Abstract
This document describes the processes for deploying the HP Intelligent Management Center. It also includes information on upgrading, removing, registering, backing up, and restoring IMC. This document is intended for use by network engineers and system administrators responsible for installing network management software.
Legal and notice information

© Copyright 2014 Hewlett-Packard Development Company, L.P.

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

The information contained herein is subject to change without notice. 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.

Acknowledgements

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

VMware®, VMware® vCenter™, VMware vSphere®, and VMware® Enterprise Plus Edition™ are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
Contents

1 Introduction to Intelligent Management Center ................................................................. 1
   IMC components .................................................................................................................. 1
   IMC Platform ...................................................................................................................... 1
   Service components ......................................................................................................... 2
   IMC editions ....................................................................................................................... 4
   Installation and deployment .............................................................................................. 4
   Prerequisites for deploying IMC in distributed mode ....................................................... 5
   Installing Java Runtime Environment (JRE) ..................................................................... 6

2 Preparing for installation .................................................................................................... 7
   Hardware requirements ...................................................................................................... 7
   Setting the Java memory size on 32-bit OS ....................................................................... 10
   Installing IMC on a virtual machine .................................................................................. 10
   Preparing the installation environments ......................................................................... 11
      Uninstalling previous versions of IMC ......................................................................... 11
      Ports and firewalls ......................................................................................................... 11
   Setting the system time .................................................................................................... 11

3 Installing and deploying the IMC Platform ..................................................................... 13
   Installing the IMC Platform ............................................................................................. 13
      Configuration restrictions and guidelines .................................................................. 13
   Installing the IMC Platform ............................................................................................. 14
   Deploying the IMC Platform ............................................................................................ 20
      Deploying the IMC Platform on the master server .................................................... 20
      Deploying the IMC Platform on a subordinate server ................................................ 25
      Deploying a single IMC Platform subcomponent ....................................................... 34
   IMC service logon accounts ............................................................................................ 35

4 Installing and deploying IMC service components ......................................................... 36
   Installing and deploying IMC NTA ................................................................................... 39
   Installing IMC NTA .......................................................................................................... 40
   Deploying NTA subcomponents on the master server ................................................... 44
   Deploying NTA subcomponents on a subordinate server ............................................. 45
   Installing and deploying IMC TAM .................................................................................. 48
   Installing and deploying IMC MVM .................................................................................. 51
      Installing IMC MVM ...................................................................................................... 51
      Deploying MVM subcomponents on the master server ............................................. 52
      Deploying MVM subcomponents on a subordinate server ........................................ 53
   Installing and deploying IMC UAM ................................................................................. 58
      Installing IMC UAM ...................................................................................................... 58
      Deploying UAM subcomponents on the master server ............................................. 59
      Deploying UAM subcomponents on a subordinate server ........................................ 66

5 Installing plug-ins ............................................................................................................. 70
   Installing DHCP plug-ins ................................................................................................. 70
      Installing DHCP plug-ins on the MS DHCP server ................................................... 70
      Installing DHCP plug-ins on the Linux DHCP server ............................................... 71
   Installing VRM agent plug-ins ........................................................................................ 72
      Installing a VRM Windows agent .................................................................................. 72
Documents

Websites

Conventions
1 Introduction to Intelligent Management Center

HP Intelligent Management Center (IMC) provides the network management functions through various components. Some of the components are highly CPU-intensive and, if they are deployed on the same server, might deplete the server resources and cause service interruptions.

To solve this problem, you can deploy IMC in distributed mode. Instead of deploying all the components on the same server, you can deploy the IMC Platform on the master server, and selectively deploy the CPU-intensive components, such as NTA, UBA, UAM, and EAD on one or more subordinate servers. This scales to networks from 200 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 Resource 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.

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

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

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

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

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

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

- **Network Traffic Analyzer (NTA)**—Is a graphical network-monitoring tool with real-time information about users and applications consuming network bandwidth. NTA is a reliable solution for enterprise and campus network traffic analysis. It defends the network against virus attacks and applies varying levels of bandwidth traffic to different services and applications.

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

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

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

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

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

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

- **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.

- **Branch Intelligent Management System (BIMS)**—Provides support for service operations, delivering high reliability, scalability, flexibility, and IP investment returns. Based on the TR-069 protocol, IMC BIMS offers resource, configuration, service, alarm, group, and privilege management. It allows the remote management of customer premises equipment (CPE) in WANs.

- **Remote Site Manager (RSM)**—Securely extends the IMC core platform capability to remote sites by deploying remote agents. These agents manage and monitor the remote network, and apply policies and configurations to the remote network devices on behalf of the central IMC server.

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

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

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

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

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

For information about all service components, see *v7.1 HP Intelligent Management Center Getting Started Guide*.

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

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

- Network Element (NE) Management
- Report Management
- Resource Management
- Security Control Center
IMC editions

The following editions of IMC are available:

- Enterprise
- Standard
- Basic

Table 1 lists the differences between the editions.

### Table 1 Differences between IMC editions

<table>
<thead>
<tr>
<th>Item</th>
<th>Basic</th>
<th>Standard</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>1000</td>
<td>Extensible</td>
<td>Extensible</td>
</tr>
<tr>
<td>Hierarchical Network</td>
<td>Not supported</td>
<td>Lower-level NMS only</td>
<td>Supported</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></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>Supported only on windows</td>
<td>Not supported</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 on installing a remote database for IMC on Windows:

- 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 on installing a remote database for IMC on Linux:

- Oracle 11g Installation and Configuration Guide (for Linux)
- Oracle 11g R2 Installation and Configuration Guide (for Linux)
- 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. Install puts copies of the installation packages on the master server. Deploy decompresses the installation packages and runs deployment scripts on the master server or subordinate servers as needed.

To install and deploy in a distributed deployment:
1. Install and deploy the IMC Platform on the master server.
2. Install and deploy the IMC subcomponents on the master or subordinate servers as needed.
3. Install the service components on the master server.
4. Deploy the service components on the master 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 tasks, for example, the RADIUS and portal servers in User Access Manager.

In a distributed deployment, the master server provides centralized Web services. For more information about accessing IMC, see "6 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 policy.

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

Prerequisites for deploying IMC in distributed mode

- The master and subordinate servers must use the same operating system.
- The master and subordinate servers must have the same operating system bit size (32 or 64).
- 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.

To install IMC on Linux with an 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 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 (for Linux).

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

For more information about other IMC Platform subcomponents, see "3 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 "4 Installing and deploying IMC service components."

- The following components must be deployed on the master server:
  - NE Management
  - Report Management
  - Resource Management
Start the IMC service in the Intelligent Deployment Monitoring Agent on the master server before deploying IMC components on subordinate servers.

If the 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 "7 Upgrading, backing up, or removing IMC."

When you deploy or upgrade components on a subordinate server, make sure the subordinate server can communicate with the master server.

NOTE:
To use Firefox for accessing IMC on Linux, install JRE 6.0 or JDK first. For the detailed operation procedure, see "11 FAQ."

Installing Java Runtime Environment (JRE)

To install JRE 6.0 on a subordinate server, run the JRE 6.0 setup in the IMC package as follows:

1. On the subordinate server, launch the Web browser and enter 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.
2. On the login page, enter the username and password.
3. Click Login to enter the Home tab.
4. Select the System tab and click Deploy Components.
5. Click When fail to start Remote Installation Wizard, download and install JRE.
6. 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.
2 Preparing for installation

The following information describes requirements that all IMC servers must meet.

Hardware requirements

Table 2 and Table 3 use the following terms:

- **Node**—IMC servers, database servers, and devices managed by IMC are called nodes.
- **Management Node**—Each of the devices managed by IMC is a management node, including switches, routers, IMC servers, database servers, and PCs.
- **Collection unit**—Represents a performance instance that is collected every 5 minutes. If a performance instance uses another collection interval, it corresponds to a number of collection units calculated with the formula: 5 minutes/instance collection interval in minutes.
  
  For example, the collection interval is set to 10 minutes for all performance instances. A monitored device contains 1 CPU, 1 memory bar, and 10 interfaces. To collect performance data for CPU, memory, response time, reachability rate, and interface send and receive rates, the total collection units of the device are: \((1+1+1+(10 \times 2)) \times 5/10 = 12\).
  
- **CPU**—The CPU must be no less than a Pentium 4 3.0 GHz processor.
- **Java heap size**—Maximum memory size to be used by Java processes on the IMC Web server.

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

To improve the input/output (I/O) performance, follow these guidelines:

- If the number of 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.
- If 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.
- If the number of collection units is from 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. If you want to set RAID level 5 or 10, install the correct number of parity disks.

Table 2 Server requirements for 32-bit operating systems

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

<table>
<thead>
<tr>
<th>Management scale</th>
<th>System minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>10 K to 100 K</td>
</tr>
<tr>
<td></td>
<td>10 Kows: 6 GB</td>
</tr>
<tr>
<td></td>
<td>Linux: 8 GB</td>
</tr>
<tr>
<td></td>
<td>100 GB</td>
</tr>
</tbody>
</table>

### Table 3: Server requirements for 64-bit operating systems

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Collection units</th>
<th>Online operators</th>
<th>CPU¹</th>
<th>Server memory</th>
<th>Max. Java heap</th>
<th>Storage required for installation</th>
<th>Storage required for operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 5 K</td>
<td>0 to 5 K</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td>50 GB</td>
<td></td>
</tr>
<tr>
<td>5 K to 50 K</td>
<td>5 K to 50 K</td>
<td>10</td>
<td>2</td>
<td>Windows: 4 GB</td>
<td>2 GB</td>
<td>3 GB</td>
<td>60 GB</td>
</tr>
<tr>
<td>0 to 10 K</td>
<td>0 to 10 K</td>
<td>30</td>
<td></td>
<td>Linux: 6 GB</td>
<td>3 GB</td>
<td>100 GB</td>
<td></td>
</tr>
<tr>
<td>200 to 1 K</td>
<td>10 K to 100 K</td>
<td>10</td>
<td>4</td>
<td>Windows: 8 GB</td>
<td>3 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 to 20 K</td>
<td>0 to 20 K</td>
<td>30</td>
<td></td>
<td>Linux: 12 GB</td>
<td>4 GB</td>
<td>100 GB</td>
<td></td>
</tr>
<tr>
<td>1 K to 2 K</td>
<td>20 K to 200 K</td>
<td>10</td>
<td>6</td>
<td>Windows: 16 GB</td>
<td>4 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 K to 5 K</td>
<td>0 to 30 K</td>
<td>40</td>
<td>8</td>
<td>Windows: 24 GB</td>
<td>8 GB</td>
<td>5 GB</td>
<td>80 GB</td>
</tr>
<tr>
<td></td>
<td>30 K to 300 K</td>
<td>20</td>
<td></td>
<td>Linux: 8 GB</td>
<td>25 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 K to 10 K</td>
<td>0 to 40 K</td>
<td>50</td>
<td></td>
<td>Windows: 16 GB</td>
<td>12 GB</td>
<td>7 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td></td>
<td>4 K to 400 K</td>
<td>20</td>
<td></td>
<td>Linux: 12 GB</td>
<td>30 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 K to 15 K</td>
<td>0 to 40 K</td>
<td>50</td>
<td>24</td>
<td>Windows: 64 GB</td>
<td>16 GB</td>
<td>10 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td></td>
<td>40 K to 400 K</td>
<td>20</td>
<td></td>
<td>Linux: 12 GB</td>
<td>60 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ CPU: 2 cores for 500-1000 K operations, 4 cores for 1-10 K operations, 6 cores for 2-20 K operations, 8 cores for 5-10 K operations, and 24 cores for 10 K to 15 K operations.
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.

Table 4 lists the software requirements for IMC deployment.

Table 4 Software requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating</td>
<td>Windows Server 2003</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td>system</td>
<td>(32bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003</td>
<td>Service Pack 2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>(64bit)</td>
<td>and KB942288</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>R2 (32bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008</td>
<td>Service Pack 2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>(32bit)</td>
<td>and KB942288</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>(64bit)</td>
<td>(64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008</td>
<td>Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>R2 (64bit)</td>
<td>KB2836988</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
<td>Service Pack 4</td>
</tr>
<tr>
<td></td>
<td>(64bit)</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>Microsoft SQL Server</td>
<td>Service Pack 3</td>
</tr>
<tr>
<td></td>
<td>2005</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server</td>
<td>Embedded deployments</td>
</tr>
<tr>
<td></td>
<td>2008</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2008 R2 SP2</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Express</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server</td>
<td>Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>2008 R2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server</td>
<td>Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>2012</td>
<td></td>
</tr>
<tr>
<td><strong>Linux</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating</td>
<td>Red Hat Enterprise</td>
<td>N/A</td>
</tr>
<tr>
<td>system</td>
<td>Linux 5 (32 &amp; 64bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Linux 5.5 (32 &amp;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Linux 5.9 (32 &amp;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Linux 6.1 (64bit)</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>Oracle 11g Release 1</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Oracle 11g Release 2</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

After database installation, restart the database server. Make sure the database automatically starts up.
Setting the Java memory size on 32-bit OS

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

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

1. Use a text editor (such as WordPad in Windows or vi in Linux) to edit 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.
   - If the jserver process cannot start up, decrease the above values until it starts up.
   - If 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.

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

- Number of CPUs
- Number, model, and MAC addresses of network adapters
- Number of disk drives, storage paths
- Assignments of storage

Although changing the settings does not affect VM migration, IMC will not operate correctly.

Table 5 Hypervisor platform requirements

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

Uninstalling previous versions of IMC

If IMC was previously installed on the system, thoroughly remove it first. For instructions on removing IMC, see "7 Upgrading, backing up, or removing IMC."

After you remove IMC:

- In Windows, locate and delete the IMC-Reserved folder in the WINDOWS folder of the system disk.
- In Linux, locate and delete the IMC-Reserved folder in the /etc directory.

Ports and firewalls

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

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

Other IMC components may have additional port requirements.

Setting the system time

HP recommends the following settings:

- Set the time zone to GMT or Coordinated Universal Time.
- Do not enable seasonal time adjustments such as daylight savings time.
- Before installing IMC, check that the system time, date, and time zone settings on the server are correct.
- When deploying IMC in distributed mode, make sure that the time zone settings of all servers are the same.
- Use the Network Time Protocol (NTP) to synchronize the time on all servers.

After IMC is started, do not modify the system time of the server. Otherwise, intermittent problems can occur, such as:

- When jumping to a future time, the system takes 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.
- When you modify the system time to a past time, data with overlapping time can occur, and data processing may 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 you restart all primary and subordinate servers. For problems localized to a subordinate server, you need to restart only the server.
3 Installing and deploying the IMC Platform

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

Start by installing the IMC Platform on the master server. Then deploy the subcomponents on the master and subordinate servers as needed. Table 7 shows the IMC Platform subcomponents and the optional servers.

Table 7 IMC Platform subcomponents and deployment requirements

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

Installing the IMC Platform

Configuration restrictions and guidelines

To install IMC on Windows, follow these guidelines:

- On Windows Server 2003 or Windows Server 2003 R2, you must log in as an administrator and then install IMC.
- On Windows Server 2008 or Windows Server 2008 R2, you must first right-click the install.bat script and select Run as Administrator from the shortcut menu.

To install IMC on Linux, follow these guidelines:
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.

To install IMC on other Linux operating systems except Red Hat Linux 6, start the IMC installation wizard by running the `install.sh` script in the install directory of the IMC installation DVD as a root user.

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

Installing the IMC Platform

1. Log in to the operating system, insert the installation DVD into the DVD-ROM drive, enter the install directory, right-click the `install.bat` script and select Run as Administrator from the shortcut menu. The Select Locale page appears, as shown in Figure 1.

**Figure 1 Select Locale**

2. Select the country/region, language, and installation type.
   IMC supports typical and custom installations.
   - **Typical**—Install and deploy all Platform subcomponents on the master server. A typical installation is a good place to start a centralized deployment, although service components could be installed on subordinate servers.
   - **Custom**—Allows you to select IMC Platform subcomponents to install and deploy on the master server as needed. This installation method is available for both local and remote databases.

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

   The Checking Database Connectivity dialog box appears, as shown in Figure 2.
3. Enter parameters for database connectivity in the dialog box:
   a. Select the database type and instance name.
   b. Enter the SQL server superuser name (`sa` by default) and password.
   c. Enter a 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.
   d. Select `local host` as the **Database Location**, and specify the listening port (`1443` by default).
   e. Enter a database location or select a network service name or click to add a network service name.
      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*.

4. Click **OK**.

   After database connectivity check is passed, the **Welcome to HP iMC Installation Wizard** window appears, as shown in **Figure 3**.
5. Click **Next**.

The **Agreement** window appears, as shown in Figure 4.

**Figure 4 Agreement**

6. Read the license agreement and third party license and select **Accept**.
7. Click **Next**.

The **Choose Target Folder** window displays the subcomponents, as shown in **Figure 5**.

**Figure 5 Choose Target Folder page**

![Choose Target Folder](image)

8. Select the components you want to install and specify the installation location.

By default, IMC is installed in the `\Program Files\iMC` directory of the disk with the maximum free space on Windows or in `/opt/iMC` on Linux. In this example, IMC is installed in `E:\Program Files\iMC`.

You can enter a path or click **Browse** to select another local path.

**NOTE:**

- At least 5 GB free space must be available.
- The installation path must be local.
- Linux does not support the IMC installation in a path with a symlink path.

1. Click **Next**.

The **Deployment and Upgrade Options** window appears, as shown in **Figure 6**.
2. Select Deploy or upgrade at once or Deploy or upgrade later as needed. In this example, select Deploy or upgrade later.

3. Click Next.

The Installation Summary window appears, as shown in Figure 7.
The Installation Summary window provides the following information:

- Name, description, version, and required disk space of 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

4. Click Install.

The Installing window appears, as shown in Figure 8.

**Figure 8 Installing common components**

After the installation is complete, the Installation Completed page appears, as shown in Figure 9.
5. Perform either of the following tasks:
   - To start to deploy the IMC Platform, select **Open deployment monitoring agent**.
   - To continue to install other IMC components, select **Install other iMC Components**.
   In this example, select **Open deployment monitoring agent**.

6. Click **Finish**.

### Deploying the IMC Platform

### Deploying the IMC Platform on the master server

1. In the **Installation Completed** window (see Figure 9), select **Open deployment monitoring agent** and then click **Finish**.
   
   Then the system automatically starts the Intelligent Deployment Monitoring Agent and displays the **Batch deploy** window, as shown in Figure 10.
NOTE:
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, and select Batch Deploy from the right-click menu of the target components to start batch deployment.

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

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

Optional components include:

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

You can also select the components to be deployed as needed, except that the Resource Manager component is required. In this configuration example, select the following components:

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

2. Click **OK**.

The **Database Configuration Info** window appears, as shown in Figure 11.

**Figure 11 Database Configuration Info**

![Database Configuration Info Window]

3. Enter the password for the superuser, which is used for installing the IMC database.

4. Select the location for saving data files:

   By default, the data files are stored in the `\imcdata` directory of the IMC installation path on windows or `/opt/imcdata` on Linux. You can also click **Browse** to select another data file location. In this example, data files are stored in `E:\Program Files\imcdata`. Make sure the location for saving data files does not include any files. Otherwise, IMC deployment fails.
NOTE:
You must select a writable, uncompressed disk drive. Otherwise, an error can occur during IMC deployment. To change the compression setting of a disk drive:

- Right-click the disk name and select Properties from the shortcut menu.
- On the General tab of the disk properties window that appears, clear the selection of Compress drive to save disk space.
- Click OK.

5. Manually enter the location for saving data files and click Next.

The Configure Web Service Port window appears, as shown in Figure 12.

Figure 12 Configure Web Service Port

6. Set HTTP Port and HTTPS Port.

The default port for HTTP access is 8080, and that for HTTPS access is 8443. You can change the port numbers as needed.

NOTE:
- Make sure the specified Web service ports are opened in the firewall settings and are not being used by any other services.
- If UAM is to be installed for the IMC system, set HTTP Port to 80. You cannot change the HTTP port number after IMC installation is complete. To change the HTTP port number, you must reinstall IMC.

7. Click Deploy.

After the deployment, the Batch deploy succeeded window appears, as shown in Figure 13.
8. Select **Start iMC Server now** and click **OK**.

The system immediately starts the IMC service and displays the *Intelligent Deployment Monitoring Agent* window, as shown in Figure 14. Click the **Deploy** tab to view information about the component deployment.

**Figure 14 Information about component deployment**

<table>
<thead>
<tr>
<th>Component Name/Description</th>
<th>Version</th>
<th>Status</th>
<th>Deployment Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>iMC Platform - Resource Management</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - Alarm Management</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - User Self-Service Manager</td>
<td></td>
<td>Undeployed</td>
<td></td>
</tr>
<tr>
<td>iMC Platform - Guest Access Management</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - Intelligent Configuration</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - Performance Management</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - ACL Management</td>
<td></td>
<td>Undeployed</td>
<td></td>
</tr>
<tr>
<td>iMC Platform - Network Asset Management</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - Security Control Center</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - Security Control Center</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - System Management</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - System Management</td>
<td></td>
<td>Undeployed</td>
<td></td>
</tr>
<tr>
<td>iMC Platform - Security Management</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - Security Management</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - Virtual Resource Manager</td>
<td></td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>iMC Platform - Virtual Resource Manager</td>
<td></td>
<td>Undeployed</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**

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

If you do not select **Start iMC Server now**, follow these steps to manually start the IMC service after deployment completion:

1. In the *Intelligent Deployment Monitoring Agent* window, select the **Monitor** tab, as shown in Figure 15.
2. Click Start iMC.

You can also select the **Automatically start the services when the OS starts** box to start IMC with the operating system.

To view the enabling and running status of each process, click the **Process** tab to enter the process management window.

### Deploying the IMC Platform on a subordinate server

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

Just like the IMC Platform installation, the subordinate server installation requires administrative privileges:

1. **Log in to the operating system as a user with administrator privileges.**
   - 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, 2008 R2, 2012 or 2012 R2, right-click `installslave.bat` (see below) and select **Run as Administrator** from the shortcut menu.
   - To install IMC on Linux, start the IMC installation wizard by running `installslave.sh` as a root user.
   - To install IMC on Linux, all of the installation files must be on the local server.

2. **Uncompress the installation files.**
   - If installing from DVD on Red Hat Linux 6, copy all installation files to the local server.
   - If installing on Linux, make sure you have rights to run the `chmod -R 775 .\linux\install\install.sh` command.
3. Run \windows\install\installslave.bat (or \linux\install\installslave.sh). A window will appear, asking you to select a country/region, language, and installation type.

If you deploy IMC components to a subordinate server 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, enter the install directory of the IMC installation DVD. Right-click the installslave.bat script and select Run as Administrator from the shortcut menu.

   The Address of Master window appears, as shown in Figure 16.

   a. To start the remote installation wizard of the Intelligent Deployment Monitoring Agent on Linux, log in to the system as a root user and run the installslave.sh script in the install directory in the IMC installation DVD.

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

   Figure 16 Address of Master

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

   The Checking Database Connectivity window appears, as shown in Figure 17.
3. Enter parameters for database connectivity in the dialog box:
   a. Select the database type and instance name. Use the default instance or select Other Instance from the list to specify an instance name.
   b. Enter the database superuser name (sa by default) and password.
      The parameters appear only when you install IMC on Windows.
   c. In distributed deployment, if more than one SQL Server or MySQL database is used, make sure you set the same listening port for them.
   d. Select a network service name or click the icon to add a network service name for connecting to the local 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.
   e. Select local host for the database location, enter the superuser name (sa by default) and password, and listening port number (1433 by default), as shown in Figure 17.
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
   192.168.40.207 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**.

3. On the IMC homepage, click the **System** tab, and select **System Configuration > Deploy Component**.

4. On the **Installed Components** page, click **Start deploy**.
   A dialog box appears, as shown in **Figure 18**.

   **Figure 18 Whether to launch the Intelligent Deployment Monitoring Agent**
   
   ![Message from webpage]
   
   This operation requires the Intelligent Deployment Monitoring Agent be installed and started. Are you sure to continue?

   ![OK | Cancel]

5. Click **OK**.

   The **Downloading application** dialog box appears, as shown in **Figure 19**, indicating that Java file **jre.exe** is being downloaded.

   If JRE6.0 has been installed on the subordinate servers, the system starts the remote installation wizard when you click **OK**.

   **Figure 19 Downloading application**

   ![Java Web Start]

   **Name:** Deployer Monitor Agent
   **Publisher:** IMC Development Team
   **From:** http://192.160.40.207:0000

After the Java file is downloaded and installed, the **Checking Database Connectivity** window appears, as shown in **Figure 17**. After configuration completion, click **OK** to check database connectivity. When the check is passed, the **Choose Target Folder for Deployment** dialog box appears, as shown in **Figure 20**.

**Installing the Intelligent Deployment Monitoring Agent**

After successfully starting the remote installation wizard, you can start to install the deployment monitoring agent.
By default, IMC is deployed in the `\Program Files\iMC` directory of the disk with the maximum free space on Windows or in `/opt/iMC` on Linux. In this example, IMC is deployed in `E:\Program Files\iMC`.

To deploy IMC in another location, either type a path or click **Browse** to select another path. If the installation path includes any files, a confirmation dialog box appears. Click **OK** to delete all the files in the installation path.

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

   After the files are downloaded, the **Installation Completed** dialog box appears, as shown in Figure 21.
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, as shown in Figure 22.
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 components as needed and click **OK**.
   The system starts downloading the files.
   After downloading is complete, perform one of the following tasks:
- If the Web service port configuration window appears, set HTTP Port (8080 by default) and HTTPS Port (8443 by default) as needed.

**Figure 24 Web port configuration**

![Web port configuration window](image)

- If the database configuration information window appears, perform the following tasks:
  - Enter the password for the user **sa** for the current database, which is the superuser name specified during IMC installation.
  - Select a data file location.
    
    By default, data files are stored in the `\Program Files\imcdata` directory of the disk with the maximum free space on Windows or `/opt/imcdata` on Linux. In this example, data files are stored in `E:\Program Files\imcdata`. 
5. Click **Deploy** to start the deployment. After the deployment is finished, the **Batch deploy result** dialog box prompting **Batch deploy succeeded** appears.

**Figure 26 Batch deploy result**

6. Click **OK**.

7. After successfully finishing the deployment, select the **Deploy** tab in the Intelligent Deployment Monitoring Agent, as shown in **Figure 27**.
8. 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).

9. 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.

10. 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 29.

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

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

     The Batch deploy dialog box appears.

  b. Select the component, and then click OK.

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

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

IMC common service components include:
- Application Performance Manager (APM)
- Branch Intelligent Management System (BIMS)
- Endpoint Admission Defense (EAD)
- Intelligent Analysis Reporter (IAR)
- MPLS VPN Manager (MVM)
- Network Traffic Analyzer (NTA)
- QoS Manager (QoSM)
- Remote Site Manager (RSM)
- Service Health Manager (SHM)
- Service Operation Manager (SOM)
- TACACS+ Authentication Manager (TAM)
- User Access Manager (UAM)
- User Behavior Auditor (UBA)
- Virtual Application Networking Fabric Manager (VAN SAN)
- Virtual Application Networking Software Defined Network (VAN SDN)
- Wireless Service Manager (WSM)
- iNode Dissolvable Client
- IPsec VPN Manager
- VAN Connection Manager
- Voice Service Manager

Table 8 IMC subcomponents and deployment requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Subcomponent</th>
<th>Target server</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Traffic Analyzer</td>
<td>Network Traffic Analyzer</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Server</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Network Behavior Analyzer</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Server</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td>User Behavior Auditor</td>
<td>User Behavior Auditor</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td>Component</td>
<td>Subcomponent</td>
<td>Target server</td>
<td>Remarks</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------</td>
<td>-------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>User Behavior Auditor Server</td>
<td>37</td>
<td>Master and subordinate servers</td>
<td>You must configure the NTAS server.</td>
</tr>
<tr>
<td>Network Behavior Analyzer Server</td>
<td>37</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td>Network Behavior Analyzer Server</td>
<td>37</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>QoS Manager</td>
<td>QoS Management</td>
<td>Master server</td>
<td>N/A</td>
</tr>
<tr>
<td>Service Health Manager</td>
<td>Service Health Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>NQA Collector Management</td>
<td>Master and subordinate servers</td>
<td>N/A</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></td>
<td>Service Desk</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>Applications Manager</td>
<td>Applications Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>BIMS - Branch Intelligent Management System</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>BIMS</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>Wireless Service Manager</td>
<td>Wireless Service Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</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>IPsec VPN Manager</td>
<td>IPsec VPN Manager</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>MPLS VPN Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>MPLS VPN Manager</td>
<td>MPLS TE management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>L2VPN Management</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
<tr>
<td>User Access Manager</td>
<td>User Access Management</td>
<td>Master and subordinate servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Portal Web Server and Portal Proxy</td>
<td>Master and subordinate servers</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Resource Management
Report Management
Set the database password (defaults to `iMC5_uamead`) and **UAM Server’s IP Address**, which is UAM’s RADIUS server.
<table>
<thead>
<tr>
<th>Component</th>
<th>Subcomponent</th>
<th>Target server</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal Server</td>
<td>Master and subordinate servers</td>
<td></td>
<td>Set Portal Server’s IP Address, which is the IP address of the network adapter providing services externally of the server where the Portal server component is deployed.</td>
</tr>
<tr>
<td>Third Party Page Publish Server</td>
<td>Master and subordinate servers</td>
<td></td>
<td>Set the Portal Server’s Port.</td>
</tr>
<tr>
<td>End User Intelligent Profiling Server</td>
<td>Master and subordinate servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>End User Intelligent Profiling Sub Server</td>
<td>Subordinate servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Server</td>
<td>Master and subordinate servers</td>
<td></td>
<td>Set Policy Server’s IP Address.</td>
</tr>
<tr>
<td>Policy Proxy Server</td>
<td>Master and subordinate servers</td>
<td></td>
<td>Set Policy Proxy Server’s IP Address.</td>
</tr>
<tr>
<td>User SelfService</td>
<td>Master and subordinate servers</td>
<td></td>
<td>Set User SelfService’s IP Address.</td>
</tr>
<tr>
<td>User Access Management Sub Server</td>
<td>Subordinate servers</td>
<td></td>
<td>Provides RADIUS authentication for access users.</td>
</tr>
<tr>
<td>Security Policy Configuration</td>
<td>Master and subordinate servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop Asset Manager</td>
<td>Master and subordinate servers</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>EAD Security Policy</td>
<td>Master and subordinate servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop Asset Manager Proxy Server</td>
<td>Master and subordinate servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>End User Intelligent Profiling</td>
<td>Master and subordinate servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TACACS+ Authentication Manager</td>
<td>Master and subordinate servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iNode DC</td>
<td>Master and subordinate servers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Set DAM Proxy Server’s IP Address, which is the IP address of the network adapter providing services externally of the server where the DAM proxy server component is deployed.
The installation and deployment procedures for service components are the same. The following information describes how to install and deploy NTA, TAM, MVM, and UAM.

Table 9 lists the service components that use the same installation and deployment procedures as the example components.

Table 9 Service components classified by deployment procedures

<table>
<thead>
<tr>
<th>Example component</th>
<th>Component with the same procedure</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTA</td>
<td>APM, BIMS, IVM, SHM, SOM, UBA, VSM, WSM, VFM, SDNM, RAM, UCHM, QoSM, VCM, iNode DC</td>
<td>No parameter is required to complete the installation and deployment.</td>
</tr>
<tr>
<td>TAM</td>
<td>EAD</td>
<td>Additional parameters are required to complete the installation and deployment.</td>
</tr>
<tr>
<td>MVM</td>
<td>N/A</td>
<td>Additional parameters are required to complete the installation and deployment.</td>
</tr>
<tr>
<td>UAM</td>
<td>N/A</td>
<td>Additional parameters are required to complete the installation and deployment.</td>
</tr>
</tbody>
</table>

Before you deploy a service component, deploy the base IMC components and the components on which the service component depends.

See “Prerequisites for deploying IMC in distributed mode” before deploying service components in distributed mode.

Installing and deploying IMC NTA

IMC NTA includes the following subcomponents:

- Network Traffic Analyzer and Network Behavior Analyzer, which can be deployed only on the master server.
Network Traffic Analyzer Server and Network Behavior Analyzer Server, which can be deployed on the master server, a subordinate server, or both.

HP recommends that you deploy the Network Traffic Analyzer Server and Network Behavior Analyzer Server subcomponents as follows:

- On networks with moderate traffic load, deploy these subcomponents only on a subordinate server.
- On networks with high traffic load, deploy these subcomponents on the master server and a subordinate server at the same time.

The following information uses a typical IMC NTA deployment scheme, in which:

- Network Traffic Analyzer and Network Behavior Analyzer are deployed on the master server.
- Network Traffic Analyzer Server and Network Behavior Analyzer Server are deployed on a subordinate server.

**Installing IMC NTA**

1. Select **Install other iMC Components** and click **Finish** in the **Installation Completed** window (see Figure 9) or perform one of the following tasks as needed:
   - On Windows:
     - Select **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent**. On the **Monitor** tab, click **Install**.
     - Right-click the **Intelligent Deployment Monitoring Agent** icon in the system tray and select **Install** from the shortcut menu.
   - On Linux, run the **dma.sh** script in the **/deploy** directory of the IMC installation path. On the **Monitor** tab, click **Install**.
   - The **Choose folder** window appears, as shown in Figure 29.

2. Insert the IMC NTA installation CD into the DVD-ROM drive. Then, in the **Choose folder** window, click **Browse** and select the **install\components** folder on the CD.
3. Click **OK**.
   - The HP IMC Installation Wizard appears, as shown in Figure 30.
4. Click **Next**.

   The **Agreement** window appears, as shown in Figure 31.

**Figure 31 Agreement**

5. Read the license agreement and third party license and select **Accept**.
6. Click **Next**.

The **Choose Target Folder** window appears, as shown in **Figure 32**.

**Figure 32 Choose Target Folder**

The **Choose Target Folder** window displays information about the NTA components to be installed and the installation location.

7. In the **Choose Target Folder** window, click **Next**.

The **Deployment and Upgrade Options** window appears, as shown in **Figure 33**.
8. Select **Deploy or upgrade at once** or **Deploy or upgrade later** as needed. In this example, select **Deploy or upgrade later**.

9. Click **Next**.

The **Installation Summary** window appears, as shown in Figure 34.

**Figure 34 Installation Summary**
10. Verify the installation information and click Install.
After the installation is complete, the Installation Completed window appears, as shown in Figure 35.

Figure 35 Installation Completed

11. Perform either of the following tasks:
   o To start to deploy IMC NTA, select Open deployment monitoring agent.
   o To continue to install other IMC components, select Install other iMC Components.
   In this example, select Open deployment monitoring agent.

12. Click Finish.

Deploying NTA subcomponents on the master server

1. In the Installation Completed window (see Figure 35), select Open deployment monitoring agent
   and click Finish.
   The system automatically starts the Intelligent Deployment Monitoring Agent and displays the
   Batch deploy window, as shown in Figure 36.
2. Select the NTA subcomponents you want to deploy on the master server. In this example, select Network Traffic Analyzer and Network Behavior Analyzer.

3. Click **OK** to start the deployment.

   After the deployment is complete, the **Batch deploy succeeded** window appears, as shown in Figure 37.

   **Figure 37 Batch deploy succeeded**

4. Clear the **Open readme file directory** and **Start iMC Server now** options and click **OK**.

**Deploying NTA subcomponents on a subordinate server**

1. If the Intelligent Deployment Monitoring Agent is not installed on the subordinate server, install it first. (Details not shown.)
For information about how to install the Intelligent Deployment Monitoring Agent, see “Deploying the IMC Platform on a subordinate server.”

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

3. Click the **Deploy** tab in the Intelligent Deployment Monitoring Agent.

   The **Deploy** tab displays all IMC components that have been installed and their deployment information, as shown in **Figure 38**.

   **Figure 38 Information about component deployment**

   ![Component Deployment Information](image)

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Description</th>
<th>Version</th>
<th>Status</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform - Alert Management</td>
<td>Monitors and ...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - User SelfService</td>
<td>Manages the self...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - Guest Access</td>
<td>Manages guest acce...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - Intelligent Config</td>
<td>Offers software upgr...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - Report Management</td>
<td>Issues and displa...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - NE Management</td>
<td>Provides network elem...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - Performance</td>
<td>Monitors and analy...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - ACL Management</td>
<td>Configures ACLs for ...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - Network Asset</td>
<td>Manages network asset...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - Security Control</td>
<td>Monitors network ...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - General Search</td>
<td>Manages the general...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - System Management</td>
<td>Collects, filters, ...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - VLAN Management</td>
<td>Manages VLAN resource...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Platform - Virtual Resource</td>
<td>Manages virtual resou...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Network Behavior Analyzer</td>
<td>Provides basic config...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Network Behavior Analyzer Server</td>
<td>Receives network beh...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Network Traffic Analyzer</td>
<td>Manages and ...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Network Traffic Analyzer Server</td>
<td>Receives network beh...</td>
<td>7.1 (E0332)</td>
<td>Undeployed</td>
<td>Master Server</td>
</tr>
<tr>
<td>Network Traffic Analyzer Server</td>
<td>Collects and analytic...</td>
<td>7.1 (E0332)</td>
<td>Deployed</td>
<td>Master Server</td>
</tr>
</tbody>
</table>

4. Right-click any component in the list, and then select **Batch Deploy** from the shortcut menu.

   The **Batch deploy** window displays components that are not deployed, as shown in **Figure 39**.
5. Select the NTA subcomponents you want to deploy on the subordinate server. In this example, select **Network Behavior Analyzer Server** and **Network Traffic Analyzer Server**.

6. Click **OK** to start the deployment.

7. In the **Batch deploy result** dialog box, click **OK**.

8. Click the **Deploy** tab in the Intelligent Deployment Monitoring Agent.

Network Behavior Analyzer Server and Network Traffic Analyzer Server can be deployed on the master server and a subordinate server at the same time. When they are deployed only on the master or a subordinate server, an entry with **Undeployed** status appears in the deployment entry list, as shown in Figure 40.
9. Start IMC on the master server:

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

b. On the **Monitor** tab, click **Start iMC**.
   - A confirmation dialog box appears.

   c. Click **OK** to start the IMC service.

### Installing and deploying IMC TAM

TAM has only one subcomponent TACACS+ Authentication Manager that can be deployed on either the master or a subordinate server. This example deploys TAM on the master server.

To install and deploy IMC TAM on the master server:

1. Install IMC TAM on the master server in the same way IMC NTA is installed. (Details not shown.)

   For information about the installation procedures, see "Installing IMC NTA."

2. In the **Installation Completed** window (see Figure 41), select **Open deployment monitoring agent.**
3. Click Finish.

The system automatically starts the Intelligent Deployment Monitoring Agent and displays the Batch deploy window, as shown in Figure 42.

**Figure 42 Batch deploy**
4. Select the subcomponents you want to deploy. In this example, select **TACACS+ Authentication Manager** and click **OK**.

5. In the **Configure TACACS+ Authentication Manager** window (see Figure 43), configure the following parameters:
   - **Database Password/Confirm Password**—These fields are automatically populated with the database password configured when the IMC Platform is installed. Do not change the values of these fields unless the database password of the IMC Platform is changed after installation.
   - **TAM Server’s IP Address**—This field displays the IP address of the host on which TAM is to be deployed. By default, the IP address of the current host is displayed. Use the default value in this example.

![Figure 43 Configure TACACS+ Authentication Manager](image)

6. Click **Deploy**.

After the deployment is complete, the **Batch deploy succeeded** window appears, as shown in Figure 44.

![Figure 44 Batch deploy succeeded](image)
7. Perform either of the following tasks:
   - To start IMC immediately, select **Start iMC Server now** and click **OK**.
   - To start IMC later, clear the **Start iMC Server now** option and click **OK**. Then, when you are ready to start IMC, click **Start iMC** on the **Monitor** tab of the Intelligent Deployment Monitoring Agent.

### Installing and deploying IMC MVM

MVM has the following subcomponents:
- MPLS VPN Management
- MPLS Management
- MPLS TE Management
- L2VPN Management

These subcomponents can be deployed on both the master and subordinate servers. This example deploys MPLS VPN Management and MPLS Management on the master server, and MPLS TE Management and L2VPN Management on a subordinate server.

### Installing IMC MVM

1. Install IMC MVM on the master server in the same way IMC NTA is installed. (Details not shown.) For information about the installation procedures, see "Installing IMC NTA."
2. In the **Installation Completed** window (see Figure 45), select **Open deployment monitoring agent** and click **Finish**.

![Figure 45 Installation Completed](image)
Deploying MVM subcomponents on the master server

1. In the **Installation Completed** window (see Figure 45), select **Open deployment monitoring agent** and click **Finish**.

The system automatically starts the Intelligent Deployment Monitoring Agent and displays the **Batch deploy** window, as shown in Figure 46.

**Figure 46 Batch deploy**

2. Select the subcomponents you want to deploy on the master server. In this example, select **MPLS VPN Manager - MPLS VPN Management** and **MPLS VPN Manager - MPLS Management** and click **OK**.

The **Deploying** window appears, as shown in Figure 47.
After the deployment is complete, the **Batch deploy succeeded** window appears, as shown in Figure 48.

**Figure 48 Batch deploy succeeded**

3. Clear the **Open readme file directory** and **Start iMC Server now** options and click **OK**.

**Deploying MVM subcomponents on a subordinate server**

1. If the Intelligent Deployment Monitoring Agent is not installed on the subordinate server, install it first. (Details not shown.)
   For more information about installing the Intelligent Deployment Monitoring Agent, see "Deploying the IMC Platform on a subordinate server."

2. Start the Intelligent Deployment Monitoring Agent:
3. Click the **Deploy** tab in the Intelligent Deployment Monitoring Agent. The **Deploy** tab displays all IMC components that have been installed and their deployment information, as shown in Figure 49.

**Figure 49 Information about component deployment**

![Image of deployment information](image.png)

4. Right-click any component in the list, and then select **Batch Deploy** from the shortcut menu. The **Batch deploy** window displays components that are not deployed, as shown in Figure 50.
5. Select subcomponents you want to deploy. In this example, select **MPLS VPN Manager - MPLS VPN Management** and **MPLS VPN Manager - MPLS Management**.

6. Click **OK** to start the deployment.

The system displays the deployment progress on the **Deploying** page, as shown in Figure 51.

**Figure 51 Deploying**
7. In the **Please Choose L2VPN Global Parameter Operate** window (see Figure 52), configure the L2VPN parameters as needed. This example uses the default values of the parameters.

If **BGP** (Border Gateway Protocol) is selected for **VPLS** (Virtual private LAN service), **VLL** (virtual leased line) and **PBB** (provider backbone bridge) options are automatically cleared.

**Figure 52 Please Choose L2VPN Global Parameter Operate**

![](image)

8. Click **Deploy**.

The **Deploying** window appears, as shown in Figure 53.
After the deployment is complete, the **Batch deploy result** dialog box appears, as shown in Figure 54.

**Figure 54 Batch deploy succeeded**

9. Click **OK**.
10. Start IMC on the master server:
a. Start the Intelligent Deployment Monitoring Agent:
   - On Windows, select Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent.
   - On Linux, run the dma.sh script in the /deploy directory of the IMC installation path.

b. On the Monitor tab, click Start iMC.
   A confirmation dialog box appears.

c. Click OK to start the IMC service.

Installing and deploying IMC UAM

UAM includes the following subcomponents:
- Intelligent Strategy Proxy
- User Access Management
- Portal Server
- EIP Server
- EIP Sub Server
- Policy Server
- Policy Proxy Server
- User SelfService
- User Access Management Sub Server
- Third-Party Page Publish Server

HP recommends that you deploy all UAM subcomponents except EIP Sub Server and User Access Management Sub Server as follows:
- On networks with moderate traffic load, deploy these subcomponents only on a subordinate server.
- On networks with high traffic load, deploy these subcomponents on the master server and a subordinate server at the same time.

EIP Sub Server and User Access Management Sub Server can be deployed only on a subordinate server. This example deploys EIP Sub Server and User Access Management Sub Server on a subordinate server and other subcomponents on the master server.

Installing IMC UAM

1. Install IMC UAM on the master server in the same way IMC NTA is installed. (Details not shown.)
   For information about the installation procedures, see "Installing IMC NTA."

2. In the Installation Completed window (see Figure 55), select Open deployment monitoring agent and click Finish.
Deploying UAM subcomponents on the master server

1. In the **Installation Completed** window (see Figure 55), select **Open deployment monitoring agent** and click **Finish**.

   The system automatically starts the Intelligent Deployment Monitoring Agent and displays the **Batch deploy** window, as shown in Figure 56.
2. Select subcomponents you want to deploy. In this example, select all UAM subcomponents except User Access Management Sub Server and EIP Sub Server.

3. Click **OK** to start the deployment.

4. In the **Strategy Proxy Server Configuration** window (see Figure 57), configure the following parameters:
   
   a. Enter the IP address of the host on which Strategy Proxy Server is to be deployed in the **IPv4 Address(Client)** field. In this example, use the default value of the parameter.
   
   b. Enter the IP address of the host on which User Access Management Sub Server is to be deployed in the **IPv4 Address(Server)** field. In this example, use the default value of the parameter.
If Strategy Proxy Server and User Access Management are deployed on the same host but associated with different NICs, enter the IP addresses of the NICs in the two fields.

5. Click **Deploy**.

6. In the **Configure User Access Management** window (see Figure 58), configure the following parameters:
   - **Database Password/Confirm Password**—These fields are automatically populated with the database password configured when the IMC Platform is installed. Do not change the values of these fields unless the database password of the IMC Platform is changed after installation.
   - **UAM Server's IPv4 Address**—This field displays the IP address of the host on which UAM is to be deployed. By default, the IP address of the current host is displayed. Use the default value in this example.
7. Click **Deploy**.

8. In the **Configure Portal Component** window (see Figure 59), configure the following parameters:
   a. Enter the IP address of the host where the portal server is to be deployed in the **Portal Server's IPv4 Address** field. In this example, use the default value of the parameter.
   
b. Enter the HTTP port number of the Apache server in the **Apache Server's Http Port** field. In this example, use the default value (8888) of the parameter.
9. Click Deploy.

10. In the Configure EIP Server window (see Figure 60), enter the IP address of the host where the EIP server is to be deployed in the EIP Server’s IPv4 Address field. In this example, use the default value of the parameter.

Figure 60 Configure EIP Server
11. Click **Deploy**.

12. In the **Configure Policy Server** window (see Figure 61), enter the IP address of the host where Policy Server is to be deployed in the **Policy Server’s IPv4 Address** field. In this example, use the default value of the parameter.

**Figure 61 Configure Policy Server**

13. Click **Deploy**.

14. In the **Configure User SelfService** window (see Figure 62), enter the IP address of the host where User SelfServer is to be deployed in the **User SelfServer’s IPv4 Address** field. In this example, use the default value of the parameter.
15. Click **Deploy**.

16. In the **Third-Party Page Publish Server Configuration** window (see Figure 63), enter the port number in the **HTTP Port** field. In this example, use the default value (8899) of the parameter.

**Figure 63 Third-Party Page Publish Server Configuration**

![Third-Party Page Publish Server Configuration](image)

17. Click **Deploy**.
After the deployment is complete, the **Batch deploy succeeded** dialog box appears, as shown in Figure 64.

**Figure 64 Batch deploy succeeded**

18. Click **OK**.

### Deploying UAM subcomponents on a subordinate server

1. If the Intelligent Deployment Monitoring Agent is not installed on the subordinate server, install it first. (Details not shown.)
   For information about how to install the Intelligent Deployment Monitoring Agent, see "Deploying the IMC Platform on a subordinate server."

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

3. Click the **Deploy** tab in the Intelligent Deployment Monitoring Agent.
   The **Deploy** tab displays all IMC components that have been installed and their deployment information, as shown in Figure 65.
4. Right-click any component in the list, and then select **Batch Deploy** from the shortcut menu. The **Batch deploy** window displays components that are not deployed.

**Figure 66 Batch deploy**

5. Select subcomponents you want to deploy. In this example, select **User Access Manager - EIP Sub Server** and **User Access Manager - User Access Management Sub Server**.

6. Click **OK**.

After files are downloaded, the system automatically deploys the components.
7. In the **Configure EIP Server** window (see Figure 67), enter the IP address of the host where EIP Sub Server is to be deployed in the **EIP Server’s IPv4 Address** field. In this example, use the default value of the parameter.

![Figure 67 Configure EIP Server](image)

8. Click **Deploy**.

9. In the **Configure User Access Management Sever** window (see Figure 68), enter the IP address of the host where User Access Management Sub Server is to be deployed in the **UAM SUB Server’s IPv4 Address** field. In this example, use the default value of the parameter.

![Figure 68 Configure User Access Management Sever](image)
10. Click **Deploy**.
   After the deployment is complete, the **Batch deploy result** dialog box appears, as shown in **Figure 69**.

   **Figure 69 Batch deploy result**
   ![Batch deploy result dialog box]

11. Click **OK**.

12. Start IMC on the master server:
   a. Start the Intelligent Deployment Monitoring Agent:
      - On Windows, select **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent**.
      - On Linux, run the **dma.sh** script in the `/deploy` directory of the IMC installation path.
   b. On the **Monitor** tab, click **Start iMC**.
      A confirmation dialog box appears.
   c. Click **OK** to start the IMC service.
5 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 allows IMC to obtain the names of terminals, such as servers, PCs, and printers, from the DHCP server. To accomplish this, make sure that the following conditions exist:

- 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.

This section describes how to install DHCP plug-ins on MS DHCP and Linux DHCP servers respectively.

Installing DHCP plug-ins on the MS DHCP server

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

1. Modify the file qvdm.conf, so that 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 IP address of the master server 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 server 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, right-click the IMC DHCP Plug service on the Services (Local) list, and select Start to start the IMC DHCP plug service.

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

Installing DHCP plug-ins on the Linux DHCP server

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

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 Notepad to open the qvdm.conf file in the \server\conf directory of the IMC installation path on the Windows server running IMC.
   b. Add the following line to the file:
      
      l2topoPCNameDhcpSwitch=1
   c. Save and exit the file, and restart IMC in the Intelligent Deployment Monitoring Agent.

2. Install the IMC DHCP plug-in on the Linux DHCP server.
   The DHCP plug-in installer dhcp-plug-linux.zip is saved in the tools directory of the IMC Linux installer.
   a. Copy the plug-in installer to the Linux DHCP server.
   b. Decompress the installer.
   c. Use the VI editor to open the imf.cfg file in the /server/imf/server/conf directory of the dhcp-plug-linux folder.
   d. Modify the IMGAddress into the IMC server IP address, and modify the IMGPort (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. If the file does not exist, enter the /server/conf/ directory of the dhcp-plug-linux folder, and use the VI editor to open the qvdm.conf file, and add the following line to the file to specify the path of the dhcpd.leases file.
       
       DhcpPlugIpAllocPath=<Current path>/dhcpd.leases
   c. Save and exit the file.

4. Execute the install.sh script in the dhcp-plug-linux folder.
After the installation is complete, the dhcp-plug service is added to the system services, and has been automatically started.

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

---

**NOTE:**
To uninstall a DHCP plug-in, run the file `uninstall.sh` in the `dhcp-plug-linux` directory.

---

**Installing VRM agent plug-ins**

Virtual Resource Management (VRM) is a subcomponent of the IMC Platform to manage virtual networks. It must work with a VRM Windows or Linux agent for virtual network management.

**Installing a VRM Windows agent**

If Microsoft Hyper-V servers exist in the network, you must install VRM Windows agents for IMC to manage the Hyper-V servers.

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

---

**CAUTION:**
VRM 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 VRM Windows agent.

---

A VRM Windows agent is dependent on .NET Framework 4.5, and PowerShell 3.0. Before you install a VRM Windows agent plug-in, make sure that all the software applications are installed. For the Windows Server 2008 R2 system, they are installed by default. For other Windows operating systems, go to the Microsoft official website to download and install them.

1. The installation file vrm-plug-windows.zip of a VRM Windows agent is stored in tools folder of the IMC installation package. Decompress the file and copy the file to a directory of the server where the VRM Windows agent is to be installed.

2. Run `Register.bat` in the `vrm-plug-windows` folder. If all the related software applications are installed, the installation process is complete. Otherwise, the system prompts you to install the required software and quit the installation process. In this case, install the required software and then start the installation process again.

Do not delete the `vrm-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 `vrm-plug-windows\server\imf\server\conf` directory. Modify IMGAddress as the IP address of the primary IMC server and IMGPort as the MBP port number (8800 by default). Save your settings and quit.

4. Start the IMC VRM 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 VRM Agent** on the **Services (Local)** list, and select **Start** to start the VRM Windows agent service.

**NOTE:**

To uninstall a VRM Windows agent, run the file **UnRegister.bat** in the **vrm-plug-windows** directory.

---

**Installing a VRM Linux agent**

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

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

**Installation prerequisites**

The VRM Linux agent is a 32-bit program and applies only to Red Hat.

To install VRM Linux agent on 32-bit Red Hat Enterprise Linux 5.0 and 5.5, select a network server. No other software package is required.

To install VRM Linux agent on 64-bit Red Hat Enterprise Linux 6.X, first install the following 32-bit program packages:

- `compat-libcap1-1.10-1.i686.rpm`
- `glibc-2.12-1.107.el6.i686.rpm`
- `keyutils-libs-1.4-4.el6.i686.rpm`
- `krb5-libs-1.10.3-10.el6.i686.rpm`
- `libaio-0.3.107-10.el6.i686.rpm`
- `libcom_err-1.41.12-14.el6.i686.rpm`
- `libgcc-4.4.7-3.el6.i686.rpm`
- `libidn-1.18-2.el6.i686.rpm`
- `libssh2-1.4.2-1.el6.i686.rpm`
- `libstdc++-4.4.7-3.el6.i686.rpm`
- `nspr-4.9.2-1.el6.i686.rpm`
- `nss-3.14.0-0.12.el6.i686.rpm`
- `nss-softokn-freebl-3.12.9-11.el6.i686.rpm`
- `nss-utility-3.14.0-0.2.el6.i686.rpm`
- `openssl-1.0.0-27.el6.i686.rpm`
- `sshd-2.4.23-31.el6.i686.rpm`
- `sshd-keygen-1.05-1.el6.rf.i686.rpm`
- `sshd-1.0.0-27.el6.i686.rpm`

This example uses Red Hat Enterprise Linux 6.4. For other Red Hat Enterprise Linux 6.X, make sure the package names are the same.

To install the packages, perform the following tasks:

1. Log in to Red Hat Enterprise Linux as a root user.
2. Place the Linux installation disk to the CD-ROM drive and enter the directory where packages are saved.

3. Copy the packages to the local directory and download sshpass-1.05-1.el6.rf.i686.rpm from the network.

4. Launch the **Terminal** window and enter the directory where packages are saved.

5. Execute the command to install packages, where xxx indicates the package name.

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

---

**Installation and configuration procedure**

1. Enter the **tools** directory on the IMC installation disk, copy file `vrm-plug-linux.zip` to a local disk drive, and decompress the file.

2. Run the `install.sh` script in the decompressed file folder.

3. Enter the IP address of the master server. The default setting is `localhost`.

4. Run `ps –ef | grep imcvrmagent` to verify the installation is successful.

   When the agent is successfully installed, you can see the `imcvrmagent` process is running.

---

**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 (for example, through a wireless connection).

Follow these steps 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.

   * `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.

   If the message **Programs from unknown sources are not allowed to install** appears during installation, go to **Settings > Applications** and select **Unknown source**.

Follow these steps to log in to IMC:

3. Open the client program.

4. 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). If 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.

5. Select Save password or Auto Login as needed.

If you select Save password, you do not need to enter the password for the next logins. If you select Auto Login, you do not need to enter the login name and password for the next logins.

6. 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 tasks.
- Play IMC videos.

---

**NOTE:**

If RADIUS authentication or LDAP authentication is used or if you change the login password, you must first log in to IMC from a PC successfully before you can use a mobile client to log in to IMC.

---

### Installing LLDP agent plug-ins

When the VRM 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
- lldp-agent-windows.zip

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

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

---

**IMPORTANT:**

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

---

### Installing an LLDP Linux agent

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

To install and configure an LLDP Linux agent:
1. Set executable permission to the `install.sh` script and run the script in the LLDP Linux agent installation file folder.
   The LLDP Linux agent is installed.

2. Configure the LLDP Linux agent.
   The configuration file `lldpagent.conf` is located in the `conf` directory of the LLDP Linux agent installation file folder.

   LLDP agent plug-ins support either LLDP or CDP, but not both at the same time. By default, the plug-ins support LLDP. To enable an LLDP agent to support CDP:
   a. Open the `lldpagent.conf` file in the `conf` directory.
      
      `vi lldpagent.conf`
   b. Delete the pound sign (#) from the string `#Agent=CDP`.

   You can set the interval at which LLDP or CDP packets are sent. The default setting is 300 seconds. To change the setting, delete the pound sign (#) from the string `#INTERVAL=300` and then change the value.

3. Restart the lldp-agent service.
   
   `service lldp-agent restart`

**Installing an LLDP Windows agent**

LLDP Windows agent plug-ins support 32-bit and 64-bit Windows operating systems.

To install and configure an LLDP Windows agent:

1. Run the `install.bat` script in the LLDP Windows agent installation file folder.
   The LLDP Windows agent is installed.

2. Configure the LLDP Windows agent.
   
   The configuration file `lldpagent.conf` is located in the `conf` directory of the LLDP Windows agent installation file folder.

   LLDP agent plug-ins support either LLDP or CDP, but not both at the same time. By default, the plug-ins support LLDP. To enable an LLDP agent to support CDP:
   a. Open the `lldpagent.conf` file in the `\Program\lldpAgent` directory on the Windows system disk.
   b. Delete the pound sign (#) from the string `#Agent=CDP`.

   You can set the interval at which LLDP or CDP packets are sent. The default setting is 300 seconds. To change the setting, delete the pound sign (#) from the string `#INTERVAL=300` and then change the value.

3. Restart the lldp-agent service.
6 Logging into IMC

IMC is a browser-based management tool. HP recommends accessing IMC with the following Web browsers:

- Internet Explorer 10 or 11
- Firefox 30 or later
- Chrome 35 or later

Accessing IMC

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

1. Enter the IMC login page, use one of the following methods:

   - Through HTTP
     Enter http://192.168.4.44:8080/imc in the address bar of your browser and press Enter. The portion 192.168.4.44 is the IP address of the master server, and 8080 is the HTTP port set during the IMC Platform deployment. A security certificate message appears. For more information, see IMC Getting Started Guide.

   - Through HTTPS
     Enter http://192.168.4.44:8443/imc in the address bar of your browser and press Enter. The portion 192.168.4.44 is the IP address of the master server, and 8443 is the HTTPS port set during the IMC Platform deployment. A security certificate message appears. For more information, see IMC Getting Started Guide.

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

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

   IMPORTANT:
   Change the admin password immediately after the initial login.

Securing IMC

HP recommends performing the following tasks to secure IMC:

- Create individual administrative user accounts and disable the default admin account.
- Tie the administrative accounts to a central AAA server via LDAP or RADIUS.
- Retain one administrative account (not named admin) with a local password to recover from loss of access to the AAA server.
- Enable the verification code feature on the IMC login page. For more information, see IMC Getting Started Guide.

See v7.1 HP Intelligent Management Center Base Platform Administrator Guide.
Accessing UAM

There are several web-based features in UAM that have different URLs than IMC.

- 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

  Where, 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.

- 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, where 192.168.4.22 is the IP address of the server where the SOM service desk is deployed, and 8080 is the HTTP port number set the first time the IMC Platform subcomponents were deployed.

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

Table 10 Hardware and browser requirements

<table>
<thead>
<tr>
<th>OS</th>
<th>Hardware</th>
<th>Browser version</th>
<th>Browser setting requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>• CPU: 2.0 GHz or higher&lt;br&gt;• Memory: 2 GB or higher&lt;br&gt;• Hard Disk: 20 GB or higher&lt;br&gt;• CD-ROM: 48 X or higher&lt;br&gt;• Network Adapter: 100 Mbps or higher&lt;br&gt;• Sound card: Required&lt;br&gt;• Display: Recommended width 1280</td>
<td>• IE 10 or 11&lt;br&gt;• Firefox 30 or later&lt;br&gt;• Chrome 35 or later</td>
<td>• Turn off the pop-up blocker in Internet Explorer.&lt;br&gt;• Enable Cookies in Internet Explorer.&lt;br&gt;• Add IMC as a trusted site.</td>
</tr>
</tbody>
</table>

JRE 1.6.0_update10 or later is recommended. If a client has no JRE, IMC prompts the user to install JRE for the client.

If IMC can be accessed from an IMC server, but nowhere else, make sure the Web service ports of IMC are open in the firewall settings on the IMC master server.

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 Notepad (as administrator) 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.html`.
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-login to IMC. 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.

Figure 70 User agreement on login page
7 Upgrading, backing up, or removing IMC

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

Before you upgrade IMC, complete the following tasks:
- Download upgrade packages of the correct version from the HP website.
- Back up the database and IMC installation path. For more information, see "Backing up IMC."

Back up IMC

To back up the IMC installation directory and database files:
- Use DBMan in the Intelligent Deployment Monitoring Agent of the master server to back up database files.
- Manually copy the IMC installation directory on master and subordinate servers to specific paths.

Upgrading IMC

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

In distributed deployment mode, upgrade all components deployed on subordinate servers separately. The following example describes how to upgrade the IMC Platform on Windows.

1. Use one of the following methods to start the upgrade:
   - On the **Installation Completed** window as shown in Figure 9, select **Install Other Components**, and click **Finish**.
   - After you have installed and deployed the IMC Platform, click **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent** (or run the `dma.sh` script in `/deploy` of the IMC installation path on Linux), to start the Intelligent Deployment Monitoring Agent and then click **Install new components** on the **Monitor** tab.
IMPORTANT:

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

- To upgrade IMC in Windows Server 2008 or Windows Server 2008 R2, you must first select Start > All Programs > HP Intelligent Management Center. Then right-click Deployment Monitoring Agent, and select Run as Administrator from the shortcut menu to open the deployment monitoring agent.

2. On the system tray of Windows, right-click the Deployment Monitoring Agent icon, and select Install from the menu.

The Choose folder window appears, as shown in Figure 71.

Figure 71 Choose folder

![Choose folder window](image)

3. Click Browse, and select folder install\components in the upgrade files.

4. Click OK.

The Welcome to HP iMC Installation Wizard window appears, as shown in Figure 72.

Figure 72 Welcome to HP iMC Installation Wizard

![Welcome to HP iMC Installation Wizard](image)
5. Click **Next**.

The **Agreement** window appears, as shown in **Figure 73**.

**Figure 73 Agreement**

6. Read the license agreement carefully, select **Accept**, and click **Next**.

The **Upgrade Common Components** window appears, as shown in **Figure 74**.

**Figure 74 Upgrade Common Components**

7. Click **OK**.

The system automatically upgrades common components, as indicated by the **Upgrade Common Components** window in **Figure 75**.

**Figure 75 Upgrade Common Components**
After the common components are upgraded, the **Choose Target Folder** window appears, as shown in **Figure 76**.

**Figure 76 Choose Target Folder**

![Choose Target Folder window](image)

The **Choose Target Folder** window displays the components to be upgraded. The system will install the upgrade files in the location where the IMC Platform is installed.

8. Check the information and click **Next**.

The **Deployment and Upgrade Options** window appears, as shown in **Figure 77**.
9. Select **Deploy or upgrade at once** or **Deploy or upgrade later** as needed. In this example, select **Deploy or upgrade at once**.

The **Installation Summary** window appears, as shown in Figure 78.

**Figure 78 Installation Summary**

10. Check the installation information and click **Install**.
The **Installing** window appears, as shown in Figure 79.

**Figure 79 Installing**

![Installing window](image)

The wizard is installing the components. The installation will take a while. The time needed depends on the size of the components.

Note that the iMC is not ready for use right after installation. You need to proceed with iMC platform and components deployment.

When the installation is complete, the wizard will guide you through the component deployment.

The iMC supports distributed deployment. On the iMC Web-based management interface, you can select System > Component Deployment to deploy specified components on other computers for load sharing. This brings more efficiency to the HP iMC.

The installation wizard installs the components. Installation takes awhile.

**Upgrading components on the master server**

After the installation is finished, the **Batch upgrade** window appears, as shown in Figure 80.
1. Select the components you want to upgrade, and then click OK.
   After the selected components are upgraded, the Batch upgrade result window appears, as shown in Figure 81.

   Figure 81 Batch upgrade result

2. Click OK.
   If you have used DBMan for IMC auto backup or restoration before upgrade, the Auto Backup and Restore Configuration window appears after you click OK.

3. Click OK in the Auto Backup and Recovery Settings window to upgrade automatic backup and restoration configuration.

Upgrading components on a subordinate server

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. 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 of the master server.

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

Before you can complete upgrade to IMC 5.1 or later in distributed mode, follow the instructions on the popup dialog box (see Figure 82) to upgrade the Oracle database configuration for communication between the master and subordinate servers.

**Figure 82 Important message**

![Important Message](image)

RESTORING IMC

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:

1. Restore the IMC database. See "Manual restoration."
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 on master and subordinate servers.
4. Copy the backed up IMC installation directory to the IMC installation path on master and subordinate servers.

5. Restart the Intelligent Deployment Monitoring Agent and IMC service.

Removing IMC

The IMC uninstallation 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 more than one server, remove it first from all subordinate servers and then from the master server.

To remove an IMC component from a subordinate server:

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

To remove an IMC component from the master server:

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

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.
Removing all IMC components at one time

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.

NOTE:
- When reinstalling IMC, you must manually delete the folder named imcdata, which is created on the master server upon previous installation of IMC if you have re-installed an SQL server database after you uninstalled IMC.
- If 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.

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.
   Confirmation dialog boxes appear.
5. Click OK.
   After the uninstallation is complete, the uninstallation result window appears.
6. In the Uninstallation Completed dialog box, clear the OS reboot option and click OK.
7. 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).
8. Reboot the system.

Follow the same procedures to remove IMC on all other servers.
8 Registering IMC and incremental node licenses

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

The IMC registrations on Windows and Linux systems are similar. The following describes how to register IMC on a Windows Server 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, as shown in Figure 83.

Figure 83 License Information

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

Registering the first license

1. Go to the HP My Networking system website (http://hp.com/networking/mynetworking/), log in to My Networking portal, and the HP Passport sign-in page appears, as shown in Figure 84.
2. Enter the **User ID** and **Password**, and then click **Sign in**. The **Home** page appears, as shown in **Figure 85**.

**Figure 85 Home page**

3. Click **Register license** under the **Licenses** section of the home page. The **Enter Order number or Registration ID** page appears, as shown in **Figure 86**.
4. Enter the **Order number** or **Registration ID**, and click **Next**.

The **Enter the email associated with Order number** page appears, as shown in **Figure 87**.

**Figure 87 Enter the email associated with Order number page**

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

The **Select the Product License** page appears, as shown in **Figure 88**.

**Figure 88 Select the Product License page**
6. Select the product you want to register by activating the radio button to the left of Prod #.

7. Enter the quantity to be redeemed, and then click **Next**.

The **Enter details** page appears, as shown in Figure 89.

**Figure 89 Enter details page**

<table>
<thead>
<tr>
<th>Enter Registration ID or order number</th>
<th>Enter details</th>
<th>License agreement</th>
<th>Confirmation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please select the base product that will receive this license</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order number</td>
<td>R7703263BBB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product number</td>
<td>M2F21AAE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product name</td>
<td>HP IMC Ent SW Pkfm w/200-node E-LTU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redeem quantity</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base product number</td>
<td>50111-5194</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base product name</td>
<td>Base software for IMC Enterprise Edition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base software serial number*</td>
<td>Enter the software serial number here</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friendly name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer notes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

The **License agreement** page appears, as shown in Figure 90.

**Figure 90 License agreement page**

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

The **Confirmation** page appears, as shown in Figure 91.
10. Click **Save as** to download and save the license key file. Remember the location and file name for the next step of Activating the License in IMC.

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

**Registering incremental node licenses**

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

To register an Incremental Node license:

1. Select the Incremental Node License you want to register on the **Select the Product License** page, as shown in Figure 92.
2. Click **Next**.

The **Enter details** page appears, as shown in Figure 93.

**Figure 93 Enter details page**

3. Select your base product and enter the Base software serial number, and then click **Next**.

The **Confirmation** page appears, as shown in Figure 91.

4. Click **Save as** to download and save the license key file.

You need to remember the location and file name for the next step of Activating the License in IMC.
Activating IMC

To activate IMC:

1. Return to the License Information page, as shown in Figure 83.
2. Select Activate now.
   The Activate Your Product page appears, as shown in Figure 94.

   **Figure 94 Activate Your Product**

3. Select the license file in the format of .txt.
4. Select the license type, which can be Register/Activate host license or Register/Activate back-up license, as needed.
5. Click OK.
   The Activations Succeeded dialog appears, as shown in Figure 95.

   **Figure 95 Activation Succeeded**

6. Reboot the system.
   Your IMC system has now been successfully Registered and Activated.

Registering the IMC license for stateful/stateless failover

Registering the IMC license for stateful failover

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

**Figure 97 Registering your product**

13. Click **Browse** to select the locally saved IMC license file.
14. Select **Register/Activate host license** from the **Please select the license's type** list.
15. Click **OK**.
16. Reboot the IMC.
The IMC has been successfully activated.
Registering the IMC license for stateless failover

When registering the IMC license for stateless failover, only the serial number of the primary server is required to get the license file. Use this file on both the IMC primary server and the IMC backup server to activate the license.

1. Run IMC on the primary server.
2. After the IMC starts up, access the IMC login page of the primary server.
3. Click **Activate**.
   
   The **License Information** page appears.

   **Figure 98 License information**

   ![License Information](image)

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

   **Figure 99 Registering your product**

   ![Registering your product](image)

10. Click **Browse** to select the locally saved IMC license file.
11. Select **Register/Activate host license** from the **Please select the license's type** list.
12. Click OK.

13. Reboot the IMC.
   
   The IMC has been successfully activated on the primary server.

14. Access the IMC login page of the backup server.

15. Click **Activate**.
   
   The **License Information** page appears.

16. Click **Activate Now**.
   
   The registration page appears.

17. Click **Browse** to select the locally saved IMC license file. (This license file is the same as the file used for the IMC registration on the host.)

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

   **Figure 100 Registering your product**

   ![Register Your Product](image)

<table>
<thead>
<tr>
<th>License File *</th>
<th>Browse...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please select the license’s type *</td>
<td>Register/Activate back-up license</td>
</tr>
</tbody>
</table>

19. Click **OK**.

20. Reboot the IMC.
   
   The IMC has been successfully activated on the backup server.

### Upgrading to an IMC V7.1 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 V7.1.

You need to download your updated IMC license file from My Networking and reactivate your IMC V7.1.

To update your IMC license file from My Networking and reactivate your IMC V7.1:

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.

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

3. Log in to My Networking

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

5. Locate your IMC licenses

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

7. Click on **View Licenses** from the **My Licenses** navigation.

8. Locate your IMC Platform license in the list of your licenses. When necessary copy and paste your IMC serial number into the search field and click **Search**.

9. Download the updated IMC license file

10. Click corresponding to the IMC Platform license. The license information page appears.

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

12. Choose to save the license file, and choose where to save the license file. Save the license file so that you can locate it again when you need it.

### Updating your IMC V7.1 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 V7.1 is now fully licensed with the equivalent licenses you had previously.
9 Security settings

Anti-virus software

To ensure secure operations, HP recommends installing anti-virus software on IMC servers and keeping the virus definitions up to date.

Port settings

⚠️ CAUTION:
- HP recommends using ACL configurations on a firewall rather than on a switch to control data packets. Otherwise, packet fragmentations will be filtered.
- If you have installed firewall software on the IMC server, besides setting the ports listed in Table 11, set an IP address for the master server and all subordinate and database servers to ensure correct communication between them.

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

Table 11 and Table 12 list the port numbers sent to the IMC server. In this way, you can prevent abnormal attacks.

Table 11 Ports used by the IMC Platform

<table>
<thead>
<tr>
<th>Default port number</th>
<th>Usage</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 8080, configurable</td>
<td>HTTP access to IMC</td>
<td>IMC master server</td>
</tr>
<tr>
<td>TCP 8443, configurable</td>
<td>HTTPS access to IMC</td>
<td>IMC master server</td>
</tr>
<tr>
<td>TCP 61616</td>
<td>Java Message Broker</td>
<td>IMC master server</td>
</tr>
<tr>
<td>UDP 161</td>
<td>Port to add a device to 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>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>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>

A sample of the Windows Firewall configuration after IMC platform installation is:

```bash
netsh advfirewall firewall add rule name="HP IMC HTTP" protocol=TCP localport=8080 action=allow dir=IN
netsh advfirewall firewall add rule name="HP IMC" protocol=TCP localport=61616 action=allow dir=IN
```

**NOTE:**

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.
10 Database backup and restoration

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.

Basic database backup and restoration operations

DBMan supports both manual and automatic database backup and restoration. It is integrated in the Intelligent Deployment Monitoring Agent, as shown in Figure 101.

Figure 101 Environment tab

On the left of the Environment tab displays the software and hardware information of the server(s), on the right displays the usage of the user database file and log file, and at the bottom is the DBMan database backup and restoration configuration area, which includes:

- **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 all data files (including running configuration files and database files) of the current IMC server.
- **Restore**—Replace the current database files with the backup database files to restore the database to the specified time point.
- **View Log**—View the database backup and restoration log.

**NOTE:**
To ensure correct operation of IMC, do not back up and restore database between different OSs.

**Manual backup**

Manual backup allows you to manually back up IMC databases immediately.

To perform a manual backup:

1. Start the Intelligent Deployment Monitoring Agent on the server.
2. Click the **Environment** tab as shown in Figure 101.
3. Click **Backup**.
   A confirmation dialog box appears.

   **Figure 102 Confirmation dialog box**

   ![Confirmation dialog box](image)

   - To prevent data loss or inconsistency, make sure you backup or recover all data for the distributed IMC platform and components. Do you want to continue?

   ![Yes | No](image)

4. Click **Yes**.
   The **Select database backup path** dialog box appears.
5. Select the backup file save path.
6. Click **OK**.
   DBMan starts to back up all databases files on the master and subordinate servers to the specified path.

**Automatic backup**

You can configure DBMan to periodically back up the IMC data files to the local database, and to upload the backup data files to the FTP server, master server, or the backup server in stateless failover scenarios.

To configure automatic backup:

1. Start the Intelligent Deployment Monitoring Agent on the master server.
2. Click the **Environment** tab.
3. Click **Configure**.
   The **Auto Backup and Recovery Settings** dialog box appears, as shown in Figure 103.
4. Read the prompt on the Auto Backup and Recovery Settings dialog box carefully, select Auto Backup Model, and click OK, as shown in Figure 103.

The Auto Backup and Recovery Settings window appears, as shown in Figure 104.

Figure 104 Auto Backup mode
5. Click the **Basic Configuration** tab and configure the following parameters:
   - **Daily backup time (HH:mm)** — Enter the time at which the automatic backup operation starts every day. By default, the daily backup time is 04:00.
   - **Master Server IP of Backup System** — Enter the IP address of the master server in the backup system. This option is applicable to database backup in stateless failover scenarios. Make sure automatic restoration is enabled for the backup system.

6. Click the **Primary Server** tab and configure the following parameters:
   - **Storage Path of Other Files** — Enter or browse to the path where the backup data files are stored on the master server.
   - **Local Back Up** — Select the boxes in the **Local Back Up** column for the databases you want to back up on the master server. By default, the boxes in the **Local Back Up** column are selected for all databases. You can select or clear the boxes for all databases.
   - **Upload To Backup System** — Select the box in the **Upload To Backup System** column for a database on the master server to upload the database file to the specified FTP server or the master server of the backup system. By default, the boxes in the **Upload To Backup System** column are cleared for all databases. You can select or clear the boxes for all databases. After you select this box, you must configure the FTP server, the master server IP of the backup system, or both.

7. Click the **Subordinate Server** tab and configure the following parameters:
   - **Storage Path of Other Files** — Enter or browse to the path where the backup data files are stored on a subordinate server.
   - **Local Back Up** — Select the boxes in the **Local Back Up** column for the databases you want to back up on a subordinate server. By default, the boxes in the **Local Back Up** column are selected for all databases. You can select or clear the boxes for all databases.
   - **Upload To Backup System** — Select the box in the **Upload To Backup System** column for a database on a subordinate server to upload the database file to the specified FTP server or the master server of the backup system. By default, the boxes in the **Upload To Backup System** column are cleared for all databases. You can select or clear the boxes for all databases. After you select this box, you must configure the FTP server, the master server IP of the backup system, or both.

8. Click the **Extension Configuration** tab and configure the following parameters:
   - **Backup file lifetime (days)** — Enter how many days a backup database file can be kept. Expired files are automatically deleted.
   - **Delete local files after upload even if upload fails** — Specify whether to delete local backup files after uploading the backup files to the FTP server or the backup server. To configure the FTP server, manually create or configure the `dbman_ftp.conf` file in the `\dbman\etc` directory of the IMC installation directory. The configuration file includes the configuration items `ftp_ip`, `ftp_user`, and `ftp_password` in the following format:
     ```
     ftp_ip=1.1.1.1
     ftp_user=admin
     ftp_password=1234
     ```
   - **Upload backup files of Subordinate Servers to Master Server** — Specify whether to upload local backup files from subordinate servers to the master server.

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

10. Click **OK**.
Manual restoration

⚠️ CAUTION:
HP recommends restoring database files for the IMC Platform and deployed components together. If you restore only some of them, data loss or inconsistency might occur.

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

Manual restoration includes the following types:

- **Locally Restore**—Applicable to scenarios where all backup files are saved on the master server. For example, manually backed up files, backup files uploaded to the master server, and backup files uploaded by using FTP.

- **Remotely Restore**—Applicable to scenarios where backup files are saved on the master and subordinate servers. The master server locates the path that saves the backup files on the master and subordinate servers and then restores them. Before performing remote restoration, you must configure automatic backup and restoration parameters. Then DBMan can automatically locate running configuration files and database files.

To perform a manual restoration:
1. Start the Intelligent Deployment Monitoring Agent on the master server.
2. Click the Environment tab.
3. Click Restore.
   
   The Restoration Type dialog box appears.

   ![Restoration Type dialog box](image)

4. Perform one of the following tasks:
   
   If all backup files are saved on the master server:
   
   a. Click Locally Restore.
      
      The Confirm dialog box appears.

      ![Confirmation dialog box](image)

   b. Click Yes.
      
      The dialog box for selecting the databases to restore appears.
c. Select database files to be restored and click **OK**.
   The **Confirm** dialog box appears.

   **Figure 107 Confirmation dialog box**
   ![Confirmation dialog box](image)
   Do you want to start IMC immediately after restoring it?
   Yes  No

   **Figure 108 Configure Remote Restoration dialog box**
   ![Configure Remote Restoration dialog box](image)
   Please first configure the databases to be restored. Select the database files (.db) from the database backup path of automatic backup, and then click **OK** to restore the databases.
   1.127.0.0.1
   192.166.1.223
   File List
   Configure
   OK  Cancel

   b. Click **Configure** to select the database files to be restored on the master and subordinate servers and click **OK**.
   The **Confirm** dialog box appears.

   **Figure 109 Confirmation dialog box**
   ![Confirmation dialog box](image)
   Do you want to start IMC immediately after restoring it?
   Yes  No

   c. Click **Yes**.

   d. Click **Yes**.
   DBMan starts to restore the databases.

If backup files are saved on the master and subordinate servers:

a. Click **Remotely Restore**.
   The **Configure Remote Restoration** dialog box appears.

   **Figure 108 Configure Remote Restoration dialog box**
   ![Configure Remote Restoration dialog box](image)
   Please first configure the databases to be restored. Select the database files (.db) from the database backup path of automatic backup, and then click **OK** to restore the databases.
   127.0.0.1
   192.166.1.223
   File List
   Configure
   OK  Cancel

   b. Click **Configure** to select the database files to be restored on the master and subordinate servers and click **OK**.
   The **Confirm** dialog box appears.

   **Figure 109 Confirmation dialog box**
   ![Confirmation dialog box](image)
   Do you want to start IMC immediately after restoring it?
   Yes  No

   c. Click **Yes**.
DBMan starts to restore the databases.

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

5. Click **OK**.

IMC will be automatically started.

**NOTE:**
During the restoration process, DBMan shuts down and restarts IMC and the database service.

---

**Automatic restoration**

Automatic restoration applies to the backup server in stateless failover scenarios. Automatic restoration must work together with automatic backup on the primary server. To synchronize data on the primary server to the backup server, make sure the following requirements are met:

- The master server IP address of the backup system is configured in DBMan of the primary server.
- The boxes in the **Upload to Backup System** column in the **Databases to Back Up** area are selected in DBMan of the primary server.
- Restoration settings are configured in DBMan of the backup server.

After automatically backing up data, the primary server performs the following operations:

1. Immediately uploads backup data to the restoration path (**Backup files location**) on the backup server.
2. Instructs the backup server to automatically restore the data.

To configure automatic restoration on the backup server:

1. Start the Intelligent Deployment Monitoring Agent on the master of the failover system.
2. Click the **Environment** tab.
3. Click **Configure**.

The **Auto Backup and Recovery Settings** dialog box appears, as shown in Figure 110.

**Figure 110 Auto Backup and Recovery Settings**

![Auto Backup and Recovery Settings](image)

4. Read the prompt on the **Auto Backup and Recovery Settings** dialog box carefully, select **Auto Restore Model**, and click **OK**, as shown in Figure 110.

The **Auto Backup and Recovery Settings** page appears, as shown in Figure 111.
5. Click the **Primary Server** tab and configure the following parameters:
   a. In the **Backup files location** field, enter or browse to a path where the uploaded backup data files are stored on the master server.
   b. In the **Databases to Restore** area, select the boxes in the **Restore** column for the databases you want to restore. By default, the boxes are selected for all databases.

6. Click the **Subordinate Server** tab and configure the following parameters:
   a. In the **Backup files location** field, enter or browse to a path where the uploaded backup data files are stored on a subordinate server.
   b. In the **Databases to Restore** area, select the boxes in the **Restore** column for the databases you want to restore. By default, the boxes are selected for all databases.

7. Click **OK**.
NOTE:
Automatic restoration settings in this example apply only to the failover system that is deployed in distributed mode and uses a local database.

Database backup and restore by using DBMan

Database backup and restoration includes the following types:

- **Database backup and restoration for a single IMC system**—You can configure DBMan to automatically or manually back up the database files to the local server. However, you can only manually restore the backed up database files.

- **Database backup and restoration in IMC stateless failover**—The primary server automatically backs up and uploads database files to the backup server. The backup server performs automatic restoration. When the primary server fails, IMC automatically switches to the backup server.

Database backup and restoration for a single IMC system

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

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

Database backup and restoration in IMC stateless failover

⚠️ **CAUTION:**

Before you configure DBMan, make sure the primary and backup servers use the same operating system, IMC version and patches, and database type and version.

Commonly used stateless failover scenarios are configured as follows:

- The primary IMC system is deployed in distributed mode and uses a local database.
- The failover system is deployed in centralized or distributed mode.

The license type is selected as primary server license on the primary server, and as backup server license on the master of the failover system.

Automatic backup and automatic restoration are configured on the primary server and backup server, respectively.

In a stateless failover scenario, the primary IMC system performs the following operations:

1. Uses DBMan to periodically back up database files.
2. Uploads the backup database files to the backup server.
3. Instructs the backup server to perform automatic restoration to synchronize data from the primary IMC system.

Then the backup server automatically restores database files.
NOTE:
In a stateless failover scenario, you can perform any of the tasks in the **Auto Backup and Recovery Settings** dialog box to back up data:

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

For more information about automatic backup, see "Automatic backup."

For more information about automatic restoration, see "Automatic restoration."

**Configuration guidelines**

- To add more configurations in the backup and restoration configuration file besides the properties configured with DBMan in the Automatic Backup and Restoration window, write the configurations to be added to file `dbman_addons.conf` at the `\dbman\etc` directory in the installation path. After you save the file, IMC automatically executes the configurations you added.
  
  For example, write the following before or after database restoration:
  ```
  BeforeSQLScript_monitor_db_imc_monitor = D:\1.bat
  AfterSQLScript_monitor_db_imc_monitor = D:\2.bat
  ```

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

When I uninstall IMC 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 do I install the Java running environment on Linux so that I can access IMC through Firefox?

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

1. Download JDK

Address: http://www.oracle.com/technetwork/java/javase/downloads/index.html

Make sure the correct version is downloaded. For example: you must download jdk-6u12-linux-i586-rpm.bin for x86-based Linux.

2. Install JDK

Upload the installation file jdk-6u12-linux-i586-rpm.bin to the server. Suppose the installation file is saved in directory /tmp, execute the following commands:

   cd /tmp
   sh jdk-6u12-linux-i586-rpm.bin

   After executing the commands above, press the Space bar to view the copyright information, and then enter yes to finish the JDK installation.

   Thus, JDK is installed in directory /usr/java/jdk1.6.0_12. At the same time, a link /usr/java/default pointing the directory /usr/java/jdk1.6.0_12 is generated automatically, equivalent to JDK is installed in directory /usr/java/default.

3. Configure JDK for Firefox

   On the Linux operating system, execute the following commands:

   cd /var/local/firefox/plugins/
   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 do I solve the problem?

This is because the current time zone setting on the server is different from that when IMC was installed.

To modify the time zone of the server, use the tzselect command.

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. When I check the specified log file according to the prompt information, 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 a sa user, and then execute the following commands:

   use model
When installing IMC on a PC running Windows Server 2008 R2, the system prompts that 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.

![Windows Installer](image)

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

Use `service imcdmsd start` to start the JavaService.

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

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

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 as shown in Figure 113 appears.
2. Select the Advanced tab, and click Settings in the Performance area. Then the Performance Options dialog box as shown in Figure 114 appears.

Figure 114 Performance options
3. On the **Performance Options** dialog box, select the **Advanced** tab, and click **Change** in the **Virtual memory** area. Then the **Virtual Memory** dialog box as shown in **Figure 115** appears.

![Virtual Memory](image)

**Figure 115 Virtual memory**

4. Select the **System managed size** option, click **Set**, and then click **OK**.

After an error occurs in deployment or upgrade of a component, the component remains in Deploying or Upgrading state in the Intelligent Deployment Monitoring Agent on the master server. How do I solve the problem?

IMC does not actively refresh the component states. To view the latest state of the component:
1. Stop the Intelligent Deployment Monitoring Agent and quit the program.
2. Restart the **HP iMC server** service. In Linux, enter the `/etc/init.d` directory, and execute the `./imcdmsd restart` command to restart IMC service.
3. Open and start the Intelligent Deployment Monitoring Agent on the master or subordinate server.

If a subordinate server is faulty and cannot be rectified, how do I handle the components that are deployed on the server?

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

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

Contacting HP

For worldwide technical support information, see the HP support website:
http://www.hp.com/support

Before contacting HP, collect the following information:
- Product model names and numbers
- Technical support registration number (when applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber’s Choice for Business website:
http://www.hp.com/go/wwalerts

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

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:
http://www.hp.com/support/manuals
- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see HP A-Series Acronyms.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
Conventions

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

GUI conventions

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

Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>△ <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.