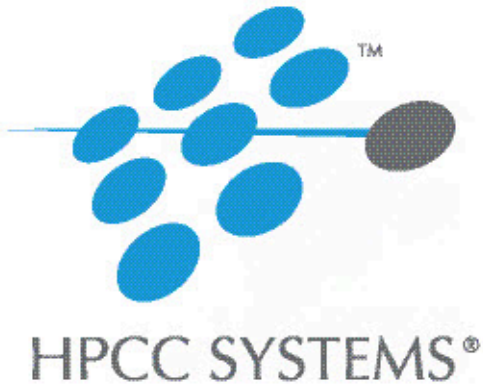
HPCC Systems® Monitoring and Reporting (Technical Preview)

Boca Raton Documentation Team



HPCC Systems® Monitoring and Reporting (Technical Preview)

Boca Raton Documentation Team

We welcome your comments and feedback about this document via email to <docfeedback@hpccsystems.com>

Please include **Documentation Feedback** in the subject line and reference the document name, page numbers, and current Version Number in the text of the message.

2021 Version 8.2.34-1

Introduction

The HPCC Systems® platform supports graphical monitoring and reporting components.

Ganglia:

The HPCC Systems monitoring component leverages Ganglia, an open source, scalable, distributed monitoring system to display system information in a graphical manner.

With the the graphical monitoring component you can:

- See system information at a glance
- View a grid of Roxie clusters
- Examine Roxie metrics
- Keep a historical record of metrics
- Drill down to individual server metrics
- Quickly detect troubled nodes
- More applications, such as better informed resource planning and allocation

Nagios

The HPCC Systems reporting and alerting component leverages Nagios, a powerful monitoring and notification system, which can help you identify and resolve infrastructure problems before they affect critical processes.

With the HPCC Systems reporting and alerting component you can set up alerts to inform of any changes to:

- Disk Usage
- Roxie
- Dali
- Dafilesrv
- Sasha
- Service Bindings on ESP Servers
- SSH connectivity
- Users on system
- System Load

Ganglia

The HPCC Systems monitoring component leverages Ganglia, an open source, scalable, distributed monitoring system, to produce a graphical view of a Roxie cluster's servers. Ganglia leverages widely accepted technologies for data representation. It provides near real-time monitoring and visualizations for performance metrics. If your enterprise already has a Ganglia monitoring server, you can easily add Roxie clusters to its monitoring.

Ganglia Overview

Ganglia Monitoring has two primary components: the viewer and the Ganglia Monitoring Daemon (gmond). Installation and configuration will vary depending on your system.

On an **RPM-based system**, install the *ganglia-gmond-modules-python* RPM running a command such as:

```
sudo rpm -i ganglia-gmond-modules-python-3.4.0-1.x86_64.rpm
```

On a **Debian-based system**, install the *ganglia-monitor* running a command such as:

```
sudo apt-get install ganglia-monitor
```

The specific steps required to install and configure Ganglia are covered in the Ganglia wiki:

http://sourceforge.net/apps/trac/ganglia/wiki/ganglia_gmond_python_modules

The Viewer

In order to use Ganglia with Roxie you must have the following packages installed on every node you wish to monitor.

- ganglia-gmond
- ganglia-gmond-python
- python-lxml

For the visualization component you must have:

- ganglia-gmetad

Proper installation and operations of the Ganglia component depends on these components.

Ganglia Monitoring Daemon

The monitoring daemon is required on the Roxie nodes you wish to monitor. Install the *gmond* daemon on the nodes you wish to monitor. Installation and configuration are described in;

http://sourceforge.net/apps/trac/ganglia/wiki/ganglia_gmond_python_modules

If you have a Ganglia monitoring server running in your environment, you already have the required components and prerequisites. Verify that you have */etc/ganglia/conf.d* and */etc/ganglia/.pyconf* files in place and then add the Roxie nodes you wish to monitor. You can do that by installing the Ganglia components and HPCC Systems Monitoring components on to each Roxie node.

If you do not have Ganglia, or want to install it, read the Ganglia documentation provided at the above link, and install it and any system dependencies. You will then need to download and install the HPCC Systems Monitoring component.

Installing the HPCC Systems Monitoring component

The HPCC Systems Monitoring component is available for download. The HPCC Systems Monitoring components leverage the Ganglia monitoring tools, and would only be needed if you do not already have Ganglia monitoring components on your system.

To get the HPCC Systems Monitoring components, find the appropriate package for your system.

Packages are available for download from the HPCC Systems® site:

hpccsystems.com/download

or

http://hpccsystems.com/download/free-community-edition/all

Find and install the appropriate package for your system.

For example, if you have a CentOS 8.x system, get the RPM package.

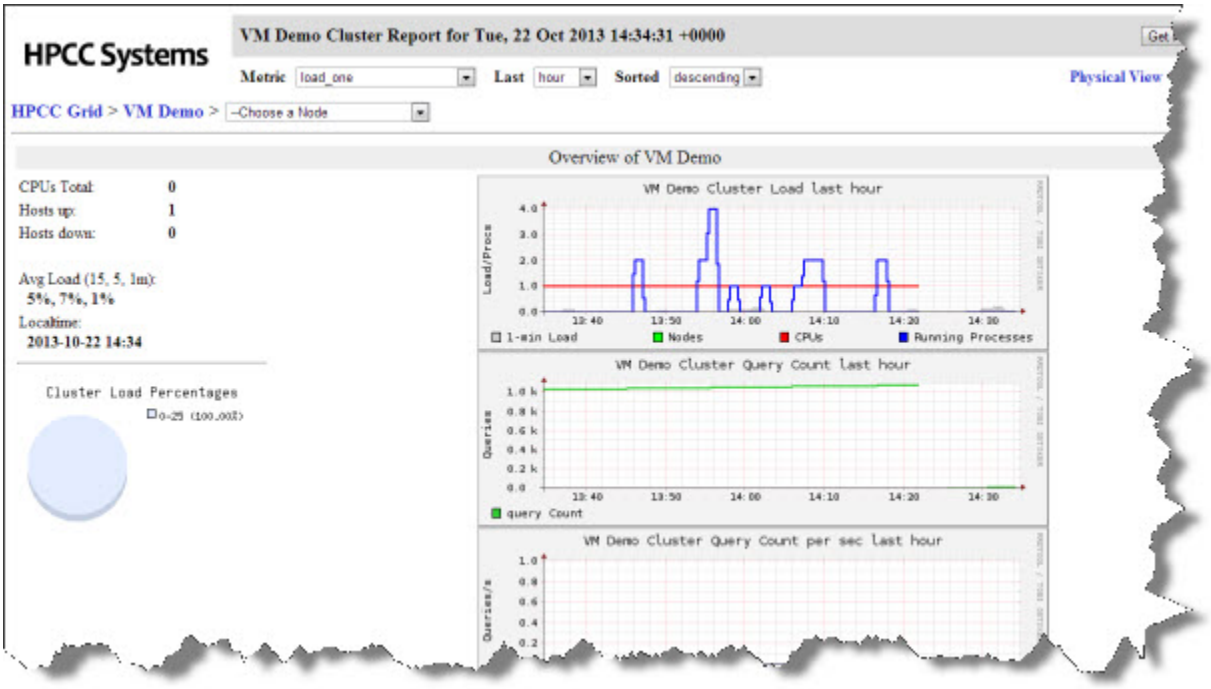
```
hpccsystems-ganglia-monitoring-7.12.18-rc1.el8.x86_64.rpm
```

Install the monitoring package on the system that you want to monitor. Optionally, you can look at that installation package provided and use that as a guide to implement your own customized monitoring components.

The HPCC Systems Ganglia Viewer

A Ganglia viewer comes preinstalled and configured in the 4.2.x (or later) HPCC Systems Virtual Machine. The monitoring provided with the Virtual Machine is set up to monitor Roxie instances on the network. This document introduces the monitoring and describes how to get it working on your system.

Figure 1. HPCC Systems Monitoring



The above image is an overview summary of all the monitored Roxie nodes in the cluster named VM Demo.

The Viewer

If you already have a Ganglia monitoring server running in your network, the viewer component may already be in place. If you do not have Ganglia then you will need to install and configure the viewer.

Refer to the https://github.com/hpcc-systems/ganglia-monitoring/tree/master/vm_precise directory. There you will see the resources used to configure the Ganglia for the virtual machine and can use them as the examples to configure it for your enterprise.

The script, *install_graphs_helper.sh* available from the github link above and also provided with the virtual machine, is what is used to embed the viewer component. Using this script as a basis, you can then similarly configure and deploy the viewer component for your system.

Metrics in the Virtual Machine

An easy way to understand how the metrics work and how to implement them on a larger system, is to examine the metrics in action.

Ganglia integration is built into the current HPCC Systems Virtual Machine images. Download and start up a virtual image and look at how the monitoring component works.

This allows you:

- A preview of the metrics
- A quickstart
- A guide for set up

Evaluate the value of the content and decide what aspects of measurement are relevant to your needs.

Get the latest HPCC Systems® Virtual Image File

The complete details for installing and running HPCC Systems in a virtual machine are available in the document: **Running HPCC Systems in a Virtual Machine**, available from http://hpccsystems.com/download/docs .

The following steps are a quick summary, assuming you have some familiarity with running virtual machines.

1. Download the latest HPCC Systems Virtual Machine image file from:

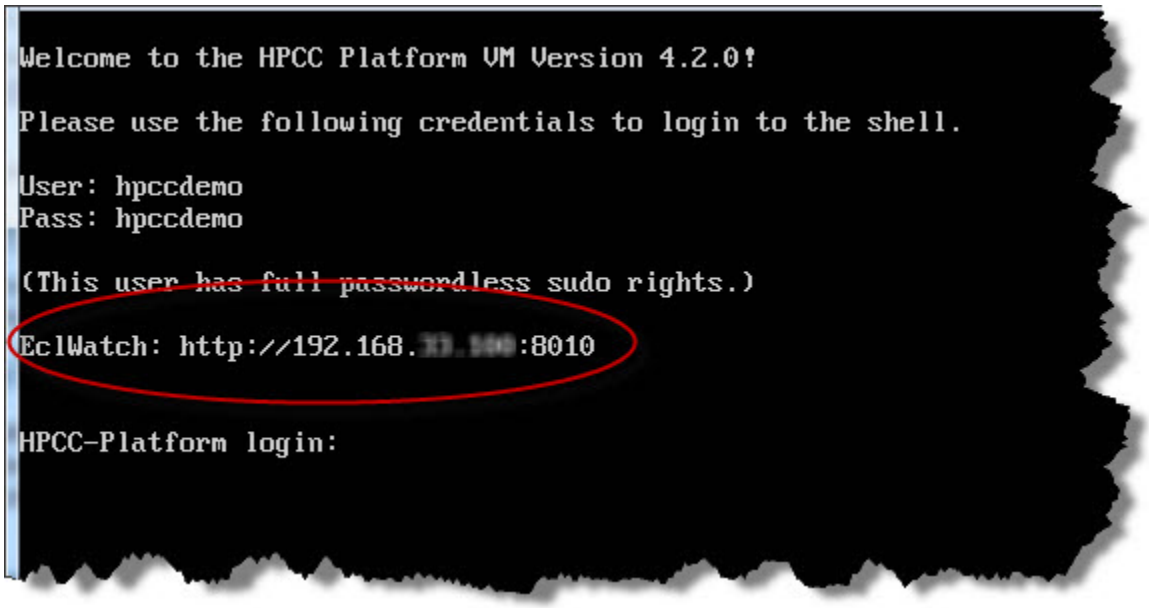
   http://hpccsystems.com/download/hpcc-vm-image

2. Save the file to a folder on your machine.

3. Open your virtualization software, import the virtual machine and start it.

4. Once the VM initialization completes, you will see a window similar to the following:

Figure 2. VM Welcome Screen



	Your virtual IP address could be different from the ones provided in the example images. Please use the IP address provided by **your** installation.

Note the IP Address of your VM Instance.

5. In your browser, enter the URL displayed (circled in red above) in the previous image (without the :8010)

   For Ganglia enter the *IP Address*/ganglia. For Nagios enter the *IP Address*/nagios3.

   For example, *http://nnn.nnn.nnn.nnn/nagios3*, where nnn.nnn.nnn.nnn is your Virtual Machine's IP address displayed at the VM welcome screen.

We encourage experienced users to use SSH and log into the VM and further examine the configuration of a 1-node monitoring solution.

Viewing the Metrics

To view the metrics page, go to the following page(s) in your browser.

Ganglia:

```
http://nnn.nnn.nnn.nnn/ganglia
```

Where the *nnn.nnn.nnn.nnn* is your ESP server running ECL Watch.

Nagios:

```
http://nnn.nnn.nnn.nnn/nagios3
```

Where the *nnn.nnn.nnn.nnn* is your ESP server running ECL Watch.

Ganglia Integration with HPCC Systems

The Roxie nodes are able to report metrics to Ganglia when the nodes have Ganglia monitoring and the associated dependencies installed.

Review the Ganglia wiki: http://sourceforge.net/apps/trac/ganglia/wiki/ganglia_gmond_python_modules to understand the requirements.

1. Install the Ganglia components on every node.

2. Configure the Ganglia as appropriate for your system

   The Ganglia configuration files can be typically found in the */etc/ganglia/* directory.

3. Install the HPCC Systems® monitoring component on every node.

4. Deploy the monitoring daemon (gmond) and the HPCC Systems Monitoring package to each of the nodes you wish to monitor.

The VM graphs can be used to monitor Roxie clusters. You can add more Roxie nodes installed anywhere on the same network utilizing multi-cast.

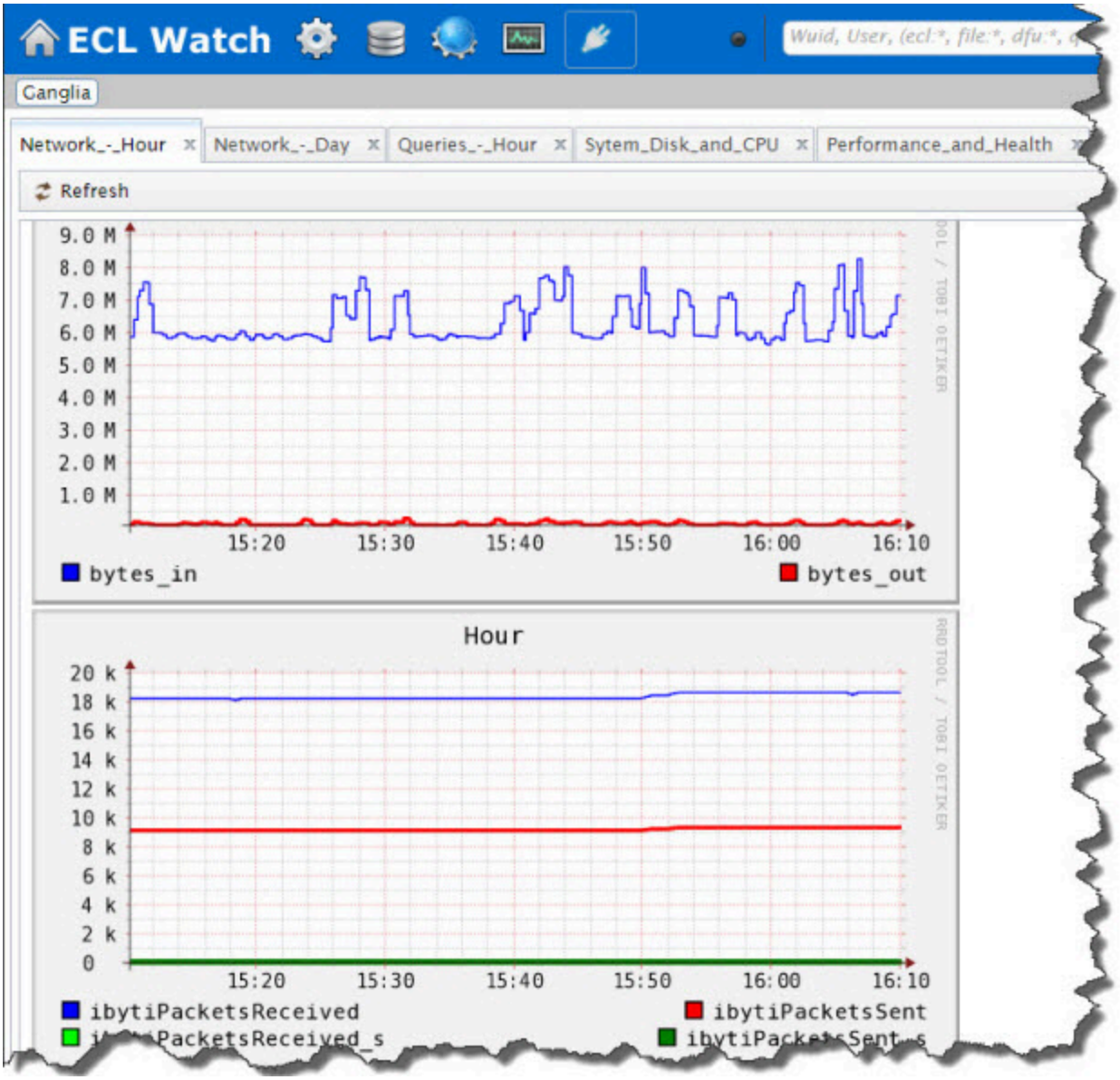
To add a new Roxie node, install the HPCC Systems Monitoring package on to each Roxie node to monitor. In most basic configurations you may need to add the node(s) IP address(es) to the */etc/ganglia/gmetad.conf* file. As long as the new Roxie node can communicate with (for example ping) the Monitoring component host, the graphs for that will automatically be added to the graph display.

NOTE: Some of the graphs take some time to populate with data. These graphs may appear blank or empty at first, but will render properly as more data accumulates to populate the graph.

Ganglia in ECL Watch

With the Ganglia for HPCC Systems Plugin installed. You can view the Ganglia statistics and graphs right through the ECL Watch interface. The out of the box monitoring displays several key statistics by default. You can customize and configure the views.

Figure 3. Ganglia in ECL Watch



The default Plugins page has a tab for Custom Monitoring where you can easily add some custom monitoring components.

Select the Custom Monitoring tab, and press the Metrics button. Use the drop menus to display the various graphing utilities.

Installing Ganglia in ECL Watch

In order to get the Ganglia in ECL Watch, You need to have Ganglia on your HPCC Systems.

1. Install or ensure you have the HPCC Systems Monitoring components on a node where ECL Watch is installed.
2. Ensure that the Ganglia gtemad daemon is running.
3. Restart the ESP if this is the initial installation of any of those components.
4. Start or connect to ECL Watch on that node.
5. Click the plugin icon at the top of the ECL Watch page.

   The graphs display data.

It is also possible for EclWatch/Esp to be on a separate, different node from the gmetad machine, as long as the rrd data directories are exposed to the plugin.

Configuring Ganglia graphs in ECL Watch

The configuration of Ganglia in ECL Watch is maintained in the **ganglia.json** file. That can be found in the HPCC Systems® system directory/componentfiles. The default HPCC Systems® system directory ganglia resources is:

/opt/HPCCSystems/componentfiles/files/ganglia

The configuration can be customized and modified to suit your specific needs.

Nagios

The HPCC Systems Reporting component leverages Nagios, an open source, system and network infrastructure monitoring application to monitor and alert HPCC Systems Administrators. Nagios leverages established and accepted open source technologies to alert users to changes or potential issues. Nagios provides regular periodic system monitoring and reporting.

With the HPCC Systems integration, you can generate Nagios configuration files to monitor HPCC Systems server health. Once the Nagios is configured, you can monitor:

- Disk Usage
- Roxie
- Dali
- Dafilesrv
- Sasha
- Service Bindings on ESP Servers

With additional available (3rd party) plugins, check utilities, and modification of the config file, Nagios can also monitor:

- SSH connectivity
- Users on system
- System load
- Disk / CPU / Memory usage
- Network infrastructure
- More...

Nagios Introduction

Nagios is a powerful monitoring and notification system, which can be used with HPCC Systems to help identify and resolve infrastructure problems before they affect critical processes. Nagios hardware notifications can help keep your system highly available and alerts can assist in pre-emptive maintenance for processes which are down or behaving outside expected parameters to ensure system stability, reliability, and uptime. Scripts and tools are provided to extract HPCC Systems platform system metrics and easily integrate that data into Nagios.

Administrators should note that different platforms may not support all plugins. The *hpcc-nagios-tools* utility can be used to simplify the addition of custom plugins. Many additional Nagios plugins and utilities are available from 3rd parties.

The Nagios package is not simply an "install and run" utility, it requires additional steps to configure and use properly. If you are not already familiar with Nagios, then you should:

- Familiarize yourself with the base Nagios package from https://www.nagios.org
- Set up a base Nagios installation, such as one on a virtual machine.
- Review our HPCC Systems Monitoring and Reporting documentation in its entirety.
- Review our VM installation and configuration.

Nagios sets thresholds to trigger alerts. A check may indicate a failure or high load that caused a timeout, so some historical baseline would be helpful. Ganglia maybe useful for that purpose. Nagios monitoring uses a polling interval to check system health. Frequency and number of checks would depend on the needs in the cluster. Alerts are only useful if they are actionable. Consider who gets alerted (tiered escalations), when they get alerted (thresholds, multiple), and what types of alerts (none?, email, text, phone, EclWatch etc...) before configuring your environment.

Nagios in the Virtual Machine

An easy way to understand how the Nagios works and how to implement it on a larger system, is to examine an established session in action.

Nagios integration is built into the current HPCC Systems Virtual Machine images. Download and start up a virtual image and look at how the monitoring component works.

The Nagios component for HPCC Systems on the VM allows you:

- A preview of the alerts
- A quickstart
- A guide for set up

Evaluate the value of the content and decide what aspects are relevant to your needs.

Get the latest HPCC Systems® Virtual Image File

The complete details for installing and running HPCC Systems in a virtual machine are available in the document: **Running HPCC Systems in a Virtual Machine**, available from http://hpccsystems.com/download/docs .

The following steps are a quick summary, assuming you have some familiarity with running virtual machines.

1. Download the latest HPCC Systems Virtual Machine image file from:

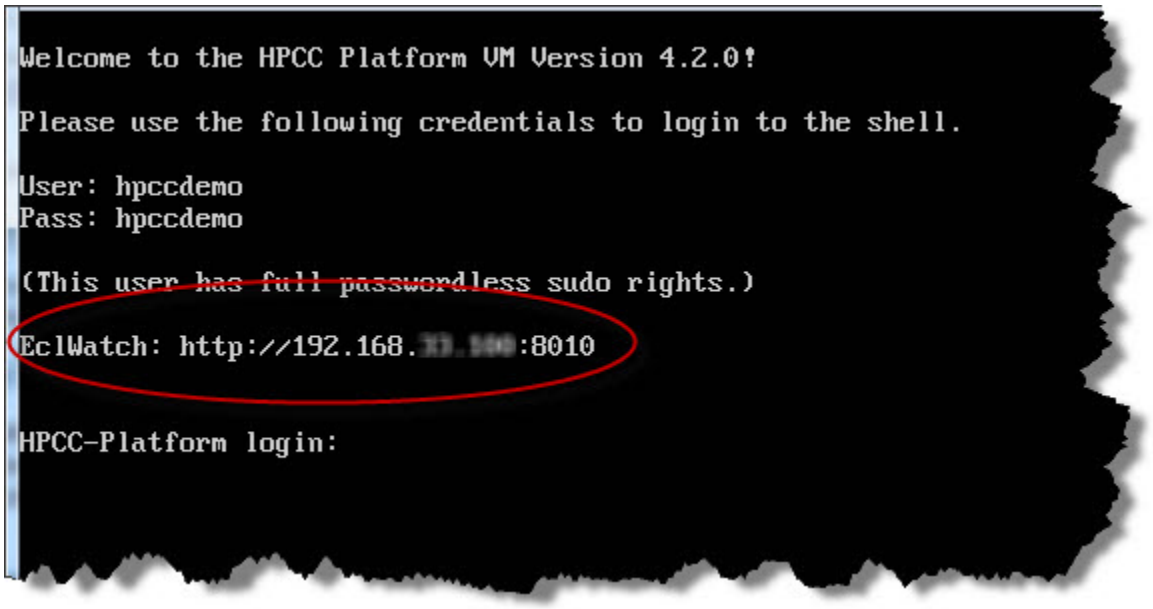
   http://hpccsystems.com/download/hpcc-vm-image

2. Save the file to a folder on your machine.

3. Open your virtualization software, import the virtual machine and start it.

4. Once the VM initialization completes, you will see a window similar to the following:

Figure 4. VM Welcome Screen



	Your virtual IP address could be different from the ones provided in the example images. Please use the IP address provided by **your** installation.

Note the IP Address of your VM Instance.

5. In your browser, enter the URL displayed (circled in red above) in the previous image (without the :8010)

   For Ganglia enter the *IP Address*/ganglia. For Nagios enter the *IP Address*/nagios3.

   For example, *http://nnn.nnn.nnn.nnn/nagios3*, where nnn.nnn.nnn.nnn is your Virtual Machine's IP address displayed at the VM welcome screen.

We encourage experienced users to use SSH and log into the VM and further examine the configuration of a 1-node monitoring solution.

Viewing the Metrics

To view the metrics page, go to the following page(s) in your browser.

Ganglia:

```
http://nnn.nnn.nnn.nnn/ganglia
```

Where the *nnn.nnn.nnn.nnn* is your ESP server running ECL Watch.

Nagios:

```
http://nnn.nnn.nnn.nnn/nagios3
```

Where the *nnn.nnn.nnn.nnn* is your ESP server running ECL Watch.

Nagios Interface

There are a number of Nagios configurations available. To get a better understanding of Nagios configuration, look at the configuration delivered with the VM. To login to the Nagios admin page:

1. Go to *http://nnn.nnn.nnn.nnn/*nagios3

   Where the *nnn.nnn.nnn.nnn* is your ESP server running ECL Watch.

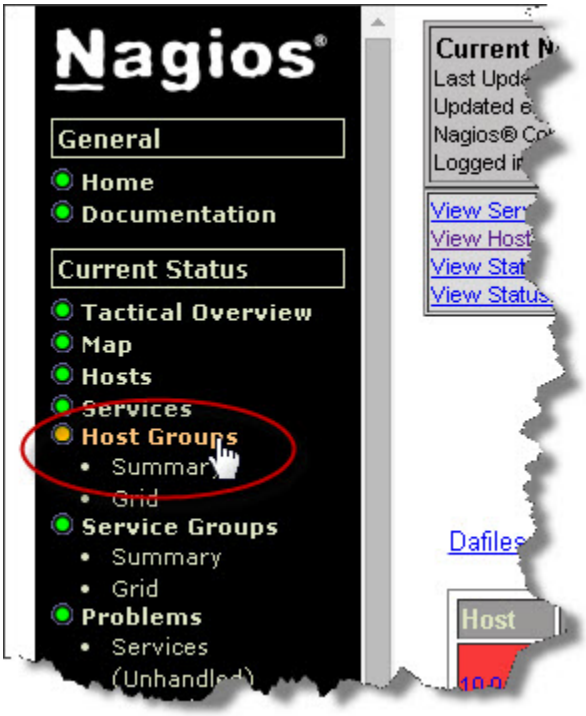
2. Login with username : nagiosadmin

3. Enter the password : nagiosadmin

Once logged in the Nagios landing page displays. This page displays information about Nagios and contains links to the various components, items, and documentation.

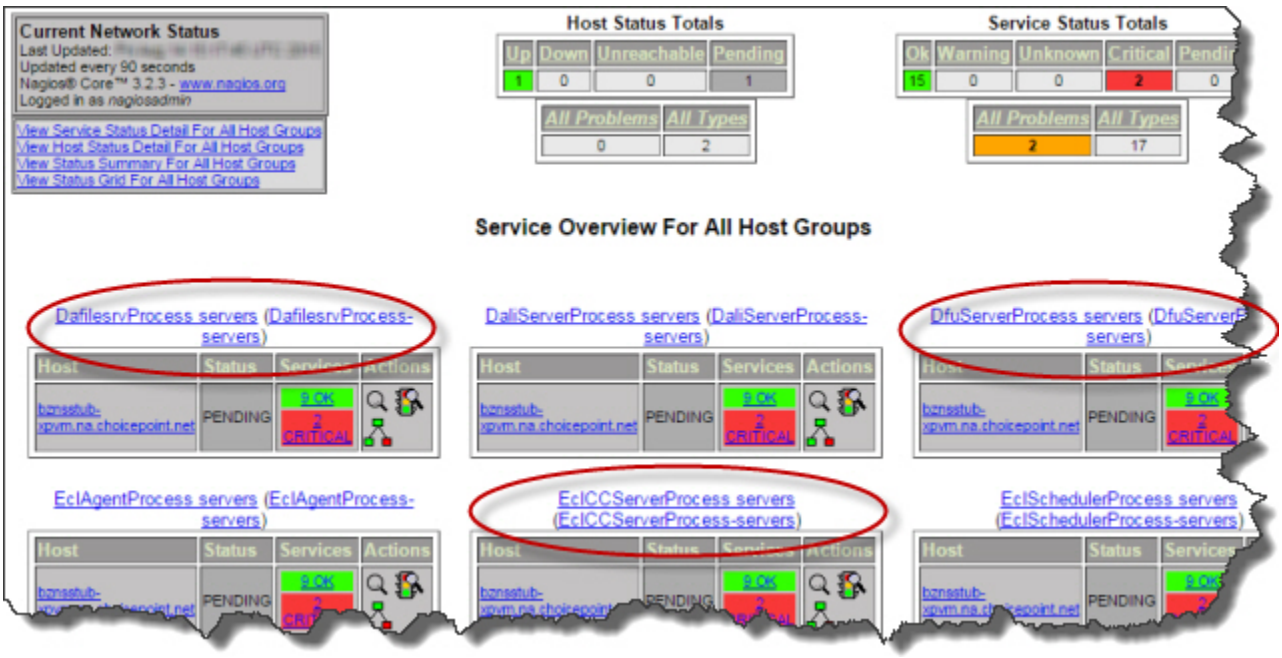
To view the configuration, click on the **Host Groups** link from the Nagios navigation menu on the left side of the page.

Figure 5. Nagios Host Groups



This displays the Host Groups being monitored.

Figure 6. Nagios Host Groups



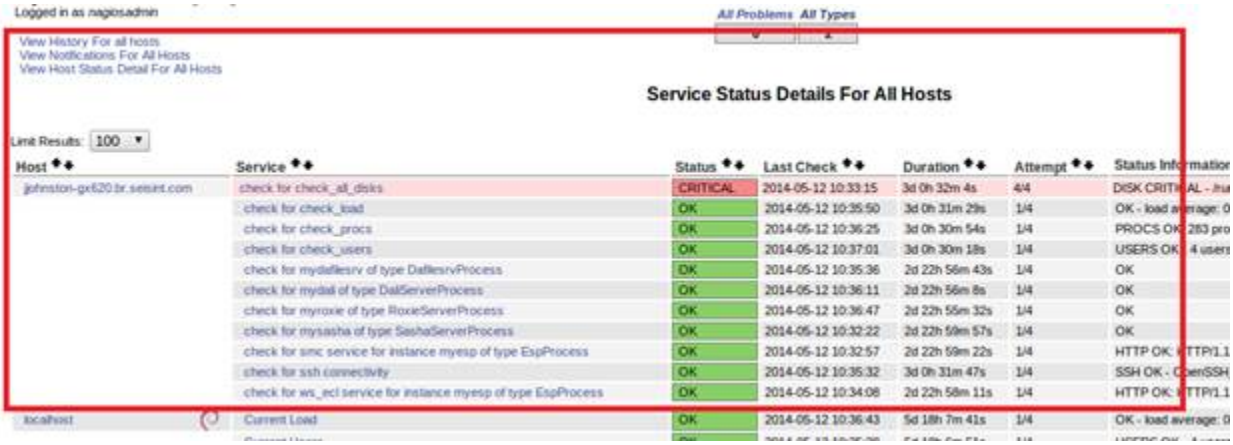
Nagios Services

Click on the **Services** link from the Nagios navigation menu on the left side of the page.

Figure 7. Nagios Services

The services link displays the Service Status details for the systems being monitored.

Figure 8. Nagios Service status



You can see the service status for the systems being monitored.

Installation of Nagios

The HPCC Systems Nagios package provides tools and utilities for generating Nagios configurations. These configurations check HPCC Systems and perform some of the HPCC Systems specific checks. HPCC Systems Nagios installation is provided on the HPCC Systems® portal.

HPCC Systems Nagios Installation Package

To get the HPCC Systems Nagios monitoring on your system you need the Installation package. Download the installation package from the HPCC Systems portal.

The HPCC Systems® web portal is where you can find HPCC Systems resources, downloads, plugins, as well as helpful information.

http://hpccsystems.com/

You can find the HPCC Systems Monitoring and Reporting Installation packages at:

http://hpccsystems.com/download/free-community-edition/monitoring

Download the appropriate installation package for your operating system.

Install Nagios

To Install Nagios for HPCC Systems, you must have HPCC Systems platform installed and also have the open-source Nagios package installed.

1. Install the **hpcc-nagios-monitoring** on the node that will be doing the monitoring. The node where you install the Nagios monitoring must have network connectivity to all the monitored nodes.

   With the hpcc-nagios tools installed, you have HPCC Systems check utilities in:

   ```
   /usr/lib/nagios/plugins/
   ```

2. Generate Nagios configuration files. There are several configuration options for Nagios. Determine your needs and customize accordingly.

   The main features included are tools to generate Nagios configurations. The generated configurations can be modified with optional flags to fit the environment that is being monitored. The default package also provides some utilities to monitor HPCC Systems processes such as Roxies, ESP Services by node and port, Dali, and dafilesrv. Other processes could also be monitored if a check utility is provided and the generated config file is modified (find/replace all would probably suffice).

Generate a host groups configuration for Nagios.

```
/opt/HPCCSystem/bin/hpcc-nagios-tools -env   \
/etc/HPCCSystems/environment.xml -g -out /etc/nagios3/config.d/hpcc_hostgroups.cfg
```

Generate a services configuration file.

```
/opt/HPCCSystem/bin/hpcc-nagios-tools -env   \
/etc/HPCCSystems/environment.xml -s -out /etc/nagios3/config.d/hpcc_services.cfg
```

Generate an escalation notifications file.

```
./hpcc-nagios-tools -ec -env /etc/HPCCSystems/environment.xml  \
-enable_host_notify -enable_service_notify -set_url localhost/nagios3 \
-disable_check_all_disks -out /etc/nagios3/conf.d/hpcc_notifications.cfg
```

The configurations you generate can be used as is, merged with existing configurations, or modified to meet your specific needs.

3. Integrate the host and services configuration files into the Nagios configuration folders.

4. Restart Nagios for the new configuration to take effect.

Nagios Options

You may need to override some of the default values, depending on your Linux distribution. For different distributions you may need to modify some of the check scripts. Use the override flags to properly name all the check scripts in the configuration files as appropriate for your distribution.

The thresholds levels are dependent on your specific needs and environments. The default values are starting points. Evaluation of your specific needs over time will help you determine appropriate thresholds for your production environment(s).

To override the defaults, modify the generated configurations as needed.

Monitoring tools like Ganglia can help to determine what the thresholds should be.

hpcc-nagios-tools usage

hpcc-nagios-tools -env <*environment file*> **-out** <*output path*> **[**options**]**

Available optional parameters:

Option/Flag	Detail	Default Value
-c or -cfggen	The path to the configgen	/opt/HPCCSystems/sbin/configgen
-g or -hostgroup	generate host group file	
-s or -service	generate service and host file	
-t or -host	generate host file	
-n or -nrpe	generate client plugin cfgs for nrpe	
-e or -env	HPCC Systems environment configuration file	/etc/HPCCSystems/environment.xml
-ec or -escalation_cmds	generate escalation commands	
-enable_host_notify	enable host notifications	0
-enable_service_notify	enable service notifications	0
-set_url	set the url link for escalation notifications	NotificationURL
-override_send_serivce_status	override send_status escalation command	/opt/HPCCSystems/bin/send_status -o $HOSTADDRESS$ -s $SERVICESTATE$ -d '$SERVICENOTES$' -t $TIMET$ -n $SERVICEDISPLAYNAME$
-override_send_host_status	override send_status escalation command	/opt/HPCCSystems/bin/send_status -o $HOSTADDRESS$ -s $HOSTSTATE$ -d '$HOSTNOTES$' -t $TIMET$ -n $HOSTDISPLAYNAME$
-override_service_status	override host_notification_commands	send_service_status
-override_host_status	override service_notification_commands	send_host_status
-override_eclwatch_host_port	Override eclwatch host port for escalation commands. This flag may be specified multiple times.	
-o or -output	outpfile where the generated configuration will be written	
-r or -retry	keep attempting to resolve IP to hostnames. Stops after 1st failure.	
-lookup	look up hostname form ip	
-u or -user	MACRO name to use for username for esp server login. Example: $USER1$	

Option/Flag	Detail	Default Value
-p or -pass	MACRO to use for password for esp server login. Example: $USER2$	
-attempts	max host retry attempts	10
-sysload1warn	load1 warning threshold	5
-sysload5warn	load5 warning threshold	4
-sysload15warn	load15 warning threshold	3
-sysload1crit	load1 critical threshold	10
-sysload5crit	load5 critical threshold	6
-sysload15crit	load15 critical threshold	4
-diskspacewarn	disk space % warning threshold	15
-diskspacecrit	disk space % critical threshold	8
-usernumwarn	users logged in warning threshold	5
-usernumcrit	users logged in critical threshold	10
-totalprocswarn	total process warning threshold	350
-totalprocscrit	total process critical threshold	500
-checkperiod	host check period	24x7
-contacts	host contacts	eclwatch
-contactgroups	host contact groups	eclwatch_group
-notify_interval	host contact groups	1
-notify_period	host contact groups	24x7
-set_esp_username_pw	Set specific login credentials for ESP checks. All fields are required (esp name, user name, password). Can be specified more than once to support multiple ESP servers.	<esp name> <user name> <password>
-override_retry_interval	check retry_interval	1
-override_active_checks_enabled	active_checks	1
-override_passive_checks_enabled	passive_checks	1
-override_parallelize_check	parallelize_check	1
-override_obsess_over_service	obsess_over_service	1
-override_check_freshness	check_freshness	0
-override_event_handler_enabled	event_handler_enabled	1
-override_is_volatile	is_volatile	0
-override_normal_check_interval	normal_check_interval	1
-override_flap_detection_enabled	flap_detection_enabled	1
-override_process_perf_data	process_perf_data	1
-override_failure_prediction_enabled	failure_prediction_enabled	1
-override_retain_status_information	retain_status_information	0
-override_retain_nonstatus_information	retain_nonstatus_information	0

Option/Flag	Detail	Default Value
-check_all_disks	enable/disable check_all_disks service check	check_all_disks
-override_check_all_disks	check_all_disk plugin name	check_all_disks
-check_users	enable/disable check_users service check	check_users
-override_check_users	check_users plugin name	check_users
-check_procs	enable/disable check_procs service check	check_procs
-override_check_procs	check_procs plugin name	check_procs
-check_load	enable/disable check_load service check	check_load
-override_check_load	check_load plugin name	check_load
-check_ssh	enable/disable ssh service check	checkSSH
-set_catch_all_hostgroup	create a hostgroup and include all nodes as memebers	
-set_host_check_command	set the check_command for hosts	
-check_host	enable/disable check host check	check_host
-disable_use_of_note_for_host_port	the send command will use the detail/note for host:ip insteaad of param	true
-use_https	Use https connection for esp service calls. **HIGHLY RECOMMENDED** when using username/password	
-d or -debug	verbose debug output\n	

Use the available option flags to customize the configuration of Nagios as appropriate for your environment.

Help

For help with HPCC Systems Nagios enter:

```
/opt/HPCCSystems/bin/hpcc-nagios-tools
```

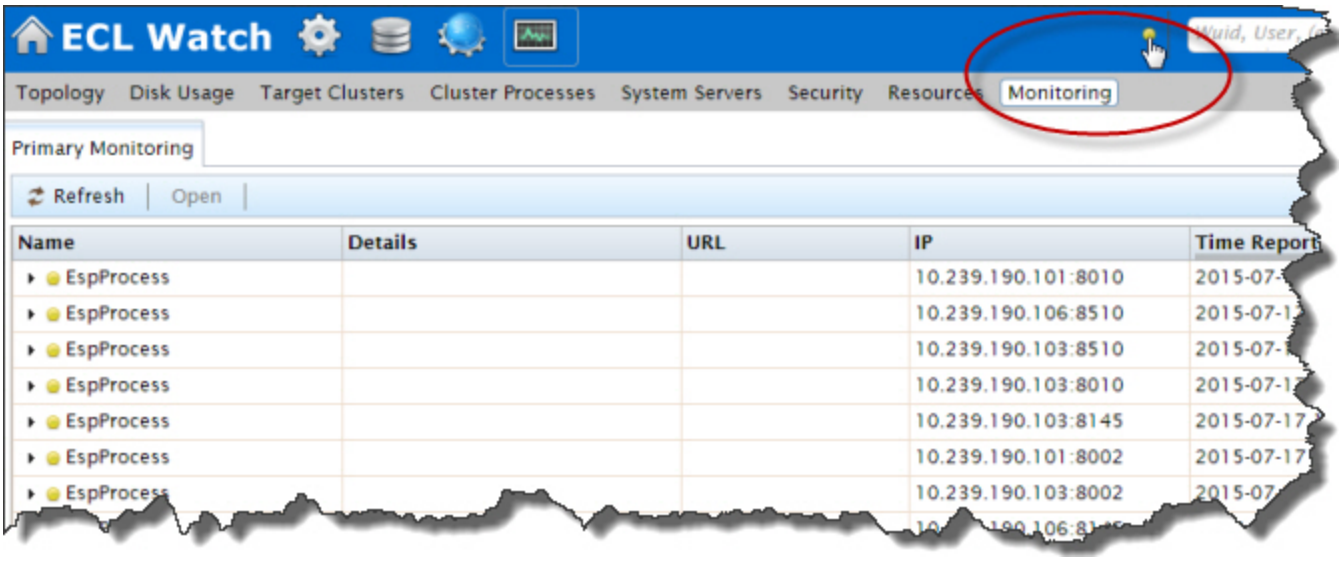
Entering the command without any parameters or options specified displays all the available options.

Nagios in ECL Watch

ECL Watch is set up for monitoring your system with Nagios. ECL Watch has an API that can interface with Nagios and provide Nagios monitoring right in ECL Watch. Nagios escalations can be pointed to any ECL Watch version 5.4 (and later) and are viewable directly in ECL Watch.

By default all ECL Watch services defined in the environment.xml will receive notifications generated using *hpcc-nagios-tools*. You can override that if not desired. The ECL Watch instances need not be in the cluster that is being monitored.

Figure 9. Nagios in ECL Watch



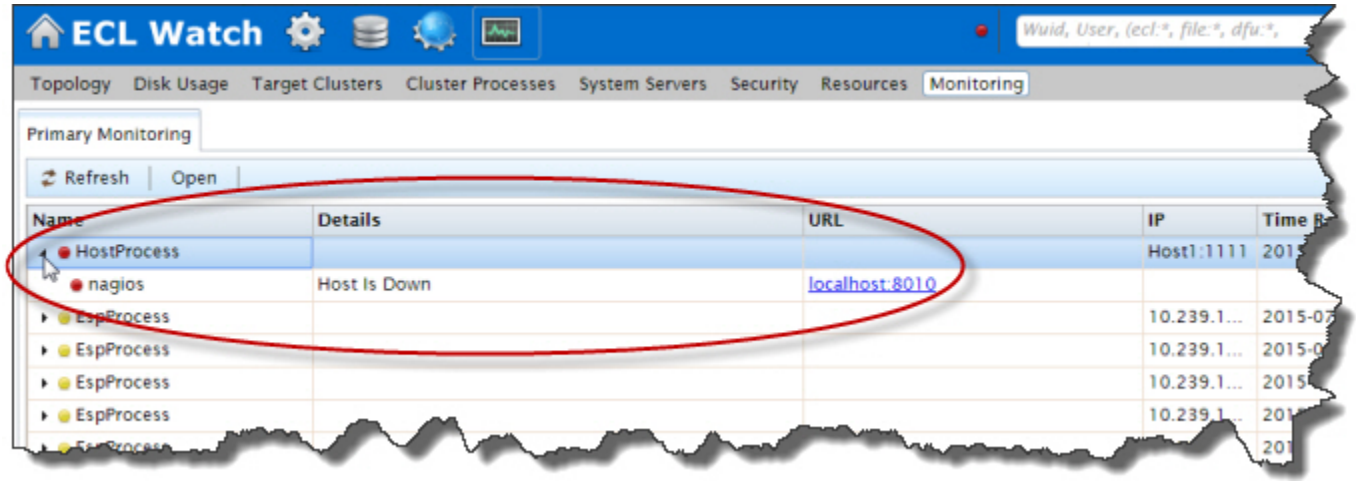
Once you have Nagios configured for your environment, you can see at a glance if there are any alerts. Along the top banner of the ECL Watch window, you will see a small indicator light. The light is darkend (gray) if there is no system data being reported, typically indicative that your system is not yet configured for monitoring.

The light is green when all systems are reporting normal. The light is yellow when there is warning. The light turns red when there is an alert. All the alerts are configurable through the Nagios configuration.

By default ECL Watch monitoring maintains the latest update for 30 minutes. This means that once Nagios stops escalations to ECL Watch any status, including Normal will expire from the list. Nagios escalations notification behavior and frequency is configurable, refer to the Nagios documentation for more information. An empty list could indicate 'no data' or 'no outages', by default no alerts generate when everything is up and running.

To delve further into any warnings or alerts, you can press the indicator light at the top. You can also access the *Primary Monitoring* page by pressing the **Operations** link, then press the **Monitoring** link in the navigation sub-menu.

Figure 10. Nagios in ECL Watch



This displays the all the messages and alerts reported to the monitoring system. For more information on a specific message, press the arrow next to the message you want.