HPE IMC Centralized Deployment Guide with Remote Database

Abstract
This document describes the processes and procedures to follow when deploying the HPE Intelligent Management Center in addition to the procedures for upgrading, removing, registering, backup, and restore. This document is intended for use by network engineers or system administrators responsible for installing network software and components.
The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.


Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are trademarks of the Microsoft group of companies.

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

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.
8 Upgrading IMC ................................................................. 62
   Preparing for the upgrade .............................................. 62
   Upgrading IMC .................................................................. 62
   Upgrading the IMC platform ............................................. 62
   Restoring IMC ................................................................. 69
9 Uninstalling IMC .............................................................. 70
   Uninstalling an IMC component ........................................ 70
   Uninstalling all IMC components at a time ........................ 70
10 Registering IMC and incremental node licenses .................. 72
   Registering IMC ............................................................... 72
   Registering first license .................................................. 72
   Registering incremental node licenses .............................. 76
   Activating IMC ............................................................... 77
   Registering the IMC license for stateful/stateless failover .... 78
   Registering the IMC license for stateful failover ................. 78
   Registering the IMC license for stateless failover .............. 79
11 Security settings ............................................................ 82
   Anti-virus software ......................................................... 82
   Port settings ................................................................... 82
12 Backing up and restoring the database ............................... 84
   Configuration restrictions and guidelines ......................... 85
   Installing and upgrading DBMan on the database server .... 85
   Installing DBMan ............................................................ 85
   Upgrading DBMan .......................................................... 88
   Backing up and restoring databases for a single IMC system 89
   Backing up databases ...................................................... 89
   Restoring databases ....................................................... 91
   Backing up and restoring databases in stateless failover scenarios 92
   Backing up databases ...................................................... 92
   Restoring databases ....................................................... 93
13 FAQ ........................................................................... 95
1 Overview

The following information describes how to deploy IMC in centralized mode and to use a remote database. This deployment scheme scales to networks from 200 to 10000 devices.

IMC components

IMC includes the IMC platform and service components.

IMC platform

The IMC platform is the base component to provide IMC services and includes the following subcomponents:

- Resource Management
- Alarm Management
- User Selfservice Management
- Guest Access Management
- Intelligent Configuration Center
- Report Management
- Network Element (NE) Management
- Performance Management
- ACL Management
- Network Asset Management
- Security Control Center
- General Search Service Management
- Syslog Management
- VLAN Management
- Virtual Resource Management
- Server & Storage Automation

Service components

Service components are optional and purchased separately from the IMC platform. The IMC platform is the basis for implementing various services and must be installed before you install a service component.

The service components are as follows:

- **User Access Manager (UAM)**—Provides policy-based AAA (Authentication, Authorization and Accounting) services. UAM software extends management to wired, wireless and remote network users and enables the integration of network device, user, guest and terminal management on a single unified platform.

- **TACACS+ Authentication Manager (TAM)**—Provides basic AAA functions for network device or IT users for network device management security. TAM can assign users with different privileges, monitor login and command execution operations, and simplify user management.

- **Endpoint Admission Defense (EAD) Security Policy**—Endpoint Admission Defense integrates security policy management and endpoint posture assessment to identify and isolate
risks at the network edge. The security policy component allows administrators to control endpoint admission based on an endpoint’s identity and posture.

- **MPLS VPN Manager (MVM)**—Provides functions such as VPN autodiscovery, topology, monitoring, fault location, auditing, and performance evaluation, as well as VPN and service deployment. MVM also contains a traffic engineering component that helps operators monitor an entire network and deliver service quality by distributing suitable network resources as needed.

- **IPsec VPN Manager (IVM)**—Provides features for all aspects of IPSec VPN management, which allows administrators to construct an IPSec VPN network, effectively monitor the operation and performance of the VPN network, and quickly locate device faults for full IPSec VPN lifecycle management.

- **Voice Service Manager (VSM)**—Provides a solution for reducing the voice network maintenance cost and improving maintenance efficiency. VSM is designed for enterprise-level voice networks.

- **Wireless Service Manager (WSM)**—Provides unified management of wired and wireless networks, adding network management functions into existing wired network management systems. WSM software offers wireless LAN (WLAN) device configuration, topology, performance monitoring, RF heat mapping, and WLAN service reports.

- **Network Traffic Analyzer (NTA)**—A graphical network-monitoring tool that provides realtime information about users and applications consuming network bandwidth. A reliable solution for enterprise and campus network traffic analysis, NTA defends the network against virus attacks and applies varying levels of bandwidth traffic to different services and applications.

- **User Behavior Auditor (UBA)**—Provides comprehensive log collection and audit functions supporting log formats such as NAT, flow, NetStreamV5, and DIG. UBA provides DIG logs to audit security-sensitive operations and digest information from HTTP, FTP, and SMTP packets.

- **Service Operation Manager (SOM)**—Allows IT organizations to adhere to ITIL v3.0, including IT services such as policy design, operation, and improvement. Based on a unified configuration management database (CMDB), SOM provides configurable flows and options for self service, as well as management of asset configuration, change, fault events, problem recognition, and auto-generation of a knowledge base.

- **Application Manager (APM)**—Allows administrators to visualize and measure the health of critical business applications and their impact on network performance. With the available data, administrators can easily determine which business process is affected and which application issues to prioritize.

- **QoS Manager (QoSM)**—Enhances visibility and control over QoS configurations and helps administrators focus on QoS service planning by providing a robust set of QoS device and configuration management functions. It allows administrators to organize traffic into different classes based on the configured matching criteria to provide differentiated services, committed access rate (CAR), generic traffic shaping (GTS), priority marking, queue scheduling, and congestion avoidance.

- **Service Health Manager (SHM)**—Provides visual service quality management functions. SHM integrates the alarm, performance, NTA, and NQA data. It uses key quality indexes and service level agreements to monitor and measure service health.

- **VAN Connection Manager (VCM)**—Provides a solution for physical network configuration migration. VCM tracks the startup, stopping, and migration of virtual machines (VMs), and according to the latest VM location, VCM deploys a physical network configuration. VCM allows collaboration for physical and virtual networks. It also provides compatibility between physical and virtual networks of different vendors.

- **Branch Intelligent Management System (BIMS)**—Provides support for service operations, delivering high reliability, scalability, flexibility, and IP investment returns. Based on the TR-069 protocol, IMC BIMS offers resource, configuration, service, alarm, group, and privilege management. It allows the remote management of customer premise equipment (CPE) in WANs.
- **Remote Site Manager (RSM)**—Securely extends the IMC core platform capability to remote sites by deploying remote agents. These agents manage and monitor the remote network, and apply policies and configurations to the remote network devices on behalf of the central IMC server.

- **Resource Automation Manager (RAM)**—Provides a solution for customizing network services for users and automatically deploying network services.

- **VAN SDN Manager (SDNM)**—Manages OpenFlow-based SDN. SDNM allows you to manage an OpenFlow network through RESTful APIs provided by H3C VCF Controller or HP SDN controllers. Combined with the device management, reports, and homepage widgets functions in the IMC platform, SDNM also allows you to perform visual management and monitoring on the OpenFlow network.

- **VAN Fabric Manager (VFM)**—Provides an integrated solution for managing both the LANs and SANs in data centers by working with HP devices. VFM depends on VRM to obtain virtual machine (VM) migration information.

- **Unified Communications Health Manager (UCHM)**—Provides a solution for monitoring the health status of networks deployed with Microsoft Lync Server. It allows you to manage network resources including the Lync Servers, PSTN gateways, and Lync client endpoints.

- **Intelligent Analysis Reporter (iAR)**—Extends the reporting capabilities within IMC to include customized reporting. iAR includes a report designer, which can save designs into report templates. Report formats include charts. Reports can be automatically generated at specified intervals and distributed to key stakeholders.

## IMC editions

The following editions of IMC are available:

- Enterprise
- Standard
- Basic

### Table 1 Differences between IMC editions

<table>
<thead>
<tr>
<th>Item</th>
<th>Basic</th>
<th>Standard</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>50</td>
<td>Extensible</td>
<td>Extensible</td>
</tr>
<tr>
<td>Hierarchical network management</td>
<td>Not supported</td>
<td>Lower-level NMS only</td>
<td>Supported</td>
</tr>
<tr>
<td>Distributed deployment</td>
<td>Not supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows</td>
<td>Windows and Linux</td>
<td>Windows and Linux</td>
</tr>
<tr>
<td>Embedded database</td>
<td>Supported</td>
<td>Supported only on Windows</td>
<td>Not supported</td>
</tr>
<tr>
<td>Separate database</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

For information about installing a separate database for IMC on Windows, see the following documents:

- [SQL Server 2008 Installation and Configuration Guide](#)
- [SQL Server 2008 R2 Installation and Configuration Guide](#)
- [SQL Server 2012 Installation and Configuration Guide](#)
- [SQL Server 2014 Installation and Configuration Guide](#)
- [MySQL 5.5 Installation and Configuration Guide](#)
- [MySQL 5.6 Installation and Configuration Guide](#)
For information about installing a separate database for IMC on Linux, see the following documents:

- Oracle 11g Installation and Configuration Guide
- Oracle 11g R2 Installation and Configuration Guide
- Oracle 12c Installation and Configuration Guide
- MySQL 5.5 Installation and Configuration Guide
- MySQL 5.6 Installation and Configuration Guide

Installation and deployment

IMC uses the install + deploy model:

- During installation, the installation package of the IMC component is copied to the server and loaded to the Intelligent Deployment Monitoring Agent.
- During deployment, the installation package is decompressed on the server and database scripts are created for the component.

The IMC components are operational only after they are deployed. In centralized deployment, all IMC components are installed and deployed on the same server.

IMC automatically creates a database user for each component when the component is deployed. HP recommends not modifying the database user configuration, including the database user password and password policy.

If the deployment or upgrade process is interrupted, IMC automatically stores logs in a compressed file in the \tmp directory of the IMC installation path. You can use the logs to quickly locate the problem or error.
2 Preparing for installation

Hardware requirements

The tables in this section use the following terminology:

- **Node**—IMC servers, database servers, and devices managed by IMC are called nodes.
- **Collection unit**—Represents a performance instance collected every 5 minutes. When a performance instance uses another collection interval, it corresponds to a number of collection units calculated with the formula: 5 minutes/instance collection interval in minutes.

For example, the collection interval is set to 10 minutes for all performance instances. A monitored device contains 1 CPU, 1 memory bar, and 10 interfaces. To collect performance data for CPU, memory, response time, reachability rate, and interface send and receive rates, the total collection units of the device are: \((1+1+1+(10 \times 2)) \times 5/10 = 12\).

- **Java heap size**—Java heap size that can be used by the IMC Web server.

To set the Java heap size for IMC:
- On Windows, run the `setmem.bat heap size` script in the `\client\bin` directory of the IMC installation path.
- On Linux, run the `setmem.sh heap size` script in the `/client/bin` directory of the IMC installation path.

Set `heap size` to a value in the range of 256 to 1024 for a 32-bit OS, or in the range of 256 to 32768 for a 64-bit OS. The java heap size cannot exceed the physical memory size.

To improve the I/O performance, follow these guidelines:
- When the number of the collection units is from 100 K to 200 K, install two or more disks and a RAID card with a cache of at least 256 MB.
- When the number of collection units is from 200 K to 300 K, install two or more disks and a RAID card with a cache of at least 512 MB.
- When the number of collection units is 300 K to 400 K, install four or more disks and a RAID card with a cache of at least 1 GB.

Optimal hardware requirements vary with scale, other management factors, and are specific to each installation. Please consult HP Support, or your local account teams for exact requirements. If service components are added to the IMC platform, be sure to read the release notes of each component.

**Table 2 Hardware requirements for 32-bit Windows operating system**

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nodes</td>
</tr>
<tr>
<td>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td>0 to 200</td>
<td>5 K to 50 K</td>
</tr>
<tr>
<td>200 to 500</td>
<td>0 to 10 K</td>
</tr>
<tr>
<td>200 to 500</td>
<td>10 K to 100 K</td>
</tr>
</tbody>
</table>
### Table 3 Hardware requirements for 64-bit Windows operating system

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nodes</td>
</tr>
<tr>
<td>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td>0 to 200</td>
<td>5 K to 50 K</td>
</tr>
<tr>
<td>200 to 1 K</td>
<td>0 to 10 K</td>
</tr>
<tr>
<td>200 to 1 K</td>
<td>10 K to 100 K</td>
</tr>
<tr>
<td>1 K to 2 K</td>
<td>0 to 20 K</td>
</tr>
<tr>
<td>1 K to 2 K</td>
<td>20 K to 200 K</td>
</tr>
<tr>
<td>2 K to 5 K</td>
<td>0 to 30 K</td>
</tr>
<tr>
<td>2 K to 5 K</td>
<td>30 K to 300 K</td>
</tr>
<tr>
<td>5 K to 10 K</td>
<td>0 to 40 K</td>
</tr>
<tr>
<td>5 K to 10 K</td>
<td>40 K to 400 K</td>
</tr>
<tr>
<td>10 K to 15 K</td>
<td>0 to 40 K</td>
</tr>
<tr>
<td>10 K to 15 K</td>
<td>40 K to 400 K</td>
</tr>
</tbody>
</table>

### Table 4 Hardware requirements for 32-bit Linux operating system

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nodes</td>
</tr>
<tr>
<td>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td>0 to 200</td>
<td>5 K to 50 K</td>
</tr>
<tr>
<td>200 to 500</td>
<td>0 to 10 K</td>
</tr>
<tr>
<td>200 to 500</td>
<td>10 K to 100 K</td>
</tr>
</tbody>
</table>
Table 5 Hardware requirements for 64-bit Linux operating system

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes</td>
<td>Collection units</td>
</tr>
<tr>
<td>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td>0 to 200</td>
<td>5 K to 50 K</td>
</tr>
<tr>
<td>200 to 1 K</td>
<td>0 to 10 K</td>
</tr>
<tr>
<td>200 to 1 K</td>
<td>10 K to 100 K</td>
</tr>
<tr>
<td>1 K to 2 K</td>
<td>0 to 20 K</td>
</tr>
<tr>
<td>1 K to 2 K</td>
<td>20 K to 200 K</td>
</tr>
<tr>
<td>2 K to 5 K</td>
<td>0 to 30 K</td>
</tr>
<tr>
<td>2 K to 5 K</td>
<td>30 K to 300 K</td>
</tr>
<tr>
<td>5 K to 10 K</td>
<td>0 to 40 K</td>
</tr>
<tr>
<td>5 K to 10 K</td>
<td>40 K to 400 K</td>
</tr>
<tr>
<td>10 K to 15 K</td>
<td>0 to 40 K</td>
</tr>
<tr>
<td>10 K to 15 K</td>
<td>40 K to 400 K</td>
</tr>
</tbody>
</table>

Software requirements

Table 6 Software requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows Server 2008 (32-bit)</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 (64-bit)</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2</td>
<td>Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
<td>KB2836988</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
<td>N/A</td>
</tr>
<tr>
<td>Database</td>
<td>SQL Server 2008</td>
<td>Service Pack 3</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2008 R2</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2012</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2014</td>
<td>N/A</td>
</tr>
<tr>
<td>Item</td>
<td>Requirement</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>SQL Server 2008 R2 SP2 Express</td>
<td>Used as the embedded database for SNS and standard editions only.</td>
<td></td>
</tr>
</tbody>
</table>

### Linux

#### Operating system

<table>
<thead>
<tr>
<th>OS Version</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux Server 5.5 (32-bit)</td>
<td>N/A</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 5.5 (64-bit)</td>
<td>N/A</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 5.9 (32-bit)</td>
<td>N/A</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 5.9 (64-bit)</td>
<td>N/A</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 6.1 (64-bit)</td>
<td>N/A</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 6.4 (64-bit)</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Database

<table>
<thead>
<tr>
<th>Database</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 11g Release 1</td>
<td>N/A</td>
</tr>
<tr>
<td>Oracle 11g Release 2</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Both Linux and Windows

<table>
<thead>
<tr>
<th>Database</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL Enterprise Server 5.5</td>
<td>N/A</td>
</tr>
<tr>
<td>MySQL Enterprise Server 5.6</td>
<td>N/A</td>
</tr>
</tbody>
</table>

## VM requirements

HP recommends installing IMC on a physical server.

### Table 7 Hypervisor platform requirements

<table>
<thead>
<tr>
<th>OS</th>
<th>Hypervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>VMware ESX</td>
</tr>
<tr>
<td></td>
<td>Windows Hyper-V</td>
</tr>
<tr>
<td>Linux</td>
<td>H3C CAS</td>
</tr>
<tr>
<td></td>
<td>VMware ESX</td>
</tr>
</tbody>
</table>

### Table 8 Hypervisor platform requirements

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Hypervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>VMware Workstation 6.5.x</td>
</tr>
<tr>
<td></td>
<td>VMware Workstation 9.0.x</td>
</tr>
<tr>
<td></td>
<td>VMware ESX Server 4.x</td>
</tr>
<tr>
<td></td>
<td>VMware ESX Server 5.x</td>
</tr>
<tr>
<td>Hyper-V</td>
<td>Windows Server 2008 R2 Hyper-V</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 Hyper-V</td>
</tr>
</tbody>
</table>

If IMC is installed on a virtual machine, do not change the following virtual machine settings:

- CPU cores
- Number, model, and MAC addresses of network adapters
- Number of disk drives
- Storage paths
Assignment of storage

If the settings are changed, IMC might not operate correctly.

Preparing the installation environment

To ensure correct installation and operation of IMC, do not install IMC with other network management products on the same server.

Do not install IMC in an IPv6 environment.

Uninstalling previous versions of IMC

If IMC was previously installed on the system, thoroughly uninstall it first. For information about uninstalling IMC, see “9 Uninstalling IMC.”

After you uninstall IMC:

- On Windows, delete the **IMC-Reserved** folder from the **WINDOWS** folder of the system disk.
- On Linux, delete the **IMC-Reserved** folder from the **/etc** directory.

Checking ports and firewalls

Make sure the IMC Web service ports and database listening ports are open in the firewall. Table 9 lists the default IMC Web service ports and database listening ports for the IMC platform.

**Table 9 IMC port requirements**

<table>
<thead>
<tr>
<th>Server</th>
<th>Usage: protocol/default port</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td>HTTP: TCP/8080</td>
<td>Browser to IMC</td>
</tr>
<tr>
<td>Web</td>
<td>HTTPS: TCP/8443</td>
<td>Browser to IMC</td>
</tr>
<tr>
<td>Database</td>
<td>SQL Server database: TCP/1433</td>
<td>IMC and components to the database</td>
</tr>
<tr>
<td>Database</td>
<td>Oracle database: TCP/1521</td>
<td>IMC and components to the database</td>
</tr>
<tr>
<td>Database</td>
<td>MySQL database: TCP/3306</td>
<td>IMC and components to the database</td>
</tr>
</tbody>
</table>

**NOTE:**

Other IMC components might have additional port requirements. For more information, see “11 Security settings.”

Make sure the **javaw.exe** and **java.exe** programs are not blocked by the firewall. On Windows, these programs are located in the **\common\jre\bin** directory of the IMC installation path. On Linux, these programs are located in the **/common/jre/bin/java** directory of the IMC installation path.

Use tools such as **netstat -a** and **telnet hostname port** to verify access between systems.

Checking the database configuration

Before you install IMC, make sure the database server and client are correctly installed and configured.
IMC uses a local database client to communicate with a remote database server. The client version must match the version of the database server.

On the remote database server, you must create a data file folder for storing IMC data. You will need to specify the path to the folder during IMC installation.

Additional database requirements vary by the database type: SQL Server or Oracle.

For a SQL Server database, the following requirements must be met:

- Set the startup type of the SQL Server and SQL Server Agent services to Automatic.
  To view the service startup type, click Start, and then select Administrative Tools > Services.
- The startup account of the SQL Server service must have write permissions to all disks on the database server. HP recommends using the Local System account.

For an Oracle database, the following requirements must be met:

- Configure the Oracle database service to start automatically with the operating system.
- The database server and client use the same network service name, which contains the IP address of the database server as the host name.

Checking the installation environment

The IMC installation package provides a tool (envcheck) to check the system environment and database connectivity.

To use the envcheck tool:

1. Copy the envcheck tool (envcheck.bat for Windows or envcheck.sh for Linux) from the tools folder to the install folder of the IMC installation package.
2. Run the tool.
   The Checking installation environments dialog box appears.
   The system checks the port availability, free physical memory, and legacy database server or client.
   After the checks are complete, the Checking installation parameters dialog box appears, as shown in Figure 1. The following information uses Windows and Microsoft SQL Server as an example.
3. Configure the parameters for checking database connectivity:
   - **Database Type**—Select the database type. Options are **Microsoft SQL Server**, **MySQL**, and **Oracle**. The default is **Microsoft SQL Server**.
   - **Instance Name**—To connect to the default instance of the database, select **Default Instance**. To connect to a named instance, select **Other Instance** and enter the instance name.

   **NOTE:**
   If you install IMC on Linux and use an Oracle database, the **Network Service Name** parameter appears instead of **Instance Name**. You can select a network service name or click the **Add Network Service Name** icon to add a network service name. For information about configuring the network service name, see Oracle 11g Installation and Configuration Guide or Oracle 11g R2 Installation and Configuration Guide.

   - **Superuser**—Enter the database superuser name. The default is **sa**.
   - **Password**—Enter the password of the superuser.
   - **Database Location**—Select **other server** from the list.
   - **Database Server Address**—Enter the IP address of the database server.
   - **Listening Port**—Enter the listening port of the database server. The default is **1433**.
   - **Installation Location**—Specify the local directory for storing the IMC installation package.
   - **Data File Location**—Specify the directory on the database server for storing IMC data files. Make sure the specified data file location exists on the database server and does not include any files.
   - **HTTP Port**—Enter the HTTP port number for the IMC Web server. The default is **8080**.
   - **HTTPS Port**—Enter the HTTPS port number for the IMC Web server. The default is **8443**.

4. Click **OK**.
The **Checking installation environments** dialog box displays the check results, as shown in Figure 2.

**Figure 2** Check results

<table>
<thead>
<tr>
<th>Checking port occupied...</th>
<th>Passed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking physical memory size...</td>
<td>Passed</td>
</tr>
<tr>
<td>Checking database installation...</td>
<td>Passed</td>
</tr>
<tr>
<td>Checking database connectivity...</td>
<td>Passed</td>
</tr>
</tbody>
</table>

5. Click **Exit**.

Fix any failed check items according to the check results.

**Superuser account**

Before IMC installation, obtain the password of the database superuser account or other database user accounts that have superuser privileges.

During the IMC platform installation, IMC uses the superuser account and password for database access, and then creates database files and user accounts for each deployed component. The deployed IMC platform subcomponents and service components use their own user accounts for database access.

If the password of the superuser account is changed after IMC deployment, be sure to update the password in IMC. If the password is not promptly updated, you cannot view database information on the **Environment** tab, deploy new components, or update existing components for IMC.

To update the database user password in IMC:

1. Start the Intelligent Deployment Monitoring Agent and click the **Environment** tab.
2. Click **Change Password**.

   The **Change Password** button appears only when the Intelligent Deployment Monitoring Agent detects an incorrect database user password.

3. Enter the new database password and click **OK**, as shown in **Figure 3**.
Table 10 lists the default superuser accounts of SQL Server, MySQL, and Oracle databases.

Table 10 Database superuser accounts

<table>
<thead>
<tr>
<th>Database</th>
<th>Superuser</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server</td>
<td>sa</td>
</tr>
<tr>
<td>Oracle</td>
<td>system, sys</td>
</tr>
<tr>
<td>MySQL</td>
<td>root</td>
</tr>
</tbody>
</table>

Setting the system time

HP recommends the following settings:
- Set the time zone to GMT or Coordinated Universal Time.
- Do not enable seasonal time adjustments such as daylight savings time.
- Before installing IMC, verify that the system time, date, and time zone settings on the server are correct.

After IMC is started, do not modify the system time on the server. Otherwise, problems might occur, including:
- When jumping to a future time, the system might get so occupied in processing the sudden burst of expired data that realtime data sampling will be delayed. The delay is automatically recovered after the processing of expired data is complete.
• When you modify the system time to a past time, data with overlapping time occurs, and data processing might become abnormal. After the overlapping time is past, data processing becomes normal again.
3 Installing and deploying the IMC platform

The following information describes how to install and deploy the IMC platform on a Windows host that uses a remote SQL Server database.

Selecting the installation type

1. Log on to Windows as an administrator.
2. Run the install.bat script in the install directory of the IMC installation package.
   The Select Locale dialog box appears, as shown in Figure 4.
   
   **Figure 4** Select Locale dialog box

3. Select the country/region, language, and installation type.
   IMC supports typical and custom installations.
   o **Typical**—In typical installation mode, all platform subcomponents are automatically installed and deployed on the local host without manual intervention.
   o **Custom**—In custom installation mode, you can select desired platform subcomponents to install on the local host. After installation is complete, you must manually deploy the platform subcomponents.
4. Click OK.

To install the IMC platform on a Linux host, use the following guidelines:
   - Run the install.sh script in the install directory of the IMC installation package as a root user.
   - If Linux 6.x is used, copy the IMC installation package to a local directory before you run the install.sh script.
- If the IMC installation package is transferred through FTP, grant read access to the install.sh script by executing `chmod -R 775 install.sh` in the directory of the script.

### Installing the IMC platform in typical mode

1. In the **Select Locale** dialog box, select the **Typical** installation type and click **OK**. The **Checking installation parameters** dialog box appears, as shown in Figure 5.

   **Figure 5** Checking installation environment

   ![Checking installation environment](image)

2. Configure the parameters as needed. In this example, enter the password of the database superuser **sa**, use the default settings for other parameters, and click **OK**.

   The system checks the installation environment and database connectivity, and then displays the check results.

   Fix any failed check items according to the check results.

   After the checks are passed, the system installs and deploys all IMC platform subcomponents.

   After IMC installation and deployment is complete, the **Batch deploy succeeded** dialog box appears, as shown in Figure 6.
3. Click OK.

**Installing the IMC platform in custom mode**

1. In the Select Locale dialog box, select the Custom installation type and click OK. The Checking Database Connectivity dialog box appears, as shown in Figure 7.

2. Configure the parameters as needed.
   In this example, enter the password of the database superuser sa, use the default settings for other parameters, and click OK.
   The system checks the installation environment and database connectivity, and then displays the check results.
Fix any failed check items according to the check results.
After the checks are passed, the IMC installation wizard appears, as shown in Figure 8.

**Figure 8 IMC installation wizard**

3. Click **Next**.
   The **Agreement** page appears, as shown in **Figure 9**.
4. Read the license agreement, select **Accept**, and click **Next**.
   The **Choose Target Folder** page appears, as shown in Figure 10.
5. Select the components you want to install and specify a local path as the installation location. The installation program checks whether the specified installation path contains any files. If the path contains files, a message is displayed. Click OK to delete the files.

The default installation location is X:\Program Files\iMC, where X is the drive letter of the disk that has the largest amount of free space.

**NOTE:**
- If you install the IMC platform on a Linux host, do not use a symlink path as the installation location.
- On Linux, the default installation location is /opt/iMC.

6. Click Next.

The **Deployment and Upgrade Options** page appears, as shown in Figure 11.
7. Select **Deploy or upgrade later**.
8. Click **Next**.

The **Installation Summary** page appears, as shown in **Figure 12**.
9. Verify the installation summary and click **Install**.

After the installation is complete, the **Installation Completed** page appears, as shown in Figure 13.
10. Select **Open deployment monitoring agent** and click **Finish**.
    The system automatically starts the Intelligent Deployment Monitoring Agent and displays the **Batch deploy** dialog box, as shown in **Figure 14**.

**Figure 14** Batch deploy dialog box
11. Select the components to be deployed and click **OK**.

The **Database Configuration** page appears, as shown in Figure 15.

**Figure 15** Database Configuration page

12. Enter the password of the superuser.

13. In the **Data File Location** field, enter the data file folder you created on the database server.

Make sure the specified data file location is on a readable, writable, and uncompressed disk drive and does not include any files.

14. Click **Next**.

The **Configure Web Service Port** page appears, as shown in Figure 16.
15. Enter the HTTP and HTTPS port numbers. This example uses the default port numbers 8080 and 8443.
   If you specify other port numbers, make sure the specified ports are not used by other services.

16. Click **Deploy**.
   After the deployment is complete, the **Batch deploy succeeded** dialog box appears, as shown in Figure 17.

**Figure 17** Batch deploy succeeded dialog box

17. Click **OK**
4 Managing IMC by using the Intelligent Deployment Monitoring Agent

The Intelligent Deployment Monitoring Agent is automatically installed after the IMC platform is installed.

As the IMC management and maintenance tool, the Intelligent Deployment Monitoring Agent provides IMC operation information as well as a variety of management options, such as:

- Starting and stopping IMC.
- Installing new components.
- Upgrading existing components.
- Deploying and removing components.

Starting the Intelligent Deployment Monitoring Agent

Click Start, and then select All Programs > HP Intelligent Management Center.

The Intelligent Deployment Monitoring Agent appears.

As shown in Figure 18, the agent contains the following tabs: Monitor, Process, Deploy, and Environment. By default, the Monitor tab is displayed.

The following information describes the functionality of each tab.
NOTE:
To start the Intelligent Deployment Monitoring Agent on Linux, run the `dma.sh` script in the `/deploy` directory of the IMC installation path.

Monitor tab

As shown in Figure 19, the Monitor tab displays the performance information of the IMC server, including the disk, CPU, and physical memory usage information.

The tab also provides the following options:

- **Start iMC**—Click this button to start IMC. This button is available when IMC is stopped.

  IMPORTANT:
  For correct operation, the **HP iMC Server** service must start with an account that has read/write permissions on the IMC installation folder. By default, the **HP iMC Server** service starts with the **Local System** account.

- **Stop iMC**—Click this button to stop IMC. This button is available when IMC is already started.

- **Automatically start the services when the OS starts**—Select this option to automatically start IMC when the operating system starts.

- **Install**—Click this button to install new components or upgrade existing components.
Figure 19 Monitor tab of the Intelligent Deployment Monitoring Agent

Process tab

As shown in Figure 20, the Process tab displays IMC process information.
The right-click menu of a manageable process provides the following options:

- **Start Process**—Select this option to start the process. This option is available when the process is stopped.
- **Stop Process**—Select this option to stop the process. This option is available when the process is started.
- **Auto Start**—Select this option to enable automatic startup of the process when IMC is started.
- **Manual Start**—Select this option to require manual startup of the process.
- **Refresh Process Status**—Select this option to refresh the status of the process.

**Deploy tab**

As shown in Figure 21, the **Deploy** tab displays information about all deployed components.
The right-click menu of a component provides the following options:

- **Deploy the Component**—Select this option to deploy the component on the local host.
  
  This option is available only when the selected component is in **Undeployed** state.

- **Batch Deploy**—Select this option to batch deploy components on the local host.
  
  Components can be deployed only when they have been installed but in **Undeployed** state.

- **Undeploy the Component**—Select this option to undeploy the component.
  
  This option is available only when the selected component is in **Deployed** state.

- **Undeploy the Component (Master only)**—Select this option to delete component information from the master server.
  
  This option is available only when the subordinate server where the component is deployed cannot operate correctly.

- **Upgrade the Component**—Select this option to upgrade the component.

- **Batch Upgrade**—Select this option to upgrade components in batches.

- **Remove this Component**—Select this option to remove the component from the host.
  
  This option is available only when the selected component is in **Undeployed** state.

- **Show Pre-Requisites**—Select this option to view all components that the selected component depends on. The component can be deployed only after the dependent components have been deployed.
  
  This option is unavailable if the component does not depend on any other components.

- **Show Dependencies**—Select this option to view all components that depend on the selected component.
  
  This option is unavailable if no other components depend on the selected component.
Environment tab

As shown in Figure 22, the Environment tab displays the software, hardware, and database information for the current IMC server. The tab also provides database backup and restoration options in the Database Backup and Restore area. For more information, see "12 Backing up and restoring the database."

Figure 22 Environment tab of the Intelligent Deployment Monitoring Agent
5 Installing and deploying IMC service components

The following information describes how to install and deploy the service components. Table 11 lists all service components and subcomponents in IMC.

Table 11 Service components and subcomponents

<table>
<thead>
<tr>
<th>Component</th>
<th>Subcomponent</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Access Manager</td>
<td>• Intelligent Strategy Proxy</td>
</tr>
<tr>
<td></td>
<td>• User Access Management</td>
</tr>
<tr>
<td></td>
<td>• User Access Management Sub Server</td>
</tr>
<tr>
<td></td>
<td>• Portal Server</td>
</tr>
<tr>
<td></td>
<td>• EIP Server</td>
</tr>
<tr>
<td></td>
<td>• EIP Sub Server</td>
</tr>
<tr>
<td></td>
<td>• Policy Server</td>
</tr>
<tr>
<td></td>
<td>• Policy Proxy Server</td>
</tr>
<tr>
<td></td>
<td>• User SelfService</td>
</tr>
<tr>
<td></td>
<td>• Third-Party Page Publish Server</td>
</tr>
<tr>
<td>TACACS+ Authentication Manager</td>
<td>TACACS+ Authentication Manager</td>
</tr>
<tr>
<td>EAD Security Policy</td>
<td>• Security Policy Configuration</td>
</tr>
<tr>
<td></td>
<td>• Desktop Asset Manager</td>
</tr>
<tr>
<td></td>
<td>• Desktop Asset Manager Proxy Server</td>
</tr>
<tr>
<td>iNode DC</td>
<td>iNode Dissolvable Client</td>
</tr>
<tr>
<td>MPLS VPN Manager</td>
<td>• MPLS VPN Management</td>
</tr>
<tr>
<td></td>
<td>• MPLS TE management</td>
</tr>
<tr>
<td></td>
<td>• L2VPN Management</td>
</tr>
<tr>
<td>IPsec VPN Manager</td>
<td>IPsec VPN Manager</td>
</tr>
<tr>
<td>Voice Service Manager</td>
<td>Voice Service Manager</td>
</tr>
<tr>
<td>Wireless Service Manager</td>
<td>• Wireless Service Manager</td>
</tr>
<tr>
<td></td>
<td>• Wireless Intrusion Prevention System</td>
</tr>
<tr>
<td></td>
<td>• Wireless Location Manager</td>
</tr>
<tr>
<td></td>
<td>• Wireless Location Engine</td>
</tr>
<tr>
<td>Network Traffic Analyzer</td>
<td>• Network Traffic Analyzer</td>
</tr>
<tr>
<td></td>
<td>• Network Traffic Analyzer Server</td>
</tr>
<tr>
<td></td>
<td>• Network Behavior Analyzer</td>
</tr>
<tr>
<td></td>
<td>• Network Behavior Analyzer Server</td>
</tr>
<tr>
<td>User Behavior Auditor</td>
<td>• User Behavior Auditor</td>
</tr>
<tr>
<td></td>
<td>• User Behavior Auditor Server</td>
</tr>
<tr>
<td></td>
<td>• Network Behavior Analyzer</td>
</tr>
<tr>
<td></td>
<td>• Network Behavior Analyzer Server</td>
</tr>
<tr>
<td>Service Operation Manager</td>
<td>• CMDB Management</td>
</tr>
<tr>
<td></td>
<td>• Service Desk</td>
</tr>
<tr>
<td>Application Manager</td>
<td>Application Manager</td>
</tr>
<tr>
<td>QoS Manager</td>
<td>QoS Management</td>
</tr>
<tr>
<td>Service Health Manager</td>
<td>• Service Health Management</td>
</tr>
</tbody>
</table>
All the service components can be installed in the same way, but their deployment procedure might differ. Based on the deployment procedure, the service components can be classified into several categories, as shown in Table 12.

**Table 12** Service components classified by deployment procedure

<table>
<thead>
<tr>
<th>Example component</th>
<th>Similar components</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTA</td>
<td>IVM, VSM, WSM, UBA, SOM, APM, QoSM, SHM, VCM, BIMS, RSM, RAM, SDNM, VFM, UCHM, iNode DC</td>
</tr>
<tr>
<td>UAM</td>
<td>EAD, TAM</td>
</tr>
<tr>
<td>MVM</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The following information describes how to install and deploy NTA, UAM, and MVM.

## Installing and deploying IMC NTA

1. Start the Intelligent Deployment Monitoring Agent, and then click **Install** on the **Monitor** tab. The **Choose folder** dialog box appears, as shown in Figure 23.

   **Figure 23** Choose folder dialog box

2. Click **Browse** and select the `\install\components` folder in the NTA installation package.
3. Click **OK**. The IMC installation wizard appears, as shown in Figure 24.
4. Click **Next**.
   
The **Agreement** page appears, as shown in **Figure 25**.
5. Read the license agreement and third-party license and select Accept.
6. Click Next.
   The Choose Target Folder page appears, as shown in Figure 26.
   The Installation Location field is automatically populated with the installation location of the IMC platform and cannot be modified.
7. Select the NTA subcomponents you want to install.
8. Click Next.
   The Deployment and Upgrade Options page appears, as shown in Figure 27.
9. Select **Deploy or upgrade later**.
10. Click **Next**.

    The **Installation Summary** page appears, as shown in **Figure 28**.
11. Verify the installation information and click **Install**.
   After the installation is complete, the **Installation Completed** page appears, as shown in Figure 29.
12. Select **Open deployment monitoring agent** and click **Finish**.

The **Batch deploy** dialog box appears, as shown in Figure 30.
13. Select the NTA subcomponents you want to deploy.
   In this example, select all the NTA subcomponents.

14. Click OK.
   The system starts to deploy the selected NTA subcomponents.
   After the deployment is complete, the **Batch deploy succeeded** dialog box appears, as shown in Figure 31.

**Figure 31 Batch deploy succeeded dialog box**

15. Configure the **Start iMC Server now** option as needed and click OK.
Installing and deploying IMC UAM

1. Install IMC UAM in the same way IMC NTA is installed. For information about the procedure, see "Installing and deploying IMC NTA."

2. On the Installation Completed page shown in Figure 32, select Open deployment monitoring agent and click Finish.

Figure 32 Installation Completed page

The Batch deploy dialog box appears, as shown in Figure 33.
3. Select the UAM subcomponents you want to deploy and click **OK**. In this example, select all the UAM subcomponents except EIP Sub Server and User Access Management Sub Server.

The EIP Sub Server and User Access Management Sub Server subcomponents must be deployed on subordinate servers in distributed deployment.

The IMC deployment wizard starts and displays the **Strategy Proxy Server Configuration** page, as shown in Figure 34.
4. Configure the following parameters:
   o **IPv4 Address(Client)**—Enter the IP address of the Intelligent Strategy Proxy component. By default, this field is automatically populated with the IP address of the local host.
   o **IPv4 Address(Server)**—Enter the IP address of the User Access Management component. By default, this field is automatically populated with the IP address of the local host.

Modify the default settings only when the local host has multiple NICs and you want to associate Intelligent Strategy Proxy and User Access Management with different NICs.

5. Click **Deploy**.
   The **Configure User Access Management** page appears, as shown in Figure 35.
6. Configure the following parameters:
   o **Database Password/Confirm Password**—These fields are automatically populated with the password of the database superuser `sa` specified during IMC platform installation. If the database user password is changed after IMC platform installation, enter the new password in these fields.
   o **UAM Server's IPv4 Address**—This field is automatically populated with the IP address of the local host.

7. Click **Deploy**.
   The **Configure Portal Component** page appears, as shown in Figure 36.
8. Use the default settings and click **Deploy**.

   The **Configure EIP Server** page appears, as shown in **Figure 37**.
9. Use the default settings and click **Deploy**.

The **Configure Policy Server** page appears, as shown in Figure 38.
10. Use the default settings and click **Deploy**.

The **Configure User SelfService** page appears, as shown in **Figure 39**.
11. Use the default settings and click **Deploy**.
   
   The **Third-Party Page Publish Server Configuration** page appears, as shown in **Figure 40**.
12. Use the default settings and click **Deploy**.
   All the selected UAM subcomponents are deployed.
   The **Batch deploy succeeded** dialog box appears, as shown in **Figure 41**.

**Figure 41 Batch deploy succeeded dialog box**

13. Configure the **Start iMC Server now** option as needed and click **OK**.

**Installing and deploying IMC MVM**

1. Install IMC MVM in the same way IMC NTA is installed. For information about the procedure, see "Installing and deploying IMC NTA."
2. On the **Installation Completed** page shown in **Figure 42**, select **Open deployment monitoring agent** and click **Finish**.
Figure 42 Installation Completed page

The **Batch deploy** dialog box appears, as shown in Figure 43.
3. Select the MVM subcomponents you want to deploy and click **OK**.
In this example, select all the MVM subcomponents.

The **Please Choose L2VPN Global Parameter Operate** page appears, as shown in **Figure 44**.
4. Configure the L2VPN parameters as needed. VPLS can use either LDP or BGP for signaling. When BGP is selected, the VLL and PBB options become unavailable.

5. Click Deploy. After the deployment is complete, the **Batch deploy succeeded** dialog box appears, as shown in Figure 45.

**Figure 45** Batch deploy succeeded dialog box

6. Configure the **Start iMC Server now** option as needed and click **OK**.
6 Installing plug-ins

Installing DHCP plug-ins

To enable IMC to obtain endpoint names from a DHCP server, install the DHCP plug-in on the DHCP server.

Installing a DHCP plug-in on an MS DHCP server

1. On the IMC server, edit the `qvdm.conf` file to enable IMC to obtain endpoint names or FQDNs from DHCP servers:
   a. In the `\server\conf` directory of the IMC installation path, use Notepad to open the `qvdm.conf` file.
   b. Add the following line to the file:
      `l2topoPCNameDhcpSwitch=1`
   c. Save and close the file.
   d. Restart IMC in the Intelligent Deployment Monitoring Agent.

2. On the MS DHCP server, edit the `imf.cfg` file so that the DHCP server can communicate with IMC:
   a. Transfer the plug-in installation package `dhcp-plug-windows.zip` from the `\windows\tools` directory of the IMC installation package on the IMC server to the MS DHCP server.
   b. Decompress the installation package.
   c. Use Notepad to open the `imf.cfg` file in the `\dhcp-plug-windows\server\imf\server\conf` directory.
   d. Edit the `imf.cfg` file:
      - Set the value of `IMGAddress` to the IP address of the IMC server.
      - Set the value of `IMGPort` to the IMG port number, which is 8800 by default.
   e. Save and close the file.

3. Run the `install.bat` script in the `dhcp-plug-windows` directory.
   After the installation is complete, a new service `iMC DHCP Plug` is added to the system services.

4. Start the `iMC DHCP Plug` service:
   a. Click `Start`, and then select `Administrative Tools > Component Services`.
   b. On the `Component Services` page, select `Services (Local)` from the navigation tree.
   c. On the `Services (Local)` list, right-click the `iMC DHCP Plug` service and select `Start`.

To uninstall the DHCP plug-in, run the `uninstall.bat` script in the `dhcp-plug-windows` directory.

**IMPORTANT:**
Do not delete the directory where the plug-in installation package `dhcp-plug-windows.zip` is decompressed. If you delete the directory, you cannot uninstall the DHCP plug-in completely.
Installing a DHCP plug-in on a Linux DHCP server

1. On the IMC server, edit the qvdm.conf file to enable IMC to obtain endpoint names or FQDNs from DHCP servers:
   a. In the serverconf directory of the IMC installation path, use Notepad to open the qvdm.conf file.
   b. Add the following line to the file:
      ```
      l2topoPCNameDhcpSwitch=1
      ```
   c. Save and close the file.
   d. Restart IMC in the Intelligent Deployment Monitoring Agent.

2. On the Linux DHCP server, edit the imf.cfg file so that the DHCP server can communicate with IMC.
   a. Transfer the plug-in installation package dhcp-plug-linux.zip from the tools directory of the IMC installation package on the IMC server to the Linux DHCP server.
   b. Decompress the installation package.
   c. Use the vi editor to open the imf.cfg file in the /dhcp-plug-linux/server/imf/server/conf directory.
      ```
      vi imf.cfg
      ```
   d. Edit the imf.cfg file:
      - Set the value of IMGAddress to the IP address of the IMC server.
      - Set the value of IMGPort to the IMG port number, which is 8800 by default.
   e. Save and close the file.

3. Set the path of the dhcpd.leases file, which stores DHCP address allocation information:
   a. Determine the path of the dhcpd.leases file. The default path is /var/lib/dhcp.
   b. Use the vi editor to open the qvdm.conf file in the /dhcp-plug-linux/server/imf/server/conf directory, and then add the following line to the file:
      ```
      DhcpPlugIpAllocPath=<file-path>/dhcpd.leases
      ```
      Replace `<file-path>` with the path of the dhcpd.leases file.
   c. Save and close the file.

4. Run the install.sh script in the dhcp-plug-linux directory.

After the installation is complete, the system automatically starts the dhcp-plug service and adds the service to the system services.

To manually start the dhcp-plug service, execute the service dhcp-plug start command.

To stop the dhcp-plug service, execute the service dhcp-plug stop command.

To uninstall the DHCP plug-in, run the uninstall.sh script in the dhcp-plug-linux directory.

⚠️ IMPORTANT:

Do not delete the directory to which the plug-in installation package dhcp-plug-linux.zip is decompressed. If you delete the directory, you cannot uninstall the DHCP plug-in completely.

Installing VRM plug-ins

Virtual Resource Management (VRM) is a subcomponent of the IMC platform to manage virtual networks. VRM plug-ins include VRM Windows agents and VRM Linux agents.
Installing a VRM Windows agent

⚠️ CAUTION:
VRM Windows agents can be installed on Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. A Windows server can have only one VRM Windows agent.

Install VRM Windows agents for IMC to manage Microsoft Hyper-V servers on the network.

When the Microsoft Hyper-V servers are managed by Microsoft VMM servers, HP recommends that you install VRM Windows agents on Microsoft VMM servers. A VRM Windows agent can manage up to 50 Hyper-V servers. If more than 50 Hyper-V servers exist on the network, install additional VRM Windows agents.

Before you run the VRM agent installer, make sure the .NET Framework 4.5 and PowerShell 3.0 applications are already installed on the server. The applications are available on the Microsoft website.

To install a VRM Windows agent:

1. Decompress the `vrm-plug-windows.zip` file in the `tools` directory of the IMC installation package.
2. Save the decompressed files to a local directory on the server to install the VRM agent.
3. Run `Register.bat` in the `vrm-plug-windows` directory.
   
   The installation program verifies installation of .NET Framework 4.5 and PowerShell 3.0. Then, it installs the VRM Windows agent and automatically closes after the installation is complete.
   
   Do not delete the `vrm-plug-windows` directory or files in the directory after installation. It is the service registration path.
4. Use Notepad to open the `imf.cfg` file in the `\vrm-plug-windows\server\imf\server\conf` directory.
5. Edit the `imf.cfg` file:
   - Set the value of `IMGAddress` to the IP address of the IMC server.
   - Set the value of `IMGPort` to the IMG port number, which is 8800 by default.
6. Save and close the file.
7. Start the IMC VRM Agent service:
   - Click `Start` and select `Administrative Tools > Component Services`.
   - On the `Component Services` page, select `Services (Local)` from the navigation tree.
   - On the `Services (Local)` list, right-click `iMC VRM Agent` and select `Start`.

If a VRM Windows agent was previously installed, run the `UnRegister.bat` script in the `vrm-plug-windows` directory to uninstall the VRM Windows agent first.

Installing a VRM Linux agent

VRM uses a Linux agent to manage KVM virtual networks for Red Hat, Ubuntu, and Fedora, and Citrix XenServer virtual networks. With the agent, VRM can obtain virtual network data and set the virtual network parameters. Each VRM Linux agent can manage up to 200 physical KVM and Xen servers. You can install multiple VRM Linux agents as needed.

VRM Linux agents can run on Red Hat Linux 6.0 or later versions.

Installation prerequisites

A VRM Linux agent is a 32-bit program and applies to 32-bit and 64-bit Red Hat Linux.

To install the VRM Linux agent on 32-bit Red Hat Enterprise Linux, make sure the Linux supports the Web server function and has the `sshpass-1.05-1.el5.rf.i386.rpm` software package installed.
To install the VRM Linux agent on 64-bit Red Hat Enterprise Linux, first install the following 32-bit software packages:

- compat-libcap1-1.10-1.i686.rpm
- glibc-2.12-1.107.el6.i686.rpm
- keyutils-libs-1.4-4.el6.i686.rpm
- krb5-libs-1.10.3-10.el6.i686.rpm
- libaio-0.3.107-10.el6.i686.rpm
- libcom_err-1.41.12-14.el6.i686.rpm
- libgcc-4.4.7-3.el6.i686.rpm
- libidn-1.18-2.el6.i686.rpm
- libssh2-1.4.2-1.el6.i686.rpm
- libstdc++-4.4.7-3.el6.i686.rpm
- nspr-4.9.2-1.el6.i686.rpm
- nss-3.14.0.0-12.el6.i686.rpm
- nss-softokn-freebl-3.12.9-11.el6.i686.rpm
- nss-util-3.14.0.0-2.el6.i686.rpm
- openldap-2.4.23-31.el6.i686.rpm
- sshpass-1.05-1.el6.rf.i686.rpm
- openssl-1.0.0-27.el6.i686.rpm

This example uses Red Hat Enterprise Linux 6.4. For other Linux 6 versions, the package names might include different versions.

To install the required software packages:
1. Log in to Linux as root.
2. Insert the Linux installation disk into the CD drive and enter the directory where packages are saved.
3. Save the packages to a local directory and download sshpass-1.05-1.el6.rf.i686.rpm from the Internet.
4. Launch a terminal window and enter the local directory where the packages are saved.
5. Install packages, where xxx indicates the package name.

```
rpm -i --nodeps xxx
```

Installation procedure
1. Decompress the vrm-plug-linux.zip file in the tools directory of the IMC installation package.
2. Save the decompressed files to a local directory.
3. Run the install.sh script in the vrm-plug-linux folder.
4. Enter the IP address of the IMC server. The default setting is localhost.
5. Verify that the installation is successful.

```
ps -ef | grep imcvnmagent
```

When the agent is successfully installed, the imcvnmagent process is running.

If a VRM Linux agent was previously installed, run the uninstall.sh script in the vrm-plug-linux directory to uninstall the VRM Linux agent first.

### Installing LLDP plug-ins

When the VRM component is deployed, you must install an LLDP plug-in for topology calculation.
An LLDP plug-in contains the following packages:

- lldp-agent-redhat.zip
- lldp-agent-ubuntu.zip
- lldp-agent-windows.zip

Packages lldp-agent-redhat.zip and lldp-agent-ubuntu.zip apply to KVM servers and the lldp-agent-windows.zip package applies to Microsoft Hyper-V servers. Before you install the LLDP plug-ins, save and decompress the packages to the target servers.

Make sure the lldp-agent-windows.zip package is saved to a non-system disk.

**IMPORTANT:**

Do not delete the folder where the decompressed installation packages are located after the LLDP agent installation. If you delete the folder, the LLDP plug-in cannot be uninstalled completely.

### Installing an LLDP Windows agent

LLDP Windows agents support 32-bit and 64-bit Windows operating systems.

To install and configure an LLDP Windows agent:

1. Run the install.bat script in the LLDP Windows agent installation path. The LLDP Windows agent is installed.
2. Configure the LLDP Windows agent.
   
   The LLDP Windows agent supports either LLDP or CDP, but not both at the same time. By default, the agent supports LLDP.
   
   To enable the LLDP agent to support CDP and set the packet sending interval:
   
   a. Open the lldpagent.conf file in the \Program Files\lldpAgent directory on the Windows system disk.
   
   b. Delete the pound sign (#) from the string #Agent=CDP.
   
   c. Delete the pound sign (#) from the string #INTERVAL=10 and set the interval as needed. The default setting is 300 seconds.
   
   d. Save and close the file.
3. Restart the lldp-agent service.

### Installing an LLDP Linux agent

The installation procedures for packages lldp-agent-redhat.zip and lldp-agent-ubuntu.zip are the same. The following information describes the installation procedure for the lldp-agent-redhat.zip package.

An LLDP Linux agent must be installed on 64-bit Linux, including Red Hat 5.5, Ubuntu 11.0, and their later versions.

To install and configure an LLDP Linux agent:

1. Set the executable permission to the install.sh script and run the script in the LLDP Linux agent installation path. The LLDP Linux agent is installed.
2. Configure the LLDP Linux agent.
   
   The LLDP Linux agent supports either LLDP or CDP, but not both at the same time. By default, the agent supports LLDP.
   
   To enable the LLDP agent to support CDP and set the packet sending interval:
a. Open the lldpagent.conf file in the conf directory.
   
   vi lldpagent.conf

b. Delete the pound sign (#) from the string #Agent=CDP.

c. Delete the pound sign (#) from the string #INTERVAL=10 and set the interval as needed. The default setting is 300 seconds.

d. Save and close the file.

3. Restart the lldp-agent service.
   
   service lldp-agent restart
7 Accessing IMC

IMC is a browser-based management tool accessible from PCs. IMC of the Enterprise edition is also accessible from a mobile device.

Hardware, software, and browser requirements

Table 13 lists the hardware, software, and browser requirements for accessing IMC.

Table 13 Requirements for accessing IMC from a PC

<table>
<thead>
<tr>
<th>OS</th>
<th>Hardware and software</th>
<th>Browser version</th>
<th>Browser setting requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Recommended</td>
<td>• IE 10 or 11</td>
<td>• Turn off the popup blocker.</td>
</tr>
<tr>
<td></td>
<td>resolution: 1280 pixels in width.</td>
<td>• Firefox 30 or later</td>
<td>• Enable Cookies.</td>
</tr>
<tr>
<td></td>
<td>JRE 1.6.0_update27 or later is installed.</td>
<td>• Chrome 35 or later</td>
<td>• Add IMC as a trusted site.</td>
</tr>
</tbody>
</table>

Accessing IMC from a PC

Accessing IMC

1. Enter a URL in either of the following formats in the address bar of the browser:
   - http://ip-address:port/imc
   - https://ip-address:port/imc
   
   In the URL strings, **ip-address** is the IP address of the IMC server, and **port** is the HTTP or HTTPS port number used by IMC. By default, IMC uses HTTP port 8080 and HTTPS port 8443. The IMC login page appears.

2. Enter the user name and password and click **Login**.
   By default, the IMC superuser name and password are **admin** and **admin**.

   **IMPORTANT:**
   - For security purposes, change the password of the IMC superuser **admin** immediately after the first login.
   - When you attempt to access IMC using HTTPS, a certificate error message might appear. For more information, see HP IMC Getting Started Guide.

Accessing the UAM self-service center

When the UAM User SelfService subcomponent is deployed, access the user self-service center by entering a URL in either of the following formats in the address bar of the browser:

- http://ip-address:port
- http://ip-address:port/selfservice

In the URL, **ip-address** is the IP address of the IMC server where the UAM SelfService subcomponent is deployed and **port** is the HTTP port number used by IMC. The default HTTP port number is 8080.
Accessing the SOM service desk

When the SOM Service Desk subcomponent is deployed, access the SOM service desk by entering the following URL in the address bar of the browser:

http://ip-address:port/servicedesk

In the URL, \textit{ip-address} is the IP address of the IMC server where the SOM service desk is deployed and \textit{port} is the HTTP port number used by IMC. The default HTTP port number is 8080.

Accessing IMC from a mobile device

1. Open the browser on the mobile device.
2. Enter http://ip-address:port/imc in the browser's address bar.
   
   In the URL, \textit{ip-address} is the IP address of the IMC server and \textit{port} is the HTTP port number of IMC. The default HTTP port number is 8080.
   
   The IMC login page appears.
3. Enter the user name and the password in \textit{Operator} and \textit{Password} fields.
   
   The operator must have been added to IMC. The operator account used for login must belong to an operator group that has the \textbf{IMC Platform - Resource Management > Mobile Client Access} operation privilege.
4. Select \textbf{Mobile} or \textbf{PC} as needed.
   
   The PC version of IMC requires complex operations and provides all functions. The mobile version of IMC requires simple operations and provides only the following functions:
   
   o View information about faulty devices and interfaces, and query devices.
   o View device alarms.
   o Receive realtime alarms.
   o Test device reachability by using a \textbf{ping} or \textbf{tracert} command.
   o View custom views and device views.
5. Click \textbf{Login}.

Securing IMC

HP recommends performing the following tasks to secure IMC:

- Change the password of the IMC superuser admin immediately after the first login.
- Tie the administrative accounts to a central AAA server via LDAP or RADIUS.
- Retain one administrative account (not named admin) with a local password to recover from loss of access to the AAA server.
- Enable the verification code feature on the IMC login page.

Displaying a user agreement

A user agreement on the IMC login page informs operators of the rights and obligations for IMC login. To log in to IMC, operators must accept terms of the user agreement.

To display a user agreement on the IMC login page:

1. On the IMC server, enter the \texttt{\textbackslash client\textbackslash conf} directory of the IMC installation path (\texttt{/client/conf} on Linux).
2. Use WordPad (or vi on Linux) to open the \texttt{commonCfg.properties} file.
3. Change the value of the `enableTerms` parameter to `true`.
4. Save and close the `commonCfg.properties` file.
5. Prepare a user agreement in an HTML file named `terms.html`.
6. Save the `terms.html` file to the `\client\web\apps\imc` directory of the IMC installation path (`/client/web/apps/imc` on Linux).
7. Display the IMC login page.
   A User agreement link appears, as shown in Figure 46.
8. Click the link to view terms of the user agreement.

Figure 46 Viewing the user agreement on the login page
8 Upgrading IMC

The following example describes how to upgrade the IMC platform. Upgrade IMC service components in the same way the IMC platform is upgraded.

Preparing for the upgrade

Before you upgrade the IMC platform, complete the following tasks:

- Obtain compatible upgrade packages for the IMC platform and all the deployed service components. After the IMC platform upgrade, you must upgrade all the service components to match the new IMC platform version.
- Back up IMC database files using DBMan manual backup (see "12 Backing up and restoring the database"). Stop all IMC processes, and then save the IMC installation directory to a backup path. If the upgrade fails, you can use these files to restore IMC.

Upgrading IMC

⚠️ CAUTION:

- Make sure you have compatible upgrade packages for all deployed IMC components. If components do not have upgrade packages, they cannot be upgraded after the IMC platform upgrade and might become invalid.
- Do not upgrade IMC by running the \install\install.bat script in the IMC installation path.
- If the reporting function of an upgraded service component relies on the Report Management component, upgrade the Report Management component to match the service component version.

Upgrading the IMC platform

1. Start the Intelligent Deployment Monitoring Agent, and then click Install on the Monitor tab. The Choose folder dialog box appears, as shown in Figure 47.

   Figure 47 Choose folder dialog box

2. Click Browse and select the \install\components directory in the upgrade package.
3. Click OK.

   The IMC installation wizard appears, as shown in Figure 48.
Figure 48 IMC installation wizard

4. Click Next.
   The Agreement page appears, as shown in Figure 49.
5. Read the license agreement, select **Accept**, and click **Next**.
   
   The Upgrade Common Components dialog box appears, as shown in Figure 50.

   **NOTE:**
   
   Common components include the Intelligent Deployment Monitoring Agent and common background services.

   **Figure 50** Upgrade Common Components dialog box

6. Click **OK**.
   
   The system automatically upgrades common components and displays the upgrade progress, as shown in Figure 51.
After the common components are upgraded, the **Choose Target Folder** page appears, as shown in Figure 52.

The page displays the components to be installed and the installation location.

**Figure 52 Choose Target Folder page**

7. Verify the information and click **Next**.

The **Deployment and Upgrade Options** page appears, as shown in Figure 53.
8. Select **Deploy or upgrade at once** and click **Next**.

The **Installation Summary** page appears, as shown in Figure 54.
9. Verify the installation summary and click **Install**.
After the installation is complete, the **Batch upgrade** dialog box appears, as shown in **Figure 55**.
10. Select the components you want to upgrade and click **OK**.
    After the upgrade is complete, the **Batch upgrade result** dialog box shown in Figure 56 or Figure 57 appears. The dialog box content varies depending on whether auto backup and restoration settings have been configured in DBMan before the upgrade.

**Figure 56** Batch upgrade result without auto backup and restoration

**Figure 57** Batch upgrade result with auto backup and restoration

11. Click **OK**.
12. If the **Auto Backup and Recovery Settings** dialog box appears, configure the auto backup and restoration settings and click **OK**.
To start IMC, click **Start iMC** on the **Monitor** tab of the Intelligent Deployment Monitoring Agent.

## Restoring IMC

If the IMC upgrade fails, restore IMC to the version before the upgrade.

To restore IMC:

1. Manually restore the IMC database. For more information, see "12 Backing up and restoring the database."
2. After the database restoration is complete, stop IMC in the Intelligent Deployment Monitoring Agent.
3. Close the Intelligent Deployment Monitoring Agent.
4. Stop the **HP iMC Server** service by selecting **Start > All Programs > Control Panel > System and Security > Administrative Tools > Services.**
5. In the IMC installation directory, back up log files necessary for upgrade failure analysis, and then delete all the files in the directory.
6. Copy the backup IMC installation directory to the IMC installation path.
7. Start the **HP iMC Server** service by selecting **Start > All Programs > Control Panel > System and Security > Administrative Tools > Services.**
8. Start IMC in the Intelligent Deployment Monitoring Agent.

For IMC running in stateful failover mode, restore IMC only on the primary server in the failover system.
9 Uninstalling IMC

Uninstall IMC component by component or uninstall all components at one time.

If you want to reinstall IMC, complete the following tasks before the reinstallation:

- If you have reinstalled the database after IMC is uninstalled, you must manually delete the folder that stores data files of the previous IMC system. The default folder is named \imcdata. 
- If IMC installation or uninstallation is interrupted with an error, manually delete the IMC installation directory and the \imc-Reserved folder. The \imc-Reserved folder is located in the WINDOWS folder or the Linux etc directory.

Uninstalling an IMC component

Before uninstalling an IMC component, uninstall all components that depend on it.

To uninstall an IMC component:

1. Open the Intelligent Deployment Monitoring Agent.
2. On the Monitor tab, click Stop IMC.
3. On the Deploy tab, right-click the component to be uninstalled and select Undeploy the Component.
   A confirmation dialog box appears.
4. Click OK.
   The Intelligent Deployment Monitoring Agent undeploys the component. After the undeployment is complete, an operation success dialog box appears.
5. Click OK.
6. On the Deploy tab, right-click the component that is undeployed and select Remove this Component.
   A confirmation dialog box appears.
7. Click OK.
   The Intelligent Deployment Monitoring Agent uninstalls the component. After the uninstallation is complete, an operation success dialog box appears.
8. Click OK.

Uninstalling all IMC components at a time

1. Open the Intelligent Deployment Monitoring Agent.
2. On the Monitor tab, click Stop IMC.
3. On Windows, select Start > All Programs > HP Intelligent Management Center > Uninstall HP Intelligent Management Center.
   On Linux, run the uninstall.sh script in the /deploy directory of the IMC installation path.
   An uninstall wizard appears.
4. Click Uninstall.
   A confirmation dialog box appears.
5. Click OK.
   The Intelligent Deployment Monitoring Agent uninstalls all the components. After the uninstallation is complete, the Uninstallation Completed dialog box appears.
6. Click OK.
7. Delete the **iMC-Reserved** folder in the **WINDOWS** folder or the Linux `/etc` directory.
8. Reboot the operating system.
10 Registering IMC and incremental node licenses

An unregistered IMC version delivers the same functions as that of a registered version, but can be used only for 60 days since the date the service was first started. To unlock the time limitation or add extra nodes to IMC, you must purchase and register the IMC licenses.

The IMC registration procedures on Windows and Linux systems are similar. The following describes how to register IMC on a Windows Server 2008 R2 machine. Ensure you register IMC before any additional node licenses.

NOTE:
To transfer an existing license to a different Serial Number, contact HP Support.

Registering IMC

1. On the IMC login page, click Activate.
   The License Information page appears, as shown in Figure 58.
   Figure 58 License Information page

   ![License Information](image)

2. Select and copy or make a note of the Serial Number (this is unique to your installation of IMC).

Registering first license

1. Go to the HP My Networking system website (http://hp.com/networking/mynetworking/) and log in to My Networking portal.
   The HP Passport sign-in page appears, as shown in Figure 59.
2. Enter the user ID and password and click **Sign in**.

   The **Home** page appears, as shown in **Figure 60**.

**Figure 60** Home page

3. Click **Register license** under the **Licenses** section of the **Home** page.

   The **Enter Order number** or **Registration ID** page appears, as shown in **Figure 61**.
Figure 61 Enter Order number or Registration ID page

4. Enter the **Order number** or **Registration ID**, and click **Next**.
The **Enter the email associated with Order number** page appears, as shown in Figure 62.

Figure 62 Enter the email associated with Order number page

5. Enter an email address associated with the **Order number** and click **Next**.
The **Select the Product License** page appears, as shown in Figure 63.

Figure 63 Select the Product License page

6. Select the product you want to register by activating the radio button to the left of the license **Product #**.
7. Enter the quantity to be redeemed and click **Next**.

The **Enter details** page appears, as shown in **Figure 64**.

**Figure 64** Enter details page

8. Enter the IMC software serial number and click **Next**.

The **License agreement** page appears, as shown in **Figure 65**.

**Figure 65** License agreement page

9. Read the license agreement, select **I accept all of the above terms**, and click **Finish**.

The **Confirmation** page appears, as shown in **Figure 66**.
10. Click **Save as** to download and save the license key file. Remember the location and file name for the next step of activating the license in IMC.

11. If you want to email the confirmation information and license key file, enter the recipient’s email address in the **Send license confirmation to** field, add any **Comments** and click **Send email**. Also, you can view the details of the license you have registered.

**Registering incremental node licenses**

Registering an Incremental Node License is similar to registering the first license. The following information describes only the differences between them.

To register an Incremental Node license:

1. On the **Select the Product License** page, select the Incremental Node License you want to register.
2. Click **Next**. The **Enter details** page appears, as shown in **Figure 68**.

**Figure 68** Enter details page

3. Select the base product, enter the base software serial number, and click **Next**. The **Confirmation** page appears.

4. Click **Save as** to download and save the license key file. Remember the location and file name for activating the license in IMC.

**Activating IMC**

1. Access the **License Information** page, as shown in **Figure 58**.
2. Select **Activate now**.
   The **Register Your Product** page appears, as shown in **Figure 69**.

   **Figure 69** Register Your Product page

<table>
<thead>
<tr>
<th>Register Your Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>License File</td>
</tr>
<tr>
<td>Please select the license’s type</td>
</tr>
<tr>
<td>Register/Activate host license</td>
</tr>
<tr>
<td>OK</td>
</tr>
</tbody>
</table>

3. Select the license file in TXT format.
4. Select the license type, which can be **Register/Activate host license** or **Register/Activate back-up license**.
5. Click **OK**.
   The **Registration Succeeded** page appears, as shown in **Figure 70**.

   **Figure 70** Registration succeeded page

<table>
<thead>
<tr>
<th>Registration succeeded.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please restart IMC in Intelligent Deployment Monitoring Agent to complete activation. Thanks for using HP products.</td>
</tr>
<tr>
<td>OK</td>
</tr>
</tbody>
</table>

   IMC has been successfully registered and activated.

### Registering the IMC license for stateful/stateless failover

### Registering the IMC license for stateful failover

1. Run IMC on the primary server.
2. After the IMC starts up, access the IMC login page.
3. Click **Activate**.
   The **License Information** page appears, as shown in **Figure 71**.
4. Record the serial number of the primary server that is displayed in the Serial Number area.
5. Switch the IMC services to the backup server and access the IMC login page again.
6. Click Activate.
   The License Information page appears.
7. Record the serial number of the backup server in the Serial Number area.
8. Go to the HP My Networking system website at http://hp.com/networking/mynetworking/, enter required information, and enter the serial numbers of the host and the IMC stateful server.
9. Download and save the IMC license file locally. For more information, see "Registering first license."
10. Switch the IMC services back to the primary server and access the IMC login page again.
11. On the IMC login page, click Activate.
    The License Information page appears.
12. Click Activate Now.
    The registration page appears, as shown in Figure 72.

   **Figure 72** Registering your product

13. Click Browse to select the locally saved IMC license file.
14. Select Register/Activate host license from the Please select the license's type list.
15. Click OK.
    IMC has been successfully activated.

**Registering the IMC license for stateless failover**

When registering the IMC license for stateless failover, only the serial number of the primary server is required to get the license file. Use this file on both the IMC primary server and the IMC backup server to activate the license.
1. Start IMC on the primary server.
2. After the IMC starts up, access the IMC login page of the primary server.
3. Click **Activate**.
   The License Information page appears, as shown in Figure 73.

**Figure 73** License information

4. Record the serial number of the primary server that is displayed in the **Serial Number** area.
5. Go to the HP My Networking system website at http://hp.com/networking/mynetworking/, enter required information, and enter the serial number of the host.
6. Download and save the IMC license file locally. For more information, see “Registering first license.”
7. Access the IMC login page of the primary server again.
8. Click **Activate**.
   The License Information page appears.
9. Click **Activate Now**.
   The registration page appears, as shown in Figure 74.

**Figure 74** Registering your product

10. Click **Browse** to select the locally saved IMC license file.
11. Select **Register/Activate host license** from the **Please select the license’s type** list.
12. Click **OK**.
   IMC is successfully activated on the primary server.
14. Access the IMC login page of the backup server.
15. Click **Activate**.
   The License Information page appears.
16. Click **Activate Now**.
   The registration page appears.
17. Click **Browse** to select the locally saved IMC license file. This license file is the same as the file used for the IMC registration on the host.

18. Select **Register/Activate back-up license** from the **Please select the license's type** list.

![Figure 75 Registering your product](image)

19. Click **OK**.

    IMC has been successfully activated on the backup server.
11 Security settings

Anti-virus software

For security purposes, HP recommends installing anti-virus software on IMC servers and keeping the virus definitions up to date.

Port settings

HP recommends using a firewall to protect the IMC server cluster by filtering out non-service data sent to the cluster.

NOTE:
- HP recommends you use ACL configurations on a firewall rather than that on a switch to control data packets without filtering packet fragmentations.
- NTA/UBA typically uses probes for log collection. When a firewall is deployed between the probes and the IMC server, configure ACLs on the firewall to allow IP packets sent by the probes to IMC.

Make sure the ports used by the IMC components (listed in Table 14 and Table 15) are not blocked by the firewall.

Table 14 Port numbers used by the IMC platform

<table>
<thead>
<tr>
<th>Default port number</th>
<th>Usage</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP 161</td>
<td>Port to add a device to the IMC</td>
<td>Device</td>
</tr>
<tr>
<td>UDP 22</td>
<td>Port for SSH operations</td>
<td>Device</td>
</tr>
<tr>
<td>TCP 23</td>
<td>Port for Telnet operations</td>
<td>Device</td>
</tr>
<tr>
<td>UDP 514, 515</td>
<td>Port for syslog operations</td>
<td>IMC server</td>
</tr>
<tr>
<td>UDP 162</td>
<td>Port for trap operations</td>
<td>IMC server</td>
</tr>
<tr>
<td>TCP 8080, configurable</td>
<td>HTTP access to IMC</td>
<td>IMC server</td>
</tr>
<tr>
<td>TCP 8443, configurable</td>
<td>HTTPS access to IMC</td>
<td>IMC server</td>
</tr>
<tr>
<td>UDP 69</td>
<td>Port for Intelligent Configuration Center to perform configuration management through TFTP</td>
<td>IMC server</td>
</tr>
<tr>
<td>TCP 20, 21</td>
<td>Port for Intelligent Configuration Center to perform configuration management through FTP</td>
<td>IMC server</td>
</tr>
<tr>
<td>TCP 2810</td>
<td>Port for data file backup and restoration by using DBMan</td>
<td>IMC server</td>
</tr>
</tbody>
</table>

Table 15 Port numbers used by the IMC NTA/UBA

<table>
<thead>
<tr>
<th>Default port number</th>
<th>Usage</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP 9020, 9021, 6343</td>
<td>Port for the IMC server to receive logs</td>
<td>IMC server</td>
</tr>
<tr>
<td>TCP 8051</td>
<td>Listening port used to monitor the command for stopping the NTA/UBA service</td>
<td>IMC server</td>
</tr>
<tr>
<td>TCP 9099</td>
<td>JMX listening port for the NTA/UBA service</td>
<td>IMC server</td>
</tr>
<tr>
<td>Default port number</td>
<td>Usage</td>
<td>Location</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>UDP 18801, 18802, 18803</td>
<td>Communication ports between NTA and UBA</td>
<td>IMC server</td>
</tr>
</tbody>
</table>
12 Backing up and restoring the database

DBMan is the automatic backup and restoration tool for the IMC platform and service component databases, and provides a full-range system disaster backup solution. DBMan uses a standard database backup and restoration mechanism to process the complete databases.

DBMan supports both manual and automatic database backup and restoration. It is integrated in the Environment tab of the Intelligent Deployment Monitoring Agent, as shown in Figure 76.

**Figure 76 Environment tab**

The Environment tab includes the following areas:

- **Running Environment**—Displays software and hardware information on the IMC server.
- **Database Space Usage**—Displays the database and log file usage information.
- **Database Backup and Restore**—Provides the following database backup and restoration options:
  - **Configure**—Allows you to configure automatic database backup and restoration settings. The automatic backup and restoration function is typically used in stateless failover scenarios.
  - **Backup**—Immediately backs up all IMC data files (including configuration files and database files) to a specified path.
  - **Restore**—Immediately restores previously backed up database files.
  - **View Log**—Allows you to view the database backup and restoration logs.
Configuration restrictions and guidelines

To ensure correct operation, do not back up and restore IMC databases between different operating systems.

When you use DBMan to back up and restore IMC databases, follow these restrictions and guidelines:

- In automatic backup configuration, use the **Upload to Backup System** option to back up database files to a backup IMC system or an FTP server.
- The **Upload to Backup System** option requires one of the following configurations:
  - The **Master Server IP of Backup System** is specified for database backup.
  - An FTP server is configured in the `dbman_ftp.conf` file in the `\dbman\etc` directory of the IMC installation path. For example:
    ```
    ftp_ip=1.1.1.1
    ftp_user=admin
    ftp_password=1234
    ```
- To add additional backup and restoration settings, edit the `dbman_addons.conf` file in the `\dbman\etc` directory of the IMC installation path. The settings take effect immediately after the file is saved.
  
  For example, add the following strings to the `dbman_addons.conf` file to specify tasks to perform before or after database restoration:
  ```
  BeforeSQLScript_monitor_db_IMC_monitor = D:\1.bat
  AfterSQLScript_monitor_db_IMC_monitor = D:\2.bat
  ```

Installing and upgrading DBMan on the database server

Install DBMan on the remote database server to automatically synchronize database backup and restoration settings from the IMC server.

**Installing DBMan**

1. On the database server, enter the **install** directory of the IMC installation package.
2. Right-click the **installslave.bat** script and select **Run as Administrator** from the shortcut menu.
   
   The **Address of Master** page appears, as shown in **Figure 77**.

   **Figure 77** Configuring the IMC server IP address

   ![Address of Master](image)

3. Enter the IP address of the IMC server and click **OK**.
   
   The **Checking Database Connectivity** dialog box appears, as shown in **Figure 78**.
4. Configure the parameters as needed.
5. Click OK.

The system checks the installation environment and database connectivity. After the checks are passed, the system displays the remote IMC installation wizard, as shown in Figure 79.
6. Specify the deployment location.
7. Click **Install**.
   After the installation is complete, the **Installation Completed** page appears, as shown in Figure 80.
8. Click **Finish**.

DBMan automatically starts when the operating system is started.

**Upgrading DBMan**

When IMC is upgraded, the database server displays the **Upgrade Common Component** dialog box, as shown in Figure 81. Click **Yes**. DBMan is automatically upgraded as a common component.

**Figure 81** Upgrade Common Component dialog box
Backing up and restoring databases for a single IMC system

Backing up databases

A single IMC system supports both manual and automatic backup:

- **Manual backup**—Immediately backs up all IMC data files.
- **Automatic backup**—Allows you to schedule a task to automatically back up selected data files at the specified time.

**Manual backup**

1. On the **Environment** tab, click **Backup**. A confirmation dialog box appears.
2. Click **OK**. The **Select database backup path** dialog box appears.
3. Specify a local path to save the backed up data files. Make sure the specified path has enough space.
4. Click **OK**.

**Automatic backup**

1. On the **Environment** tab, click **Configure**. A confirmation dialog box appears.
2. Click **OK**. The **Auto Backup and Recovery Settings** dialog box appears, as shown in Figure 82.

**Figure 82** Auto Backup and Recovery Settings

3. Read information in the **Auto Backup and Recovery Settings** dialog box, select **Auto Backup Model**, and click **OK**. The page for configuring automatic backup settings appears, as shown in Figure 83.
4. On the Basic Configuration tab, configure the following parameters:
   o **Daily backup time (HH:mm)**—Enter the time at which the automatic backup operation starts every day. By default, the daily backup time is 04:00.
   o **Backup file lifetime (days)**—Enter how many days a backup file can be kept. Expired files are automatically deleted.
   o **Master Server IP of Backup System**—This parameter is applicable to database backup in stateless failover scenarios. To upload the database files to the master server of backup system, specify the master server IP address in this field. Make sure automatic restoration is enabled for the backup system.
5. Click the **Primary Server** tab and configure the following parameters:
   - **IMC Backup Path**—Specify the path where the backup IMC data files are stored on the IMC server.
   - **Database Backup Path**—Specify the path where the backup database files are stored on the database server.
   - **Local Backup**—Select the databases to back up locally on the database server. By default, all databases are selected.
   - **Upload To Backup System**—Select the databases to upload to an FTP server or the master server of a backup system. By default, no database is selected. When you select **Upload To Backup System** for a database, the **Local Backup** option is forcibly selected for the database. To configure the FTP server, see “Configuration restrictions and guidelines.”

6. Click the **Advanced Configuration** tab and configure the following parameters:
   - **Delete local files after upload even if upload fails**—Specify whether to delete local backup files after they are uploaded.

7. Click **OK**.

### Restoring databases

A single IMC system supports only manual restoration of the databases. Manual restoration immediately replaces the current database files with previously backed up files.

When you perform manual restoration, follow these restrictions and guidelines:

- Make sure IMC has been started at least once after installation before you restore the IMC databases.
- Make sure the automatic backup and restoration parameters have been configured. Otherwise, DBMan cannot locate IMC data files or database files during restoration.
- Restore database files for the IMC platform and service components together. If you restore only some of the database files, data loss or inconsistency might occur.
- During manual database restoration, the IMC service and database service are automatically stopped and restarted.

To perform a manual restoration:

1. On the **Environment** tab, click **Restore**.
   - The **Restoration Type** dialog box appears, as shown in **Figure 84**.

   **Figure 84** Restoration Type dialog box

2. Click **Remotely Restore**.
   - The **Configure Remote Restoration** page appears, as shown in **Figure 85**.
3. Click **Configure** to select the database files to be restored, and then click **OK**. The **Confirm** dialog box appears.

4. Click **Yes**.
   The system starts restoring the database files. The **Message** dialog box appears after the restoration is complete.

5. Click **OK**.
   The IMC service will be automatically started.

### Backing up and restoring databases in stateless failover scenarios

A typical stateless failover scenario includes a primary IMC system and a backup IMC system. For stateless failover, configure automatic backup on the primary IMC system and configure automatic restoration on the backup IMC system.

During automatic backup and restoration, the master server of the primary IMC system performs the following operations:

1. Uses DBMan to periodically back up database files locally.
2. Uploads the backed up database files to the backup IMC system.
3. Instructs the backup IMC system to restore the received database files locally.

HP recommends that you restore database files for all components together. If you restore databases for only some of the components, the other components might become unavailable.

### Backing up databases

In stateless failover, configure automatic backup on the master server of the primary IMC system.

Before the configuration, make sure the following settings are consistent on the primary and backup IMC systems:

- OS
• Database type and version
• IMC version and patches

When you configure automatic backup, make sure you specify the correct master server of the backup system on the Basic Configuration tab. For more information about configuring automatic backup, see "Automatic backup."

Restoring databases

This example describes the automatic restoration settings on a backup IMC system that is deployed in centralized mode and uses a remote database.

To configure automatic restoration:

1. On the Environment tab, click Configure.
   
   The Auto Backup and Recovery Settings dialog box appears, as shown in Figure 86.

   Figure 86 Auto Backup and Recovery Settings dialog box

2. Read information in the Auto Backup and Recovery Settings dialog box, select Auto Restore Model, and click OK.
   
   The page for configuring auto restoration settings appears, as shown in Figure 87.
Figure 87 Configuring auto restoration settings

3. Click the **Primary Server** tab and configure the following parameters:
   - **Backup files location of IMC**—Specify the local path that stores the backup IMC data files uploaded by the primary IMC system.
   - **Backup files location of database**—Specify the path on the remote database server that stores the backup database files uploaded by the primary IMC system.
   - **Databases to Restore**—Select databases to restore. By default, all databases are selected.

4. Click **OK**.
**13 FAQ**

How do I install the Java running environment on Linux to access IMC by using Firefox?

To install the Java running environment, install and configure JDK or JRE for Firefox. This example uses JDK.

   Make sure the installation file matches the requirements of the operating system. For example, download **jdk-6u12-linux-i586-rpm.bin** for x86-based Linux.

2. Copy the JDK installation file to a local directory. In this example, save the installation file in the /tmp directory and install JDK:
   ```bash
cd /tmp
sh jdk-6u12-linux-i586-rpm.bin
```

3. Press the spacebar to view the copyright information, and then enter **yes** to finish the JDK installation.
   JDK is installed in the `/usr/java/jdk1.6.0_12` directory. At the same time, a `/usr/java/default` link pointing to the `/usr/java/jdk1.6.0_12` directory is generated automatically, equivalent to JDK is installed in the `/usr/java/default` directory.

   ```bash
cd /var/local/firefox/plugins/
ln -s /usr/java/default/jre/plugin/i386/ns7/libjavaplugin_oji.so
```

5. Run `/var/local/firefox/firefox` to verify that you can access IMC.

After IMC installation is complete, how do I change the database file storage path?

1. Stop the IMC service by using the Intelligent Deployment Monitoring Agent.
2. Transfer the databases of IMC components to the new storage path on the database server. This example uses **D:\imcdata**.
3. At the CLI, access the `\deploy` directory of the IMC installation path and modify the database file storage path.
   ```bat
pwdmgr.bat -changeDataDir "D:\imcdata"
```
   Figure 88 shows that the storage path has been successfully modified.

**Figure 88** Modifying the database file storage path

4. Start the IMC service.

On Linux, the time displayed on IMC (such as the login time and operation log record time) is different from the time on the server, and the difference might be several hours.

This problem might occur if the time zone settings on the server where IMC runs are changed after
IMC installation. To resolve the problem, use the `tzselect` command to modify the time zone of the server.

After IMC is installed on the Windows Server 2003 64-bit OS, the IMC background processes cannot be started.

For correct IMC operation on Windows Server 2003 64-bit OS, install patch `WindowsServer2003-KB942288-v4-x64.exe` on the OS.

1. Stop IMC.
2. Install the patch.
3. Execute `vcredist.exe` in the `\deploy\components\server\` directory of the IMC installation path.

During the component deployment process, a deployment failure error message appears and the system displays "Execute database script error!" The log file includes an error message that the object `dbo.qv.id` already exists. How do I resolve the problem?

1. Log in to the Query Analyzer of SQL Server as `sa` and execute the following commands:
   ```
   use model
   EXEC sp_droptype 'qv_id'
   ```
2. Redeploy the component that failed to be deployed.

When installing IMC on Windows Server 2008 R2, the system displays a message that the Windows Installer cannot be installed, as shown in Figure 89.

**Figure 89** Windows Installer dialog box

![Windows Installer dialog box](image)

To resolve the problem:

1. In the **Windows Installer** dialog box, click **Browse**.
2. In the root directory of the disk, locate the folder whose name contains digits and the `abcdef` string, and then select the `vc_red.msi` file in the folder.
3. Click **OK**.
4. Continue the installation.

On Linux, how do I start JavaService when Xwindows is closed?

Use the `service IMCdmsd start` command to start the JavaService.

On Windows, the IMC service cannot be started or stopped after IMC runs for a period of time.

This problem is caused by insufficient virtual memory.

To resolve the problem, set the virtual memory to the system managed size:

1. On the IMC server, click **Control Panel**, and then click the **System** icon.
The **System Properties** dialog box appears, as shown in Figure 90.

**Figure 90** System Properties dialog box

2. Click the **Advanced** tab, and then click **Settings** in the **Performance** area. The **Performance Options** dialog box appears, as shown in Figure 91.
3. Click the **Advanced** tab, and then click **Change** in the **Virtual memory** area. The **Virtual Memory** dialog box appears, as shown in Figure 92.
4. Select **System managed size** and click **Set**.
5. Click **OK**.

On Linux, popup windows cannot be found during IMC deployment or upgrade.

When Xshell or Xstart is used for remote access on Linux, a window might appear on top of popup windows. To resolve this problem, move the window away to view the popup windows.