CA Unified Infrastructure Management

Getting Started Guide

8.0

Document Revision History

Version	Date	Changes
8.0	September 2014	Rebranded for UIM 8.0.
7.6	June 2014	No revisions.
7.5	March 2014	No revisions.
7.1	December 2013	No revisions.
7.0	September 2013	Revised for NMS 7.0.
6.5	March 2013	Minor revisions for NMS 6.5.
6.2	December 2012	Revisions and documentation fixes for NMS 6.2.
6.1	September 2012	Minor revisions and documentation fixes for NMS 6.1.
3.0	June 2012	Revised for NMS 6.0.
2.0	October 2011	Simplified and revised.
1.0	June 2010	Initial version of *Nimsoft Server Getting Started Guide.*

Contact CA

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

Send comments or questions about CA Technologies product documentation to nimsoft.techpubs@ca.com.

To provide feedback about general CA Technologies product documentation, complete our short customer survey which is available on the support website at http://ca.com/docs.

Copyright Notice

Legal information on third-party and public domain software used in this product is documented in the *Third-Party Licenses and Terms of Use* *(*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Contents

Chapter 1: Introduction

CA Unified Infrastructure Management is a network management solution that enables you to monitor and manage performance and availability across complex environments. The flexible, modular, and scalable architecture allows you to:

- Monitor every port on every server, hub, switch and router in your IT environment.
- Discover TCP/IP networks, display topologies, monitor network health, and gather performance data so that you can quickly identify the root cause of network failures.
- Maintain device inventory for asset management and rapidly add new IT monitoring capabilities as your infrastructure evolves.
- View dashboards and receive notifications on outages in real time.
- Configure UIM components from anywhere in your network.
- Drill down into device metrics and performance reports, analyze network data, and develop reports on network trends.
- Manage network areas that are segmented by highly restrictive firewalls and compartmentalize or restrict operator actions and views of the network.

CA UIM components also seamlessly integrate with CA UIM Service Desk.

Components

CA Unified Infrastructure Management consists of:

- **CA UIM Server**, which includes the distributed software that monitors your IT environment and collects, controls and stores the data
- **Infrastructure Manager**, a Windows-based interface for configuration and management of your UIM system
- **AdminConsole**, a browser-based management console that provides many of the same features of Infrastructure Manager
- **Unified Management Portal** (UMP), a web-based portal that lets you discover devices and view your data, alarms and messages in a variety of ways

About This Guide

This guide provides an overview of the CA Unified Infrastructure Management solution. It is written for systems administrators, IT professionals and business managers who need a basic understanding of the UIM components and how they work together.

This guide focuses on four areas:

- UIM Server (see page 9) provides an introduction to UIM monitoring. It describes the infrastructure components, the message flow, and system security.
- Admin Console (see page 21) introduces you to the browser-based management console that enables you to configure and manage your UIM components.
- Infrastructure Manager (see page 23) gives an overview of the Windows-based configuration and management interface.

  Note: As of this release, some configuration tasks can only be completed in Infrastructure Manager.
- Unified Management Portal (see page 25) introduces you to UMP, a customizable web-based interface where you can view alarms and messages, monitor and manage computer systems, create and view reports, and perform many other tasks.
- Alarms (see page 29) provides an introduction to how alarms are created and handled.

For more information. see the following documents, available either from the documentation library or from the **Downloads** tab at support.nimsoft.com:

- *CA UIM Server Installation Guide*
- *CA UIM Server Configuration Guide*
- *CA UIM Server Infrastructure Manager Guide*
- *CA UIM Admin Console Guide*
- *CA UIM Unified Management Portal User Information*
- *CA UIM Server Release Notes and Upgrade Guide*

Chapter 2: UIM Server

Data collection and storage is handled by CA Unified Infrastructure Management Server (UIM Server). The distributed components work together to provide fault and performance monitoring. This section describes the components, explains how they work together, and provides scenarios that show how they can be distributed for various deployments.

This section contains the following topics:

Supported Systems

CA Unified Infrastructure Management server and monitoring software is supported on Windows, Linux and Solaris systems. Monitoring software is also supported on AIX and HP-UX systems. For a complete list of supported operating systems, databases, and browsers, see the CA Unified Infrastructure Management Compatibility Matrix.

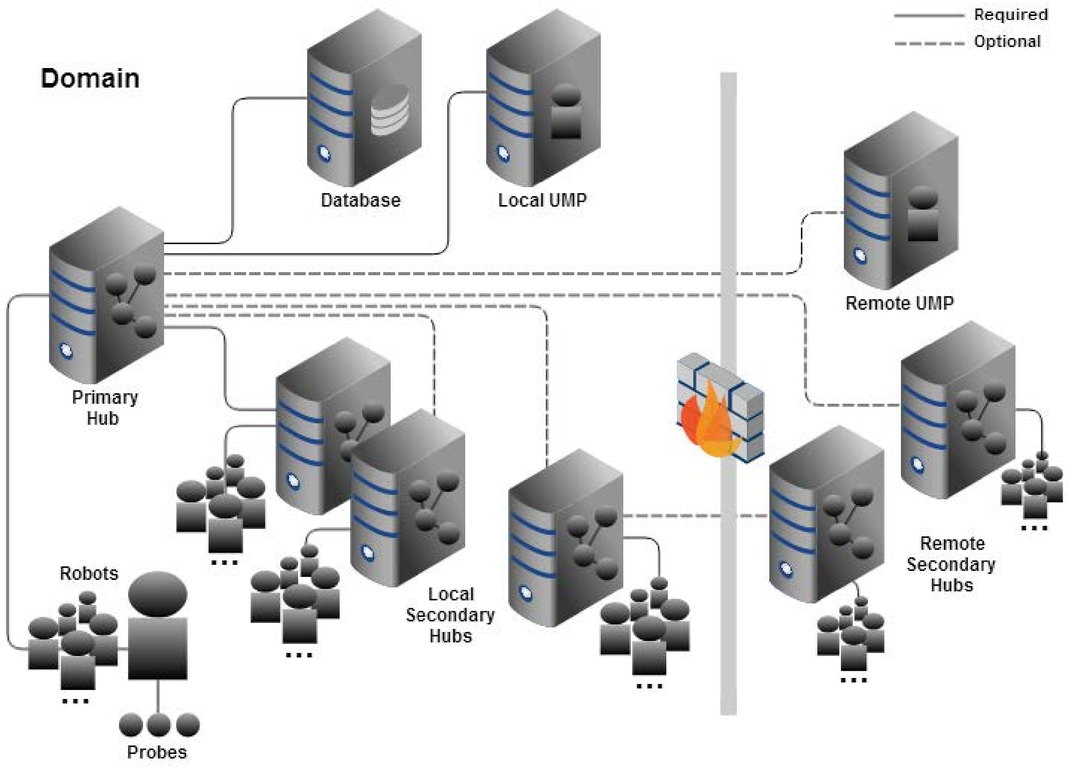
System Architecture

The CA Unified Infrastructure Management system architecture consists of the infrastructure, which is the distributed software that monitors your IT environment and controls the data, and the database that stores the data.

All infrastructure components are organized in a hierarchy. From bottom to top, the components are:

- Probes
- Robots
- Hub
- Domain

The following illustration shows a CA Unified Infrastructure Management domain, encompassing the server, database, management consoles, and infrastructure (hub, robots, probes):



The components allow you to customize your monitoring setup and organize the flow of data.

Probes

A *probe* is small piece of software that performs a dedicated task. CA Unified Infrastructure Management has two types of probes:

- **Monitoring probes** gather availability and performance data. Some probes gather data from the computer on which they reside. Remote probes monitor devices external to themselves, such as network switches and routers.
- **Service probes** (also called infrastructure or utility probes) provide product utility functions.

Probes can be easily configured for your own specific monitoring requirements. For example, you can configure them to run at a specific time (timed probe) or continuously (daemon probe). Each probe maintains its own configuration file.

UIM tools allow you to easily and efficiently deploy probes to *robots*, the next component in the UIM hierarchy.

Custom Probes

CA's out-of-the-box solutions provide a quick start and typically cover about 80% of the needs for server and workstation monitoring in most organizations.

Because the remaining 20% varies from site to site, CA allows you to develop your own solutions that are targeted directly at the problems causing the most trouble. The Software Development Kits (SDKs) let you develop probes and utilities that integrate with your UIM environment. SDKs are available for the following programming languages:

- Perl
- C
- Java
- Visual Basic/.NET

Marketplace Probes

The CA UIM Marketplace allows developers to make their third-party UIM packages available to users. To go to the marketplace, click the shopping cart icon in Admin Console.

By default, marketplace probes are required to run in a restricted environment for security reasons:

- They must run on a passive robot. Passive robots do not send messages to the hub; messages are sent only at the hub’s request. Robots can be either:
  - Installed as passive robots. For instructions, see Installing Robots and Secondary Hubs in the *UIM Server Installation Guide.*
  - Converted from active mode to passive mode in Infrastructure Manager.
- They must run by a specified non-root user. This is accomplished by executing a callback to specify the user for marketplace probes. This can be done in Admin Console or Infrastructure Manager.

Robots

Robots manage the probes. A robot starts and stops its probes at the required times, and collects, queues, and forwards the monitoring data. A robot is installed on each computer you want to monitor.

Each robot has three dedicated tasks:

- **Control the probes** attached to the robot, which includes starting and stopping them at the required times (accomplished with the robot’s *controller* probe).
- **Collect, queue and forward** the probe messages (accomplished with the *spooler* probe).
- **Provide a simple database service** for its probes. This allows the robot to store data for threshold monitoring and data trending, and ensures collected data survives power outages (accomplished with the *hdb* probe).

The three probes mentioned here are service probes that are present on every CA Unified Infrastructure Management robot.

All robots are basically identical; it is the collections of probes they manage that distinguish them. Probes can be grouped together into packages so that you can appropriately deploy them to various types of servers.

If a robot contains a hub probe it is promoted to the next level in the domain hierarchy: the *hub*.

Hubs

A *hub* is a robot that has additional responsibilities. Just as a robot manages its probes, the hub manages its robots. Every CA Unified Infrastructure Management deployment has one or more hubs. All hubs perform these tasks:

- **Collect all messages** coming from the robots
- **Quickly dispatch the messages** to connected subscribers and/or queues
- **Maintain system information**, such as name-tables

Hubs have the following designations depending on their purpose:

- The **primary hub** communicates with the database. Every deployment has one, and only one, primary hub. This hub is created when you install the UIM Server software.
- **Secondary hubs** can be used to scan the network (device discovery), perform baseline calculations on QoS metrics, or group robots according to function, geographical location, departmental code, or other criteria. Although secondary hubs are optional, almost all deployments have them. Secondary hubs are created after UIM Server is installed. They can be created or removed as needed to meet the needs of your IT environment.
- A **failover hub** is a secondary hub that performs the primary hub's actions if the primary hub changes state (becomes unavailable).
- **Tunnel hubs** use VPN-like connections to communicate through firewalls.
- A **relay hub** is installed in a CA Unified Infrastructure Management ITMaaS deployment. It communicates with the CA Unified Infrastructure Management monitoring service in the cloud.

Domain

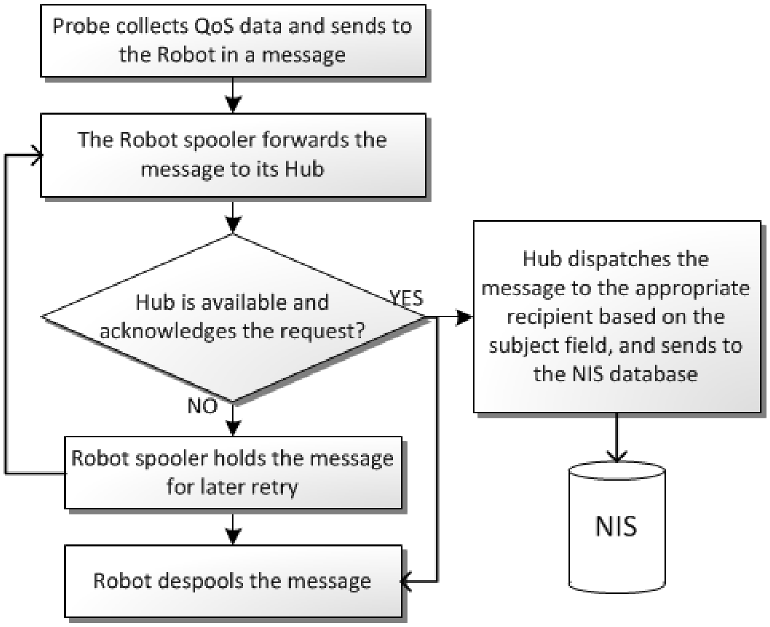
The *domain* is a logical set into which all of the CA Unified Infrastructure Management infrastructure components are grouped.

The domain is created when you install the CA Unified Infrastructure Management server software. A site is normally set up with one domain. Various security aspects, such as user profiles, permissions, and access rights are distributed within the domain.

Message Flow

Overview

The following diagram shows how data flows from a probe to the database.


Probe collects QoS data and sends to the Robot in a message
The Robot spooler forwards the message to its Hub
Hub is available and acknowledges the request?
YES
NO
Hub dispatches the message to the appropriate recipient based on the subject field, and sends to the NIS database
NIS
Robot spooler holds the message for later retry
Robot despools the message

The following sections explain the elements involved in data transfer.

Bus

The CA Unified Infrastructure Management message bus provides a set of services to the robots, hubs, database and management consoles. The message flow on the bus is managed using routing and naming schemes.

Message Model

The message flow is based on request/response and publish/subscribe models:

- **Request/response** is the standard way of communicating over the network. A client issues a request to a server and the server responds to the request.
- **Publish/subscribe** allows clients to send data—such as alerts, performance data, or messages targeted for gateway servers—without a designated receiver. It also allows clients to select messages based on subject.

Subscribe Mechanism

The subscribe mechanism enables probes and robots to select messages based on subject rather than on sender address. A client that is configured to receive CA Unified Infrastructure Management messages sends a subscribe request to the hub. The client then receives messages matching the subscribed subjects from the hub. A client may use the following methods when subscribing:

- **Subscribe**—client connects to the hub and gets messages as long as the client is running.
- **Attach**—the hub configures a message queue to hold the messages if the client is not running. When the client comes back up, all messages are passed on, including those that were received when the client was inactive.

Message Queues

Message queues transfer messages to and from the hubs. Queues fall into two categories:

- **Permanent** queues are stored in the local hub database and survive a hub restart. This type of queue ensures that messages are delivered even if the receiver is down when a message is generated.

  *Example:*Alarm Server probe (nas). If the hub that is running this service goes down and then comes back up, it fetches all alarms generated while it was down. This ensures no alarms are lost.

- **Temporary** queues are used for less-critical communication paths.

  Example: UMP alarm viewer portlet. When a user starts UMP, the portlet subscribes to alarm messages and a temporary queue is created. Messages are forwarded to this queue as long as the alarm viewer is active. When the viewer is closed, the queue is removed.

Queues are set up in two ways:

- **Automatically.** In most situations involving a single domain/subnet, queues are an automatic and transparent part of the infrastructure. Permanent queues are set up between hubs during installation. Temporary queues are created as needed.
- **Manually.** Using Admin Console or Infrastructure Manager, you can create additional queues between hubs according to need. The following queues can be deployed when adding secondary hubs:
    - Alarm. With multiple secondary hubs, you can set up a queue to send all alarms to a specific secondary hub.
    - QoS. With multiple secondary hubs, you can forward on QoS messages to the primary hub. Note that installing nas on a hub will create the necessary queue automatically.
    - Discovery. With multiple secondary hubs hosting discovery agents, the gathered device discovery data must reach the primary hub where the discovery server is hosted. You must set up probe_discovery queues on all hubs that exist along this communication path. For details, see the section "Configure probe_discovery Queues" in the *Discovery User Guide*, available in the Documentation Library.
    - Baselines. With one or more baseline_engine probes hosted on secondary hubs, you must set up qos_baseline queues to route baseline data to the primary hub. See the section "Recommended Multiple Hub (tiered) Probe Deployment" in the baseline_engine probe online help, available in the Documentation Library.

The Name Service

Each robot's controller maintains a list of:

- All probes controlled by the robot.
- All *active* probes (probes that listen to a bound port and respond to a command set). This list is distributed to the hub upon request. For example, Infrastructure Manager often requests this information.

The names found in these tables are the basis for the name-to-IP port resolution, and constitute what we define as a CA Unified Infrastructure Management address. A client may query the controller for a name/IP resolution in a similar manner as queried from DNS or WINS, based on the service name (for example, nas).

System Security

System security is ensured through:

- **Access**—Who has permission to do what?
- **Authentication**—Is the client who he/she/it claims to be?
- **Encryption**—Can we make it impossible for others to read the data?

Access Control Lists (ACLs)

A login is required to gain access to your CA Unified Infrastructure Management infrastructure and monitoring data. Access Control Lists (ACLs) allow you to further restrict user permissions. The CA Unified Infrastructure Management administrator can:

- **Attach user accounts** to one of five default ACLs: Superuser, Administrator, Operator, Dashboard Designer, and Guest. The pre-defined permissions for these ACLs (except Superuser) can be further restricted.
  - New users are created in **Infrastructure Manager** or **UMP**
  - ACLs are administered in the **Infrastructure Manager** > **Security** > **Manage Access Control List** dialog. For a listing of default ACL permissions, refer to the section on ACL Permissions Reference (see page 35).
- **Create new ACLs** with customized permissions
- **Configure the hub** to forward login requests to an LDAP server and to access the container with the user groups.

Session Identification (SID)

Session Identifications (SIDs) allow users and probes to execute commands. Any request must have a valid SID.

Each user is granted a SID upon login.

Console Security

Web-based console access can be secured with authentication using SSL certificates, and encrypted data transfer over HTTPS.

Admin Console

By default Admin Console connects with the UIM Server by HTTP. It can be configured to connect securely with HTTPS, using either a self signed- or certificate authority-signed SSL certificate. For details, see the section "Manage Security" in the online help for Admin Console, available from the Documentation Library.

UMP (Unified Management Portal)

For information on configuring UMP to communicate securely, see the *HTTPS Implementation Guide* for UMP, available from the Documentation Library.

Probe Security

Probes can be categorized as simple or complex:

- Most probes have simple tasks, such as monitoring performance and sending an alarm if a threshold is reached. These probes do not need a SID, because they only send messages.
- Other have more complex tasks, such as collecting information from, and executing commands on, other probes. These probes need permission to connect to and execute commands on remote probes. Because of this they are a potential security risk.

For a probe to obtain an SID, two conditions must be met:

1. The probe must be installed on a robot in order to generate a signed checksum. This requires administration rights and cannot be performed by intruders or operators.
2. The controller must start the probe. A magic number scheme ensures that this cannot be circumvented.

If these requirements are met, the robot’s controller connects to the hub to get the appropriate SID for the probe. This requires that the probe has been added to the security configuration with the appropriate permissions and IP mask.

Monitor Across Firewalls

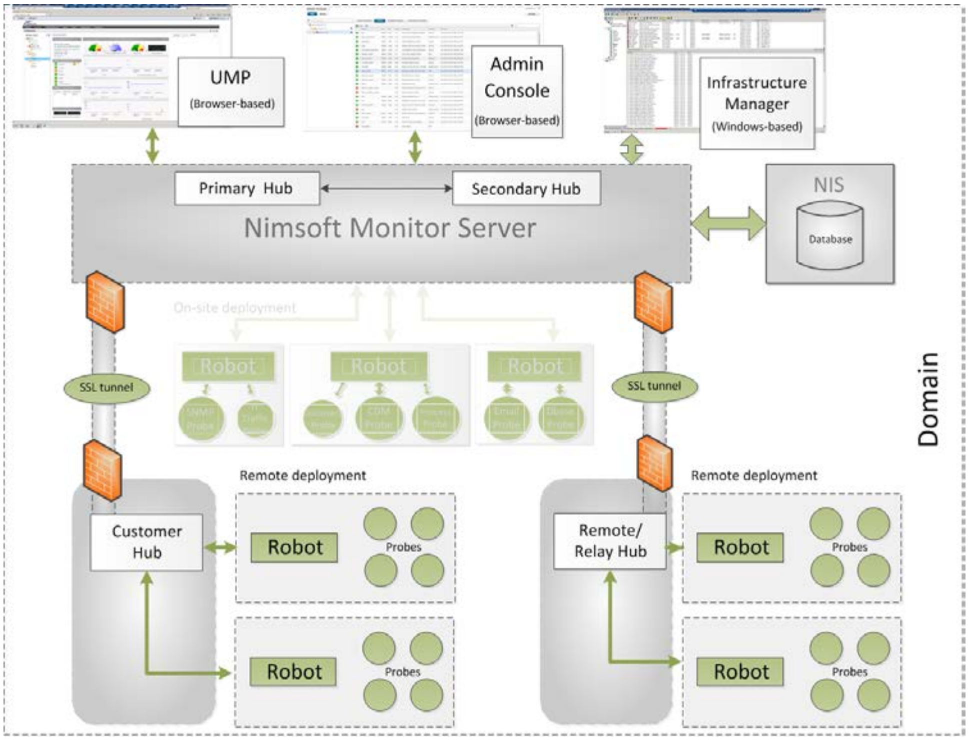
Most companies have one or more firewalls in their network, both internally between different networks and externally against the Internet or a network DMZ.

Because network administrators are often reluctant to open a firewall for the number of IP addresses and ports that management applications require, it can be difficult to administer and monitor the whole network from a central location.

The solution is to set up a secure shell (SSH) tunnel between two hubs that are separated by a firewall. The tunnel sets up a VPN (Virtual Private Network) connection between the two hubs. All requests and messages are routed over the tunnel and dispatched on the other side. This routing is transparent to users.

You can create tunnels between any CA Unified Infrastructure Management hubs:

- The DMZ wizard lets you easily set up tunnels between hubs during installation. For instructions, see the section on DMZ Installation in the *UIM Server Installation Guide*, available from the documentation library.
- In Admin Console or Infrastructure Manager,you can set up tunnels by configuring the hub probe. Access the online help from within the configuration GUIs for instructions.



Chapter 3: Admin Console

Admin Console provides most of the management capabilities required to manage your UIM components. Its browser-based GUI allows you to manage your UIM infrastructure on virtually any desktop or server operating system. Admin Console can also be run within a portlet in UMP.

UIM administrators and users with administrator or superuser permissions can access Admin Console.

Admin Console (accessible in a web browser, or "stand-alone" mode) is installed and available after UIM Server installation is complete. To access it, use the link given on the UIM Serverweb page (http://<*servername_or_server_IP_address*>:8080): **Management (Admin Console)**. The Admin Console portlet is installed during UMP installation.

By default Admin Console connects with the server by HTTP. It can be configured to connect securely with HTTPS, using either a self signed- or certificate authority-signed SSL certificate. Security features, as well as other topics, are described more fully in its online help, available in the Nimsoft Documentation Library.

This section contains the following topics:

The Admin Console Interface

The Admin Console has the following elements.

- **Main window** --provides a view of your infrastructure. The main window is divided into two sections.
  - The left navigation pane displays the hubs and robots in a tree structure.
  - The right pane displays either robot or probe information based on your selection in the navigation pane.
  - At the top of each section is a filter used to customize your view of the interface.

- The **Infrastructure** button in the upper left of the main window. Click this button to view and configure your infrastructure components.
  - Select a hub in the navigation pane and the right side of the screen displays the robot information and properties for that hub.
  - Select a robot in the navigation pane, and the right pane provides four options for accessing information about your robot: Robot Properties, Probes, Packages Installed, and Environment variables.
- The **Archive** button in the upper left of the main window. Click this button to view and use the probe package archive.
  - Deploy, import, group, and delete probe packages from this screen.
  - The *local archive* screen displays the probes that reside in the archive on the hub. The local archive contains all probes that were installed during UIM Server installation, and those that have been downloaded subsequently.
  - The *web archive* screen displays the list of probe packages on the UIM support archive.
  - The *distribution activity* screen displays a log of probe package distributions, along with the status of each distribution.

Chapter 4: Infrastructure Manager

Infrastructure Manager is the primary interface for configuration and management of your UIM components. It provides:

- A hierarchical view of systems being monitored
- An alarm window to view all alarms and messages
- Interfaces that allow you to configure your hubs, robots, and probes.

Infrastructure Manager connects to an active hub and allows you to control, configure, and manage all robots and probes connected to that hub.

For more information, see the *Infrastructure Manager* Guide,available in the documentation library (../../InfrastructureManager/index.htm).

The Infrastructure Manager Interface

The Infrastructure Manager window has the following elements.

- **Main menu** and **toolbar**. Pull-down menus and quick access buttons allow you to customize your view of the interface, locate infrastructure elements, and manage user accounts.
- **Console pane** (left). This pane provides a hierarchical view of your infrastructure and uses color-coded icons to indicate element status. This pane contains the following nodes:
  - **Domains** shows your hub-robot-probe structure
  - **Dynamic Views** groups robots by operating system
  - **Groups** displays user-created groups of hubs, robots or probes
  - **Archive** lets you access probe packages and licenses stored in the current hub’s archive
  - **URLs** and **Applications** let you launch web pages or other applications
- **Main window pane** (upper right). This pane displays details about the element selected in the console pane. For example, if you click a hub in the console pane, all of the hub's robots are displayed in the main window pane.

  This pane also has its own dynamic toolbar, which provides quick access to functions related to the displayed elements.

- **Doc Pane** (lower right). This pane appears if the **View > Dock Pane** menu option is checked. It can display:
  - Alarms
  - System messages
  - The contents of the main window pane
  - Previously docked windows

Chapter 5: Unified Management Portal

The Unified Management Portal (UMP) is a web-based interface that lets you:

- Scan your network (discovery) or import device data from an external source, such as a CMDB
- Monitor and manage computer systems
- Graph QoS data
- View and manage alarms
- Create SLAs and view SLA performance reports
- Create, view, and schedule reports
- Create and view custom dashboards
- Open and manage Service Desk tickets
- Manage users

Note: Documentation for UMP is available from its online help (../../../UMP/Most_Current_Version/index.htm).

This section contains the following topics:

UMP Portlets

The following lists many of the applications, or portlets, are available within UMP. For more information on each of these, refer to the UMP user documentation (../../../UMP/Most_Current_Version/index.htm).

- **Account Admin** lets you create, modify, or delete users. You can also set passwords for users.
- **Alarm Console** allows full viewing, filtering, and managing of alarms.
- **Cloud User Experience Monitor** lets you monitor web sites and cloud services from around the globe and measures the status of your transactions and services from more than 60 locations.

- **Custom Dashboards** let you:
  - Access your custom dashboards, which display QoS data and alarms from monitored systems on your network
  - View your alarms
  - See the Dynamic Views, which display the state (alarm level, performance, etc.) of the monitored systems on your network
- **Dashboard Designer** lets you design custom dashboards.
- **Discovery Status** displays a pie chart showing the discovery status of systems on your network. Discovery continuously searches your network for computer systems and updates the diagram to show the current status. Click the chart to displays an additional system information.
- **Dynamic Views** displays automatically generated QoS dashboards for the systems discovered on your network. In the portlet's tree pane, you can select a system to see additional information.
- **List Viewer** displays data (text, numbers, gauges, alarms, or graphs) in a table format.
- **List Designer** lets you design lists to be displayed in the List Viewer portlet.
- **Maintenance Mode** lets you temporarily stop monitoring for selected systems . The monitoring settings are retained so that monitoring resumes when maintenance mode ends.
- **Remote Admin** is a management console for discovery and configuration data. It allows you to specify monitoring properties for the systems discovered on the network.
- **QoS Chart** provides a visual representation of QoS data. You select the host, QoS measurement, target, and time range, and the data is displayed as a graph. You also can display multiple measurements in a single graph, view multiple graphs at once, and save a set of graphs as a report.
- **Relationship Viewer** displays the relationships among devices on your network in intuitive, visual diagrams. It also performs root cause analysis (RCA) to determine the device causing an outage and suppresses alarms from dependent nodes.
- **Reports** displays:
  - Quality of Service (QoS) reports, which must be manually created using the report_engine probe GUI. This GUI is launched by double-clicking the report_engine probe in Infrastructure Manager. See the online probe documentation for details on the report_engine.
  - Service Level Agreement (SLA) reports, which are automatically created for SLAs built in the Service Level Manager.

- **Unified Reports** gives you a comprehensive set of Business Intelligence (BI) tools that provide static and interactive reporting and data analysis capabilities. The Unified Reports support drag-and-drop dashboarding, built-in charting, web reporting, and report scheduling, distribution and historical versioning.
- **Unified Service Monitoring (USM)** provides the Discovery Wizard for automating device entry, and end-user views of monitored systems, organized according to user account.
- **Web Content** lets you to link to a web page.

Dashboard Designer

Dashboard Designer lets you create custom dashboards using a variety of template widgets, such as alarm objects, meter objects, charts, and tables. In this portlet you can:

- Filter alarm objects to reflect the state of specific systems
- Connect meter objects different data sources, such as QoS, probes, or variables
- Use panels to build dashboards with several levels in a tree structure
- Use table objects to present the output from a database query as a table in a dashboard
- Configure the dashboard layout and background with a wide range of colors, fonts sounds and data sources

Four dashboard templates are available: two for network devices and two for server systems. You can use these templates as-is or customized them as needed. A preview tool lets you see the appearance and layout of the dashboard before publishing it.

Dashboards that you save and publish are available on the Custom Dashboards tab.

Custom Dashboards

The Custom Dashboards portlet displays the dashboards you create. Which dashboards you see depends on the permissions set in the ACL for your user account. In this portlet:

- The color of the icons in the tree structure represents the highest alarm severity for alarm objects on the dashboards. Double-click an icon and the corresponding dashboard is launched in the dashboard pane.
- The dashboards can contain meters, alarm objects, gauges, charts, tables, panels, and so on.
- Alarm and panel objects reflect the severity level of the alarm with the highest severity. Double-clicking an alarm object brings up the alarm list, enabling you to manage the alarms.
- The Mini Map tool zooms in on an area of a dashboard. A minimized version of the dashboard is shown in the Mini Map window. A slider lets you zoom in or out of the dashboard on the canvas.

Chapter 6: Alarms

Alarm monitoring probes check host computers for symptoms of error situations. This may be checking free disk space, log file contents, performance problems or stopped system processes. When a problem is found, the robot sends a message describing the problem to the hub.

CA UIM delivers several standard probes that are designed to monitor a wide range of operating systems and applications. CA works closely with the vendors of such systems to provide focused monitoring for the everyday problems that affect their users and support staff.

NOTE: This section describes features available to a user with maximum privileges. Some menu options and buttons may be unavailable (grayed out) depending on user privileges. The alarms a user can see, and the actions he or she can perform, are defined in an ACL.

This section contains the following topics:

Alarm Window

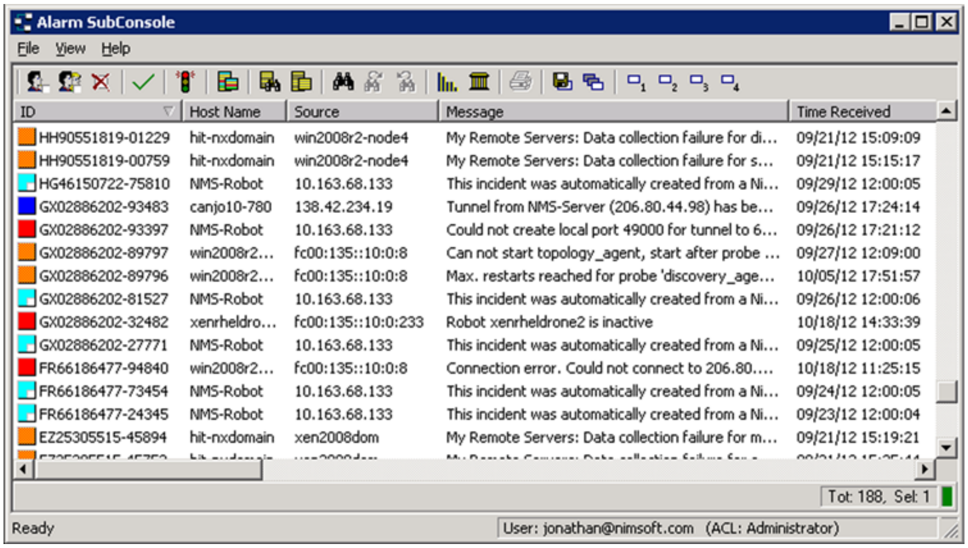
The alarm console, which is a component of Infrastructure Manager and UMP, allows users to view and operate on the alarms. The console is fully event driven and updates automatically. In this console, you can:

- Define complex filters to quickly get to specific subsets of alarms
- Perform a set of management operations based on your user privileges (create and attach notes, manage actions and filters, or set alarms to visible/invisible states)
- Accept and acknowledge alarms
- View transaction history and query functionality against historical data

The console displays information about alarms in a table format. Toolbar icons and menu options let you view information and take action on alarms.

This window is accessible in several forms:

- In UMP as the *Alarms Console* portlet
- In the lower-right pane of Infrastructure Manager
- As the *Alarm SubConsole*, a stand-alone application launched from Infrastructure Manager (shown here)



ID	Host Name	Source	Message	Time Received
🟧 HH90551819-01229	hit-nxdomain	win2008r2-node4	My Remote Servers: Data collection failure for di...	09/21/12 15:09:09
🟧 HH90551819-00759	hit-nxdomain	win2008r2-node4	My Remote Servers: Data collection failure for s...	09/21/12 15:15:17
▣ HG46150722-75810	NMS-Robot	10.163.68.133	This incident was automatically created from a Ni...	09/29/12 12:00:05
🟦 GX02886202-93483	canjo10-780	138.42.234.19	Tunnel from NMS-Server (206.80.44.98) has be...	09/26/12 17:24:14
🟥 GX02886202-93397	NMS-Robot	10.163.68.133	Could not create local port 49000 for tunnel to 6...	09/26/12 17:21:12
🟧 GX02886202-89797	win2008r2...	fc00:135::10:0:8	Can not start topology_agent, start after probe ...	09/27/12 12:09:00
🟧 GX02886202-89796	win2008r2...	fc00:135::10:0:8	Max. restarts reached for probe 'discovery_age...	10/05/12 17:51:57
▣ GX02886202-81527	NMS-Robot	10.163.68.133	This incident was automatically created from a Ni...	09/26/12 12:00:06
🟥 GX02886202-32482	xenrheldro...	fc00:135::10:0:233	Robot xenrheldrone2 is inactive	10/18/12 14:33:39
▣ GX02886202-27771	NMS-Robot	10.163.68.133	This incident was automatically created from a Ni...	09/25/12 12:00:05
🟥 FR66186477-94840	win2008r2...	fc00:135::10:0:8	Connection error. Could not connect to 206.80....	10/18/12 11:25:15
▣ FR66186477-73454	NMS-Robot	10.163.68.133	This incident was automatically created from a Ni...	09/24/12 12:00:05
▣ FR66186477-24345	NMS-Robot	10.163.68.133	This incident was automatically created from a Ni...	09/23/12 12:00:04
🟧 EZ25305515-45894	hit-nxdomain	xen2008dom	My Remote Servers: Data collection failure for m...	09/21/12 15:19:21

Tot: 188, Sel: 1

Ready

User: jonathan@nimsoft.com (ACL: Administrator)

For more information see the *Alarm Console User Guide*, available from the **Downloads** tab at support.nimsoft.com.

Alarm Sever Probe (nas)

The Alarm Server (nas) is a service probe that receives alarm messages distributed by the hub. It functions in this way:

1. An alarm message is generated by a probe somewhere in the UIM infrastructure. This "broadcast-type" message does not have specified receiver and can be retrieved by any processes subscribing to the alarm subject.
2. The nas, which subscribes to the alarm subject, acts upon the incoming message by storing information about the alarm in a database in the nas subdirectory.
3. When the data is requested (such as when a user views alarms in UMP or Infrastructure Manager), the Alarm Server sends the stored data.

This probe also:

- Supports message suppression
- Supports alarm enrichment, where alarm messages can be altered based on defined rules
- Provides clients updated events and repository services (get, list, close etc.)
- Supports message filtering
- Supports automatic actions (auto-operator)
- Provides mirroring capabilities
- Handles alarm messages

Handling Alarms

Alarms can be handled in several ways. You can:

- Work with them in the alarm console
- Install a gateway to forward the alarms to other messaging infrastructures (e-mail, GSM/SMS, pager or SNMP messages)
- Integrate them more tightly to a systems management framework using one of the available framework integration kits
- Handle them automatically by setting up profiles in the nas probe’s *Auto Operator*

All methods ensure that operators are automatically informed about problems a few seconds or minutes after the symptom appear.

Message Suppression

Many error situations in the monitored system can result in a huge number of alarms. For example, if the logmon probe monitors a logfile for an application that enters an infinite loop and logs errors within the loop, a huge number of identical alarms can be generated. This creates an unnecessary load on the system, network and primary hub.

The message suppression mechanism lets you avoid this problem. The suppression models supported by the nas are:

- **Standard** suppression, a simple model that suppresses messages with an exact match on message subsystem id, severity level and message text.
- **Key** suppression, a model based on a suppression key that follows a message. When the key suppression is enabled, messages with matching suppression key are suppressed.

Automated Acknowledge

You can use key suppression to automatically clean up in the alarm list when the probe detects that the critical situation is resolved. This is done by enabling automatic acknowledge based on key. This means that alarms with the clear severity level automatically acknowledge any previous alarms with the same suppression key.

For example, a reasonable configuration of the disk-monitoring probe would be to send the first alarm (95% full) with severity level serious, while the last one (55% full) could have severity level clear. If the last alarm arrives, everything is back to normal and the administrator does not have to respond to the first alarm after all. The alarm is automatically acknowledged by the nas, leaving the administrator’s "to-do" list with as little "noise" as possible.

Subsystem IDs (SIDs)

In the Alarm console, alerts are classified by their subsystem ID, identifying which part of the system the alert relates to. This is a hierarchical list of codes, allowing you to group alarms as widely or narrowly as desired.

This list is stored in the nas. If you develop or customize probes, you can define your own list of subsystems. This list also maps the subsystem code into a text string for improved readability.

Alarm Transaction Log Files

It is useful to follow the complete message life from the initial message , through multiple suppressions, to message closure (acknowledgement). A filtering mechanism (tunable by the administrator) enables the nas to log all transactions to a specific transaction logfile.

To keep the transaction logfile as manageable as possible, it is automatically copied at configured intervals. The saved logs are named trans_*timestamp*.log, where *timestamp* is the time the file was created (in seconds).

Use the nas configuration tool to view the transaction log or tune the settings.

Notification Messages

The following types of messages are generated:

- **alarm_new**: an alarm message is received and message footprint was not previously recorded
- **alarm_update**: an alarm message is received and the message footprint already exists
- **alarm_close**: client closed (acknowledged) an alarm and it was removed from the currently active alarms

All transactions are logged to the transaction log file.

Appendix A: ACL Permissions Reference

UIM Server includes five pre-defined Access Control List templates, with these permissions:

Permissions	**Administrator (super)**	**Dashboard Designer (admin)**	**Guest (open)**	**Operator (write)**	**Superuser (super)**	**Description**
Accept	Y	Y	-	Y	Y	Assign alarms to yourself
Unassign	Y	Y	-	-	Y	Unassign alarms
Dynamic Views States	Y	-	-	Y	Y	General access to Dynamic Views alarm state information
Invisible Alarms	-	Y	-	-	Y	Show alarms that are set to be invisible
Reassign	Y	Y	-	-	Y	Override assignment at Assign/Acknowledge
Alarm History	Y	Y	-	Y	Y	Transaction history and alarm queries
Acknowledge	Y	Y	-	Y	Y	Close alarms
Alarm Management	Y	Y	-	-	Y	Various alarm management features
Assign	Y	Y	-	-	Y	Assign alarms to another user
Alarm Details	Y	Y	Y	Y	Y	General access to alarm lists and alarm details
Automation - View Items	Y	Y	Y	Y	Y	Unimplemented
Automation - Change configuration items	Y	Y	-	Y	Y	Unimplemented
Automation - Manage Workflows	-	-	-	-	Y	Unimplemented
Automation - Create and Modify Workflows	-	-	-	-	Y	Unimplemented
Dashboard Design	-	Y	-	-	Y	Create, modify, and delete dashboards

Permissions	**Administrator**	**Dashboard Designer**	**Guest**	**Operator**	**Superuser**	**Description**
Discovery	-	Y	-	-	Y	Discover and create template panels
Dynamic Views	Y	Y	-	Y	Y	Display Dynamic Views
Web Publish	-	Y	-	-	Y	UIM Server HTML management
Dashboard Upload	-	Y	-	-	Y	Upload dashboards to archive
Dashboard Download		Y	-	-	Y	Download dashboards from archive
Archive Management	Y	-	-	-	Y	Create and modify packages
Extended Security	Y	-	-	-	Y	Various security maintenance features
Maintenance Mode	Y	-	-	-	Y	Robot maintenance mode management
Manage ACL	Y	-	-	-	Y	Create, modify, and delete ACLs
License Management	**Y**	**-**	**-**	**-**	**Y**	**Add and delete licenses**
User Administration	Y	-	-	-	Y	Create, modify, and delete users
Portal Administration	Y	-	-	-	Y	Web portal admin access
Modify Profiles	Y	-	-	-	Y	Modify and save user profiles
Distribution	Y	-	-	-	Y	Distribute archive packages
Program Options	Y	Y	-	-	Y	Change various program attributes
Basic Management	Y	-	-	-	Y	Restart, move, download, drop, etc.

Permissions	Administrator	Dashboard Designer	Guest	Operator	Superuser	Description
Manage Profiles	Y	-	-	-	Y	Create, rename, and delete user profiles
Management Tools	Y	-	-	-	Y	Various tools (find/connect, etc.)
Archive Management	Y	-	-	-	Y	Create and modify packages
Probe Configuration	Y	-	-	-	Y	Probe configuration tool management
Execution Level1	Y	-	-	-	Y	Probe Command Execution Level 1
Execution Level2	Y	-	-	-	Y	Probe Command Execution Level 2
Execution Level3	Y	-	-	-	Y	Probe Command Execution Level 3
Alarm Summary	Y	Y	Y	Y	Y	Display alarm summary information
Custom Reports	Y	Y	Y	Y	Y	Display customer reports
Dashboard Publish	-	Y	-	-	Y	Make published dashboards generally available
Dynamic Views Reports	Y	Y	Y	Y	Y	Display Dynamic Views Reports
Unified Reports	Y	Y	-	-	Y	Access to Unified Reports
Discovery Pie	-	Y	-	-	Y	Display discovery information
Custom Dashboards	Y	Y	Y	Y	Y	Display custom dashboards
Discovery Management	-	Y	-	-	Y	Set computer system properties
Account Administration	Y	-	-	-	Y	Manage Account contacts and customize their portal content

Permissions	Administrator	Dashboard Designer	Guest	Operator	Superuser	Description
User Monitoring	Y	-	-	-	Y	Display and disconnect user sessions
Report Designer	Y	Y	-	-	Y	Create, modify, and delete reports
Dynamic Views Dashboards	Y	Y	-	Y	Y	Display Dynamic Views dashboards
Dashboard Designer	Y	Y	-	-	Y	Create, modify, and delete private dashboards
Default Customization	Y	-	-	-	Y	Customize default portal content for UIM users
User Customization	Y	Y	Y	Y	Y	Customize own portal content
Change Password	Y	Y	-	Y	Y	Contact can change own password
SLM Admin	Y	-	-	-	Y	Run Service Level Manager with full access
SLO Access	Y	Y	-	Y	Y	Allow portlet users to browse SLO data
QoS Access	Y	Y	-	Y	Y	Allow portlet users to browse QoS series
SLM View	Y	Y	-	Y	Y	Run Service Level Manager in read-only mode
Service Desk	Y	Y	-	Y	Y	Access to Service Desk and My Tickets portlets
USM Edit Monitoring Templates	Y	-	-	-	Y	Create, edit, and delete monitoring templates
USM Group Modification	Y	-	-	-	Y	Create, edit, and delete groups

Permissions	Administrator	Dashboard Designer	Guest	Operator	Superuser	Description
USM Self Service Monitoring	Y	-	-	-	Y	Enable or disable out-of-box monitoring templates
USM Basic	Y	Y	-	Y	Y	Access to USM portlet
USM Automatic Robot Installation	Y	-	-	-	Y	Automatically deploy and install robots to targeted system
USM Modify Individual Monitors for Computer Systems	Y	-	-	-	Y	Create, modify, and delete individual SOC monitors
List Viewer	Y	Y	-	Y	Y	View lists and groups
List Designer	Y	Y	-	-	Y	Create, modify, and delete lists and groups
Report Scheduler	Y	Y	-	Y	Y	Access to ReportScheduler portlet
NetFlow	Y	Y	-	-	Y	Access to NetFlow portlet
NetFlow Configuration	Y	-	-	-	Y	Allow portlet users to configure NetFlow probe settings
Web service	-	-	-	-	Y	Access to UIM Web Service API
Cloud UE Monitor	Y	Y	-	Y	Y	Access to Cloud User Experience Monitor portlet

Glossary

Acknowledge

All new alarm messages received by the Alarm Server (nas) are initially marked un-acknowledged and presented to an operator. When the operator has verified and addressed the problem, the operator can acknowledge the message, indicating that the problem is under control. The message is then deleted from the alarm server database. A copy is kept in the history database.

Alarm levels

The supported alarm levels are: clear (0), information (1), warning (2), minor (3), major (4), and critical (5).

Alarm message

An alarm is a general message with its subject set to alarm. The message is normally generated by a probe responding to a threshold breach, and published as a "raw" alarm message.

Calculation method

A calculation method is the set of rules and conditions that determine how SLA compliance is calculated.

Calculation profile

Calculation profiles are created by users to define the calculation properties for Service Level Objects and Quality of Service Constraints. These profiles are based on built-in plug-ins distributed with the Service Level Manager application. The profiles are grouped either as SLO calculations as QoS calculations, depending on whether the selected plug-in supports single-data or multi-data series.

Compliance percentage

The compliance percentage is defined to be the percentage of time that the QoS, constrained by factors such as operating period and thresholds, should be considered compliant within the compliance period.

Compliance period

The compliance period defines the period of time that an SLA should meet the requirements stated by the compliance percentage, typically a day, a week or a month.

Daemon probe

A daemon probe is always active. If it stops, the robot immediately attempts to restart it.

Data types

The data types used to calculate compliance are Automatic (Interval), in which QoS data is recorded at intervals, or Asynchronous, in which QoS data is only recorded each time the measured value changes.

Domain

A *domain* is a logical set into which all infrastructure components are grouped. A deployment typically has one domain. MSPs or very large deployments might use different domains for each company or enterprise.

History

When an alarm message is acknowledged, it is deleted from the NAS database but kept in a history database. The contents of this database can be viewed in the alarm window.

Hub

A hub is a service in the UIM infrastructure that manages a group of robots, collects and redistributes messages published by the probes, maintains several central services, and manages messages.

Infrastructure

Infrastructure refers to the UIM domain, hubs, robots and probes.

Infrastructure Manager

Infrastructure Manager is a Windows-based UIM configuration and management interface. It provides a hierarchical view of systems being monitored, an alarm window to view all alarms and messages, and configuration interfaces.

UIM address

A UIM address consists of four basic elements (the domain, hub, robot, and probe), each separated by a forward slash. The UIM API has functions that resolve a UIJ address to an IP-address and a port.erating period

The operating period constrains the QoS samples to one or more time-specifications within the compliance period. This means that samples falling outside these time specifications will not influence the SLO/SLA compliance requirements. Each operating period is defined as a union of one or more time-specifications.

Probe

A *probe* is small piece of software that performs a dedicated task. **Monitoring probes** gather availability and performance data. **Service probes** (also called utility probes) provide product utility functions to the infrastructure. Probes can be easily configured for your own specific monitoring requirements.

Published message

A message is published when it is sent to the nearest hub without being directed to a particular receiver. The message can then be delivered to all clients subscribed to the Subject ID found in the message.

Quality of Service (QoS)

The QoS is the actual value collected by a probe and used centrally to determine the state of the service level objective. If the probe is configured to deliver Quality of Service, then a QoS message is issued. This value is used for alarms.

Quality of Service (QoS) messages

Quality of Service messages provide trending data periodically. They normally contain data (such as response times and availability) used for Service Level monitoring and reporting.

Robot

The robot is the first line of management for the probes. The robot starts and stops the probes at the required times, and collects, queues and forwards messages from the probes to the hub.

Service Level Agreement (SLA)

A Service Level Agreement (SLA) is an agreement to deliver a service within a specified/fixed time-period. Both parties (such as an IT department delivering services to another department, or a company and an external service provider) agree on measurable service levels.

Subject ID (SID)

A Subject ID is a text string that classifies messages and makes it possible for clients to subscribe to some messages and ignore others. All messages with the same subject should also have identical data structure.

Subscribe

A client (such as a probe or gateway) can subscribe to messages based on the subject ID. This allows it to receive all similar messages (such as alarms).

Subsystem ID

The subsystem ID is a field in all alarm messages containing one or more numbers separated by periods, for example 2.31.4. The subsystem ID corresponds to modules within the monitored system, such as security or disk systems. The Alarm Console groups the incoming alarms according to subsystem, allowing you to quickly view all alarms for a particular area.

Suppression

Suppression treats multiple identical alarms as one message. Alarm probes sometimes generate a number of identical alarms. Enabling suppression reduces the number of unnecessary messages presented to the operator.

Timed probe

A timed probe runs once and then terminates, awaiting the next point in time when it is configured to start.