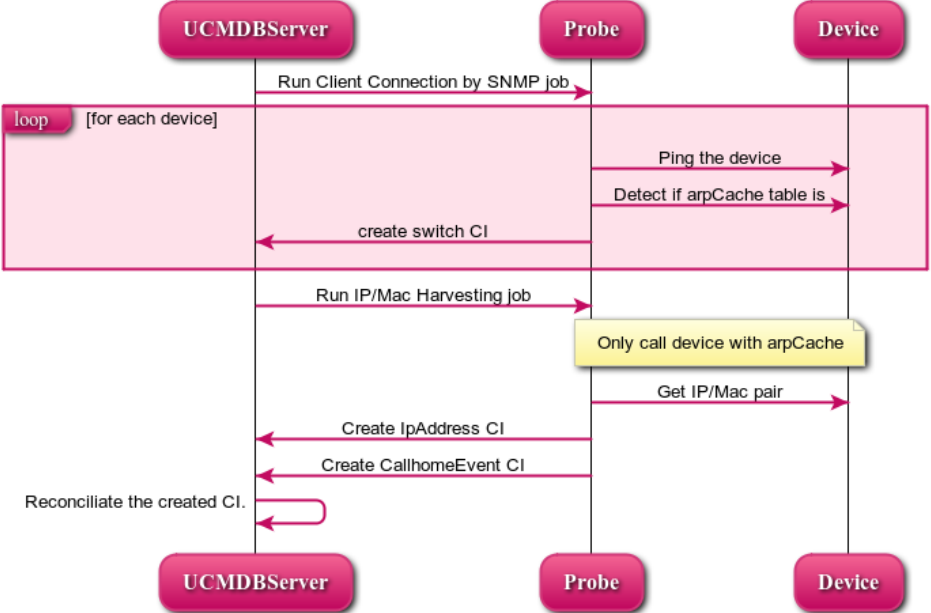
This mode is a recommended mode for you.



Agent-Driven Mode	Description
Inventory discovery	<p>Describes how UCMDB obtains the detailed Inventory data of a device.</p> <p>The inventory discovery workflow of this mode is as follows:</p>  <pre> sequenceDiagram title Inventory triggered by Callhome participant UCMDBServer participant Probe participant Agent UCMDBServer->>Probe: Run Inventory by Scanner job Probe->>Agent: Run scanner and get scanfile Agent-->>Probe: Create Node CI topology with inventory info Probe-->>UCMDBServer: Merge the Node CI topology with the dummy node and UDA created by callhome UCMDBServer->>UCMDBServer: Reconciliation </pre> <p>www.websequencediagrams.com</p>
Advantages	<ul style="list-style-type: none"> • The only available solution for the Client environment without SNMP. • Secure because UCMDB do not need any other credentials but the Universal Discovery Protocol.
Disadvantages	<ul style="list-style-type: none"> • Need a preinstalled agent on every device. • No remedy if the agent fails because the agent is the only connection channel. • Difficult to troubleshoot if there is no remote access to the device.
Prerequisite	To apply this mode, you must have a method to install and upgrade an agent without UCMDB.
Related jobs	<ul style="list-style-type: none"> • Call Home Processing • Inventory Discovery by Scanner
Attention	9. A score (1 - 10) to evaluate the mode. The higher the score is, the more recommended the mode is for you.
Other information	<ul style="list-style-type: none"> • Call Home must be processed in time. • It is recommended to create an Enrichment rule to clean the dummy node. For details on an Enrichment rule, see <i>HP Universal CMDB Data Flow Management Guide</i>.

SNMP-Agent Mode

In this mode, an agent is preinstalled on devices. Data Flow Probe only has the Universal Discovery Protocol. When a device is in the network, the probe can detect its IP address by using the **IP MAC Harvesting by SNMP** job, and a series of jobs can be triggered to discover Node and Node Element CI.

SNMP-Agent Mode	Description
Basic discovery	<p>Describes how UCMDB knows that the device exists in the environment.</p> <p>The basic discovery workflow of this mode is as follows:</p> <div><p>IP/Mac Harvesting</p><pre>sequenceDiagram participant UCMDBServer participant Probe participant Device Note over UCMDBServer, Probe: Run Client Connection by SNMP job UCMDBServer->>Probe: Run Client Connection by SNMP job Note over UCMDBServer, Probe, Device: loop [for each device] Probe->>Device: Ping the device Device-->>Probe: Detect if arpCache table is Probe->>UCMDBServer: create switch CI Note over UCMDBServer, Probe: Run IP/Mac Harvesting job UCMDBServer->>Probe: Run IP/Mac Harvesting job Note over Probe: Only call device with arpCache Probe->>Device: Get IP/Mac pair Device-->>Probe: Probe->>UCMDBServer: Create IpAddress CI Probe->>UCMDBServer: Create CallhomeEvent CI UCMDBServer->>UCMDBServer: Reconciliate the created CI.</pre><p>www.websequencediagrams.com</p></div>
Inventory discovery	<p>Describes how UCMDB obtains the detailed Inventory data of a device.</p> <p>The inventory discovery workflow of this mode is as follows:</p>

SNMP-Agent Mode	Description
	<p style="text-align: center;">Inventory with agent workflow</p> <pre> sequenceDiagram participant UCMDBServer participant Probe participant Agent UCMDBServer->>Probe: Run Host connection by Shell job Probe->>Agent: Connect and run some shell command Agent-->>Probe: Probe-->>UCMDBServer: Create UDA CI, create Node CI topology UCMDBServer->>Probe: Run Inventory by Scanner job Probe->>Agent: Run scanner and get scanfile Agent-->>Probe: Probe-->>UCMDBServer: Create Node CI topology with inventory info Note over UCMDBServer,Probe: Merge the Node CI topology with the result of Host Connection by Shell job UCMDBServer->>UCMDBServer: Reconciliation </pre> <p style="text-align: right; font-size: small;">www.websequencediagrams.com</p>
Advantages	<ul style="list-style-type: none"> • Simple and clear scenario without Call Home in it. • Secure because UCMDB do not need any other credentials but the Universal Discovery Protocol. • With the IP MAC Harvesting by SNMP job, all new IP addresses can be discovered in real time.
Disadvantages	<ul style="list-style-type: none"> • SNMP is a must, which is not acceptable for many customers. • Need a preinstalled agent on every device. • No remedy if the agent fails because the agent is the only connection channel. • Difficult to troubleshoot if there is no remote access to the device.
Prerequisite	<p>To apply this mode, you must have a method to install and upgrade an agent without UCMDB. The SNMP community string is necessary to run the IP MAC Harvesting by SNMP job.</p>
Related jobs	<ul style="list-style-type: none"> • IP MAC Harvesting by SNMP • Host Connection by Shell • Inventory Discovery by Scanner
Attention	<p>9. A score (1 - 10) to evaluate the mode. The higher the score is, the more recommended the mode is for you.</p>

SNMP-Combined Mode

In this mode, the SNMP credential is required to connect to a router or switch. Data Flow Probe first pings the Client environment and discovers routers with arpCache enabled. Then the probe reads the arpCache table to get the IP address or MAC address pair. With the IpAddress CI, the probe discovers all other elements.

SNMP-Combined Mode	Description
Basic discovery	<div><p>Describes how UCMDB knows that the device exists in the environment.</p><p>The basic discovery workflow of this mode is as follows:</p><div><p>IP/Mac Harvesting</p></div></div>
Inventory discovery	<div><p>Describes how UCMDB obtains the detailed Inventory data of a device.</p><p>The inventory discovery workflow of this mode is as follows:</p></div>

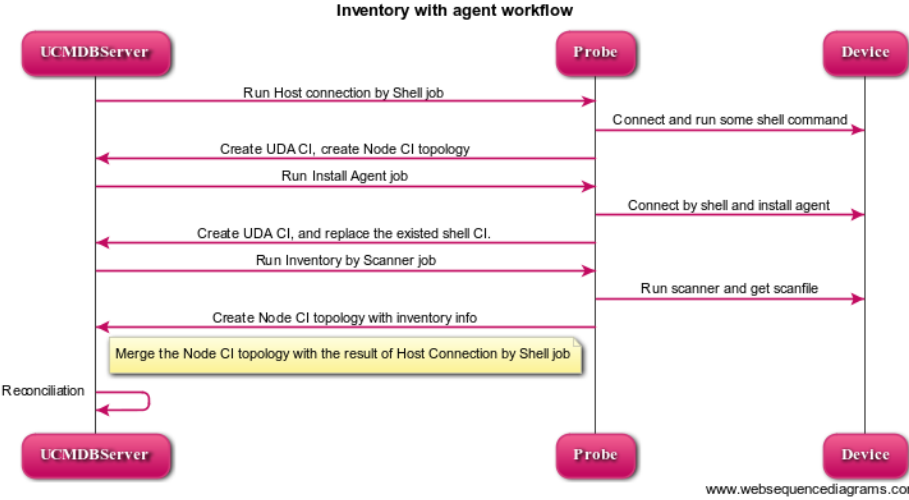
SNMP-Combined Mode	Description
	<p style="text-align: center;">Inventory with agent workflow</p> <pre> sequenceDiagram participant UCMDBServer participant Probe participant Device UCMDBServer->>Probe: Run Host connection by Shell job Probe-->>UCMDBServer: Create UDA CI, create Node CI topology UCMDBServer->>Probe: Run Install Agent job Probe-->>UCMDBServer: Create UDA CI, and replace the existed shell CI. UCMDBServer->>Probe: Run Inventory by Scanner job Probe-->>UCMDBServer: Create Node CI topology with inventory info UCMDBServer->>Probe: Merge the Node CI topology with the result of Host Connection by Shell job UCMDBServer->>UCMDBServer: Reconciliation Probe->>Device: Connect and run some shell command Device->>Probe: Connect by shell and install agent Probe->>Device: Run scanner and get scanfile </pre> <p style="text-align: right; font-size: small;">www.websequencediagrams.com</p>
Advantages	<ul style="list-style-type: none"> • With the IP MAC Harvesting by SNMP job, all new IP addresses can be discovered in real time.
Disadvantages	<ul style="list-style-type: none"> • SNMP is a must, which is not acceptable for many customers. • The Host Connection by SNMP job runs by default and can cause performance issues. • Certain ratio of lost devices exists, because the long discovery process cannot catch the changing IP address. • No method to troubleshoot the lost device problem.
Prerequisite	<p>To apply this mode, you must have the following credential:</p> <ul style="list-style-type: none"> • SNMP credential • Root privilege credential to install an agent
Related jobs	<ul style="list-style-type: none"> • Client Connection by SNMP • IP MAC Harvesting by SNMP • Host Connection by Shell • Host Connection by SNMP • Install UD Agent

SNMP-Combined Mode	Description
	<ul style="list-style-type: none"> Update UD Agent Inventory Discovery by Scanner
Attention	9. A score (1 - 10) to evaluate the mode. The higher the score is, the more recommended the mode is for you.
Other information	For the Client environment, it is recommended to use the passive discovery if you can accept the Agent-Driven mode. For details, see "Agent-Driven Mode" on page 26 .

SNMP-Agentless Mode

This mode is rarely seen because the Client environment is usually upgraded from DDMI.

SNMP-Agentless Mode	Description
Basic discovery	<p>Describes how UCMDB knows that the device exists in the environment.</p> <p>The basic discovery workflow of this mode is as follows:</p> <pre> sequenceDiagram participant UCMDBServer participant Probe participant Device UCMDBServer->>Probe: Run Client Connection by SNMP job loop [for each device] Probe->>Device: Ping the device Probe->>Device: Detect if arpCache table is Device->>UCMDBServer: create switch CI end UCMDBServer->>Probe: Run IP/Mac Harvesting job Note over Probe: Only call device with arpCache Probe->>Device: Get IP/Mac pair Device->>UCMDBServer: Create IpAddress CI Device->>UCMDBServer: Create CallhomeEvent CI UCMDBServer->>UCMDBServer: Reconcillate the created CI. </pre> <p>www.websequencediagrams.com</p>
Inventory	Describes how UCMDB obtains the detailed Inventory data of a device.

SNMP-Agentless Mode	Description
discovery	<p>The inventory discovery workflow of this mode is as follows:</p> 
Advantages	<ul style="list-style-type: none"> • With the IP MAC Harvesting by SNMP job, all new IP addresses can be discovered in real time. • Less request for the credential privilege.
Disadvantages	<ul style="list-style-type: none"> • SNMP is a must, which is not acceptable for many customers. • The Host Connection by SNMP job runs by default and can cause performance issues. • Certain ratio of lost devices exists, because the long discovery process cannot catch the changing IP address. • No method to troubleshoot the lost device problem. • Minor credential privilege can cause scanner issues.
Prerequisite	To apply this mode, you must have the SNMP credential.
Related jobs	<ul style="list-style-type: none"> • Client Connection by SNMP • IP MAC Harvesting by SNMP • Host Connection by Shell • Host Connection by SNMP • Install UD Agent

SNMP-Agentless Mode	Description
	<ul style="list-style-type: none"> • Update UD Agent • Inventory Discovery by Scanner
Attention	2. A score (1 - 10) to evaluate the mode. The higher the score is, the more recommended the mode is for you.
Other information	This mode is a less used mode.

No-SNMP Agent Mode

This is a new feature in UCMDB 10.20. With this mode, you can perform the Inventory discovery without the SNMP community string to routers or switches.

This mode is the only available active mode for the Client environment without the SNMP protocol.

No-SNMP Agent Mode	Description
Basic discovery	<p>Describes how UCMDB knows that the device exists in the environment.</p> <p>The basic discovery workflow of this mode is as follows:</p> <div style="text-align: center;"> <p>Ping the device</p> <pre> graph TD subgraph Top UCMDBServer1[UCMDBServer] -- "Run IP Range by ICMP job" --> Probe1[Probe] Probe1 -- "Ping" --> Device1[Device] end subgraph Bottom Device2[Device] --> Probe2[Probe] Probe2 -- "Create IPAddress CI" --> UCMDBServer2[UCMDBServer] end </pre> <p>www.websequencediagrams.com</p> </div>
Inventory discovery	<p>Describes how UCMDB obtains the detailed Inventory data of a device.</p> <p>The inventory discovery workflow of this mode is as follows:</p>

No-SNMP Agent Mode	Description
	<div><p>Inventory with agent workflow</p><pre>sequenceDiagram participant UCMDBServer participant Probe participant Device UCMDBServer->>Probe: Run Host connection by Shell job UCMDBServer->>Probe: Create UDA CI, create Node CI topology UCMDBServer->>Probe: Run Install Agent job UCMDBServer->>Device: Connect and run some shell command UCMDBServer->>Device: Connect by shell and install agent UCMDBServer->>Probe: Create UDA CI, and replace the existed shell CI. UCMDBServer->>Probe: Run Inventory by Scanner job UCMDBServer->>Device: Run scanner and get scanfile UCMDBServer->>Probe: Create Node CI topology with inventory info UCMDBServer->>Probe: Merge the Node CI topology with the result of Host Connection by Shell job UCMDBServer->>UCMDBServer: Reconciliation</pre><p>www.websequencediagrams.com</p></div>
Advantages	Can work without the SNMP community string.
Disadvantages	Without the IP MAC Harvesting by SNMP job, all new IP addresses cannot be discovered in real time.
Related jobs	<ul style="list-style-type: none">• Range IPs by ICMP• Host Connection by Shell• Install UD Agent• Update UD Agent• Inventory Discovery by Scanner
Attention	8. A score (1 - 10) to evaluate the mode. The higher the score is, the more recommended the mode is for you.

Chapter 3: Migration Procedure

This chapter includes:

How to Migrate DDMI Server Configuration Data to Universal Discovery	36
How to Configure Universal Discovery	40
How to Migrate DDMI Agents to Universal Discovery Agents	71
Check the Migration Status	72
How to Configure DDMI and Universal Discovery for Interoperability	72

How to Migrate DDMI Server Configuration Data to Universal Discovery

To migrate DDMI server configuration data to Universal Discovery, do the following:

1. Export DDMI server configuration data
 - a. Locate the **DDMIMigration.pl** script on the UCMDB Server at the following location:

- **Windows:**C:\hp\UCMDB\UCMDBServer\tools\migration
 - **Linux:**C:/opt/hp/UCMDB/UCMDBServer/tools/migration
 - b. Copy the script to any directory on each DDMI server that you want to migrate.
 - c. For each DDMI server, open a Command prompt and navigate to the directory where you copied the script. At the Command prompt, run the following command:

perl DDMIMigration.pl

You can see the following message:

```
Administrator: C:\Windows\system32\cmd.exe
G:\DDMI>perl DDMIMigration.pl
Start to extract the migration data.
Extracting system configuration.
Extracting the deployment credentials.
Extracting the SNMP configuration profile.
Extracting the virtualization profile.
Extracting the discovery configuration profile.
Extracting the network configuration profile.
Extracting the agent configuration profile.
Extracting the scanner configuration profile.
Extracting the device groups.
Copying the scanner configuration files.
Copying the pre-scan and post-scan scripts.
Copying the user SAI files.
Copying the XMLEnricher configuration file.
Copying the agent certification files.
The migration data is saved to DDMIMigrationData.zip
G:\DDMI>
```

Note:

- By default, the data is archived in a file called **DDMIMigrationData.zip**.
- For options that are available for this script, see ["Server Configuration Data Export Script Resources" on page 82](#).
- Maximum amount of device groups that can be imported is 20. If device groups exceed 20, remove some groups and run the script again. Then, create the remaining management zones in Universal Discovery manually.

For more information about the type of information that is migrated, see ["Results" on page 39](#).

2. Import the data to Universal Discovery

- Open the JMX Console, enter **importMigrationDatafromDDMI** in the quick search field and click the link that appears.

importMigrationDataFromDDMI

Import Migration Data from DDMI

Name	Type	Value	Description
customerid	int	<input type="text"/>	Customer Id
isCreateActivity	boolean	<input checked="" type="radio"/> True <input type="radio"/> False	True if you want to create activities.
probeName	java.lang.String	<input type="text"/>	Name of the Probe that you want to use to manage all of the IP ranges.
primaryCallHomeAddress	java.lang.String	<input type="text"/>	The primary call home address for Data Flow Probe. If blank, the IP Address of "probeName" is used.
SecondaryCallHomeAddress	java.lang.String	<input type="text"/>	The secondary call home address for Data Flow Probe. If blank, the IP Address of "probeName" is used.
configurationZipPackageName	java.lang.String	DDMIMigrationData.zip	File name of the archive (.zip) file.
overrideGlobalConfig	boolean	<input checked="" type="radio"/> True <input type="radio"/> False	True if the global configuration file in UCMDB is overwritten.
stopWhenConflict	boolean	<input checked="" type="radio"/> True <input type="radio"/> False	True if imported data has conflicting with the existed data in UCMDB.

- In the **importMigrationDataFromDDMI** method, the following parameters are displayed:

- **customerId.** The customer ID that you want to migrate.

If you do not know the **customerId** parameter for the customer you are migrating, do the following:

- In UCMDB, go to **Data Flow Management > Data Flow Probe Setup**.
- In the **Domains and Probes** pane, select a Data Flow Probe and note the customer name at the top right of the window.
- Go to **JMX Console > Customer and States > ShowAllCustomers** method and note the **customerId** that maps to the customer name.
- **isCreateActivity.**
 - **True.** Creates new activities in Management Zones. These activities contain the migrated data.
 - **False.** No activities are created. However, Management Zones are created.
- **primary|Secondary Call Home Address.** The primary and the secondary Call Home IP addresses for the Data Flow Probe.

For example:

<UD_CallHomeIPAddressPrimary> , <UD_CallHomeIPAddressSecondary>

Note:

- If this field is left blank, the IP address of the Data Flow Probe is used.
- In some cases, data that is entered in these fields may not appear in the UCMDB Infrastructure activity. In these cases, reenter the data in the activity.
- The DDMI Call Home IP addresses are pre-populated, so it is not necessary to enter this information.

- **probeName.** The name of the Data Flow Probe to which to map the data.
- **configurationzipPackageName.** The name of the archive file that was created in step 1.
- **overrideGlobalConfig.**

- **True.** The XML Enricher global configuration file in UCMDB is overwritten by the DDMI configuration file.
- **False.** The XML Enricher global configuration file in UCMDB is not overwritten and the DDMI configuration file is ignored.
- **stopWhenConflict.**

Specifies how to handle IP address range conflicts.

- **True.** If overlapping IP address ranges exist in DDMI and UCMDB, no IP address ranges are imported to UCMDB.
- **False.** If the same IP address range exists in UCMDB, only IP address ranges that are not in conflict are imported. Ranges that are in conflict are ignored. Additionally, Management Zones that contained the conflicted ranges are not imported.

Note: It is recommended to import DDMI server configuration data to a clean probe because of IP Address conflict issues.

3. Results

- Success messages and warning messages are displayed.
- For some common issues that may occur, see ["Server Configuration Data Import Troubleshooting" on page 89](#).
- In addition to the data that is contained in the archive file that was created in step 1, the following information is imported into UCMDB:
 - **Deployment credentials.** Credentials are imported and keys are regenerated automatically.
 - **SNMP configuration profile.**
 - **Device groups.**
 - **System configuration.**
 - **VMware configuration.**
 - **XML Enricher configuration file.** For details, see ["overrideGlobalConfig." on the previous page](#).

- **Certificates.**
 - acstrust.cert
 - agentca.pem
 - acskeystore.bin
- **IP address ranges.**
- Additionally, the following resources are imported:
 - Pre-scan and post-scan scripts
 - Scanner configuration files (.cxz)
 - User SAI files
- However, not all information exported from DDMI can work properly in Universal Discovery, further tuning is required. For details, see ["How to Configure Universal Discovery" below](#).
- Basically, only the following information from DDMI is used for Universal Discovery without any change:
 - **Deployment credentials.**
 - **SNMP configuration profile.**
 - **VMware configuration.**
 - **XML Enricher configuration file.**
 - **Certificates.**
 - **Pre-scan and post-scan scripts.**
 - **User SAI files.**

How to Configure Universal Discovery

This task describes how to configure Universal Discovery to run Inventory Discovery in your environment.

This section includes:

Change of the Migrated Configuration	41
Configure Data Flow Probe	42
Configure Inventory Discovery	44
Step-by-Step Configuration for Experienced Users	68


Change of the Migrated Configuration

Before configuring the Universal Discovery, perform the following steps:

Check the IP address range of the probe

Basically, all IP addresses configured on DDMI will be imported as Client IP addresses. The importation cannot merge continuous IP address ranges or remove duplicated IP addresses. Therefore, it is recommended to review the IP address configuration here.


If the imported IP address ranges do not meet your expectation, manually delete all imported IP address ranges and add new IP address ranges as follows:

- Select **Data Flow Management > Data Flow Probe Setup > Domains and Probes > a domain > Data Flow Probes > the probe.**
- In the Ranges pane, select the IP address range that you want to delete, and click .
- For details on how to add IP address ranges, see ["Configure Data Flow Probe" on the next page.](#)

Check the management zone

The notion of DDMI Device Group do not match perfectly with the Universal Discovery Management Zone. The Management Zone defines jobs to run on defined IP addresses. There is no need to create too many zones if you are running the same job. One zone corresponding to one probe is the normal configuration that is widely used.

Delete all management zones and recreate one zone that covers the whole probe as follows:

- Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery tab > Management Zones** tree, select the management zone and click .
- For details on how to create a management zone, see the relevant section in ["Configure Inventory Discovery" on page 44.](#)


Change the migration job schedule

In the zone-based mode, the schedule is defined for the activity instead of for each specific job. You can use the **No module** as a workaround. For details, see ["Step-by-Step Configuration for Experienced Users" on page 68](#).

Change the aging time

The default frequency for the **Inventory Discovery by Scanner** job is 14 days. The default value of **Actual Deletion Period** is 40 days, which is too short and can cause data loss.


For the Node CI type and NodeElement CI type, change the **Default Value** of **Actual Deletion Period** as follows:

- Select **Modeling > CI Type Manager > CI Types** pane > **Managed Object** tree > **ConfigurationItem > InfrastructureElement > Node** or **NodeElement** CI type.
- Click the **Attributes** tab in the right-hand pane, select **Actual Deletion Period**, and Click .
- In the **Edit Attribute** dialog box, Click the **Details** tab, change **40** to **140** in the **Default Value** field.
- Click **OK**.

Configure Data Flow Probe

After you install Universal Discovery, perform the following steps to configure the Data Flow Probe:

1. Manually add the IP address range.

Select **Data Flow Management > Data Flow Probe Setup > Domains and Probes > a domain > Data Flow Probes > the probe**, and in the Ranges pane click **New Range** .


For more information, see the section that describes how to edit IP Ranges in the *HP Universal CMDB Data Flow Management Guide*.

Note:

- It is not recommended to mix Data Center IP address with Client IP address in a single probe.

- Merge a single IP into the IP Range if possible, because too many IP ranges can be the root cause of performance issues.
- Do not overuse **Excluded IP Ranges**. For example, split one IP range into two IP ranges instead of having one IP range with an excluded IP range.

2. Manually add the credential if the credential imported from DDMI is not enough.

Select **Data Flow Management > Data Flow Probe Setup > Domains and Probes > a domain > Credentials > the protocol**, and in the right-hand pane click .

For more information, see the *Define Credentials* section in the *HP Universal CMDB Data Flow Management Guide*.

Note: Limit your credential list because too many credentials can cause performance issues.

3. Import the IP range and credential.

You can import the IP range and credential by JMX Console. Do the following:

- Open JMX Console and enter **importCredentialsAndRangesInformation** in the quick search field and click the link that appears.

importCredentialsAndRangesInformation

Imports from a provided file credentials and ranges.

Name	Type	Value	Description
customerId	int	<input type="text"/>	Customer Id
fileName	java.lang.String	<input type="text"/>	Name of file to import
password	java.lang.String	<input type="text"/>	Password to use for imported file's decryption (if the file was encrypted)
isEncrypted	boolean	<input checked="" type="radio"/> True <input type="radio"/> False	True if the imported file is encrypted. False if the imported file is not encrypted (please note that non-encrypted file doesn't contain credentials' sensitive information (like passwords)).
includeProbeRange	boolean	<input checked="" type="radio"/> True <input type="radio"/> False	True for the exported file will include the probe ranges.
notAllowOverlap	boolean	<input checked="" type="radio"/> True <input type="radio"/> False	True if overlap ranges will not be imported

Invoke

- Specify the value that you need.
- Click **Invoke**.

Note:

- It is recommended to clear the probe's IP range before the importation, because UCMDB do not allow duplicate IPs in the same domain.

- To clear the probe’s IP range, remove the probe from UCMDB UI and wait until the probe is detected by the server again.

Configure Inventory Discovery

This section includes:

Modify the UCMDB Environment	44
Configure Agent-Only Mode	47
Configure Agentless Mode	49
Configure Combined Mode	51
Configure Agent-Driven Mode	54
Configure SNMP-Agent Mode	56
Configure SNMP-Agentless Mode	59
Configure SNMP-Combined Mode	62
Configure No-SNMP Mode	65

Modify the UCMDB Environment

The following configuration changes are suitable for powerful Data Flow Probes that are aimed to immediately collect information. If your probe hardware is limited, contact HP Software Support for recommendation.

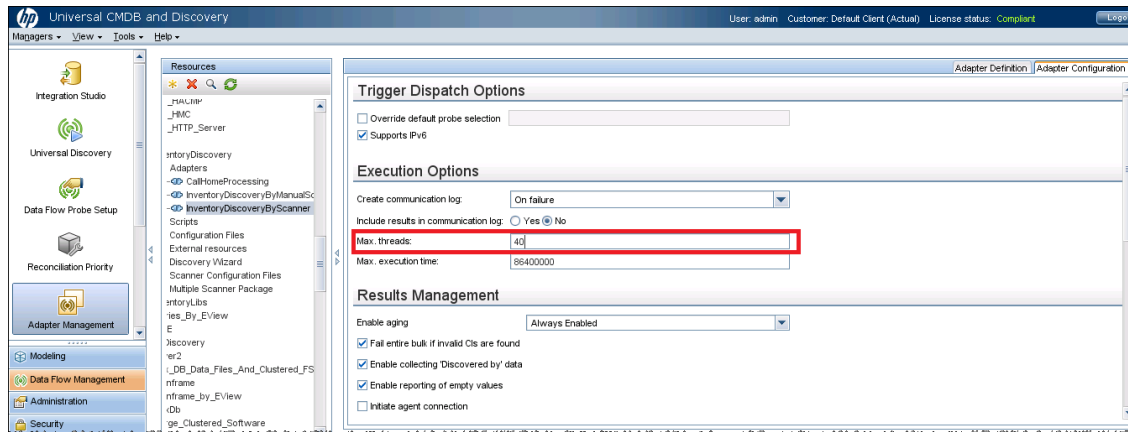
To modify the UCMDB environment, do the following:

- Open **<install>\hp\UCMDB\DataFlowProbe\bin\WrapperEnv.conf** and do the following change:

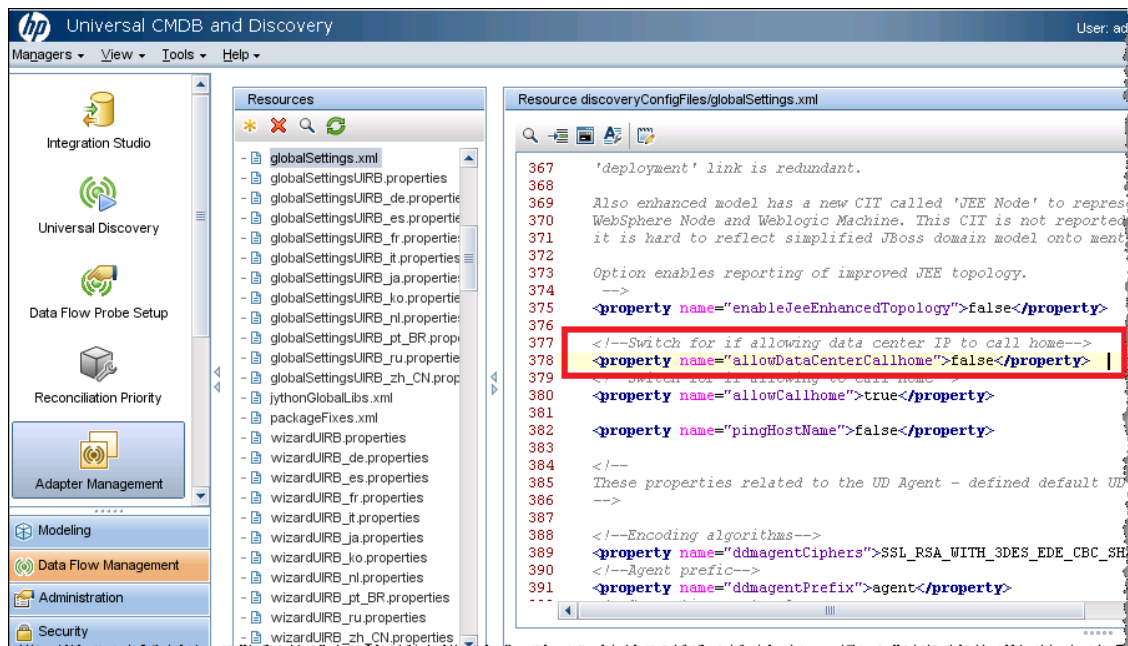

```
set.GATEWAY_MIN_MEM=512
set.GATEWAY_MAX_MEM=3072
```
- Open **<install>\hp\UCMDB\DataFlowProbe\bin\DataFlowProbe.properties** and do the following change:


```
appilog.agent.local.services.poolThreads = 160
appilog.agent.local.services.defaultMaxJobThreads =16
appilog.agent.probe.maxConnection = 40
```

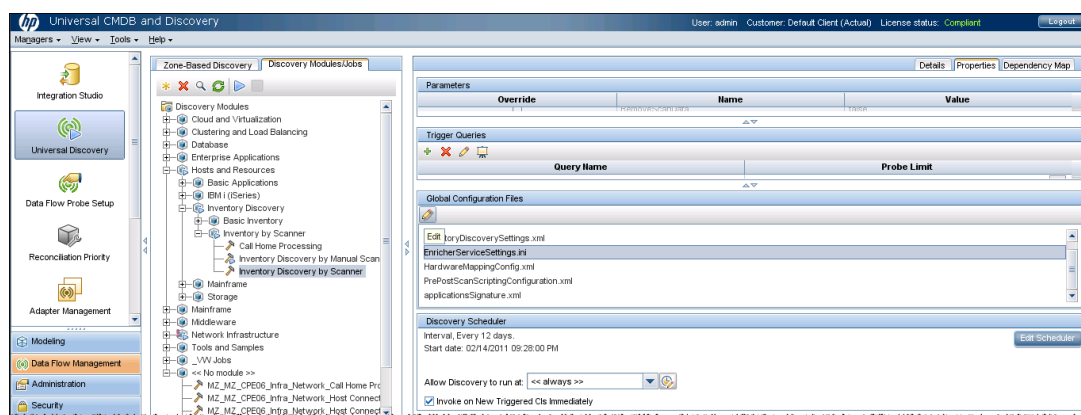
- Change **Max. threads** of **Inventory Discovery by Scanner** to **40** as follows:
 - a. Go to **Data Flow Management > Adapter Management > Resources** pane > **Packages** tree > **InventoryDiscovery > Adapters**, and click **InventoryDiscoveryByScanner**.
 - b. In the right-hand pane, click the **Adapter Configuration** tab, change **Max. threads** to **40** in the Execution Options pane.



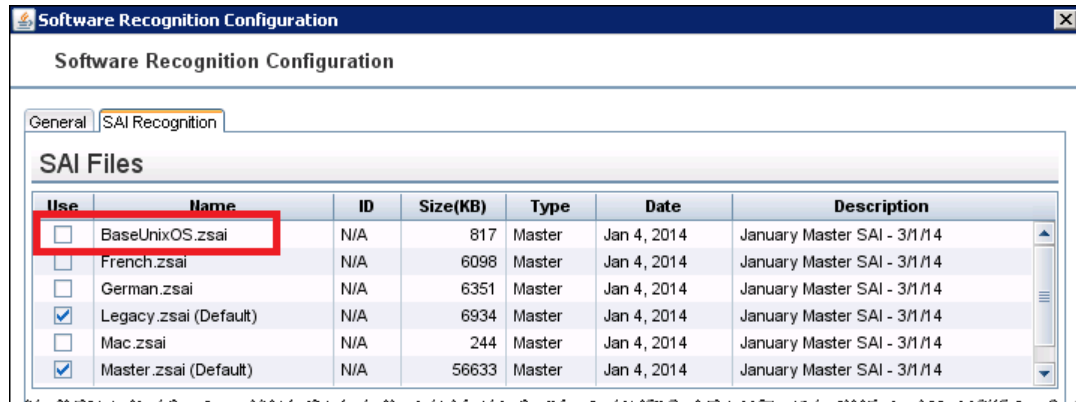
- Disable Data Center Call Home in the **globalSettings.xml** file as follows:
 - a. Go to **Data Flow Management > Adapter Management > Resources** pane > **Packages** tree > **AutoDiscoveryContent > Configuration Files**, and click **globalSettings.xml**.
 - b. In the right-hand pane, change the value of **allowDataCenterCallhome** to **false**.



- Disable **BaseUnixOS.zsai** as follows:
 - a. Go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs tab > Discovery Modules tree > Hosts and Resources > Inventory Discovery > Inventory by Scanner**, and click **Inventory Discovery by Scanner**.
 - b. In the right-hand pane, click the **Properties** tab, select the **EnricherServiceSettings.ini** file in the Global Configuration Files pane, and click the **Edit** button.



- c. In the Software Recognition Configuration dialog box, click the **SAI Recognition** tab, and clear the **BaseUnixOS.zsai** check box if it is selected.



Configure Agent-Only Mode


To configure the Agent-Only mode, do the following:

1. Create a management zone.

Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery** tab, click **New** , and select **New Management Zone**.

For details on how to create a management zone, see *HP Universal CMDB Data Flow Management Guide*.

2. Create an Infrastructure Discovery activity.

- a. Select the management zone that you created, click , and select **New Discovery Activity > Infrastructure**.
- b. On the Define Credentials page, only choose the credential that you need.

- c. If the default Preferences page is not suitable for this mode, you can specify it as follows:

New Infrastructure Discovery Activity

Activity Name
Define Credentials
Preferences
Universal Discovery Agent Deployment
Schedule Discovery
Summary

Preferences
Configure the discovery preferences.

IPv4 Ping Sweep Strategy for Data Center Ranges ? ☐ No Ping Sweep
☒ Ping Sweep within the ranges of the Management Zone
☐ Ping only discovered Class C Networks
☐ Ping only discovered Class B or C Networks

☐ Ping all IPv6 addresses within the ranges of the Management Zone


☐ IP/MAC Address Harvesting ?
 Delay between SNMP requests (ms) 50 ?

☐ Discover Network Devices in Client IP Ranges ?

☐ Resolve DNS Names ?
 DNS Servers ?

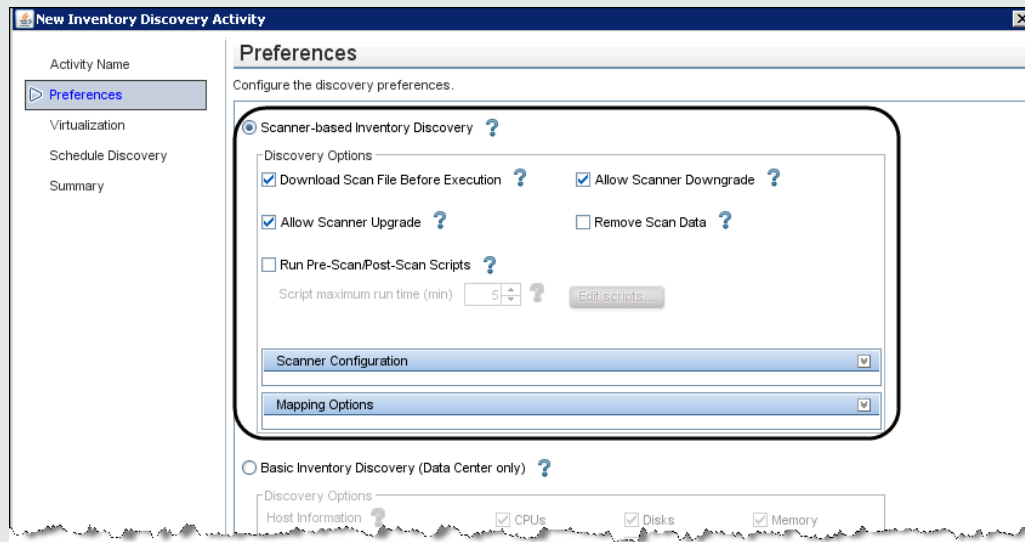
☐ Microsoft Windows Domains ?

- d. On the Universal Discovery Agent Deployment page, select **Update UD Agent**. For the Agent-Only mode, it is not recommended to use the Call Home feature.
3. Activate the Infrastructure Discovery activity.
- Right-click the Infrastructure Discovery activity that you created, and select **Activate**.
4. Create an Inventory Discovery activity.

Select the management zone that you created, click , and select **New Discovery Activity > Inventory**.

Note:

- Only **Scanner-based Inventory Discovery** is involved here.



- You can skip the Schedule Discovery page, because the **Inventory Discovery by Scanner** job is designed to be run every two weeks and the period cannot be changed.

5. Active the Inventory Discovery activity.

Right-click the Inventory Discovery activity that you created, and select **Activate**.

Configure Agentless Mode


To configure the Agentless mode, do the following:

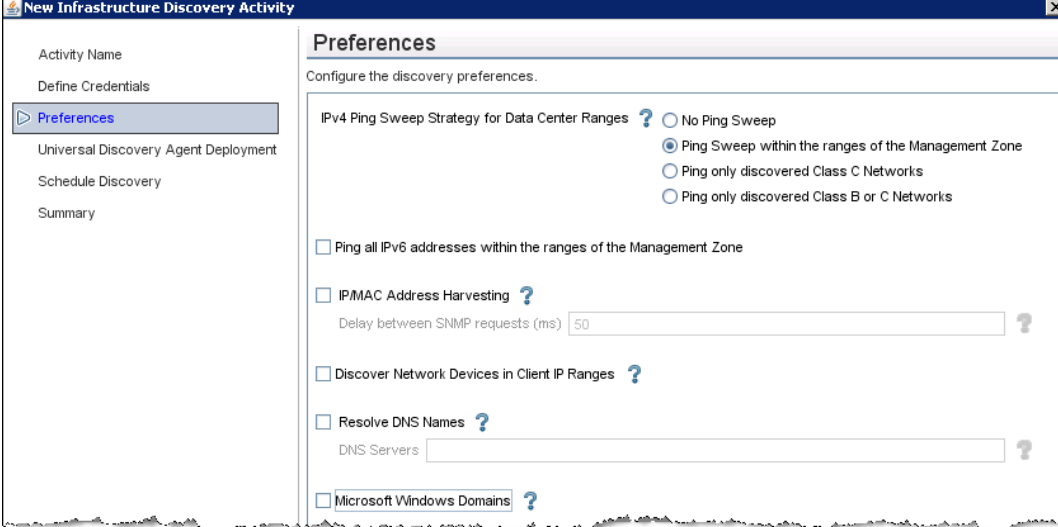
- Create a management zone.

Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery** tab, click **New** , and select **New Management Zone**.


For details on how to create a management zone, see *HP Universal CMDB Data Flow Management Guide*.

- Create an Infrastructure Discovery activity.

- a. Select the management zone that you created, click , and select **New Discovery Activity > Infrastructure**.
- b. On the Define Credentials page, select **NTCMD Protocol** and **SSH Protocol** to respectively cover Windows and Non-Windows (Unix, Linux, Solaris, and so on) devices.
- c. If the default Preferences page is not suitable for this mode, you can specify it as follows:



- d. On the Universal Discovery Agent Deployment page, do not select any check box.
3. Activate the Infrastructure Discovery activity.
- Right-click the Infrastructure Discovery activity that you created, and select **Activate**.
4. Create an Inventory Discovery activity.

Select the management zone that you created, click , and select **New Discovery Activity > Inventory**.

Note:

- Only **Scanner-based Inventory Discovery** is involved here.

- You can skip the Schedule Discovery page, because the **Inventory Discovery by Scanner** job is designed to be run every two weeks and the period cannot be changed.

5. Active the Inventory Discovery activity.

Right-click the Inventory Discovery activity that you created, and select **Activate**.

Configure Combined Mode


To configure the Combined mode, do the following:

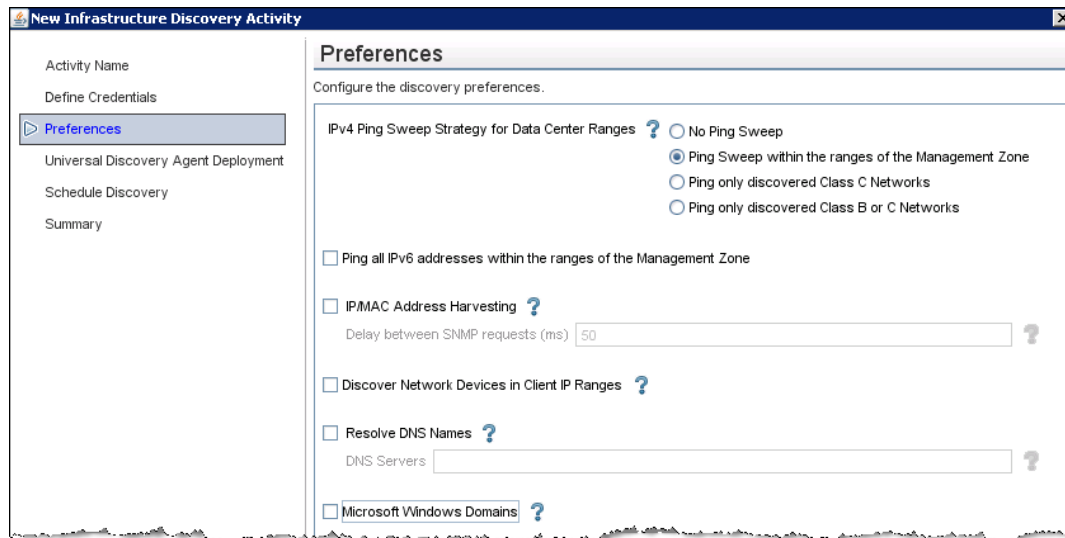
- Create a management zone.

Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery** tab, click **New** , and select **New Management Zone**.

For details on how to create a management zone, see *HP Universal CMDB Data Flow Management Guide*.

- Create an Infrastructure Discovery activity.

- a. Select the management zone that you created, click , and select **New Discovery Activity > Infrastructure**.
- b. On the Define Credentials page, select **NTCMD Protocol** and **SSH Protocol** to respectively cover Windows and Non-Windows (Unix, Linux, Solaris, and so on) devices.
- c. If the default Preferences page is not suitable for this mode, you can specify it as follows:



New Infrastructure Discovery Activity

Activity Name
Define Credentials
Preferences
Universal Discovery Agent Deployment
Schedule Discovery
Summary

Preferences

Configure the discovery preferences.

IPv4 Ping Sweep Strategy for Data Center Ranges ?
☐ No Ping Sweep
☒ Ping Sweep within the ranges of the Management Zone
☐ Ping only discovered Class C Networks
☐ Ping only discovered Class B or C Networks

☐ Ping all IPv6 addresses within the ranges of the Management Zone

☐ IP/MAC Address Harvesting ?
Delay between SNMP requests (ms) 50 ?

☐ Discover Network Devices in Client IP Ranges ?

☐ Resolve DNS Names ?
DNS Servers ?

☐ Microsoft Windows Domains ?

- d. On the Universal Discovery Agent Deployment page, select **Install UD Agent**, **Update UD Agent** and **Install UD Agent to run under root account on UNIX machines**, and type a Call Home probe address if you want to use the Call Home feature.


The screenshot shows the 'Edit Infrastructure Discovery Activity' window with the 'Universal Discovery Agent Deployment' tab selected. The left sidebar contains a tree view with 'Universal Discovery Agent Deployment' highlighted. The main panel, titled 'Control the UD Agent deployment', contains the following settings:

- Agent Deployment:**
 - ☒ Install UD Agent
 - ☐ Migrate DDMI Agent
 - ☒ Update UD Agent
 - ☐ Uninstall UD Agent
- ☒ Install UD Agent to run under root account on UNIX machines
- ☐ Software utilization period (days): 31
- Primary Call Home Probe Address: 16.186.86.186
- Secondary Call Home Probe Address: (empty field)
- Call Home Request Frequency: 3
- Credential for UD Agent Installation: Universal Discovery Protocol Credential 1 (with a 'Select Credential' button)
- Credential for UD Agent Update: Universal Discovery Protocol Credential 1 (with a 'Select Credential' button)

3. Activate the Infrastructure Discovery activity.

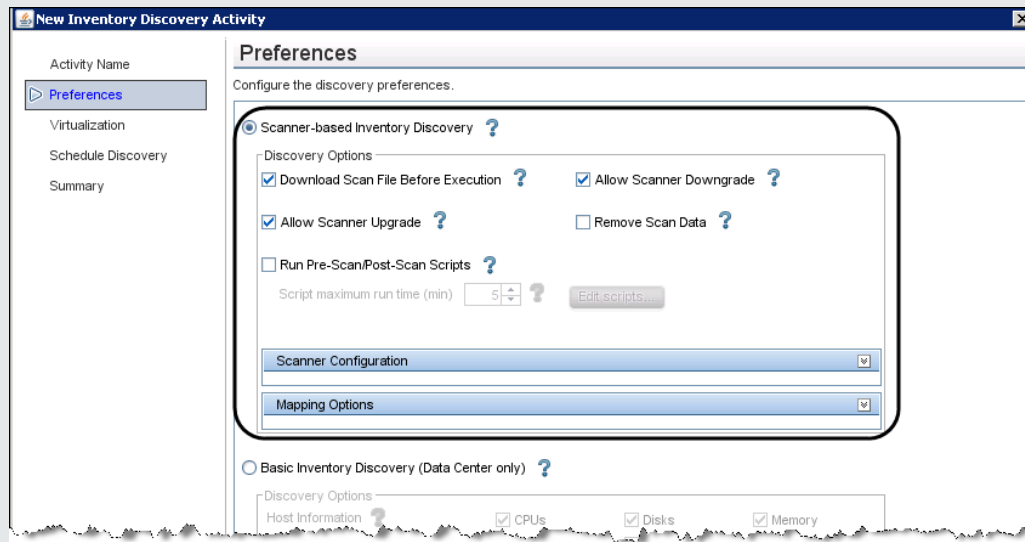
Right-click the Infrastructure Discovery activity that you created, and select **Activate**.

4. Create an Inventory Discovery activity.

Select the management zone that you created, click , and select **New Discovery Activity > Inventory**.

Note:

- Only **Scanner-based Inventory Discovery** is involved here.



- You can skip the Schedule Discovery page, because the **Inventory Discovery by Scanner** job is designed to be run every two weeks and the period cannot be changed.

5. Active the Inventory Discovery activity.

Right-click the Inventory Discovery activity that you created, and select **Activate**.

Configure Agent-Driven Mode


To configure the Agent-Driven mode, do the following:

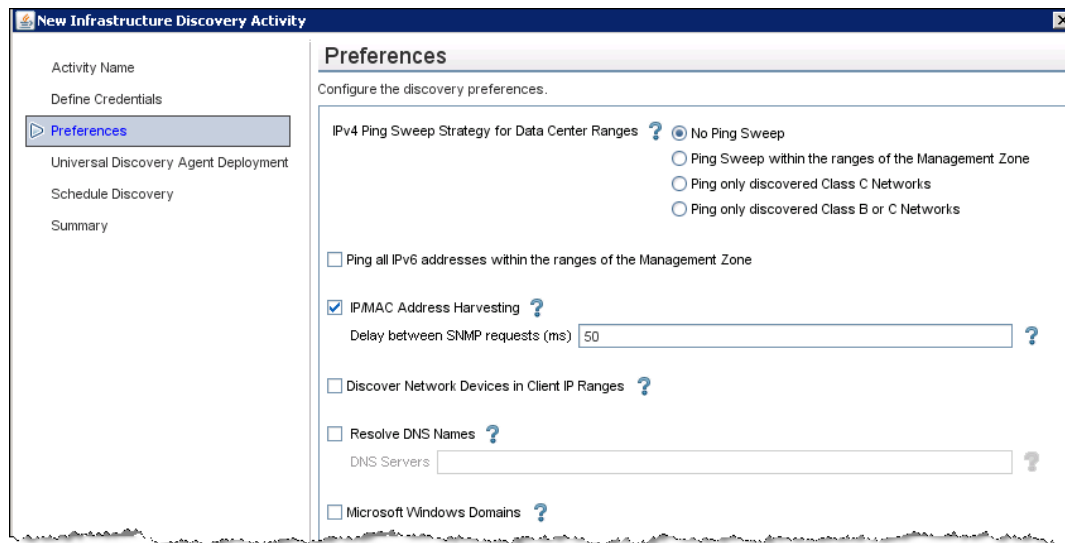
- Create a management zone.

Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery** tab, click **New** , and select **New Management Zone**.

For details on how to create a management zone, see *HP Universal CMDB Data Flow Management Guide*.

- Create an Infrastructure Discovery activity.

- a. Select the management zone that you created, click , and select **New Discovery Activity > Infrastructure**.
- b. On the Define Credentials page, only choose the credential that you need.
- c. If the default Preferences page is not suitable for this mode, you can specify it as follows:



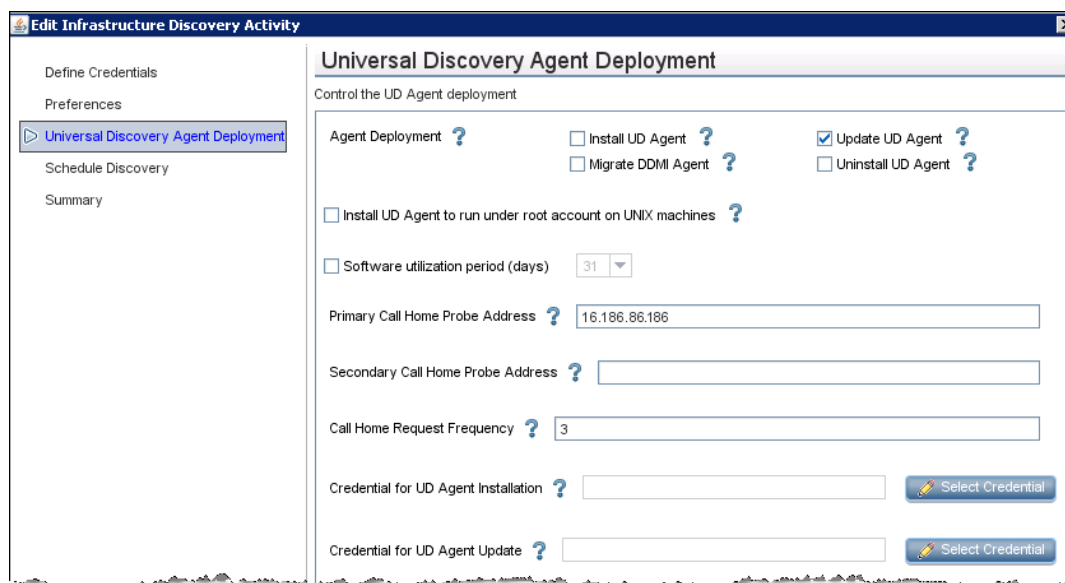
The screenshot shows the 'New Infrastructure Discovery Activity' window with the 'Preferences' tab selected. The left sidebar contains a tree view with 'Preferences' highlighted. The main area is titled 'Preferences' and contains the following settings:

- Activity Name:** (empty field)
- Define Credentials:** (empty field)
- Preferences:** (selected tab)
- Universal Discovery Agent Deployment:** (empty field)
- Schedule Discovery:** (empty field)
- Summary:** (empty field)

The 'Preferences' section includes the following options:

- IPv4 Ping Sweep Strategy for Data Center Ranges:**
 - ☒ No Ping Sweep
 - ☐ Ping Sweep within the ranges of the Management Zone
 - ☐ Ping only discovered Class C Networks
 - ☐ Ping only discovered Class B or C Networks
- ☐ Ping all IPv6 addresses within the ranges of the Management Zone
- ☒ IP/MAC Address Harvesting
 - Delay between SNMP requests (ms):
- ☐ Discover Network Devices in Client IP Ranges
- ☐ Resolve DNS Names
 - DNS Servers:
- ☐ Microsoft Windows Domains

- d. On the Universal Discovery Agent Deployment page, select **Update UD Agent**, and type a Call Home probe address if you want to use the Call Home feature.



The screenshot shows the 'Edit Infrastructure Discovery Activity' window with the 'Universal Discovery Agent Deployment' tab selected. The left sidebar contains a tree view with 'Universal Discovery Agent Deployment' highlighted. The main area is titled 'Universal Discovery Agent Deployment' and contains the following settings:

- Define Credentials:** (empty field)
- Preferences:** (empty field)
- Universal Discovery Agent Deployment:** (selected tab)
- Schedule Discovery:** (empty field)
- Summary:** (empty field)


The 'Universal Discovery Agent Deployment' section includes the following options:

- Agent Deployment:**
 - ☐ Install UD Agent
 - ☒ Update UD Agent
 - ☐ Migrate DDMI Agent
 - ☐ Uninstall UD Agent
- ☐ Install UD Agent to run under root account on UNIX machines
- ☐ Software utilization period (days):
- Primary Call Home Probe Address:**
- Secondary Call Home Probe Address:**
- Call Home Request Frequency:**
- Credential for UD Agent Installation:** [Select Credential](#)
- Credential for UD Agent Update:** [Select Credential](#)

3. Activate the Infrastructure Discovery activity.

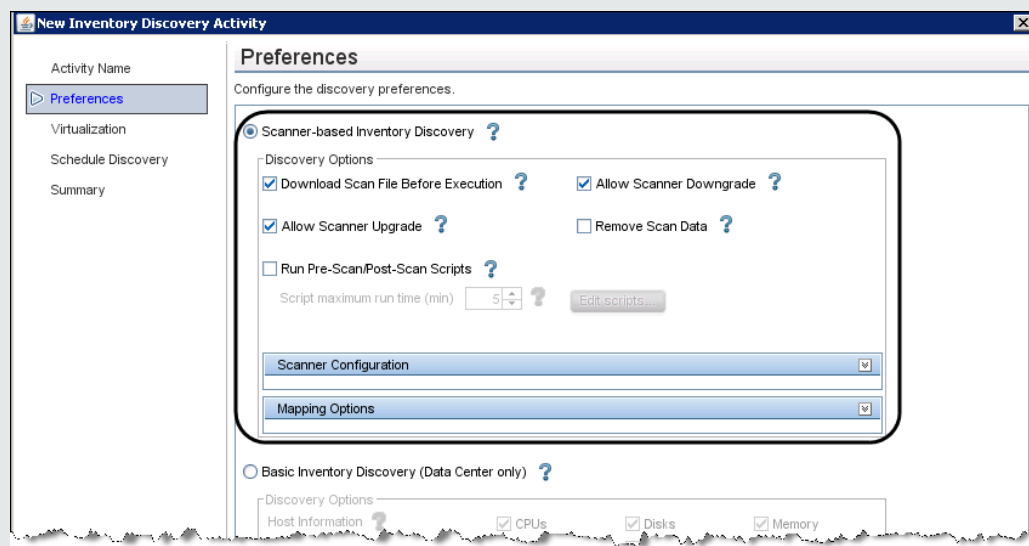
Right-click the Infrastructure Discovery activity that you created, and select **Activate**.

4. Create an Inventory Discovery activity.

Select the management zone that you created, click , and select **New Discovery Activity > Inventory**.

Note:

- Only **Scanner-based Inventory Discovery** is involved here.



- You can skip the Schedule Discovery page, because the **Inventory Discovery by Scanner** job is designed to be run every two weeks and the period cannot be changed.

5. Active the Inventory Discovery activity.

Right-click the Inventory Discovery activity that you created, and select **Activate**.

Configure SNMP-Agent Mode


To configure the SNMP-Agent mode, do the following:

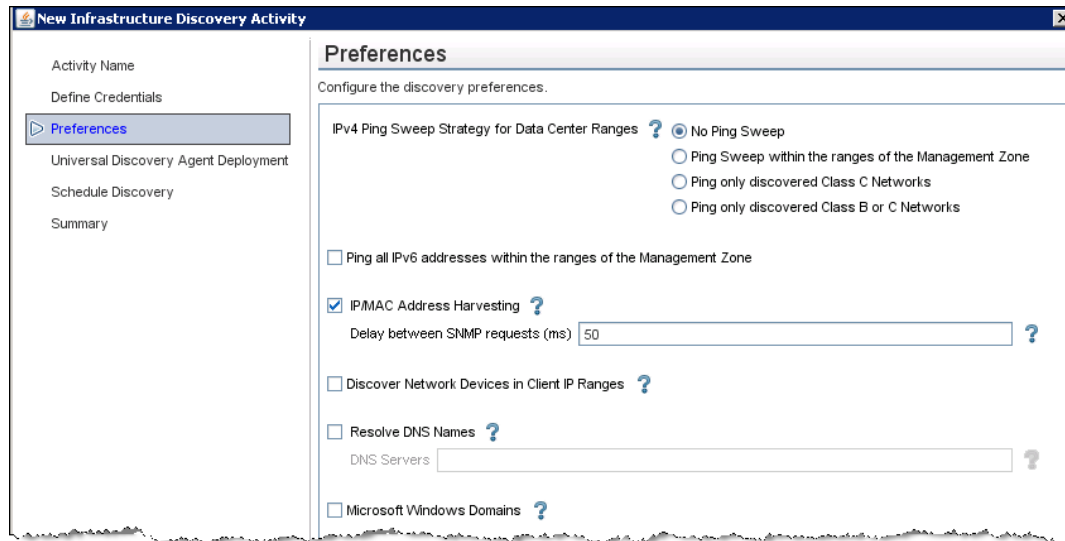
1. Create a management zone.

Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery** tab, click **New** , and select **New Management Zone**.

For details on how to create a management zone, see *HP Universal CMDB Data Flow Management Guide*.

2. Create an Infrastructure Discovery activity.

- a. Select the management zone that you created, click , and select **New Discovery Activity > Infrastructure**.
- b. On the Define Credentials page, only choose the credential that you need.
- c. If the default Preferences page is not suitable for this mode, you can specify it as follows:



New Infrastructure Discovery Activity

Activity Name
Define Credentials
Preferences
Universal Discovery Agent Deployment
Schedule Discovery
Summary

Preferences
Configure the discovery preferences.

IPv4 Ping Sweep Strategy for Data Center Ranges ? ☒ No Ping Sweep
☐ Ping Sweep within the ranges of the Management Zone
☐ Ping only discovered Class C Networks
☐ Ping only discovered Class B or C Networks

☐ Ping all IPv6 addresses within the ranges of the Management Zone

☒ IP/MAC Address Harvesting ?
 Delay between SNMP requests (ms) ?

☐ Discover Network Devices in Client IP Ranges ?

☐ Resolve DNS Names ?
 DNS Servers ?

☐ Microsoft Windows Domains ?

- d. On the Universal Discovery Agent Deployment page, select **Update UD Agent**, and type a Call Home probe address if you want to use the Call Home feature.


The screenshot shows the 'Edit Infrastructure Discovery Activity' window with the 'Universal Discovery Agent Deployment' tab selected. The left sidebar contains links for 'Define Credentials', 'Preferences', 'Universal Discovery Agent Deployment' (highlighted), 'Schedule Discovery', and 'Summary'. The main panel is titled 'Universal Discovery Agent Deployment' and 'Control the UD Agent deployment'. It contains several configuration options:

- Agent Deployment:** Includes checkboxes for 'Install UD Agent', 'Migrate DDMI Agent', 'Update UD Agent' (checked), and 'Uninstall UD Agent'.
- Install UD Agent to run under root account on UNIX machines:** An unchecked checkbox.
- Software utilization period (days):** A dropdown menu set to '31'.
- Primary Call Home Probe Address:** A text field containing '16.186.86.186'.
- Secondary Call Home Probe Address:** An empty text field.
- Call Home Request Frequency:** A text field containing '3'.
- Credential for UD Agent Installation:** An empty text field with a 'Select Credential' button.
- Credential for UD Agent Update:** An empty text field with a 'Select Credential' button.

3. Activate the Infrastructure Discovery activity.

Right-click the Infrastructure Discovery activity that you created, and select **Activate**.

4. Create an Inventory Discovery activity.

Select the management zone that you created, click , and select **New Discovery Activity > Inventory**.

Note:

- Only **Scanner-based Inventory Discovery** is involved here.

The screenshot shows the 'New Inventory Discovery Activity' window with the 'Preferences' tab selected. The 'Scanner-based Inventory Discovery' section is highlighted with a red box. It contains the following options:

- ☒ Download Scan File Before Execution
- ☒ Allow Scanner Upgrade
- ☐ Run Pre-Scan/Post-Scan Scripts
- ☒ Allow Scanner Downgrade
- ☐ Remove Scan Data

Below these options is a section for 'Script maximum run time (min)' with a value of 5 and an 'Edit scripts...' button. Further down are sections for 'Scanner Configuration' and 'Mapping Options'. At the bottom, the 'Basic Inventory Discovery (Data Center only)' section is visible, with options for 'Host Information', 'CPUs', 'Disks', and 'Memory'.

- You can skip the Schedule Discovery page, because the **Inventory Discovery by Scanner** job is designed to be run every two weeks and the period cannot be changed.

5. Active the Inventory Discovery activity.

Right-click the Inventory Discovery activity that you created, and select **Activate**.

Note:


If you use any UCMDB versions before 10.20, do the following in the Client environment, and consult HP Software Support for details.

- Apply Hotfix for virtual IP addresses.
- Apply the Enrichment rule to clean the Call Home event.

Configure SNMP-Agentless Mode


To configure the SNMP-Agentless mode, do the following:

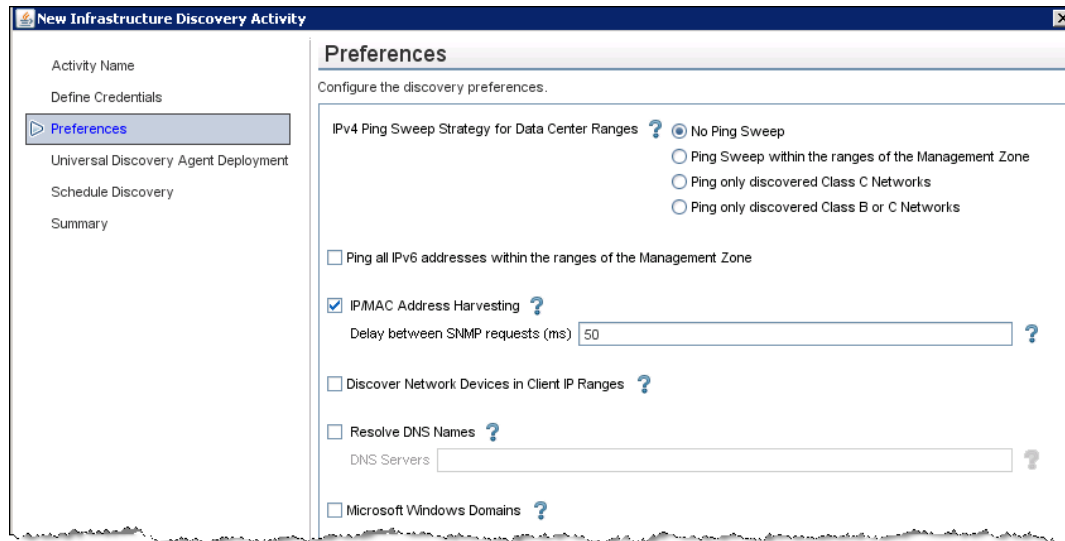
1. Create a management zone.

Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery** tab, click **New** , and select **New Management Zone**.

For details on how to create a management zone, see *HP Universal CMDB Data Flow Management Guide*.

2. Create an Infrastructure Discovery activity.

- a. Select the management zone that you created, click , and select **New Discovery Activity > Infrastructure**.
- b. On the Define Credentials page, only choose the credential that you need.
- c. If the default Preferences page is not suitable for this mode, you can specify it as follows:



New Infrastructure Discovery Activity

Activity Name

Define Credentials

Preferences

Universal Discovery Agent Deployment

Schedule Discovery

Summary

Preferences

Configure the discovery preferences.

IPv4 Ping Sweep Strategy for Data Center Ranges ? ☒ No Ping Sweep

☐ Ping Sweep within the ranges of the Management Zone

☐ Ping only discovered Class C Networks

☐ Ping only discovered Class B or C Networks

☐ Ping all IPv6 addresses within the ranges of the Management Zone

☒ IP/MAC Address Harvesting ?

Delay between SNMP requests (ms) ?

☐ Discover Network Devices in Client IP Ranges ?

☐ Resolve DNS Names ?

DNS Servers ?

☐ Microsoft Windows Domains ?

- d. On the Universal Discovery Agent Deployment page, select **Update UD Agent**, and type a Call Home probe address if you want to use the Call Home feature.


The screenshot shows the 'Edit Infrastructure Discovery Activity' window with the 'Universal Discovery Agent Deployment' tab selected. The left sidebar contains links for 'Define Credentials', 'Preferences', 'Universal Discovery Agent Deployment' (highlighted), 'Schedule Discovery', and 'Summary'. The main panel is titled 'Universal Discovery Agent Deployment' and contains the following controls:

- Agent Deployment** section:
 - ☐ Install UD Agent ?
 - ☒ Update UD Agent ?
 - ☐ Migrate DDMI Agent ?
 - ☐ Uninstall UD Agent ?
- ☐ Install UD Agent to run under root account on UNIX machines ?
- ☐ Software utilization period (days): 31
- Primary Call Home Probe Address ? : 16.186.86.186
- Secondary Call Home Probe Address ? : (empty field)
- Call Home Request Frequency ? : 3
- Credential for UD Agent Installation ? : (empty field) [Select Credential]
- Credential for UD Agent Update ? : (empty field) [Select Credential]

3. Activate the Infrastructure Discovery activity.

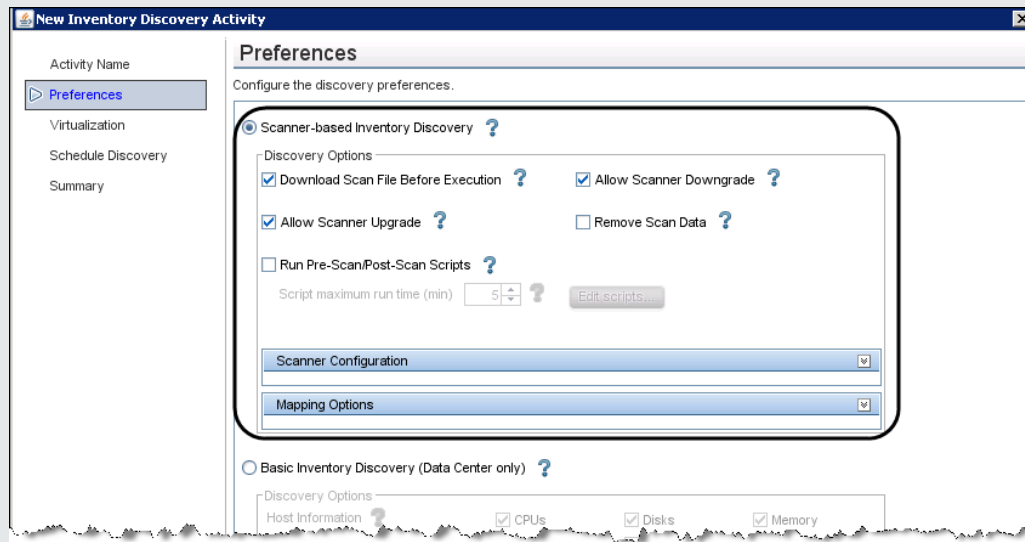
Right-click the Infrastructure Discovery activity that you created, and select **Activate**.

4. Create an Inventory Discovery activity.

Select the management zone that you created, click , and select **New Discovery Activity > Inventory**.

Note:

- Only **Scanner-based Inventory Discovery** is involved here.



- You can skip the Schedule Discovery page, because the **Inventory Discovery by Scanner** job is designed to be run every two weeks and the period cannot be changed.

5. Active the Inventory Discovery activity.

Right-click the Inventory Discovery activity that you created, and select **Activate**.

Note:


If you use any UCMDB versions before 10.20, do the following in the Client environment, and consult HP Software Support for details.

- Apply Hotfix for virtual IP addresses.
- Apply the Enrichment rule to clean the Call Home event.

Configure SNMP-Combined Mode


To configure the Combined mode, do the following:

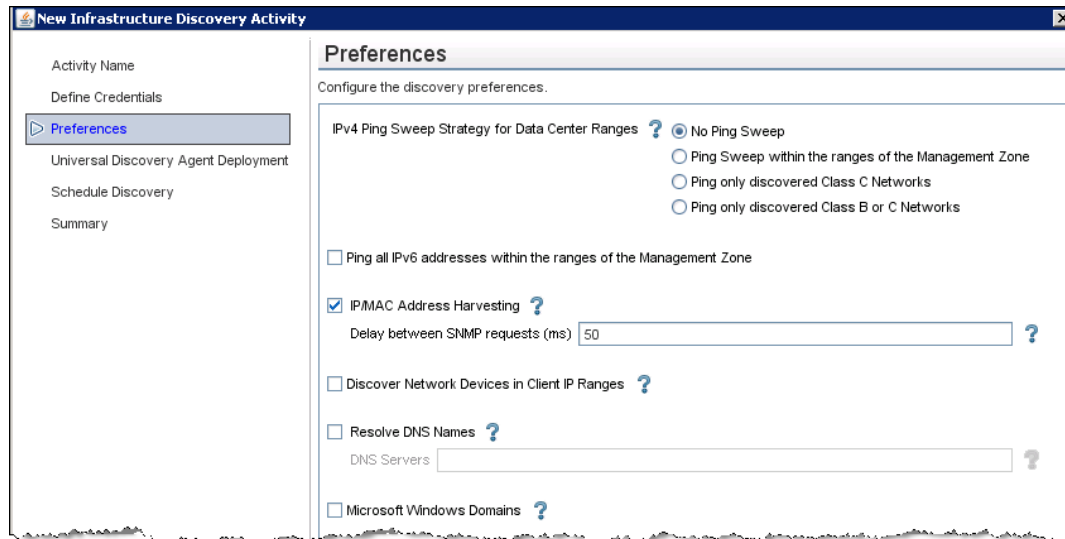
1. Create a management zone.

Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery** tab, click **New** , and select **New Management Zone**.

For details on how to create a management zone, see *HP Universal CMDB Data Flow Management Guide*.

2. Create an Infrastructure Discovery activity

- a. Select the management zone that you created, click , and select **New Discovery Activity > Infrastructure**.
- b. On the Define Credentials page, select **NTCMD Protocol** and **SSH Protocol** to respectively cover Windows and Non-Windows (Unix, Linux, Solaris, and so on) devices.
- c. If the default Preferences page is not suitable for this mode, you can specify it as follows:



New Infrastructure Discovery Activity

Activity Name
Define Credentials
Preferences
Universal Discovery Agent Deployment
Schedule Discovery
Summary

Preferences
Configure the discovery preferences.

IPv4 Ping Sweep Strategy for Data Center Ranges ? ☒ No Ping Sweep
☐ Ping Sweep within the ranges of the Management Zone
☐ Ping only discovered Class C Networks
☐ Ping only discovered Class B or C Networks

☐ Ping all IPv6 addresses within the ranges of the Management Zone

☒ IP/MAC Address Harvesting ?
 Delay between SNMP requests (ms) ?

☐ Discover Network Devices in Client IP Ranges ?

☐ Resolve DNS Names ?
 DNS Servers ?

☐ Microsoft Windows Domains ?

- d. On the Universal Discovery Agent Deployment page, select **Install UD Agent**, **Update UD Agent** and **Install UD Agent to run under root account on UNIX machines**, and type a Call Home probe address if you want to use the Call Home feature.


The screenshot shows the 'Edit Infrastructure Discovery Activity' window with the 'Universal Discovery Agent Deployment' tab selected. The left sidebar contains a tree view with 'Universal Discovery Agent Deployment' highlighted. The main panel is titled 'Universal Discovery Agent Deployment' and contains the following settings:

- Control the UD Agent deployment**
 - Agent Deployment**
 - ☒ Install UD Agent
 - ☐ Migrate DDMI Agent
 - ☒ Update UD Agent
 - ☐ Uninstall UD Agent
 - ☒ Install UD Agent to run under root account on UNIX machines
 - ☐ Software utilization period (days): 31
 - Primary Call Home Probe Address: 16.186.86.186
 - Secondary Call Home Probe Address: (empty)
 - Call Home Request Frequency: 3
 - Credential for UD Agent Installation: Universal Discovery Protocol Credential 1 (with 'Select Credential' button)
 - Credential for UD Agent Update: Universal Discovery Protocol Credential 1 (with 'Select Credential' button)

3. Activate the Infrastructure Discovery activity.

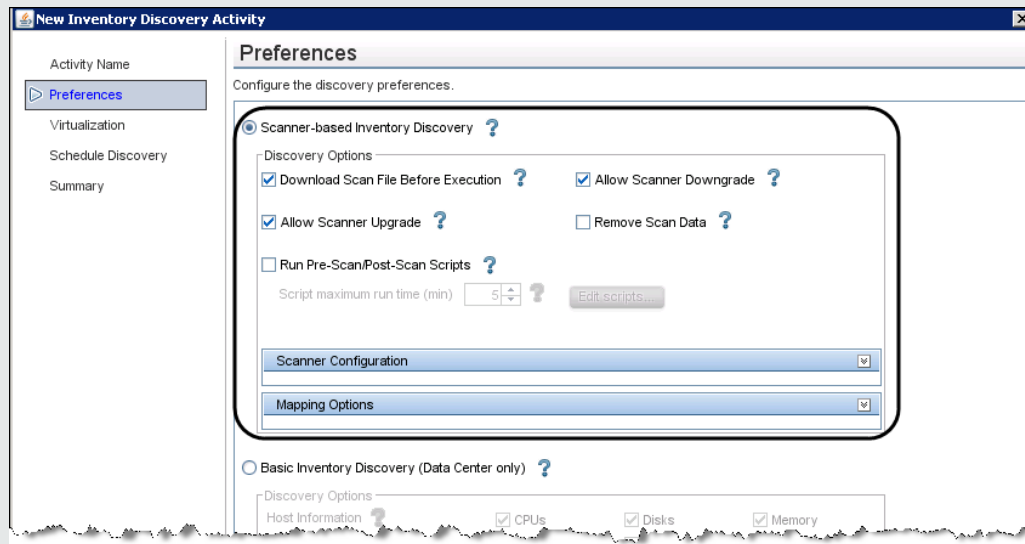
Right-click the Infrastructure Discovery activity that you created, and select **Activate**.

4. Create an Inventory Discovery activity.

Select the management zone that you created, click , and select **New Discovery Activity > Inventory**.

Note:

- Only **Scanner-based Inventory Discovery** is involved here.



- You can skip the Schedule Discovery page, because the **Inventory Discovery by Scanner** job is designed to be run every two weeks and the period cannot be changed.

5. Active the Inventory Discovery activity.

Right-click the Inventory Discovery activity that you created, and select **Activate**.

Note:


If you use any UCMDB versions before 10.20, do the following in the Client environment, and consult HP Software Support for details.

- Apply Hotfix for virtual IP addresses.
- Apply the Enrichment rule to clean the Call Home event.

Configure No-SNMP Mode


To configure the No-SNMP mode, do the following:

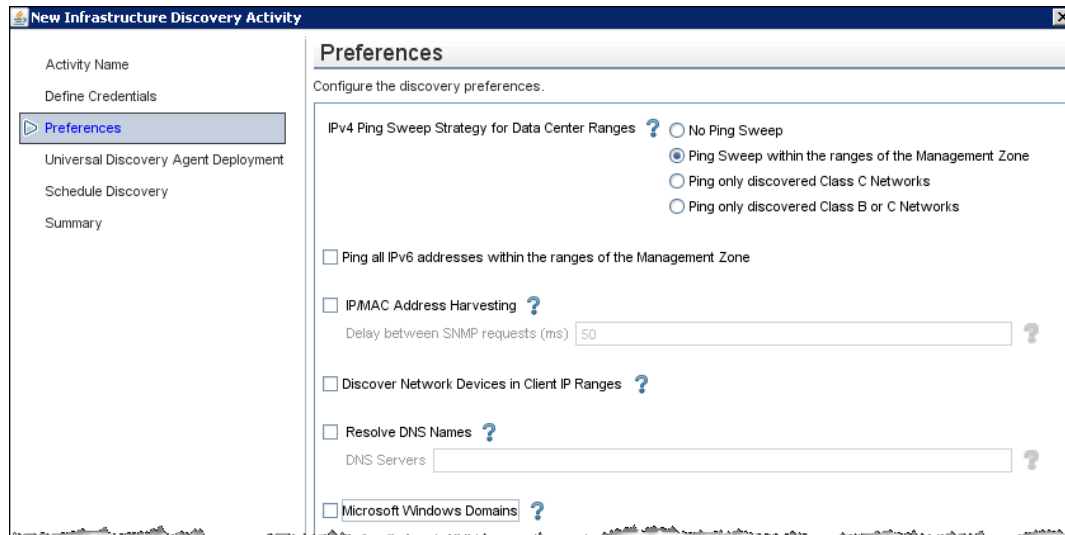
1. Create a management zone.

Go to **Data Flow Management > Universal Discovery > Zone-Based Discovery** tab, click **New** , and select **New Management Zone**.

For details on how to create a management zone, see *HP Universal CMDB Data Flow Management Guide*.

2. Create an Infrastructure Discovery activity.

- a. Select the management zone that you created, click , and select **New Discovery Activity > Infrastructure**.
- b. On the Define Credentials page, only choose the credential that you need.
- c. If the default Preferences page is not suitable for this mode, you can specify it as follows:



New Infrastructure Discovery Activity

Activity Name
Define Credentials
Preferences
Universal Discovery Agent Deployment
Schedule Discovery
Summary

Preferences
Configure the discovery preferences.

IPv4 Ping Sweep Strategy for Data Center Ranges ?
☐ No Ping Sweep
☒ Ping Sweep within the ranges of the Management Zone
☐ Ping only discovered Class C Networks
☐ Ping only discovered Class B or C Networks

☐ Ping all IPv6 addresses within the ranges of the Management Zone

☐ IP/MAC Address Harvesting ?
 Delay between SNMP requests (ms) 50 ?

☐ Discover Network Devices in Client IP Ranges ?

☐ Resolve DNS Names ?
 DNS Servers ?

☐ Microsoft Windows Domains ?

- d. On the Universal Discovery Agent Deployment page, select **Update UD Agent**, and type a Call Home probe address if you want to use the Call Home feature.


The screenshot shows the 'Edit Infrastructure Discovery Activity' window with the 'Universal Discovery Agent Deployment' tab selected. The left sidebar contains links for 'Define Credentials', 'Preferences', 'Universal Discovery Agent Deployment' (highlighted), 'Schedule Discovery', and 'Summary'. The main panel is titled 'Universal Discovery Agent Deployment' and contains the following controls:

- Agent Deployment** section:
 - ☐ Install UD Agent ?
 - ☒ Update UD Agent ?
 - ☐ Migrate DDMI Agent ?
 - ☐ Uninstall UD Agent ?
- ☐ Install UD Agent to run under root account on UNIX machines ?
- ☐ Software utilization period (days) : 31
- Primary Call Home Probe Address : 16.186.86.186
- Secondary Call Home Probe Address : (empty field)
- Call Home Request Frequency : 3
- Credential for UD Agent Installation : (empty field) [Select Credential]
- Credential for UD Agent Update : (empty field) [Select Credential]

3. Activate the Infrastructure Discovery activity.

Right-click the Infrastructure Discovery activity that you created, and select **Activate**.

4. Create an Inventory Discovery activity.

Select the management zone that you created, click , and select **New Discovery Activity > Inventory**.

Note:

- Only **Scanner-based Inventory Discovery** is involved here.

New Inventory Discovery Activity

Activity Name

Preferences

Virtualization

Schedule Discovery

Summary

Preferences

Configure the discovery preferences.

Scanner-based Inventory Discovery

Discovery Options

☒ Download Scan File Before Execution

☒ Allow Scanner Upgrade

☐ Run Pre-Scan/Post-Scan Scripts

Script maximum run time (min) 5

☒ Allow Scanner Downgrade

☐ Remove Scan Data

Scanner Configuration

Mapping Options

Basic Inventory Discovery (Data Center only)

Discovery Options

Host Information

☒ CPUs

☒ Disks

☒ Memory

- You can skip the Schedule Discovery page, because the **Inventory Discovery by Scanner** job is designed to be run every two weeks and the period cannot be changed.

5. Active the Inventory Discovery activity.

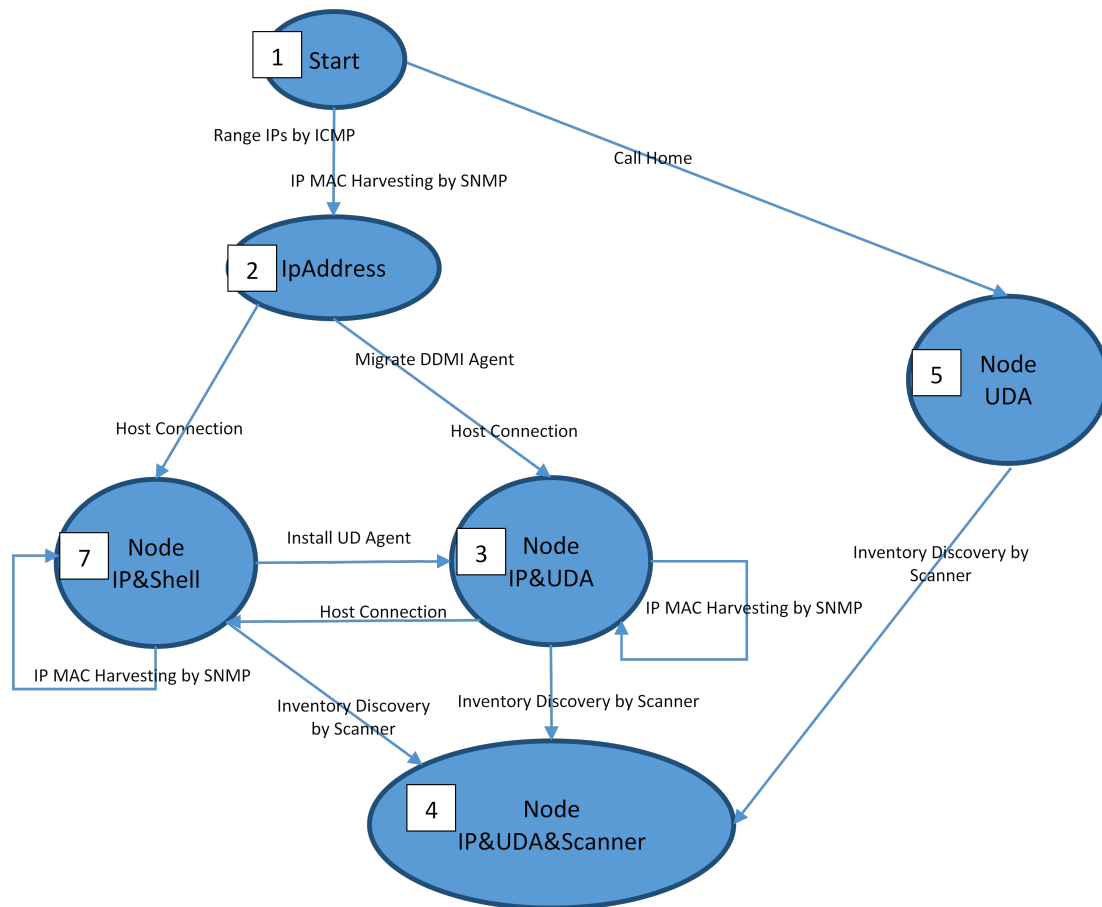
Right-click the Inventory Discovery activity that you created, and select **Activate**.

Step-by-Step Configuration for Experienced Users

This task describes the procedure of step-by-step configuration for experienced users only.

1. CI Status transition

The following diagram is the fundamental idea of the step-by-step configuration.



In this diagram, the discovery status is defined by picking up some combination of key CIs. Those CIs play an important role in triggering fundamental jobs.

All the discovery modes mentioned above are included in this diagram, for example:

Agent-Only Mode: 1 (Range IPs by ICMP) > 2 (Host Connection by Shell) > 3 (Inventory Discovery by Scanner) > 4

Agentless Mode: 1 (Range IPs by ICMP) > 2 (Host Connection by Shell) > 7 (Inventory Discovery by Scanner) > 4

Combine Mode: 1 (Range IPs by ICMP) > 2 (Host Connection by Shell) > 7 (Inventory Discovery by Scanner) > 3 (Install UD Agent) > 4

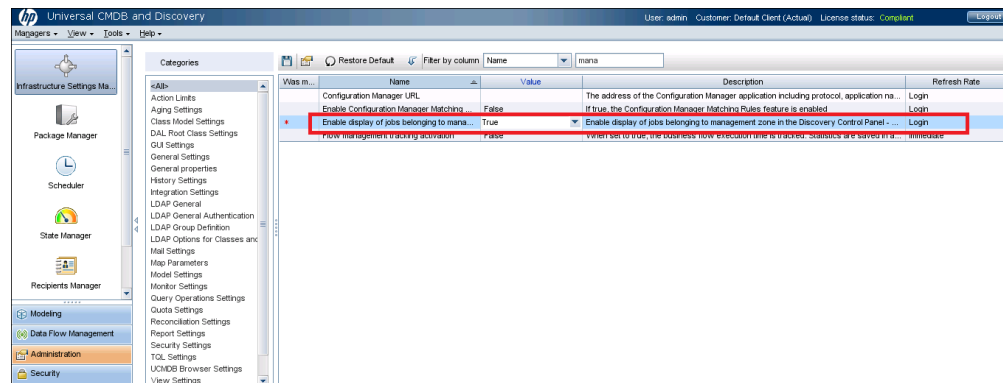
SNMP-Agent Mode: 1 (IP MAC Harvesting by SNMP) > 2 (Host Connection by Shell) > 3 (Inventory Discovery by Scanner) > 4

2. Step-by-step discovery

- a. Decide the mode that you want to use for discovery.
- b. Configure the mode. For details, see the relevant section in ["Configure Inventory Discovery" on page 44](#).
- c. Modify the job.

The default activated job may be inappropriate, so you must manually disable the unnecessary job according to the environment.

- i. Go to **Administration > Infrastructure Settings Management**, and change the value of the **Enable display of jobs belonging to management zone** attribute to **True**.



- ii. Go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab > **Discovery Modules** tree, and activate or deactivate jobs under **<< No module>>**.

Note:

- When you edit the activity, it is recommended to deactivate unrelated jobs under **<< No module>>** to keep your system robust.

- Do not start a job until its precedent job finishes.
- Use the right-hand pane to troubleshoot when jobs fail or do not return the expected CIs for the next job to be triggered.

How to Migrate DDMI Agents to Universal Discovery Agents


This task describes how to migrate DDMI agents to Universal Discovery agents.

Agents can be migrated using automatic, semi-automatic, or manual methods.

• Automatic migration

Agent migration is performed automatically using activities in UCMDB.

In UCMDB, configure the Infrastructure Discovery activity as follows:

- a. On the Universal Agent Deployment page, ensure the **Migrate DDMI Agent** check box is selected.
- b. On the Summary page, save the changes and click  on the toolbar to activate the activity.

For more information, see the section describing the Infrastructure Discovery Activity in ["Configure Inventory Discovery" on page 44](#).

Note: In this method, the **Migrate DDMI Agent** job can trigger all single IP addresses with no Node related. This operation can cause performance issues if you have the dynamic environment.

• Semi-automatic migration

Agent migration is performed semi-automatically. Besides using activities in UCMDB, you can manually activate the **Migrate DDMI Agent** job. If no DDMI agent remains in the environment, this job can be deactivated. For details on modifying the job, see ["Step-by-Step Configuration for Experienced Users" on page 68](#).

Note: It is recommended to use this method if you want to control the migration closely.

- **Manual migration**

Agent migration is performed manually using remote access technology, third-party tools, or any other distribution method.

- a. Uninstall the DDMI agents. For details, see the documentation that was supplied with your version of DDMI.
- b. Install the Universal Discovery agent manually. For details, see the section describing how to install the Universal Discovery agent manually in *HP Universal CMDB Data Flow Management Guide*.

Note: (UNIX) To remove legacy customized start-up scripts during migration, see the section describing ["How to Clean Up Legacy DDMI Agent Start-Up Scripts"](#) on page 80.

Check the Migration Status

When you begin to migrate Universal Discovery agents, you can perform the following steps to check the migration status:

1. Run the **UDA Status Collector** job.

Go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab > **Discovery Modules** tree > **Tools and Samples > UD Agent Management**, right-click **UDA Status Collector**, and select **Activate**.

2. Check the **Agent Status Report**.

Go to **Modeling > Reports > Custom Reports** pane > **Custom** tree > **Discovery Status**, double-click **Agent Status Report**. For details, see the *How to Generate a Custom Report* section in *HP Universal CMDB Modeling Guide*.

How to Configure DDMI and Universal Discovery for Interoperability

This task describes how configure Universal Discovery agents to interoperate with DDMI and Universal Discovery in a phased migration approach.

The Universal Discovery Agent can be utilized by both the DDMI server and the Universal Discovery Data Flow Probe for discovery and inventory.

In this mode, Universal Discovery agents provide inventory data to DDMI servers. However, only shell communication capabilities are provided to Data Flow Probes.

Note: In UCMDB 10.01, the scan file can be collected by both DDMI and Universal Discovery. In UCMDB 10.20, this feature is disabled. Universal Discovery cannot collect the scan file, and the Universal Discovery Agent only works as a shell command. Contact HP Software Support if you want the scan file on the Universal Discovery side.

This task includes the following steps:

1. ["Prerequisites" below](#)
2. ["Configure Universal Discovery" below](#)
3. ["Configure DDMI" on the next page](#)
4. ["Results " on the next page](#)

1. Prerequisites
 - Ensure that the DDMI server database is running.
 - Ensure that UCMDB is running.
2. Configure Universal Discovery
 - **Zone Based Activities.** In the **Inventory Discovery** wizard on the **Preferences** page, ensure that **Scanner Based Inventory** is not selected.
 - **Manual.** Ensure that you do not run the **Inventory Discovery by Scanner** job.

Note:

- Universal Discovery cannot perform scanner-based inventory discovery during a phased migration period. During this period, only DDMI can perform a scanner-based inventory discovery. You can enable scanner-based inventory discovery or run scanner-based inventory discovery after DDMI is retired.

- For details on configuring activities and on configuring jobs manually, see *HP UCMDB Discovery and Integrations Content Guide* and the *HP Universal CMDB Data Flow Management Guide* respectively.

3. Configure DDMI

- a. **Install scanner patch.** Apply the latest patch to the DDMI server. Download the patch from the [HP Software Support Online Portal](http://support.openview.hp.com/selfsolve/patches) (<http://support.openview.hp.com/selfsolve/patches>). Search for **DDMI > Cumulative Scanner Patches**.
- b. **Set Agent Communications options.** **DDMI > Server > Administration > Discovery Configuration > Configuration Profiles > Agent Configuration Profiles > Settings** tab.
 - i. Ensure that **Allow Agent Upgrade** is not selected.
 - ii. Ensure that **Allow Agent Communication** is selected. Additionally, in the **Agent deployment actions** drop down, select **No action**.
- c. **Restart the system monitor service.** Stop and restart the **HP DDMI System Monitor** service on the server that is running DDMI.

4. Results

- The Universal Discovery agent can provide services to both the DDMI server and UCMDB.
- The software utilization plug-in runs according to the **collect utilization data** setting for your DDMI server.

Chapter 4: After Migration

This chapter includes:

How to Run the Device Inventory Report	75
How to Import DDMI SAls to UCMDB	76

How to Run the Device Inventory Report

This task describes how to run the Device Inventory Report. This report is useful for troubleshooting device migration issues. For example, if you notice that certain devices or certain components were not migrated to Universal Discovery, this report will show the possible reasons.

1. Prerequisites

UCMDB server is running.

2. Copy the script

Copy the script file from the following location in UCMDB to each DDMI Server you want to migrate: **<UCMDB Server> Tools folder > Migration folder > DDMIInventoryReport.pl**

3. Run the script

On the DDMI Server, open a command line shell and type the following at the command prompt:

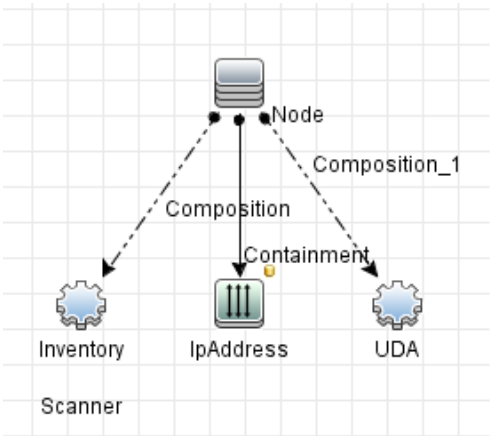
```
perl DDMIInventoryReport.pl
```

4. Results

- Summary data about each device is displayed.
- A file is created that contains detailed information about each device. The format for the file is as follows: **<DDMIServerName>.csv**

where **<DDMIServerName>** is the name created for each DDMI Server.

- After the migration is complete, analyze the summary data and the accompanying .csv file. Compare the data to the data in UCMDB. To do this, you can create customized TQL queries in UCMDB to ensure that devices were migrated as expected. For example, the following TQL query may be used:



Note: This example assumes that all device information is current and available in DDMI. Customize this topology to suit your specific conditions.

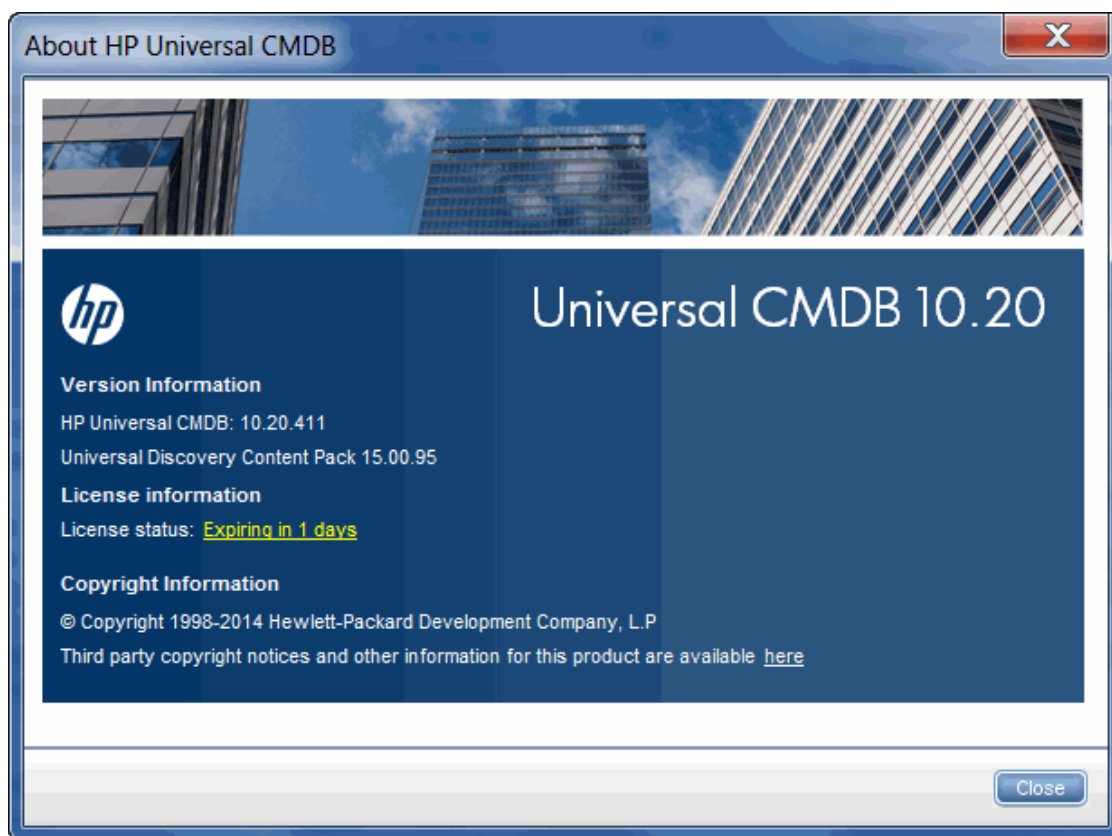
Null or inconsistent data in the .csv file may yield answers why certain information was not migrated as follows:

Issue	Result
Agent Version value is null	Universal Discovery Agent is not migrated
Scan File value is null	Inventory Scanner is not migrated
Scan Date value is less than two months before migration date.	Inventory Scanner may not be migrated

How to Import DDMI SAls to UCMDB

To import the latest DDMI SAls to UCMDB,

1. Download the latest DDMI 9.32 DK package.
 - a. Download the latest DDMI 9.32 DK package (**HPED_XXXXX.zip**) from the [Discovery Knowledge Packs for DDMI](#) community on HP Live Network.
 - b. Extract the zip file to get the SAI summary html files and **DiscoveryKnowledge-9.3.XXXX.cab**.
 - c. Then extract the **DiscoveryKnowledge-9.3.XXXX.cab** file to get the Master SAI files.
2. Check the current UCMDB and Content Pack update versions by going to **Help > About HP Universal CMDB** in UCMDB.



3. Create a new .dat file with a file name **version.dat**
 - a. Add the file content in the following format:

```
<CP_version>-minVersion=<UCMDB_version>
```

For example, Based on the version information available from the screenshot above, the file content is as follows:

```
15.00.95-minVersion=10.2
```

- b. Modify the CP version in the **version.dat** file to make sure the version is higher than the current CP version. The new version does not have to be a real version number. The purpose is to enable the import.

For example, if the current content is 15.00.95-minVersion=10.2, modify it to something like 15.0**1**.95-minVersion=10.2.

- c. Save the file.

4. Create fake CP packages with the SAI files you get from the DDMI DK package, so that the SAI files can be imported like you are importing them from real CP packages.

Create two zip packages (**SAI.zip** and **SAI_HTML-summary.zip**) to include the SAIs and the SAI HTML files. Make sure you follow the folder structures below strictly:



```
SAI.zip
- packages
  - Sai.zip
    - discoverySaiResources
      - BaseUnixOS.zsai
      - French.zsai
      - German.zsai
      - Legacy.zsai
      - Mac.zsai
      - Master.zsai
      - Unix.zsai
  - version.dat
```

```
SAI_HTML-summary.zip
- discoverySaiResources
  - SAI_DOC
    - BaseUnixOS-summary.html
    - French-summary.html
    - German-summary.html
    - Legacy-summary.html
    - Mac-summary.html
    - Master-summary.html
    - Unix-summary.html
```

5. Import the **SAI.zip** and **SAI_HTML-summary.zip** packages.

- a. Go to **Data Flow Management > Software Library**.

- b. In the SAI Files pane, click **Import**  and select **Import SAI From CP**.

- c. In the Import CP Files dialog box, locate the **SAI.zip** package you created and click **Open**.
- d. Go to **Administration > Package Manager**.
- e. Click **Deploy packages to server (from local disk)** .
- f. In the Deploy Packages to Server dialog box, click **Add** .
- g. In the Deploy packages to server (from local disk) dialog box, locate the **SAI_HTML-summary.zip** package you created and click **Open**.
- h. Click **Deploy**.

Note: Once you upgrade the UCMDB to a newer version, the SAls and SAI HTML summary files you imported will be replaced by the newer ones in the UCMDB.

Chapter 5: Reference Information

This chapter includes:

How to Clean Up Legacy DDMI Agent Start-Up Scripts	80
Server Configuration Data Export Script Resources	82
Universal Discovery Resources for UNIX	83
Universal Discovery Resources for Windows	87
Server Configuration Data Import Troubleshooting	89
Terminology Changes from DDMI to Universal Discovery	90
Migrated Reports from DDMI to Universal Discovery	96
Mapping Attributes from DDMI to UCMDB	97
Java Viewer Mapping from DDMI to Universal Discovery	106

How to Clean Up Legacy DDMI Agent Start-Up Scripts

This task describes how to remove any customized start-up scripts that may be running on UNIX discovery nodes. You may need to remove these scripts when you have removed DDMI agents and are installing Universal Discovery agents.

Note: Perform this task only if you have legacy start-up scripts.

This task includes the following steps:

1. ["Prerequisites " on the next page](#)
2. ["Export the installation file" on the next page](#)
3. ["Edit the installation file" on the next page](#)
4. ["Copy the script to the remote node" on the next page](#)
5. ["Results " on page 82](#)

1. Prerequisites

Customized start-up scripts for DDMI agents are installed on the discovery nodes that you want to migrate.

2. Export the installation file

- a. In UCMDB, go to **Administration > Package Manager** and export the **UDAgentManagement** archive file.
- b. From the **discoveryResources\ud_agents** directory, extract the **agentinstall.sh** file.

Note: For more information on exporting resources, see the section describing exporting resources using the Package Manager in the *HP Universal CMDB Administration Guide*.

3. Edit the installation file

Edit the **agentinstall.sh** file as follows:

- a. In the line **#DDMI_SCRIPT_FILE=/tmp/sample_script.sh**, replace the placeholder **/tmp/sample_script.sh** with the path to your customized startup script that you want to remove. Then, uncomment the line.
- b. Uncomment the next four lines of code.

4. Copy the script to the remote node

Automatic.

Using the Package Manager, deploy the newly-edited **agentinstall.sh** file to UCMDB.

Note: For more information, see the section describing deploying packages using the Package Manager in the *HP Universal CMDB Administration Guide*. You can deploy specific resources without deploying the entire package. See the sub-section describing how to deploy specific resources.

Manual.

Copy the **agentinstall.sh** file, together with other Universal Discovery Agent installation files and certificate files, to the remote machine.

Note: For more information, see the section describing how to copy the UD Agent installation and the UD Protocol certificate in *HP Universal CMDB Data Flow Management Guide*.

5. Results

To confirm that your customized startup script for the DDMI agent is removed, go to the path that you specified in the **agentinstall.sh** file and verify the start-up script is removed.

Server Configuration Data Export Script Resources

The Perl export script that is used for exporting data from DDMI is named as follows:

DDMIMigration.pl

The following command options are available:

Option	Description
-filename	<p>Changes the name of the archive (.zip) file.</p> <p>Note: It is not recommended to use this option to change file names for files that are contained in the archive.</p> <p>Tip: You can also change the name of the archive file by using the operating system.</p>
-scancfgprefix	<p>By default, the host name of the DDMI server is appended as a prefix to each scanner configuration file. This option replaces this host name with the specified value.</p> <p>Note: This option can only be used for scanner configuration files.</p>
-help	<p>Displays copyright information and command line usage instructions. Additionally, help messages are displayed.</p>

The following is an example command:

```
perl DDMIMigration.pl -filename:samplefile.zip
```

Universal Discovery Resources for UNIX

Resources

The following script files are available for manual agent installations and upgrades:

Platform	Resource Name	Description
UNIX	agentinstall.sh	<ul style="list-style-type: none"> Installs the Universal Discovery Agent. Replaces the non-native version of the UD Agent with a version that is packaged in the native operating system version of the discovery node.
	agentupgrade.sh	Upgrades the DDMI agent to a Universal Discovery agent. However, this version of the Universal Discovery agent is not packaged in the native operating system version of the discovery node.

These files are available in the **Package Manager**. For more information on exporting resources, see *How to Export a Package in the HP Universal CMDB Administration Guide*.

Additionally, discovery resources for UNIX and the UNIX variants that are also available in the **Package Manager** are as follows:

Operating System	Platform	File Name
HP-UX	ia64	hp-ud-agent-hpux-ia64.depot
	HPPA	hp-ud-agent-hpux-hppa.depot
Linux (Red Hat, SUSE, CentOS, Oracle)	x86,x64	hp-ud-agent-linux-x86.rpm
Linux (Ubuntu)	x86,x64	hp-ud-agent-linux-x86.deb
AIX	POWER	hp-ud-agent-aix-ppc.bff
Solaris	x86	hp-ud-agent-solaris-x86.i86pc
	SPARC	hp-ud-agent-solaris-sparc.sparc
Mac OS X	x86	hp-ud-agent-macosx-x86.dmg

Parameters

You can use parameters in a command line interface to customize the discovery installation as follows:

```
filename [--help] [--url0 ipaddress] [--url1 ipaddress] [--url2 ipaddress] [--port number] [--timeout
seconds] [--cert path] [--usage] [--softwareutilization] [--softwareutilizationonly] [--period days] [--
home path] [--upgrade] [--uninstall] [--clean] [--temp] [--user] [--group] packagename

--isnative
```

where:

Parameter Name	Description
cert	Path to install certificate files. Default: Working directory
clean	Specifies a type of uninstall procedure. Most Universal Discovery Agent files and scanner files are deleted. Note: This parameter can only be used together with the uninstall and home parameters.
filename	The name of the installation file. Note: <ul style="list-style-type: none"> This is a mandatory parameter. The filename is usually agentinstall.sh.
group	Specifies the group name for the user account that you want to run the Universal Discovery Agent under. Note: Use this parameter together with the user parameter.
help	Displays help messages.
home	Directory that contains the Universal Discovery Agent log and the software utilization data files. Default: HOME directory
packagename	Full path for the package installation file. Default: Working directory

Parameter Name	Description
	<p>Note: This parameter is required when installing or upgrading the Universal Discovery Agent.</p>
period	<p>Number of days to retain software utilization data.</p> <p>Default: 365 days</p>
port	<p>Port number for the Universal Discovery Agent to use for communication with the Data Flow Probe.</p> <p>Type 2738 or 7738</p> <p>Default: 2738</p> <p>Note: If you change this port number manually after installation, the new port number takes effect only after the Universal Discovery Agent is restarted.</p>
softwareutilization	Enables software utilization.
softwareutilizationonly	<p>Enables the Software Utilization plug-in only.</p> <p>Note:</p> <ul style="list-style-type: none"> • The Universal Discovery Agent is disabled. • This parameter is supported only when installing the Universal Discovery Agent manually.
temp	<p>Directory that contains Universal Discovery Agent and scanner temporary files.</p> <p>Default: \$TEMP directory.</p>
timeout	<p>Frequency (in seconds) that the Universal Discovery Agent contacts the Data Flow Probe for Call Home.</p> <p>Default: 86400 seconds</p>
uninstall	<p>Uninstalls the Universal Discovery Agent.</p> <p>Note: When you use this parameter:</p> <ul style="list-style-type: none"> • All parameters except the clean parameter are ignored.

Parameter Name	Description
	<ul style="list-style-type: none"> The filename parameter is required.
upgrade	Upgrades the Universal Discovery Agent.
url0 url1 url2	IP address for Data Flow Probe that is used for Call Home messages. Note: If you are performing a migration from DDMI to Universal Discovery, this parameter is also used for the DDMI server.
usage	Displays help messages. Note: This parameter provides the same information as the help parameter.
user	The user account that is used to start up the Universal Discovery Agent.
isnative	Returns whether a native or non-native Universal Discovery Agent is installed.

Universal Discovery Agent Error Codes

The following error codes may be returned when using installation or upgrade scripts as follows:

Error Code	Description
1	General error
2	Wrong parameter
3	Not root user
4	File creation error
5	Wrong platform
6	Install package error
7	Directory missing
8	File missing
9	File not executable

Error Code	Description
10	Link startup script error
11	Startup script error
12	Universal Discovery Agent is already installed Note: Applicable only when performing an installation operation.
13	System package installer error
14	Run agent with non-root user error
15	The DDMI agent is installed.

Universal Discovery Resources for Windows

Resources

Discovery resources for Windows are as follows:

Platform	Resource Name	Description
Windows (x86)	hp-ud-agent-win32-x86- <VersionNumber> .msi	This installer package is required for all installations.
	agentupgrade.cmd	Used when upgrading or migrating DDMI agents to Universal Discovery Agents.

Parameters

You can use parameters in a command line interface to customize the Universal Discovery Agent installation, uninstallation, or upgrade as follows.

```
c:\AgentTest>msiexec <InstallOption> <Product.msi> /log <UPGRADELOGFILEPATH> [CLEAN=ON]
SETUPTYPE=Enterprise PORT=7738 TIMEOUT=900 CERTPATH=c:\ PERIOD=90
SOFTWAREUTILIZATION=ON URL0=15.178.179.124 URL1=15.178.179.125 URL2=15.178.179.126
```

Parameter Name	Description
InstallOption	Indicates the type of operation. The following options are supported:

Parameter Name	Description
	<ul style="list-style-type: none"> • /i: Installs the Universal Discovery Agent. • /x: Uninstalls the Universal Discovery Agent.
Product.msi	<p>Indicates the product file name.</p> <p>For example, hp-ud-agent-win32-x86-10.20.000.xxx.msi</p>
UPGRADELOGFILEPATH	<p>Specify a path to save a log file.</p> <p>Note:</p> <ul style="list-style-type: none"> • Only use with the agentupgrade.cmd script. • Use together with the /log switch.
CLEAN	<p>Indicates the type of uninstall procedure. Most Universal Discovery Agent files and scanner files are deleted.</p> <p>Note:</p> <ul style="list-style-type: none"> • This parameter must be used together with the uninstall option. • If you do not want to use this option, omit the parameter from the string.
SETUPTYPE	<p>Indicates the operational mode.</p> <p>Type Enterprise or Manual.</p> <p>Note: The manual parameter value is called "Software Utilization Plug In Only" in the Agent Installation Wizard User Interface.</p>
PORT	<p>Port number for Universal Discovery Agent to use for communication with Data Flow Probe.</p> <p>Type 2738 or 7738.</p> <p>Note: The default value is 2738. If you change this port number manually after installation, the new port number takes effect only after the Universal Discovery Agent is restarted.</p>
TIMEOUT	Frequency that the Universal Discovery Agent contacts the Data Flow Probe

Parameter Name	Description
	<p>when the Universal Agent sends Call Home messages.</p> <p>Measured in seconds.</p> <p>Default is 86400 seconds.</p> <p>Note: This parameter is called Call Home Frequency in the Infrastructure Discovery activity.</p>
CERTPATH	<p>Path to install certificate files.</p> <p>Default is the working directory.</p>
PERIOD	<p>Number of days to retain software utilization data.</p> <p>Default is 365 days.</p>
SOFTWAREUTILIZATION	<p>Enable or disable Software Utilization plug in.</p> <p>Use "ON" to enable and "OFF" to disable.</p> <p>Default is "OFF".</p>
URL0 URL1 URL2	<p>IP address for Data Flow Probe that is used for Call Home messages.</p> <p>Note: If you are performing a migration from DDMI to Universal Discovery, this parameter is also used for the DDMI server.</p>

Universal Discovery Agent Error Codes

For error codes that may be returned when using installation or upgrade packages, see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa376931\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa376931(v=vs.85).aspx).

Server Configuration Data Import Troubleshooting

Issues and error messages that can occur when importing server configuration data are as follows:

Issue	Description
An error message is displayed warning about duplicate or overlapping IP address ranges	These IP ranges are not migrated. Either modify the IP ranges in DDMI or modify IP ranges in UCMDB and run the migration script again.

Issue	Description
	<p>Tip: To continue migrating data even though a conflict occurs, set the stopWhenConflict option to false in the importMigrationDataFromDDMI method that is accessible from the JMX console.</p>
An error message is displayed warning about duplicate credentials.	These credentials are not migrated. The migration scripts analyze the user label for each credential to determine if a duplicate exists.
Some device groups in DDMI have the same name as Management Zones in UCMDB	The Management Zone that has the same name as a device group is overwritten, including the activity information.

Terminology Changes from DDMI to Universal Discovery

This section describes terminology and methodology changes from DDMI to Universal Discovery.

Conceptual Changes

DDMI	Universal Discovery
<p>Device Groups. Device Groups are logical groupings of devices based on IP ranges, and devices can belong to more than one group. Configuration profiles are applied to a device group.</p> <p>To access device groups, Administration > Discovery Configuration > Device Groups. To specify how the devices in groups are discovered, you create and assign a configuration profile to a device group.</p>	<p>Management Zones. Management Zones are defined by a collection of IP ranges or device types. Management Zones are used when you want to discover all the managed objects of the region using the same scheduling policy and parameters. You assign IP ranges to Data Flow Probes, and then you assign Data Flow Probes to Management Zones.</p> <p>For more information about IP ranges, see Effects of Range Type on Discovery Workflows in the <i>HP Universal CMDB Data Flow Management Guide</i>.</p> <p>For more information about Management Zones, see Zone-based Discovery Overview in the <i>HP Universal CMDB Data Flow Management Guide</i>.</p>
<p>Passive Discovery. In Passive Discovery, DDM Inventory utilizes IP/MAC Address Harvesting as the first method of discovery. The job does not actively look</p>	<p>IP/MAC Harvesting. IP/MAC Address Harvesting is offered as a discovery preference in the Infrastructure Discovery Activity. Additionally, when an IP range is Client type, IP/MAC Address Harvesting is the only method of</p>

DDMI	Universal Discovery
<p>for devices via ICMP, but will include them if it already has the IP to MAC address mapping.</p> <p>The Passive Discovery configuration profile is applied to the device group.</p>	<p>discovery.</p> <p>Passive Discovery jobs are still available. Configure the IP range as Client type when configuring an IP range on the Data Flow Probe. For more information on setting up IP range types, see <i>Effects of Range Type on Discovery Workflows and Data Reconciliation</i>. Then, run the Infrastructure Discovery Activity with IP/MAC Harvesting enabled.</p>

Product Configuration

In Universal Discovery, activities have simplified the administration of jobs. For example, both active and passive jobs can be run on the same schedule and using the same parameters- by activating a single activity.

Discovery Type	DDMI	Universal Discovery
Active Discovery	The Active Discovery configuration profile is applied to the device group.	Run the Infrastructure Discovery Activity for a Management Zone. For more information, see the section describing the Infrastructure Discovery Activity in the <i>HP UCMDB Discovery and Integrations Content Guide</i> .
Discovery via SNMP	The SNMP configuration profile is applied to the device group.	Run the Infrastructure Discovery Activity and ensure that IP/MAC Harvesting is enabled. For more information, see the section describing the Infrastructure Discovery Activity in the <i>HP UCMDB Discovery and Integrations Content Guide</i> .

Committing/Activating Configuration Changes

DDMI	Universal Discovery
All configuration changes are activated at Administration > Discovery Configuration > Activation .	All configuration changes are activated when you select Activate Activity on the Summary page of an activity wizard.

Agent

Feature	DDMI	Universal Discovery
Interoperability	N/A	UD Agents automatically detect whether a DDMI server or a Data Flow Probe is attempting communication by examining message headers. Therefore, the UD Agent can support both environments simultaneously.
Data Directory	N/A	Each time the UD Agent is run, it checks the UD default data directory. If no files exist, it checks the DDMI default data directory. If files exist, it moves the files from the DDMI default directory to the UD default directory. For information about UD Agent file locations, see <i>Universal Discovery Agent Installation Resources</i> .
Agent deployment/migration	This is performed at the following location: Administration > Discovery Configuration > Configuration Profiles > Agent tab.	<p>This is performed automatically using the Infrastructure Discovery Activity, or performed manually using third party tools or remote access technologies.</p> <p>For details on the Infrastructure Discovery activity, see <i>HP UCMDB Discovery and Integrations Content Guide</i>.</p> <p>For complete agent migration information, see "DDMI to Universal Discovery Migration Options Overview" on page 11.</p>
Call Home	Call Home is enabled at the following location: Administration > System Configuration > Discovery services	Call Home is always enabled. The UD Agent calls home using a fixed frequency regardless of whether the device has been scanned successfully or not, or whether the

Feature	DDMI	Universal Discovery
		<p>scan file has been successfully uploaded to the Data Flow Probe or not. Additionally, Call Home occurs at more frequent intervals than in DDMI. For more information, see the section that describes how to configure call home.</p> <p>Note: Call Home settings are automatically migrated when using the Server Migration Tool.</p>
Inventory Scanning	Scanners are configured at Administration > Discovery Configuration > Configuration Profiles > Scanner tab	Inventory Discovery Activity > Preferences. For more information, see the section that explains inventory discovery scanners.
Virtualization discovery	You apply the Virtualization profile to a device group. In the Scanner Generator, you select the Virtual Machines option on the Hardware Data page to enable or disable detection, and you can indicate if you want containers included in a hardware detection scan. Scanners can detect if they are in a virtual environment and stop running if you set the time out option in the Miscellaneous tab.	In the Inventory Discovery wizard on the Virtualization page, select Include Virtualization Topology .
Credentials	You can specify a collection of deployment credentials that are valid for devices in your network. You can then associate one or more sets of these credentials with an Agent configuration profile.	<p>You specify login credentials when you configure an Infrastructure Discovery Activity for a Management Zone. For more information, see the section describing the Infrastructure Discovery activity in the <i>HP UCMDB Discovery and Integrations Content Guide</i>.</p> <p>Note: Credentials are</p>

Feature	DDMI	Universal Discovery
		<p>automatically migrated from DDMI to Universal Discovery when using the Server Migration Tool.</p>

Data Access

DDMI	Universal Discovery
Data can be directly accessed using DBI connections to the MySQL database.	<p>The following APIs are available:</p> <ul style="list-style-type: none"> • UCMDB Java API • UCMDB Web Service API. • Data Flow Management Web Service API <p>In addition to searching the database via TQL, you can use a text search using the search engine.</p> <p>For more information, see the section describing the UCMDB APIs in the <i>HP Universal CMDB Developer Reference Guide</i>.</p>

Data Migration

When using the Perl import script and JMX console to migrate server data, DDMI Profile data is imported into Universal Discovery activities as follows:

DDMI Profile	Universal Discovery Activity
Basic	Infrastructure Discovery activity
Network	<p>Note: Schedule data for network profiles are migrated only when Force ARP Table To Be Read is selected in DDMI.</p>
Agent	

DDMI Profile	Universal Discovery Activity
Scanner	Inventory Discovery activity
VmWare	<p>Note: If you want to run virtualization topology discoveries, you must have VmWare credentials configured for VmWare profiles in DDMI before you migrate to Universal Discovery. Alternatively, enable Virtualization Topologies discoveries manually on the Virtualization Page in the Inventory Discovery Activity after you migrate.</p>

DDMI data is imported into Universal Discovery as follows:

DDMI	Universal Discovery
Deployment credentials	SSH, NTCMD, and VmWare credentials are imported and keys are regenerated automatically.
SNMP configuration profile	Mapped to protocol parameters for the SNMP protocol.
Device groups	Device groups are migrated to Management Zones and appear using the following convention: <DDMIServerHostName_DeviceGroup>
System configuration	Agent and scanner-related configurations.
VMware configuration	VMware VIMware protocol.
XML Enricher configuration file	To import, set the overrideGlobalConfig parameter to True in the JMX console import method. For more information, see "How to Migrate DDMI Server Configuration Data to Universal Discovery" on page 36.
Certifacts (DDMi agent)	<p>The following files are imported:</p> <ul style="list-style-type: none"> acstrust.cert agentca.pem acskeystore.bin <p>Note: The UD Agent protocol is created from these files.</p>
IP address	IP address ranges are mapped to either Client or Data Center type according to the

DDMI	Universal Discovery
ranges	<p>following criteria:</p> <p>The IP address range is set to Client type when Actively Ping Devices is disabled and Allow ICMP and SNMP is enabled for the configuration profile that is applied to the device group for the range. All other ranges are set to Data Center type.</p> <p>For more information on IP range types, see the section that describes the effects of range types on discovery workflows and data reconciliation.</p>

Migrated Reports from DDMI to Universal Discovery

The following table displays DDMI reports and their corresponding reports in Universal Discovery.

DDMI	Universal Discovery
Scanned Device Summary Report and all its child reports	Custom > Inventory > Node Summary Report
Recognized Applications/App Lic	Custom > Inventory > Application License Report
Recognized Applications/App Running Util	Custom > Inventory > Software Utilization Report
Recognized Applications/OS Reported	Custom > Inventory > Recognized Applications Report
Recognized Applications/Virtual Devices - Solaris Zones	Custom > Virtualization > Solaris Zone Report
Recognized Applications/Virtual Devices - VMware Hosts, Virtual Machines	Custom > Virtualization > VMware Host Report
Recognized Applications/Virtual Devices - VMware Virtual Center	Custom > Virtualization > VMware Virtual Center Report
Recognized Applications/Network Disc/Device Inventory by Virtual	Custom > Inventory > Node Summary by VLAN Report
Status/Device Status/Agent status	Custom Report > Discovery Status > Agent Status Report
Status/Device Status/Scanner execution details	Custom Report > Discovery Status > Scanner Execution Details Report

DDMI	Universal Discovery
Status/Device Status/Scan file status	Custom Report > Discovery Status > Scan File Status Report
Status/Device Status/Device exceptions	Custom Report > Discovery Status > Discovery Error Report

Mapping Attributes from DDMI to UCMDB

This section describes mappings between DDMI attributes to UCMDB CIs and attributes.

Note: You can create a custom mapping of attributes that are contained in scan files to UCMDB CIs. To do this, see the section on how to map scan file attributes to UCMDB.

Scanner

DDMI Attribute	UCMDB CI	UCMDB Attribute
hwScannerVersion	inventory-scanner	version
hwScanCmdLine		scanner_command_line
hwScanDuration		scan_duration
hwScanDate		startup_time
hwScannerDescription		description
hwCreationMethod		scanner_type
hwFilesTotal		files_total
hwFilesProcessed		files_processed
hwFilesRecognised		files_recognized

Node Elements

DDMI Attribute	UCMDB CI	UCMDB Attribute
hwDisplayGraphicsAdapterName	graphics_adapter	name
<index_of_card>		board_index
hwDisplayGraphicsAdapterMemoryMB		graphics_card_memory
hwDisplayDesktopResolutionX		current_display_mode_resolution_x
hwDisplayDesktopResolutionY		current_display_mode_resolution_y
hwDisplayDesktopColourDepth		current_display_mode_colour_depth
hwDisplayDesktopColours		current_display_mode_colours
hwDisplayDesktopRefreshRate		current_display_mode_refresh_rate
hwDisplayDesktopResolution		current_display_mode_resolution
hwsmbiosBaseBoardSerialNumber	hardware_board	serial_number
<index of board>		board_index
hwsmbiosBaseBoardVersion		hardware_version
hwsmbiosBaseBoardName		name
hwsmbiosBaseBoardManufacturer		vendor
hwCardName		name
<index of board>		board_index
hwCardClass		type
hwCardBus		bus
hwCardVendor		vendor
hwCardID		vendor_card_id
hwCardRevision		hardware_version

DDMI Attribute	UCMDB CI	UCMDB Attribute
hwOSServiceName	windows_service	service_name
hwOSServiceDisplayName		name
hwOSServiceFileName		service_commandline
hwOSServiceUser		service_startuser
hwOSServiceType		service_type
hwOSServiceStartup		service_starttype
hwOSServiceStatus		service_operatingstatus
hwOSServiceDescription		service_description
hwOSServiceName	daemon	name
hwOSServiceFileName		daemon_path
hwMonitorName	display_monitor	name
hwMonitorVendorCode		vendor
hwMonitorSerialNumber		serial_number

SMBIOS

DDMI Attribute	UCMDB CI	UCMDB Attribute
hwsmbiosChassisType	node	chassis_type

BIOS

DDMI Attribute	UCMDB CI	UCMDB Attribute
hwBiosDate	node	bios_date
hwBiosVersion hwBiosBootPromVersion		bios_version
hwBiosSource		bios_source

Cluster

DDMI Attribute	UCMDB CI	UCMDB Attribute
hwOSClusterName	mscluster	name
hwOSClusterDescription		description
hwOSClusterVendor		vendor
Microsoft Cluster SW		discovered_product_name

Network

DDMI Attribute	UCMDB CI	UCMDB Attribute
hwNICInterfaceName	interface	interface_name
hwNICDescription		interface_description
hwNICPhysicalAddress		mac_address
hwNICType		interface_type
hwNICCurrentSpeed		interface_speed
hwNICIPAddresses		containment
hwNICPrimaryWins		primary_wins
hwNICSecondaryWins		secondary_wins
hwNICGateway		gateways
hwNICIPAddress	ip_address	ip_address/name
hwNICSubnetMask		ip_netmask
hwNICIPAddressType		ip_address_type
<not available>		routing_domain
hwNICUsesDHCP hwNICIPAddressType hwNICFeatures		ip_address_property

Software

DDMI Attribute	UCMDB CI	UCMDB Attribute
name	installed_software	name
publisher		discovered_vendor
maindir		file_system_path
licencedby		is_suite_component
lastUsed		last_used_date
typeid		software_category_id
language		software_language
version		version
release		release
type		software_type
hwRecognitionMethod		recognition_level
versionid		sai_version_id
useddayslastmonth		usage_days_last_month
useddayslastquarter		usage_days_last_quarter
useddayslastyear		usage_days_last_year
usagehourslastmonth		usage_hours_last_month
usagehourslastquarter		usage_hours_last_quarter
usagehourslastyear		usage_hours_last_year
useddailypeak		usage_hours_last_year_daily_peak
usagepercent		usage_percent
commercial		software_license_type

DDMI Attribute	UCMDB CI	UCMDB Attribute
usedayslastmonthfoc	installed_software	infocus_usage_days_last_month
usedayslastquarterfoc		infocus_usage_days_last_quarter
usedayslastyearfoc		infocus_usage_days_last_year
usagehourslastmonthfoc		infocus_usage_hours_last_month
usagehourslastquarterfoc		infocus_usage_hours_last_quarter
usagehourslastyearfoc		infocus_usage_hours_last_year
usedailyaveragefoc		infocus_usage_hours_last_year_daily_average
usedailypeakfoc		infocus_usage_hours_last_year_daily_peak
usagepercentfoc		infocus_usage_percent

Note: Scan file attributes ending with "foc" are also contained in the Software Utilization CI.

Basic Node

DDMI	UCMDB CI	UCMDB Attribute
hwMemoryData.hwMemTotalMB	node	memory_size
hwSwapFiles.hwMemSwapFileSize (Array)		swap_memory_size
hwOSHostWindowsName (Windows)		discovered_os_name
hwOSHostUnixType (Linux)		
hwOSHostUnixType (HP-UX)		
hwOSHostUnixType (Sun)		
hwOSHostUnixType (AIX)		
hwOSHostUnixType (Mac)		
hwOSHostOsCategory	node	discovered_os_vendor
hwOSInternalVersion (Linux)		discovered_os_version
hwOSInternalVersion + "." + hwOSBuildLevel (Windows)		
hwOSHostVersion (HP-UX)		
hwOSInternalVersion AIX - hwOSHostVersion (Sun)		
hwOSHostVersion (Mac)		
hwOSHostLinuxType (Linux)	node	host_osinstalltype
hwOSHostWindowsNTMode + hwOSHostEdition (Windows)		
hwOSHostMacOsType (Mac)		
"release" + hwOSHostVersion (Red Hat Linux)	node	host_osrelease
hwOSBuildLevel (Windows)		
hwOSServiceLevel (HP-UX)		
hwOSServiceLevel (AIX)		
hwOSServiceLevel (Sun)		

DDMI	UCMDB CI	UCMDB Attribute
hwOSHostOsCategory		os_family
hwBiosAssetTag		bios_asset_tag
hwsmbiosSystemUUID		bios_uuid
hwsmbiosProductName hwBiosData.hwBiosMachineModel		discovered_model
hwsmbiosSystemManufacturer hwBiosData.hwBiosManufacturer		discovered_vendor
hwLocalMachineID (Windows)		net_bios_name
hwDomainName		domain_name
hwNetworkTcpip.hwIPRoutingEnabled hwVirtualMachine.hwVirtualMachineType		node_role
hwIPHostName + "." + hwIPDomain		primary_dns_name
hwBiosData.hwBiosSerialNumber hwsmbiosSystemSerialNumber hwsmbiosChassisSerialNumber		serial_number
hwNetworkDNSServer (Unix) hwNICDNSServer (Windows) (Mac)		dns_servers
hwOSDefaultUserName	nt	registeredowner
hwOSDefaultOrganisationName		registrationorg
hwOSServiceLevel		servicepack

DDMI	UCMDB CI	UCMDB Attribute
hwCPUs.hwCPUDescription	Cpu	cpu_type
hwCPUs.hwCPUSpeed		cpu_clock_speed
hwCPUCoreCount/hwPhysicalCPUCount		core_number
hwCPUCount/hwPhysicalCPUCount		logical_cpu_count
hwCPUs.hwCPUType		cpu_specifier
hwCPUs.hwCPUVendor		cpu_vendor
index		cpu_id
hwPhysicalDiskData.hwPhysicalDiskType	DiskDevice	disk_type
hwPhysicalDiskData.hwPhysicalDiskSize		Device.disk_size
hwPhysicalDiskData.hwPhysicalDiskID		name
hwPhysicalDiskData.hwPhysicalDiskNumber		
hwSCSIDevices.hwSCSIDeviceName		model_name
hwSCSIDevices.hwSCSIDeviceVendor		vendor
hwMountPoints.hwMountPointMountedTo	FileSystem	mount_point
hwMountPoints.hwMountPointVolumeMedia		disk_type
hwMountPoints.hwMountPointVolumeTotalSize		disk_size
hwMountPoints.hwMountPointVolumeFreeSpace		free_space
hwMountPoints.hwMountPointVolumeType		filesystem_type
hwMountPoints.hwMountPointVolumeDevice		name
hwMountPoints.hwMountPointVolumeType	LogicalVolume	logicalvolume_fstype
hwMountPoints.hwMountPointVolumeFreeSpace		logicalvolume_free
hwMountPoints.hwMountPointVolumeTotalSize		logicalvolume_size

DDMI	UCMDB CI	UCMDB Attribute
hwNetworkSharePath	file_system_export	file_system_path
hwNetworkShareName		share_names
hwNetworkSharePath		name
hwNetworkShareRemark		description
hwsmbiosMemoryArrayDeviceLocator -else- hwsmbiosMemoryArrayBankLocator	memory_unit	name
index		memory_unit_index
hwsmbiosMemoryArraySize		size
hwsmbiosMemoryArraySerialNumber		serial_number
hwsmbiosMemoryModuleSocketDesignation		name
index		memory_unit_index
hwsmbiosMemoryModuleInstalledSize		size
hwMemoryBank		name
index		memory_unit_index
hwMemoryDIMMSizeMB		size
hwNetworkLogonName	winosuser	name
hwNetworkLogonDomain		winosuser_domain
hwNetworkLogonName	osuser	name

Java Viewer Mapping from DDMI to Universal Discovery

The following is a mapping of sections in the Java Viewer to Universal Discovery reports:

Java Viewer	UCMDB
Software Inventory	Recognition Application Report
Software Inventory	Software Utilization Report
Hardware	Hardware Node Element Topology Report
	Node Inventory Report

Attribute values that are contained in Configuration Items (CIs) can be displayed in the Configuration Item Properties dialog box. For more information, see the section describing the CI properties dialog box in the *HP Universal CMDB Modeling Guide*.

Chapter 6: Inventory Discovery Troubleshooting

This chapter includes:

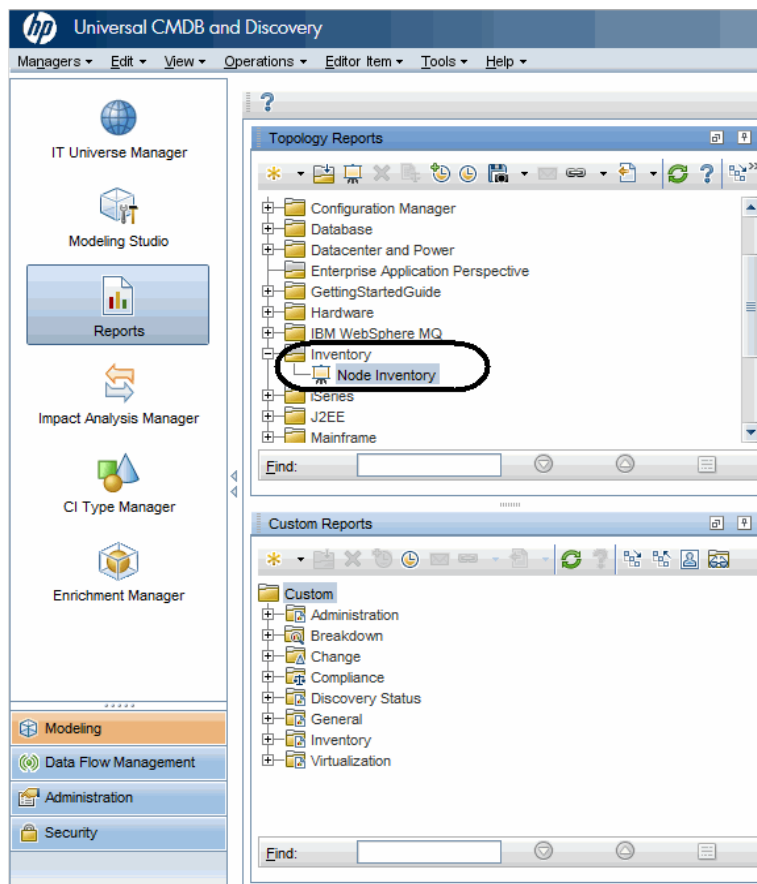
How to view all information related to a device in a centralized view?	109
How to troubleshoot network availability and latency issue related to a device?	111
How to check the key indexes of the discovery history information for a discovered device?	117
How to check device related logs for a discovered device?	123
How to invoke discovery job relevant to the discovered device manually and check status to identify potential discovery errors?	126
How to check which pattern (management zone) is used in the discovery for a discovered device?	136
How to check detailed discovery settings used in the discovery for a discovered device?	138
How to check the SNMP credentials used in the discovery for a discovered device?	142

How to view all information related to a device in a centralized view?

Question: How can I view all relevant information to a device in a centralized view?

To view all information related to a device in a centralized view,

1. Select **Modeling > Reports**.
2. In the Topology Reports pane, expand **Inventory > Node Inventory**.



3. Double-click **Node Inventory** or right-click it and select **Open Report**.

The Node Inventory report opens in the right pane.

4. Do either of the following to view device details:

- Page 110 of 144

Display Label	Discovered Location	Discovered Vendor	Discovered Model	Serial Number	BaseAsset Tag	Bus Version	Bus Serial Number	Classified Type	Discovered Os Vendor	Discovered Os Name	Note Operating System Release	Discovered Os Version	Note Operating System Installation type	Last Access Time	Last Modified Time	Count	CPU
-RAM 886 R#2														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
-RAM 886 R#3														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
HyperV		V-Mware, Inc.	VMware Virtual Platform	VMWARE-6A5C-F4BC-7A-E3ACD10-D819-0440-C7BF	V-Mware-Z 14 14 14 7a f6 c8 a5 c2 d1 de 9d a4 e4 c7 bf	INTEL® E040000		Other	Microsoft	Windows 2008 R2	7601	6.1.7601	Server Enterprise	Sun Dec 14 2014 06:04 PM CST	Wed Dec 10 2014 05:33 PM CST		
CPU														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	1	
Intel(R) Xeon(R) CPU L5640 @ 2.27GHz														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	Genus	
Disk Device														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	3	
Memory														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
REC\\Mitar\\VMWare OSE CORP_ID														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Virtual disk_0														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Graphics Adapter														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	1	
440B-L Desktop Reference Platform				None										Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Hardware Board														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	5	
440B-L Desktop Reference Platform				None										Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Intel(R) D3714AB/E PCI Bus Master /OE Controller														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Intel(R) PRO/1000 MT Network Connection														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
LSI Adapter SAS-3000 series, i-port with 10Gb														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
M-Mage VMCU Bus Device														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		

2014-12-15 01:45 PM

For more information about the topology report, see the *HP Universal CMDB Modeling Guide*.

How to troubleshoot network availability and latency issue related to a device?

Question: How should I troubleshoot network availability and latency issue related to a device?

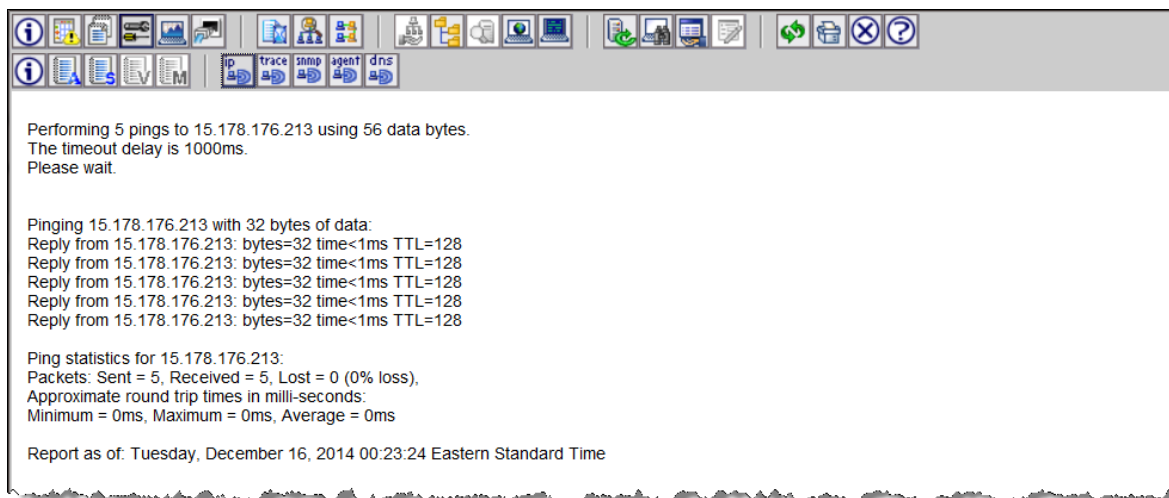
You can troubleshoot network availability and latency issue related to a device in the following ways:

- [IP Ping and Agent Ping](#)
- [SNMP Ping](#)
- [Tracert and DNS Query](#)

IP Ping and Agent Ping

In DDMI, you can use IP ping and agent ping.

Result of the IP ping looks similar to the following:



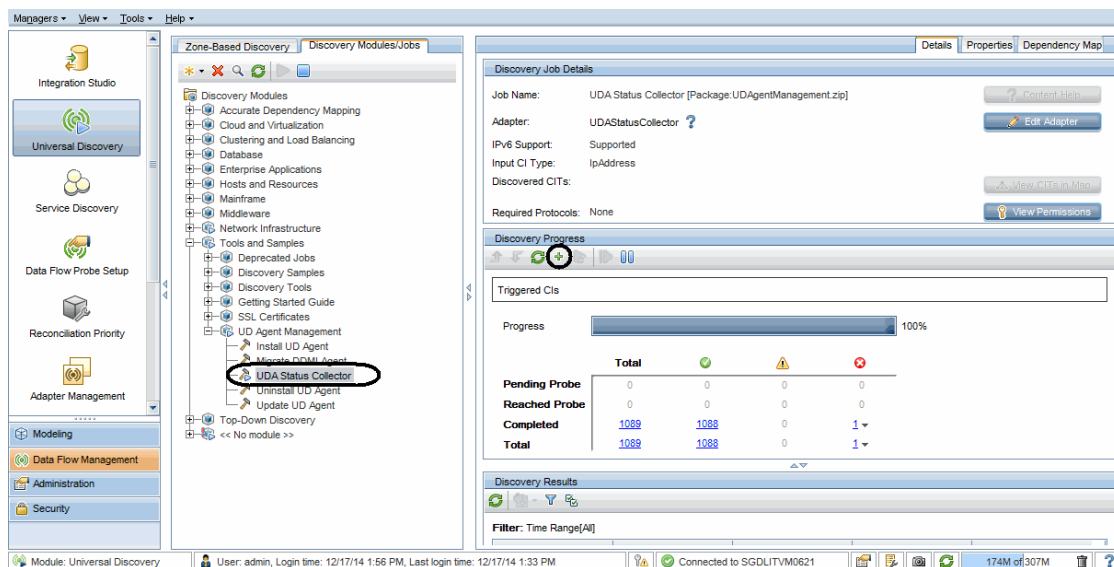
Result of the agent ping looks similar to the following:





In UD, you can also use IP ping and agent ping via the UDA Status Collector job.

To use IP ping and agent ping

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > UDA Status Collector**.
3. If the UDA Status Collector job is not activated, right-click **UDA Status Collector**, and select **Activate**.



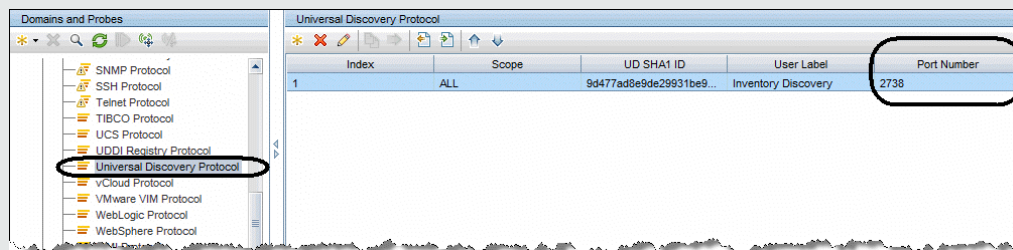
4. In the Discovery Progress pane, click the **Add CI**  button.
5. In the Choose CIs to Add dialog box, select the IP address of your interest, and click the **Add**  button.

The UDA Status Collector job will ping using IP and agent port to check.

Note: Agent port can be found in the **Port Number** parameter value of the Universal Discovery Protocol credential. This is a default parameter in the protocol, and is applied to all agent connections using this protocol.

To view the agent port,

- a. In the Data Flow Management module, go to **Data Flow Probe Setup**.
- b. In the Domains and Probes tree, select a domain of your interest and expand the **Credentials** node, and then select **Universal Discovery Protocol**.
- c. In the Universal Discovery Protocol credentials displayed in the right pane, check the value for the **Port Number** column.



6. Click the **Close** button to exit the Choose CIs to Add dialog box.

To view the IP ping and agent ping result

1. Access the JMX console on the Data Flow Probe by launching the Web browser and enter the following address:

http://<machine name or IP address>.<domain_name>:1977/

where **<machine name or IP address>** is the machine on which the Data Flow Probe is installed. You may have to log in with the user name and password.

2. Locate the **exportUdaStatus** operation to invoke.

On the MBean View page, select **type=JobsInformation**. Locate the **exportUdaStatus** operation.

Invoke

exportJobsExecutionTimelineXML

Export the job execution history time line as xml file to be used by Excel

Name	Type	Value	Description
groupByCycle	boolean	<input checked="" type="radio"/> True <input type="radio"/> False	

Invoke

exportUdaStatus

Export UDA Status to CSV

Name	Type	Value	Description
path	java.lang.String	c:\udastatus	

Invoke

resumeNowWorkflowJobOnDestination

resumes a workflow trigger ci that is currently in the state of parking

Name	Type	Value	Description
jobId	java.lang.String		

3. Provide a folder name in the **Value** field.

4. Click **Invoke** to run the operation.

The UDA status is exported to a CVS file.

5. Open the exported CSV file to view details of the result from the UDA Status Collector job.

The CSV file shows status details similar to the following:

ipaddress	computerName	alive	portAlive	isDDMI	isWin	osType	agentVersion	UDUniqueid	isNative
16.60.169.33	myd-vm11101.hpswl-abs.adapps.hp.com	TRUE	TRUE	FALSE	FALSE	Linux	v10.20.000-build:346	73a911c4-b0fa-4e10-2047-b270e5a0cb18	TRUE

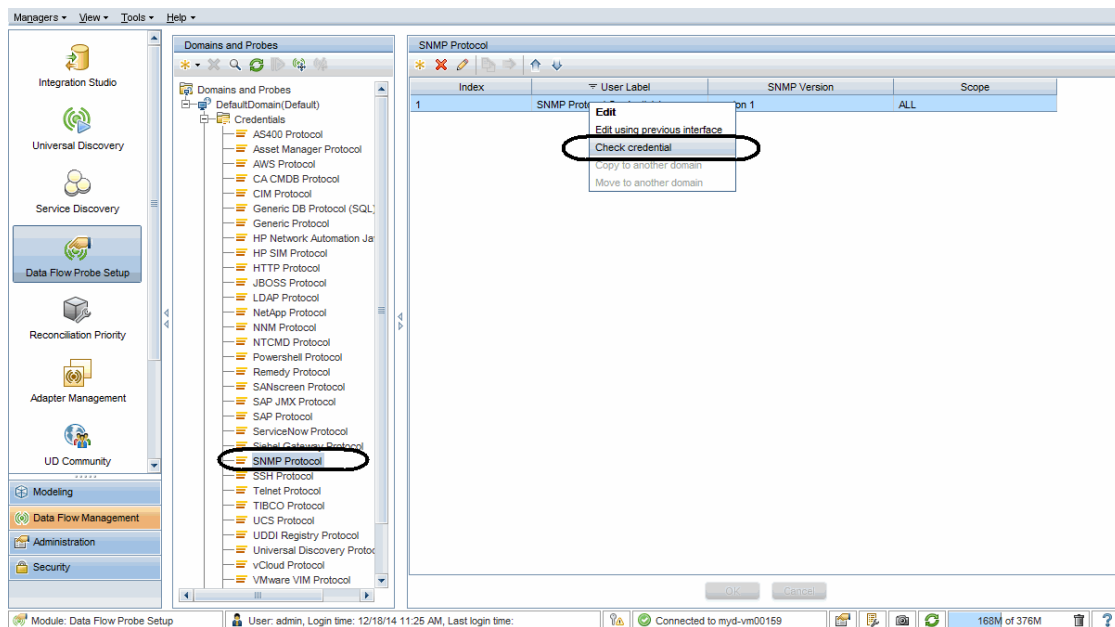
SNMP Ping

To run SNMP ping in UDI,

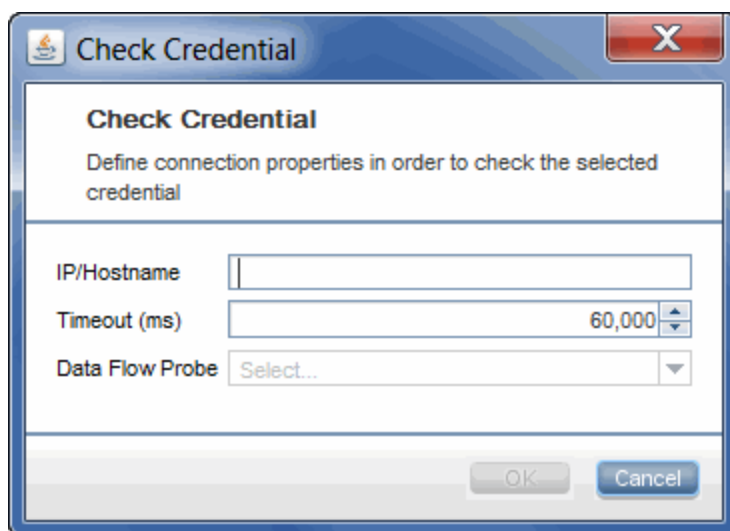
1. In the Data Flow Management module, go to **Data Flow Probe Setup**.
2. In the Domains and Probes tree, expand the **Credentials** node, and select **SNMP Protocol**.

All SNMP credentials are displayed in the right pane.

3. Right-click the SNMP credential you want to use to run SNMP ping, and select **Check credential** from the pop-up menu.



4. In the Check Credential dialog box, specify the host name or IP address (in IPv4/IPv6 format) of the remote machine on which you want the protocol to run SNMP ping, specify a connection timeout (in milliseconds), and select the probe to use.



5. Click **OK**.

The result returns soon.

Tracert and DNS Query

Currently UD does not have such functionalities as DDMi did.

How to check the key indexes of the discovery history information for a discovered device?

Question: For a discovered device, how should I check the key indexes of the discovery history information? For example, when was the device first discovered? When was it last seen?

To answer this question, let's take a look at the information available from DDMi first:

DDMi Parameter	Value
First discovered:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:20:45 Eastern Standard Time
Added to map:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:48:51 Eastern Standard Time
Last seen:	2 minutes 1 second ago at: Monday, December 15, 2014 21:06:55 Eastern Standard Time in ping or poll by DDM Inventory
Last moved:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:50:47 Eastern Standard Time
Agent last contacted:	1 day 17 hours 7 minutes ago at: Sunday, December 14, 2014 04:01:01 Eastern Standard Time
Agent upgrade time:	2 weeks 6 days 1 hour ago at: Tuesday, November 25, 2014 19:56:04 Eastern Standard Time
Scanner model last updated:	2 weeks 6 days 0 hours ago at: Tuesday, November 25, 2014 20:12:35 Eastern Standard Time
Device last modeled as an unmanaged device:	3 hours 12 minutes 6 seconds ago at: Monday, December 15, 2014 17:56:50 Eastern Standard Time
Device last replied to ICMP during modeling:	2 weeks 3 days 21 hours ago at: Thursday, November 27, 2014 23:12:44 Eastern Standard Time
Mean break diagnosis time:	2 minutes (major alarm)
Agent platform:	Windows (x86)
Agent port number:	2738

DDMi Parameter	Value
Agent version:	10.20.000.346
AUM agent upgrade state:	No AUM agent
Workflow type:	Agent
Scanner version:	9.32.000.2421
Scanner configuration:	<default_delta>
Scan file location:	https://15.155.155.155/nm/scans/QASERVER1_005056B81459.xsf
Scan type:	HP Discovery and Dependency Mapping Inventory
Scan CRC:	295532891
Scan modification time:	2014-11-25 22:47:26
Mean device modeler update run time:	4 minutes 52 seconds
Recent device modeler update run times:	4 minutes 48 seconds, 4 minutes 17 seconds, 6 minutes 32 seconds, 3 minutes 53 seconds
Rulebase id:	266305

In Universal Discovery, you can find similar attributes for most of DDMI parameters as shown in the table below:



DDMi Parameter	Corresponding Attributes in UD
First discovered:	Create Time attribute (of the node CI)
Added to map:	N/A
Last seen:	Last Access Time attribute (of the node CI)
Last moved:	N/A
Agent last contacted:	Last Access Time attribute (of the UDA CI Type)
Agent upgrade time:	LastModifiedTime attribute (of the UDA CI Type)
Scanner model last updated:	LastModifiedTime attribute (of the InventoryScanner CI Type)
Device last modeled as an unmanaged device:	N/A

DDMi Parameter	Corresponding Attributes in UD
Device last replied to ICMP during modeling:	N/A
Mean break diagnosis time:	N/A
Agent platform:	Platform attribute (of the UDA CI Type)
Agent port number:	Application Listening Port Number attribute (of the UDA CI Type)
Agent version:	Version attribute (of the UDA CI Type)
AUM agent upgrade state:	N/A
Workflow type:	N/A
Scanner version:	Version attribute (of the InventoryScanner CI Type)
Scanner configuration:	ScannerConfiguration attribute (of the InventoryScanner CI Type)
Scan file location:	ProcessedScanFilePath attribute (of the InventoryScanner CI Type)
Scan type:	Scan Type attribute (of the InventoryScanner CI Type)
Scan CRC:	N/A
Scan modification time:	Last Access Time or Scan File Last Downloaded Time attribute (of the InventoryScanner CI Type)
Mean device modeler update run time:	N/A
Recent device modeler update run times:	Scan Duration attribute (of the InventoryScanner CI Type)
Rulebase id:	N/A

Note: "N/A" indicates that there is no corresponding attribute in UD now.

To check similar information in UD,

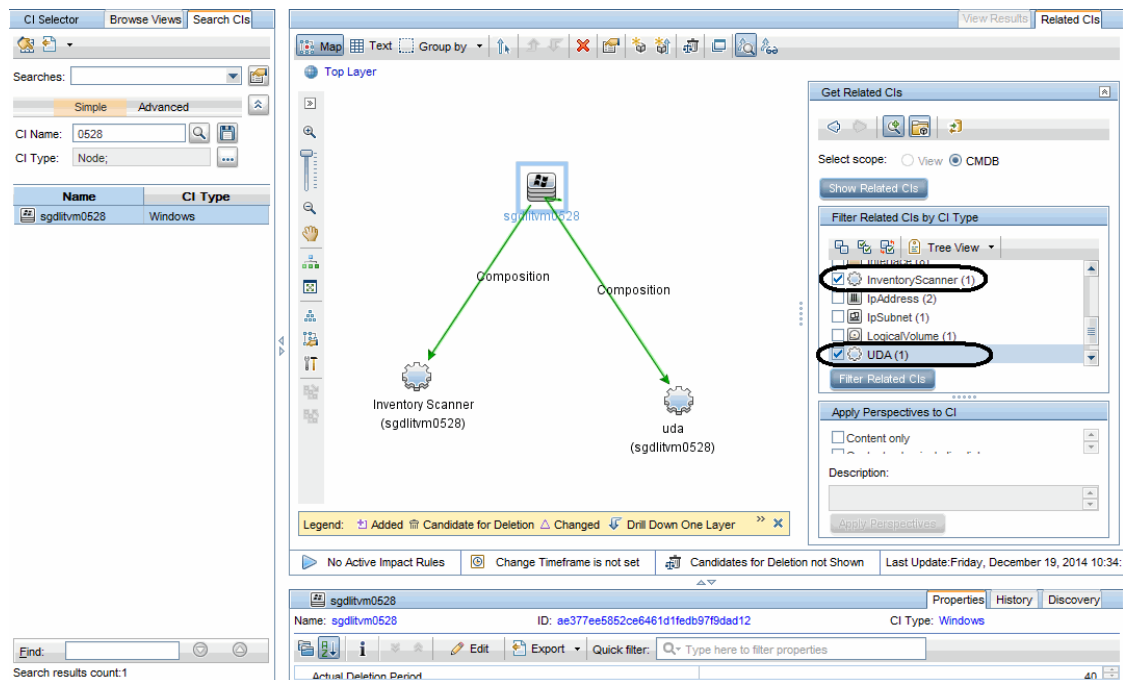
1. In UCMDB, go to **Modeling > IT Universal Manager**.
2. In the CI Selector pane, go to the **Search CIs** tab.

3. In the Simple search mode, search for a CI of Node CI type.
 - a. In the **CI Name** field, enter a keyword to search, for example, **0528**.
 - b. For the **CI Type** field, click , locate and select the **Node** CI type.
 - c. Click .
4. Click the node CI in the search result list.

The node CI map displays in the Related CIs pane.

5. In the Filter Related CIs by CI Type sub-pane, locate and select **Inventory Scanner** and **UDA** CI types, then click **Filter Related CIs**.

The Related CIs map refreshes.



The screenshot displays the HP Universal CMDB interface. On the left, the 'CI Selector' pane shows a search for 'sgdlitvm0528' with 'Node' as the CI Type. The main map area shows a tree structure with 'sgdlitvm0528' at the top, branching into 'Inventory Scanner (sgdlitvm0528)' and 'uda (sgdlitvm0528)' via 'Composition' relationships. On the right, the 'Get Related CIs' pane is active, showing 'Filter Related CIs by CI Type' with 'InventoryScanner (1)' and 'UDA (1)' selected. Below the map, the 'CI Details' pane for 'sgdlitvm0528' is visible, showing its ID and CI Type.

6. Click the **uda** or **Inventory Scanner** CI icon in the map.

In the CI Details pane below the map, check attributes that correspond to DDMI parameters.

The highlighted **uda** attributes in the screenshot below correspond to similar DDMI parameters.

uda (sgdlitvm0528)		Properties	History	Discovery
Name: uda (sgdlitvm0528)		ID: b4d11b46f879822f59d86b66dfc3a98c		CI Type: UDA
		Quick filter: <input type="text" value="Type here to filter properties"/>		
Actual Deletion Period	40			
Allow CI Update	True			
Application Category				
Application Installed Path				
Application IP	16.187.190.28			
Application IP Routing Domain	DefaultDomain			
Application IP Type	IPv4			
Application Listening Port Number	2738			
Application Timeout				
Application Username				
Application Version Description				
Architecture	amd64			
classification				
Container name	(sgdlitvm0528)			
Create Time	Thu Dec 18 2014 03:08 PM GMT+08:00			
Created By	UCMDBDiscovery: Host Connection by Shell			
Deletion Candidate Period	20			
Description				
DiscoveredProductName	uda			
Display Label	uda (sgdlitvm0528)			
Edition				
Enable Aging	True			
Global Id	b4d11b46f879822f59d86b66dfc3a98c			
Is Candidate For Deletion	False			
Last Access Time	Thu Dec 18 2014 11:57 PM GMT+08:00			
LastModifiedTime	Thu Dec 18 2014 11:57 PM GMT+08:00			
layer	software			
Name				
Note				
Origin				
Platform	windows			
ProductName				
Reference to the OS credentials dictionary entry	NA			
StartupTime				
Updated By	Enrichment: Enrichment's rule: SoftwareElementDisplayLabel...			
User Label				
Vendor				
Version	v10.20.000 build:364			

The highlighted **Inventory Scanner** CI attributes in the screenshot below correspond to similar DDMI parameters.

Inventory Scanner (sgdlitvm0528)

PropertiesHistoryDiscovery

Name: Inventory Scanner (sgdlitvm0528)

ID: 00601fdc3845ee3a50e5b148618e8be3

CI Type: InventoryScanner

Download

Info

Refresh

Star

Export

Edit

Quick filter:

Type here to filter properties

Actual Deletion Period

40

Allow CI Update

True

Application Category

Application Installed Path

Application IP

Application IP Routing Domain

Application IP Type

IPv4

Application Listening Port Number

Application Timeout

Application Username

Application Version Description

classification

Container name

(sgdlitvm0528)

Create Time

Thu Dec 18 2014 03:51 PM GMT+08:00

Created By

UCMDBDiscovery: Inventory Discovery by Scanner

Deletion Candidate Period

20

Description

Hardware-only Inventory Scanner

DiscoveredProductName

Inventory Scanner

Display Label

Inventory Scanner (sgdlitvm0528)

Edition

Enable Aging

True

FilesProcessed

0

FilesRecognized

0

FilesTotal

0

Global Id

00601fdc3845ee3a50e5b148618e8be3

Is Candidate For Deletion

False

Last Access Time

Thu Dec 18 2014 11:57 PM GMT+08:00

LastModifiedTime

Thu Dec 18 2014 11:57 PM GMT+08:00

layer

software

Name

Note

Origin

ProcessedScanFilePath

C:\hp\UCMDB\DataFlowProbe\runtime\xmlenricher\Scans\pr...

ProcessedScanFileProbe

DataFlowProbe

ProductName

root_iconproperties

Scan File Last Downloaded Time

Thu Dec 18 2014 03:49 PM GMT+08:00

ScanDuration

1

ScannerCommandLine

-cfg:scan.cxz -l:local.xsf -appliance

ScannerConfiguration

_hwnonly.cxz

* ScannerType

WINDOWS_X64

StartupTime

Thu Dec 18 2014 10:13 AM GMT+08:00

Updated By

Enrichment: Enrichment's rule: SoftwareElementDisplayLabel...

Upgrade Date

Thu Dec 18 2014 03:43 PM GMT+08:00

User Label

Vendor

Version

10.20.000 build 364

How to check device related logs for a discovered device?

Question: For a discovered device, where should I check the device related logs? Such as agent deployment log, scanner deployment log, virtualization log, and so on.


The following sections provide details about checking device related log in Universal Discovery.

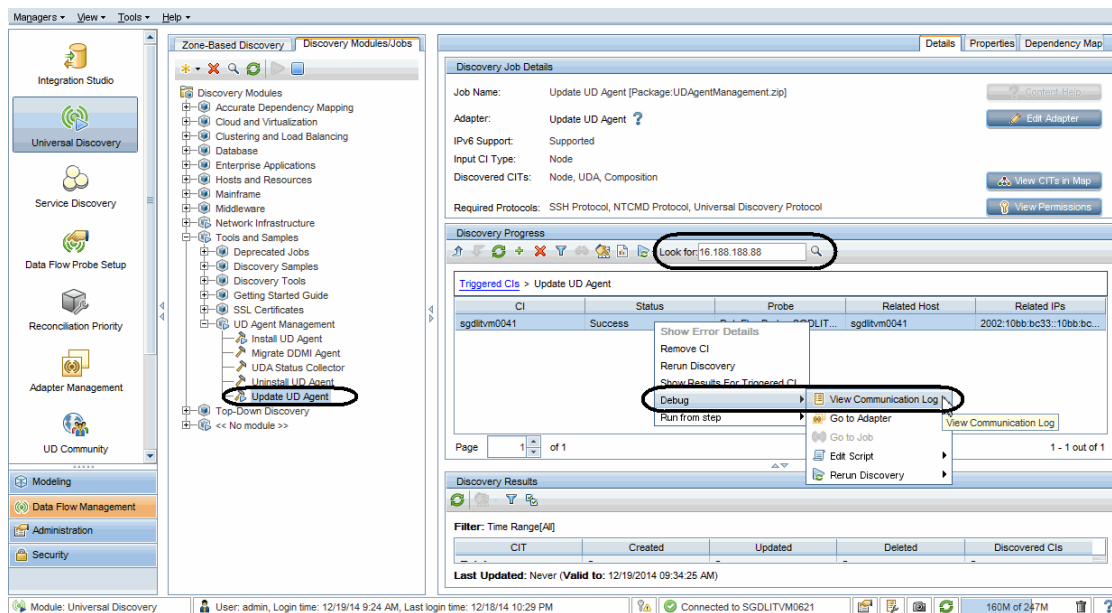
- [Agent deployment log](#)
- [Scanner deployment log](#)
- [Virtualization log](#)

Agent deployment log

The agent related action record (the Install UD Agent job and the Update UD Agent job) can be found in the Communication Log.

To view communication log for agent related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Install UD Agent** (or **Update UD Agent**).
3. Right-click **Install UD Agent** (or **Update UD Agent**), select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target agent and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.



7. In the communication log that opens,


- search **Step [Install Agent]** as keyword to locate the log entry where probe starts the agent installation
- search **Step [Check Agent Installed]** as keyword to locate the log entry that indicates whether the agent is installed

Scanner deployment log

The Inventory Discovery by Scanner job related action record (the Install UD Agent job and the Update UD Agent job) can be found in the Communication Log.

To view communication log for scanner deployment related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
3. Right-click **Inventory Discovery by Scanner**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.

5. In the **Look for** field that is just enabled, enter the IP address for the scanner and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.
7. In the communication log that opens,
 - search **Step [Run Scanner]** as keyword to locate the log entry where the probe starts running the scanner
 - search **Step [Download Scan File]** as keyword to locate the log entry that indicates the probe starts downloading the scan file

Virtualization log

This log is not frequently used in DDMI. However, in UD, the Communication Log for the following jobs can provide you detailed logs about virtualization environments:

- VMware ESX Connection by VIM job
- VMware vCenter Connection by VIM job

How to invoke discovery job relevant to the discovered device manually and check status to identify potential discovery errors?

Question: For a discovered device, to identify any potential discovery errors, how should I invoke discovery job relevant to the device manually, and check the progress/on-going status of the discovery?

In DDMi, if you find any error in the discovery result, you can run the DDMi jobs in an ad-hoc way. In UD, similar jobs are available to provide similar functionalities.


The table below describes DDMi jobs and the corresponding UD jobs that can be run in an ad-hoc way:

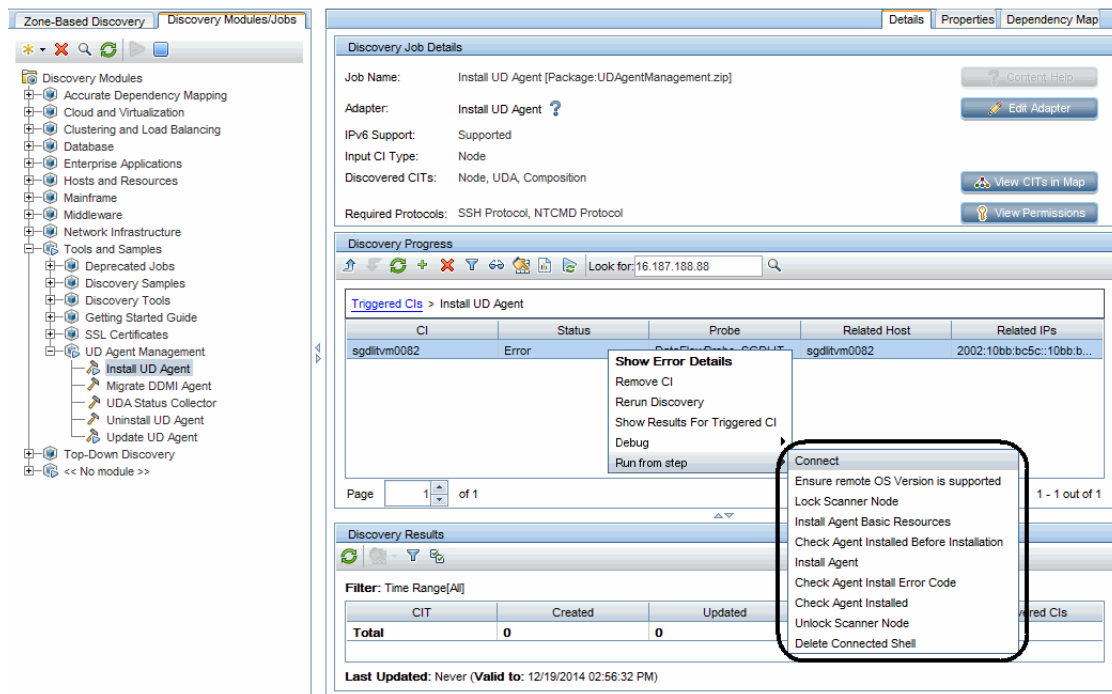
DDMi Job	UD Job
Deploy Agent	Install UD Agent
Upgrade Agent	Update UD Agent
Run Scanner	Run Scanner
Retrieve Scan File	Download Scan File
Uninstall Agent	Uninstall UD Agent
Run Agentless Scanner	Run Agentless Scanner
Enrich XML	Parse Enriched Scan File
Run Rulebase	The normalization functionality is included the Rerun Discovery option for each job
Run VMware Discovery	VMware discovery jobs

For details, click the UD job of your interest in the table above.

Install UD Agent

To invoke discovery job relevant to the device manually,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Install UD Agent**.
3. Right-click **Install UD Agent**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an action>**.



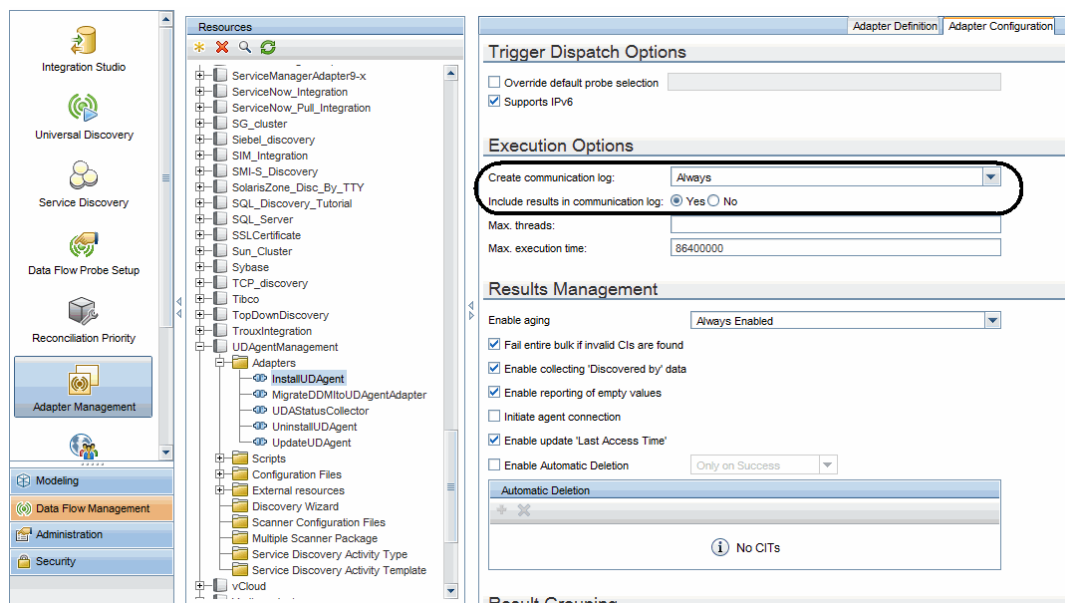
The screenshot displays the UCMDB interface for managing discovery jobs. On the left, the 'Discovery Modules' tree is expanded to 'Tools and Samples > UD Agent Management > Install UD Agent'. The main window shows the 'Discovery Job Details' for 'Install UD Agent'. Below this, the 'Discovery Progress' section includes a search bar with the IP address '16.187.188.88'. A table titled 'Triggered CIs > Install UD Agent' lists one CI with the status 'Error'. A context menu is open over this entry, with the 'Connect' option highlighted. Below the table, the 'Discovery Results' section shows a filter set to 'Time Range[All]' and a table indicating 0 CIs created and 0 updated.

To check the progress/on-going status of the discovery job,

1. Modify the adapter's configuration to make sure that the communication log is always created.

In this case, modify the Install UD Agent adapter's configuration.

- a. In the Data Flow Management module, go to **Adapter Management**.
- b. In the Resources pane, expand **UDAgentManagment > Adapters > InstallUDAgent**.
- c. In the right pane, click the **Adapter Configuration** tab.
- d. In the Execution Options section, set the following:
 - **Create communication log: Always**
 - **Include results in communication log: Yes**




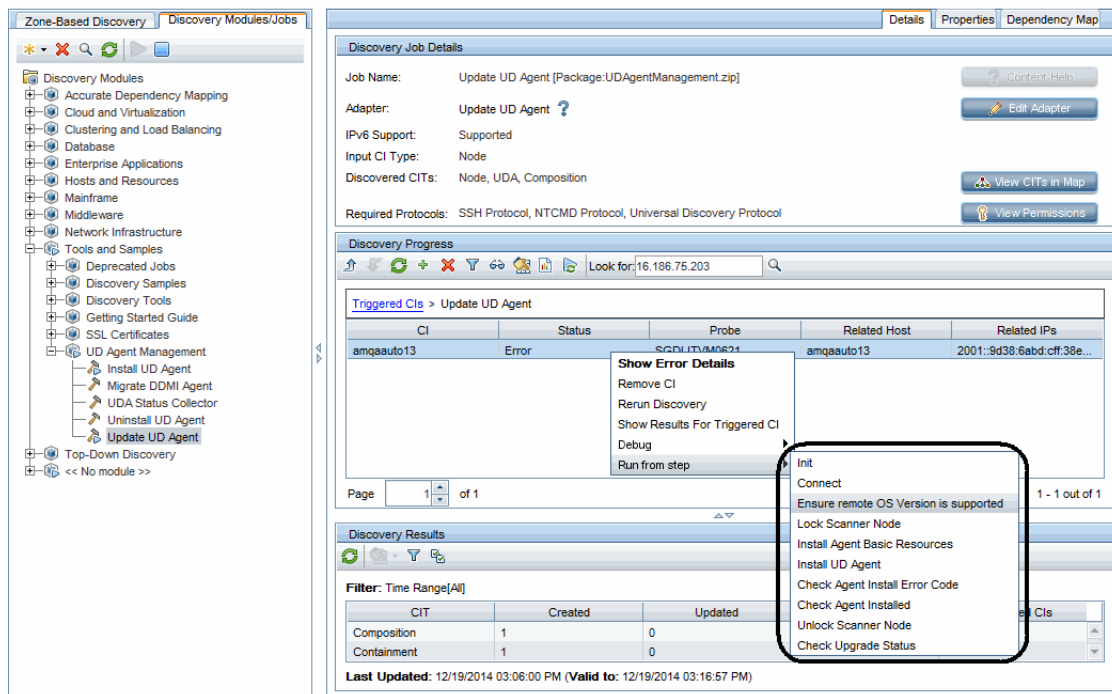
2. Return to the Universal Discovery window, right-click the returned entry, from the context menu, select **Debug > View Communication Log**

For details, see ["How to check device related logs for a discovered device?"](#) on page 123.

Update UD Agent

To invoke discovery job relevant to the device manually, and check progress and status of the discovery job:

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Update UD Agent**.
3. Right-click **Update UD Agent**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an action>**.



The screenshot displays the UCMDB interface for the 'Update UD Agent' discovery job. The left pane shows the 'Discovery Modules/Jobs' tree with 'Update UD Agent' selected under 'Tools and Samples > UD Agent Management'. The main pane shows the 'Discovery Job Details' for 'Update UD Agent [Package:UDAgentManagement.zip]'. Below this is the 'Discovery Progress' section, which includes a 'Triggered CIs' table. The table has columns for CI, Status, Probe, Related Host, and Related IPs. One entry, 'amqaauto13', is listed with a status of 'Error'. A context menu is open over this entry, showing options like 'Show Error Details', 'Remove CI', 'Rerun Discovery', 'Show Results For Triggered CI', 'Debug', and 'Run from step'. The 'Run from step' option is highlighted, and a sub-menu is open, listing actions such as 'Init', 'Connect', 'Ensure remote OS Version is supported', 'Lock Scanner Node', 'Install Agent Basic Resources', 'Install UD Agent', 'Check Agent Install Error Code', 'Check Agent Installed', 'Unlock Scanner Node', and 'Check Upgrade Status'. The 'Discovery Results' section at the bottom shows a table with columns for CIT, Created, and Updated, with data for 'Composition' and 'Containment'.

CIT	Created	Updated
Composition	1	0
Containment	1	0

Last Updated: 12/19/2014 03:06:00 PM (Valid to: 12/19/2014 03:16:57 PM)

7. To check the progress/on-going status of the discovery job,

- a. Modify the Update UD Agent adapter's configuration to make sure that the communication log is always created.


For detailed instructions, see ["To check the progress/on-going status of the discovery job," on page 127.](#)

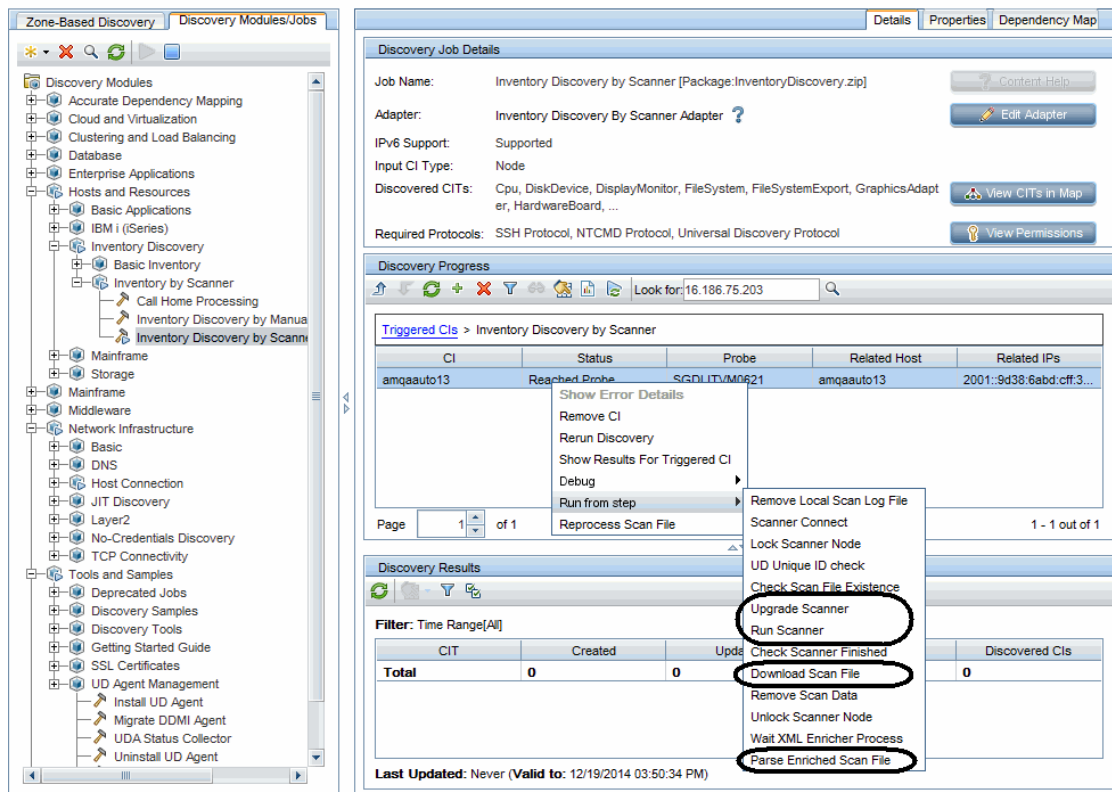
- b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

For details, see ["How to check device related logs for a discovered device?" on page 123.](#)

Upgrade Scanner / Run Scanner / Download Scan File / Parse Enriched Scan File / Run Agentless Scanner



To invoke discovery job relevant to the device manually, and check progress and status of the discovery job:

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
3. Right-click **Inventory Discovery by Scanner**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.
5. In the **Look for** field that is just enabled, enter the IP address for the scanner and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an action>**.



Note: To Run Agentless Scanner, before selecting a **Run from step** option, set Universal Discovery Protocol scope to **Probes: Disabled**.

To do so,

- In the Data Flow Management module, go to **Data Flow Probe Setup**.
- Expand **Domains and Probes > DefaultDomain(Default) > Credentials > Universal Discovery Protocol**.
- In the right Universal Discovery Protocol pane, right-click a protocol and select **Edit**.
- In the Universal Discovery Protocol Parameters dialog box, click the **Edit**  button for the Network Scope field.
- In the Scope Definition dialog box, click the **Edit**  button for the Selected Probes section.

f. In the Selected Probes dialog box, clear the check box for **All Data Flow Probes** and click **OK** three times to exit.

g. Repeat [step c](#) through [step f](#) for other protocols.



Index	Scope	UD SHA1 ID	User Label	Port Number
1	Probes: Disabled	76d388aed5256fc385f27...	Universal Discovery Pro...	2738

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

7. To check the progress/on-going status of the discovery job,

a. Modify the Inventory Discovery by Scanner adapter's configuration to make sure that the communication log is always created.

For detailed instructions, see ["To check the progress/on-going status of the discovery job," on page 127.](#)


b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log.**

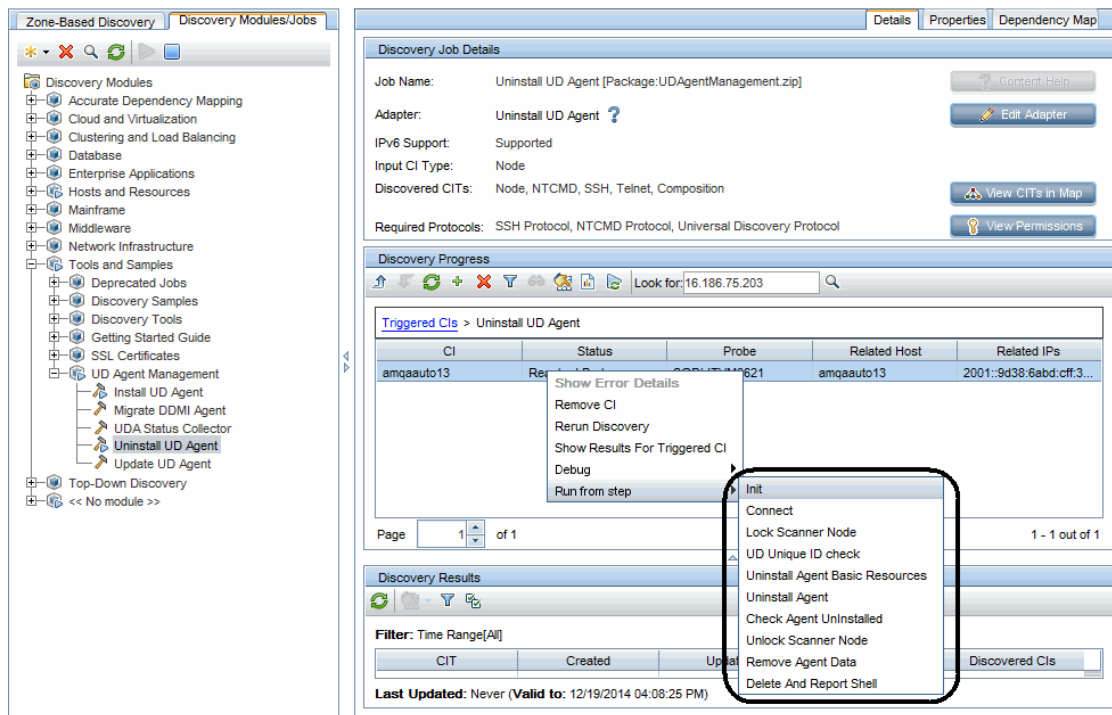
For details, see ["How to check device related logs for a discovered device?" on page 123.](#)

Uninstall Agent

To invoke discovery job relevant to the device manually, and check progress and status of the discovery job:

1. In UCMDDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Uninstall UD Agent.**
3. Right-click **Uninstall UD Agent**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.

5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Run from step** > **<Select an action>**.



7. To check the progress/on-going status of the discovery job,
 - a. Modify the Uninstall UD Agent adapter's configuration to make sure that the communication log is always created.

For detailed instructions, see ["To check the progress/on-going status of the discovery job,"](#) on page 127.

- b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug** > **View Communication Log**.

For details, see ["How to check device related logs for a discovered device?"](#) on page 123.

Rerun Discovery

The Run Rulebase feature is implemented in UD normalization, which covers all jobs.

To invoke the normalization manually, in the Discovery Progress pane, right-click the CI entry returned from your search and select **Rerun Discovery** from the context menu, which will perform the normalization.

Note: Normalization cannot be invoked alone in UD. By selecting **Rerun Discovery**, you can invoke the normalization, but would also trigger other operations included in the discovery job in addition to the normalization.

To check the progress/on-going status of the discovery job,

1. Modify the concerning adapter's configuration to make sure that the communication log is always created.


For detailed instructions, see ["To check the progress/on-going status of the discovery job," on page 127.](#)

2. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log.**

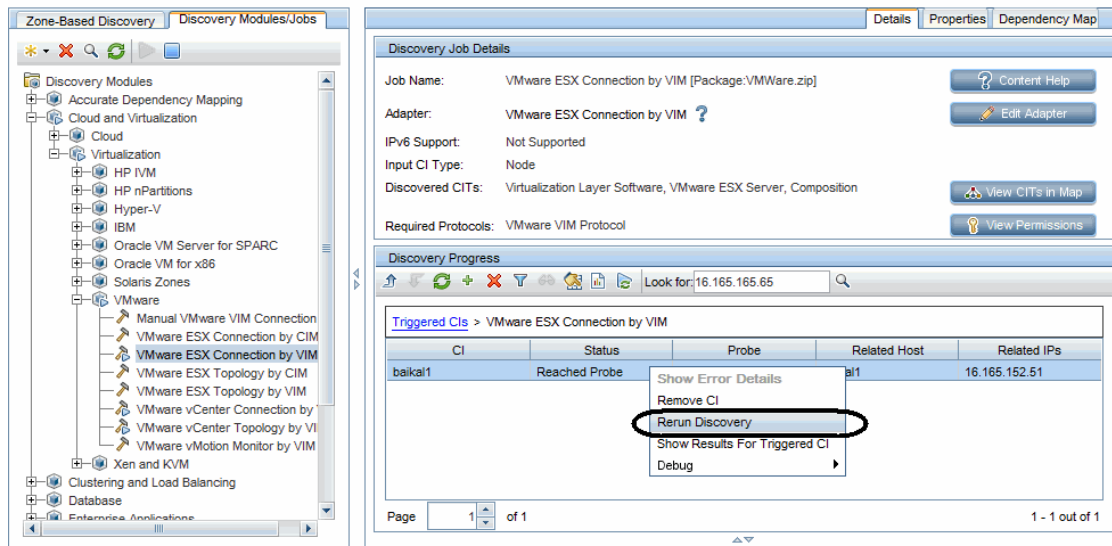
For details, see ["How to check device related logs for a discovered device?" on page 123.](#)

VMware Discovery Jobs

To invoke the VMware discovery job manually,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Cloud and Virtualization > VMware > <select a job>.**
3. Right-click the selected job, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .

6. Right-click the returned entry, and select **Rerun Discovery** from the context menu.



7. To check the progress/on-going status of the discovery job,

- a. Modify the concerning adapter's configuration to make sure that the communication log is always created.

For detailed instructions, see ["To check the progress/on-going status of the discovery job," on page 127.](#)

- b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.


For details, see ["How to check device related logs for a discovered device?" on page 123.](#)

How to check which pattern (management zone) is used in the discovery for a discovered device?

Question: For a discovered device, how should I check which pattern (management zone) is used in the discovery?

In UD, there are two ways to check the management zone used:

- **From IT Universe Manager**

- In the Modeling module, go to **IT Universe Manager**.
- On the Search CIs tab, enter the IP address for a discovered device in the **CI Name** field, select **Managed Object** for the **CI Type** field, and click .
- Click the returned entry on the Search CIs tab. CI details are displayed in the right pane.
- Go to the **Properties** tab for the CI and check the value for the following attributes:
 - Created By
 - Updated By

For example,

Create Time	Thu Dec 4 2014 10:36 PM IST
Created By	UCMDBDiscovery: MZ_SGDLITVM0567 test_infrastructure_Network_Range IPs by ICMP
Deletion Candidate Period	

UcldbRoutingDomain	DefaultDomain
Updated By	UCMDBDiscovery: MZ_SGDLITVM0567 test_infrastructure_Network_Host Connection by Shell
User Label	

- **From the Management Zone Description**

- In the Data Flow Management module, go to **Universal Discovery > Zone-Based Discovery**.
- From the Management Zones tree, select a management zone. The Management Zone description displays in the right pane.

For example

Management Zone:SGDLITVM0567_AIX Machines

Description:

Ranges Method: Based on partial Data Flow Probe ranges

Ranges:

Domains and Probes

DefaultDomain

QASERVER7

Range	Type
16.157.130.92	Data Center
16.157.132.236	Data Center
16.157.132.237	Data Center
16.173.232.59	Data Center

How to check detailed discovery settings used in the discovery for a discovered device?

Question: For a discovered device, how should I check the detailed discovery settings (such as job parameters and scan settings) used in the discovery?

In UD, there are two ways to check detailed settings used in the discovery:

- **From UI** (the Properties tab and the Edit Inventory Discovery Activity dialog box)
 - Run jobs in **Discovery Modules/Jobs**

The Properties tab of the Inventory Discovery by Scanner job displays all parameters and scanner settings of the job

- i. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
- ii. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
- iii. In the pane, go to the **Properties** tab.

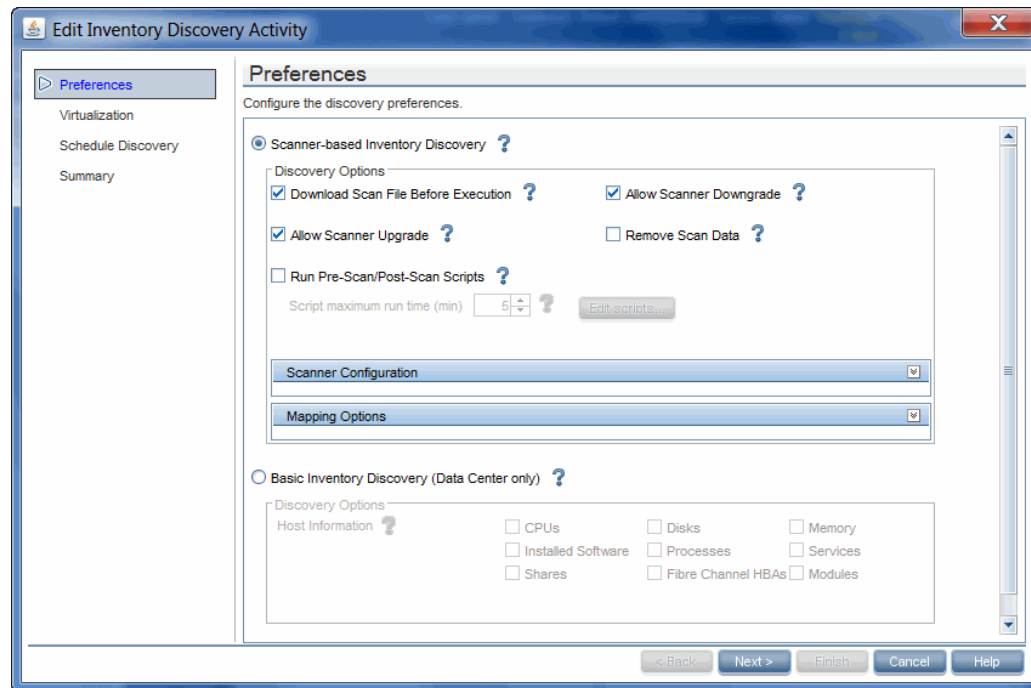
All parameters and scanner settings of the job are displayed.

Override	Name	Value
<input type="checkbox"/>	DownloadScanFileBeforeExecution	true
<input type="checkbox"/>	IsPrePostScriptAllowed	false
<input type="checkbox"/>	IsScannerDowngradeAllowed	true
<input type="checkbox"/>	IsScannerUpgradeAllowed	true
<input type="checkbox"/>	MappingConfiguration	Scan file model mapping configurations
<input type="checkbox"/>	P2PServerPorts	*
<input type="checkbox"/>	PrePostScriptExecTimeout	5
<input type="checkbox"/>	RemoveScanData	false
<input type="checkbox"/>	ScannerConfigurationFile	use file c:\default.ccx for all platforms
<input type="checkbox"/>	ScannerLogLevel	info
<input type="checkbox"/>	collectIPv6Connectivity	false
<input type="checkbox"/>	discoverProcesses	false
<input type="checkbox"/>	discoverRunningSW	Microsoft Hyper-V Hypervisor, VMware VirtualC...
<input type="checkbox"/>	enableStamping	true
<input type="checkbox"/>	filterP2PProcessesByName	system,svchost.exe,lsass.exe,System Idle Proc...
<input type="checkbox"/>	ignoreP2PLocalConnections	false
<input type="checkbox"/>	onlyStampingClient	true

- Run jobs in **Zone-Based Discovery**
 - i. In the **Data Flow Management** module, go to **Universal Discovery > Zone-Based Discovery**.

- ii. From the Management Zones tree, select a management zone.
- iii. Right-click a discovery job and select **Edit** from the context menu.

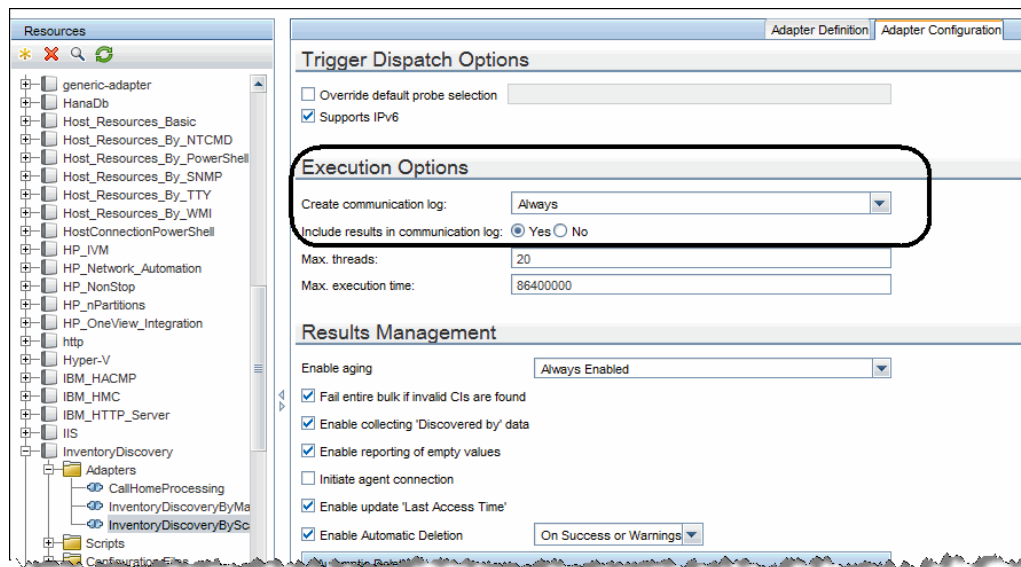
The Edit Discovery Activity dialog box opens.




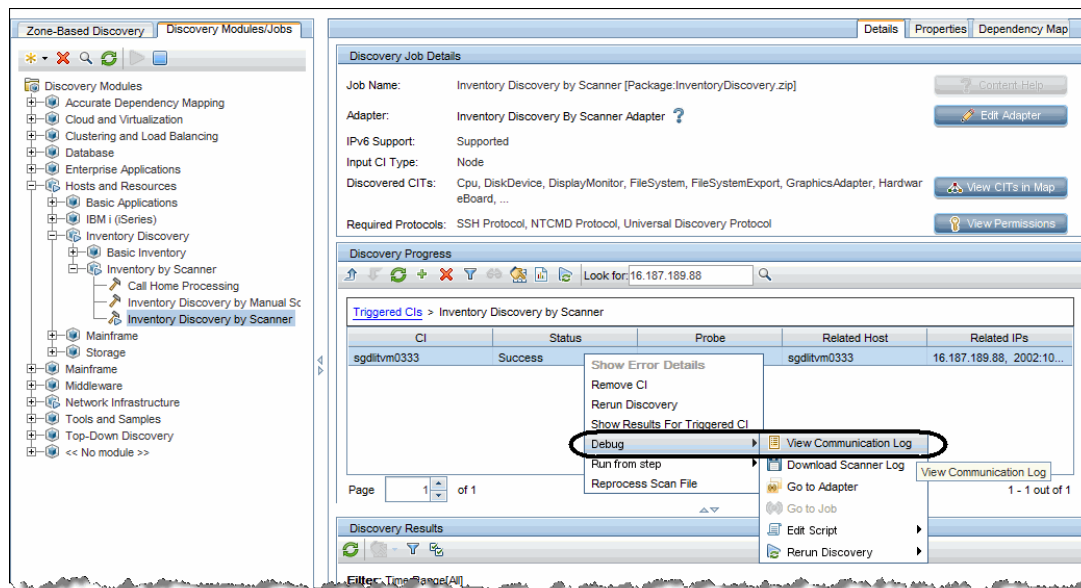
You can find the discovery job parameters and scanner settings in this dialog box.

- From the **Communication Log**
 - a. Modify the configuration of the adapter for the Inventory Discovery by Scanner job to make sure that the communication log is always created.
 - i. In the Data Flow Management module, go to **Adapter Management**.
 - ii. In the Resources pane, expand **InventoryDiscovery > Adapters > InventoryDiscoveryByScanner**.
 - iii. In the right pane, click the **Adapter Configuration** tab.
 - iv. In the Execution Options section, set the following:
 - **Create communication log: Always**

- **Include results in communication log: Yes**



- In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
- In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
- (Optional) Right-click **Inventory Discovery by Scanner**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
- In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.
- In the **Look for** field that is just enabled, enter the IP address for the scanner and click .
- Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.



h. In the log that opens, search keywords to check details:


- To locate where the job parameters start in the log, search **<params>**.
- To locate where the job parameters end in the log, search **</params>**.
- To locate where the scanner configuration file is used in the log, search **Config file to be used:**.

How to check the SNMP credentials used in the discovery for a discovered device?

Question: For a discovered device, how should I check the SNMP credentials used in the discovery?

To check the SNMP credentials used in the discovery, you can search the Communication Log of the Host Connection by SNMP job.

To view communication log for agent related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Network Infrastructure > Host Connection > Host Connection by SNMP**.
3. (Optional) Right-click **Host Connection by SNMP**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.
7. In the log that opens, search **<CONNECT start** as keyword to locate the entry in the log that indicates starting from when the device is connected.

For example:

```
<CONNECT start="08:05:20" duration="4" CMD="client_connect" RESULT="success"
type="snmp" credentialsId="7_1_CMS">
  <ClientProperties>
    <prop name="protocol_index" value="1" />
    <prop name="protocol_timeout" value="3000" />
    <prop name="credentialsId" value="7_1_CMS" />
    <prop name="cm_credential_id" value="7_1_CMS" />
    <prop name="snmpprotocol_version" value="version 2c" />
    <prop name="protocol_type" value="snmpprotocol" />
```

```

    <prop name="snmpprotocol_postfix" value="" />
    <prop name="port" value="161" />
    <prop name="protocol_netaddress" value="DEFAULT" />
    <prop name="ip_address" value="16.187.190.19" />
    <prop name="snmpprotocol_privalg" value="3DES" />
    <prop name="snmpprotocol_authalg" value="MD5" />
    <prop name="protocol_port" value="161" />
    <prop name="snmpprotocol_retry" value="2" />
    <prop name="snmpprotocol_snmpmethod" value="getnext" />
    <prop name="user_label" value="SNMP Protocol Credential 1" />
    <prop name="snmpprotocol_authmethod" value="noAuthNoPriv" />
    <prop name="retry" value="2" />
    <prop name="protocol_username" value="" />
    <prop name="protocol_in_use" value="false" />
  </ClientProperties>
</CONNECT>

```

This log example indicates that the device is connected successfully by SNMP and the credential ID is **7_1_CMS**.

The log information between the **<ClientProperties>** and **</ClientProperties>** tags are the details of the SNMP credential used in the discovery. Among these properties information, to find out the credential name, you can check the value for the **user_label** attribute (highlighted above) of the SNMP credential that you defined in the SNMP protocol.

Note: The SNMP community strings you defined in the protocol are encrypted in UD, therefore they are not visible in the log.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on DDMI to Universal Discovery Migration Walkthrough Guide (Universal CMDB 10.22)

Just add your feedback to the email and click send.

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

We appreciate your feedback!