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.
© Copyright 2015 Hewlett Packard Enterprise Development LP

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.
Contents

Overview ............................................................................................................................. 1

IMC components ................................................................................................................. 1
IMC platform ....................................................................................................................... 1
Service components ............................................................................................................. 1
IMC editions ........................................................................................................................ 3
Installation and deployment .............................................................................................. 4
Deployment restrictions and guidelines ............................................................................. 4

Preparing for installation ................................................................................................. 6

Hardware requirements ..................................................................................................... 6
Software requirements ...................................................................................................... 8
VM requirements ................................................................................................................ 9
Preparing the installation environment ........................................................................... 10
Uninstalling previous versions of IMC ........................................................................... 10
Checking ports and firewalls ............................................................................................ 10
Checking the database configuration .............................................................................. 11
Checking the installation environment ............................................................................ 11
Superuser account .............................................................................................................. 13
Setting the system time ..................................................................................................... 14

Installing and deploying the IMC platform ..................................................................... 16

Selecting the installation type ........................................................................................... 16
Installing the IMC platform ............................................................................................... 17
Deploying IMC on a subordinate server ........................................................................... 27
Starting the remote installation wizard .......................................................................... 27
Installing the Intelligent Deployment Monitoring Agent ................................................. 29
Deploying the IMC Platform subcomponents .................................................................. 31

Managing IMC by using the Intelligent Deployment Monitoring Agent ..................... 35

Starting the Intelligent Deployment Monitoring Agent ................................................... 35
Monitor tab .......................................................................................................................... 36
Process tab ........................................................................................................................... 37
Deploy tab ............................................................................................................................ 37
Environment tab .................................................................................................................. 39

Installing and deploying IMC service components ......................................................... 40

Installing and deploying IMC NTA .................................................................................... 42
Installing IMC NTA ............................................................................................................. 42
Deploying IMC NTA on the master server ....................................................................... 48
Deploying NTA subcomponents on a subordinate server ............................................... 50
Installing and deploying IMC UAM .................................................................................. 51
Installing IMC UAM .......................................................................................................... 51
Deploying UAM on the master server .............................................................................. 51
Deploying UAM on a subordinate server ........................................................................ 59
Installing and deploying IMC MVM .................................................................................. 63
Installing IMC MVM .......................................................................................................... 63
Deploying MVM .................................................................................................................. 63

Installing plug-ins ............................................................................................................ 66

Installing DHCP plug-ins ................................................................................................. 66
Installing a DHCP plug-in on an MS DHCP server ............................................................ 66
Installing a DHCP plug-in on a Linux DHCP server .......................................................... 67
Installing VRM plug-ins ..................................................................................................... 67
Installing a VRM Windows agent ...................................................................................... 68
Installing a VRM Linux agent ............................................................................................. 68
Installing LLDP plug-ins .................................................................................................... 70
Installing an LLDP Windows agent ................................................................................... 70
Overview

The following information describes how to deploy IMC in distributed mode and to use a remote database. This deployment scheme scales to networks of 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 service component deployment.

IMC includes the following service components:
- **User Access Manager (UAM)**—Provides policy-based Authentication, Authorization, and Accounting (AAA) 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 for 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. As 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 application program interfaces (APIs) provided by H3C virtual converged framework (VCF) controllers or HPE 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 HPE 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>Remote database</td>
<td>Not supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

For information about installing a remote 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
For information about installing a remote 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

In distributed deployment, the master server is the management center of IMC. It interacts with subordinate servers to implement network management. A subordinate server is responsible for specific tasks, for example, network analysis for NTA and portal for UAM.

To improve server performance, IMC uses the “Install + Deploy” model.

- **Install**—Copies the IMC installation packages to the server and loads them to the Intelligent Deployment Monitoring Agent.
- **Deploy**—Decompresses the installation packages and runs deployment scripts on the server.

The IMC components are operational only after they are deployed. In distributed deployment, all IMC components are installed on the master server and deployed on the master server or a subordinate server as needed. The master server provides centralized Web services.

IMC automatically creates a database user for each component when the component is deployed. As a best practice, do not modify the database user configuration, including the database user password and password policy.

If the deployment or upgrade process is interrupted, IMC automatically stores logs as a compressed file in the `tmp` directory of the IMC installation path. You can use the logs to quickly locate the issue or error.

### Deployment restrictions and guidelines

To deploy IMC in distributed mode, follow these restrictions and guidelines:

- The master and subordinate servers must use the same operating system.
- You can use SQL Server and MySQL databases for Windows. You can use Oracle and MySQL databases for Linux.
- When you use Oracle, make sure all databases used by the master and subordinate servers have different network service names.
- The following subcomponents must be deployed on the master server:
  - Resource Management
  - NE Management
  - Report Management
  - Network Asset Management
  - Security Control Center
  - Virtual Resource Management
  - Server & Storage Automation

For more information about the deployment for other subcomponents, see Table 11. For more information about the deployment for other service components, see Table 12.
If the IMC Intelligent Deployment Monitoring Agent is already installed on subordinate servers, uninstall it before you deploy IMC components in distributed mode. For more information about how to uninstall the Intelligent Deployment Monitoring Agent, see "Uninstalling IMC."
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 using 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: \((1+1+1+(10\times2))\times5/10=12\).

- **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 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 a minimum of 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 a minimum of 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 a minimum of 1 GB.

Optimal hardware requirements vary with scale, other management factors, and are specific to each installation. Consult Hewlett Packard Enterprise 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 a 32-bit Windows operating system

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nodes</strong></td>
<td><strong>Collection units</strong></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 a 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 200</td>
</tr>
<tr>
<td>0 to 200</td>
<td>5 K to 50 K</td>
</tr>
<tr>
<td>200 to 1 K</td>
<td>200 to 1 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>1 K to 2 K</td>
</tr>
<tr>
<td>1 K to 2 K</td>
<td>1 K to 2 K</td>
</tr>
<tr>
<td>2 K to 5 K</td>
<td>2 K to 5 K</td>
</tr>
<tr>
<td>2 K to 5 K</td>
<td>2 K to 5 K</td>
</tr>
<tr>
<td>5 K to 10 K</td>
<td>5 K to 10 K</td>
</tr>
<tr>
<td>5 K to 10 K</td>
<td>5 K to 10 K</td>
</tr>
<tr>
<td>10 K to 15 K</td>
<td>10 K to 15 K</td>
</tr>
<tr>
<td>10 K to 15 K</td>
<td>10 K to 15 K</td>
</tr>
</tbody>
</table>

### Table 4 Hardware requirements for a 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 200</td>
</tr>
<tr>
<td>0 to 200</td>
<td>5 K to 50 K</td>
</tr>
<tr>
<td>200 to 500</td>
<td>200 to 500</td>
</tr>
<tr>
<td>200 to 500</td>
<td>200 to 500</td>
</tr>
</tbody>
</table>
Table 5 Hardware requirements for a 64-bit Linux operating system

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nodes</strong></td>
<td><strong>Collectio n units</strong></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><strong>Windows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows Server 2008 (32-bit) Service Pack 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 (64-bit) Service Pack 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 Service Pack 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 KB2836988</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 N/A</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>SQL Server 2008 Service Pack 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL Server 2008 R2 Service Pack 2</td>
<td></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 2012</td>
<td>Service Pack 2</td>
<td></td>
</tr>
<tr>
<td>SQL Server 2014</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>SQL Server 2008 R2 SP2 Express</td>
<td>Used as the embedded database for the SNS and standard editions only.</td>
<td></td>
</tr>
</tbody>
</table>

### Linux

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

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

### Both Linux and Windows

<table>
<thead>
<tr>
<th>Database</th>
<th>Requirement</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL Enterprise Server 5.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MySQL Enterprise Server 5.5</td>
<td>Up to 1000 devices are supported.</td>
<td></td>
</tr>
<tr>
<td>MySQL Enterprise Server 5.6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### VM requirements

As a best practice, install IMC on a physical server.

#### Table 7 Hypervisor platform requirements

<table>
<thead>
<tr>
<th>OS</th>
<th>Hypervisor</th>
</tr>
</thead>
</table>
| Windows | • VMware ESX  
|         | • Windows Hyper-V |
| Linux | • VMware ESX |

#### 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>Vendor</td>
<td>Hypervisor</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------</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 configuration 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 the correct installation and operation of IMC, make sure no other network management products are installed on the same server as IMC.

Do not install IMC in an IPv6 environment.

Uninstalling previous versions of IMC

If IMC was previously installed on the system, then thoroughly uninstall it first. For information about uninstalling IMC, see "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.

Table 9 IMC port requirements

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

IMC data can be stored on a remote database server. In distributed deployments, the data of all IMC servers is typically stored on the same remote database server.

To use a SQL database server:
- Install a SQL Server client that has the same version as the database.
- Create a folder to store IMC data files on the SQL server. You are required to provide the folder to save IMC data on the remote database during IMC deployment.
- As a best practice, use the account `LocalSystem` for the SQL Server service on the database server. This enables the database superuser used for installing IMC to have read and write access to all disks on the database server. To use another account, you must grant the account read and write access to the database file folder. For more information, see *SQL Server 2005/2008/2008 R2/2012 Installation Guide*.

To use an Oracle database:
1. Install an Oracle client that has the same version as the database.
2. Create a network service name and set the network service name to be the IP address of the database server.

Before installing IMC, first install the database server, and then configure the database services to automatically start with the operating system.

For example, to use a SQL Server database for IMC, install the database before IMC installation, and then set the startup type of the `SQL Server` and `SQL Server Agent` services to `Automatic`.

To view the startup type of the database services, click `Start`, and then select `Administrative Tools > Services`.

Checking the installation environment

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

To check the installation environment:
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:
   o **Database Type**—Select the database type. Options are Microsoft SQL Server, MySQL, and Oracle. The default is Microsoft SQL Server.
   o **Instance Name**—To connect to the default instance of the database, select Default Instance. To connect to a named instance, select Other Instance, and then 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. For more information about configuring the network service name, see Oracle 11g Installation and Configuration Guide or Oracle 11g R2 Installation and Configuration Guide.

   o **Superuser**—Enter the database superuser name. The default is sa.
   o **Password**—Enter the password of the superuser.
   o **Database Location**—Select other server from the list.
   o **Database Server Address**—Enter the IP address of the database server. This field is editable only when other server is selected as the database location.
   o **Listening Port**—Enter the listening port of the database server. The default is 1433.
   o **Installation Location**—Specify the local directory for storing the IMC installation package.
   o **Data File Location**—Specify the local directory for storing the data files.
   o **HTTP Port**—Enter the HTTP port number for the IMC Web server. The default is 8080.
   o **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.
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 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.

To perform the following tasks, you must update the password in IMC if the password of the superuser account is changed after IMC deployment:

- View database information on the **Environment** tab.
- Deploy new components.
- Update existing components.

To update the database user password in IMC:

1. Start the Intelligent Deployment Monitoring Agent, and then 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 then click **OK**, as shown in **Figure 3**.
Figure 3 Changing the superuser password

Table 10 lists the default superuser accounts.

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</td>
</tr>
<tr>
<td></td>
<td>• sys</td>
</tr>
<tr>
<td>MySQL</td>
<td>root</td>
</tr>
</tbody>
</table>

Setting the system time

Follow these guidelines when you set the system time:
- 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.

Do not modify the system time on the server after IMC is started. If you modify the system time, the following issues might occur:
- 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.
Installing and deploying the IMC platform

You must install the database before installing IMC. This example uses the SQL server 2008 R2 database. For information about how to install the database, see SQL Server 2008 R2 Installation and Configuration Guide.

Table 11 shows the IMC Platform subcomponents and the optional servers.

<table>
<thead>
<tr>
<th>Component</th>
<th>Subcomponents</th>
<th>Optional server</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMC Platform</td>
<td>Resource Management</td>
<td>Master</td>
</tr>
<tr>
<td></td>
<td>Alarm Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Guest Access Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Performance Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Network Asset Management</td>
<td>Master</td>
</tr>
<tr>
<td></td>
<td>ACL Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Intelligent Configuration Center</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>NE Management</td>
<td>Master</td>
</tr>
<tr>
<td></td>
<td>Report Management</td>
<td>Master</td>
</tr>
<tr>
<td></td>
<td>General Search Service Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Security Control Center</td>
<td>Master</td>
</tr>
<tr>
<td></td>
<td>Syslog Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>VLAN Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>User Selfservice Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Virtual Resource Management</td>
<td>Master</td>
</tr>
<tr>
<td></td>
<td>Server &amp; Storage Automation</td>
<td>Master</td>
</tr>
</tbody>
</table>

Selecting the installation type

1. Log in 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.
3. Select the country/region, language, and the Custom installation type. IMC supports typical and custom installations.
   - **Typical**—Installs and deploys all platform subcomponents on the local host without manual intervention.
   - **Custom**—Allows you to select desired platform subcomponents to install and deploy on the master server. After the installation completes, you must manually deploy the platform subcomponents. A custom installation is required to start a distributed deployment.

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 to the host 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**

1. In the **Select Locale** dialog box, select the Custom installation type, and then click **OK**.
   The **Checking Database Connectivity** dialog box appears, as shown in Figure 5.
2. Configure the parameters as needed. For descriptions about the parameters, see "Checking the installation environment."

3. Click OK.

After the checks are passed, the IMC installation wizard appears, as shown in Figure 6.
4. Click Next.

The Agreement page appears, as shown in Figure 7.
5. Read the license agreement, select Accept, and then click Next. The Choose Target Folder page appears, as shown in Figure 8.
6. Select the components you want to install and specify a local path as the installation location. The installation program examines whether the specified installation path contains 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.

7. Click Next.

The Deployment and Upgrade Options page appears, as shown in Figure 9.
8. Select **Deploy or upgrade at once** or **Deploy or upgrade later**. In this example, select **Deploy or upgrade later**.
9. Click **Next**.

The **Installation Summary** page appears, as shown in Figure 10.
10. Verify the installation summary, and then click **Install**.

After the installation is complete, the **Installation Completed** page appears, as shown in Figure 11.
11. Select **Open deployment monitoring agent**, and then click **Finish**.

The system automatically starts the Intelligent Deployment Monitoring Agent and displays the **Batch deploy** dialog box, as shown in **Figure 12**.

**Figure 12 Batch deploy dialog box**
12. Select the components to be deployed, and then click OK.
   The Database Configuration page appears, as shown in Figure 13.

Figure 13 Database Configuration page

13. Enter the password of the superuser.

14. Set the data file location.
   You must first create a folder to save data files on the database server.
   Make sure the specified data file location is on a readable and uncompressed disk drive and does not include any files.

15. Click Next, and then click OK in the confirmation dialog box that appears.
   The Configure Web Service Port page appears, as shown in Figure 14.
16. 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.

17. Click **Deploy**.
   After the deployment is complete, the **Batch deploy succeeded** dialog box appears, as shown in **Figure 15**.

**Figure 15 Batch deploy succeeded dialog box**

18. Click **OK**.
Deploying IMC on a subordinate server

Before you deploy IMC subcomponents on a subordinate server for the first time, install the Intelligent Deployment Monitoring Agent on the subordinate server.

Make sure you have started IMC on the master server.

Starting the remote installation wizard

You can start the remote installation wizard through the installation package or IE. As a best practice, use the installation package.

Starting the remote installation wizard through the installation package

1. On the subordinate server, right-click the installslave.bat script in the install directory of the installation package and select Run as Administrator.
   
   The Address of Master page appears, as shown in Figure 16.

   To start the remote installation wizard on Linux, run the installslave.sh script in the install directory of the installation package as a root user. If the installation file is obtained by using FTP, you must first authorize the installslave.sh script by executing chmod –R 775 installslave.sh in the directory of the script.

   Figure 16 Address of Master

   ![Address of Master](image)

2. Enter the IP address of the master server, and then click OK.

   The Checking Database Connectivity dialog box appears, as shown in Figure 17.
3. Configure the parameters as needed. For descriptions about the parameters, see "Checking the installation environment."

4. Click OK to start checking the database connectivity.

After the installation environment check is passed, the Remote Installation Wizard appears, which means that you have successfully started the remote installation wizard.

**Starting the remote installation wizard through IE**

1. On the subordinate server, launch the IE browser and enter http://ipaddress:port/iMC in the address bar.

   The ipaddress string is the IP address of the master server and port is the HTTP service port number set during IMC deployment.

   The IMC login page appears.

2. Enter the username and password of the superuser, and then click Login.

   The Home tab appears.

3. Click the System tab, and then select System Configuration > Deploy Component.

4. On the Installed Components page, click Start deploy.

   A dialog box appears.
5. Click **OK**.
   The **Downloading application** dialog box displays the download process for the Java file jre.exe.
   If JRE6.0 has been installed on the subordinate servers, the system starts the remote installation wizard when you click **OK**.

6. After the Java file is downloaded and installed, the **Checking Database Connectivity** dialog box appears, as shown in Figure 17.

7. Configure the parameters as needed. For descriptions about the parameters, see "Checking the installation environment."

8. Click **OK** to start checking the database connectivity.
   After the installation environment check is passed, the **Remote Installation Wizard** appears, which means that you have successfully started the remote installation wizard.

**Installing the Intelligent Deployment Monitoring Agent**

1. On the **Choose Target Folder for Deployment** dialog box, as shown in Figure 20, specify the deployment location for the Intelligent Deployment Monitoring Agent.
   The default deployment location is the `\Program Files\iMC` directory of the disk with the maximum free space on Windows or is `/opt/iMC` on Linux. This example uses `C:\Program Files\iMC`. 

The installation program examines whether the specified installation path contains files. If the path contains files, a message is displayed. Click **OK** to delete the files.

**Figure 20 Choose Target Folder for Deployment**

2. **Click Install.**

The system starts to download files. After the files are downloaded, the **Installation Completed** dialog box appears, as shown in **Figure 21**.
3. Click **Finish**.

### Deploying the IMC Platform subcomponents

1. Click the **Deploy** tab.
   The **Deploy** tab displays information about all IMC components that have been installed.

2. Right-click a platform subcomponent that has not been deployed, and then select **Batch Deploy** from the shortcut menu.
   The **Batch deploy** dialog box appears.
3. Select the subcomponents you want to deploy, and then click OK. The system starts downloading the files.
4. Perform the following tasks after the download is complete:
   a. On the Configure Web Service Port page, set HTTP Port (8080 by default) and HTTPS Port (8443 by default), as needed.
b. On the **Database Configuration** page, perform the following tasks:

- Enter the password for the user *sa* for the current database, which is the superuser name specified during IMC installation.

- Specify the data file location on the database server. The default location is the `C:\Program Files\imcdata` directory of the disk with the maximum free space on Windows or is `/opt/imcdata` on Linux. This example uses `C:\Program Files\imcdata`. 
5. Click **Deploy** to start the deployment.  
   After the deployment is finished, the **Batch deploy result** dialog box appears.

**Figure 25 Batch deploy result**

6. Click **OK**.
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 IMC 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 26**, 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.

**Figure 26 Intelligent Deployment Monitoring Agent**
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 27, the Monitor tab displays the performance information for 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.
- **Exit**—Click this button to exit the Intelligent Deployment Monitoring Agent.

Figure 27 Monitor tab of the Intelligent Deployment Monitoring Agent
Process tab

As shown in Figure 28, the Process tab displays IMC process information.

**Figure 28 Process tab of the Intelligent Deployment Monitoring Agent**

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 29, 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 deployment 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 are 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 30, 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 about the Environment tab, see "Backing up and restoring the database."

Figure 30 Environment tab of the Intelligent Deployment Monitoring Agent
**Installing and deploying IMC service components**

The following information describes how to install and deploy the service components. Table 12 lists all service components and subcomponents in IMC.

**Table 12 Service components and subcomponents**

<table>
<thead>
<tr>
<th>Component</th>
<th>Subcomponent</th>
<th>Optional server</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Access Manager</td>
<td>Intelligent Strategy Proxy</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>User Access Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>User Access Management Sub Server</td>
<td>Subordinate</td>
</tr>
<tr>
<td></td>
<td>Portal Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>EIP Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>EIP Sub Server</td>
<td>Subordinate</td>
</tr>
<tr>
<td></td>
<td>Policy Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Policy Proxy Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>User SelfService</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Third-Party Page Publish Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>TACACS+ Authentication Manager</td>
<td>TACACS+ Authentication Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>EAD Security Policy</td>
<td>Security Policy Configuration</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Desktop Asset Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Desktop Asset Manager Proxy Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>iNode DC</td>
<td>iNode Dissolvable Client</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>MPLS VPN Manager</td>
<td>MPLS VPN Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>MPLS TE management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>L2VPN Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>IPsec VPN Manager</td>
<td>IPsec VPN Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Voice Service Manager</td>
<td>Voice Service Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Wireless Service Manager</td>
<td>Wireless Service Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Wireless Intrusion Prevention System</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Wireless Location Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Wireless Location Engine</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Network Traffic Analyzer</td>
<td>Network Traffic Analyzer</td>
<td>Master</td>
</tr>
<tr>
<td></td>
<td>Network Traffic Analyzer Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Network Behavior Analyzer</td>
<td>Master</td>
</tr>
<tr>
<td>Component</td>
<td>Subcomponent</td>
<td>Optional server</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>User Behavior Auditor</td>
<td>Network Behavior Analyzer Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>User Behavior Auditor Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Network Behavior Analyzer</td>
<td>Master</td>
</tr>
<tr>
<td></td>
<td>Network Behavior Analyzer Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Service Operation Manager</td>
<td>CMDB Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Service Desk</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Application Manager</td>
<td>Application Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>QoS Manager</td>
<td>QoS Management</td>
<td>Master</td>
</tr>
<tr>
<td>Service Health Manager</td>
<td>Service Health Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>NQA Collector Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>VAN Connection Manager</td>
<td>VAN Connection Management</td>
<td>Master</td>
</tr>
<tr>
<td>Branch Intelligent Management System</td>
<td>Branch Intelligent Management System</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Auto-Configuration Server</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Resource Automation Manager</td>
<td>Resource Automation Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>VAN SDN Manager</td>
<td>VAN SDN Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>VAN Fabric Manager</td>
<td>VAN Fabric Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>UC Health Manager</td>
<td>UC Health Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Endpoint Mobile Office</td>
<td>Mobile Office Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Mobile Office MDM Proxy</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Intelligent Strategy Proxy</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Security Service Manager</td>
<td>Security Service Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Load Balancing Manager</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td>Business Service Manager</td>
<td>Business Service Manager</td>
<td>Master</td>
</tr>
<tr>
<td>IT Service Manager</td>
<td>CMDB Management</td>
<td>Master or subordinate</td>
</tr>
<tr>
<td></td>
<td>Service Desk</td>
<td>Master or subordinate</td>
</tr>
</tbody>
</table>

All 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 13.

Table 13 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>
</tbody>
</table>
The following information describes how to install and deploy NTA, UAM, and MVM.

## Installing and deploying IMC NTA

### Installing 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 31**.

   ![Choose folder dialog box](image)

   **Figure 31 Choose folder dialog box**

2. Click **Browse**, and then select the **install\components** folder in the NTA installation package.

3. Click **OK**.
   The IMC installation wizard appears, as shown in **Figure 32**.
4. Click **Next**.

   The **Agreement** page appears, as shown in [Figure 33](#).
5. Read the license agreement and third-party license, and then select Accept.
6. Click Next.
   The Choose Target Folder page appears, as shown in Figure 34.
   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 in the component list.
8. Click Next.

The Deployment and Upgrade Options page appears, as shown in Figure 35.
9. Select **Deploy or upgrade later**.
10. Click **Next**.

The **Installation Summary** page appears, as shown in **Figure 36**.
11. Verify the installation information, and then click **Install**.

After the installation is complete, the **Installation Completed** page appears, as shown in Figure 37.
Deploying IMC NTA on the master server

1. Select Open deployment monitoring agent, and then click Finish.

   The system automatically starts the Intelligent Deployment Monitoring Agent and displays the Batch deploy page, as shown in Figure 38.
2. Select the NTA subcomponents you want to deploy. In this example, select all the NTA subcomponents.

3. 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 39.

**Figure 39 Batch deploy succeeded dialog box**

4. Select **Start iMC Server now**, and then click OK.
Deploying NTA subcomponents on a subordinate server

1. Install the Intelligent Deployment Monitoring Agent on the subordinate server if it has not been installed. (Details not shown.)

2. Start the Intelligent Deployment Monitoring Agent:
   - On Windows, select Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent.
   - On Linux, run the dma.sh script in the /deploy directory of the IMC installation path.

3. Click the Deploy tab in the Intelligent Deployment Monitoring Agent.
   The Deploy tab displays all IMC components that have been installed and their deployment information.

4. Right-click any component in the list, and then select Batch Deploy from the shortcut menu.
   The Batch deploy page displays components that are not deployed, as shown in Figure 40.

Figure 40 Batch deploy

5. Select the NTA subcomponents you want to deploy on the subordinate server. In this example, select Network Behavior Analyzer Server and Network Traffic Analyzer Server.

6. Click OK to start the deployment.
   After the deployment is finished, the Batch deploy result dialog box, prompting Batch deploy succeeded, appears.
7. Select **Start iMC Server now**, and then click **OK**.

### Installing and deploying IMC UAM

#### Installing IMC UAM

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

#### Deploying UAM on the master server

1. On the **Installation Completed** page shown in Figure 42, select **Open deployment monitoring agent**, and then click **Finish**.

The **Batch deploy** dialog box appears, as shown in Figure 43.
Select the UAM subcomponents you want to deploy, and then 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 can be deployed only on subordinate servers in distributed deployment.

The IMC deployment wizard starts and displays the Intelligent Strategy Proxy Configuration page, as shown in Figure 44.
3. 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.

4. Click **Deploy**.
   The **Configure User Access Management** page appears, as shown in Figure 45.
5. Configure the following parameters:
   - **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.
   - **UAM Server’s IPv4 Address**—This field is automatically populated with the IP address of the local host.

6. Click **Deploy**.
   The **Configure Portal Component** page appears, as shown in Figure 46.
7. Use the default settings, and then click **Deploy**.

   The **Configure EIP Server** page appears, as shown in Figure 47.
8. Use the default settings, and then click **Deploy**.

The **Configure Policy Server** page appears, as shown in Figure 48.
9. Use the default settings, and then click **Deploy**.

The **Configure User SelfService** page appears, as shown in Figure 49.
10. Use the default settings, and then click **Deploy**.

The **Third-Party Page Publish Server Configuration** page appears, as shown in Figure 50.
11. Use the default settings, and then click **Deploy**.
All the selected UAM subcomponents are deployed.
The **Batch deploy succeeded** dialog box appears, as shown in Figure 51.

**Figure 51 Batch deploy succeeded dialog box**

12. Configure **Start iMC Server now** as needed, and then click **OK**.

**Deploying UAM on a subordinate server**

1. In the Intelligent Deployment Monitoring Agent, click the **Deploy** tab.
The **Deploy** tab displays information about all IMC components that have been installed.
2. Right-click a component that is not deployed, and then select **Batch Deploy** from the shortcut menu.
The **Batch deploy** dialog box appears, as shown in [Figure 52](#).

**Figure 52 Batch deploy dialog box**

![Batch deploy dialog box](image)

3. Select the UAM subcomponents you want to deploy.
   In this example, select User Access Management Sub Server and EIP Sub Server.

4. Click **OK**.
   The system starts to deploy the selected UAM subcomponents.
   The IMC deployment wizard starts and displays the **Configure EIP Server** page, as shown in [Figure 53](#).
5. Enter the IP address of the EIP Sub Server component in the **EIP Server’s IPv4 Address** field. By default, this field is automatically populated with the IP address of the local host.

6. Click **Deploy**.

The **Configure User Access Management Sever** page appears, as shown in **Figure 54**.
Figure 54 Configure User Access Management Sever page

7. Enter the IP address of the host where User Access Management Sub Server is to be deployed in the UAM SUB Server's IPv4 Address field. By default, this field is automatically populated with the IP address of the local host.

   After the deployment is complete, the batch deploy result dialog box appears, as shown in Figure 55.

Figure 55 Batch deploy result dialog box

8. Configure Start iMC Server now as needed, and then click OK.

62
Installing and deploying IMC MVM

Installing IMC MVM

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

Deploying MVM

MVM subcomponents can be deployed on both the master and subordinate servers. The following information only describes deploying subcomponents on the master server. You can deploy MVM on a subordinate server in the same way it is deployed on the master server.

To deploy MVM:

1. On the Installation Completed page shown in Figure 56, select Open deployment monitoring agent, and then click Finish.

   Figure 56 Installation Completed page

   ![Installation Completed dialog box](image)

   The Batch deploy dialog box appears, as shown in Figure 57.
2. Select the MVM subcomponents you want to deploy, and then click OK. In this example, select all the MVM subcomponents. The Please Choose L2VPN Global Parameter Operate page appears, as shown in Figure 58.
3. 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.

4. Click **Deploy**.
   After the deployment is complete, the **Batch deploy succeeded** dialog box appears, as shown in Figure 59.

**Figure 59 Batch deploy succeeded dialog box**

5. Configure **Start iMC Server now** as needed, and then click **OK**.
Installing plug-ins

Installing DHCP plug-ins

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

Installing a DHCP plug-in on an MS DHCP server

1. On the master server, edit the qvdm.conf file to enable IMC to obtain endpoint names or FQDNs from DHCP servers:
   a. In the server\config directory of the IMC installation path, use Notepad to open the qvdm.conf file.
   b. Add the following line to the file:
      
      l2toPCNameDhcpSwitch=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\config directory.
   d. Edit the imf.cfg file:
      - Set the value of IMGAddress to the IP address of the master 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 then 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 because the DHCP plug-in will not be uninstalled completely.
Installing a DHCP plug-in on a Linux DHCP server

1. On the master 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 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 master 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 of the plug-in installation package.

⚠️ **IMPORTANT:**
Do not delete the directory where the plug-in installation package `dhcp-plug-linux.zip` is decompressed because the DHCP plug-in will not be uninstalled completely.

Installing VRM plug-ins

Virtual Resource Management (VRM) is a subcomponent of the IMC platform to manage virtual networks. VRM must work with a VRM Windows agent for Hyper-V or VRM Linux agent for KVM.
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, install VRM Windows agents on Microsoft VMM servers as a best practice. 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 the 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\serverimf\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:
   - 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 Service (Local) list, right-click IMC VRM Agent, and then 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 of KVM and Xen, 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 Red Hat Enterprise Linux as root.
2. Insert the Linux installation disk into the CD-ROM drive, and then 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 then enter the local directory where the packages are saved.
5. Install packages, where xxx indicates the package name.
   
   ```bash
   rpm -i --nodeps xxx
   ```

**Installation procedure**

To install a VRM Linux agent:

1. Decompress the vrmd-plugin-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 vrmd-plugin-linux folder.
4. Enter the IP address of the IMC server. The default setting is localhost.
5. Verify that the installation is successful.

   ```bash
   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 vrmd-plugin-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 LLDP agent installation because DHCP plug-ins will not be uninstalled completely.

Installing an LLDP Windows agent

LLDP Windows agent plug-ins 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 configuration file lldpagent.conf is located in the conf directory of the LLDP Windows agent installation path.
   The LLDP Windows agent supports both LLDP and CDP. You can enable either of them, but not both. 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=300, and then 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 configuration file lldpagent.conf is located in the conf directory of the LLDP Linux agent installation path.
   The LLDP Linux agent supports both LLDP and CDP. You can enable either of them, but not both. 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=300, and then set the interval as needed.
      The default setting is 300 seconds.
   d. Save and close the file.

3. Restart the llp-agent service.
   service llpd-agent restart
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 14 lists the hardware, software, and browser requirements for accessing IMC.

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

Accessing IMC from a PC

Accessing IMC

1. Enter a URL in either of the following formats in the address bar of the browser:
   o http://ipaddress:port/imc
   o https://ipaddress:port/imc

   In the URL strings, ipaddress is the IP address of the master 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 then click Login.

   By default, the IMC superuser name and password are both admin.

   **IMPORTANT:**
   - For security purposes, change the password of the IMC superuser admin immediately after the first login.
   - When you attempt to access IMC by using HTTPS, a certificate error message might appear. For more information, see HPE 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://ipaddress:port
- http://ipaddress:port/selfservice

In the URL, ipaddress is the IP address of the master server and port is the HTTP port number used by IMC.
Accessing the SOM service desk

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

http://ipaddress:port/servicedesk

In the URL, ipaddress is the IP address of the master server and port is the HTTP port number used by IMC.

Accessing IMC from a mobile device

1. Open the browser on the mobile device.
2. Enter http://ipaddress:port/imc in the browser’s address bar.
   In the URL, ipaddress is the IP address of the IMC server and 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 the Operator and Password fields.
   Make sure the operator has been added to IMC. The operator account used for login must belong to an operator group that has the IMC Platform - Resource Management > Mobile Client Access operation privilege.
4. Select Mobile or 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:
   - View information about faulty devices and interfaces, and query devices.
   - View device alarms.
   - Receive realtime alarms.
   - Test device reachability by using a ping or tracert command.
   - View custom views and device views.
5. Click Login.

Securing IMC

As a best practice, perform 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 master server, enter the \client\conf directory of the IMC installation path (/client/conf on Linux).
2. Use Notepad (or vi on Linux) to open the 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 HTML format named `terms.html`.

6. Save the `terms.html` file to the `\client\web\apps\imc` directory of the IMC installation path on the master server (`/client/web/apps/imc` on Linux).

7. Display the IMC login page.

   A **User agreement** link appears. Operators can click the link to view the terms of the user agreement.

   **Figure 60 Viewing the user agreement on the login page**
Upgrading IMC

The following information describes how to upgrade IMC components, using the IMC platform as an example.

Preparing for the upgrade

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

- Obtain the upgrade packages for the IMC platform and all the deployed service components. After the IMC platform upgrade, you must upgrade all the service components.
- Back up the IMC installation directory and database files. If the upgrade fails, you can use the backup files to restore IMC.

To back up the IMC installation directory and database files:

a. Use DBMan in the Intelligent Deployment Monitoring Agent to back up the database files. For more information, see manual backup described in "Backing up and restoring the database."

b. Stop all IMC processes, and then manually copy the IMC installation directory to a specific path.

Upgrading IMC

⚠️ CAUTION:

- Make sure you have compatible upgrade packages for all deployed IMC components. If components do not have upgraded 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 61.

   Figure 61 Choose folder dialog box

2. Click Browse, and then select the \install\components directory in the upgrade package.
3. **Click OK.**
   The IMC installation wizard appears, as shown in Figure 62.

**Figure 62 IMC installation wizard**

![IMC Installation Wizard](image)

4. **Click Next.**
   The **Agreement** page appears, as shown in Figure 63.
Figure 63 Agreement page

![License Agreement Screen](image)

5. Read the license agreement, select **Accept**, and then click **Next**.
The **Upgrade Common Components** dialog box appears, as shown in **Figure 64**.

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

Figure 64 Upgrade Common Components dialog box

![Upgrade Common Components Dialog](image)

6. Click **OK**.
The system automatically upgrades common components and displays the upgrade progress, as shown in **Figure 65**.
After the common components are upgraded, the Choose Target Folder page appears, as shown in Figure 66. The page displays the components whose upgrade packages are to be installed and the installation location.

7. Verify the information, and then click Next.

The Deployment and Upgrade Options page appears, as shown in Figure 67.
8. Select **Deploy or upgrade at once**, and then click **Next**.

The **Installation Summary** page appears, as shown in **Figure 68**.
9. Verify the installation summary, and then click **Install**.

After the installation is complete, the **Batch upgrade** dialog box appears, as shown in Figure 69.
10. Select the components you want to upgrade, and then click **OK**. After the upgrade is complete, the **Batch upgrade result** dialog box shown in **Figure 70** or **Figure 71** appears. The dialog box content varies depending on whether auto backup and restoration settings have been configured in DBMan before the upgrade.

**Figure 70 Batch upgrade result without auto backup and restoration**

**Figure 71 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 then click **OK**.

13. To start IMC, click **Start iMC** on the **Monitor** tab of the Intelligent Deployment Monitoring Agent.
Restoring IMC

If the IMC upgrade still fails, restore IMC to the version before the upgrade:

1. Restore the IMC database. For more information, see manual restoration described in "Backing up and restoring the database."
2. After the restoration is complete, stop IMC in the Intelligent Deployment Monitoring Agent.
3. Close the Intelligent Deployment Monitoring Agent.
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 HP iMC Server 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 active server in the failover system.
Uninstalling IMC

The IMC uninstallation procedures on Windows and Linux systems are similar. The following information describes how to uninstall IMC on Windows Server 2012 R2.

To reinstall IMC, complete the following tasks before 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 interrupts with an error, manually delete the IMC installation directory and the iMC-Reserved folder. The iMC-Reserved folder is located in the WINDOWS directory 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 to stop the IMC service.
3. On the Deploy tab, right-click the component to be uninstalled, and then 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 then 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

First uninstall the components deployed on subordinate servers, and then uninstall the components deployed on the master server.

Uninstalling the IMC components from each subordinate server

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**.
5. Click **OK** in the confirmation dialog boxes that appear. The Intelligent Deployment Monitoring Agent uninstalls all the components. After the uninstallation is complete, the **Uninstallation Completed** dialog box appears.
6. Clear the OS reboot option, and then click **OK**.
7. Delete the **iMC-Reserved** folder in the **WINDOWS** folder or the Linux /etc directory.
8. Reboot the operating system.

**Uninstalling the IMC components from the master server**

1. Start 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. Clear the OS reboot option, and then click **OK**.
7. Delete the **iMC-Reserved** folder in the **WINDOWS** folder or the Linux /etc directory.
8. Reboot the operating system.
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 HPE Support.

Registering IMC

1. On the IMC login page, click **Activate**.
   The **License Information** page appears, as shown in **Figure 72**.
   **Figure 72 License Information page**

   ![License Information](image)

   - **Serial Number**: JG747AEE
   - **Product Number**: IMCM-20CBE300CBE350426B2

   Your license is a trial version, and it will expire on January 22, 2016. Please click the **Activate** link to reactivate the license before the expiration date.

   Use the product number and serial number to register your product. For more information, see the installation guide.

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

Registering first license


   The **HPE Passport sign-in** page appears, as shown in **Figure 73**.
2. Enter the user ID and password and click **Sign in**. The **Home** page appears, as shown in Figure 74.

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 75.
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 76.

5. Enter an email address associated with the Order number and click Next. The Select the Product License page appears, as shown in Figure 77.
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 78.

Figure 78 Enter details page

8. Enter the IMC software serial number and click Next.
   The License agreement page appears, as shown in Figure 79.

Figure 79 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 80.
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. Select the Incremental Node License you want to register on the **Select the Product License** page.
2. Click Next. The Enter details page appears, as shown in Figure 82.

Figure 82 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 72.
2. Select Activate now.
   The Register Your Product page appears, as shown in Figure 83.

Figure 83 Register Your Product page

<table>
<thead>
<tr>
<th>Register Your Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Key File</td>
</tr>
<tr>
<td>Register as Primary</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 as needed.
5. Click OK.
   The Registration Succeeded dialog box appears, as shown in Figure 84.

Figure 84 Registration succeeded dialog box

   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 85.
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. Log in to the HPE My Networking system website ([http://hpe.com/networking/mynetworking/](http://hpe.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 86**.

**Figure 86 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 87.

**Figure 87 License information**

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>JG74TAEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Number</td>
<td>IMCM-20CBE500CBEF5042682</td>
</tr>
</tbody>
</table>

4. Record the serial number of the primary server that is displayed in the Serial Number area.
5. Log in to the HPE My Networking system website (http://hpe.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 88.

**Figure 88 Registering your product**

<table>
<thead>
<tr>
<th>Activation Key File</th>
<th>Browse...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register as</td>
<td>Primary</td>
</tr>
</tbody>
</table>

10. Click **Browse** to select the locally saved Activation key file.
11. Select **Primary** from the **Register** list.
12. Click **OK**.
   IMC has been 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 **Backup** from the **Register as** list.

**Figure 89 Registering your product**

19. Click **OK**.

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

Anti-virus software

As a best practice to improve security, install anti-virus software on IMC servers and keep the virus definitions up to date.

Port settings

As a best practice, use a firewall to protect the IMC server cluster by filtering the non-service data sent to the cluster. If the firewall is installed on the master server or subordinate servers, open the IP addresses of the subordinate servers or the master server in the firewall to ensure correct communication between them.

**NOTE:**
- As a best practice to prevent packet fragmentations from being filtered, use ACL configurations on a firewall rather than on a switch to control data packets.
- 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 15 and Table 16) are not blocked by the firewall.

### Table 15 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 16 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>Default port number</td>
<td>Usage</td>
<td>Location</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>TCP 9099</td>
<td>JMX listening port for the NTA/UBA service</td>
<td>IMC server</td>
</tr>
<tr>
<td>UDP 18801, 18802, 18803</td>
<td>Communication ports between the NTA and UBA</td>
<td>IMC server</td>
</tr>
</tbody>
</table>
Backing up and restoring the database

**IMPORTANT:**

In distributed deployment, DBMan is available only on the master server.

DBMan is an automatic backup and restoration tool for the IMC platform and service component databases, and it provides a full-range system disaster backup solution. DBMan uses a standard 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 90.

**Figure 90 Environment tab**

The Environment tab includes the following areas:

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

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

- To ensure correct operation, do not back up and restore IMC databases between different operating systems.
- 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 conditions:
  - 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 DBMan on the database server

By default, DBMan is not installed on the remote database server. Before database backup and restoration, install DBMan on the database server.

DBMan can be installed automatically when you install the Intelligent Deployment Monitoring Agent. To start the remote installation wizard for installing the Intelligent Deployment Monitoring Agent, see "Starting the remote installation wizard through the installation package."

To install the Intelligent Deployment Monitoring Agent after the wizard has been started, see "Installing the Intelligent Deployment Monitoring Agent."

After installation, DBMan will be started when you start the server.

Upgrading DBMan

When you upgrade IMC, the **Upgrade Common Component** dialog box appears, as shown in Figure 91. Click **Yes** to upgrade common components including DBMan.
Backing up and restoring databases for a single IMC system

Back 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**.
2. In the confirmation dialog box that appears, click **OK**.
   The **Auto Backup and Recovery Settings** dialog box appears, as shown in Figure 92.
3. Read information in the **Auto Backup and Recovery Settings** dialog box, select **Auto Backup Model**, and then click **OK**.

The page for configuring auto backup settings appears, as shown in Figure 93.
4. On the **Basic Configuration** tab, configure the following parameters:
   - **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.
   - **Backup file lifetime (days)**—Enter how many days a backup file can be kept. Expired files are automatically deleted.
   - **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 **Master Server** tab, and then configure the following parameters:
Storage Path of iMC Files—Enter or browse to the path where the backup IMC files are stored.

Storage Path of Database Files—Enter or browse to the path where the backup database files are stored.

Local Back Up—Select the databases to back up locally on the master 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 Subordinate Server tab, and then configure the following parameters:

TIP:
In distributed deployment, each subordinate IMC server has a separate Subordinate Server tab in DBMan.

Storage Path of iMC Files—Enter or browse to the path where the backup IMC files are stored.

Storage Path of Database Files—Enter or browse to the path where the backup database files are stored.

Local Back Up—Select the databases to back up locally on the subordinate 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 Back Up option is forcibly selected for the database. To configure the FTP server, see “Configuration restrictions and guidelines.”

7. Click the Extension 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.

Upload backup files of Subordinate Servers to Master Server—Specify whether to upload local backup files from subordinate servers to the master server.

8. Click OK.

Restoring databases

A single IMC system supports only manual restoration of the databases.

Manual restoration immediately replaces all database files with the backup database files. It supports the following types:

- Locally Restore—Applicable to scenarios where all backup files are saved on the master server.
- Remotely Restore—Applicable to scenarios where backup files are saved on the master and subordinate servers.

As a best practice, 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.

Make sure IMC has been started at least once after installation before you restore the IMC databases.

To perform a manual restoration:

1. On the Environment tab, click Restore.
The **Restoration Type** dialog box appears, as shown in Figure 94.

**Figure 94 Restoration Type dialog box**

![Restoration Type dialog box](image)

2. Perform one of the following operations:
   
   If all backup files are saved on the master server:
   
   a. Click **Locally Restore**.
      
      The **Confirm** dialog box appears, as shown in Figure 95.

      **Figure 95 Confirming the operation**

      ![Confirm dialog box](image)

   b. Click **Yes**.
      
      The **Select the data file to be restored** dialog box appears.

   c. Select database files to be restored, and then click **OK**.
      
      A confirmation dialog box appears.

      **Figure 96 Confirmation dialog box**

      ![Confirmation dialog box](image)

   d. Click **Yes**.
      
      The system starts restoring the database files.

   If backup files are saved on the master and subordinate servers:
   
   a. Click **Remotely Restore**.
      
      The **Configure Remote Restoration** dialog box appears.
b. Click **Configure** to select the database files to be restored on the master and subordinate servers, and then click **OK**.

A confirmation dialog box appears.

**Figure 98 Confirmation dialog box**

![Confirmation dialog box](image)

C. Click **Yes**.

The system starts restoring the database files.

After the local or remote restoration is complete, the system displays a restoration success message.

3. Click **OK**.

The IMC service will be automatically started.

**NOTE:**

- Before remote restoration, you must configure automatic backup and restoration parameters. Then DBMan can automatically locate running configuration files and database files.
- During the restoration process, DBMan shuts down and restarts IMC and the database service.

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

A typical stateless failover scenario includes a primary IMC system and a backup IMC system:
The primary IMC system is deployed in distributed mode and uses a remote database.

The backup IMC system is deployed in centralized or distributed mode.

For stateless failover, configure automatic backup on the primary server and configure automatic restoration on the backup server. During automatic backup and restoration, the primary server performs the following operations:

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

As a best practice, restore database files for all components together. If you restore databases for only some of the components, the other components might become unavailable.

NOTE:
In a stateless failover scenario, you can perform any of the operations in the Auto Backup and Recovery Settings dialog box to back up data:

- Clear the option Delete local files after upload even if upload fails in the automatic backup configuration on the primary server.
- Set a path in Backup files location fields in the automatic restoration configuration on the backup server.

**Backing up databases**

In a stateless failover scenario, you can configure automatic backup on the primary server.

Before the configuration, make sure the following settings are the same on the primary server and the backup server:

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

For more information about how to configure automatic backup, see "Automatic backup."

**Restoring databases**

In a stateless failover scenario, you can configure automatic restoration on the backup server. After receiving the backed up database files from the primary server, the backup server automatically restores the database files locally.

This example describes the automatic restoration settings for a failover IMC system that is deployed in distributed mode and uses a remote database.

To configure automatic restoration:

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 99.
3. Read information in the **Auto Backup and Recovery Settings** dialog box, select **Auto Restore Model**, and then click **OK**.
   The page for configuring automatic restoration settings appears, as shown in **Figure 100**.
4. Click the Master Server tab and configure the following parameters:
   - **Backup files location of iMC**—Enter or browse to the path where the uploaded backup IMC files are stored on the master server.
   - **Backup files location of database**—Enter or browse to the path where the uploaded backup database files are stored on the master server.
   - **Restore**—Select databases to restore. By default, all databases are selected.

5. Click the Subordinate Server tab and configure the following parameters:
   - **Backup files location of iMC**—Enter or browse to the path where the uploaded backup IMC files are stored on a subordinate server.
   - **Backup files location of database**—Enter or browse to the path where the uploaded backup database files are stored on a subordinate server.
   - **Restore**—Select databases to restore. By default, all databases are selected.

6. Click OK.
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.

1. Download the JDK installation file from Oracle website:
   Make sure 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 then install JDK:
   ```
   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.
   On the Linux operating system, execute the following commands:
   ```
   cd /var/local/firefox/plugins/
   ln -s /usr/java/default/jre/plugin/i386/ns7/libjavaplugin_oji.so
   ```
   After the installation, run /var/local/firefox/firefox to 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 then modify the database file storage path:
   ```
   pwdmgr.bat -changeDataDir "D:\imcdata"
   ```
   Figure 101 shows that the storage path has been successfully modified.

Figure 101 Modifying the database file storage path

4. Start the IMC service.
On Linux, the time on the server (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. How can I resolve this issue?

This issue occurs because the current time zone setting on the server is different from that when IMC was installed. You can use the `tzselect` command to modify the time zone of the server.

After IMC is installed in the Windows Server 2003 64-bit OS, the IMC background processes cannot be started. How can I resolve this issue?

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 occurs and the system displays a database script execution error message. The log file includes an error message that the object `dbo.qv.id` already exists. How can I resolve this issue?

1. Log in to the Query Analyzer of SQL Server as sa, and then execute the following commands:
   ```sql
   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 indicates that the Windows Installer cannot be installed, as shown in Figure 102. How can I resolve this issue?

Figure 102 Windows Installer dialog box

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

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

Use `service IMCdmsd start` to start the JavaService.

On Windows, IMC service processes cannot be started or stopped after IMC runs for a period of time. How can I resolve this issue?

This issue is caused by insufficient virtual memory.
To resolve this issue, 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 103.

**Figure 103 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 104.
3. Click the *Advanced* tab, and then click *Change* in the *Virtual memory* area. The *Virtual Memory* dialog box appears, as shown in Figure 105.
4. Select **System managed size**, and then click **Set**.

5. Click **OK**.

**On Linux, popup windows cannot be found during IMC deployment or upgrade. How can I resolve this issue?**

When Xshell or Xstart is used for remote GUI access on Linux, a window might appear on top of popup windows. To resolve this issue, move the window away to view the popup windows.
# About HPE IMC documents

The following are the documents available for HPE IMC:

<table>
<thead>
<tr>
<th>Documents</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware specifications and installation</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HPE IMC Getting Started Guide</strong></td>
<td>Quickly guides you through the IMC main features and troubleshooting common problems.</td>
</tr>
<tr>
<td><strong>HPE IMC Centralized Deployment Guide with Embedded Database</strong></td>
<td>Provides a complete guide to IMC platform and components installation and centralized deployment using embedded database.</td>
</tr>
<tr>
<td><strong>HPE IMC Centralized Deployment Guide with Local Database</strong></td>
<td>Provides a complete guide to IMC platform and components installation and centralized deployment using local database.</td>
</tr>
<tr>
<td><strong>HPE IMC Centralized Deployment Guide with Remote Database</strong></td>
<td>Provides a complete guide to IMC platform and components installation and centralized deployment using remote database.</td>
</tr>
<tr>
<td><strong>HPE IMC Distributed Deployment Guide with Local Database</strong></td>
<td>Provides a complete guide to IMC platform and components installation and distributed deployment using local database.</td>
</tr>
<tr>
<td><strong>HPE IMC Distributed Deployment Guide with Remote Database</strong></td>
<td>Provides a complete guide to IMC platform and components installation and distributed deployment using remote database.</td>
</tr>
<tr>
<td><strong>HPE IMC Probe Installation Guide</strong></td>
<td>Provides a complete guide to IMC Probe installation and deployment.</td>
</tr>
<tr>
<td><strong>HPE IMC RSM Installation Guide</strong></td>
<td>Provides a complete guide to IMC RSM installation and deployment.</td>
</tr>
<tr>
<td><strong>HPE IMC iHATool Installation Guide</strong></td>
<td>Provides a complete guide to IMC iHATool installation.</td>
</tr>
<tr>
<td><strong>SQL Server 2008 Installation and Configuration Guide</strong></td>
<td>Guides you through installing SQL Server 2008 for IMC.</td>
</tr>
<tr>
<td><strong>SQL Server 2008 R2 Installation and Configuration Guide</strong></td>
<td>Guides you through installing SQL Server 2008 R2 for IMC.</td>
</tr>
<tr>
<td><strong>SQL Server 2012 Installation and Configuration Guide</strong></td>
<td>Guides you through installing SQL Server 2012 for IMC.</td>
</tr>
<tr>
<td><strong>SQL Server 2014 Installation and Configuration Guide</strong></td>
<td>Guides you through installing SQL Server 2014 for IMC.</td>
</tr>
<tr>
<td><strong>Oracle 11g Installation and Configuration Guide (for Linux)</strong></td>
<td>Guides you through installing Oracle 11g on Linux for IMC.</td>
</tr>
<tr>
<td><strong>Oracle 11g R2 Installation and Configuration Guide (for Linux)</strong></td>
<td>Guides you through installing Oracle 11g R2 on Linux for IMC.</td>
</tr>
<tr>
<td><strong>Oracle 12c Installation and Configuration Guide (for Linux)</strong></td>
<td>Guides you through installing Oracle 12c on Linux for IMC.</td>
</tr>
<tr>
<td><strong>MySQL 5.5 Installation and Configuration Guide (for Linux)</strong></td>
<td>Guides you through installing MySQL 5.5 on Linux for IMC.</td>
</tr>
<tr>
<td><strong>MySQL 5.5 Installation and Configuration Guide (for Windows)</strong></td>
<td>Guides you through installing MySQL 5.5 on Windows for IMC.</td>
</tr>
<tr>
<td><strong>MySQL 5.6 Installation and Configuration Guide (for Linux)</strong></td>
<td>Guides you through installing MySQL 5.6 on Linux for IMC.</td>
</tr>
<tr>
<td><strong>Documents</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td><em>MySQL 5.6 Installation and Configuration Guide (for Windows)</em></td>
<td>Guides you through installing MySQL 5.6 on Windows for IMC.</td>
</tr>
<tr>
<td><em>Red Hat Enterprise Linux 6.4 Installation Guide</em></td>
<td>Guides you through installing Red Hat Enterprise Linux 6.4 for IMC.</td>
</tr>
<tr>
<td><em>Red Hat Enterprise Linux 7.0 Installation Guide</em></td>
<td>Guides you through installing Red Hat Enterprise Linux 7.0 for IMC.</td>
</tr>
<tr>
<td><strong>Software configuration</strong></td>
<td></td>
</tr>
<tr>
<td><em>HPE IMC Enterprise and Standard Platform Administrator Guide</em></td>
<td>Describes operation procedures on the IMC platform.</td>
</tr>
<tr>
<td><em>HPE IMC Quality of Service Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC Quality of Service Manager.</td>
</tr>
<tr>
<td><em>HPE IMC Service Health Manager Administrator Guide</em></td>
<td>Describes operation procedures on the Service Health Manager.</td>
</tr>
<tr>
<td><em>HPE IMC VAN Connection Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC VAN Connection Manager.</td>
</tr>
<tr>
<td><em>HPE IMC VAN Software Defined Network Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC VAN Software Defined Network Manager.</td>
</tr>
<tr>
<td><em>HPE IMC VAN Fabric Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC VAN Fabric Manager.</td>
</tr>
<tr>
<td><em>HPE IMC Application Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC Application Manager.</td>
</tr>
<tr>
<td><em>HPE IMC Branch Intelligent Management System Administrator Guide</em></td>
<td>Describes operation procedures on the IMC Branch Intelligent Management System.</td>
</tr>
<tr>
<td><em>HPE IMC Business Service Performance Administrator Guide</em></td>
<td>Describes operation procedures on the IMC Business Service Performance.</td>
</tr>
<tr>
<td><em>HPE IMC IPsec VPN Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC IPsec VPN Manager.</td>
</tr>
<tr>
<td><em>HPE IMC MPLS VPN Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC MPLS VPN Manager.</td>
</tr>
<tr>
<td><em>HPE IMC Network Traffic Analyzer Administrator Guide</em></td>
<td>Describes operation procedures on the IMC Network Traffic Analyzer.</td>
</tr>
<tr>
<td><em>HPE IMC Service Operation Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC Service Operation Manager.</td>
</tr>
<tr>
<td><em>HPE IMC User Behavior Auditor Administrator Guide</em></td>
<td>Describes operation procedures on the IMC User Behavior Auditor.</td>
</tr>
<tr>
<td><em>HPE IMC UC Health Manager Admin Guide</em></td>
<td>Describes operation procedures on the IMC UC Health Manager.</td>
</tr>
<tr>
<td><em>HPE IMC Wireless Service Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC Wireless Service Manager.</td>
</tr>
<tr>
<td><em>HPE IMC User Access Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC User Access Manager.</td>
</tr>
<tr>
<td><em>HPE IMC TACACS+ Authentication Manager Administrator Guide</em></td>
<td>Describes operation procedures on the IMC TACACS+ Authentication Manager.</td>
</tr>
<tr>
<td>Documents</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Online Help</td>
<td>Helps you properly use IMC.</td>
</tr>
<tr>
<td>Operations and maintenance</td>
<td></td>
</tr>
<tr>
<td>Readme</td>
<td>Provides most recent IMC release information.</td>
</tr>
</tbody>
</table>
Document conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Command conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Bold text represents commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td><em>Italic</em> text represents arguments that you replace with actual values.</td>
</tr>
<tr>
<td>#</td>
<td>A line that starts with a pound (#) sign is comments.</td>
</tr>
</tbody>
</table>

GUI conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Window names, button names, field names, and menu items are in Boldface. For example, the <strong>New User</strong> window appears; click <strong>OK</strong>.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Multi-level menus are separated by angle brackets. For example, <strong>File &gt; Create &gt; Folder</strong>.</td>
</tr>
</tbody>
</table>

Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>△ WARNING!</td>
<td>An alert that calls attention to important information that if not understood or followed can result in personal injury.</td>
</tr>
<tr>
<td>△ CAUTION:</td>
<td>An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.</td>
</tr>
<tr>
<td>☛ IMPORTANT:</td>
<td>An alert that calls attention to essential information.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
<tr>
<td>☀ TIP:</td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  [www.hpe.com/assistance](http://www.hpe.com/assistance)
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  [www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center Get connected with updates page:
    [www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates)
  - Software Depot website:
    [www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

**IMPORTANT:**
Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

<table>
<thead>
<tr>
<th>Website</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking websites</td>
<td></td>
</tr>
</tbody>
</table>
Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product’s service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.