IMC

Intelligent Management Center PLAT 7.2 (E0403P10)

© Copyright 2016 Hewlett Packard Enterprise Development LP

Table of Contents

What's New in this Release

The version IMC PLAT 7.2 (E0403P10) can be upgraded from only IMC PLAT 7.2 (E0403), IMC PLAT 7.2 (E0403L01), IMC PLAT 7.2 (E0403L02), IMC PLAT 7.2 (E0403P03), IMC PLAT 7.2 (E0403P04),IMC PLAT 7.2 (E0403P06), and IMC PLAT 7.2 (E0403L09).

To upgrade from versions prior to v 7.2, upgrade both the IMC Platform and all the deployed service components through each released version. The upgrade path is V3.3 >> V5.0 >> V5.1 >> V5.2 >> V7.0 >> V7.1>> V7.2. Before you upgrade the IMC Platform, download upgrade packages for all deployed service components from HP's website, and before you install them pay special attention to the section "Platform Compatibility" in their readme. If an upgrade package is not available for a service component, HP recommends not upgrading the IMC Platform, or you can remove the service component before upgrading the IMC Platform. When the service component is removed, its data is lost. It is not possible to import the database taken from a previous version into V7.2. The following lists all features released after IMC PLAT 7.1 (E0302).

Features released in IMC PLAT 7.2 (E0403P10)

- The Instance column was added to the Table page accessed by using the Table View mode in the MIB management tool.
- The Alarm > Alarm Settings > Alarm Notification page supports auto sending of recovery alarms.
- On the Alarm > Trap Management page, the Oracle or SQLServer version supports traps with the trap OID not exceeding 500 characters, and the MySQL version supports traps with the trap OID not exceeding 250 characters.
- VRM supports ESX6.0.

Features released in IMC PLAT 7.2 (E0403L09)

- Adds support for the HPE Aruba 2930F VSF series on the Resource > Network Topology > Stack Topology page.
- Supports configuring the device synchronization time on the System > Automatic Device Sync Time page.
- Supports Cisco devices whose banners contain the pound signs (#) on the Service > Configuration Center page.
- Supports configuring permitted VLANs for trunk ports of a device that has aggregate interfaces on the Resource > Network Topology > Device > Add to Current VLAN page.
- Supports Cisco Nexus switches on the Service > Configuration Center page.
- Supports displaying interface aliases in performance alarms on the Alarm > Alarm Browse > All Alarms page.
- Supports viewing the CPU and memory recovery alarms of the iMC server on the Alarm > Alarm Browse > All Alarms page.
- Supports configuring whether to escalate alarms for devices with the maintenance tag on the System > System Configuration > System Settings page.
- Supports setting the lifetime for the collected original performance data in the iMC/server/conf/qvdm.conf file.
- Supports configuring whether to send recovery alarms for alarm notifications and forwarding in the iMC/server/conf/qvdm.conf file.
- H3C devices support configuring MACsec links.
- More detailed logs are needed for importing traps through MIB files. For example, the total number of MIB files processed and the total number of MIB files parsed successfully.
- The IMC topology supports displaying and managing server clusters.
- The IMC platform supports customizing the function framework in the UCD by functional point.
- The Real-Time Location page supports adding tags to devices.
- The 3D topology supports selecting the number of switches and the environment & power facility type when you configure environment & power facilities through a right-click.
- The data center topology map supports CAD files.
- Adds the rack height (U) field to the .csv file for the automatical building function of the 3D topology.
- Adds the memory monitoring index for the single device monitor in the IMC dashboard.
- The IMC dashboard supports automatically fitting the custom topology to the screen size.

- The network topology supports setting the font size and color for device labels (the settings take effect only on the current view).
- Adds the loop legend description to the topology.
- The topology link management function supports exporting links to an excel file.
- The elements on the dashboard need the corresponding labels and the object names must be displayed on the labels.

Features released in IMC PLAT 7.2 (E0403P06)

- None

Features released in IMC PLAT 7.2 (E0403P04)

- The **Resource > Network Topology** page supports the tree layout.
- The **Resource > Network Topology > Custom View** page provides multiple levels of custom views.
- The **Resource > Network Topology** page supports the stack topology of HPE Aruba 5400R series devices.
- The **Resource > Network Topology > Data Center** page supports monitoring Cointech hygrothermographs.
- The **Resource > Network Topology > Data Center** page supports recording user operations performed on racks (for example, clicks and browses) and the pauses in the 3D room.
- The 3D room provides RESTful APIs for obtaining rack information and the rack and room locations for a device.
- RESTful APIs for obtaining device MIB tables.
- The **Device Detail > Interface List** page supports displaying an interface alias that contains more than 64 characters.
- The **Service > Network Devices > Device Details** page supports adding VXLANs in the EVPN mode.
- The **Service > VXLANs Traffic Information** page provides the VXLAN monitoring feature.
- The **Service > Network Devices > Device Details** page supports configuring ACs.
- The **Service > Network Devices > Device Details** page supports adding L3VNI interfaces in distributed networks.
- The **Service > Network Devices > Device Details** page supports binding VPN instances to DHCP relay IP addresses in distributed networks.
- The **Service > Network Devices > Device Details** page supports adding VSI interface MAC addresses and secondary IP addresses.

Features released in IMC PLAT 7.2 (E0403P03)

- The Dashboard page provides a toolbar on the topology.
- The Dashboard page provides automatic switch between views.
- The Dashboard page supports component-based filtering for widgets to be added.
- The **Resource > Network Topology** page provides subview alignment in the right-click menu of the topology.

- The **Resource > Network Topology** page provides the Add Monitor option in the right-click menu of topology links in performance management.
- The **Resource > Network Topology** page provides the vertical distance configuration between the device icon and the device label.
- The **Resource > Network Topology** page displays the status of connections in link aggregation by expanding the stack topology.
- The **Alarm > Alarm Settings > Alarm Notification** page supports the asterisk (*) wildcard character in parameter settings.
- The **System > Operator Management > Authentication Server** page supports RADIUS server and TACACS server configuration.
- The **System > Operator Management > Authentication Server** page allows you to define the accessible user groups, device groups, and custom views by OU in advanced settings.
- The **Service > Configuration Center** page provides software update for Cisco 800, 2651, 2800 series devices.
- The **Service > Configuration Center** page provides configuration backup and restoration and software update for Aruba 3810 series, 7000 series, and IAP series wireless devices.
- Support for integration with DCN, identifying the VSC and VRS roles, and displaying connection relationships between the roles in the topology.
- VRM supports Windows Hyper-V Server 2012 R2 and SCVMM 2012 R2.
- VRM supports obtaining storage information from VMware hosts.

Features released in IMC PLAT 7.2 (E0403L02)

- Open data sources of iCC for reports, including deployment tasks, backup history reports, device configuration backup, and device software update.
- Backup and restoration of i-Ware configuration on security products.
- Obtaining information about the VMware NTP server, network card speed, and duplex mode in VRM.
- Configuring whether to assign all trunk and hybrid ports to a device VLAN when you add it through the RESTful interface.
- SCOM supports the HTTPS protocol.
- Adding custom templates for performance indexes.
- Displaying custom TopN indexes in the device view, interface view, custom view, IP view, and query result page.
- DBman can back up configuration files that include realtime performance monitoring and traffic topology settings.
- The Lower-Level NMS Performance View widget was added to Dashboard to provide monitoring data of the lower-level NMS.
- The procedure of modifying NMS parameters for devices that failed access parameter verification was added to batch operations.
- The Download Logs feature in Log Configuration supports automatically downloading the software version information.
- Netconf log management in Log Configuration.
- Basic query and advanced query on the operator management page.
- Trap group management was added to the trap management page for trap filtering.
- The Alarm Notification feature supports displaying user information in the destination mail address.

- Using a public IP address as the lower-level NMS address in Hierarchical IMC Alarming settings.
- Using the custom view to filter alarms in Dashboard.
- The Alarm Notification feature supports adding relationships among alarm parameters for alarm configuration.
- Configuring the number of hierarchical alarms to be displayed in Hierarchical IMC Alarming settings.
- Backing up FW, IPS, ACG, and LB data of the H3C i-Ware platform.
- The ACL, VLAN, and iCC features in the Service module support Cisco Nexus series switches.

Features released in IMC PLAT 7.2 (E0403L01)

- RESTful API for querying global VLANs.
- Optimized menus in the More and Operation columns in the device list.
- The Deploy Software option was added to the right-click menu of devices on the topology.
- The fabric topology does not display loop links.
- Displaying PE-PE links of IRF fabric devices.
- When unrecovered alarms are not acknowledged option was added to the Alarm Sound Settings page.
- V2 report of unused interfaces.
- Quick service process view.
- Viewers were assigned the privilege of modifying the collection interval on the realtime performance monitoring page.
- On the Resource >> Network Topology page, the fabric topology does not display the loop links.
- Modifying ports in the DBMan configuration file.
- The Resource >> Network Topology page displays PE-PE links of IRF fabric devices.
- DBMan allows you to modify ports in the dbman.conf file in the /dbman/etc directory of the IMC installation path.

Features released in IMC PLAT 7.2 (E0403)

- Supports OneView integration.
- Supports VXLAN.
- Custom views support upper-level views by using the API POST plat/res/view/custom
- Supports the following new operating system: RHEL 7.x.
- Supports Oracle 12c Release 1
- Adding the Perspective QSP template.
- Adding system integration with AirWave
- Integration with Aruba ClearPass and Aruba AirWave trap definitions in trap management of the alarm module.
- Reporting alarms to upper-level IMC administrators for processing when the grace days for alarm acknowledgement expires on the Alarm Notification page of the alarm module.
- The tools directory provides iMC-MIB-Download_Windows.zip or iMC-MIB-Download_Linux.zip to import IMC trap definitions to MIB files

- Set the autocfg_exec_mode parameter to 1 in the file /server/conf/qvdm.conf of the IMC installation path, and then restart the imciccdm program to support serial execution of auto deployment plans.
- Backup function for HP PROCURE 2520 device configurations on the Service > Configuration Center page.
- Using the device model as the display name in the topology.
- Custom report feature.
- Custom view eAPI and upper-level views.
- Starting and stopping a single process by using command lines in Linux.
- Access to interface lists of interface views by clicking icons on the Interface View TopN widget on the home page.
- Displays route relationships among devices on a route topology based on device routing tables.
- In Intelligent Policy Center, Action Management supports the Restart VM operation.
- On the device query page, the advanced query provides the Device Alarms field.
- On the all alarms page, the advanced query provides the logical combination of NO.
- Supports custom interfaces for third-party mails servers.
- The performance view provides the Modify the Upper-Level Folder feature.
- The configuration template library supports access control by operator group.
- Configuration template deployment supports exporting parameters from CSV files.
- The VRM component supports detecting unmanaged hosts under a managed vManager.
- Device and interface (link) maintenance tagging.
- Displaying or hiding interface aliases in interface-related alarms.
- Sending alarm notification in long SMS messages.
- A Test button is provided to test the SMS modem.
- Scenario-based trap-to-alarm rule configuration.
- Displaying the STP root bridge in the MSTP topology.
- Topology diagnosis.
- Managing Extreme x460 series devices by using Resource Management.
- The default setting for DismanPing is FALSE in the global configuration.
- Configuring a rule to automatically add interfaces of new devices to an interface view.
- Email alarm notifications provide a link for users to confirm the alarms.
- A REST API for obtaining trap definitions is provided.

Enhancements released in IMC PLAT 7.1 (E0303P16)

- None

Features released in IMC PLAT 7.1 (E0303L15)

- VMware IOPS storage read and write performance indexes were added to VRM monitoring.
- ACL management supports devices running Comware V7.1 B58 and later versions.

- On the device query page, the advanced query provides the Device Alarms field.
- On the all alarms page, the advanced query provides the logical combination of NO.
- Supports custom interfaces for third-party mails servers.
- The performance view provides the Modify the Upper-Level Folder feature.
- The configuration template library supports access control by operator group.
- Configuration template deployment supports exporting parameters from CSV files.
- Support auto deployment for CentOS-6.6-X86_64 and CentOS-7-x86_64 operating systems.
- IP/MAC learning results are added in batches to IP/MAC and terminal MAC bindings.

Enhancements released in IMC PLAT 7.1 (E0303P13)

- The 3D room provides basic lighting elements such as point lighting and tube lighting.
- Elements in the 3D room support automatic alignment.
- In the 3D room, the Save buttons for rooms and racks provide Successfully Saved messages.
- The 3D room supports the query function.
- Adding the text label element for the display tiling. The text label element supports entering single-line text in the text label or text field.
- Supports EAPI interfaces used for querying IMC license information.
- Supports EAPI interfaces used for querying device additional information.
- The monitoring settings page provides the instance view switch link that allows users to access the instance view page.
- The Alarm > Trap Definition > Device Severity page provides the link that allows users to access the device trap level rule page. When custom trap level rules have different devices but have the same trap, same parameters, and same level, these custom trap level rules are displayed in a rule.
- The advanced query on the Alarm > All Alarms page supports multiple query criteria, and supports AND and OR relationships between the query criteria.
- The device panels of S10500 and S12500 switches support power supplies and fans with colored borders. The border color of a power supply or fan indicates the current status of the power supply or fan. The color of green indicates that the power supply or fan is working correctly. The color of red indicates that the power supply or fan is faulty. The color of grey (no border) indicates that getting the status of the power supply of fan failed (unknown status).
- When the status of a device alarm or link alarm becomes red, the device icon or the link blinks.
- On the performance instance threshold page, the value ranges of start and end values are optimized.
- For a single index in a single performance, the default maximum number of instances is increased to 150.
- On the SMSC settings page, serial number registration for the SMS Center sending method supports entering keys.
- LiveUpdate URL changes to https://h10145.www1.hpe.com/web/services/pcm3/PcmWebSvc.asmx.

Features released in IMC PLAT 7.1 (E0303H12)

- None

Features released in IMC PLAT 7.1 (E0303L11)

- Modifying a single device location or modifying device locations in batches.
- The **Alarm > Trap Definition > Modify Trap** page supports modifying the level of network management alarms.
- The **Home > Alarm Panel > Alarm Sound Setting** page supports customizing alarm sounds per operator.
- The **Resource > Performance Management > Performance** Option page provides the TopN Index tab that allows users to modify TopN indexes.
- The Display Option tab on the **Resource > Performance Management > Performance Option** page supports configuring the colors and roughness of curves of the performance trend chart.
- The device and interface details pages provide the **Modify Display Index** link that allows users to customize display indexes.
- The **Resource > Performance Management > Monitoring Settings** page provides the Cancel button for each monitor index for each device. The button enables users to cancel all monitor instances for a monitor index at one time.
- The **At a Glance** page supports sorting the interface traffic list by the Monitored Objects field.
- Supporting notifying administrators by mails before license expiration.
- The **Service > Auto Deployment Plan** page supporting adding device quickly by the scanner gun for auto deployment.
- DBMan supports backing-up and restoring multiple database of one IMC component.

Enhancements released in IMC PLAT 7.1 (E0303P10)

- The **Resource > Service Monitoring** page supports Web addresses that begin with https:// for Internet service monitor adding.
- The **Alarm > Trap Management > Trap to Alarm** page supports configuring Trap to Alarm rules in batches according to scenarios.
- The **System > System Configuration > SMSC Settings** page supports viewing the sending records of SMS messages.
- The **System > System Configuration > Quick Service Process** page provides the quick service process feature that integrates service configuration procedures into templates. You can add the quick service process widget to the home page.
- The **System > Group Management > Device Group** page supports adding subgroups.
- The **Service > Policy Control Center** page supports the policy management feature.
- The **Service > Configuration Center > Auto Deployment Plan** page provides the basic and advanced query features.

Features released in IMC PLAT 7.1 (E0303L08)

- Adding the Last Change column to the interface list on the device details page in the device view.
- Modifying the template access rights for adding or modifying of SNMP, Telnet, and SSH templates in the resource management module.
- The **System > Operator Management > Data Privilege Configure** page provides global access right configuration for SNMP, Telnet, and SSH templates. This feature is unavailable when the IMC platform cooperates with RSM.
- The **System > Operator Management > Authentication Server** configuration enables IMC to use LDAP authentication when no operator exists in the system.
- The **Alarm > Alarm Browse > Real-Time Alarms** page provides the Show Root Alarms option that filters out common alarms and displays only the root alarms.
- Data collection of performance indexes for Alcate/Allied-Telesis devices.

Features released in IMC PLAT 7.1 (E0303L07)

- Providing the Periodic Monitoring page in the Performance Management module. Monitoring data during specified work time is displayed for devices in different custom views.
- Clicking MIB Upload on the Trap Definition page in the Alarm Management module to import trap definitions through a MIB file. The MIB file can be in ZIP format.
- Resizing columns on the Real-Time Alarms page in the Alarm Management module.
- Installing Deployment Monitoring Agent on the database server and performing DBMan operations.
- Adding the Release Date column in the **Service > Software Library** page.
- Sending the configuration report for an auto deployment plan to a mailbox on the Add Auto Deployment Plan page in the Service Management module.
- Adding the isSTPEnable and isSSHEnable predefined policies in the compliance policy list in the Service Management module.
- Adding the MAC vendor management function on the terminal access page in the Resource Management module.
- Traps are allowed to self recover when traps are defined in IMC. However, traps for link states are still not allowed to self recover. Traps for link states has the follow types:
  Link Down (1.3.6.1.6.3.1.1.5.2.0) or Link UP (1.3.6.1.6.3.1.1.5.3.0)
  Link State Down (1.3.6.1.4.1.2011.10.4.1.1.2.6.8) or Link State UP (1.3.6.1.4.1.2011.10.4.1.1.2.6.9)
  Link State Down (1.3.6.1.4.1.25506.4.1.1.2.6.8) or Link State UP (1.3.6.1.4.1.25506.4.1.1.2.6.9)
- Seting the log file size. Use either of the following methods to set the log file size:
  Method 1
  - Enter the \server\conf directory of the IMC installation path.
  - Open the qvdm.conf file.
  - Set the LogFileSize field.
    The maximum value is 2047 MB and the minimum value is 1 MB.

Method 2

- Enter the \server\bin directory of the IMC installation path.
- Set the environment variable.
  start_env.bat
- Set the log size for a process.
  logset -p1 -s50

This method sets the log file size only for the specified process. You do not need to restart IMC.

Enhancements released in IMC PLAT 7.1 (E0303P06)

- The asset report that meets the requirements of HP post-sale service contracts is added, and the device asset report (Concise) is added.
- On the **Resource > Performance Management > Service Monitoring > Add Service Monitor** page, the maximum length of an FQDN for a DNS service monitor is 255
- Supports deleting security MAC-port bindings for devices running Comware V5.

Features released in IMC PLAT 7.1 (E0303H03)

- None

Features released in IMC PLAT 7.1 (E0303L02)

- Provides the Modify ACL button on the View ACL page for ACL devices
- Provides new schemes and alarm widgets for the dashboard.
- Provides the Star theme.

Features released in IMC PLAT 7.1 (E0303L01)

- None

Features released in IMC PLAT 7.1 (E0303)

- None

Features released in IMC PLAT 7.1 (E0302)

- Baseline software audit supports ComwareV7 devices using the IPE software package.
- Automatically deletes devices that are unreachable for a given period of time from IMC.
- Supports centrally performing compliance check for devices across multiple RSMs.
- Modifies the information display mode of the error information for report script executions on the login page.

- Cancels the limit on the number of exported alarms. Supports creating more tabs in the exported excel file, with each tab containing up to 5000 rows.
- Limits the URL length to 128 characters in Service Monitoring of Performance Management.
- Supports the backup and restore function for Juniper SRX650 devices in ICC.
- Enhances the IP address management function by displaying IP address segment statistics and displaying idle IPs in each IP address segment.
- Supports sorting and searching capabilities for the lists on some network element information pages, for example, the IP route pages.
- Displays the custom view list in a tree, and sorts the custom views by name by default.
- Reads the private MIB of an MSM device to get and show its sysuptime.
- Supports using SCP to deploy configurations to Cisco 2960 /3750 switches.
- Supports writing the operation logs to the imcforeground.log file. Users can disable/enable this feature in IMC system settings. This feature is enabled by default.
- Supports firmware upgrade for stacked Cisco 2960s devices.
- Allows an operator to use the full name (which can contain characters other than ASCII characters) to log in to IMC and shows the full name in the top right corner of IMC page after the login succeeds.
- Supports copying customized homepages and my favorites.
- Supports importing a file to batch modify device labels on the **Resource > Import/Export Device** page.
- Supports showing power supply and fan status in device panel view for devices that can provide related info in the MIBs.
- Supports showing device label (alias name) and IP info in the device panel view for 10500 and 3800 devices.
- Supports using SCP to back up configuration files for Cisco 7606 devices.
- Improves the topology link labels as follows: sets different background colors for different link labels; keeps the link label direction the same as the link direction; supports displaying abbreviated interface names for interface names in link labels.
- Adds the sysLocation as an optional parameter for customizing the alarm forwarding format.
- Displays the device type names on the Y-Axis of the Device View widget on the IMC homepage.
- Automatically sets the heap size for JServer according to the total physical memory size of the IMC server during the IMC installation process.
- Supports manually drawing curve links in the topology.
- Supports disabling/enabling MSTP info gathering for L2 topologies.
- Allows using hyphens (-), underscores (_), pluses (+) and spaces ( ) in VLAN descriptions.
- Shows links between Cisco switches correctly when the interfaces are configured as channel trunk.
- Supports HTML5 dashboards.
- ICC uses only CLI rather than template to perform compliance checks. It will not be affected by TFTP or SFTP.
- Supports reading data in timeticket format from the MIBs.
- Uses CLI to deploy Quickfix for compliance check, and supports Quickfix for HP devices.

- Shows the hard disk sizes of the virtual machines on the Web interfaces.
- Shows the local storage information of the virtual machines on the Web interfaces.
- Shows the link between the VM and the storage when the virtual host is open in the virtual network topology.
- Provides new dashboard widgets to show the VM performance.
- Performs the privilege check for switches connected to VMs before VM migration.
- Supports forwarding syslogs and traps to ArcSight by using the filter tools.
- Optimizes ICC prompts.
- Implements 3D datacenters by using WebGL 3D.
- Adds a new theme named Sky Blue as the default theme.
- Supports SQL Server 2014.
- Combines HA with DBMAN to provide HA deployments for IMC and databases.
- When a viewer with only the permission to the custom topology logs in to IMC and views the topology, the topology does not provide the right-click shortcut menus, tool bar, and tips.
- Adds the function of collaborating with Microsoft SCOM and forwarding alarms in IMC to SCOM.
- Supports forwarding SMS through email.
- The Resource > Performance Management > Monitoring Settings page displays monitor devices, monitor indexes, and monitor instance in a tree structure. The Switch to Instance List link is deleted.

[Table of Contents]

Problems Fixed in this Release

IMC PLAT 7.2 (E0403P10) fixes the following problems,including all bugs fixed after IMC PLAT 7.1 (E0302).

Resolved Problems in IMC PLAT 7.2 (E0403P10)

1. When an operator modifies an ACL in IMC, the ACL rule numbers of the ACL change.
2. When an operator modifies an ACL in IMC, the ACL name of the ACL is deleted.
3. When a larger number of syslog to alarm rules are configured and the rules contain views, upgrading syslogs to alarms takes a long time.
4. When staged alarm notification is configured, the recipients of recovery alarms are not identical to the recipients of alarms.
5. When multiple devices are selected to execute access parameters checking, an error occurs when accessing the IMC home page and the log information indicates that the system is busy.
6. When no data is returned during the interaction of some GSM modems, SMS message test fails.

7. If the Telnet service is disabled on HP ProCurve devices, configuration backup fails.
8. When alarms are forwarded through SMS messages, the SMS messages support including alarm generation time.
9. An operator fails to access the operator page after clicking Add Operator or Modify Operator.
10. The expiration date of the VXLAN module is not identical to the expiration date of the IMC platform on the About page.
11. An operator fails to access the next page when the number of performance views exceeds the selected maximum display number of 50. When the maximum display number is set to 8, no page navigation icons are displayed.
12. iMC server throws Java exception when trying to TEST SNMP parameters in Batch operations SSH settings page.
13. Deprecate the REST interface /imcrs/vrm/host/templete for VRM.
14. After Java 8 is installed, a dialog box displaying " Block potentially unsafe components from being run " appears when you click SSH on device Action list.

Resolved Problems in IMC PLAT 7.2 (E0403L09)

1. The device software library does not display the HP 5900AF-5920AF_7.10.R2418P06-B software downloaded from LiveUpdate.
2. The AP monitoring data becomes abnormal when the AP is rebooted.
3. Failure to back up the configuration for HP PROCURVE 26/28 series devices.
4. The VRM plugin cannot work properly because there is a line feed between the IP address and the port number in the VRM plugin configuration file.
5. On the IMC operator group management page, the Access Lower-Level NMS privilege (the privilege is added by default) is added to the viewer group to control the viewers' access to the snapshot of lower-level NMS view on the IMC resource page.
6. The IP addresses of online accounts are not correct on the access log history page.
7. You will receive the same Email twice if you configure two email addresses on the alarm notification page.
8. The system fails to upgrade the IMC inventory component when other database users are used.
9. After debugging is enabled, the IMC web page is unusable.
10. When you click Add or Modify on the System > Operators page, the page might hang or be busy.
11. If a transceiver module is plugged or unplugged, the transceiver module change is not displayed after the asset synchronization interval.

Resolved Problems in IMC PLAT 7.2 (E0403P06)

1. When two cloud views point to each other's parent custom view, page errors occur.
2. VRM does not support Windows Server 2012 R2.
3. When an operator logs in to the backup IMC of an IMC system that has the primary and backup IMC licenses registered, the following message appears: Invalid license.

4. The statuses of subviews of a custom view are not counted in determining the status of the custom view.
5. The widgets on the dashboard cannot be refreshed.
6. Sometimes the mail sending feature for auto backup plans is unavailable and users cannot receive mails.

Resolved Problems in IMC PLAT 7.2 (E0403P04)

1. When device synchronization is performed for multiple times, database access errors occur.
2. After Syslog events are occurred for a monitor index, an operator increases the threshold and reduces the repeat times value to be smaller than the occurrence times. Then, the performance module reports alarms even when the threshold is not exceeded.
3. Devices cannot be added to IMC by using SNMPv3 templates.
4. If IMC polls immediately after devices are restarted, the year in the generation time of interface down alarms might be 1970.
5. When IMC is upgraded to iMC PLAT 7.2 (E0403), iMC PLAT 7.2 (E0403L01), iMC PLAT 7.2 (E0403L02), or iMC PLAT 7.2 (E0403P03), alarm forwarding mails does not support the plaintext format.
6. When an operator attempts to delete a custom trap filter rule, a "system busy" message appears.
7. When an MP link recovers from the down state, the status of the MP link is not displayed correctly.
8. When services do not respond for a short time, service down alarms are generated in service monitoring.
9. VXLAN traffic information is generated based only on a single index.
10. Licenses for the iMC platform do not include the VXLAN license.
11. The ACL device list does not display HPE OEM devices of the H3C brand.
12. Aggregate interfaces cannot be added for devices running Comware 7.
13. When IMC is upgraded from versions earlier than IMC PLAT 5.1 (E0202) to IMC PLAT 7.2 (E0403L02) or IMC PLAT 7.2 (E0403P03), the Access Parameter Template page might display SNMP, Telnet, or SSH parameters as SNMP, Telnet, or SSH templates.
14. On the MSTI list page, VLANs mapped to MSTIs are incorrect for HP devices.

Resolved Problems in IMC PLAT 7.2 (E0403P03)

1. When the custom view contains multiple levels of cloud views in the custom topology, the status of a custom view or cloud view is incorrect in a custom topology.
2. The iMC platform components are exposed to OpenSSL security vulnerabilities CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, and CVE-2015-1794.
3. When the alarm matches two mail notification rules, an alarm mail is sent twice.
4. When idle interfaces are used as an interface filter criterion in port group view, subinterfaces of an aggregated link are displayed.

Resolved Problems in IMC PLAT 7.2 (E0403L02)

1. When the WSM component is deployed, an operator can successfully change the theme of a dashboard through the theme menu, but the theme menu displays each theme name as undefined.
2. The operator can successfully delete a report on the My Reports page but fails to delete another report without refreshing the page.
3. When an operator logs in to IMC as a maintainer or viewer and attempts to access the realtime performance monitoring page, a page error occurs.
4. When a large number of performance monitor instances exist on a device, the At a Glance page of the device is loading and cannot display data.
5. When an operator logs in to the standard platform of IMC, the Resource tab does not display the Maintenance Task option.
6. When the screen resolution is set to 1280 and the IMC Web page theme is set to ash black, the basic management view page displays contents in the navigation bar at the top of the page in separate lines.
7. When an operator accesses the System Settings page, the System Settings page does not display the Task History Lifetime field.
8. When the alarm module is deployed, the tip information of each device in racks in the 3D room does not contain the alarm information.
9. The software products downloaded from LiveUpdate cannot be displayed in the software library of iCC.
10. The resource background fails to be started if you install SSM, create a virtual firewall, delete the firewall, and then restart the resource background.
11. A Syslog of more than 1024 bytes cannot be displayed correctly in IMC.
12. After an AP is rebooted, traffic statistics for the AP are displayed incorrectly.
13. If an alarm matches two rules in the alarm notification settings, alarm notification mails are repeatedly received for the alarm.
14. When a new rule is to be added to a compliance policy, in the device series selection window, the selected entries are cleared after entries are paged forward or backward.

Resolved Problems in IMC PLAT 7.2 (E0403L01)

1. VLAN topologies are inaccessible in QSP view.
2. When a virtual machine on a host is cloned, the system displays a page for fixing the operation failure.
3. In QSP view, menus under Deploying Firmware are incorrect.
4. Customized columns on the network asset page are not displayed when the operator who customized them relogs in to IMC.
5. When interfaces on Comware devices are bound with VPN instances, the interface list for Comware devices does not display interface address information.
6. When a member port of an aggregate interface comes up again, the interface-down alarm for the port is not recovered.
7. IMC cannot display the CPU usage of each processor for a Linux server that has multiple processors.
8. Alarms sometimes are not triggered for services monitored on the Device Details page.
9. Direct link status does not change when the interface status in the route topology is changed.

10. When a new sFlow probe instance is added for a device, existing instances for sFlow probes are overridden.
11. VMs cannot be deleted from a host that runs CAS.
12. The sending time in SMS message delivery records is in 12-hour format for SMS messages delivered through the IMC SMS sender, third-party SMS sender, or mail-to-SMS conversion function.
13. In the RSM edition, the page crashes when an interface view is added.
14. Security holes #576313:Security holes exist when Apache Commons Collections Java library insecurely deserializes data.
15. Query criteria are invalid in the alarm query view after the IMC PLAT is upgraded to a version later than IMC PLAT 7.1 (E0303P13).
16. An error page appears when the parameter setting page of the custom report function is opened in a service component.
17. On the custom topology, device labels are modified to Korean character strings, and they become illegible after the topology is reloaded.
18. Device alarm event configuration entries cannot be added.
19. Lower-level IMC does not have the left navigation tree when it is accessed from the upper-level IMC system.

Resolved Problems in IMC PLAT 7.2 (E0403)

1. This symptom occurs when a user views the dashboard that contains the per-level alarm trend chart.The dashboard displays data incorrectly.
2. This symptom occurs when a user adds the per-level alarm trend chart (the alarm class is all alarms) and the per-class statistics trend chart (the alarm class is configuration alarms) to the dashboard and monitors alarms for some time.Curves of the per-level alarm trend chart fall at irregular intervals.
3. This symptom occurs when a user selects a device on the Applet network topology, right-clicks the device, and then selects Open Device Panel from the shortcut menu.A page error occurs when a user accesses the device panel.
4. This symptom occurs when Enable Mail Notification is selected in license expiration mail notification settings on the system settings page.The mail content is incorrect and the mail format requires optimization.
5. This symptom occurs when a user accesses the system settings page with the alarm module not installed.Accessing the system settings page takes a long time.
6. This symptom occurs when a user clicks Add Link on the link management page for a custom topology.An error for the Add Link page occurs.
7. This symptom occurs when a maintainer logs in to IMC and double-clicks a cloud in the converged topology.A maintainer fails to open the topology for a cloud.
8. This symptom occurs when a user clicks the Add Link icon on the converged topology, or right-clicks the converged topology and selects Add Link from the shortcut menu.An error for the Link Management page occurs.
9. This symptom occurs when a user clicks Save in the toolbar on the converged topology.The note and the background area cannot be saved.
10. This symptom occurs when a uses accesses a REST API.The associated model schema for a REST API does not exist.
11. This symptom occurs after the WSM component is installed.The REST APIs of license management are unavailable and the response codes are 404.

12. This symptom occurs when a maintainer who has no management rights to self-service accounts modifies a user.A page error occurs when a maintainer attempts to modify a user.
13. This symptom occurs when the SSA version is upgraded from IMC PLAT 7.1 (E0303) to IMC PLAT 7.1 (E0303P13).A page error occurs when a user configures server power supply trap information.
14. This symptom occurs when IMC had ever been started before it was upgraded to IMC PLAT 7.1 (E0303P13).The Device Asset Report(Concise) cannot be obtained after IMC was upgraded to IMC PLAT 7.1 (E0303P13).
15. This symptom occurs when a user exports the Device Asset Report(Concise).The summary report at the end of the Device Asset Report(Concise) is displayed incorrectly after the Device Asset Report(Concise) is exported to an EXCEL file.
16. This symptom occurs when the performance management module is installed and monitoring objects are added in IMC that runs in Linux and uses an Oracle database.The performance background process restarts sometimes.
17. This symptom occurs when a user deploys the alarm management module of the IMC PLAT 7.1 (E0303P13) version, undeploys and removes the module, and then deploys the module again.An error occurs during the deployment of the alarm management module of the IMC PLAT 7.1 (E0303P13) version.
18. This symptom occurs when the sending alarm SMS message feature is enabled in IMC that runs in Linux.Alarm SMS messages cannot be received.
19. IMC runs on Linux and uses the Oracle database. An error page appears after an operator clicks Refresh on the server details page that contains an empty server name field.
20. The disk space of the IMC server is full after DBMan automatic backup runs for a long period of time in distributed, standalone, or primary/backup IMC deployment.
21. An operator disables the route topology feature and then synchronizes devices. The custom topology still contains links added by the route topology feature.
22. The topology page displays an incorrect link state after an operator performs the following procedure:
    a. On the topology page, changes the link interface for a device whose state has changed from reachable to unreachable.
    b. Views the link status.
23. The SNMP parameters test displays a Failure message after an operator performs the following procedure:
    a. Clicks MIB Management in the Action section of a device's Device Details page, and then opens the SNMP parameter configuration page.
    b. Configures the read-only community string in the Read-Only Community String field, and leaves the Read-Write Community String field empty.
    c. Clicks Test.
24. An operator configures an SMS messaging alarm notification rule with a plus sign (+) preceding the country code. The cellphone cannot receive alarm notification SMS messages.
25. The following error message appears after an operator deletes a trap definition from the trap definition list:
    Operation failed with error code 4002. Please contact your administrator.
26. An error page appears after an operator configures the alarm reporting feature for the first time on the hierarchical IMC alarming configuration page.

27. When an operator modifies index settings on the Add Monitor page and attempts to select the Global Index Settings option, a page error appears.
28. Monitor data loss occurs on the realtime performance monitoring page after a performance management module upgrade.
29. SMS messages cannot be sent by using the Convert Mail into SMS sending method after the reboot of IMC.
30. When a single mail notification rule on the Alarm Notification page contains more than one recipient address, sending of alarm notification mails fails.
31. A page error might occur when an operator clicks the ACL Configuration icon for a device on the ACL device list page of the ACL management module.
32. If a .csv file contains SNMPv3 parameters, it cannot be imported to auto deployment plans.
33. When the report module is deployed after the IMC platform with a remote database is upgraded to IMC PLAT 7.2 (E0403), the following message appears: Invalid object name 'TBL_RPTVIEWER_INSTALL_UPDATE'.
34. Database files backed up by running DBMan commands cannot be restored through DBMan.
35. After a device that includes aggregation interfaces is added to IMC, the VLAN device list does not display the device.
36. When the log level of the alarm module is set to Debug, CoreDump sometimes occurs in the background process of the alarm module.
37. If an online endpoint uses an IP address different than the endpoint IP/MAC address binding in the terminal access module, IMC generates IP/MAC address inconsistency alarms for the endpoint multiple times.
38. CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-2015-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6676, CVE-2015-6677, CVE-2015-6678, CVE-2015-6682, CVE-2015-5572, CVE-2015-5576, CVE-2015-6679, CVE-2015-5571.
39. All configuration template files in iCC will be cleared if you update an early version to IMC PLAT 7.1 (E0303P16) or later.

Resolved Problems in IMC PLAT 7.1 (E0303P16)

1. This symptom might occur during server synchronization. The imccimdm process terminates and the system produces a core dump file.
2. The query result is empty by specifying the start and end time for the RESTful API Query Single-Index TopN Data.
3. This symptom occurs when the IPC module executes configuration file deployment that contains only the action parameter settings. Configuration file deployment failed and the system displays the message "The deployed devices do not exist."
4. This symptom occurs when an operator modifies a log level in the log configuration module. The prompt message for a log level modification operation is incorrect.
5. This symptom occurs after the operator adds a user-defined device vendor. The system cannot display the device definition page when an operator returns from the device vendor page.

6. CVE-2015-3113. Heap-based buffer overflow in Adobe Flash Player allows arbitrary code execution via unspecified vectors. This issue exists in Adobe Flash Player embedded in IMC.
7. CVE-2015-5122. Use-after-free vulnerability exists in the DisplayObject class in the ActionScript 3 implementation in Adobe Flash Player of Chrome installations. It allows arbitrary code execution or launching of a DoS attack (memory corruption) by using crafted Flash content that leverages improper handling of the opaqueBackground property. This issue exists in Adobe Flash Player embedded in IMC.
8. CVE-2014-8176. If a DTLS peer receives application data between ChangeCipherSpec and Finished messages, buffering of such data may cause an invalid free, resulting in a segmentation fault or potentially, memory corruption.
9. CVE-2015-1788. OpenSSL enters an infinite loop when processing an ECParameters structure in which the specified curve is over a specially-malformed binary polynomial field. This vulnerability might be exploited to perform DoS attacks against any system that processes public keys, certificate requests, or certificates.
10. CVE-2015-1789. X509_cmp_time does not properly check the length of the ASN1_TIME string and can read a few bytes out of bounds. In addition, X509_cmp_time accepts an arbitrary number of fractional seconds in the time string. An attacker might craft malformed certificates and CRLs of various sizes and potentially cause a segmentation fault, resulting in a DoS attack on applications that verify certificates or CRLs.
11. CVE-2015-1790. The PKCS#7 parsing code does not handle missing inner EncryptedContent correctly. An attacker can craft malformed PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.
12. CVE-2015-1791. The race condition vulnerability might be exploited to launch a double free of the ticket data by using NewSessionTicket when a multi-threaded client attempts to reuse a previous ticket.
13. CVE-2015-1792. The CMS code can enter an infinite loop when verifying a signedData message that contains an OID of an unknown hash function. The issue causes the system to be vulnerable to DoS attacks.

Resolved Problems in IMC PLAT 7.1 (E0303L15)

1. Security vulnerability exists on components of the IMC platform that use the OpenSSL library.
2. When SSA monitors multiple servers, the collected data is incorrect.
3. The system obtains incorrect server information when multiple operators perform server operations at the same time. For example, an operator synchronizes Server A information while another operator adds Server B to SSA management.
4. After SSA on a Linux server is upgraded from the basic version to IMC PLAT 7.1 (E0303P14), the system displays an error page when an operator performs auto discovery of servers.
5. When servers are deleted from a custom view, the system automatically deletes the servers from server resources.

6. When **Per-class statistics - All Alarms** is enabled in the display tiling configuration, the alarm panel cannot correctly display the per-class alarm statistics.
7. An operator clicks a MAC address in the online client list of WLAN Manager to view the details. However, display of the MAC address details page is incorrect.
8. An operator clicks an AP label in the fit AP list of WLAN Manager to view the details. However, display of the AP details page is incorrect.
9. When **Per-class TopN alarms - Configuration Alarms** is enabled in the dashboard configuration, the alarm panel data filtered by alarm class is incorrect.
10. After upgrade to a version later than IMC PLAT 7.1 (E0303P13), the system foreground generates logs with an excessive file size.
11. The system generates a "415 Unsupported Media Type" error when executing a RESTful interface by a PUT request through Swagger.
12. The system cannot generate V2 periodic reports that include parameters of long integer type.
13. The RADIUS server configuration and interface 802.1X configuration cannot be made on the device details page for Comware V7 devices.
14. NETCONF is not upgraded with the IMC platform upgrade to IMC PLAT 7.1 (E0303) or later, because the NETCONF upgrade package is not decompressed in the upgrade.
15. This symptom occurs when a user views the dashboard that contains the per-level alarm trend chart. The dashboard displays data incorrectly.
16. This symptom occurs when a user adds the per-level alarm trend chart (the alarm class is all alarms) and the per-class statistics trend chart (the alarm class is configuration alarms) to the dashboard and monitors alarms for some time. Curves of the per-level alarm trend chart fall at irregular intervals.
17. This symptom occurs when a user selects a device on the Applet network topology, right-clicks the device, and then selects Open Device Panel from the shortcut menu. A page error occurs when a user accesses the device panel.
18. This symptom occurs when Enable Mail Notification is selected in license expiration mail notification settings on the system settings page. The mail content is incorrect and the mail format requires optimization.
19. This symptom occurs when a user accesses the system settings page with the alarm module not installed. Accessing the system settings page takes a long time.
20. This symptom occurs when a user clicks Add Link on the link management page for a custom topology. An error for the Add Link page occurs.
21. This symptom occurs when a maintainer logs in to IMC and double-clicks a cloud in the converged topology. A maintainer fails to open the topology for a cloud.
22. This symptom occurs when a user clicks the Add Link icon on the converged topology, or right-clicks the converged topology and selects Add Link from the shortcut menu. An error for the Link Management page occurs.
23. This symptom occurs when a user clicks Save in the toolbar on the converged topology. The note and the background area cannot be saved.
24. This symptom occurs when a uses accesses a REST API. The associated model schema for a REST API does not exist.

25. This symptom occurs after the WSM component is installed. The REST APIs of license management are unavailable and the response codes are 404.
26. This symptom occurs when a maintainer who has no management rights to self-service accounts modifies a user. A page error occurs when a maintainer attempts to modify a user.
27. This symptom occurs when the SSA version is upgraded from IMC PLAT 7.1 (E0303) to IMC PLAT 7.1 (E0303P13). A page error occurs when a user configures server power supply trap information.
28. This symptom occurs when IMC had ever been started before it was upgraded to IMC PLAT 7.1 (E0303P13). The Device Asset Report(Concise) cannot be obtained after IMC was upgraded to IMC PLAT 7.1 (E0303P13).
29. This symptom occurs when a user exports the Device Asset Report(Concise). The summary report at the end of the Device Asset Report(Concise) is displayed incorrectly after the Device Asset Report(Concise) is exported to an EXCEL file.
30. This symptom occurs when the performance management module is installed and monitoring objects are added in IMC that runs in Linux and uses an Oracle database. The performance background process restarts sometimes.
31. This symptom occurs when a user deploys the alarm management module of the IMC PLAT 7.1 (E0303P13) version, undeploys and removes the module, and then deploys the module again. An error occurs during the deployment of the alarm management module of the IMC PLAT 7.1 (E0303P13) version.
32. This symptom occurs when the sending alarm SMS message feature is enabled in IMC that runs in Linux. Alarm SMS messages cannot be received.
33. In the intelligent deployment monitoring agent, the automatic recovery function is enabled and operates for a period of time. Then automatic recovery failed and the disk is filled with logs.

Resolved Problems in IMC PLAT 7.1 (E0303P13)

1. Operation logs are not recorded when you add, delete, or modify the dashboard view.
2. The Y-axis names of the monitoring charts are not completely displayed when you view the realtime performance monitoring page on the IE11 browser.
3. The GSM modem name is incorrectly displayed when you view the GSM modem configuration on the SMSC settings page.
4. Data is incorrectly displayed when you add multiple performance views in a single view of the dashboard.
5. A page error occurs when you save devices for which monitor is canceled as a new view.
6. You can add monitor, cancel monitor, and modify thresholds on the monitor settings page when you log in as a viewer.
7. The interfaces for a link cannot be displayed when you add a link in the Applet topology.
8. The IMC platform components have 13 OpenSSL security vulnerabilities.
9. Attackers are allowed to establish connections with users by sending unauthorized requests because the IMC platform components have the cURL and libcurl security vulnerabilities CVE-2015-3143 and CVE-2015-3148.
10. APM fails to obtain monitoring data when monitoring the FTP server.

11. The HP 10508 switch panel is incorrectly displayed when the page for displaying the switch panel is opened.
12. The HP 5900 switch panel is incorrectly displayed on the rack topology when the switch is added to the rack in the data center topology.

Resolved Problems in IMC PLAT 7.1 (E0303H12)

1. When device configuration files are backed up in batches periodically through TFTP and some devices are unreachable, all TCP ports of the IMC server are used up after some time.
2. When automatic backup is enabled on the primary IMC server and automatic restoration on the backup IMC server, and the size of a database file that the primary IMC server backs up exceeds 2 GB, automatic restoration fails on the backup IMC server.
3. When a subview is selected for an automatic backup plan, the parent view of the subview still can be selected for another automatic backup plan.
4. When a user views details of hpicfArpProtectErrantReply and hpicfDhcpSnoopErrantReply traps in IMC, the MAC address and IP address fields on details pages of hpicfArpProtectErrantReply and hpicfDhcpSnoopErrantReply traps display illegible characters.
5. When a view of the dashboard has multiple performance views, the dashboard displays data incorrectly.
6. On the monitoring settings page, when a user cancels monitoring for a device, selects the device, and then clicks Save as New View, a page error occurs.
7. When a user views and modifies a deleted data entry on the service monitoring page, a page error occurs.
8. In the Web desktop edition of IMC, when a user accesses the performance option page by clicking the Default Monitoring Indexes link, clicks Set, and then clicks Select Colors, a page error occurs.
9. A user fails to sort the interface traffic list on the At A Glance page by clicking the Monitored Objects field of the list.
10. When a user views the user tracking report in IMC that uses the MySQL database with more than 150000 records in the config_db.tbl_l2topo_user_tracking table, the CPU usage of the MySQL process on the IMC server is more than 95 percent and the user tracking report cannot be displayed for a long time.
11. If a user accesses the System > System Configuration > IMC Server Info page when CPU and memory information about the IMC server cannot be collected, a page error occurs.

Resolved Problems in IMC PLAT 7.1 (E0303L11)

1. When a SNMP device is added with the device category as PC and then the device category of the SNMP device is modified to SNMP, IMC fails to recognize the Comware platform software version (V3, V5, or V7) of the device.
2. When a user logs into IMC, accesses the report module, and then exports Custom View Data Summary Report V2 in the CVS format, the first column of the exported report is empty.

3. When a periodic report of Device Category Statistics Report V2 is added, the generated history report Device Category Statistics Report V2 has only the title, without data and legends.
4. When the Y-axis name is set to a long string and the Y-axis unit is set to a short string at the same time or the Y-axis name is set to a short string and the Y-axis unit is set to a long string at the same time, the real-time performance monitoring page collapses.
5. When a viewer logs in to IMC, the viewer has rights to add monitors, modify monitors, and modify properties on the monitor settings page.
6. When a user views Performance View Summary Report V2, the report has no data.
7. When more than 10 device additional information items are added for a device, the device additional information items on the details page of the device have duplicate data.
8. When a user adds devices by clicking the **Add Device** link on the device view page, the user fails to add devices.
9. After a user adds a custom view with the **Automatically Add New Devices** field set to **From Designated Rule** in a MySQL environment, a page error occurs when viewing or modifying the custom view.
10. When DBMan is used for auto backup and auto restoration, DBMan performs only the auto backup operation without performing the auto restoration operation.
11. If multiple auto backup plans are executed at the same time point, some of the mails that send backup results to users are lost.

Resolved Problems in IMC PLAT 7.1 (E0303P10)

1. After the IMC platform is upgraded to the SP10 version without the deployment of the performance management module, the IMC logon page prompts the script execution failure for the performance report.
2. If an operator has access to a performance view but has no access to the folder to which the performance view belongs, a repot page error occurs when the operator attempts to view the Performance View All Summary Report for all performance views or the Performance View Summary Report for the performance view.
3. When a user accesses the HTML5 topology in H3C SNS IMC and clicks a device node on the topology, the performance information for the device does not appear on the topology.
4. When the alarm module is not installed with the IMC platform, the mail sever settings feature in the IMC platform is not supported.
5. When a user uses IE 11 to access the IMC home page and views a widget that has much data, the scrollbar bar does not appear on the widget.
6. When the By Device Model option is selected in the filter settings in the auto discovery plan, a user fails to delete existing device models.
7. When a large number of devices are configured at the same time, imccmdmdrdm runs a large number of processes each named scripttool and the CPU usage reaches 100%.
8. When alarms are recovered manually and the hierarchical alarming feature is disabled, IMC still sends recovery alarms to the registered upper-level network management address.

9. When IMC contains over 7000 devices, device operations such as device deletion or polling interval configuration fail or only partially succeed.
10. An operator unmanages an unreachable device, and then manages the device again after the device becomes reachable. However, the device is not in Normal state although it does not include unrecovered alarms.
11. After IMC is upgraded to support periodic monitoring, performance data that already exists before the upgrade becomes unavailable for devices that are not monitored by any periodic monitors.
12. The 3D panel of a Huawei AR28-31 device does not display interface or status information.
13. The Environment Monitor page of a device crashes when an operator makes another attempt to reset a board after a failed reset.
14. A server or network error occurs when an operator configures SNMP parameters on the System > Resource Management > MIB Management page by using the Config SNMP parameter tool.
15. When a user views the performance data, the performance module displays the maximum and minimum data values for a time range (this week or this month) that are calculated based on the weighted average algorithm instead of the original maximum and minimum data values for a time range.
16. When IMC is configured to send SMS messages to the specified mobile phone numbers by using the Convert Mail into SMS method, some of the specified mobile phone numbers fail to receive SMS messages.
17. If the commonThirdpartyAppContext.xml file in the \client\conf\ directory of the IMC installation path is edited, the file is overwritten by the default file after an IMC upgrade.
18. When IMC monitors about a large number of devices (about 1800), accessing the device view page takes about three minutes.
19. When the home page has multiple Port Group TopN widgets that have different configuration parameters, data display errors occur for these widgets.
20. After the common indexes in the performance option in the IMC platform are modified, the common indexes in RSM are inconsistent with those in the IMC platform when a user adds a monitor in RSM.
21. When IMC has a large number monitor instances and the value of the Interface Info Display field on the System > System Settings page is set to Interface Alias, the loading time for the Resources > Monitoring page is slow.
22. In IMC 7.1 E0303, device display of HP 5130 causes termination with java errors.
23. When IMC is configured to send SMS messages through a GSM modem and alarm statistics SMS is enabled, an SMS message containing special characters ~^|[]{} cannot be correctly displayed after it is received.

Resolved Problems in IMC PLAT 7.1 (E0303L08)

1. During periods of poor network conditions or slow TFTP server/client processing speed, the system automatically deploys large resource files to a newly discovered server through TFTP. However, the file transfer process is slow and causes high CPU usage.
2. IMC is configured to log in to a device through Telnet or SSH by using the Username + Password authentication mode. However, it still tries to use the super password for device login.

3. When accessing a device through SSH, IMC connects to the default SSH port (TCP port 22) instead of the SSH port specified for the device in the IMC platform.
4. It takes the system about 30 minutes to start the performance management process when the number of monitored devices exceeds 10000.
5. In a periodic performance monitor group, the alarm threshold of a device monitor index is exceeded during a non-work time period. The system generates an alarm for the device even though the device's performance data is not displayed.
6. When an administrator adds a maintainer or viewer, the manageable device groups, user groups, and custom views assigned to the maintainer or viewer cannot be saved.
7. A page error occurs when an operator attempts to add a maintainer or viewer with specified manageable Level 1 location views in the WSM privilege management area.
8. An operator adds a routing-based auto discovery plan and then a network segment-based auto discovery plan, but cannot enter the modification page of the routing-based auto discovery plan.
9. An operator accesses the IMC home page by using IE 10. After the operator clicks a device name in the performance TopN widget, the device detailed information appears in the widget instead of a separate device details page.
10. Operators can view information about interface views on the Interface View TopN widget even if they do not have access to these views.
11. An operator uploads a background file on the Regional Map Configuration page for display tiling, backs up data by using DBman, reinstalls IMC, and restores data to IMC. Then the display tiling feature fails to load the background file.
12. When IMC runs on Linux and uses an Oracle database, an operator cannot access the MAC vendor configuration page.
13. On the IMC [RAM-Service deployment] page, the following configuration is deployed: bandwidth guarantee, traffic shaping, QoS access control, CAR rate limiting, CBQ policy, and interface rate limiting. However, commands on the deployment details page are not displayed in separate lines.

Resolved Problems in IMC PLAT 7.1 (E0303L07)

1. When the amount of the device MIB information is large, page errors might occur.
2. If a new icon file is uploaded when modifying the device icon, the new device icon displays differently from the original icon in size on the custom topology of the HTML5 topology.
3. If IMC uses a MySQL database, the compliance check task remains in running state for a device with a large configuration file.

Resolved Problems in IMC PLAT 7.1 (E0303P06)

1. If a compliance check task of more than 180 days is deleted by the system, the compliance check task might fail to be executed after IMC is restarted.
2. A VLAN fails to be deleted on the VLAN device information page.

3. When you add or modify a DNS service monitor on the Service Monitoring page, you can input up to 32 characters for the FQDN.
4. On the performance monitoring data statistics page, when you switch between time ranges or open a sub-page, the data statistics are not refreshed and you are logged out.
5. Link-down traps for aggregation group member ports are repeatedly generated though the aggregation group member ports are always down.
6. After you configure interface trap filtering in batches, the interface traps are not filtered.
7. If a non-admin operator configured with custom device group privilege exports alarms into a .CSV file on the All Alarms page, the exported .CSV file does not have data.
8. The security vulnerabilities CVE-2014-3566 are fixed.

Resolved Problems in IMC PLAT 7.1 (E0303H03)

1. In the Linux system which enable both IPv4 and IPv6, import device software fails.
2. If you perform the SNMP test when the device location information is null, the SNMP test fails.
3. Page errors occur when a user adds, modifies, and copy mail notifications on the **Alarm Notification** page.
4. An operator who has customized homepage widgets logs in to IMC and customizes homepage widgets again, but the modifications for the homepage widgets cannot be saved.
5. IMC sends alarm notifications through a SMS sender and mobile phones fails to receive the SMS messages of alarm notifications.
6. A user adds a performance widget on the Flex-based display tiling page, right clicks on the performance widget and selects **Parameter Configuration** from the shortcut menu, and then clicks **Add Instance** on the page that appears. The user fails to add a monitor instance.
7. A user fails to add or modify device groups on a Linux host with Oracle database.
8. When a user points to an alarm level legend at the lower-left corner of the IMC home page, the alarm statistics graph for the alarm level does not appear. However, IMC displays the alarm statistics graphs correctly on other pages when the same operations are performed.
9. A user accesses the **Access Details** or **Online Users** page and adds multiple columns by clicking **Customize GUI**, but IMC fails to automatically resize columns.
10. When you modify the users that an account name belongs to through the user modifying function of the platform, clicking an account name on the **All Access Users** list causes an error.
11. In a stateless failover environment where all platform components are deployed on the active host and the GAM component is not deployed on the standby host, you will fail to immediately restore the database on the standby host.

Resolved Problems in IMC PLAT 7.1 (E0303L02)

1. A viewer can access the **System > Panel Management** page by entering the URL of the page in the address bar, and then perform all administrative operations on the page.
2. The monitor graph of RMON statistics groups on a device displays an incorrect time axis that does not match the actual time.
3. An operator cannot access the device details page by clicking the device label of an HP 1950 device.
4. If a performance view contains performance trend graphs with breaks in them, the following reports are unavailable: Performance Data Detail Report and View Format Line Chart Report.
5. Newly-added custom TopN monitor widgets display incorrect data after a refresh on the home page.
6. When IMC monitors more than 2100 devices, a viewer cannot access the **Resource > Monitoring Settings** page.
7. The Performance Trend widget for display tiling lacks data of some monitoring instances if not all instances use the same collection time interval.
8. IMC is stuck on loading if an operator attempts to display the Monitoring Settings page for a large number of monitored devices.
9. The Resource > Service Monitoring page becomes faulty after an operator clicks the Real-time Monitoring icon on the performance data page of an instance. The problem persists even if the operator exits and relogs in to IMC.
10. After IMC is upgraded to the 7.1(E0302) version, some page responds slowly.

Resolved Problems in IMC PLAT 7.1 (E0303L01)

1. Error page occur if the ACL Devices Only box is cleared on the ACL device page when the number of devices in the platform exceeds 2100.

Resolved Problems in IMC PLAT 7.1 (E0303)

1. The enterprise edition should include the NTA component.
2. Sounds on the alarm panel cannot be muted from the sound settings.

Resolved Problems in IMC PLAT 7.1 (E0302)

1. The "Server Errors" message might appear when you perform either of the following tasks: 1) Add custom indexes on the Resource > Global Index Settings page. 2) Query indexes on the Resource > Global Index Settings page.
2. The Liveupdate feature failed.

[Table of Contents]

IMC Software Distribution Contents

The IMC PLAT 7.2 (E0403P10) distribution list contains the following files and folders:

1. **manual\readme_plat_7.2 (E0403P10).html** - This file
2. **windows\install** - IMC installation program
3. **linux\install** - IMC installation program for Red Hat Enterprise Linux

[Table of Contents]

Installation Prerequisites

Server Requirements

The following are the minimum hardware requirements and supported software programs to run IMC:

- Minimum hardware requirements
  - Pentium 4 3.0 GHz processor
  - 4 GB of RAM
  - 50 GB hard disk space

- Operating system (Versions marked X64 are recommended):
  - Windows Server 2008 with Service Pack 2
  - Windows Server 2008 X64 with Service Pack 2
  - Windows Server 2008 R2 with Service Pack 1
  - Windows Server 2012 with KB2836988
  - Windows Server 2012 R2
  - Red Hat Enterprise Linux 5.5 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5.5 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5.9 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5.9 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 6.x X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 7.x X64 (Enterprise and Standard versions only)

- VMware:
  - VMware Workstation 6.5.x
  - VMware Workstation 9.0.x
  - VMware ESXi Server 4.x
  - VMware ESXi Server 5.x

- Hyper-V:
    - Windows Server 2008 R2 Hyper-V
    - Windows Server 2012 Hyper-V

- Database
    - Microsoft SQL Server 2008 Service Pack 3 (Windows only)
    - Microsoft SQL Server 2008 R2 Service Pack 2 (Windows only)
    - Microsoft SQL Server 2012 Service Pack 3 (Windows only)
    - Microsoft SQL Server 2014 (Windows only)
    - Oracle 11*g* Release 1 (Linux only)
    - Oracle 11*g* Release 2 (Linux only)
    - Oracle 12*c* Release 1 (Linux only)
    - MySQL Enterprise Server 5.5 (Linux and Windows) (Up to 1000 devices are supported)
    - MySQL Enterprise Server 5.6 (Linux and Windows) (Up to 1000 devices are supported)

Note: 64-bit operating systems are recommended over 32-bit operating systems because of the larger amount of available memory for applications.

Note: Optimal hardware requirements vary with scale, other management factors, and are specific to each infrastructure. Please consult HP, or your local account teams and precise requirements can be provided.

GSM modem (optional)

A GSM modem is required for forwarding alarm messages. The following models have been tested to work with IMC. For more information about a specific GSM modem, see its product manual.

- WaveCom M2306B
- WaveCom TS-WGC1 (Q2403A)
- Wanxiang serial port GSM modem (DG-C1A)
- Wanxiang USB GSM modem (DG-U1A)
- Wanxiang USB min GSM modem (DG-MINI)
- WaveCom M1206B GSM modem (chip: 24PL)
- WaveCom USB M1206B GSM modem (chip: Q24PL, Q2403A)

[Table of Contents]

Client Prerequisites

PC Requirements

- Minimum hardware requirements
    - 2.0 GHz processor
    - 2048 MB of RAM
    - 50 GB hard disk space

- Operating system
    - Windows XP SP3 or later

- Browser
    - IE 10 or 11 is recommended.
    - Firefox 30 or later is recommended.
    - Chrome 35 or later is recommended.
    - Turn off the blocking settings in the browser.
    - Add the IMC website to the trusted sites of the browser.
    - The recommended resolution width is 1280.
    - JRE 1.6.0_update27 or later is recommended. If a client has no JRE, IMC prompts the user to install JRE for the client.

[Table of Contents]

Installing and Upgrading IMC

To install IMC on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2, first modify the user account control settings:

1. Open the Control Panel from the Start menu and click **System and Security**.
2. In the **Action Center**, click the **Change User Account Control Settings** link.
3. In the **User Account Control Settings** window, set the **Choose when to be notified about changes to your computer** to **Never notify**.

To upgrade IMC:

1. Back up the IMC database on the **Environment** tab in the Deployment Monitoring Agent.
2. Manually copy the IMC installation directory to a backup path.
3. Stop IMC in the Deployment Monitoring Agent.

4. Click **Install** on the **Monitor** tab of the Deployment Monitoring Agent
5. Select the **windows/install/components** directory in the upgrade package and click **OK**.
6. Click **OK** in the popup message dialog box.
7. Click **Start** in the **Upgrade Common Components** dialog box to upgrade common components.
8. After common components are upgraded, click **Close**.
9. In distributed deployment mode, stop the Deployment Monitoring Agent on the master server and restart the Deployment Monitoring Agent on every subordinate server. Click **Yes** in the popup message dialog box to upgrade common components on every subordinate server.
10. The Deployment Monitoring Agent displays all components that need to be upgraded. Click **OK** to start upgrading.
11. In distributed deployment mode, upgrade all components deployed on every subordinate server.
12. After all components are updated, start all processes in the Deployment Monitoring Agent.

For more information about installation and upgrade procedures, see *IMC Getting Started Guide* and IMC deployment guides.

Important:

1. *Before you upgrade the IMC Platform, download upgrade packages for all deployed service components from HP's website, and before you install them pay special attention to the section "Platform Compatibility" in their readme. If an upgrade package is not available for a service component, HP recommends not upgrading the IMC Platform, or you can remove the service component before upgrading the IMC Platform. When the service component is removed, its data is lost.*
2. *If the Deployment Monitoring Agent displays a list of components incompatible with the new version of the IMC Platform, you must download upgrade packages for these components before you can continue the upgrade process.*
3. *All service components must use v7.0 or higher to work with IMC PLAT 7.0. After the IMC Platform is upgraded, upgrade the deployed service components, such as WSM, UAM, EAD, NTA/UBA, APM, and SOM. Before installing or upgrading a service component on this platform software, please verify the section "Platform Compatibility" in the service component ¡¯s readme. Otherwise, IMC might not be started. For the compatibility matrix, see readme files of the service components.*
4. *If you receive the message "Upgrade JVM failed..." during the upgrade process, delete the folder in the* ***\common\jre*** *directory of the IMC installation path and continue to upgrade.*
5. *For data integrity, HP recommends backing up database on the* ***Environment*** *tab of the Deployment Monitoring Agent, and copying the IMC installation directory to a secure location after the upgrade.*

[Table of Contents]

Removing IMC

To remove IMC on Windows, run the uninstallation wizard by selecting **All Programs > Intelligent Management Center > Uninstall IMC** from the Start menu, or you can remove the Intelligent Management Center in the **Add or Remove Programs** window of the Control Panel.

To remove IMC on Linux, enter the **deploy** directory of the IMC installation path by using the **cd** command, and then execute **uninstall.sh**. IMC is typically installed in the **/opt/iMC** directory.

Follow the directions in the uninstallation wizard, and manually delete all files in the IMC directory when the process is complete.

[Table of Contents]

Running the Deployment Monitoring Agent

The Deployment Monitoring Agent is a GUI program to manage the deployment of the IMC modules and monitor the performance and the state of processes of the IMC server. After the installation finished, the Deployment Monitoring Agent is automatically started to guide the user through deployment.

On Windows, run the Deployment Monitoring Agent by selecting **All Programs > Intelligent Management Center > Deployment Monitoring Agent** from the Start menu. On Linux, run the Deployment Monitoring Agent by executing **dma.sh** in the **deploy** directory of the IMC installation path.

If Deployment Monitoring Agent cannot start, make sure the HP IMC Server service is running. This service is automatically started along with the OS and runs as a daemon/background process. On Windows, you can start the service in Windows Services. On Linux, you can start the service with the **service imcdmsd start** command.

IMC must be started from the Deployment Monitoring Agent.

[Table of Contents]

Starting IMC

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

[Table of Contents]

Logging in to IMC through a Web Browser

Once the server is running, you can access the IMC user interface using a Web browser. Enter the following address in the Address Bar of a browser:

```
http://hostname:port/imc
```

Where *hostname* is the host name or IP address of the IMC server (the default is localhost if you launch the Web browser on the IMC server machine), and *port* is the Web server port (the default is 8080) used by IMC.

You can also access the IMC user interface with Web browser through HTTPS. Enter the following address in the address bar of a browser:

```
https://hostname:port/imc
```

Where *hostname* is the host name or IP address of the IMC server (the default is localhost if you launch the Web browser on the IMC server machine), and *port* is the Web server port for HTTPS (the default is 8443) used by IMC.

When the IMC login page appears, use the username "admin" and password "admin" to log into IMC.

Refer to the IMC Online Help for details on how to add operators, and add your devices to IMC.

The default security level in the IE properties is High. If you try to log in to IMC with this default, the system will prompt "Content from the Web site listed below is being blocked by the Internet Explorer Enhanced Security Configuration." Click Add to add the IMC website to the trusted sites. If you do not add the IMC website to the trusted sites and determine not to display the prompt any more, you may fail to log in to IMC. To solve the problem, use either of the following methods:

1. Set the security level to **Medium**.
   - Start IE and select **Tools > Internet Options**.
   - Select the **Security** tab, and then click **Custom Level**.
   - In the popup dialog box, set the security level to **Medium**.
2. Add the website of the IMC server to the trusted sites.
   - Start IE and select **Tools > Internet Options**.
   - Select the **Security** tab, Select **Trusted sites**, and the click **Sites**.
   - Add the website of the IMC server in the popup dialog box.

On your first access to **Resource > Network Topology**, the browser prompts "The application's digital signature cannot be verified. Do you want to run the application?" Below the prompt are the name "topo", and the publisher "IMC Development Team". Select the "**Always trust content from this publisher**" checkbox, and click **Run**.

Note: *In centralized deployment, when the "User Access Manager - User SelfService" component is deployed, you will enter the Self-Service login page rather than the IMC login page if you enter **http://hostname:port/** in the address bar. To enter the IMC login page, change the string following **window.location.href**= into '**/imc/login.jsf**'**;** in the index.html file in directory **\client\web\apps\ROOT**.*

[Table of Contents]

Monitoring the Server

On the **Monitor** tab of the Deployment Monitoring Agent, you can see the Disk Usage, CPU Usage, and Physical Memory Usage of the IMC server. On the **Process** tab of the Deployment Monitoring Agent, you can see all IMC processes and their running status. On the **Environment** tab of the Deployment Monitoring Agent, you can see the OS information and database usage.

You can see the monitoring data of the IMC server only when IMC is started. For information about starting IMC, see "Starting IMC".

[Table of Contents]

Distributed Deployment

The IMC components can be installed on more than one server to meet specific performance requirements. A distributed IMC system typically has one master server with IMC Platform deployed and multiple subordinate servers with service components deployed.

To install IMC on a subordinate server, execute the **installslave.bat** file on Windows (or **installslave.sh** on Linux) by either double-clicking the file or running the command in the folder where **installslave.bat** (or **installslave.sh**) is located.

For information about deploying IMC in distributed mode, see IMC deployment guides.

[Table of Contents]

Platform Specific Issues

Windows - General Issues

- Please be especially careful about how filenames are capitalized and used. This is essential in order to ensure consistent behavior across platforms that might use case-sensitive file systems.

Linux - General Issues

- The IMC server must be run from a root user account in order to receive SNMP traps, accept syslog messages, and facilitate ftp file transfers.
- UNIX filenames are case sensitive. Care must be taken when references are made to python scripts and xml files.

[Table of Contents]

Port Usage

IMC uses the following TCP/IP ports.

Component	Subcomponent	Protocol	Port	Configurable	Use	Server	Client	N
IMC Platform	-	TCP	8025	No	Used by the **jserver** process to receive the SHUTDOWN command.	IMC master server.	IMC master server.	Int use
IMC Platform	-	TCP	9091	No	JMX monitoring port used by the **jserver** process.	IMC master server.	IMC master server.	Int use
IMC Platform	-	TCP	9044	No	Used by the **HP IMC Server** service to receive the SHUTDOWN command.	IMC master and subordinate servers.	IMC master and subordinate servers.	Int use

IMC Platform	-	TCP	9055	No		Used by the **Deployment Monitoring Agent** process to receive the SHUTDOWN command.	IMC master and subordinate servers.	IMC master and subordinate servers.	Int use
IMC Platform	-	TCP	61616	No		Used for communication in a distributed deployment environment.	IMC master server.	IMC master and subordinate servers.	Int use
IMC Platform	-	TCP	61626	No		Used for communication between the **HP IMC Server** and **Deployment Monitoring Agent** processes.	IMC master and subordinate servers.	IMC master and subordinate servers.	Int use
IMC Platform	Resource Management	UDP	161	No		Used to access network devices through SNMP.	Network devices.	IMC master and subordinate servers.	
IMC Platform	Resource Management	UDP	162	No		Used to receive SNMP Traps from network devices.	IMC master and subordinate servers.	Network devices.	
IMC Platform	Resource Management	TCP	22	No		SSH/SFTP port, which the configuration center uses to back up and restore the device software and configuration file through SSH/SFTP.	Network devices.	IMC master and subordinate servers.	

IMC Platform	ICC	TCP	20/21	No	FTP port, which the configuration center uses to back up and restore the device software and configuration file through FTP.	Network devices.	IMC master and subordinate servers.
IMC Platform	ACL Management	TCP	23	No	Telnet port, which the resource management module, ACL management module, and configuration center use to access the device through Telnet.	Network devices.	IMC master and subordinate servers.
IMC Platform	Alarm Management	TCP	25	No	SMTP port, which the resource management module uses to send alarms through email.	SMTP Server	IMC master and subordinate servers.
IMC Platform	Resource Management	ICMP		No	ICMP port, which the resource management module uses to discover devices and check the reachability of the devices.	Network devices.	IMC master and subordinate servers.
IMC Platform	Resource Management	UDP	69	Yes	IMC-specific tftp daemon.	IMC master and subordinate servers.	

IMC Platform	Resource Management	TCP	80	Yes	Used to launch the Web network management system of the device.	Network devices.	IMC master and subordinate servers.
IMC Platform	Virtual Resource Management	TCP	443	Yes	HTTPS port, which the virtual network management module uses to obtain VMware virtual network data in SSL.		IMC master and subordinate servers.
IMC Platform	Syslog Management	UDP	514/515	Yes	IMC-specific syslog daemon.	IMC master and subordinate servers.	Network devices.
IMC Platform	Resource Management	TCP/UDP	137	No	NetBIOS name resolution service port, used by the IMC resource management module and terminal access module.		IMC master and subordinate servers.
IMC Platform	-	TCP	8080	Yes	IMC-specific Web server for HTTP protocol, which can be changed during installation.	IMC master server.	
IMC Platform	-	TCP	8443	Yes	IMC-specific Web server for HTTPS protocol, which can be changed during installation.	IMC master server	

IMC Platform	-	TCP	8800	No	IMC messaging gateway listening port.	IMC master and subordinate servers.	IMC master and subordinate servers.	Int use
IMC Platform	-	TCP	21190-21199	No	Java RMI communication port.	IMC master and subordinate servers.	IMC master and subordinate servers.	Int use
IMC Platform	-	TCP	1433	Yes	SQL Server database listening port (on Windows only).	SQL Server.	IMC master and subordinate servers.	
IMC Platform	-	TCP	3306	Yes	MySQL database listening port.	MySQL Server.	IMC master and subordinate servers.	
IMC Platform	-	TCP	1521	Yes	Oracle database listening port (on Linux only).	Oracle Server.	IMC master and subordinate servers.	
IMC Platform	DBMan	TCP	2810	No	Used for communication in DBMan.	DBMan.	DBMan.	Int use

Note: *On Linux, you must run IMC with root privileges to bind TCP/IP ports 69, 162, and 514.*

Note: *IMC cannot be bound to TCP/IP ports 69, 162, and 514 if they are used by other SNMP, TFTP, or syslog applications.*

Note: *Make sure the firewall on each IMC server does not block programs javaw.exe and java.exe. The programs are located in directory \common\jre\bin (/common/jre/bin/java for Linux) of the IMC installation path.*

[Table of Contents]

Memory Allocation

The amount of memory allocated to the IMC jserver can be adjusted by a script. The memory size should be tuned to make use of as much memory as required by your particular IMC server. Move to the "client\bin" (or "client/bin" on Linux OS) sub-directory of the original IMC installation directory (using the "cd" command), and use the `setmem.bat (or setmem.sh on Linux OS)` script.
For example, to allocate 1024 MB RAM, move to the "installation directory\client\bin" (or "installation directory/client/bin" on Linux OS) directory, and run the script:

`setmem.bat` *`1024`* (Windows OS)

`setmem.sh` *`1024`* (Linux OS)

The default and maximum memory that can be allocated to the IMC jserver is listed below:

OS Type	Default allocatable memory	Maximum allocatable memory
Windows 32-bit	512 MB	1024 MB
Windows 64-bit	2048 MB	Depending on the physical memory
Linux 32-bit	512 MB	1280 MB
Linux 64-bit	2048 MB	Depending on the physical memory

[Table of Contents]

Known Problems

Installation/Upgrade/Patch

- For a correct installation, the installation path can contain letters, digits, underlines, and spaces, but cannot contain other special characters.
- If the system installed with IMC has insufficient memory, java overflow might occur. To prevent this issue, install IMC in a 64-bit OS with sufficient memory.
- During IMC platform upgrade from 7.1 (E0303L07), the system might display a message that directory iMC/deploy/jdk should be deleted manually. If you see the message, perform the following steps:
    - Start Windows Task Manager.
    - On the Processes tab, click the View menu and select Select Columns. Select the Command Line column and click OK.
    - Select the process named javaw.exe and click End Process.
    - In the dialog box that displays the upgrade error message, click Retry.

Other Problems

- If the system is busy, the progress bar may be shown for a long time when you perform an operation.
- IMC does not support the PoE features of Comware V3 devices.
- Configuration Center does not support the software upgrade of IRF devices through SSH/SFTP.
- Configuration Center does not support the software upgrade of old IRF2 devices or a device with dual main boards.
- If you configure a link aggregation across different units of IRF/IRF2 devices, the layer 2 topology cannot display the links because the master device cannot collect complete information about links of the subordinate members. Ensure you configure link aggregations only on the master device.
- When you view the check result of a compliance check task, the system might display "Do you want to abort the script?" if the check result contains too many devices and policies. Click **No** to continue the operation.
- A prompt "Connection to the server disconnected. Check the connection and try again" is displayed after the realtime performance monitoring runs for a while. Ignore the message and click **OK**.
- If the device model is not correct for a third-party device, select **System > Device Model** to edit the setting.
- In an SNMP packet, the SNMP variables of the visible string type, the encoding mode must be GBK or ASCII.
- If you upgrade your IMC to IMC PLAT 7.1, make sure you upgrade all components after the upgrade package is installed. Otherwise, IMC cannot start.
- The device locations might change on the Google map topology in windows of different sizes or in full screen with different resolutions.
- Discontinue monitoring the VM performance indices when the VM migrated to other hypervisor.
- If you cannot open the Applet topology after upgrading Java to the latest version for the client, select Control Panel > Java > Security, and set the Security Level to Middle.
- When you execute the backup.bat(.sh) script to back up IMC before upgrading IMC, only files are backed up, but the database is not backed up.
- In the dashboard, the realtime performance monitoring data for memory utilization is displayed for CPU utilization.
- In the converged topology, the status of a subview is always displayed as grey, which is displayed based on alarms of the highest level on the devices in the subview.
- The following problems occur to the 3D chassis in the data center: the added virtual devices and trays cannot be displayed; the device locations in the 3D chassis are incorrect; after you configure the chassis, the newly added devices can be displayed only after the 3D chassis is reloaded.
- In the Linux system, import device software fails when both IPv4 and IPv6 exist.
- If IP addresses on two different network segments are configured on the IMC server, the non-default initial configuration file fails to be downloaded when a device with zero configurations is automatically deployed.
- The SNMP test fails when the device location information is null.

- A user creates a view on the Flex-based display tiling page and adds performance trend widgets and widgets of other types for the view. The user configures no parameters for all widgets. The view displays the URL of the third-party control when the user accesses the view page for the first time. The URL of the third-party control disappears and the performance trend widgets become unavailable when the user accesses the view page for a second time.
- After VLAN interfaces are undeployed for tenants through RAM, the system prompts a configuration conflict if you deploy the same VLAN interfaces.
- When VLANs are deployed to a device, access interface configurations fail.
- After the Telnet or SSH parameters are modified for devices, the devices are not immediately synchronized in the ACL manager.
- A Cisco low-end switch is added to the IMC platform with the SSH access method, Password authentication mode, and an empty password field. When an operator syncs or tests connectivity to the switch, the memory usage of the resource background process soars in seconds and the process eventually crashes.
- Some of the E1POS interfaces of a device are not displayed on the device interface list, which is accessed by selecting POS Access > Interfaces on the device details page.
- When a user logs on to IMC with the browser in windowed mode and then maximizes the browser, the page size cannot be adjusted. To solve this problem, refresh the page.
- After the BIMS component is deployed on IMC, the V2 report still cannot be viewed. To solve this problem, delete the castor-0.9.9.1.jar in **iMC\client\repository\castor\jars\** folder, and copy the castor-1.2.jar from **iMC\client\web\apps\rptviewer\WEB-INF\lib\** folder to the **iMC\client\repository\castor\jars\** folder.
- Chrome42+ disables NPAPI, including JRE. Because of this, IMC cannot open applet when using Chrome 42+.
- There are more than 20 devices in a filter rule, fail to add the Syslog filter rule.
- Add monitor again after the VM migrated to other hypervisor, discontinue monitoring the VM performance indices when the VM migrated to other hypervisor.
- This symptom occurs when use the converged topology feature. In the converged topology, the status of a subview is always displayed as grey, which is displayed based on alarms of the highest level on the devices in the subview.
- Open data center topology, The following problems occur to the 3D chassis in the data center: the added virtual devices and trays cannot be displayed; the device locations in the 3D chassis are incorrect; after you configure the chassis, the newly added devices can be displayed only after the 3D chassis is reloaded.
- This symptom occurs when IP addresses on two different network segments are configured on the IMC server. The non-default initial configuration file fails to be downloaded when a device with zero configurations is automatically deployed.
- An operator frequently switches between floors of a room, On a room topology, frequent switches between floors cause the windows and doors to display incorrectly.
- A user creates a view on the Flex-based display tiling page and adds performance trend widgets and widgets of other types for the view. The user

configures no parameters for all widgets. The view displays the URL of the third-party control when the user accesses the view page for the first time. The URL of the third-party control disappears and the performance trend widgets are unavailable when the user accesses the view page for the second time.

- This symptom occurs if the target device is not synchronized after VLAN interfaces are undeployed.After VLAN interfaces are undeployed for tenants through RAM, the system prompts a configuration conflict if you deploy the same VLAN interfaces.
- This symptom occurs if the Layer 2 aggregate interface configuration changes made in the VLAN manager are not synchronized to devices.When VLANs are deployed to a device, access interface configurations fail.
- This symptom occurs when the Telnet or SSH parameters are modified for devices. After the Telnet or SSH parameters are modified for devices, the devices are not immediately synchronized in the ACL manager.
- A Cisco low-end switch is added to the IMC platform with the SSH access method, Password authentication mode, and an empty password field. An operator tests connectivity to the switch, or sync the device to IMC platform.When an operator syncs or tests connectivity to a newly added Cisco low-end switch, the memory usage of the resource background process soars in seconds and the process eventually crashes.
- An operator accesses the POS Access > Interfaces page from the device details page. Some of the E1POS interfaces of a device are not displayed on the device interface list page.
- A server automatic deployment plan contains a Windows OS template that has more than three partitions with the Use free capacity option selected.IMC failed to deploy the OS template in a server automatic deployment plan.
- This symptom occurs when DHCP is configured to assign IP addresses on a bare metal server and auto deployment is enabled in SSA.Auto deployment is not triggered for a bare metal server.
- This symptom occurs when a user operates multiple servers at the same time. For example, a user synchronizes server A and adds server B to SSA for management at the same time.An error occurs when IMC obtains server information.
- This symptom occurs when SSA monitors multiple servers.SSA collects data incorrectly.
- This symptom occurs when the CAS version is earlier than E0209.No data is collected when VRM monitors CAS.
- On the custom topology, device labels are modified to Korean character strings, and they become illegible after the topology is reloaded.
- The default background of the H3C Web desktop edition is changed to the HPE image.
- In HPE RSM edition, the HPE logo is not aligned to the upper-left corner on the login page.
- The topology does not support displaying complete distributed trunk links for HP switches.
- Traps cannot be received when the trap OID exceed 128 characters or the trap packet exceeds 4096 bytes.
- When the SNMP packet maximum size on a device is set to a value greater than 4096, SNMP packets from the device cannot be parsed.

- In a non-English operating system, you must modify the language to English (United States) in the Control Panel > Region and Language window. Then, click Copy settings in the Administrative tab, and select Welcome screen and system accounts and New user accounts.
- In an English operation system, you must use the default language format in the Control Panel > Region and Language window.
- The Axis2(CVE-2010-1632) vulnerability exists. To solve this problem, manually delete the folder iMC\client\web\apps\imcws.
- After Java 8 is installed, a security warning dialog box displaying that the publisher is unknown appears when you click SSH on device Action list. To solve this problem, manually import the iMC\client\security\newksp12.p12 certificate file into the Signer CA certificate of jdk.

[Table of Contents]

Issued: Sep 2016

© Copyright 2016 Hewlett Packard Enterprise Development LP