Abstract
This document describes the processes and procedures to follow when installing the HP 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.
# Contents

1 Introduction to Intelligent Management Center
   - IMC components ................................................................. 1
   - IMC Platform ........................................................................ 1
   - Service components ............................................................ 2
   - IMC editions ......................................................................... 3

2 Preparing for installation ................................................................ 5
   - Hardware requirements ......................................................... 5
   - Software requirements .......................................................... 7
   - Setting the Java memory size on 32-bit OS ......................... 8
   - Installing IMC on a virtual machine ................................. 8
   - Checking the installation environments .......................... 8
   - Checking the system time .................................................... 9
   - Setting the time zone .......................................................... 10

3 Installation and deployment requirements ..................................... 11
   - Terms and concepts .......................................................... 11
     - Installation and deployment ............................................. 11
     - Installation modes ......................................................... 11
     - Superuser ...................................................................... 12
   - Prerequisites for deploying IMC in distributed mode .......... 12
     - Checking installation environments ............................. 13
     - Installing Java Runtime Environment (JRE) .................. 13
   - Prerequisites for installing a separate database ............... 15
   - Restrictions of using the embedded database .................. 16
   - IMC service logon accounts .............................................. 16
   - Obtaining IMC installation and deployment methods ....... 17

4 Installing and deploying the IMC Platform .................................... 18
   - Installing the IMC Platform .................................................. 19
     - Typical installation ......................................................... 19
     - Custom installation ...................................................... 23
   - Deploying the IMC Platform ............................................... 29
     - Deploying IMC in centralized mode with a separate database 29
     - Deploying IMC in centralized mode with the embedded database 33
     - Deploying a single IMC component .............................. 34

5 Installing and deploying IMC service components ...................... 35
   - Installing IMC Network Traffic Analyzer (NTA) .............. 37
   - Deploying IMC Network Traffic Analyzer (NTA) ............ 42
     - Deploying to a centralized server .................................. 42
     - Deploying to subordinate servers ................................. 43

6 Installing plug-ins ...................................................................... 51
   - Installing DHCP plug-ins ................................................... 51
     - On the MS DHCP server ................................................. 51
     - On the Linux DHCP server ........................................... 52
   - Installing VNM agent plug-ins .......................................... 53
     - Installing a VNM Windows agent ................................. 53
     - Installing a VNM Linux agent ...................................... 54
   - Installing Android clients ............................................... 58
1 Introduction to Intelligent Management Center

Intelligent Manager Center (IMC) runs on Windows or Linux. When running on Windows, IMC stores and manages data through SQL Server or MySQL. When running on Linux, IMC stores and manages data through Oracle or MySQL.

To ensure proper operation of IMC, you need to install the operating system, database, and IMC software.

IMC does not provide separate client software for access. HP recommends that you access the IMC system using the following Web browsers:

- Internet Explorer 8.0 or later
- Firefox 3.6 or later

IMC components

IMC includes the IMC Platform and service components.

IMC Platform

The IMC Platform is the base component for providing IMC services and includes the following subcomponents:

- ACL Management
- Alarm Management
- Data Analysis Manager
- Data Analyzer
- Guest Access Management
- Intelligent Configuration Center
- Network Asset Management
- Network Element (NE) Management
- Performance Management
- Report Management
- Resource Management
- Security Control Center
- Syslog Management
- User Selfservice Management
- Virtual Network Management
- VLAN Management
Service components

Service components are optional and purchased separately from the IMC Platform. Their installation and deployment are based on the IMC Platform.

Primary service components are as follows:

- **Access and admission control**—Authenticates and authorizes the use of access services. Also cooperates with user management and network resource management to provide enhanced access service management.

- **Access user management**—Uses centralized mode and is integrated with device and topology management.

- **Applications Manager**—Allows system and network administrators to remotely manage application programs and resources. It also allows them to monitor various types of programs and services running on the network, such as Web application programs, application servers, Web servers, databases, network services, and systems.

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

- **Endpoint Admission Defense (EAD) Security Policy**—Endpoint Admission Defense enforces enterprise security policies on terminals to enhance terminal defense capabilities, control network access, and ensure network security.

- **User Behavior Auditor** provides a simple, efficient log auditing tool to help operators quickly and accurately view the network access information to locate problems.

- **IPsec VPN Manager**—Provides unified management of IPsec VPN configurations. It offers high-efficiency management and flexible deployment for network domains, IPsec device configurations, and security proposal templates.

- **MPLS VPN Manager**—Provides topology discovery for BGP/MPLS VPNs, status/performance monitoring, fault location, and service deployment.

- **Network Traffic Analyzer and User Behavior Auditor**—Network Traffic Analyzer simplifies bandwidth usage monitor on enterprise networks and provides easy-to-understand reports. **QoS Manager**—Manages QoS configurations on network devices to control and manage QoS for the overall network.

- **Remote Site Manager**—Remotely manages branch networks that might be isolated by firewalls or NAT devices, and greatly saves the network management costs by cutting down the needs of deploying network management software and IT staff on each branch.

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

- **Service Operation Manager**—Provides a solution to the operation and maintenance of enterprise IT networks. It focuses on the key service switching and operation part in the ITIL lifecycle, and supports for flows related with IT network operation and maintenance. With the flow management capability, Service Operation Manager makes all IT operation and maintenance activities controllable, measurable, and auditable.

- **User Access Manager**—Provides the following features:
Wireless Service Manager—Provides WLAN management functions to implement unified wired and wireless network management. With WSM, administrators can add wireless management functions to the existing wired network management system, saving investment and maintenance costs.

For information about all service components, see HP IMC Getting Started Guide.

The IMC Platform is the basis for implementing various services and must be installed before service component deployment.

The server on which the IMC Platform subcomponents are deployed is called the master server, and other IMC servers are called the subordinate servers.

The master server must contain at least the following IMC Platform subcomponents:

- Data Analysis Manager
- NE Management
- Report Management
- Resource Management
- Security Control Center
- Virtual Network Management

## IMC editions

Two editions of IMC are available:

- IMC Enterprise
- Standard

Table 1 shows the differences between the editions.

### Table 1 Differences between IMC editions

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

The embedded database uses SQL Server 2008 R2 SP2 Express. For information about the database installation procedures, see SQL Server 2008 R2 Installation and Configuration Guide.

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

- SQL Server 2005 Installation and Configuration Guide
- SQL Server 2008 Installation and Configuration Guide
- SQL Server 2008 R2 Installation and Configuration Guide
- MySQL 5.5 Installation and Configuration Guide (for Windows)
For information about installing a separate database for IMC on Linux, see the following documents:

- *Oracle 11g Installation and Configuration Guide*
- *Oracle 11g R2 Installation and Configuration Guide*
- *MySQL 5.5 Installation and Configuration Guide (for Linux)*
2 Preparing for installation

This chapter describes detailed information about the IMC installation requirements for both hardware and software.

Hardware requirements

Tables in this section list the server requirements for the operating system on which IMC is installed. They use the following terms:

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

For example, when the collection interval is 10 minutes for all performance instances, to collect performance data including CPU, memory, interface send and receive rates, unreachability rate, and response time on a device that contains one CPU, one memory bar, and 10 interfaces, the total collection units of the device are: \((1+1+10\times2+1+1)\times5/10=12\)

- **CPU**—The frequency of the CPU must be no less than 2.5 GHz.
- **Java heap size**—Maximum memory size to be used by Java processes on the IMC Web Server.

The hardware requirements of IMC vary with the components and networking circumstances. For more information, see the release notes of each component.

To improve the I/O performance, follow these guidelines:

- When the number of the collection units is from 100 K to 200 K, install two or more disks and a RAID card with a cache of 256 MB or more.
- 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 512 MB or more.
- 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 1 GB or more.
- HP recommends that you set the RAID level to 0. When you want to set the RAID level to 5 or 10, install the proper number of parity disks.

**Table 2 Server requirements in a 32-bit Windows operating system**

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
<td><strong>Collection unit</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td></td>
<td>5 K to 50 K</td>
</tr>
<tr>
<td>200 to 500</td>
<td>0 to 10 K</td>
</tr>
<tr>
<td></td>
<td>10 K to 100 K</td>
</tr>
</tbody>
</table>
### Table 3: Server requirements in a 64-bit Windows operating system

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node Collection unit</strong></td>
<td><strong>Online operator</strong></td>
</tr>
<tr>
<td>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td></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></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></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></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></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></td>
<td>40 K to 400 K</td>
</tr>
</tbody>
</table>

### Table 4: Server requirements in a 32-bit Linux operating system

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node Collection unit</strong></td>
<td><strong>Online operator</strong></td>
</tr>
<tr>
<td>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td></td>
<td>5 K to 50 K</td>
</tr>
<tr>
<td>200 to 500</td>
<td>0 to 10 K</td>
</tr>
<tr>
<td></td>
<td>10 K to 100 K</td>
</tr>
</tbody>
</table>

### Table 5: Server requirements in 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 Collection unit</strong></td>
<td><strong>Online operator</strong></td>
</tr>
<tr>
<td>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td></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></td>
<td>10 K to 100 K</td>
</tr>
</tbody>
</table>
## Management scale

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 K to 2 K</td>
<td>6 cores 16 GB 6 GB 4 GB</td>
</tr>
<tr>
<td>2 K to 5 K</td>
<td>8 cores 24 GB 8 GB 5 GB</td>
</tr>
<tr>
<td>5 K to 10 K</td>
<td>16 cores 32 GB 12 GB 7 GB</td>
</tr>
<tr>
<td>10 K to 15 K</td>
<td>24 cores 64 GB 16 GB 10 GB</td>
</tr>
</tbody>
</table>

## System minimum requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2003 (32-bit)</td>
<td>Service Pack 2 is required.</td>
</tr>
<tr>
<td>Windows Server 2003 (64-bit)</td>
<td>Service Pack 2 (64-bit) and KB942288 are required.</td>
</tr>
<tr>
<td>Windows Server 2003 R2 (32-bit)</td>
<td>Service Pack 2 is required.</td>
</tr>
<tr>
<td>Windows Server 2003 R2 (64-bit)</td>
<td>Service Pack 2 (64-bit) and KB942288 are required.</td>
</tr>
<tr>
<td>Windows Server 2008 (32-bit)</td>
<td>Service Pack 2 is required.</td>
</tr>
<tr>
<td>Windows Server 2008 (64-bit)</td>
<td>Service Pack 2 (64-bit) is required.</td>
</tr>
<tr>
<td>Windows Server 2008 R2 (32-bit)</td>
<td>Service Pack 1 is required.</td>
</tr>
<tr>
<td>Windows Server 2008 R2 (64-bit)</td>
<td>Service Pack 1 is required.</td>
</tr>
<tr>
<td>SQL Server 2008 R2</td>
<td>Service Pack 2 is required for SQL Server 2008 R2.</td>
</tr>
<tr>
<td>SQL Server 2012</td>
<td>These databases can be used for both Standard and Professional editions.</td>
</tr>
<tr>
<td>MySQL 5.1</td>
<td>None</td>
</tr>
<tr>
<td>MySQL 5.5</td>
<td>None</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 5 (32-bit)</td>
<td>None</td>
</tr>
<tr>
<td>Item</td>
<td>Requirement</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 5 (64-bit)</td>
<td>None</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 5.5 (32-bit)</td>
<td>None</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 5.5 (64-bit)</td>
<td>None</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server 6.1 (64-bit)</td>
<td>None</td>
</tr>
<tr>
<td>Oracle 11g Release 1</td>
<td>None</td>
</tr>
<tr>
<td>Oracle 11g Release 2</td>
<td>None</td>
</tr>
<tr>
<td>MySQL 5.1</td>
<td>None</td>
</tr>
<tr>
<td>MySQL 5.5</td>
<td>None</td>
</tr>
</tbody>
</table>

### Setting the Java memory size on 32-bit OS

HP recommends using a 64-bit operating system for the server when simultaneously deploying IMC Platform and service components.

When the server runs a 32-bit operating system, manually modify the assignable memory size of Java after deployment using the following method:

1. Use the editor (such as WordPad in Windows or vi in Linux) to run the `\client\bin\startup.bat` script or the `startup.sh` script on Linux,
2. Replace `set JAVA_OPTS=-server -Xmx512m -Xrs -XX:PermSize=64m -XX:MaxPermSize=386m ...` with `set JAVA_OPTS=-server -Xmx1024m -Xrs -XX:PermSize=64m -XX:MaxPermSize=576m ...`.
3. Save the file and restart the jserver process.
   - When the jserver process cannot start up, decrease the above values until it can start up.
   - When an out of memory error occurs after the jserver process starts up, use a 64-bit operating system.

### Installing IMC on a virtual machine

You can install IMC on a VMware virtual machine. Before installation, set the path where the virtual machine is located and hardware information including:

- Types and number of CPUs
- Number, models, and MAC addresses of network adapters
- Number and space of disk drives

After you install IMC, do not change the previous configuration or IMC installation path. Although changing them does not affect VM migration, IMC cannot operate properly.

### Checking the installation environments

For database installation instructions, see related database documents.
All of the requirements, listed in Table 7, must be met before installation.

⚠️ **CAUTION:**

- To ensure proper installation and operation of IMC, do not install IMC with other network management products on the same server.
- Use the same operating system bit count on the master and subordinate servers when you deploy IMC in distributed mode.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>Meets the specifications of CPU, memory, and hard disk in the contract.</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>Make sure that the type and version of the operating system, database version, and IMC version meet the installation requirements. The server is restarted after database installation.</td>
</tr>
<tr>
<td><strong>Database installation check</strong></td>
<td>Before installing IMC, install the database. During the IMC installation procedure, the corresponding database connections are checked. On Linux, a 32-bit operating system must use the 32-bit Oracle database and a 64-bit operating system must use the 64-bit Oracle database.</td>
</tr>
<tr>
<td><strong>Auto startup of SQL Server service</strong></td>
<td>Select <strong>Control Panel &gt; Administrative Tools &gt; Services</strong> and ensure the Startup Type item of the MSSQLSERVER is set to <strong>Automatic</strong>.</td>
</tr>
<tr>
<td><strong>Auto startup of SQL Server Agent</strong></td>
<td>Select <strong>Control Panel &gt; Administrative Tools &gt; Services</strong> and ensure the Startup Type item of the SQL SERVERAGENT is set to <strong>Automatic</strong>.</td>
</tr>
</tbody>
</table>
| **Uninstallation of IMC software** | A thorough uninstallation is required when IMC was previously installed on the system. For instructions on removing IMC, see "Removing IMC." Reboot the system after the IMC is uninstalled. To completely remove IMC:  
  - **Windows:** After you remove IMC, locate and delete the IMC-Reserved folder in the WINDOWS folder of the system disk.  
  - **Linux:** Locate and delete the IMC-Reserved folder in the /etc/ directory. |
| **Firewall settings check**  | To deploy IMC in distributed mode, open the listening port on the server installed with the database. The default listening port number is:  
  - SQL server database: 1433  
  - Oracle database: 1521  
  - MySQL database: 3306 |
| **Hardware**                | Meets the specifications of the CPU, memory, and hard disk in the contract.       |

**Checking the system time**

Before installing IMC, check that the system time, date, and time zone settings on the server are correct.

- When the settings on the server are incorrect, you need to adjust the settings.
After IMC is started, do not modify the system time of the server; otherwise, the following or other intermittent problems can occur.

- When you modify the system time to a future time that differs from the current time, the system can take a long time to process a large amount of data. It can exceed the maximum time that the data can be saved in the database. This affects the current data sampling speed and results in delay. After the processing of such data is complete, the delay is gradually recovered.
- When you modify the system time to a past time, data with overlapping time can occur, and data processing might become abnormal. After the overlapping time is past, data processing becomes normal again.

When you encounter other problems caused by system time modification for a master server, HP recommends that you restart all master and subordinate servers. For a subordinate server, you need to restart only the server.

When deploying IMC in distributed mode, ensure that the time zone settings of all servers are the same. In addition, HP recommends using the Network Time Protocol (NTP) to synchronize the time on all servers.

**Setting the time zone**

Before installing IMC in the Windows Server 2003 operating system, deselect *automatically adjust clock daylight saving changes* when you set the time zone in the **Date & Time** window.
3 Installation and deployment requirements

The following information describes important concepts and requirements for IMC installation and deployment. Read the information carefully before you install and deploy IMC.

Terms and concepts

- Installation and deployment
- Installation modes

Installation and deployment

To improve server performance, IMC uses the Install and Deploy model. IMC Install copies the IMC installation file to the master server and IMC Deploy decompresses the installation package and creates a database script on the master server or subordinate servers as needed.

Before IMC deployment, you must install the target components on the master server. The components of IMC are operational only after they are deployed.

You can deploy IMC in two ways:

- **Centralized deployment**—All IMC components are deployed to the master server. This deployment mode does not have any subordinate server.
- **Distributed deployment**—Basic IMC components are deployed to the master server, and other IMC components are deployed to the master server or subordinate servers.

**NOTE:**

- Master server is the management center of IMC. It interacts with subordinate servers to implement network management.
- Subordinate server is responsible for specific management tasks. For example, tasks performed by Performance Management and by Intelligent Configuration Center (ICC).

In the distributed deployment, the master server provides centralized Web services. You can access the master server for performing all management functions. For more information about accessing IMC, see "Logging in to IMC."

IMC automatically creates a database user when a service component is deployed. HP does not recommend you to modify the database user configuration, including the user’s password and password security strategy.

When the deployment or upgrade process is interrupted, IMC automatically stores logs as a compressed file in the `\tmp` directory of the IMC installation path. With the logs, you can quickly locate the problem or error that occurred in IMC deployment or upgrade.

Installation modes

IMC supports typical and custom installation.

- **Typical installation**—Allows you to quickly install and deploy all platform components on the master server.
Before performing the typical installation, you must first configure the installation parameters, such as database connectivity, installation location, and Web service port numbers. Typical installation applies to centralized deployment. All subcomponents of the IMC Platform must use a local database, embedded or separate.

- **Custom installation**—Allows you to select certain platform components to install and deploy on the master server and specify a remote database server. This installation method is available for both local and remote databases.

### Superuser

IMC installation requires you to enter a superuser account to test the database connectivity. You can use the default superuser account `sa` or enter another account who has the superuser privileges.

IMC uses this superuser account to create database files and user accounts for IMC Platform subcomponents and service components during deployment. After deployment, IMC Platform subcomponents and service components use their respective user accounts to for database access, instead of using the superuser account.

If the password of the superuser account has changed since IMC deployment, update the password by clicking **Change Password** on the **Environment** tab of the Intelligent Deployment Monitoring Agent. Otherwise, you cannot view database information on the **Environment** tab, deploy new components, or update existing components.

### Prerequisites for deploying IMC in distributed mode

- **Operating system and database of the master and subordinate servers:**
  Make sure that all subordinate servers and the master server use the same operating system. You can use SQL Server and MySQL database on Windows. You can use Oracle and MySQL database on Linux.

- **Components required to be deployed on the master server:**
  The following components of the IMC Platform must be deployed on the master server:
  - Data Analysis Manager
  - NE Management
  - Report Management
  - Resource Management
  - Security Control Center
  - Virtual Network Management

  For more information about other IMC Platform subcomponents, see "Installing and deploying the IMC Platform." The service components required to be deployed on the master server vary with the services you want IMC to offer. For more information, see "Installing and deploying IMC service components."

- To deploy components on the master server or a subordinate server, you must first install the IMC Platform subcomponents and service components on the master server.

- Before you deploy IMC components on the subordinate servers, first start the IMC service in the Intelligent Deployment Monitoring Agent on the master server.

- When the IMC Intelligent Deployment Monitoring Agent is already installed on the subordinate servers, uninstall it before you can deploy IMC components in distributed mode. For more information about uninstalling the Intelligent Deployment Monitoring Agent, see "Removing IMC."
To install IMC on Linux by using the Oracle database, you must configure the network service name. The following is an example of an application scenario:
When Server A (master server), and Servers B and C (subordinate servers) use local databases and have been configured with network service names TNSNAME_A for connecting to Server A, TNSNAME_B for connecting to Server B, and TNSNAME_C for connecting to Server C, respectively, you must configure the other two unavailable network service names for each server (for example, TNSNAME_B and TNSNAME_C for Server A).
For more information about network service name configuration, see Oracle 11g Installation and Configuration Guide or Oracle 11g R2 Installation and Configuration Guide.

Java Runtime Environment (JRE) 6.0 is installed on the subordinate servers.

To ensure a smooth process in distributed deployment, do not install, deploy, undeploy, or update IMC on the master and subordinate servers simultaneously.

When you deploy or upgrade components on a subordinate server, make sure the subordinate server can communicate with the master server, and does not operate the IMC Intelligent Deployment Monitoring Agent on the master and subordinate servers, such as starting IMC.

⚠️ CAUTION:
During the distributed deployment process, do not simultaneously install, deploy, undeploy, or update the IMC software on the master and subordinate IMC servers; otherwise, faults might occur.

Checking installation environments

IMC installation package provides a tool to check the system environments, database connectivity, and database installation environments.

The system environments check includes the following items:
- Whether or not the service port to be used by IMC is idle. If it is used by another program, you must remove that program or modify the service port of that program.
- Whether or not the physical memory reaches 2 GB.
- Whether or not database software is installed.

The database connectivity check requires you to enter various parameters for test. For example, if you are using a SQL Server database, the tool requires you to enter the following parameters:
- **Database Type**—Select the database type, SQL Server, MySQL, or Oracle.
- **Instance Name**—Use the default instance or select Other Instance to specify a user-defined instance.
- **Superuser**—Enter the database superuser name, default name sa or another account who has the superuser privileges.
- **Password**—Enter the password of the superuser.
- **Database Location**—Select the location of the database server from the list, local host or other server.
- **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. Otherwise, this field displays 127.0.0.1.
- **Listening Port**—Enter the listening port of the database server. The default is 1433.
- **Installation Location**—Enter or browse to the local directory where the IMC installation package is stored.
• **Data File Location**—Enter or browse to the local or remote directory where the database files are stored. If a remote database server is used, make sure the directory already exists on the database server, and IMC will verify the read and write access to that directory.

• **HTTP Port**—Enter the HTTP port number. The default is 8080.

• **HTTPS Port**—Enter the HTTPS port number. The default is 8443.

The database installation environments check includes the following items:

• Whether or not IMC supports the operating system version and patches.

• Whether or not .Net Framework 2.0 SP2 is installed.

• Whether or not the free space on the system disk reaches 512 MB.

To check the IMC installation environments:

1. **Copy the tool** ([envcheck.bat](#) for Windows, [envcheck.sh](#) for Linux) from the [tools](#) folder to the **install** folder of the IMC installation package.

2. **Run the tool.** The tool starts to check the system environments. If the check is passed, the system tests the database connectivity in the **Checking Installation Parameters** window or tests the installation environments for installing the embedded database.

3. **View the check result.** If not all check items are passed, adjust your installation environments and run the tool again.

4. **Click Exit.**

### Installing Java Runtime Environment (JRE)

Use either of the following methods to install JRE 6.0:

• **Method 1:**
  Download the program from [http://www.oracle.com/technetwork/java/index.html](http://www.oracle.com/technetwork/java/index.html) and install it.

• **Method 2:**
  Run the JRE 6.0 setup in the IMC package as follows:
  a. On the subordinate server, launch the Web browser and enter [http://192.168.4.44:8080/imc](http://192.168.4.44:8080/imc) (192.168.4.44 is the IP address of the master server, and 8080 is the HTTP port number) in the address bar.
  b. On the login page, enter the username and password.
  c. Click **Login** to enter the **Home** tab.
  d. Select the **System** tab, and then click **Deploy Components**.
  e. Click **When fail to start Remote Installation Wizard, download and install JRE.**
  f. In the popup **jre.exe** file download window, click **Save** before running the file or directly click **Run**.

**IMPORTANT:**

• Make sure you have installed a 64-bit browser and 64-bit JRE on Windows Server 2003 R2 SP2 (64bit). Otherwise, IMC errors might occur.

• To use Firefox for accessing IMC on Linux, install JRE 6.0 or JDK first. For more information, see "FAQs."
Prerequisites for installing a separate database

You can install a separate database to store IMC data. In centralized deployment mode, the database software must be installed and running on the same server where IMC is located. In distributed deployment, the separate database can be located on a dedicated database server or another IMC server. Typically the data of all IMC servers in deployment mode is stored on the same database server.

To use a separate Oracle database, follow these guidelines:

- Install the Oracle client on mater and subordinate servers. The client version must match the database version.
- Configure the IP address of the database server as the network service name for master and subordinate servers.

To use a separate SQL database server, follow these guidelines:

- Install the SQL Server client on mater and subordinate servers. The client version must match the database version.
- HP recommends using the account LocalSystem for the SQL Server service on the database server, so that the database superuser used for installing IMC has 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 Installation Guide.
- Create a data file folder for saving data files on the database server.
- Verify the data file folder path on the operating system.

When IMC runs on Windows, you can verify the data file folder path as follows:

a. Select Start > Run.

The Run dialog box appears.

b. Enter cmd and click OK.

You enter the command line mode.

c. Log in to the remote database server by using the command:

```
osql -S192.168.2.24 -Usa -PiMC123
```

In the previous character string, 192.168.2.24 is the IP address of the database server, sa is the database user name, and iMC123 is the password.

d. Execute the following command on the database server:

```
CREATE DATABASE imc_test_db
ON
(NAME=N'PRMDATA01',
 FILENAME= N'E:\imcdata\imc_test_db01.mdf',
 SIZE=16MB,
 FILEGROWTH=20%)
go
```

In the command output, E:\imcdata is the path of the data file folder on the database server, the same as the data file location to use in IMC deployment, as shown in Figure 1.

e. Observe the execution result.

The test is successful when no error message appears when the execution is complete. You can configure IMC to use the data file location.
f. Delete the test data file `imc_test_db01.mdf` and log file `imc_test_db_log.LDF` from the database server.

When you configure IMC to use a remote SQL server database, follow these guidelines:

- Specify the folder that the database server uses to store IMC data by entering the path of the created data file folder in the **Data File Location** field, as shown in Figure 1.
- Make sure the folder path is not a Windows shortcut or Linux symlink. Then IMC checks whether or not the folder path exists and is accessible on the database server.
- When the path is invalid, IMC quits the deployment. To restart the deployment, first create the data file folder on the database server.

**Figure 1 Database Configuration Info window**

![Database Configuration Info window](image)

Restrictions of using the embedded database

The embedded database software, SQL Server 2008 SP2 Express, is shipped with the installation packages of IMC Standard and SNS editions. To use the embedded database on these IMC editions, follow these guidelines:

- The IMC server must use a Windows operating system on which no SQL server database has been installed.
- The number of nodes to be managed by IMC does not exceed 1000. Otherwise, install a separate database.

**IMC service logon accounts**

By default, the IMC system service **H3C iMC Server** is logged on and started using the **LocalSystem** account. To use another account for IMC service logon, you must grant the account read and write access to the IMC installation folder, and then start IMC by using the Intelligent Deployment Monitoring Agent.
Obtaining IMC installation and deployment methods

Installing IMC on Windows and Linux is similar. The following information discusses installing the IMC Platform and service components on Windows Server 2003.

The IMC software is available on the HP website.
4 Installing and deploying the IMC Platform

The following information describes the installation and recommended deployment schemes of the IMC Platform.

When you use only the IMC Platform to manage your network, HP recommends using centralized deployment to deploy all IMC subcomponents to the same server.

- To manage a large number of devices and use IMC Enterprise edition, use a separate database. For more information, see "Software requirements."
- To manage a small number of devices and use IMC Standard edition, use either the embedded IMC database or a separate database. For more information, see "Software requirements."
- IMC Standard edition supports both embedded and separate databases. HP recommends that you use a separate database. When the IMC Standard edition runs on Linux, it must use a separate database.
- When using the embedded database, make sure that SQL Server database is not installed on the master or subordinate servers.

To deploy the IMC subcomponents to the subordinate servers, see Table 8.

Table 8 IMC Platform subcomponents and deployment requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Subcomponents</th>
<th>Optional server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Management</td>
<td></td>
<td>Master server</td>
</tr>
<tr>
<td>Alarm Management</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>Data Analysis Manager</td>
<td></td>
<td>Master server</td>
</tr>
<tr>
<td>Data Analyzer</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>Guest Access Management</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>Performance Management</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>Network Asset Management</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>ACL Management</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>Intelligent Configuration Center</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>NE Management</td>
<td></td>
<td>Master server</td>
</tr>
<tr>
<td>Report Management</td>
<td></td>
<td>Master server</td>
</tr>
<tr>
<td>Security Control Center</td>
<td></td>
<td>Master server</td>
</tr>
<tr>
<td>Syslog Management</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>VLAN Management</td>
<td></td>
<td>Master server</td>
</tr>
<tr>
<td>User Selfservice Management</td>
<td></td>
<td>Master and subordinate servers</td>
</tr>
<tr>
<td>Virtual Network Management</td>
<td></td>
<td>Master server</td>
</tr>
</tbody>
</table>
Installing the IMC Platform

To install the IMC Platform:

1. Log in to the operating system as a user with administrator privileges.
2. Decompress the installation file.
3. Run the `install\install.bat` script in the downloaded installation package to install IMC. A window will appear, as shown in Figure 2, asking you to select a country/region, language, and installation type.

When you are using other Windows server operating systems or Linux, follow these guidelines:

- To install IMC in Windows Server 2003 or Windows Server 2003 R2, you must log in as an administrator.
- To install IMC in Windows Server 2008 or Windows Server 2008 R2, right-click the `install.bat` script and select Run as Administrator from the shortcut menu, or modify the User Account Control Settings and then restart the OS. After installing IMC, you can restore the related settings as needed.
- To modify the user account control settings, click Start > Control Panel > System and Security. Click Change User Account Control Settings in the Action Center. Set the Choose when to be notified about changes to your computer to Never notify in the User Account Control Settings window.
- To install IMC on Linux except Red Hat Linux 6, start the IMC installation wizard by running the `install.sh` script in the downloaded installation package as a root user.
- To install IMC on Red Hat Linux 6, copy all installation files from the IMC installation DVD to the local server and then run the `install.sh` script on the local server.
- When the installation file is obtained via FTP, you must first authorize the `install.sh` script by executing `chmod -R 775 install.sh` in the directory of the script.

![Figure 2 Select Locale (on Windows Server 2003)](image)

Typical installation

The following information describes typical and custom installation. Typical installation supports both the separate database and the embedded database.
**Typical installation with a separate database**

To complete a typical installation with a separate database:

1. In Figure 2, select the country or region and language, click **Typical**, and click **OK**.
   
   The window for checking installation parameters appears.

2. Configure the installation parameters to check before you can install and deploy IMC components. See Figure 3.

**Figure 3 Checking installation parameters**

![Checking installation parameters](image)

- **a.** Select the database type and instance name. Use the default instance or select **Other Instance** from the list to specify an instance name.

- **b.** Enter the database superuser name (**sa** by default), password, and listening port (**1433** by default).

   These parameters appear only when you install IMC on Windows.

   In distributed deployment, if more than one SQL Server or MySQL database is used, make sure you set the same listening port for them.

- **c.** Select a network service name or click ![add](image) to add a network service name.

   This parameter appears only when you install IMC on Linux to use an Oracle database. When a local database is used, you must configure a network service name for connecting to the local database address. For more information, see *Oracle 11g Installation and Configuration Guide* or *Oracle 11g R2 Installation and Configuration Guide*.

- **d.** Use the default installation location and database file location, or customize the installation location and database file location as needed.

- **e.** Configure the Web service port numbers (**8080** for **HTTP** and **8443** for **HTTPS** by default). You can also use other service port numbers that are not used by other services.

3. **Click **OK**.**

   The system starts to check the installation environment.

   When the installation environment fails the check, modify parameters according to the check results, and then proceed with the installation.

4. **Click **Continue** when you see a message reminding you of less than 2 GB free space for the installation environment.**
When the check is passed, the system directly installs and deploys all IMC Platform subcomponents.

**Typical installation with the embedded database**

To complete a typical installation with the embedded database:

1. In Figure 2, select the country or region and language, click **Typical**, and click **OK**.

   The window for checking installation environments appears and displays the check results, as shown in Figure 4.

**Figure 4 Checking installation environments**

```
Checking installation environments. Please wait...

Checking physical memory size... Passed
Checking database installation...
Database or database client is not installed on this computer. Checking prerequisites for embedded database...
  OS Version and Patch: Meet the requirements.
  .Net Framework 2.0 SP2: Installed
  Free space on system partition (more than 512MB): Passed
  Passed
  Current server allows the use of embedded database. Click "Continue" to continue.
```

The check items include:

- Whether or not the database listening port is used by another service.
- Whether or not the physical memory reaches 2 GB.
- Whether or not IMC supports the operating system version. For more information about the operating system versions supported by IMC, see "Software requirements."
- Whether or not .Net Framework 2.0 SP2 is installed.
- Whether or not the free space on the system disk reaches 512 MB.

2. Adjust the installation environments according to the check results.

3. When the installation environments check is passed, click **Continue**.

   The window for checking installation parameters appears, as shown in Figure 5.

**Figure 5 Checking installation parameters**

```
Checking installation parameters

<table>
<thead>
<tr>
<th>Installation Location:</th>
<th>[C:\Program Files\IMC]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data File Location:</td>
<td>[C:\Program Files\imcdata]</td>
</tr>
<tr>
<td>HTTP Port:</td>
<td>8080</td>
</tr>
<tr>
<td>HTTPS Port:</td>
<td>4443</td>
</tr>
</tbody>
</table>
```

21
4. Configure the installation parameters:
   
   a. Use the default installation location and data file location, or browse to select other locations as needed. Make sure the disk for IMC installation has at least 5 GB of free space, and the disk for storing data files has at least 30 GB of free space. Otherwise, IMC installation or Configure the Web service port numbers (8080 for HTTP and 8443 for HTTPS by default). You can also use other service port numbers that are not used by other services.

5. Click OK.

The system starts to install the embedded database to the same partition where the Windows folder is located, and install and deploy all IMC Platform subcomponents. When the installation is complete, you can log in to the database by using username sa and password iMC-Install2008.

Completing typical installation

After IMC installation and deployment is complete, the Batch deploy succeeded window appears, as shown in Figure 6.

Figure 6 Batch deploy succeeded

To start IMC immediately, select Start iMC Server now, and then click OK. The Intelligent Deployment Monitoring Agent window appears, as shown in Figure 7.

To start IMC later, click OK. When you want to start IMC, click Start iMC on the Monitor tab of the Intelligent Deployment Monitoring Agent.

Figure 7 Intelligent Deployment Monitoring Agent
The **Intelligent Deployment Monitoring Agent** window allows you to perform the following operations:

- Click the **Deploy** tab to view the deployed components. The **Deploy** tab shown in Figure 7 contains two data analyzer components, one in Deployed state and the other in Undeployed state, because the component can be deployed on multiple servers (one for each server).
- Click the **Process** tab to view the running process information.
- Click the **Monitor** tab to view the IMC startup information, as shown in Figure 8. When the startup is complete, the **Start iMC** button is grayed out.
- To disable IMC, click **Stop iMC**.
- You can select **Automatically start the services when the OS starts** when you want IMC to automatically start at the system startup.
- To install new components, click **Install**, as shown in Figure 8, or right-click the **Intelligent Deployment Monitoring Agent** icon on the Windows system tray, and then select **Install** from the shortcut menu. For more information, see "Installing and deploying IMC service components."

---

**Figure 8 Intelligent Deployment Monitoring Agent**

---

**Custom installation**

To complete a custom installation:

1. In Figure 2, select the country or region and language, click **Custom**, and then click **OK**.

   If the embedded database is used, the system directly checks the following installation environment items:
   - Whether or not the listening port used by the Intelligent Deployment Monitoring Agent and service is used by another service.
   - Whether or not the physical memory reaches 2 GB.
   - Whether or not a database is installed.
   - Whether or not the database can be normally connected.

   If a separate database is used, the window for checking database connectivity dialog box appears, as shown in Figure 9.
2. Enter parameters for checking the database connectivity:
   o Select the database type and instance name. Use the default instance or select Other Instance from the list to specify an instance name.
   o Enter the database superuser name (sa by default), password, and listening port number (1433 by default). You can also use another port number that is not used by another service. The parameters appear only when you install IMC on Windows.
   o Select a network service name or click ▶ to add a network service name.
      This parameter appears only when you are installing IMC on Linux that uses an Oracle database.
      When a local database is used, configure a network service name for connecting to the local database address.
      When a remote database is used, configure a network service name for connecting to the database server address.
      For more information about network service name configuration, see Oracle 11g Installation and Configuration Guide or Oracle 11g R2 Installation and Configuration Guide.
   o Select the database location.
      When you select local host, enter the superuser name and password.
      When you select other server, specify the server IP address and enter the superuser name and password for the specified database server.

3. Click OK.
   The system starts to check the database connectivity. After the installation environment check, the HP IMC Installation Wizard appears.

4. Click Continue when you see a message reminding you of less than 2 GB free space for the installation environment.
   When the check is passed, the Welcome to HP iMC Installation Wizard window appears, as shown in Figure 10.
5. Click Next.

The Agreement window appears, as shown in Figure 11.

Figure 11 Agreement

6. Read the license agreement and third party license, select Accept, and then click Next.

The Choose Target Folder window appears, as shown in Figure 12.
7. Select the components you want to install and specify the installation location.

By default, IMC is installed in `C:\Program Files\iMC` (or in `/opt/iMC` on Linux). You can enter a path or click **Browse** to select a path to install it in another folder.

⚠️ **CAUTION:**
- In the partition where you want to install the IMC software, at least 5 GB free space must be available.
- You must choose a local installation path.
- Linux does not support the IMC installation in a **symlink** path.

In the **Choose Target Folder** window, you can also view information about the components that you want to install. These components include Resource Manager, NE Management, Alarm Management, and Performance Management.

8. Click **Next**.

The **Deployment and Upgrade Options** window appears, as shown in Figure 13.
9. Select an option according to the option descriptions in the window and click **Next**.

The *Deploy or upgrade later* option is selected in this example. The **Installation Summary** window appears, as shown in Figure 14.

**Figure 14 Installation Summary**

The **Installation Summary** window provides the following information:
- Name, description, version, and disk space required by each component to be installed
- IMC installation location
- Total disk space required by the installation
- Free disk space of the partition where IMC is to be installed

10. Click **Install**.

The **Installing common components** window appears, as shown in Figure 15.
The wizard shows the process of component installation.

After the installation is complete, the **Installation Completed** window appears, as shown in **Figure 16**.

**Figure 16 Installation Completed**

In the **Installation Completed** window, you can perform the following tasks:

- When you install only the IMC Platform without any service component, select the **Open deployment monitoring agent** box and then click **Finish** to start deployment.
- When you continue to install other service components, decompress the installation file, select the **Install other iMC Components** box and then click **Finish**. For more information, see "Installing and deploying IMC service components."
- You can click **Finish** to close the window without selecting any of the two boxes.

To open the Intelligent Deployment Monitoring Agent on Windows, select **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent**.

To open the Intelligent Deployment Monitoring Agent on Linux, run the `dma.sh` script in `/deploy` of the IMC installation path.
Deploying the IMC Platform

This section describes the IMC deployment procedures in various modes.

Deploying IMC in centralized mode with a separate database

1. After installation, in the window shown in Figure 16, select **Open deployment monitoring agent** and then click **Finish**. The system automatically starts the Intelligent Deployment Monitoring Agent. For the first deployment, a **Batch deploy** window appears as shown in Figure 17.

   **Figure 17 Batch deploy**

2. You can also start the Intelligent Deployment Monitoring Agent by selecting **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent** (or running the **dma.sh** script in /deploy of the IMC installation path on Linux). Then select the **Deploy** tab, select **Batch Deploy** from the right-click menu of the target components to start batch deployment.

   In the **Batch deploy** window, the components to be deployed by default include:

   - Alarm Management
   - Data Analysis Manager
   - Data Analyzer
   - Intelligent Configuration Center
   - NE Management
   - Performance Management
   - Report Management
   - Resource Management
   - Security Control Center

   Optional components include:

   - ACL Management
   - Guest Access Manager
   - Network Asset Management
   - Syslog Management
3. You can also select the components to be deployed as needed, except that the Resource Management component is required. Click OK. The Database Configuration Info window appears, as shown in Figure 18.

Figure 18 Database Configuration Info

4. Enter the password for the superuser, which you used for installing the IMC database.

5. Select the location for saving data files.
   - When IMC uses a local database, it stores the data files in `C:\Program Files\imcdata` on windows or `/opt/imcdata` on Linux by default. You can also click Browse to customize the data file location.
   - When IMC uses a remote database, you must enter the path of the existing data file folder on the database server. Make sure the folder path is not a Windows shortcut or Linux symlink. Then IMC checks whether or not the folder path exists and is accessible on the database server. When the path is invalid, IMC quits the deployment. Then you must create the data file folder on the database server and restart the deployment.

   **NOTE:**
   When IMC uses a local database, you must select a writable, uncompressed disk drive. When you do not, an error can occur during IMC deployment. To change the compression setting of a disk drive:
   - Right-click the disk name and select Properties from the shortcut menu.
   - On the General tab of the disk properties window that appears, clear the selection of Compress drive to save disk space.
   - Click OK.

6. Select a path to save the data files and click Next. The Configure Web Service Port window appears, as shown in Figure 19.
7. The default port for HTTP access is 8080 and that for HTTPS access is 8443. You can change these port numbers as needed. Make sure that the Web service ports that you set here are not being used by another service.

8. Click **Deploy**.

   The **Deploying** window appears, as shown in Figure 20.

**Figure 20 Deploying IMC components**

After the deployment, the **Batch deploy succeeded** window appears, as shown in Figure 21.
9. In the **Batch deploy succeeded** window, select **Open readme file directory**, **Start iMC Server now**, or both.

   In this example, select **Start iMC Server now** and click **OK**.

   The system immediately starts the IMC service and opens the **Intelligent Deployment Monitoring Agent** window, as shown in Figure 22.

   In this window, select the **Deploy** tab to view information about the component deployment.

Figure 22 Information about component deployment

   The Data Analyzer can be deployed to multiple servers (once for each server). Therefore, after this component is deployed, another Data Analyzer with status **Undeployed** appears in the component list.

10. After the deployment is finished, follow these steps to start the IMC service:

   a. In the **Intelligent Deployment Monitoring Agent** window, select the **Monitor** tab, as shown in Figure 23.

   b. Click **Start iMC**.

   c. You can also select the **Automatically start the services when the OS starts** box to start IMC with the operating system.
d. To view the enabling and running status of each process, click the Process tab to enter the process management window.

Deploying IMC in centralized mode with the embedded database

Deploying IMC with an embedded database in centralized mode is applicable to small-sized networks because it can only manage a small number of devices.

The SQL Server 2008 R2 Express SP2 database is embedded in IMC Standard edition. For information about the installation procedures, see SQL Server 2008 R2 Installation and Configuration Guide.

Deploying the IMC Platform with an embedded database in centralized mode is similar to that with a separate database. However, when you deploy the IMC Platform with an embedded database in centralized mode:

1. Select the components to be deployed from the Batch deploy window, and click OK to enter the Database Configuration Info window, as shown in Figure 24.
2. Select **Install embedded database**. Otherwise, you cannot deploy the components.

3. Select the location for saving database files.
   By default, database files are stored in `C:\Program Files\imcdata`.
   When you do not want to use the default location, click **Browse** and select another local location.

4. Select a path to save the data files and click **Next**.
   The **Configure Web Service Port** window appears, as shown in Figure 19.

   The subsequent deployment procedure is the same as "Deploying IMC in centralized mode with a separate database."

   The SQL Server 2008 R2 Express database will be installed to the same partition where the Windows folder is located. When the installation is complete, you can log in to the database by using username **sa** and password **iMC-Install2008**.

---

**Deploying a single IMC component**

To deploy a single IMC component, use either of the following methods in the window, as shown in Figure 22.

- **Method 1:**
  Right-click the target component and then select **Deploy the Component** from the shortcut menu.

- **Method 2:**
  a. Select any target component and then select **Batch deploy** from the shortcut menu.
     The **Batch deploy** dialog box appears.
  b. Select the component and then click **OK**.

Some IMC components depend on others. When deploying such components, consider the dependencies between components. On the **Deploy** tab, select **Show Dependencies** from the right-click menu of a component to view the components in which the selected component depends. When the component does not depend on any components, **Show Dependencies** is grayed out.

The detailed deployment procedure for a single component is similar to the batch deployment.
5 Installing and deploying IMC service components

This following information describes the recommended IMC Platform plus service components deployment mode, how to install, and deploy the service components.

IMC common service components include:
- Applications Manager
- Connection Resource Manager
- EAD Security Policy
- IPsec VPN Manager
- MPLS VPN Manager
- Network Traffic Analyzer and User Behavior Auditor
- QoS Manager
- Remote Site Manager
- Service Operation Manager
- User Access Manager

The subcomponents and deployment requirements are listed in Table 9.

Table 9 IMC subcomponents and deployment requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Subcomponents</th>
<th>Optional server</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications Manager</td>
<td>Applications Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>Connection Resource</td>
<td>Connection Resource Manager</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td>Manager</td>
<td>EAD Security Policy</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EoC Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>EPON Manager</td>
<td>EPON Manager</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td>iNode Dissolvable Client</td>
<td>iNode Dissolvable Client</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>IPsec VPN Manager</td>
<td>IPsec VPN Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>MPLS VPN Manager</td>
<td>MPLS VPN Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>MPLS TE management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>L2VPN Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>Component</td>
<td>Subcomponents</td>
<td>Optional server</td>
<td>Remarks</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Traffic Analyzer</td>
<td>Network Traffic Analyzer Master server</td>
<td>Master server N/A</td>
<td>You must first deploy the data analyzer component.</td>
</tr>
<tr>
<td></td>
<td>Network Traffic Analyzer Server Master and subordinate servers</td>
<td>N/A</td>
<td>Set the database password (defaults to IMC5_uamead) and the UAM Server IP Address, which is the IP address of the network adapter providing services externally of the server where UAM is deployed.</td>
</tr>
<tr>
<td></td>
<td>Network Behavior Analyzer Master server</td>
<td>Master server N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Behavior Analyzer Server Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>QoS Manager</td>
<td>QoS Management Master server</td>
<td>Master server N/A</td>
<td></td>
</tr>
<tr>
<td>Remote Site Manager</td>
<td>Remote Site Manager Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Service Operation Manager</td>
<td>CMDB Management Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Desk Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Service Health Manager</td>
<td>Service Health Management Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NQA Collector Management Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>User Behavior Auditor</td>
<td>User Behavior Auditor Master server</td>
<td>Master server N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Behavior Auditor Server Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Behavior Analyzer Master server</td>
<td>Master server N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Behavior Analyzer Server Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>User Access Manager</td>
<td>User Access Management Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Portal Web Server and</td>
<td>Portal Web Server and Portal Proxy Master and subordinate servers</td>
<td>N/A</td>
<td>Set the Portal Server IP Address, which is the IP address of the network adapter providing services externally of the server where the Portal server component is deployed.</td>
</tr>
<tr>
<td>Portal Proxy</td>
<td>Portal Proxy Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Portal Server</td>
<td>Portal Server Master and subordinate servers</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Subcomponents</td>
<td>Optional server</td>
<td>Remarks</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td>Policy Server</td>
<td>Master and subordinate servers</td>
<td>Set the Policy Server IP Address, which is the IP address of the network adapter providing services externally of the server where the policy server component is deployed.</td>
<td></td>
</tr>
<tr>
<td>Policy Proxy Server</td>
<td>Master and subordinate servers</td>
<td>Set the Policy Proxy Server IP Address, which is the IP address of the network adapter providing services externally of the server where the policy proxy server component is deployed.</td>
<td></td>
</tr>
<tr>
<td>User SelfService</td>
<td>Master and subordinate servers</td>
<td>Set the User SelfService IP Address, which is the IP address of the network adapter providing services externally of the server where the user selfservice component is deployed.</td>
<td></td>
</tr>
<tr>
<td>Desktop Asset Manager</td>
<td>Master and subordinate servers</td>
<td>Set the database password (defaults to IMC5_uamead), and the DAM Server IP Address, which is the IP address of the network adapter providing services externally of the server where DAM is deployed.</td>
<td></td>
</tr>
<tr>
<td>Desktop Asset Manager Proxy Server</td>
<td>Master and subordinate servers</td>
<td>Set the DAM Proxy Server IP Address, which is the IP address of the network adapter providing services externally of the server where the DAM proxy server component is deployed.</td>
<td></td>
</tr>
<tr>
<td>Voice Service Manager</td>
<td>Voice Service Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>Wireless Service Manager</td>
<td>Wireless Service Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The installation and deployment procedures for the common service components are similar. The following information uses the installation of NTA as an example.

**Installing IMC Network Traffic Analyzer (NTA)**

1. In the **Installation Completed** window, as shown in Figure 16, select the **Install other iMC Components** box.
2. Click **Finish** to enter the **Choose folder** dialog box, as shown in Figure 25.
NOTE:
You can also install a new component with either of the following methods:

- Select Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent and click Install in the Monitor tab to begin installation, or
- In the system tray, right-click the Intelligent Deployment Monitoring Agent icon and select Install from the popup menu to install a new component.

3. In the Choose folder window, click Browse.
4. Select the install\components folder in the IMC NTA downloaded installation package.
5. Click OK.
   A window, as shown in Figure 26, displays to guide you through the IMC installation.

Figure 26 Welcome to HP IMC Installation Wizard

6. Click Next.
   The Agreement window appears, as shown in Figure 27.
7. Read the license agreement and third party license, and select **Accept**.

8. Click **Next**.

   The **Choose Target Folder** window appears, as shown in Figure 28.

**Figure 28 Choose Target Folder**

The **Choose Target Folder** window displays information about the NTA.

Some IMC components depend on other components to function. When the latter are not installed, the **Description** of a dependent component to be installed in the **Choose Target Folder** window might be **Do Not Install**. In this case, you can view which components that this component depends on by selecting **Show Dependent Influence** from the right-click menu in the component list.

In centralized deployment, the system specifies the installation location of the NTA as the installation location of the IMC Platform by default.

9. After confirmation, click **Next**.

   The **Deployment and Upgrade Options** window appears, as shown in Figure 29.
10. Select an option as needed. In this example, **Deploy or upgrade later** is selected.

11. Click **Next**.

   The **Installation Summary** window appears, as shown in Figure 30.

**Figure 30 Installation Summary**

12. After confirming the related installation information, click **Install**.

   The **Installing** window appears, as shown in Figure 31.
The wizard is installing the component. After the installation is finished, the **Installation Completed** window appears, as shown in Figure 32.

The following information describes the installation of the NTA only.

13. Select **Open deployment monitoring agent** in the **Installation Completed** window and click **Finish**.

To install other IMC common components, select **Install other iMC Components** in the **Installation Completed** window and click **Finish** to begin the installation. The installation procedure is similar to that of NTA.

In addition to the previous installation methods, you can also start a new component installation wizard with either of the following methods:

- **Method 1:**
  After installing and deploying IMC:
a. Select Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent (or run the dma.sh script in /deploy of the IMC installation path on Linux) to start the Intelligent Deployment Monitoring Agent.

b. Click Install in the Monitor tab to begin installation.

⚠️ CAUTION:

To install IMC in Windows Server 2008 or Windows Server 2008 R2, you must first modify the User Account Control Settings. After installing IMC, you can restore the related settings as needed.

c. Modify the User Account Control Settings, click Start > Control Panel > System and Security.
   Click Change User Account Control Settings in the Action Center, and the User Account Control Settings window appears.
   In the window, set the Choose when to be notified about changes to your computer to Never notify.

   Method 2:
   In the system tray, right-click the Intelligent Deployment Monitoring Agent icon and select Install from the popup menu to install a new component.
   The detailed installation procedure is the same as the previously described.

Deploying IMC Network Traffic Analyzer (NTA)

Before deploying service components, read service components and deployment requirements in Table 9.

HP recommends that you deploy NTA by:

1. Deploying the Network Traffic Analyzer component and the Network Behavior Analyzer component to the master server.
2. Deploying the Network Traffic Analyzer Server component and the Network Behavior Analyzer Server component to the subordinate server.

You can configure components to use their respective local or remote databases, which can be a remote database server or the database on another IMC server.

- Before deploying service components, deploy the basic IMC components and the components on which the service components depend. For more information about the deployment procedure, see "Deploying IMC in centralized mode with a separate database."
- See "Prerequisites" before deploying service components in distributed mode.
- Before installing a separate SQL Server or Oracle database, you must install the SQL Server or Oracle database client on the server where IMC is deployed.
- The MySQL database only supports using a separate database server when it is deployed as a separate database.

Deploying to a centralized server

This section describes how to deploy the IMC Network Traffic Analyzer and Network Behavior Analyzer to the master server.

1. After installation, in the window, as shown in Figure 32, select Open deployment monitoring agent and then click Finish.
The system automatically starts the Intelligent Deployment Monitoring Agent. A Batch deploy window appears at the same time, as shown in Figure 33.

You can also start the Intelligent Deployment Monitoring Agent by selecting:

- **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent** (or running the dma.sh script in /deploy of the IMC installation path on Linux).
- Then the Deploy tab, selecting Batch Deploy from the right-click menu of the target components to start batch deployment.

**Figure 33 Batch deploy**

2. In the **Batch deploy** window, select the components to deploy.
   In this example, select **Network Traffic Analyzer** and **Network Behavior Analyzer**.

3. Click **OK** to start deploying the components.
   After the deployment is complete, the **Batch deploy result** dialog box prompting **Batch deploy succeeded** appears.

4. Click **OK**.

5. On the Intelligent Deployment Monitoring Agent that appears, select the **Monitor** tab, and click **Start iMC** to start IMC.
   After IMC is normally started, you can perform deployments on the subordinate servers.

**Deploying to subordinate servers**

The following information describes the deployment of IMC NTA to separate subordinate servers.

Before deploying IMC NTA, install the Intelligent Deployment Monitoring Agent on the subordinate servers.

IMC allows you to launch the remote installation wizard through the IMC installation DVD (recommended) or the IE browser. When IMC runs on Linux, you must start the remote installation wizard through the IMC installation DVD.

**Starting the remote installation wizard through the IMC installation DVD**

1. On the subordinate servers, run the **installslaves.bat** script in the install directory of the IMC downloaded installation package.
The **Address of Master** window appears, as shown in Figure 34.

To start the remote installation wizard of the Intelligent Deployment Monitoring Agent on Linux:

a. Run the `installslave.sh` script in the install directory of the IMC downloaded installation package.

b. When the installation file is obtained via FTP, you must first authorize the `installslave.sh` script by executing `chmod -R 775 install.sh` in the directory of the script.

Figure 34 Address of Master

2. Type the IP address of the master server, and click **OK**.

The **Checking Database Connectivity** window appears, as shown in Figure 35.

Figure 35 Checking Database Connectivity

3. Enter parameters for checking the database connectivity in the dialog box:
   - Select the database type and instance name. Use the default instance or select **Other Instance** from the list to specify an instance name.
   - Enter the database superuser name (**sa** by default), password, and listening port number (**1433** by default). The parameters appear only when you install IMC on Windows.
   - In distributed deployment, if more than one SQL Server or MySQL database is used, make sure you set the same listening port for them.
   - Select a network service name or click ![Network Service Name](image) to add a network service name. This parameter appears only when you install IMC on Linux to use an Oracle database. When a local database is used, configure a network service name for connecting to the local database address. When a remote database is used, configure a network service name for connecting to the database server address.
For more information, see Oracle 11g Installation and Configuration Guide and Oracle 11g R2 Installation and Configuration Guide.

- When using the database on the subordinate server, select **local host** for the database location, and enter the superuser name (**sa** by default) and password, as shown in Figure 35.
- When using a remote database server, select **other server** for the database location, specify the server IP address, and enter the superuser name (**sa** by default) and password of the corresponding database, as shown in Figure 36.

**Figure 36 Checking Database Connectivity**

4. Click **OK** to start checking the database connectivity.
   After the installation environment check is passed, the IMC Installation Wizard appears.

5. Input the correct master server IP address, and click **OK**.

6. The **Choose Target Folder for Deployment** window of the **HP iMC Remote Installation Wizard** appears, as shown in Figure 39, which means that you have successfully started the remote installation wizard.

When you have deployed other components before deploying the current component, the **Database Configuration Info** window, as shown in Figure 43, does not appear when you deploy the current component if:

- The password for the user **sa** is not modified
- The available space of the disk saving the data file exceeds 1 GB

**Starting the remote installation wizard through IE**

1. On a subordinate server, launch the Web browser and enter **http://192.168.4.44:8080/imc** in the address bar.
   192.168.4.44 is the IP address of the master server and 8080 is the HTTP port number.
   The IMC login page appears.
2. Enter the username and password, and then click **Login**.
   The **Home** tab appears.
   192.168.4.44 is the IP address of the master server, and 8080 is the HTTP port for Web services.
   The username and password of the super user for the system are both **admin**.
3. Select the **System** tab to enter the **System Management** page.
4. Click Component Deploy.

5. On the Installed Components page, click Start deploy.
   A dialog box appears, as shown in Figure 37.

**Figure 37 Launch the Intelligent Deployment Monitoring Agent**

6. Click OK.
   The **Downloading application** dialog box appears, as shown in Figure 38, indicating that Java file (jre.exe) is being downloaded.
   When JRE6.0 has been installed on the subordinate servers, the system starts the remote installation wizard when you click OK.

**Figure 38 Downloading application**

After the Java file is downloaded and installed, the **Choose Target Folder for Deployment** dialog box appears, as shown in Figure 39.

**Installing the Intelligent Deployment Monitoring Agent**

After successfully starting the remote installation wizard, install the deployment monitoring agent.
Figure 39 Choose Target Folder for Deployment

As shown in Figure 39, the default deployment location is C:\Program Files\IMC (or in /opt/IMC on Linux).

When you want to deploy IMC in another location, you can either type a path or click Browse to select one path.

1. After selecting a deployment location, click Install to start file downloading.
   After the files are downloaded, the Installation Completed dialog box appears, as shown in Figure 40.

Figure 40 Installation Completed

2. Click Finish.

Deploying Network Traffic Analyzer

1. On the subordinate servers, select Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent (or run the dma.sh script in /deploy of the IMC installation path on Linux).

2. In the displayed window, select the Deploy tab, as shown in Figure 41.
3. Select the Network Behavior Analyzer Server component that has not been deployed, right-click it, and select **Batch Deploy** from the shortcut menu.

The **Batch deploy** window appears, as shown in **Figure 42**.

![Figure 42 Batch deploy](image)

4. In the **Batch deploy** window, select **Network Behavior Analyzer Server** and **Network Traffic Analyzer Server**, and click **OK**.

The system downloads the files. After downloading is complete, the **Database Configuration Info** window appears, as shown in **Figure 43**.
5. Enter the password for the user sa for the current database, which is the superuser name for installing IMC, and select a data file location. By default, IMC saves the data file in C:\Program Files\IMCdata.

6. To modify the data file location, click Browse to select a file location.

7. When you configure IMC to use a remote SQL server database, specify the folder that the database server uses to store IMC data by entering the path of the folder in the Data File Location field, as shown in Figure 43.

   Make sure the folder path is not a Windows shortcut or Linux symlink. Then IMC checks whether or not the folder path exists and is accessible on the database server. When the path is invalid, IMC quits the deployment.

   To restart the deployment, first create the data file folder on the database server.

8. Click Deploy to start the deployment.

   After the deployment is finished, the Batch deploy result dialog box prompting Batch deploy succeeded appears.

9. Click OK.

10. After successfully finishing the deployment, select the Deploy tab in the Intelligent Deployment Monitoring Agent, as shown in Figure 44.
11. On the master server, select Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent (or run the dma.sh script in /deploy of the IMC installation path on Linux).

12. In the displayed window, select the Monitor tab and click Start IMC.
A dialog box appears asking you when you want to start the IMC service.

13. Click OK.
After all processes start, IMC is ready for use.
6 Installing plug-ins

To support some IMC functions, you must install necessary plug-ins.

Installing DHCP plug-ins

A DHCP server installed with a DHCP plug-in lets IMC obtain the names of terminals, such as servers, PCs, and printers, from the DHCP server. To accomplish this task, ensure that:
- At least one DHCP server exists in the network.
- All DHCP servers in the network have DHCP plug-ins installed.

To view the names obtained from the DHCP server, select Terminal Access > Unauthorized Access List or History Access Log List from the navigation tree.

The following information describes how to install DHCP plug-ins on MS DHCP and Linux DHCP servers respectively.

On the MS DHCP server

1. Modify the file qvdm.conf, so that the IMC supports getting the terminal name or terminal domain name through the MS DHCP server.
   a. Enter the \server\conf\ directory in the IMC installation path, open the file qvdm.conf in Wordpad, and add the following line to the file:
      l2topoPCNameDhcpSwitch=1
   b. Save and exit the file.
   c. Restart IMC in the Intelligent Deployment Monitoring Agent.
2. Install the IMC DHCP plug-in on the MS DHCP server.
   The DHCP plug-in installer dhcp-plug-windows.zip is saved in the \windows\tools\ directory of the IMC installer.
   a. Copy the plug-in installer to the MS DHCP server.
   b. Decompress the installer.
   c. Use Wordpad to open the imf.cfg file in the \server\imf\server\conf directory of the dhcp-plug-windows folder.
   d. Modify the IMGAddress into the master server IP address and IMGPort (which is 8800 by default) to the IMG port number.
   e. Save and exit the file.
3. Run the install.bat script in the dhcp-plug-windows folder.
   After the installation, a new service IMC DHCP Plug is added to the system services.
4. Start the IMC DHCP plug service.
   a. Click Start, and select Administrative Tools > Component Services to open the Component Services window.
   b. Select Services (Local) from the navigation tree.
c. Right-click the **IMC DHCP Plug** service on the **Services (Local)** list and then select **Start** to start the IMC DHCP plug service.

To uninstall a DHCP plug-in, run the file **uninstall.bat** in the **dhcp-plug-windows** directory.

⚠️ **CAUTION:**

Do not remove the directory which the plug-in installer **dhcp-plug-windows.zip** is extracted to. Otherwise, the DHCP plug-in cannot be uninstalled completely.

---

### On the Linux DHCP server

1. Modify the file **qvdm.conf**, so that IMC supports getting the terminal DNS name or terminal name through the Linux DHCP server.
   a. Use the VI editor to open the **qvdm.conf** file in the **/server/conf** directory of the IMC installation path:
      ```
      vi qvdm.conf
      ```
   b. Add the following line to the file:
      ```
      l2topoPCNameDhcpSwitch=1
      ```
   c. Save and exit the file, and restart IMC in the Intelligent Deployment Monitoring Agent.

2. Install the IMC DHCP plug-in on the Linux DHCP server.
   The DHCP plug-in installer **dhcp-plug-linux.zip** is saved in the tools directory of the IMC Linux installer.
   a. Copy the plug-in installer to the Linux DHCP server.
   b. Decompress the installer.
   c. Use the VI editor to open the **imf.cfg** file in the **/server/imf/server/conf/** directory of the **dhcp-plug-linux** folder.
      ```
      vi imf.cfg
      ```
   d. Modify the IMGAddress into the IMC server IP address, and modify the IMGPort (which is 8800 by default) to the IMG port number that you set when installing IMC.
   e. Save and exit the file.

3. Check whether the path of the DHCP server IP allocation information file, **dhcpd.leases**, is correct.
   a. Enter the **/var/lib/dhcp** directory of the Linux operating system, and check whether the **dhcpd.leases** file exists.
   b. When the file does not exist, enter the **server/conf/** directory of the **dhcp-plug-linux** folder, use the VI editor to open the **qvdm.conf** file, and add the following line to the file to specify the path of the **dhcpd.leases** file.
      ```
      DhcpPlugIpAllocPath=<Current path>/dhcpd.leases
      ```
   c. Save and exit the file.

4. Execute the **install.sh** script in the **dhcp-plug-linux** folder.

After the installation is complete, the **dhcp-plug** service is added to the system services, and has been automatically started.

You can use the **server dhcp-plug stop** command to stop the service or use the **server dhcp-plug start** command to start the service.

To uninstall a DHCP plug-in, run the **uninstall.sh** script in the **dhcp-plug-linux** directory.
Installing VNM agent plug-ins

Virtual Network Management (VNM) is a module on the IMC Platform to manage virtual networks. It must work with a VNM Windows or Linux agent for virtual network management.

Installing a VNM Windows agent

When Microsoft Hyper-V servers exist in the network, install VNM Windows agents for IMC to manage the Hyper-V servers.

A VNM Windows agent must be installed on one Windows server. When the Microsoft Hyper-V servers are managed by Microsoft VMM servers, HP recommends that you install VNM Windows agents on the Microsoft VMM server. A VNM Windows agent can work for up to 50 Hyper-V servers. When more than 50 Hyper-V servers exist in the network, install more VNM Windows agents.

CAUTION:
VNM Windows agents can only be installed on Windows servers that can access all Hyper-V servers. A Windows server can be installed with only one VNM Windows agent.

A VNM Windows agent is dependent on NET Framework 2.0, NET Framework 2.1, NET Framework 3.0, and PowerShell 2.0. Before you install a VNM Windows agent, make sure that all the software applications are installed. For the Windows Server 2008 R2 system, they are installed in by default; for other Windows operating systems, go to the Microsoft official website to download and install them.

1. The installation file vnm-plug-windows.zip of a VNM Windows agent is stored in tools folder of the IMC installation package. Decompress the file and copy the file to any directory of the server where the VNM Windows agent is to be installed.
2. Run Register.bat in the vnm-plug-windows folder. When all the related software applications are installed, the installation process is complete. Otherwise, the system prompts you to install the required software and quit the installation process. In this case, install the required software and then start the installation process again.

CAUTION:
Do not remove the directory to which the plug-in installer dhcp-plug-windows.zip is extracted. Otherwise, the DHCP plug-in cannot be uninstalled completely.

3. Do not delete the vnm-plug-windows folder or the files in the folder after installation. It becomes the service registration path.
4. Use Wordpad to open the imf.cfg file in the vnm-plug-windows/serverimf/server/conf directory. Modify IMGAddress as the IP address of the master IMC server and IMGPort as the MBP port number (8800 by default).
5. Save your settings and quit.
6. Start the IMC VNM plug service.
   a. Click Start, and then select Administrative Tools > Component Services to open the Component Services window.
   b. Select Services (Local) from the navigation tree, right-click iMC VNM Agent on the Services (Local) list, and select Start to start the VNM agent service.

To uninstall a VNM agent plug-in, run the file UnRegister.bat in the vnm-plug-windows directory.
Installing a VNM Linux agent

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

VNM Linux agents can run on 32-bit or 64-bit Red Hat 6.0 or later versions.

A VNM Linux agent plug-in contains an SSH key deployment tool “ssh-key-tool” and an agent installation tool. Linux uses SSH key pairs for authentication. The communication between a KVM server and a VNM Linux agent or another KVM server is based on SSH key trust. Before you install a VNM Linux agent, establish SSH key trust among KVM servers and between each KVM server and the agent.

Introduction to the SSH key deployment tool

Use this tool to establish SSH key trust relationships, including global SSH key trust establishment, KVM trust adding, and SSH key trust maintenance.

- Establishing global SSH key trust relationships
  The first time you install a KVM Linux agent, establish the global trust relationships among KVM servers and between each KVM server and the agent, see Figure 45.

Figure 45 Global trust relationships

- Adding SSH key trust relationships for new KVM servers
  After the KVM Linux agent is installed, you can add SSH key trust relationships for new KVM servers that are added to the network, see Figure 46.
Figure 46 KVM trust adding

![KVM trust adding diagram]

- Maintaining SSH key trust relationships
  When multiple KVM Linux agents are installed, you might need to shut down some of the agents or change their management scopes. Use SSH key deployment tool to maintain the trust relationships among the KVM servers and between a KVM server and the agent, see Figure 47.

Figure 47 Trust relationship maintenance

![Trust relationship maintenance diagram]

Installation prerequisites

The VNM Linux agent is a 32-bit program and applies only to Red Hat. To install the VNM Linux agent on 64-bit Red Hat, first install the following 32-bit program compatibility packages:

- Library for getting and setting POSIX.1e capabilities (compat-libcap1-1.10-1.i686.rpm)
- Linux-native asynchronous I/O access library (libaio-0.3.107-10.el6(i686))
- GCC version 4.4 shared support library (libgcc-4.4.5-6.el6(i686))
- GUN Standard C++ Library (libstdc++-4.4.5-6. el6 (i686))

1. Insert the installation disk of Red Hat Linux 6.0 or above to the CD-ROM drive.
2. Enter the **System > Administration > Add/Remove Software** window.
3. Select **All Packages** on the left, and then select and install the packages mentioned above in the software package list on the right.

**Installation and configuration procedure**

1. Establish global SSH key trust relationships with the SSH key deployment tool:
   a. Enter the **tools** directory on the IMC installation disk, copy file **vnm-plug-linux.zip** to a local disk drive, and decompress the file.
   b. Run the **install.sh** script in the decompressed file folder and then enter 1 when you see the following menu:

   ```
   [root@daemon8930 vnm-plug-linux]# ./install.sh
   [1] Deploy SSH Key for KVM.
   [2] Install the vnm linux agent.
   Please enter your choice(1|2|3):
   ```
   c. Enter 1 when you see the SSH key deploy type menu:

   ```
   Please choose the ssh key deploy type:
   [2] Deploy SSH Key for new added KVM.
   Please enter your choice(1|2|3):
   ```
   d. Enter y when you see the following message:

   ```
   Please add the target KVM to the ssh-key-tool/conf/host.txt(y/n):
   ```
   e. Enter the username and the password of the KVM server in the following format.

   ```
   ip:10.153.146.12 user:root passwd:imcimc
   ```

   In the previous character string, **root** and **imcimc** are the username and password of the KVM server, respectively. Edit these fields and add more commands according to the KVM server settings.
   f. Save the **host.txt** file with the :wq command.

   An execution result message appears.

2. Install the VNM Linux agent:
   a. On the VNM Linux agent installation interface, enter 2.

   ```
   Deploy SSH Key for KVM.
   Install the vnm linux agent.
   Exit the install program.
   Please enter your choice(1|2|3):
   ```
   b. Enter the IP address of the master server. The default setting is **localhost**.

   ```
   Please enter the iMC Master Server IP Address(Default:localhost):
   ```
   c. Check whether or not the installation is successful by entering **ps -ef | grep imcvnmagent**.

   When the agent is successfully installed, you can see the **imcvnmagent** process is running.

3. Add SSH key trust for new KVM servers:
   Perform this step when new KVM servers connect to the network, so they can establish SSH key trust relationships with the agent, with every existing KVM server, and among themselves.
   a. Run the **install.sh** script in the VNM Linux agent installation file folder and then enter 1 when you see the following menu:

   ```
   [root@daemon8930 vnm-plug-linux]# ./install.sh
   ```
[1] Deploy SSH Key for KVM.
[2] Install the vnm linux agent.

Please enter your choice(1|2|3):

b. Enter 2 when you see the SSH key deploy type menu:

Please choose the ssh key deploy type:
[2] Deploy SSH Key for new added KVM.

Please enter your choice(1|2|3):

c. Enter y when you see the following message:

Please enter the existed KVM to the ssh-key-tool/conf/host.txt(y/n):

d. Enter the username and the password of each new KVM server in the following format.

```
ip:10.153.146.12 user:root passwd:imcimc
```

In the previous character string, root and imcimc are the username and password of the KVM server, respectively. Edit these fields and add more commands according to the KVM server settings.

e. Save the new_host.txt file with the :wq command.

The SSH key trust relationships are successfully deployed for the new KVM server.

f. Restart the vnm-plug service in the system services.

4. Maintain SSH key trust relationships:

a. Run the install.sh script in the VNM Linux agent installation file folder and then enter 1 when you see the following menu:

```
[root@daemon8930 vnm-plug-linux]# ./install.sh
[1] Deploy SSH Key for KVM.
[2] Install the vnm linux agent.
Please enter your choice(1|2|3):
```

b. Enter 3 when you see the SSH key deploy type menu:

Please choose the ssh key deploy type:
[2] Deploy SSH Key for new added KVM.

Please enter your choice(1|2|3):

c. Enter y when you see the following message:

Please enter the existed KVM to the ssh-key-tool/conf/host.txt(y/n):

d. Enter the username and the password of the KVM server to be modified in the following format.

```
ip:10.153.146.12 user:root passwd:imcimc
```

In the previous character string, root and imcimc are the username and password of the KVM server, respectively. Edit these fields according to the KVM server settings.

e. Save the new_host.txt file with the :wq command.

f. Restart the vnm-plug service in the system services.
Installing Android clients

Mobile clients (such as smart phones) can access IMC resources to manage and monitor IMC. This edition of IMC supports the access of mobile devices running an Android operating system.

A mobile device must meet the following requirements before it can access IMC:

- The device is installed with the operating system of Android 2.1 update 1 or a later version.
- The screen resolution is HVGA (480*320) or WVGA (800*480).
- The mobile device can communicate with the IMC server (through wireless connection, for example).

To install an Android client:

1. Access the website \texttt{http://imc-addr:port/imc/noAuth/imc.apk} by using the embedded browser of the mobile device to automatically download the client installation program.
   a. imc-addr is the IP address of the IMC server, and port is the HTTP port number (8080 by default) set when IMC was deployed for the first time.

2. Install the program as prompted.
   When the message \texttt{Programs from unknown sources are not allowed to install} appears during installation, locate to Settings > Applications, and then select Unknown source.

To log in to IMC:

1. Open the client program.
2. Enter the IMC server address, login name, and password.
   The IMC server address is in the format of \texttt{http://imc-addr:port}, where imc-addr is the IP address of the IMC server and port is the HTTP port number (8080 by default). Do not add /imc to the end of the address. To use a secure connection, enter the address in the format of \texttt{https://imc-addr:port} (the port number defaults to 8443). When HTTPS does not use the default port number when IMC was deployed for the first time, enter the specified port number.
   The login name must be an existing login name, which has the privilege to access iMC Platform > Resource Manager > Mobile Client Access in IMC.
3. Select Save password or Auto Login as needed.
   When you select Save password, you do not need to enter the password for the next logins. When you select Auto Login, you do no need to enter the login name and password for the next logins.
4. Click Login to log in to the IMC server.

You can use the Android client to implement the following functions:

- View information about faulty devices and interfaces, and query specific devices.
- View device alarms.
- Inform real-time alarms.
- Test device reachability by using ping or traceroute.
- View custom views and device views.
- Use an Android browser to access IMC to perform configuration and management operations.
- Play IMC videos.
NOTE:
When RADIUS authentication or LDAP authentication is used or when you change the login password, you must first log in to the IMC from a PC successfully before you can use a mobile client to log in to IMC.

Installing LLDP agent plug-ins

When the VNM component is deployed, you must install an LLDP agent for topology calculation.

An LLDP agent contains the following packages: lldp-agent-redhat.zip, lldp-agent-ubuntu.zip, and lldp-agent-windows.zip. The first two packages are installed on a KVM server and the last package is installed on a Microsoft Hyper-V server. The installation procedure for lldp-agent-redhat is similar to that for lldp-agent-ubuntu, and the following sections describe the installation procedure for lldp-agent-redhat.

Before the LLDP agent installation, copy the three packages to the target server and decompress the packages. If a Windows server is used, copy the lldp-agent-windows.zip file to a non-system disk.

IMPORTANT:
Do not delete the folder where the decompressed installation packages reside after completing the LLDP agent installation.

Installing an LLDP Linux agent

LLDP Linux agent plug-ins apply only to 64-bit Linux, including Redhat 5.5, Ubuntu 11.0, and their later versions.

To install and configure an LLDP Linux agent:
1. Set executable permission to the install.sh script and run the script in the LLDP Linux agent installation file folder.
   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 file folder.
   LLDP agent plug-ins support either LLDP or CDP, but not both at the same time. By default, the plug-ins support LLDP. To enable an LLDP agent to support CDP:
   a. Open the lldpagent.conf file in the conf directory.
      vi lldpagent.conf
   b. Delete the pound sign (#) from the string #Agent=CDP.
      You can set the interval at which LLDP or CDP packets are sent. The default setting is 300 seconds.
      To change the setting, delete the pound sign (#) from the string #INTERVAL=300 and then change the value.
3. Restart the lldp-agent service.
   service lldp-agent restart

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 file folder.
   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 file folder.

LLDP agent plug-ins support either LLDP or CDP, but not both at the same time. By default, the plug-ins support LLDP.

To enable an LLDP agent to support CDP:
   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`.
   You can set the interval at which LLDP or CDP packets are sent. The default setting is 300 seconds.
   To change the setting, delete the pound sign (#) from the string `#INTERVAL=300` and then change the value.
   c. Restart the `lldp-agent` service.
IMC does not provide separate client software for access. HP recommends that you access the IMC system using the following Web browsers:

- Internet Explorer 8.0 or later
- Firefox 3.6 or later

Access methods

To log in to IMC:

1. Enter the IMC login page using one of the following methods:
   
   Through HTTP:
      `192.168.4.44` is the IP address of the master server, and `8080` is the HTTP port set the first time the IMC platform subcomponents were deployed.
   b. The IMC login page appears. You can enable the verification code feature on the IMC login page. For more information, see `IMC Getting Started Guide`.
   
   Through HTTPS
   a. Enter `https://192.168.4.44:8443/imc` in the address bar of your browser and press Enter.  
      `192.168.4.44` is the IP address of the master server, and `8443` is the HTTPS port set the first time the IMC platform subcomponents were deployed.
   b. A security certificate message appears. For more information, see `IMC Getting Started Guide`.
   c. Confirm the message and then the IMC login page appears.

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

   By default, the IMC superuser name and password are `admin`. To enhance security, change the superuser password after login.

   o When the UAM user self-service component is deployed, access the IMC self-service center by entering either of the following addresses in the address bar of the browser:
     
     http://192.168.4.66:8080/
     
     http://192.168.4.66:8080/selfservice
     
     `192.168.4.66` is the IP address of the server where the UAM user self-service is deployed and `8080` is the HTTP port number set the first time the IMC platform subcomponents were deployed.
     
   o When the SOM service desk is deployed, access the service desk by entering `http://192.168.4.22:8080/servicedesk` in the address bar of the browser.
     
     `192.168.4.22` is the IP address of the server where the SOM service desk is deployed and `8080` is the HTTP port number set the first time the IMC platform subcomponents were deployed.

If you cannot access IMC using the Web browsers, check your hardware and browser configuration, as shown in Table 10.
Table 10 Hardware and browser requirements

<table>
<thead>
<tr>
<th>OS</th>
<th>Hardware</th>
<th>Browser version</th>
<th>Browser setting requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>• CPU: 2.0 GHz or higher</td>
<td>IE 8.0 or later</td>
<td>• Turn off the pop-up blocker in Internet Explorer.</td>
</tr>
<tr>
<td></td>
<td>• Memory: 1 GB or higher</td>
<td>Firefox 3.6 or later</td>
<td>• Enable the Cookies in Internet Explorer.</td>
</tr>
<tr>
<td></td>
<td>• Hard Disk: 20 GB or higher</td>
<td></td>
<td>• Add the IMC site to the trusted sites.</td>
</tr>
<tr>
<td></td>
<td>• CD-ROM: 48 X or higher</td>
<td></td>
<td>• Make sure the Screen Resolution is 1024x768 or higher.</td>
</tr>
<tr>
<td></td>
<td>• Network Adapter: 100 Mbps or higher</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sound card: Required.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Displaying a user agreement

You can display a user agreement on the IMC login page to inform 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, access the \client\conf directory (/client/conf on Linux) in the IMC installation path.
2. Open the commonCfg.properties file in WordPad or vi.
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.
6. Save the terms.html file to the \client\web\apps\imc directory (/client/web/apps/imc on Linux) in the IMC installation path.

Re-enter the IMC login page. A User agreement link appears under the username and password area. Operators can click the link to view terms of the user agreement. The Login button is grayed out unless I accept the terms in the user agreement is selected.
8 Installing RSM

Remote Site Manager (RSM) is a separate IMC service component that enables administrators on the IMC primary site to remotely manage and monitor branch networks, even when they are protected by firewalls or NAT devices. With RSM, administrators can manage resources, reports, and ACLs on branch networks.

Figure 48 RSM application scenario

As shown in Figure 48, the headquarters communicates with three branch networks via the Internet. IMC is deployed on the headquarters site, but cannot directly manage the branch networks that are protected by firewalls and NAT devices. Install RSM on the branch networks to enable IMC to manage them as remote sites.

These terms are used in the following information:

- **IMC primary site**—Master server in the IMC server cluster located at the headquarters.
- **Remote site**—Branch server on which RSM is installed.

RSM components

RSM uses a separate installation program, which is similar to IMC and offers the following components:

- Resource Management
- Alarm Management
- Intelligent Configuration Center
- Report Management
- NE Management
- Performance Management
- ACL Management
- Network Management
- Security Control Center
- VLAN Management
You can select and install components as needed. RSM has the same hardware and software requirements as the IMC Platform, for more information, see “Preparing for installation.”

Installation prerequisites

RSM installation is the same as IMC installation in the following aspects:

- Supporting remote databases
- Offering typical and custom installation modes
- Upgrade, deploy, and undeploy methods
- Dbman operations

Different from IMC, RSM does not support distributed deployment and cannot use the embedded database.

Before RSM installation, make sure the version of IMC is compatible with the RSM version. For more information, see “Upgrading RSM.”

Installation procedure

To install RSM on a remote site running Windows Server 2003:

1. Log in to Windows as a user with administrator privileges.
2. Insert the RSM installation disk in the DVD-ROM drive.
3. Run the `install.bat` script in the downloaded installation package to install RSM.
   
   A window appears, as shown in Figure 49, asking you to select a country/region, language, and installation type.

4. Select the Country/Region where you are located and Language, select Typical or Custom, as needed, and then click OK.

To start the installation wizard on Linux, run the `install.sh` script in the downloaded installation package as a root user.

The following information describes typical and custom installation.
Typical installation

Typical installation quickly installs all components and does not support remote databases.

To complete a typical installation:

1. **In Figure 49, select Typical, and then click OK.**
   
The **Agent installation options** window appears, as shown in Figure 50.

   **Figure 50 RSM installation options**

   ![RSM installation options](image)

2. **Configure the installation options:**
   
   a. **Enter the server URL of the IMC primary site in the format of** `http://server IP address:8080`.
   b. **Enter the username and password of the admin operator.**

   **3. Click OK.**

      When the installer can normally connect to the IMC primary site, the following window appears, as shown in Figure 51.

   **Figure 51 The number of devices managed window**

   ![The number of devices managed](image)

   **4. Enter the number of devices to be managed.**

      The number cannot exceed the maximum value displayed on the window. The upper limit is calculated by subtracting all nodes managed by the IMC primary site and those already assigned to other remote sites from the total manageable nodes permitted by the licenses.

   **5. Click OK.**

      The installer starts to check the installation prerequisites.

      - When the installation prerequisites cannot pass the check, modify parameters according to the check results, and then run the installation file again.
      - When the check is passed, the following window appears, as shown in Figure 52.
6. Configure the installation parameters to check before you can install and deploy RSM.
   - Select a database type, and then use the default instance or select Other Instance to specify an instance name in the popup Instance Name window.
   - Enter the database superuser name (sa by default), password, and listening port (1433 by default).
   - Use the default installation location and database file location, or customize the installation location and database file location as needed.
   - Set the Web service port numbers (8080 for HTTP and 8443 for HTTPS by default).

**NOTE:**

When you install IMC on Linux that uses an Oracle database, select a network service name or click to add a network service name. When a local database is used, you must configure a network service name for connecting to the local database address. For more information, see Oracle 11g Installation and Configuration Guide or Oracle 11g R2 Installation and Configuration Guide.

7. Click OK.

The installer tests the database connectivity. When the connectivity is normal, the installer directly installs and deploys all RSM components.
When the installation and deployment procedures are complete, the **Intelligent Deployment Monitoring Agent** window appears, as shown in Figure 54.

The **Intelligent Deployment Monitoring Agent** window contains the following tabs:

- **Monitor**—Allows you to start or stop IMC, and to configure IMC as a startup item of the operating system by selecting *Automatically start the services when the OS starts*. See Figure 55.
- **Process**—Displays running status of the components.
- **Deploy**—Displays versions, deployment status, and deployment locations of the RSM components.
- **Environment**—Displays database information and provides the Dbman tool. For more information about Dbman, see "Security and backup."
Custom installation

Custom installation allows you to select components as needed and supports remote databases.

To complete a custom installation:

1. In Figure 49, select Custom and then click OK.

   The Agent installation options window appears, as shown in Figure 56.

2. Configure the installation options:
   a. Enter the server URL of the IMC primary site in the format of http://server IP address:8080.
   b. Enter the username and password of the admin user.

3. Click OK.

   When the installer can normally connect to the IMC primary site, the following window appears, as shown in Figure 57.
4. Enter the number of devices to be managed. The installer automatically calculates the maximum number of manageable devices. The number cannot exceed the maximum value displayed on the window.

5. Click OK. The Checking Database Connectivity window appears, as shown in Figure 58.

6. Configure the parameters to check the database connectivity:
   - Select a database type, and then use the default instance or enter the custom instance name in the Instance Name combo box.
   - Enter the database superuser name (sa by default) and password.
   - Set the installation location:
     To use a local database, select local host from the Installation Location list. The Database Server Address is automatically populated.
     To use a remote database, select Remote host from the Installation Location list and then enter the IP address of the database in the Database Server Address field.
   - Set the listening port (1433 by default).
NOTE:

When you install IMC on Linux that uses an Oracle database, select a network service name or click to add a network service name. When a local database is used, you must configure a network service name for connecting to the local database address. For more information, see Oracle 11g Installation and Configuration Guide or Oracle 11g R2 Installation and Configuration Guide.

7. Click OK.

   The installer starts to connect to the database. When the connection fails, check the database settings and the parameters you enter in the previous step. When the database is connected, the Welcome to HP iMC Installation Wizard window appears, as shown in Figure 59.

Figure 59 Welcome to HP iMC Installation Wizard

![Welcome to HP iMC Installation Wizard](image)

8. Click Next.

   The Agreement window appears, as shown in Figure 60.
Figure 60 Agreement

9. Read the license agreement and third party license, select Accept, and then click Next. The Choose Target Folder window appears, as shown in Figure 61.

Figure 61 Choose Target Folder

10. Select the components you want to install and then specify the installation location. Make sure the target disk has enough space.

11. Click Next. The Deployment and Upgrade Options window appears, as shown in Figure 62.
12. Set whether or not you want the components to be deployed or upgraded immediately after they are installed.

13. Click Next.

The Installation Summary window appears, as shown in Figure 63.

The Installation Summary window provides the following information:

- Name, description, version, and disk space required by each component to be installed
- IMC installation location
- Total disk space required by the installation
Free disk space of the target partition

14. Click **Install**.

The system starts to install the RSM components. When the installation is complete, the **Installation Completed** window appears, as shown in Figure 64. When you have installed all RSM components, the window does not appear.

**Figure 64 Installation Completed**

In the **Installation Completed** window, you can perform the following operations:

- To complete installation and start deployment, select **Open deployment monitoring agent** box and then click **Finish**.
- To install other components, select **Install other iMC Components** and then click **Finish**.
- To complete installation without deployment, simply click **Finish**.

**Deploying RSM components**

To deploy RSM components:

1. Start the Intelligent Deployment Monitoring Agent with one of the following methods:
   - In Figure 64, select **Open deployment monitoring agent** and then click **Finish**.
   - Select **Start** > **All Programs** > **HP Intelligent Management Center** > **HP Deployment Monitoring Agent** on Windows, or run the **dma.sh** script in the **deploy** directory of the IMC installation path on Linux.

When the Intelligent Deployment Monitoring Agent is started for the first time, the **Batch deploy** window appears, as shown in Figure 65.
2. Select the components you want to deploy and any dependent components for them.
3. Click **OK**.
   The **Database Configuration** window appears, as shown in **Figure 66**.

**Figure 66 Database Configuration**

![Database Configuration Window](image)

4. Set the database parameters:
   - Enter the password for the superuser you configured in the RSM installation.
   - Browse to customize the location for storing data files. The default directory is **C:\Program Files\imcdata** for Windows and **/opt/imcdata** for Linux.
5. Click **Next**.
   The **Configure Web Service Port** window appears, as shown in **Figure 67**.
6. Set the HTTP and HTTPS service ports. The default HTTP port is 8080 and the default HTTP port is 8443.

7. Click Deploy.

The Deploying window appears, as shown in Figure 68.

When the deployment is complete, you can start the remote site with the Intelligent Deployment Monitoring Agent, as shown in Figure 69.
On the Monitor tab, you can start or stop IMC, and to configure IMC as a startup item of the operating system by selecting **Automatically start the services when the OS starts**.

To install other components or upgrade deployed components, click **Install** on the Monitor tab. The installation and deployment methods are the same as those for the IMC Platform. For more information, see "Installing and deploying the IMC Platform" and "Installing and deploying IMC service components."

### Registering RSM

IMC primary and remote sites share the number of manageable nodes permitted by the licenses you purchased. RSM on a single remote site can manage up to 1000 nodes. For example, when a company purchases licenses to manage up to 5000 nodes and uses 3500 nodes on the IMC primary site for management, RSM on all remote sites together can manage 1500 nodes at most.

Similar to IMC, an unregistered RSM version is a 60-day trial, and you must register licenses for RSM. When the RSM trial expires on a remote site, you cannot log in to the IMC primary site from that site unless you register RSM.

RSM licenses are separate from the IMC Platform licenses and must be registered on the IMC primary site. Registering an RSM license is similar to registering an IMC license. For more information, see "Registering IMC and incremental node licenses." An unregistered IMC primary site can only manage one remote site.

Assign a number of manageable nodes to each remote site when you install RSM on a site. These nodes will be automatically released when RSM is removed from that site. If a network problem occurs during removal of a remote site, the nodes assigned to that site for management might not be automatically released. To solve this problem, release the nodes manually.

To perform a manual release:

1. Log on to the IMC primary site.
2. Back up the **agent.xml** file, which is located in the `\client\conf` directory of the IMC installation path.
3. Open the file and delete the configuration segment of the remote site from which RSM has been removed. The configuration segment is marked by a pair of agent elements.

4. Save and close the file.

5. Restart the jserver process of the Intelligent Deployment Monitoring Agent.

For more information about the file contents, see "Modifying the configuration file on a remote site."

Configuring RSM for use

In NAT or other special application environments, the address or port settings of IMC and RSM might change. To ensure normal communication between IMC and RSM, you must modify the RSM configuration files (agent.xml) on IMC primary site and remote sites, respectively.

Modifying the configuration file on the IMC primary site

The file contains the following default contents:

```
<agentConfig local="server" nextId="2">
  <agent defaultProtocol="http" host="IMC-ADDR" id="0" type="local">
    <property name="name" value="iMC Server"/>
    <property name="description" value="iMC Server"/>
    <property name="resReserved" value="JcNzDSRUXrc="/>
    <property name="httpPort" value="8080"/>
    <property name="httpsPort" value="8443"/>
  </agent>
  <agent defaultProtocol="http" host="RSM1-ADDR" id="1" type="remote">
    <property name="name" value="RSM1"/>
    <property name="description" value="RSM Site 1"/>
    <property name="state" value="disconnected"/>
    <property name="lastStateChangeTime" value="2012-10-12 09:55:28.301"/>
    <property name="resReserved" value="72HeIWz8iKg="/>
    <property name="httpPort" value="8080"/>
    <property name="httpsPort" value="8443"/>
  </agent>
  ...
</agentConfig>
```

In the file contents, you can modify only the parameters whose values are highlighted in bold text.

The configuration segment with the `local` type represents the configuration of the local server, which is the IMC primary site. You can modify values of the following attributes:

- **host**—Modify the local server address to the public IP address or hostname of the local server. Make sure the IP address or hostname is globally effective and can be reached by remote sites.
- **defaultProtocol**—Modify the protocol to be used for RSM and IMC communication. The value can be `http` or `https`.
- **httpPort**—Modify the HTTP port number.
- **httpsPort**—Modify the HTTPS port number.

Configuration segments with the `remote` type represent the configuration of remote IMC sites. You can modify values of the following attributes:
• **host**—Modify the remote server address to the public IP address of that server. Make sure the IP address is globally effective.

• **defaultProtocol**—Modify the protocol to be used for RSM and IMC communication. The value can be **http** or **https**.

• **httpPort**—Modify the HTTP port number.

• **httpsPort**—Modify the HTTPS port number.

### Modifying the configuration file on a remote site

After the primary IMC site has the RSM configuration file modified and the IMC service restarted, remote sites automatically update their respective local RSM configuration files. If a remote site failed to update the RSM configuration file, you can manually modify its RSM configuration file.

The file contains the following default contents:

```xml
<agentConfig local="agent">
  <agent defaultProtocol="http" host="RSM-ADDR" id="1" type="local">
    <property name="name" value="RSM "/>
    <property name="description" value="RSM-Site"/>
    <property name="resReserved" value="72HeIWz8iKg="/>
    <property name="httpPort" value="8080"/>
    <property name="httpsPort" value="8443"/>
  </agent>
  <agent defaultProtocol="http" host="IMC-ADDR" id="0" type="remote">
    <property name="name" value="iMC Server"/>
    <property name="description" value="iMC Server"/>
    <property name="state" value="disconnected"/>
    <property name="lastStateChangeTime" value="2012-10-12 18:20:20.980"/>
    <property name="resReserved" value="JcNzDSRUXrc="/>
    <property name="httpPort" value="8080"/>
    <property name="httpsPort" value="8443"/>
  </agent>
</agentConfig>
```

The first configuration segment with the **local** type represents the configuration of the local server, which is the remote site. You can modify values of the following attributes:

- **host**—Modify the local server address to the public IP address or hostname of the local server. Make sure the IP address or hostname is globally effective and can be reached by the IMC primary site.

- **defaultProtocol**—Modify the protocol to be used for RSM and IMC communication. The value can be **http** or **https**.

- **httpPort**—Modify the HTTP port number.

- **httpsPort**—Modify the HTTPS port number.

The second configuration segment represents the configuration of the IMC primary site. You can modify values of the following attributes:

- **host**—Modify the IMC primary server address to the public IP address of that server. Make sure the IP address is globally effective.

- **defaultProtocol**—Modify the protocol to be used for RSM and IMC communication. The value can be **http** or **https**.
• **httpport**—Modify the HTTP port number.
• **httpsport**—Modify the HTTPS port number.

Testing site connectivity

You can test whether the IMC primary site and a remote site can normally communicate each other.

To test site connectivity:

1. Log on to the IMC primary site or a remote site.
2. Enter `http://peer-address:port/imcrs` in the address bar of the browser.

If communication between the two sites is normal, an **Identity Authentication** window appears, displaying the public IP address of the peer server. Otherwise, a communication failure occurs.

Upgrading RSM

To ensure normal cooperation between RSM and IMC, make sure their versions are compatible and have correct patches installed. For example, RSM version 5.2 is not compatible with IMC version 5.1.

Upgrade RSM or IMC to the same version if one of the following cases occurs:

- Synchronization automatically ends.
- Remote service calling cannot be executed on the IMC primary site or a remote site.
- An operator who has the RSM management privileges cannot log in to any remote site from the IMC primary site.
- RSM is properly operating on remote sites, but cannot synchronize data from the IMC primary site.

For information about the upgrade procedures, see “Upgrading IMC.”
9 Upgrading, backing up, or removing IMC

The following information describes how to upgrade IMC components, using upgrading IMC Platform patches as an example.

After installing the IMC Platform and components, when you want to upgrade the IMC Platform, first make the following preparations:

- Components require IMC V5.0 or a later version. For the compatibility matrix, see the readme file.
- For data safety, HP recommends that you back up the database and the entire IMC installation path because it is not done during upgrade. For how to back up the IMC database, see "Basic database backup and restore," "Database backup and restore for a single IMC system," "Database backup and restore in IMC stateless failover," and "Database backup and restoration to a remote database server."
- Download the upgrade packages for all listed components before you upgrade the IMC Platform.

Backing up IMC

You can back up the IMC installation directory and database files.

To back up the IMC installation directory, execute the backup.bat script that is located in the IMC installation package. If IMC uses a local database, the backup.bat script also backs up the database files.

To backup files of a remote database, use Dbman in the Intelligent Deployment Monitoring Agent. Dbman cannot back up the IMC installation directory.

According to the IMC deployment, use one of the following methods to back up IMC:

- If IMC uses a local database and is deployed in centralized mode, back up IMC by executing the backup.bat script on the master server.
- If IMC uses a local database and is deployed in distributed mode, back up IMC by executing the backup.bat script on the master and all subordinate servers.
- If IMC uses remote databases, execute the backup.bat script to back up the IMC installation directory and use Dbman to back up the database of each component. For more information, see "Basic database backup and restore."
- If IMC is deployed in stateful failover mode, back up IMC by executing the backup.bat script only on the servers that are online.

Backing up IMC by executing backup.bat

1. Log in to the operating system as an Administrator.
2. Run the install\backup.bat script in the downloaded installation package. The Backup IMC window appears, as shown in Figure 76.
CAUTION:

- To back up IMC in Windows Server 2003 or Windows Server 2003 R2, you must log in as an administrator and then back up IMC.

- To back up IMC in Windows Server 2008 or Windows Server 2008 R2, you must first right-click the `backup.bat` script and select Run as Administrator from the shortcut menu, or modify the User Account Control Settings and then restart the server. After backing up IMC, you can restore the related settings as needed.

- To modify the user account control settings, select Start > Control Panel > System and Security, click Change User Account Control Settings in the Action Center, and set the Choose when to be notified about changes to your computer to Never notify in the User Account Control Settings window.

To back up IMC on Linux, you must start the IMC installation wizard by running the `backup.sh` script in the install directory of the IMC installation package as a root user.

When the installation file is obtained via FTP, you must first authorize the `install.sh` script by executing `chmod -R 775 install.sh` in the directory of the script.

---

**Figure 70 Back up IMC**

3. Check the size of the backup files and make sure the disk for saving the files has enough memory. Insufficient memory may cause backup failure.

4. Click Browse to customize the location for saving the backup files as shown in Figure 71.

**Figure 71 Choose the backup file location**

5. Click Start to start backing up IMC.

After the backup is complete, the backup file directory generates a package `IMC.zip`, which contains the complete backup files under the IMC installation path. In the backup directory also is a folder named `db\`, which contains the database backup data of all components. If a separate database is used, the `db` folder is empty.

---

**Back up IMC databases by using Dbman**

For more information, see "Basic database backup and restore."

---

**Upgrading IMC**
CAUTION:

- Make sure you have compatible upgrade packages for all deployed IMC components. Otherwise, IMC becomes invalid after upgrade.
- To upgrade IMC from version 3.x to version 5.x, re-log in to the registration website and obtain a new activation file.
- Do not upgrade IMC by running the `install\install.bat` script in the IMC installation path.

To upgrade an IMC component, ensure that the IMC Platform has been installed, and the components on which the component you want to upgrade depends have been installed and upgraded. Before you upgrade a service component that is related to the Report Management subcomponent, upgrade the Report Management subcomponent to a version compatible with the service component. Otherwise, the report function might be abnormal.

In distributed deployment mode, upgrade all components deployed on subordinate servers separately.

The following example describes how to upgrade the IMC Platform on Windows.

1. Use one of the following ways to start upgrade:
   - On the [Installation Completed] window, as shown in Figure 16, select [Install Other Components], and click [Finish], or
   - After you have installed and deployed the IMC Platform, click [Start] > [All Programs] > [HP Intelligent Management Center] > [HP Deployment Monitoring Agent] (or run the `dma.sh` script in `/deploy` of the IMC installation path on Linux), to start the Intelligent Deployment Monitoring Agent and then click [Install new components] on the [Monitor] tab.

CAUTION:

- To upgrade IMC in Windows Server 2003 or Windows Server 2003 R2, log in as an administrator and then upgrade IMC.
- To upgrade IMC in Windows Server 2008 or Windows Server 2008 R2, you must first select [Start] > [All Programs] > [H3C Intelligent Management Center], right-click [Deployment Monitoring Agent], and select [Run as Administrator] from the shortcut menu to open the deployment monitoring agent, or modify the [User Account Control Settings] and then restart the server. After upgrading IMC, you can restore the related settings as needed.
- To modify the user account control settings, select [Start] > [Control Panel] > [System and Security], click [Change User Account Control Settings] in the Action Center, and set the [Choose when to be notified about changes to your computer] to [Never notify] in the [User Account Control Settings] window.

2. On the system tray of Windows, right-click the [Deployment Monitoring Agent] icon, and select [Install] from the menu.
   - The [Choose folder] window appears, as shown in Figure 72.

   ![Figure 72 Choose folder](image)

3. Click [Browse], and select folder `install\components` in the upgrade files.
4. Click [OK].
The **Welcome to HP IMC Installation Wizard** window appears, as shown in Figure 73.

**Figure 73 Welcome to HP IMC Installation Wizard**

5. Click **Next**. The **Agreement** window appears, as shown in Figure 74.

**Figure 74 Agreement**

6. Read the license agreement carefully, select **Accept**, and click **Next**. The **Upgrade Common Components** window appears, as shown in Figure 75.
7. Click OK.

The system starts upgrading common components, as indicated by the Upgrade Common Components window in Figure 76.

![Figure 76 Upgrade Common Components](image1)

After the common components are upgraded, the Choose Target Folder window appears, as shown in Figure 77.

![Figure 77 Choose Target Folder](image2)

The Choose Target Folder window displays the components to be upgraded. The system installs the upgrade files in the location where the IMC Platform is installed.
8. Check the information, click **Next**, and the **Deployment and Upgrade Options** window appears, as shown in **Figure 78**.

**Figure 78 Deployment and Upgrade Options**

![Deployment and Upgrade Options](image)

9. Select a deployment and upgrade option as prompted by the window.
   
   In this example, select **Deploy or upgrade at once**, and click **Next**. The **Installation Summary** window appears, as shown in **Figure 79**.

**Figure 79 Installation Summary**

![Installation Summary](image)

10. Check the installation summary, click **Install**, and the **Installing** window appears, as shown in **Figure 80**.
The installation wizard installs the components.

After the installation is finished, the **Batch upgrade** window appears, as shown in Figure 81.

11. Select the components you want to upgrade, and then click **OK**.

   After the selected components are upgraded, the **Batch upgrade result** window appears, as shown in Figure 82.

12. Click **OK**.

If you have used Dbman for IMC auto backup or restoration before upgrade, the **Auto Backup and Restore Configuration** window appears.
13. Click **OK**.

The automatic backup and restoration process starts. After that, you can launch IMC by clicking **Start iMC** on the **Monitor** tab of the Intelligent Deployment Monitoring Agent.

After the processes of all components are started normally, IMC is ready for use.

When upgrading service components related to the Report Management module, you must also upgrade the Report Management module to the version compatible with these related service components, so that you can use the report function properly.

When this is a distributed deployment, upgrade all components deployed on subordinate servers separately.

### Completing IMC upgrade for Oracle

To complete upgrade to IMC 5.1 or later in distributed mode, install a tool by following the instructions on a popup dialog box (see Figure 83). The tool is used to upgrade the Oracle database configuration for communication between the master and subordinate servers.

**Figure 83 Important message**

Your IMC servers are deployed in distributed mode.

Follow these steps to upgrade the Oracle configuration on each IMC server:

1. Copy the installation package `linux/tools/oraupgrade.tar.gz` to current server.
2. Unzip the package with the `tar -xzf oraupgrade.tar.gz` command.
3. Run `oraupgrade/fxora.sh` and operate following instructions that appear.
4. When you see the Successful message, click **OK**.

### Restoring IMC

⚠️ **CAUTION:**

In the Windows operating system, use WinRAR or 7-Zip to decompress the package, other than the decompression tool included with the Windows system.

When errors occur in IMC upgrading, you must restore IMC. Depending on the IMC deployment, use one of the following restore methods:

- If IMC uses a local database, embedded or separate, restore IMC installation directories and database files on all IMC servers, including the master and all subordinate servers.
- If IMC uses a remote database, restore the installation directory on each IMC server, embedded or separate, and restore the database of each component on the database server. For more information, see "Manual restore."
- For IMC deployed in stateful failover mode, only restore IMC on the servers that are online.

To restore IMC:

2. When the restoration is complete, stop the Intelligent Deployment Monitoring Agent and IMC service.
3. Manually delete all the files in the IMC installation path.
4. Decompress the IMC.zip package to the IMC installation path.
5. Restart the Intelligent Deployment Monitoring Agent and IMC service.

Removing IMC

Removing IMC on Windows and Linux systems is similar. The following describes how to remove IMC from a Windows Server 2003-based machine.

Removing an IMC component

Before removing an IMC component, remove any components that depend on it.

If the IMC component is deployed on more than one server, remove it first from all subordinate servers and then from the master server.

To remove an IMC component from a subordinate server:
1. Launch the Intelligent Deployment Monitoring Agent on the subordinate server.
2. On the Deploy tab, right-click the component you want to remove, and then select Remove this Component from the shortcut menu.
   The Intelligent Deployment Monitoring Agent removes the selected component from the subordinate server.

To remove an IMC component from the master server:
1. Launch the Intelligent Deployment Monitoring Agent on the master server.
2. On the Monitor tab, click Stop IMC to stop the IMC service.
3. On the Deploy tab, select Undeploy the Component from the right-click menu of the component that you want to undeploy.
   A dialog box appears, indicating that the component was successfully undeployed.
4. Click OK.
5. On the Deploy tab, select Remove this Component from the right-click menu of the component that you have undeployed.
   A dialog box appears, indicating that the component was successfully removed.
6. Click OK.

When you remove an IMC component deployed in distributed mode, undeploy the component on the subordinate server where it was deployed, and then remove the component on the master server.

Before removing a component, remove the components that depend on it, when any.

In the following two cases, the deployment information of a removed component cannot be cleared automatically:
- The component was removed from the subordinate servers by force, which is an incorrect operation.
- The subordinate server crashed when the component was being removed from it.

To solve the problem, perform the following steps:
1. Select the component on the **Deploy** tab of the Intelligent Deployment Monitoring Agent on the master server.
2. Right-click **Uninstall the Component** for the master server only.

To re-install a component removed from a monitoring agent, you must restart the deployment monitoring agent and HP IMC server, with the following steps:
1. Quit the deployment monitoring agent window.
2. Restart the **HP IMC server** service.
3. Start the Intelligent Deployment Monitoring Agent.
4. Click **Install** in the **Monitor** tab to begin installation.

---

### Removing all IMC components at one time

The following sections describe how to remove the IMC software deployed in centralized and distributed modes respectively.

When reinstalling IMC, you must manually delete the folder named **IMCdata**, which is created on the master server upon installation of IMC when you have re-installed an SQL server database after you uninstalled IMC.

When you fail to install or uninstall IMC, manually delete the IMC installation folder and the **IMC-Reserved** folder in the Windows installation directory (or delete this folder in the `/etc` directory on Linux operating systems); otherwise, IMC cannot be reinstalled.

#### Removing IMC deployed in centralized mode

1. Launch the Intelligent Deployment Monitoring Agent.
2. On the **Monitor** tab, click **Stop IMC** to stop the IMC service.
3. Launch the IMC uninstaller.
   - On windows, select **Start** > **All Programs** > **HP Intelligent Management Center** > **Uninstall HP Intelligent Management Center**.
   - On Linux, run the `uninstall.sh` script in `/deploy` of the IMC installation path.
   A window appears to guide you through the rest of the process.
4. Click **Uninstall**.
5. Click **Finish** when the **Uninstallation Completed** dialog box appears.
6. Delete the **IMC-Reserved** folder in the WINDOWS folder of the system disk (or delete the **IMC-Reserved** folder in the `/etc/` directory on Linux).
7. Reboot the system.

#### Removing IMC deployed in distributed mode

In distributed deployment mode, you must first remove components deployed from each subordinate server, and then remove the IMC software from the master server. The remove procedures are the same on all servers.

To remove all IMC components from an IMC server:
1. Launch the Intelligent Deployment Monitoring Agent.
2. On the **Monitor** tab, click **Stop IMC** to stop the IMC service.
3. Launch the IMC uninstaller.
- On Windows, select **Start** > **All Programs** > **HP Intelligent Management Center** > **Uninstall HP Intelligent Management Center**.

- On Linux, run the `uninstall.sh` script in `/deploy` of the IMC installation path. A window appears to guide you through the rest of the process.

4. **Click Uninstall**.

5. **Click Finish** when the **Uninstallation Complete** dialog box appears.

6. **Delete the IMC-Reserved folder** in the WINDOWS folder of the system disk (or delete the IMC-Reserved folder in the `/etc/` directory on Linux).

7. **Reboot the system**.
10 Registering IMC and incremental node licenses

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

The IMC registrations on Windows and Linux systems are similar. The following describes how to register IMC on a Windows Server 2003-based machine. Ensure you Register and Activate IMC before any additional node licenses.

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

Registering IMC

From the IMC login page click on the Activate link to enter the License Information page appears, as shown in Figure 84.

Figure 84 License Information

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

Registering first license

1. Go to the HP My Networking system website (http://hp.com/networking/mynetworking/), log in to My Networking portal, and the HP Passport sign-in page appears, as shown in Figure 85.
2. Enter the **User ID** and **Password**, and then click **Sign in**.

The **Welcome** page appears, as shown in Figure 86.

**Figure 86 Welcome page**
3. Click the My Licenses tab from the tabular navigation system on the top. The **Enter Order number or Registration ID** page appears, as shown in Figure 87.

**Figure 87 Enter Order number or Registration ID page**

![My Licenses and Enter Order number or Registration ID page](image)

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 88.

**Figure 88 Enter the email associated with Order number page**

![My Licenses and Enter the email associated with Order number page](image)

5. Enter an email address associated with the **Order number**, and then click **Next**. The **Select the Product License** page appears, as shown in Figure 89.
6. Select the product for which you want to register or activate a license.

7. Enter the quantity to be redeemed, and then click Next.
   The Enter details page appears, as shown in Figure 90.

Figure 90 Enter details page

8. Enter the Base software serial number, and then click Next.
   The License agreement page appears, as shown in Figure 91.
9. Read the license agreement, select **I accept all of the above terms**, and then click **Finish**. The **Confirmation** page appears, as shown in Figure 92.

10. Click **Save as**, download and save the license key file. Remember the location and file name for the next step of Activating the License in IMC.

11. When you need to email the confirmation, enter the **Send license confirmation to** and **Comments**, and then click **Send email** on this page. 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. This 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, as shown in Figure 93.

Figure 93 Select the Product License page

2. Click Next.

The Enter details page appears, as shown in Figure 94.
3. Select your base product and enter the Base software serial number, and then click **Next**.
   The **Confirmation** page appears, as shown in Figure 92.

4. Click **Save as**, download and save the license key file.
   You need to remember the location and file name for the next step of Activating the License in IMC.

**Activating IMC**

To activate IMC:

1. Return to the **License Information** page, as shown in Figure 84.
2. Select **Activate now**.
   The **Activate Your Product** page appears, as shown in Figure 95.

**Figure 95 Activate Your Product**

3. Select the license file in the format of .txt.
4. Select the license type, which can be **Register/Activate host license** or **Register/Activate back-up license**, as needed.
5. Click **OK**.
   The **Activations Succeeded** dialog appears, as shown in Figure 96.
Figure 96 Activation Succeeded

Reboot the system.

Your IMC system has now been successfully Registered and Activated.

Upgrading to an IMC V5.0 license

Your existing eSupport account including your IMC licenses have been transferred to My Networking and a HP Passport account has been created with your eSupport user name.

The HP My Networking system address: http://hp.com/networking/mynetworking.

Your IMC license file has been updated in My Networking to support IMC V5.0.

You need to download your updated IMC license file from My Networking and reactivate your IMC V5.0.

To update your IMC license file from My Networking and reactivate your IMC V5.0:

1. Locate your IMC Serial Number:
   a. Follow the **Activate** link from the IMC login page to enter the **License Information** page and your IMC serial number appears.
   b. Select your IMC serial number, and copy and paste the serial from the IMC License information page to My Networking.

2. Reset your new HP Passport password so you can login to My Networking using your new HP Passport account:

Your eSupport user account has been transferred to My Networking and a HP Passport account has been created using your eSupport user name.

   c. Reset your HP Passport password before you can log in by following the **Forgot Password** link.
   d. Provide the email address of your eSupport account user to receive instructions on resetting your password.
   e. Follow the email instructions to click on the **Choose a new password** link.
   f. Enter your new HP Passport password and select your security questions and answers.

Your HP Passport password is now reset, allowing you to log in to My Network using the HP Passport account with your eSupport user name and password.

3. Log in to My Networking

4. Click **Continue** in the Change HP Passport password page to log into My Networking.
   The **Welcome <username>** page appears.

5. Locate your IMC licenses

6. Click the **My Licenses** tab from the tabular navigation system on the top.
   The **Enter Order number or Registration ID** page appears.

7. Click on **View Licenses** from the **My Licenses** navigation.
8. Locate your IMC Platform license in the list of your licenses. When necessary copy and paste your IMC serial number into the search field and click **Search**.

9. Download the updated IMC license file

10. Click corresponding to the IMC Platform license.

   The license information page appears.

11. Click the **Download License** link.

12. Choose to save the license file, and choose where to save the license file.

   Save the license file so that you can locate it again when you need it.

---

**Updating your IMC V5.0 license file**

1. Follow the Activate link on the IMC login page to enter the **License Information** page.

2. Click **Activate now**.

   The **Activate Your Product** page appears.

3. Browse to the location where you saved the license file and select it, and click **OK**.

   The **Activations Succeeded** dialog appears.

4. Select the license file which should be in .txt format.

5. Select the license type, which can be **Register/Activate host license** or **Register/Activate back-up license**, as needed.

6. Click **OK**.

   The **Activations Succeeded** dialog appears.

   Your IMC V5.0 is now fully licensed with the equivalent licenses you had previously.

---

**Upgrading to IMC V5.1 license**

To upgrade IMC V5.0 to IMC V5.1, you only need to upgrade the license of QoSM components. The QoSM license upgrade process is the same as the V5.0 license upgrade process. For more information, see "Upgrading to an IMC V5.0 license."
11 Security and backup

Anti-virus software

To ensure the secure running of the IMC server, HP recommends that you install anti-virus software, and update the virus library.

Port settings

To ensure the steady running of the IMC server, HP recommends that you use a firewall to control the data sent to the IMC server cluster, that is, filter the non-service data sent to the IMC server. In this way, you can prevent abnormal attacks.

⚠️ CAUTION:

- HP recommends that you use ACL configurations on a firewall rather than on a switch to control data packets. Otherwise, packet fragmentations are filtered.
- When you have installed firewall software on the IMC server, besides setting the ports listed in Table 10, set an IP address for the master server and all subordinate and database servers to ensure normal communication between them.

Table 11 and Table 12 list the port numbers used by IMC components.

Table 11 Port numbers used by the IMC PLAT

<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>Port for the access to the IMC through HTTP</td>
<td>IMC server</td>
</tr>
<tr>
<td>TCP 8443, configurable</td>
<td>Port for the access to the IMC through HTTPS</td>
<td>IMC server</td>
</tr>
<tr>
<td>UDP 69</td>
<td>Port for Intelligent Configuration Center to perform configuration management through TFT</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>
</tbody>
</table>

Table 12 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>

When a firewall resides between the probe and the IMC server, you need to configure an ACL on the firewall so that all the IP packets from the probe can be sent to the IMC server.

**Basic database backup and restore operations**

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

Dbman is integrated in the Intelligent Deployment Monitoring Agent, as shown in Figure 97.

**Figure 97 Environment tab**

The screen is broken into the following sections.

- The software and hardware information of the servers displays on the left of the **Environment** tab.
- The usage of the user database file and log file displays on the right.
- The Dbman database backup and restoration configuration displays at the bottom.

The Dbman database backup and restoration configuration includes the following options:

- **Configure**—Provides automatic backup and restoration function, which can back up and restore database files on a regular basis. You can also upload backup database files to an FTP server for storage. The automatic backup and restoration function is used mainly in stateless failover scenarios.
- **Backup**—Immediately backs up the database files of the current IMC server. This function is available only when the current IMC server uses a local database.
- **Restore**—Replace the current database files with the backup database files to restore the database to the specified time point. This function is available only when the current IMC server uses a local database.
• **View Log**—View the database backup and restoration log. The log size can be set by using the Configure function.

**Manual backup**

Manual backup allows you to manually back up IMC databases immediately. Make sure the target IMC system uses a local database, embedded or separate.

To perform a manual backup:

1. Start the Intelligent Deployment Monitoring Agent on the server.
2. Click the Environment tab as shown in Figure 97.
3. Click Backup.
   The Select database backup path dialog box appears.
4. Select the backup file save path.
5. Click OK.
   Dbman starts to back up all databases used by the IMC system on the server to the specified path.

**Automatic backup**

You can configure automatic database backup to periodically back up the IMC database files to the local database, and to upload the backup database files to the FTP server.

To configure automatic backup:

1. Start the Intelligent Deployment Monitoring Agent on the local master or subordinate server.
2. Click the Environment tab as shown in Figure 97.
3. Click Configure.
   The Auto Backup and Restore Configuration dialog box appears, as shown in Figure 98.
4. Enable automatic database backup and restoration and configure general parameters:
   - **Enable auto backup and restoration**—Enable or disable Dbman.
   - **Max Size of Log File**—Enter the maximum size of the log file for database backup and restoration, in MB. If the log file exceeds the maximum size, the system automatically creates a new log file. Log files are stored in the `iMC_install\dbman\log` directory.
   - **File Lifetime**—Enter how many days an automatic backup or restoration file can be kept. Expired files are automatically removed.

5. Configure the following automatic restoration parameters:
   - **Operation Type**—Select the operation to perform, automatic backup or automatic restoration. Select **Auto Backup** in this configuration.
   - **Backup Time in a Day**—Enter the hour at which the automatic backup operation starts every day.
   - **Backup File Location**—Enter or browse to the path where backup files are located. Make sure the path is located on a disk that has enough free space. Do not set the path to the operating system drive because the operating system cannot start normally when this drive is fully occupied.
   - **Upload backup files to FTP Server**—Select this option to specify an FTP server to store backup files.
   - **FTP Host**—Enter the IP address of the FTP server.
   - **FTP User**—Enter the FTP username. With a username specified, IMC automatically uploads the backup database files to the working directory of the user on the FTP server. Without a username, IMC uploads the backup database files to the root directory of the FTP server.
FTP Password—Enter the FTP user password.

6. Click OK.
Dbman automatically backs up the IMC databases at the specified time and uploads the backup database files to the FTP server.

Manual restore

⚠️ CAUTION:
When restoring databases of the IMC system, also restore databases of all components that have been deployed. If you restore only some of them, data loss might occur.

Manual restoration allows you to restore the IMC database files of a specified backup time point. Make sure IMC is started at least once after installation and the backup database files exist.

To perform a manual restoration:
1. Start the Intelligent Deployment Monitoring Agent on the server.
2. Click the Environment tab as shown in Figure 97.
3. Click Restore.
   A Confirmation dialog box appears, as shown in Figure 99.

Figure 99 Confirmation dialog box

4. Click Yes.
5. Select database files of all components and click OK in the popup dialog box.
6. Click OK in the popup dialog box.
Dbman starts to restore the databases and displays a restoration success message after the restoration is complete.
7. Click OK. IMC will be automatically started.

NOTE:
During the restoration process, Dbman shuts down and restarts IMC and the database server.

Automatic restore

Automatic restoration applies to stateless failover scenarios to regularly restore IMC service database files on an IMC server or database server. You can configure automatic backup on the primary server and enable the FTP server function on the backup server. When new backup database files are uploaded from the primary server, the backup server immediately replaces existing database files with the new files to implement database restoration.

To configure automatic restoration:
1. Start the Intelligent Deployment Monitoring Agent on the local server.
2. Click the Environment tab as shown in Figure 97.

3. Click Configure.

   The Auto Backup and Restore Configuration dialog box appears, as shown in Figure 100.

Figure 100 Auto Backup and Restore Configuration

4. Enable automatic database backup and restoration and configure general parameters:
   - **Enable auto backup and restoration**—Enable or disable Dbman.
   - **Max size of log file**—Enter the maximum size of the log file for database backup and restoration. If the log file exceeds the maximum size, the system automatically creates a new log file. Log files are stored in the `iMC_install\dbman\log` directory.
   - **File lifetime**—Enter how many days an automatic backup or restoration file can be kept. Expired files are automatically removed.

5. Configure the following automatic restoration parameters:
   - **Operation type**—Select the operation to perform, automatic backup or automatic restoration. Select Auto Restore in this configuration.
   - **Location to archive restored files**—Enter or browse to the path where the files to be restored are located. The path must be the same as the default working directory of the FTP user account that is specified for automatic backup. The backup server automatically restores the databases immediately after it receives the database backup files.
   - **Backup files location**—Enter or select a backup path to save database backup files after restoration.

6. Click OK.
Database backup and restore for a single IMC system

You can perform manual backup, automatic backup, and manual restoration for a single IMC system that uses one or more local databases.

If a single IMC system uses a remote database, see "Database backup and restoration to a remote database server."

This section describes how to back up and restore IMC databases locally in different deployment scenarios.

Application scenario—centralized deployment

The IMC Platform and all service components are deployed on the same server and use a local database.

To back up the local database of such a single IMC system, perform manual backup or configure automatic backup by using Dbman. For more information, see "Manual backup" or "Automatic backup."

To restore the local database for such a single IMC system, perform manual restoration. For more information, see "Manual restore."

Application scenario—distributed deployment

The IMC Platform and service components are deployed to multiple servers and use their respective local databases.

To back up the local databases of such a single IMC system, perform manual backup or configure automatic backup by using Dbman. For more information, see "Manual backup" or "Automatic backup."

IMPORTANT:

To ensure normal operation of the backed up database, make sure the master and all subordinate servers use the same automatic backup time.

To restore the local database for such a single IMC system, perform manual restoration. For more information, see "Manual restore."

Database backup and restore in IMC stateless failover

In a stateless failover scenario, the primary and backup servers use their respective local databases. The primary server automatically backs up and uploads database files to the backup server. When the primary server fails, IMC automatically switches to use the database files on the backup server.

Before you configure database backup in a stateful failover scenario, make sure that:

- The primary and backup servers use the same operating system, IMC version and patches, and database type and version.
• FTP server is configured on all backup servers.

This section describes how to back up and restore IMC databases for IMC stateless failover scenario in different deployment scenarios. For how to back up and restore databases for an IMC stateful failover scenario, see "Database backup and restoration to a remote database server."

Application scenario—centralized deployment

IMC is deployed in centralized mode on two servers. The license type is selected as primary server license on one server, and as backup server license on another server.

NOTE:
To implement database backup to the backup server for IMC deployed in centralized mode, the IMC components of the master server and the backup server must be deployed in the same way.

Database backup
IMC servers in stateless failover support automatic database backup, and do not support manual backup. With automatic backup configured, the primary server periodically backs up the IMC database files and uploads them to the backup server. For more information, see "Automatic backup."

Database restoration
IMC servers in stateless failover support both automatic database restoration and manual database restoration. H3C recommends you to use automatic database restoration. For more information, see "Manual restore."

In special cases, you might perform manual database restoration. To do that, make sure the database files of all IMC components are uploaded to the backup server for restoration. Otherwise, data loss will occur. For more information about manually restoring the database, see "Manual restore."

Application scenario—distributed deployment

Back up databases locally
You can back up IMC databases to the backup server cluster (distributed mode) in the following scenarios:

• Application scenario 1:
Deploy an IMC system in distributed mode on the master server cluster and backup server cluster respectively. Both server clusters must use the same number of IMC servers and component distribution. Set up a separate database for each cluster.

Select the license type as master server license on the master server cluster, and select the license type as backup server license on the backup server cluster.

In this scenario, Dbman periodically backs up the IMC databases on each server in the master server cluster to the corresponding server in the backup server cluster so that when the primary server in the master server cluster fails, you can log in to the IMC system of the primary server in the backup server cluster to perform operations.

• Application scenario 2:
Deploy an IMC system in distributed mode on the master server cluster and an IMC system in centralized mode on the backup server. Set up a separate database for each cluster.

Select the license type as master server license on the master server cluster, and select the license type as backup server license on the backup server.
In this scenario, Dbman periodically backs up the IMC databases on each server in the master server cluster to the backup server so that when the primary server in the master server cluster fails, you can log in to the IMC system of the backup server to perform operations.

IMC servers in stateless failover support automatic database backup, and do not support manual backup. With automatic backup configured, the primary server (master or subordinate) periodically backs up the IMC database files and uploads them to the specified backup server. For more information, see "Automatic backup."

**IMPORTANT:**
To ensure normal operation of the backed up database, make sure the master and all subordinate servers use the same automatic backup time.

You can perform a manual backup or configure automatic backup to restore the database files on the backup server. For more information, see "Manual restore" or "Automatic restore."

**Backing up databases to a remote database**

You can back up IMC databases to the backup server cluster (distributed mode) in the following scenarios:

- **Application scenario 1:**
  Deploy an IMC system in distributed mode on the master server cluster and backup server cluster respectively, and each of them uses a remote database server. Select the license type as master server license on the master server cluster, and select the license type as backup server license on the backup server cluster.

- **Application scenario 2:**
  Deploy an IMC system in distributed mode on the master server cluster and an IMC system in centralized mode on the backup server, and each of them uses a remote database server. Select the license type as master server license on the master server cluster, and select the license type as backup server license on the backup server.

These two scenarios require database backup and restoration to a remote database server. For more information about backup and restoration on the local database server, see "Database backup and restoration to a remote database server."

**Database backup and restoration to a remote database server**

To back up or restore database files on a remote database server for IMC, you must copy the backup configuration and other files generated by Dbman on the IMC servers to the database server, and install and run Dbman on the database server. Otherwise, you can receive a message when attempting to perform automatic backup or restoration to a remote database in the Intelligent Deployment Monitoring Agent, as shown in Figure 101.
This chapter describes how to use Dbman that is installed in the **INSTDIR** directory of the remote database server. You can replace the **INSTDIR** string in the commands with the actual directory name.

### Installing and running Dbman on the database server

The first time you backup up or restore IMC using a remote database server, you must install and run Dbman on the database server.

#### On Windows

To install and run Dbman on a Windows database server:

1. Run the `vcredist.exe` file that is located in the `{components\common\server}` directory of the IMC installation package to install Microsoft Visual C++ 2008 Redistributable to the database server.
2. Copy the `dbman` folder in the IMC installation path on the master server to the **INSTDIR** directory on the database server.
3. If subordinate servers exist, copy the `dbman\etc` folders to the database server as follows:
   a. Rename the `dbman.conf` file in the `{dbman\etc}` folder on each subordinate server using the format of `dbman.partn.conf`. Make sure no two `dbman.partn.conf` files are named the same.
   b. Copy each `{dbman\etc}` folder and paste it to the `{INSTDIR\dbman}` folder on the database server. All files in the `{INSTDIR\dbman\etc}` folder are overwritten except the `dbman.conf` file.
4. Open the Command Prompt window and enter the logical disk where the **INSTDIR** folder is located.
5. Use the `cd` command to enter the `{INSTDIR\dbman\bin}` folder:
   ```
   cd {INSTDIR\dbman\bin}
   ```

#### On Linux

To install and run Dbman on a Linux database server:

1. Set the following environment variable:
   ```
   export LD_LIBRARY_PATH= $LD_LIBRARY_PATH:/INSTALL_DIR/dbman/bin:/$ORACLE_HOME/lib
   ```
2. Copy the `dbman` folder in the IMC installation path to the **INSTDIR** directory on the database server.
3. If subordinate servers exist, copy the `dbman\etc` folders to the database server as follows:
   a. Rename the `dbman.conf` file in the `{dbman\etc}` folder on each subordinate server using the format of `dbman.partn.conf`. Make sure no two `dbman.partn.conf` files are named the same.
   b. Copy each `{dbman\etc}` folder and paste it to the `{INSTDIR\dbman\etc}` folder on the database server. All files in the `{INSTDIR\dbman\etc}` folder are overwritten except the `dbman.conf` file.
4. Open the Terminal window.
5. Use the `cd` command to enter the `/INSTDIR/dbman/bin` folder.

```
cd /INSTDIR/dbman/bin/
```

### Using Dbman on the database server

When Dbman is running on the database server, you can perform database backup and restoration operations by following the aids on the screen, including:

- Start automatic backup and restoration: `dbman`
- Stop automatic backup and restoration: `dbman -k`
- Manually back up: `dbman -backup "path where the backup file is saved"`
- Manually restore: `dbman -restore "specifies the path and name of the file to be restored"`
- Check whether Dbman runs normally: `dbman -c`

When you perform database backup and restoration, follow these guidelines:

- Make sure Dbman has the latest configuration. Otherwise, update it. For more information, see "Updating Dbman for the database server."
- Dbman does not support automatic database restoration when it runs on the database server.
- Do not close the Command Prompt window or Terminal window when automatic backup is being performed. Otherwise, the backup process terminates.
- To perform manual restoration, shut down the Intelligent Deployment Monitoring Agent first.
- If a SQL Server database is used, manual restoration restores the database. Make sure the SQL Server database is not used by other programs on the database server.
- To restore multiple databases simultaneously, use colons (;) to separate the database files. See the following example:
  ```
  dbman -restore "C:\monitor_db_imc_monitor_db_20090626_095700_full.db;config_db_imc_config_db_20090626_095714_full.db"
  ```

### Updating Dbman for the database server

If Dbman is already installed and running on the database server, update it for the database server in any of the following cases:

- The IMC Platform is upgraded.
- The automatic backup and restoration settings on the Environment tab of the Intelligent Deployment Monitoring Agent are changed.

To update Dbman for the database server:

1. Shut down Dbman on the database server:
   ```
   dbman -k
   ```
2. Copy the `dbman` folder in the IMC installation path on the master server to the `INSTDIR` directory on the database server.
3. If subordinate servers exist, copy the `dbman\etc` folders to the database server as follows:
   
   a. Rename the `dbman.conf` file in the `\dbman\etc` folder (`/dbman/etc on Linux`) on each subordinate server using the format of `dbman.partn.conf`. Make sure no two `dbman.partn.conf` files are named the same.

   b. Copy each `\dbman\etc` folder (`/dbman/etc on Linux`) and paste it to the `INSTDIR\dbman` folder (`/INSTDIR/dbman on Linux`) on the database server. All files in the
The `\INSTDIR\dbman\etc` folder (\INSTDIR/dbman/etc on Linux) are overwritten except the `dbman.conf` file.

4. Run Dbman on the database server:
   ```
dbman
   ```

   After that, you can perform database backup and restoration using Dbman on the database server.

Configuration guidelines

- When a component of the IMC system, such as NTA, has a large amount of data, do not configure backup and restoration for such data when configuring Dbman. To disable Dbman from backing up the database, create a file with extension `.skip` (for example, nta.skip) in the `dbman\etc` folder of the database server of the component, and write the following to the file:
  ```
dbName=nta_db (for SQL Server/MySQL)
dbUserName=IMC_nta (for Oracle)
  ```

  After you save the `.skip` file, Dbman automatically reads the file and does not back up the database in the file.

- To add more configurations in the backup and restoration configuration file besides the properties configured with Dbman in the Automatic Backup and Restoration window, write the configurations to be added to file `dbman_addons.conf` at the `dbman\etc` directory in the installation path. After you save the file, IMC automatically executes the configurations you added.

  For example, write the following before or after database restoration:
  ```
BeforeSQLScript_monitor_db_IMC_monitor = D:\1.bat
AfterSQLScript_monitor_db_IMC_monitor = D:\2.bat
  ```

- In an IMC stateless failover system, a backup license for the iAR report/table customization function provides only the reading right. To synchronize the report/table template of the master system to the backup system, you must advertise that template on the backup system by using the trial version and then register the backup system.
12 FAQs

When I uninstall IMC in distributed mode from the master server, the component data in the Oracle database cannot be deleted. Why?

This is because the data is used by other users that IMC cannot drop.

Restart the operating system or the Oracle database.

When I was deploying IMC components by using SQL Server 2008 R2 Express, I failed to create my database. How can I solve this problem?

Modify the security attribute of the IMC data folder after deploying IMC components by following these steps:
1. Right-click the IMC data folder (the default folder is IMCdata).
2. Click Properties on the shortcut menu. The Properties dialog box appears.
3. Select the Security tab and allow Users to have full control of the folder.
4. Click OK.

How to install the Java running environment on Linux so that I can access IMC properly through Firefox?

To install the Java running environment, install JDK or JRE and then configure JDK or JRE for Firefox. JDK is taken for example in the following part.
1. Download JDK
Address: http://www.oracle.com/technetwork/java/javase/downloads/index.html

Make sure the correct version is downloaded. For example: you must download jdk-6u12-linux-i586-rpm.bin for x86-based Linux.
2. Install JDK
Upload the installation file jdk-6u12-linux-i586-rpm.bin to the server. Suppose the installation file is saved in directory /tmp, execute the following commands:
cd /tmp
sh jdk-6u12-linux-i586-rpm.bin

After executing the commands above, press the Space bar to view the copyright information, and then enter yes to finish the JDK installation.
Thus, JDK is installed in directory /usr/java/jdk1.6.0_12. At the same time, a link /usr/java/default pointing the directory /usr/java/jdk1.6.0_12 is generated automatically, equivalent to JDK is installed in directory /usr/java/default.
3. Configure JDK for Firefox
On the Linux operating system, execute the following commands:
cd /var/local/firefox/plugins/
lsp -s /usr/java/default/jre/plugin/i386/ns7/libjavaplugin_oji.so

After executing the commands above, you can run /var/local/firefox/firefox to access IMC.
In Linux, the current system time in IMC (such as the login time and operation log record time) is different from that on the server, and the difference may be several hours. How to solve the problem?

This is 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 edition, the IMC background processes cannot be started. How to solve the problem?

Before installing IMC in Windows Server 2003 64-bit OS, you must first install the WindowsServer2003-KB942288-v4-x64.exe patch. Otherwise, part of IMC processes cannot start after installation and deployment.

When this problem has occurred, fix the problem as follows: stop IMC, install the patch mentioned above, and then manually execute "IMC installation path\deploy\components\server\vcredist.exe."

When IMC database is installed on a remote database server (Windows Server 2008 or Windows Server 2008 R2), how to solve the abnormality occurred during the deployment process?

This is because the user that enabled the SQL Server on the remote database server is not assigned the write access to the IMCdata folder in the IMC installation path.

To solve the problem, manually change the access right of the IMCdata folder on the remote database server.

During the component deployment process, an error message “Deployment is stopped with error. For details, see the log.” appears, and “Execute database script error!” is displayed in the system log. Then check the specified log file according to the prompt information, and only the error information that the object dbo.qv.id already exists is displayed. How do I solve the problem?

Log in to the Query Analyzer of SQL Server as an sa user, and then execute the following commands:

```sql
use model
EXEC sp_droptype 'qv_id'
```

Then, deploy the component again.

When installing IMC on a PC running Windows Server 2008 R2, the system indicates the Windows Installer cannot be installed, as shown in the following figure. How do I solve this problem?

On the Windows Installer dialog box, click Browse. On the dialog box for selecting a file, search any folder whose name contains digits and letters abcdef in the root directory, select file vc_red.msi in the folder, and click OK. Then, you can continue the installation.

In Linux, how can I solve the problem that the JavaService is closed when Xwindows is closed?

Use `service IMCdmsd start` to start the JavaService.
The report cannot work properly when IMC adopts distributed deployment in Linux with the service components deployed on subordinate servers, and the master server uses Oracle database on a remote database server. What to do to solve the problem?

1. Check the configuration files in `\common\conf\server-addr.xml` of the IMC installation path, and the database names of the components on the subordinate servers.

Take the following environment for example:

The master server is at 192.168.0.1, and the database server is at 192.168.0.100. Deploy UAM component on server A at 192.168.0.2, and deploy WSM components on server B at address 192.168.0.3.

Run the `server-addr.xml` file to view the following information:

```xml
<component address="127.0.0.1" id="IMC-PLAT">
  <db-config address="192.168.0.100" dbname="192_168_0_100" oracle-sid="orcl"
    password="-105-61-35-5-31-10-226-222-232-161-198-206-190" type="Oracle"
    username="IMC_config"/>
</component>
......
<component address="192.168.0.2" id="IMC-UAM">
  <db-config address="192.168.0.2" dbname="192_168_0_2" oracle-sid="orcl"
    password="-105-61-35-5-31-10-226-222-232-161-198-206-190" type="Oracle"
    username="ead"/>
</component>
......
<component address="192.168.0.3" id="IMC-WSM">
  <db-config address="192.168.0.3" dbname="192_168_0_3" oracle-sid="orcl"
    password="-105-61-35-5-31-10-226-222-232-161-198-206-190" type="Oracle"
    username="IMC_wsm"/>
</component>
</component>
```

The configuration information shows that the database names of the components deployed on server A and server B are 192_168_0_2 and 192_168_0_3.

2. Check the `SORACLE_HOME/network/admin/tnsnames.ora` file on the master server, and the configuration of the databases 192_168_0_2 and 192_168_0_3.

```
192_168_0_2 =
(DESCRIPTION =
 (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.0.2)(PORT = 1521))
 (CONNECT_DATA =
  (SERVER = REMOTE)
  (SERVICE_NAME = orcl))
 )
......
192_168_0_3 =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.0.3)(PORT = 1521))
 )
 (CONNECT_DATA =
```
3. Use vi to run the $ORACLE_HOME/network/admin/tnsnames.ora file on the database server 192.168.0.100 to check whether the above configuration exists. When not, add the above configuration to the file.

On Windows, IMC service processes cannot be started or stopped after IMC runs for a certain period of time. How to solve the problem?

This problem is caused by insufficient virtual memory. Set the virtual memory to the system managed size on the server.

Follow these steps to set the virtual memory to the system managed size:

1. On the server, open the Control Panel window, and click the System icon. The System Properties dialog box appears, as shown in Figure 102.

![Figure 102 System properties](image)

2. Select the Advanced tab, and click Settings in the Performance area. Then the Performance Options dialog box appears, as shown in Figure 103.
3. On the **Performance Options** dialog box, select the **Advanced** tab, and click **Change** in the **Virtual memory** area. Then the **Virtual Memory** dialog box appears, as shown in Figure 104.

Figure 104 Virtual memory

4. Select the **System managed size** option, click **Set**, and then click **OK**.
After an error occurs in deployment or upgrade of a component, the component remains to be in Deploying or Upgrading state in the IMC Intelligent Deployment Monitoring Agent on the master server. How to solve the problem?

IMC does not actively refresh the component states. To view the latest state of the component:

1. Stop the IMC Intelligent Deployment Monitoring Agent and quit the program.
2. Restart the H3C iMC server service.
3. Open and start the IMC Intelligent Deployment Monitoring Agent on the master or subordinate server.

When a subordinate server is faulty and cannot be rectified, how to handle the components that are deployed on the server?

You can undeploy the components from the faulty subordinate server and deploy them to an available subordinate server. To do that:

1. Open the IMC Intelligent Deployment Monitoring Agent on the master server and click the **Deploy** tab.
2. Right-click a target component and then select **Undeploy the Component (Master only)** from the shortcut menu. This option appears only when the master server cannot connect to one or multiple subordinate servers. Repeat this step to undeploy more components.
3. Deploy the components to another subordinate server.

The component data is deleted from the subordinate server when you undeploy the components. Make sure the subordinate server has a secure data backup or uses a remote database. Otherwise, the data is lost.
Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (when applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber’s Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see HP A-Series Acronyms.

Websites

- HP.com http://www.hp.com
Conventions

The following information describes the conventions used in this documentation set.

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 bold text. 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><img src="image" alt="WARNING!" /></td>
<td>Indicates that the failure to follow directions could result in bodily harm or death.</td>
</tr>
<tr>
<td><img src="image" alt="CAUTION" /></td>
<td>Indicates that failure to follow directions could result in damage to equipment or data.</td>
</tr>
<tr>
<td><img src="image" alt="IMPORTANT" /></td>
<td>Provides clarifying information or specific instructions.</td>
</tr>
<tr>
<td><img src="image" alt="NOTE" /></td>
<td>Provides additional information.</td>
</tr>
<tr>
<td><img src="image" alt="TIP" /></td>
<td>Provides helpful hints and shortcuts.</td>
</tr>
</tbody>
</table>

Port numbering in examples

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

acronyms list, 126
activating IMC, 104
Android client, 58
   installing, 58
   using, 58
anti-virus software, 107
application scenario, 13
backing up IMC, 84
backup and restore, 108
centralized deployment, 11
centralized mode
   backup and restore, 114
   embedded database, 33
   removing IMC, 96
   user-supplied database, 29
centralized server deployment, 43
configuration guidelines, 118
contacting HP, 126
custom installation, 23
database
   backup and restore, 108
   backup and restore on backup server cluster, 114
   backup in distributed mode, 113
Dbman, 108
deploying IMC, 18, 29
   components, 34
   methods, 17
   preparation, 8
   prerequisites, 12, 43
   service components, 35
deployment and upgrade options, 26
DHCP plug-ins, 51
distributed deployment, 11
distributed mode
   database backup and restore, 113
   Oracle or MySQL database, 12
   prerequisites, 12
   removing IMC, 96
embedded database, 33
enterprise edition, 3
FAQs, 119
Firefox 3.6, 1
firewall recommendation, 107
first license registration, 98
hardware requirements, 5
HP Passport sign-in, 99
HP support websites, 126
IMC
   activating, 104
   backing up, 84
   components, 1
   editions, 3
   logging in, 61
   registering, 98
   removing, 95
   removing a component, 95
   restoring, 94
   uninstallation, 95
   upgrading, 89
   virtual machine installation, 8
IMC Platform
   deploying, 29
   installing, 18, 19
incremental node licenses, 103
installation
   custom, 11, 23
   plug-in, 51
   typical, 11, 19
Installation Summary, 27
installing
   DHCP plug-ins, 51
   IMC on a virtual machine, 8
   IMC Platform, 18, 19
   intelligent deployment monitoring agent, 47
   Java Runtime Environment, 14
methods, 17
preparation, 8
remote installation wizard, 44
service components, 35
VNM agent plug-ins, 53
Intelligent deployment monitoring agent, 22
Java Runtime Environment (JRE) installation, 14
license
  agreement, 25
  incremental node, 103
  registering for IMC, 98
  third party, 25
  upgrading to IMC v5.0, 105
license file, 106
Linux DHCP server, 52
logging in to IMC, 61
master server, 11
Microsoft Hyper-V server, 53
MS DHCP server, 51
MySQL database, 12
Network Traffic Analyzer
  centralized server deployment, 43
  deploying, 42, 48
  installing, 37
  subordinate servers deployment, 44
NTA. See Network Traffic Analyzer
NTP, 9
plug-in installation, 51
port numbers used by IMC components, 107
port settings, 107
preparing
  system time, 9
  time zone, 10
registering IMC, 98
remote installation wizard, 44
removing
  an IMC component, 95
  components at one time, 96
  IMC, 95
requirements
  deployment, 11
  hardware, 5
  installation, 11
  software, 7
restoring IMC, 94
server requirements, 5
  Linux, 6
  Windows, 5
service components, 1, 35
software requirements, 7
standard edition, 3, 18
subcomponents, 18
subordinate server, 11
Subscriber’s Choice for Business website, 126
superuser name, 24, 45
support, 126
system time, 9
technical support, 126
time zone, 10
typical installation, 19
uninstallation, IMC, 95
upgrading IMC, 89
  IMC V5.0 license, 105
  license file, 106
user-supplied database, 29
virtual machine installation, 8
VNM agent plug-ins, 53
web browser requirements, 1
websites, 126

for deploying IMC in distributed mode operations