Managing Your Infrastructure

Overview

The **Infrastructure** panel is your starting point for monitoring the systems in your environment. From the 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 are combined in a meaningful way
- views, which enable non-administrative users to view only the systems in which they are interested

Working with Elements

Elements are the systems or network devices that you monitor using Uptime Infrastructure Monitor. You can add the following types of Elements:

Element Type	Description
Agent	A system that has an Uptime Infrastructure Monitor Agent installed on it.
Hyper-V Server	A system that is running the Microsoft Hyper-V virtualization software and a is central control point for VMs and groupings such as clusters and resource pools. A Hyper-V server's inventory, system configurations, storage profiles, and performance data can be represented in Uptime Infrastructure Monitor alongside physical systems and network devices. When a Hyper-V VM is added, its resources are detected and automatically imported.
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.
Network Device	An agentless, SNMP-based switch or router whose performance and configuration data is retrieved by focusing on specific OID values.
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. Uptime Infrastructure Monitor 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, Uptime Infrastructure Monitor directly polls the agents installed on the VIO and LPARs on a pSeries server for workload and other data.
pSeries LPAR Server (HMC)	A pSeries server that is hosting multiple LPARs, and is a managed server under the supervision of an HMC (Hardware Management Console). We recommend adding pSeries servers that are managed by an HMC using the Auto Discovery process. For more information about managing pSeries servers, see Auto Discovery for HMC-Managed pSeries Servers.
Virtual Node	An agentless device that Uptime Infrastructure Monitor can communicate with using an IP address.
VMware ESX	A system that is running 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. This is a legacy option for users running older (version 3 or 4) ESX versions independent of a VMware vCenter management tool. Normally, users would add a VMware vCenter Server as an Element to monitor ESX hosts and VMs.
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 Uptime Infrastructure Monitor 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 Uptime Infrastructure Monitor Agent installed on it. WMI-based monitoring only works if the Monitoring Station is running on Windows.

You can add multiple systems to Uptime Infrastructure Monitor in a batch operation using a text file and a command line utility. For more information about using multiple systems, see Adding Multiple Systems.

Adding Systems or Network Devices

To add systems or network devices, do the following:

1. In the Infrastructure panel, click **Add System/Network Device**.
2. Enter a descriptive name for the server in the **Display name in Uptime** field.
   This name appears in the Uptime Infrastructure Monitor 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 Uptime Infrastructure Monitor, but a more descriptive or meaningful name is displayed in the Uptime Infrastructure Monitor Web interface.
3. Optionally, enter a description of the system in the **Description** field.
4. Select the **Type of System/Device** from the list:
   - Agent
   - Hyper-V Server
   - Net-SNMP v2
   - Net-SNMP v3
   - Network Device
   - Novell NRM
   - pSeries LPAR Server (HMC)
   - pSeries LPAR Server (VIO)
   - 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.
   You can use the actual name or IP address of the machine as the host name.
6. Configure the system- or device-specific settings. The options depends on the system or device type you selected in step 4:
   - **Agent**
     Configure the following:
     - **Port**
       The port on which the Uptime Infrastructure Monitor Agent is listening.
     - **Use SSL**
       Select this check box if you want to securely communicate with the Uptime Infrastructure Monitor Agent.

     Use the Global Credentials Settings page on the Config tab to globally configure the Uptime Infrastructure Monitor Agent information. If this step is complete, and the **Use Uptime Agent Global Configuration** check box is selected, the agent port and SSL options do not appear. For more information about supported platforms for an agent, see Supported Agent Platforms.

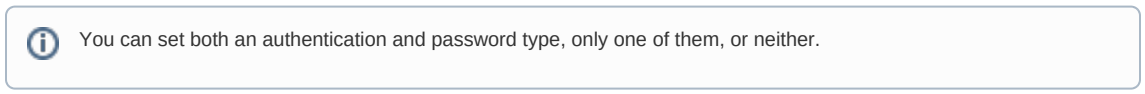
   - **Hyper-V Server**
     Enter information in the following fields:
     - **Windows Domain**
       The Windows domain in which the Hyper-V server resides.
     - **Username** and **Password**
       The username and associated password of the Hyper-V server administrator account.

       Use the Global Credentials Settings page on the Config tab to globally configure the Uptime Infrastructure Monitor Hyper-V information. If this step is complete, and the **Use Hyper-V Global Credentials** check box is selected, the Windows domain and user credentials options do not appear.

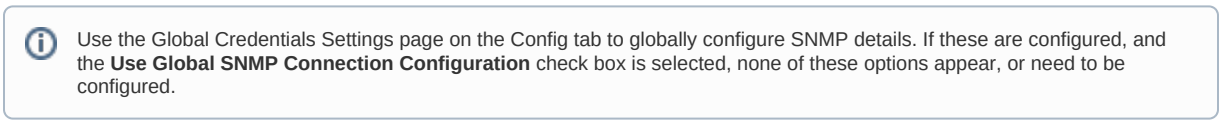
     - In the **Sync Settings - Virtual Machines** section, indicate whether you would like Uptime Infrastructure Monitor to **Collect Virtual Machine data**.
       If you choose to ignore VMs in the Hyper-V inventory by clearing this check box, skip to the next configuration point; otherwise, configure how Uptime Infrastructure Monitor's Sync works with a Hyper-V server's inventory of VMs.
       - Select the **Collect Uptime Agent data** or **Collect WMI Agentless data** (if you are using data collection via WMI) to enable additional monitoring for VMs that are using the Uptime Infrastructure Monitor Agent or WMI. For more information about managing VM monitoring, see Standalone Monitoring for Virtual Machines. If you have defined global Agent or WMI settings in the Uptime Infrastructure Monitor Config panel, you can select the **Use Uptime Agent Global Configuration** or **Use WMI Global Configuration** check box accordingly; otherwise, configure the appropriate fields:
         - For the Uptime Infrastructure Monitor Agent, indicate the **Port** on which it is listening, and whether it uses SSL to communicate securely with Uptime Infrastructure Monitor.

        - For data collection via WMI, indicate the **Window Domain** on which WMI is implemented, and the **Username** and **Password** required for access.
    - Indicate whether Uptime Infrastructure Monitor should **Notify on newly discovered VMs**, then select the desired **Alert Profile** and **Action Profile**.
      If enabled, Uptime Infrastructure Monitor can send notifications about, or perform scripted actions in response to, new VMs discovered in the Hyper-V inventory during a Sync operation. For more information about Sync, see Managing Sync / vSync.

- **Net-SNMP v2**
  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).
- **Net-SNMP v3**
  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 determines how encrypted information traveling between the Net-SNMP instance and Uptime Infrastructure Monitor is 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 used to encrypt information traveling between the Net-SNMP instance and Uptime Infrastructure Monitor.
    - **Privacy Type** (optional)
      From the list, select one of the following options that determines how information traveling between the Net-SNMP instance and Uptime Infrastructure Monitor is 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.

      
      You can set both an authentication and password type, only one of them, or neither.

- **Network Device** (using version 2 of the SNMP protocol)
  By default, the network device's **SNMP Version** is set to **v2**; 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 (enabling you to retrieve read-only information from the device) and private (enabling you to access all information on the device).
    - **Is Device Pingable?**
      This option specifies whether Uptime Infrastructure Monitor can contact the network device using the ping utility.
      There are scenarios in which you might not want the network device to be pingable (e.g., you have a firewall in place). Before selecting this check box, you should try to contact the network device using the ping utility. If you cannot ping it, ensure the check box is left cleared. Then, change the default host check for the network device. For more information about managing host checks, see Changing Host Checks.

  
  Use the Global Credentials Settings page on the Config tab to globally configure SNMP details. If these are configured, and the **Use Global SNMP Connection Configuration** check box is selected, none of these options appear, or need to be configured.

- **Network Device** (using version 3 of the SNMP protocol)
  If your network device 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 determines how encrypted information traveling between the network device and Uptime Infrastructure Monitor is 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 is used to encrypt information traveling between the network device and Uptime Infrastructure Monitor.
    - **Privacy Type** (optional)
      From the list, select an option that determines how information traveling between the network device and Uptime Infrastructure Monitor is 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.

      > You can set both an authentication and password type, only one of them, or neither.

    - **Is Node Pingable?**
      This option specifies whether Uptime Infrastructure Monitor can contact the network device using the ping utility.
      There are scenarios in which you might not want the network device to be pingable (e.g., you have a firewall in place). Before selecting this check box, you should try to contact the network device using the ping utility. If you cannot ping it, ensure the check box is left cleared. Then, change the default host check for the network device. For more information about managing host checks, see Changing Host Checks.

  > Use the Global Credentials Settings page on the Config tab to globally configure SNMP details. If these are configured, and the **Use Global SNMP Connection Configuration** check box is selected, none of these options appears, or need to be configured.

- **Novell NRM**
  Complete the following fields:
    - **Port**
      The port on which the NRM is listening. By default, the non-SSL port is 8008, and when SSL is used, the port is 8009.
    - **Use SSL**
      Select this check box if you want to securely communicate with the NRM.
    - **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.
- **pSeries LPAR Server (HMC)**
  If you are adding a pSeries server that is managed by a Hardware Management Console, complete the following fields:

  > Although you can manually add HMC-managed pSeries servers, we recommend using the Auto Discovery process as this adds all the pSeries servers managed by the HMC, and automatically populates the respective managed server names. For more information about managing pSeries servers, see Auto Discovery for HMC-Managed pSeries Servers.

    - **HMC Host Name**
      The host name of the Hardware Management Console that is managing the pSeries server.
    - **Managed Server**
      The HMC's unique identifier for the pSeries server. This information can be retrieved from the HMC itself (e.g., by running `lssyscfg -r sys -F name`).

      > For HMC-managed pSeries servers, the above two fields are used in conjunction with the `Host Name` field. The pSeries `Host Name` and Managed Server name identify the p frame on the network, and within the HMC cluster, respectively. The `HMC Host Name` is required to identify the Hardware Management Console in order to retrieve some configuration and workload information about the pSeries server.

    - **Username**
      The username required to log in to the HMC.
    - **Password**
      The password used to access the HMC.
- **pSeries LPAR Server (VIO)**
  If you are adding a pSeries server that is not managed by an HMC, but instead communicates with the Uptime Infrastructure Monitor Agent on a Virtual I/O server that's using IVM (Integrated Virtual Manager), configure the following:
    - **Port**
      The port on which the Uptime Infrastructure Monitor Agent is listening.
    - **Use SSL**
      Select this check box if you want to securely communicate with the Uptime Infrastructure Monitor Agent.

  > Use the Global Credentials Settings page on the Config tab to globally configure information for the Uptime Infrastructure Monitor Agent on the Virtual I/O server. If this is done, and the **Use Uptime Agent Global Configuration** check box is selected, the agent port and SSL options do not appear.

- **VMware ESX**
  Complete the following fields:
  - **Username**
    The user name required to log into the VMware ESX server.
  - **Password**
    The password required to log into the VMware ESX server.
- **VMware vCenter Server**
  Complete the following fields:
  - **Web Services Port**
    The port that the VMware vCenter Web Service uses to communicate with Uptime Infrastructure Monitor.
  - **Username**
    The name of the VMware vCenter administrator account.
  - **Password**
    The password for the VMware vCenter account.
  - In the **vSync Settings - Virtual Machines** section, indicate whether you would like Uptime Infrastructure Monitor to **Collect Virtual Machine data**.
    If you choose to ignore VMs in the VMware vCenter inventory by clearing this check box, skip to the next configuration point; otherwise, configure how Uptime Infrastructure Monitor's vSync works with a vCenter's inventory of VMs.
    - Select the **Collect Uptime Agent data** or **Collect WMI Agentless data** (if you are using data collection via WMI) to enable additional monitoring for VMs that are using the Uptime Infrastructure Monitor Agent or WMI. For more information about managing VM monitoring, see Standalone Monitoring for Virtual Machines. If you have defined global Agent or WMI settings in the Uptime Infrastructure Monitor Config panel, you can select the **Use Uptime Agent Global Configuration** or **Use WMI Global Configuration** check box accordingly; otherwise, configure the appropriate fields:
      - For the Uptime Infrastructure Monitor Agent, indicate the **Port** on which it is listening, and whether it uses SSL to communicate securely with Uptime Infrastructure Monitor.
      - For data collection via WMI, indicate the **Window Domain** on which WMI is implemented, and the **Username** and **Password** required for access.
    - Indicate whether Uptime Infrastructure Monitor should **Notify on newly discovered VMs**, then select the desired **Alert Profile** and **Action Profile**.
      If enabled, Uptime Infrastructure Monitor can send notifications about, or perform scripted actions in response to, new VMs discovered in the VMware vCenter inventory during a vSync operation. For more information about vSync, see Managing Sync / vSync.
  - **vSync Settings - vSphere ESX Hosts** section, indicate whether Uptime Infrastructure Monitor should **Notify on new discovered hosts**, and then select the desired **Alert Profile** and **Action Profile**.
    If enabled, Uptime Infrastructure Monitor can send notifications about, or perform scripted actions in response to, new ESX hosts discovered in the VMware vCenter inventory during a vSync operation. For more information about vSync, see Managing vSync.
- **WMI Agentless**
  Complete the following fields:
  - **Windows Domain**
    The Windows domain in which WMI is 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.

> WMI information can be globally configured in the Global Credentials Settings page on the Config tab. If this is done, and the **Use WMI Global Credentials** check box is selected, none of these options appears, or needs to be configured.

7. If you want to associate this system with a group, select the name of the group from the **Group** dropdown list. For more information about defining groups, see Working with Groups.
8. If you want to associate this system with a service group, select the name of the group from the **Service Group** dropdown list. For more information about defining service groups, see Service Groups.
9. Click **Save**.
   A window listing general information about the system you have added appears.
10. If you want to add another system or network device, click **Add Another**. Then, repeat the previous steps in this section. Otherwise, click **Close**.
11. Click **Save**.

Adding VMware Instances to Uptime Infrastructure Monitor

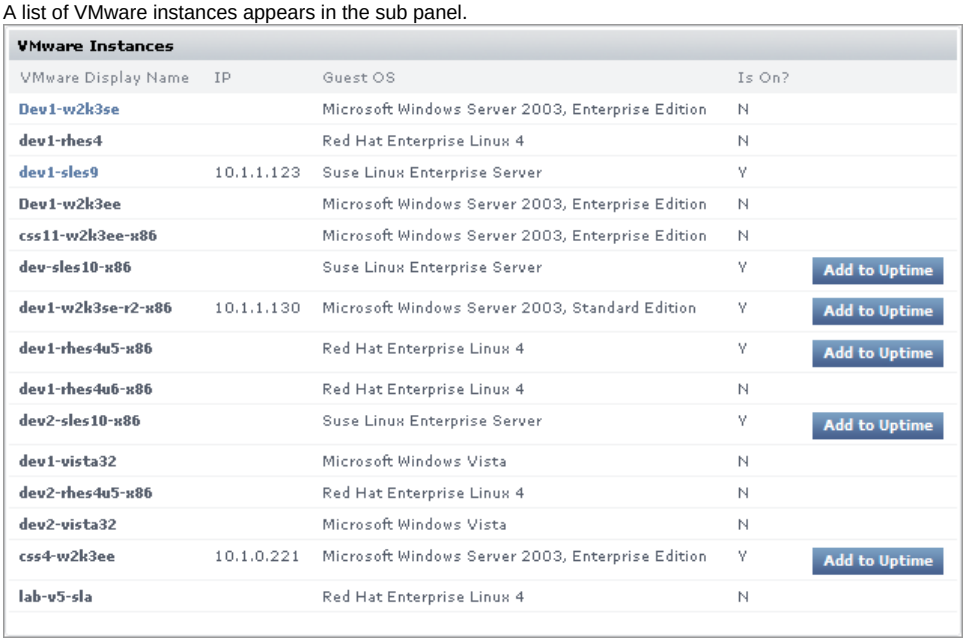
Uptime Infrastructure Monitor can monitor both a VMware ESX server, as well as VMware instances.

> Ideally, VMware instance monitoring is performed by adding an entire VMware vCenter server and allowing Uptime Infrastructure Monitor's auto-discovery process to add all of its inventory (including ESX servers and VMware instances). However, as a legacy option, you can manually add an ESX server to Uptime Infrastructure Monitor's monitored inventory, and then manually add VMware instances.

To add VMware instances to Uptime Infrastructure Monitor from an ESX Server that was manually added as an Uptime Infrastructure Monitor Element, do the following:

1. In the 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.

2. Click the **Info** tab, and then click **VMware Instances**.
   A list of VMware instances appears in the sub panel.



VMware Instances

VMware Display Name	IP	Guest OS	Is On?	
Dev1-w2k3se		Microsoft Windows Server 2003, Enterprise Edition	N	
dev1-rhes4		Red Hat Enterprise Linux 4	N	
dev1-sles9	10.1.1.123	Suse Linux Enterprise Server	Y	
Dev1-w2k3ee		Microsoft Windows Server 2003, Enterprise Edition	N	
css11-w2k3ee-x86		Microsoft Windows Server 2003, Enterprise Edition	N	
dev-sles10-x86		Suse Linux Enterprise Server	Y	Add to Uptime
dev1-w2k3se-r2-x86	10.1.1.130	Microsoft Windows Server 2003, Standard Edition	Y	Add to Uptime
dev1-rhes4u5-x86		Red Hat Enterprise Linux 4	Y	Add to Uptime
dev1-rhes4u6-x86		Red Hat Enterprise Linux 4	N	
dev2-sles10-x86		Suse Linux Enterprise Server	Y	Add to Uptime
dev1-vista32		Microsoft Windows Vista	N	
dev2-rhes4u5-x86		Red Hat Enterprise Linux 4	N	
dev2-vista32		Microsoft Windows Vista	N	
css4-w2k3ee	10.1.0.221	Microsoft Windows Server 2003, Enterprise Edition	Y	Add to Uptime
lab-v5-sla		Red Hat Enterprise Linux 4	N	

3. Click the **Add to Uptime** button for the instance you wish to add.
   The **Add System** window appears.

> The **Add to Uptime** button is not visible if the VMware instance is not powered on.

4. If necessary, you can change any of the following options:
   - **Display name in Uptime**
   - **Description**
   - **Group**
   - **Service Group**
5. Click **Save** to add the instance to Uptime Infrastructure Monitor.

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 Uptime Infrastructure Monitor 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 Uptime Infrastructure Monitor. For more information, see Adding Systems or Network Devices.

Supported Versions of SNMP

The Uptime Infrastructure Monitor 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 Uptime Infrastructure Monitor

After you have added pSeries servers, whether managed by an HMC, to Uptime Infrastructure Monitor, you can add individual LPARs from those systems to Uptime Infrastructure Monitor. While Uptime Infrastructure Monitor collects workload data from all LPARs on a pSeries server (whether they were added to Uptime Infrastructure Monitor), adding LPARs can help you keep track of any specific LPAR.

To add an LPAR to Uptime Infrastructure Monitor, do the following:

1. In the 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 Uptime** button beside the LPAR that you want to add to Uptime Infrastructure Monitor.
   The Add System window appears.
4. If necessary, you can change any of the following options:
   - **Display name in Uptime**
   - **Description**
   - **Group**
   - **Service Group**
5. Click **Save** to add the LPAR to Uptime Infrastructure Monitor.

> 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 Uptime Infrastructure Monitor Agent. Using WMI allows you to avoid the overhead associated with managing and updating all of the systems on which an Uptime Infrastructure Monitor Agent is installed.

> 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 Uptime Infrastructure Monitor
- its system type was set to "Agent" when originally added to Uptime Infrastructure Monitor, but is 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. Consult the Microsoft documentation or developer resources for information on connecting to WMI on a remote computer. For more information about supported platforms when using agentless monitoring, see Supported Platforms via Agentless Monitoring.

Adding a WMI System to Uptime Infrastructure Monitor

To add an agentless WMI system to Uptime Infrastructure Monitor, do the following:

1. On the Uptime Infrastructure Monitor tool bar, click **Infrastructure**, then click **Add System/Network Device**.
2. Complete the **Display name in Uptime** 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 Uptime Infrastructure Monitor is monitoring.
5. Select the **Use WMI Global Credentials** check box if they are configured, and you would like to use them (see Configuring Global WMI Credentials for more information); otherwise complete the following fields:
   If you want to associate this system with a group, select its name from the **Group** dropdown list.
   - **Windows Domain**
     The Windows domain in which WMI is 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 Service Group, select its name in the **Service Group** dropdown list.
7. Click **Save**.

Switching an Element to WMI Data Collection

To change the data collection source for an individual Windows Element from the Uptime Infrastructure Monitor Agent to WMI, do the following:

1. On the **Global Scan** dashboard or **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 are 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 is 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 Uptime Infrastructure Monitor Agent, do the following:

1. On the **Global Scan** dashboard or **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 **Uptime Agent** data collection option.
5. Select the **Use Uptime Agent Global Configuration** check box if it is configured, and you would like to use it (see Configuring a Global Uptime Infrastructure Monitor Agent Configuration for more information); otherwise complete the following options:
   - **Port**
     The port through which the Uptime Infrastructure Monitor Agents communicate with the Uptime Infrastructure Monitor 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 are set (see Configuring Global WMI Credentials for more information).
2. On the Uptime Infrastructure Monitor 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 is refreshed to reflect the changes.

Converting Multiple Elements to Agent-Based Data Collection

To change multiple WMI Elements to use the Uptime Infrastructure Monitor Agent for data collection, do the following

1. Ensure a global Uptime Infrastructure Monitor Agent configuration exists (see Configuring a Global Uptime Infrastructure Monitor Agent Configuration for more information).
2. On the Uptime Infrastructure Monitor 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 Uptime Infrastructure Monitor Agent.
5. Click **Convert to Agent**.
   When the conversion is complete, the lists of agent-based and WMI Elements is refreshed to reflect the changes.

For bulk WMI-to-agent conversions, the port used by all of the converted Uptime Infrastructure Monitor Agents must match the port specified in the global agent configuration.

Novell NRM Systems

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

Adding a Novell NRM System to Uptime Infrastructure Monitor

To add a Novell NRM version 6.5 system to Uptime Infrastructure Monitor, do the following:

1. On the Uptime Infrastructure Monitor tool bar, click **Infrastructure** and then click the **Add System/Network Device** tab.
2. Complete the **Display name in Uptime** 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 or IP address of the machine that Uptime Infrastructure Monitor should monitor.
   - **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 *8009*.
   - **Username**
     The NRM administrator account name. This field is mandatory.
   - **Password**
     The NRM administrator password. This field is mandatory.

     
     The password is encrypted and stored in the Uptime Infrastructure Monitor 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 Uptime Infrastructure Monitor

Uptime Infrastructure Monitor 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. Uptime Infrastructure Monitor 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

Uptime Infrastructure Monitor monitors connections on a per-server basis. NRM displays only the following metrics:

- the number of connections that are 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 is sluggish. If the number of Packet Receive Buffers reaches the maximum, and no Event Control Blocks (ECBs) are available, the server becomes very sluggish and does 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 were created but which are not currently used.

If the available ECB count is zero, the server becomes sluggish until enough ECBs are created to fill the demand. The server recovers as long as the number of Packet Receive Buffers does not increase to the maximum that you can allocate.

LAN Traffic

This statistic shows whether 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 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 were 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 were taken.

Adding Multiple Systems

It can be time consuming to add large numbers of systems and network devices to Uptime Infrastructure Monitor individually through the Web interface. You can, however, add multiple systems to Uptime Infrastructure Monitor using a text file and the `addsystem` command line tool.

A text-based "hosts file" can contain entries that mirror the fields in Uptime Infrastructure Monitor's **Add System** window; these fields provide profile and connection information about the system or network device. The hosts file format is as follows:

- A series of name-value pairs. Each name-value pair is separated by a colon, and is on a separate line.
- The information for each host is separated by a pair of percentage signs (%%), and is also on its own separate line.

Hosts File Name-Value Pairs

The following table explains the properties you can include in a host file to describe Elements. The properties required to add a system or network device depends on the type of Element you want. For example, to add an Agent-based system, you only need to provide information for `Host Name`, `Type`, and `Port`. (For more information, see Working with Elements for a summary of Element types, and Adding Systems or Network Devices for configuration information by Element type.)

Element Property	Description	Required / Optional
`Host Name`	The name or IP address of the Element (i.e., system or network device) that you are adding to Uptime Infrastructure Monitor.	required
`Display Name`	The Element name as you want it to appear in the Uptime Infrastructure Monitor Web interface. There are some views, such as **Infrastructure**, that display the host name alongside the display name.	required, but can be identical to the `Host Name` value
`Description`	A short description of the Element. This field is optional.	optional
`Type`	The type of Element, which can be one of the following: • `Agent` • `Hyper-V` • `Novell NRM` • `Net-SNMP v2` • `Net-SNMP v3` • `pSeries LPAR Server (HMC)` • `Virtual Node` • `VMware ESX` • `WMI Agentless`	required
`Service Group`	The name of the Uptime Infrastructure Monitor service group to which you want to add the Element. Service groups allow you to group multiple service monitors and simultaneously apply them to multiple Elements. (See Service Groups for more information.)	optional
`Port`	The port on which Uptime Infrastructure Monitor connects to the Element. When a port is required, Uptime Infrastructure Monitor uses a default whose value depends on the type of Element (e.g., network devices defaults to an SNMP port of 161).	required for these Element types: • Agent • Hyper-V • Network Device • Novell NRM • Net-SNMP v2 • Net-SNMP v3 • VMware vCenter • WMI Agentless
`Community`	If the Element is a network device or a server using version 2 of the Net-SNMP protocol, you must specify the read community, which acts like a user ID or password, in order to access the system or device. Use one of the following options: • `public`: enables you to retrieve read-only information • `private`: enables you to access all information	required for network devices or servers using version 2 of the Net-SNMP protocol
`HMC Hostname`	The name or IP address of the Hardware Management Console (HMC) that is used to manage one or more pSeries servers in your infrastructure. For pSeries servers, this field is used in conjunction with the `Managed Server`, as well as `Host Name` fields.	required for pSeries servers managed by an HMC
`Managed Server`	The unique identifier for a pSeries server that is managed by an HMC. This managed server name can be retrieved from the HMC itself (e.g., by running **`lssyscfg -r sys -F name`**). For pSeries servers, this field is used in conjunction with the `Host Name` and `HMC Host Name` fields.	required for pSeries servers managed by an HMC

`Username`	The username required to access the Element.	required for the following Element types: • Hyper-V • Network Device (using version 3 of the Net-SNMP protocol) • Novell NRM • Net-SNMP v3 • pSeries LPAR Server (HMC) • VMware ESX • VMware vCenter
`Password`	The password required to access the Element.	required for the following Element types: • Hyper-V • Novell NRM • pSeries LPAR Server (HMC) • VMware ESX • VMware vCenter Server
`Group`	The name of the Uptime Infrastructure Monitor infrastructure group to which you want to add the Element. Infrastructure groups help you organize all of your monitored systems and network devices. (See Working with Groups for more information.)	optional
`SSL`	For some types of servers, you can specify whether Uptime Infrastructure Monitor securely communicates with an installed Agent using SSL. Valid options are `true` and `false`. By default, SSL is not enabled.	optional for the following Element types: • Agent • Novell NRM • pSeries LPAR Server (VIO)
`Authentication Method`	If the Element is a network device or server using version 3 of the Net-SNMP protocol, you must specify an authentication method to determine how encrypted information traveling between the Net-SNMP instance and Uptime Infrastructure Monitor is authenticated. Use one of the following options: • `MD5`: a widely-used method for creating digital signatures • `SHA`: a secure method of creating digital signatures	required for network devices or servers using version 3 of the Net-SNMP protocol
`Privacy Password`	If the Element is a network device or server using version 3 of the Net-SNMP protocol, you must specify the password used to encrypt information traveling between the Net-SNMP instance and Uptime Infrastructure Monitor.	required for network devices or servers using version 3 of the Net-SNMP protocol
`Privacy Type`	If the Element is a network device or server using version 3 of the Net-SNMP protocol, you must specify how information traveling between Uptime Infrastructure Monitor and the Net-SNMP instance is encrypted. Use one of the following options: • `DES`: an older method used to encrypt information • `AES`: the successor to DES, which is used with a variety of software, including SSL servers	required for network devices or servers using version 3 of the Net-SNMP protocol
`Pingable`	For network devices and nodes, use this field to specify whether Uptime Infrastructure Monitor can contact it using the ping utility. Valid options are `true` and `false`. By default, the this field is set to `false`.	optional for network devices and nodes
`WMI Domain`	For Windows-based Elements using WMI for data collection, the Windows domain in which WMI is implemented.	required for WMI Agentless
`WMI Username`	For Windows-based Elements using WMI for data collection, the name of the account with access to WMI on the Windows domain.	required for WMI Agentless
`WMI Password`	For Windows-based Elements using WMI for data collection, the password for the account with access to WMI on the windows domain.	required for WMI Agentless

Examples of Hosts File Entries

The following table contains sample host file entries for different Element types that you can add to `Uptime Infrastructure Monitor`:

Host Type	Sample Hosts File Entry

Agent	Host Name: prod-mainSystem Display Name: prod1 Description: Main production server Type: Agent Service Group: Production Systems Port:9998 Group: Windows 2003 Servers
Novell NRM	Host Name: novell01 Display Name: dn3 Type: Novell NRM SSL: true Port: 546 Group: Unix Boxes Group: Novell System
Net-SNMP v2	Host Name: gateway.mydomain.com Display Name: gatewaySNMP Description: snmp v2 Type: Net-SNMP v2 Read Community: myCo-pub
Net-SNMP v3	Host Name: SNMP-1 Display Name: SNMP-1 Description: Net-SNMP system Type: Net-SNMP v3 Read Community: public Username: myUsername Password: myPassword Privacy Password: myOtherPassword Group: Linux Systems
pSeries LPAR	Host Name: 10.1.2.42 Display Name: HMC Managed Server HMC Hostname: 10.1.1.255 Type: pSeries LPAR Server (HMC) Managed Server: Server-7610-31C-SN01B030K Username: hscroot Password: hscroot
Virtual Node	Host Name: router-Toronto Display Name: Toronto Router Description: Router for Toronto branch Type: Virtual Node Pingable: True Group: Routers
WMI Agentless	Host Name: Win7-Production Display Name: Windows 7 Production Description: Win7 agentless/WMI Type: WMI Agentless Group: Windows Boxes WMI Domain: windomain WMI Username: administrator WMI Password: password

Creating a Hosts File

The simplest way to create a hosts file 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 keep a list of all systems and network devices in a spreadsheet. You can then save the list as a text file or a comma-separated values file, then use a script to manipulate these files into the proper format.

Adding Multiple Systems to Uptime Infrastructure Monitor

To add multiple systems to Uptime Infrastructure Monitor, do the following:

1. Copy the hosts file to the directory in which you installed the Uptime Infrastructure Monitor 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, and full path to, the text file that contains the list of systems that you want to add to Uptime Infrastructure Monitor.
   The systems listed in the file are added to Uptime Infrastructure Monitor, unless one of the following occurs:

- Uptime Infrastructure Monitor cannot connect to the system
- the system does not exist in your environment
- the system is already added to Uptime Infrastructure Monitor

> If you have deployed Uptime Infrastructure Monitor UI instances, ensure you always run command-line scripts such as `addsystem` on the primary Monitoring Station that is actually performing data collection.

Editing a System Profile

After you have added a system to Uptime Infrastructure Monitor, 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 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 Uptime**
     The descriptive name for the system that appears in the Uptime Infrastructure Monitor Web interface.
   - **Description**
     A brief functional description of the system.
   - **Parent Group**
     Select the group of systems in Uptime Infrastructure Monitor that you want to associate with this system.
   - **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 Uptime Infrastructure Monitor retrieves. If you select 10 processes, and there are 20 running on the system, Uptime Infrastructure Monitor retrieves the 10 busiest processes.
   - **Is monitored?**
     Click this checkbox to turn off monitoring for this system. If monitoring is turned off, the system does not appear on the **Global Scan** dashboard.
3. Click **Save**.

Working with Applications

An Application is comprised of one or more service monitors, and is an effective way to monitor and report on business functions that are most accurately represented by multiple services. For example, you can create an Application that monitors a server's Web services, database, and file system capacity.

An Application definition can include as many service monitors as required to fully represent the business function. As part of an Application definition, service monitors can be one of two types:

- master service monitor: used to determine the status of the Application as a whole
- regular service monitor: does not affect Application status, but helps provide a complete picture by representing a secondary service, or a direct dependency of a master service

All master service monitors affect Application status equally, using their respective configured thresholds. You can configure an Application to reach a warning- or critical-level status as a whole using one of the following conditions:

- when any master service monitor violates its threshold
- only when all master service monitors violate respective thresholds
- when a fixed number of master service monitors violates respective thresholds
- when a percentage of master service monitors violates respective thresholds

Note that Applications are meant to report as OK, WARN, or CRIT; Application status is not affected by component service monitors that are in an UNKNOWN or MAINT state. (Note, however, that an Application as a whole can be put into temporary maintenance via **Infrastructure**.)

The ability to control the total number of service monitors, as well as the number that need to violate thresholds before affecting the Application's collective status allows you to give different Applications varying levels of robustness. As a result, each of your Applications provides the most accurate status possible, with fewer false positives. For example, a Web server cluster of 10 servers might only cause alerts when three or more of them are down, whereas a mission-critical application causes an alert when any of its master service monitors fail.

Viewing Details About Applications

After you have added an Application to Uptime Infrastructure Monitor, the name of the Application appears in the **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 the Application is 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 monitored
- the host that the service monitor is attached to
- whether the service is a master service monitor

The **Alert Profiles** and **Action Profiles** sections of the subpanel displays which Alert Profiles and Action Profiles are associated with the Application.

Adding Applications

To add an Application, do the following:

1. In the Infrastructure panel, click **Add Application**.
2. In the **Add Application** window, enter a descriptive name in the **Name of Application** field.
   This name appears in both the Infrastructure panel and Global Scan dashboard.
3. Optionally, enter a description in the **Description of Application** field.
4. Optionally, select the group of systems in your Uptime Infrastructure Monitor environment with which this system is associated from the **Parent Group** dropdown list.
   By default, the Application is added to the 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 **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**.

Editing Applications

To edit an Application, do the following:

1. In the 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 Uptime Infrastructure Monitor, 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 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 are combined in a meaningful way.

You can group systems by their geographical location or by their function. The name of the group describes the servers or they way in which they are 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)

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

Adding Groups

To add a group, do the following:

1. On the 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 becomes subordinate in the **Parent Groups** list, then click **Add**.

   If this is the first group that you have defined, only Infrastructure appears 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 Uptime Infrastructure Monitor 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.

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

To add a nested group, do the following:

1. In the 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 group becomes 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 Infrastructure panel.

Working with Views

Not every user who 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 sees 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** dashboard.

Adding Views

To add a view, do the following:

1. In the Infrastructure tree panel, click **Add View**.
2. In the **Add View** window, enter a descriptive name in the **View Name** field.
   This name appears 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.

   If this is the first group that you have defined, this option does not appear.

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 organized any of your Elements into groups, these are listed in a dropdown. Selecting an Element group displays member Elements you can add to the view. You can also select the **All** view to display all Elements in your environment as a flat list.
7. Select one or more entries from the **Available User Groups** list, then click **Add**.
8. 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
- Uptime Infrastructure Monitor user groups with similar privileges

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

> 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 appears 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 is 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 **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 Uptime Infrastructure Monitor, do the following:

1. In the *Infrastructure* panel, locate the Element or Uptime Infrastructure Monitor 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*.

> You can only delete Elements that were created in Uptime Infrastructure Monitor. You cannot manually remove Elements that represent Hyper-V components imported via Sync or VMware vSphere components imported via vSync.

Acknowledging Alerts

When a problem occurs on a system that Uptime Infrastructure Monitor 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, Uptime Infrastructure Monitor:

- records the acknowledgement, which can be viewed in the Service Monitor Outages report
- sends an acknowledgement message to any Uptime Infrastructure Monitor 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.
   The *System General Information* subpanel appears.
2. In the *Tree* panel, click the *Services* tab and then click Status.
   Status information for the monitors associated with the Element appears in the subpanel.

3. Click the *Acknowledge* icon in the Ack column.
   The acknowledgement message window appears.
4. Type a comment relating to the alert or why it was acknowledged, and then click *Submit*.
   An email containing the following information is sent to any Uptime Infrastructure Monitor user who received the last alert:
   - the user name and email address of the person who acknowledged the alert
   - the name of the Element and service monitor involved
   - a comment relating to the alert or reason for acknowledgement

   The following is a sample alert acknowledgement message:
   Uptime Infrastructure Monitor Administrator (jsmith@myDomain.com)
   acknowledged the WARN status of File System Capacity (Web Server 2) with comment:
   Initial check of problem. More information to come.
5. In the Uptime Infrastructure Monitor Web interface, the acknowledge icon changes.