

Managing Your Infrastructure

Overview

The *My Infrastructure* panel is your starting point for monitoring the systems in your environment. From the *My Infrastructure* panel, you can add:

- systems or network devices
- Applications, which provide the overall status for one or more services
- service level agreements, which measure compliance to infrastructure performance goals
- groups, which are sets of systems or devices that have been combined in a meaningful way
- views, which enable non-administrative users to view only the systems in which they are interested

Working with Systems

Systems are the network devices that you will monitor using *up.time*. You can add the following types of systems:

- Agent

A system that has an *up.time* agent installed on it. In the *Global Scan* and *My Infrastructure* panels, agent systems are denoted by this icon:

- Net-SNMP v2 or Net-SNMP v3

These are servers that use version 2 or 3 of the Net-SNMP protocol to monitor and manage systems in a TCP/IP-based network. Net-SNMP version 3 adds security features that are lacking in Net-SNMP version 2.

All of the data gathered from Net-SNMP is based on the following MIB implementations:

- RFC 1213 (Management Information Base for Network Management of TCP/IP-based internets)

Presents network interface information.

- UCD-SNMP-MIB

Presents general system state information.

- Host Resources MIB (RFC 2790)

Presents system performance data.

Note - For information on Net-SNMP, see [Understanding the up.time DataStore](#).

- Network Device

A device without an agent, but with which *up.time* can communicate using an IP address.

- Novell NRM

A system that is running version 6.5 of Novell Remote Manager (NRM), a Web-based interface to newer Novell NetWare servers. Novell NRM saves server statistics in an XML file. *up.time* can retrieve the XML file, parse it, and then store the information in the DataStore.

- pSeries LPAR Server (VIO)

A pSeries server that is hosting multiple logical partitions (LPARs). The VIO (virtual input/output) handles the physical I/O requests from the LPARs that are on the server. In this configuration, *up.time* directly polls the agents installed on the VIO and the LPARs on a pSeries server for workload and other data.

Note - You can also add pSeries servers that are managed by a Hardware Management Console (HMC) to up.time. You must do this using the Auto Discovery feature. See [Auto Discovery for HMC-Managed pSeries Servers](#) for more information.

You can add multiple systems to *up.time* in a batch operation using a text file and a command line utility. See [Adding Multiple Systems](#) for more information.

- Virtual Node

In a clustered environment, a device with which *up.time* can communicate using a floating IP address.

- VMware ESX

A system that is running version 3 or 4 of the VMware ESX server software, which enables a single host to run multiple virtual servers and their applications. ESX includes features like the ability to balance the computing loads of a group of virtual servers as well as backup data and better manage clusters.

You do not need to install an agent on an ESX server.

- VMware vCenter Server

A central control point for a VMware vSphere datacenter that includes ESX hosts, VMs, as well as groupings such as clusters, datacenters, vApps, and resource pools. A VMware vCenter server's inventory, system configurations, storage profiles, and performance data can be represented in *up.time* alongside physical systems and network devices. When a VMware vCenter is added, its resources are detected and automatically imported.

- WMI Agentless

A Windows-based system whose metrics collection is managed by WMI (Windows Management Instrumentation), and does not have an *up.time* agent installed on it. *Note - WMI-based monitoring only works if the Monitoring Station is running on Windows.*

Adding Systems or Network Devices

To add systems or network devices, do the following:

1. In the *My Infrastructure* panel, click *Add System/Network Device*.
 2. Enter a descriptive name for the server in the *Display name in up.time* field.
This name will appear in the *up.time* interface. A system can have a different display name than the hostname. For example, you can assign the display name *Toronto Mail Server* to a system with the host name *10.1.1.6*. This way, IP addresses are stored in *up.time* but a more descriptive or meaningful name is displayed in the *up.time* Web interface.
 3. Optionally, enter a description of the system in the *Description* field.
 4. Select one of the following options from the *Type of System/Device* dropdown list:
 - Agent
 - Net-SNMP v2
 - Net-SNMP v3
 - Network Device
 - Novell NRM
 - pSeries LPAR Server (VIO)
 - pSeries LPAR Server (HMC)
 - Virtual Node
 - VMware ESX
 - VMware vCenter Server
 - WMI Agentless (only present on Monitoring Stations running on Windows)
 5. Enter the host name of the system in the *Host Name* field.
The host name can be the actual name of the machine that *up.time* will be monitoring. You can also enter an IP address in this field.
 6. If applicable, enter the port number at which you will be connecting to the system in the *Port* field.
In most cases, you can use the default port.
 7. Configure the system- or device-specific settings:
 - If you selected *Agent* in step 4 and want to securely access the system, click the *Use SSL* option.
Note: If the *up.time* Agent's information has been globally configured in the *Config* section, the agent port and SSL options will not appear.
 - If you selected *Net-SNMP v2* in step 4, enter information in the following fields:
 - *SNMP Port*
The port on which the Net-SNMP instance is listening.
 - *Read Community*
A string that acts like a user ID or password, giving you access to the Net-SNMP instance.
Common read communities are *public* (enables you to retrieve read-only information from the device) and *private* (enables you to access all information on the device).
 - If you selected *Net-SNMP v3* in step 4, enter information in the following fields:
 - *SNMP Port*
The port on which the Net-SNMP instance is listening.
 - *Username*
The name that is required to connect to the Net-SNMP instance.
 - *Authentication Password*
The password that is required to connect to the Net-SNMP instance.
 - *Authentication Method (optional)*
From the list, select one of the following options, which will determine how encrypted information travelling between the Net-SNMP instance and *up.time* will be authenticated:
 - MD5: A widely-used method for creating digital signatures used to authenticate and verify the integrity of data.
 - SHA: A secure method of creating digital signatures. SHA is considered the successor of MD5 and is widely used with network and Internet data transfer protocols.
 - *Privacy Password*
The password that will be used to encrypt information travelling between the Net-SNMP instance and *up.time*.
 - *Privacy Type (optional)*
From the list, select one of the following options, that determine how information travelling between the Net-SNMP instance and *up.time* will be encrypted:
 - DES: An older method used to encrypt information.
 - AES: The successor to DES, which is used with a variety of software that require encryption including SSL servers.
- Note - You can set both the authentication and password types, only one of them, or neither.*
- If you selected *Network Device* in step 4, and it uses version 2 of the SNMP protocol, complete the following fields:
 - *SNMP Port*
The port on which the network device is listening.
 - *Read Community*
A string that acts like a user ID or password, giving you access to the network device instance.
Common read communities are *public* (enables you to retrieve read-only information from the device) and *private* (enables you to access all information on the device).
 - *Is Node Pingable?*
This options specifies whether *up.time* can contact the node using the ping utility.
There are scenarios in which you might not want the node to be pingable (e.g., you have a firewall in place). Before selecting

this check box, you should try to contact the node using the ping utility. If you cannot ping the node, ensure the check box is left cleared. Then, change the default host check for the node. See [Changing Host Checks](#) for more information.

- Exports NetFlow Data to Scrutinizer?

If Scrutinizer has been integrated with *up.time*, and is also receiving NetFlow data from the node, select this check box. You will then be able to call a Scrutinizer instance directly from the node's Graphing tab in *up.time*.

Note that if global SNMP details have been configured in the *Config* section, none of these options will appear, or need to be configured.

- If you selected *Network Device* in step 4, and it uses version 3 of the SNMP protocol, complete the following fields:
 - SNMP Version
Change this to v3 to reveal configuration options relevant to version 3 of the SNMP protocol.
 - SNMP Port
The port on which the network device is listening.
 - Username
The name that is required to connect to the network device.
 - Authentication Password
The password that is required to connect to the network device.
Authentication Method (optional)
From the list, select an option that will determine how encrypted information travelling between the network device and *up.time* will be authenticated:
 - MD5: A widely-used method for creating digital signatures used to authenticate and verify the integrity of data.
 - SHA: A secure method of creating digital signatures. SHA is considered the successor of MD5 and is widely used with network and Internet data transfer protocols.
 - Privacy Password
The password that will be used to encrypt information travelling between the network device and *up.time*.
 - Privacy Type (optional)
From the list, select an option that will determine how information travelling between the network device and *up.time* will be encrypted:
 - DES: An older method used to encrypt information.
 - AES: The successor to DES, which is used with a variety of software that require encryption including SSL servers.

Note - You can set both the authentication and password types, only one of them, or neither.

- Is Node Pingable?
This option specifies whether *up.time* can contact the node using the ping utility.
There are scenarios in which you might not want the node to be pingable (e.g., you have a firewall in place). Before selecting this check box, you should try to contact the node using the ping utility. If you cannot ping the node, ensure the check box is left cleared. Then, change the default host check for the node. See [Changing Host Checks](#) for more information.
- Exports NetFlow Data to Scrutinizer?
If Scrutinizer has been integrated with *up.time*, and is also receiving NetFlow data from the node, select this check box. You will then be able to call a Scrutinizer instance directly from the node's Graphing tab in *up.time*.

Note that if global SNMP details have been configured in the *Config* section, none of these options will appear, or need to be configured.

- If you selected *Novell NRM* in step 4, enter information in the following fields:
 - Username
The user name that is required to access the Novell NRM Web interface.
 - Password
The password that is required to access the Novell Web interface.
- If you selected *VMware ESX* in step 4, enter information in the following fields:
 - User Name
The user name required to log into the VMware ESX server.
 - Password
The password required to log into the VMware ESX server.
- If you selected *VMware vCenter Server* in step 4, enter information in the following fields:
 - User Name
The name of the VMware vCenter administrator account.
 - Password
The password for the VMware vCenter account.
 - Notification Settings
When a vSync operation is performed to check for changes to the VMware vCenter inventory, these check boxes indicate whether *up.time* will send notifications about, or perform scripted actions in response to, newly discovered ESX servers or VMs. (For more information, see [Managing vSync](#).)
 - Additional VM Guest Performance Data Collection
These options enable additional monitoring for VMware vCenter VMs using the *up.time* agent or WMI. (See [Standalone Monitoring for vCenter VMs](#).)
For the *up.time* agent, indicate the port on which it is listening, and whether it is securely communicating with *up.time* using SSL.
For data collection via WMI, indicate the host and domain on which WMI has been implemented, and the username and password required for access.
- If you selected *WMI Agentless* in step 4, enter information in the following fields:
 - Windows Domain
The Windows domain in which WMI has been implemented.
 - User Name
The name of the account with access to WMI on the Windows domain.
 - Password
The password for the account with access to WMI on the windows domain.

Note that if global WMI credentials have been defined in the *Config* section, none of these options will appear, or need to be configured.

8. If you want to associate this system with a group, select the name of the group from the *Group* dropdown list.
See [Working with Groups](#) for more information on defining groups.
9. If you want to associate this system with a service group, select the name of the group from the *Service Group* dropdown list.
See [Service Groups](#) for more information.

10. Click *Save* .
A window listing general information about the system you have added appears.
11. If you want to add another system or network device, click *Add Another* . Then, repeat steps 2 to 14.
Otherwise, click *Close* .
12. Click *Save*.

Adding VMware Instances to up.time

VMware ESX server software enables a single host to run multiple virtual servers and their applications. *up.time* can monitor both the server that is running VMware ESX, and VMware instances, which are the virtual servers that are running on the VMware server.

To add VMware instances to *up.time* , do the following:

1. In the *My Infrastructure* panel, click the name of the VMware server that contains instances that you want to monitor.

A new window containing information about the system appears.

1. Click the *Info* tab, and then click *VMware Instances* .
2. A list of VMware instances appears in the sub panel. Click the *Add to up.time* button.

The *Add System* window appears. *Note - The Add to up.time button is not visible if a VMware instance is not on.*

1. If necessary, you can change any of the following options:
2. Display name in *up.time*
3. Description
4. Group
5. Service Group
6. Click *Save* to add the instance to *up.time* .

SNMP-based Systems

Simple Network Management Protocol (SNMP) is a widely-used protocol that monitors the health of computer and network equipment. The SNMP Poller enables you to query SNMP devices or systems for a given object identifier (OID) of an SNMP Management Information Base (MIB). You can use the monitor to translate or clean up the returned response, then set thresholds for them.

SNMP works on the basis that network management systems send out a request, and managed devices send a response. SNMP messages consist of a header and a PDU (protocol data units). The headers consist of the SNMP version number and the community name; the community name is used as a form of security. Requests and responses between network management systems and devices is implemented using one of four operations: Get, GetNext, Set, and Trap.

- Get, GetNext, and Set (as well as the response PDU) consist of PDU type, Request ID, Error status, Error index and Object/variable fields
- Trap consists of Enterprise, Agent, Agent address, Generic trap type, Specific trap code, Timestamp and Object/Value fields

A MIB is a collection of hierarchically organized definitions, accessed using SNMP. All of the manageable features of all managed devices from different vendors are arranged in this tree. MIB definitions describe the properties of objects within a managed device, and OIDs uniquely identify managed objects in a MIB hierarchy.

Managed objects can exist in either scalar or tabular form. Scalar objects define a single object instance, identified by its ".0"; tabular objects define multiple related object instances grouped in MIB tables, and is identified by its index value.

The MIB hierarchy can be depicted as a tree. Each vendor of SNMP equipment has an exclusive section of the MIB tree structure under their control. Vendors define private branches including managed objects for their own products. Each branch of the MIB tree has a number and name, and a point on the tree is named according to its complete path from the top of the tree (for example, .1.3.6.1.2.1.1.1.0.). Nodes near the top of the tree are very general, whereas each ending node represents a particular feature on a specific device.

Net-SNMP

The *up.time* SNMP monitor also supports Net-SNMP, which is a suite of command line and graphical applications that do the following:

- request information from SNMP agents
- set information on SNMP agents
- generate and handle SNMP traps

To take advantage of the Net-SNMP features, you must:

- Install and configure the Net-SNMP application suite on your server. Visit <http://net-snmp.sourceforge.net> for more information:
- Have a Net-SNMP agent already installed on the host or hosts that you want to monitor. The Net-SNMP *HOST-RESOURCES-MIB* (used to gather performance statistics from a host) must also be enabled. See the Net-SNMP documentation for details.
- Add a Net-SNMP Element to *up.time* . For more information, see [Adding Systems or Network Devices](#).

Supported Versions of SNMP

The *up.time* SNMP monitor works with the following versions of SNMP:

- v2

The second implementation of the SNMP protocol, which contains additional protocol operations as well as improved security and data authentication.

- v3

The latest implementation of the SNMP protocol, which adds security and privacy features that are missing in versions 1 and 2 of the protocol.

See [SNMP Poller](#) and [Network Device Port Monitor](#) for more information.

Adding Individual LPARs to up.time

After you have added pSeries servers - whether managed by an HMC or not - to *up.time*, you can add individual LPARs from those systems to *up.time*. While *up.time* collects workload data from all LPARs on a pSeries server (whether they have been added to *up.time* or not), adding LPARs can help you keep track of any specific LPAR.

To add an LPAR to *up.time*, do the following:

1. In the *My Infrastructure* panel, click the name of the pSeries server that contains the LPAR that you want to monitor.
A new window containing information about the system appears.
2. Click the *Info* tab, and then click *Logical Partitions*.
A list of LPARs appears in the sub panel.
3. Click the *Add to up.time* button beside the LPAR that you want to add to *up.time*.
The *Add System* window appears.
4. If necessary, you can change any of the following options:
 - Display name in *up.time*
 - Description
 - Group
 - Service Group
5. Click *Save* to add the LPAR to *up.time*.



Note - It can take up to 15 minutes for the Monitoring Station to retrieve enough samples to provide historical graphing data to the Monitoring Station.

Agentless WMI Systems

If the Windows-based component of your infrastructure already makes use of WMI (Windows Management Instrumentation), Windows Elements can be configured to use it for data collection as an alternative to the *up.time* Agent. Using WMI allows you to avoid the overhead associated with managing and updating all of the systems on which an *up.time* Agent has been installed.

Note - WMI-based monitoring can only be performed if the Monitoring Station itself is running on Windows.

An Element can be set to use WMI through the following methods:

- its system type is set to "WMI Agentless" when it is first added to *up.time*
- its system type was set to "Agent" when originally added to *up.time*, but is being individually modified to use WMI
- it is part of a bulk agent-to-WMI conversion with other agent-based Elements

Globally defined WMI credentials can be used for the second and third method. In the latter's case, configuring these is mandatory. Refer to [Configuring Global WMI Credentials](#) for more information.

Regardless of which method is used, when changing a Windows Element's data collection method, all historical data is retained.

WMI Requirements

In order to monitor agentless systems through WMI in a secure environment (e.g., through a firewall), you need to create an exception for WMI on the host end. For example, to allow WMI access through Windows Firewall, refer to the following MSDN articles:

- for Windows XP or Windows Server 2003:
<http://msdn.microsoft.com/en-us/library/aa389286%28v=VS.85%29.aspx>
- for Windows Vista or Windows Server 2008:
<http://msdn.microsoft.com/en-us/library/aa822854%28v=VS.85%29.aspx>

Adding a WMI System to up.time

To add an agentless WMI system to *up.time*, do the following:

1. On the *up.time* tool bar, click *My Infrastructure*, then click *Add System/Network Device*.
2. Complete the *Display name in up.time* and *Description* fields.
See [Adding Systems or Network Devices](#) for more information.
3. Select *WMI Agentless* from the *Type of System/Device* dropdown list.
4. In the *Host Name* field, enter the actual name or IP address of the machine that *up.time* will be monitoring.
5. Select the *Use WMI Global Credentials* check box if they have been configured, and you would like to use them (see [Configuring Global WMI Credentials](#) for more information); otherwise complete the following fields:
 - Windows Domain
The Windows domain in which WMI has been implemented.
 - Username
The name of the account with access to WMI on the Windows domain.
 - Password
The password for the account with access to WMI on the windows domain.
6. If you want to associate this system with a group, select its name from the *Group* dropdown list.
7. If you want to associate this system with a Service Group, select its name *Service Group* dropdown list.

8. Click **Save**.

Switching an Element to WMI Data Collection

To change the data collection source for an individual Windows Element from the *up.time* Agent to WMI, do the following:

1. In the *Global Scan* or *My Infrastructure* panels, click the name of the Windows server.
2. Click the *Info* tab, then click *Info & Rescan*.
3. Click the *Edit Collection Method* link found beside the *Collection Method* setting.
The *Edit Data Collection Method* window appears.
4. Select the *WMI Agentless* data collection option.
5. Select the *Use WMI Global Credentials* check box if they have been configured, and you would like to use them (see [Configuring Global WMI Credentials](#) for more information); otherwise complete the following fields:
 - **Windows Domain**
The Windows domain in which WMI has been implemented.
 - **Username**
The name of the account with access to WMI on the Windows domain.
 - **Password**
The password for the account with access to WMI on the windows domain.
6. Click **Save** to retain your changes and close the pop-up window.

Switching an Element to Agent-Based Data Collection

To change the data collection source for an individual Windows Element from WMI to the *up.time* Agent, do the following:

1. In the *Global Scan* or *My Infrastructure* panels, click the name of the Windows server.
2. Click the *Info* tab, then click *Info & Rescan*.
3. Click the *Edit Collection Method* link found beside the *Collection Method* setting, as shown below
The *Edit Data Collection Method* window appears.
4. Select the *up.time Agent* data collection option.
5. Select the *Use up.time Agent Global Configuration* check box if it has been configured, and you would like to use it (see [Configuring a Global up.time Agent Configuration](#) for more information); otherwise complete the following options:
 - **Port**
The port through which the *up.time* Agents communicate with the *up.time* Monitoring Station.
 - **Use SSL**
Select this check box if the agent securely communicates with the Monitoring Station using SSL.
6. Click **Save** to retain your changes and close the pop-up window.

Converting Multiple Elements to WMI Data Collection

To change multiple agent-based Elements to use WMI for data collection, do the following

1. Ensure the global settings for WMI credentials have been set (see [Configuring Global WMI Credentials](#) for more information).
2. On the *up.time* tool bar, click *Config*.
3. In the tree panel, click *Bulk Element Conversion*.
4. In the *Windows Agent Elements* section, select the check boxes that correspond to the agent-based Elements whose data collection method is to be changed to WMI.
5. Click *Convert to WMI*.
When the conversion is complete, the lists of agent-based and WMI Elements will be refreshed to reflect the changes.

Converting Multiple Elements to Agent-Based Data Collection

To change multiple WMI Elements to use the *up.time* Agent for data collection, do the following

1. Ensure a global *up.time* Agent configuration exists (see [Configuring Global WMI Credentials](#) for more information).
2. On the *up.time* tool bar, click *Config*.
3. In the tree panel, click *Bulk Element Conversion*.
4. In the *WMI Elements* section, select the check boxes that correspond to the WMI Elements whose data collection method is to be changed to the *up.time* Agent.
5. Click *Convert to Agent*.
When the conversion is complete, the lists of agent-based and WMI Elements will be refreshed to reflect the changes.



Note - For bulk WMI-to-agent conversions, the port used by all of the converted up.time Agents must match the port specified in the global agent configuration.

Novell NRM Systems

up.time collects performance metrics and availability information from version 6.5 of the Novell Remote Manager (NRM) using HTTP or HTTPS. *up.time* extracts performance information from the NRM by reading and parsing XML files.

Adding a Novell NRM System to up.time

To add a Novell NRM version 6.5 system to *up.time*, do the following:

1. On the *up.time* tool bar, click *My Infrastructure* and then click the *Add System/Network Device* tab.
2. Complete the *Display name in up.time* and *Description* fields.
See [Adding Systems or Network Devices](#) for more information.

3. Select *Novell NRM* from the *Type of System/Device* dropdown list.
4. Complete the following fields:
 - Host name
The actual name of the machine that *up.time* will be monitoring, or the IP address of the machine.
 - Port
The port on which the NRM is listening. The default is *8008* for a port that is not using SSL. The default for a port that is using SSL is *8008*.
 - Username
The NRM administrator account name. This field is mandatory.
 - Password
The NRM administrator password. This field is mandatory.
Note - The password is encrypted and stored in the up.time DataStore.
5. If you want to associate this system with a group, select its name from the *Group* dropdown list.
6. If you want to associate this system with a Service Group, select its name *Service Group* dropdown list.
7. Click *Save*.

NRM Statistics Captured by up.time

up.time captures the following Novell NRM system (version 6.5) statistics:

Each statistic returns one of the following statuses:

- Good

The statistic is well within the threshold suspect value.

- Suspect

The statistic is between the threshold good and critical values.

- Bad

The statistic is greater than the threshold critical value.

Work To Do Response Time

This statistic enables you to view how processes share the CPU. The response time is the amount of time that a Work To Do process requires to run.

If this statistic returns a value of Suspect, you can check the running threads to determine why there is a delay in the Work To Do threads. If the value is Bad, thread is probably running more than it should or it is hung. You should identify the parent NetWare Loadable Module and then unload and reload it if possible.

Allocated Service Processes

This statistic enables you to view, as a graph, how the service processes are allocated on your server.

If the service processes are approaching the maximum, increase the value of the Maximum Server Processes Set parameter. If you have only a few available server processes, increase the Minimum Server Processes Set parameter.

If the status is Bad, examine your server by doing the following:

1. In Novell NRM, click *Profiling / Debugging*.
2. Check the information for server process functions.
3. Change the *Maximum Server Processes* and the *Minimum Server Process Set* parameters.

Available Server Processes

This statistic enables you to view the number of available processes on your server as a graph. The graph charts the processes that are available every five seconds over a 50 second period.

If the status is Suspect or Bad, you should increase the Set parameters for Maximum Server Processes and the Minimum Server Processes settings. If the number of available server processes has not reached the maximum and is not increasing, you should add memory to your server.

Abended Thread Count

This statistic enables you to view the threads that have ended abnormally (abended) and are suspended. This statistic returns the following statuses:

If the status is Suspect or a Bad, your server has abended and has recovered automatically by suspending the offending thread while leaving the rest of the server processes running. As a result, some of the server's functions were compromised. You must determine which module, driver, or hardware the abended threads belong to, and then take the appropriate action.

CPU Utilization

This statistic enables you view, as a graph, how busy any given CPU is. *up.time* tracks usage on a per CPU basis, collecting data every 30 seconds. The graph displays a 10 second history.

If the status is Suspect or Bad, determine which thread or module is causing the most CPU cycles and take appropriate action, including the following:

- unloading and reloading the module
- reporting problems to the vendor of the module
- loading an updated module

To determine which thread or module is using the most CPU cycles, do the following:

1. In Novell NRM, click *Profile / Debug* .
2. Do one of the following:
 - View the Execution Profile Data by Thread data.
 - Click *Profile CPU Execution by NLM* .

Connection Usage

up.time monitors connections on a per-server basis. NRM displays only the following metrics:

- the number of connections that are being used
- the peak number of connections used on this server

Available Memory

This statistic enables you to view the amount of memory that is not allocated to any service. Most, if not all, of this memory is used by the file system cache. When available memory gets too low, modules might not be able to load or file system access might become sluggish.

DS Thread Usage

This statistic enables you view the number of server threads that Novell eDirectory uses. The server thread limit ensures that threads are available for other functions as needed - for example, when large number of users log in at the same time.

eDirectory uses multiple server threads. However, its thread requirements should not cause poor performance because eDirectory cannot use more than its allocated maximum number of threads.

If this statistic returns a Good status, eDirectory is using less than 25% of the available server threads. If it returns a Suspect status, eDirectory is using between 25% and 50% of the available server threads. If the status is Bad, eDirectory is using more than 50% of the available server threads.

Packet Receive Buffers

This statistic enables you to view the status of Packet Receive Buffers for the server. Packet Receive Buffers transmit and receive packets. You can set the maximum or minimum number of buffers to allocate using the Maximum Packet Receive Buffers or Minimum Packet Receive Buffers SET parameters. The minimum number of buffers is the number of packets that are allocated at when the system is initialized.

If the number of Packet Receive Buffers is increasing, the system will be sluggish. If the number of Packet Receive Buffers reaches the maximum, and no Event Control Blocks (ECBs) are available, the server will become very sluggish and will not recover.

Available Event Control Blocks (ECBs)

This statistic enables you to view the status of available Event Control Blocks (ECBs). Available ECBs are Packet Receive Buffers that have been created but which are not currently being used.

If the available ECB count is zero, the server will become sluggish until enough ECBs are created to fill the demand. The server will recover as long as the number of Packet Receive Buffers does not increase to the maximum that can be allocated.

LAN Traffic

This statistic shows whether or not your server can transmit and receive packets. If this statistic returns a Good status, the server is able to accept or transmit packets through the network board. If the status is Bad, the network board is not transmitting or receiving packets.

All servers should be able to transmit or receive packets. If your server is not transmitting, your LAN is not functioning properly. Check the drivers and protocol bindings for the network board on the server. If the drivers and protocol bindings are functioning properly, then the network board is probably faulty. If the network board is functioning, you should perform a diagnostic on your LAN.

Available Disk Space

This statistic enables you to view the status of the available disk space on all mounted volumes on a server. This statistic returns the following statuses:

Disk Throughput

This statistic enables you to view the status of amount of the data that is being read from and written to the storage media on this server.

If this statistic returns a Good status, then the storage system is experiencing reads or writes, and there are no pending disk I/Os. If the status is Suspect, the storage system has disk I/Os pending, no reads or writes have occurred, and less than four samples have been taken. If the status is Bad, the storage system has disk I/Os pending, no reads or writes have occurred, and four or more samples have been taken.

Adding Multiple Systems

It can be time consuming to add large numbers of systems to *up.time* using the Web interface. You can, however, add multiple systems to *up.time* using the *addsystem* command line tool and a text file.

A text file, called a *hosts file* , contains entries which mirror the fields in the *Add System* window of the *up.time* Web interface. These fields contain information about the systems that you want to add.

You can find examples of entries in a hosts file in the section [Examples of Hosts File Entries](#).

Creating a Hosts File

There are a number of ways in which you can create a hosts file. The simplest way is to use a text editor to type the entries in a file. If you have a large number of systems to add, you can copy and paste an entry, and modify the fields as needed.

If you keep a list of all the systems in your environment in a spreadsheet, you can save the list as a text file or a comma separated values (*.csv*) file. Then, you can write a script that can manipulate the text or *.csv* file into the proper format.

Fields in the Hosts File

The following table explains the fields that you can include in the hosts file. The fields that are needed to add a system will vary depending on the type of system that you want to add. For example, to add an agent system you only need to include the Host Name, Type, and Port fields. See [Working with Systems](#) for more information.

Field	Description
Host Name	The name or the IP address of the system that you want to add to <i>up.time</i> .
Display Name	The name for the system that will appear in the <i>up.time</i> Web interface.
Description	A short description of the system. This field is optional.
Type	<p>The type of system, which can be one of the following:</p> <ul style="list-style-type: none"> Agent Node Novell NRM Net-SNMP v2 Net-SNMP v3 pSeries LPAR Server (HMC) Virtual Node WMI Agentless
Service Group	<p>The name of the <i>up.time</i> service group - which enables you to simultaneously apply common service checks to hosts that you are monitoring - to which you want to add the system.</p> <p>This field is optional.</p>
Port	The number of the port on which you will be connecting to the system. Leave this field blank to use the default port for the type of system that you are adding.
Community	<p>If you are adding a Net-SNMP system to <i>up.time</i> , specify the read community (which acts like a user ID or password) that gives you access to the system. Valid options are:</p> <ul style="list-style-type: none"> <i>public</i> , which enables you to retrieve read-only information. <i>private</i> , which enables you to access all information
HMC Hostname	The name or the IP address of the Hardware Management Console (HMC) that is being used to manage one or more pSeries LPAR servers in your environment.
Managed Server	The unique identifier of a pSeries LPAR server that is managed by an HMC.
Username	If you are adding a Net-SNMP or Novell NRM system to <i>up.time</i> , specify the user name required to access the system.
Password	If you are adding a Net-SNMP or Novell NRM system to <i>up.time</i> , specify the password required to access the system.
Group	<p>The name of the Element group - a set of systems that have been combined in a meaningful way - to which you want to add this system.</p> <p>This field is optional.</p>
SSL	<p>For agent systems, use this field to determine whether or not <i>up.time</i> will securely communicate with an agent installed on the system using SSL. Valid options are <i>true</i> and <i>false</i> .</p> <p>This field is optional.</p>
Authentication Method	<p>For Net-SNMP systems, use this field to determine how encrypted information travelling between the Net-SNMP instance and <i>up.time</i> will be authenticated. Valid options are:</p> <ul style="list-style-type: none"> <i>MD5</i> , a widely-used method for creating digital signatures. <i>SHA</i> , a secure method of creating digital signatures.

Privacy Password	For Net-SNMP systems, the password that will be used to encrypt information travelling between the Net-SNMP instance and <i>up.time</i> .
Privacy Type	For Net-SNMP systems, how information travelling between <i>up.time</i> and the Net-SNMP instance is encrypted. Valid options are: <i>DES</i> , an older method used to encrypt information. <i>AES</i> , the successor to DES, which is used with a variety of software including SSL servers.
Pingable	For nodes, use this field to specify whether or not <i>up.time</i> can contact the node using the ping utility. Valid options are <i>true</i> and <i>false</i> .
WMI Domain	The Windows domain in which WMI has been implemented.
WMI Username	The name of the account with access to WMI on the Windows domain.
WMI Password	The password for the account with access to WMI on the windows domain.

Adding Multiple Systems to *up.time*

To add multiple systems to *up.time* , do the following:

1. Copy the hosts file to the directory in which you installed the *up.time* Monitoring Station.
2. At the command line, navigate to the *scripts* folder.
For example, if you installed the Monitoring Station in the default location on a Windows system, navigate to the following folder:
C:\Program Files\uptime software\uptime\scripts
3. Enter the following command:
addsystem <path_and_filename>
Where *<path_and_filename>* is the name of the text file that contains the list of systems that you want to add to *up.time* along with its full path.
The systems listed in the file are added to *up.time*, unless:
 - *up.time* cannot connect to the system.
 - The system does not exist in your environment.
 - The system has already been added to *up.time* .

Examples of Hosts File Entries

The following table contains sample host file entries for each type of system that you can add to *up.time* :

Host Type	Sample Hosts File Entry
Agent	<i>Host Name: prod-mainSystem</i> <i>Display Name: prod1</i> <i>Description: Main production server</i> <i>Type: Agent</i> <i>Service Group: Production Systems</i> <i>Port:9998</i> <i>Group: Windows 2003 Servers</i>
Node	<i>Host Name: www.myDomain.ca</i> <i>Display Name: Your Domain</i> <i>Description: A Web site</i> <i>Type: Node</i> <i>Group: Web Sites</i>
Novell NRM	<i>Host Name: novell01</i> <i>Display Name: dn3</i> <i>Type: Novell NRM</i> <i>SSL: true</i> <i>Port: 546</i> <i>Group: Unix Boxes</i> <i>Group: Novell System</i>
Net-SNMP v2	<i>Host Name: gateway.mydomain.com</i> <i>Display Name: gatewaySNMP</i> <i>Description: snmp v2</i> <i>Type: Net-SNMP v2</i> <i>Read Community: myCo-pub</i>
Net-SNMP v3	<i>Host Name: SNMP-1</i> <i>Display Name: SNMP-1</i> <i>Description: Net-SNMP system</i> <i>Type: Net-SNMP v3</i> <i>Read Community: public</i> <i>Username: myUsername</i> <i>Password: myPassword</i> <i>Privacy Password: myOtherPassword</i> <i>Group: Linux Systems</i>

pSeries LPAR	<i>Host Name: 10.1.2.42</i> <i>Display Name: HMC Managed Server</i> <i>HMC Hostname: 10.1.1.255</i> <i>Type: pSeries LPAR Server (HMC)</i> <i>Managed Server: Server-7610-31C-SN01B030K</i> <i>Username: hscroot</i> <i>Password: hscroot</i>
Virtual Node	<i>Host Name: router-Toronto</i> <i>Display Name: Toronto Router</i> <i>Description: Router for Toronto branch</i> <i>Type: Virtual Node</i> <i>Pingable: True</i> <i>Group: Routers</i>
WMI Agentless	<i>Host Name: Win7-Production</i> <i>Display Name: Windows 7 Production</i> <i>Description: Win7 agentless/WMI</i> <i>Type: WMI Agentless</i> <i>Group: Windows Boxes</i> <i>WMI Domain: windomain</i> <i>WMI Username: administrator</i> <i>WMI Password: password</i>

Editing a System Profile

After you have added a system to *up.time*, you might need to change some of the basic information about that system. You can do this by editing the system profile.

To edit a system profile, do the following:

1. In the **My Infrastructure** panel, click the gear icon beside the Element whose profile you want to modify, then click **Edit**. The **Edit System** window appears.
2. In the **Edit System** window, change any or all of the following options:
 - **Display name in up.time**
The descriptive name for the system that appears in the up.time Web interface.
 - **Description**
A brief functional description of the system.
 - **Parent Group**
Select the group of systems in up.time with which this system will be associated.
 - **Custom Field 1 to Custom Field 4**
These fields enable you to include additional information about the system. For example, you can record the types of reports that should be run on this system, or when maintenance is scheduled.
The information in the Custom Fields is displayed when you view system information by clicking the **Info & ReScan** link in the Tree panel.
 - **Number of processes to retrieve**
The default number of processes running on the system that up.time will retrieve. If you select 10 processes, and there are 20 running on the system, *up.time* retrieves the 10 busiest processes.
 - **Is monitored?**
Click this checkbox to turn monitoring off for this system. If monitoring is turned off, the system will not appear in the **Global Scan** panel.
3. Click **Save**.

Working with Applications

An Application provides the overall status for one or more services. You can, for example, add an Application that checks the status of a system's Web services, database, and file system capacity.

When creating an Application, you must specify the following:

- master service monitor(s)

One or more monitors can be used to determine the status of the Application as a whole.

- regular service monitors

Other service monitors that are associated with a master service monitor, but are not used to determine the status of the Application as a whole.

- warning and critical conditions for multiple master service monitors

You can configure an Application to reach a warning- or critical-level state when a specific number, percentage, or all master service monitors enter those states.

This allows you to give different Applications different levels of robustness by assigning more or less "weight" to their respective groups of master service monitors. As a result, each of your Applications will provide the most accurate status possible, and fewer false positives. For example, a web server cluster of 10 servers might only cause alerts when three of them are down, whereas a mission-critical application will cause an alert when all of its master service monitors fail.

For more information on services, see [Using Service Monitors](#).

Adding Applications

To add an Application, do the following:

1. In the *My Infrastructure* panel, click *Add Application* .
2. In the *Add Application* window, enter a descriptive name for the Application in the *Name of Application* field.
This name will appear in both the *My Infrastructure* and *Global Scan* panels.
3. Optionally, enter a description for the Application in *Description of Application* field.
4. Optionally, select the group of systems in your *up.time* environment with which this system will be associated from the *Parent Group* dropdown list.
By default, the Application is added to the My Infrastructure group.
For more information on groups, see [Working with Groups](#).
5. In the *Application Status* section, define how many master service monitors must be in a warning- or critical-level state to affect the Application as a whole.
You can include a defined number, a percentage or all master service monitors in this condition.
6. Select one of the following options from the dropdown list above the *Available Master Service Monitors* list:
 - the name of a specific system, which displays all its service monitors
 - *All* , which displays all service monitors for every system in your environment
7. Select one or more of the service monitors from the *Available Master Service Monitors* list, and then click *Add* .
8. Select one of the following options from the dropdown list above the *Available Regular Service Monitors* list:
 - the name of a specific system, which displays all its service monitors
 - *All* , which displays all service monitors for every system in your environment
9. Select one or more of the service monitors from the *Available Regular Service Monitors* list and then click *Add* .
10. Click *Save* .
After closing the *Add Application* window, the name of the newly created Application appears in the *My Infrastructure* panel as a link that can be clicked to view the Application's details.
11. If required, associate Alert Profiles with the Application by clicking *Edit Alert Profiles* when viewing the Application's details.
12. In the *Alert Profile Selector* pop-up window, select one or more of the *Available Alert Profiles* from the list, then click *Save* .
13. If required, associate Action Profiles with the Application by clicking *Edit Action Profiles* when viewing the Application's details.
14. In the *Action Profile Selector* pop-up window, select one or more of the *Available Action Profiles* from the list, then click *Save* .

Viewing Details About Applications

After you have added an Application to *up.time* , the name of the Application appears in the *My Infrastructure* panel. The name of the Application is a hyperlink.

You can view detailed information about that Application by clicking the name of the Application, which opens the *Application General Information* subpanel.

The *Application Profile* section of the subpanel displays the following information about the Application:

- the name of the Application
- the description, if available
- the group of systems to which the Application belongs
- whether or not the Application is being monitored

The *Application Member Services* section of the subpanel contains the following information about the service monitors that are part of the Application:

- the name of the service that is being monitored
- whether or not the service is a master service monitor

The *Alert Profiles* section of the subpanel displays which Alert Profiles have been associated with the Application.

For information about viewing more details about Applications, see .

Editing Applications

To edit an Application, do the following:

1. In the **My Infrastructure** panel, click the gear icon beside the Application you want to modify, then click **Edit**.
The **Edit Application** window appears.
2. Edit the Application setting as described in [Adding Applications](#).

Working with SLAs

In *up.time* , a service level agreement (SLA) measures your organization's ability to meet pre-defined performance goals. These goals focus on various aspects of your IT infrastructure, and each can include any number of monitored systems.

From the *My Infrastructure* panel, you can view your existing SLA details by clicking the SLA name (see [Viewing SLA Details](#) for more information).

For information about creating and using SLAs, see [Adding and Editing SLA Definitions](#).

Working with Groups

At sites with multiple systems to monitor, searching through a large list of systems is time consuming. To avoid this problem, you can define *groups* of systems. Groups are sets of systems that have been combined in a meaningful way.

You can group systems by their geographical location or by their function. The name of the group should describe the servers or the way in which they have been grouped. For example, you can create a group called *Database Servers* that contains all of the database servers in your environment.

You can assign the following to groups:

- Elements, which can be systems, nodes, SLAs, or Applications
- the user groups that are allowed to view the systems or Elements in a group (see [Working with User Groups](#) for more information on user groups)



Note - If you plan to group your systems, you should first map out what groups you need and which systems will be part of those groups.

Adding Groups

To add a group, do the following:

1. On the *My Infrastructure* panel, click *Add Group*.
2. Enter a descriptive name for the group in the *Group Name* field.
3. Optionally, enter a description of the group in the *Group Description* field.
4. To make this group a subgroup, select the name of the existing group to which it will be subordinate in the *Parent Groups* list, then click *Add*.
Note - If this is the first group that you have defined, only My Infrastructure will appear in the dropdown list.
5. To give this group its own subgroups, select one or more entries from the *Available Groups* list, then click *Add*.
6. Select the Elements that you want to add to this group from the *Available Elements* list, then click *Add*.
7. Select one or more sets of users who can view this group from the *Available User Groups* list, then click *Add*.
8. Click *Save*.

Adding Nested Groups

You can also create *nested groups*. Nested groups enable you to further group your systems. For example, you can create a parent group called *Datacenters*, and then add two nested groups called *Production* and *Disaster Recovery*.

You can assign the following to nested groups:

- groups of Elements
- individual Elements
- the *up.time* user groups that are allowed to view the systems or Elements in a group

Note that you cannot assign a parent group to a subgroup or to any other ancestor.



Note - Before you begin, ensure that you have at least one parent group defined.

Adding a Nested Group

To add a nested group, do the following:

1. In the *My Infrastructure* panel, click *Add Group*.
2. Enter a descriptive name for the group in the *Group Name* field.
3. Optionally, enter a description of the group in the *Group Description* field.
4. Select the group with which the new one will be associated from the *Parent Group* dropdown list.
5. To give this nested group its own subgroups, select one or more entries from the *Available Groups* list, then click *Add*.
6. Select the Elements that you want to add to this group from the *Available Elements* list, and then click *Add*.
7. Select one or more sets of users who can view this group from the *Available User Groups* list, and then click *Add*.
8. Click *Save*.

Editing Groups

To edit groups, do the following:

1. In the *Infrastructure* panel, click the gear icon beside the group that you want to modify, then click **Edit**.
The **Edit Element Group** window appears.
2. Edit the group as described in [Adding Groups](#).
3. Click **Save**.

To delete a group, click its gear icon, then click **Delete**, but note that only empty groups can be deleted from the **My Infrastructure** panel.

Working with Views

Not every user that accesses the Monitoring Station needs to view all Elements that are a part of your infrastructure. Some users may, for example, only need to be interested in five to 10 of the available servers. You can limit the servers that one or more users will see by creating specific *views*, which are subsets of the servers in your environment. By creating views, it becomes easier for users to not only monitor systems, but to also browse and compare historical data. Views appear in the Views section on the *Infrastructure* panel, as well as the *Global Scan* panel.

Adding Views

To add a view, do the following:


1. In the *Infrastructure* panel, click *Add View* .
2. In the *Add View* window, enter a descriptive name in the *View Name* field.
This name will appear when listing views in the *Infrastructure* panel.
3. Optionally, enter a description in *View Description* field.
4. To make this view a child of an existing one, select it from the *Parent View* dropdown list.
Note - If this is the first group that you have defined, only My Infrastructure will appear in the dropdown list.
5. To give this view its own child views, select one or more entries from the *Available Element Views* list, then click *Add* .
6. Select one or more Elements from the *Available Elements* list, then click *Add* .
If you have combined your Elements into groups, select a group from the dropdown at the top of the list. Or, select *All* from the dropdown to display all of the Elements in your environment
7. Select one or more users from the *Available Users for View* list, then click *Add* .
8. To add previously defined groups of users, select one or more entries from the *Available User Groups* list, then click *Add* .
9. Click *Save* .

Adding Nested Views

You can also create nested views in order to categorize and better manage a larger set of existing views. The following can be assigned to nested views:

- existing Element views
- individual Elements
- individual users who have view access to the Elements in a view
- *up.time* user groups with similar privileges

You cannot assign a parent view to a child view or to any other ancestor.

 *Note - Before you begin, ensure that you have at least one parent view defined.*

Adding a Nested View

To add a nested view, do the following:

1. In the *Infrastructure* panel, click *Add View* .
2. In the *Add View* window, enter a descriptive name in the *View Name* field.
This name will appear when listing views in the *Infrastructure* panel.
3. Optionally, enter a description in *View Description* field.
4. In the *Parent View* dropdown list, select the view to which this nested view will be subordinate.
5. To give this nested view its own child views, select one or more entries from the *Available Element Views* list, then click *Add* .
6. Select one or more users who can view this group from the *Available Users* list, then click *Add* .
7. To add previously defined groups of users, select one or more entries from the *Available User Groups* list, then click *Add* .
8. Click *Save* .

Editing Views

To view and edit views, do the following:


1. In the **My Infrastructure** panel, click the gear icon beside the View that you want to modify, then click **Edit**.
The **Edit View** window, which contains system and user information, appears.
2. Edit the view as described in [Adding Views](#).
3. Click **Save**.

Deleting Elements, Applications, and Views

If you have administrator privileges, you can delete a Element, or view in the *Infrastructure* panel.

To remove an Element, Application, or View from *up.time* , do the following:

1. In the *Infrastructure* panel, locate the Element or *up.time* grouping you want to permanently remove.
2. Click the Element or grouping's gear icon.
3. In the pop-up menu, click *Delete* .
4. On the dialog box that appears, click *OK* .

 *Note - You can only delete Elements that were created in up.time . You cannot manually remove Elements that represent VMware vSphere components imported into up.time via vSync.*

Acknowledging Alerts

When a problem occurs on a system that *up.time* is monitoring, the Monitoring Station sends alerts: these are notifications about the problem, sent to users who are qualified to receive them. If the user role to which they belong is configured to do so, they can also acknowledge an alert.

When you acknowledge an alert, *up.time* :

- records the acknowledgement, which can be viewed in the Service Monitor Outages report
- sends an acknowledgement message to any *up.time* user who received the last alert

- turns off alert escalation, but continues monitoring the problem, and only sends an alert when the status of the system or Application returns to OK

To acknowledge alerts, do the following:

1. In the *Infrastructure* panel, click the name of the Element that generated the alert.
2. The *System General Information* subpanel appears.
3. In the *Tree* panel, click the *Services* tab and then click *Status*.
4. Status information for the monitors associated with the Element appears in the subpanel.
5. Click the *Acknowledge* icon in the *Ack* column.
6. The acknowledgement message window appears.
7. Type a comment relating to the alert or why it has been acknowledged, and then click *Submit*.
8. An email containing the following information is sent to any *up.time* user who received the last alert:
9. the user name and email address of the person who acknowledged the alert
10. the name of the Element and service monitor involved
11. a comment relating to the alert or reason for acknowledgement
12. The following is a sample alert acknowledgement message:
13. *up.time Administrator (jsmith@myDomain.com)*
14. *acknowledged the WARN status of File System Capacity (Web Server 2) with comment:*
15. *Initial check of problem. More information to come.*
16. In the *up.time* Web interface, the acknowledge icon will change.