CA Nimsoft Monitor

Getting Started Guide

6.50

Document Revision History

Version	Date	Changes
1.0	6/30/2010	Initial version *Nimsoft Server Getting Started Guide*
2.0	10/24/2011	Simplified and revised
3.0	6/29/2012	Revisions for NMS version 6.00
6.10	9/10/2012	Minor revisions and documentation fixes for Nimsoft Monitor version 6.10
6.20	12/14/2012	Revisions and documentation fixes for Nimsoft Monitor version 6.20
6.50	3/31/2013	Revisions for CA Nimsoft Monitor version 6.50

Contact Nimsoft

For your convenience, Nimsoft provides a single site where you can access information about Nimsoft products.

At http://support.nimsoft.com/, you can access the following:

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

Provide Feedback

If you have comments or questions about Nimsoft product documentation, you can send a message to support@nimsoft.com.

Legal Notices

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks

Nimsoft is a trademark of CA.

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

For information on licensed and public domain software, see the *Nimsoft Monitor Third-Party Licenses and Terms of Use* document at: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Contents

Chapter 1: Introduction

Solution Overview

CA Nimsoft Monitor 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 rapidly add new IT monitoring capabilities as your infrastructure evolves.

Capabilities

Nimsoft Monitor is available either on-demand or on-premise. Both use models provide many monitoring capabilities. For example, Nimsoft Monitor can:

- 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
- Provide real-time dashboards and notifications on outages
- Seamlessly integrate with CA Nimsoft Service Desk

Benefits

Nimsoft Monitor's robust infrastructure and easy-to-use management tools provide many benefits to users. With this solution, you can:

- Configure your monitoring infrastructure and view the data from anywhere in your network
- Drill down into device metrics and performance reports
- Manage network areas that are segmented by highly restrictive firewalls
- Compartmentalize or restrict operator actions and views of the network
- Maintain device inventory for asset management
- Develop reports on network trends and analyze network data

Components

Nimsoft Monitor consists of:

- **Nimsoft Monitor Server**, which includes the distributed software that monitors your IT environment and controls the data, and the database that stores the data
- **Infrastructure Manager**, the primary interface for configuration and management of your Nimsoft system
- **Unified Management Portal** (UMP), a web-based portal that lets you view your data, alarms and messages in a variety of ways

About This Guide

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

This guide focuses on four areas of Nimsoft Monitor:

- Nimsoft Monitor Server (see page 9) provides an introduction to Nimsoft monitoring. It describes the infrastructure components, the message flow, and system security.
- Unified Management Portal (see page 19) 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.
- Infrastructure Manager (see page 23) gives an overview of Nimsoft's primary interface for configuration and management of your Nimsoft system.
- Nimsoft Alarms provides an introduction to how alarms are created and handled.

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

- *Nimsoft Monitor Server Installation Guide*
- *Nimsoft Monitor Server Configuration Guide*
- *Nimsoft Monitor Server Infrastructure Manager Guide*
- *NMS Release Notes and Upgrade Guide*

Chapter 2: Nimsoft Monitor Server

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

This section contains the following topics:

Supported Systems

NMS 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 Nimsoft Compatibility Support Matrix.

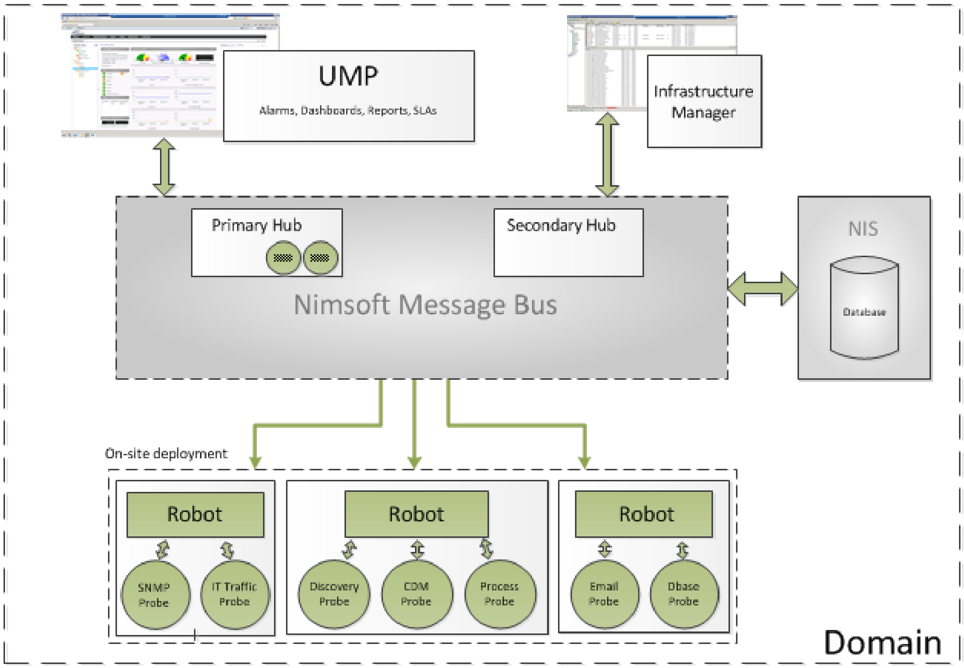
System Architecture

The Nimsoft Monitor system architecture consists of the infrastructure, which is the distributed software that monitors your IT environment and controls the data, and the Nimsoft Information Store (NIS), 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 illustration below shows a Nimsoft 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. The following sections describe the components from the bottom up to show how they work together.

Probes

A *probe* is small piece of software that performs a dedicated task. At the bottom of the hierarchy, they can be thought of as connectors and workers within NMS. Nimsoft has two types of probes:

- **Monitoring probes,** which 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 utility probes) provide product utility functions to NMS.

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.

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

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 Nimsoft 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 Nimsoft 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 Nimsoft 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 NMS server software.
- **Secondary hubs** can be used to 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 the NMS server software 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 is unavailable.
- **Tunnel hubs** use VPN-like connections to communicate through firewalls.
- A **relay hub** is installed in a Nimsoft ITMaaS deployment. It communicates with the Nimsoft service.

Domain

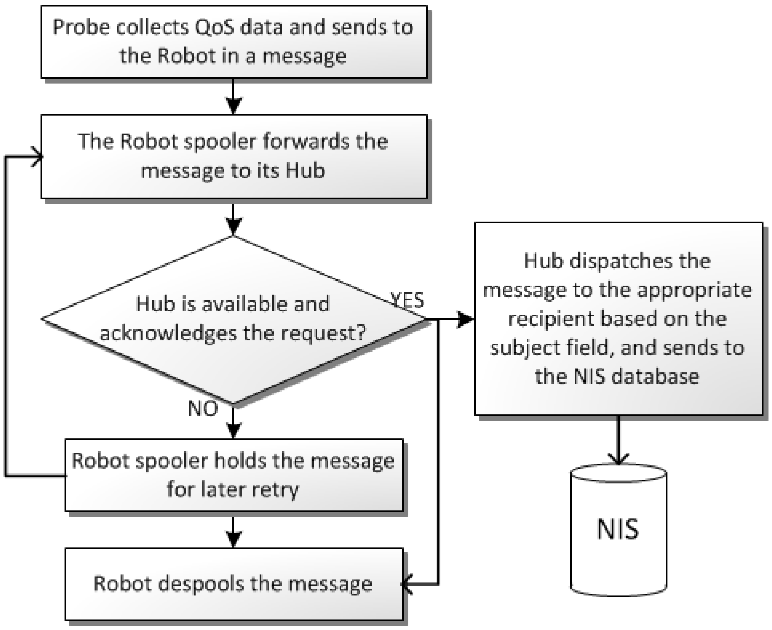
The *domain* is a logical set into which all of the Nimsoft infrastructure components are grouped.

The domain is created when you install the NMS 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 Nimsoft 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 Nimsoft 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: Nimsoft Alarm Server probe (nas). If the hub 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, queues are a transparent part of the infrastructure. Permanent queues are set up between hubs during installation. Temporary queues are created as needed.
- **Manually.** You can create queues with Infrastructure Manager, the primary interface for configuring and managing your Nimsoft system. For example, if you have multiple secondary hubs, you might set up a queue to send all alarms to a specific secondary hub.

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 Nimsoft 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).

Security Model

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 Nimsoft infrastructure and monitoring data. Access Control Lists (ACLs) allow you to further restrict user permissions. The Nimsoft 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.
- **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.

New users are created in Infrastructure Manager or UMP. ACLs are administered in Infrastructure Manager.

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.

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 a 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.

Monitoring 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.

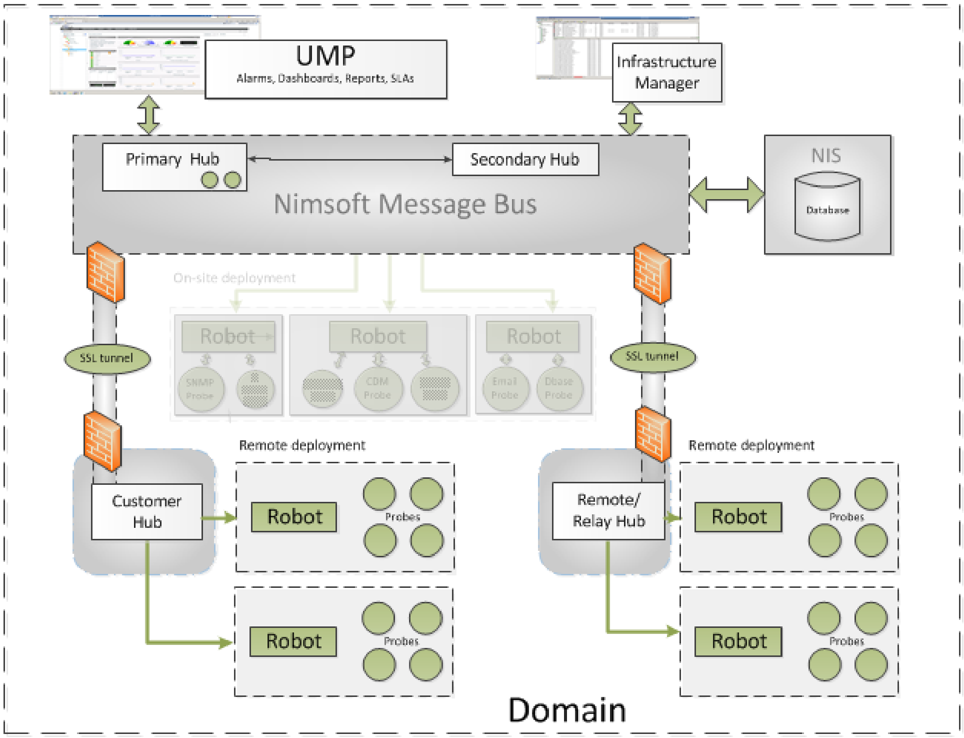
Because network administrators are often reluctant to open a firewall for the number of IP addresses and ports that management applications require, it can be difficult to administer and monitor the whole network from a central location.

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 Nimsoft hubs.

The DMZ wizard lets you easily set up tunnels between hubs. For instructions:

- See the *Nimsoft Monitor Server Installation Guide* available from the **Downloads** tab at support.nimsoft.com
- In Infrastructure Manager, double-click the hub probe to access the online help



Chapter 3: Unified Management Portal

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

- 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 Portlets

The following lists many of the applications, or portlets, are available within UMP:

- **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 a 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.
- **Nimsoft 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 Nimsoft 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 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 4: Infrastructure Manager

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:
  - Nimsoft alarms
  - System messages
  - The contents of the main window pane
  - Previously docked windows

For more information, see the *Infrastructure Manager* Guide, available from the **Downloads** tab at support.nimsoft.com.

Chapter 5: Nimsoft 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.

Nimsoft delivers several standard probes that are designed to monitor a wide range of operating systems and applications. Nimsoft 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

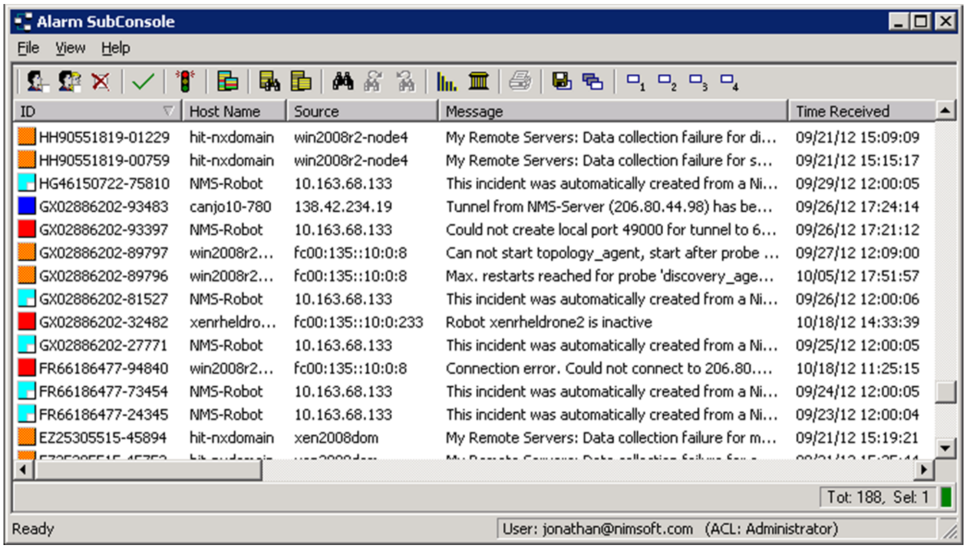
The alarm console, which is a component of Infrastructure Manager and UMP, allows users to view and operate on the alarms. The console is fully event driven and updates automatically. In this console, you can:

- 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. Here's how it works:

1. An alarm message is generated by a probe somewhere in the Nimsoft 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
- 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

Custom Probes

Nimsoft'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, Nimsoft allows you to develop your own solutions that are targeted directly at the problems causing the most trouble. The Nimsoft Software Development Kit (SDK) lets you develop probes and utilities that integrate with your Nimsoft environment. The SDK is available for the following programming languages:

- Perl
- C
- Java
- Visual Basic

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 NMS server.

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.

Glossary

acknowledge

All new alarm messages received by the Nimsoft 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 Nimsoft 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 Nimsoft 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 Nimsoft domain, hubs, robots and probes.

Infrastructure Manager

Infrastructure Manager is the primary interface for configuration and management of your Nimsoft system. It provides a hierarchical view of systems being monitored, an alarm window to view all alarms and messages, and configuration interfaces.

Nimsoft address

A Nimsoft address consists of four basic elements, the domain, hub, robot, and probe, each separated by a forward slash. For example in /Nimsoft/oslo/wscase/nas. The Nimsoft API has functions that resolve a Nimsoft address to an IP-address and a port.

operating 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 Nimsoft 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 Nimsoft 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. Nimsoft 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.