

# GWNMS Cacti

## Contents

This section reviews the GroundWork Monitor NMS Cacti.

### 1.0 About Cacti

The GroundWork NMS Cacti package is an open source toolkit for graphing network resources, and is integrated into GroundWork Monitor as an optional component of the GroundWork Network Management Suite (NMS). When the GroundWork NMS Cacti package has been installed, a "Cacti" menu item will be present in the main drop-down menu.

In simple terms, Cacti is an integrated toolkit that periodically measures the resource utilization levels of selected network devices and then publishes dynamic, user-defined graphs from that data. Whereas most of the components in GroundWork Monitor are designed for the purpose of monitoring the devices on a network (such as measuring the available resources on a host and then generating alarms when conditions require it), Cacti is primarily designed to help administrators visualize the resource utilization of the network devices.

More specifically, Cacti uses an open-ended polling engine to take timed sample readings from user-specified devices, stores those readings in a set of dynamic databases, and provides tools that allow administrators to build highly customized graphs of the collected data. From there, administrators can use the Cacti web interface to display historical graphs about the various resources on their network, and can build new graphs that combine data in multiple ways to further assist in visualizing the overall state of the network. In addition, Cacti supports plugins that allow it to be extended with additional capabilities, such as device discovery and basic alarms, which further contribute to the visualization feature set.

This document discusses the basic configuration and operation of Cacti. For more detailed discussion, refer to the [online Cacti documentation](#).

### 2.0 Configuring the Cacti Package

The GroundWork NMS Cacti package has its own unique configuration process.

#### 2.1 Managing User Access

The Cacti web pages are provided by a NMS-specific instance of Apache, although the Cacti web front-end is also integrated into GroundWork Monitor through the use of the JBoss Portal. As such, users who have been granted the appropriate role-based permission to access the Cacti object can do so by logging into GroundWork Monitor, and then choosing the "Cacti" entry from the main drop-down menu.

However, Cacti also has its own separate user accounts and access controls, which are independent of the GroundWork Monitor controls. More specifically, Cacti only has a single predefined administrative user account, with the username of "admin" and the password of "admin". Furthermore, most of the built-in web pages are unrestricted, and do not require any authentication. If you want to restrict access to the Cacti web server or some of its web pages, you may need to create the appropriate user accounts and access controls within Cacti.



This process is separate from the process of determining which users have access to the "Cacti" item in the GroundWork Monitor main menu. For information on configuring user access to the "Cacti" menu item, refer to [System Administration](#) documentation.

#### 2.2 Managing User Accounts

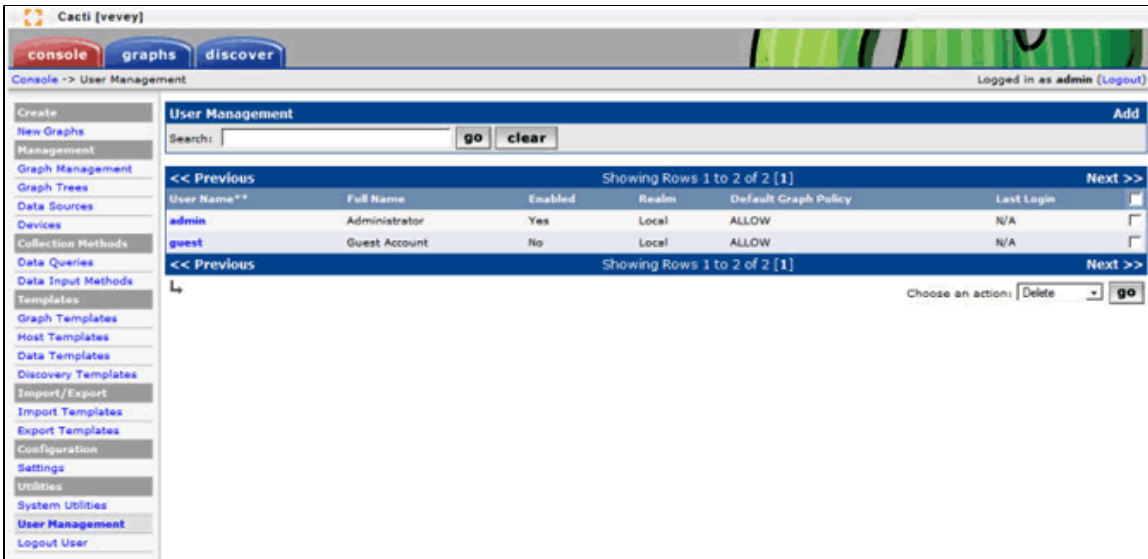
The GroundWork NMS Cacti package includes technology that automatically creates a user account in Cacti whenever that user first accesses Cacti through GroundWork Monitor. As such, user accounts do not need to be explicitly created in Cacti in order for users to access those pages. However, it may sometimes be necessary to manage the user accounts directly.

If you wish to create a new user account in Cacti; you can either add a new account from scratch or you can copy an existing account. Accounts that are created by copying an existing account inherit the attributes and access controls of the original account. Meanwhile, accounts that are created from scratch inherit the attributes and access controls associated with the "default" user account.

By default, Cacti uses the Guest user account as the default template for new user accounts. To select a different account for the new user template, click on the "Settings" menu item in the left navigation bar, click on the "Authentication" tab of the resulting screen, choose an existing user account from the "User Template" drop-down box, and then click the "Save" button at the bottom of the screen.

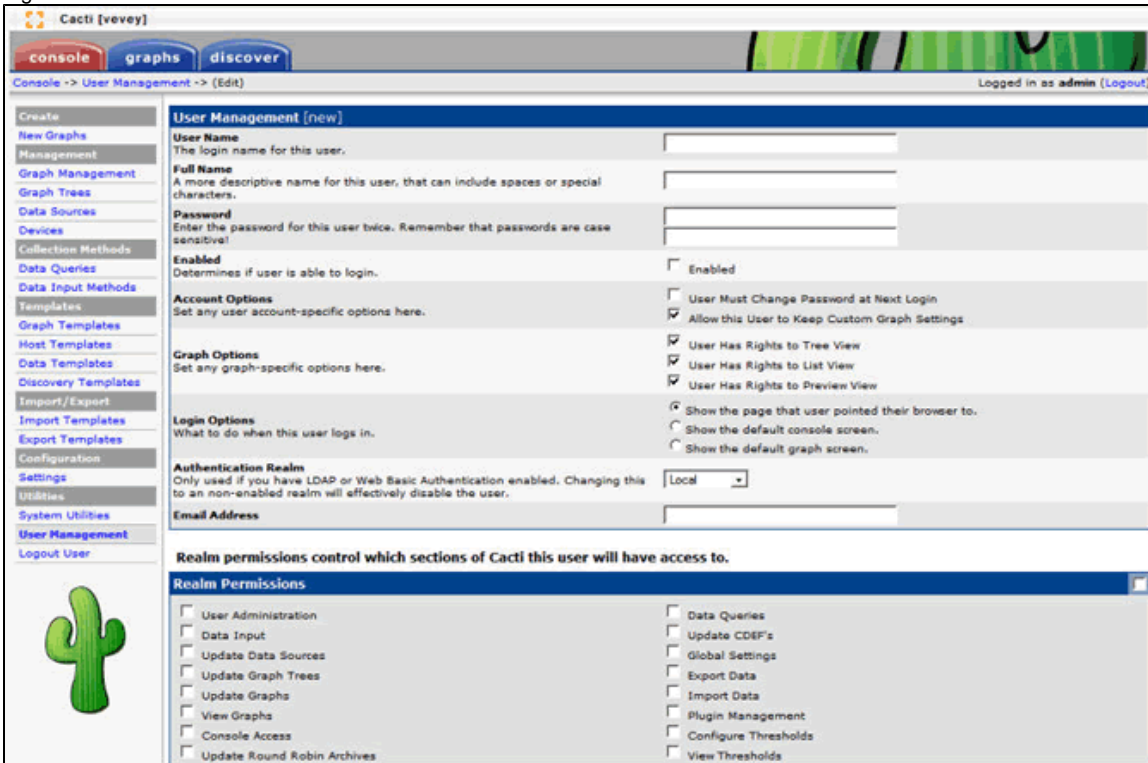
To create the user accounts, click on the "User Management" menu item in the left navigation bar. You will then be presented with a screen that lists the currently defined user accounts, similar to the following:

Figure: User Accounts



To create a new user account with the default settings, click the "Add" hyperlink in the top right corner. A new screen will be displayed that allows you to specify the account name, the user's full name, the user's password, and so forth, similar to the following:

Figure: New User Accounts



Once you are finished setting the account details, click the "create" button in the bottom right corner.

If you wish to simply copy an existing user account and its settings, return to the main user account page, click the checkbox to the right of the account you wish to copy, choose the "Copy" option from the drop-down box in the lower right corner, and then click the "go" button next to it. A new screen will be displayed that allows you to specify the account name, the user's full name, and the authentication realm to use. Once you have entered the desired values, click the "yes" button. You will then be returned to the main user account page.



You will have to edit the account to change the password and other attributes. To edit the account, return to the main user account page, and click the hyper linked account name you wish to modify.

To delete a user account, return to the main user account page, click the checkbox to the right of the desired account, choose the "Delete" option from the drop-down box in the lower right corner, and then click the "go" button next to it. You will be prompted to confirm the deletion.

## 2.3 Managing Access Controls

Cacti access controls are fairly granular, and allow control over many atomic features and functions. These access controls are divided into two general areas, which are "realm" permissions that control the Web pages users are able to access, and "graph" permissions that control the specific graphs that the user is able to view. By combining the access controls, it is possible to tightly constrain a user to specific tasks.

For example, the realm permissions determine whether or not a user is able to create and modify graph trees that display multiple charts on a single web page. Meanwhile, the graph permissions determine whether or not a user is prohibited from viewing graphs for specific hosts or resources, or even whole graph trees. By selectively combining these attributes, it's possible to restrain the user to just their own tree, while also prohibiting them from including graphs of sensitive hosts in that tree.

To modify the permissions for an account, return to the main user account page, and click the hyperlinked account name you wish to modify. The user details for the selected account will be displayed, with the realm permissions and graph permissions listed in the tabs at the bottom (the individual checkboxes and drop-down lists determine the resources that the user is authorized to access). Once you have made all of the necessary modifications, click the "save" button in the bottom right corner of the screen to commit the changes.



New realm permissions may become available whenever a new Cacti plugin is installed, particularly if that plugin adds more Web pages to the Cacti interface.

## 2.4 Configuring the Polling Engine

As stated earlier, Cacti uses an open-ended polling engine to take timed sample readings from user-specified devices across a network. However, the polling engine is somewhat layered, and requires some configuration.

Essentially, Cacti uses a PHP control script that is periodically executed by the system cron daemon, which then calls upon one or more handler programs that are responsible for generating SNMP queries or executing other local programs. Any data that is returned by these processes is eventually passed back to the control script, which then updates the appropriate database files with the new data.

Specifically, the control script that Cacti uses as the front-end to its polling engine is `/usr/local/groundwork/nms/applications/cacti/poller.php`. This script provides a relatively straightforward wrapper program, and performs basic tasks such as reading Cacti variables, distributing queries across child processes, logging textual data to an appropriate log file, and other such duties.

By default, the GroundWork NMS Cacti package automatically adds the `poller.php` script to the `nagios` account's private `crontab` file, and schedules it to run every five minutes. To modify this behavior, perform the following steps:

1. Login to the GroundWork server, and use the `su root` command to elevate the login to `root` privileges.
2. From a command prompt, issue the `crontab -u nagios -e` command to edit the `crontab` file associated with the `nagios` account.
3. Locate the `crontab` entry for `poller.php`, and modify it as necessary. If you change the scheduler time interval, you need to inform Cacti of the new interval so that the graphs show the correct time values. To do this, click on the "Settings" menu item in the left navigation bar, click on the "Poller" tab of the resulting screen, set the "Cron Interval" and "Poller Interval" values to the new value, and then click the "Save" button at the bottom of the screen.
4. Save the `crontab` file and exit the editor. The cron daemon will automatically incorporate the new command-line parameters into its current schedule.

Whenever the `poller.php` script executes, it determines which of the handler programs have been chosen by the administrator, and then uses that program to process the individual queries. Cacti provides two of these handler programs. The first is called `cmd.php`, which is simply a PHP-based front end to the command environment. The other is called `spine` (formerly known as `cactid`), which is a binary tool that provides the same environment as `cmd.php` but has much less program overhead and is much faster.

By default, the GroundWork NMS Cacti package uses the `spine` handler program. If you wish to change this setting, click on the "Settings" menu item in the left navigation bar, click on the "Poller" tab of the resulting screen, choose the handler program from the "Poller Type" drop-down list, and then click the "Save" button at the bottom of the screen.

## 2.5 Setting Device Defaults

Before Cacti can begin monitoring the resources on a device, the device itself must be added to Cacti's host database. The host-specific database entry will subsequently be used to control some of the ways that Cacti queries the resources on that device.

For example, Cacti always tests to see if a device is up and responding to requests before it issues any queries for any specific resources on that device, and the device-specific database entry define the probes that should be used for this purpose. Similarly, the device-specific database entry also defines the version of SNMP that is in use along with other necessary SNMP attributes (such as the community string, or the authentication details), which in turn allows SNMP variables to be used with data queries, and the device-specific values to be used when the queries are executed.

These kinds of details can be defined when the device is first added to the database, and can also be edited later. However, it is also possible to set the default values to be used for these attributes, which can simplify the process of adding new devices to Cacti.



The "Host Template" setting that is specified when a device is first created determines the graphs and related queries that will be used to monitor the device. The default values for those options can also be assigned, and doing so will allow you to further streamline the device creation process. For more information on this process, refer to the "Managing Host Templates" section below.

To set the default method for detecting how a host is initially probed, click on the "Settings" menu item in the left navigation bar, click on the "Poller" tab of the resulting screen, choose the probe method from the "Downed Host Detection" drop-down list, set any additional values that are required for the selected method, and then click the "Save" button at the bottom of the screen.

The additional settings that are needed for a probe will be determined by the probe method that is selected. For example, the "None" option disables host probes altogether, and therefore requires no additional configuration. Meanwhile, the "SNMP" probe method does not require any additional input on this particular screen, but additional SNMP configuration is required elsewhere (see below). If you choose the "Ping" method, however, then you must also specify the type of probe in the "Ping Type" drop-down list, and if you choose to use "UDP Ping" or "TCP Ping" then you must also specify the UDP or TCP port number to use for your probes.



The "ICMP Ping" probe requires Cacti to be run under an account with `root` privileges, while the GroundWork NMS Cacti package uses the `nagios` account, which does not have those privileges. As such, the ICMP Ping probes cannot be used with the GroundWork NMS Cacti package without making significant modifications to the Cacti installation, which are beyond the scope of this document. For assistance with this issue, please contact GroundWork customer support.

If you have chosen to use SNMP probes, you must also define the default SNMP parameters to use. To set the default SNMP values for new devices, click on the "Settings" menu item in the left navigation bar, click on the "General" tab of the resulting screen, make the appropriate modifications to the fields in the "SNMP Defaults" section of the screen, and then click the "Save" button at the bottom of the screen. If you have a mixed network of SNMP v2 and v3 devices, you can set all of the options, set the "SNMP Version" field to whichever value is most prominent on your network, and then choose the other version whenever you add a device that is in the minority---the appropriate default values will be used when the version field is changed during device creation.



You can override the default probe method for a specific host by modifying the host-specific entry.



You can test individual probe methods on a specific device by modifying the probe method on the web page for that device and then saving the change.

The next time the web page for that device is displayed, Cacti will generate the currently selected probe, and display the results of the probe at the top of the page under the device name. If the results are colored black, then Cacti believes that the host is reachable, but if the results are colored red then Cacti believes that the host is unreachable and will not issue any queries for any resources on that host. You must choose a probe type that works for that device in order for Cacti to monitor the resources on that host.

## 2.6 Managing Cacti Plugins

Although Cacti is primarily designed as a graphing toolkit for network resources, it also provides a plugin interface that allows it to be extended for other purposes. For example, a "discovery" plugin can be used to look for devices across a network, match the discovered devices with an appropriate host template, and automatically create a default set of graphs for that device. Although this plugin is executed as part of the Cacti polling process, the functionality is quite a bit different from what is otherwise available in the basic package. In this regard, plugins allow Cacti to be used for more than just managing graphs of network resources.

By default, the GroundWork NMS Cacti package includes the following plugins:

- **Settings** - The settings plugin provides additional Web pages to the Cacti configuration subsystem, thereby allowing more program options to be defined than are ordinarily available.
- **Discovery** - The discovery plugin probes user-specified IP addresses with simple test packets, and then uses SNMP to query the discovered devices for system information. From there, the system information is matched against a collection of user-defined discovery templates, and if a match is found the device is added to the Cacti device database with all of the graphs that are associated with the appropriate host template.
- **Thresholds (thold)** - The "thold" plugin provides a very rudimentary alarm system, in that it watches devices and their resources, and issues email alerts whenever a user-defined threshold is crossed. In addition, the GroundWork NMS Cacti package also provides a Nagios plugin that pulls in the Cacti thold plugin output, updates the GroundWork Monitor system event log, and passes the data to the Nagios alerting mechanisms.
- **Weathermap** - The weathermap plugin allows map files that have been created in GroundWork NMS Weathermap to be displayed from inside Cacti. This allows a simple, overhead view of the entire network to be used in lieu of using host-specific graphs or hard thresholds.

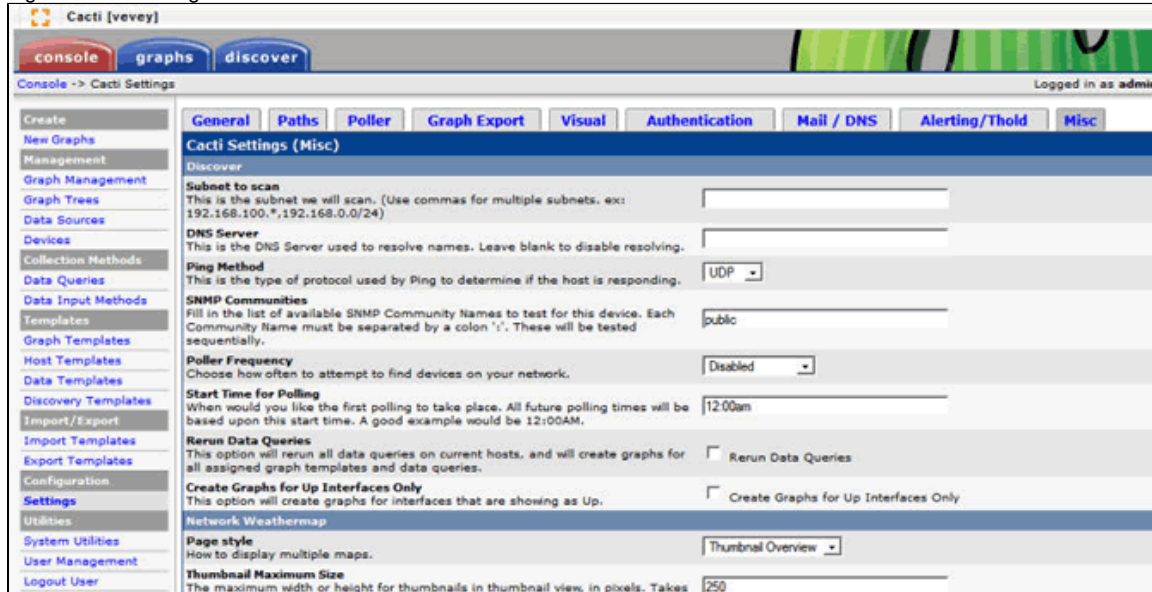
Each plugin typically has its own web pages within Cacti (but not always), and sometimes has its own menu items as well. Access to these pages and menus are typically managed by enabling one or more realm privileges in the "User Management" pages (one exception is the Settings plugin, which simply adds a new tabbed page to the configuration page).

## Configuring the Discovery Plugin

To grant user access to the discovery plugin, click on the "User Management" menu item in the left navigation bar, click on the hyperlinked user account you want to modify, activate the "View Host Auto Discovery" checkbox, and then click the "Save" button at the bottom of the screen. The next time the selected account loads a Cacti page, a large blue "discover" tab should appear at the top of the screen.

To configure the discovery plugin global settings, click on the "Settings" menu item in the left navigation bar, and then click on the "Misc" tab of the resulting screen. You should see a "Discover" section of the screen similar to the following:

Figure: Cacti Settings



The screenshot shows the Cacti web interface. At the top, there are tabs for 'console', 'graphs', and 'discover'. Below the tabs, the page title is 'Cacti Settings (Misc)'. The left sidebar contains a navigation menu with categories like 'Create', 'Management', 'Data Sources', 'Devices', 'Collection Methods', 'Data Queries', 'Templates', 'Host Templates', 'Data Templates', 'Discovery Templates', 'Import/Export', 'Export Templates', 'Configuration', 'Settings', 'Utilities', 'System Utilities', 'User Management', and 'Logout User'. The main content area is titled 'Cacti Settings (Misc)' and has several sub-tabs: 'General', 'Paths', 'Poller', 'Graph Export', 'Visual', 'Authentication', 'Mail / DNS', 'Alerting/Thold', and 'Misc'. The 'Discover' section is active, showing the following settings:

- Subnet to scan:** This is the subnet we will scan. (Use commas for multiple subnets. ex: 192.168.100.\*;192.168.0/24)
- DNS Server:** This is the DNS Server used to resolve names. Leave blank to disable resolving.
- Ping Method:** This is the type of protocol used by Ping to determine if the host is responding. (Set to UDP)
- SNMP Communities:** Fill in the list of available SNMP Community Names to test for this device. Each Community Name must be separated by a colon ':'. These will be tested sequentially. (Set to public)
- Poller Frequency:** Choose how often to attempt to find devices on your network. (Set to Disabled)
- Start Time for Polling:** When would you like the first polling to take place. All future polling times will be based upon this start time. A good example would be 12:00AM. (Set to 12:00am)
- Rerun Data Queries:** This option will rerun all data queries on current hosts, and will create graphs for all assigned graph templates and data queries. (Checkbox unchecked)
- Create Graphs for Up Interfaces Only:** This option will create graphs for interfaces that are showing as Up. (Checkbox unchecked)
- Network Weathermap:**
- Page style:** How to display multiple maps. (Set to Thumbnail Overview)
- Thumbnail Maximum Size:** The maximum width or height for thumbnails in thumbnail view, in pixels. Takes (Set to 250)

Set the fields to appropriate values, and then click the "Save" button at the bottom of the screen to continue.

For information on administering and using the discovery plugin, refer to the Using the Discovery Plugin section below.

## Configuring the Thresholds Plugin

The Thresholds plugin provides two sets of functionality, which each have their own realm permissions.

To grant user permission to manage the Thresholds plugin itself (as needed to create and manage threshold definitions), click on the "User Management" menu item in the left navigation bar, click on the hyperlinked user account you want to modify, activate the "Configure Thresholds" checkbox, and then click the "Save" button at the bottom of the screen. The next time the selected account loads a Cacti page, a new "Thresholds" menu item and a new "Thresholds Templates" menu item will appear in the left navigation bar.

To grant user permission to view the currently defined thresholds and the status of the associated data sources, click on the "User Management" menu item in the left navigation bar, click on the hyperlinked user account you want to modify, activate the "View Thresholds" checkbox, and then click the "Save" button at the bottom of the screen. The next time the selected account loads a Cacti page, a large blue "thold" tab should appear at the top of the screen.

To configure the threshold plugin settings, click on the "Settings" menu item in the left navigation bar, and then click on the "Alerting/Thold" tab of the resulting screen. A new screen should be displayed, similar to the following:

Figure: Configuring Thresholds





Activating the "Dead Hosts Notification" checkbox will cause Cacti to send notification email messages for every host that is in a "down" state. This is a global on-off switch, and there is no way to override this setting on per-host basis. As such, this option should only be used if all of the hosts that are monitored by Cacti are critical.

Set the fields to appropriate values, and then click the "Save" button at the bottom of the screen to continue.



The email server address and other similar settings are defined under the "Mail/DNS" tab. These options must be defined before the threshold alarm messages can be sent.

For more information on administering and using the threshold plugin, refer to the Using the Threshold Plugin section below.

### Configuring the Weathermap Plugin

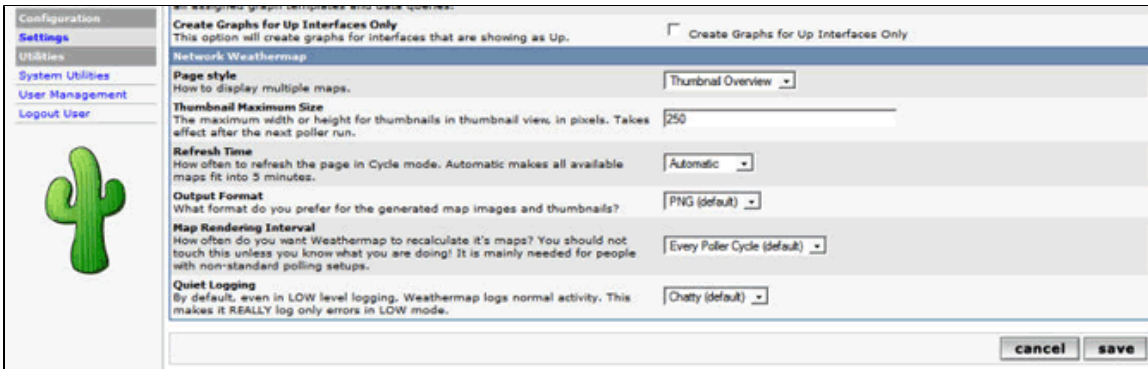
The Weathermap plugin provides two sets of functionality, which each have their own realm permissions.

To grant user permission to manage the Weathermap plugin itself (as needed to define the maps that will be available within Cacti), click on the "User Management" menu item in the left navigation bar, click on the hyperlinked user account you want to modify, activate the "Plugin->Weathermap: Configure/Manage" checkbox, and then click the "Save" button at the bottom of the screen. The next time the selected account loads a Cacti page, a new "Weathermaps" menu item will appear in the left navigation bar.

To grant user permission to view the currently available weathermaps, click on the "User Management" menu item in the left navigation bar, click on the hyperlinked user account you want to modify, activate the "Plugin->Weathermap: View" checkbox, and then click the "Save" button at the bottom of the screen. The next time the selected account loads a Cacti page, a large blue "weathermap" tab should appear at the top of the screen.

To configure the weathermap plugin settings, click on the "Settings" menu item in the left navigation bar, and then click on the "Misc" tab of the resulting screen. You should see a "Network Weathermap" section of the screen similar to the following:

Figure: Weathermap Plugin Settings



The most important option in this dialog is the "Map Rendering Interval" value, which determines how frequently the plugin generates the map output. Since the plugin is executed by the Cacti poller, setting this value to "Every Poller Cycle" will result in the maps being generated every time the poller runs (every five minutes, by default). If you need to have the maps generated more frequently, you will need to alter the poller's scheduled interval (refer to the Configuring the Polling Engine section above for more information on this process).

Set the fields to appropriate values, and then click the "Save" button at the bottom of the screen to continue.

For more information on administering and using the weathermap plugin, refer to the Using the Weathermap Plugin section below.

### 3.0 Performing Common Cacti Tasks

As was discussed earlier, Cacti uses an open-ended polling engine to gather and store timed sample readings from user-specified devices, and also provides tools that allow administrators to build highly customized, historical graphs of the various resources on their network.

From the user's perspective, the process for creating graphs is fairly straightforward. First the user identifies the device itself (such as its IP address and SNMP community string), and the platform type (such as Windows or UNIX, among others). When the user chooses the platform type, a default set of data sources are automatically enabled which define the retrieval methods to use for common pieces of data (such as using a known SNMP OID to retrieve disk usage statistics). Finally the user identifies the specific instances of each known resource that they would like to graph (such as choosing to monitor the "C:" drive of a server, while ignoring the "D:" drive). From there, Cacti takes care of the details, ensuring that the selected resources are polled with the appropriate query mechanisms, and that the data is recorded into the proper databases.

However, almost everything about the entire process can be modified if the user so chooses. For example, Cacti provides a variety of templates and editor screens that can be used to modify everything from the default host profiles down to the predefined mathematical equations that are used to manipulate the raw data values. However, these tools can require a significant time investment to fully master, and sometimes require direct programming skills, and as such are beyond the scope of this document.

A brief description of the most used web pages are provided in the remainder of this section. For more detailed discussion, refer to the [online Cacti documentation](#).

#### 3.1 Managing Device Entries

In the Cacti information model, the master object is the host device entry, which is the collection of data that identifies a device to be monitored. This data includes host identifiers such as the friendly host name and its IP address, but also includes the host template that should be used with this specific device, the method(s) to be used for probing the host to see if it is up or down, and the SNMP settings that are to be used with the device (if any).

By default, Cacti is pre-configured with an entry for "localhost" that monitors local resources with a variety of operating system commands.

To manage the Cacti device entries, click on the "Devices" menu item in the left navigation bar. You will then be presented with a screen that lists the currently defined host devices, similar to the following:

Figure: Cacti Devices

The screenshot shows the Cacti web interface. At the top, there are navigation tabs for 'console', 'graphs', and 'discover'. The main content area is titled 'Devices' and shows a table with the following data:

Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability
localhost	1	4	5	Up	0	127.0.0.1	0.04	0.04	100

Below the table, there is a 'Choose an action:' dropdown menu with 'Delete' selected and a 'go' button.

To edit an existing device entry, click on the hyperlinked name of the device.

To add a new device, click on the "Add" hyperlink in the upper right corner of the screen. A new screen will be displayed which allows you to specify the device details, similar to the following:

Figure: New Devices

The screenshot shows the 'New Device' form in Cacti. The form is titled 'Devices [new]' and contains the following sections and fields:

- Description:** Give this host a meaningful description. (Text input field)
- Hostname:** Fully qualified hostname or IP address for this device. (Text input field)
- Host Template:** Choose what type of host, host template this is. The host template will govern what kinds of data should be gathered from this type of host. (Dropdown menu, currently set to 'None')
- Notes:** Enter notes to this host. (Text area)
- Disable Host:** Check this box to disable all checks for this host. (Checkbox, currently unchecked)
- Availability/Reachability Options:**
  - Downed Device Detection:** The method Cacti will use to determine if a host is available for polling. NOTE: It is recommended that, at a minimum, SNMP always be selected. (Dropdown menu, currently set to 'Ping')
  - Ping Method:** The type of ping packet to sent. NOTE: ICMP on Linux/UNIX requires root privileges. (Dropdown menu, currently set to 'UDP Ping')
  - Ping Port:** TCP or UDP port to attempt connection. (Text input field, value: 23)
  - Ping Timeout Value:** The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings. (Text input field, value: 400)
  - Ping Retry Count:** The number of times Cacti will attempt to ping a host before failing. (Text input field, value: 1)
- SNMP Options:**
  - SNMP Version:** Choose the SNMP version for this device. (Dropdown menu, currently set to 'Not in Use')

At the bottom right of the form, there are 'cancel' and 'create' buttons.

The top section of the screen contains the basic identifying data for the device. Specifically, the "Description" field is used for the device' friendly host name, which will appear in various lists and graphs throughout Cacti (this field is also used as the primary key when Cacti graphs are linked with a host device in GroundWork Monitor, and must be identical to the Nagios device name). Meanwhile, the "Hostname" field is the specific identifier that will always be used to link the device entry with the device itself (generally speaking, a full domain is the best choice for the latter field, since it allows for better mobility than IP addresses).

The "Host template" drop-down list box is where you choose the appropriate platform type for the current device. Cacti includes a few common host platforms by default, such as "Cisco Router," "Windows 2000/XP Host," and "ucd/net SNMP Host" for UNIX-based systems, among others, and also includes non-specific host templates such as "Generic SNMP-enabled Host." As stated earlier, the host template determines the default set of data sources that are used for each device entry, which makes setup easier and faster (the default set of templates can be overridden later if needed).

The fields in the "Availability/Reachability Options" section and the "SNMP Options" section determine how Cacti will test to see if the host is up or down. Cacti will not attempt to retrieve measurement data from a host that it believes to be down, so it's important to set these fields to the correct values. By default, the values for these fields are derived from the values in the "Poller" tab of the "Settings" screen. Refer to the Configuring the



Polling Engine section above for information on how to set them.

After all the fields have been filled in, click the "Create" button in the lower right corner of the screen. The current screen will then be reloaded, with a large block of hyperlinked text at the top of the screen to "Create Graphs for this Host", and new sections at the bottom of the screen for manipulating the "Associated Graph Templates" and "Associated Data Queries" (these additional screen elements are discussed in more detail in the Managing Graphs and Data Sources section below).

If you wish to delete a device definition, return to the main device list, click the checkbox to the right of the device(s) you wish to remove, choose "Delete" from the drop-down box below the device list, and then click the "go" button next to it. A new screen will appear that itemizes the devices that have been selected for deletion. You may choose to either delete all of the graphs and data sources associated with the selected device(s), or you may also choose to keep them (the latter option may be necessary for a device that is being retired from service, but you want to keep the old data for historical analysis).



The underlying database files are not deleted in either event, and must be manually removed if you wish to reclaim the disk space.

### 3.2 Managing Graphs and Data Sources

Once a device has been defined in Cacti, you can define the resources that you want Cacti to monitor and graph. This is typically accomplished by adding or removing items to the "Associated Graph Templates" and/or "Associated Data Queries" sections of the device definition, or by directly managing the individual graphs and data sources in other screens.

In the Cacti information model, data sources point to a specific resource that is being monitored, while graph definitions describe how to render one or more data sources in a visual format. For simple resources, there may be a single data source with one data stream, and a single graph definition that points to that one piece of data. However, complex resources with multiple instances may require multiple graphs that reference multiple data sources, with multiple data streams in each data source.

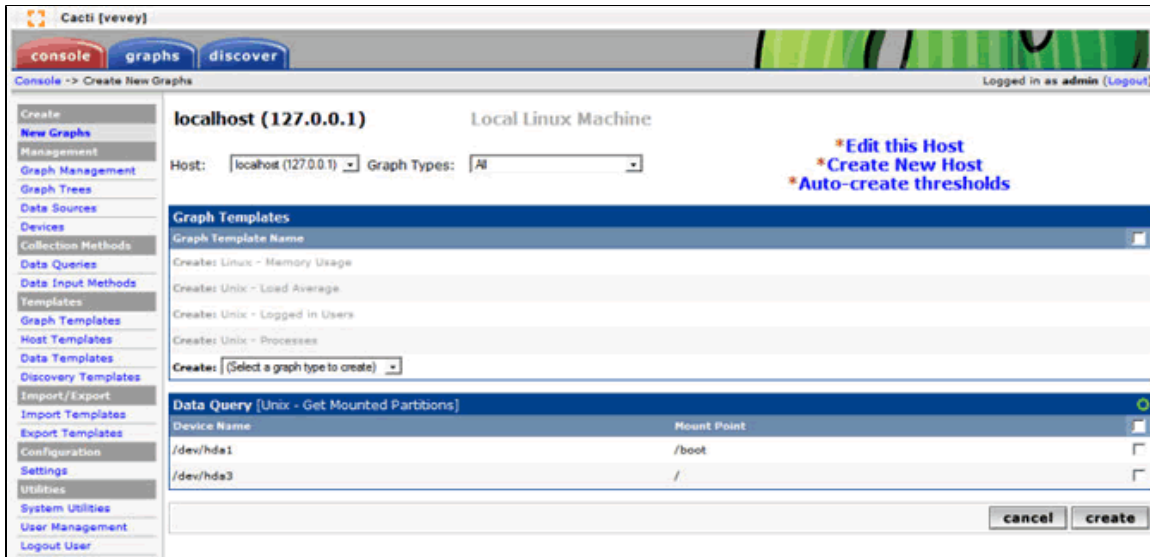
For example, the localhost device definition provides a graph that displays the number of active processes on the local system. Since this graph only requires a single column of data (the number of active processes), the underlying data source only references a single data stream. Conversely, most device definitions also provide graphs of network activity, with one graph for each active interface. In that model, multiple graphs would need to be created, each of which would use a single data source for the network interface being monitored, but with separate columns of data for the inbound and outbound traffic counters. Meanwhile, the UCD/Net-SNMP Load Average chart uses three different data sources to capture the one-minute, five-minute, and 15-minute samples, with each reading being stored in a single data column in each data source (the reasons for this will be made clear later), which the graph definition collectively renders as a single chart containing three data elements.

Although Cacti allows the individual data sources and graphs to be managed as discrete objects, it does not expect the user to manually create each object, and instead uses a variety of templates that automate the creation process. In this model, the user simply specifies the appropriate templates for the resources that need to be monitored, then choose the instance(s) of those resources that they want to be graphed, and Cacti creates the necessary data sources and graph definitions on the user's behalf.

Specifically, simple resources that only have one instance (such as a graph of the local process load) are usually created by simple "graph templates." In that situation, the user simply chooses the graph template they want to use, and Cacti automatically creates the data source(s) that are needed, and then creates a graph that points to the data source(s). Meanwhile, resources that have multiple instances (such as network interfaces) are usually created with the assistance of "data query" templates, which first list all of the discoverable instances of that resource, and then create the necessary data sources and graphs for each instance of the resource that the user selected.

For example, the device definition for localhost that is included with Cacti shows the following graph templates and data queries - each of the graph templates refer to resources that only ever have one instance, while the data queries refer to resources that can have multiple instances:

Figure: Device Definition - Graph Templates and Data Queries



New graph templates can be added from the device definition screen or by clicking on the "Create Graphs for this Host" hyperlink at the top of the screen. To add a graph template to a device from the definition screen, choose the desired graph template from the "Add Graph Template" drop-down list in the "Associated Graph Templates" section, and then click the "add" button next to it. To add a graph template from the "Create Graphs" screen, choose the desired graph template from the "Create:" drop-down list in the "Graph Templates" section, and then click the "create" button in the lower right corner. In either case, the current screen will reload with the selected graph being listed in the appropriate section.

To disassociate a graph template from a device definition, you must use the device definition screen. Locate the graph template you want to remove in the "Associated Graph Templates" section, and click the red "X" icon to its right.



You will not be prompted for confirmation. Also note that this procedure does not delete the graph or the data source, but instead only removes the graph definition from the device definition.

Separately, new data queries can only be added from the device definition screen. However, the individual instances of a data query can only be managed by clicking on the "Create Graphs for this Host" hyperlink at the top of the screen. To add a data query to a device from the definition screen, choose the desired data query from the "Add Data Query" drop-down list in the "Associated Data Queries" section, and then click the "add" button next to it.

To select the instances of the data query resource that you wish to have graphed, click the "Create Graphs for this Host" hyperlink at the top of the screen, locate the relevant Data Query section, click the checkboxes next to each desired instance, and then click the "create" button in the lower right corner.

To disassociate a data query from a device definition, you must use the device definition screen. Locate the data query that you want to remove in the "Associated Data Queries" section, and click the red "X" icon to its right.



You will not be prompted for confirmation. Also note that this procedure does not delete the graph or the data source, but instead only removes the graph definition from the device definition.

To explicitly delete an existing data source, click the "Data Sources" menu item in the left navigation bar. A new screen will be displayed that shows all of the known data sources. Click the checkbox to the right of the data source(s) you wish to delete, choose "Delete" from the drop-down box below the list of data sources, and then click the "go" button next to it. A new screen will appear that itemizes the data sources that have been selected for deletion. You may choose to either delete all of the graphs and graph items associated with the selected data queries, or you may also choose to keep them. After you have made your choice, click the "yes" button to continue, or click the "no" button to cancel the request.



The underlying database files are not deleted in either event, and must be manually removed if you wish to reclaim the disk space.

To explicitly delete an existing graph definition, click the "Graph Management" menu item in the left navigation bar. A new screen will be displayed that shows all of the known graphs. Click the checkbox to the right of the graphs(s) you wish to delete, choose "Delete" from the drop-down box below the list of graphs, and then click the "go" button next to it. A new screen will appear that itemizes the graphs that have been selected for deletion, similar to the following. You may choose to either delete all of the data sources associated with the selected graph(s), or you may also choose to keep them. After you have made your choice, click the "yes" button to continue, or click the "no" button to cancel the request.



The underlying database files are not deleted in either event, and must be manually removed if you wish to reclaim the disk space.

### 3.3 Using the Discovery Plugin

The discovery plugin included with the GroundWork NMS Cacti package is designed to locate devices on one or more networks, and possibly add them to the device database automatically. For example, the discovery plugin can detect a Windows 2003 Server host, locate a device profile to use for that host based on the SNMP system identification string, and then automatically create a Cacti device entry with all of the associated graphs already enabled.

There are two distinct tasks in this process. First, the discovery plugin scans the network addresses that are specified in the "Subnet to scan" configuration option according to the interval defined in the "Poller Frequency" configuration option, and then uses SNMP to retrieve system information from the devices that it finds. Second, the discovery plugin attempts to match the discovered devices with user-defined discovery templates, and automatically creates device definitions (with the associated graph templates and data queries) whenever a match is found.

As part of the process above, the discovery plugin compares discovered devices against devices that are already defined in Cacti, and discards the discovered devices that have the same IP address.

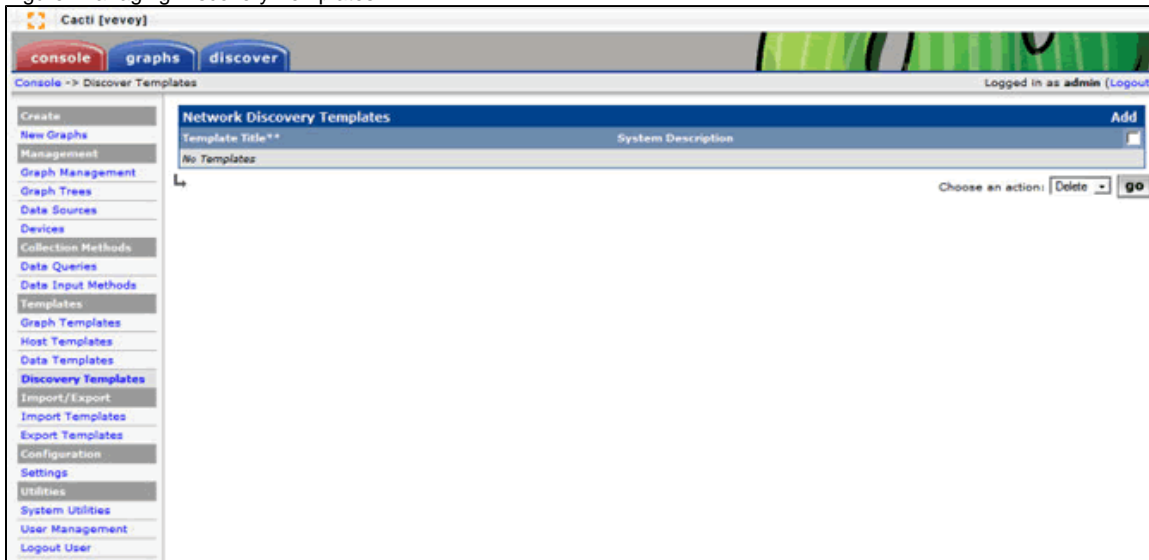


Devices which are discovered with different names may also appear as duplicate host entries.

The discovery plugin uses a holding table to store devices that cannot be matched to a discovery template. If no device templates have yet been created, then all of the newly-discovered devices will be in this table. To view this table, click the large blue "discover" tab at the top of the screen. To manually add a device in this table to Cacti, click the "Add" hyperlink to the right of the device. The discovery data will then be used to seed a new device definition, using the same screens as described in the Managing Device Entries section above.

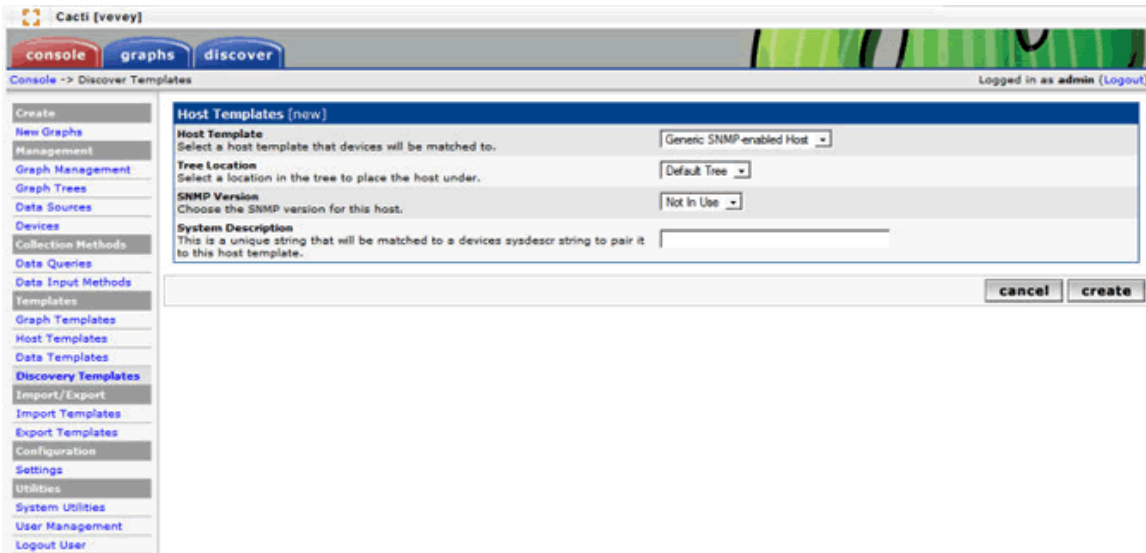
The discovery templates use rudimentary pattern matching, and are simple to create. Essentially, each discovery template identifies a substring that should appear in the SNMP system identification text, and the host template that should be used to automatically create the device definition when this occurs. Discovery templates are managed by clicking the "Discovery Templates" menu item in the left navigation bar. A new screen will be shown that lists all of the discovery templates, similar to the following (the default screen will be empty, since no discovery templates are defined by default):

Figure: Managing Discovery Templates



To add a new discovery template, click the "Add" hyperlink in the top right corner. A new screen will be displayed, similar to the following:

Figure: New Discovery Templates



As can be seen, this dialog allows you to specify the host template to use, the version of SNMP to assign to the resulting device definition, and the matching string to be compared against the SNMP system information string. Once you are finished setting the discovery template details, click the "create" button in the bottom right corner. The next time the discovery process runs, the discovered devices will be compared against the new template. If any matches are detected, the matching device will be added to Cacti, using the specified device template.

To delete a discovery template, return to the main discovery template page, click the checkbox to the right of the desired template, choose the "Delete" option from the drop-down box in the lower right corner, and then click the "go" button next to it. You will be prompted to confirm the deletion.

### 3.4 Using the Threshold Plugin

The threshold plugin included with the GroundWork NMS Cacti package is designed to issue alerts whenever a monitored device or resource crosses a user-defined threshold. For example, it can send a textual notification message if a monitored host becomes unreachable, or it can send an HTML email message with an embedded graph if a particular resource returns a reading that is higher or lower than normal. In addition, the GroundWork NMS Cacti package includes a Nagios plugin that can monitor the threshold plugin status, records the output in the GroundWork system event log, and use the output for Nagios notifications.

Host-level thresholds are enabled by a global on-off switch, as determined by the "Dead Hosts Notifications" checkbox in the "Alerting/Thold" tab under the "Settings" menu. There are no host-specific options for overriding this setting.

Resource-level thresholds can be defined in two different ways: you can manually add them to an existing data source, or you can define threshold templates and apply them to an entire device. In the latter case, only the templates that match the data source types will be inherited.

To apply thresholds to an existing data source, click on the "Data Sources" menu item in the left navigation bar, locate the data source that you want to modify, and click on the hyperlinked "Template Name" column item on the right of the row. If the threshold plugin has been configured properly, a new screen will be displayed with information about the specific data source, followed by a large thresholds form similar to the following:

Figure: Applying Thresholds

The screenshot shows the Cacti web interface for configuring a threshold. The top navigation bar includes 'console', 'graphs', 'thold', 'discover', and 'weathermap'. The current page is 'Console -> Thresholds'. On the left is a navigation menu with options like 'Create', 'New Graphs', 'Management', 'Graph Management', 'Graph Trees', 'Data Sources', 'Devices', 'Thresholds', 'Weathermaps', 'Collection Methods', 'Data Queries', 'Data Input Methods', 'Templates', 'Graph Templates', 'Host Templates', 'Data Templates', 'Threshold Templates', 'Discovery Templates', 'Import/Export', 'Import Templates', 'Export Templates', 'Configuration', 'Settings', 'Plugin Management', 'Utilities', 'System Utilities', 'User Management', and 'Logout User'. A small cactus icon is visible at the bottom left of the menu.

The main content area shows the configuration for a threshold named 'Localhost - Memory - Free'. It includes a 'Data Source Description' and a list of 'Associated Graph (graphs that use this RRD):' with one entry: '1 - Localhost - Memory Usage'. A line graph titled 'Localhost - Memory Usage' shows memory usage in kilobytes over time, with a peak around 16:00. Below the graph is a form for 'Data Source Item [mem\_buffers] - Current value: [87473.56]'. The form has several sections:

- Template settings:** 'Enabled' checkbox (unchecked).
- Mandatory settings:** 'Enabled' checkbox (checked).
- High Threshold:** 'If set and data source value goes above this number, alert will be triggered' with an input field.
- Low Threshold:** 'If set and data source value goes below this number, alert will be triggered' with an input field.
- Trigger Count:** 'Number of consecutive times the data source must be in breach of the threshold for an alert to be raised.' with an input field.
- Baseline monitoring:** 'When enabled, baseline monitoring checks the current data source value against a value in the past...' with an 'Enabled' checkbox (unchecked).
- Reference in the past:** 'Specifies the relative point in the past that will be used as a reference...' with an input field.
- Time range:** 'Specifies the time range of values in seconds to be taken from the reference in the past' with an input field.
- Baseline deviation UP:** 'Specifies allowed deviation in percentage for the upper bound threshold...' with an input field.

As can be seen, this dialog allows you to specify the high and low marks to use, information related to automatic baselining, and some options that are derived from the global preferences. Once you are finished setting the threshold details, click the "save" button in the bottom right corner, and the screen will be reloaded with the specified details. The next time the threshold process runs, all of the data sources with defined thresholds will be examined for their high and low values, with alert notifications being sent out for every network resource that meets the specified criteria.

As an alternative to defining thresholds on a one-by-one basis, you can also define a threshold template which can then be applied to a device entry, with thresholds being automatically created for the matching data sources. Threshold templates are managed by clicking on the "Threshold Templates" menu item in the left navigation bar. A new screen will be displayed that lists all of the defined threshold templates, similar to the following (the default screen will be empty, since no threshold templates are defined by default):

Figure: Threshold Templates

The screenshot shows the Cacti web interface for managing threshold templates. The top navigation bar is the same as in the previous screenshot. The current page is 'Console -> Threshold Templates'. The left navigation menu is also the same. The main content area is titled 'Threshold Templates' and contains a table with the following columns: 'Data Template', 'Data Source Name', 'High', 'Low', 'Trigger', 'Repeat', 'Email', and 'Add'. Below the table, it says 'No Data Templates'. At the bottom right of the table area, there is a 'Choose an action:' dropdown menu with 'Delete' selected and a 'GO' button.

To create a new threshold template, click the "Add" hyperlink in the top right corner. A walk-through wizard will be displayed that allows you to specify the data source template and the data field within that template which should be used for triggering high and low threshold values. After you have made your choices, a large thresholds form will be displayed similar to the one shown above. Once you are finished setting the threshold template details, click the "save" button in the bottom right corner, and you will be returned to the main templates list screen.



To apply a threshold template to a device, click on the "Devices" menu item on the left navigation bar, click the hyperlinked name of the device you want to modify, click the "Create Graphs for this Host" hyperlink at the top of the page, and then click the "Auto-create Thresholds" hyperlink at the top of the next page. If any threshold templates match the data sources in use on this device, those data sources will have the relevant threshold definitions applied. You will be notified of the thresholds that were created in the status text box at the top of the screen.

To delete a threshold template, return to the main thresholds template screen, click the checkbox to the right of the desired data source, choose the "Delete" option from the drop-down box in the lower right corner, and then click the "go" button next to it. You will be prompted to confirm the deletion.

To delete a specific threshold definition, click on the "Thresholds" menu item on the left navigation bar, click the checkbox to the right of the desired data source, choose the "Delete" option from the drop-down box in the lower right corner, and then click the "go" button next to it. You will be prompted to confirm the deletion.

If you would like to view the current status of the devices and data sources, you can click the large blue "thold" tab at the top of the screen, which will display a status screen showing the hosts and data sources that are currently being monitored. Clicking on the hyperlinked data source description will open a screen with the default Cacti historical graphs for that resource.

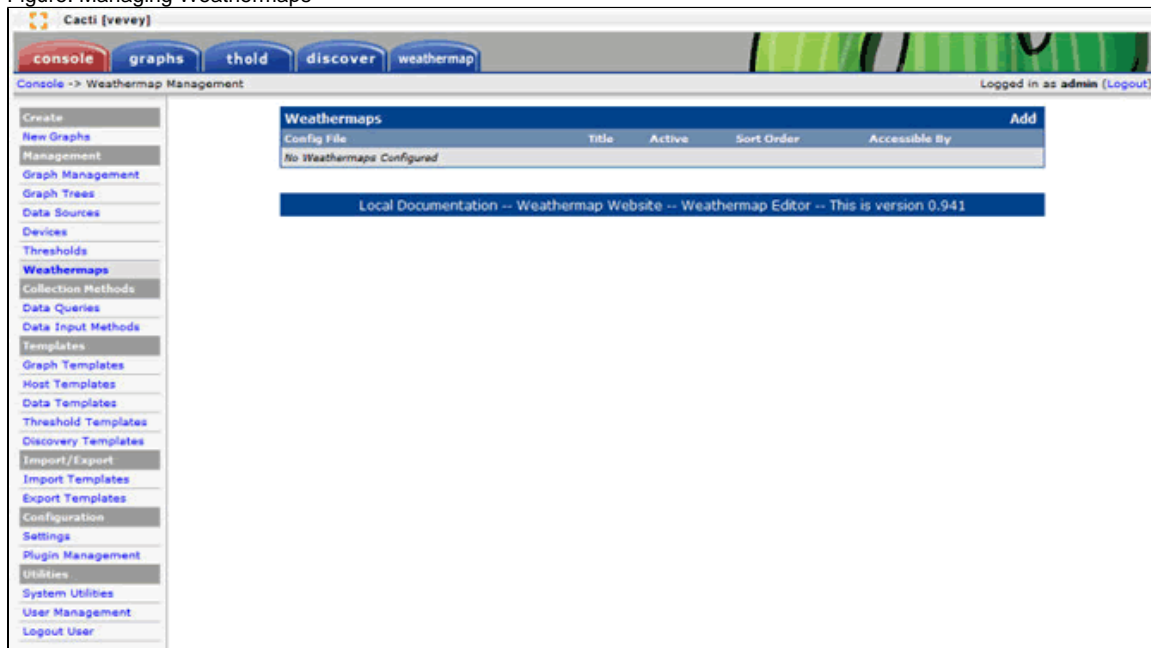
For information about integrating the threshold plugin output into Nagios and the GroundWork Monitor's system event log, refer to the Integrating Threshold Alarms section at the end of this chapter.

### 3.5 Using the Weathermap Plugin

The weathermap plugin is primarily designed to allow users to view weathermap images and HTML files from within Cacti. However, the plugin does not automatically display all of the maps that have been defined, so the desired maps must be added to the plugin before they will be available for display.

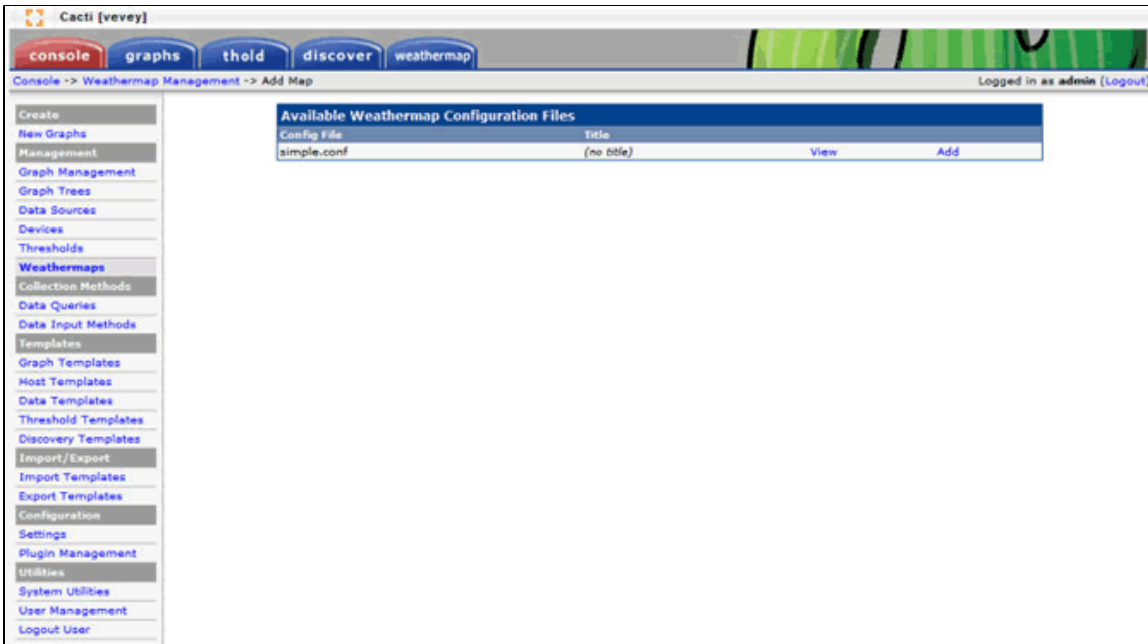
To manage the weathermaps that are available for viewing in Cacti, click on the "Weathermaps" menu item in the left navigation bar. A new screen should be displayed, similar to the following:

Figure: Managing Weathermaps



From this screen, you can choose which of the map files that you want to make visible to Cacti users. To add a new map file, click the "Add" hyperlink in the upper right corner of the screen. A new screen will be displayed which allows you to choose a map configuration file, similar to the following:

Figure: Selecting Maps



Click the "Add" hyperlink next to a map to add that map to the Cacti plugin. You will then be returned to the main weathermap management page.



The "View" hyperlink next to a link simply displays the contents of the configuration file, and does not display the map image.

Once a map has been added to the list, you can set access permissions for the map by clicking on the hyperlinked username(s) next to the map name. A new screen will be displayed which allows you to choose which specific Cacti users will have permissions to view the map output. To specifically allow access for a user account, select the desired account in the drop-down list, and click the "Update" button.



Granting access to "Anyone" will allow all users to view the weathermap page, including guest users who have not yet authenticated to Cacti. To remove a user account's permission, click the red "X" icon to the right of the desired account.

You can launch the weathermap editor to modify a map file by clicking on the map name in the main weathermap management screen.

To remove a weathermap from the list of available maps, return to the main weathermap management screen, and click the red "X" icon to the right of the weathermap file entry.



The "Recalculate All Maps Now" button is intended to allow you to immediately process the selected weathermap files through the map generator, without waiting for the Cacti poller's next scheduled run. However, this can cause problems when the poller and the Cacti web pages are executed by different system accounts. In the case of GroundWork NMS, the Apache web server and the Cacti poller are both executed by the `nagios` account, so this is not a problem for the GroundWork Weathermap package.

To view the weathermaps that have been generated, click on the large blue "weathermap" tab at the top of the screen. A new screen will be displayed that shows thumbnail views of the available maps. To view a specific map, click on the thumbnail for that map. Alternatively, you can have the weathermap plugin automatically rotate through the maps by clicking on the "automatically cycle" hyperlink above the thumbnails.

## 4.0 Integrating Cacti Data with GroundWork Monitor

The GroundWork NMS Cacti package provides three distinct methods of integrating Cacti data into GroundWork Monitor.

First, the GroundWork NMS Cacti package implements an object that allows the GroundWork Monitor Status application to display Cacti graphs for the currently selected host. This process works automatically, with no configuration or manual transfers being required. For more information on how this data appears and is used, refer to the "Status" section of the Using Applications documentation.

Second, the GroundWork NMS Cacti package also provides scripts and automation schema definitions that allow administrators to export the host definition data out of Cacti and import that data into the GroundWork Monitor Configuration database. This process can be performed manually or automatically, as the administrator sees fit, and is discussed in the sections that follow.

Finally, the GroundWork NMS Cacti package also provides a Nagios plugin that monitors the Cacti threshold plugin output, updates the GroundWork Monitor system event log with the current status, and also makes the data available to the Nagios alerting mechanisms.



### Important Notice

Cacti graphs hyperlinks in the GroundWork Monitor Status application are broken in the GWME 7.0.x releases. Fixing this requires some file changes. Please refer to the Knowledge Base article [Setting up a Hyperlink from Status to Cacti Graphs](#).

## 4.1 Exporting Host Definitions from Cacti

To export the host definitions from the Cacti configuration database, use the `/usr/local/groundwork/nms/tools/automation/scripts/extract_cacti.pl` Perl script included with the GroundWork NMS Cacti package, which exports data from Cacti and writes it into the `/usr/local/groundwork/core/monarch/automation/data/cacti_data.txt` text file.

The output file contains the following fields, each of which are separated from their neighbors by a pair of semi-colon characters:

Field Name	Field Data	Notes
Hostname	IP address or domain name	The fully-qualified unique identifier of the device. This is usually either a domain name or an IP address.
Description	Short device name	The friendly name of the device. This is the primary identifier for the device throughout Cacti.
Template	Host template	The name of the host template assigned to the device.
Disabled	Disabled flag status	Indicates if the device has been flagged as "Disabled" in Cacti. If so this field contains the string "on" but if not this field is empty.
Status	Up/Down flag value	Indicates if the device is considered to be "Up" or "Down" in Cacti. The numeric values for this field are "3" for "Up," "2" for "Recovering," "1" for "Down," and "0" for "Disabled."



The `extract_cacti.pl` Perl script is automatically executed as part of the `nagios` user's `crontab` file immediately after the `cacti.pl` discovery script is executed (once every five minutes, by default), which ensures that the output file always contains the most recent version of the configuration data.

## 4.2 Importing Host Definitions into GroundWork Monitor

The GroundWork NMS Cacti package also provides a schema template for use with GroundWork Monitor's Auto Discovery subsystem, which imports the contents of the `cacti_data.txt` text file into GroundWork Monitor's configuration subsystem. The automation schema template is `/usr/local/groundwork/core/monarch/automation/templates/schema-template-Cacti-host-profile-sync.xml`, and integrates Cacti devices and nodes into the configuration subsystem by either adding new host entries or modifying existing host entries, depending on whether or not a host entry already exists in the configuration database for the device or node in question, and by deleting entries that already exist which are not listed in the import file. If you wish to use this schema template, you must create an appropriate schema definition using the following steps:

1. Open the Auto Discovery application from the main GroundWork menu.
2. Click the Automation menu item in the top menu bar to manage the automation schema definitions.
3. Click the New Schema button to create a new schema definition.
4. Give the new schema definition the exact name of "Cacti-host-profile-sync".
5. Choose the "Cacti-host-profile-sync" template from the bottom drop-down box.
6. Click the "Add" button to finish creating the new schema definition.
7. From the schema editor screen, verify that the data file contains the output from the Cacti database tables by clicking the "View" button in the "Data source" row, and then close the pop-up window when you are finished.
8. If you wish to process the records now, click the "Process Records" button at the top of the schema editor screen, otherwise click the "Close" button to return to the schema definition window.

The GroundWork NMS Cacti package also provides the `/usr/local/groundwork/nms/tools/automation/scripts/auto_import_cacti.pl` Perl script, which can be used to automate the import process. This script looks for a schema definition entry with the name of "Cacti-host-profile-sync" and then executes that schema definition automatically. However, this script does not automatically commit the changes to the configuration database, so the changes will not be recognized until they are manually committed.

## 4.3 Integrating Threshold Alarms

The GroundWork NMS Cacti package also includes the `/usr/local/groundwork/nagios/libexec/check_cacti.pl` Perl script, which can be used to extract threshold alarms from Cacti and feed them into Nagios as alarm signals. Once the data has been passed into Nagios, they

can then be processed through the Nagios alarm and notification systems, and will also appear in the GroundWork system event log. This allows the threshold alarm signals to be processed in a more robust manner, and also allows users to view the exceptions from within GroundWork Monitor itself.

The `check_cacti.pl` Perl script can operate in multiple different ways. In the most basic mode of operation, the script can be executed as a one-time event that simply extracts the threshold data, updates Nagios, and then exits immediately (this method requires the use of a "-p" parameter on the script command-line). When the one-time method is used, the script can be executed as either a scheduled cron job, or can be executed from within Nagios as a command definition (the GroundWork NMS Cacti package does not use either of these methods by default, however). Conversely, the script can also be executed as a background daemon that polls for threshold signals on a user-specified time interval and then continues to run until the next interval (this is the default method, although the GroundWork NMS Cacti does not provide a system init script to spawn the script as a daemon on startup).

The `check_cacti.pl` script also supports multiple mechanisms for passing event data into Nagios. By default, the script passes the threshold data to Nagios through the Nagios passive interface, where it can then be picked up by a service definition that is linked to the host. Alternatively, the script data can also be passed to Nagios through the Nagios NSCA listener, which is then mapped to a service definition that is linked to the host. The former approach works well GroundWork Monitor and Cacti are running on the same server, while the latter approach is required when they are running on different hosts.



The GroundWork NMS Cacti package does not provide a predefined service definition for this tool, so any events which are passed to Nagios will be treated as spurious log messages.

Due to the manual labor required to fully integrate the threshold alarms into Nagios and GroundWork Monitor, users are advised to contact GroundWork customer support when first configuring the integration component.