



vFoglight™ 5.2.4.5

Cartridge for Guest Process Investigation
User Guide



© 2009 Quest Software, Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

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.

Trademarks

Quest, Quest Software, the Quest Software logo, Aelita, Akonix, Akonix L7 Enterprise, Akonix L7 Enforcer, AppAssure, Benchmark Factory, Big Brother, DataFactory, DeployDirector, ERDisk, Foglight, Funnel Web, I/Watch, Imceda, InLook, IntelliProfile, InTrust, Invertus, IT Dad, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, MessageStats, NBSpool, NetBase, Npulse, NetPro, PassGo, PerformaSure, Quest Central, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL LiteSpeed, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Tag and Follow, Toad, T.O.A.D., Toad World, vANALYZER, vAUTOMATOR, vCONTROL, vCONVERTER, vEssentials, vFOGLIGHT, vOPTIMIZER, vRANTER PRO, vReplicator, Vintela, Virtual DBA, VizionCore, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Disclaimer

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.

License Credits and Third Party Information

To view license credit information, click the License Credits link on the Welcome to vFoglight online help page.

User Guide

March 2009

Version 5.2.4.5

Table of Contents

Introduction to this Guide	7
About vFoglight	8
About this Guide.....	8
vFoglight Documentation Suite	8
Core Documentation Set	9
Cartridge Documentation Sets	10
Feedback on the Documentation.....	10
Text Conventions	11
About Vizioncore Inc.	11
Contacting Vizioncore.....	12
Contacting Vizioncore Support.....	12
Contacting Quest Support	12
Introduction to the Cartridge for Guest Process Investigation	15
Overview of the Cartridge for Guest Process Investigation	16
Understanding the Concept of Guest Process	16
Monitoring Virtual Machines with the Cartridge for Guest Process Investigation	17
Cartridge Navigation Basics	19
vFoglight GUI Panels	20
Navigation Panel	20
Display Panel.....	21
Actions Panel.....	21
Time Range.....	21
Sortable Lists.....	22
Alarms and their Status Indicators	23
Mouse Over Actions	23

Interacting with the Cartridge for Guest Process Investigation	25
Installing and Configuring WinRM	26
Downloading WinRM	26
WinRM Configuration	26
Listening for Remote Connections	27
Authentication Scheme 1 - Encrypted Basic Authentication via HTTPS	27
Authentication Scheme 2 - Unencrypted Basic Authentication	27
Deploying a Cartridge for Guest Process Investigation Agent to FglAM	28
Manual Configuration of Guest Process Agents Using the Administration Dashboards	30
Guest Process Agents Dashboard	35
Processes Dashboard	36
Navigating to the Cartridge for Guest Process Investigation Dashboard	38
WinRM Remote Access Account Restrictions	39
Process Dashboard Collection Options	39
Enable Process Collection	40
Configure Collection	40
Enable Process Collection	42
Time Range Menu	43
Using the Cartridge for Guest Process Graphs and Charts	44
Changing the Monitored Processes Viewed	44
Changing the Chart Type	45
Zoom Using the x and y Axis of the Graph	46
Process Info Dashboard View	48
Understanding %CPU Values in Foglight	48
CPU Usage by Process	48
Memory Usage By Process	49
CPU At a Glance	49
Memory At a Glance	50
Monitored Processes	50
Using the Monitored Processes View	50
Process Information Data Sources	54
Windows	54
Process Name	54
Process ID	54
Parent Process ID	55

Processor Utilization (%)	55
Total Processor Time	55
Memory Utilization	55
Virtual Memory Size	55
Working Set Size	55
Swap Size.....	56
Page Faults	56
Data Read	56
Data Written.....	56
Data Other	56
Read Operations	56
Write Operations.....	56
Other Operations	56
Linux.....	57
Process Name	57
Process ID (PID).....	57
Parent Process ID (PPID).....	57
Processor Utilization (%)	57
Total Processor Time	57
Memory Utilization.....	57
Working Set Size	58
Virtual Memory Size	58
Swap Size.....	58
Solaris	58
Process Name	58
Process ID (PID).....	58
Parent Process ID (PPID).....	58
Processor Utilization (%)	58
Total Processor Time	59
Memory Utilization	59
Working Set Size	59
Virtual Memory Size	59
Troubleshooting the Cartridge for Guest Process Investigation.....	59
Why did I get a message saying "Error - Missing Input" after clicking the Save button in the Configuration Settings dialog box?.....	59

Why did I get a message saying "Error: Invalid Agent" after clicking the Save button in the Configuration Settings dialog box? 60

Why did I get a message saying "Error: No Agent Provided" after clicking the Save button in the configuration settings dialog box? 60

Why is the Save button disabled on the Configuration Settings dialog box? 60

I have saved my configuration settings, and the Enable Process Collection checkbox is checked, but I still do not see any data. What is wrong? 60

I have saved my configuration settings, but the Enable Process Collection checkbox is disabled and I do not see any data. What is wrong? 61

Index 63

Introduction to the Cartridge for Guest Process Investigation

This section contains the following topics:

Overview of the Cartridge for Guest Process Investigation	16
Understanding the Concept of Guest Process	16
Monitoring Virtual Machines with the Cartridge for Guest Process Investigation	17

Overview of the Cartridge for Guest Process Investigation

Virtual machines are quickly becoming the industry norm in IT infrastructures. Companies use virtual machines to reduce server growth, reduce costs, and conserve energy.

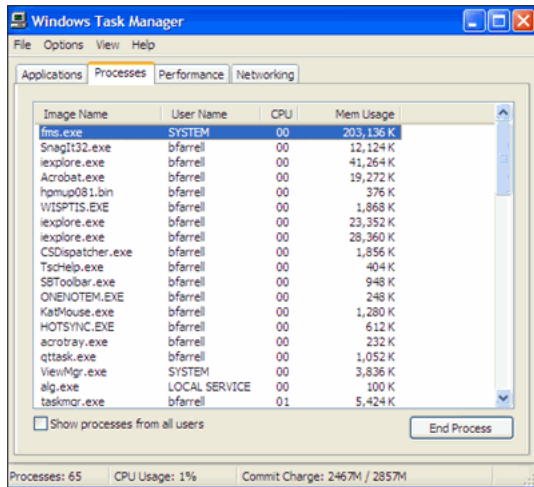
The monitoring of internal resource contention problems of virtual machine environments presents a unique set of challenges. In order for a corrective triage of problems to take place, running processes, active users and current services must be monitored.

However, accessing process information on virtual machines can be an inefficient and time-consuming process. Monitoring virtual machine environments with the vFoglight Cartridge for Guest Process Investigation simplifies monitoring and troubleshooting of virtual machines experiencing performance problems.

Note The Cartridge For Guest Process Investigation is specific to the host selected. It provides the same process monitoring information for physical or virtual machines.

Understanding the Concept of Guest Process

The term “guest process” is based on the concept of one “physical machine” hosting “x” number virtual machines. A guest process is a set of internal processes running on one virtual machine. Windows operating systems provide the Task Manager to view and troubleshoot internal process on a physical machine. Those using virtual machines do not have this type of monitoring tool.



To monitor virtual machines, the user currently has to bring up a separate monitor from the one used to monitor the virtual machine, then view Perfmon to get details on what is happening on the host. This is a time-consuming and inefficient process because users have to sit and repeatedly watch real-time displays to spot the recurrence events. Those monitoring virtual environments need the ability to set an unattended tool, and let that tool draw attention to virtual machine(s) that are having performance problems.

Monitoring Virtual Machines with the Cartridge for Guest Process Investigation

The vFoglight Cartridge for Guest Process Investigation allows you to monitor the virtual infrastructure, health, and performance of processes inside virtual machines. Guest Process agents are configured with virtual machines to send data back to vFoglight. Alarms in vFoglight alert the user to problems which are then monitored to determine what internal process might be affecting the performance of a virtual machine.

For example, you may have a virtual machine that is running too slowly. You need to determine the root cause. You can configure that machine with the Cartridge for Guest Process Investigation and monitor its processes over a period of time. This reveals that several instances of a single program are open and taking up all of the memory. You close down those instances and the machine returns to its normal state.

Cartridge Navigation Basics

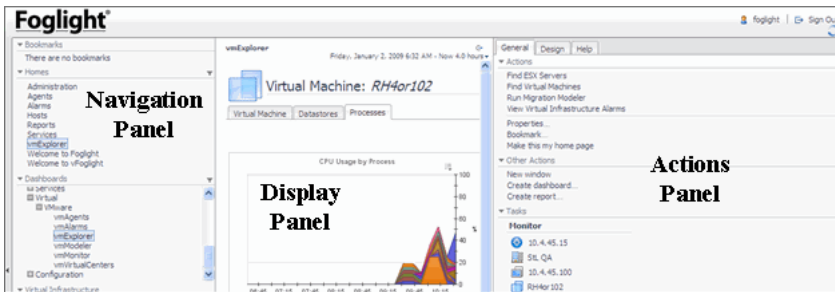
This chapter describes the basic vFoglight navigation techniques necessary for using the Cartridge for Guest Process Investigation. This section contains the following topics:

vFoglight GUI Panels.....	20
Navigation Panel	20
Display Panel.....	21
Actions Panel.....	21
Time Range	21
Sortable Lists.....	22
Alarms and their Status Indicators.....	23
Mouse Over Actions	23

vFoglight GUI Panels

Depending on where you log to vFoglight, you may see either the contents of the first bookmark (the Welcome page is the default) listed under Bookmarks, or a home page. For further details, refer to the *vFoglight User Guide*. Typically, the GUI is divided into the following three panels:

- The navigation panel on the left.
- The larger display panel in the middle.
- The actions panel on the right.



Navigation Panel

The navigation panel operates like a drawer. Its default state is open. To close the navigation panel, click the arrow at the far left of the vFoglight GUI. Click that arrow again to open the navigation panel. The navigation panel lists all of the dashboards that are available to the current user for viewing. You can use the navigation panel to select a dashboard to view in the display panel. To access a specific dashboard, open the appropriate module (the Virtual module, for example). The navigation panel also provides access to the vFoglight Administration and Configuration areas, and may provide access to some cartridge-specific navigation views (for example, the Virtual Infrastructure View for the VMware Cartridge vmExplorer Dashboard).

Note If you do not see any dashboards in the navigation panel, the user id you signed in with may not have been assigned to a group. For details, refer to the vFoglight User Guide.

Display Panel

The display panel is used to view current dashboards and reports, as well as to create new dashboards and reports. You can increase the size of this area by resizing the navigation panel, or, if the actions panel is open, by closing the actions panel.

Actions Panel

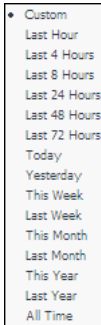
The actions panel operates like a drawer. Its default state is closed. To open the actions panel, click the arrow at the far right of the vFoglight GUI. Click that arrow again to close the actions panel. The actions panel contains the various actions and tasks you can perform with the current dashboard. It also contains views and data that you can add to a dashboard or report you are creating and provides access to the online help files.

Time Range

The default behavior of the VMware Cartridge is to display metrics, alerts, and messages that have occurred within the last four hours. This time range, however, is configurable. To configure the Time Range, use the Time Range menu located in the upper right corner of the vFoglight GUI.



Using the Time Range menu, you can select from the listed predefined time ranges or you can specify a custom range using either a sliding time bar or precision controls to specify dates and times.



When you modify the time range for a dashboard or view, it adjusts the range for all of the contained views contained within and drilldowns accessed from that dashboard or view. It does not adjust the time range for any parent views.

Sortable Lists

In certain vFoglight dashboards, some levels of views contain sortable lists. An example of this is the Monitored Processes, Process Name column in the Cartridge for Guest Process Investigation.

Monitored Processes:





Select All Deselect All Update

	Process Name	Instances	CPU Usage			
			Average	Max	Average	Max
<input checked="" type="checkbox"/>	WINZIP32	1.0 count	n/a	n/a	0.0 %	0.0 %
<input checked="" type="checkbox"/>	wireshark	1.0 count	0.0 %	n/a	0.0 %	0.0 %
<input checked="" type="checkbox"/>	wmiprvse	1.0 count	0.0 %	0.1 %	0.0 %	0.0 %
<input checked="" type="checkbox"/>	wscript	1.0 count	n/a	n/a	0.0 %	0.0 %
<input checked="" type="checkbox"/>	WZQKPICK	1.0 count	0.0 %	0.0 %	0.0 %	0.0 %

It is possible to sort this list by column using any of the column headings. Click a column heading once to sort the list in ascending order. The list is redrawn according to your specification. Click the column heading again to re-sort the list in descending order. This is handy when you want to have an organized view of virtual machines or ESX Server objects sorted by name, parent container, status, etc.

Alarms and their Status Indicators

The Cartridge for Guest Process Investigation uses status indicators to show specific alarms raised within the virtual infrastructure. Four status indicators, similar to those displayed in the following figure, are used throughout the vFoglight Cartridge dashboards. The status indicators may be displayed as round and colored with the number off to the side (as shown below) or they may be displayed as rectangular and colored with the number in the center of the indicator.

	Fatal	1
	Critical	2
	Warning	3
	Normal	5

The vFoglight alarm types respond to thresholds that are defined within the VMware Cartridge rules. As metrics change and move through thresholds, alarms are raised. As a metric moves through thresholds, the severity of an alarm changes, which causes the associated status indicator to change. For detailed information about VMware Cartridge rules and metrics, refer to the vFoglight Cartridge for VMware Reference Guide. It is important to note that with the VMware Cartridge an event that triggers an alarm for an object does not trigger an alarm for any of the object's parents. For example, a single Virtual Machine running at a high CPU utilization does not trigger an alarm for its parent ESX Server. An alarm would only be triggered for the parent ESX Server if the server itself was running at a high CPU utilization.

Mouse Over Actions

Many items within vFoglight dashboards display additional information when you hover the cursor over them. For example, when you hover the cursor over a graph you are likely to see a specific value or values that correspond(s) to the position of the cursor. When you hover the cursor over an individual metric, you are likely to see a small descriptive popup.

Interacting with the Cartridge for Guest Process Investigation

This chapter takes you through the various dashboards and associated views in the Cartridge for Guest Process Investigation Cartridge. This section contains the following topics:

Installing and Configuring WinRM	26
Deploying a Cartridge for Guest Process Investigation Agent to FglAM	28
Manual Configuration of Guest Process Agents Using the Administration Dashboards	30
Processes Dashboard	36
Guest Process Agents Dashboard	35
Process Information Data Sources	54
Troubleshooting the Cartridge for Guest Process Investigation	59

Installing and Configuring WinRM

To collect process information from remote Windows installations, the Cartridge for Guest Process Investigation relies on Windows Remote Management (WinRM) to expose the process information data. While some Windows installations include WinRM, others require download and installation.

The Cartridge for Guest Process Investigation is compatible with two types of WinRM authentication:

- Encrypted (HTTPS) basic authentication
- Unencrypted (HTTP) basic authentication

After WinRM is installed and properly configured, ensure that process information collection is successful before moving on to the configuration of other WinRM installations.

The following provides WinRM installation and configuration procedures:

- [Downloading WinRM](#)
- [WinRM Configuration](#)
- [Listening for Remote Connections](#)

Downloading WinRM

Click [here](#) to view WinRM installation instructions.

WinRM installations can be viewed for:

- Windows Server 2003 (x86 and 64-bit systems)
- Windows XP (x86 and 64-bit systems)

WinRM Configuration

During configuration of WinRM, it is recommended that you reference WinRM help if required for more specific configuration instructions. Type "winrm" at the command prompt to access help.

Note After configuration is complete, ensure the Windows Remote Management service is started.

Listening for Remote Connections

WinRM on the monitored Windows machine must be configured to listen for incoming connections from remote parties. There are several methods and options available for creating a listener.

The following example shows one method to create a listener:

```
"winrm create winrm/config/listener?Address=*&Transport=HTTP"
```

Authentication Scheme 1 - Encrypted Basic Authentication via HTTPS

This authentication scheme establishes an encrypted HTTPS session with WinRM. This configuration requires that WinRM be configured with an HTTPS listener and an appropriate certificate that identifies the machine WinRM is running on.

In addition to this WinRM configuration, the server that is running the vFoglight Agent Manager (or servers that are not vFoglight) must be configured to trust the WinRM Server's Certificate. You must configure the vFoglight Agent Manager to trust third party certificates.

Note FglAM can be installed on servers that are not vFoglight servers. It is the FglAM server that needs configured, not the vFoglight server. These procedures discuss installing FglAM on the same machine as vFoglight.

The following provides an example for configuring WinRM with an HTTPS Listener and Certificate:

```
* winrm create winrm/config/listener?Address=*&Transport=HTTPS  
@{CertificateThumbprint="PASTE_CERTIFICATE_THUMBPRINT_HERE"}
```

Authentication Scheme 2 - Unencrypted Basic Authentication

Within the second authentication scheme, you are able to establish a session with WinRM using unencrypted, basic authentication. The following are example commands for setting those configuration values:

```
* winrm set winrm/config/service/auth @{Basic="true"}  
* winrm set winrm/config/service @{AllowUnencrypted="true"}
```

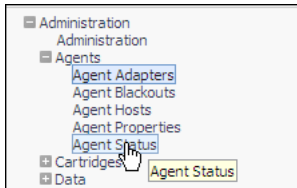
Deploying a Cartridge for Guest Process Investigation Agent to FglAM

Note Before you can deploy the Guest Process Investigation Agent to another machine, the vFoglight Agent Manager must be installed on that machine.

The Cartridge for Guest Process Investigation allows you to monitor process information on multiple host machines. It may reach a point when the vFoglight Agent Manager server becomes slowed down from monitoring large numbers of host machines. The following procedures outline how to create and deploy the Guest Process Investigation Cartridge agent to another vFoglight Agent Manager to monitor addition hosts. This allows you to spread out the monitoring workload and avoid slowing down a single machine.

To deploy the Cartridge for Guest Process Investigation agent to another vFoglight Agent Manager:

- 1 From the navigation panel, Select **Dashboards > Administration > Agent**.
- 2 Select **Agent Status**.



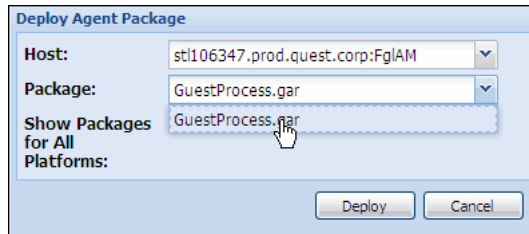
- 3 Click **Deploy**.

The Create Agent dialog displays.

- 4 From the Host drop-down, select the desired Host.

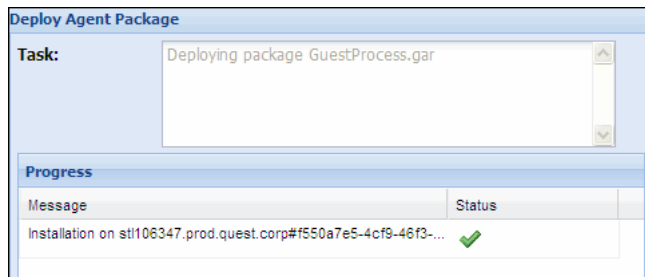


- 5 From the Package drop-down list, select the required package.



6 Click **Deploy**.

The agent installs on the selected host.

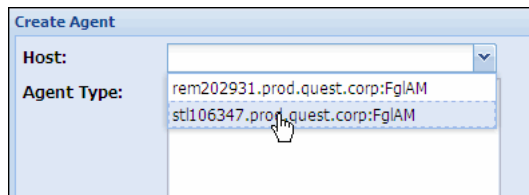


7 Click **OK**.

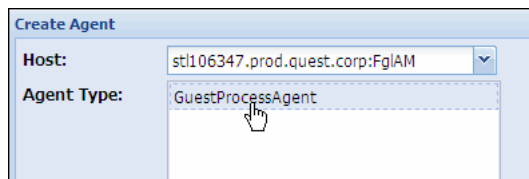
8 Click **Create**.

The Create Agent dialog displays.

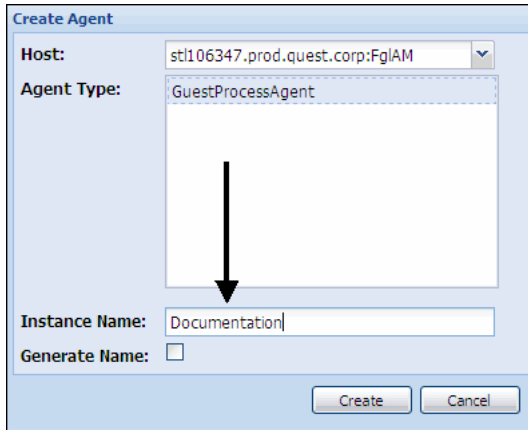
9 From the Host drop-down, select the desired host.



10 From the Agent Type drop-down, select the Guest Process Agent.



- 11 Enter the desired name in **Instance Name**.



The screenshot shows a 'Create Agent' dialog box with the following fields and controls:

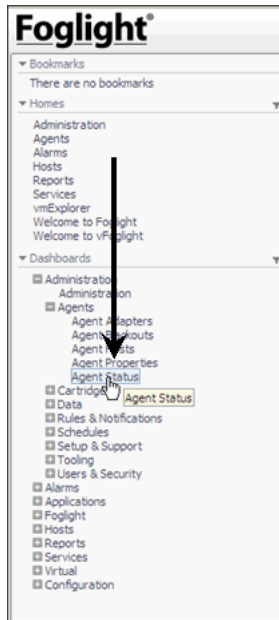
- Host:** A dropdown menu showing 'st1106347.prod.quest.corp:FglAM'.
- Agent Type:** A text box containing 'GuestProcessAgent'.
- Instance Name:** A text box containing 'Documentation'. A black arrow points from the 'Agent Type' field down to this field.
- Generate Name:** A checkbox that is currently unchecked.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom right.

- 12 Click **Create**.
The agent creates.
- 13 Click **Activate**.

Manual Configuration of Guest Process Agents Using the Administration Dashboards

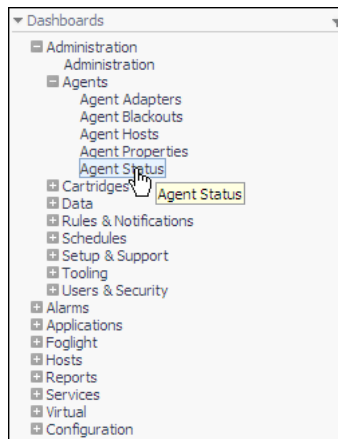
Note The Guest Process agent can be configured from the Agent Administration dashboards in vFoglight. This is not recommended.

Use the Administration Agents dashboard for manual agent configuration.

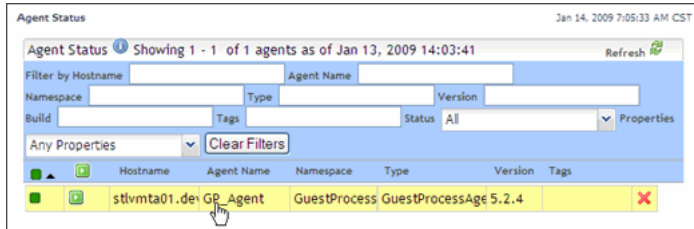


To manually configuration a Guest Process Investigation agents using the Administration Dashboards:

- 1 Navigate to Agent Status in the navigation panel (**Dashboards > Administration > Agents > Agent Status**).



- 2 Select the required agent.

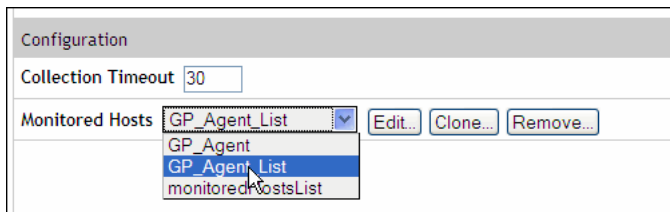


3 Click **Edit Properties**.

The Agent Status dashboard displays.

Note It is important to note that Agent Name must match the Monitored Hosts list name. For example, if the Agent Name is "GP_Agent", the Monitored Hosts list name must be "GP_Agent". If the Agent Name and Monitored Hosts list name does not match, the vFoglight dashboards will not display the agents data correctly.

4 From the Monitored Hosts drop-down, select the desired agent list.



The agent list dialog displays.

5 Click **Edit**.

The selected monitored host list displays.

The screenshot shows the 'GP_Agent_List' dialog. It contains a table with the following data:

Monitored	Sample Interval	Host Name	User Name	Password	Operating System	SSH port	Use SSL	WinRM Port	Win URL Path
True	30	stidevfoxgscs	administrator	*****	windows	22	False	80	wsm
True	30	10.4.44.140	root	*****	solaris	22	True	443	
True	30	10.20.4.27	oracle	*****	solaris	22	True	443	
True	30	rh4or102	oracle	*****	linux	22	True	443	
True	30	stlvmt_ora11g	administrator	*****	windows	22	False	80	wsm

At the bottom right of the dialog, there is an 'Add new row' button.

6 Click **Add new row**.

The configuration dialog displays.

- 7 The configuration dialog allows you to complete the required fields to connect to a host machine.

The screenshot shows a configuration dialog box with the following fields and values:

- Monitored: True False
- Sample Interval:
- Host Name:
- User Name:
- Password:
- Operating System: (dropdown menu)
- SSH port:
- Use SSL: True False
- WinRM Port:
- WinRM URL Path:

A "Cancel" button is located at the bottom right of the dialog.

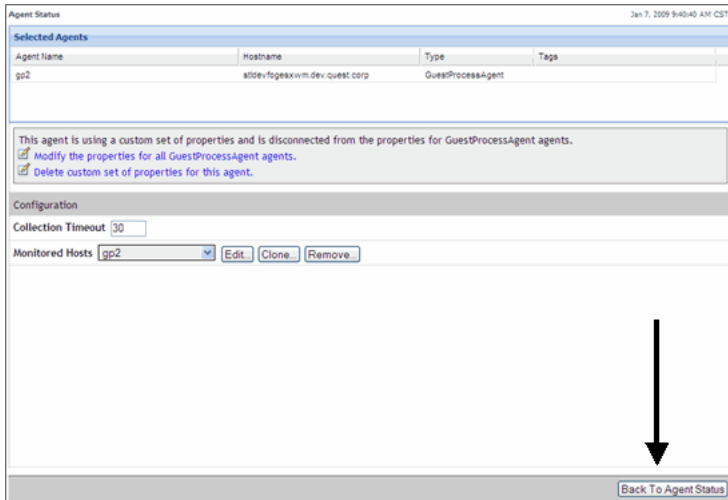
- **Monitored:** Allows you to collect process info from the host machine.
- **Sample Interval (seconds):** Allows you to set the collection rate between vFolight and the host in seconds.
- **Host Name:** Name of the host you are connecting to.
- **User Name:** User name of the host you are connecting to.
- **Password:** Password of the host you are connecting to.
- **Operating System:** Allows you to select the operating system, i.e., Windows, Solaris, Linux.

Note For Windows: In order to access that information through WinRM, the provided account information must be an account that is a member of the local computer's administrators group on the remote machine. For more information, click [here](#). This link takes you to a MSDN site that discusses this requirement. Review Step three of the instructions for connecting to a remote computer using a different account.

Note For Linux/Solaris: The username and password must be an account with SSH access to the host being monitored.

- **Windows Host:** The following default values are used:
 - **Use SSL:** False
 - **WinRM Communication Port:** 80

- **WinRM URL Path:** wsman
 - **Linux or Solaris Host:** The following default values are used:
 - **SSH Port:** 22
 - **Use SSL:** Using SSL ensures an encrypted connection between the agent and the monitored host. This requires the vFoglight Agent Manager (FglAM) to be configured to trust the monitored host's certificate. For procedures on installing the vFoglight Agent Manager, refer to the *vFoglight Getting Started Guide*.
 - **WinRM Port:** If the default port is not acceptable, this setting allows you to override that port.
 - **WinRM URL Path:** If the default URL path to the WinRM Listener Endpoint is not acceptable, this setting allows you to override that path.
- 8 Fill in the required parameters.
 - 9 Click **Save**.
 - 10 Close the agent list dialog.
 - 11 Click **Back to Agent Status**.

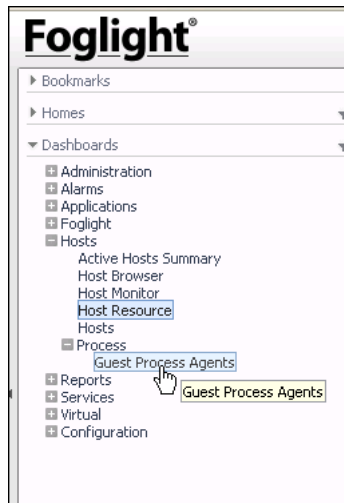


Guest Process Agents Dashboard

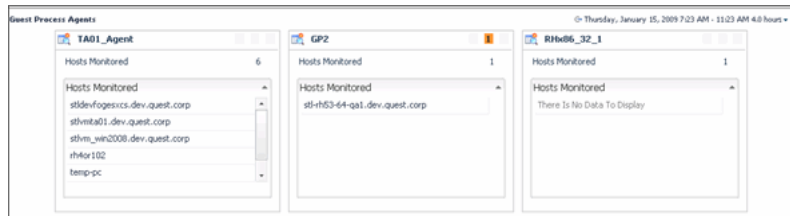
The Guest Process Agents dashboard allows you to view the Guest Process Agents configured and the hosts being monitored.

To view the *Guest Process Agents dashboard*:

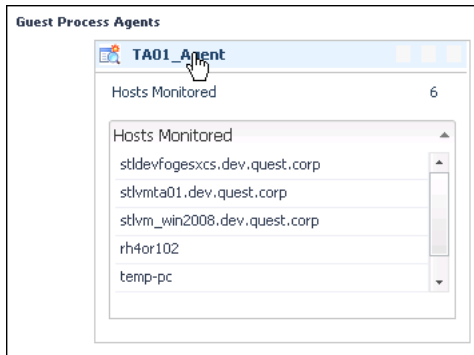
- 1 From the navigation panel select (**Dashboards > Hosts > Processes > Guest Process Agents**).



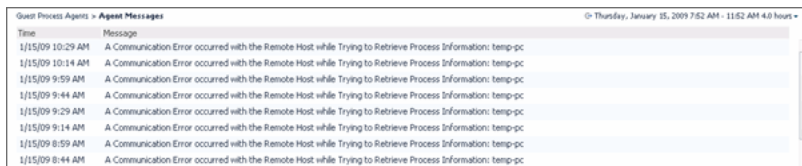
The Guest Process Agents dashboard displays.



- 2 To drill-down and view Guest Process agent information, click the agent name.

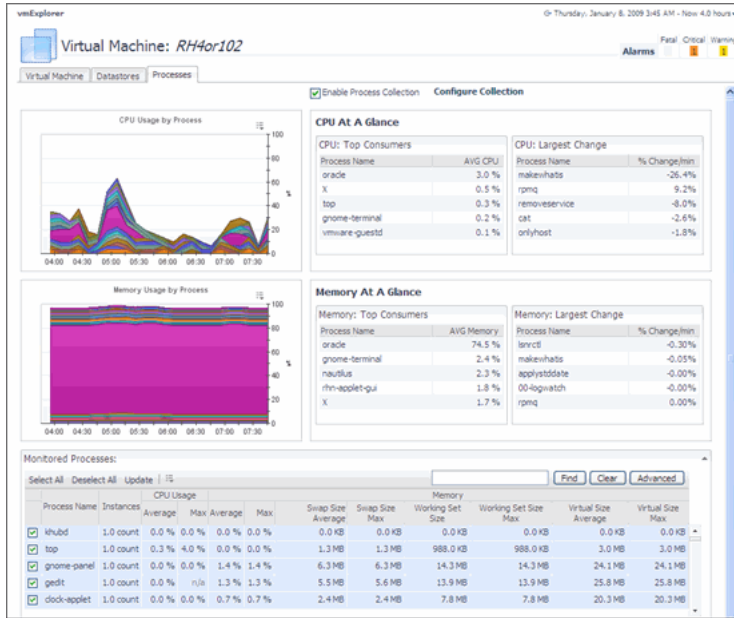


The Agent Messages view displays providing any errors that make have occurred between the Guest Process Investigation agent and the host.



Processes Dashboard

The Processes dashboard displays information on the host that is collecting and sending details to vFoglight. This dashboard can be used to view the process information of the host being monitored and troubleshoot issues with that machine. The following figure shows an example of a typical processes dashboard with embedded views of the processes being monitored.

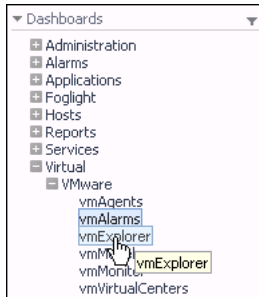


Navigating to the Cartridge for Guest Process Investigation Dashboard

You access the Process dashboard from the vmExplorer.

To view the Process dashboard:

- 1 From the navigation panel select (**Dashboards >Virtual> VMware> vmExplorer**).

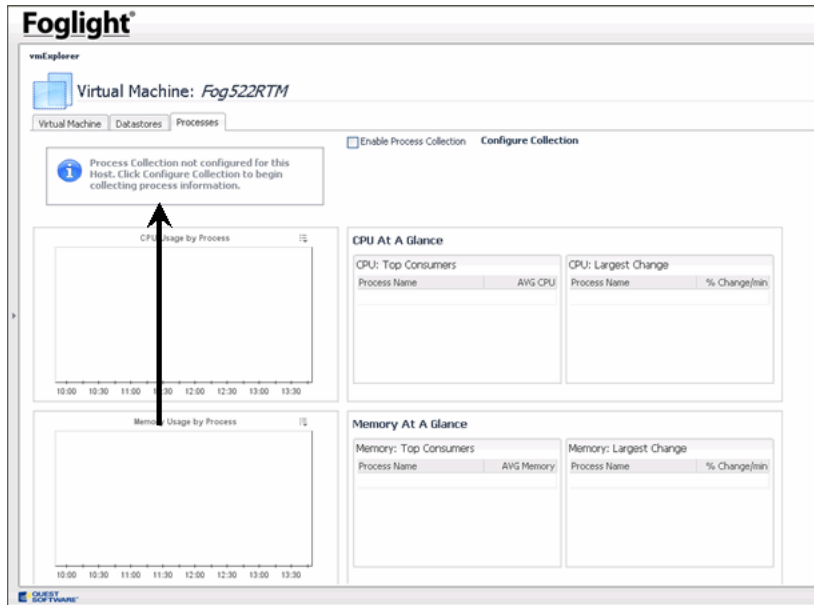


The vmExplorer view displays.

- 2 Click the **Processes** tab.



The Processes view displays. The first time you view the Processes dashboard, the graphs and charts contain no process info. The Guest Process Cartridge for Investigation must first be configured with the host machine before process information is displayed. For more information, see “[Configure Collection](#)” on page 40.



WinRM Remote Access Account Restrictions

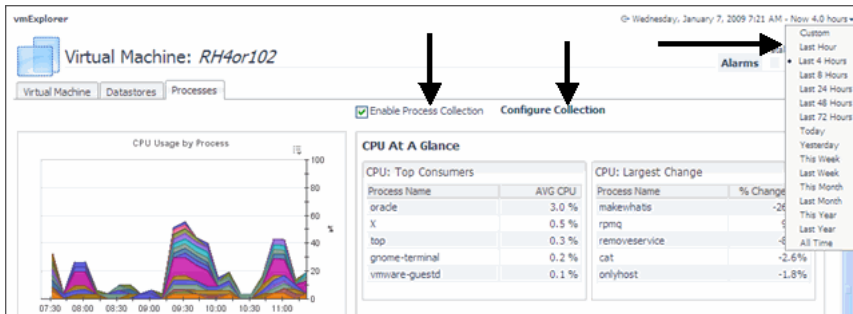
For more information, click [here](#). This link takes you to a MSDN site that discusses this requirement. Review Step three of the instructions for connecting to a remote computer using a different account.

Process Dashboard Collection Options

Note The data displayed can be for either a physical or virtual machine.

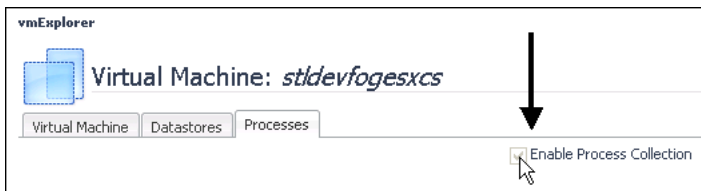
The Processes dashboard provides the following options:

- [Enable Process Collection](#)
- [Configure Collection](#)
- [Enable Process Collection](#)



Enable Process Collection

Checking the Enable check box enables the agent selected. Processes are then sent from the agent to the Processes view.



Configure Collection

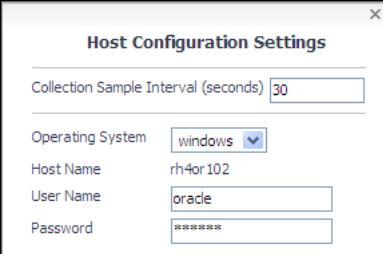
Configuration Collection displays the Host Configuration Settings dialog that provides the following options:

- [Configured Agents](#)
- [Advanced Options](#)
- [Available Collection Agents](#)

Configured Agents

Note Using fgcmd for Guest Process Investigation Agents is strongly discouraged. It is recommended that you use the configuration screens provided with the Guest Processes dashboards.

Configuration Settings allow you to complete the required fields to connect to a host machine.



Host Configuration Settings

Collection Sample Interval (seconds)

Operating System

Host Name

User Name

Password

- **Collection Sample Interval (seconds):** Allows you to set the collection rate between vFolight and the host in seconds.
- **Operating System:** Allows you to select the operating system, i.e., Windows, Solaris, Linux.

Note For Windows: In order to access that information through WinRM, the provided account information must be an account that is a member of the local computer's administrators group on the remote machine. For more information, click [here](#). This link takes you to a MSDN site that discusses this requirement. Review Step three of the instructions for connecting to a remote computer using a different account.

Note For Linux/Solaris: The username and password must be an account with SSH access to the host being monitored.

- **Host Name:** Name of the host you are connecting to.
- **User Name:** User name of the host you are connecting to.
- **Password:** Password of the host you are connecting to.

Advanced Options

Advanced Options provides connection settings to remote hosts.

Note the following when configuring hosts:

- **Windows Host:** The following default values are used:
 - **Use SSL:** False
 - **WS-Man Communication Port:** 80
 - **WS-Man URL Path:** wsman
- **Linux or Solaris Host:** The following default values are used:
 - **SSH Port:** 22

Advanced Options contains the following settings:

▼ **Advanced Options**

Enable Process Collection

Use SSL

WinRM Port

WinRM URL Path

SSH Port

- **Enable Process Collection:** Enables the collection for the machine.
- **Use SSL:** Using SSL ensures an encrypted connection between the agent and the monitored host. This requires the vFoglight Agent Manager (FglAM) to be configured to trust the monitored host's certificate. For procedures on installing the vFoglight Agent Manager, refer to the *vFoglight Getting Started Guide*.
- **WinRM Port:** If the default port is not acceptable, this setting allows you to override that port.
- **WinRM URL Path:** If the default URL path to the WinRM Listener Endpoint is not acceptable, this setting allows you to override that path.
- **SSH Port:** If the default port is not acceptable, it can be overridden using the SSH Port.

Available Collection Agents

Available Collection Agents provides a list of agents configured to collect process info.

Available Collection Agents:	
Agent Name	Hosts Monitored
gp2	7

Enable Process Collection

Checking the Enable check box enables collections for the machine. Processes are then sent from the agent to the Processes view.

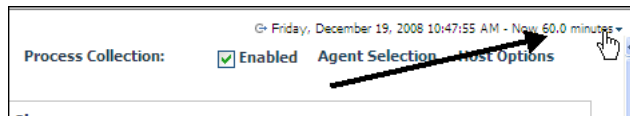


Time Range Menu

From the upper right-hand corner of the Process dashboard, you can select the Time Range Menu to set collection time ranges for the host machine sending process info to vFoglight.

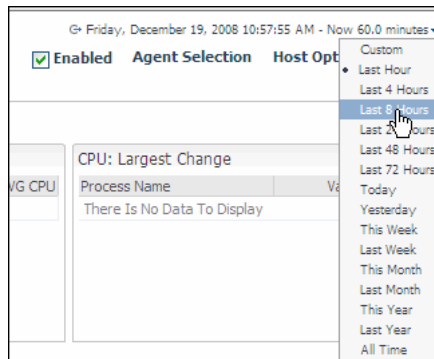
To set the time range menu:

- 1 Click the Time Range Menu in the upper right-hand corner of vFoglight.



The Time Range Menu displays.

- 2 Select the desired time range.



Using the Cartridge for Guest Process Graphs and Charts

When using the Cartridge for Guest Process Investigation graphs and charts, you can do the following to change the views of monitored process:

- Change the monitored process viewed
- Change the chart time
- Perform zoom functions

Changing the Monitored Processes Viewed

The Monitored Processes view allows you to view all or selected processes on the host being monitored.

To change the monitored processes view in Guest Process Investigation charts:

- 1 In the Monitored Processes view you can:
 - **Selected all:** Selects all the processes running on the host machine.
 - **Deselect all:** Deselects all the process running n the host machine.
 - **Update:** Updates the Guest Process Investigation charts once the selection process is made.

Monitored Processes:

Select All Deselect All Update | ⌵

	Process Name	Instances	CPU Usage	
			Average	Average
<input checked="" type="checkbox"/>	wuaudct	1	0.0 %	0.1 %
<input checked="" type="checkbox"/>	update	1	0.0 %	0.8 %
<input checked="" type="checkbox"/>	mrtstub	1	0.0 %	0.0 %
<input checked="" type="checkbox"/>	MRT	1	0.0 %	1.7 %
<input checked="" type="checkbox"/>	windows-kb890830-v2.6-delta	1	0.0 %	0.3 %
<input checked="" type="checkbox"/>	userinit	1	0.0 %	0.2 %

- 2 Select the monitored process you want to view.

Monitored Processes:

Select All Deselect All Update | ☰

	Process Name	Instances	Last Updated	CPU Usage				Swap Aver
				Average	Max	Average	Max	
<input checked="" type="checkbox"/>	mrtstub	1	1/14/09 4:27 PM	0.0 %	n/a	0.0 %	0.0 %	364.0
<input checked="" type="checkbox"/>	sqlbrowser	1	1/15/09 10:26 AM	0.0 %	0.0 %	0.0 %	0.0 %	728.0
<input type="checkbox"/>	cmd	1	1/15/09 10:20 AM	0.0 %	0.0 %	0.0 %	0.0 %	1.5
<input checked="" type="checkbox"/>	smss	1	1/15/09 10:21 AM	0.0 %	0.0 %	0.0 %	0.0 %	152.0
<input checked="" type="checkbox"/>	System	1	1/15/09 10:21 AM	0.4 %	8.3 %	0.0 %	0.0 %	0.0

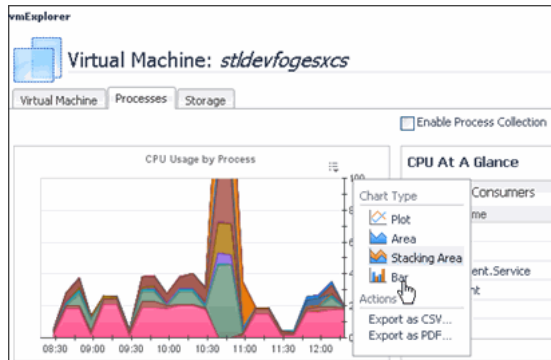
- 3 Click **Update**.
- 4 The CPU Usage by Process and Memory Usage by Process graphs update.

Changing the Chart Type

The vFoglight views allow you to select different chart types.

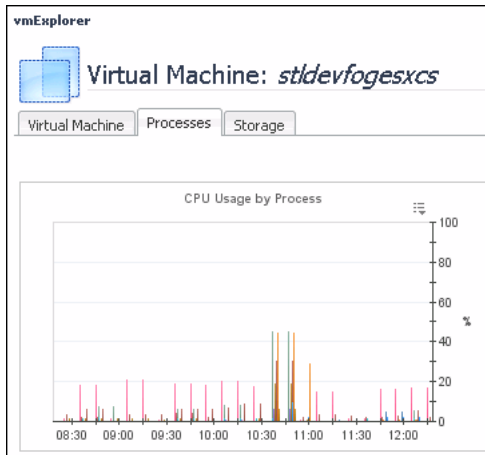
To change chart types:

- 1 Click the chart drop-down in the upper right-hand corner of the chart.



- 2 Select the desired chart.

The current chart change its view to the selected chart.

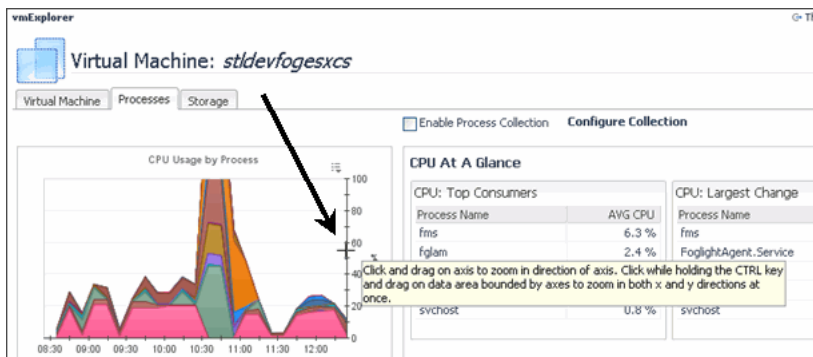


Zoom Using the x and y Axis of the Graph

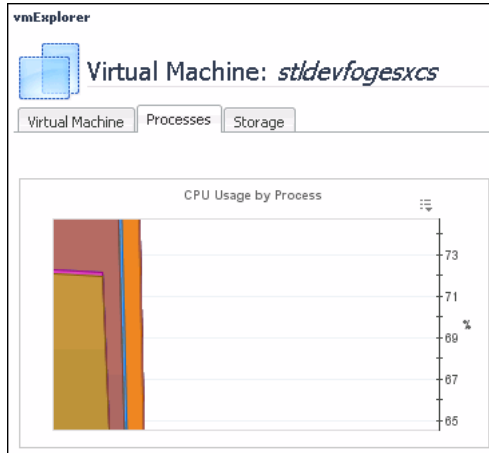
The Guest Process Investigation charts allow you to zoom in for a specific time range for the x and y axis.

To zoom to a specific time range:

- 1 Place the cursor over the x or y axis.

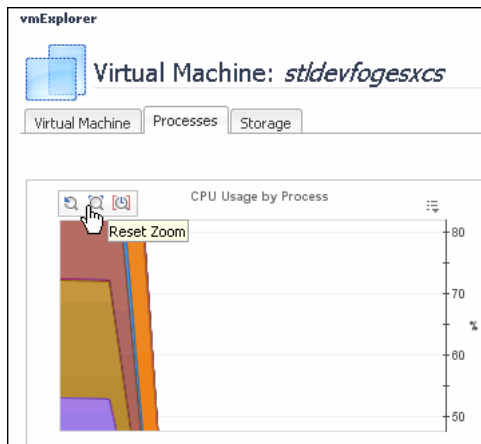


- 2 Click and drag over the desired time range.



The graph zooms to the select time range.

- 3 To reset the zoom, click in the upper left-hand corner.



Process Info Dashboard View

The Process Info Dashboard contains the following embedded views:

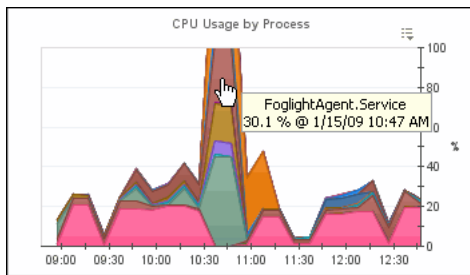
- [CPU Usage by Process](#)
- [CPU At a Glance](#)
- [Memory At a Glance](#)
- [Memory At a Glance](#)
- [Monitored Processes](#)

Understanding %CPU Values in vFoglight

Unlike other data whose values represent a single point in time (when the data is collected), each %cpu data value gathered by the Cartridge for Guest Process Investigation is the average CPU utilization over time between successful data collections. For example, if the configured sample interval is 30 seconds, a process's %cpu utilization is an average of its utilization over the 30 second time period, assuming two back-to-back collects were successful. For this reason, decreasing the sample interval results in values that are real-time, making individual peaks and valleys become more apparent, while increasing the sample interval does the opposite.

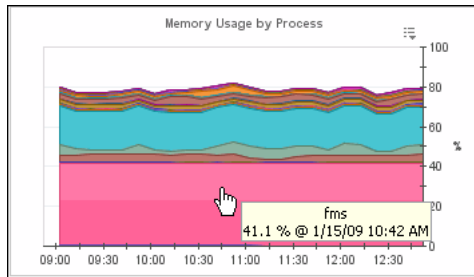
CPU Usage by Process

This view displays the cumulative CPU usage by processes over time. It shows the total process load on a given virtual machine CPU. Mousing over the processes displays a popup of the services.



Memory Usage By Process

This view displays the memory usage by processes over time. It shows the load on memory for processes on a given virtual machine. Mousing over the processes displays a popup of the services.



CPU At a Glance

This displays how the memory is being used based on the following:

- The top five processes using the most CPU. These five processes are the “top consumers” for that memory.
- The top five processes that have had the largest recent change in CPU usage.

CPU: Top Consumers		CPU: Largest Change	
Process Name	AVG CPU	Process Name	Variation
fglam	2.1 %	fglam	— 0%
java	1.0 %	java	— 0%
svchost	0.2 %	taskmgr	— 0%
System	0.2 %	svchost	— 0%
taskmgr	0.2 %	System	— 0%

Memory At a Glance

Note It is possible for multi-instance processes to display %Memory values that are over 100%. This occurs because the PS Command used to query the system returns %Memory values that include the memory used by shared libraries. Since the %Memory values for all individual processes are summed to generate the value, the memory used by shared libraries may be included multiple times.

This displays how the memory is being used based on the following:

- The top five processes using the most memory. These five processes are the “top consumers” for that memory.
- The top five processes that have had the largest recent change in memory usage.

Memory: Top Consumers		Memory: Largest Change	
Process Name	AVG Memory	Process Name	Variation
java	0.1 %	mysqld	— 0%
fglam	0.1 %	fglam	— 0%
mysqld	0.1 %	winlogon	— 0%
svchost	0.0 %	GravitixService	— 0%
explorer	0.0 %	svchost	— 0%

Monitored Processes

Monitored Processes is the table of all running processes on a given host. The list is sortable, filterable, and allows you to do process searches.

Monitored Processes:							
Select All	Deselect All	Update	Show/Hide columns	Average	Max	Average	Max
Process Name	Instances	Average	Max	Average	Max	Swap Size	Average
There Is No Data To Display							

Using the Monitored Processes View

The Monitored Processes view allows you to:

- Choose which processes to view.
- Export reports as a PDF or CSV.

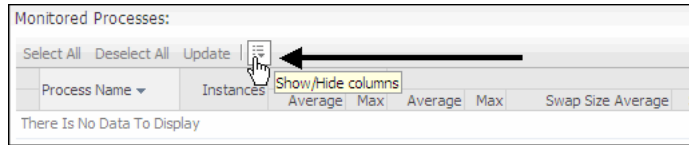
- Search for individual processes.

Choosing Which Processes to View

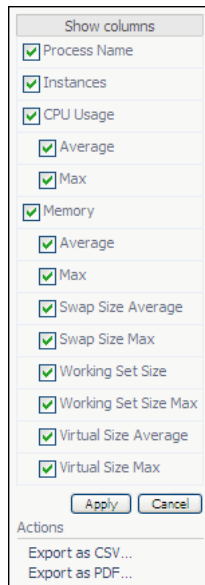
During the monitoring of processes, you may want to view certain processes.

To choose individual processes:

- 1 Click the **Show/Hide** columns menu.



The Show Columns menu displays.



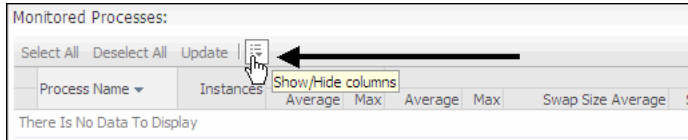
- 2 Select the processes you wish to view.
- 3 Click **Apply**.

Exporting Reports as a PDF or CSV

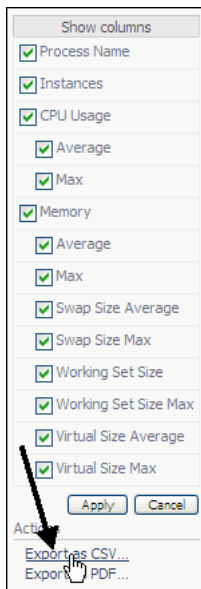
The Cartridge for Guest Process Investigation allows you to export process information to a PDF or CSV format.

To export process info to PDF or CSV:

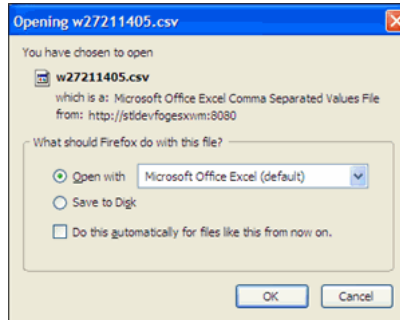
- 1 Click the **Show/Hide** columns menu.



The show columns menu displays.



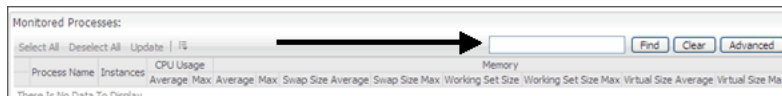
- 2 Click the desired output format (CSV or PDF).
 - a Clicking **Export as CSV** displays a dialog allowing you to choose the save options. Select the desired options and click **OK**.



- b Clicking **Export as PDF** exports the process info data into PDF format and opens in the PDF software loaded on your machine.

Searching for Individual Processes

Using the search allows you to find process information on individual processes.



- **Find:** This field allows you enter the individual process you want to search for. You can select the “Use Regular Expressions” option. Regular expressions can be used to create complex match schemes



- **Clear:** Clears search field.
- **Advanced:** Allows you to enter a process name and set search parameters.

Process Name: CPU Use Regex

Average: < 60

Max:

Average:

Max:

Swap Size Average:

Swap Size Max:

Working Set Size:

Working Set Size Max:

Virtual Size Average:

Virtual Size Max:

Find Clear

Process Information Data Sources

The Cartridge for Guest Process Investigation retrieves process information machine data from the following operating systems:

- [Windows](#)
- [Linux](#)
- [Solaris](#)

The following provides detailed information regarding process information collected by the Cartridge for Guest Process Investigation.

Windows

For process information on a Windows machine, data from Common Information Model (CIM) classes is used. Below is information about the specific classes and fields used to provide process information.

Process Name

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: Name

Process ID

- CIM Class: Win32_PerfRawData_PerfProc_Process

- CIM Field: IDProcess

Parent Process ID

- CIM Class: Win32_Process
- CIM Field: ParentProcessId

Processor Utilization (%)

Processor Utilization requires a calculation involving data from several CIM Classes and Fields. In addition, this calculation requires two samples of data and therefore is not available until after a second data collection is performed.

- CIM Classes: Win32_PerfRawData_PerfProc_Process, Win32_Processor
- CIM Fields: Frequency_PerfTime, Timestamp_PerfTime, PercentProcessorTime

Total Processor Time

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: PercentProcessorTime

Memory Utilization

Memory Utilization requires a calculation involving data from several CIM Classes and Fields.

- CIM Classes: Win32_PerfRawData_PerfProc_Process, Win32_PhysicalMemory
- CIM Fields: WorkingSet, Capacity

Virtual Memory Size

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: VirtualBytes

Working Set Size

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: WorkingSet

Swap Size

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: PageFileBytes

Page Faults

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: PageFaultsPersec

Data Read

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: IOReadBytesPersec

Data Written

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: IOWriteBytesPersec

Data Other

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: IOOtherBytesPersec

Read Operations

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: IOReadOperationsPersec

Write Operations

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: IOWriteOperationsPersec

Other Operations

- CIM Class: Win32_PerfRawData_PerfProc_Process
- CIM Field: IOOtherOperationsPersec

Linux

For process information on a Linux machine, data exposed by remotely executing the PS Command is used. The following explains what data is used to provide process information.

Process Name

The PS Command Output from requesting the "comm" field is used as the process name. This contains the executable name only. No command line modifications are included.

Process ID (PID)

The PS Command Output from requesting the "pid" field is used as the Process ID or PID.

Parent Process ID (PPID)

The PS Command Output from requesting the "ppid" field is used as the Parent Process ID or PPID.

Processor Utilization (%)

The CPU utilization of this process is obtained by a calculation involving the PS Command Output from requesting the "cputime" and "etime" fields. The calculation involves taking two samples of data. The process CPU utilization will only be available after a second sample is taken.

Total Processor Time

The PS Command Output from requesting the field "cputime" is used as the amount of time the process has consumed the CPU.

Memory Utilization

The PS Command Output from requesting the field "%mem" is used as the percentage of physical system memory being consumed by the process.

Working Set Size

The PS Command Output from requesting the field "rss" is used as the amount of physical memory currently being consumed by the process. This is referred to as the working set size of the process.

Virtual Memory Size

The PS Command Output from requesting the field "vsize" is used as the virtual memory size of the process.

Swap Size

The PS Command Output from requesting the field "size" is used as the swap size of the process.

Solaris

For process information on a Solaris machine, data exposed by remotely executing the PS Command is used. The following explains what data is used to provide process information.

Process Name

The PS Command Output from requesting the "comm" field is used as the process name. This contains the executable name only. No command line modifications are included.

Process ID (PID)

The PS Command Output from requesting the "pid" field is used as the Process ID or PID.

Parent Process ID (PPID)

The PS Command Output from requesting the "ppid" field is used as the Parent Process ID or PPID.

Processor Utilization (%)

The CPU utilization of this process is obtained by a calculation involving the PS Command Output from requesting the "cputime" and "etime" fields. The calculation

involves taking two samples of data. The process CPU utilization will only be available after a second sample is taken.

Total Processor Time

The PS Command Output from requesting the field "cputime" is used as the amount of time the process has consumed the CPU.

Memory Utilization

The PS Command Output from requesting the field "pmem" is used as the percentage of physical system memory being consumed by the process.

Working Set Size

The PS Command Output from requesting the field "rss" is used as the amount of physical memory currently being consumed by the process. This is referred to as the working set size of the process.

Virtual Memory Size

The PS Command Output from requesting the field "vsz" is used as the virtual memory size of the process.

Troubleshooting the Cartridge for Guest Process Investigation

The following provides a list of questions you may have when using the Cartridge for Guest Process Investigation.

Why did I get a message saying "Error - Missing Input" after clicking the Save button in the Configuration Settings dialog box?

This message is a result of one or more missing values in the Configuration Settings dialog box. Check the following fields to ensure you have entered a correct value:

- Sample Interval
- Host Name (this field fills in automatically)
- Username

- Password
- Operating System

Why did I get a message saying "Error: Invalid Agent" after clicking the Save button in the Configuration Settings dialog box?

This message is a result of the server not finding the Agent selected under Advanced Options. Try selecting a different Agent.

Why did I get a message saying "Error: No Agent Provided" after clicking the Save button in the configuration settings dialog box?

This message is a result of no Agent being selected under Advanced Options. Normally, an agent is selected for you. If you did not deselect the agent, it is possible there are no agents currently available. Consult the *Guest Process Investigation User Guide* to ensure you have followed all required steps to deploy a Guest Process Investigation agent.

Why is the Save button disabled on the Configuration Settings dialog box?

The save button is disabled if any of the fields have not been provided. Complete all the fields and try again.

I have saved my configuration settings, and the Enable Process Collection checkbox is checked, but I still do not see any data. What is wrong?

If it has been longer than sixty seconds since saving the configuration settings and you do not see any data, check the following:

- a Ensure one or more processes in the process list at the bottom of the dashboard are checked. Only checked processes will be shown in the CPU and memory graphs.
- b This cartridge is not able to test the saved configuration immediately after it is entered. Open the Configuration Settings dialog box and verify that all information is correct.
- c It is possible that the DNS name did not resolve during the configuration process. To collect process information for this hosts, use the manual configuration process. For more information, see "[Manual Configuration of Guest Process Agents Using the Administration Dashboards](#)" on page 30.

I have saved my configuration settings, but the Enable Process Collection checkbox is disabled and I do not see any data. What is wrong?

The configuration could not be saved. You should see a popup after clicking the Save button with a message. If this message indicated that an error occurred, search this troubleshooting section for information regarding the specific error you encountered.

Index

A

about vFoglight 8

Authentication

Encrypted Basic Authentication via HTTPS 27

Unencrypted Basic Authentication 27

C

cartridge 10

Cartridge for Guest Process Investigation

Monitoring Virtual Machines 17

contacting Quest 12

core 9

D

documentation 8, 9, 10

F

feedback 10

G

Guest Process

%CPU Values in Foglight 48

Understanding the Concept 16

I

Installation Steps

Installing and Configuring WinRM 26

M

Manual Configuration of Guest Process Agents 30

N

Navigating in vFoglight

Alarms and their Status Indicators 23

Mouse-over Actions 23

Sortable List 22

Time Range 21

Navigation in vFoglight

vFoglight GUI Panels 20

O

Overview

Cartridge for Guest Process Investigation 16

P

Process Information Data Sources

Linux

Memory Utilization 57

Parent Process ID (PPID) 57

Process ID (PID) 57

Process Name 57

Processor Utilization (%) 57

Swap Size 58

Total Processor Time 57

Virtual Memory Size 58

Working Set Size 58

Solaris

Memory Utilization 59

Parent Process ID (PPID) 58

Process ID (PID) 58

Process Name 58

Processor Utilization (%) 58

Total Processor Time 59

Virtual Memory Size 59

Windows

<i>Data Other</i>	56	Configuration	26
<i>Data Read</i>	56	Downloading WinRM	26
<i>Data Written</i>	56	Installation and Configuring WinRM with the Cartridge	
<i>Memory Utilization</i>	55	for Guest Process Investigation	26
<i>Other Operations</i>	56	Listening for Remote Connection	26
<i>Page Faults</i>	56		
<i>Parent Process ID</i>	55		
<i>Process ID</i>	54		
<i>Process Name</i>	54		
<i>Processor Utilization (%)</i>	55		
<i>Read Operations</i>	56		
<i>Swap Size</i>	56		
<i>Total Processor Time</i>	55		
<i>Virtual Memory Size</i>	55		
<i>Working Set Size</i>	55		
<i>Write Operations</i>	56		

S

suite 8
support 12

T

technical support 12
text conventions 11

Troubleshooting

Invalid Agent 60
Missing Input 59
No Agent Provided 60
Not seeing data 60
Not seeing data after saving configuration settings 61

V

vFoglight GUI Panels

Actions Panel 21
Display Panel 21
Navigation Panel 20

W

WinRM