vFabric Hyperic Administration

v.5.7

June 2013
Legal Notice

Copyright © 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com
Contents

Discover and Import Resources to Inventory .................................................. 7
  Using the Auto-Discovery Portlet .............................................................. 7
  Using the Auto-Discovery Results Page .................................................... 10
  Options for Running and Controlling Resource Discovery ....................... 12
Manage Resource Auto-Discovery ............................................................... 15
  Configure Auto-Discovery Frequency ....................................................... 15
  Scan a Platform On-Demand ..................................................................... 16
  Prevent Resource Discovery ..................................................................... 17
  Solving Auto-Discovery Problems ........................................................... 18
Set Up Alert Notifications and Escalations ................................................. 19
  Tailor Alert Notification Templates ........................................................... 19
  Configure Roles for Role-Based Alert Notifications ................................... 22
  Enable SNMP Trap Notifications .............................................................. 23
  Enable Syslog Notifications for Escalations ............................................... 26
  Configure and Manage Escalations ............................................................ 28
  Set Up Alert Action Script ....................................................................... 32
  Configure a Custom Control Action ........................................................... 36
Configure Monitoring and Alerting for a Resource ..................................... 38
  Configure Metric Baselines ....................................................................... 38
  Set Up Log Tracking for a Resource ........................................................... 41
  Set Up Configuration Tracking for a Resource .......................................... 47
  Define an Alert for a Resource .................................................................. 50
  Define a Recovery Alert for a Resource Alert ........................................... 56
  Define Host Dependencies for Hierarchical Alerting ................................ 57
  Schedule Resource Downtime ................................................................... 59
Configure Monitoring and Alerting for a Resource Type ............................ 60
  Tailor Metric Collection for a Resource Type ............................................. 60
  Define an Alert ........................................................................................... 62
About vFabric Hyperic Administration

*vFabric Hyperic Administration* describes how to get resources into VMware® vFabric™ Hyperic® inventory, configure monitoring and alerting, and manage users and roles.

**Intended Audience**

*vFabric Hyperic Administration* is intended for Hyperic administrators who implement and support Hyperic resource monitoring and alerting.
Discover and Import Resources to Inventory

Auto-discovery is the process of identifying new and changed resources on a platform. The Hyperic Agent auto-discovers most platform, server, and service types. The auto-discovery functionality supported for a resource type is defined in plugin that manages it.

Generally speaking, the auto-discovery process works like this:

1. Upon first startup on a supported platform, the Hyperic Agent discovers the platform, and the manageable servers running on the platform.
2. You review auto-discovery results in Hyperic user interface, and upon your approval, the platform, the servers, and the services running on the platform and servers are added to Hyperic inventory.
3. The Hyperic Agent periodically scans the platform for new and changed resources. Like new resources, changes to resources must be approved before the changes are introduced to inventory.

The topics in this section describe how Hyperic resource auto-discovery works, and provide instructions for viewing auto-discovery results and importing discovered resources to Hyperic inventory.

Using the Auto-Discovery Portlet

Contents of the Auto-Discovery Portlet

The Auto-Discovery portlet on the Hyperic Dashboard lists recently added or modified platforms and servers, and allows an authorized user to view discovery details, and to import the new or changed resource data to the Hyperic database.

By default, the Auto-Discovery portlet lists the (up to) five most recently new or changed platforms. To set the maximum number of platforms that can appear in the list, see Configure the Number of Auto-Discoveries Displayed.

A platform appears in the Auto-Discovery portlet if it, or a server running on it, is new or changed. The rules are these:

- **The platform is new** — A platform appears as new in the portlet, if neither its IP address or FQDN match that of an existing platform in inventory. In this case, any new servers discovered on the platform appear below the platform in the portlet.
- **The platform has a new server** — A new server has been discovered on the platform since the last scan. The new server is listed below the platform.
- **Platform or server properties have changed** — One or more inventory properties for the platform, or for one or more of the servers running it, have changed since the last scan. Servers with changed properties are listed below the platform.
The image below shows the Auto-Discovery portlet after the agent was started for the first time on a platform.

![Auto-Discovery portlet]

The **Auto-Discovery** portlet presents the following information for each platform it contains:

- **Hostname** — The hostname of the platform is a link to a page — the **Auto-Discovery Results** page - that contains detailed information about the scan results for the platform and servers running there. See [Using the Auto-Discovery Results Page](#).
- **Platform type** — The resource type for the platform.
- **Status** — Indicates the type of change that was detected for a resource, either "new" or "modified".
- **Changes** — If the **Status** for a resource is "modified", the **Changes** column contains a summary of what changed. For example:
  - "server set changed" — Applies to platforms; this value indicates that changes to one or more servers on the platform were detected. The changed server(s) are listed below the platform.
  - "name change" — Indicates that the name of the resource has changed; a resource name can change when a resource is upgraded from one version to another, if version number forms a portion of the resource name, as is often the case.
  - "install path changed" — Indicates that the installation path for a server has changed; the installation path for a resource can change when a resource is upgraded from one version to another, if version number forms a portion of the path, as is often the case.
  - "IP set changed" — Indicates that the IP address has changed. When the agent detects an IP address not associated with an existing platform in inventory, it checks for a platform with a matching FQDN - if found, Hyperic recognizes the platform as existing.
  - "FQDN changed"
For each newly discovered or changed server on the platform:
- **Installation path** —
- **Status** — Indicates "new" or "modified"
- **Changes** — If Status is "modified", the Changes column contains a summary of what changed.

**About Discovery and Import of Services**
The Auto-Discovery Portlet does not display new or changed services. Services are discovered during a run-time scan and are automatically added to Hyperic inventory. For more information, see Resource Auto-Discovery Processes.

**Import or Skip Resources in Auto-Discovery Portlet**
You can process the contents of the Auto-Discovery Portlet in these ways:
- To import all resources—leave all resources selected, and click **Add to Inventory**.
- To skip all resources—leave all resources selected, and click **Skip Checked Resources**.
- To import selected resources—Either:
  - De-select the resources you do not want to add to inventory, and click **Add to Inventory**, or
  - De-select the resources you do want to add to inventory and **Skip Checked Resources**.

**About Skipped Resources**
If you do not import a resource displayed in the Auto-Discovery portlet, note:
- If you skip a new platform, you skip its servers as well.
- During the next platform scan, skipped resources will reappear in the portlet after the next scan that detects them. If you have resources that you do not want the agent to discover, see the relevant section in Options for Running and Controlling Resource Discovery.

If the Hyperic Agent discovered all of the resource properties required to monitor a resource, it starts monitoring that resource as soon as you add it to inventory. This is the case for most resource types. Note however, that some level of configuration is required to start managing some resources types - see the **Configuration Properties** section on a resource's **Inventory** tab for configuration requirements.
Configure the Number of Auto-Discoveries Displayed

To set the number of completed auto-discoveries displayed in the portlet, click the gear icon in the upper left corner of the portlet. On the Display Settings page, select "10" or "all", and click OK.

Using the Auto-Discovery Results Page

Learn About Auto-Discovery
See Resource Auto-Discovery Processes.

Contents of the Auto-Discovery Results Page

The Auto-Discovery Results page appears when you click a platform name in the Dashboard's Auto-Discovery portlet. The page shows the results of the most recent platform scan - the new or changed resource information that was discovered, as well as information for unchanged resources. You can filter the page for new, modified, or unchanged resources. You can selectively import new and changed data to inventory.

<table>
<thead>
<tr>
<th>Platform Type</th>
<th>Fully Qualified Domain Name: Marie-McGarrys-MacBook-Pro-19:local</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacOSX</td>
<td></td>
</tr>
<tr>
<td>Auto-Discovery Details</td>
<td>Properties State: Modified Properties</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Import Values/Dont Import</td>
</tr>
</tbody>
</table>

Network Properties - New, modified, or ignored values based on the current inventory of this platform.

<table>
<thead>
<tr>
<th>View: New</th>
<th>IP Address: 192.168.1.157</th>
<th>Netmask: 255.255.254.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address: 00:17:32:8f:19:00</td>
<td>Action:</td>
<td></td>
</tr>
<tr>
<td>Auto-Discovery Details</td>
<td>Properties State: Action: New Properties Import Values</td>
<td></td>
</tr>
</tbody>
</table>

Servers - - New, modified, or ignored values based on the current inventory of this Platform.

<table>
<thead>
<tr>
<th>View: All Server Types</th>
<th>New</th>
<th>Action: Import Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type</td>
<td>Install Path</td>
<td>Server Status</td>
</tr>
<tr>
<td>Marie-McGarrys-MacBook-Pro-19:local MacOSX FileServer</td>
<td>/</td>
<td>new</td>
</tr>
<tr>
<td>Marie-McGarrys-MacBook-Pro-19:local MacOSX ProcessServer</td>
<td>/</td>
<td>new</td>
</tr>
<tr>
<td>Marie-McGarrys-MacBook-Pro-19:local MacOSX NetworkServer</td>
<td>/</td>
<td>new</td>
</tr>
</tbody>
</table>

The Auto-Discovery Results page has three sections:

- **Platform Type** — This section contains the following data and controls:
  - **Platform Type** — The resource type of the platform.
  - **Fully Qualified Domain Name** — The platform's FQDN.
  - **Import Values/Do Not Import** (callout #1 in screenshot) — In this version of Hyperic, this control has no effect. Changing the value has no impact on what values are imported.
• **Network Properties** — This section contains the following data and controls:
  o **All States/New/Modified/Unchanged** selector (callout #2 in screenshot) — This pulldown allows you to filter the IP addresses that appear in the list by change state.
  o The following data is shown for each IP address matching the currently selected filter value:
    ▪ **IP Address**
    ▪ **Netmask**
    ▪ **MAC Address**
    ▪ **Properties State** — Value indicates if the connection properties are "New", "Unchanged", or "Changed".

• **Servers** — This section contains the following data and controls:
  o **Server Types** selector (callout #3 in screenshot) — This pulldown allows you restrict the list to servers of a particular type.
  o **All States/New/Modified/Unchanged** filter (callout #4 in screenshot) — This pulldown allows you to filter the servers that appear in the list by change state.
  o The following data is shown for each server in the list:
    ▪ **Server** — The name of the resource.
    ▪ **Server type** — The resource type of the server.
    ▪ **Install Path** — Where the server is installed
    ▪ **Server Status** — Value indicates whether the server is "New", "Unchanged", or "Modified."
    ▪ **Import Values/Do Not Import** (callout #5 in screenshot) — The value of this pull-down controls whether the server data will be imported when the **OK** button is clicked.

**Import or Skip Resources in Auto-Discovery Results Page**

To process the contents of the **Auto-Discovery Results** page:

1. View the new and changed properties in the **Network Properties** section of the page.
2. If you do not want to import the new or changed network properties to Hyperic inventory, select "Do Not Import" from the pulldown in the **Platform Type** section of the page (callout #1 in screenshot).
3. View the new and changed servers listed in the **Servers** section of the page.
4. For each each new or changed server:
   o If you do not want to import a new or changed server to Hyperic inventory, select "Do Not Import" from the pulldown in the **Action** column
5. Click **OK** to import the resource data which you have approved for import.
Configure Resources for Monitoring
If the Hyperic Agent discovered all of the resource properties required to monitor a resource, it starts monitoring that resource as soon as you add it to inventory. This is the case for most resource types. Note however, that some level of configuration is required to start managing some resources types - see the Configuration Properties section on a resource's Inventory tab for configuration requirements.

Options for Running and Controlling Resource Discovery

This section describes options for initiating and preventing Hyperic resource discovery processes.

For information about different types of auto-discovery scanning, see Resource Auto-Discovery Processes.

Scan a Platform On-Demand

To initiate a platform scan:

1. Navigate to the platform you want to scan.
2. Select New Auto-Discovery from the Tools menu.
   - The New Auto-Discovery page appears.

3. You can run default scan only, or run a file scan in addition to the default scan. The different scan types are described in Resource Auto-Discovery Processes.
   - To run a default scan only, click OK at the top of the page.
   - To run a file scan in addition to the default scan:
     i. Check the the Server Types that Hyperic should look for on the platform.
     ii. In ScanDirs, specify the directories that HQ should scan.
     iii. In ExcludeDirs, specify the directories that Hyperic should not scan.
     iv. In fsTypes, select the type of file system to scan: local disks, network-mounted disks, or both ("all").
     v. In depth, specify the depth in the directory structure to which HQ should scan.
     vi. To have Hyperic follow symlinks when scanning, check Should symlinks be followed.
     vii. Click OK at the bottom of the screen.

Some Platforms Cannot Be Scanned
You can only initiate an auto-discovery scan for a platform that runs an Hyperic Agent. Platforms that are remotely monitored, such as Cisco and other network device platforms that do not run an agent, cannot be scanned.
Configure Default and Runtime Scanning Frequency

Configure Frequency of Default Scan
By default, an HQ Agent runs a default scan upon startup and every 15 minutes thereafter. To change the frequency, uncomment the `autoinventory.defaultScan.interval.millis` line in the `agent.properties` file, and set the desired value in milliseconds.

- `autoinventory.defaultScan.interval.millis`

**Description**
Specifies how frequently the agent performs a default autoinventory scan. The default scan detects servers and platform services, typically using the process table or the Windows registry. Default scans are less resource-intensive than runtime scans.

**Default**
Commented out, set to 86,400,000 milliseconds, or 1 day.

Note however, that by default, the agent performs the default scan at startup and every 15 minutes thereafter.

Disable Default Scan
To prevent the HQ Agent from running default scans on the platform, uncomment the `autoinventory.defaultScan.interval.millis` property in the `agent.properties` file, and set it to "-1". For example:

`autoinventory.defaultScan.interval.millis=-1`

Configure Frequency of Runtime Scan
By default, an HQ Agent runs a runtime scan once a day. To change the frequency, edit the `autoinventory.runtimeScan.interval.millis` line in the `agent.properties` file, and set the desired value in milliseconds.

`autoinventory.runtimeScan.interval.millis`

**Description**
Specifies how frequently the agent performs a runtime scan. A runtime scan may use more resource-intensive methods to detect services than a default scan. For instance, a runtime scan may involve issuing an SQL query or looking up an MBean.

**Default**
86,400,000 milliseconds, or 1 day.
Exclude a Plugin Resource Hierarchy
If you do not want the Hyperic Agent to discover a resource, you can prevent the agent from loading the plugin. Specify the plugin or plugins that you do not want the agent to load at startup with the `agent.exclude` property in the `agent.properties` file on the platform.

Disable Platform Service Discovery
To disable auto-discovery of platform services, update `agent.properties` with the following property settings.

```
sigar.mirror.procnet
```

**Description**
mirror `/proc/net/tcp` on linux

**Default**
true

```
netservices.netstat
```

**Description**
Add the `netservices.netstat` property to `agent.properties` and set it to "false" to prevent the agent from auto-discovering network services running on the platform.

**Default**
As installed, `agent.properties` does not contain this property, and by default, an HQ Agent discovers network services running on a platform.

Disable Service Discovery for a Server Instance
If you do not want the agent to discover the services running in a server, you can disable the behavior in the Monitoring section of the Configuration Properties page for a server instance.
Manage Resource Auto-Discovery

Configure Auto-Discovery Frequency

Configure Frequency of Default Scan
By default, an HQ Agent runs a default scan upon startup and every 15 minutes thereafter. To change the frequency, uncomment the `autoinventory.defaultScan.interval.millis` line in the `agent.properties` file, and set the desired value in milliseconds.

- `autoinventory.defaultScan.interval.millis`

**Description**
Specifies how frequently the agent performs a default autoinventory scan. The default scan detects servers and platform services, typically using the process table or the Windows registry. Default scans are less resource-intensive than runtime scans.

**Default**
Commented out, set to 86,400,000 milliseconds, or 1 day.

*Note however, that by default, the agent performs the default scan at startup and every 15 minutes thereafter.*

Disable Default Scan
To prevent the HQ Agent from running default scans on the platform, uncomment the `autoinventory.defaultScan.interval.millis` property in the `agent.properties` file, and set it to "-1". For example:

```properties
autoinventory.defaultScan.interval.millis=-1
```

Configure Frequency of Runtime Scan
By default, an HQ Agent runs a runtime scan once a day. To change the frequency, edit the `autoinventory.runtime.Scan.interval.millis` line in the `agent.properties` file, and set the desired value in milliseconds.
autoinventory.runtimeScan.interval.millis

**Description**
Specifies how frequently the agent performs a runtime scan. A runtime scan may use more resource-intensive methods to detect services than a default scan. For instance, a runtime scan may involve issuing an SQL query or looking up an MBean.

**Default**
86,400,000 milliseconds, or 1 day.

### Scan a Platform On-Demand

To initiate a platform scan:

1. Navigate to the platform you want to scan.
2. Select **New Auto-Discovery** from the **Tools** menu.
   - The **New Auto-Discovery** page appears.

   **Some Platforms Cannot Be Scanned**
   You can only initiate an auto-discovery scan for a platform that runs an Hyperic Agent. Platforms that are remotely monitored, such as Cisco and other network device platforms that do not run an agent, cannot be scanned.

3. You can run default scan only, or run a file scan in addition to the default scan. The different scan types are described in **Resource Auto-Discovery Processes**.
   - To run a default scan only, click **OK** at the top of the page.
   - To run a file scan in addition to the default scan:
     i. Check the the **Server Types** that Hyperic should look for on the platform.
     ii. In **ScanDirs**, specify the directories that HQ should scan.
     iii. In **ExcludeDirs**, specify the directories that Hyperic should *not* scan.
     iv. In **fsTypes**, select the type of file system to scan: local disks, network-mounted disks, or both ("all").
     v. In **depth**, specify the depth in the directory structure to which HQ should scan.
     vi. To have Hyperic follow symlinks when scanning, check **Should symlinks be followed**.
     vii. Click **OK** at the bottom of the screen.
Prevent Resource Discovery

This section describes options for preventing Hyperic resource discovery processes.

For information about different types of auto-discovery scanning, see Resource Auto-Discovery Processes.

Configure an Agent to Not Load a Plugin

If you do not want a Hyperic Agent to discover a resource, you can prevent the agent from loading the plugin. Specify the plugin or plugins that you do not want the agent to load at startup with the `agent.exclude` property in the `agent.properties` file on the platform.

Remove Plugin from All Agents

You can remove a plugin from all agents with Plugin Manager. For more information, see Plugin Deployment and Management.

Disable Platform Service Discovery

To disable auto-discovery of platform services, update `agent.properties` with the following property settings.

```
sigar.mirror.procnet
```

**Description**
mirror `/proc/net/tcp` on linux

**Default**
true

```
netservices.netstat
```

**Description**
Add the `netservices.netstat` property to `agent.properties` and set it to "false" to prevent the agent from auto-discovering network services running on the platform.

**Default**
As installed, `agent.properties` does not contain this property, and by default, an HQ Agent discovers network services running on a platform.

Disable Service Discovery for a Server Instance

If you do not want to the agent to discover the services running in a server, you can disable the behavior in the Monitoring section of the Configuration Properties page for a server instance.
**Solving Auto-Discovery Problems**

Refer to the sections below if you have trouble with resource discovery.

**Removed Resources Not Rediscovered**

If you delete a resource, and then immediately scan the platform, it is possible that the deleted resource will not be rediscovered during that scan.

In Hyperic, the resource deletion process is asynchronous. If you delete many resources at once, if the deletion of a resource is not complete when the next scan is performed, the agent will find the resource already exists, and not report it as new or changed.

**Discovered Resources Not Imported**

If a resource still appears in the Auto-Discovery Portlet after you clicked Add to Inventory to import it to inventory, you can use HQ Health to troubleshoot the problem. Use the available database queries to check the autoinventory queue - if the resource you wish to add appears in the queue, use the Purge Autoinventory Queue action. Initiate an auto-discovery scan and try importing the resource after it is re-discovered.

**Auto-Discovering WebLogic Server on Linux and Solaris**

To auto-discover a WebLogic Server instance on Linux or Solaris, the Hyperic Agent must be able to read its current working directory /proc/$pid/cwd. To ensure that the agent has sufficient privileges, you can:

- Run the Hyperic Agent as the same user that runs the WebLogic Server Administration Server,
- Run the Hyperic Agent as root, or
- Under Solaris 10 only, grant the agent account permission to read /proc/$pid/ files within the Solaris 10 Least Privilege Model (LPM). For instructions, see Configure Agent Account Privileges under Solaris 10 in Getting Started with vFabric Hyperic.

For additional information about solving problems with auto-discovery of WebLogic Server, see WebLogic Server.

**Auto-Discovering Server Types on Solaris**

A Hyperic Agent can fail to auto-discover some types of servers running under Solaris for a combination of reasons.

Solaris limits the length of the publicly-viewable process arguments struct member to 80 bytes, which can result in truncation of process arguments that the agent needs to read. To obtain all arguments, the agent will attempt to access the process address space file{{/proc/$pid/as}} and fail, if it lacks permission.
If the Hyperic Agent does not auto-discover servers under Solaris, run the agent as root, or grant the agent account permission to read /proc/$pid/ files within the Solaris 10 Least Privilege Model (LPM). For instructions, see Configure Agent Account Privileges under Solaris 10 in Getting Started with vFabric Hyperic.

Set Up Alert Notifications and Escalations

Tailor Alert Notification Templates

Groovy Server Pages Define Notification Content and Format

The content and format of alert notifications are governed by Groovy Server Pages in \server-n.n.n-EE\hq-engine\hq-server\webapps\ROOT\WEB-INF\alertTemplates.

- subject.gsp - defines the subject line in email notifications
- html_email.gsp - defines the body of an HTML email alert notification
- text_email.gsp - defines the body of a text email alert notification
- sms_email.gsp - defines the body of an SMS alert notification
- opennms_notify.gsp - defines an OpenNMS SNMP trap
- snmp_trap.gsp - defines an SNMP trap

The following sections describe the content of each type of notification.

Email Notifications

Recipients can be specific HQ users, all HQ users with a given role, or external recipients. Email to an HQ user is sent in the mail format specified in the user’s HQ user profile.

Email Notification Subject Line

The subject line of an email notification contains the string "HQ" followed by the alert priority, the alert definition name, the name of the resource for which the alert conditions were met, and the alert status.

```
[HQ] ${priority} - ${alertDef.name} ${resource.name} ${status}
```

For example, this subject line:

```
[HQ]!! - High Disk Usage saint Win32 File System R:\(remote/NTFS)
```

notifies the recipients of a medium priority alert named "High Disk Usage" that was triggered for the resource whose name is "saint Win32 File System R:\(remote/NTFS)".
Email Notification Body

The body of the alert notification provides these details:

- Resource name
- Alert name
- Alert date/time
- Triggering condition, for instance, the threshold value for the alert and the actual value that triggered the alert
- Alert severity
- For an Alert on an individual resource, the last value of each of the resource's indicator metrics before the alert was triggered
- For group alerts, an "Additional Information" section that lists the group's specific member resources that triggered the alert and a link to a metric chart showing the triggering metric values
- A link to the alert detail in the Hyperic user interface.

Variables Available for Notification Templates

The table below lists the alert-related class fields you can reference as variables in the .gsp templates that govern the content of alert notifications.

You can insert a variable of this form:

$ClassVar.FieldVar

where `ClassVar` is the class with the field, and `FieldVar` is a field for which the class contains a `get()` method.

For example, this variable

`${alertDef.description}`

renders the alert definition description from an AlertDefinitionInterface class.

Append the variable for the desired field to the variable of class that provides it, with a dot (.) separator to specify the variable for a field.

<table>
<thead>
<tr>
<th>For data about</th>
<th>from this class</th>
<th>use this class variable</th>
<th>and a field variable</th>
<th>resulting in</th>
</tr>
</thead>
<tbody>
<tr>
<td>The alert definition for the fired alert</td>
<td>AlertDefinitionInterface</td>
<td>alertDef</td>
<td>description id name priority</td>
<td>alertDef.description alertDef.id alertDef.name alertDef.priority</td>
</tr>
<tr>
<td>The fired alert</td>
<td>AlertInterface</td>
<td>alert</td>
<td>id timestamp</td>
<td>alert.id alert.timestamp</td>
</tr>
<tr>
<td>For data about...</td>
<td>from this class..</td>
<td>use this class variable</td>
<td>and a field variable....</td>
<td>resulting in...</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Alert actions</td>
<td>ActionExecutionInfo</td>
<td>action</td>
<td>longReason</td>
<td>action.longReason</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>shortReason</td>
<td>action.shortReason</td>
</tr>
<tr>
<td>Resource that fired the alert</td>
<td>Resource</td>
<td>resource</td>
<td>instanceid</td>
<td>resource.instanceid</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>mtime</td>
<td>resource.mtime</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>owner</td>
<td>resource.owner</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>prototype</td>
<td>resource.prototype</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>resourceType</td>
<td>resource.resourceType</td>
</tr>
<tr>
<td>Notification recipients</td>
<td>AuthzSubject</td>
<td>user</td>
<td>active</td>
<td>user.active</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>department</td>
<td>user.department</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>emailAddress</td>
<td>user.emailAddress</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>firstName</td>
<td>user.firstName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>fullName</td>
<td>user.fullName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>htmlEmail</td>
<td>user.htmlEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>lastName</td>
<td>user.lastName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>phoneNumber</td>
<td>user.phoneNumber</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>smsAddress</td>
<td>user.smsAddress</td>
</tr>
<tr>
<td>status of an alert</td>
<td>no class variable required</td>
<td>status</td>
<td>status</td>
<td>status</td>
</tr>
<tr>
<td>Note: May be used only in subject.gsp.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>whether an escalation action is an SMS notification</td>
<td>no class variable required</td>
<td>IsSms</td>
<td>IsSms</td>
<td>IsSms</td>
</tr>
<tr>
<td>Note: May be used only in subject.gsp.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configure Roles for Role-Based Alert Notifications

Roles for Alert Notifications
In addition to using roles to grant access to permissions and resources, you can use roles to satisfy your alert notification requirements. When you create an alert definition, you can designate one or more roles to be notified when the alert fires. Designating a role to be notified is easier than designating individual users. Role-based notifications also simplify notification rule management - you can add or remove users from the role, instead of adding or removing individual users to be notified when alerts fire.

Typically, you create roles specifically for use in alert definitions. Roles created for use in alert definitions have no permissions and no assigned resource groups - only users.

Follow the Sun Alerting with Role-Based Alert Calendars
If you use role-based alert notifications, you can specify an Alert Calendar that dictates when users assigned to a role can be notified about an alert. The purpose of this calendar is to ensure that the appropriate people are notified at the appropriate times of the day (for example, a worker in California doesn't want to be notified of an alert at 4 a.m. PST, but a worker in New York can be notified at the same time, which is 7 a.m. EST) when an alert is triggered.

The alert calendar can be most usefully applied in an escalation scheme, wherein multiple sets of people can be selected for notification, but only the one whose alert calendar is currently open will be notified.

You set up multiple roles, each with a unique alert calendar that spans different time periods, that together cover the calendar. You create an escalation with one or more notification actions (email or SMS), and assign all of the roles that span the calendar to the notification action(s) in the escalation. When the alert fires, only the users in the role whose calendar is currently open will be notified.

Creating Roles
An authorized user can access the New Role command in the Administration tab of the HQ user interface.

You can also create HQ roles using the HQApi role command.
Enable SNMP Trap Notifications

This section has information about enabling vFabric Hyperic to send SNMP traps to an SNMP management system.

Note: For information about enabling Hyperic to receive traps, see Configuring Hyperic as an SNMP Trap Receiver.

Configure HQ Server to Send SNMP Traps

1. Click HQ Server Settings on the Administration page.
2. At the bottom of the page, in the "SNMP Server Configuration Properties" section, define the properties for your version of SNMP. See the appropriate section below.

Configure vFabric Hyperic Server for SNMP v1

Select "v1" from the SNMP Protocol Version pulldown and supply values for the properties defined in the table below.

The table below defines the properties for configuring Hyperic Server for SNMP V1 communications with an NMS.

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
<th>Allowable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap OID</td>
<td>The OID of the notification to be sent. Supplies the value of snmpTrapOID.0 - the second varbind in a trap or inform that Hyperic Server generates. (The first varbind is SysUpTime.0.)</td>
<td></td>
</tr>
<tr>
<td>Default Notification Mechanism</td>
<td>Your selection governs the notification type that will appear as the default notification type option in the &quot;Notification Mechanism&quot; pulldown list that is presented in configuration dialogs when user configures an SNMP notification as an alert action, or as a step in an escalation.</td>
<td>For v1 of the SNMP protocol, choose V1 Trap. This is the only trap type you can generate for SNMP v1.</td>
</tr>
<tr>
<td>Enterprise OID</td>
<td>Enterprise OID.</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>The community name to be sent with the trap.</td>
<td></td>
</tr>
</tbody>
</table>
| Generic ID | Single digit identifier of the trap type. | 0 - coldStart  
1 - warmStart  
2 - linkDown  
3 - linkUp  
4 - authenticationFailure  
5 - egpNeighborLoss  
6 - enterpriseSpecific |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific ID</td>
<td>The specific trap code for an enterprise-specific trap (when <strong>Generic ID</strong> is set to to 6).</td>
<td></td>
</tr>
<tr>
<td>Agent Address</td>
<td>Address of the managed object that generates the trap.</td>
<td></td>
</tr>
</tbody>
</table>

**Configure vFabric Hyperic Server for SNMP v2c**

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
<th>Allowable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap OID</td>
<td>The OID of the notification to be sent. Supplies the value of <code>snmpTrapOID.0</code> - the second varbind in a trap or inform that Hyperic Server generates. (The first varbind is <code>SysUpTime.0</code>.)</td>
<td></td>
</tr>
</tbody>
</table>
| Default Notification Mechanism | Specifies the default notification type that will appear in configuration dialogs when an authorized user configures an SNMP notification as an alert action, or as a step in an escalation. This choice simply defines the default option - the user configuring an alert action or escalation can choose a different message type. | • V1 Trap  
• V2c Trap  
• Inform |
| Community | The community name to be sent with the trap. |
Configure vFabric Hyperic Server for SNMP v3

This section lists the properties for enabling vFabric Hyperic to send SNMP notifications to an NMS. When Hyperic is so enabled, you can use SNMP notifications in alert definitions - as alert actions and escalation steps.

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
<th>Allowable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap OID</td>
<td>The OID of the notification to be sent. Supplies the value of snmpTrapOID.0 - the second varbind in a trap or inform that Hyperic Server generates. (The first varbind is SysUpTime.0.)</td>
<td></td>
</tr>
<tr>
<td>Default Notification Mechanism</td>
<td>Specifies the default notification type that will appear in configuration dialogs when an authorized user configures an SNMP notification as an alert action, or as a step in an escalation. This choice simply defines the default option - the user configuring an alert action or escalation can choose a different message type.</td>
<td>V1 Trap, V2c Trap, Inform</td>
</tr>
<tr>
<td>Security Name</td>
<td>The username Hyperic's SNMP agent should use when sending notifications to the NMS.</td>
<td>Required.</td>
</tr>
<tr>
<td>Local Engine ID</td>
<td>ID of Hyperic's SNMP agent; this value appears automatically, and is not user-configurable.</td>
<td></td>
</tr>
<tr>
<td>Auth Protocol</td>
<td>The SNMP authentication protocol Hyperic Server should use for communications with the NMS.</td>
<td>none, MD5, SHA</td>
</tr>
<tr>
<td>Auth Passphrase</td>
<td>The SNMP authorization passphrase configured for use when communication with the NMS.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration Option

**Privacy Protocol**
The SNMP Privacy Protocol Hyperic Server should use for communication with the NMS.

- none
- DES
- 3DES
- AES-128
- AES-192
- AES-256

**Privacy Passphrase**
The SNMP privacy passphrase configured for use when communication with the NMS.

**Context Engine ID**
The EngineID of the NMS. This, along with Context Name, identifies the SNMP context for accessing management data.

Required for v1 and v2c traps. Do not supply for Inform.

**Context Name**
The name of the SNMP context that provides access to management information on the NMS. A context is identified by the Context Name and Context Engine ID.

### Using SNMP Traps in Alert Definitions

After the configuration above is complete, the “SNMP Trap” notification tab is available when you define or edit an alert definition.

### Enable Syslog Notifications for Escalations

#### About Syslog Notifications in Alert Escalations

You can enable Hyperic to issue a syslog notification as a step in an alert escalation. The notification will log a line in the following format:

```
SyslogAction[ALERT_ID]: DB_1 4 META/PRODUCT/VERSION RESOURCE_NAME : ALERT_NAME - ALERT_CONDITION
```

where:

- **ALERT_ID** is a number representing the alert ID in HQ.
- **META** is the "Meta" string configured for the syslog action in the escalation.
- **PRODUCT** is the "Product" string configured for the syslog action in the escalation.
- **VERSION** = is the "Version" string configured for the syslog action in the escalation.
• RESOURCE_NAME identifies the resource for which the alert was fired.
• ALERT_NAME identifies the alert definition that fired the alert.
• ALERT_CONDITION is the alert condition and reported measurement that led to the alert firing, for example, "If Availability > 0.0 (actual value = 1")"

Enable Syslog Notifications

You enable syslog notification in the HQ Server's server-log4j.xml file, in SERVER_HOME/conf.

Enable the Syslog Receiver

syslogd, the syslog receiver, must be enabled to accept remote logging, even on localhost. This can be done by passing -r to syslogd at startup.

Enable Syslog Appender

In the appenders section of the file, uncomment these lines and change the logger level to INFO instead of ERROR.

```xml
<appender name="SYSLOG" class="org.apache.log4j.net.SyslogAppender">
    <errorHandler class="org.apache.log4j.helpers.OnlyOnceErrorHandler" />
    <param name="Facility" value="SYSLOG" />
    <param name="FacilityPrinting" value="true" />
    <param name="SyslogHost" value="localhost" />  
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%c{1} [%r]: %m%n" />
    </layout>
</appender>

<logger name="org.hyperic.hq.bizapp.server.action.log.SyslogAction">
    <level value="INFO" />
    <appender-ref ref="SYSLOG" />
</logger>
```

Note: If you want to configure a different Facility for the appender, note that it must be syslog-configured.

If server-log4j.xml does not contain the lines shown above, add them in the appenders section. All appenders in the file must be grouped together.

Restart Hyperic Server

After the Hyperic Server is restarted, syslog notification will be presented as an option when you set up an escalation.
Configure and Manage Escalations

For a description of the functionality that escalation schemes enable in Hyperic, see Introduction to Escalations.

Create an Escalation

Step 1 - Create New Escalation Scheme

1. Click Administration in the masthead.
2. Click Escalation Schemes Configuration.
3. Enter values in the Name and optionally, the Description fields.
4. Configure acknowledgment options in the "If the alert is acknowledged" section:
   - **Allow user to pause escalation for** - Click to enable a user to pause the escalation when acknowledging the alert. Select "Until Fixed" or a duration from the pulldown list. (Options range from 5 minutes to 72 hours.) A user acknowledging an alert with this escalation will have the option to pause the escalation process for the period you specify.
   - **Continue escalation without pausing** - With this default value, a user acknowledging an alert with this escalation will not be offered the option to pause the escalation.
5. Configure state change notification options in the "If the alert state has changed" section:
   - **Notify previously notified users of the change** - With this default setting, when the state of the alert changes, state change notifications will be sent only to recipients who have already received a notification in previous escalation steps.
   - **Notify entire escalation of the change** - Click if you want alert state change notifications to be sent to every notification recipient in the escalation - whether or not they have received a previous notification.
6. Configure escalation repeat behavior in the "If alert is fixed" section:
   - **Stop escalation execution** - With this default setting, the escalation will not be repeated for an alert that is unfixed at the end of the escalation.
   - **Repeat escalation actions** - Click to repeat the escalation process if the alert has not been fixed by the end of the escalation.
7. Click Next Step.

Step 2 - Create Escalation Actions

After performing Step 1 - Create New Escalation Scheme:

1. On the Escalation Configuration page, click Create Action.
2. In the Create Escalation Scheme Actions section, select an action type and proceed to the directions for that type.
   - Email - Create an Email or SMS Action
   - SMS - Create an Email or SMS Action
   - Sys Log - Create a Sys Log Action
- SNMP Trap - [Create an SNMP Notification Action](#)
- Suppress Alert - [Create a Suppress Alerts Action](#)

**Create an Email or SMS Action**

After selecting the “Email” or “SMS” action type:

1. Select a notification target type from the **Choose Who to Notify** pulldown:
   - Notify Roles* - You will be prompted to select one or more Hyperic roles. The Hyperic users with those role assignments will be notified.
   - Notify HQ Users - You will be prompted to select one or more Hyperic users to be notified.
   - Notify Other Recipients - You will be prompted to enter a comma-separated email list of the email addresses for the individuals you be notified.

2. Leave “continue” selected if you want the next step in the escalation to occur immediately after the current one. To specify a delay before the next step is performed, select an interval from the pulldown. The intervals range from 5 minutes to 24 hours.

3. Click **Save**.

4. Repeat **Step 2 - Create Escalation Actions** to add another step to the escalation, as desired

**Create a Sys Log Action**

This option is available if the configuration described in **Enable Syslog Notifications for Escalations** has been performed.

After selecting the “Sys Log” action type:

1. Supply the value for these segments of the syslog message:
   - meta
   - product
   - version

2. Leave “Then continue” selected if you want the next step in the escalation to occur immediately after the current one. To specify a delay before the next step is performed, select an interval from the pulldown. The intervals range from 5 minutes to 24 hours.

3. Click **Save**.
4. Repeat Step 2 - Create Escalation Actions to add another step to the escalation.

**About Syslog Notifications**

You can enable Hyperic to issue a syslog notification as a step in an alert escalation. The notification will log a line in the following format:

```
SyslogAction[ALERT_ID]: DB_1 4 META/PRODUCT/VERSION
RESOURCE_NAME : ALERT_NAME - ALERT_CONDITION
```

where:

- **ALERT_ID** is a number representing the alert ID in HQ.
- **META** is the "Meta" string configured for the syslog action in the escalation.
- **PRODUCT** is the "Product" string configured for the syslog action in the escalation.
- **VERSION** is the "Version" string configured for the syslog action in the escalation.
- **RESOURCE_NAME** identifies the resource for which the alert was fired.
- **ALERT_NAME** identifies the alert definition that fired the alert.
- **ALERT_CONDITION** is the alert condition and reported measurement that led to the alert firing, for example, "If Availability > 0.0 (actual value = 1)"

**Create an SNMP Notification Action**

You can define an SNMP notification to be performed as a step in an escalation if the Hyperic Server is configured for your NMS. See "SNMP Server Configuration Properties" on Hyperic Server Settings help page for more information.

The trap or inform sent when the escalation step is performed will contain three variable bindings:

- **sysUptimeOID.0** - No configuration is required for this binding.
- **snmpTrapOID.0** - This binding is configured on the HQ Server settings page. You can customize this variable for a specific action.
- A variable binding for the alert data specified in `snmp_trap.gsp`, a Groovy Server Page template that returns the alert definition name and the "short reason" for firing. This template can be customized, as desired. For more information, see Tailor Alert Notification Templates.
- any additional variable bindings you define.

To configure an SNMP notification as an escalation step:

1. After selecting the "SNMP Notification" action type, enter:
   - **IP Address** - Enter the address and port of the target SNMP server.
   - **Use Default SNMP Trap OID** – By default, this checkbox is selected. You need to clear the checkbox if you want to specify your own SNMP Trap OID.
   - **SNMP Trap OID** – You can optionally specify a Trap OID other than the default.
- **Notification Mechanism** - Choose the type of notification to send.
  - v1 Trap
  - v2c Trap
- Inform - not supported if Hyperic Server is configured for SNMP v1.
- **OID** - Enter the OID of the notification that will contain the alert details specified in the in snmp_trap.gsp, template.

2. For each additional variable binding you wish to add, click **Add Another Variable Binding** and enter:
   - **OID** - Enter an additional OID to include in the notification.
   - **Value** - Enter a value for the OID. You can enter plain text, or an alert variable.
     For more information, see Variables Available for Notification Templates.

3. Leave "Then continue" selected if you want the next step in the escalation to occur immediately after the current one. To specify a delay before the next step is performed, select an interval from the pulldown. The intervals range from 5 minutes to 24 hours.

4. Click **Save**.

5. Repeat **Step 2 - Create Escalation Actions** to add another step to the escalation.

### Create a Suppress Alerts Action

This action stops the alert from repeated firing - it is useful if the alert definition for the fired alert is not is not configured to "fire once until fixed", and but you want to stop repetitive firing at a specific point in the escalation process. After this step in the escalation process is performed, the alert will not fire again until fixed.

After selecting the "SNMP Notification" action type:

1. Leave “Then continue” selected if you want the next step in the escalation to occur immediately after the current one. To specify a delay before the next step is performed, select an interval from the pulldown. The intervals range from 5 minutes to 24 hours.

2. Click **Save**.

3. Repeat **Step 2 - Create Escalation Actions** to add another step to the escalation.

### View an Escalation

To view an escalation:

1. Click **Administration** in the masthead.
2. Click **Escalation Schemes Configuration**.
3. In the "Escalation Name" panel on the left side of the page, click the escalation's name.
   - The escalation details appear on the right side of the page.

### Edit an Escalation

Edits to an escalation scheme take effect for all alert definitions to which the escalation has previously been assigned. When you edit an escalation, you can:

- Edit an escalation's **Name**, **Description**, and its acknowledgment, notification, and repeat behaviors.
• Delete actions from an escalation.
• Add actions to an escalation.

You cannot edit an escalation action, you must delete it and create a new action.

To edit an escalation:

1. Navigate to the escalation as described in View an Escalation.
2. To change the scheme's Name, Description, or high-level instructions, click Edit, change the values, and click Save.
3. To delete an existing action, click Delete to the right of the action.
4. To create a new action, choose an action type and and follow the instructions in Step 2 - Create Escalation Actions.

**Editing an Escalation Affects Escalations in Progress**
When you edit an escalation scheme, HQ will immediately stop executing any escalations that are in progress for alerts to which the escalation is assigned. Note that once an escalation for an alert has been stopped: * The alert cannot be acknowledged.

• No further notifications of alert state changes will be issued. So, although an alert with a stopped escalation can be "fixed", notification recipients configured for the escalation will not be notified that the alert was fixed.

**Delete an Escalation**
To delete an escalation:

1. Navigate to the escalation as described in View an Escalation.
2. In the "Escalation Name" section, click Delete to the right of the scheme's name.

**Deleting an Escalation Affects Associated Alerts and Escalations in Progress**
When you delete an escalation scheme:

• HQ will immediately stop executing any escalations that are in progress for alerts to which the escalation is assigned.

• The escalation will be removed from any alert definition to which the escalation is was assigned; when an alerts that had the escalation fires, the escalation process will not be performed.

**Set Up Alert Action Script**

**Define a Script Action for an Alert**
A script action allows you to access and use Hyperic environment variables that contain information about a fired alert. You can use the data in any fashion you wish, for instance in a web service call to external management system.
To use the script action feature, write a script that implements the action or logic you wish to perform with the alert-related environment variables. When you configure the alert, specify the script to be executed when the alert fires. The script is server-side only, meaning it must be accessible and executable by the same user running the HQ Server process.

**Agent-side Scripts**

If you wish to execute agent-side scripts, see [Configure a Custom Control Action](#).

Script actions can be defined for resource alerts and resource type alerts. In this version of Hyperic, escalation schemes do not support script actions.

**Script actions are synchronous**

Script actions execute one at a time. Until a script action completes, additional alerts will not fire on the resource.

**Script actions and memory**

Script actions are forked by the Hyperic Server's Java process. Most operating systems duplicate the Java process's memory before executing the new process; exact behavior varies by operating system. If the operating system does not provide for over-committing memory, script execution requires an amount of free memory equal to the amount of memory that the Hyperic Server's Java process consumes — otherwise, the script action will not run.

**Environment Variables for Fired Alert Data**

The environment variables for fired alert data are prefixed with the string "HYPERIC_". The table below describes the variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Example Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>HYPERIC_ALERT_ALERT_TIME</td>
<td>The time at which the alert fired, in milliseconds from epoch.</td>
<td>1219167000000</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Example Output</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>HYPERIC_ALERT_CONDITION</td>
<td>The condition that caused the alert to fire. Note: This environment variable is supported only on Unix-based platforms. The value contains the Java \n character, which causes errors under Windows. In Windows environments, use the HYPERIC_ALERT_SUMMARY variable, which provides the same information without the \n character.</td>
<td>If Load Average 5 Minutes &gt; 1.0 (actual value = 1.4)</td>
</tr>
<tr>
<td>HYPERIC_ALERT_DESCRIPTION</td>
<td>The description of the alert that fired.</td>
<td>This alert will fire when the load rises</td>
</tr>
<tr>
<td>HYPERIC_ALERT_ID</td>
<td>The internal Hyperic ID for the alert that fired. <strong>Note:</strong> The HYPERIC_ALERT_ID for an alert is not committed to the Hyperic database until all alert actions are complete. Therefore, an alert action script (whether it uses SQL or HQApi) cannot query or update the Hyperic database using the alert's HYPERIC_ALERT_ID, because that value will not yet exist in the Hyperic database.</td>
<td></td>
</tr>
<tr>
<td>HYPERIC_ALERT_NAME</td>
<td>The name of the alert that fired.</td>
<td>High Load</td>
</tr>
<tr>
<td>HYPERIC_ALERT_PRIORITY</td>
<td>The priority of the alert that fired, 1 for High, 2 for Medium, 3 for Low.</td>
<td>2</td>
</tr>
<tr>
<td>HYPERIC_ALERT_SUMMARY</td>
<td>A condensed data string that contains the relevant alert and resource names and values which triggered the alert.</td>
<td>Mac OS X DOWN The-Idea-Men Availability (0.0%)</td>
</tr>
</tbody>
</table>
### Variable Description Example Output

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Example Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>HYPERIC_FIXED_ALERT_ID</td>
<td>This variable was added in Hyperic 4.5.1.2. Valid for recovery alerts only. Supplies the internal Hyperic ID for the primary alert to which the recovery alert is assigned.</td>
<td></td>
</tr>
<tr>
<td>HYPERIC_FIXED_ALERT_NAME</td>
<td>This variable was added in Hyperic 4.5.1.2. Valid for recovery alerts only. Supplies the name of the primary alert to which the recovery alert is assigned.</td>
<td>High Load</td>
</tr>
<tr>
<td>HYPERIC_PLATFORM_NAME</td>
<td>The platform on which this alert fired.</td>
<td>localhost.hyperic.com</td>
</tr>
<tr>
<td>HYPERIC_RECOVERY_ALERT</td>
<td>A boolean that indicates if the alert is a recovery alert.</td>
<td>false</td>
</tr>
<tr>
<td>HYPERIC_RESOURCE_ID</td>
<td>The internal ID for the resource for which the alert fired.</td>
<td></td>
</tr>
<tr>
<td>HYPERIC_RESOURCE_NAME</td>
<td>The name of the resource for which the alert fired.</td>
<td>localhost.hyperic.com</td>
</tr>
</tbody>
</table>

### Example Script

The following script is an example of using the alert variables. The example script simply writes the time that the script executed and the variables to a log file; it is not a representative use case. The purpose of script actions is to enable more complex alert actions, and actions that meet the unique needs of your environment.

```perl
#!/usr/bin/perl
my $logfile = "/tmp/output.txt";
my $date = localtime();
open LOGFILE, ">$logfile" or die "Cannot open log file for writing";
print LOGFILE "# Running script at $date", "\n";
foreach $key (sort keys(%ENV)) {
    if ($key =~ m/^HYPERIC$/) {
        my $msg = "$key = $ENV{$key}";
        print LOGFILE $msg, "\n";
    }
}
close LOGFILE;
```
Assign the Script Action to an Alert

To assign a script action to an alert definition:

1. Select the alert definition.
2. Click the Script tab in the Alert Definition page.
3. Enter the full path to script and click Set.

Configure a Custom Control Action

This section has instructions for how to configure Hyperic to run a script or executable that implements a resource control action. To learn about control actions in Hyperic see Run Resource Control Actions.

Step 1 - Install Executable

Install the executable that implements the control action on each managed platform where it will be used. Note that the account under which the Hyperic Agent runs must have:

- Adequate permissions to run the file.
- Adequate permissions to perform the tasks defined in the executable.

You can control the permissions required to run the file with chmod or an equivalent utility in your environment. If the tasks defined in the executable require permissions not granted to the account the Hyperic Agent runs under, one option is to add specific "NOPASSWD" entries in the sudoers file on the platform.

As a best practice, create a "control_scripts" (or similar) directory in /opt/hyperic, or a directory high enough in the agent installation that it will not be overwritten during an agent upgrade.

Step 2 - Configure Control Action as a Platform Service

In this step, you must configure the means by which an authorized user can invoke the custom control action. To do so, you configure it as a platform service of type "FileServer File Service" on each platform where the action will be used.

1. Browse to the platform in the Resource Hub.
2. Select "New Platform Service" from the Tools menu.
3. Name the service.
   - Note: Including the platform name in the name for the new service will help you distinguish it from other services of the same type.
4. (Optional) Describe the functionality of the control action in "Description".
5. Select "FileServer File" from the "Service Type" pulldown.
6. Click OK.
   - The Inventory page for the new platform service appears.
7. Click Edit in the "Configuration Properties" section of the Inventory page.
   - The Configuration Properties page for the new platform service appears.
8. On the Configuration Properties page:
   a. path — Enter the path to the executable in the "path" field in the "Shared" section, including the name of the file itself. This can be a relative path if the executable is in the Hyperic Agent directory structure. A better practice is to store the script external to the agent directory structure, and specify the full path to the executable, for example, /opt/hyperic/control_scripts/test.sh.
   b. timeout — Check the value in the "timeout" field in the "Control" section. This is the time in seconds HQ will wait for a response from the control before declaring it as a failed action. The default is 30 seconds, and under most circumstances should be adequate.
9. If the executable requires higher privileges than those available to the account running the Hyperic Agent, you can use the "prefix" field in the "Control" section to specify the sudo command. In this case, the local sudoers file has an entry for the user to run the script with a NOPASSWD directive.
10. Click OK.
Configure Monitoring and Alerting for a Resource

Configure Metric Baselines

Learn About Baselines
See Baselines.

Configure Global Baselining Properties
You configure the properties that control baseline calculations on the HQ Server Settings page, available on the HQ Administration tab.

In vFabric Hyperic, these properties control the baselining process. Changing the data set used to calculate baselines can affect baseline accuracy.

<table>
<thead>
<tr>
<th>Server Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline Frequency</td>
<td>The frequency with which Hyperic calculates a baseline for each metric.</td>
<td>3 days</td>
</tr>
<tr>
<td>Baseline Dataset</td>
<td>The time range of metric data used in calculating the baseline.</td>
<td>7 days</td>
</tr>
<tr>
<td>Baseline Minimum Data Points</td>
<td>The minimum number of data points used in calculating a baseline.</td>
<td>40</td>
</tr>
<tr>
<td>Track Out-of-Bounds Metrics</td>
<td>Controls whether or not Hyperic tracks out-of-bounds metrics — measurements that are greater than expected high range for a metric, or less than the expected low range for a metric.</td>
<td>off</td>
</tr>
</tbody>
</table>

Recalculate Baselines for a Resource
The baseline and expected high and low range values for every metric are calculated periodically — by default, every three days.

For an individual resource, you can recalculate baseline and high/low range values on-demand; when you do, the calculation will be based on the currently selected metric display range. Note that, the next time Hyperic does its periodic baseline calculations, baselines will again be based on the configured "Baseline Dataset" property.

To recalculate the metric baseline and expected range values for one or more metrics for a resource.
1. Navigate to the **Metric Data** tab on the resource's **Monitor** page.

2. Set the metric display range upon which you wish to calculate baselines.

3. Checkmark each metric whose baseline values you want to set.

4. Click **Set Baselines**.

The "Low Range", "Baseline", and "High Range" values for the selected metrics will be set to the low, average and peak values for the current display range.

You can also initiate re-calculation of the baseline values for a single resource metric when you chart the metric. See the following section for more information.

**Reset Baselines for a Charted Metric**

To recalculate baselines for an individual metric from a metric chart:
1. Chart the metric whose baseline you want to recalculate — click the chart icon next to it on the Metric Data minitab.

2. Click **Edit Range**, select the desired period of history upon which to base the baseline, and redraw the chart.

3. In the "Metric Baseline & Expected Range" section, click **Change Value** next to the **Baseline** field.
   A new baseline value is displayed. For example:
   
   New value calculated from current Display Range: 26.5 MB

4. Click **Save Value** to save the calculated value as the baseline value for the metric.
   New values for "High Range" and "Low Range" appear.
5. If you wish, you can modify the values for "High Range" and "Low Range", as long as the prior is greater than the latter. To do so:
   a. Click Change Value next to the "High Range" and "Low Range" field.
   b. Enter a value.
   c. Click Save Value.

Set Up Log Tracking for a Resource

Log Tracking Overview

IT problems can often be detected or diagnosed from messages generated by operating systems, application servers, network services, or middleware throughout the environment. Hyperic can monitor messages in log files and in memory, and record events in the Hyperic database based on criteria you specify.

Configure Log Tracking

Hyperic Resource Types that Support Log Tracking

Hyperic supports log tracking for operating system platforms, network services, and most server types. If a resource supports log tracking, its Configuration Properties page contains log tracking configuration options.

Supported Log Message Types

Hyperic can monitor and record events for:
- Log file messages that specify log levels using log4j log levels.
- Events written to Windows Event Logs.
- Network request results for a variety of network services.

Log Tracking Configuration Options

You enable and configure log tracking for a resource on its Configuration Properties page. Navigate to the resource's Inventory page, and click Edit in the Configuration Properties section to display the Configuration Properties page.

Note: Log and configuration tracking must be enabled for a resource if you wish to log events for log messages or configuration changes. Event logging is automatic for alerts and control actions. Log tracking configuration options vary somewhat by resource type.

Log tracking options vary by resource type. See the following sections for more detail:

- Log Tracking for Resources with Log4j Logs
- Log Tracking for Network Services
- Log Tracking for Windows Platforms
Log Tracking for Resources with Log4j Logs

This section describes the log tracking configuration options for resources that whose log files use log4j levels.

An authorized user can set the values of these configuration options:

- Enable/disable log tracking.
- Specify one or more files to track, as a comma-separated list. The Hyperic Agent must be able to read these files, so make sure permissions are set appropriately.
- Specify the highest log level to track:
  - Error - Messages with log level "FATAL" or "ERROR"
  - Warn
  - Info
  - Debug
- Specify substrings or expressions to use as include/exclude filter criteria. Enter a substring or a regular expression that a log message must contain or match in Log Pattern Match. For more information, see [http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html](http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html).

Log Tracking for Network Services

This section describes the log tracking configuration options for network services.
An authorized user can set the values of these configuration options:

- Enable/disable log tracking.
- Specify the highest log level to track:
  - Error
  - Warn
  - Info
  - Debug
- Specify substrings or expressions to use as include/exclude filter criteria. Enter a substring or a regular expression that a log message must contain or match in Log Pattern Match.

Log Tracking for Windows Platforms

This section describes the log tracking configuration options for platforms of type "win32".
An authorized user can set the values of these configuration options:

- Enable/disable log tracking.
- Specify one or more Event Log to track:
  - System - contains events logged by Windows system components. For example, if a driver fails to load during startup, an event is recorded in the system log. Windows predetermines the events that are logged by system components.
  - Application - contains events logged by programs. For example, a database program may record a file error in the application log. Events that are written to the application log are determined by the developers of the software program.
  - Security - contains events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. A Windows administrator or member of the Windows Administrators group specify which events are recorded in the security log.
  - "*" causes all event logs to be tracked
- Specify the highest log level to track:
  - Error - Windows Events with level "ERROR"
  - Warn - Windows Events with level "WARNING"
  - Info - Windows Events with level "INFORMATION" or "SUCCESS"
  - Debug - No Windows Event types map to this level

Content of Logged Windows Events

When Windows log tracking is enabled, an entry of this form is logged for events that match the criteria you specified on the resource's Configuration Properties page:

[Timestamp] Log Message (EventLogName):EventLogName:EventAttributes

where:

- **Timestamp** - is when the event occurred
- **Log Message** - is an text string
- **EventLogName** - is the Windows event log type, "System", "Security", or "Application".
- **EventAttributes** - a colon delimited string made of the Windows event Source and Message attributes.

For example, this log entry:

04/19/2010 06:06 AM Log Message (SYSTEM): SYSTEM: Print: Printer HP LaserJet 6P was paused.

is for an Windows event written to the Windows System event log at 6:06 AM on 04/19/2010. The Windows event Source and Message attributes, are "Print" and "Printer HP LaserJet 6P was paused.", respectively.
Tailoring the Content and Format of Logged Windows Events

You can configure the last portion of the log data that the agent writes for a Windows event - referred to above as EventAttributes. You can include additional event attributes, for example User and Computer. To do so, you add the platform.log_track.eventfmt property to the agent.properties file for the Hyperic Agent monitoring the Windows platform.

Usage of platform.log_track.eventfmt property is described below.

platform.log_track.eventfmt Property

Description
Specifies the content and format of the Windows event attributes that a Hyperic Agent includes when logging a Windows event as an event in Hyperic. agent.properties does not contain the platform.log_track.eventfmt property, you must explicitly add it if you want to tailor the data logged for Windows events.

Default Behavior
When Windows log tracking is enabled, an entry of this form is logged for events that match the criteria you specified on the resource’s Configuration Properties page:

[Timestamp] Log Message (EventLogName):EventLogName:EventAttributes

where:
- **Timestamp** - is when the event occurred
- **Log Message** - is an text string
- **EventLogName** - is the Windows event log type, "System", "Security", or "Application".
- **EventAttributes** - a colon delimited string made of the Windows event Source and Message attributes.

For example, this log entry:

04/19/2010 06:06 AM Log Message (SYSTEM): SYSTEM: Print: Printer HP LaserJet 6P was paused.

is for an Windows event written to the Windows System event log at 6:06 AM on 04/19/2010. The Windows event Source and Message attributes, are "Print" and "Printer HP LaserJet 6P was paused.", respectively.

Configuration
You can use the parameters below to configure the Windows event attributes that the agent writes for a Windows event. Each parameter maps to Windows event attribute of the same name.

- **%user%** — The name of the user on whose behalf the event occurred.
- **%computer%** — The name of the computer on which the event occurred.
- **%source%** — The software that logged the Windows event.
- **%event%** — A number identifying the particular event type.
- **%message%** — The event message.
- **%category%** — An application-specific value used for grouping events.
For example, with this property setting:
```
platform.log_track.eventfmt=%user%@%computer%
%source%:%event%:%message%
```
the Hyperic Agent will write the following data when logging Windows event:

```
04/19/2010 06:06 AM Log Message (SYSTEM): SYSTEM: HP_Administrator@Office
Print:7:Printer HP LaserJet 6P was paused.
```

This entry is for an Windows event written to the Windows System event log at 6:06 AM on 04/19/2010. The software associated with the event was running as "HP_Administrator" on the host "Office". The Windows event's Source, Event, and Message attributes, are "Print", "7", and "Printer HP LaserJet 6P was paused.", respectively.

**View Log Events**

Log events for a particular resource are indicated in the timeline at the bottom of the resource's Indicators page. A circular indicator over the timeline indicates a timeslice in which one or more events of any type - log events, configuration change events, or alerts - were logged. Click the event indicator to view the data collected at that time.

In vFabric Hyperic, you can use the **Event Center** to view events over time for all, or selected groups of resources, and filter by log event severity. For more information see **Event Center**.

**Defining Alert Conditions Based on Log Events**

For information about defining alert conditions based on log events see the "Step 3: Define Alert Condition Set" in **Define an Alert for a Resource**.

**Log Tracking Support Classes**

For information about the Hyperic support class for log events for log file messages that specify a log4j level, see **Log4JLogTrackPlugin**.

For information about the Hyperic support class for tracking Windows Event logs, see **Win32EventTrackPlugin**.
Plugin classes monitor network services log events using the `plugin.getManager().reportEvent` method.

**Set Up Configuration Tracking for a Resource**

**Hyperic Configuration Tracking Functionality**

For supported resource types, you can configure Hyperic to track changes made to configuration files (or other local files of interest) and log events for the associated resource. Configuration tracking is supported for most platform and server types; typically not for services.

Configuration tracking functionality for server types varies by resource type, plugins that have been updated to use the event-based tracking added in Hyperic 4.6.5 track more information about file changes than those that still use the still-supported polling-based tracking.

The plugins that are updated to use event-based tracking are listed in [Set Up Event-Based Configuration Tracking for a Server](#). Follow the instructions in that section for those server types. For other server types, and for platform and service types that support configuration tracking see [Set Up Polling-Based Configuration Tracking](#).

**Learn about Configuration Tracking**

See [Log and Configuration Event Tracking](#) for information about:

- What resource types support configuration tracking,
- Prerequisites for configuration tracking,
- The differences between Hyperic's event-based and polling-based configuration tracking,
- Where to view configuration events in the Hyperic user interface, and
- Support for using configuration change events in alerts.

**Set Up Event-Based Configuration Tracking for a Server**

The instructions in the section apply to server types whose plugin uses event-based configuration tracking, listed below.

- Tomcat
- Apache
- WebSphere
- WebLogic Server
- JBoss
- PostgreSQL
- mySQL
- Oracle

To enable and configure configuration tracking for a resource of one of the previous server types:
1. Navigate to the server instance.
2. Select **Configure Server** from the **Tools** menu.

   The Configuration Properties page appears.

   ![Configuration Properties](image)

3. In the Monitoring section of the page:
   a. Make sure that the **Enable Config Tracking** box, which enables and disables configuration tracking for the server, is checked.

   **If you are satisfied with the default filter definition in the "Configuration Files" in, skip the following step, and click OK.**

   b. In the "Configuration Files" box, specify the files you wish to monitor in this fashion:

   ```plaintext
   path;recurse;regex1|regex2,path2;recurse;regex1|regex2|...|regexN
   ```

   where:
   - **path** — An absolute path, or a path relative to the managed resource's discovered install directory.
Example Configuration Files setting
For MySQL, the default value of the Configuration Files field, which specifies which files to track is:

```
/;false;my\cnf;\;false;my\cnf;~;false;\my\cnf;\;false;\usr/local/mysql/data;false;\my\cnf;\;false;\usr/local/var;false;\my\cnf;\;false;\%WINDIR%\;false;\my\ini|\my\cnf;\;false;\my\ini|\my\cnf;\;false;\my\ini|\my\cnf
```

When configuration tracking is enabled, this filter causes Hyperic to track `my.cnf` in the following directories:

- MySqlHome/etc
- MySqlHome/etc/mysql
- MySqlHome
- the home directory of the user under which MySQL runs
- /usr/local/mysql/data
- /usr/local/var
- the Windows directory
- c:

and track `my.ini` in the following directories:

- the Windows directory
- c:/
- MySqlHome

Set Up Polling-Based Configuration Tracking

For platforms and services that support configuration tracking, and server types that have the agent uses a cryptographic hash function to continuously compare a original version of the file with the current version to see if it has changed.

To enable and configure configuration tracking for a platform or service:

1. Navigate to the resource instance.
2. Select Configure ... from the Tools menu.
   The Configuration Properties page appears.
3. On the Edit Configuration Properties page:
a. Click the **Enable Config Tracking** box to turn configuration tracking on and off for the resource.
b. Enter the path, relative to the resource's installation directory, to each file you wish to track. Separate files with a comma.
c. Click **OK**.

**View Configuration Events for a Resource**

You can view configuration event data on:

- The **Monitor** page for a resource. For more information, see `ui-Monitor.CurrentHealth` in *vFabric Hyperic User Interface*.
- The **Event Center** page. For more information see `ui-Event.Center` in *vFabric Hyperic User Interface*.

**Configure Alerts Based on Configuration Events**

1. Enable and configure configuration tracking as described above.
2. For the instructions in Define an Alert for a Resource, or Define an Alert for a Resource Type and choose the "Config Changed" condition type.

**Define an Alert for a Resource**

Follow these instructions to define an alert for an individual resource.

**Step 1 - Select Target Resource**

1. Navigate to the resource to which the new alert definition will apply.
2. Click the **Alert** tab.
3. Click **Configure**.
4. Click **New** to display the **New Alert** page.

**Step 2 - Define Alert Properties**

- Supply property values in the "Alert Properties" section of the **New Alert Definition** page.
- **Name** — Name assigned by the user creating an alert definition. A fired alert is identified, in the Hyperic user interface and alert notifications, by the alert definition name and a timestamp. An alert definition name should clearly communicate the nature of the problem. For example, "Down" for an alert on availability, or "Low Memory" for an alert on free memory.
- **Description** — Description entered by the user creating the alert definition.
- **Priority** — The severity of the problem, as defined by the person creating the alert definition: "Low", "Medium", or "High". A consistent policy for defining an alert definition priority makes it easier to triage problems appropriately. An alert’s priority is shown in Hyperic pages that present alert status and in alert notifications. You can sort alerts by priority in vFabric Hyperic’s **Alert Center** or **Operations Center**.
- **Active** — The current enabled/disabled status of the alert definition. Alerts only fire for enabled alert definitions. When an alert definition is disabled, Hyperic does not evaluate its condition or fire alerts for it.

**Step 3 - Define Alert Condition Set**

Define the rules for triggering and firing the alert in the "Condition Set" section of the New Alert Definition page.

**Condition Set**

An alert condition specifies a resource metric value or event that will initiate the alert firing process.

The condition types you can choose when you define an alert vary by resource type and Hyperic version. If a condition type is not supported by your version of Hyperic or is not valid for the target resource, it will not appear as an option.

To define a condition, choose one of the following condition types, and supply required parameter values.

- **Metric condition** - To base the alert on the value of a metric that Hyperic collects for the resource:
  
a. **Metric** - Select a metric from the selector list. Only currently enabled metrics are listed. (If the metric you're looking for is not listed, see the note below.)
   b. **Define the rule for evaluating the metric value.** You can:
      - Compare metric value to an absolute value. Select an operator: > (greater than), < (less than), = (equal to), or != (not equal to), and enter a metric value. If the metric value is a percentage, specify it as a float value. For example, enter .99 for 99%, 1.0 for 100%. Use a period (.) as a decimal separator, rather than a comma (,).
      - Compare metric value to its minimum, baseline, or maximum value *, in vFabric Hyperic only. Select an operator: > (greater than), < (less than), = (equal to), or != (not equal to), and choose "Min Value", "Baseline Value" or "Max Value". Baselining must be enabled. For more information, see Baselines.
      - Fire upon change in metric value. Click value changes.

**To Enable Collection of a Metric**

If you want to base a metric condition on a metric that is not currently collected, you have to enable collection of that metric. To do so, update the metric collection settings for the resource type (choose Monitoring Defaults from the Administration tab), or for the specific resource (click Metrics on the Monitor tab for the resource).
• **Inventory Property Condition** - To define a condition that is triggered when the value of an inventory property for resource changes, select an inventory property. The pulldown contains only those inventory properties that are valid for the type of the resource to which the alert applies.

• **Control Action Condition** - When you define an alert for a resource that supports control actions, you can define a condition that is triggered when a particular control action is performed. If desired, you can base the condition on a control action with a particular result status: "in progress", "completed", or "failed". Pulldowns allow you to select a control action that the resource supports, and a result status if desired.

• **Events/Log Level Condition** - To define a condition that is triggered by a log event, select a message severity level ("error", "warn", "info", "debug", "all") and optionally a match string. The condition is satisfied each time a message of the selected severity that contains the match string (if one was specified) is written to a log file that Hyperic is tracking. Log tracking must be enabled for the resource. To determine the log files that Hyperic monitors for the resource, see the **Configuration Properties** section of the resource's **Inventory** tab. The log files that Hyperic monitors for a resource are defined using the `server.log_track.files` property. For configuration instructions, see **Set Up Log Tracking for a Resource**.

• **Config Changed... Condition** - This type of condition is triggered by a change to a configuration file that Hyperic is configured to monitor for the resource. To limit the condition to a single file, enter its filename in the "match filename" field. If you don't specify a filename, a change to any file monitored will trigger the alert. To determine the log files that Hyperic monitors for the resource, see the **Configuration Properties** section of the resource's **Inventory** tab. The files that Hyperic monitors for a resource are defined using the `server.config_track.files` property. The maximum length for filename entered is 25 characters. For configuration instructions, see **Set Up Configuration Tracking for a Resource**.

**Define Additional Conditions**

In vFabric Hyperic, you can define up to three conditions for an alert. To add another condition, click **Add Another Condition** and specify whether both the new condition and the preceding one must be satisfied for the alert to be triggered ("AND") or only one must be satisfied ("OR").

**Define Recovery Alert Behavior**

To designate the alert you’re defining as a recovery alert, select the primary alert definition from the pulldown.

A recovery alert condition should detect when the condition that fired the primary alert is no longer true. When a recovery alert fires, it marks the primary alert "Fixed", and the primary alert definition is re-enabled. The primary alert definition should be configured to **Generate one alert and then disable alert definition until fixed**, as described below. For more information, see **Define a Recovery Alert for a Resource Alert**.
Enable Actions
You can make the condition absolute - (one strike you're out) or fire after the condition occurs repeatedly. Choose either:

- **Each time conditions are met.** The alert fires upon a single occurrence of the condition, or
- **Once every _ times conditions are met within a time period of _ minutes.** This option configures an alert to fire when the condition(s) occur multiple times over a period of time. Enter the number of occurrences and period of time.

Enable Action Filters
An action filter can be used to control alert firing and alert actions.

**Disable an Alert Definition upon Firing**
Click **Generate one alert and then disable alert definition until fixed** to disable the alert definition after firing and reenable it when the alert that triggered it is marked "Fixed".

This option eliminates redundant firing for the same problem. If you do not choose this option, the alert will fire repeatedly as long as the triggering condition is still true.

In vFabric Enterprise this configuration option, used in conjunction with recovery alerts, automates the process of disabling and re-enabling an alert definition. Result: (1) no redundant alerts for the same problem, and (2) you don't have manually "fix" an alert triggered by a transient problem.

**Disregard Control Actions for Related Alerts.**
The **Disregard control actions that are defined for related alerts** option appears on **New Alert Definition** pages for resources that support control actions. This option only applies when:

1. The current alert definition will include an alert action
2. The resource associated with the alert is a member of an application
3. There are other members of the same application with alerts that fire control actions (ideally the same control action)

Under these circumstances, this configuration option ensures that if multiple alerts are fired within a short period for resources that are members of the same application, only one control action will be executed. For example, this would prevent a server from being restarted several times in a short period of time for the same alert conditions. For instance, you might have an alert with an action to restart a Tomcat server if the JVM Free Memory got too low and another alert with an action to restart the same server if the JVM Active Thread count got too high. If both alerts fired at the same time and they were filtering control actions, only 1 restart control action would be executed and not two.

**Step 4 - Define Alert Actions**
You assign actions to an alert definition on the **Alert Definition** page, which appears when you save a new alert definition or edit an existing alert definition.
The **Alert Definition** page is similar to the **New Alert** page, with the addition of **Edit** controls in the "Alert Properties" and "Condition Set" sections, and tabs at the bottom of the page for defining alert actions.

You can specify multiple actions to be performed automatically when an alert fires. The types of actions available in the **Alert Definition** page vary based on: (1) the type of resource the alert applies to, (2) your version of Hyperic, and (3) whether you've configured Hyperic for the types of actions that must be enabled before you can use them, such as escalations, OpenNMS trap actions, and in vFabric Hyperic, SNMP notifications.

To define an alert action, select one of the tabs and supply the required information:

**Escalation**

Select an escalation from the "Escalation Scheme" pulldown; the tab refreshes and shows the escalation steps. You must define an escalation before you can assign it to an alert definition. Using an escalation that is configured to repeat until the alert is fixed is a good way to prevent redundant alerts firing for the same problem. To create an escalation, click **Escalation Schemes Configuration** on the **Administration** tab. For more information about escalations, see [Configure and Manage Escalations](#).

**Control Action**

In vFabric Hyperic, you can define a resource control action for Hyperic to perform when the alert fires. The control action can target the current resource (the one to which the alert definition is assigned) or a different resource on the same platform, as long as the resource type has Hyperic-supported control actions. To configure a control action for the alert, select the **Control Action** tab and click **Edit**. The **Add Control Action** page appears; click the thumbnail below for a screenshot. Follow the instructions on the associated help page. You can only assign a single control action to an alert definition. **Note:** You cannot assign a control action to a resource type alert.
Notify Roles
In vFabric Hyperic you can specify one or more roles as notification recipients. Hyperic users with a role you specify will be notified when an alert is fired. Click Add to List on the Notify Roles tab. On the roles selection page, choose the role(s) to be notified when the alert fires. The help page has instructions.

For information about creating roles specifically for use in notification actions, see Configure Roles for Role-Based Alert Notifications.

Notify HQ Users
Click Add to List on this tab to specify one or more Hyperic users as notification recipients. On the user selection page, choose the users to be notified when the alert fires. The help page has instructions.

Notify Other Recipients
Click Add to List on this tab to specify non-Hyperic user email recipients for alert notifications. The help page has instructions.

Script
In vFabric Hyperic, to assign a script action to the alert definition, click the Script tab, enter the full path to the script, and click Set. Hyperic will run the script when the alert fires. Scripts can reference alert-related Hyperic environment variables to perform custom notification logic. For information, see Define a Script Action for an Alert.

**Script actions are synchronous**
Script actions execute one at a time. Until a script action completes, additional alerts will not fire on the resource.

OpenNMS
If Hyperic Server is configured for OpenNMS integration, you can use this tab to configure Hyperic to send an SNMP trap to OpenNMS when the alert fires. The notification will be generated by opennms_notify.gsp alert notification template.

To configure an OpenNMS trap action, enter:
- **Server** - Listen address for the OpenNMS server
- **Port** for the OpenNMS server.

For more information, see [http://support.hyperic.com/display/hyperforge/HQU+OpenNMS](http://support.hyperic.com/display/hyperforge/HQU+OpenNMS).
SNMP Notification

If the Hyperic Server is configured to send SNMP notifications to your NMS, you can use this tab to configure a trap notification action. See SNMP Server Configuration Properties for more information.

The notification sent when the alert fires will contain three variable bindings:

- **sysUptimeOID.0** - No configuration is required for this binding.
- **snmpTrapOID.0** - This binding is configured on the HQ Server settings page.
- **A variable binding for the alert data specified in the snmp_trap.gsp alert notification template** - the alert definition name and the "short reason" for firing. Note that Alert templates may be customized, as described in Tailor Alert Notification Templates.

### Including more variable bindings in SNMP messages

For richer capability, you can configure a SNMP notification as a step in an escalation. An SNMP notification in an escalation can be configured with additional variable bindings. For more information, see Configure and Manage Escalations.

To configure an SNMP notification action enter:

- **IP Address** - the address and port of the target NMS.
- **OID** - The OID of the notification to send, which will contain the alert details specified in the snmp_trap.gsp template.
- **Notification Mechanism** - The type of SNMP notification to send:
  - v1 Trap
  - v2c Trap
  - Inform

### Define a Recovery Alert for a Resource Alert

#### Understanding Recovery Alerts

A recovery alert is special type of alert definition that you pair with a properly configured primary alert definition to streamline alert management. The purpose of a recovery alert is to fire when the condition that fired another alert - the "primary" alert - is no longer true, and then mark the primary alert "fixed" and re-enable the primary alert definition. This strategy prevents redundant alerts and automates the task of marking an alert "fixed".

You can define a recovery alert for a resource alert, and in vFabric Hyperic, a resource type alert. You cannot and do not need to define a recovery alert for a resource group alert in vFabric Hyperic - recovery alert behavior is automatic for resource group alerts.

To effectively leverage the benefits of recovery alert functionality you need to:
• Configure the primary alert definition to fire once when triggered and then disable itself until that fired alert is fixed. This prevents multiple alerts for a single incident.
• Configure a recovery alert definition and assign it to the primary alert definition. Make the recovery alert condition the opposite of the primary alert condition. The recovery alert fires when the primary alert condition is no longer true. Upon firing, the recovery alert marks the alert fired by the primary alert "fixed", and re-enables the primarily alert definition, so that if the problem occurs again, the primary alert is again triggered.

Properly configured primary and recovery alert definitions keep users notified of problems without deluging them with alert notifications.

**Define Primary Alert Definition to Disable Itself**

You can only define a recovery alert for a primary alert definition that already exists. Before setting up a recovery alert, create the primary alert definition, and choose the "Disable alert until re-enabled manually or by recovery alert" option.

**Create a Recovery Alert Definition for a Resource Alert**

To create a recovery alert definition:

1. Browse to the resource to which the primary alert is assigned.
2. Click **New** and follow the directions in **Define an Alert for a Resource**, making sure, when defining the "Condition Set" to
   a. specify the condition that is the opposite of the primary alert definition's condition. For example if the primary alert condition is "1 Minute Load Avg > 2.0.", define the recovery alert condition as "1 Minute Load Avg < 2.0.".
   b. Use the **Recovery Alert** pulldown to select the primary alert.

**Define Host Dependencies for Hierarchical Alerting**

**Define Network Host Relationships**

The **Network and Host Dependency Manager**, available from the "Plugins" section of the **Administration** tab, allows you to define relationships between a top level platform (a network device or virtual host) and lower level (operating system) platforms that depend on it.

**Note:** For information about platforms in Hyperic, see **Platforms** on **About Platforms, Servers, and Services**.

Defining dependency relationships extends the benefits of Hyperic hierarchical alerting to top level platforms.

For more information see **Manage Alert and Notification Volume**.
**vSphere Resource Relationships**

If you manage vSphere resources using the vSphere plugin, do not use the **Network Host Dependency Manager** to configure dependencies for vSphere resources. vSphere resource types will be removed from the **Network Host Dependency Manager** pulldown menus in a future release. For information about the vSphere virtual resource hierarchy, see [vSphere](#).

---

**Step 1 - Select a Top Level Platform to Update**

To define or change the dependent platforms for a top level platform, you first select the top level platform. For ease of navigation, the **Network and Host Dependency Manager** provides two ways to find a top level platform. Depending on how many top level platforms you have in inventory, and what you know about your target, one of the following options may be preferable.

**Option A - Browse a Filtered List of Top Level Platforms**

You can peruse a complete or filtered list of top level platforms in inventory to find the one you want to update.

1. Select the **By Top Level Platform** tab to list all top level platforms in inventory.
2. Filter the list, as desired:
   - Enter the leading characters of the top level platform name in the "Name" field.
   - Select a type of device or host from the **Type** pull-down.
   - Use the **Show** pull-down to limit the display to: all top level platforms, those with existing dependent platforms, or those with none.
3. Select a top level platform from the filtered list.
   - Any dependent platforms already assigned to the top level platform are listed.
4. To add or remove dependent platforms, follow the instructions in **Step 2**.

**Option B - Navigate from a Dependent Platform**

If the top level platform you want to update already has a dependent platform, you can start from there.

1. Select the **By Dependent Platform** tab to list all operating system platforms that have a top level platform defined.
2. Filter the list, as desired:
   - Enter the leading characters of the platform name in the "Name" field.
   - Select an operating system platform type from the "Type" pull-down.
3. The dependent platforms that match the filter settings are listed in this format:
   - **dependent platform name > top level platform name**
4. Click top level platform name to select it.
   - The dependent platforms already assigned to the top level platform are listed.
5. To add or remove dependent platforms, follow the instructions in **Step 2**.
Step 2 - Manage a Top Level Platform’s Dependents

1. Navigate to the desired top level platform and select it, using one of the methods described in Step 1.
2. To remove dependencies:
   - Use the Select and Remove controls on the page.
3. To add dependencies:
   - Click Add.
   - The Available Platforms popup lists operating system platforms in inventory that are not currently assigned to a top level platform.
   - Filter the list, as desired:
     - Enter the leading characters of the operating system platform name in the "Name" field.
     - Select a operating system platform type from the "Type" pull-down.
   - Select one or more operating system platforms from the list.
   - Click Add Dependency to save the association immediately.
   - Click Done to close the window when you are done updating dependencies for the top level platform.

Schedule Resource Downtime

Schedule Downtime

The Schedule Downtime page, available from the Tools menu when a resource, or a resource group is selected, allows you to schedule a downtime period, during which alerts for the resource(s). You define a period of time - a start and end date and time. At the start of the downtime period, currently active alert definitions for resources in the group are disabled. At the end of the period, those alert definitions are re-enabled.

Only a Hyperic user with the Super User role may schedule downtime.

To schedule or reschedule maintenance:

1. Navigate to the individual resource (a platform, server, or service) or the resource group for which you wish to schedule downtime.
2. Choose Schedule Downtime from the Tools menu.
   The Schedule Downtime page appears.
3. On the Schedule Downtime page, enter the start and end dates and times for the downtime and click Schedule.

Related Information

For information about scheduling downtime from a program, script, or a command-line interface with Hyperic’s web services API, see HQApi maintenance command.
Configure Monitoring and Alerting for a Resource Type

Tailor Metric Collection for a Resource Type

Metric collection settings for a resource type are configured on the Monitoring Defaults page for the resource type.

Template Changes Vs. Custom Configurations

Note that an authorized user can tailor metric collection settings on a per resource basis (on the resource's Metric Data minitab in the Resource Hub.) When you save changes to the metric collection settings for a resource type on the Monitoring Defaults page, the settings you configure will apply to all resources of that type in inventory. So, any custom metric collection configuration for resources of that type will be overwritten. Note however, that if a user has chosen a different set of indicator metrics for a resource instance (on the resource's Indicators minitab in the Resource Hub) changing the indicator metrics for a resource type on the Monitoring Defaults page will not override the user's selections.

Navigate to the Monitoring Defaults Page for a Resource Type

1. Click the Administration tab.
2. Click Monitoring Defaults in the "HQ Server Settings" section of the Administration tab.
3. Scroll to the desired resource type on the Monitoring Defaults page, and click Edit Metric Template in that row.
The screenshot below is the **Monitoring Defaults** page for the vSphere Host resource type.

![Monitoring Defaults page](image)

**Enable Collection of a Metric**

To enable the collection of a metric, follow the directions in Change a Metric Collection Interval. Collection of the metric is now enabled by default with the specified collection interval on every resource of this type.

**Disable Collection of a Metric**

To disable the collection of a metric, check the metric name at the left and click **Disable Collection** at the bottom of the page.
Change a Metric Collection Interval

1. Check the metric name at the left.
2. In Collection Interval for Selected at the bottom of the page, enter a time value and select a unit of time measure for the collection interval.
3. Click the Collection Interval for Selected control at the bottom of the Monitoring Defaults page.

Set Indicator Metrics

To select the indicator metrics for a resource type (indicator metrics are the metrics that are charted on a resource's Indicators minitab in the Resource Hub) check the metric name at the left for each metric you wish to be an indicator, and click the Set Selected Metrics as Indicators control at the bottom of the Monitoring Defaults page.

The metrics you configure will be the default indicators for the resource type.

Changes to indicator metrics apply to existing resources but only for users that have not explicitly changed the default indicator page on the resources (of the specified type). If a user has changed the default indicator page for a resource, that will not be overwritten with changes made here.

APIs for Metric Collection Settings

As an alternative to the updating metric collection settings from the Hyperic user interface, you can use Hyperic APIs to perform updates from the command line or from scripts to perform bulk updates:

- **HQApi metric command** - for listing and updating metric collection settings for an individual resource.
- **HQApi metricTemplate command** - for listing and updating metric collection settings for all instances of a resource type.

For general information, see [vFabric Hyperic Web Services API](#).

Define an Alert

Define a Resource Type Alert

This page explains how to define an resource type alert. A resource type alert is applied to all resources of the specific type that currently exist and new resources of the type that get created in the future. Only HQ Administrators can create resource type alerts.

**Step 1 - Select Target Resource Type**

1. Click Administration in the masthead.
2. Click Monitoring Defaults in "HQ Server Settings" section of the page.
3. On the HQ Monitoring Defaults Configuration page, click Edit Alerts for the resource type for which you want to define an alert. The Monitoring Defaults page will display any alert definitions already assigned to the alert.
4. Click **New** to create a new alert definition.

**Step 2 - Define Alert Properties**

On the **New Alert** page, define each property in the "Alert Properties" section.

- **Name** — Name assigned by the user creating an alert definition. A fired alert is identified, in the Hyperic user interface and alert notifications, by the alert definition name and a timestamp. An alert definition name should clearly communicate the nature of the problem. For example, "Down" for an alert on availability, or "Low Memory" for an alert on free memory.
- **Description** — Description entered by the user creating the alert definition.
- **Priority** — The severity of the problem, as defined by the person creating the alert definition: "Low", "Medium", or "High". A consistent policy for defining an alert definition priority makes it easier to triage problems appropriately. An alert's priority is shown in Hyperic pages that present alert status and in alert notifications. You can sort alerts by priority in vFabric Hyperic's **Alert Center** or **Operations Center**.
- **Active** — The current enabled/disabled status of the alert definition. Alerts only fire for enabled alert definitions. When an alert definition is disabled, Hyperic does not evaluate its condition or fire alerts for it.

**Step 3 - Define Alert Condition Set**

On the **New Alert** page, define the Condition Set, and click **OK** when you are done.

**Condition Set**

An alert condition specifies a resource metric value or event that will initiate the alert firing process.

The condition types you can choose when you define a alert vary by resource type and Hyperic version. If a condition type is not supported by your version of Hyperic or is not valid for the target resource, it will not appear as an option.

To define a condition, choose one of the following condition types, and supply required parameter values.

- **Metric condition** - To base the alert on the value of a metric that Hyperic collects for the resource:
  a. **Metric** - Select a metric from the selector list. Only currently enabled metrics are listed. (If the metric you're looking for is not listed, see the note below.)
  b. Define the rule for evaluating the metric value. You can:
     o **Compare metric value to an absolute value.** Select an operator: >*(greater than)*, <*(less than)*, ==*(equal to)*, or !=*(not equal to)*, and enter a metric value. If the metric value is a percentage, specify it as a float value. For example, enter .99 for 99%, 1.0 for 100%. Use a period (.) as a decimal separator, rather than a comma (,).
To Enable Collection of a Metric

If you want to base a metric condition on a metric that is not currently collected, you have to enable collection of that metric. To do so, update the metric collection settings for the resource type (choose Monitoring Defaults from the Administration tab), or for the specific resource (click Metrics on the Monitor tab for the resource).

- **Inventory Property Condition** - To define a condition that is triggered when the value of an inventory property for resource changes, select an inventory property. The pulldown contains only those inventory properties that are valid for the type of the resource to which the alert applies.

- **Control Action Condition** - When you define an alert for a resource that supports control actions, you can define a condition that is triggered when a particular control action is performed. If desired, you can base the condition on a control action with a particular result status: "in progress", "completed", or "failed". Pulldowns allow you to select a control action that the resource supports, and a result status if desired.

- **Events/Log Level Condition** - To define a condition that is triggered by a log event, select a message severity level ("error", "warn", "info", "debug", "all") and optionally a match string. The condition is satisfied each time a message of the selected severity that contains the match string (if one was specified) is written to a log file that Hyperic is tracking. Log tracking must be enabled for the resource. To determine the log files that Hyperic monitors for the resource, see the Configuration Properties section of the resource's Inventory tab. The log files that Hyperic monitors for a resource are defined using the server.log_track.files property. For configuration instructions, see Set Up Log Tracking for a Resource.

- **Config Changed... Condition** - This type of condition is triggered by a change to a configuration file that Hyperic is configured to monitor for the resource. To limit the condition to a single file, enter its filename in the "match filename" field. If you don't specify a filename, a change to any file monitored will trigger the alert. To determine the log files that Hyperic monitors for the resource, see the Configuration Properties section of the resource's Inventory tab. The files that Hyperic monitors for a resource are defined using the server.config_track.files property. The maximum length for filename entered is 25 characters. For configuration instructions, see Set Up Configuration Tracking for a Resource.

* Compare metric value to its minimum, baseline, or maximum value*, in vFabric Hyperic only. Select an operator: > *(greater than)*, < *(less than)*, = *(equal to)*, or != *(not equal to)*, and choose "Min Value", "Baseline Value" or "Max Value". Baselining must be enabled. For more information, see Baselines.

* Fire upon change in metric value. Click value changes.
Define Additional Conditions
In vFabric Hyperic, you can define up to three conditions for an alert. To add another condition, click Add Another Condition and specify whether both the new condition and the preceding one must be satisfied for the alert to be triggered (“AND”) or only one must be satisfied (“OR”).

Define Recovery Alert Behavior
To designate the alert you’re defining as a recovery alert, select the primary alert definition from the pulldown.

A recovery alert condition should detect when the condition that fired the primary alert is no longer true. When a recovery alert fires, it marks the primary alert "Fixed", and the primary alert definition is re-enabled. The primary alert definition should be configured to Generate one alert and then disable alert definition until fixed, as described below. For more information, see Define a Recovery Alert for a Resource Alert.

Enable Actions
You can make the condition absolute - (one strike you’re out) or fire after the condition occurs repeatedly. Choose either:

- Each time conditions are met. The alert fires upon a single occurrence of the condition, or
- Once every _ times conditions are met within a time period of _ minutes. This option configures an alert to fire when the condition(s) occur multiple times over a period of time. Enter the number of occurrences and period of time.

Enable Action Filters
An action filter can be used to control alert firing and alert actions.

Disable an Alert Definition upon Firing
Click Generate one alert and then disable alert definition until fixed to disable the alert definition after firing and reenable it when the alert that triggered it is marked "Fixed".

This option eliminates redundant firing for the same problem. If you do not choose this option, the alert will fire repeatedly as long as the triggering condition is still true.

In vFabric Enterprise this configuration option, used in conjunction with recovery alerts, automates the process of disabling and re-enabling an alert definition. Result: (1) no redundant alerts for the same problem, and (2) you don’t have manually "fix" an alert triggered by a transient problem.
Disregard Control Actions for Related Alerts.

The Disregard control actions that are defined for related alerts option appears on New Alert Definition pages for resources that support control actions. This option only applies when:

1. The current alert definition will include an alert action
2. The resource associated with the alert is a member of an application
3. There are other members of the same application with alerts that fire control actions (ideally the same control action)

Under these circumstances, this configuration option ensures that if multiple alerts are fired within a short period for resources that are members of the same application, only one control action will be executed. For example, this would prevent a server from being restarted several times in a short period of time for the same alert conditions. For instance, you might have an alert with an action to restart a Tomcat server if the JVM Free Memory got too low and another alert with an action to restart the same server if the JVM Active Thread count got too high. If both alerts fired at the same time and they were filtering control actions, only 1 restart control action would be executed and not two.

Step 4 - Define Alert Actions

You assign actions to an alert definition on the Alert Definition page, which appears when you save a new alert definition or edit an existing alert definition.

The Alert Definition page is similar to the New Alert page, with the addition of Edit controls in the "Alert Properties" and "Condition Set" sections, and tabs at the bottom of the page for defining alert actions.

You can specify multiple actions to be performed automatically when an alert fires. The types of actions available in the Alert Definition page vary based on: (1) the type of resource the alert applies to, (2) your version of Hyperic, and (3) whether you've configured Hyperic for the types of actions that must be enabled before you can use them, such as escalations, OpenNMS trap actions, and in vFabric Hyperic, SNMP notifications.

To define an alert action, select one of the tabs and supply the required information:

Escalation

Select an escalation from the "Escalation Scheme" pulldown; the tab refreshes and shows the escalation steps. You must define an escalation before you can assign it to an alert definition. Using an escalation that is configured to repeat until the alert is fixed is a good way to prevent redundant alerts firing for the same problem. To create an escalation, click Escalation Schemes Configuration on the Administration tab. For more information about escalations, see Configure and Manage Escalations.
Control Action

In vFabric Hyperic, you can define a resource control action for Hyperic to perform when the alert fires. The control action can target the current resource (the one to which the alert definition is assigned) or a different resource on the same platform, as long as the resource type has Hyperic-supported control actions. To configure a control action for the alert, select the Control Action tab and click Edit. The Add Control Action page appears; click the thumbnail below for a screenshot. Follow the instructions on the associated help page. You can only assign a single control action to an alert definition. **Note:** You cannot assign a control action to a resource type alert.

<table>
<thead>
<tr>
<th>Control Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Type:</strong> PostgreSQL 8.2</td>
</tr>
<tr>
<td><strong>Resource Name:</strong> Marie-McGarrys-MacBook-Pro-15.local HQ PostgreSQL 8.2</td>
</tr>
<tr>
<td><strong>Control Type:</strong> none</td>
</tr>
<tr>
<td>Ok</td>
</tr>
</tbody>
</table>

Notify Roles

In vFabric Hyperic you can specify one or more roles as notification recipients. Hyperic users with a role you specify will be notified when an alert is fired. Click Add to List on the Notify Roles tab. On the roles selection page, choose the role(s) to be notified when the alert fires. The help page has instructions.

For information about creating roles specifically for use in notification actions, see Configure Roles for Role-Based Alert Notifications.

Notify HQ Users

Click Add to List on this tab to specify one or more Hyperic users as notification recipients. On the user selection page, choose the users to be notified when the alert fires. The help page has instructions.

Notify Other Recipients

Click Add to List on this tab to specify non-Hyperic user email recipients for alert notifications. The help page has instructions.

Script

In vFabric Hyperic, to assign a script action to the alert definition, click the Script tab, enter the full path to the script, and click Set. Hyperic will run the script when the alert fires. Scripts can reference alert-related Hyperic environment variables to perform custom notification logic. For information, see Define a Script Action for an Alert.
Script actions are synchronous
Script actions execute one at a time. Until a script action completes, additional alerts will not fire on the resource.

OpenNMS
If Hyperic Server is configured for OpenNMS integration, you can use this tab to configure Hyperic to send an SNMP trap to OpenNMS when the alert fires. The notification will be generated by opennms_notify.gsp alert notification template.

To configure an OpenNMS trap action, enter:
- **Server** - Listen address for the OpenNMS server
- **Port** for the OpenNMS server.

For more information, see [http://support.hyperic.com/display/hyperforge/HQU+OpenNMS](http://support.hyperic.com/display/hyperforge/HQU+OpenNMS).

SNMP Notification
If the Hyperic Server is configured to send SNMP notifications to your NMS, you can use this tab to configure a trap notification action. See [SNMP Server Configuration Properties](#) for more information.

The notification sent when the alert fires will contain three variable bindings:
- **sysUptimeOID.0** - No configuration is required for this binding.
- **snmpTrapOID.0** - This binding is configured on the **HQ Server** settings page.
- A variable binding for the alert data specified in the `snmp_trap.gsp` alert notification template - the alert definition name and the "short reason" for firing. Note that Alert templates may be customized, as described in [Tailor Alert Notification Templates](#).

Including more variable bindings in SNMP messages
For richer capability, you can configure a SNMP notification as a step in an escalation. An SNMP notification in an escalation can be configured with additional variable bindings. For more information, see [Configure and Manage Escalations](#).

To configure an SNMP notification action enter:
- **IP Address** - the address and port of the target NMS.
- **OID** - The OID of the notification to send, which will contain the alert details specified in the `snmp_trap.gsp` template.
- **Notification Mechanism** - The type of SNMP notification to send:
  - v1 Trap
  - v2c Trap
  - Inform
Define a Recovery Alert for a Resource Type Alert

Understanding Recovery Alerts
A recovery alert is a special type of alert definition that you pair with a properly configured primary alert definition to streamline alert management. The purpose of a recovery alert is to fire when the condition that fired another alert - the "primary" alert - is no longer true, and then mark the primary alert "fixed" and re-enable the primary alert definition. This strategy prevents redundant alerts and automates the task of marking an alert "fixed".

You can define a recovery alert for a resource alert, and in vFabric Hyperic, a resource type alert. You cannot and don't need to define a recovery alert for a resource group alert in vFabric Hyperic — recovery alert behavior is automatic for resource group alerts.

To effectively leverage the benefits of recovery alert functionality you need to:

- Configure the primary alert definition to fire once when triggered and then disable itself until that fired alert is fixed. This prevents multiple alerts for a single incident.
- Configure a recovery alert definition and assign it to the primary alert definition. Make the recovery alert condition the opposite of the primary alert condition. The recovery alert fires when the primary alert condition is no longer true. Upon firing, the recovery alert marks the alert fired by the primary alert "fixed", and re-enables the primarily alert definition, so that if the problem occurs again, the primary alert is again triggered.

Properly configured primary and recovery alert definitions keep users notified of problems without deluging them with alert notifications.

Define Primary Alert Definition to Disable Itself
You can only define a recovery alert for a primary alert definition that already exists. Before setting up a recovery alert, create the primary alert definition, and choose the "Disable alert until re-enabled manually or by recovery alert" option.

Create a Recovery Alert Definition for a Resource Type Alert
To create a recovery alert definition for a resource type alert:

1. Click Administration in the masthead.
2. Click Monitoring Defaults in "HQ Server Settings" section of the page.
3. On the HQ Monitoring Defaults Configuration page, click Edit Alerts for the resource type to which the primary alert is defined. The Monitoring Defaults page will display any alert definitions already assigned to the alert.
4. Click **New** and follow the directions in Define an Alert for a Resource Type, making sure, when defining the "Condition Set" to
   a. specify the condition that is the opposite of the primary alert definition's condition. For example if the primary alert condition is "1 Minute Load Avg > 2.0.", define the recovery alert condition as "1 Minute Load Avg < 2.0.
   b. Use the **Recovery Alert** pulldown to select the primary alert.
About Global Monitoring and Alerting Settings

These sections describe options and settings that are defined globally for a Hyperic deployment.

Configure Global Alert Properties

The settings in the Global Alert Properties section of the Administration > HQ Server Settings page enable immediate and global control of alert processing.

- Alerts - Disable or enable all alert definitions for all resources immediately. Disabling stops any alerts from firing; notifications defined in escalations that are currently in progress will be completed.
- Alert Notifications - Disable or enable alert notifications for all resources immediately. Disabling stops all notifications, include those for alerts with escalations currently in progress.
- Hierarchical Alerting * - This setting controls whether alerts are evaluated using the hierarchical alerting method. When hierarchical alerting is enabled, before firing an alert for a resource, HQ considers the availability and alert status of the resource’s parent. The purpose of hierarchical alerting is to avoid firing alerts for every resource affected by a single root cause. For more information, see Manage Alert and Notification Volume.

Note: You can extend the effect of hierarchical alerting by configuring the relationship between a network device or virtual host and the platforms that depend on it using the Network and Host Dependency Manager available in the "Plugins" section of the Administration tab. For more information see Manage Alert and Notification Volume.

Configure Alert Notification Throttling

You can use notification throttling to limit the number of alert email actions (notifications sent by email for a fired alert) that HQ will issue in a 15 second interval. When the threshold you specify is reached, HQ stops sending email alert notifications and instead sends a summary of alert activity every ten minutes to the recipients you specify.

After starting to throttle, HQ re-evaluates notification volume for fired alerts every 10 minutes; when it determines that the per interval volume of individual notifications that fired alerts would generate is less than the configured threshold, HQ resumes sending individual notifications.

In the Notification Throttling Configuration Properties section of the Administration > HQ Server Settings page:

1. Click the Notification Throttling ON control.
2. In the "Threshold" field, enter the maximum number of notifications you want sent in a 15 second interval.
3. Enter one or more email addresses in the "Notification Email(s) field".

For related information, see Manage Alert and Notification Volume.
Configure Alert Notification Email Properties

The settings in the Email Configuration Properties section of the Administration > HQ Server Settings are used to form notifications that Hyperic sends for a fired alert.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base URL</td>
<td>The address:port where the Hyperic Server listens for web application requests. The initial value of Base URL is the web application listen port configured when the Hyperic Server was installed, for example: <a href="http://Ms-MacBook-Pro-15.local:7080">http://Ms-MacBook-Pro-15.local:7080</a>. Base URL forms the prefix of the URL to which Hyperic appends the remainder of the URL, which points to the Alert Detail page for the fired alert. For example: <a href="http://Ms-MacBook-Pro-15.local:7080/alerts/Alerts.do?mode=viewAlert&amp;eid=5:10611&amp;a=16431">http://Ms-MacBook-Pro-15.local:7080/alerts/Alerts.do?mode=viewAlert&amp;eid=5:10611&amp;a=16431</a></td>
</tr>
<tr>
<td>From Email Address</td>
<td>The email address listed as the sender of the alert emails. For example: <a href="mailto:hq@demo2.vmware.com">hq@demo2.vmware.com</a></td>
</tr>
</tbody>
</table>

Configure Metric Baselining Properties

In vFabric Hyperic, the properties in the Automatic Baseline Configuration Properties section of the Administration > HQ Server Settings page control the Hyperic baselining process and the accuracy of the baseline.

<table>
<thead>
<tr>
<th>Server Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline Frequency</td>
<td>The frequency with which HQ calculates a baseline for each metric.</td>
<td>3 days</td>
</tr>
<tr>
<td>Baseline Dataset</td>
<td>The time range of metric data used in calculating the baseline.</td>
<td>7 days</td>
</tr>
<tr>
<td>Baseline Minimum Data Points</td>
<td>The minimum number of data points used in calculating a baseline.</td>
<td>40</td>
</tr>
<tr>
<td>Track Out-of-Bounds Metrics</td>
<td>Controls whether or not HQ tracks OOB metrics.</td>
<td>off</td>
</tr>
</tbody>
</table>
Configure Hyperic Version and Security Announcements

Hyperic sends email announcements to Hyperic administrators when a key release is upcoming, or to distribute important product information. You can configure the level of messages you wish to receive or disable receipt of Hyperic notifications with the **HQ Version and Security Announcements** property, in the **Announcement Properties** section of the **Administration > HQ Server Settings** page. You can choose:

- All
- Major — default value
- None
Manage Alert and Notification Volume

Manage Alerting for Optimal Visibility into Problems

The purpose of alerting is to speed the process of detecting and resolving problems. Rapid detection and response can be compromised when multiple alerts fire as a result of the same problem, or if responders are inundated by repetitive alert notifications. Excessive alert and notification are less likely when:

- A given problem or root cause results in one, rather than many, alerts.
- An alert status of “unfixed” indicates a problem that still exists and needs attention, rather than a transient issue that occurred, and then went away.
- A single problem doesn’t result in a firestorm of redundant notifications.

The following sections describe options for controlling the volume of alerts and notifications.

Prevent Multiple Alerts for the Same Problem

When the volume of fired alerts is high, prioritizing and resolving problems is harder. You can reduce the overall volume of fired alerts without sacrificing visibility if you limit the number of times a given alert definition fires an alert for the same incident.

- **Use repeating escalations** - Assign an escalation that repeats until the alert is fixed. An alert is in escalation cannot re-fire. The use of repeating escalations for all alerts is highly recommended and the best way to control alert volume in Hyperic.
- **Fire one alert then disable the definition** - You can configure an alert definition to fire once and disable itself until that alert is marked fixed. When the alert is marked “fixed” the alert definition is re-enabled. Note that if you have vFabric Hyperic, you can define an associated recovery alert to automatically fix the alert when the triggering condition is no longer true.

Disable all Alert Notifications

If the volume of notifications exceeds manageable levels you can disable alert notifications globally. This option stops all alert notifications immediately including those resulting from escalations in process.

1. Click the Administration tab.
2. Click HQ Server Settings.
3. In the “Global Alert Properties” section, click the Alert Notifications OFF or ON control.

The change takes effect immediately. No alert notifications will be issued when OFF is selected. Escalations currently in progress will be terminated.
Hierarchical Alerting Prevents a Cascade of Alerts in Resource Hierarchies

Hierarchical alerting prevents a single root cause in the same resource hierarchy from causing a cascade of alerts to fire.

When hierarchical alerting is enabled, the alert evaluation process takes into account the availability and alert status of a resource's parent. Specifically, when an agent reports that a resource with an active alert definition is unavailable, HQ checks the availability of the resource's parent in the resource hierarchy. Hyperic will fire an alert for the child resource only if:

- the parent is available, or
- the parent is unavailable, and there is not an enabled, single-condition alert definition on its Availability metric.

Hierarchical alerting takes advantage of Hyperic’s knowledge of the platform-server-service resource hierarchy, obtained via the auto-discovery process. For example, before firing an alert for a service, Hyperic checks the availability and alert status of its parent server. Similarly, before firing an alert for a server, Hyperic checks the availability and alert status of its parent platform.

Hierarchical alerting is a global behavior that applies to all resources in inventory; it is enabled by default. You enable or disable hierarchical alerting in the "Global Alert Settings" section of the HQ Server Settings page, accessible from the Administration tab in the vFabric Hyperic user interface. The change takes effect immediately.

Hierarchical Alerting and vSphere Resources
This version of Hyperic does not fully support hierarchical alerting for the vSphere virtual resources hierarchy (VMware vCenter - vSphere Host - vSphere VM).

Configure Network Host Dependencies for Hierarchical Alerting

You can extend the reach of hierarchical alerting beyond the basic platform-server-service hierarchy to top level platforms - network devices or virtual hosts upon which operating system platforms depend.

To enable Hyperic to consider a top-level platform’s availability and alert status before firing an alert for a dependent resources, you must define the relationship between a top-level platform and the operating system platforms that depend on it. To do so, you use the Network Host Dependency Manager, available in the "Plugins" section on the Administration tab of the vFabric Hyperic user interface. The help page for the Network Host Dependency Manager provides instructions.
vSphere Resource Relationships in vFabric Hyperic
If you manage vSphere resources using the new vSphere plugin, do not use the Network Host Dependency Manager to configure dependencies for vSphere resources. vSphere resource types will be removed from the Network Host Dependency Manager pulldown menus in a future release. For information about the vSphere virtual resource hierarchy, see vSphere.

Set a Notification Throttle

You can configure the Hyperic Server to throttle back alert notifications in the event of an alert storm. You configure the maximum number of notifications that Hyperic will issue within a fifteen second interval. When the threshold is reached, Hyperic stops sending individual alert notifications, and instead, sends a summary of alert activity to designated recipients every ten minutes. When the volume of notifications falls below the specified threshold, Hyperic resumes sending individual notifications.

Notification throttling is disabled by default. You configure it on the HQ Server Settings page, available from the Administration tab.

Enable or Disable all Alert Definitions

You can disable or enable alert definitions globally, if you want to turn alerting on or off for all resources in inventory.

1. Click the Administration tab.
2. Click HQ Server Settings.
3. In the "Global Alert Properties" section, click the Alerts ON or OFF control.

The change takes effect immediately. No alerts will be fired for any resource when OFF is selected. Escalations currently in progress will be completed.
Manage Alert Definitions

View and Edit Alert Definitions

There are a variety of ways to navigate to pages that list and provide detailed information about alert definitions.

List Alert Definitions for a Resource

1. Browse the resource.
2. Click the Alert tab.
3. Click the Configure tab to see a list of alert definitions for the resource.

For information about alert definition list for a resource, see $ui-Alert.ListDefinition$ in vFabric Hyperic User Interface.

List Alert Definitions for a Resource Type

1. Click Administration in the masthead.
2. Click Monitoring Defaults in "HQ Server Settings" section.
3. On the HQ Monitoring Defaults Configuration page, click Edit Alerts for the resource type.
4. The Monitoring Defaults page displays alert definitions for the resource type.

For information about alert definition list for a resource type, see $ui-Alert.ListTypeDefinition$ in vFabric Hyperic User Interface.

List Alert Definitions for a Resource Group

1. Browse the resource group.
2. Click the Alert tab.
3. Click the Configure tab to see a list of alert definitions for the resource group.

For information about alert definition list for a resource, see $ui-Alert.ListDefinition$ in vFabric Hyperic User Interface.

View All Alert Definitions for all Resources

To view all alert definitions:

1. Click the Analyze tab in the Masthead.
2. Click Alert Center.
3. Click Definitions.

For information about the information and options on the Resource Alert Definitions page, see $ui-Alert.Center$ in vFabric Hyperic User Interface.
**View and Edit an Alert Definition**

To view the details of an alert definition click the alert definition name in an alert definition list for the resource it is assigned to, or, in vFabric Hyperic, in the **Definitions** tab in the **Alert Center**.

For information about the information and options available on the **Alert Definition** page, see *ui-Alert.Edit* in vFabric Hyperic User Interface.

**Enable and Disable Alert Definitions**

**Enable or Disable a Resource Alert Definition**

There are multiple ways you can enable or disable a resource alert definition in the HQ user interface:

- On the **Alerts** tab for a resource:
  a. Browse the the resource to which the alert definition is assigned.
  b. Click the **Alerts** tab.
  c. Click **Configure** to display a list of alert definitions for the resource.
     The page will include any alert definitions that the resource inherits from a resource type alert definition, marked with an asterisk. If you enable or disable the alert definition at this level, the change will be overridden by subsequent updates to the alert definition at the resource type level.
  d. Checkmark the alert definition you wish to enable or disable and toggle the **Set Active** control.

- On the **Alert Definition** page:
  e. Navigate to the **Alert Definition** page, by clicking the alert definition name on the **Alert Center** page or the **Alert Detail** page for an alert that has fired.
  f. Click **Edit** in the "Alert Properties" section of the **Alert Definition** page.
  g. Toggle the **Set Active** button.

**Enable or Disable Multiple Alert Definitions for a Resource**

1. Browse the the resource to which the alert definition is assigned.
2. Click the **Alert** tab.
3. Click **Configure** to display a list of alert definitions for the resource.
4. Checkmark the alert definitions you wish to enable or disable and toggle the **Set Active** control.
Enable or Disable a Resource Type Alert Definition
When you enable or disable a resource type alert, the change applies to all resources of that type.

1. Click **Administration** in the masthead.
2. Click **Monitoring Defaults** in "HQ Server Settings" section.
3. On the **HQ Monitoring Defaults Configuration** page, click **Edit Alerts** for the resource type.
4. The **Monitoring Defaults** page displays alert definitions for the resource type.
5. Click one or more alert definitions, and toggle the **Set Active** button.

Enable or Disable an Group Alert Definition

1. Browse the the group to which the alert definition is assigned.
2. Click the **Alert** tab.
3. Click **Configure** to display a list of alert definitions for the group.
4. Checkmark the alert definition you wish to enable or disable and toggle the **Set Active** control.

Enable or Disable all Alert Definitions for Multiple Resources
You can disable or enable all of the alert definitions for selected resources on the **Browse Resource** page.

1. Click the **Resources** tab.
2. Use the filter options at the top of the page to list the resources of interest.
3. Place a checkmark next to one or more resources.
4. Click **Enable all Alerts** or **Disable all Alerts**.

Enable or Disable all Alert Definitions
You can disable or enable alert definitions globally, if you want to turn alerting on or off for all resources in inventory.

1. Click the **Administration** tab.
2. Click **HQ Server Settings**.
3. In the "Global Alert Properties" section, click the **Alerts ON or OFF** control.
The change takes effect immediately. No alerts will be fired for any resource when OFF is selected. Escalations currently in progress will be completed.

Enable Alert Definition Change Logging

The Hyperic audit subsystem logs changes made to alert definitions. When an alert definition is enabled, disabled, or deleted, the event is written to the database. The information includes the username of the person who made the change.
You can configure Hyperic Server to also write the audit events to the `server.log` file in the server's `logs` directory. To do so, add the following section to `ServerHome/conf/server-log4j.xml`, near the end of the file, before the root stanza.

```xml
<!-- Use this category to log every instance of a group alert firing. Comment out if the log messages become unwieldy. -->
<category name="org.hyperic.hq.galerts.processor.MemGalertDef.Fired">
  <priority value="DEBUG" />
</category>

<category name="org.hyperic.hq.common.server.session.AuditManagerEJBImpl">
  <priority value="DEBUG"/>
</category>
```

The entries are written to `logs/server.log`, similar to the following:

```
2009-03-18 15:56:20,088 INFO [main][org.hyperic.hq.common.server.session.AuditManagerEJBImpl@259] Audit Manager starting up
2009-03-18 15:58:28,223 DEBUG [main][org.hyperic.hq.common.server.session.AuditManagerEJBImpl@87] Audit:Audit[user=admin,purpose=12288,time=1237409692209,resource=,msg=HQ Started]
2009-03-18 16:01:12,114 DEBUG [UserLoginListener1][org.hyperic.hq.common.server.session.AuditManagerEJBImpl@87] Audit:Audit[user=hqadmin,purpose=16384,time=1237410072113,resource=,msg=HQ Administrator logged in]
2009-03-18 16:05:18,485 DEBUG [http-0.0.0.0-7080-4][org.hyperic.hq.common.server.session.AuditManagerEJBImpl@87] Audit:Audit[user=hqadmin,purpose=20482,time=1237410318484,resource=Linux,msg=Alert definition deleted (High Load)]
```
Create and Manage Resource Groups and Applications

Learn About Groups and Applications
See About Groups in Hyperic and About Applications in Hyperic.

Configure and Manage Resource Groups

This section has instructions for creating and managing groups.

Learn About HQApi group Command
For information about creating a group using the HQApi see HQApi group command.

Create a Group

1. Click New Group on either:
2. The Dashboard's Summary Counts portlet
3. The Tools menu on the Browse > Resources page
   The New Group page appears.
4. On the New Group page, enter
   o Name: The name of the group
   o Description: (optional) A description of the group
   o Location: (optional) The physical location of the group's hardware
   o Make group private: Checkmark to make the group private. A private group is invisible to other users, including admin users. You can share a private group with other users by associating it with a role. Note that the name you assign to a private group is automatically prefixed with the string "private to username", where username is the creator's Hyperic username.
   o Contains Resources: Select the type of group:
     ▪ Compatible/cluster - the group will contain resources of a single type. For example, "Linux" or "JBoss 4.2"
     ▪ Mixed - the group will contain multiple resource types. Mixed groups are useful for role-based resource access control.
     ▪ The Select Resource Type pulldown appears to the right of the Contains Resources — the options vary depending upon whether you are created a compatible or mixed group.
     ▪ For a compatible group, the Select Resource Type pulldown contains a list of all resource types in inventory.
     For a mixed group, the Select Resource Type pulldown contains these choices:
       • Groups
       • Platforms, Servers, & Services
       • Applications
5. Click OK to create the group. The Inventory page for the new group appears.
6. Add resources to the new group, following the instructions in Add Resources to a Group.

Add Resources to a Group
To add resources to a group:

1. Navigate to the group's Inventory page, if it is not currently selected.
2. Click Add To List in the Resources section of the page.
3. On the Add to Group page, filter the resource list as desired by entering all or a part of the resource name in the Filter By Name field. If you are creating a mixed group, a pulldown that allows filtering by resource type as well.
4. Checkmark desired resources and click the blue arrow to move them from the Resources column to the Add Resources column. (The arrow is enabled when you select a resource.)
5. After moving desired resources to the Add Resources column, click OK.

Assign Roles to a Group
To add a role to a group:

1. Navigate to the group's Inventory page, if it is not currently selected.
2. Click Add To List in the Roles section of the page.
3. On the Add to Roles toGroup page, checkmark desired roles and click the blue arrow to move them from the Roles column to the Add To Roles column.
4. After moving desired roles to the Add Resources column, click OK.

Edit a Group's Inventory Properties

Remove Resources from a Group
To remove resources from a group:

1. Navigate to the group's Inventory page, if it is not currently selected.
2. In the Resources section, checkmark the resources you want to remove.
3. Click Remove From List.

Remove Roles from a Group
To remove roles from a group:

1. Navigate to the group's Inventory page, if it is not currently selected.
2. In the Roles section, checkmark the roles you want to remove.
3. Click Remove From List.
Define an Alert for a Resource Group

This section explains how to define an alert for a compatible group - a group whose members are all of the same resource type.

Understanding Resource Group Alerts

A resource group alert is an alert assigned to a compatible group - a group or resources you have defined that contains selected resources, all of which have the same resource type.

Resource group alerts are different than resource alerts in these ways:

- **A resource group alert definition has a single condition** - A resource group alert definition is based on a single condition.
- **A resource group alert condition is based on the behavior of multiple resources** - Resource group alerts are evaluated differently than other HQ alert types. A resource alert or resource type alert is fired for a specific resource based on monitoring results for that resource only. A resource group alert fires when a metric condition is true for a specified number or percentage of the resources in the group.
- **The only action a resource group alert can trigger is an escalation** - The only action you can assign to a group alert definition is an escalation.
- **A resource group alert fixes itself** - Although you can mark a group alert fixed - from the group's Alerts tab or other alert views - you don't need to. HQ automatically marks a group alert "fixed" when the condition that caused it to fire is no longer true. This shows up in the UI as "The problem fixed itself." in the "Alert Detail" screen.

Define a Resource Group Alert

**Step 1 - Select Target Compatible Group**

1. Browse to the compatible group to which the new alert definition will apply.
2. Click the Alert tab.
3. Click Configure.
4. Click New to display the New Alert page.

**Step 2 - Define Alert Properties**

On the New Alert page, define each property in the "Alert Properties" section.

- **Name** — Name assigned by the user creating an alert definition. A fired alert is identified, in the Hyperic user interface and alert notifications, by the alert definition name and a timestamp. An alert definition name should clearly communicate the nature of the problem. For example, "Down" for an alert on availability, or "Low Memory" for an alert on free memory.
- **Description** — Description entered by the user creating the alert definition.
• **Priority** — The severity of the problem, as defined by the person creating the alert definition: "Low", "Medium", or "High". A consistent policy for defining an alert definition priority makes it easier to triage problems appropriately. An alert's priority is shown in Hyperic pages that present alert status and in alert notifications. You can sort alerts by priority in vFabric Hyperic's Alert Center or Operations Center.

• **Active** — The current enabled/disabled status of the alert definition. Alerts only fire for enabled alert definitions. When an alert definition is disabled, Hyperic does not evaluate its condition or fire alerts for it.

**Step 3 - Define Alert Condition**

Determine why the alert will fire.

1. Select how many (an absolute number or percentage) of the resources in the group (the number of members is shown) that must satisfy the condition.
2. Select the metric and the comparison value that those resources must satisfy.
3. Click OK when you are done.

**Step 4 - Assign Escalation Action**

Assign an escalation to the alert. The series of notifications defined in the escalation will be performed when an alert is fired. You must define an escalation before you can assign it to an alert definition. Click Escalation Schemes Configuration on the Administration tab to define an escalation.

**Schedule Downtime for a Resource Group**

**Schedule Downtime**

The Schedule Downtime page, available from the Tools menu when a resource, or a resource group is selected, allows you to schedule a downtime period, during which alerts for the resource(s). You define a period of time - a start and end date and time. At the start of the downtime period, currently active alert definitions for resources in the group are disabled. At the end of the period, those alert definitions are re-enabled.

Only a Hyperic user with the Super User role may schedule downtime.

To schedule or reschedule maintenance:

1. Navigate to the individual resource (a platform, server, or service) or the resource group for which you wish to schedule downtime.
2. Choose Schedule Downtime from the Tools menu. The Schedule Downtime page appears.
3. On the Schedule Downtime page, enter the start and end dates and times for the downtime and click Schedule.
Create and Manage Applications

This section has instructions for configuring an application in Hyperic.

Related Information
For information about scheduling downtime from a program, script, or a command-line interface with Hyperic’s web services API, see HQApi maintenance command.

Learn About Applications
See About Applications in Hyperic.

Instrument Java Components (Optional)
You can gain deeper visibility into the health of Java applications by instrumenting application services.

The Hyperic Agent can auto-discover and manage Java application services via Model MBeans that adhere to a specified ObjectName naming convention and expose a specified set of service data. This enables deeper visibility into application health: you can monitor application services along with the hosting application server and its internal services. For more information, see Java Applications.

Note: Although instrumentation provides deeper visibility into Java application health, it is not required for application monitoring.

Create an Application
1. Click Browse on the Resources tab.
2. Click New Application in the Tools menu.
   The New Application page appears.
3. In the "General Properties" section of the New Application page, enter:
   - Name — Supply the name of the application.
   - Description — Enter a description of the application, if desired.
   - Location — Enter the location of the application, if desired.
4. In the "Application Properties" section of the New Application page, provide desired contact information:
   - Engineering Contact
   - Business Owner
   - IT Contact
5. Click OK.
   The Inventory page for the application appears
Add Services to an Application

1. In the "Services" section of the Inventory page for the application, click Add to List. The Edit Application page appears.
2. Checkmark desired services and click the blue arrow to move them from the Services column to the Add Services column. (The arrow is enabled when you select a resource.)
3. After moving desired resources to the Add Services column, click OK.

Add Application to a Group

4. In the "Groups" section of the Inventory page for the application, click Add to List. The Edit Application page lists existing mixed groups of applications.
5. Checkmark desired groups and click the blue arrow to move them from the Groups not containing this resource column to the Add to Groups column. (The arrow is enabled when you select a resource.)
6. After moving desired resources to the Add to Groups column, click OK.

Monitoring an Application with Indicator Charts
After you have created an application and added services to it, you can start monitoring all the application's components as a whole using indicator charts.

Initially, the Monitor tab displays only the availability metric indicator for the new application. The services you added are listed, along with "Host Servers" (the servers that host the listed services), on the Resources minitab tab, and through those you can add more metrics to the display.

Mapping vCenter Virtual Machine IDs to vFabric Hyperic Platforms

In order for vCenter Operations Manager to synchronize information from a vCenter server with vFabric Hyperic, the vFabric Hyperic platforms must have a unique identifier assigned that can be mapped to the corresponding vCenter virtual machine.

To configure unique IDs for vFabric Hyperic platforms:

1. On the masthead, click the Administration tab.
2. Select the HQ Server Settings link.
3. In the vCenter Server Settings section, enter the appropriate values:
   a. Enter the URL of the vCenter SDK in the vCenter URL text box. The URL is generally https://<IP address of vCenter Server>/sdk
   b. Enter the username of a user with vCenter administrator privileges in the vCenter User text box.
   c. Enter the password for the specified user in the vCenter Password text box.
4. Click Ok.
5. (Optional) Verify that the properties have been correctly applied.
   a. On the Resources tab, click a platform link.
   b. Verify that vCenter UUID and MOID values appear in the summary information at the top of the page.

Configuring Hyperic as an SNMP Trap Receiver

Receiving SNMP Traps from Network Devices or Systems

You can set up Hyperic to receive and log SNMP messages from a remote network management system or other SNMP-capable system or device. You can set alerts based on the received SNMP data to trigger notifications or other responses.

The process involves configuring the agent and the network system or device to communicate with each other, and creating a platform of type "Network Device" to represent the remote system or device.

Step 1 - Select and Enable an Agent to Receive Traps

When you configure an platform of type "Network Device" you provide specify connection information for an Hyperic Agent running on an operating system in your environment - that agent will receive the SNMP data. The agent you designate must be able to receive traps.

Note that the Hyperic Agent's default UDP port for receiving traps is 162, in the privileged range, which the agent cannot access unless it runs as as root (or as an Administrative user on Windows).

If you run the agent under the context of an non-administrative user, configure a non-privileged port to receive SNMP traps, by adding this property to its agent.properties file.

```
snmpTrapReceiver.listenAddress=udp:0.0.0.0/1620
```

This setting enables the agent to receive traps through any interface on the platform at UDP port 1620. If desired, you can specify an specific interface's IP address, or different port in the unprivileged range (1024 or above). Restart the Hyperic Agent after defining the listen address.

Why Don't I See the Open Port With `netstat`?
If you try to check that the SNMP port is open at this point, netstat will not show it open. Once you complete all steps in this procedure netstat output will produce expected results.
Step 2 - Configure Trap Generator

Set up the Hyperic Agent as a trap destination on the SNMP-enabled system or application, supplying the Hyperic Agent’s SNMP listen address and port - either the default connection settings, or if applicable, those configured in the previous step.

Step 3 - Create a Proxy Platform for Trap Data

In Hyperic, remotely monitored resources are represented as a platform. To create a platform for the remote device or host:

1. Select **New Platform** from the **Tools** menu.
2. Enter a name for your platform.
3. Select "Network Device" from the **Platform Type** pulldown.
4. Enter the FQDN of the network device or host.
5. Select the agent connection from the pulldown list - it must have connectivity to the SNMP port on the device or host.
6. Enter the IP address of the network device or host. Do not use 127.0.0.1, even if the application is local to the agent being used for the SNMP connection.
7. The netmask or MAC address of the device or server may be required depending on the configuration of the device.
8. Click **OK**.
9. The **Inventory** tab for the new platform is displayed.
10. Click **Edit** button in the **Configuration Properties** section.
11. Select the interface.index the device uses to uniquely identify interface services. Most devices work with the default ("ifDescr").
12. Supply or validate the snmpIp, snmpPort and SNMP community string.
13. Select the value for snmpVersion that corresponds to the device.
14. If you use SNMP v3, it is likely that authentication is configured, in which case enter username, password and auth type.
15. Check the box next to **Enable Log Tracking**, then click **OK**.

Monitoring will start in a few minutes.

Solving Problems

If the configuration is not accepted:

- Verify the IP address, SNMP port, SNMP version, and authentication settings, as applicable.
- Verify that the agent you selected for the proxy platform has network connectivity and can reach the SNMP port of the network device (check firewalls).
- Make sure that the community string configured for the proxy platform is the same as the community string the trap generator uses to send traps. If the strings do not match, traps cannot be sent to the proxy platform - instead, traps will be routed to the default platform, if that platform has log tracking enabled.
Check the Hyperic Agent log file to make sure that the agent has opened the proper UDP port. If properly configured, you should see messages similar to:

```
2008-06-05 16:45:05,447 DEBUG [SNMPTrapReceiver]
  snmpTrapReceiver.listenAddress=udp:0.0.0.0/1620
2008-06-05 16:45:05,572 DEBUG [SNMPTrapReceiver] Add 1:10003 for 10.2.0.2-switch
```
Manage Hyperic Users and Roles

Create and Manage User Accounts

If you use external authentication...

If Hyperic is configured to use your enterprise directory for user authentication, you do not have to manually create user accounts. Hyperic will automatically create an account for users that are externally authenticated by your LDAP, Active Directory, or Kerberos system. See the requirements on Create and Manage Roles in vFabric Hyperic.

Create a New User Account

The sections below have instructions for creating a user, and in vFabric Hyperic, assigning roles to the user.

Define User Account Attributes

To create a new Hyperic user:

1. Click New User on the Administration page.
2. The New User page appears.
3. Enter values for:
   - Name
   - Username — The username the user logs in with.
   - Phone
   - Department
   - Password — Passwords must contain at least 6 case-sensitive characters and numbers, and no spaces or quotation marks.
   - Email — User's email address.
   - Format — Toggle the radio button to select HTML or plain text.
   - SMS Address — An email-to-SMS gateway email address for the user's SMS device.
      - For a cellular phone on the Cingular network, this might look like 4155551212@mobile.mycingular.com. Check with the service provider for details about an email-to-SMS configuration. Basic alert notification sent to this user's SSS address will be in long format, which can result in up to five separate messages on the SMS device each time notification is sent by HQ. Hyperic recommends that SMS alerting be used in conjunction with escalations, not basic alert notification, but short format is used there.
   - Enable Login — Toggle the radio button to disable or enable the account. The user cannot log in when the login is disabled.
4. Click:
   - OK in Hyperic HQ to save the new account.
   - OK and Assign to Roles in vFabric Hyperic.

Assign Roles to a New User Account

In vFabric Hyperic, the roles to which a user is assigned govern which resources the user may access, and the operations the user can perform on those resources. Each role in vFabric Hyperic defines a permission matrix; users with a role may exercise the permissions it grants, on the resources in groups assigned to the role.

To assign roles to a user:

1. In the "Roles" panel on the left side of the page, checkmark each role to which you want to assign the user, and click the blue arrow to move the roles to the "Add to Roles" panel.
2. Click OK when you are done adding users to the role.

List User Accounts

1. Click List Users on the Administration page.
   The List Users page appears.
   The List Users page lists the following information for each user account.
   - First Name
   - Last Name
   - UserName — Click a user name to view and edit the user account.
   - Email — Click an email address to send mail to the user.
   - Department

View a User Account

1. List user accounts, following the instructions in List User Accounts.
2. Click the UserName for the user account you wish to view.
   The UserName page appears.
   - The General Properties section contains this information:
     - Name
     - Username — The username the user logs in with.
     - Phone
     - Department
     - Password — The user's password is not displayed. If you have the permission to modify the password, a Change... link is present.
     - Email — User’s email address. Click to send an email to the user.
     - Format — Format for email notifications sent to the user — HTML or plain text.
- **SMS Address** — An email-to-SMS gateway email address for the user's SMS device.
- **Enable Login** — Indicates whether or not the account is enabled. The user cannot log in when the login is disabled.
  - The **Roles Assigned To** section contains:
    - A list of the roles to which the user is assigned.
    - An **Add to List** button — click it to assign additional roles to the user.

**Modify User Account Settings**
- Navigate to the user account, as described in [View a User Account](#).

**Change Password**
The **Change Password** page allows you to change a user's account password.

**Requirements for changing passwords**
In vFabric Hyperic, only a user with a role that grants "Full" or "Read/Write" permissions to user accounts may change another user's password. You must enter your current password in order to change an account password, whether the account is yours, or another user's.

To change the password for a vFabric Hyperic account:

1. Click the **Administration** tab in the Hyperic user interface.
2. Click **List Users** in the "Authentication/Authorization" section. The **List Users** page appears.
3. Click the link in the "UserName" column for the user whose password you wish to change.
4. In the "General Properties" section of the page that appears, click the **Change...** link in the "Password" field. The **Change Password** page appears.
5. Enter your password in the **Enter Your Current Password** field. The password entered must be the password of the user making the change, not the password of the user whose password is being changed.
6. Enter the new password for the selected account in the **New Password** field.
7. Re-enter the password in the **Confirm New Password** field.
8. Click **OK**.

**Edit Account Settings**

1. Click **Edit** in the "General Properties" section of the **UserName** page. The "Edit **UserName**" page appears.
   a. Enter values for:
      o **Name**
      o **Username** — The username the user logs in with.
- **Phone**
- **Department**
- **Email** — User's email address.
- **Format** — Toggle the radio button to select HTML or plain text.
- **SMS Address** — An email-to-SMS gateway email address for the user's SMS device.
  - For a cellular phone on the Cingular network, this might look like 4155551212@mobile.mycingular.com. Check with the service provider for details about an email-to-SMS configuration. Basic alert notification sent to this user's SSS address will be in long format, which can result in up to five separate messages on the SMS device each time notification is sent by HQ. Hyperic recommends that SMS alerting be used as a step in an escalations, not basic alert notification, but short format is used there.
- **Enable Login** — Toggle the radio button to disable or enable the account. The user cannot log in when the login is disabled.

b. Click **OK**.

**Update Roles Assigned to a User**

1. Click **Add to List** in the "Roles Assigned To* section of the **UserName** page. The *Edit **UserName** page appears.

2. In the "Roles" panel on the left side of the page, checkmark each role to which you want to assign the user, and click the blue arrow to move the roles to the "Add to Roles" panel.

3. Click **OK** when you are done adding users to the role.

**Create and Manage Roles in vFabric Hyperic**

**Create a Role**

---

**Learn About Roles**
For an introduction to roles in vFabric Hyperic, see [User Accounts and Roles in Hyperic](#).
Role Names and LDAP Authorization

If you use LDAP or Active Directory for user authorization, vFabric Hyperic can automatically assign users to Hyperic roles whose name matches a group to which the user is assigned — if the Hyperic role names and LDAP group names adhere to a required naming convention.

To take advantage of this functionality:

- A role name in Hyperic must match a group name in your authorization directory. In addition to being identical, both role name and group name must be prefixed by "org\", for example "org\Admin".
- Hyperic Server must be configured to use your LDAP system. For instructions see Configure LDAP Properties or Configure Kerberos Properties.

1. Click New Role on the Administration page.
2. In the "Properties" section of the New Role page, enter:
   - Name
   - Description, if desired.
3. In the Permissions section, select a permission level - Full, Read-Write, Read-Only, or None for each type:
   a. Users
      - Grant Full to enable role users to create and delete HQ user accounts.
      - Grant Read-Write to enable role users to edit HQ users accounts.
   b. Roles
      - If you select Full, which enables role users to create roles, HQ will ensure that the role's permission level to Users and Groups is at least Read-Only, because to create a role, you need to view users and groups.
   c. Groups
      - Grant Full to enable role users to delete groups created by others.
      - Grant Read-Write to enable role users to modify groups created by others.
      Note that regardless of the permission level you select, any user can create groups, and as the owner of such groups, delete them.
   d. Platforms
      - If you select Full, which enables role users to delete platforms and their child resources, HQ will require that the role’s permission level to Servers and Services is also Full.
      - If you select Full or Read-Write, HQ will automatically checkmark the Can Fix/Ack Alerts? and Can Control? capabilities.
      - If you select Read-Only, you have the option to grant alert management or resource control capabilities by clicking Can Fix/Ack Alerts? or Can Control? respectively.
      - If you select None, you cannot grant alert management or resource control permissions.
e. **Servers**
   - If you select **Full**, which enables role users to delete servers and child services, HQ will require that the role’s permission level to Platforms is at least **Read-Write**, and its permission level to Services is **Full**.
   - If you select **Full** or **Read-Write**, HQ will automatically checkmark the **Can Fix/Ack Alerts?** and **Can Control?** capabilities.
   - If you select **Read-Only**, you have the option to grant alert management or resource control capabilities by clicking **Can Fix/Ack Alerts?** or **Can Control?** respectively.
   - If you select **None**, you cannot grant alert management or resource control permissions.

f. **Services**
   - If you select **Full**, HQ will require that the role’s permission level to Servers is at least **Read-Write**.
   - Grant at least **Read-Only** if you are going to grant the role **Full** permission to Applications.
   - If you select **Full** or **Read-Write**, HQ will automatically checkmark the **Can Fix/Ack Alerts?** and **Can Control?** capabilities.
   - If you select **Read-Only**, you have the option to grant alert management or resource control capabilities by clicking **Can Fix/Ack Alerts?** or **Can Control?** respectively.
   - If you select **None**, you cannot grant alert management or resource control permissions.

g. **Applications**
   - Grant **Full** if you want role users to be able to create and delete applications.
   - Grant **Read-Write** if you want role users to be able to modify change applications created by others.

h. **Escalations**
   - Grant **Full** if you want role users to be able to create and delete escalations groups.
   - Grant **Read-Write** if you want role users to be able to modify escalations.

The role is saved, and the refreshed role page will have three new sections: "Assigned Users", "Assigned Groups", and "Alert Calendar".

Proceed to **Assign Users to a Role**.

**Assign Users to a Role**

In vFabric Hyperic, each user you assign to a role can exercise the permissions defined for the role, on resources in the groups assigned to the role.

1. If you are not currently viewing the role to which you wish to assign users, navigate to the role.
2. Click **Add to List** in the "Assigned Users" section of the page.
   The Assign Users to Role page appears.
3. On the "Users" panel on the left side page, checkmark each HQ user you wish to add to the role, and click the blue arrow to move the users to the "Assign To Role" panel.
4. Click **OK** when you are done adding users to the role.

If you are creating a role purely for the purpose of role-based alert notification, skip to [Define Alert Calendar for Follow-the-Sun Role-Based Notifications](#). Otherwise proceed to [Assign Groups to a Role](#).

### Assign Groups to a Role

In vFabric Hyperic, the groups of resources you assign to a role constitute the population of resources to which users with that role may exercise the permissions associated with the role. (For example, if the role's permission level to Platforms is **None**, role users will not have access to platforms in groups assigned to the role.)

**Permissions are granted only to groups of individual resources**

Assigning a group of groups or a group of applications to a role does **not** grant permissions to individual resources in nested groups or applications. Groups you assign to a role for the purpose of granting permissions must contain individual resources, as opposed to other groups or applications.

For more information, see [User Accounts and Roles in Hyperic](#).

1. If you are not currently viewing the role to which you wish to assign groups, navigate to the role.
2. Click **Add to List** in the "Assigned Groups" section.
   
   The Assign Groups to Role page appears.

3. On the "Groups" panel on the left side of the page, checkmark each resource group you wish to add to the role, and click the blue arrow to move the groups to the "Assign To Role" panel.
4. Click **OK** when you are done adding groups to the role.

Proceed to [Define Alert Calendar for Follow-the-Sun Role-Based Notifications](#), as desired.

### Define Alert Calendar for Follow-the-Sun Role-Based Notifications

An alert calendar defines the availability calendar during which role users are available for alert notifications. You should define an alert calendar if:

- You are creating a role that will be a recipient of alert notifications, and
- The users assigned to the role users are available only during specific intervals only.
By default, a role's alert calendar settings specify that role users are available for notifications 24 hours a day, 7 days a week, with no exceptions. To define a narrower availability calendar:

1. For each day in the week,
   a. Use the first set of From and To pull-downs to specify a start time and an end time that role users are availability for notifications.
   b. If there is a period of time within the availability period specified in the previous step, during which role users should *not* receive notifications, click Except, and use the From and To pull-downs on the right to specify that period of time.

2. Click Save after defining the alert calendar.

You must define additional role or roles with complementary alert calendars to ensure that there is a role whose users are available during periods of time that the current role's alert calendar does not include.

**Customize Role-Specific Dashboard**

When you create a role, vFabric Hyperic creates a Dashboard with the same name as the role, which Hyperic users with the role can select from the Select a Dashboard pull-down in the upper left corner of the Hyperic Dashboard.

As desired, you can add, remove, or reconfigure the portlets on the role dashboard to meet the needs of role users. For more information see Role-Based Dashboards in vFabric Hyperic.

**Use Roles for Follow the Sun Alerting**

HQ allows you to notify users of incidents based on support schedules, greatly simplifying the management of 24x7 or rotating support teams. This is accomplished through the use of role-based alert calendars. The alert calendar can be most usefully applied in an , wherein multiple sets of people can be selected for notification, but only the one whose alert calendar is currently open will be notified.

To implement follow the sun alerting:

1. Create multiple roles.
2. For each role, assign complementary alert calendars (that is, alert calendars that span different periods of time, but all together cover the calendar).
   On the "Edit Role" screen, follow the instructions on *ui-Admin.Role* for creating a calendar for a role.
3. Define an escalation scheme with at least one "SMS" or "email" escalation action. For instructions, see Configure and Manage Escalations.
   In the escalation action, instruct HQ to notify "All users assigned to a specific role" and then select all of the just-defined roles.
4. Create an alert and assign that escalation scheme to it.

When the alert is fired, HQ will start performing the escalation actions but will only notify the roles whose alert calendars are currently open.
List Roles

- Click List Roles on the Administration page.

The List Roles page appears.

The List Roles page lists the following information for each role.
- **Name** — Click a role name to view and edit the role.
- **Number of Members**
- **Description**

View a Role

1. List roles, following the instructions in List Roles.
2. Click the name of role you wish to view.

Properties Section

The Properties section contains this information:

- Name
- Owner — The user who created the role.
- Description
- Administer HQ Server Configuration
- Dashboard Name

Permissions Section

The Permissions section displays the permission matrix for the role.

- **None** - No access at all to instances of the type.
- **Read-Only** - Allows role users to view instances of the type, but not create, edit, or delete them.
  - For Platforms, Servers, Services, Groups, also enables:
    - **Read-Only** access to alert definitions for the inventory type.
      
      *A role with Read-Only permission level does not have permissions to enable/disable/fix/ack alerts or control resources - these capabilities must be explicitly granted.*
    - **Read-Write** - Allows role users to view and edit instances of the type, but not create or delete them. For Platforms, Servers, Services, Groups, also gives:
      - **Full** access to alert definitions for the inventory type,
      - Permission to manage alerts (enable/disable, fix, acknowledge) for the inventory type.
      - Permission to perform supported control operations on resources of the inventory type.
- **Full** - Allows role users to create, edit, delete, and view instance of the type. For Platforms, Servers, Services, Groups, also gives:
  - **Full** access to alert definitions for the inventory type.
  - Permission to manage alerts (enable/disable, fix, acknowledge) for the inventory type.
  - Permission to perform supported control operations on resources of the inventory type.

Click **Edit** to modify the permission matrix.

### Assigned Users

The Assigned User section lists the following information for each user assigned to the role:

- First Name
- Last Name
- UserName — Click to view the user.

Click **Add to List** to add users to the role.

### Assigned Groups

The Assigned Groups section lists the following information for each group assigned to the role:

- **Group** — The name of the group. Click to view the group.
- **Description**

Click **Add to List** to add users to the role.

### Alert Calendar

The Alert Calendar section defines the availability calendar during which role users are available for alert notifications.

Custom alerts calendars enable "follow the sun" alert notifications. To implement a follow the sun notification strategy, you create multiple roles with complementary alert calendars. You assign a user to the role whose alert calendar matches the user's availability.

By default, a role's alert calendar settings specify that role users are available for notifications 24 hours a day, 7 days a week, with no exceptions.

To define an availability calendar for a role:

1. For each day in the week,
   - Use the first set of **From** and **To** pull-downs to specify a start time and an end time that role users are availability for notifications.
   - If there is a period of time within the availability period specified in the previous step, during which role users should not receive notifications, click **Except**, and use the **From** and **To** pull-downs on the right to specify that period of time.
2. Click **Save** after defining the alert calendar.
You must define additional role or roles with complementary alert calendars to ensure that there is a role whose users are available during periods of time that the current role's alert calendar does not include.

**Edit a Role**

1. List roles, following the instructions in [List Roles](#).
2. Click the name of role you wish to edit.
3. To make changes to:
   - Role permissions — Click **Edit** in the **Permissions** section of the page. See [Create a Role](#) for instructions.
   - Which users are assigned to the role — Click **Edit** in the **Assigned Users** section of the page. See [Assign Users to a Role](#) for instructions.
   - The alert calendar for role — Follow the instructions in [Define Alert Calendar for Follow-the-Sun Role-Based Notifications](#).

**Role-Based Dashboards in vFabric Hyperic**

**Role-Based Dashboards**

A role-based dashboard is a version of the HQ dashboard available to users assigned to the role. A role-based dashboard can be customized to match the needs and interests of users with that role. You can configure the contents of a role-based dashboard to meet the needs of users with that role.

A role-based dashboard is available in addition to a user's personal dashboard. Every vFabric Hyperic user has a personal dashboard, and a role-based dashboard for each role to which he is assigned.

Any modification to a role-based dashboard affects all users with the role; unlike a personal dashboard, a role-based dashboard cannot be customized on a per user basis.

**Role-Based Dashboards are Automatically Available**

Upon creation of a new role, a copy of the standard vFabric Hyperic dashboard is saved and available to members of the role. Any HQ user with this role can navigate to it using the **Select a Dashboard** pull-down, and designate it as his default dashboard.

The default dashboard for a new user is his personal dashboard. To set a role-based dashboard to be the default, a user must select select it and click **Make Default**.

**Permissions for Modifying Role-Based Dashboards**

A role-based dashboard can be modified by:

- an HQ administrator with the Super User role
- an HQ user assigned to the role, if the role grants the "Modify" permission for "Roles"
Tailor a Role-Based Dashboard

To tailor the layout and content of a role-based dashboard:

1. Select the role-based dashboard from the Select a Dashboard pull-down on the currently displayed dashboard.
2. Add, configure, remove, and rearrange the portlets in the dashboard, as desired. See the instructions on ui-Dashboard.

Modifications to a role-based dashboard are immediate, and will appear any time a user with that role accesses it.

Manage Inventory with HQApi

For information about managing HQ inventory with HQApi, see these topics in Web Services API.
View and Manage Resource Data

View Inventory Properties for a Resource

In the Hyperic user interface, a resource's Inventory Page presents a variety of resource properties and key information about the resource's closest "relatives" in the resource hierarchy. The information on the Inventory page varies by both inventory type and resource type, and includes auto-discovered and user-configured resource properties. For a fundamental inventory type — a platform, serve, or service — the Inventory Page contains a "Configuration Properties" section, where you can view and update the properties that enable or tailor monitoring behaviors for the resource.

Learn About Resources in Hyperic
See Resources, Resource Types and Inventory Types in vFabric Hyperic Overview.

View Inventory Properties for a Platform

Navigate to the Inventory Page for a Platform

To display the Inventory page for a platform, use Resources > Browse > Platforms to navigate to the platform, and click the Inventory tab.

Inventory Page Header

The sections below describe the data and controls that appear at the top of the Inventory page for a platform.

Resource Properties

The properties at the top of the Inventory page for a platform provide identifying information about the managed product. The inventory properties displayed for a platform vary slightly by platform type, but typically will include most of these properties.

The properties displayed are:

- **Description**
- **Owner** - By default, the Hyperic user under whose account the resource was added to inventory. Click Change... to assign a different resource owner.
- **Secondary DNS**
- **Default Gateway**
- **Vendor**
- **Vendor Version**
- **IP Address**
- **Primary DNS**
- **CPU Speed**
The plugin developer controls which resource properties are displayed at the top of a resource's Inventory page: any properties enclosed in a <properties> element for a resource type appear in the page header when you browse to an instance of that type.

Map Control for a Platform

Click the Map control in the page header for a graphical view the servers on the platform. The platform is displayed at the bottom of the map; servers are displayed above the platform. Resource names are in bold and the resource type is displayed just below in smaller type. Click a resource name to navigate to that server.

Tools Menu for a Platform

The screenshot below is the Tools menu for a platform.

When a platform is selected, the Tools menu has the following commands:

- **Configure Platform** — Opens the Configuration Properties page for the platform, where you can edit the resource's configuration properties.
- **Clone Platform** — Creates a new platform with the same configuration as an existing platform. For more information, see *Clone a Platform*.
- **Delete Platform** — Delete the platform, its platform services, servers, and the services in the servers from inventory.

**Do you want to rediscover the platform?**

Note that if you delete all of the platforms that a Hyperic Agent manages, the Hyperic Server also removes the saved authentication token for that agent from the Hyperic database. So if you delete a platform that is managed by an agent that does not manage any other platforms (as in the case of an agent that manages only the platform it runs on), the agent will no longer be able to connect to the Hyperic Server. If you want the agent to rediscover the platform where the agent runs, you must repeat the agent setup process. Otherwise (if you do not want the agent to re-discover the platform it runs on) shut down the agent, and uninstall the agent from that platform.

- **New Server** — Displays the **New Server** page, where you can manually add a new server to the platform. (For instance, a server that was not auto-discovered.) For more information, see *Create a Server*.
- **New Platform Service** — Displays the **New Service** page, where you can manually add a new service, for instance a remotely monitored network service, to the platform. For more information, see *Create a Platform Service*.
- **New Auto-Discovery** — See *Scan a Platform On-Demand*
- **Enable All Alerts On This Agent** —
- **Disable All Alerts On This Agent**
- **Add to Dashboard Favorites** — Adds the platform to the **Favorite Resources** portlet on the current Hyperic user's Dashboard.
- **Add to Group** — Opens the **Group Manager** page, which lists the groups to which the platform may be added. You can add a platform to a group if:
  - You have permission to access the group, and:
    - The group is a mixed group that contains platforms, servers, and services.
    - The group is a compatible group of the selected platform's platform type.

**General Properties for a Platform**

The General Properties section of the **Inventory** page for a platform lists the following information:

- **Description** — A description of the platform. This is an optional, user-configured value.
- **Date Created** — The date the platform was added to the Hyperic inventory
- **Location**
- **Date Modified, Modified By** — The date the platform was last modified and the user who modified it.
- **Resource Type** — The platform type.
Click the **Edit** button to open a page where you can edit the platform's **Name** or **Description**.

### Type and Network Properties for a Platform

The Type and Network Properties section of the Inventory page for a platform lists the following information:

- **Platform Type** — The type of platform (This value cannot be changed.)
- **Agent Connection** — The IP address:port pair that the Hyperic Server will use to connect to the Hyperic Agent on the platform device.
  - In the case of a platform type that is monitored by a Hyperic Agent on a different platform, such as a network or virtual host, this property identifies the agent that manages the platform.
- **Fully Qualified Domain Name** — The platform’s FQDN.
- **IP Address, MAC Address, Netmask** — One or more sets of these identifiers for the platform. There is at a minimum one set for the loopback (local) IP address — 127.0.0.1 — and then additional sets for each network interface on the device.

Click the **Edit** button to open a page where you can selected platform properties.

### Servers on a Platform

The "Servers" section lists the following information for each server on the platform.

- **Server** — The resource name, presented as a hyperlink you can click to navigate to the server.
- **Server Type**
- **Install Path**
- **Description**
- **Availability** — Current availability of the server.

There are two controls available:

- **New** — Click to add a server to the platform.
- **Delete** — Click to delete a server from the platform. Services in the server will also be deleted.
Services on a Platform

This section lists the following information for each platform service on the platform:

- **Service** — The resource name, presented as a hyperlink you can click to navigate to the service.
- **Description**
- **Availability** — Current availability of the platform service.

There are three controls available:

- **View** — This pull-down allows you to filter the list to display only platform services of a selected type.
- **New** — Click to add a platform service to the platform.
- **Delete** — Click to delete a platform service from the platform.

Groups Containing a Platform

This section lists the following information for each the group of which the platform is a member.

- **Group** — The resource name, presented as a hyperlink you can click to navigate to the group.
- **Description**

There are two controls available:

- **Add to List** — Click to add the platform to a group.
- **Remove From List** — If you have checkmarked one or more groups in the list, this control allows you to remove the resource from the selected groups.

Configuration Properties for a Platform

This section displays the configuration properties for the platform.

- **Shared** — These properties are typically only present for platform types that Hyperic does not auto-discover, and vary by platform type.
- **Monitoring** — These properties control log and configuration tracking for the platform. For more information see Log and Configuration Event Tracking.

View Inventory Properties for a Server

This section describes the contents of the Inventory page for a server.

Learn about Servers

See Resources, Resource Types and Inventory Types in vFabric Hyperic Overview.

Inventory Page for a Server

To display the Inventory page for a server, use Resources > Browse > Servers to navigate to the server, and click the Inventory tab.
In vFabric Hyperic, a user can view and modify resources only to the extent that the user’s role(s) permit. For more information see User Accounts and Roles in Hyperic in vFabric Hyperic Administration.

Inventory Page Header for a Server

The sections below describe the data and controls that appear at the top of the Inventory page for a server.

Resource Properties

The properties at the top of the Inventory page for a server provide identifying information about the managed product. The inventory properties displayed for a server vary by server type, but typically will include vendor name and software version.

The properties displayed in the screenshot below (for a JBoss server) are:

- Java Vendor
- Owner - By default, the Hyperic user under whose account the resource was added to inventory. Click Change... to assign a different resource owner.
- Build Date
- JBoss Version
- Version Name

The plugin developer controls which resource properties are displayed at the top of a resource’s Inventory page: any properties enclosed in a <properties> element for a resource type appear in the page header when you browse to an instance of that type.

Map Control for a Server

Click the Map control in the page header to view the server’s child services(s) and its parent platform.
The map in the screenshot above, for a PostgreSQL 8.2 server, shows that:

- The server has multiple children of resource type "PostgreSQL 8.2 Table service" - which have been automatically grouped into an autogroup with the same name as the resource type.
- The server runs on the platform of type "MacOSX" named "Marie-McGarrys-MacBook-Pro-46.local".

Click the name of a child or parent resource to view its Monitor page.

**Tools Menu for a Server**

When a server is selected, the **Tools** menu has the following commands:

- **Configure Server** — Opens the **Configuration Properties** page for the server, where you can edit the resource's configuration properties.
- **Delete Server** — Delete the server and all its child services from inventory.
- **New Service** — Displays the **New Service** page, where you can manually add a new child service to the server. (For instance, a service that was not auto-discovered.)
- **Add to Dashboard Favorites** — Adds the server to the **Favorite Resources** portlet on the current Hyperic user's Dashboard.
- **Add to Group** — Opens the **Group Manager** page, which lists any compatible groups of the same type as the server.

In **vFabric Hyperic**, a user can view and modify resources only to the extent that the user's role(s) permit. For more information see [User Accounts and Roles in Hyperic](#).

**General Properties for a Server**

The **General Properties** section of the **Inventory** page for a server lists the following information about the server:

- **Description** — A description of the server. This is an optional, user-configured value.
- **Resource type** — The server type.
- **Date Created** — The date the server was added to the Hyperic inventory
- **Date Modified, Modified By** — The date the server properties were last modified and the user who modified them

Click the **Edit** button to open a page where you can edit the server's Name or Description.

**Type and Host Properties**

The **Type and Host Properties** section of the **Inventory** page for a server lists the following information about the server:

- **Install Path** — The path where this server is installed.
- **Host Platform** — The platform where the server runs.
Click the **Edit** button to open a page where you can edit the server's Install Path.

<table>
<thead>
<tr>
<th>Type &amp; Host Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Path: Applications/EE4-1908/server-4.4.0-EE/no-engine/serverdefault</td>
</tr>
<tr>
<td>Host Platform: Mark-McGarrye-MacBook-Pro-46.local</td>
</tr>
</tbody>
</table>

### Services on a Server

The Services section of the Inventory page for a server contains:

- The total number of child services on the server, and the number of services of each service type discovered on the server.
- The following columns for each service:
  - **Service** — Name of the service
  - **Service Type** — Resource type of the service.
  - **Description** — Text description of the service. This is an optional, user-configured value.
  - **Availability** — Current availability of the service.

To delete one or more services from inventory, click the box to the left of each service you wish to delete, and click **Delete**.

### Groups Containing a Server

The Groups Containing This Resource section of the Inventory page for a server lists the groups of which this server is a member. To view the Inventory page for a group, click its name.

### Configuration Properties for a Server

The Configuration Properties section of the Inventory page for a resource contains the configuration options and currently selected values for the resource. Configuration properties for the resource are presented in three sections:

- **Shared** — The properties in this section relate to more than one management function, for instance both monitoring and control actions.
- **Monitoring** — These properties set options related to log tracking, configuration tracking, and, for servers, here is where you can disable auto-discovery of child services.
- **Control** — If Hyperic supports control actions for the currently selected resource type, this section includes any configuration properties required to enable resource control, for example, the path of the start script to use to start a server.

Click **Edit** to open the Edit Configuration Properties page for the currently selected resource.

The plugin developer defines each configuration property for a resource type in the plugin descriptor. The plugin or the descriptor may set the initial value for a configuration property. For some types of resources, you may need to supply configuration property values to enable monitoring.
View Inventory Properties for a Service
This section describes the contents of the Inventory page for a service.

Learn about Services
See Resources, Resource Types and Inventory Types in vFabric Hyperic Overview.

Inventory Page for a Service
To display the Inventory page for a service, use Resources > Browse > Services to navigate to the service, and click the Inventory tab.

To view a screenshot of the Inventory page for a service, see Inventory Page - Service.

Inventory Page Header for a Service
The sections below describe the data and controls that appear at the top of the Inventory page for a service.

Resource Properties
The properties at the top of the Inventory page for a service provide identifying information including:
- Description
- Owner - By default, the Hyperic user under whose account the resource was added to inventory. Click Change... to assign a different resource owner.

The plugin developer controls which resource properties are displayed at the top of a resource's Inventory page: any properties enclosed in a <properties> element for a resource type appear in the page header when you browse to an instance of that type.

Map Control for a Service
The Map control presents graphical view of the service and the resources that are related to it. The map illustrates hierarchical inventory relationships, and a resource's membership in groups or applications.

The screenshot below is a resource map for a service of type "ActiveMQ Embedded 5.3 Topic".

- The service runs in an "ActiveMQ Embedded 5.3" server, which is hosted on a "MacOSX" platform
- The service is part of an application called "myap".
Tools Menu for a Service

When a service is selected, the Tools menu has the following commands:

- **Configure Service** — Opens the **Configuration Properties** page for the service, where you can edit the resource's configuration properties.
- **Delete Service** — Delete service from inventory.
- **Add to Dashboard Favorites** — Adds the service to the **Favorite Resources** portlet on the current Hyperic user's Dashboard.
- **Add to Group** — Opens the **Group Manager** page, which lists the groups to which the service may be added. You can add a service to a group if:
  - You have permission to access the group, and:
    - The group is a mixed group that contains platforms, servers, and services.
    - The group is a compatible group of the selected service's service type.

General Properties for a Service

The **General Properties** section of the **Inventory** page for a service lists the following information:

- **Description** — A description of the service. This is an optional, user-configured value.
- **Date Created** — The date the service was added to the Hyperic inventory
- **Location**
- **Date Modified, Modified By** — The date the service was last modified and the user who modified it.
- **Resource Type** — The service type.

Click the **Edit** button to open a page where you can edit the service's Name or Description.

Groups Containing a Service

This "Groups Containing this Resource" section lists the following information for each the group of which the service is a member.

- **Group** — The resource name, presented as a hyperlink you can click to navigate to the group.
- **Description**

There are two controls available:

- **Add to List** — Click to add the service to a group.
- **Remove From List** — If you have checkmarked one or more groups in the list, this control allows you to remove the resource from the selected groups.

Configuration Properties for a Service

This section displays the configuration properties for the service.

- **Shared** — These properties vary by service type.
- **Monitoring** — These properties control log and configuration tracking for the service.
View Inventory Properties for a Group

This section describes the contents of the Inventory page for a group.

Learn about Groups

See About Groups in Hyperic in vFabric Hyperic Overview.

Navigate to the Inventory Page for a Group

To display the Inventory page for a compatible or mixed group, use:

- **Resources > Browse > Compatible Groups/Clusters**, or
- **Resources > Browse > Mixed Groups**

and click the Inventory tab.

In vFabric Hyperic, a user can view and modify resources only to the extent that the user’s role(s) permit. For more information see User Accounts and Roles in Hyperic.

Inventory Page Header for a Group

The sections below describe the data and controls that appear at the top of the Inventory page for a group.

Resource Properties for a Group

The properties at the top of the Inventory page for either a compatible or mixed group are:

- **Description**
- **Owner** — By default, the Hyperic user under whose account the resource was added to inventory. Click Change to assign a different resource owner.

Map Control for a Compatible Group

The Map control is present on the Inventory tab for a compatible group, not for a mixed group. The map for a compatible group shows the members of the group.

The screenshot below is a resource map for compatible group that contains servers of type "VMware VI3 VM" - the name of each member resource is shown as a hyperlink.
Tools Menu for a Group

The Tools menu for a compatible or a mixed group has the following commands:

- **New Group** — Opens the New Group page, where you can create a new group.
- **Delete Group** — Deletes the group, but not its member resources.
- **Add to Dashboard Favorites** — Adds the group to the Favorite Resources portlet on the current Hyperic user's Dashboard.
- **Add to Group** — Opens the Group Manager page, which lists the groups to which the group may be added. You can add a group to another group if:
  - You have permission to access the target group, and:
  - The target group is a mixed group that contains groups.
- **Schedule Downtime** — This option opens the Schedule Downtime popup, where you can schedule a period of time during which alerts for members of the group will not fire. For more information see Schedule Downtime for a Resource Group.

General Properties for a Group

The General Properties section of the Inventory page for a service lists the following information:

- **Description** — A description of the service. This is an optional, user-configured value.
- **Date Created** — The date the service was added to the Hyperic inventory
- **Location**
- **Date Modified, Modified By** — The date the service was last modified and the user who modified it.
- **Resource Type** — The service type.

Click the **Edit** button to open a page where you can edit the service's Name or Description.

Resources

This section lists the following information for each the group of which the service is a member.

- **Group** — The resource name, presented as a hyperlink you can click to navigate to the group.
- **Description**

There are two controls available:

- **Add to List** — Click to add the service to a group.
- **Remove From List** — If you have checkmarked one or more groups in the list, this control allows you to remove the resource from the selected groups.

Roles a Group is Assigned To

The "Roles Assigned To" section is present in vFabric Hyperic only ---- it lists the roles to which the group is assigned, which, along with the permission matrix for the role, governs the access that users with the role have to resources in the group.
For more information about roles, groups, and resource permissions, see *Roles in vFabric Hyperic* in *vFabric Hyperic Overview*.

View Inventory Properties for an Application

This section describes the contents of the Inventory page for an application.

Learn about Applications

See *About Applications in Hyperic* in *vFabric Hyperic Overview*.

Inventory Page for an Application

In Hyperic, an application is an inventory type, configured by an authorized user. An application is a set of selected services, usually running in different servers on multiple platforms, that together fulfill a single business purpose. Configuring applications enables you to manage your infrastructure from an application — as opposed to a hardware — perspective.

To display the Inventory page for an application, use Resources > Browse > Applications to navigate to the application, and click the Inventory tab.

In vFabric Hyperic, a user can view and modify resources only to the extent that the user's role(s) permit. For more information see *User Accounts and Roles in Hyperic* in *vFabric Hyperic Administration*.

The following screenshot shows the Inventory tab for the application. Note:

- This is the tab you use to add services to an application.
- The "Service Counts" section shows the total number of services in the application, and the number of each type.
- The "Services" section lists key information for each service in the application.
Inventory Page Header for an Application

The sections below describe the data and controls that appear at the top of the Inventory page for an application.

Resource Properties

The properties at the top of the Inventory page for an applications are:

- Owner - By default, the Hyperic user under whose account the resource was added to inventory. Click **Change** to assign a different resource owner.
Tools Menu for an Application

When an application is selected, the Tools menu has the following commands:

- **Delete Application** — remove the application from inventory.
- **Add to Dashboard Favorites** — Adds the application to the Favorite Resources portlet on the the current Hyperic user's Dashboard.
- **Add to Group** — Opens the Group Manager page described below in Group Manager.

In vFabric Hyperic, a user can view and modify resources only to the extent that the user’s role(s) permit. For more information see User Accounts and Roles in Hyperic.

General Properties for an Application

The General Properties section of the Inventory page for an application lists the following information about the application:

- Description — A description of the application. This is an optional, user-configured value.
- Location — An optional property.
- Date Created — The date the application was created.
- Date Modified, Modified By — The date the application was last modified and the user who modified it.

Click the **Edit** button to open a page where you can edit the application’s Name or Description.

Application Properties

The General Application section of the Inventory page for an application lists the following information about the application:

- Application Type — This property, supported in previous versions of Hyperic, is no longer used.
- Engineering Contact — An optional property.
- Business Owner — The date the application was created.
- IT Operations Contact — The date the application was last modified and the user who modified it.

Click the **Edit** button to open a page where you can edit the contact-related properties for the application.

Service Counts for an Application

The Service Counts section of the Inventory page for an application lists the total number of services in the application and the number of services of each service type.
Services in an Application

The Services section of the Inventory page for an application lists the following information for each of the services in the application:

- name — Name of the service
- Entry Point — Whether the service is the entry point for the application.
- Service Type — Resource type of the service.
- Res Type —
- Host Server — Name of the server where the service runs.
- Availability — Current availability of the service.

You update the application in these ways:

- To add services to the application, click Add to List---the Edit ApplicationName appears.
- To remove one or more services from the application, click the box to the left of each service you wish to delete, and click Delete.

Note: The Dependencies control relates to functionality not implemented in this version of Hyperic.

Groups Containing an Application

The Groups Containing This Resource section of the Inventory page for an application lists the groups to which it belongs.

- To view the inventory page for a group to which the application belongs, click the group's name.
- Click Add To List to select the groups to which you wish to add the application.
- To remove the application from a group, checkmark the group, and click Remove From List.

Group Manager

The Group Manager, which appears when you click Add to List on the Groups Containing This Resource section of a resource's Inventory page, lists the groups to which you can add the application. Only groups that contain applications appear on the list, and only those that do not already contain the current application.

Create a Platform, Server, or Service Manually

Most resource types are automatically discovered, and auto-discovery is the only way an operating system platform can be added to inventory. Conversely, auto-discovery of network or virtual platform types is not possible — you must add such platforms to inventory manually.

Most server types are auto-discovered. You create a server manually only if the managing plugin does not support server discovery, or if the plugin fails to discover a server, for instance, because it has an other-than-expected name in the process list or Windows registry.
Network services that are monitored remotely cannot be auto-discovered—you must manually create a platform service to represent a network service.

**Note:** For information about auto-discovery, see Resource Auto-Discovery Processes.

### Create a Platform

This section has general instructions for creating a platform in Hyperic.

For information about creating a platform using the HQApi see HQApi resource command in vFabric Hyperic Web Services API.

### When to Create a Platform Manually

Operating system platform types are auto-discovered and cannot be manually added to inventory. The only platform types you can manually add to inventory are:

- Cisco IOS
- Cisco PIXOS
- GemFire Distributed System
- NetApp Filer
- Network Device
- VMWare VI3 Host
- Network Host
- VMWare vSphere Host
- VMWare vSphere VM
- Xen Host

### Need to Know What a "Platform" Is?

See Resources, Resource Types and Inventory Types for more information.

### Add a Platform to Inventory from the Hyperic User Interface

1. Click **New Platform** on either:
   - The Dashboard’s **Summary Counts** portlet
   - The **Tools** menu on the **Browse > Resources**.

2. On the **New Platform** page, enter:
   - **Name** — The name of the platform
   - **Description** — (optional) A description of the platform
   - **Location** — (optional) The physical location of the platform hardware
   - **Platform Type** — Select the platform type from the list. Once you create the platform, you cannot change its type.
   - **Fully Qualified Domain Name** — The platform’s FQDN
- **Agent Connection** — The IP address:port pair of the Agent the proxied connection to this platform should go through. When a platform is created manually (on this screen), the platform cannot or does not run an Agent itself, and therefore the Agent must connect to the platform via proxy. The list contains the IP address:port pairs from all the currently deployed Agents.
- **IP Address** — (optional)
- **MAC Address** — (optional)
- **Netmask** — At a minimum specify values for the loopback (local) IP address, and then additional sets of values for each network interface on the device.

3. Click **OK**.
   - The Inventory page for the new platform is displayed.
   - The platform's **Owner** defaults to the account that created the platform.

**Configure Platform for Monitoring**

After creating the new platform, you may need supply values for one or more configuration properties. See the resource's Inventory page for configuration options and requirements.

**Clone a Platform**

vFabric Hyperic's Clone Platform feature allows you to copy configuration properties for servers and manually created platform services from one platform to one or more other platforms.

**Note:** Manually created platform services are the types of platform services that cannot be auto-discovered - typically the types you configure to proxy metrics for network services and devices, such as "HTTP", "POP3", or "DNS" services.

Platform cloning is supported between platforms of the same type (for example, "Linux") that run the same version of the Hyperic Agent.

**How to Clone a Platform**

The Clone Platform page is available on the **Tools** menu when a platform is selected.

1. Navigate to the platform whose inventory resources you wish to clone.
2. Choose **Clone Platform** from the **Tools** menu.
3. On the Clone Platform page, the "Available clone targets" list shows platforms of the same type as the source platform. You can narrow the list by entering a string in the "Search resources" box.
4. Move desired target platforms from the "Available clone targets" list to the "Selected clone targets" list.
5. Click **Queue for Cloning**. Cloning occurs asynchronously. You can perform other functions in the user interface without waiting for the cloning process to complete.
What Cloning is Good For

Platform cloning makes it easy to replicate configuration properties for resources of the same type. For instance,

- You have a dozen Linux platforms, each running Tomcat 6.0, JBoss 4.2, and MySQL 5.0. The Hyperic Agent is installed on each platform, and has auto-discovered the Tomcat, JBoss, and MySQL instances on each platform. You want to implement an identical log tracking configuration for servers of the same type on each of platforms. You edit the "Configuration Properties" on the Inventory page for the Tomcat, JBoss, and MySQL instances on one of the platforms. You can use Clone Platform to copy the configuration settings to the Tomcat, JBoss, and MySQL instances on the other 11 platforms.
- You are setting up multiple platforms to monitor network services or devices. To enable network monitoring, on each platform you need a properly configured platform service to serve as a proxy for each remote service or device. You can configure the platform services on one platform, and use Clone Platform to create platform services with the same configuration properties on each of the other platforms.

What Cloning Does

The cloning process can create new resources on the target platform or update an existing resource's configuration properties. The cloning process:

- Copies the configuration properties for each server on the source platform to corresponding servers of the same type on the target platforms. If there is not a corresponding server of the same type on a target platform, it is created, with the same configuration properties as the source server.
- Copies the configuration properties for each manually created platform service on the source platform to the target platforms - adding a new platform service to the target platform's inventory, or updating configuration properties of corresponding instances in the target platform inventory.
- Cloning occurs asynchronously, so you can perform other functions in the Hyperic user interface after initiating the process. The Event Center indicates the start and stop of the cloning process for the source platform.

What Cloning Doesn't Do

The cloning process:

- Does not update auto-discovered properties
- Does not create or update auto-discovered platform services, such as CPUs or File Server Mounts
- Does not create or update services that comprise the cloned servers; the child services will be added to inventory on the target platform via auto-discovery.
Create a Platform Service

This section has general instructions for creating a service in Hyperic.

For information about creating a service using the HQApi see HQApi resource command.

When to Manually Create a Platform Service

There are two types of platform services in Hyperic:

- System services local to an operating system platform, such as CPUs, network interfaces, filesystems, and so on. Most local service are auto-discovered by the system plugin.
- Remote services that the Hyperic Agent monitors over the network, such as HTTP, FTP, DNS, and other services using a supported protocol. Because such services are monitored by a remote agent, they cannot be auto-discovered. For network services, you manually configure platform service on the platform running the Hyperic Agent that will monitor the service.

Create a Platform Service

1. Use Browse > Resources > Platforms to navigate to the platform to which you wish to add a service.
2. Select New Platform Service from the Tools menu.
3. On the New Platform Service page enter:
   - Name - A meaningful name for the service.
   - Description - (optional) A description of the service
   - Service Type - Select the desired service type from the pull-down list.
4. Click OK to create the new service.
   - The Inventory tab for the new service appears and prompts: "This resource has not been configured". Please set its Configuration Properties.
5. Click Configuration Properties in the prompt.
6. On the Configuration Properties page, enter values for the required configuration properties, which are prefixed with a red asterisk, and optional properties as appropriate. For information about the configuration properties for a service type, click the link in the Configuration Notes column for it in the following Configuration Instructions for Platform Services table.
Configuration Instructions for Platform Services

The table below lists all supported platform service types in Hyperic. The **Configuration Notes** column for a network service or another platform service type that require configuration has a link to a configuration properties reference for the service type. No configuration instructions are provided for auto-discovered platform services.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Configuration Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>The Hyperic Agent on a platform automatically discovers CPUs on the platform.</td>
<td>It is not necessary to manually configure CPU monitoring. For information about metrics available for a CPU, see <a href="#">CPU Service</a> in <em>vFabric Hyperic Resource Configuration and Metrics</em>.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Use to monitor a remote Dynamic Host Configuration Protocol server.</td>
<td>See <a href="#">DHCP Platform Service</a> in <em>vFabric Hyperic Resource Configuration and Metrics</em>.</td>
</tr>
<tr>
<td>DNS</td>
<td>Use to monitor a remote Domain Name System server.</td>
<td>See <a href="#">DNS Platform Service</a> in <em>vFabric Hyperic Resource Configuration and Metrics</em>.</td>
</tr>
<tr>
<td>FileServer File</td>
<td>Use to monitor a file.</td>
<td>See <a href="#">FileServer File Service</a> in <em>vFabric Hyperic Resource Configuration and Metrics</em>.</td>
</tr>
<tr>
<td>FileServer Mount</td>
<td>Use to monitor a filesystem mount point and associated disks and raid arrays.</td>
<td>See <a href="#">FileServer Mount Service</a> in <em>vFabric Hyperic Resource Configuration and Metrics</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The Hyperic Agent auto-discovers local mount points. You only need to explicitly configure a FileServer Mount service to monitor a remote network file system (NFS). Alternatively, you can install an Hyperic Agent on the system that hosts the NFS, in which case the NFS will be auto-discovered.</td>
<td></td>
</tr>
<tr>
<td>FileServer Directory Tree</td>
<td>Use to monitor a directory and the entire tree under that directory.</td>
<td>See <a href="#">FileServer Directory Tree Service</a> in <em>vFabric Hyperic Resource Configuration and Metrics</em>.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Use to monitor a particular URL.</td>
<td>See <a href="#">HTTP Platform Service</a> in <em>vFabric Hyperic Resource Configuration and Metrics</em>.</td>
</tr>
<tr>
<td>FTP</td>
<td>Use to monitor a remote File Transfer Protocol server.</td>
<td>See <a href="#">FTP Platform Service</a> in <em>vFabric Hyperic Resource Configuration and Metrics</em>.</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Configuration Notes</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InetAddress Ping</td>
<td>Use to ping a remote host for availability.</td>
<td>See InetAddress Ping Platform Service in vFabric Hyperic Resource Configuration and Metrics.</td>
</tr>
<tr>
<td>Multiprocess</td>
<td>Use to monitor multiple related processes. For example, to monitor the number of httpd processes running on Apache and the system resource they consume in aggregate.</td>
<td>See Multiprocess Service in vFabric Hyperic Resource Configuration and Metrics.</td>
</tr>
<tr>
<td>Note: Because the Hyperic Agent auto-discovers network interfaces, manual configuration of a NetworkServer Interface is rare.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>Use to monitor a remote Post Office Protocol 3 server. Configure along with an SMTP service to monitor incoming and outgoing email services.</td>
<td>See POP3 Platform Service in vFabric Hyperic Resource Configuration and Metrics.</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Configuration Notes</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Process</td>
<td>Use to monitor a process using a Hyperic SIGAR Process Table Query Language (PTQL) query. To configure, you supply the PTQL query in the form: Class.Attribute. operator=value For example, Pid.PidFile.eq=/var/run/sshd.pid</td>
<td>See Process Service in vFabric Hyperic Resource Configuration and Metrics.</td>
</tr>
<tr>
<td>RPC</td>
<td>Use to monitor a Remote Procedure Call service. <strong>Note:</strong> Not available on Windows platforms.</td>
<td>See RPC Platform Service in vFabric Hyperic Resource Configuration and Metrics.</td>
</tr>
<tr>
<td>Script</td>
<td>Used to configure Hyperic to periodically run a script that collects a system or application metric.</td>
<td>Script Service</td>
</tr>
<tr>
<td>SMTP</td>
<td>Use to monitor a remote Simple Mail Transfer Protocol server. Configure along with a POP3 service to monitor incoming and outgoing email services.</td>
<td>See SMTP Platform Service in vFabric Hyperic Resource Configuration and Metrics.</td>
</tr>
<tr>
<td>SSH</td>
<td>Use to monitor a remote SSH service.</td>
<td>See SSH Platform Service in vFabric Hyperic Resource Configuration and Metrics.</td>
</tr>
<tr>
<td>TCP Socket</td>
<td>Use to monitor the availability of a remote TCP socket</td>
<td>See TCP Socket Platform Service in vFabric Hyperic Resource Configuration and Metrics.</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Configuration Notes</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows Service</td>
<td>Use to monitor an application that runs as a service under Windows.</td>
<td>To configure it, you supply its Service Name in Windows. To determine the Service Name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select Run from the Windows Start menu.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Type services.msc in the run dialog and click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. In the list of services displayed, right-click the service you wish to monitor and choose Properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Locate the Service Name on the General tab. See Windows Service Service.</td>
</tr>
</tbody>
</table>

Create a Server

This section has general instructions for creating a platform in Hyperic.

**Note:** For information about creating a server using the HQApi see HQApi resource command in Web Services API.

When to Create a Server Manually

Most server types that Hyperic manages are auto-discovered, rather than manually added to inventory on the New Server page.

You may need to create a server manually under some circumstances, for instance, if:

- The plugin that manages the server does not support auto-discovery of server instances.
- The auto-discovery method used by the plugin failed, because the entry it looked for in the process table or Windows registry was not found. For example, the server’s name in the process list is different than the plugin uses to detect server instances.

Create a Server

1. Use Browse > Resources > Platforms to navigate to the platform to which you wish to add a server.
2. Select New Server from the Tools menu.
3. On the New Server page enter:
   - **Name**---The name of the server
   - **Description**---(optional) A description of the server
   - **Server Type**---Select the server type for the new resource.
   - **Install Path**---If there are other servers of the type you are creating on the current platform, make sure that the installation path you define for the new server instance is unique, and not the same as any of the other servers of the same type. For autodiscovered servers, the plugin sets the value of the Install Path property, and uses it as the basis for the resource’s autoinventory identifier.
Note that if you create a server manually, you must specify the **Install Path** property, but it need not be the actual installation path for the server. The only requirement is that all servers of the same resource type on the same platform have unique **Install Path** property values.

4. Click **OK**.

The **Inventory** tab for the resource appears. See **Inventory Page for a New Server** for more information.

**Inventory Page for a New Server**

The Inventory page for a server that is newly added to inventory. It contains these sections:

- **General Properties**---The server's **Owner** is the username for the Hyperic account that created the server.
- **Type and Host Properties**---The **Host Platform** is the name of the platform to which you added the server.
- **Services**---This section of the page lists services discovered in the server instance. For an new server instance, no services appear until any required configuration properties are defined. You can manually add services to a server, but it is uncommon.
- **Groups Containing this Resource**---Click **Add to List** in this section if you wish to assign the server to one or more resource groups.
- **Configuration Properties**---The properties in the section vary, depending on the resource type of the server you are created.
  - **Shared** For some server types, you need to supply resource connection or authorization credential data in this section in order to monitor and manage the resource.
  - **Monitoring**---If the server type supports log or configuration tracking, you can configure tracking options in this section.
  - **Control**---If the server type supports control actions, you configure associated options in this section.

**Configure Server for Monitoring**

After creating the new server, you may need supply values for one or more configuration properties. See the resource's Inventory page for configuration options and requirements.

**Create a Service**

This section has general instructions for creating a service in Hyperic.

For information about creating a service using the HQApi see **HQApi resource command** in **Web Services API**.

**When to Create a Service Manually**

In Hyperic, a **service** is a component that runs in a server (for example, an EJB), or is associated with an operating system (for example, a CPU). System-level service, and services that an agent will manage remotely are referred to as **platform services**.
Most service types are auto-discovered by the plugin that manages that service type. Services that run on a platform are discovered along with the platform itself by the Hyperic's system plugin. Services that run in a local server are auto-discovered by the plugin that manages the host server — for example, the plugin that manages Tomcat discovers the services running in Tomcat.

The only service types in Hyperic that are routinely created explicitly are remote platform services. For information about creating and configuring remote services, see Create a Platform Service.

Add a Service to Inventory from the Hyperic User Interface

1. Use Browse > Resources > Server to navigate to the server to which you wish to add a service.
2. Select New Service from the Tools menu.
3. On the New Service page enter:
   - Name — The name of the service.
   - Description — (optional) A description of the service
   - Server Type — The service type.
   - Host Server — Contains the name of the server upon which you are creating the service.
4. Click OK.

The server's Owner defaults to the account that created the service.

Remove Resources from Hyperic Inventory

Delete a Resource Manually

To delete a resource from the Hyperic inventory:

1. Use Browse > Resources to navigate to the resource you wish to delete.
2. Select the Delete ResourceType option from the Tools menu.

Monitoring ceases and the resource is removed from Hyperic inventory. Note that if the resource has child resources, those children (and their children, as applicable) will be removed as well.

Resources you delete will disappear from the resource list immediately. Removal of the resources from the Hyperic database occurs asynchronously; there may be a slight delay before resources are removed from the database. If you restart agent prior to the resource is removed from the database, errors might occur if you re-add the resource to memory after the agent redisCOVERs it.

Do not try to re-import a platform immediately after deleting it — this may fail. Note also that until the delete process running in background completes, a deleted platform will still appear in the Hyperic Health’s Agent tab. Similarly, the Hyperic license count displayed in the web user interface will not be decremented until the delete process is completed.
Delete Resources with HQApi

You can delete resources with the HQApi resource command, using the `delete` command option.
Plugin Deployment and Management

Key Hyperic Plugin Management Features

Hyperic product plugin management and deployment features ensure that all Hyperic Agents reporting the Hyperic Server run exactly the same product plugins as those deployed to the server. The key features are:

- **Plugin management interface** — **Plugin Manager** is a user interface for deployment-wide management of product plugins. You use the **Plugin Manager** to deploy and manage plugins on the Hyperic Server and Hyperic Agents that report to the server. For more information, see **About Plugin Manager** below.

- **Server-Agent Plugin Synchronization (SAPS)** — A Hyperic Agent and the Hyperic Server it reports to cooperate to ensure that the agent is running exactly the same set of plugins as the server. For more information, see **About Plugin Sync at Startup** below. SAPS is enabled by default, and can be disabled using the `server.pluginsync.enabled` property in the server's `ServerHome\conf\server.conf` file.

Version Requirements for Plugin Synchronization

The SAPS process will *not* synchronize plugins on agents of an earlier version than the Hyperic Server. The Hyperic Server can only synchronize plugins on agents running the same or later version. The **Plugin Manager** user interface indicates how many of the agents reporting to the server are in sync. If there are agents that are out-of-date, you can see which agents need upgrading.

Plugin Administration Tasks

If you run Hyperic with SAPS enabled, you can use **Plugin Manager** to administer plugins on up-to-date agents throughout your Hyperic deployment. The primary tasks you perform are:

- **Deploy and update custom plugins** — If you develop your own plugin, or customize a built-in plugin, use **Plugin Manager** to upload and deploy the new or modified plugin to the Hyperic Server and to all up-to-date agents in your deployment. Plugins you deploy with **Plugin Manager** are deployed to a directory external to the Hyperic Server’s installation directory, so that they are not overwritten by a server upgrade. For more information, see **Resource Plugin Deployment Directories** below.
- Remove plugins — For optimal Hyperic scalability, it is good practice reduce agent footprint by running only the plugins you use, and to remove a plugin if you have no resources of the types the plugin manages. You can remove one or more plugins from all up-to-date agents in your deployment with a single Plugin Manager command. (Prior to version 4.6, Hyperic releases did not provide a friendly mechanism for plugin removal; the suggested alternative was to configure each agent to include or exclude selected plugins, using the plugins.exclude or plugins.exclude agent properties. This method is still supported.)

Manual plugin deployment not supported
Prior to Hyperic 4.6, product plugins were manually deployed to agents and the Hyperic Server, separately, with no mechanism to determine or enforce consistency between the server and agents. In Hyperic 4.6 and later, manual plugin deployment is not supported — use Plugin Manager for all product plugin administration tasks.

Resource Plugin Deployment Directories

There are two product plugin deployment directories on the Hyperic Server:

- ServerHome/hq-engine/hq-server/webapps/ROOT/WEB_INF/hq-plugins/ — This is the deployment directory for the standard plugins packaged with Hyperic Server.
- user.dir/hq-plugins — When you deploy a custom plugin, or a customized version of a built-in plugin, Plugin Manager deploys it to the hq-plugins subdirectory of the current working directory of the Hyperic Server process. Custom plugins are deployed to a separate plugin directory, external to the server installation, so that they will not be overwritten when you upgrade the Hyperic Server. You can configure the server to store custom plugins in a different directory with the server.plugin.custom.dir property. For more information, see server.custom.plugin.dir.

On the Hyperic Agent all product plugins reside in the same directory — AgentHome/bundles/agent-x.y.z/pdk/plugins/ — which is where built-in plugins are installed, and where Plugin Manager deploys custom plugins, including customized versions of built-in plugins.

About Plugin Manager

Plugin Manager, available on the HQ Server Settings section of the Administration tab, is a user interface for deployment-wide management of product plugins. You can use the Plugin Manager to administer plugins on the Hyperic Server and on all up-to-date Hyperic Agents that report to the server.

Plugin Manager displays all plugins deployed to the Hyperic Server, and the status of each plugin on agents reporting to the server.
You can use **Plugin Manager** to upload new plugins, update existing plugins, and remove plugins. The changes you make are replicated on all up-to-date agents that report to the server. Note that plugins you upload must comply with plugin naming conventions, and may not be larger than 5 MB.

When you remove one or more plugins using **Plugin Manager**, all resources in inventory of types managed by the plugin are removed from inventory.

For information about using the **Plugin Manager**, see [Manage Plugins with the Plugin Manager](#).

**About Custom Plugin Deployment with Plugin Manager**

When you upload a new or updated plugin with the **Plugin Manager**:

1. The plugin is copied to the Hyperic Server's `user.dir/hq-plugins` directory.
2. If a product plugin of the same name exists in the server's `hq-plugins` directory (likely to be the case if you are deploying a customized version of a built-in plugin), the version in `user.dir/hq-plugins` henceforth is loaded, rather than the version in the server's `hq-plugins` directory (`ServerHome/hq-engine/hq-server/webapps/ROOT/WEB-INF/hq-plugins`).
3. The Hyperic Server updates and restarts each up-to-date agent. Note that agent update and agent restart are asynchronous — the server processes two queues: one of agents that still need the update pushed, and one of those that have the update and need to be restarted.
   - The server pushes the new or changed plugins to all up-to-date agents, up to four at a time. A built-in throttle mechanism limits the number of agent update threads.
   - The server issues a restart command to each updated agent, up to 20 in parallel. A built-in throttle mechanism limits the number of agent restart threads.

**About Plugin Removal with Plugin Manager**

You can use the **Plugin Manager** to remove one or more plugins from the Hyperic Server and all up-to-date agents that report to the server.

When you remove a plugin:

1. The plugin is removed from its deployment directory on the Hyperic Server.
2. The plugin is removed from its deployment directory on each up-to-date Hyperic Agent reporting to the server, and each agent is restarted.
3. All resources in inventory managed by the removed plugin are removed from Hyperic's resource inventory.
About Plugin Sync at Startup

Server-side and agent-side plugins can become out-of-sync if you manually add or remove plugins and do not apply updates consistently to the server and to every agent.

To detect plugin mismatches caused by inconsistent manual deployment, the Hyperic Server checks for out-of-sync plugins every time it starts up, and every time an agent connects to it upon agent start or restart. (The Hyperic Server does the post-startup checks five minutes after startup, so that any agents that were restarted while the server was down to sync their plugin inventory.) In the case of a mismatch between server-side and agent-side plugins, the Hyperic Server updates the agent.

The synchronization behavior described in the sections below apply only to up-to-date agents, as noted in Version Requirements for Plugin Synchronization.

About Plugin Sync at Agent Startup

When an up-to-date agent starts up and loads the plugins in its plugin directory, it sends a plugin status report to the server, including the MD5 checksum of each plugin it loaded.

On receipt of a plugin status report from an up-to-date agent, the Hyperic Server compares the MD5 checksum of each plugin that the agent loaded with the MD5 checksum of the corresponding plugin (a plugin with the same name) currently deployed on the server.

For a mismatch:
- If the agent loaded a plugin with the same name but different MD5 checksum than one that is currently deployed to the Hyperic Server, the server pushes its version to the agent.
- If the agent did not load a plugin that is currently deployed to the server (the agent did not load a plugin with the same name as one that the server loaded), the server pushes the plugin to the agent.
- If the agent loaded a plugin that is not deployed to the Hyperic Server (there is no plugin with the same name on the server), the server removes the plugin from the agent.

After adding or removing agent plugins as necessary, the server restarts the agent.

About Plugin Sync at Server Startup

When the Hyperic Server starts up and loads the plugins in its deployment directories, it compares the MD5 checksum of the plugins it loaded with the MD5 checksums in the plugin status report last received from each agent.

For a mismatch:
- If an agent’s last plugin status report included a plugin with the same name but different MD5 checksum than one that is currently deployed to the Hyperic Server, the server pushes its version to the agent.
• If an agent’s last plugin status report does not include a plugin that is currently deployed to the server (the agent did not load a plugin with the same name as one that the server loaded), the server pushes the plugin to the agent.
• If an agent’s last plugin status report included a plugin that is not deployed to the Hyperic Server (there is no plugin with the same name on the server), the server removes the plugin from the agent.

After updating the agent plugins appropriately, the server restarts the agent.

**Disable Server-Agent Plugin Synchronization**

SAPS is enabled by default. To disable SAPS, add the following line to ServerHome/conf/hq-server.conf:

server.pluginsync.enabled=false