Abstract
This document describes the processes and procedures to follow when deploying 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.
Legal and notice information

© Copyright 2013 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

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

## 1 Introduction to Intelligent Management Center
- IMC components ......................................................................................................................... 1
- IMC Platform ................................................................................................................................. 1
- Service components ....................................................................................................................... 1
- IMC editions .................................................................................................................................. 3
- Installation and deployment ........................................................................................................... 4
- Prerequisites for installing a remote database ............................................................................... 4
- Prerequisites for deploying IMC in distributed mode ................................................................. 6
- Installing Java Runtime Environment (JRE) .................................................................................. 7
- Obtaining IMC installation and deployment methods ................................................................. 8

## 2 Preparing for installation
- Hardware requirements ................................................................................................................ 9
- Software requirements ................................................................................................................ 11
- Setting the Java memory size on 32-bit OS ................................................................................. 12
- Installing IMC on a virtual machine .......................................................................................... 12
- Checking the installation environments ...................................................................................... 13
  - Checking installation environments ....................................................................................... 13
  - Superuser .................................................................................................................................. 15
- Checking the system time ............................................................................................................ 15
- Setting the time zone .................................................................................................................. 15

## 3 Installing SQL Server 2008 R2
- Installing the SQL Server 2008 R2 on database server ............................................................... 16
- Configuring TCP/IP properties for SQL Server 2008 R2 ............................................................. 38
- Installing the SQL Server client on IMC server ......................................................................... 41

## 4 Installing and deploying the IMC Platform
- Installing the IMC Platform ........................................................................................................ 50
- Deploying the IMC Platform ....................................................................................................... 57
  - Deploying the IMC Platform on the master server .................................................................. 57
  - Deploying the IMC Platform to a subordinate server ............................................................. 61
  - Deploying a single IMC Platform subcomponent ................................................................. 67
- IMC service logon accounts ....................................................................................................... 68

## 5 Installing and deploying IMC service components
- Installing IMC Network Traffic Analyzer (NTA) ........................................................................ 72
- Deploying IMC NTA ..................................................................................................................... 76
  - Deploying to master server ....................................................................................................... 76
  - Deploying to subordinate servers ........................................................................................... 77

## 6 Installing plug-ins
- Installing plug-ins ....................................................................................................................... 80
  - On the MS DHCP server .......................................................................................................... 80
  - On the Linux DHCP server ....................................................................................................... 81
- Installing VNM agent plug-ins .................................................................................................... 82
  - Installing a VNM Windows agent ............................................................................................ 82
  - Installing a VNM Linux agent .................................................................................................. 83
- Installing Android clients .......................................................................................................... 87
- Installing LLD P agent plug-ins ................................................................................................ 88
- Installing an LLD P Linux agent ................................................................................................. 88
1 Introduction to Intelligent Management Center

To meet the ever-increased server and database performance requirements for managing large networks, HP recommends that you deploy IMC in distributed mode and use a remote dedicated database server. This scheme is applicable to managing networks of more than 1000 users and 500 to 15000 devices.

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
- General Search Service Management
- 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:

- **Application Manager (APM)**—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
o Application servers
o Web servers
o Databases
o Network services
o Systems

• **VAN Connection Manager (VCM)**—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 VCM 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.

• **IPsec VPN Manager (IVM)**—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 (MVM)**—Provides topology discovery for BGP/MPLS VPNs, status/performance monitoring, fault location, and service deployment.

• **Network Traffic Analyzer (NTA)**—Network Traffic Analyzer simplifies bandwidth usage monitor on enterprise networks and provides easy-to-understand reports.

• **QoS Manager (QoSM)**—Manages QoS configurations on network devices to control and manage QoS for the overall network.

• **Remote Site Manager (RSM)**—Remotely manages branch networks that might be isolated by firewalls or NAT devices, and greatly reduces the network management costs by eliminating the need to deploy network management software and IT staff on each branch.

• **Service Health Manager (SHM)**—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 (SOM)**—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 (UAM)**—Provides the following features:
  o **Access user management**—Uses centralized mode and is integrated with device and topology management.
  o **Access and admission control**—Authenticates and authorizes the use of access services, and cooperates with user management and network resource management to provide enhanced access service management.

• **User Behavior Auditor (UBA)**—For increasingly complex service application environments and more network facilities, User Behavior Auditor provides a simple, efficient log auditing tool to help operators quickly and accurately view the network access information to locate problems.

• **Wireless Service Manager (WSM)**—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.

- **Branch Intelligent Management System (BIMS)**—Allows remote monitoring and management of the two types of devices that cannot be managed through SNMP or Telnet:
  - Devices that use dynamic IP addresses.
  - Devices that are located behind the NAT gateways.

Branch Intelligent Management System provides a cost-effective and efficient solution to manage large numbers of geographically dispersed devices that have similar service requirements.

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:

- Resource Management
- NE Management
- Report Management
- Security Control Center
- Virtual Network Management

**IMC editions**

Three editions of IMC are available:

- Enterprise
- Standard
- Basic

**Table 1 Differences between IMC editions**

<table>
<thead>
<tr>
<th>Item</th>
<th>Basic</th>
<th>Enterprise</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>1000</td>
<td>Extensible</td>
<td>Extensible</td>
</tr>
<tr>
<td>Hierarchical Network Management</td>
<td>Not supported</td>
<td>Supported</td>
<td>Lower-level NMS only</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows</td>
<td>Windows and Linux</td>
<td>Windows and Linux</td>
</tr>
<tr>
<td>Distributed deployment</td>
<td>Not supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Embedded database</td>
<td>Supported</td>
<td>Not supported</td>
<td>Supported only on windows</td>
</tr>
<tr>
<td>Remote database server</td>
<td>Not supported</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
• SQL Server 2012 Installation and Configuration Guide
• MySQL 5.5 Installation and Configuration Guide (for Windows)
• MySQL 5.6 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)
• MySQL 5.6 Installation and Configuration Guide (for Linux)

Installation and deployment

To improve the server performance, IMC uses the "Install + 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.

In IMC distributed deployment, first install the IMC Platform to the master server, and then deploy the service components to the master server or subordinate servers as needed. The master server is the management center of IMC. It interacts with subordinate servers to implement network management. A subordinate server is responsible for specific management tasks, for example, tasks performed by Performance Manager and by Intelligent Configuration Center.

IMPORTANT:
Use the same operating system bit count (32 or 64) on the master and subordinate servers when you deploy IMC in distributed mode.

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 "7 Logging in to IMC."

IMC automatically creates a database user when a service component is deployed. HP recommends not modifying 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.

Prerequisites for installing a remote database

You can store IMC data on a remote database server. In distributed deployment, the remote 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 dedicated database server.

To use a separate Oracle database, follow these guidelines:
• Install the Oracle client on master 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 master 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.
  To do that:
  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. 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.
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 databases for Windows. You can use Oracle and MySQL databases for Linux. When you use Oracle, the master and subordinate servers cannot use the same database instance name.

- Components required to be deployed on the master server:
  The following components of the IMC Platform must be deployed on the master server:
  - NE Management
  - Report Management
  - Resource Management
  - Security Control Center
  - Virtual Network Management
  For more information about 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.

## 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:**
  1. Run the JRE 6.0 setup in the IMC package as follows:
  2. 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) in the address bar, where 192.168.4.44 is the IP address of the master server, and 8080 is the Web service port of IMC.
  3. b. On the login page, enter the username and password.
  4. c. Click Login to enter the Home tab.
  5. d. Select the System tab and click Deploy Components.
  6. e. Click When fail to start Remote Installation Wizard, download and install JRE.
  7. f. In the popup jre.exe file download window, click Save or click Run.

⚠️ IMPORTANT:

- Make sure you have installed a 64-bit browser and 64-bit JRE on Windows Server 2008 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 "12 FAQ."
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 2008 R2.

The IMC software is available on the HP website.
2 Preparing for installation

This chapter describes the requirements that all the candidate IMC servers must meet for IMC distributed deployment.

HP recommends using a 64-bit operating system on the master server and all subordinate servers.

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

- **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>0 to 200</td>
<td>0 to 5 K</td>
</tr>
<tr>
<td></td>
<td>5 K to 50 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</strong></td>
<td><strong>Collection unit</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</strong></td>
<td><strong>Collection unit</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</strong></td>
<td><strong>Collection unit</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>
</tbody>
</table>
### Software requirements

IMC runs on Windows or Linux. When running on Windows, IMC stores and manages data through SQL Server. When running on Linux, IMC stores and manages data through Oracle or MySQL.

To ensure correct operation of IMC, install the operating system, database, and IMC software correctly.

**Table 6 Software requirements**

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Window Server 2003 (32bit)</td>
<td>Service Pack 2 is required.</td>
</tr>
<tr>
<td></td>
<td>Window Server 2003 (64bit)</td>
<td>Service Pack 2 (64-bit) and KB942288 are required.</td>
</tr>
<tr>
<td></td>
<td>Window Server 2003 R2 (32bit)</td>
<td>Service Pack 2 is required.</td>
</tr>
<tr>
<td></td>
<td>Window Server 2003 R2 (64bit)</td>
<td>Service Pack 2 (64-bit) and KB942288 are required.</td>
</tr>
<tr>
<td></td>
<td>Window Server 2008 (32bit)</td>
<td>Service Pack 2 is required.</td>
</tr>
<tr>
<td></td>
<td>Window Server 2008 (64bit)</td>
<td>Service Pack 2 (64-bit) is required.</td>
</tr>
<tr>
<td></td>
<td>Window Server 2008 R2</td>
<td>Service Pack 1 is required.</td>
</tr>
<tr>
<td></td>
<td>Window Server 2012 (64bit)</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2008 R2</td>
<td>Service Pack 2 is required for SQL Server 2008 R2.</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2012</td>
<td>Service Pack 1 is required for SQL Server 2012</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2008 R2 SP2 Express</td>
<td>These databases can be used for both Standard and Professional editions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Make sure the latest database service packs are installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The database is the embedded database of Standard and SNS editions.</td>
</tr>
<tr>
<td>Item</td>
<td>Requirement</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td>MySQL 5.5</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>MySQL 5.6</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**Operating system**

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Requirement</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Professional Linux Server 5 (32bit)</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Red Hat Professional Linux Server 5 (64bit)</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Red Hat Professional Linux Server 5.5 (32bit)</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Red Hat Professional Linux Server 5.5 (64bit)</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Red Hat Professional Linux Server 6.1</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Red Hat Professional Linux Server 6.4</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**Database**

<table>
<thead>
<tr>
<th>Database</th>
<th>Requirement</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 11g</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Oracle 11g Release 2</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>MySQL 5.5</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>MySQL 5.6</td>
<td>None</td>
<td></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

HP recommends installing IMC on physical servers.
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

This example describes how to install Microsoft SQL Server 2008 R2. For instructions on installing databases of other versions, see the installation guides of the databases.

Before installation, make sure all the requirements listed in Table 7 are met.

⚠️ **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 the operating system and database meet the IMC installation requirements as described in &quot;Software requirements.&quot; The server is restarted after database installation.</td>
</tr>
<tr>
<td><strong>Auto startup of SQL Server service and SQL Server Agent</strong></td>
<td>Select Control Panel &gt; Administrative Tools &gt; Services and make sure the Startup Type items of MSSQLSERVER and SQLSERVERAGENT are set to Automatic.</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, make sure the IMC Web service ports and database listening port are open on the master server. The default Web service ports are 8080 (HTTP) and 8443 (HTTPS). The default database listening port is as follows:
  
  - SQL server database: 1433
  - Oracle database: 1521
  - MySQL database: 3306 |
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.

Superuser

IMC installation requires you to enter a superuser account to test the database connectivity. You can use the default superuser account sa (for SQL Server) 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.

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 2008 R2 operating system, deselect automatically adjust clock daylight saving changes when you set the time zone in the Date & Time window.
3 Installing SQL Server 2008 R2

To deploy IMC in distributed mode and use a remote database, you must install and configure the SQL server on database server, and then install the SQL Server client on IMC server. This chapter first describes how to install and set up SQL Server 2008 R2 on the database server, and then describes how to install SQL Server 2008 R2 client on IMC server. For instructions on installing other databases, see the related documents.

Installing the SQL Server 2008 R2 on database server

1. Run the setup program.

   The SQL Server Installation Center window appears.

2. Select Installation from the navigation tree, and click **New installation or add features to an existing installation**.

   The Setup Support Rules page appears.

   The system runs a check to identify problems that might occur when you install SQL Server Setup support files.
Figure 3 Setup Support Rules page

3. After the check is passed, click OK.
   
   The **Product Key** page appears.
4. Enter the product key and click **Next**.
   The **License Terms** page appears.
5. Select I accept the license terms and click Next.

The Setup Support Files page appears.
6. Click **Install** to start installing setup support files. The **Setup Support Files** page appears.
Upon completion of the installation, the **Setup Role** dialog box appears.
7. Select **SQL Server Feature Installation** and click **Next**.

The **Feature Selection** page appears.
8. Select the features you want to install and click Next. The Installation Rules page appears.
9. Click Next.

   The Instance Configuration page appears.
10. Select **Default instance** and use the default instance **MSSQLSERVER**. Do not modify the default instance ID.

An advanced user can select **Named instance** and enter a custom instance ID. For more information about the installation procedure, see *SQL Server 2008 R2 Installation and Configuration Guide*.

11. Click **Next**.

The **Disk Space Requirements** page appears.
Figure 12 Disk Space Requirements page

12. Click **Next**.

   The **Server Configuration** page appears.
13. Click **Use the same account for all SQL Server services.**

The **Use the same account for all SQL Server 2008 R2 services** page appears.

**Figure 14 Use the same account for all SQL Server 2008 R2 services page**

Specify a user name and password for all SQL Server service accounts.

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT AUTHORITY\SYSTEM</td>
<td></td>
</tr>
</tbody>
</table>

14. Specify the account name and password, and click **OK** to go back to the **Server Configuration** page.
15. Click the **Collation** tab.
16. Use the default settings and click **Next**.

The **Database Engine Configuration** page appears.
17. In the **Authentication Mode** area, select **Mixed Mode**, and set the password for user \texttt{sa}, and add a SQL Server administrator.

SQL Server 2008 R2 has password complexity requirements. For information, see the online help on SQL Server 2012.

For IMC to correctly identify the \texttt{sa} logon password during installation, make sure the password does not contain any of the following characters: left bracket (<), right bracket (>), vertical bar (|), and \textbackslash (\).

If you do not want to change the password of the \texttt{sa} user, create a user with \texttt{sa} user privileges and make sure the password does not contain any of the previous characters. For more information about creating a database user, see SQL Server 2008 R2 Installation and Configuration Guide.
18. Use the default settings of the **Data Directions** (Figure 19) and the **FILESTREAM** tab (Figure 20).
Figure 19 Data Directories tab page
19. Click **Next**.

The **Error Reporting** page appears.
20. Click **Next**.

The **Installation Rules** page appears.
21. Click **Next**.

The **Ready to Install** page shows a tree view of installation options that were specified during Setup.
22. To continue, click **Install**. The **Installation Progress** page appears.
23. After installation, the **Complete** page provides a link to the summary log file for the installation and other important notes, as shown in **Figure 25**.

24. Click **Close**.
Configuring TCP/IP properties for SQL Server 2008 R2

After you finish the database installation, configure the TCP/IP properties for the database.

1. Select Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager, as shown in Figure 26.

   The SQL Server Configuration Manager page appears, as shown in Figure 27.
2. In the **SQL Server Configuration Manager** window, select **SQL Server Network Configuration > Protocols for MSSQLSERVER** from the navigation tree, and double-click **TCP/IP** on the main pane, or you can select **TCP/IP** and click the **Properties** icon on the toolbar. The **TCP/IP Properties** dialog box appears.

![Figure 27 SQL Server Configuration Manager window](image.png)

![Figure 28 Configuring TCP/IP properties](image.png)

3. On the **Protocol** tab, make sure **Yes** is selected for **Listen All**.
4. Click the **IP Address** tab, select **Yes** for the **Enabled** option of each IP address, and set **TCP Port** to 1433 (the default setting). Make sure the **TCP Dynamic Ports** field is null for IPAll and each IPn (such as IP1, IP2, IP3, etc), as shown in Figure 29.

You can also specify another TCP port, but you must make sure the specified **TCP Port** has not been used by any other instances and application.

**Figure 29 Configuring IP addresses for TCP/IP**

5. Click **OK** to save the configuration.

The following message appears:

*Any changes made will be saved; however, they will not take effect until the service is stopped and restarted.*

6. Click **OK**.

Restart the SQL server to validate the configuration.

**NOTE:**

- If you did not select **Yes** for **Listen All** on the **TCP/IP Properties** dialog box, enter the dialog box to update the previously-configured IP addresses if the server IP address changes after installing SQL Server 2008 R2. Otherwise, you cannot connect to the database.
- The master and subordinate servers must use the same listening port.
Installing the SQL Server client on IMC server

This chapter describes how to install the SQL Server client on an IMC server. Make sure the client version matches the SQL server version.

1. On the **Feature Selection** dialog box, select client components, as shown in Figure 30. See "Installing the SQL Server 2008 R2 on database server" for how to enter the Feature Selection dialog box.

**Figure 30 Feature Selection dialog box**

2. Select the features (Management Tools – Basic and SQL Client Connectivity SDK) shown in Figure 31, and click **Next**.
3. Click **Next**.

   The **Disk Space Requirements** dialog box appears.
4. Click **Next** and proceed to configure error report settings.
5. Use the default setting on the dialog box, and click **Next**.

The **Installation Configuration Rules** dialog box appears.
6. Click **Next**.

   The **Ready to Install** dialog box appears.
7. Confirm the installation information, and click **Install** to start installing SQL Server 2008 R2 client and to enter the **Installation Progress** dialog box.
The components installed are relevant to the features selected previously. When the installation process is complete, the **Complete** dialog box appears.
8. Click Close to close the Complete dialog box.

After the SQL Server client is installed, you can verify whether or not it can connect to the SQL server.

To test the connectivity between the SQL Server client and the SQL server:

9. Select Run from the Start menu, and enter cmd in the Run dialog box.

10. In the CMD window, enter either command:
    - For the default instance:
      `osql -h172.8.9.63 -Usa -PiMC123`
    - For a custom instance:
      `osql -h172.8.9.63\instancename -Usa -PiMC123`

In the previous commands, **172.8.9.63** is the IP address of the SQL server, **sa** and **iMC123** are the username and password of the default superuser, and **instancename** represents the name of the custom instance.

If the SQL command prompt appears, you have successfully connected to the SQL server and entered the SQL command mode.
Figure 38 Testing connectivity
After each IMC server is installed with the SQL Server client, you can start to install the IMC Platform on the master server and deploy the IMC Platform subcomponents on the master and subordinate servers as needed.

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>Master server</td>
<td></td>
</tr>
<tr>
<td>Alarm Management</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td>Guest Access Management</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td>Performance Management</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td>Network Asset Management</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td>ACL Management</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td>Intelligent Configuration Center</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td>NE Management</td>
<td>Master server</td>
<td></td>
</tr>
<tr>
<td>Report Management</td>
<td>Master server</td>
<td></td>
</tr>
<tr>
<td>General Search Service Management</td>
<td>Master server</td>
<td></td>
</tr>
<tr>
<td>Security Control Center</td>
<td>Master server</td>
<td></td>
</tr>
<tr>
<td>Syslog Management</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td>VLAN Management</td>
<td>Master server</td>
<td></td>
</tr>
<tr>
<td>User Selfservice Management</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td>Virtual Network Management</td>
<td>Master server</td>
<td></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 39, 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.
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 39 Select Locale (on Windows Server 2008 R2)

4. In Figure 39, select the country or region, language, and installation type. IMC supports typical and custom installation.
   - **Typical installation**—Allows you to quickly install and deploy all platform subcomponents 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 subcomponents 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.

To deploy IMC in distributed mode and to use a remote database, select the Custom installation mode and click OK.

The Checking Database Connectivity window appears.
5. 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 for connecting to the remote database address.
     This parameter appears only when you are installing IMC on Linux that uses an Oracle database. 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 other server, specify the server IP address and enter the superuser name and password for the specified database server.
6. Click OK.
   The system starts to check the database connectivity. When the check is passed, the Welcome to HP iMC Installation Wizard window appears.
7. Click Next.
   The Agreement window appears.

8. Read the license agreement and third party license and select Accept.

9. Click Next.
    The Choose Target Folder window appears.
The **Choose Target Folder** window displays the subcomponents.

10. Select the subcomponents 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 subcomponents that you want to install. These subcomponents include Resource Manager, NE Management, Alarm Management, and Performance Management.

11. Click **Next**.

    The **Deployment and Upgrade Options** window appears.
12. Select an option as needed. This example uses Deploy or upgrade later.

13. Click Next.

The Installation Summary window appears.

Figure 45 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

14. Click Install.

The Installing common components window appears.
The wizard shows the process of component installation. After the installation is complete, the **Installation Completed** window appears.

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 "5 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

Deploying the IMC Platform on the master server

1. After installation, in the window shown in Figure 47, select **Open deployment monitoring agent** and click **Finish**. The system automatically starts the Intelligent Deployment Monitoring Agent. For the first deployment, a **Batch deploy** window appears.

**Figure 48 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 subcomponents to be deployed by default include:

- Alarm Management
- Intelligent Configuration Center
- NE Management
- Performance Management
- Report Management
- Resource Management
- Network Asset Management
- Security Control Center
- User Self-service Management

Optional subcomponents include:

- ACL Management
- General Search Service Management
- Guest Access Manager
- Syslog Management
- Virtual Network Management
VLAN Management

You can also select the subcomponents to be deployed as needed, except that the Resource Management subcomponent is required. In this configuration example, select the following subcomponents:

- Alarm Management
- Intelligent Configuration Center
- NE Management
- Performance Management
- Report Management
- Resource Management
- Network Asset Management
- Security Control Center
- User Self-service Management

3. Click **OK**.

   The **Database Configuration Info** window appears.

   **Figure 49 Database Configuration Info**

   ![Database Configuration Info](image)

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

   5. Select the location for saving data files. 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. IMC checks whether or not the folder path exists and is accessible on the database server. If the path is invalid, IMC quits the deployment. Then you must create the data file folder on the database server and restart the deployment.

   6. Select a path to save the data files and click **Next**.

   The **Configure Web Service Port** window appears.
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 the specified ports are open in the system firewall on the IMC master server and are not being used by another service.

8. Click **Deploy**.

   The *Deploying* window appears.

**Figure 51 Deploying IMC subcomponents**

After the deployment, the **Batch deploy succeeded** window appears.
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.

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

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 54.

   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 the IMC Platform to a subordinate server

After the deployment on master server is completed, you can deploy IMC subcomponents to subordinate servers.

If you deploy IMC subcomponents to subordinate servers for the first time, install the Intelligent Deployment Monitoring Agent on each subordinate server. IMC allows you to launch the remote installation wizard through the IMC installation DVD (recommended) or the IE browser. If 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 a subordinate server, run the installslave.bat script in the install directory of the IMC installation DVD. The Address of Master window appears.
   
   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.

2. Type the IP address of the master server, and click OK.
The Checking Database Connectivity window appears.

**Figure 56 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) and password.
   - 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 the icon to add a network service name for connecting to the remote database address.
   - This parameter appears only when you install IMC on Linux to use an Oracle database. For more information about the network service name configuration, see Oracle 11g Installation and Configuration Guide or Oracle 11g R2 Installation and Configuration Guide.
   - Select other server, specify the server IP address and enter the superuser name and password for the specified database server.

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

**Starting the remote installation wizard through IE**

1. On a subordinate server, launch the IE 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 service port number set during IMC deployment.

   The IMC login page appears.

2. Enter the username and password, and then click Login. The username and password of the super user for the system are both admin.

   The Home tab appears.

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.

**Figure 57 Whether to launch the Intelligent Deployment Monitoring Agent**

<table>
<thead>
<tr>
<th>Windows Internet Explorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you sure to launch Deployer Monitor Agent?</td>
</tr>
<tr>
<td><strong>OK</strong></td>
</tr>
</tbody>
</table>

6. Click **OK**.

The **Downloading application** dialog box appears, 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 58 Downloading application**

<table>
<thead>
<tr>
<th>Java Web Start</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downloading application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name:</th>
<th>Deployer Monitor Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publisher:</td>
<td>Hangzhou HOC Technologies Co., Ltd.</td>
</tr>
<tr>
<td>From:</td>
<td><a href="http://192.168.1.140:8080">http://192.168.1.140:8080</a></td>
</tr>
</tbody>
</table>

After the Java file is downloaded and installed, the **Choose Target Folder for Deployment** dialog box appears, as shown in **Figure 59**.

**Installing the Intelligent Deployment Monitoring Agent**

After successfully starting the remote installation wizard, you can start to install the deployment monitoring agent.
As shown in Figure 59, the default deployment location is C:\Program Files\iMC (or in /opt/iMC on Linux). To deploy IMC in another location, either type a path or click Browse to select another path.

1. After selecting a deployment location, click Install to start file downloading.

   After the files are downloaded, the Installation Completed dialog box appears.

2. Click Finish.
Deploying the IMC Platform subcomponents

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. The Deploy tab displays information about all IMC components that have been installed.

Figure 61 Information about component deployment

![Component Deployment Information](image)

3. Right-click any platform subcomponent that has not been deployed, and then select Batch Deploy from the shortcut menu.

The Batch deploy window appears.
4. In the **Batch deploy** window, select the subcomponents as needed and click **OK**. The system starts downloading the files. After downloading is complete, the **Database Configuration Info** window appears.

5. Enter the password for the user **sa** for the current database, which is the superuser name specified during installing IMC, and select a data file location.
By default, IMC saves the data file in C:\Program Files\imcdata. You can also click Browse to select another location.

6. 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 76.

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.

7. Click Deploy to start the deployment.

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

8. Click OK.

9. After successfully finishing the deployment, select the Deploy tab in the Intelligent Deployment Monitoring Agent.

Figure 64 Information about component deployment

10. 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).

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

12. Click OK.

After all processes start, IMC is ready for use.

Deploying a single IMC Platform subcomponent

To deploy a single IMC component, use either of the following methods in the window, as shown in Figure 53.
• Method 1:
  Right-click the target component and select **Deploy the Component** from the shortcut menu.

• Method 2:
  a. Select any target component and select **Batch deploy** from the shortcut menu.

  The **Batch deploy** dialog box appears.

  b. Select the component and 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.

**IMC service logon accounts**

By default, the IMC system service **HP 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.
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:
- Application Manager
- Branch Intelligent Management System
- EAD Security Policy
- iNode Dissolvable Client
- IPsec VPN Manager
- MPLS VPN Manager
- Network Traffic Analyzer and User Behavior Auditor
- QoS Manager
- Remote Site Manager
- Service Health Manager
- Service Operation Manager
- User Access Manager
- VAN Connection Manager
- Voice Service Manager
- Wireless Service Manager

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>Application Manager</td>
<td>Application Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>VAN Connection Manager</td>
<td>VAN Connection Manager</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td>BIMS</td>
<td>BIMS - Branch Intelligent Management System</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>BIMS - Auto-Configuration Server</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Mobile Branch Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>EAD Security Policy</td>
<td>Security Policy Configuration</td>
<td>Master and subordinate servers</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>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>IPsec VPN Manager</td>
<td>IPsec VPN Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></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></td>
<td></td>
<td></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></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>L2VPN Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Traffic</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Analyzer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Traffic</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Analyzer Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Behavior</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Analyzer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Behavior</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Analyzer Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS Manager</td>
<td>QoS Management</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Site Manager</td>
<td>Remote Site Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Operation Manager</td>
<td>CMDB Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>Service Health Manager</td>
<td>Service Desk</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Health</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NQA Collector Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Behavior Auditor</td>
<td>User Behavior Auditor</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td>User Behavior Auditor</td>
<td>Master and subordinate servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Behavior</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Analyzer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Behavior</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Analyzer Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Access Manager</td>
<td>User Access Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Portal Web Server and</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Portal Proxy</td>
<td></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>Portal Server</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
<td>Set the <strong>Portal Server IP Address</strong>, 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>Policy Server</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
<td>Set the <strong>Policy Server IP Address</strong>, which is the IP address of the network adapter providing services externally of the server where the policy server component is deployed.</td>
</tr>
<tr>
<td>Policy Proxy Server</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
<td>Set the <strong>Policy Proxy Server IP Address</strong>, which is the IP address of the network adapter providing services externally of the server where the policy proxy server component is deployed.</td>
</tr>
<tr>
<td>User SelfService</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
<td>Set the <strong>User SelfService IP Address</strong>, which is the IP address of the network adapter providing services externally of the server where the user selfservice component is deployed.</td>
</tr>
<tr>
<td>Desktop Asset Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
<td>Set the database password (defaults to <code>IMC5_uamead</code>), and the <strong>DAM Server IP Address</strong>, which is the IP address of the network adapter providing services externally of the server where DAM is deployed.</td>
</tr>
<tr>
<td>Desktop Asset Manager Proxy Server</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
<td>Set the <strong>DAM Proxy Server IP Address</strong>, which is the IP address of the network adapter providing services externally of the server where the DAM proxy server component is deployed.</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. This section takes the installation of NTA as an example.
Installing IMC Network Traffic Analyzer (NTA)

1. In the Installation Completed window (see Figure 47), select the Install other iMC Components box.
2. Click Finish to enter the Choose folder dialog box.

Figure 65 Choose folder

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.
- 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 welcome window appears to guide you through the IMC installation.

Figure 66 Welcome to HP IMC Installation Wizard

6. Click Next.

The Agreement window appears.
7. Read the license agreement and third party license and select **Accept**.

8. Click **Next**.

   The **Choose Target Folder** window appears.

   **Figure 68 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.
10. Select an option as needed. This example uses **Deploy or upgrade later**.
11. Click **Next**.
   
   The **Installation Summary** window appears.

**Figure 70 Installation Summary**

12. After confirming the related installation information, click **Install**.
   
   The **Installing** window appears.
The wizard is installing the component. After the installation is finished, the **Installation Completed** window appears.

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.


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 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 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 the IMC Platform on the master server."

- See Table 9 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 master 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 72, select Open deployment monitoring agent and then click Finish. Then the system automatically starts the Intelligent Deployment Monitoring Agent. A Batch deploy window appears at the same time, as shown in Figure 73.
You can also start the Intelligent Deployment Monitoring Agent by selecting:

a. 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).

b. Then the **Deploy** tab, selecting **Batch Deploy** from the right-click menu of the target components to start batch deployment.

**Figure 73 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. For more information, see “Deploying the IMC Platform to a subordinate server.”

To Deploying service components to subordinate servers:

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.
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.

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

The system starts the deployment.
After the deployment is finished, the **Batch deploy result** dialog box prompting **Batch deploy succeeded** appears.

5. Click **OK**.

6. After successfully finishing the deployment, select the **Deploy** tab in the Intelligent Deployment Monitoring Agent.

Figure 76 Information about component deployment

![Image of component deployment table]

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Description</th>
<th>Version</th>
<th>Status</th>
<th>Deployment Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligent Management</td>
<td>Manages network resources such as traffic...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Access Management</td>
<td>Monitors and troubleshoots network traffic...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>User Self-Monitor</td>
<td>Monitors the self-service business...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Access Management</td>
<td>Manages network access accounts...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>HP Monitoring</td>
<td>Manages network element availability...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Performance Management</td>
<td>Monitors and analyzes network performance...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>AG Management</td>
<td>Configures ACLs for devices...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Network Asset Management</td>
<td>Manages network assets...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Security Controller</td>
<td>Monitors network events and controls...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>General Site Services</td>
<td>Manages the general site service...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Snyder Management</td>
<td>Collects data about network traffic...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Virtual Network Management</td>
<td>Manages virtual networks...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Network Behavior Analyzer</td>
<td>Provides a basic configuration and management...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Traffic Analyzer Server</td>
<td>Receives network traffic data...</td>
<td>7.0</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
</tbody>
</table>

7. 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).

8. 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.

9. 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:
      ```bash
      vi qvdm.conf
      ```
   b. Add the following line to the file:
      ```bash
      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.
      ```bash
      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.
      ```bash
      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 server 2008 R2 SP1/2012 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 4.5, and PowerShell 3.0. 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 restart the installation process.

   Do not delete the vnm-plug-windows folder or the files in the folder after installation. It becomes the service registration path.

3. 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).

4. Save your settings and quit.

5. Start the IMC VNM 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, 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.

Figure 77 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.
• 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.

**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))
- glibc2.12-1.80.el6.i686.rpm
- nss-softokn-freebl-3.12.9-11.el6.i686.rpm
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**, 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 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 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 `host.txt` file with the `:wq` command.

f. Enter y when you see the following message:

```
Please add the target KVM to the ssh-key-tool/conf/new_host.txt(y/n):
```

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

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

h. Save the `new_host.txt` file with the `:wq` command.

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

i. 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 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 host.txt file with the :wq command.
f. Enter y when you see the following message:
Please add the target KVM to the ssh-key-tool/conf/new_host.txt(y/n):

g. Enter the username and the password of each new KVM server in the following format.
    ip:10.153.146.12 user:root passwd:imcimc

h. Save the new_host.txt file with the :wq command.
i. 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 update1 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 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 Programs from unknown sources are not allowed to install appears during installation, locate to Settings > Applications and 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 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 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 llap-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.

1 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 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 change the value.
   c. Restart the lldp-agent service.
7 Logging in to IMC

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 or 9
- Firefox 3.6 or later

Access methods

Before you log in the IMC, make sure the Web service ports of IMC are open in the firewall settings on the IMC master server. The default Web service ports of IMC are 8080 (HTTP) and 8443 (HTTPS).

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:
     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 the IMC login page appears.

2. Enter the username and password and 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.
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: 2 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 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 operations."
- Download the upgrade packages for all listed components before you upgrade the IMC Platform.

Backing up IMC

Because IMC uses a remote database in this example, you must back up the IMC installation directory and database files separately.

To back up the IMC installation directory, execute the `backup.bat` script that is located in the IMC installation package.

To backup the database files of a remote database, use `Dbman` in the Intelligent Deployment Monitoring Agent. Dbman cannot back up the IMC installation directory. For more information, see "Basic database backup and restore operations."

If IMC is deployed in stateful failover mode, back up IMC by executing the `backup.bat` script only on the active servers.

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 80.

⚠️ CAUTION:

- To back up IMC in Windows Server 2003 or Windows Server 2003 R2, you must log in as an administrator and 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 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 you 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 80** Backing 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.

**Figure 81** Choosing 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. In this example, the `db` folder is empty because a remote database is used.

**Backing 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.

Because in this example IMC is deployed in distributed mode, you must upgrade components deployed on the master server and subordinate servers, respectively.

The following describes how to upgrade the IMC Platform.

93
1. Use one of the following ways to start upgrade:
   - On the **Installation Completed** window, as shown in Figure 47, 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 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 upgrade IMC.
   - To upgrade IMC in Windows Server 2008 or Windows Server 2008 R2, you must first select **Start > All Programs > HP 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 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 you 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.

   **Figure 82 Choose folder**

   3. Click **Browse**, and select folder **install\components** in the upgrade files.
   4. Click **OK**.
   - The **Welcome to HP IMC Installation Wizard** window appears.
5. Click **Next**. The **Agreement** window appears.

**Figure 84 Agreement**

6. Read the license agreement carefully, select **Accept**, and click **Next**. The **Upgrade Common Components** window appears.
Figure 85 Upgrade Common Components

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

Figure 86 Upgrade Common Components

After the common components are upgraded, the Choose Target Folder window appears.
Choose Target Folder

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.

7. Check the information, click Next, and the Deployment and Upgrade Options window appears.

Deployment and Upgrade Options

8. 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.
9. Check the installation summary, click **Install**, and the **Installing** window appears.

**Figure 90 Installing**

The installation wizard installs the components.

**Upgrading IMC on master server**

After the installation is finished, the **Batch upgrade** window appears.
1. Select the components you want to upgrade and click **OK**.
   After the selected components are upgraded, the *Batch upgrade result* window appears.

2. Click **OK**.
   If you have used Dbman for IMC auto backup or restoration before upgrade, the *Auto Backup and Restore Configuration* window appears.
   Make sure Dbman has the latest configuration. Otherwise, update it. For more information, see “Updating Dbman for the database server.”
Upgrading IMC on subordinate servers

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

On the subordinate server, 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.

On the Deploy tab, select any component that has not been upgraded, right-click it, and select Batch Deploy from the shortcut menu.

The Batch deploy window appears, and then click Install new components on the Monitor tab.

Starting IMC after upgrading

After IMC is upgraded, 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.
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 95). The tool is used to upgrade the Oracle database configuration for communication between the master and subordinate servers.

Figure 94 Important message

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 an error occurs during the IMC upgrade, check the environment (for example, check whether the database is available) and upgrade IMC again. If the IMC upgrade still fails, follow these steps to restore IMC to the version before the upgrade:

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.

For IMC deployed in stateful failover mode, only restore IMC on the active servers.

Removing IMC

Removing IMC on Windows and Linux systems is similar. The following describes how to remove IMC from a Windows Server 2008 R2-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 subordinate server, remove it first from subordinate server 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 select **Undeploy the Component** from the shortcut menu.
   The Intelligent Deployment Monitoring Agent undeploys the selected component from the subordinate server.
3. 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.
4. Click **OK**.

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**.

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 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 a 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.

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.
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 2008 R2-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.

**Figure 95 License Information**

<table>
<thead>
<tr>
<th>License Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
</tr>
<tr>
<td>Product Number</td>
</tr>
<tr>
<td>Serial Number</td>
</tr>
<tr>
<td>Activate</td>
</tr>
</tbody>
</table>

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

**Registering first license**

2. Enter the **User ID** and **Password** and click **Sign in**.

The **Welcome** page appears.

---

**Figure 96 HP Passport sign-in**

2. Enter the **User ID** and **Password** and click **Sign in**.

The **Welcome** page appears.

---

**Figure 97 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.

**Figure 98 Enter Order number or Registration ID page**

4. Enter the **Order number** or **Registration ID**, and click **Next**.

   The **Enter the email associated with Order number** page appears.

**Figure 99 Enter the email associated with Order number page**

5. Enter an email address associated with the **Order number** and click **Next**.

   The **Select the Product License** page appears.
6. Select the product for which you want to register or activate a license.

7. Enter the quantity to be redeemed and click Next.
   The Enter details page appears.

8. Enter the Base software serial number and click Next.
   The License agreement page appears.
9. Read the license agreement, select I accept all of the above terms, and click Finish. The Confirmation page appears.

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 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.

   Figure 104 Select the Product License page

   ![Select the Product License page]

2. Click Next.
   
   The Enter details page appears.
3. Select your base product, enter the base software serial number, and click **Next**. The **Confirmation** page appears (see Figure 103).

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 (see Figure 96).
2. Select **Activate now**.
   The **Activate Your Product** page appears.

### Figure 106 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.
6. Reboot the system.

Your IMC system has now been successfully Registered and Activated.

**Upgrading to an IMC V7.0 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.


Your IMC license file has been updated in My Networking to support IMC V7.0.

You need to download your updated IMC license file from My Networking and reactivate your IMC V7.0.

To update your IMC license file from My Networking and reactivate your IMC V7.0:

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 \( \rightarrow \) 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 V7.0 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 V7.0 is now fully licensed with the equivalent licenses you had previously.
10 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 TFTP</td>
<td>IMC server</td>
</tr>
<tr>
<td>TCP 20, 21</td>
<td>Port for Intelligent Configuration Center to perform configuration management through FTP</td>
<td>IMC server</td>
</tr>
</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.

### Figure 108 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.

This example uses a remote database and you can use Dbman for automatic database backup and restoration.

### Installing Dbman on the database server

To back up or restore database files on a remote database server for IMC, you must set the Auto Backup and Restore Configuration on the IMC server, 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.

To install Dbman on database server:

1. Start the Intelligent Deployment Monitoring Agent on the local master or subordinate server.
2. Click the *Environment* tab as shown in Figure 108.
3. Click *Configure*.
   
   The *Auto Backup and Restore Configuration* dialog box appears.

#### Figure 109 Auto Backup and Restore Configuration

![Auto Backup and Restore Configuration dialog box](image)

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.
o **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.

   The **Message** dialog box appears.

   **Figure 110 Database backup prompt message**

   ![](Figure 110 Database backup prompt message)

   **Installing Dbman on Windows Server and Linux are similar. This example uses the Windows Server.**

7. 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.

8. Copy the **dbman** folder in the IMC installation path on the master server to the **INSTDIR** directory on the database server.

   In this example, the **INSTDIR** directory is the directory in which Dbman is installed on the remote database server. You should replace the **INSTDIR** with the actual directory name.

9. For subordinate servers, 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.
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`

**Automatic backup**

Run Dbman on the database server:

1. Open a cmd window and enter the `D:\Program Files\dbman\bin\` folder by executing the following command:
   ```
   D:\cd Program Files\dbman\bin
   ```
2. Enable Dbman automatic database backup by executing the `dbman` command.
   Dbman automatically backs up the database files of the IMC server at the automatic back up interval configured in the Intelligent Deployment Monitoring Agent.

**Figure 111 CMD window**

![CMD window]

Do not close the **Command Prompt** window or **Terminal** window when automatic backup is being performed. Otherwise, the backup process terminates.

**Stopping automatic backup**

To stop Dbman automatic backup, execute the following command:

```
D:\cd Program Files\dbman\bin
dbman -k
```

**Manual backup**

Execute the following command on a cmd window to back up the database immediately:

```
D:\
```
cd Program Files\dbman\bin\ndbman -backup “backupfilesdir”

Where backupfilesdir is path where the backup file is stored.

**Manual restoration**

To perform manual restoration to restore the database immediately, 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 manually restore the database, executing the following commands on the cmd window:

D:
cd Program Files\dbman\bin\ndbman -restore “rstrdir file;file;…”

Where rstrdir and file specify the path and name of the file to be restored.

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”

**Checking Dbman status**

Execute the following commands to check the running status of Dbman:

D:
cd Program Files\dbman\bin\ndbman -c

**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 “Installing Dbman on the database server” and “Using Dbman on the database server.”
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 `\INSTDIR\dbman\etc` folder (`\INSTDIR/dbman/etc` on Linux) are overwritten except the `dbman.conf` file.

   If the EAD component is deployed, you must copy the script file folder in the `dbman` directory of the server with the EAD component deployed to the `INSTDIR/Dbman` directory.

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 register the backup system.
11 FAQ

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.

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 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:

   ```bash
   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:

   ```bash
   cd /var/local/firefox/plugins/
   ln -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.

To solve this problem, stop IMC, install the patch mentioned above, and 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 execute the following commands:

use model
EXEC sp_droptype 'qv_id'

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>
```

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 `$ORACLE_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)))
)
3. Use vi to run the SORACLE_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.

   **Figure 112 System properties**

2. Select the Advanced tab, and click Settings in the Performance area. The Performance Options dialog box appears.
3. On the Performance Options dialog box, select the Advanced tab, and click Change in the Virtual memory area. The Virtual Memory dialog box appears.

4. Select the System managed size option, click Set, and 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 HP 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 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
- HP Networking http://www.hp.com/go/networking
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><strong>WARNING!</strong></td>
<td>Indicates that the failure to follow directions could result in bodily harm or death.</td>
</tr>
<tr>
<td><strong>CAUTION</strong></td>
<td>Indicates that failure to follow directions could result in damage to equipment or data.</td>
</tr>
<tr>
<td><strong>IMPORTANT</strong></td>
<td>Provides clarifying information or specific instructions.</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>Provides additional information.</td>
</tr>
<tr>
<td><strong>TIP</strong></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.
acronyms list, 127
activating IMC, 110
Android client, 87
  installing, 87
  using, 87
anti-virus software, 113
application scenario, 6
backing up IMC, 92
backup and restore, 92, 114
centralized deployment, 16
centralized server deployment, 76
configuration guidelines, 119
contacting HP, 127
database
  backup and restore, 92, 114
Dbman, 92, 114
deploying IMC, 50, 57
  methods, 8
  preparation, 13
  prerequisites, 6
  service components, 69
deployment and upgrade options, 54
DHCP plug-ins, 80
dialog box
  completion, 48
  disk space requirements, 43
  error reporting, 44
  feature selection, 41
  installation progress, 47
  installation rules, 42, 45
  ready to install, 46
distributed deployment, 16
distributed mode
  Oracle or MySQL database, 6
  prerequisites, 6
time radio radio
enterprise edition, 3
FAQ, 121
firewall recommendation, 113
first license registration, 104
hardware requirements, 9
HP Passport sign-in, 105
HP support websites, 127
IMC
activating, 110
backing up, 92
components, 1
editions, 3
logging in, 90
registering, 104
removing, 101
removing a component, 101
restoring, 101
uninstallation, 101
upgrading, 93
virtual machine installation, 12
IMC Platform
deploying, 57
installing, 50
incremental node licenses, 109
installation
  custom, 51
  plug-in, 80
  typical, 51
Installation Summary, 55
installing
  DHCP plug-ins, 80
  IMC on a virtual machine, 12
  IMC Platform, 50
  Java Runtime Environment, 7
  methods, 8
  preparation, 13
  service components, 69
  VNM agent plug-ins, 82
installing SQL
  client, 41
  feature selection, 41
Java Runtime Environment (JRE) installation, 7
license
  agreement, 53
  incremental node, 109
  registering for IMC, 104
  third party, 53
  upgrading to IMC v5.0, 111
license file, 112
Linux DHCP server, 81
logging in to IMC, 90
master server, 16
Microsoft Hyper-V server, 82
MS DHCP server, 80
MySQL database, 6
Network Traffic Analyzer
  centralized server deployment, 76
  installing, 72
  subordinate servers deployment, 77
NTA. See Network Traffic Analyzer
NTP, 15
plug-in installation, 80
port numbers used by IMC components, 113
port settings, 113
preparing
  system time, 15
  time zone, 15
registering IMC, 104
removing
  an IMC component, 101
  components at one time, 102
IMC, 101
requirements
  deployment, 16
  hardware, 9
  installation, 16
restoring IMC, 101
server requirements, 9
  Linux, 10
  Windows, 9
service components, 1, 69
standard edition, 3, 50
subcomponents, 50
subordinate server, 16
Subscriber’s Choice for Business website, 127
superuser name, 52
support, 127
system time, 15
technical support, 127
time zone, 15
uninstallation, IMC, 101
upgrading IMC, 93
  IMC V5.0 license, 111
  license file, 112
virtual machine installation, 12
VNM agent plug-ins, 82
web browser requirements, 1
websites, 127