QUEST SOFTWARE®

Foglight® 5.5.8

User Guide

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:
Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com

Refer to our Web site for regional and international office information.

Patents

This product includes patent pending technology.

Trademarks

Quest, Quest Software, the Quest Software logo, Foglight, IntelliProfile, PerformaSure, Spotlight, StealthCollect, TOAD, Tag and Follow, Vintela Single Sign-on for Java, and vFoglight are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. For a complete list of Quest Software's trademarks, please see http://www.quest.com/legal/trademark-information.aspx. Other trademarks and registered trademarks are property of their respective owners.

Third Party Contributions

Foglight contains some third party components. For a complete list, see the License Credits page in Foglight online help.

User Guide
November 2010
Version 5.5.8

Table of Contents

Introduction to this Guide

The *Foglight User Guide* helps you monitor your enterprise from a variety of perspectives using the Alarms, Domains, Service Operations Console, and Hosts dashboards. It presents workflows for drilling down and investigating problems in your monitored environment using these dashboards.

This guide also introduces you to navigating the Foglight browser interface and using reports to share data from Foglight with others in your organization.

This guide is intended for users who have been assigned the Operator or Advanced Operator role and who need to perform tasks such as monitoring their environment, working with alarms, and creating reports.

Note This guide uses terminology that is specific to the Foglight browser interface. For more information about these terms, see the *Foglight User Help* (navigate to **Help > Help Contents > Using Foglight > Foglight User Help > Getting Started with Foglight > Working with Dashboards** in the action panel and then click **Working with Dashboards**).

About Quest Software, Inc.

Quest Software simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest go to *www.quest.com*.

Contacting Quest Software

Email	*info@quest.com*
Mail	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	*www.quest.com*

Refer to our web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to SupportLink, our self-service portal. Visit SupportLink at *http://support.quest.com*.

From SupportLink, you can do the following:

- Retrieve thousands of solutions from our online Knowledgebase
- Download the latest releases and service packs
- Create, update and review Support cases

View the *Global Support Guide* for a detailed explanation of support programs, online services, contact information, policies and procedures. The guide is available at: *http://support.quest.com*.

1

Getting Started with Foglight

This chapter provides instructions for logging in to Foglight and describes the Welcome page you see when you log in with the Operator or Advanced Operator role. It also introduces you to navigating the Foglight browser interface and discusses best practices for navigation.

Note Your administrator may have configured Foglight so that the actual displays are different from those described in this chapter. The following information is intended as a general guide.

Perform these steps before following the instructions in this chapter:

- Obtain your Foglight user name and password from your administrator.
- Ensure that your Web browser has JavaScript functionality enabled.

Logging in to Foglight

This section describes how to log in to the Foglight browser interface.

To log in to Foglight:

1. Open a Web browser instance.

   Note For a list of browsers supported by Foglight, see the *System Requirements and Platform Support Guide*.

2. Navigate to a URL that uses the following syntax:

   ```
   http://localhost:8080/
   ```

   where *localhost* is the name of the machine that has a running instance of the Foglight Management Server.

   The Foglight login page appears.

3 Enter your user name and password in the login page.

This guide assumes that you are a user with the Operator or Advanced Operator role, in which case the Welcome to Foglight page is the first dashboard you see when you log in to Foglight.

Note The appearance of the Welcome page and the range of dashboards you can access from this page vary depending on your user role. If you have Administrator-level permissions, you can access advanced dashboards and configuration workflows. See the *Foglight Administration and Configuration Guide*. Users with the Operator role (but not the Administrator role) have permission to access a smaller set of dashboards.

If you have the Cartridge Developer role only (and do not have the Administrator or Operator role), your home page is the Getting Started page instead of the Welcome to Foglight page.

Starting from the Welcome Page

An Operator’s welcome page lists the following commonly-performed tasks:

- **View, Acknowledge, and Clear Recent Alarms**: View the state of all alarms across the entire Foglight installation in the Alarms dashboard so you can take immediate action on them. The alarm count by time is also shown, allowing you to identify alarm storms or outage events. This link takes you to the Alarms dashboard. Another way to access this dashboard is by choosing **Alarms** under **Homes** on the navigation panel. See “Viewing, Acknowledging, and Clearing Alarms” on page 15.
- **View Enterprise Health Organized by Monitoring Domain**: View an end-to-end, top-level summary of all domains in the Domains dashboard and drill down to view their managed instances. This link takes you to the Domains dashboard. Another way to access this dashboard is by choosing **Domains** under **Homes** on the navigation panel. See “Monitoring Your Domains” on page 23.
- **View the Health of Critical Services:** Choose a level of service as a focal point by subscribing to services of interest and viewing their dependencies. This link takes you to the Service Operations console. Another way to access this dashboard is by choosing **Services Operations Console** under **Homes** on the navigation panel. For more information, see “Monitoring Your Services” on page 27.
- **View the Health of the Monitored Hosts in Your Enterprise:** View alarms and a high-level summary of performance on your monitored hosts. This link takes

you to the Hosts dashboard. Another way to access the Hosts dashboard is by choosing **Hosts** under **Homes** on the Navigation panel. For more information, see "Monitoring Your Hosts" on page 37.

- **Report on Your Enterprise:** View reports that are scheduled, run a report using a report template, create a custom report, schedule a report to run at a specific time, and manage reports. This link takes you to the Reports dashboard. Another way to access this dashboard is by choosing **Reports** under **Homes** on the navigation panel. For more information on reports, see "Reporting on Your Enterprise" on page 43.
- **Tap into the Foglight Community:** Takes you to the *foglight.org* Web site, which discusses topics related to Application Management and Foglight.

The Welcome to Foglight page is your default home page. For instructions on changing your home page to a dashboard of your choice, see "Choosing a Home Page" on page 12.

Working with Dashboards

For information about how to work with Foglight dashboards and a description of the common elements that are found on most dashboards, see the *Foglight User Help* (navigate to **Help** > **Help Contents** > **Using Foglight** > **Foglight User Help** > **Getting Started with Foglight** > **Working with Dashboards** in the action panel and then click **Working with Dashboards**).

Navigating Foglight

In addition to the links on the Welcome page, use the navigational aids described in the sections below to navigate Foglight.

Note Foglight displays dynamic data that is updated regularly. For this reason, avoid using your browser's navigation buttons, as this may display cached views or result in an error message. Use the links in the navigation panel and display area instead.

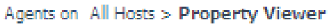
Using the Navigation Panel

Use the left-hand navigation panel to move between dashboards. This panel lists all dashboards that are available to you based on your roles. Expand a module and select a dashboard to view it in the display area (for example, **Dashboards > Services > Service Levels**).

Foglight remembers the state of the navigation panel between logins, so if you collapse the navigation panel when you log out, it is collapsed the next time you log in.

Using the Breadcrumb Trail

The name of the current dashboard is displayed in bold at the top of the dashboard, at the end of a path called the breadcrumb trail:



Agents on All Hosts > **Property Viewer**

When you move directly from one dashboard to another, the names of the previous dashboards are displayed in a breadcrumb trail.

Use the links in the breadcrumb trail to return to previously-viewed dashboards in a workflow or series of drilldowns.

Using Drilldowns

Use the graphical and text links in views to drill down to additional details that help you diagnose problems. Depending on the link, you drill down to a different dashboard or a smaller view called a popup that appears above the dashboard you are currently viewing.

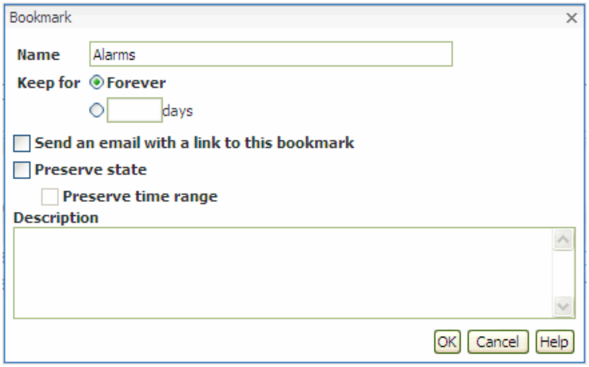
You can drill down from many different parts of a view, including names of monitored components (such as hosts or services), the Explore links in a popup, and items like charts, tables, cylinders, and icons.

For example, in the Service Operations Console, click the icon in the Host tier column that indicates that the tier is in a fatal state (). An Outstanding Alarm(s) popup appears that lists the hosts in the tier. Drill down further into a host's health or alarms to diagnose problems.

Using Bookmarks

Use bookmarks to keep track of dashboards and views that you want to revisit or access quickly, without having to drill down several levels. A bookmark can be a snapshot of data that is “frozen” at a specific point in time, or it can be updated with current data when you access it. For example, you could create a bookmark to quickly access the System Overview on a particular host from last Wednesday.

You create a bookmark by navigating to the dashboard you want to bookmark, selecting **Bookmark** from the action panel, and then selecting options from the Bookmark dialog. See the online help for the Bookmark dialog for details.



Bookmark

Name: Alarms

Keep for: ● Forever
○ days

□ Send an email with a link to this bookmark

□ Preserve state

□ Preserve time range

Description

The bookmarks you create are listed in the Bookmarks section of the navigation panel. When you select a bookmark, it appears in the display area.

To email a link to a bookmark:

1. In the Bookmarks area of the navigation panel, select a bookmark to display it.
2. Select **Email** from the action panel.

   An email window opens, containing a link to the bookmark.
3. Fill in the required information and click **Send**.

To delete a bookmark in the navigation panel:

1. Place the cursor over the dimmed delete icon beside the name of the bookmark.

   The icon turns red: ⛔.
2. Click the delete icon.
3. On the confirmation dialog, click **Delete** to delete the bookmark.

Opening a New Window

Opening a new window instead of using the current browser is useful, for example, when you want to open a link or print a document, such as a PDF. When you use a new window, the document downloads or prints in the background and you are prevented from accidentally closing the browser window when closing the PDF.

To open a new window:

1. Click the **New Window** link in the action panel to open a new browser window and change the URL to create a sub-session.
2. Navigate and click on the sub-session tab to reload the new browser window or tab independently of the source session.

Choosing a Home Page

You can choose any dashboard and make it your personal home page. Other dashboards can also be designated as home pages by a dashboard developer. These are listed under Homes in the navigation panel.

To set your personal home page:

1. Select any dashboard in the navigation panel on the left. Choose the dashboard that is most appropriate for your needs.
2. Click **Make this my home page** in the actions panel.

   The dashboard is listed under **Homes** in the navigation panel and will be the first page that Foglight displays every time you log in.

If you later choose another dashboard as your home page, it replaces the previous one.

Note You can have multiple homes. When you mark something as a home page, it becomes the default home and it is added to the list of possible homes. For example, if you add the Service Operations Console as your home page, Foglight adds it to the your default set of homes and it becomes your current home. If you log out and log back in, you will access the Service Operations Console.

Getting Started FAQ

When I log into Foglight, why I do not see any dashboards in the navigation panel?

Foglight controls access to dashboards and views by means of roles. Your Foglight administrator assigns users to groups and then assigns roles to those groups.

If you do not see any dashboards in the navigation panel, the user you signed in as may not have been assigned to a group. Contact your Foglight administrator for assistance.

What determines which dashboards and views I can access?

When you try to access a dashboard or view, Foglight matches the roles of the groups to which you belong against the relevant roles and the allowed roles that were set for that dashboard or view.

Relevant roles control which dashboards and views are listed in the navigation and action panels. Allowed roles control which dashboards and views a group can access. In some dashboards, one or more views may not be available because your roles have not been set as allowed roles for them.

The Operator and Advanced Operator roles have the following permissions:

This role:	Has these permissions:
Operator	Access to basic dashboards. Operators can also access dashboards like Services, Agents, and Hosts.
Advanced Operator	Extends Operator to include dashboards like the Service Builder.

If I navigate away from a dashboard, do I see the same views when I return?

Yes. If you leave a dashboard and then return to it, you see the last views that were displayed.

2

Viewing, Acknowledging, and Clearing Alarms

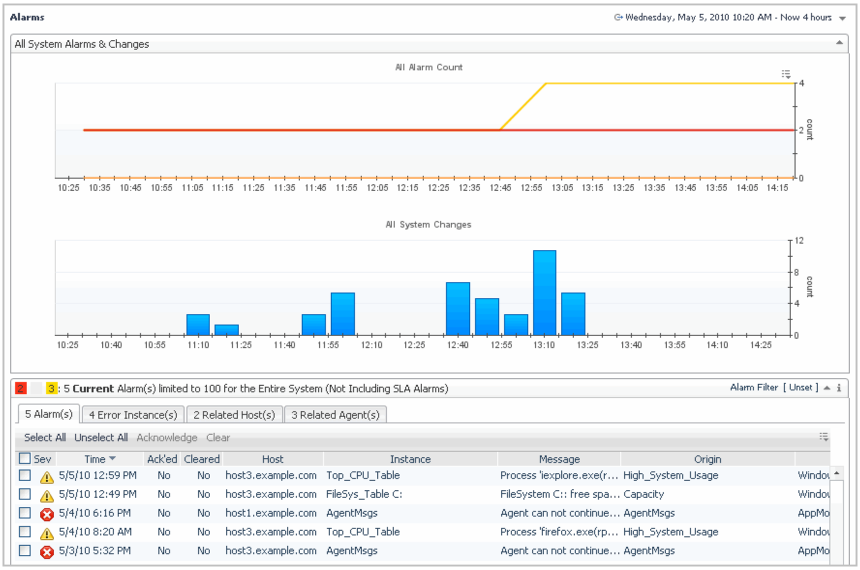
Alarms are triggered by problems in your monitored environment. Foglight fires alarms when a rule determines that certain pre-defined conditions are met.

Use the Alarms dashboard to view the state of alarms across your monitored environment and take immediate action on them. The Alarms dashboard shows alarm counts by time, allowing you to identify alarm storms or outage events.

Note This chapter discusses managing alarms from the Alarms dashboard, but alarm lists appear in many places in Foglight — for example, at the bottom of the Service Operations Console or in the popup that appears when you click an alarm in the Domains dashboard. You can view details about, acknowledge, or clear alarms in these alarm lists by following essentially the same steps described in this chapter.

Access the Alarms dashboard from the Welcome page (**Homes** > **Main**) by clicking **View, Acknowledge, and Clear Recent Alarms**.

Tip You can also access this dashboard from the navigation panel: select **Homes > Alarms**.



Alarms

Wednesday, May 5, 2010 10:20 AM - Now 4 hours

All System Alarms & Changes

2 3: 5 **Current** Alarm(s) limited to 100 for the Entire System (Not Including SLA Alarms)

Alarm Filter [Unset]

5 Alarm(s) | 4 Error Instance(s) | 2 Related Host(s) | 3 Related Agent(s)

Select All Unselect All Acknowledge Clear

□	Sev	Time	Ack'ed	Cleared	Host	Instance	Message	Origin	
□	⚠	5/5/10 12:59 PM	No	No	host3.example.com	Top_CPU_Table	Process 'iexplore.exe(r…	High_System_Usage	Windo
□	⚠	5/5/10 12:49 PM	No	No	host3.example.com	FileSys_Table C:	FileSystem C:: free spa…	Capacity	Windo
□	⊗	5/4/10 6:16 PM	No	No	host1.example.com	AgentMsgs	Agent can not continue…	AgentMsgs	AppMo
□	⚠	5/4/10 8:20 AM	No	No	host3.example.com	Top_CPU_Table	Process 'firefox.exe(rp…	High_System_Usage	Windo
□	⊗	5/3/10 5:32 PM	No	No	host3.example.com	AgentMsgs	Agent can not continue…	AgentMsgs	AppMo

The Alarms dashboard displays data for the selected time range in two different views, which are described below. The time range is shown at the top right of the dashboard; for information about changing or freezing the time range, see the *Foglight User Help* (navigate to **Help** > **Help Contents** > **Using Foglight** > **Foglight User Help** > **Getting Started with Foglight** > **Working with Dashboards** in the action panel and then click **Working with Dashboards** > **Zonar and Time Range** > **Time Range**).

All System Alarms and Changes

This view contains charts that summarize the alarm and change activity for the current time range. Hover over a line or bar in a chart to cause a tooltip to appear that lists the number of alarms or changes that occurred nearest to that time. The alarm count in this view includes SLA (Service Level Agreement) alarms.

Alarm(s) for the Entire System

This view lists up to 5000 alarms for the current or historical time range. It does not list SLA alarms. You can filter the list, sort it by column, or acknowledge and clear alarms.

The totals for each severity of alarm (Warning, Critical, or Fatal) and the total number of alarms are listed in the view’s title. The alarms list also shows cleared alarms and indicates whether an alarm has been acknowledged or cleared. Cleared alarms appear dimmed and can be filtered out using the Alarm Filter dialog (click **Alarm Filter** in the right corner of the table).

To see more detailed information about an alarm, hover over or click a column to display a dwell or a popup. You can select an alarm and investigate, acknowledge, or clear it.

The alarm list view allows you to select different perspectives on alarms. This chapter discusses using the Alarm(s) tab. For information about using the other tabs, see the *Foglight User Help* (navigate to **Help > Help Contents > Using Foglight > Foglight User Help > Getting Started with Foglight > Working with Dashboards** in the action panel and then click **Working with Dashboards > Common Views > Alarm List**).

Viewing Alarms

This section discusses viewing alarms in more detail.

Filtering the Alarm List

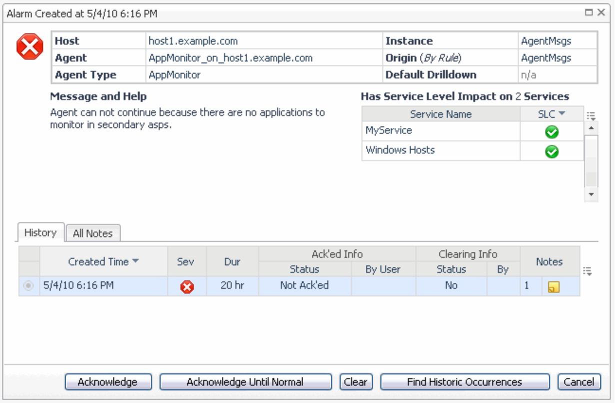
You can filter the list by different criteria by clicking **Alarm Filter** in the top-right corner of the view and changing the settings in the Alarm Filter dialog box.

For example, you can filter the list of alarms to show only **Current** or **Historical** alarms. Selecting **Current** shows all outstanding alarms, regardless of when they are fired. This is essentially the current outstanding set of alarms that need to be addressed. Use **Current** if you want to see what is immediately noteworthy. In contrast to **Current**, **Historical** shows all alarms that fired during a certain interval, regardless of whether they are active or cleared. Use **Historical** if you want to see what is happening in your monitored environment during a specific time range.

In the Alarm Filter dialog box, you can also set the maximum number of results to display in the table.

Viewing Alarm Details

To view details about an alarm, click its severity icon in the Alarm(s) list. Doing so displays information about that alarm in the Alarm Details dialog box:



Alarm Created at 5/4/10 6:16 PM

Host	host1.example.com	**Instance**	AgentMsgs
Agent	AppMonitor_on_host1.example.com	**Origin** (*By Rule*)	AgentMsgs
Agent Type	AppMonitor	**Default Drilldown**	n/a

Message and Help

Agent can not continue because there are no applications to monitor in secondary asps.

Has Service Level Impact on 2 Services

Service Name	SLC
MyService	✓
Windows Hosts	✓

History | All Notes

	Created Time	Sev	Dur	Ack'ed Info		Clearing Info		Notes	
				Status	By User	Status	By		
○	5/4/10 6:16 PM	☒	20 hr	Not Ack'ed		No		1	▨

This dialog box shows the alarm's service level impact and its full history. The history includes all consecutive alarms fired by the same rule on the same instance regardless of the dashboard's time range. Consecutive alarm firings are instances where an alarm fires, is cleared (the alarm condition no longer exists), and then fires again.

The Alarm Details dialog box also illustrates how the alarm has changed severity in the current alarm chain. See the *Foglight User Help* (navigate to **Help > Help Contents > Using Foglight > Foglight User Help > Getting Started with Foglight > Working with Dashboards** in the action panel and then click **Working with Dashboards > Common Views > Alarm List > Alarm Chaining**).

You can also drill down from this dialog box to investigate the alarm in more detail. For example, click on the icon in the Service Level Impact table for information about the service whose Service Level Agreement is affected by the alarm. Performing impact analysis on an alarm helps you to determine the priority for fixing the problem that caused the alarm to fire.

Investigating the Alarm Source

The Instance field in the Alarm Details dialog box lists the object in your monitored environment that is the source of the alarm. Click the listing for an alarm source to display its health summary. The health summary shows the number of alarms by severity and the health of the alarm source and lists the agents and host associated with the alarm source.

In addition, it provides a list of related views that show quick drilldowns to help identify the root cause. This list is based on the views that match the type of the alarm source. If no related views are available, then the default views (for example, Data Browser) are provided.

Adding Alarm Notes

Using alarm notes is a handy way to record information about an alarm for other users to view. For example, if an urgent alarm comes up that you want to investigate, you can add a note to the alarm that you are checking if a certain process is causing the problem. The note is attached to the alarm along with your user name and a timestamp.

You can view, filter, add, and edit alarm notes from the Alarm Details dialog box. Use the **History** tab to attach notes to a particular alarm in the history table. Use the **All Notes** tab to attach a note to the most recent alarm in the alarm history. For more information, see the *Foglight User Help* (navigate to **Help** > **Help Contents** > **Using Foglight** > **Foglight User Help** > **Getting Started with Foglight** > **Working with Dashboards** in the action panel and then click **Working with Dashboards** > **Common Views** > **Alarm List** > **Alarm Notes**).

Acknowledging an Alarm

The Ack'ed column displays No for any alarms that have not been acknowledged. Once an alarm has been acknowledged, this setting cannot be changed.

If you have the Advanced Operator role, you can acknowledge alarms. To acknowledge multiple alarms at once, follow the instructions in "To acknowledge one or more alarms:" on page 19. To cause alarms to remain acknowledged until the monitored object returns to a normal state, follow the instructions in "To acknowledge an alarm until the alarm source returns to a normal state:" on page 20.

Tip Choose Acknowledge Until Normal if, for example, a series of alarms is due to a known situation. Anyone looking at the Alarms dashboard will know that this known problem has been acknowledged.

To acknowledge one or more alarms:

1. Use the Alarm Filter to apply a filter on current or historical alarms.
2. In the Alarm(s) list, select the alarms that you want to acknowledge.
3. Click **Acknowledge** at the top of the table.

   The current alarms are acknowledged and Yes is listed in the Ack'ed column for them. If the alarms fire again at a later time (usually because the condition has recurred), they appear in the list as unacknowledged.

4. Hover the cursor over Yes in the Ack'ed column.

A dwell appears that lists the alarm as acknowledged as well as your user name, and the time and date when you acknowledged the alarm. Foglight also stores this information in an audit report.

To acknowledge an alarm until the alarm source returns to a normal state:

1. Use the Alarm Filter to apply a filter on current or historical alarms.
2. In the Alarm(s) list, click **No** in the row for the alarm.

   The Alarm Details dialog box appears.
3. Click **Acknowledge Until Normal.**

   Note This option is available for an outstanding (not-yet-cleared) alarm only.

   The current alarm and all consecutive alarms fired by the same rule on the same object remain acknowledged until the first alarm fired after the alarm source returns to a normal state. Ack'ed til Normal and your user name appear in the Ack'ed Info column.
4. Close the dialog box.

   In the Alarm(s) list, Foglight displays Yes in the Ack'ed column for the alarm.

Clearing an Alarm

In most cases, Foglight clears alarms when the condition that triggered them changes. For example, an alarm fires when the CPU usage metric for a monitored host exceeds a certain threshold. If the metric's value drops below this threshold, Foglight clears the original alarm. If the alarm condition occurs again, the alarm reappears.

If you have the Advanced Operator role, you can also manually clear alarms. However, you should only do so when alarms do not clear themselves — for example, for log messages or one-time events that generate alarms.

The Cleared column in the Alarm(s) list indicates whether an alarm has been cleared or not. In addition, cleared alarms appear dimmed.

To clear one or more alarms:

1. Use the Alarm Filter to apply a filter on current or historical alarms.
2. In the Alarm(s) list, select one or more alarms that you want to clear.
3. Click **Clear** at the top of the table.

If you are filtering the list on current alarms, the alarms are removed from the list. If you are filtering the list on historical alarms, the alarms appear dimmed and Yes is listed in the Cleared column for them.

Alternatively, you can clear an alarm from the Alarms Details dialog box. It appears dimmed in the dialog box when you have done so. If you are filtering the Alarm(s) list to show current alarms, the alarm is also removed from the list.

3

Monitoring Your Domains

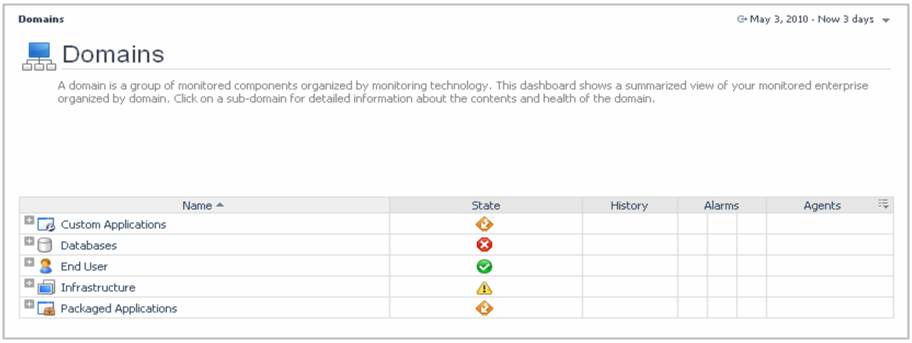
In Foglight, domains are monitored components grouped together by a common technology. For example, operating systems are grouped together in the Infrastructure domain and application servers are part of the Custom Applications domain. Domains represent parts of your environment that you are interested in monitoring.

Each technology type is considered a subdomain. For example, each type of operating system in the Infrastructure domain is a subdomain.

Use the Domains dashboard to monitor your environment if you are a domain administrator or simply prefer to think of your environment in terms of domain groups. This dashboard allows you to obtain a high-level view of the state of your monitored domains and investigate problems in a particular domain. It also shows you what domains you are not monitoring, but could be.

Access the Domains dashboard from the Welcome page by clicking **Homes** > **Main** >**View Enterprise Health Organized by Monitoring Domain**.

Tip You can also access the Domains dashboard from the navigation panel: select **Homes > Domains** or **Dashboards > Services > Domains**.



Domains

May 3, 2010 - Now 3 days

Domains

A domain is a group of monitored components organized by monitoring technology. This dashboard shows a summarized view of your monitored enterprise organized by domain. Click on a sub-domain for detailed information about the contents and health of the domain.

Name ▲	State	History	Alarms	Agents
⊞ Custom Applications	◆			
⊞ Databases	✖			
⊞ End User	✓			
⊞ Infrastructure	⚠			
⊞ Packaged Applications	◆			

Viewing Details About a Domain or Subdomain

Drill down on a domain name to view a high-level summary of its monitored components. For example, click **Infrastructure** to view all monitored virtual and physical hosts in the Hosts dashboard.

By default, the Domains dashboard shows only top-level domains. Expand a domain node to view its subdomains.

Each monitored subdomain comprises the actual instances of that technology type in your environment. Click a subdomain name to drill down to details about it. For example, click **Linux** to navigate to the list of Linux hosts or click **Oracle** to drill down to the Oracle Global View.

Investigating Problems in a Domain

Use the Domains dashboard to monitor for problems in your domains — for example, to see if a domain is in a Critical state, or if any alarms have been fired for its components — and take action on them.

Investigating a Domain or Subdomain’s State

By default, a domain or subdomain reflects the current worst state (normal, warning, critical, or fatal) of its components.

Click the **State** icon to investigate the state of a domain or subdomain that is displaying a warning, critical, or fatal icon.

A popup appears that lists the domain or subdomain’s alarm sources (for example, hosts, application servers, or databases) and their health. These are the components that contributed to the domain or subdomain’s state.

Depending on the problem you are investigating, do one of the following to drill down to more detailed views:

- Click an alarm source to drill down and see more details about it.
- Drill down to views that display the health of all alarm sources.
- Drill down to view the health of the current object (for example, Infrastructure domain or the Linux subdomain).
- Drill down to view all outstanding alarms for the domain or subdomain.

Investigating a Subdomain’s Health

Foglight displays each monitored subdomain’s recent health in the History column. This column summarizes the subdomain’s health for the dashboard’s time range.

The colored segments in the column represent the subdomain’s alarm severity state at different intervals within the time range. Yellow segments represent warning alarms, orange segments represent critical alarms, and red segments represent fatal alarms. Green segments represent intervals without alarms.

To investigate the health history:

1. Hover the cursor over a segment in the health history bar to display a popup with a list of related alarms that occurred during that interval.
2. Click the health history bar.

   A more detailed Health History view appears.
3. Click and drag the timeline to zoom in on an interval in the bar.

   The chart zooms in on the selected time range.

   Tip After zooming in, hover the cursor over the bar to cause the zoom menu to appear. To restore the previous time range used by the bar, click the Previous Zoom icon ( ). To restore the bar’s timeline to its initial state, click the Restore Zoom icon ( ). To freeze the dashboard’s time range at the same interval spanned by the bar’s zoomed-in range, click the Update page with zoomed time range icon ( ).

4. Click a red, orange, or yellow segment in the detailed health history bar to find alarms that are causing the host to be in a non-normal state during that interval.

   A popup with details about the alarms that fired during that interval appears. See "Viewing, Acknowledging, and Clearing Alarms" on page 15 for more information about working with alarms.

Investigating a Subdomain's Alarms

The counts in the Alarms column represent the total number of alarms fired for the components in a subdomain; for example, for all monitored virtual hosts in the **Infrastructure > VMWare** subdomain.

Use this column to view the number and type of alarms fired for these components during the dashboard's current time range.

Click an alarm to display a popup that contains the standard alarm list. See "Viewing, Acknowledging, and Clearing Alarms" on page 15 for more information about working with alarms.

Investigating Problems with a Subdomain's Agents

You can view the state of the agents related to a subdomain in the Agents column.

Click a warning, critical, or fatal state icon to display a list of agents with health problems or drill down to the Agents dashboard. For more information, see the online help for the Agents dashboard.

4

Monitoring Your Services

In Foglight, a service is any component or group of components that you want to monitor. If you have the Advanced Operator role, you create services in the Service Builder dashboard that reflect the components in your monitored environment that are meaningful or interesting to your organization.

Examples of services include:

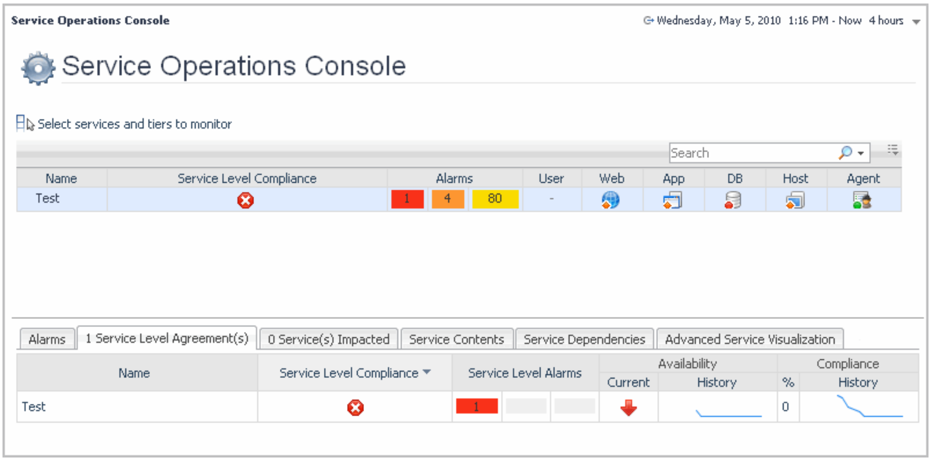
- An application, including its Web servers, application servers, and databases.
- A collection of related systems, such as all Windows machines in your monitored environment.
- A business process, such as retail banking.

Each service can include any component in your monitored environment, including other services. A service inherently has a service level and relationships of impact and dependency to other services.

The Service Operations Console is the best way to monitor a selected set of services. Use it to tailor the way Foglight presents information about monitored components so that it suits your specific needs.

Access the Service Operations Console from the Welcome page (**Homes > Welcome**) by clicking **View the Health of Critical Services**.

Tip You can also access this dashboard from the navigation panel: select **Homes > Service Operations Console**.



Service Operations Console

Wednesday, May 5, 2010 1:16 PM - Now 4 hours

Service Operations Console

Select services and tiers to monitor

Search

Name	Service Level Compliance	Alarms			User	Web	App	DB	Host	Agent
Test	⊗	1	4	80	-					

Alarms | 1 Service Level Agreement(s) | 0 Service(s) Impacted | Service Contents | Service Dependencies | Advanced Service Visualization

Name	Service Level Compliance	Service Level Alarms			Availability		Compliance	
					Current	History	%	History
Test	⊗	1			▼		0	

Follow the instructions in this chapter to monitor a specific group of services that interests you by:

- Selecting these services.
- Displaying service breakdowns based on the tiers that are relevant to you.
- Drilling down to see more information about your services, such as the state of the monitored components within a tier and see the hosts that are related to it.
- Viewing details about your services, such as their state, contents, and dependencies.

Selecting the Services You Want to Monitor

By default, no services are listed in the Service Operations Console. This is by design: it gives you the opportunity to customize the Service Operations Console to suit your needs. Select the set of services that you want to monitor so that they appear in this dashboard.

To select services:

1 Click **Select services and tiers to monitor**.

The Select services and tiers to monitor dialog appears.

2 In the Service Selector tab, explicitly select each service you want to monitor (selecting a service does not automatically select its children).

Tip Use the search features to find services you are interested in. The search is per keyword, delimited by spaces. For example, if you want to search on “Global Service” (instead of “Global”), add quotes around “Global Service” to match that exact string.

3 Click **Apply**.

The Service Operations console displays only the services you selected.

4 In the Tier Selector tab, select the tiers that interest you. Foglight lists columns for these tiers in the Service Operations Console. For example, as a database administrator, you can hide the Web Tier column if it is not relevant to you.

Note Columns for the Host and Agent tiers are always shown by default.

5 Click **Apply**.

The Service Operations console displays only the tiers you selected for each service to which you subscribed.

Monitoring a Service

Once you subscribe to a service, you can view details about it and drill down on it.

These sections describes workflows for monitoring the overall health of your critical services and investigating problems with them.

Investigating Service Level Compliance and Availability

You monitor services because you have a specific business requirement to ensure the availability of these components. The icons in the Service Level Compliance column reflect the availability of your services. Use this column as a starting point for investigating how problems with your services affect their service levels.

Foglight automatically examines each service and establishes its availability and service level compliance. By default, a service is available if it does not have any fatal alarms.

In Foglight, a service’s state is based on the worst state of the components it includes. For example, a MyApplication service contains services for its Web servers, application servers, and databases. The databases service is in a fatal state because it has a fatal alarm and the other two are in a warning state. MyApplication is also in a fatal state and is listed as non-compliant with its Service Level Agreement (SLA).

To investigate a service's availability and service level compliance:

1. In the row for the service, click the Fatal icon in the Service Level Compliance column. This icon indicates that your service is not compliant with its SLA.

   A Service Level Compliance Summary popup appears for that service.

2. Use this dialog to view the service level agreements, compliance, current and recent availability, and any service level alarms that have been fired for that service.

3. If there is anything in the dialog that you want to investigate further, drill down on that aspect of service level compliance.

   For example, the Availability History sparkline displays dips that concern you. You want to investigate your service's availability for a specific interval you are concerned about, so you click **Explore > Service Level Agreement(s)** to navigate to the Service Levels dashboard. You then zoom in on one of the availability graphs in this dashboard. See the online help for the Service Levels dashboard for more information about it.

Tip Both current availability and SLA measurements are important; use them in different situations:

- Use the current availability measurement to find and address immediate problems quickly.
- Use SLA measurements to determine if you are meeting overall service level expectations.

Investigating Alarms

Investigate a service's alarms to get more details about the problems contributing to its non-normal state.

To investigate alarms related to a service:

- Click the icon that represents the service's warning, critical, or fatal alarms.

  An alarm list appears showing only those alarms. See "Viewing, Acknowledging, and Clearing Alarms" on page 15 for information about working with alarms.

Drilling Down into a Service

When you drill down into a service by clicking on its name, the view that appears depends on whether or not your Foglight administrator configured a custom view using the Service Builder. If your administrator did not configure a custom drill-down, you see a generic Service Breakdown link that flows according to what is stored in the service. If your administrator chose a custom view, it appears in the drill-down popup.

Viewing the State of and Drilling Down into a Tier

Use the tier icons to get an at-a-glance overview of each tier’s state. A tier’s state is the aggregate of its components’ state; it is a rollup of all alarms fired for components in that tier.

If one of your services’ tiers is in a warning, critical, or fatal state, hover the mouse over the icon to view information about the state and health of the components in that tier, alarms for that tier, and other tier-specific information.

Click an icon to view the same information in a popup that also allows you to drill down further to related views and dashboards. For example, you can investigate specific alarms or see metrics relevant to a particular component (such as CPU, memory, disk, and network metrics for a host).

Default Tiers

With the exception of the Host and Agent tiers, the default tiers in the Service Operations Console are similar to the domains you monitor. These tiers are described below.

Note Your Foglight administrator uses the Tier Definition dashboard to decide what tiers are relevant globally to users in your organization. The group of tiers you see in the Service Operations Console might be larger or smaller than the set described below.

User

The User tier icon displays the worst state of all components monitored by agents included in the EU (End User) cartridges.

Web

If your Foglight administrator assigns a service to the Web tier using the Service Builder dashboard, Foglight categorizes components as part of this tier. The Web tier icon displays the worst state of all components in the service.

App

The App tier icon displays the worst state of all components monitored by agents included in the cartridges for .NET, Siebel, SAP, PeopleSoft, Oracle eBusiness, and Java EE technologies.

Database

The Database tier icon displays the worst state of all components monitored by agents included in the cartridges for Oracle, SQL Server, Sybase and DB2.

Permanent Tiers

The Host and Agent tiers are always displayed in the Service Operations Console.

Host

The Host tier icon displays the worst state of all hosts that are part of that service. This set of hosts includes:

- All hosts your Foglight administrator added directly to the service.
- All hosts your Foglight administrator added to one of the services it contains (services nested in its hierarchy).
- All monitored host(s) related to the components your Foglight administrator added to this service.

Agent

The Agent tier icon displays the worst state of all the agents that are part of that service. This set of agents includes:

- All agents your Foglight administrator added directly to the service.
- All agents your Foglight administrator added to one of the services it contains (services nested in its hierarchy).
- Agents on all monitored host(s) that are related to the components your Foglight administrator added to the service.

Viewing More Details About Your Services

View more details about one of your services by selecting it and then clicking one of the tabs at the bottom of the dashboard.

Select the Tab...	To show...
Alarms	A list of alarms fired for components included in the selected service. The alarm count includes all filtered alarms fired on hosts that are part of the service. See “Viewing, Acknowledging, and Clearing Alarms” on page 15 for information about working with alarms.
Service Level Agreement(s)	A summary of the service level compliance, alarms, and availability. This summary also appears in the Service Levels dashboard. For more information, see “Investigating Service Level Compliance and Availability” on page 29 or the online help for the Service Levels dashboard.
Service(s) Impacted	The list of services that are impacted by the state of the current service. For more information, see “Understanding What Services are Impacted” on page 34.
Service Contents	The contents of a service without having to drill down into it. A service’s contents include all components added to the selected service and its child services, no matter how many levels deep they are nested.
Service Dependencies	The list of services on which the selected service depends. That is, the list of services added to the selected service. This diagram shows the composition of your service and the state of each component it contains. Use it to quickly scan for the root cause of a problem reported on the service. For details, see “Visualizing the Dependencies Among Services” on page 35.
Advanced Service Visualization	Advanced Service Visualization allows you to define relationships among services. A relationship can be visualized as a flow from one tier to another. This functionality is for advanced users. Consult your Foglight administrator if it is not configured.

Understanding What Services are Impacted

Each of your services can have an impact on other services to which it is related. Use the Services Impacted view to see details about the services that are impacted by the state of one particular service.

For example, you are responsible for monitoring a service called Application Servers, which represents the application servers for your Banking Application. You subscribe to this service and notice that Foglight has fired has three critical alarms for it. This means that Application Servers is now in a critical state.

To find out if Application Servers' state impacts other services, you select Application Servers and click the Service(s) Impacted tab.

Your Banking Application service is listed and its health is critical. The Banking Application service depends on and contains the service Application Servers. Foglight has not fired alarms for any of the other services that the Banking Application service contains, so Banking Application's state is critical, just like Application Servers'.

To investigate impacted services:

1. In the table at the top of the dashboard, select the service that you want to investigate.
2. Click the Services Impacted tab.

   Foglight lists the other services that are impacted by the state of the one that you selected, as well these services' health (the state they are in — warning, critical, or fatal), alarms, and health history.

   A serivce's health reflects the aggregate state of its components; it is a rollup of all alarms fired for components it contains. Foglight displays each impacted service's recent health in the Health History column. This column summarizes the service's health for the dashboard's time range. The colored segments represent the service's alarm severity states at different intervals within the time range. Yellow segments represent warning alarms, orange segments represent critical alarms, and red segments represent fatal alarms.

   See "Viewing, Acknowledging, and Clearing Alarms" on page 15 for information about working with alarms and "To investigate the health history:" on page 25 for information about drilling down into a health history bar.
3. Click the name of an impacted service to investigate it further.

   A popup appears.

4 Drill down even further by following the links to more detailed views.

Click this link	If you want to see...
Service Level Agreement(s)	A summary of the service level compliance, alarms, and availability. See “Service Level Agreement(s)” on page 33 for more information.
Monitored Component(s)	The Service Breakdown view for that service.
Default Service Breakdown or Drilldown: <View Name>	If your Foglight administrator did not configure a drilldown view, the link is **Default Service Breakdown**. and clicking the link takes you to a view that lists all components added to the service and their status. If your Foglight administrator configured a view, the link is **Drilldown: <View Name>** and clicking the link takes you to that view.
Edit Service	The Service Builder for the selected service. You can only follow this link if you have the Administrator role. For details about the Service Builder, see the online help for that dashboard.

Visualizing the Dependencies Among Services

Click the **Service Dependencies** tab to display a graphic representation of the hierarchy of services that the selected service comprises. Use the components’ state icons to trace the critical path of performance issues across a domain.

Use the depth control in the upper right corner to set the number of levels (1-4) in the diagram. The default setting is two levels.

The dots above the depth control determine the scale of the diagram.

- Click the smaller dot to reduce the scale for easier navigation of large diagrams.
- Click the medium dot to restore the diagram to its original scale.
- Click the largest dot to zoom to the highest zoom level.

By default, Foglight arranges the components in a tree diagram. You can also manually change the components’ layout to position them as you wish. When you move a component, Foglight deselects the **Auto Arrange** check box. Select the **Auto Arrange** check box to return to the original layout.

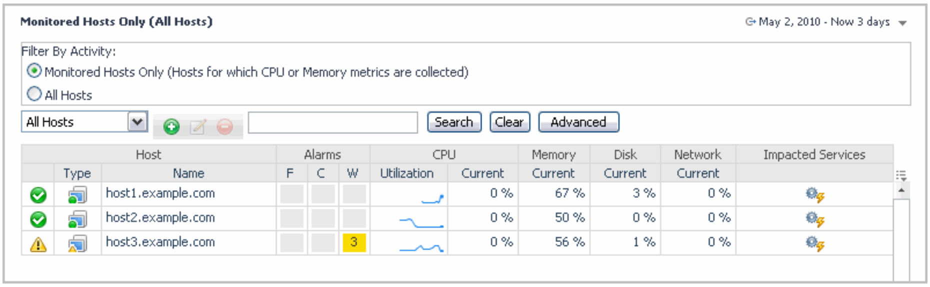
5

Monitoring Your Hosts

This chapter describes how to monitor hosts using workflows that start in the Hosts dashboard. By following these workflows, you can view the performance of all monitored hosts or drill down on a single host.

Access the Hosts dashboard from the Welcome page (**Homes** > **Welcome**) by clicking **View the Health of the Monitored Hosts in Your Enterprise**.

Tip You can also access this dashboard from the navigation panel: select **Homes > Hosts**.



Monitored Hosts Only (All Hosts) May 2, 2010 - Now 3 days

Filter By Activity:

● Monitored Hosts Only (Hosts for which CPU or Memory metrics are collected)

○ All Hosts

	Host		Alarms			CPU		Memory	Disk	Network	Impacted Services
	Type	Name	F	C	W	Utilization	Current	Current	Current	Current	
✓		host1.example.com					0 %	67 %	3 %	0 %	
✓		host2.example.com					0 %	50 %	0 %	0 %	
⚠		host3.example.com			3		0 %	56 %	1 %	0 %	

Use the Hosts dashboard to monitor for problems in your environment if you are responsible for the availability of a set of hosts and prefer to think in terms of systems. The Hosts dashboard provides the best high-level summary of host state and performance, including alarms, CPU, memory, disk, and network utilization.

Drill down from this dashboard to different dashboards and views that provide more detail about your hosts. You can also use this dashboard to see if a host's state has an impact on services and view the health history of each host.

Selecting a Set of Hosts to Monitor

The Hosts dashboard is useful for monitoring environments with a large number of hosts, since you can choose to show only a subset of these hosts or display all hosts.

In many cases, you need to focus on a subset of these hosts. There are different ways to do this in the Hosts dashboard:

- Use the field at the top of the table to filter the list of hosts by name — for example, to display only the hosts with “database” in their names.
- Use the menu under the Filter By Activity area to show only hosts in a specific category — for example, all Windows hosts.

If you need to see data for all hosts in your environment, you can:

- Work with the default settings in the Filter By Activity area and the menu underneath it (**Monitored Hosts Only** and **All Hosts**, respectively).

  All hosts for which Foglight collects CPU and memory metrics are listed in the table.
- Select **All Hosts** from the Filter By Activity area and leave the default setting **All Hosts** in the menu underneath this area.

  All hosts in your monitored environment are listed in the table.

Tip If you have the Advanced Operator role, you can save the results of your search as a filter using the groups toolbar above the table. Type the search criteria in the field in this toolbar, click **Search** to filter the list of hosts by name, and then click the plus-sign button (⊕). The filter is listed in the menu, along with the default filters.

Identifying the Types of Hosts You Are Monitoring

The icons in the Type column allow you to see at a glance what kind of hosts you are monitoring: physical hosts are identified by the icon , VMware images by the icon , and ESX servers by the icon .

Monitoring Your Hosts’ State

Now that you have chosen the group of hosts you want to monitor, refer to the icons in the first column in the table to see the state of these hosts at a glance. Each state indicator shows the host’s aggregate alarm state (excluding the state of agents on that host).

Investigating Alarms for a Host

Investigate a host’s alarms to get more details about the problems contributing to its non-normal state. In the row for the host, click the icon that represents warning, critical, or fatal alarms to display an alarm list filtered to show only the warning, critical, or fatal alarms for that host. See “Viewing, Acknowledging, and Clearing Alarms” on page 15 for information about working with alarms.

Viewing A Host’s Performance

The CPU, Memory, Disk, and Network columns allow you to obtain a concise overview of your hosts’ performance in these metric categories. The values in these columns — and the popups and drilldowns available from them — change with the dashboard's time range.

These columns display recent and current values for each metric category. Recent values are displayed as a sparkline in the Utilization column.

Tip By default, a sparkline is shown only in the CPU Utilization column. To display sparklines for other metric categories, click the **Show columns** icon (☰) at the top of the table and select the **Utilization** checkbox under Memory, Disk, or Network.

To investigate a host’s CPU-, memory-, disk-, and network-related performance:

1. Hover the cursor over the sparkline or current value in the CPU, Memory, Disk, and Network column for that host.

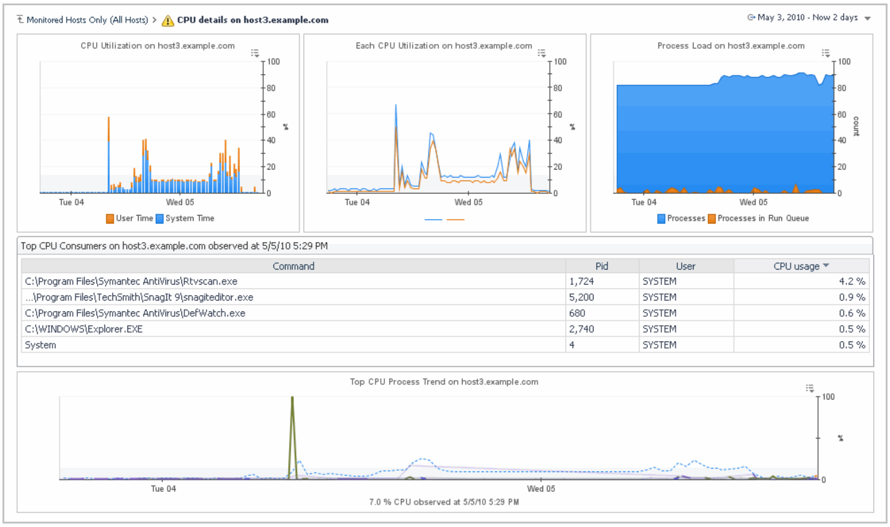
   A popup appears. It contains a utilization chart for that metric.

2. To investigate further, click the sparkline or current value.

   A dashboard appears that contains details for that metric category.

   Tip Hover over a line or area in a chart to display data for the nearest time in a tooltip.

If you click this column...	**This dashboard appears...**
CPU	CPU Details (example shown below): use it to identify the top CPU consumers on the host, see the top processes’ utilization trends, and view charts for CPU utilization process load.
Memory	Memory Details: use it to investigate overall memory utilization on the host and the amount of memory the top processes are consuming. The Top Memory Consumers table lists both resident and virtual sizes for the top processes.
Disk	Disk Details: use it to identify the top disk I/O consumers on the host, see the utilization trends of the top CPU processes, and view charts for disk size and bytes read and written.
Network	Network Details: use it to investigate the aggregate network utilization of the host and view the activity of your network connections.


Monitored Hosts Only (All Hosts) > CPU details on host3.example.com
May 3, 2010 - Now 2 days
CPU Utilization on host3.example.com
100
80
60
40
20
0
%
Tue 04
Wed 05
🟧 User Time 🟦 System Time
Each CPU Utilization on host3.example.com
100
80
60
40
20
0
%
Tue 04
Wed 05
Process Load on host3.example.com
100
80
60
40
20
0
count
Tue 04
Wed 05
🟦 Processes 🟧 Processes in Run Queue
Top CPU Process Trend on host3.example.com
100
%
0
Tue 04
Wed 05
7.0 % CPU observed at 5/5/10 5:29 PM

Top CPU Consumers on host3.example.com observed at 5/5/10 5:29 PM

Command	Pid	User	CPU usage
C:\Program Files\Symantec AntiVirus\Rtvscan.exe	1,724	SYSTEM	4.2 %
...\Program Files\TechSmith\SnagIt 9\snagiteditor.exe	5,200	SYSTEM	0.9 %
C:\Program Files\Symantec AntiVirus\DefWatch.exe	680	SYSTEM	0.6 %
C:\WINDOWS\Explorer.EXE	2,740	SYSTEM	0.5 %
System	4	SYSTEM	0.5 %

Seeing If a Host’s State Impacts Your Services

If one of your hosts is in a state other than Normal (✓), use the impacted services popup to view which of your services that host might impact. This popup helps you establish whether critical services are affected by problems with your hosts and decide if immediate action is necessary to resolve these problems.

Note You can only view user-defined impacted services. System services are not shown.

To view a host’s impacted services:

- Click the icon (⚙) in the Impacted Services column for the host you are investigating.

The impacted services popup shows a summary that lists the name of the impacted service, its aggregate state, and its aggregate state history.

Note The Service Health History column is hidden by default. To view it, click the Show columns icon (☰) and then select the column in the popup.

Tip In addition to the dashboards described in this chapter, Foglight provides you with other views on your hosts. For details, see the online help for the dashboards listed under **Dashboards > Hosts** in the navigation panel.

6

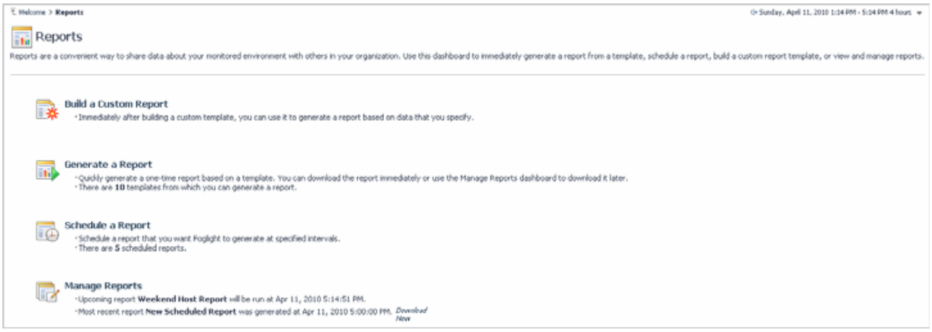
Reporting on Your Enterprise

Reports are a convenient way to share data about your monitored environment with others in your organization. Create reports using:

- Pre-defined reports — use out-of-the-box templates to obtain a quick, high-level perspective on your data. See “Generating and Scheduling Reports” on page 44.
- Custom reports — create custom report templates to tailor your reports content and presentation to suit your needs. See “Building a Custom Report” on page 45.

Operators can run reports, build custom report templates, and view generated reports. Advanced Operators can also schedule and manage reports. The Reports dashboard is your starting point for working with reports. Use it to create and schedule reports and access the Manage Reports dashboard. Access the Reports dashboard from the Welcome page (**Homes** > **Welcome**) by clicking **Report on Your Enterprise**.

You can also access this dashboard from the navigation panel: select **Homes > Reports**.



Welcome > **Reports**

Sunday, April 11, 2010 1:14 PM - 5:14 PM 4 hours

Reports

Reports are a convenient way to share data about your monitored environment with others in your organization. Use this dashboard to immediately generate a report from a template, schedule a report, build a custom report template, or view and manage reports.

Build a Custom Report
- Immediately after building a custom template, you can use it to generate a report based on data that you specify.

Generate a Report
- Quickly generate a one-time report based on a template. You can download the report immediately or use the Manage Reports dashboard to download it later.
- There are **10** templates from which you can generate a report.

Schedule a Report
- Schedule a report that you want Foglight to generate at specified intervals.
- There are **5** scheduled reports.

Manage Reports
- Upcoming report **Weekend Host Report** will be run at Apr 11, 2010 5:14:51 PM.
- Most recent report **New Scheduled Report** was generated at Apr 11, 2010 5:00:00 PM. *Download Now*

The Reports dashboard also provides you with at-a-glance reporting details. It displays the number of report templates available to you, the number of scheduled reports, and information about upcoming scheduled reports and recently-generated reports.

Generating and Scheduling Reports

Foglight contains a number of pre-defined report templates. Each template serves a particular purpose, but many templates have the same expected inputs. The values you specify for these inputs define the content of the report.

Use a template as-is to quickly generate or schedule a report or optionally change the report input values to meet your requirements.

Tip Hover the cursor over a template name in the Generate Report or Schedule Report wizard to view the template’s description in a tooltip.

Generating a Report

Click **Generate a Report** on the Reports dashboard to select and generate a report immediately (for example, a PDF report) using the Generate Report wizard. See the online help for the Reports dashboard for details about using this wizard.

Scheduling a Report

Click **Schedule a Report** on the Reports dashboard to select and schedule a report using the Schedule Report wizard. See the online help for the Reports dashboard for details about using this wizard.

Tip You can also create a scheduled version of a report that has been generated. For more information, see the online help for the Manage Reports dashboard.

Adding a New Schedule

If the out-of-box schedules available in the Schedule Report wizard do not meet your requirements, your Foglight administrator can define a new schedule using the Simple New Schedule Wizard. This is the same wizard that Foglight administrators use to create new blackout schedules. Ask your Foglight administrator for assistance if you need a new schedule.

Building a Custom Report

You can also create a custom report template, which is similar to creating a dashboard. By creating your own report templates, you can build reports directly from any dashboard or tailor the content and presentation of reports to suit your requirements.

Creating a Custom Report Template

Click **Build a Custom Report** on the Reports dashboard to choose the building blocks for your custom report using the Create Report wizard. See the online help for the Create Report wizard for details about using this wizard.

Immediately after building a custom template, you can use it to generate a report based on data that you specify.

Tip You can create a report based on a monitoring dashboard you are currently viewing: select **General > Create Report...** from the action panel.

Generating a Custom Report

Custom report templates that you create appear under My Dashboards in the navigation panel. To run a report immediately based on one of these templates, select the template and click **Run report** (Run report) in the toolbar. From this dashboard, you can also schedule a report based on the template by clicking **Schedule report** (Schedule report).

Foglight also lists custom report templates in the Generate Report and Schedule Report wizards.

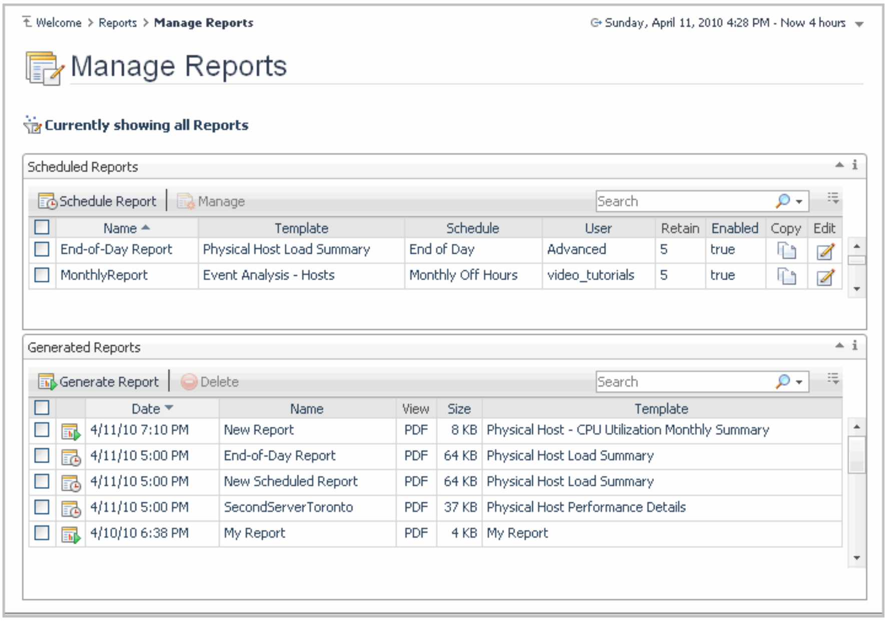
Each time you schedule or generate a report based on a custom report template, you can change the data Foglight includes in the report by setting the input values.

Deleting a Custom Report Template

Delete any custom report template that you have created by selecting the template under My Dashboards and clicking **Delete this Report** in the Action panel (**General > Actions**). Foglight removes the report from My Dashboards and the report template list.

Managing Reports

Click **Manage Reports** on the Reports dashboard to access the Manage Reports dashboard.



Welcome > Reports > **Manage Reports**

Sunday, April 11, 2010 4:28 PM - Now 4 hours

Manage Reports

Currently showing all Reports

Scheduled Reports

Schedule Report | Manage

Search

□	Name	Template	Schedule	User	Retain	Enabled	Copy	Edit
□	End-of-Day Report	Physical Host Load Summary	End of Day	Advanced	5	true		
□	MonthlyReport	Event Analysis - Hosts	Monthly Off Hours	video_tutorials	5	true		

Generated Reports

Generate Report | Delete

Search

□		Date	Name	View	Size	Template
□		4/11/10 7:10 PM	New Report	PDF	8 KB	Physical Host - CPU Utilization Monthly Summary
□		4/11/10 5:00 PM	End-of-Day Report	PDF	64 KB	Physical Host Load Summary
□		4/11/10 5:00 PM	New Scheduled Report	PDF	64 KB	Physical Host Load Summary
□		4/11/10 5:00 PM	SecondServerToronto	PDF	37 KB	Physical Host Performance Details
□		4/10/10 6:38 PM	My Report	PDF	4 KB	My Report

Use this dashboard to download, delete, and view details about generated reports. If you have the Advanced Operator role, you also use this dashboard to perform report-management tasks such as:

- Deleting scheduled reports. For example, you no longer require a specific scheduled report because you removed the service that it reports on.
- Enabling/disabling scheduled reports. For example, you are performing system maintenance and do not want Foglight to run scheduled reports during that time.
- Editing scheduled reports. For example, you want to change the maximum number of hosts included in a scheduled report.

You can also use the Manage Reports dashboard to generate and schedule reports from the context of your existing set of reports. For example, you view a one-time report and decide that it should be generated automatically at the end of each month. For more information, see the online help for the Manage Reports dashboard.

Index