vFoglight™ **5.2.4**

Administration and Configuration Guide

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, vRanger 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

Administration and Configuration Guide
March 2009
Version 5.2.4

Table of Contents

Introduction to this Guide

This chapter provides information about what is contained in the *vFoglight Administration and Configuration Guide*. It also provides information about the vFoglight documentation suite and Vizioncore.

This chapter contains the following sections:

About vFoglight

vFoglight helps IT organizations understand the virtual infrastructure by managing the relationships and interaction between all the components in the environment, including data centers, data stores, clusters, resource pools, hosts and virtual machines. With vFoglight, administrators can quickly determine the root-cause of an incident or problem, track virtual machine (VM) movements and understand their impact, and identify contention for resources between virtual machines.

About this Guide

This Administration and Configuration Guide provides conceptual information about vFoglight administration components, configuration instructions, and instructions on how to use the dashboards in the Administration module.

This guide is intended for vFoglight System Administrators to administer and configure vFoglight.

The Administration and Configuration Guide is organized as follows:

Chapter 1, About the Administration Module—Discusses core vFoglight concepts, introduces the Administration module (a getting started approach), and lists common administration tasks. It also lists the nodes that appear in the Administration module and describes the type of tasks you can perform using the dashboards that appear under each node: Agents, Cartridges, Data, Rules & Notifications, Schedules, Setup & Support, Tooling, and Users & Security. Read this chapter to learn about vFoglight models and scope, access the vFoglight Administration module, and find out what type of administration tasks you can perform in vFoglight.

Chapter 2, Setting Up vFoglight—Includes information about vFoglight licenses and support bundles, audit logs, and configuration items, and how to use them. Read this chapter to find out how to gather vFoglight diagnostic data during run-time, view port numbers that are used by vFoglight, or manage and install vFoglight licenses or support bundles using the Setup & Support dashboards.

Chapter 3, Managing Users and Security—Explains the security concepts and their entities used in vFoglight such as users, groups, and roles. It contains step-by-step instructions on how to use these entities in order to effectively manage security in vFoglight using the Users & Security dashboards.

Chapter 4, Managing Cartridges—Contains information on how to install and manage cartridges, and download agent packages. Use this chapter to learn about

cartridge-related concepts in vFoglight and to find out how to install and manage cartridges using the Cartridges dashboards.

Chapter 5, Managing Agents—Includes conceptual and hands-on information about collection agents and explains their purpose in vFoglight. It contains instructions on how to edit agent properties when required using the Agents dashboards.

Chapter 6, Working with Rules and Registry—Discusses the concepts of rules and registry variables and their relations with the topology model in vFoglight. It includes step-by-step instructions on how to efficiently create, edit, and manage vFoglight rules and registry variables using the Rules & Registry dashboards. It also contains several real-life examples that can help you understand their usage.

Chapter 7, Using Schedules—Explains the concept of schedules in vFoglight and their usage in rules, agent blackouts, and derived metrics. It contains instructions on how to create and manage schedules to their best potential using the Schedules dashboards.

Chapter 8, Working with Data—Provides conceptual information about the topology model, collected metrics, and their data types. Additionally, it instructs you how to add custom data types to the topology model, create derived metrics, assign threshold levels to metrics, and manage the periods of time in which vFoglight samples or purges data, using the Data dashboards.

Chapter 9, Building Script Agents—Provides insight into advanced administration tasks such as building custom agents or using queries to retrieving data from the data model. It contains detailed instructions on how to upload agent scripts, build and deploy and script agents, and to drill through topology to retrieve data using the vFoglight query language, all using the Tooling dashboards.

Chapter 10, Using the Query Language—Discusses the vFoglight query language contains instructions on how to use it. vFoglight uses a query language to set the scope for rules and derived metrics, to create rule conditions and expressions, to reference expressions in messages, and to create derived metric expressions.

Appendix A, vFoglight Client Reference—Contains examples of dashboards and command-line output in environments that use the vFoglight Client for agent communication and management.

vFoglight Documentation Suite

The vFoglight documentation suite is made up of the core documentation set, plus the documentation set for each vFoglight cartridge that you deploy. Documentation is provided in a combination of online help, PDF and HTML.

- **Online Help:** You can open the online help by selecting the Help tab from vFoglight's action panel.
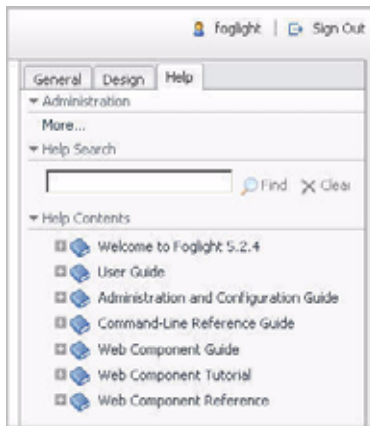
- **PDF:** The *Getting Started Guide*, *What's New Guide*, *System Requirements and Platform Support Guide*, *Installation and Setup Guide* set, *Administration and Configuration Guide*, *vFoglight User Guide*, *Command-Line Reference Guide*, *Web Component Guide*, and *Web Component Tutorial*, are provided as PDF files. The PDF guides are included in the zip file downloaded from Vizioncore. Adobe® Reader® is required.

- **HTML:** Release Notes are provided in HTML.

Core Documentation Set

The core documentation set consists of the following files:

- *Release Notes* (HTML)
- *Getting Started Guide* (PDF)
- *What's New Guide* (PDF)
- *System Requirements and Platform Support Guide* (PDF)

- *Installation and Setup Guide* set (all in PDF format):
  - Installation and Setup Guide—*Installing on Windows with an Embedded MySQL Database*
  - Installation and Setup Guide—*Installing on Windows with an External MySQL Database*
  - Installation and Setup Guide—*Installing on Windows with an External Oracle Database*
- *Administration and Configuration Guide* (PDF and online help)
- *vFoglight User Guide* (PDF and online help)
- *Advanced Configuration Guide* set
  - *Command-Line Reference Guide* (PDF and online help)
  - *Web Component Guide* (PDF and online help)
  - *Web Component Tutorial* (PDF and online help)
  - *Web Component Reference* (online help)

Cartridge Documentation Sets

When you deploy a cartridge, the documentation set for the cartridge is installed. The online help for the cartridge is integrated automatically with the core vFoglight help. When you open the help, the name of the cartridge is displayed in a top level entry within the table of contents.

Some cartridges include additional PDF guides, which may be one or more of the following: a *Getting Started Guide*, an *Installation Guide*, a *User Guide*, and a *Reference Guide*.

Feedback on the Documentation

We are interested in receiving feedback from you about our documentation. For example, did you notice any errors in the documentation? Were any features undocumented? Do you have any suggestions on how we can improve the documentation? All comments are welcome. Please submit your feedback to the following email address:

info@vizioncore.com

Please do not submit Technical Support related issues to this email address.

Text Conventions

The following table summarizes how text styles are used in this guide:

Convention	Description
`Code`	Monospace text represents code, code objects, and command-line input. This includes: • Java language source code and examples of file contents • Classes, objects, methods, properties, constants, and events • HTML documents, tags, and attributes
Variables	Monospace-plus-italic text represents variable code or command-line objects that are replaced by an actual value or parameter.
Interface	Bold text is used for interface options that you select (such as menu items) as well as keyboard commands.
Files, components, and documents	Italic text is used to highlight the following items: • Pathnames, file names, and programs • The names of other documents referenced in this guide

About Vizioncore Inc.

Vizioncore was formed in July 2002 as a consulting and software-development company with the mission to create easy-to-use software solutions that performed reliable and repeatable automation of datacenter functions specifically for the Citrix platform. A main corporate goal was to enable business partners to offer solutions that targeted real-world IT issues and provided the best possible installation and automation for their clients' systems.

Vizioncore's solutions have proved successful in organizations from small to mid-sized businesses to large enterprises, in a wide variety of vertical industries, including Financial Services, Government, Healthcare, Manufacturing, and High Tech. Vizioncore, Inc. can be found in offices around the globe and at www.vizioncore.com.

Contacting Dell

Note: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1   Visit http://support.dell.com.

2   Verify your country or region in the Choose A Country/Region drop-down menu at the bottom of the page.

3   Click Contact Us on the left side of the page.Note: Toll-free numbers are for use within the country for which they are listed.

4   Select the appropriate service or support link based on your need.

5   Choose the method of contacting Dell that is convenient for you.

Country (City) International Access Code Country Code City Code	Service Type	Area Codes, Local Numbers, and Toll-Free Numbers Web and E-Mail Addresses
Anguilla	Web Address	www.Dell.com/ai
	E-Mail Address	la-techsupport@dell.com
	Technical Support., Customer Service, Sales	toll-free: 800-335-0031
Antigua and Barbuda	Web Address	www.Dell.com.ag
	E-Mail Address	la-techsupport@dell.com
	Technical Support., Customer Service, Sales	1-800-805-5924
Aomen	Technical Support	
	Dell™ Dimension™, Dell Inspirion™, Dell	0800-105
	Optiplex™, Dell Lattitude™, and Dell	
	Precision™Servers and Storage	0800-105
Argentina (Buenos Aires) International Access Code: 00 Country Code: 54 City Code: 11	Web Address	www.dell.com.ar
	E-Mail Address for Desktop/ Portable Computers	la-techsupport@dell.com
	E-Mail Address for Servers and EMC® Storage Products	la_enterprise@dell.com toll-free: 0-800-444-0730
	Customer Service	
	Technical Support	toll-free: 0-800-444-0733
	Technical Support Services	toll-free: 0-800-444-0724
	Sales	0-800-444-3355
Aruba	Web Address	www.Dell.com/aw
	E-Mail Address	la-techsupport@dell.com
	Technical Support., Customer Service, Sales	toll-free: 800-1578
Australia (Sydney) International Access Code: 0011 Country Code: 61 City Code: 2	Web Address	support.ap.dell.com
	Contact Dell Web Address	support.ap.dell.com/contactus
	Technical Support., Customer Service, Sales	13DELL-133355

Austria (Vienna) International Access Code: 900 Country Code: 43 City Code: 1	Web Address	Support.euro.dell.com
	E-Mail Address	Tech_support_central_europe@dell.com
	Home/Small Business Sales	0820 240 530 00
	Home/Small Business Fax	0820 240 530 49
	Home/Small Business Customer Service	0820 240 530 14
	Home/Small Business Support	0820 240 530 17
	Preferred Accounts/Corporate Customer	0820 240 530 16
	Service Preferred Accounts/Corporate Customer	0820 240 530 17
	Switchboard	0820 240 530 00
Bahamas	Web Address	www.dell.com/bs
	E-Mail Address	la-techsupport@dell.com
	Technical Support., Customer Service, Sales	toll-free: 1-866-874-3038
Barbados	Web Address	www.dell.com/bb
	E-Mail Address	la-techsupport@dell.com
	Technical Support., Customer Service, Sales	1-800-534-3142
Belgium (Brussels)	Web Address	Support.euro.dell.com
	General Support	02 481 92 88
	General Support Fax	02 481 92 95
	Customer Service	02 713 15 65
	Corporate Sales	02 481 91 00
	Fax	02 481 91 99
	Switchboard	02 481 91 00
Bolivia	Web Address	www.dell.com/bo
	E-Mail Address	la_techsupport@dell.com
	Technical Support., Customer Service, Sales	toll-free: 800-10-0238
Brazil International Access Code: 00 Country Code: 55 City Code: 51	Web Address	www.dell.com/br
	E-Mail Address	BR_TechSupport@dell.com
	Customer Service and Tech Support	0800 970 3355
	Technical Support Fax	51 2104 5470
	Customer Service Fax	51 2104 5480
	Sales	0800 722 3498
British Virgin Islands	Technical Support, Customer Service, Sales	toll-free: 1-866-278-6820
Brunei Country Code: 673	Technical Support (Penang, Malaysia)	604 633 4966
	Customer Service (Penang, Malaysia)	604 633 4888
	Transaction Sales (Penang, Malaysia)	604 633 4955
Canada (North York, Ontario) International Access Code: 011	Online Order Status Web Address	www.dell.ca/ostatus
	AutoTech (automated Hardware and Warranty Support)	support.ca.dell.com
	Customer Service	toll-free:1-800-247-9362
	Home/Home Office	toll-free:1-800-847-4096
	Small Business	toll-free:1-800-906-3355
	Medium/Large Business, Government, Education	toll-free:1-800-387-5757
	Hardware Warranty Phone Support	
	Computers for Home/Home Office	toll-free:1-800-847-4096
	Computers for Small/Medium/Large Business Government	toll-free:1-800-387-5757
	Printers, Projectors, Televisions, Handheld, Digital	1-877-335-5767
	Jukebox, and Wireless Sales	toll-free:1-800-999-3355
	Home and Home Office Sales	toll-free:1-800-387-5752
	Small Business	toll-free:1-800-387-5755
	Medium/Large Business, Government	1 866 440 3355
	Spare Parts and Extended Service	
Cayman Islands	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	1-877-262-5415

Chile (Santiago)	Web Address	www.dell.com/cl
Country Code: 56	E-Mail Address	la-techsupport@dell.com
City Code: 2	Sales and Customer Support	toll-free: 1230-020-4823
China (Xiamen)	Technical Support Web Address	support.dell.com.cn
Country Code: 86	Technical Support E-Mail Address	support.dell.com.cn/email
City Code: 592	Customer Service E-Mail Address	customer_cn@dell.com
	Technical Support Fax	592 818 14350
	Technical Support – Dimension and Inspiron	toll-free: 800 858 2969
	Technical Support – OptiPlex, Lattitude and Dell Precision	toll-free: 800 858 0950
	Technical Support – Servers and Storage	toll-free: 800 858 0960
	Technical Support – Projectors, PDAs, Switches, Routers, etc	toll-free: 800 858 2920
	Technical Support – Printers	toll-free: 800 858 2311
	Customer Service	toll-free: 800 858 2060
	Customer Service Fax	592 818 1308
	Home and Small Business	toll-free: 800 858 2222
	Preferred Accounts Division	toll-free: 800 858 2557
	Large Corporate Accounts GCP	toll-free: 800 858 2055
	Large Corporate Accounts Key Accounts	toll-free: 800 858 2628
	Large Corporate Accounts North	toll-free: 800 858 2999
	Large Corporate Accounts North Government and Education	toll-free: 800 858 2955
	Large Corporate Accounts East	toll-free: 800 858 2020
	Large Corporate Accounts East Government and Education	toll-free: 800 858 2669
	Large Corporate Accounts Queue Team	toll-free: 800 858 2572
	Large Corporate Accounts South	toll-free: 800 858 2355
	Large Corporate Accounts West	toll-free: 800 858 2811
	Large Corporate Accounts Spare Parts	toll-free: 800 858 2621
Columbia	Web Address	www.dell.com/co
	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	01-800-915-4755
Costa Rica	Web Address	www.dell.com/cr
	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	0800-012-0231
Czech Republic (Prague)	Web Address	support.euro.dell.com
International Access Code: 00	E-Mail Address	czech_dell@dell.com
Country Code: 420	Technical Support	22537 2727
	Customer Service	22537 2707
	Fax	22537 2714
	Technical Fax	22537 2728
	Switchboard	22537 2711
Denmark (Copenhagen)	Web Address	Support.euro.dell.com
International Access Code: 00	Technical Support	7023 0182
Country Code: 45	Customer Service – Relational	7023 0184
	Home/Small Business Customer Service	3287 5505
	Switchboard – Relational	3287 1200
	Switchboard Fax – Relational	3287 1201
	Switchboard – Home/Small Business	3287 5000
	Switchboard Fax – Home/Small Business	3287 5001
Dominica	Web Address	www.dell.com/dm
	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-866-278-6821

Dominican Republic	Web Address	www.dell.com/do
	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	1-800-156-1588
Ecuador	Web Address	www.dell.com/ec
	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales (Calling from Quito)	toll-free: 999-119-877-655-3355
	Technical Support, Customer Service, Sales (Calling from Guayaquil)	toll-free: 1800-999-119-877-655-3355
El Salvador	Web Address	www.dell.com/sv
	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	800-6132
Finland (Helsinki) International Access Code: 990 Country Code: 358 City Code: 9	Web Address	support@euro.dell.com
	E-Mail Address	fi_support@dell.com
	Technical Support	0207 533 555
	Customer Service	0207 533 538
	Switchboard	0207 533 533
	Sales under 500 employees	0207 533 540
	Fax	0207 533 530
	Sales over 500 employees	0207 533 533
	Fax	0207 533 530
France (Paris) (Montpellier) International Access Code: 00 Country Code: 33 City Codes: (1) (4)	Web Address	Support.euro.dell.com
	Home and Small Business	
	Technical Support	0825 387 270
	Customer Service	0825 832 833
	Switchboard	0825 004 700
	Switchboard (calls from outside of France)	04 99 75 40 00
	Sales	0825 004 700
	Fax	0825 004 701
	Fax (calls from outside of France)	04 99 75 40 01
	Corporate	
	Technical Support	0825 004 719
	Customer Service	0825 338 339
	Switchboard	55 94 71 00
	Sales	01 55 94 71 00
Germany (Frankfurt) International Access Code: 00 Country Code: 49 City Code: 69	Web Address	support.euro.dell.com
	E-mail Address	tech_support_central_europe@dell.com
	Technical Support	069 9792-7200
	Home/Small Business Customer Service	0180-5-224400
	Global Segment Customer Service	069 9792-7320
	Preferred Accounts Customer Service	069 9792-7320
	Large Accounts Customer Service	069 9792-7320
	Public Accounts Customer Service	069 9792-7320
	Switchboard	069 9792-7000
Greece International Access Code: 00 Country Code: 49	Web Address	Support.euro.dell.com
	Technical Support	00800-44 14 95 18
	Gold Service Technical Support	00800-44 14 00 83
	Switchboard	2108129810
	Gold Service Switchboard	2108129811
	Sales	2108129800
	Fax	2108129812
Grenada	Web Address	www.dell.com/gd
	E-Mail Address	la-techsuppo@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-866-540-3355

Guatemala	Web Address	www.dell.com/gt
	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	1-800-999-0136
Guyana	E-Mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-877-270-4609
Hong Kong International Access Code: 001 Country Code: 852	Web Address	support.ap.dell.com
	Technical Support E-mail Address	support.dell.com.cn/email
	Technical Support - Dimension and Inspiron	00852-2969 3188
	Technical Support - OptiPlex, Latitude, and Dell Precision	00852-2969 3191
	Technical Support - Servers and Storage	00852-2969 3196
	Technical Support - Projectors, PDAs, Switches, Routers, etc .	00852-3416 0906
	Customer Service	00852-3416 0910
	Large Corporate Accounts	00852-3416 0907
	Global Customer Programs	00852-3416 0908
	Medium Business Division	00852-3416 0912
	Home and Small Business Division	00852-2969 3105
India	Dell Support Website	support.ap.dell.com
	Portable and Desktop Support	
	Desktop Support E-mail Address	india_support_desktop@dell.com
	Portable Support E-mail Address	india_support_notebook@dell.com
	Phone Numbers	080-25068032 or 080-25068034 or your city STD code + 60003355 or toll-free: 1-800-425-8045
	Server Support	
	E-mail Address	india_support_Server@dell.com
	Phone Numbers	080-25068032 or 080-25068034 or your city STD code + 60003355 or toll-free: 1-800-425-8045
	Gold Support Only	
	E-mail Address	eec_ap@dell.com
	Phone Numbers	080-25068033 or your city STD code + 60003355 or toll-free: 1-800-425-9045
	Customer Service	
	Home and Small Business	India_care_HSB@dell.com toll-free : 1800-4254051
	Large Corporate Accounts	India_care_REL@dell.com toll free : 1800-4252067
	Sales	
	Large Corporate Accounts	1600 33 8044
	Home and Small Business	1600 33 8046

Ireland (Cherrywood)	Web Address	Support.euro.dell.com
International Access Code: 00 Country Code: 353 City Code: 1	**Technical Support**	
	E-mail Address	dell_direct_support@dell.com
	Business computers	1850 543 543
	Home computers	1850 543 543
	At Home Support	1850 200 889
	Sales	
	Home	1850 333 200
	Small Business	1850 664 656
	Medium Business	1850 200 646
	Large Business	1850 200 646
	E-mail Address	Dell_IRL_Outlet@dell.com
	Customer Service	
	Home and Small Business	204 4014
	Business (greater than 200 employees)	1850 200 982
	General	
	Fax/Sales fax	204 0103
	Switchboard	204 4444
	U.K. Customer Service (dealing with U.K.only)	0870 906 0010
	Corporate Customer Service (dial within U.K. only)	0870 907 4499
	U.K. Sales (dial within U.K. only)	0870 907 4000
Italy (Milan)	Web Address	Support.euro.dell.com
International Access Code: 00 Country Code: 39 City Code: 02	**Home and Small Business**	
	Technical Support	02 577 826 90
	Customer Service	02 696 821 14
	Fax	02 696 821 13
	Switchboard	02 696 821 12
	Corporate	
	Technical Support	02 577 826 90
	Customer Service	02 577 825 55
	Fax	02 575 035 30
	Switchboard	02 577 821
Jamaica	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales (dial from within Jamaica only)	1-800-440-920

Japan (Kawasaki)	Web Address	support.jp.dell.com
International Access Code: 001 Country Code: 81 City Code: 44	Technical Support - Dimension and Inspiron	toll-free: 0120-198-26
	Technical Support outside of Japan - Dimension and Inspiron	81-44-520-1435
	Technical Support - Dell Precision, OptiPlex, and Latitude	toll-free: 0120-198-433
	Technical Support outside of Japan - Dell Precision, OptiPlex, and Latitude	81-44-556-3894
	Technical Support - Dell PowerApp™, Dell PowerEdge™, Dell PowerConnect™, and Dell PowerVault™,	toll-free: 0120-198-498
	Technical Support outside of Japan - PowerApp, PowerEdge, PowerConnect, and PowerVault	81-44-556-4162
	Technical Support - Projectors, PDAs, Printers, Routers	toll-free: 0120-981-690
	Technical Support outside of Japan - Projectors, PDAs, Printers, Routers	81-44-556-3468
	Faxbox Service	044-556-3490
	24-Hour Automated Order Status Service	044-556-3801
	Customer Service	044-556-4240
	Business Sales Division - up to 400 employees	044-556-1465
	Preferred Accounts Division Sales - over 400 employees	044-556-3433
	Public Sales - government agencies, educational institutions, and medical institutions	044-556-5963
	Global Segment Japan	044-556-3469
	Individual User	044-556-1657
	Individual User Online Sales	044-556-2203
	Individual User Real Site Sales	044-556-4649
	Switchboard	044-556-4300
Korea (Seoul)	Web Address	Support.ap.dell.com
International Access Code: 001 Country Code: 82 City Code: 2	Technical Support, Customer Service	toll-free: 080-200-3800
	Technical Support - Dimension, PDA, Electronics, and Accessories	toll-free: 080-200-3801
	Sales	toll-free: 080-200-3600
	Fax	2194-6202
	Switchboard	2194-6000
Latin America	Customer Technical Support (Austin, Texas, U.S.A.)	512 728-4093
	Customer Service (Austin, Texas, U.S.A.)	512 728-3619
	Fax (Technical Support and Customer Service) (Austin, Texas, U.S.A.)	512 728-3883
	Sales (Austin, Texas, U.S.A.)	512 728-4397
	SalesFax (Austin, Texas, U.S.A.)	512 728-4600 or 512 728-3772
Luxemborg	Web Address	Support.euro.dell.com
International Access Code: 00 Country Code: 352	Support	3420808075
	Home/Small Business Sales	+32 (0)2 713 15 96
	Corporate Sales	26 25 77 81
	Customer Service	+32 (0)2 481 91 19
	Fax	26 25 77 82
Macao	Technical Support	toll-free: 0800 105
Country Code: 83	Customer Service (Xiamen, China)	34 160 910
	Transaction Sales (Xiamen, China)	29 693 115

Malaysia (Penang) International Access Code: 00 Country Code: 60 City Code: 4	Web Address	Support.ap.dell.com
	Technical Support - Dell Precision, OptiPlex, and Latitude	toll-free: 1800 880 193
	Technical Support - Dimension, Inspiron, and Electronics and Accessories	toll-free: 1800 881 306
	Technical Support - PowerApp, PowerEdge, PowerConnect, and PowerVault	toll-free: 1800 881 386
	Customer Service	toll-free: 1800 881 306 (option 6)
	Transaction Sales	toll-free: 1800 888 202
	Corporate Sales	toll-free: 1800 888 213
Mexico International Access Code: 00 Country Code: 52	Web Address	www.dell.com/mx
	E-mail Address	la-techsupport@dell.com
	Customer Technical Support	001-877-384-8979 or 001-877-269-3383
	Sales	50-81-8800 or 01-800-888-3355
	Customer Service	001-877-384-8979 or 001-877-269-3383
	Main	50-81-8800 or 01-800-888-3355
Montserrat	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	Toll-free: 1-866-278-6822
Netherlands Antilles Netherlands (Amsterdam) International Access Code: 00 Country Code: 31 City Code: 20	E-mail Address	la-techsupport@dell.com
	Web Address	support.euro.dell.com
	Technical Support	020 674 45 00
	Technical Support Fax	020 674 47 66
	Home/Small Business Customer Service	020 674 42 00
	Relational Customer Service	020 674 43 25
	Home/Small Business Sales	020 674 55 00
	Relational Sales	020 674 50 00
	Home/Small Business Sales Fax	020 674 47 75
	Relational Sales Fax	020 674 47 50
	Switchboard	020 674 50 00
	Switchboard Fax	020 674 47 50
New Zealand International Access Code: 00 Country Code: 64	Web Address	Support.ap.dell.com
	E-mail Address	Support.ap.dell.com/contactus
	Technical Support, Customer Service, Sales	0800 441 567
Nicaragua	Web Address	www.dell.com/ni
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	001-800-220-1377
Norway (Lysaker) International Access Code: 00 Country Code: 47	Web Address	Support.euro.dell.com
	Technical Support	671 16882
	Relational Customer Service	671 17575
	Home/Small Business Customer Service	231 62298
	Switchboard	671 16800
	Fax Switchboard	671 16865
Panama	Web Address	www.dell.com/pa
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	011-800-507-1264
Peru	Web Address	www.dell.com/pe
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	0800-50-669

Poland (Warsaw) International Access Code: 011 Country Code: 48 City Code: 22	Web Address	support.euro.dell.com
	E-mail Address	pl_support_tech@dell.com
	Customer Service Phone	57 95 700
	Customer Service	57 95 999
	Sales	57 95 999
	Customer Service Fax	57 95 806
	Reception Desk Fax	57 95 998
	Switchboard	57 95 999
Portugal International Access Code: 00 Country Code: 351	Web Address	Support.euro.dell.com
	Technical Support	707200149
	Customer Service	800 300 413
	Sales	800-300-410 or 800-300 -411 or 800-300-412 or 21-422-07-10
	Fax	21-424-01-12
Puerto Rico	Web Address	www.dell.com/pr
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	1-877-537-3355
St. Kitts and Nevis	Web Address	www.dell.com/kn
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-866-540-3355
St. Lucia	Web Address	www.dell.com/lc
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-866-464-4352
St. Vincent and the Grenadines	Web Address	www.dell.com/vc
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-866-464-4353
Singapore International Access Code: 005 Country Code: 65	NOTE: The phone numbers in this section should be called from within Singapore or Malaysia only.	
	Web Address	support.ap.dell.com
	Technical Support - Dimension, Inspiron, and Electronics and Accessories	toll-free: 1 800 394 7430
	Technical Support - OptiPlex, Latitude, and Dell Precision	toll-free: 1 800 394 7488
	Technical Support - PowerApp, PowerEdge, PowerConnect, and PowerVault	toll-free: 1 800 394 7478
	Customer Service	toll-free: 1 800 394 7430 (option 6)
	Transaction Sales	toll-free: 1 800 394 7412
	Corporate Sales	toll-free: 1 800 394 7419
Slovakia (Prague) International Access Code: 00 Country Code: 421	Web Address	support.euro.dell.com
	E-mail Address	czech_dell@dell.com
	Technical Support	02 5441 5727
	Customer Service	420 22537 2707
	Fax	02 5441 8328
	Tech Fax	02 5441 8328
	Switchboard (Sales)	02 5441 8328 02 5441 7585
South Africa (Johannesburg) International Access Code: 09/091 Country Code: 27 City Code: 11	Web Address	support.euro.dell.com
	E-mail Address	dell_za_suppor@dell.com
	Gold Queue	011 709 7713
	Technical Support	011 709 7710
	Customer Service	011 709 7707
	Sales	011 709 7700

Spain (Madrid)	Web Address	Support.euro.com
International Access Code: 00 **Country Code: 34** **City Code: 91**	Home and Small Business	
	Technical Support	902 100 130
	Customer Service	902 118 540
	Sales	902 118 541
	Switchboard	902 118 541
	Fax	902 118 539
	Corporate	
	Technical Support	902 100 130
	Customer Service	902 115 236
	Switchboard	91 722 92 00
	Fax	91 722 95 83
Sweden (Upplands Vasby)	Web Address	support.euro.dell.com
	Technical Support	08 590 05 199
International Access Code: 00 **Country Code: 46** **City Code: 8**	Relational Customer Service	08 590 05 642
	Home/Small Business Customer Service	08 587 70 527
	Employee Purchase Program (EPP) Support	020 140 14 44
	Technical Support Fax	08 590 05 594
Switzerland (Geneva)	Web Address	Support.euro.dell.com
	E-mail Address	Tech_support_central_Europe@dell.com
International Access Code: 00 **Country Code: 41** **City Code: 22**	Technical Support – Home and Small Business	0844 811 411
	Technical Support – Corporate	0844 822 844
	Customer Service – Home and Small Business	0848 802 202
	Customer Service – Corporate	0848 821 721
	Fax	022 799 01 90
	Switchboard	022 799 01 01
Taiwan	Web Address	support.ap.dell.com
	E-mail Address	support.dell.com.cn/email
International Access Code: 002 **Country Code: 886**	Technical Support - OptiPlex, Latitude, Inspiron, Dimension, and Electronics and Accessories	toll-free: 0080 186 1011
	Technical Support - Servers and Storage	toll-free: 0080 160 1256
	Customer Service	toll-free: 0080 160 1250 (option 5)
	Transaction Sales	toll-free: 0080 165 1228
	Corporate Sales	toll-free: 0080 165 1227
Thailand	Web Address	Support.ap.dell.com
	Technical Support (OptiPlex, Latitude, and Dell Precision)	toll-free: 1800 0060 07
International Access Code: 001 **Country Code: 66**	Technical Support (PowerApp, PowerEdge, PowerConnect, and PowerVault)	toll-free: 1800 0600 09
	Customer Service	toll-free: 1800 006 007 (option 7)
	Corporate Sales	toll-free: 1800 006 009
	Transaction Sales	toll-free: 1800 006 006
Trinidad/Tobago	Web Address	www.dell.com/tt
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-888-799-5908
Turks and Caicos Islands	Web Address	www.dell.com/tc
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-877-441-4735

U.K.(Bracknell)	Web Address	upport.euro.dell.com
International Access Code: 00 Country Code: 44 City Code: 1344	E-mail Address	dell_direct_support@dell.com
	Customer Service Website	support.euro.dell.com/uk/en/ECare/ form/home.asp
	Sales	
	Home and Small Business Sales	0870 907 4000
	Corporate/Public Sector Sales	01344 860 456
	Customer Service	
	Home and Small Business	0870 906 0010
	Corporate	01344 373 185
	Preferred Accounts (500-5000 employees)	0870 906 0010
	Global Accounts	01344 373 186
	Central Government	01344 373 196
	Local Government & Education	01344 373 199
	Health	01344 373 194
	Technical Support	
	Corporate/Preferred Accounts/PCA (1000+ employees)	0870 908 0500
	Other Dell Products	0870 353 0800
	General	
	Home and Small Business Fax	0870 907 4006
Uruguay	Web Address	www.dell.com/uy
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 000-413-598-2521
U.S.A. (Austin, Texas)	Automated Order-Status Service	toll-free: 1-800-433-9014
International Access Code: 011 Country Code: 1	AutoTech (portable and desktop computers)	toll-free: 1-800-247-9362
	Hardware and Warranty Support (Dell TV, Printers, and Projectors) for Relationship customers	toll-free: 1-877-459-7298
	Consumer (Home and Home Office) Support for Dell products	toll-free: 1-800-624-9896
	Customer Service	toll-free: 1-800-624-9897
	Employee Purchase Program (EPP) Customers	toll-free: 1-800-695-8133
	Financial Services Web Address	www.dellfinancialservices.com
	Financial Services (lease/loans)	toll-free: 1-877-577-3355
	Financial Services (Dell Preferred Accounts [DPA])	toll-free: 1-800-283-2210
	Business	
	Customer Service	toll-free: 1-800-624-9897
	Employee Purchase Program (EPP)	toll-free: 1-800-695-8133
	Customer s Support for printers, projectors, PDAs, and MP3 players	toll-free: 1-877-459-7298
	Public (government, education, and healthcare)	
	Customer Service and Support	toll-free: 1-800-456-3355
	Employee Purchase Program (EPP) Customers	toll-free: 1-800-695-8133
	Dell Sales	toll-free: 1-800-289-3355 or toll-free: 1-800-879-3355
	Dell Outlet Store (Dell refurbished computers)	toll-free: 1-888-798-7561
	Software and Peripherals Sales	toll-free: 1-800-671-3355
	Spare Parts Sales	toll-free: 1-800-357-3355
	Extended Service and Warranty Sales	toll-free: 1-800-247-4618
	Fax	toll-free: 1-800-727-8320
	Dell Services for the Deaf, Hard-of-Hearing, or Speech-Impaired	toll-free: 1-877-DELLTTY (1-877-335-5889)

U.S. Virgin Islands	Web Address	www.dell.com/vi
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	toll-free: 1-877-702-4360
Venezuela	Web Address	www.dell.com/ve
	E-mail Address	la-techsupport@dell.com
	Technical Support, Customer Service, Sales	0800-100-4752

1

About the Administration Module

The Administration module allows you to manage vFoglight in a way that best implements your business logic. It offers a set of dashboards that allow you to manage vFoglight cartridges, agents, data, rules, and security.

This chapter contains the following section:

About Models and Scope in vFoglight

A model is a principle for organizing monitoring data that vFoglight gathers from host systems. vFoglight models have a tree-like structure that contains nodes. Each node in the model can have properties, metrics, alarms and other nodes associated with it. vFoglight adds these entities to the nodes in the data model as it collects them.

vFoglight can create different types of models. *Collection models* include raw data. *Virtual models* are built on top of other models. There are two types of virtual models: *aggregate models*, that do not require any additional configuration, and *user models*, that require user-based configuration. Depending on your monitoring needs and the type and range of vFoglight cartridges that you use for gathering data, your system includes one or more collection models. An example of a collection model is the Host Model illustrated above that collects information about host machines.

The following diagram illustrates a simplified version of the Host Model that vFoglight builds in a typical business scenario.
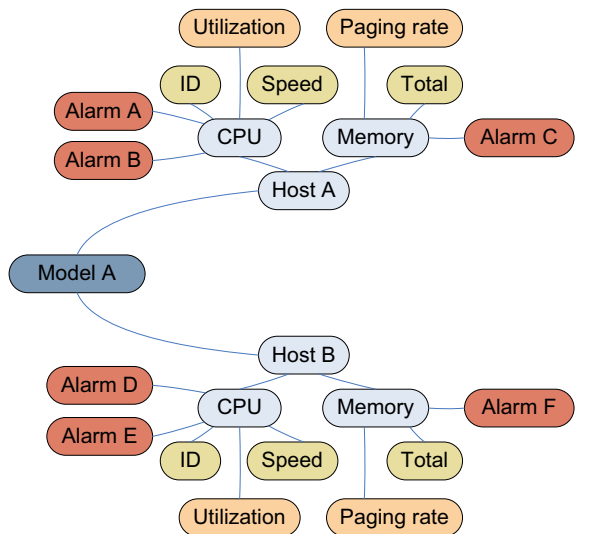
vFoglight makes use of a topology model to describe the logical and physical relationships between data nodes. Hierarchy in topology models provides the context for metrics and properties. vFoglight stores context information only once. The relationship between nodes, metrics, properties, and other nodes propagates the context across multiple data elements.

vFoglight stores metrics and properties next to one another. Unlike properties, that describe nodes and are typically static in nature, metrics change over time as vFoglight collects them. For example, in a host model, CPU ID is a property that describes a CPU node while CPU Utilization is a metric that can change between sampling periods. If the CPU ID changes, vFoglight adds a new node to the collection model with the new CPU ID and associates any collected metrics such as CPU Utilization with the newly-created node.

In vFoglight, the Data dashboards illustrate the collection model and the data nodes that vFoglight creates as it collects performance metrics from monitored hosts. The Data dashboard shows how nodes are organized and helps you identify paths to underlying objects that you can use in vFoglight queries and dashboards. Similar to directory paths, a path in the topology model traverses the collection model through a series of nodes, properties, metrics, and events that are separated by forward slashes '/'. For example, a path that retrieves the current average CPU utilization for a host can look like the following:

HostModel/hosts/<host_name>/cpus/processors/<processor>/utilization/current/ average

For complete information about the Data dashboard, see the *vFoglight User Guide.* For details on how to create dashboards, see the *Web Component Tutorial*.

vFoglight allows you to create rules and apply them to the data that you collect from multiple sources in your monitoring environment. Rules are scope-specific which means that they are associated with one or more topology types against which they run.

vFoglight uses cartridges to collect data from your virtual environment. It creates a dynamic data model while collecting data and uses that data to populate views and dashboards. The Administration Module allows you to manage vFoglight data collectors, topology and rules that implement your business logic. It also lets you manage security by granting user permissions to various vFoglight entities.

Getting Started with the Administration Module

Each vFoglight module contains a set of dashboards that you can configure and use to monitor your environment in real time. You can access them from the navigation pane on the left of the display area.
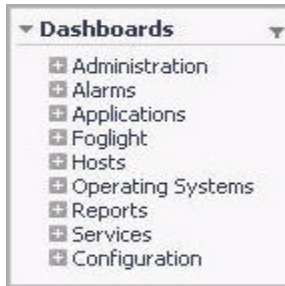
The Administration module includes a set of dashboards that allow you to manage agents, cartridges, users, and other entities. You can find them in the navigation panel under Dashboards > Administration.

The following table lists the nodes that appear in the Administration module, common tasks that are associated with each node, and references to other chapters in this manual that contain information about each node or task.

Node	Task	See
Administration	View entry points to the Administration module	Chapter 1, "Viewing the Administration Dashboard" on page 39

Node	Task	See
Agents	Manage agents and hosts	Chapter 5, "Managing Agents" on page 165
Cartridges	Manage cartridges and download agent packages	Chapter 4, "Managing Cartridges" on page 147
Data	Work with topology types, metrics, thresholds, and retention policies	Chapter 7, "Working with Data" on page 327
Rules & Notifications	Create and manage rules and registry variables	Chapter 6, "Working with vFoglight Rules and Registry" on page 183
Schedules	Create and manage schedules	Chapter 8, "Using Schedules" on page 395
Setup & Support	Manage vFoglight licenses and support bundles, and view audit and configuration items	Chapter 2, "Setting Up vFoglight" on page 53
Tooling	Build script agents	Chapter 9, "Working with vFoglight Tooling" on page 447
Users & Security	Manage users, groups, and roles	Chapter 3, "Managing Users and Security" on page 105

For a complete list of administration tasks and the dashboards that you can use to carry out each task, see "Looking at Administration Tasks" on page 50

Before you get started with the Administration module, you need to ensure that your vFoglight Management Server is up and running, adjust browser settings, and log into vFoglight, as described below.

To get started with the Administration module:

Note In order to complete this procedure, your user account must belong to a group with the Administrator role. For more information about users, groups, and roles, see "Managing Users and Security" on page 105.

---

1 Ensure that your vFoglight Management Server is running.

For example, on Windows platforms, you can start the vFoglight Management Server by choosing **Start > Programs > Vizioncore > vFoglight 5.2.4 > Start vFoglight**.

For more information, refer to the *Installation and Setup Guide*.

2 Obtain your vFoglight user name and password.

To obtain full access to the Administration module, ensure that your user account belongs to a group with the Administrator and Security roles. For more information, see "Managing Users and Security" on page 105.

3 Ensure that your Web browser has the JavaScript functionality enabled.

Note vFoglight displays dynamic data that is regularly updated. For this reason it is recommended that you do not use your browser's Back and Forward buttons, as this may cause cached views to be displayed or result in an error message.

4 Start the browser interface.

You can start the browser interface by opening a Web browser instance and navigating to the following URL:

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

Note The above URL assumes the default HTTP port number, 8080. For more information about default port assignments, see "Default port assignments" on page 65.

Where **localhost** is the name of the machine that is running the vFoglight Management Server.

The vFoglight login page appears in the Web browser.

5 Provide the user name and password you obtained in step 2.

    a In the vFoglight login page, in the **User** box, type your vFoglight user name.

    b In the **Password** box, type your vFoglight password.

    c Click **Login**.

Depending on the availability of a valid vFoglight license and your user permissions, one of the following pages appears in the display area:

    • If your vFoglight Management Server has a valid license, the Welcome page appears in the Web browser.

Navigation panel   Display area   Action panel
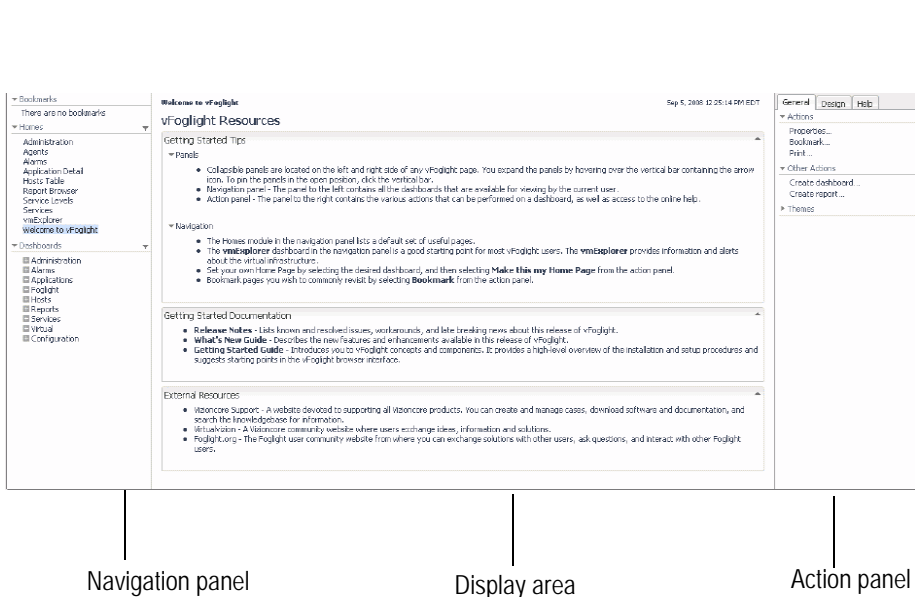
The Welcome page contains the following elements:

- *Navigation panel* shows the dashboards that the current user can access. For more information about users and security in vFoglight, see Chapter 3, "Managing Users and Security".

- *Display area* contains the current dashboard. When you log into vFoglight the **Welcome to vFoglight** page appears in the display area. Once you select a dashboard in the navigation panel, the display area refreshes to show the selected dashboard.

- *Action panel* includes any actions that you can perform in the selected dashboard.

For complete information about this page, see the *vFoglight User Guide*.

- If your vFoglight server does not have a valid license, one of the following views appears in the display area, depending on your user permissions.For more information about user permissions and security in vFoglight, see Chapter 3, "Managing Users and Security" on page 105.

Unlicense Server View	Oct 22, 2008 11:32:25 AM EDT

The server is unlicensed.

Do You Want to...
- Install a Licence
- Continue without Installing a Licence
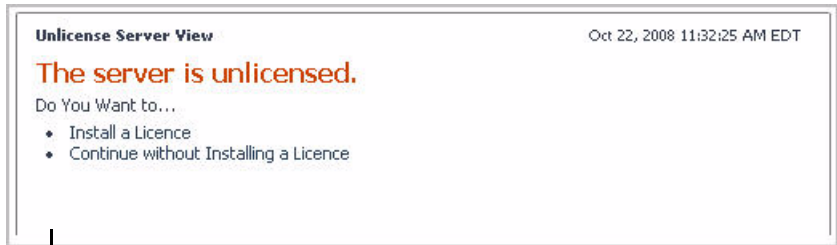
Users whose account includes the Administration role

Server Licensing Error	Oct 21, 2008 10:49:07 AM EDT

Server Licensing Error. Please contact your Administrator.

Users whose account does not include the Administration role

If your user account includes the Administration role, in the **Unlicensed Server View**, click **Install License**. In the Manage Licenses dashboard that appears, install the license for the vFoglight Management Server. For instructions on how to add a license, see Chapter 2, "Installing Licenses" on page 70.

If your user account does not include the Administration role, contact your vFoglight administrator, as indicated in the **Server Licensing Error** view.

6 On the navigation panel, under **Dashboards**, expand the **Administration** module.

A set of nodes appears under the **Administration** module.

7 Select a dashboard and look at its contents in the display area.

For example, to look at the Cartridge Inventory dashboard that allows you to manage vFoglight cartridges, on the navigation panel, under **Dashboards**, choose **Administration > Cartridges > Cartridge Inventory**.

The Cartridge Inventory dashboard appears in the display area.

You have successfully logged into vFoglight and located the dashboards that are available in the Administration module. From here, you can proceed to "Viewing the Administration Dashboard" on page 39.

Viewing the Administration Dashboard

The Administration dashboard contains links to administration dashboards that are grouped in a logical way, along with some high-level information about your environment. That information includes the number of cartridges, rules, and users, a list of licensed capabilities that reflect the features defined in your vFoglight license, and a list of audit activities such as login entries or agent-related operations. You can use this dashboard as a central point for all of your administration tasks. From here, you can navigate to any of the dashboards that come with the Administration module.

The Administration dashboard contains the following views:

- *Navigation*. Contains links to Administration dashboards.

Entry	Dashboard or View	Use it to
Explore		
Cartridges		
Inventory	Cartridge Inventory	Install, list, and manage cartridges. For more information, see "Installing and Managing Cartridges" on page 149.
Component Download	Components for Download	List and download agent installers. For more information, see "Downloading Agent Components" on page 161.
Data		
Data Management	Data Management	View the vFoglight topology.
Derived Metrics	Manage Derived Metrics	List, edit or delete derived metrics. For more information, see "Managing Derived Metrics" on page 333.
Retention Policies	Manage Retention Policies	List, edit or delete retention policies. For more information, see "Editing Retention Policies" on page 386.

Entry	Dashboard or View	Use it to
Thresholds	Manage Thresholds	List, add, edit, or delete thresholds. For more information, see "Managing Thresholds" on page 353.
Topology Types	Add Topology Type	Add topology types. For more information, see "Adding Topology Types" on page 329.
Rules and Notifications		
Registry Variables	Manage Registry Variables	List, edit, or delete registry variables. For more information, see "Managing Registry Variables" on page 185.
Rules	Manage Rules	List, edit, or delete rules. For more information, see "Managing Rules" on page 225.
Setup and Support		
Audit Information	View Audit Information	View audit log entries. For more information, see "Viewing Audit Information" on page 82.
Connection Status	Connection Status	Check connection status. For more information, see "Viewing Connection Status" on page 54.
vFoglight Configuration	vFoglight Configuration	View vFoglight configuration items. For more information, see "Viewing vFoglight Configuration" on page 56.
Licenses	Manage Licenses	List, add, or delete licenses. For more information, see "Managing Licenses" on page 69.
Support Bundles	Manage Support Bundles	List, add, or delete support bundles. For more information, see "Managing Support Bundles" on page 75.

Entry	Dashboard or View	Use it to
Schedules		
Schedule Management	Manage Schedules	List, edit, or delete schedules. For more information, see "Using Schedules" on page 395.
Tooling and Diagnostics		
Server Log Overview	Overview	Lists server log entries.
Server Performance Overview	Overview	Contains a series of tabs, each containing a dashboard about the performance of a monitoring component.
Script Agent Builder	Build Script Agent	Upload scripts for building agents. For more information, see "Building Script Agents" on page 448.
Script Editor	Script Editor	Allows you to query the vFoglight database. For more information, see "Retrieving Data with Queries and Scripts" on page 467.
Users and Security		
Groups	Manage Groups	List, add, edit, or delete groups. For more information, see "Managing Groups" on page 118.
Roles	Manage Roles	List, add, edit, or delete roles. For more information, see "Managing Roles" on page 127.
Users	Manage Users	List, add, edit, or delete users. For more information, see "Managing Users" on page 107.
Tasks		
Create		

Entry	Dashboard or View	Use it to
Topology Type	Add Topology Type	Add topology types. For more information, see "Adding Topology Types" on page 329.
Derived Metric	Create Derived Metric	Add derived metrics. For more information, see "Creating Derived Metrics" on page 342.
Threshold	Create Threshold	Add thresholds. For more information, see "Creating Thresholds" on page 361.
Registry Variable	Create Registry Variable	Add registry variables. For more information, see "Creating Registry Variables" on page 195.
Rule	Create Rule	Add rules. For more information, see "Creating Rules" on page 246.
Schedule	Create Schedule	Add schedules. For more information, see "Creating Schedules" on page 407.
Support Bundle	Manage Support Bundles	Create a server support bundle. When you click Support Bundle, a message box appears, indicating that a server support bundle is created, as illustrated below. For more information, see "Managing Support Bundles" on page 75.

Alert   ✕
Successfully Created Support Bundle!
Please click the following link to go to Support Bundle Page, or click on the close icon to stay in Administration Home
Go to Manage Support Bundle dashboard

Configure

Entry	Dashboard or View	Use it to
Directory Services	Configure Directory Services	View or edit directory services. For more information, see "Configuring Directory Services" on page 139.
Password Settings	Configure Password Services	View or edit password settings. For more information, see "Configuring Password Settings" on page 135.

- *Current Statistics*. Contains information about the installed cartridges, active agents, rules, users, and the vFoglight Management Server configuration.

- *Currently Licensed Capabilities*. Lists available licenses and their status (enabled or disabled).

- *License Information*. Contains information about one or more installed licenses.

- *Federation*. Contains information about the server federation.

- *Audited Activities*. Lists the operations that are invoked on the vFoglight Management Server.

To view the Administration dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Administration**.

The **Administration** dashboard appears in the display area.

3 In the Administration dashboard, observe the **Navigation** view.

The **Navigation** view contains links to Administration dashboards, grouped into task-specific categories.

Drill down to another dashboard in the Administration module using a link in the **Navigation** view. For example, to drill down to the Agent Hosts dashboard, under Explore > Agents, click Properties by Type.

The **Agent Properties dashboard appears** in the display area.
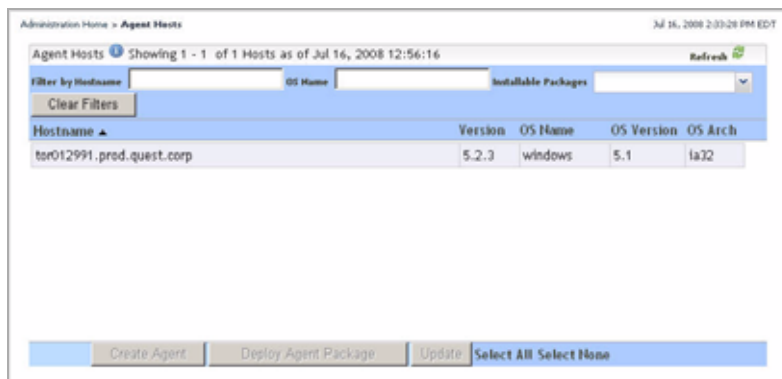
To return to the Administration dashboard, click **Administration** in the breadcrumb trail.

4 In the Administration dashboard, observe the **Current Statistics** view.

The **Current Statistic** view shows the number of cartridges, rules, and users in your monitoring environment, and shows the version of the vFoglight Management Server and its OS version.

- To find out more about the agents that are collecting data from monitored hosts in your environment, in the **Current Statistic** view, click **Active Agents**.

  The Agent Status dashboard appears in the display area.
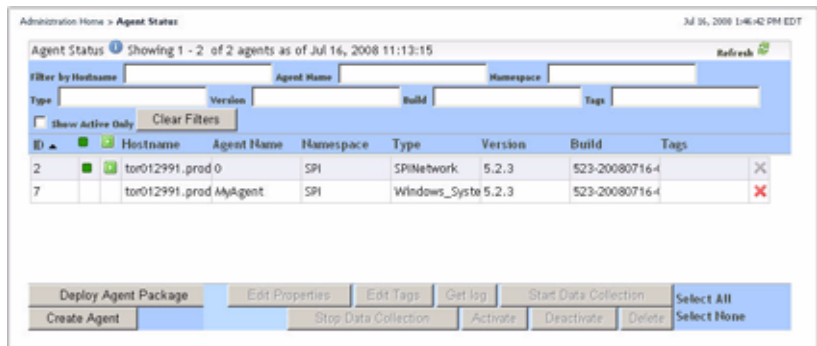
To return to the Administration dashboard, click **Administration** in the breadcrumb trail.

- To find out more about the cartridges that are installed on the vFoglight Management Server, in the **Current Statistic** view, click **Installed Cartridges**.

  The Cartridge Inventory dashboard appears in the display area.
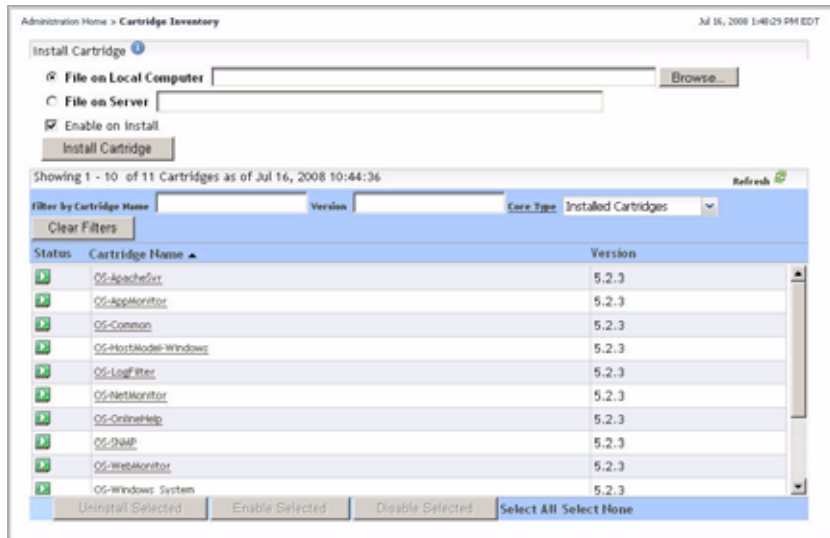
For complete information about the Cartridge Inventory dashboard, see Chapter 4, "Installing and Managing Cartridges" on page 149.

To return to the Administration dashboard, click **Administration** in the breadcrumb trail.

• To find out more about the rules that exist in your environment, in the **Current Statistic** view, click **Rules**.

The Manage Rules dashboard appears in the display area.
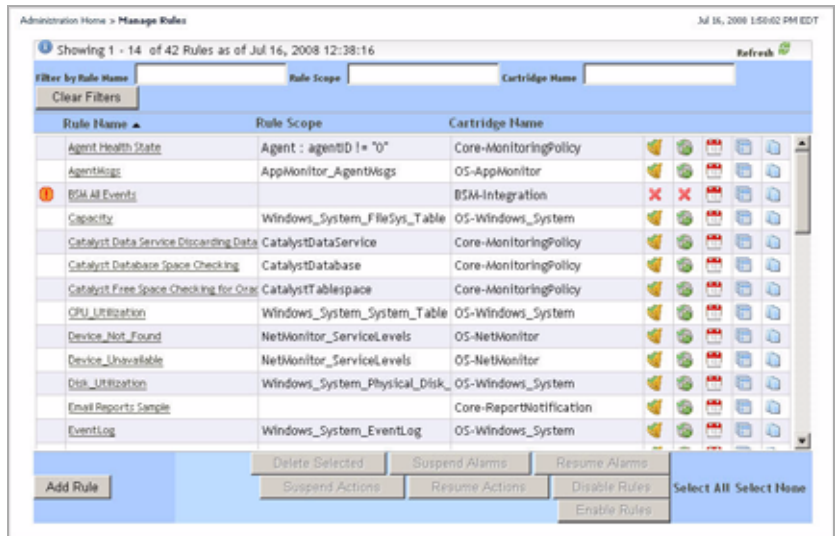
For complete information about the Manage Rules dashboard, see Chapter 6, "Managing Rules" on page 225.

To return to the Administration dashboard, click **Administration** in the breadcrumb trail.

- To find out more about the server configuration, that exist in your environment, in the **Current Statistic** view, click **Server Version** or **Server OS**.

The vFoglight Configuration dashboard appears in the display area.
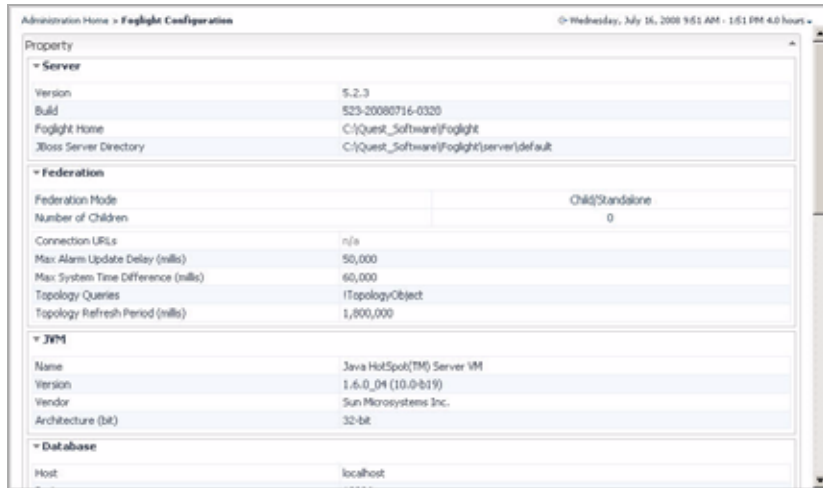
To return to the Administration dashboard, click **Administration** in the breadcrumb trail.

5 In the Administration dashboard, observe the **Currently Licensed Capabilities** view.

The **Currently Licensed Capabilities** view lists license-related features, indicating which features are included in your license. An icon appears to the right of each capability, indicating if the capability is licensed or not.

6 In the Administration dashboard, observe the **License Information** view.

The **License Information** view lists the numbers of installed and expired licenses and the licenses that are to expire within the next 30 days.

To find out more about your vFoglight licenses, click an entry in the **License Information** view.

The Manage Licenses dashboard appears in the display area.
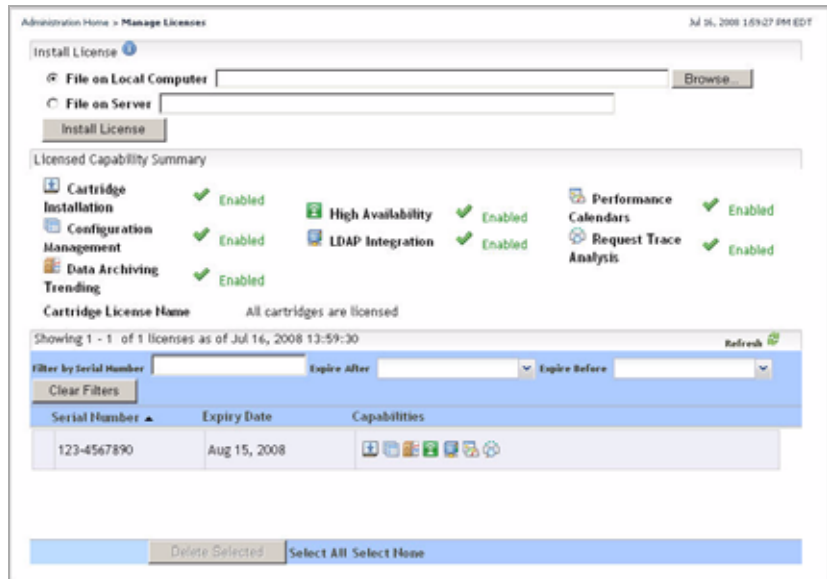
To return to the Administration dashboard, click **Administration** in the breadcrumb trail.

7 In the Administration dashboard, observe the **Federation** view.

The **Federation** view shows the federation mode of the vFoglight Management Server and the number of its children in the topology model.

To find out more about the federation configuration, click an entry in the **Federation** view.

The **vFoglight Server Topology** view appears in the display area.
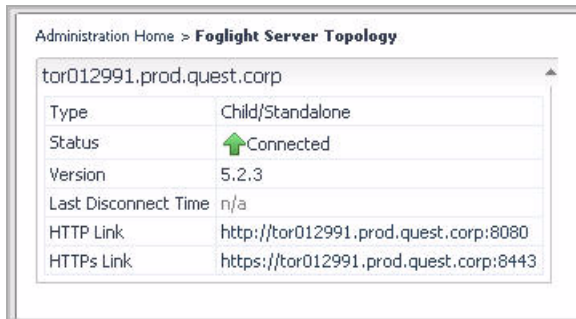
To return to the Administration dashboard, click **Administration** in the breadcrumb trail.

8 In the Administration dashboard, observe the **Audited Activities** view.

The **Audited Activities** view lists log entries that show information about operations performed on the vFoglight Management Server. For example, this list includes information about agent activation, agent package deployment, user authentication, and other types of tasks.

From here, you can proceed to configuring vFoglight as required by your business needs. To find out about the features that are offered by the Administration module, see "Looking at Administration Tasks" on page 50.

Looking at Administration Tasks

If you have the required roles, you can use the vFoglight Administration module to carry out any of the tasks listed in the table below.

> **Note** For more information about roles and security in vFoglight, see Chapter 3, "Managing Users and Security" on page 105.

Task	See
Install, list, and manage cartridges	"Installing and Managing Cartridges" on page 149

Task	See
Add topology types	"Adding Topology Types" on page 329
Add derived metrics	"Working with Derived Metrics" on page 332
Add thresholds	"Working with Thresholds" on page 353
List, edit or delete derived metrics	"Working with Derived Metrics" on page 332
List, edit or delete retention policies	"Managing Retention Policies" on page 372
List, add, edit, or delete thresholds	"Working with Thresholds" on page 353
Add registry variables	"Creating Registry Variables" on page 195
Add rules	"Creating Rules" on page 246
List, edit, or delete registry variables	"Managing Registry Variables" on page 185
List, edit, or delete rules	"Managing Rules" on page 225
Add schedules	"Creating Schedules" on page 407
List, edit, or delete schedules	"Managing Schedules" on page 397
Check connection status	"Viewing Connection Status" on page 54
View port assignments	"Viewing vFoglight Configuration" on page 56
List, add, or delete licenses	"Managing Licenses" on page 69
List, add, or delete support bundles	"Managing Support Bundles" on page 75
View audit information	"Viewing Audit Information" on page 82
Upload scripts for building agents	"Building Script Agents" on page 448
Edit and run queries and scripts	"Retrieving Data with Queries and Scripts" on page 467
View or edit directory services	"Configuring Directory Services" on page 139

Task	See
View or edit password settings	"Managing Groups" on page 118
List, add, edit, or delete groups	"Managing Groups" on page 118
List, add, edit, or delete roles	"Managing Roles" on page 127
List, add, edit, or delete users	"Managing Users" on page 107

2

Setting Up vFoglight

Once you get started with the Administration module, you can use the Setup & Support dashboards to administer vFoglight.

| Note | In order to complete each of the procedures in this chapter, your user account must belong to a group with the Administration role. For more information about users, groups, and roles, see "Managing Users and Security" on page 105. |

This chapter contains the following sections:

About vFoglight Setup

The Administration module includes a number of features that allow you to gather data about vFoglight while it is running, such as audit logs and diagnostic data that can be sent to Vizioncore Support. Additionally, it includes a set of dashboards that you can use to view vFoglight connection status, port numbers, database properties, or manage licenses and server support bundles.

Viewing Connection Status

The Connection Status dashboard provides a list of vFoglight Agent Manager instances connected to the vFoglight Management Server. It displays the host's IP address, login time, request name, and request time following information for each vFoglight Agent Manager.

To view the connection status:

Note   This procedure continues from "

---

   1   Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▸ on the left.

   2   On the navigation panel, under **Dashboards**, choose **Administration > Setup & Support > Connection Status**.

   The Connection Status dashboard appears in the display area, showing a list of vFoglight Agent Manager instances connected to the vFoglight Management Server.

Connection Status			Apr 7, 2008 10:44:49 AM EDT
Connection Status ⓘ Showing 1 - 1 of 1 connections as of Apr 01, 2008 15:33:12			Refresh
Client IP ▲	**Login Time**	**Request**	**Time**
127.0.0.1	Apr 01, 2008 14:59:22	/console/admin/support/connectionStatus.action	Apr 01, 2008 15:33:12
Select All Select None			

Viewing vFoglight Configuration

The vFoglight Configuration dashboard provides information about vFoglight configuration items.

The configuration settings that appear in this dashboard reflect the settings that you specify at or after the installation while others can be set at run-time. For example, the database settings whose values appear in the vFoglight Configuration dashboard are typically set after the installation in the file *<vfoglight_home>/config/foglight.config*. Any changes to the parameters in this file take effect only after a restart of the vFoglight Management Server. Other types of settings reflect the version, and in some cases, the patch level of the components that come with vFoglight, such as the vFoglight Management Server, WCF, JVM, or refer to the OS of the computer on which the vFoglight Management Server is installed, and its patch level. These settings cannot be changed unless you choose to upgrade to a higher version of vFoglight, if one is available. There are also some settings that can be defined using vFoglight registry variables. For example, the values that reflect global mail settings, which vFoglight uses for sending emails, as required, are specified in the vFoglight registry. Changes to these settings do not require a system restart.

The vFoglight Configuration dashboard contains the following views:

- Federation
- Server
- Federation Configuration
- Database
- JVM
- OS
- WCF
- Mail (Global Settings)
- Ports

Federation

vFoglight federation allows for partitioning a monitoring environment into logical units, where each unit is served by a separate instance of the vFoglight Management Server (federated server), while the operation of those servers is managed by a central vFoglight Management Server (federation server). The federated servers can be used to collect data from different types of environments, while the federation server can access

the data from one or more federated servers. For information on how to set up a federated environment, see the *Installation and Setup Guide*.

The **Federation** view displays the following settings:
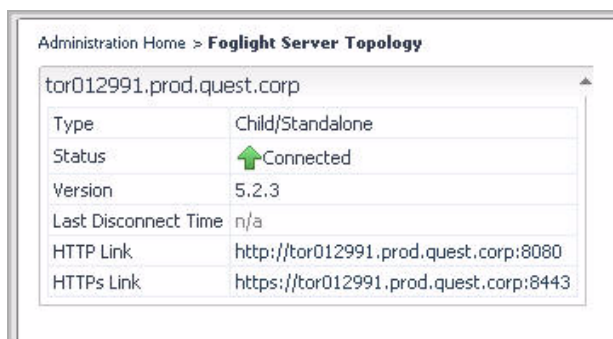
- **Federation Mode**. The Federation Mode setting indicates if the vFoglight Management Server whose configuration items you are viewing runs in federation mode.

- **Number of Children**. The number of children of the vFoglight Management Server whose configuration items you are viewing. If the server does not run in federation mode, or has no children, the number is zero '0'.

Federation	
Federation Mode	Child/Standalone
Number of Children	0

For information on how to view the information on the vFoglight Configuration dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67.

From the **Federation** view, you can drill down to the **vFoglight Server Topology** view by clicking **Federation Mode** or **Number of Children** to see additional details about the federation status.

Administration Home > **Foglight Server Topology**

tor012991.prod.quest.corp	
Type	Child/Standalone
Status	Connected
Version	5.2.3
Last Disconnect Time	n/a
HTTP Link	http://tor012991.prod.quest.corp:8080
HTTPs Link	https://tor012991.prod.quest.corp:8443

Server

The **Server** view displays the following settings:

- **Version**. The version number of the vFoglight Management Server whose configuration items you are viewing.

- **Build**. The build version of the vFoglight Management Server whose configuration items you are viewing.

- **vFoglight Home**. The installation directory of the vFoglight Management Server on the computer on which it is installed.

- **JBoss Server Directory**. The installation directory of the JBoss application server that is running vFoglight Management Server, on the computer on which the vFoglight Management Server is installed.

Server	
Version	5.2.3
Build	523-20080811-0040
Foglight Home	C:\Quest_Software\Foglight
JBoss Server Directory	C:\Quest_Software\Foglight\server\default

For information on how to view the information on the vFoglight Configuration dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67.

Federation Configuration

This view contains information about federation settings. The federation settings are defined in the file *<vfoglight_home>/config/federation.config*. For more information about this file, see the *Installation and Setup Guide*.

The **Federation Configuration** view displays the following settings:

- **Connection URLs**. The JNDI-provider URLs for federated servers. These URLs should use the JNDI JNP port (see "Ports" on page 63), as configured in *<vfoglight_home>/config/foglight.config* on the corresponding federated server. This setting is defined by the JndiURLs parameter in the file *<vfoglight_home>/config/federation.config*.

- **Max Alarm Update Delay (millis)**. The maximal delay in milliseconds that is allowed for the federation server to check all federated servers for alarm changes. This setting is defined by the MaxAlarmUpdateDelay parameter.

- **Max System Time Difference (millis)**. The maximal acceptable difference in system time between federated servers and the federation server, in milliseconds. This setting is defined by the MaxSystemTimeDifference parameter.

- **Topology Queries**. A list of one or more topology queries that identify topology objects that are be merged with the federated topology model. This setting is defined by the TopologyQueries parameter.

- **Topology Refresh Period (millis)**. The number of milliseconds between major topology refresh operations. A major topology refresh operation involves re-fetching all relevant topology objects from all federated servers and merging them into the local topology model. This setting is defined by the TopologyRefreshPeriod parameter.

Federation Configuration	
Connection URLs	n/a
Max Alarm Update Delay (millis)	50,000
Max System Time Difference (millis)	60,000
Topology Queries	!TopologyObject
Topology Refresh Period (millis)	1,800,000

For information on how to view the information on the vFoglight Configuration dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67

Database

This view contains information about database settings. The database settings are defined in the file *<vfoglight_home>/config/foglight.config*. For more information about this file, see the *Installation and Setup Guide*.

The **Database** view displays the following settings:

- **Host**. The name of the database host. This setting is defined by the foglight.database.host parameter.

- **Port**. The port number used by the database. This setting is defined by the foglight.database.port parameter.

- **Type**. The type of the database. Possible values are mysql or oracle. This setting is defined by the foglight.database.type parameter.

- **Hibernate Dialect**. The name of the component that defines the database hibernate dialect.

- **Database Name**. The name of the database. This setting is defined by the foglight.database.name parameter.

- **User**. The database user name. This setting is defined by the
  `foglight.database.user` parameter.

- **Location**. Indicates if the database is embedded or external. This setting is
  defined by the `foglight.database.embedded` parameter.

Database	
Host	localhost
Port	13306
Type	mysql
Hibernate Dialect	com.quest.nitro.hibernate.MySQLDialect
Database Name	foglight
User	foglight
Location	Embedded

For information on how to view the information on the vFoglight Configuration
dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67.

JVM

The **JVM** view displays the following settings:

- **Name**. The name of the Java Virtual Machine (JVM) of the computer in which
  the vFoglight Management Server is running.

- **Version**. The version number of the JVM.

- **Vendor**. The name of the JVM vendor.

- **Architecture (bit)**. The bit architecture of the JVM.

JVM	
Name	Java HotSpot(TM) Server VM
Version	1.6.0_04 (10.0-b19)
Vendor	Sun Microsystems Inc.
Architecture (bit)	32-bit

For information on how to view the information on the vFoglight Configuration
dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67.

OS

The **OS** view displays the following settings:

- **Type**. The name and version of the operating system on which the vFoglight Management Server is running.

- **Patch**. The patch level of the operating system on which the vFoglight Management Server is running.

OS	
Type	Windows XP x86 5.1, ia32
Patch	Service Pack 2

For information on how to view the information on the vFoglight Configuration dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67.

WCF

The **WCF** view displays the following settings:

- **Version**. The version number of the Web Component Framework (WCF) that is included with vFoglight.

- **Build**. The build version of the Web Component Framework (WCF) that is included with vFoglight.

WCF	
Version	2.8.0
Build	280-20080810-2330

For information on how to view the information on the vFoglight Configuration dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67.

Mail (Global Settings)

This view contains email settings that are used by vFoglight when sending messages to specified recipients. For example, you can configure vFoglight to generate and sent reports to a specified mail recipient, or email warning messages to vFoglight

administrators when certain thresholds are reached. For more information, see
"Viewing email settings and configuring email actions" on page 279.

Important In some situations you need to create or receive email alerts that contain a URL to the
browser interface. To ensure the URL points to the computer on which the vFoglight
Management Server is running, ensure that the CATALYST_URL registry variable
contains the correct computer name and port number.

For example: http://MyHost.MyDomain.com:8080/

For information on how to look up vFoglight registry variables, see Chapter 6, "Managing
Registry Variables" on page 185.

The **Mail (Global Settings)** view displays the following settings:

- **Connection Timeout**. The default connection timeout for sending emails to
  specified email recipients.

- **From**. The default email address used by vFoglight from which emails are sent
  when required. This setting is defined by the global value of the mail.from
  vFoglight registry variable.

- **SMTP Host**. The default email host name used by vFoglight from which emails
  are sent when required. This setting is defined by the global value of the
  mail.host vFoglight registry variable.

- **SMTP Port**. The default port number of the email server used by vFoglight from
  which emails are sent when required. This setting is defined by the global value
  of the mail.port vFoglight registry variable.

- **Recipient**. The default email address used by vFoglight to which emails are sent
  when required. This setting is defined by the global value of the
  mail.recipient vFoglight registry variable.

- **Socket Timeout**. The default socket timeout for sending emails to specified email
  recipients.

- **User**. The default user name for logging into the email server that is used by
  vFoglight to which emails are sent when required. This setting is defined by the
  global value of the mail.user vFoglight registry variable.

Mail (Global Settings)	
Connection Timeout	Not Globally Configured
From	Not Globally Configured
SMTP Host	Not Globally Configured
SMTP Port	Not Globally Configured
Recipient	Not Globally Configured
Socket Timeout	Not Globally Configured
User	Not Globally Configured

For information on how to view the information on the vFoglight Configuration dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67.

Ports

This view contains information about port settings. The port settings are defined in the file *<vfoglight_home>/config/foglight.config*. For more information about this file, see the *Installation and Setup Guide*. For details on default port assignments, see "Default port assignments" on page 65.

The **Ports** view displays the following settings:

- **Cluster Mcast Port**. Cluster Multi-cast port, used when vFoglight is running in High Availability (HA) mode. This setting is defined by the foglight.cluster.mcast_port parameter.

- **HA JNDI RMI Port**. Port for the Remote Method Invocation (RMI) naming service when vFoglight is running in HA mode. It can be used to observe the network traffic between the vFoglight Management Server and other computers on the same network. If it finds another JBoss server, it checks the partition name to see if the JBoss server is a primary or a secondary server. This setting is defined by the foglight.ha.jndi.rmi.port parameter.

- **HA JNDI JNP Port**. Port for the bootstrap JNP service when vFoglight is running in HA mode. This setting is defined by the foglight.ha.jndi.jnp.port parameter. For more information about High Availability mode, see the *Installation and Setup Guide*.

- **HA JRMP Invoker Port**. Port for the RMI/JRMP invoker when vFoglight is running in HA mode. This setting is defined by the foglight.ha.jrmp.invoker.port parameter.

- **HA Pooled Invoker Port**. Pooled invoker port when vFoglight is running in HA mode. This setting is defined by the `foglight.ha.pooled.invoker.port` parameter.

- **HA JNDI UDPGroup Port**. Port for the UDP group when vFoglight is running in HA mode. This setting is defined by the `foglight.ha.jndi.udpgroup.port` parameter.

- **HTTP Port**. HTTP/1.1 connector used for HTTP connections. This setting is defined by the `foglight.http.port` parameter.

- **HTTPS SSL Port**. HTTP/1.1 connector used for HTTPS connections. This setting is defined by the `foglight.https.port` parameter.

  Note The vFoglight Management Server uses the HTTP port for local access even if you are accessing the browser interface through an HTTPS connection. If that is the case, both ports are open: the HTTPS port for external requests coming from the browser interface and the HTTP port for local requests. For example, the reporting service accesses the vFoglight Management Server through the HTTP port while external requests use HTTPS.

- **JNDI RMI Port**. Port for the Remote Method Invocation (RMI) naming service. This setting is defined by the `foglight.jndi.rmi.port` parameter.

- **JNDI JNP Port**. Port for the bootstrap JNP service. This setting is defined by the `foglight.jndi.jnp.port` parameter.

- **JRMP INVOKER PORT**. Port for the RMI/JRMP invoker. This setting is defined by the `foglight.jrmp.invoker.port` parameter.

- **ORB (IIOP) Port**. Corba ORB port used by the Agent Adapter. This setting is defined by the `foglight.orb.port` parameter.

- **ORB (IIOP) SSL Port**. Corba ORB SSL port used by the Agent Adapter. This setting is defined by the `foglight.orb.ssl.port` parameter.

Ports	
JavaEE Agent Port (NexusTalk)	JavaEE-Cartridge is not installed or disabled
Cluster Mcast Port	45566
HA JNDI RMI Port	1101
HA JNDI JNP Port	1100
HA JRMP Invoker Port	4447
HA Pooled Invoker Port	4446
HA JNDI UDPGroup Port	1102
HTTP Port	8080
HTTPS SSL Port	8443
JNDI RMI Port	1098
JNDI JNP Port	1099
JRMP INVOKER PORT	4444
ORB (IIOP) Port	3528
ORB (IIOP) SSL Port	3529

For information on how to view the information on the vFoglight Configuration dashboard, see "Accessing the vFoglight Configuration Dashboard" on page 67.

Default port assignments

The following table shows the default port assignments. The port numbers are defined in the file *<vfoglight_home>/vFoglight/config/foglight.config*. Their default values appear during installation. For information about changing port assignments at installation time, see the *Installation and Setup Guide*.

Some of these port numbers can be seen in the **Ports** view of the vFoglight Configuration dashboard, and they are described in "Ports" on page 63.

Port Name	Default Port Number	Description
Cluster Multi-cast Port	45566	Cluster Multi-cast port. It is used when vFoglight is running in High Availability (HA) mode.
Database Port	3306	User-defined port for connecting to the database.

Port Name	Default Port Number	Description
HA JNDI JNP Port	1100	Port for the bootstrap JNP service when vFoglight is running in HA mode. For more information about High Availability mode, see the *Installation and Setup Guide*.
HA JNDI RMI Port	1101	Port for the Remote Method Invocation (RMI) naming service when vFoglight is running in HA mode. It can be used to observe the network traffic between the vFoglight Management Server and other computers on the same network. If it finds another JBoss server, it checks the partition name to see if the JBoss server is a primary or a secondary server.
HA JNDI UDP Group Port	1102	Port for the UDP group when vFoglight is running in HA mode.
HA JRMP Invoker Port	4447	Port for the RMI/JRMP invoker when vFoglight is running in HA mode.
HA Pooled Invoker Port	4446	Pooled invoker port when vFoglight is running in HA mode.
HTTP Port	8080	HTTP/1.1 connector used for HTTP connections.
HTTPS Port	8443	HTTP/1.1 connector used for HTTPS connections.

Note The vFoglight Management Server uses the HTTP port for local access even if you are accessing the browser interface through an HTTPS connection. If that is the case, both ports are open: the HTTPS port for external requests coming from the browser interface and the HTTP port for local requests. For example, the reporting service accesses the vFoglight Management Server through the HTTP port while external requests use HTTPS.

JNDI JNP Port	1099	Port for the bootstrap JNP service.
JNDI RMI Port	1098	Port for the Remote Method Invocation (RMI) naming service
JRMP Invoker Port	4444	Port for the RMI/JRMP invoker.

Port Name	Default Port Number	Description
QP5 Application Port	8448	Port for the SQL parser.
ORB (IIOP) Port	3528	Corba ORB port used by the Agent Adapter.
vFoglight Agent Manager	3529	Corba ORB SSL port used by the Agent Adapter.
JavaEE Agent	41705	Port for the JavaEE Agent

Accessing the vFoglight Configuration Dashboard

Use the vFoglight Configuration dashboard when you need to find out the configuration of your monitoring environment.

To access the vFoglight Configuration dashboard:

**Note** This procedure continues from "Getting Started with the Administration Module" on page 32.

1 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Setup & Support > vFoglight Configuration**.

The vFoglight Configuration dashboard appears in the display area, showing the vFoglight configuration items.

Foglight Configuration	⊙ Thursday, August 21, 2008 9:31 AM - 1:31 PM 4.0 hours ▾
Property	▲
Federation	
🗐 Federation Mode	Child/Standalone
🖳 Number of Children	0
Server	
Version	5.2.3
Build	523-20080811-0040
Foglight Home	C:\Quest_Software\Foglight
JBoss Server Directory	C:\Quest_Software\Foglight\server\default
Federation Configuration	
Connection URLs	n/a
Max Alarm Update Delay (millis)	50,000
Max System Time Difference (millis)	60,000
Topology Queries	!TopologyObject
Topology Refresh Period (millis)	1,800,000
Database	
Host	localhost
Port	13306
Type	mysql
Hibernate Dialect	com.quest.nitro.hibernate.MySQLDialect
Database Name	foglight
User	foglight
Location	Embedded
JVM	
Name	Java HotSpot(TM) Server VM
Version	1.6.0_04 (10.0-b19)
Vendor	Sun Microsystems Inc.
Architecture (bit)	32-bit
OS	
Type	Windows XP x86 5.1, ia32
Patch	Service Pack 2
WCF	
Version	2.8.0
Build	280-20080810-2330
Mail (Global Settings)	
Connection Timeout	Not Globally Configured

3 In the vFoglight Configuration dashboard, locate the view that contains information about a set of configuration items, as required.

For example, to find out what is the name of the database host, scroll down to the **Database** view, and inspect the **Host** setting.

For complete information about each view that appears in the vFoglight Configuration dashboard, see the following sections:

- "Federation" on page 56
- "Server" on page 57
- "Federation Configuration" on page 58
- "Database" on page 59
- "JVM" on page 60

Managing Licenses

You can manage vFoglight licenses using any of the following interfaces:

- *Manage Licenses dashboard*. Allows you install or delete vFoglight licenses, and to view licensing capabilities for each license. For details, refer to any of the following sections as required:

- *Command line*. The *fglcmd* interface includes commands for installing, listing, or removing vFoglight licenses. For complete information, see the *Command-Line Reference Guide*.

Accessing the Manage Licenses Dashboard

The Manage Licenses dashboard allows you to view, install, and delete licenses for your vFoglight Management Server installation. This page consists of three areas: Install Licenses, Licensed Capability Summary, and a listing of currently installed licenses.

To access the Manage License dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32 or "Viewing the Administration Dashboard" on page 39.

---

1 Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Setup & Support > Manage Licenses**.

The Manage Licenses dashboard appears in the display area, showing the list of installed licenses.
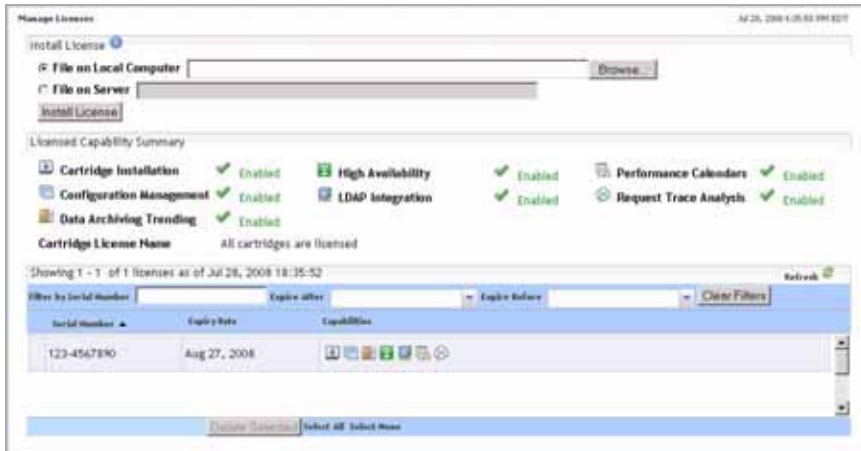
3 To sort the list by license serial number or expiry date, click **Serial Number** or **Expiry Date** as required.

4 To filter the list of licenses, in the area that shows the list of installed licenses, use the **Filter by Serial Number**, **Expire After**, and **Expire Before** boxes as required.

To clear the filters, click **Clear Filters**.

From here, you can proceed to any of the following procedures:

- "Installing Licenses" on page 70
- "Viewing License Capabilities" on page 72
- "Deleting Licenses" on page 74

Installing Licenses

The Install License area in the Manage Licenses dashboard allows you to install licenses on the vFoglight Management Server. You can use it to install a license file that is accessible from the local machine or the vFoglight Management Server machine.

Alternatively, you can install a license using the command line using the
`license:import` command that comes with the `fglcmd` interface. For details, see the
Command-Line Reference Guide.

To install a license:

Note   This procedure continues from "" on page 69.

---

1   To navigate to the license file that you can access with your local machine,
complete one of the following steps in the **Install License** area of the Manage
License dashboard.

- Ensure that the **File on Local Computer** box is selected. Then click **Browse**,
and navigate to the license file in the file browser that appears.

  The file browser closes and the **File on Local Computer** box refreshes to
  show the absolute path and name of the license file.

  or

- Select the **File on Local Computer** option, and in the box to the right, type the
absolute path and name of the license file

  Use the back slash character '\' as a directory separator on Windows platforms**.**

  Windows example:

  `C:\temp\foglight.license`

2   To navigate to the license file that is accessible by the machine on which the
vFoglight Management Server is running, complete the following steps.

  a   Select the **File on Server** box.

  b   In the **File on Server** box, type the path and name of the license file. Use
  either an absolute path or a path relative to the installation directory of the
  vFoglight Management Server.

  Note   Use the back slash character '\' as a directory separator.

  For example, both of the following file paths point to the same license file:

  ```
  C:\Vizioncore\vFoglight\license\foglight.license
  license\foglight.license
  ```

3   Click **Install License**.

  A message appears, indicating that the license installation was successful.

Install License ⓘ
License was successfully installed
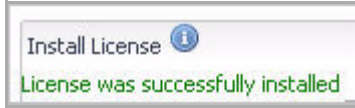
Once the vFoglight Management Server reads the license file, it stores it internally in the database and no longer requires the physical file.

Viewing License Capabilities

The Licensed Capability Summary area provides an overview of the licensed capabilities currently enabled on the vFoglight Management Server. Each capability has an icon that is associated with it:

Cartridge Installation

Configuration Management

Data Archiving Trending

High Availability

LDAP Integration

Performance Calendars

Request Trace Analysis

Additionally, Cartridge License Name in the same area lists the cartridges that are licensed with your current vFoglight license.

Alternatively, you can review licensing capabilities using the license:list command that comes with the **fglcmd** interface. For details, see the *Command-Line Reference Guide*.

To view license capabilities:

1   In the Manage Licenses dashboard, in the area that lists installed licenses, select a
    license whose capabilities you want to view.

    The **Licensed Capability Summary** area lists the capabilities of the selected
    license and the cartridges that are included in the license.

Licensed cartridges   License capabilities
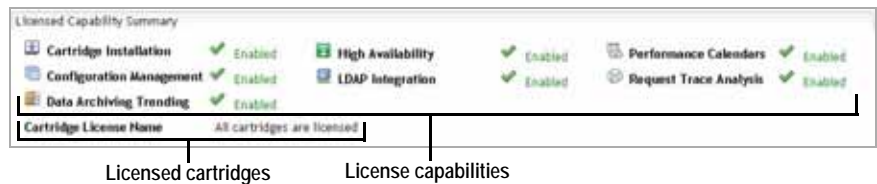
    In the **Licensed Capability Summary** area, an icon appears to the right of each
    capability, indicating if the capability is enabled or disabled.

   Capability is enabled.

   Capability is disabled.

    Cartridge License Name lists those cartridges that are licensed with the selected
    vFoglight license.

2   Additionally, in the license list under the **Licensed Capability Summary** area,
    the **Capabilities** column shows icons of those capabilities for which each license
    is enabled:

•   To find out which vFoglight cartridges are licensed for a license, point to the
    Cartridge Installation icon ( ).

    A tooltip appears, indicating the cartridges that are covered by the selected
    license.

Cartridge Installation(All)

For information on how to install a cartridge, see Chapter 4, "Managing Cartridges" on page 147.

- If a license includes a license for one or more agents, it shows agent icons ( ). When you point your mouse over that icon, a tooltip appears, showing the agent name along with the number of licensed agents.

Deleting Licenses

The license list pane allows you to delete any license currently enabled on vFoglight.

Alternatively, you can delete a license using the license:remove command that comes with the fglcmd interface. For details, see the *Command-Line Reference Guide*.

To delete a license:

Note This procedure continues from "Accessing the Manage Licenses Dashboard" on page 69.

1 In the Manage Licenses dashboard, in the area that lists installed licenses, select a row containing the license that you want to delete.

2 Click **Delete Selected**.

The **License Confirmation** dialog box appears.

3 To proceed with license deletion, in the **License Confirmation** dialog box, click Yes.

The **License Confirmation** dialog box closes. The list of installed licenses refreshes and a message indicating that the delete process was successful appears above the list.

Selected licenses were successfully deleted			
Showing 0 of 0 licenses as of Apr 07, 2008 15:26:58			Refresh
Filter by Serial Number		**Expire After**	**Expire Before**
	Clear Filters		
Serial Number ▲	**Expiry Date**	**Capabilities**	
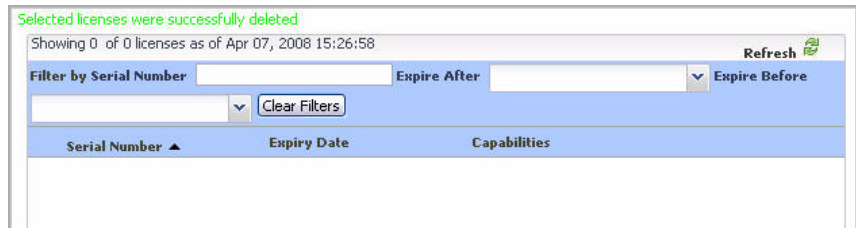
Managing Support Bundles

vFoglight allows you to gather diagnostic data from the vFoglight Management Server or the vFoglight Agent Manager. and save it in a support bundle.

There are two types of support bundles that you can create in vFoglight:

- *Server support bundles*. Contain a number of files, including a diagnostic snapshot of the vFoglight Management Server, log files, and a list of cartridges installed on the vFoglight Management Server computer. vFoglight saves each server support bundle as a .ZIP file in the *<vfoglight_home>/support/ <user_name>* directory on the machine hosting the vFoglight Management Server.

  You can create a server support bundle using the Manage Support Bundles dashboard or the support:bundle command that comes with the fglcmd interface.

  For information about managing server support bundles using the Manage Support Bundles dashboard, see the following sections:

  - "Accessing the Manage Support Bundles Dashboard" on page 76
  - "Creating Server Support Bundles" on page 77
  - "Retrieving Server Support Bundles" on page 79
  - "Viewing the Content of Server Support Bundles" on page 80

  For information about the support:bundle command, see the *Command-Line Reference Guide*.

Accessing the Manage Support Bundles Dashboard

Using the Administration module, you can gather diagnostic data from the vFoglight Management Server and save it in a support bundle for analysis by Vizioncore Support.

To access the Manage Support Bundles dashboard:

Note	This procedure continues from "Getting Started with the Administration Module" on page 32.

1   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Setup & Support > Manage Support Bundles**.

    The Manage Support Bundles dashboard appears in the display area, showing the list of existing support bundles.
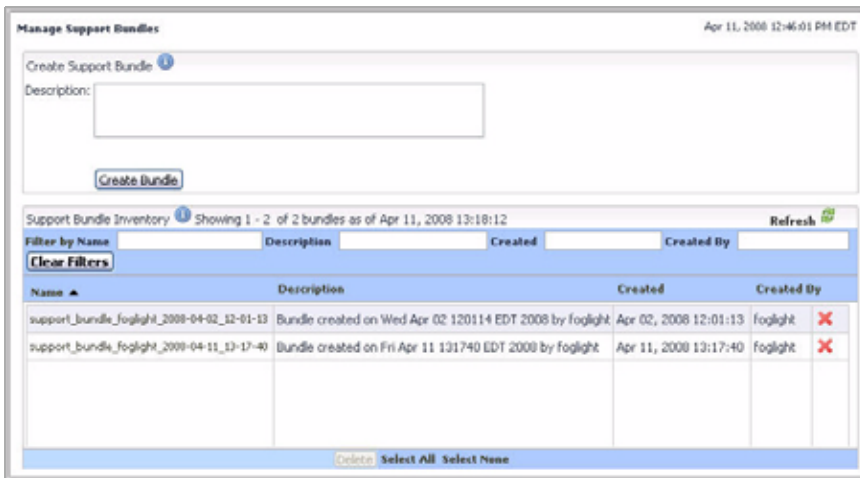
3   To sort the list by name, description, creation date, or user name, click the **Name**, **Description**, **Created**, or **Created By** column headings as required.

4   To filter the list of support bundles, in the area that shows the list of installed licenses, use the **Name**, **Description**, **Created**, or **Created By** boxes as required.

    To clear the filters, click **Clear Filters**.

From here, you can proceed to any of the following procedures:

- "Creating Server Support Bundles" on page 77
- "Retrieving Server Support Bundles" on page 79
- "Viewing the Content of Server Support Bundles" on page 80

Creating Server Support Bundles

A server support bundle contains diagnostic data gathered from the vFoglight Management Server. vFoglight saves this data in a .ZIP file. When you click Create Bundle on the Manage Support Bundles dashboard, the vFoglight Management Server creates the .ZIP file in the *<vfoglight_home>/support/<user_name>* directory on the computer hosting the vFoglight Management Server.

Alternatively, you can delete a license using the support:bundle command that comes with the fglcmd interface. For details, see the *Command-Line Reference Guide*.

Depending on the type of browser you are running and its settings, you might be able to retrieve a copy of an existing server support bundle as a file download. For more information, see "Retrieving Server Support Bundles" on page 79

To create a server support bundle:

Note   This procedure continues from "Accessing the Manage Support Bundles Dashboard" on page 76.

1   **Optional**. Specify the description of the support bundle.

In the Manage Support Bundles dashboard, in the **Create Support Bundle** area, type the description in the **Description** box.

For example: My support bundle.

2   Click **Create Bundle**.

A status bar appears above the **Create Bundle** button indicating that the bundle creation is in progress.
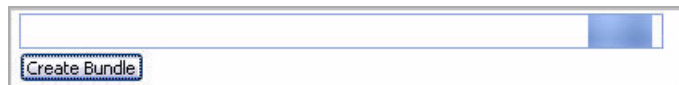
When vFoglight finishes generating the support bundle, your Web browser displays a dialog box that allows you to open or save the support bundle.
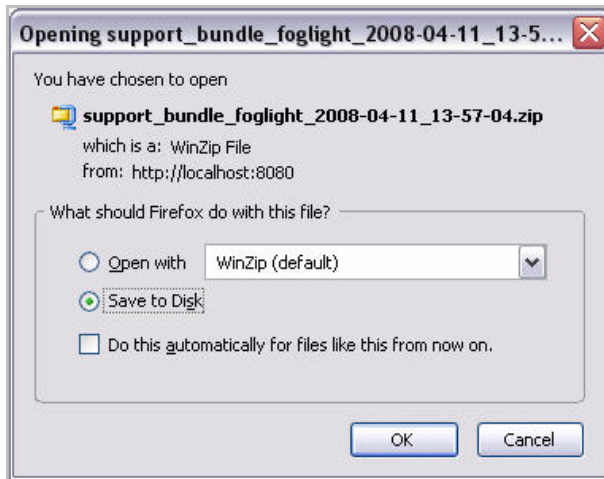
> **Note** The appearance of the above dialog box may be different, depending on the type and version of your Web browser.

3 Save the generated ZIP file to disk.

The newly-generated support bundle appears in the **Support Bundle Inventory** view.

In addition to the bundle name, the **Support Bundle Inventory** view shows the bundle description, the date and time at which it was created, and the name of the user who created it.

Retrieving Server Support Bundles

vFoglight stores support bundles in the *<vfoglight_home>/support/<user_name>*
directory on the computer hosting the vFoglight Management Server. You can retrieve a
copy of an existing support bundle as a file download using the Support Bundle
Inventory view immediately after its creation or at a later time.

To retrieve a server support bundle:

Note   This procedure continues from "Accessing the Manage Support Bundles Dashboard" on
page 76.

1   In the Manage Support Bundles dashboard, in the **Support Bundle Inventory**
    view, locate the support bundle that you want to retrieve.

2   Click the **Name** column of the row containing the support bundle.

    Your Web browser shows a dialog box that allows you to open or save the support
    bundle.
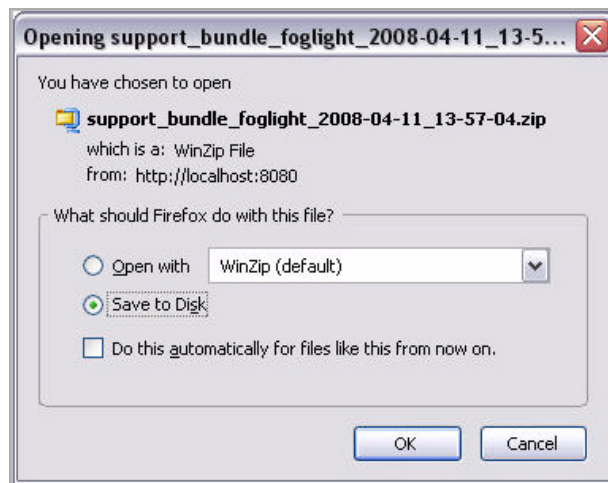
Note   The appearance of the above dialog may be different, depending on the type and
version of your Web browser.

3   Save the file to disk.

Viewing the Content of Server Support Bundles

Server support bundles contain diagnostic data gathered from the vFoglight Management Server.

To view the content of a server support bundle:

Note   This procedure continues from ".

---

1   Locate the server support bundle whose content you want to view by completing one of the following steps.

  • If you have access to the computer that is hosting the vFoglight Management Server, server support bundles are stored in the *<vfoglight_home>/support/ <user_name>* directory.

  or

  • If you do not have access to the computer that is hosting the vFoglight Management Server, retrieve the support bundle using the Support Bundle Inventory view.

2   Extract the contents of the ZIP file containing the server support bundle to a local directory.

3   Observe the file structure.

  Each server support bundle consists of a number of files. The following list illustrates a file collection sample that may appear in a server support bundle.

  Note   The list below does not include the entire list of files that are contained in server support bundle. It is a partial listing that illustrates the directory structure and describes some of the common files that appear in the support bundle.

AuditingLog_*.xml	A listing of recent auditable changes to the v*FMS/registry/rules/cartridges/security/etc* It contains information about the before and after states of a configuration object, including rules, registry variables, agent properties, schedules, derived metrics, or thresholds, for changes that occur within the applicable default time range.
DiagnosticSnapshot_*.txt	A diagnostic snapshot consisting of service status, agent status, thread dump, etc
DirectoryListing_*.txt	A full file listing for all files under the vFMS home directory
vFoglight_<version>_InstallLog.log	vFMS installation log
InstalledCartridges_*.xml	A listing of all installed cartridges, and their versions
MonitoringPolicies_*.xml	An export of the Monitoring Policies (persistent configuration) of the vFMS
support_bundle_foglight_*.xml	Brief description about this support bundle
config/	
agent-weight.config	Defines the "weight" of attached agents. Used to help determine vFMS load
foglight.config	Config parameters for the vFMS
log.config	Config parameters for the vFMS logging capabilities
remote_monitor.config	Various configuration options for running the vFMS as a service
remote_monitor.log.config	Various log configuration options for the vFMS

restart_monitor.config	vFMS restart configuration parameters (as a service)
server_restarter.log.config	Logging parameters for the vFMS
logs/	
ManagementServer_*.log	The three most recent vFMS logs
server/	
default/	
conf/	
jacorb.properties	vFMS JacORB configuration parameters
deploy/	
nitro-dyn-ds.xml	vFMS data source definition
jbossweb-tomcat55.sar/	
context.xml	JBoss application configuration file
server.xml	JBoss application configuration file

Note   The "*" indicates a date/time stamp of the format "YYYY-MM-DD_HH-MM-SS"".

Viewing Audit Information

vFoglight maintains security and change audit logs that you can view using the View Audit Information dashboard. Audit logs allow you to review information about users who have been authenticated upon logging in to the Administration Module, changes made in the Administration Module with regard to user management, or changes made to configuration items such as rules or registry variables.

The View Audit Information dashboard allows you to select the time period for which you want to view administration logs. Each log includes information such as the name of the user who made the change, the date and time at which the change was made, the action performed, and (if applicable) the name of the item that was changed (for example, the name of the rule).

For complete information, about viewing audit information, see to the following sections:

- "Accessing the View Audit Information Dashboard" on page 83
- "Filtering Audit Logs" on page 87
- "Viewing Log Entries" on page 88

Accessing the View Audit Information Dashboard

Use the View Audit Information dashboard to select a time period for which you want to view security and change audit logs and display logs. It allows you to review security and change audit logs and to filter the list of logs to show information for a specific span of time. Optionally, you can show or hide the columns that appear in the audit log table, or print the table contents to a file as required.

To access the View Audit Information dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow ▸ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Setup & Support > View Audit Information**.

    The View Audit Information dashboard appears in the display area, showing the Zonar and a list of audit logs underneath.

The Zonar displays the current date, time, and time range, and allows you to modify the current time range. The list below the Zonar displays the audit logs that the vFoglight Management Server records within the time range specified in the Zonar. For more information about the Zonar and its functionality, see the *vFoglight User Guide*.

3 **Optional**. Reduce the number of columns that appear in the audit log table.

    a In the audit log table, in the **Operation Name (Name)** column, click the **Show/Hide columns** button.

Show/Hide columns

The **Show columns** dialog box appears.

```
                 Show columns
        ☑ Time Range

        ☑ User Name

        ☑ Service Name

        ☑ Operation Name (Name)

              Apply    Cancel
        Actions
        Export as CSV...
        Export as PDF...
```

Since all of the four columns appear in the View Audit Information dashboard by default, all of the check boxes that correspond to the columns appear selected.

b To hide a column, in the **Show columns** dialog box, clear the corresponding check box.

or

To show a column, clear the corresponding check box.

For example, to display only the time range and the operation name, ensure that the **Time Range** and **Operation Name (Name)** check boxes are selected, and clear the **User Name** and **Service Name** check boxes.

c Click **Apply**.

The audit log table refreshes, showing only the selected columns.

Time Range	Operation Name (Name)
10/21/08 1:10 PM	authenticate (Logged out)
10/21/08 1:01 PM	authenticate (Login OK)
10/21/08 1:26 PM	authenticate (Login OK)
10/21/08 1:10 PM	httpsession (Session Created)
10/21/08 1:10 PM	httpsession (Session Ended)

4 Optional. Print the list of audit logs to a file.

    a In the audit log table, in the **Operation Name (Name)** column, click the
        Show/Hide columns button.

Show/Hide columns

Time Range	User Name	Service Name	Operation Name (Name)
10/21/08 1:10 PM	foglight	SecurityService	authenticate (Logged out)

    The **Show columns** dialog box appears.

    b In the **Show Columns** dialog box, under **Actions**, click one of the following
        links:

    Export as CSV, to export the table contents to a Comma Separated Values
    (CSV) file.

    Export as PDF, to export the table contents to a PDF file.

    Important If you previously show or hide one or more columns in the audit table, this
                layout is reflected in the exported file. For example, if you display only the
                time range and the operation name, only the **Time Range** and **Operation
                Name (Name)** columns are exported to a file.

    When exporting the table contents to a PDF file, the PDF output appears in a
    new tab or window (depending on the type and version of your Web browser).

When exporting the table contents to a CSV file, a dialog box appears, allowing you open the exported file, or to save it to disk.

Note   The appearance of the above dialog box may be different, depending on the type and version of your Web browser.

From here, you can proceed to any of the following procedures:

Filtering Audit Logs

When you first access the View Audit Information dashboard, it displays log entries from within the past four hours. You can filter the list of log entries to show information for a specific period of time.

To filter audit logs:

Note   This procedure continues from

- In the View Audit Information dashboard, use the Zonar to specify the period of time whose log entries you want to list.

To specify the period start and end times, click and drag the edges of the grey area in the Zonar. For complete information on how to use the Zonar in vFoglight, see the *vFoglight User Guide*.

The log entries for the selected time period appear in the log table.

Viewing Log Entries

The log entries that appear on the View Audit Information dashboard allow you to review information such as the users who have been authenticated upon logging in to the vFoglight, changes made in the Administration module with regard to user management (such as changes to settings for users, groups, and roles), or changes made to configuration items (such as rules, schedules, or registry variables).

To view an audit log entry:

Note	This procedure continues from "Accessing the View Audit Information Dashboard" on page 83.

1 In the View Audit Information dashboard, locate the row in the log table containing the entry whose details you want to view.

2 Observe the following columns for the selected entry:

• **Time Range**: Displays the date and time at which the specified action occurred.

• **User Name**: Displays the user name for the user who caused the action to be performed.

• **Service Name**: Displays the name of the vFoglight service that performed the action.

• **Operation Name (Name)**: Displays the operation that was performed by vFoglight. If applicable, the name of the item that was changed is also displayed in this column.

Backing Up, Upgrading, and Restoring vFoglight

Backup and restore processes are important aspects of database administration. This section provides suggested end-to-end backup, upgrade, and restore procedures for vFoglight installations. It includes the following sections:

- "Backing Up vFoglight" on page 89
- "Upgrading vFoglight" on page 101
- "Restoring vFoglight" on page 102

Backing Up vFoglight

The term "backing up" refers to making copies of data that can be used to restore your system after a data loss event. For details of the vFoglight recovery procedure, see "Restoring vFoglight" on page 102.

This section outlines the vFoglight backup process, which includes:

- Archiving the vFoglight configuration file, scripts, and installed cartridges.
- Backing up the entire database (MySQL or Oracle).
- Verifying the settings of environment variables (Oracle).

Saving the archive in a safe location separate from the original. The following table shows the possible ways of backing up vFoglight, some of which include the backup of the file system, and in some cases the system registry. Each option shows a sequence of actions that can be performed to back up vFoglight.

vFoglight Single Tier

vFoglight Management Server on Windows with embedded MySQL

Option 1	• Stop the vFoglight Management Server. • Perform a full system backup, including the file system and the Windows Registry.

Option 2
- Issue a `mysqldump` command to export the MySQL database.

  Alternatively, use the InnoDB HotBackup tool to back up the embedded MySQL database.

  Tip To restore the database after backing it up with the mysql command, use MySQL. To restore the database after backing it up with InnoDB HotBackup and applying the logs, shut down the vFoglight Management Server, copy the backup files to *<vfoglight_home>/mysql/data*, and start the vFoglight Management Server

- Perform a full system backup, including the file system and the Windows Registry, but excluding the MySQL data and transaction logs.

Option 3
- Issue a `mysqldump` command to export the MySQL database to a remote drive or a backup tape.

  Tip This option does not require backing up the vFoglight installation directory. To restore vFoglight after choosing this backup method, you need to complete the following actions:
  1. Install the vFoglight Management Server and any cartridges that existed in the previous installation.
  2. Shut down vFoglight.
  3. Delete the MySQL data files.
  4. Start MySQL and import the exported dump file.
  5. Shut down MySQL.
  6. Start vFoglight.
  Alternatively, instead of steps 3 through 6, use the InnoDB HotBackup tool to back up the embedded MySQL database.

vFoglight Two Tier

vFoglight Management Server on Windows with MySQL on a remote computer

Option 1
- Issue a `mysqldump` command to export the MySQL database.

  Tip To restore the database after choosing this backup method, use MySQL.

- Stop the vFoglight Management Server.
- Use backup tools from your Windows environment to back up the vFoglight installation directory.

vFoglight Management Server on Windows with Oracle on a remote computer

Option 1
- Use Oracle tools to back up the database.

  Tip To restore the database after choosing this backup method, use Oracle tools.

- Stop the vFoglight Management Server.
- Use backup tools from your Windows environment to back up the vFoglight installation directory.

The procedures below contain detailed information on how to back up the vFoglight installation directory and the database, without backing up the file system or the Windows registry.

To back up vFoglight on a Windows system:

1 Select **Stop vFoglight** from the **Start** menu to shut down the vFoglight Management Server.

   If you are running vFoglight as a Windows service, stop the service by choosing **Start > Programs > Administrative Tools > Services**, and stopping the vFoglight Management Server service.

   Important If you are using an external database and intend to upgrade vFoglight after backing it up, you should leave the database running. Doing so allows the installer to successfully upgrade the database.

   Note Failing to shut down the vFoglight Management Server correctly may result in errors.

2 Verify that the vFoglight Management Server is stopped.

   a Press **Ctrl** + **Alt** + **Delete** on your keyboard, then click **Task Manager**.

      The **Windows Task Manager** opens.

   b Select the **Processes** tab to inspect the list of processes running on your system.

      If the fms.exe process is not running, the vFoglight Management Server is stopped.

3 Back up the entire vFoglight installation directory. For detailed instructions, see "To back up the vFoglight installation directory:" on page 92.

4 Back up the entire database used by the vFoglight Management Server:

- If your system uses an Oracle database, refer to "To back up an Oracle database used by the vFoglight Management Server" on page 92 for instructions.
- If your system uses a MySQL database, refer to "To back up a MySQL database using MySQL commands:" on page 94 for instructions.

The vFoglight backup on a Windows system is now complete.

To back up the vFoglight installation directory:

1 Browse to the directory one level above the vFoglight installation directory, usually this is *C:\Program Files\vizioncore*.

2 Right-click the vFoglight installation directory. Select **Send To Compressed**.

A zip archive of the vFoglight installation directory will be created. This may take several minutes.

Note   The archive must include the ./config, ./cartridge, ./support, ./licence, and ./scripts directories and all their content.

3 Move the *vFoglight.zip* file to the desired location.

The backup of the vFoglight installation directory is now complete.

To back up an Oracle database used by the vFoglight Management Server

1 Log in to the Oracle server machine.

2 Ensure that PATH and LD_LIBRARY_PATH & ORACLE_HOME are all set correctly.

On Windows systems:

a Open a Windows Explorer window, and right-click on **My Computer**.

b Select **Properties**.

The System Properties window is displayed.
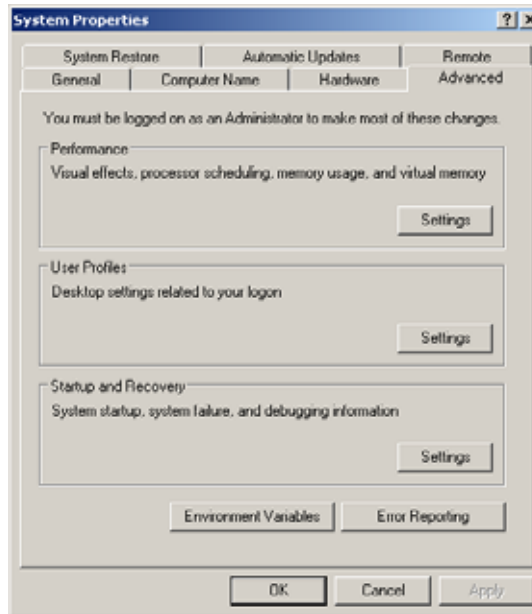
c   Click the **Advanced** tab and click **Environment Variables**.

The **Environment Variables** window is displayed.
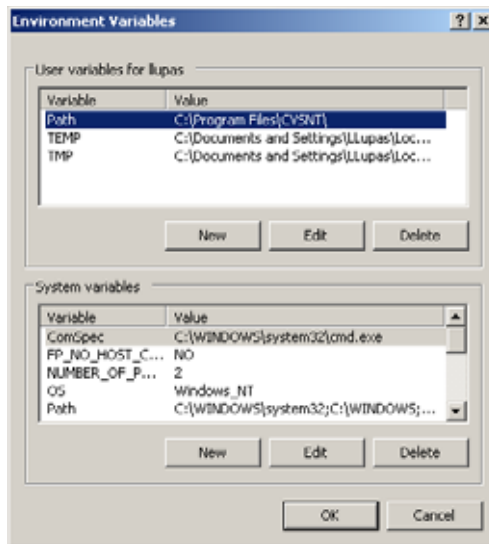
d Visually inspect the values associated with the PATH and LD_LIBRARY_PATH
   & ORACLE_HOME variables.

3 Export the Oracle database. Use the following syntax in the Oracle command
shell:

```
cd $ORACLE_HOME/bin
```

```
exp <db_usr>/<db_pwd>@<ORACLE_SID>
file=<export_filename>.dbdump
```

A .dbdump file is created.

The backup of the Oracle database is now complete.

To back up a MySQL database using MySQL commands:

1 Log in to the MySQL server machine.

2 Export the MySQL database. Use the following syntax in the MySQL command
shell:

```
mysqldump -u [database_name] -p
    -P[database_port_number] FOGLIGHT
    > [backupfile_name].sql
```

Where

- `database_name` is the database name, as configured by the `foglight.database.name` parameter in *<vfoglight_home>/config/ foglight.config*.

- `database_port_number` is the database port number, as configured by the `foglight.database.port` parameter in *<vfoglight_home>/config/ foglight.config*.

- `backupfile_name` is the name of the backup SQL file.

3 After the backup SQL file is created, stop the MySQL database by issuing the `shutdownDb.bat` command from the *<vfoglight_home>/bin* directory.

4 Verify that the database is down by verifying that the database process, `mysqld.exe`, is no longer running using the Task Manager.

The backup of the MySQL database is now complete.

> **Note** vFoglight Management Server ships with the InnoDB Hot Backup® tool. You can use this tool to back up an embedded MySQL database as an alternative to the above procedure. For information on how to use this tool, see "To back up an embedded MySQL database using the InnoDB Hot Backup tool:" on page 95.

To back up an embedded MySQL database using the InnoDB Hot Backup tool:

1 Create a directory structure that will contain the backup files.

You can create a master directory with two subdirectories: one that stores configuration files that will be used by the InnoDB Hot Backup tool, and another one, that stores the backup files. For example:

- *<vfoglight_home>/backup/config*
- *<vfoglight_home>/backup/data*

Where v*foglight_home* contains the path to the vFoglight installation directory. For example, its default location on Windows is *C:\Vizioncore\vFoglight*.

2 Create two configuration files for the InnoDB Hot Backup tool, each containing the information about

- the data that is to be backed up: `my.cnf`
- the backup location: `backup.cnf`

Open a text editor and create the two configuration files using the following syntax.

my.cnf

```
datadir="vfoglight_home/mysql/data"
innodb_data_home_dir="vfoglight_home/mysql/data"
innodb_data_file_path=ibdata1:10M:autoextend
```

```
innodb_log_group_home_dir="vfoglight_home/mysql/data"
set-variable=innodb_log_files_in_group=2
set-variable=innodb_log_file_size=64
```

backup.cnf

```
datadir="path_to_backup_data"
innodb_data_home_dir="path_to_backup_data"
innodb_data_file_path=ibdata1:10M:autoextend
innodb_log_group_home_dir="path_to_backup_data"
set-variable=innodb_log_files_in_group=2
set-variable=innodb_log_file_size=64
```

Where:

- *vfoglight_home* contains the path to the vFoglight installation directory.

- *path_to_backup_data* contains the path to the directory that is to contain the backup files, as defined in step 1.

    For example, *C:\Vizioncore\vFoglight\backup\data*.

Important   Use the back slash character '\' as a directory separator on Windows platforms.

When you are done, save the files in the *config* directory that you have created in step 1.

3 Open a Command Prompt window and navigate to the directory in which vFoglight stores the MySQL executable files, *<vfoglight_home>/vFoglight/mysql/bin*.

4 Complete one of the following steps, depending on the type of backup you want to create.

- To create an uncompressed backup, issue the following command:

```
C:\Vizioncore\vFoglight\mysql\bin>ibbackup
    ..\..\backup\config\my.cnf
    ..\..\backup\config\backup.cnf
InnoDB Hot Backup version 3.0.0; Copyright 2002-2005
Innobase Oy
License A11983 is granted to Vizioncore, Inc.

This program is legally licensed to Vizioncore
to be used in connection with a product of
Vizioncore only.

Type ibbackup --license for detailed license terms,
--help for help
```

```
Contents of ..\..\backup\config\my.cnf:
innodb_data_home_dir got value
...
Contents of ..\..\backup\config\backup.cnf:
innodb_data_home_dir got value
...
ibbackup: Found checkpoint at lsn 0 282033535
ibbackup: Starting log scan from lsn 0 282033152
...
ibbackup: Progress in MB: 100 200
080922 15:29:54 ibbackup: Full backup completed!
```

or

• To create a compressed backup, issue the following command:

```
C:\Vizioncore\vFoglight\mysql\bin>ibbackup
    --compress ..\..\backup\config\my.cnf
    ..\..\backup\config\backup.cnf
InnoDB Hot Backup version 3.0.0; Copyright 2002-2005
Innobase Oy
License A11983 is granted to Vizioncore, Inc.

This program is legally licensed to Vizioncore
to be used in connection with a product of
Vizioncore only.

Type ibbackup --license for detailed license terms,
--help for help

Contents of ..\..\backup\config\my.cnf:
innodb_data_home_dir got value
...
Contents of ..\..\backup\config\backup.cnf:
innodb_data_home_dir got value
...
ibbackup: Found checkpoint at lsn 0 282084809
ibbackup: Starting log scan from lsn 0 282084352
...
ibbackup: Progress in MB: 100 200
ibbackup: A copied database page was modified at
0282085337
ibbackup: Scanned log up to lsn 0 282085565
ibbackup: Was able to parse the log up to lsn 0
282085565
ibbackup: Maximum page number for a log record 11925
```

```
ibbackup: Compressed 210 MB of data files to 36 MB
(compression 82%).
080922 15:29:54 ibbackup: Full backup completed!
```

5 View the contents of the backup directory by issuing the following command:

```
C:\Vizioncore\vFoglight\mysql\bin>dir
   C:\Vizioncore\vFoglight\backup\data
 Volume in drive C is System
 Volume Serial Number is BCD1-A216

 Directory of C:\Vizioncore\vFoglight\backup\data

10/24/2008   10:55 AM <DIR> .
10/24/2008   10:55 AM <DIR> ..
10/24/2008   10:55 AM 5,632 ibbackup_logfile
10/24/2008   10:55 AM 02:16 PM 77,594,624 ibdata1
             2 File(s) 77,600,256 bytes
             2 Dir(s)  49,386,782,720 bytes free
```

Note   The above example illustrates the process of backing up a MySQL database on Windows, which uses the back slash character as a directory separator and the *dir* command to list files.

The backup directory contains one data file, *ibdata1*, and a log file, *ibbackup_logfile*. The backup process copies different database pages at different times. The log file, *ibbackup_logfile*, specifies the order in which the pages are backed up. Applying the log file to the backup data associates each database page with a sequence in the log file, and creates one or more log files for each data file, allowing you to successfully restore the database from the backup data when required.

6 Apply the log file to the backup data by issuing the following command:

Note   The example below illustrates the process of backing up a MySQL database on Windows, which uses the back slash character as a directory separator.

```
C:\Vizioncore\vFoglight\mysql\bin>ibbackup --apply-log
   C:\Vizioncore\vFoglight\backup\config\backup.cnf.txt
```

Note   The code line above illustrate the process of applying logs to an uncompressed backup.
If you are applying logs to a compressed backup, use the --*uncompress* option. For
example:

```
C:\Vizioncore\vFoglight\mysql\bin>ibbackup --apply-log
--uncompress C:\Vizioncore\vFoglight\backup\config
\backup.cnf
```

For more information about the command-line options for creating compressed and
uncompressed backups, see

```
InnoDB Hot Backup version 3.0.0; Copyright 2002-2005
    Innobase Oy
License A11983 is granted to Vizioncore, Inc.

This program is legally licensed to Vizioncore
    to be used in connection with a product of
    Vizioncore only.

Type ibbackup --license for detailed license terms, --help
    for help

Contents of C:\Vizioncore\vFoglight\backup\config\
    backup.cnf:
innodb_data_home_dir got value
    C:\Vizioncore\vFoglight\backup\data
innodb_data_file_path got value ibdata1:10M:autoextend
datadir got value C:\Vizioncore\vFoglight\backup\data
innodb_log_group_home_dir got value
    C:\Vizioncore\vFoglight\backup\data
innodb_log_files_in_group got value 2
innodb_log_file_size got value 134217728

081024 10:56:21 ibbackup: ibbackup_logfile's creation
    parameters:
ibbackup: start lsn 0 43520, end lsn 0 43655,
ibbackup: start checkpoint 0 43655
InnoDB: Doing recovery: scanned up to log sequence number 0
    43655
InnoDB: Starting an apply batch of log records to the
    database...
InnoDB: Progress in percents: 0 1 2 3 4 5 6 7 8 9 10 11 12
```

```
        13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
        32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
        51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69
        70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88
        89 90 91 92 93 94 95 96 97 98 99
Setting log file size to 0 134217728
InnoDB: Progress in MB: 100
Setting log file size to 0 134217728
InnoDB: Progress in MB: 100
ibbackup: We were able to parse ibbackup_logfile up to
ibbackup: lsn 0 43655
ibbackup: The first data file is
    'C:\Vizioncore\vFoglight\backup\data\ibdata1'
ibbackup: and the new created log files are at
    'C:\Vizioncore\vFoglight\backup\data\'

081024 10:56:35 ibbackup: Full backup prepared for
    recovery successfully!
```

7 View and observe the contents of the backup directory by issuing the following command:

Note   The example bellow illustrates the process of backing up a MySQL database on Windows, which uses the back slash character as a directory separator and the *dir* command to list files.

```
C:\Vizioncore\vFoglight\mysql\bin>dir
    C:\Vizioncore\vFoglight\backup\data
 Volume in drive C is System
 Volume Serial Number is BCD1-A216

 Directory of C:\Vizioncore\vFoglight\backup\data

10/24/2008    10:56 AM <DIR>   .
10/24/2008    10:56 AM <DIR>   ..
10/24/2008    10:55 AM 5,632 ibbackup_logfile
10/24/2008    10:55 AM 10,485,760 ibdata1
10/24/2008    10:56 AM 64 ib_logfile0
10/24/2008    10:56 AM 64 ib_logfile1
              4 File(s) 278,922,240 bytes
              2 Dir(s)  48,747,614,208 bytes free
```

In addition to the files *ibbackup_logfile* and *ibdata1* that were created at backup time (see step 5), the backup directory now includes two additional log files, *ib_logfile0* and *ib_logfile1*, which means that the logs have been applied successfully.

Your embedded MySQL database is successfully backed up. For instructions on how to restore the database MySQL database using these files, see "To restore an embedded MySQL database previously backed up using the InnoDB tools:" on page 104. For complete information about the InnoDB Hot Backup tool, visit the following URL: *http://www.innodb.com/hot-backup/*

Upgrading vFoglight

The vFoglight Management Server installer checks for an existing version 5.x installation of the Management Server in the target directory. If an existing 5.x installation is found in the directory, you are prompted to choose whether you want to install a new version of the vFoglight Management Server, or to upgrade that instance of the Management Server.

If you would like to install a new instance of the same version, you must select the **New Install** option in the installer and choose a different (and empty) installation folder. You cannot re-install the Management Server into the same directory as an existing installation of the same version.

When running in the upgrade mode, the installer upgrades all files in the target directory and upgrades the database. All product files in the target directory are overwritten; however, any customizations already made are retained.

Caution   Before upgrading vFoglight to a newer version, it is necessary to back up the previous vFoglight installation directory and the database used by the existing vFoglight Management Server (for instructions, see "Backing Up vFoglight" on page 89).

If you are using an external database and intend to upgrade vFoglight after backing it up, you should shut down the vFoglight Management Server, but leave the database running. Doing so allows the installer to successfully upgrade the database.

Note   If you encounter any errors during the upgrade process, you can stop the procedure and restore the previous vFoglight installation (see "Restoring vFoglight" on page 102), provided that it has been correctly backed up.

Restoring vFoglight

"Restoring" a physical backup means reconstructing it and making it available to users. This section outlines how to restore an old vFoglight installation.

Note   In order to restore a previous vFoglight installation, you must have a backed up copy of that version. For information about how to back up a vFoglight system, see "Backing Up vFoglight" on page 89.

To restore a previous vFoglight installation:

1   Restore the database used by the old vFoglight Management Server, from the database export file:

   •   If your system contains an Oracle database, see "To restore an Oracle database from the database export file:" on page 102 for instructions.

   •   If your system contains a MySQL database, see "To restore a MySQL database from the database export file:" on page 103 for instructions.

2   Restore the old vFoglight installation directory. For instructions, see "To restore the previous vFoglight installation directory:" on page 104.

3   Ensure that the vFoglight Management Server starts up successfully on the restored installation:

```
cd <installation_dir>/bin
./fms
```

   The previous vFoglight installation is now restored.

To restore an Oracle database from the database export file:

1   Log in to the Oracle database server machine.

2   If necessary, delete the database you are going to restore, so that all the tables in the database are deleted (in other words, drop the database). Choose one of the following options:

   •   Locate the *oracle_drop_db.sql* script in the *scripts/sql* directory of your vFoglight Management Server installation, and then run that script using the following syntax:

```
sqlplus <dbadmin_usr>/<dbadmin_pwd>@<ORACLE_SID>
```

```
SQL> @ <foglight_home>/scripts/sql/oracle_drop_db.sql
```

Note The files *oracle_drop_dp.sql* and *oracle_drop_db.sql* are included with vFoglight when you use an Oracle database, The are located in the *<foglight_home>/scripts/sql* directory.

or

- Execute the drop user command from the command line using the following syntax:

```
drop USER <db_usr> cascade;
```

3 Create the new database using the following syntax:

```
sqlplus <dbadmin_usr>/<dbadmin_pwd>@<ORACLE_SID>

SQL> @ <path_to_sql_script>/oracle_create_db.sql
```

4 Import the database export file into the Oracle database using the following syntax:

```
cd $ORACLE_HOME/bin

imp<db_usr>/<db_pwd>@<ORACLE_SID>
file=<export_filename>.dbdump full=yes
```

Note The ".dbdump" is the backup file you must create in order to restore your Oracle database (see "To back up an Oracle database used by the vFoglight Management Server" on page 92).

The Oracle database is now restored.

To restore a MySQL database from the database export file:

1 Log into the MySQL server machine.

2 Delete the database you are going to restore, so that all the tables in the database are deleted (i.e., drop the database).

   a Log into the MySQL database and execute the following command:

```
mysql -u root
```

   b Execute the following SQL statement:

```
DROP DATABASE <database name>
```

3 After running `mysql -u root`, execute the following SQL statement:

```
CREATE DATABASE <database name>
```

4 After running `mysql -u root`, run the SQL script created by the backup. Use the following syntax:

```
SOURCE <path to .sql file>
```

Note The ".sql" is the backup file you must create in order to restore your MySQL database (see "To back up a MySQL database using MySQL commands:" on page 94).

The MySQL database is now restored.

To restore the previous vFoglight installation directory:

1 cd to the directory where you want to install vFoglight.

2 If the backup of the old installation is not compressed, continue with step . If the backup is a ZIP file, first unzip it:

gunzip <path_to_zipfile>/<old_installation_zipfile>.tar.gz

The old vFoglight installation directory is now restored.

To restore an embedded MySQL database previously backed up using the InnoDB tools:

1 Stop the vFoglight Management Server.

2 Copy the backup data that was created with the InnoDB tool, including the data files and the log files, to the directory *<vfoglight_home>/mysql/data*. The backup data and log files use the following naming convention:

- *ibdata<1-n>*. The name of the first data file is *ibdata1*, of the second *ibdata2*, and so on. The number of data files depends on the size of the backed up database.
- *ib_logfile<0-n>*. The name of the first log file is *ib_logfile0*, of the second *ib_logfile1*, and so on. The number of log files depends on the size of the backed up database and the size of the log file specified in the backup configuration file, *backup.cnf*.

For complete information about the process of backing up an embedded MySQL database using InnoDB, see "To back up an embedded MySQL database using the InnoDB Hot Backup tool:" on page 95

3 Start the vFoglight Management Server.

Your database files are now successfully restored to their original location.

3

Managing Users and Security

This chapter introduces you to the concepts and terms related to managing security in vFoglight and looks into security-related components that you can manage using the Administration module. It also takes you through the process of creating and managing users, groups, and roles in vFoglight.

Note	In order to complete each of the procedures in this chapter, your user account must belong to a group with the Security role. For more information, see "Managing Groups" on page 118.

This chapter contains the following sections:

About Security in vFoglight

In vFoglight, user management consists of three related entities:

- *Users*. A user has a user name and a password and can belong to one or more groups. Logging in to vFoglight as a specific user authorizes you to perform a certain set of actions (based on the roles that have been assigned to the group(s) to which the user belongs). vFoglight can store user passwords on the vFoglight Management Server, or in an external directory

  For more information, see "Managing Users" on page 107, "Configuring Password Settings" on page 135, and "Configuring Directory Services" on page 139.

- *Groups*. A group can contain one or more users. Roles are assigned to users through groups. You can assign roles and add users to groups.

  For more information, see "Managing Groups" on page 118.

- *Roles*. The default roles included with vFoglight dictate what actions users can perform with regard to one or more vFoglight features or components. vFoglight System Administrators can also create custom roles. Roles are assigned to groups. Users in a group have the roles that are assigned to that group.

  For more information, see "Managing Roles" on page 127.

The following diagram illustrates the interrelationship of users, groups, and roles.

Users   Groups   Roles
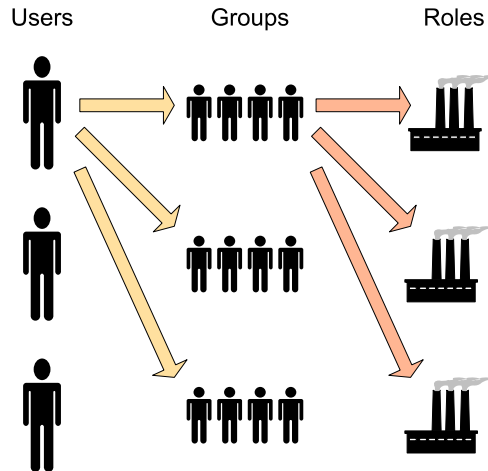
Managing Users

There are three types of users in vFoglight:

- *Internal.* Internal users include the users that are created after the installation. When you create an internal user in vFoglight, you assign a user name and password to that user. There are restrictions surrounding password formatting. See "Configuring Password Settings" on page 135 for details.

- *Built In.* Built-in users include the users that come with vFoglight. There is currently one default account that is included with vFoglight. Unless you specify a different user name at installation time, that user name is *foglight*. This account has full access to all of vFoglight features

  Note   Built-in groups cannot be deleted.

- *External*. After being validated by vFoglight, external users are mapped from one of the LDAP-compatible directory services supported by vFoglight (Active Directory, Sun Java Systems Directory Server, and OpenLDAP). For more information about configuring vFoglight to use an external directory service, see "Configuring Directory Services" on page 139.

Roles are assigned to a user through groups: when a user belongs to a group, the roles that are assigned to that group are also assigned to the user. A user can belong to one or more groups. For more information about groups, see "Managing Roles" on page 127.

If you belong to a group that includes the Security role, the Manage Users dashboard allows you to manage user accounts, add users to groups, and manage user passwords. For more information on how to use the Manage Users dashboard, see the following sections:

- "Accessing the Manage Users Dashboard" on page 108
- "Creating Users" on page 111
- "Adding Users to Groups" on page 112
- "Changing Passwords" on page 114
- "Forcing Password Changes" on page 115
- "Unlocking Passwords" on page 115
- "Deleting Internal Users" on page 117

Accessing the Manage Users Dashboard

The Manage Users dashboard contains a table that lists all of the users that have been created in the Administration Module or imported from an LDAP-compatible directory service supported by vFoglight, the groups to which these users belong, and the roles that are available to them. This dashboard also includes controls for managing user settings, creating new users, deleting non-default users, filtering the list of users, forcing a password change for new users, and unlocking a user who has been locked out after a pre-defined number of bad login attempts.

Note   Roles are not assigned directly to users. Instead, they are made available to users through the groups to which they belong. See "Managing Groups" on page 118 for complete information assigning roles and adding users to groups.

To access the Manage Users dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

1   Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Users & Security > Manage Users**.

The Manage Users dashboard appears in the display area, showing a list of all existing users:

3   To sort the list by name, group, role, or type, click the **Name**, **Groups**, **Roles (Read Only)**, or **Type** column headings as required.

4   To filter the list of users, use one or more of the following boxes at the top of the Manage Users list:

- **Name**: Type the user name for which you want to filter.
- **Groups**: Type the group name for which you want to filter.
- **Roles**: Type the role name for which you want to filter.

For example, to list only the users whose name starts with "demo", in the **Name** box, type demo.

The Manage Users list refreshes, showing the list of users whose name matches the filter pattern.
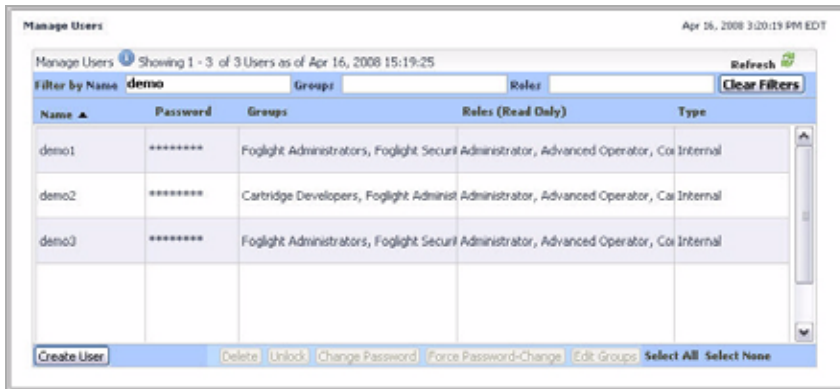
To clear the filters, click **Clear Filters**.

The Manage Users list refreshes, showing the list of all users.
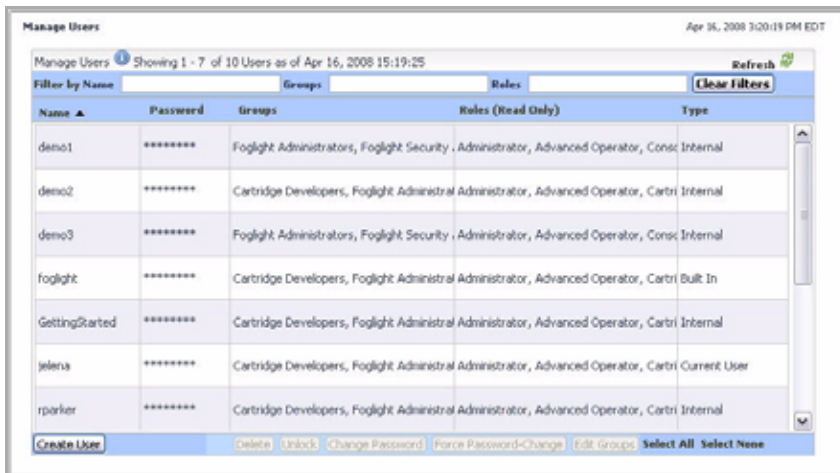
From here, you can proceed to any of the following procedures:

- "Creating Users" on page 111
- "Adding Users to Groups" on page 112
- "Changing Passwords" on page 114

Creating Users

Use the Create User button on the Manage Users dashboard to add a user account to vFoglight, as outlined below.

Alternatively, use the security:createuser **fglcmd** command to create a user. For more information, see the *Command-Line Reference Guide*.

To create a user:

Note   This procedure continues from "Accessing the Manage Users Dashboard" on page 108.

---

1   In the Manage Users dashboard, click the **Create User** button in the lower-left corner.

The **Create User** dialog box appears.

2   Specify the name and password of the user that you want to create.

   a   In the **Create User** dialog box, in the **Name** box, type the user name.

   For example: test.

   b   In the **Password** and **Confirm Password** boxes, type the user password.

   Note   The **Password** box is encrypted.

   For example: test123.

As you type the password into the **Password** and **Confirm Password** boxes, asterisk '*' characters appear.

Note Passwords must meet certain criteria. For example, by default, each password must be between seven (7) and sixteen (16) characters long. For more information, see "Configuring Password Settings" on page 135. If you specify a password that is longer than sixteen (16) characters for an end-user, that user cannot log into vFoglight.

c Click **Create**.

The **Create User** dialog box closes and the Manage Users dashboard refreshes to show the newly-created user account.

test	********			Internal

When you create users, their type appears as **Internal** on the listing.

Once you create a new user, you should ensure that the user changes their password from the one you set in the **Create User** dialog box.

- If the user belongs to group that has a Security role which allows them to access to the Manage Users dashboard, you can instruct the user to change the password using the Change Password button on the Manage Users dashboard. For instructions, see "Changing Passwords" on page 114.

- If the user has no access to the Manage Users dashboard, you can force a password change the first time the user attempts to log into vFoglight. For instructions on how to force a password change, see "Forcing Password Changes" on page 115.

Adding Users to Groups

Use the Edit Groups button on the Manage Users dashboard to add a user to one or more groups, as outlined in the procedure below.

Alternatively, you can use the Manage Groups dashboard to assign users or roles to one or more groups. For information, see "Editing Users in Groups" on page 123 and "Assigning Roles to a Group" on page 124.

Alternatively, you can assign groups to users using the security:assigngroup command that comes with the **fglcmd** interface. For more information, see the *Command-Line Reference Guide*.

To add a user to groups:

Note   This procedure continues from "Creating Users" on page 111.

---

1 In the Manage Users dashboard, select the row containing the user account whose groups you want to edit.

2 Click the **Edit Groups** button in the lower-right corner.

The **Edit Groups** dialog box appears.
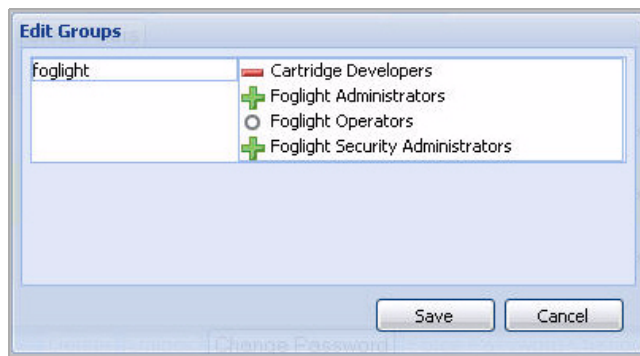
Note   The dialog box lists default vFoglight groups. If you previously added any groups, they also appear in the dialog. For information on how to add groups, see "Creating Groups" on page 122.

3 In the **Edit Groups** dialog box, select the groups to which you want the user to belong by clicking the appropriate symbol to the left of the group name.

- ![plus] : The user account is added or already belongs to this group.
- ![minus] : The user account has been removed from or does not have access to this group.
- ![circle] : There is no change in group assignment.

For example, to add a user to the vFoglight Administrators and vFoglight Security Administrators groups, ensure that the green plus sign appears to the left of the **vFoglight Administrators** and **vFoglight Security Administrators** entries, and that the red minus sign appears to the left of the other groups in the **Edit Groups** dialog box.

4 Click **Save**.

The **Edit Groups** dialog box closes and the Manage Users dashboard refreshes to show the groups that you added to the user account.

foglight | ******** | Foglight Administrators, Foglight Security Administrators, Foglight Users

Changing Passwords

Use the Change Password button on the Manage Users dashboard to change a user's password, as outlined below.

To change a user's password:

Note This procedure continues from ".

1 In the Manage Users dashboard, select the row containing the user account whose password you want to change.

2 Click the **Change Password** button at the bottom of the Manage Users dashboard.

The **Change Password** dialog box appears.

3 Specify the new password.

a In the **Change Password** dialog box, type the new password into each of the the **Password** and **Confirm Password** boxes.

Note The **Password** box is encrypted.

For example: test456.

As you type the password into the **Password** and **Confirm Password** boxes, asterisk '*' characters appear.

    b Click **OK**.

  4 The **Change Password** dialog box closes and vFoglight updates the user password in the database.

Forcing Password Changes

When you create a user account for a user that has no access to the Manage Users dashboard, use the Force Password-Change button to ensure that the user changes their password the first time they attempt to log into vFoglight.

To force a password change for a user:

Note   This procedure continues from ".

---

  1 Select the row containing the user whose password change you want to initiate the next time they attempt to log in.

  2 Click the **Force Password-Change** button at the bottom of the Manage Users dashboard.

     The **Confirm Force Password-Change** dialog box appears.

  3 Click **OK** to confirm the forced password change.

     The **Confirm Force Password-Change** dialog box closes.

     The next time the user attempts to log in they will be prompted to change their password.

Unlocking Passwords

If a user attempts to log in with an incorrect password several times in a row, vFoglight locks the user's account. You can configure the number of unsuccessful login attempts

using the Configure Password Settings dashboard. For more information, see "Editing Password Settings" on page 137.

By default any user passwords that become locked stay in that state for 15 minutes after which vFoglight unlocks them. To unlock a user account, use the Unlock button on the Manage Users dashboard.

To unlock a user's password:

Note   This procedure continues from "Accessing the Manage Users Dashboard" on page 108.

- • If possible, advise the user whose password has been locked to wait 15 minutes from the moment the password was locked for vFoglight to unlock the password automatically.

  or

  Complete the following steps:

  a Open the Manage Users dashboard

  For instructions, see "Accessing the Manage Users Dashboard" on page 108.

  b In the Manage Users dashboard, select the row containing the user account whose password you want to change.

  The **Name** column shows the following message for each user whose account is locked: This user is locked!

  c Click the **Unlock** button at the bottom of the Manage Users dashboard.

  The **Confirm Unlock** dialog box appears, asking you to confirm the unlock operation.
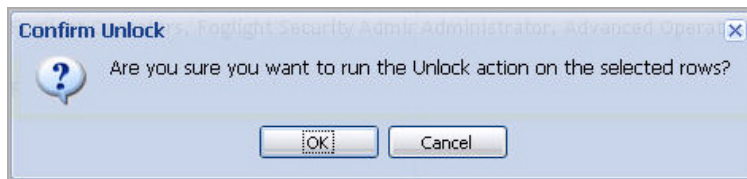
  d In the **Confirm Unlock** dialog box, click **OK**.

  The dialog box closes and the Manage Users dashboard refreshes, showing the user name in the **Name** column.

Deleting Internal Users

Use the Delete button on the Manage Users dashboard to delete user accounts from vFoglight.

You can only delete those users that you add to vFoglight after the installation. Their type appears as Internal on the Manage Users dashboard. You cannot delete the user accounts that are included with vFoglight. Their type appears as Built In. If a Built In or Internal User is the current user, their type appears as Current User.
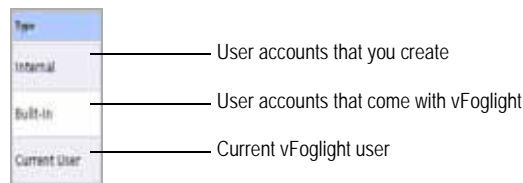
User accounts that you create
User accounts that come with vFoglight
Current vFoglight user

For more information about the types of groups that exist in vFoglight, see "Managing Groups" on page 118.

Alternatively, you can delete internal users using the `security:deleteuser` command that comes with the **fglcmd** interface. For more information, see the *Command-Line Reference Guide*.

*To delete an internal user:*

Note   This procedure continues from "Accessing the Manage Users Dashboard" on page 108.

---

1 In the Manage Users dashboard, select the row containing the user account that you want to delete.

2 Click the **Delete** button at the bottom of the Manage Users dashboard.

    The **Confirm Delete** dialog box appears, asking you to confirm the delete operation.

Confirm Delete

? Are you sure you want to run the Delete action on the selected rows?

OK   Cancel
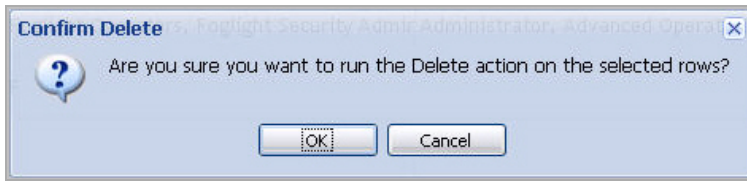
3 In the **Confirm Delete** dialog box, click **OK**.

The dialog box closes and the Manage Users dashboard refreshes.

4 Observe the Manage Users dashboard.

The user account that you deleted no longer appears in the list.

Managing Groups

A group can contain users. Roles are assigned to groups. In turn, a role that is assigned to a group is also assigned to each member of that group.

There are three types of roles in vFoglight:

- *Internal.* Include the groups that are created using the Manage Groups dashboard after the installation.

- *Built In.* Include the groups that come with vFoglight. They are as follows:

    - *Cartridge Developers*. Allows the users to modify core dashboards and system modules.

    - *Foglight Administrators*. Enables the users to access all of the dashboards that come with the Administration module, with the exception of the Users & Security dashboards. Additionally, it enables the users to use build-oriented dashboards or build their own dashboards.

    - *Foglight Operators*. Allows the users to have access to core and cartridge dashboards, and to create new dashboards.

    - *Foglight Security Administrators*. Provides access to all dashboards under the Users & Security node in the Administration module.

    Note Built-in groups cannot be deleted.

- *External*. The groups that are mapped from an LDAP-compatible directory service supported by vFoglight as part of the process of mapping external users.

For more information about configuring vFoglight to use an external directory service, see "Configuring Directory Services" on page 139.

Roles are assigned to a user through groups: when a user belongs to a group, the roles that are assigned to that group are also assigned to the user. A user can belong to one or more groups.

If you belong to a group that includes the Security role, the Manage Groups dashboard allows you to create and manage groups, add users to groups, and assign roles to groups. For more information on how to use the Manage Groups dashboard, see the following sections:

- "Accessing the Manage Groups Dashboard" on page 119
- "Creating Groups" on page 122
- "Editing Users in Groups" on page 123
- "Assigning Roles to a Group" on page 124
- "Deleting Internal Groups" on page 126

Accessing the Manage Groups Dashboard

The Manage Groups dashboard contains a table that lists all of the groups that have been created in the Administration Module or imported from an LDAP-compatible directory service supported by vFoglight, the users that belong to these groups, and the roles that have been assigned to each group.

This page also contains controls for managing group settings, creating new groups, and deleting non-default groups.

To access the Manage Groups dashboard:

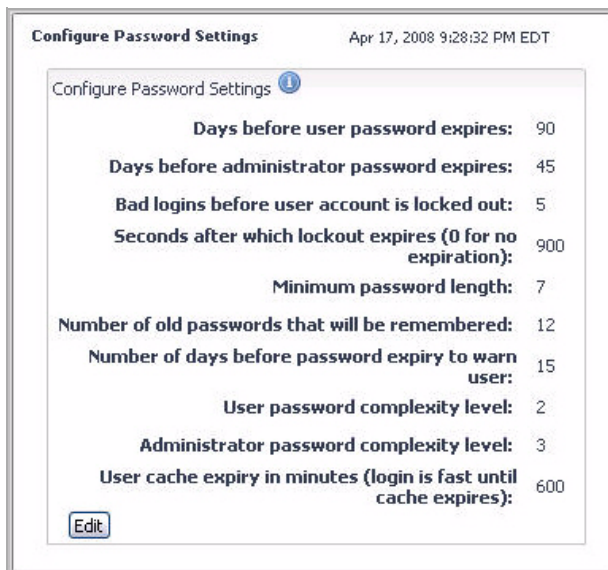**Note**   This procedure continues from "Getting Started with the Administration Module" on page 32.

1   Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Users & Security > Manage Groups**.

The Manage Groups dashboard appears in the display area, showing a list of all existing groups:
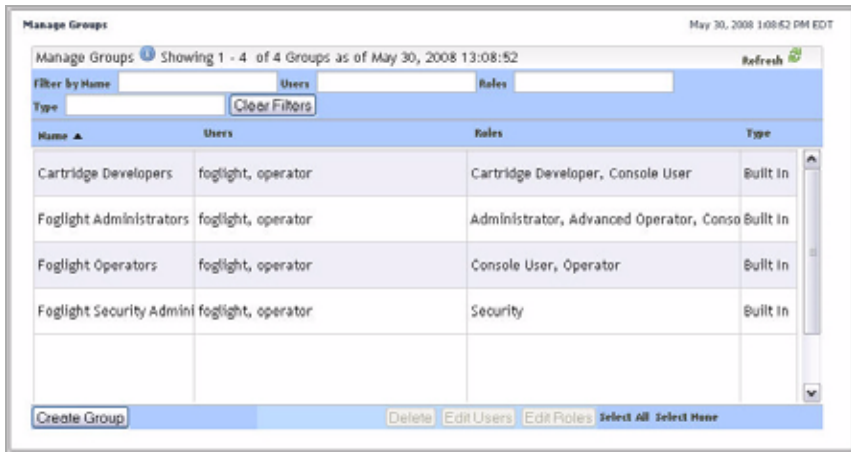
3 To sort the list by name, users, role, or type, click the **Name**, **Users**, **Roles**, or **Type** column headings as required.

4 To filter the list of groups, use one or more of the following boxes at the top of the Manage Users list:

- **Name**: Enter the group name for which you want to filter.
- **Users**: Enter the user name for which you want to filter.
- **Roles**: Enter the role name for which you want to filter.
- **Type**: Enter the type name for which you want to filter.

For example, to list only the groups whose name starts with "Foglight", in the **Name** box, type Foglight.

The Manage Groups list refreshes, showing the list of groups whose name matches the filter pattern.
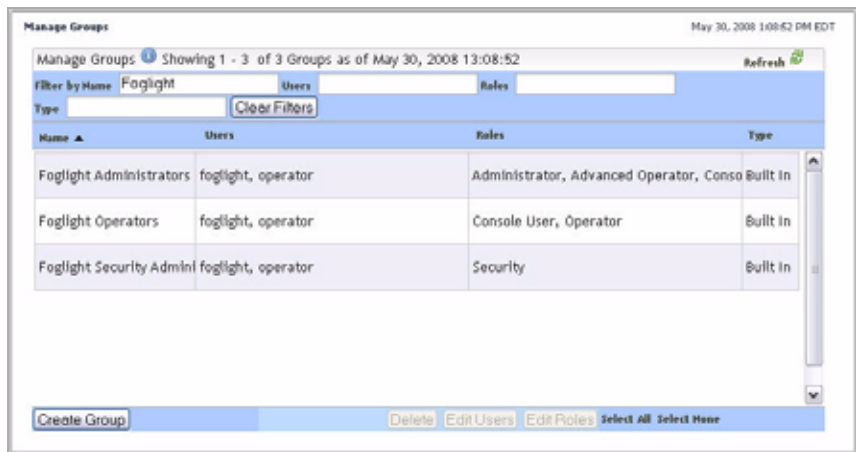
To clear the filters, click **Clear Filters**.

The Manage Groups list refreshes, showing the list of all groups.
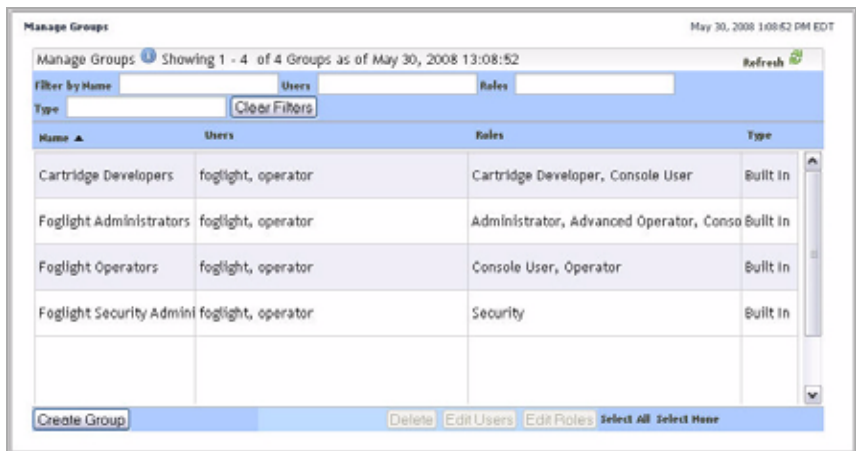
From here, you can proceed to any of the following procedures:

- "Creating Groups" on page 122
- "Editing Users in Groups" on page 123
- "Assigning Roles to a Group" on page 124

Creating Groups

Use the Create Group button on the Manage Groups dashboard to add a group to vFoglight, as outlined below.

Alternatively, you can create groups using the security:createuser command that comes with the **fglcmd** interface. For more information, see the *Command-Line Reference Guide*.

To create a group:
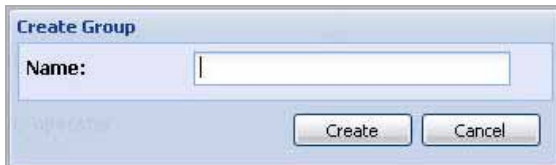
Note This procedure continues from "Accessing the Manage Groups Dashboard" on page 119.

---

1 In the Manage Groups dashboard, click the **Create Group** button in the lower-left corner.

The **Create Group** dialog box appears.

2 Specify the name of the group that you want to create.

a In the **Create Group** dialog box, in the **Name** box, type the user name.

For example: test.

b Click **Create**.

The **Create Group** dialog box closes and the Manage Groups dashboard refreshes to show the newly-created group.

When you create groups, their type appears as **Internal** on the listing.

Editing Users in Groups

Use the Edit Users button on the Manage Groups dashboard to quickly edit users in one or more groups.

Alternatively, if you need to edit groups for a single user account, use the Manage Users dashboard. For information, see "Adding Users to Groups" on page 112.

Another way to assign or remove users from groups is to use the security:assigngroup command that comes with the **fglcmd** interface. For more information, see the *Command-Line Reference Guide*.

To add users to a group:

Note   This procedure continues from "Creating Groups" on page 122.

---

   1 In the Manage Groups dashboard, select the row containing the group to which you want to add users.

   2 Click the **Edit Users** button in the lower-right corner on the left of the **Edit Roles** button.

The **Edit Users** dialog box appears.
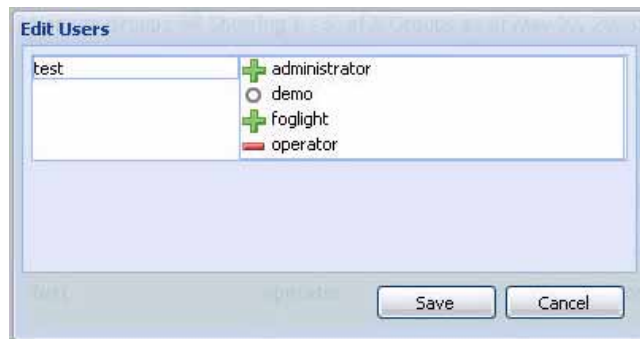
Note   The dialog box lists existing vFoglight users. If you added any users, they also appear in the dialog. For information on how to add users, see "Creating Users" on page 111.

   3 In the **Edit Users** dialog box, select the users that you want to add to the group by clicking the appropriate symbol to the left of the group name.

     •   ➕ : The user account is added or already belongs to this group.

- ▬ : The user account has been removed from or does not have access to this group.

- ◎ : There is no change in user assignment.

For example, to add the default *foglight* user account to the group, ensure that the green plus sign appears to the left of the **foglight** entry, and that the red minus sign appears to the left of the other groups in the **Edit Users** dialog box.

4 Click **Save**.

The **Edit Users** dialog box closes and the Manage Groups dashboard refreshes to show the users that you added to the group.

test	foglight		Internal

Assigning Roles to a Group

Use the Edit Roles button on the Manage Groups dashboard to quickly edit one or more roles for a group.

Alternatively, if you need to edit multiple groups for a single role, use the Manage Roles dashboard. For information, see "Editing Groups for a Role" on page 132.

Another way to assign or remove roles from groups is to use the security:assignrole command that comes with the **fglcmd** interface. For more information, see the *Command-Line Reference Guide*.

To assign roles to a group:

Note   This procedure continues from "Creating Groups" on page 122.

1 In the Manage Groups dashboard, select the row containing the group to which you want to assign one or more roles.

2 Click the **Edit Roles** button in the lower-right corner.

The **Edit Roles** dialog box appears.
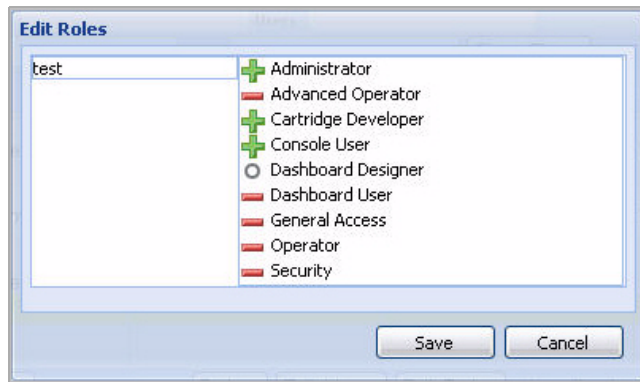
Note   The dialog box lists existing vFoglight roles. If you previously added any roles, they also appear in the dialog. For information on how to add roles, see "Creating Roles" on page 131.

3   In the **Edit Roles** dialog box, select the roles that you want to assign to the group by clicking the appropriate symbol to the left of the group name.

- ![+] : The role is added or already belongs to this group.
- ![-] : The role has been removed from or does not have access to this group.
- ![o] : There is no change in role assignment.

For example, to add default Administrator and Security roles to the group, ensure that the green plus sign appears to the left of **Administrator** and **Security** entries and that the red minus sign appears to the left of the other entries in the **Edit Roles** dialog box.

4   Click **Save**.

The **Edit Roles** dialog box closes and the Manage Groups dashboard refreshes to show the users that you added to the group.

Deleting Internal Groups

Use the Delete button on the Manage Groups dashboard to delete user accounts from vFoglight.

You can only delete those groups that you add to vFoglight after the installation. Their type appears as Internal on the Manage Users dashboard. You cannot delete any of the groups accounts that are included with vFoglight. Their type appears as Built In.
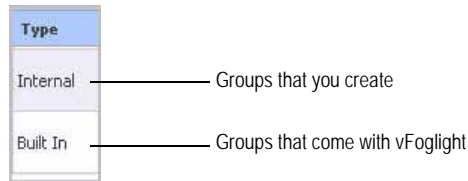
For more information about the types of groups that exist in vFoglight, see "Managing Groups" on page 118.

Alternatively, you can delete groups using the `security:deletegroup` command that comes with the **fglcmd** interface. For more information, see the *Command-Line Reference Guide*.

To delete an internal group:

Note   This procedure continues from "Accessing the Manage Groups Dashboard" on page 119.

1 In the Manage Groups dashboard, select the row containing the group that you want to delete.

2 Click the **Delete** button at the bottom of the Manage Groups dashboard.

A message box appears, asking you to confirm the delete operation.
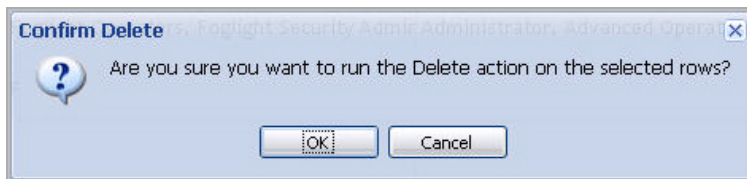
3 In the message box, click **OK**.

The message box closes and vFoglight deletes the user account.

4   Observe the Manage Groups dashboard.

The user account that you deleted no longer appears in the list.

Managing Roles

Roles are assigned to groups. A role that is assigned to a group is also assigned to each member of that group.

There are two types of roles in vFoglight:

- *Built-In*. They dictate what actions users can perform. That is, when a role is assigned to a group, it enables the members of that group to use specific features or components for which access is controlled.

  Built-In roles are also used in vFoglight to determine which dashboards appear and are accessible to each user. See the *vFoglight User Guide* for information about the relationship between roles and dashboards.

  Note   The Built-In roles cannot be deleted.

  vFoglight comes with the following Built-In roles:

  - *Administrator*. This role enables a user to access the Administration Module, the Web Console (web.xml), hidden Administration URLs, and the JMX-Console. An Administrator can manipulate agents, rules, derived metrics, registry variables, cartridges, types, and scripts. The only limitation for Administrators is that they cannot access or edit the Users and Security dashboard.

  - *Advanced Operator*. This role builds on the Operator role by adding the ability to access build-oriented dashboards such as the Service Builder, Application Builder, and the Report Builder, where users can add, manage, and manipulate scheduled reports.

  - *Cartridge Developer*. This role extends the Dashboard Designer role by allowing the user to modify core dashboards and system modules.

  - *Console User*. This role enables a user to access the Web Console (web.xml) only. It is the base level locked-down read-only role. Users assigned this role will not have access to core dashboards.

  - *Dashboard Designer*. This role builds on the Dashboard User role by adding the ability to access all dashboard tools such as Definitions, Data Sources, and

the Schema Browser. This role is for users who design dashboards using these advanced dashboard tools.

- *Dashboard User.* This role is similar to the Console User role, but with additional access to any additional dashboards associated with the user. This role also includes permission to create new dashboards, new reports, and to edit the dashboard environment.

- *General Access.* This role is for pre-5.2 cartridges installed on a version 5.2 or later vFoglight Management Server. The role will be added to the appropriate views so that dashboards from the cartridge will appear in the vFoglight interface.

  Note   The General Access role is not assigned to users, and cannot be used to log in.

- *Operator.* This is the base level role for monitoring in vFoglight. Users assigned this role have access to the core dashboard set such as Hosts, Alarms, Services, and Report Manager, with the ability to create new dashboards. This role also has access to any non-core cartridge dashboard, such as the OS Cartridge. This is the recommended default for new users.

- *Security.* This role provides access to all dashboards under Users and Security in the Administration Module.

- *Internal.* Users with the Security role can create Internal roles.

  New roles do not have any permission. They depend on how they are grouped with built-in roles to determine their behavior. For example, a new role can be created and applied to a group along with the Console User role to create a locked-down user group. This means users in this group would only have access to the dashboards specifically made available to the new role, and are able to log in to the web console.

Roles are assigned to a user through groups: when a user belongs to a group, the roles that are assigned to that group are also assigned to the user. A user can belong to one or more groups.

If you belong to a group that includes the Security role, the Manage Roles dashboard allows you to create and manage roles, and assign roles to groups. For more information on how to use the Manage Groups dashboard, see the following sections:

- "Accessing the Manage Roles Dashboard" on page 129
- "Creating Roles" on page 131
- "Editing Groups for a Role" on page 132
- "Deleting Internal Roles" on page 133

Accessing the Manage Roles Dashboard

The Manage Roles dashboard contains a table that lists roles, their type, and the groups that are assigned to each role. It also allows you to create and manage roles, and to assign roles to groups.

To access the Manage Roles dashboard:

Note This procedure continues from "Getting Started with the Administration Module" on page 32.

1 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Users & Security > Manage Roles**.

The Manage Roles dashboard appears in the display area, showing a list of all existing roles:

3 To sort the list by name, groups, or type, click the **Name**, **Groups**, or **Type** column headings as required.

4 To filter the list of roles, use one or more of the following boxes at the top of the Manage Roles list:

- **Name**: Type the role name for which you want to filter.
- **Groups**: Type the group name for which you want to filter.

- **Type**: Type the type name for which you want to filter.

For example, to list only the roles whose name starts with "Dashboard", in the **Name** box, type Dashboard.

The Manage Roles list refreshes, showing the list of roles whose name matches the filter pattern.
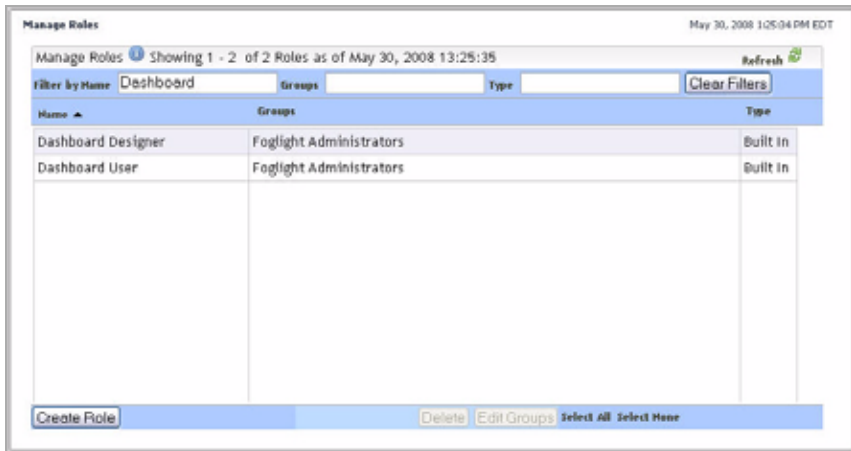
To clear the filters, click **Clear Filters**.

The Manage Roles list refreshes, showing the list of all groups.
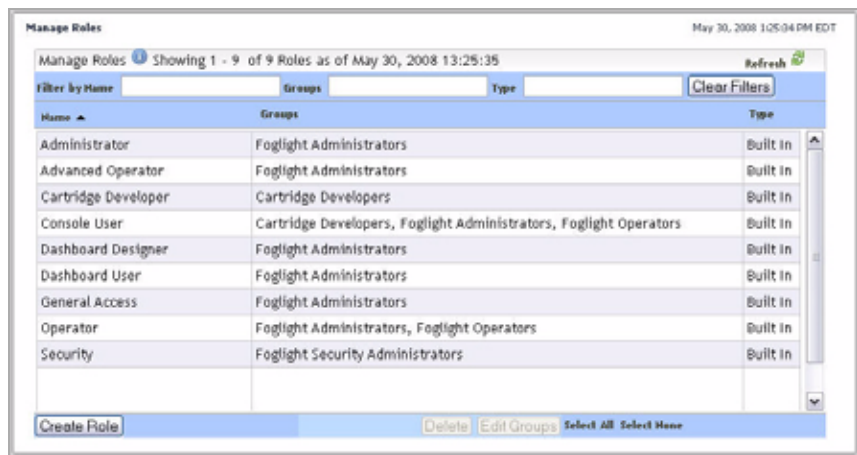
From here, you can proceed to any of the following procedures:

- "Creating Roles" on page 131
- "Editing Groups for a Role" on page 132
- "Deleting Internal Roles" on page 133

Creating Roles

Use the Create Role button on the Manage Roles dashboard to add a role to vFoglight, as outlined below.

To create a role:
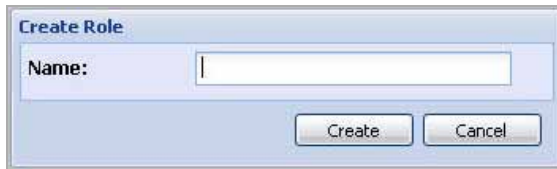
Note   This procedure continues from "Accessing the Manage Roles Dashboard" on page 129.

---

1   In the Manage Roles dashboard, click the **Create Role** button in the lower-left corner.

    The **Create Role** dialog box appears.

Create Role

| Name: | | |

Create   Cancel

---

2 Specify the name of the role that you want to create.

   a In the **Create Role** dialog box, in the **Name** box, type the user name.

    For example: test.

   b Click **Create**.

    The **Create Role** dialog box closes and the Manage Roles dashboard refreshes to show the newly-created role.

| test | | Internal |

When you create roles, their type appears as **Internal** on the listing.

Editing Groups for a Role

Use the Edit Groups button on the Manage Roles dashboard to quickly edit one or more groups for a role.

Alternatively, if you need to edit multiple roles for a single group, use the Manage Groups dashboard. For information, see "Assigning Roles to a Group" on page 124.

To edit groups for a role:

Note This procedure continues from "Creating Roles" on page 131.

---

   1 In the Manage Roles dashboard, select the row containing the role whose groups you want to edit.

   2 Click the **Edit Groups** button in the bottom of the Manage Roles dashboard.

    The **Edit Groups** dialog box appears.
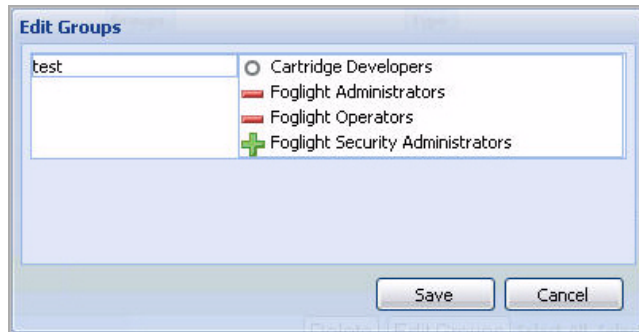
3 In the **Edit Groups** dialog box, select the users to which you want to assign the role by clicking the appropriate symbol to the left of the group name.

- ■ : The group is added to this role.
- ■ : The group has no access to the role.
- ■ : There is no change in group assignment.

For example, to assign the role to the Foglight Administrators and Foglight Security Administrators groups, ensure that the green plus sign appears to the left of the **Foglight Administrators** and **Foglight Security Administrators** entries, and that the red minus sign appears to the left of the other groups in the **Edit Groups** dialog box.

4 Click **Save**.

The **Edit Groups** dialog box closes and the Manage Roles dashboard refreshes to show the groups to which you assigned the role.

Deleting Internal Roles

Use the Delete button on the Manage Roles dashboard to delete roles from vFoglight.

You can only delete those roles that you add to vFoglight after the installation. Their type appears as Internal on the Manage Users dashboard. You cannot delete any of the groups accounts that are included with vFoglight. Their type appears as Built In.
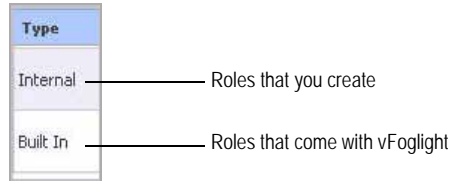
For more information about the types of roles that exist in vFoglight, see "Managing Roles" on page 127.

To delete an internal role:

Note   This procedure continues from "Accessing the Manage Roles Dashboard" on page 129.

---

   1 In the Manage Roles dashboard, select the row containing the role that you want to delete.

   2 Click the **Delete** button at the bottom of the Manage Roles dashboard.

      A message box appears, asking you to confirm the delete operation.
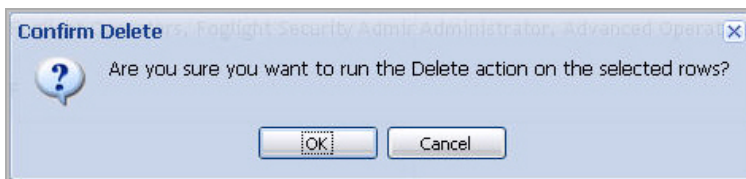
   3 In the message box, click **OK**.

      The message box closes.

   4 Observe the Manage Roles dashboard.

      The role that you deleted no longer appears in the list.

Configuring Password Settings

vFoglight automatically times out after 60 minutes of inactivity.

The following are the default restrictions that apply to passwords for administrators and for other types of internal users. For more information about the types of users in vFoglight, see "Managing Users" on page 107.

- An internal user's password expires after ninety (90) days.

- An administrator's password expires after forty-five (45) days. The one exception is the password for the default user *foglight*, which does not expire.

- A user is locked out of the system after they enter an incorrect password for five (5) consecutive login attempts.

- A user who fails five consecutive login attempts is locked out of the system for fifteen (15) minutes.

- vFoglight reminds a user fifteen (15) days before their password expires.

- The password *must*:
  - Be at least seven (7) characters long.
  - Contain both alphabetic and numeric characters.

- The password *cannot*:
  - Be the same as the user name.
  - Be a dictionary word.
  - Be just the repetition of a single character.
  - Be longer than 255 characters.

    Note   The recommended length of a password is sixteen (16) characters or fewer.

  - Be the same as any of the user's last twelve (12) passwords.

Use the Configure Password Settings dashboard to view and edit these settings as required. For instructions, see the following sections:

- "Accessing the Configure Password Settings Dashboard" on page 136
- "Editing Password Settings" on page 137
- "Changing Database Credentials" on page 138

You can configure many of these settings on the Configure Password Settings dashboard. For instructions, see "Editing Password Settings" on page 137.

Accessing the Configure Password Settings Dashboard

The Configure Password Settings dashboard contains settings for password policies that apply to administrators and internal users are set. The default settings for these policies are described in "Configuring Password Settings" on page 135.

To view password settings:

> **Note** This procedure continues from "Getting Started with the Administration Module" on page 32.

1   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Users & Security > Configure Password Settings**.

    The Configure Password Settings dashboard appears in the display area, showing a list of password settings:

Configure Password Settings	Apr 17, 2008 9:28:32 PM EDT
Configure Password Settings ⓘ	
Days before user password expires:	90
Days before administrator password expires:	45
Bad logins before user account is locked out:	5
Seconds after which lockout expires (0 for no expiration):	900
Minimum password length:	7
Number of old passwords that will be remembered:	12
Number of days before password expiry to warn user:	15
User password complexity level:	2
Administrator password complexity level:	3
User cache expiry in minutes (login is fast until cache expires):	600
[Edit]	

From here, you can proceed to any of the following procedures:

- "Editing Password Settings" on page 137

Editing Password Settings

Use the Configure Password Settings dashboard to edit any policies that you want to change.

To edit password settings:
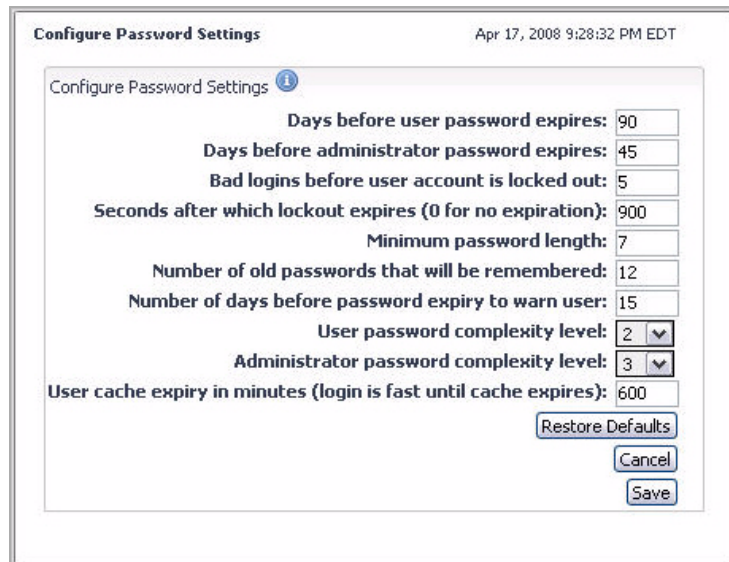
Note This procedure continues from "Accessing the Configure Password Settings Dashboard" on page 136.

---

1 In the Configure Password Settings dashboard, click the **Edit** button in the lower-left corner.

   The Configure Password Settings dashboard refreshes, showing a box to the right of each setting.

Configure Password Settings	Apr 17, 2008 9:28:32 PM EDT
Configure Password Settings ⓘ	
Days before user password expires:	90
Days before administrator password expires:	45
Bad logins before user account is locked out:	5
Seconds after which lockout expires (0 for no expiration):	900
Minimum password length:	7
Number of old passwords that will be remembered:	12
Number of days before password expiry to warn user:	15
User password complexity level:	2 ⌄
Administrator password complexity level:	3 ⌄
User cache expiry in minutes (login is fast until cache expires):	600

Restore Defaults
Cancel
Save

2 Edit the following settings as desired:

   - **Days before user password expires**
   - **Days before administrator password expires**
   - **Bad logins before user account is locked out**
   - **Seconds after which lockout expires (0 for no expiration)**

- **Minimum password length**
- **Number of old passwords that will be remembered**
- **Number of days before password expiry to warn user**
- **User cache expiry in minutes (login is fast until cache expires)**

3 Edit the password complexity levels.

You can set the complexity level that must be used in the passwords of internal users and the users with the Security role. vFoglight uses the following levels:

- **1**: Passwords are not checked for complexity.
- **2:** Passwords must contain both alphabetic and numeric characters.
- **3:** Passwords must contain at least one upper case letter, lower case letter, and numeric character, as well as at least one character that is not alphanumeric.

Type a security level into the **User password complexity level** and **Administrator password complexity level** boxes as required.

By default, the complexity level for internal users' passwords is 2. The default complexity level for the users with the Security role is set to 3.

Note   Administrators' passwords cannot be set to complexity level 1.

To restore the default values, click **Restore Defaults**.

4 Click **Save**.

The Configure Password Settings dashboard refreshes and a message appears in the upper-left, indicating that your changes have been saved.
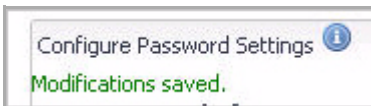
Changing Database Credentials

If you are using an external database, you may experience a situation where the database password for the vFoglight database account has changed (for example, in case password policies change). You can reconfigure vFoglight to start up with a new password by changing the configuration file (`foglight.config`) and restarting the process.

```
foglight.database.password = "[updated password here]";
```

To avoid compromising the password, users must insert an updated encrypted password.

To change the vFoglight database password:

1   Delete the current vFoglight database key from vFoglight's key store:

```
> bin\keyman delappkey dbpwd.[foglight db username]
```

2   Create a new key store entry for the updated password:

```
> bin\keyman addappkey dbpwd.[foglight db username]
    [updated password] "FoglighT db UseR PassworD"
KeyToken: 12345678901234567890123456789012345 67890
```

3   Edit the `foglight.config` file and update the following line with the generated token

```
foglight.database.password =
    "12345678901234567890123456789012345 67890";
```

For more information about changing database credentials using the command line, see the *Command-Line Reference Guide*.

Configuring Directory Services

vFoglight supports the following Lightweight Directory Access Protocol (LDAP version 3) compatible directory services:

- Active Directory
- Sun Java Systems Directory Server,
- OpenLDAP
- Novell eDirectory

The Configure Directory Services dashboard allows you to access user login information that is stored in an external directory. Once you set up the Configure Directory Services dashboard, your vFoglight users can sign in to vFoglight using the credentials from the external directory.

When you configure the LDAP directory service, vFoglight creates a user account each time an LDAP user successfully logs into vFoglight for the first time. If an LDAP user is removed from the LDAP directory service, their user account remains active in vFoglight and can only be removed by a vFoglight administrator.

You can track user login credentials using the Manage Users dashboard. This dashboard lists the users who have logged in to vFoglight using their external account credentials. For more information, see "Managing Users" on page 107.

Accessing the Configure Directory Services Dashboard

Use the Configure Directory Services dashboard to view and edit the settings that enable external users to log on to vFoglight using the credentials they previously set up in an external directory.

To access the Configure Directory Services dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

   1 Ensure that the navigation panel is open.

      To open the navigation panel, click the right-facing arrow ▶ on the left.

   2 On the navigation panel, under **Dashboards**, choose **Administration > Users & Security > Configure Directory Services**.

      The Configure Directory Services dashboard appears in the display area, showing a list of directory settings:

Configure Directory Services   May 30, 2008 1:32:46 PM EDT

Configure Directory Services ⓘ

Nearest LDAP server:	ldap://ldapsvr.mycompany.com:389/
Secondary LDAP server URL:	ldap://backupldapsvr.mycompany.com:389/
Distinguished name of the service account:	
Password:	
Confirm Password:	
LDAP query prefix:	CN=
LDAP query suffix:	,OU=Employees,DC=mycompany,DC=com
The scope(s) to search for groups:	OU=Groups,DC=mycompany,DC=com
The second group namespace:	OU=Dynamic Groups,DC=mycompany,DC=com
The third group namespace :	
The LDAP context for user searching:	ou=Employees,DC=mycompany,DC=com
Role attribute ID:	name
Is Role attribute a DN:	false
User alias attribute ID:	sAMAccountName
User attribute ID to search for groups:	member
Match on User DN:	true
JAAS LoginModule Name:	com.quest.nitro.service.security.auth.spi.NitroExter
Name of JAAS security domain:	fgl-web-console
Parent group attribute ID:	memberOf
Group attribute for nested group searching:	member
Maximum level of group nesting:	15
LDAP search timeout (milliseconds):	10000
Mode of group searching:	direct

☐ **Account is anonymous**

[Restore Defaults]
[Revert]
[Save]

From here, you can proceed to "Editing Directory Settings" on page 142.

Editing Directory Settings

Default settings for these LDAP directory servers are different. The table below shows examples of these settings for different types of LDAP directory servers. Use the following settings as guidelines; they should be substituted with the most appropriate values. Refer to the documentation for your specific LDAP server for more information about settings and values.

Examples

Setting	Active Directory	Sun Java Systems Directory Server/ OpenLDAP	Novell eDirectory
Nearest LDAP server	`ldap://ldapserver.example.com:389/`		
Secondary LDAP server URL	`ldap://backupldapserver.example.com:389/`		
Distinguished name of the service account	The distinguished name (DN) of the service account for further user searching	The distinguished name (DN) of the service account for further user searching, or a special account, `__anonymous__`	`CN=foglight_admin, O=services`
Password	User defined		
LDAP query prefix	`CN=`	`uid=`	`CN=`
LDAP query suffix	`,OU=Employees,DC=MyCompany,DC=com`		`,O=novell`
The scope(s) to search for groups	`OU=Groups,DC=MyCompany,DC=com`		`O=novell`

Setting	Active Directory	Sun Java Systems Directory Server/ OpenLDAP	Novell eDirectory
The second group namespace	`OU=Dynamic Groups,DC=MyCompany,DC=com`		N/A
The third group namespace	N/A		
The LDAP context for user searching	`OU=People,DC=example,DC=com`		`o=novell`
Role attribute ID	`name`	`cn`	`istweb`
Is Role attribute a DN	`false`		
User alias attribute ID	`sAMAccountName`	`uid`	`uniqueId`
User attribute ID to search for groups	`member`	`uniqueMember`	`CN=foglight_admin, O=services`
Match on User DN	`true`		
JAAS[1] LoginModule Name[2]	`com.quest.nitro.service.security.auth.spi.NitroExtendedLdapLoginModule`		
Name of JAAS security domain[3]	`fgl-web-console`		

Setting	Active Directory	Sun Java Systems Directory Server/ OpenLDAP	Novell eDirectory
Parent group attribute ID	`memberOf`		
Group attribute for nested group searching	`member`	`uniqueMember`	`member`
Maximum level of group nesting	`15`		
LDAP search timeout (milliseconds)	`10000`		
Mode of group searching	`direct`	`indirect`	`direct`
Account is anonymous	`false`		

[1] Java™ Authentication and Authorization Service

[2] Do not change this setting

[3] Do not change this setting

To edit directory settings:

Note This procedure continues from "Accessing the Configure Directory Services Dashboard" on page 140.

1 Obtain all of the service account information required to edit the settings on the Configure Directory Services dashboard.

2 Obtain the correct configurations for each setting.

3   In the Configure Directory Services dashboard, click the **Edit** button in the lower-
left corner.

The Configure Directory Services dashboard refreshes, showing a box to the right
of each setting.

Configure Directory Services	Apr 18, 2008 8:20:37 AM EDT

Configure Directory Services ⓘ

Nearest LDAP server:	ldap://ldapsvr.mycompany.com:389/
Secondary LDAP server URL:	ldap://backupldapsvr.mycompany.com:389/
Distinguished name of the service account:	
Password:	
Confirm Password:	
LDAP query prefix:	CN=
LDAP query suffix:	,OU=Employees,DC=mycompany,DC=com
The scope(s) to search for groups:	OU=Groups,DC=mycompany,DC=com
The second group namespace:	OU=Dynamic Groups,DC=mycompany,DC=com
The third group namespace :	
The LDAP context for user searching:	ou=Employees,DC=mycompany,DC=com
Role attribute ID:	name
Is Role attribute a DN:	false
User alias attribute ID:	sAMAccountName
User attribute ID to search for groups:	member
Match on User DN:	true
JAAS LoginModule Name:	com.quest.nitro.service.security.auth.spi.NitroExtendedLdapl
Name of JAAS security domain:	fgl-web-console
Parent group attribute ID:	memberOf
Group attribute for nested group searching:	member
Maximum level of group nesting:	15
LDAP search timeout (milliseconds):	10000
Mode of group searching:	direct

☐ Account is anonymous

Restore Defaults
Revert
Save

4   Edit the settings as required.

To restore the default values, click **Restore Defaults**.

5   Click **Save**.

The Configure Directory Settings dashboard refreshes and a message appears in
the upper-left corner, indicating that your changes have been saved.

Configure Directory Services ⓘ
Modifications saved.

4
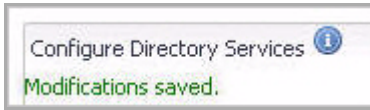
Managing Cartridges

This chapter introduces you to vFoglight cartridges and provides information on how to install and manage cartridges. It contains the following sections:

Note	In order to complete each of the procedures in this chapter, your user account must belong to a group with the Administration role. For more information about users, groups, and roles, see "Managing Users and Security" on page 105.

About vFoglight Cartridges

A cartridge is a unit that is distributed separately from the vFoglight Management Server, but can be added to the Management Server. A cartridge contains components that extend the functionality of vFoglight, such as agent installers, communication capabilities, modifications to the way that data is transformed or handled, model definitions, rules, reports, and views.

An installation of the vFoglight Management Server includes a collection of core cartridges, including the Monitoring Policy, Service Model, and other core cartridges. Core cartridges are installed with the server, and are enabled on its startup. Along with the core cartridges, your configuration can include other cartridges that are installed additionally on the server and are designed to monitor specific types of environments, such as the OS cartridge. Both core and installed cartridges can contain a set of rules, registry variables, tables, retention policies, and other vFoglight entities.

The following concepts and terms relate to cartridge management in vFoglight:

- *Cartridge*. A unit that is distributed separately from the vFoglight Management Server. Cartridges contain components that extend the functionality of vFoglight, such as agents, rules, and views.

- *Cartridge installation*. The act of installing a cartridge on the machine hosting the vFoglight Management Server. Cartridge installation makes the Management Server aware of the cartridge.

  Note   Installing a cartridge does not make it available for use by vFoglight, but simply prepares it to be enabled.

- *Enabled cartridge*. A cartridge whose components are part of the Management Server and available for use by vFoglight.

- *Cartridge component*. A cartridge contains one or more components, such as dashboards and agent installers. See "About Cartridge Components" on page 148 for more information.

About Cartridge Components

A cartridge may include one or more components. Examples of cartridge components are described below.

- *Agent installers/packages*. A cartridge may include one or more vFoglight Agent installers. An agent monitors a specific part of your environment, such as a VirtualCenter, application, or server.

See "Managing Agents" on page 165 for more information about agents.

- *Agent adapters*. Agent adapters are components that allow agents to communicate with the vFoglight Management Server.

- *Monitoring policy.* A monitoring policy contains information and settings that help vFoglight analyze the data that the agents collect, such as rules, registry variables, schedules, and derived metrics. The items included in the monitoring policy are specific to each type of cartridge.

- *Dashboards.* Dashboards display information collected from your monitored environment, such as metrics. Each dashboard is a top-level view from which you can drill down to more detailed views.

  The dashboards included with a cartridge allow the information collected by the agents to be displayed in a unified view.

  Each cartridge may include one or more dashboards.

Installing and Managing Cartridges

Use the Administration module to install cartridges on the vFoglight Management Server, enable and manage cartridges, and download agent installers.

Cartridges allow you to monitor additional operating systems, processes, databases, applications, and servers in your environment.

Adding a cartridge to the vFoglight Management Server is a two-step process. First, the *.car* file that contains the cartridge must be installed on the vFoglight Management Server. Installing a cartridge causes the server to be aware of it.

You can only install those cartridges that are listed in your vFoglight license. For information on how to find out whether your license includes a particular cartridge, see Chapter 2, "Viewing License Capabilities" on page 72.

Next, the cartridge must be enabled. Enabling a cartridge causes its components to be available for use by vFoglight. Using the vFoglight Administration Module, you can cause a cartridge to be automatically enabled upon installation or to be enabled after installation.

When a cartridge has been installed and enabled, all of the components included in the cartridge are part of the Management Server.

Use the Cartridge Inventory dashboard to view information about installed cartridges, and to install, enable, disable, and remove cartridges. For more information on how to use the Cartridge Inventory dashboard, refer to the following sections:

- "Accessing the Cartridge Inventory Dashboard" on page 150
- "Installing Cartridges" on page 155
- "Enabling Cartridges" on page 157
- "Disabling Cartridges" on page 158
- "Uninstalling Cartridges" on page 159

Accessing the Cartridge Inventory Dashboard

The Cartridge Inventory dashboard contains controls for installing, enabling, disabling, and uninstalling cartridges, as well as for viewing information about the installed cartridges.

To access the Cartridge Inventory dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32 or "Viewing the Administration Dashboard" on page 39.

1 Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Cartridges > Cartridge Inventory**.

   The Cartridge Inventory dashboard appears in the display area, showing a list of all existing cartridges.
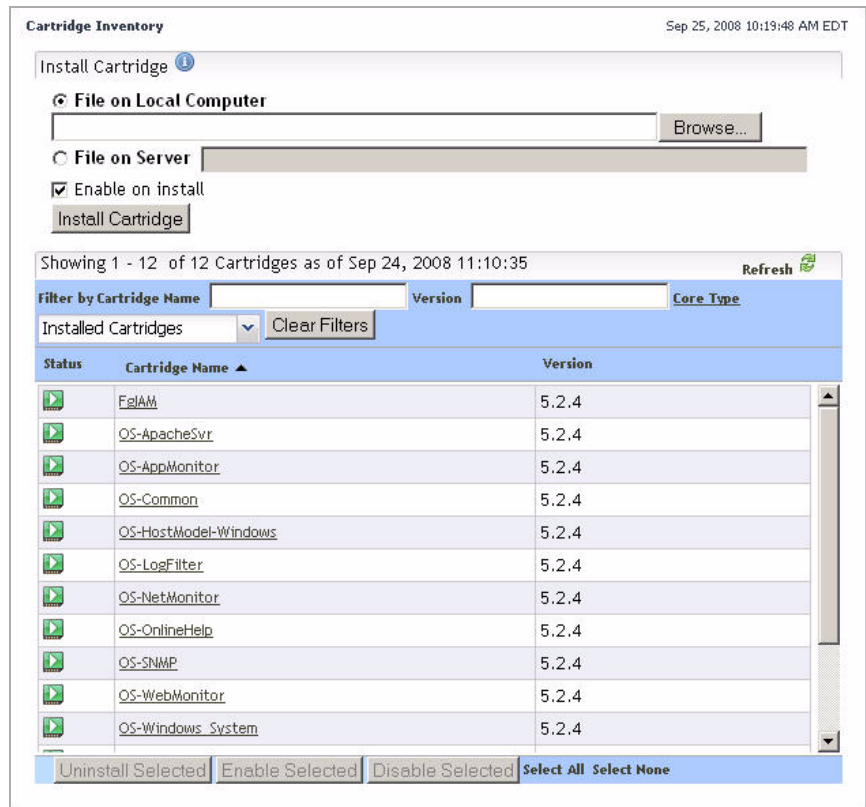
3 View information about one or more cartridges.

- Move the mouse pointer over the **Cartridge Name** column in the row containing the cartridge about which you want to view information.

  A dwell appears, showing the cartridge information.

Cartridge Name: Virtual-VMware
Version: 5.2.3
Build ID: 1014
Creation Date: Thu Oct 09, 2008 12:57:34 CDT
Author: Quest Software - St. Louis
Type: N/A
Status: Enabled

or

*   To view cartridge information and any dependencies with other cartridges, click the **Cartridge Name** column in the row containing the cartridge about which you want to view information.

    The **View Cartridge Details** view appears in the Cartridge Inventory dashboard.

Cartridge Inventory   Sep 25, 2008 10:19:48 AM EDT

View Cartridge Details

Cartridge Name: OS-Windows_System

Version: 5.2.4

Build ID: 524-20080924-0500

Creation Date: Wed Sep 24, 2008 05:02:55 EDT

Author: N/A

Type: N/A

Status: Enabled

Dependencies:

Name	Version	Match Type	Description
OS-Common	5.2.4	Latest	OS-Common-5.2.4 (matches: LATEST)

Go to Cartridge Inventory

To return to the Cartridge Inventory dashboard, in the **View Cartridge Details** view, click **Go to Cartridge Inventory**.

4 To sort the list of cartridges, click any of the **Status**, **Cartridge Name**, or **Version** column headings as required.

5 To filter the list of cartridges, use one or more of the following boxes above the cartridge table:

- **Name**: Type the cartridge name for which you want to filter.
- **Version**: Type the cartridge version for which you want to filter.
- **Core Type**: Click and select one of the following options as required: **Core Cartridges**, **Installed Cartridges**, or **All Cartridges**.

For example, to list the core cartridges that are related to the cartridges core cartridges, in the **Name** box, type Windows.

The Cartridge Inventory dashboard refreshes, showing the list of cartridges whose name matches the filter pattern.
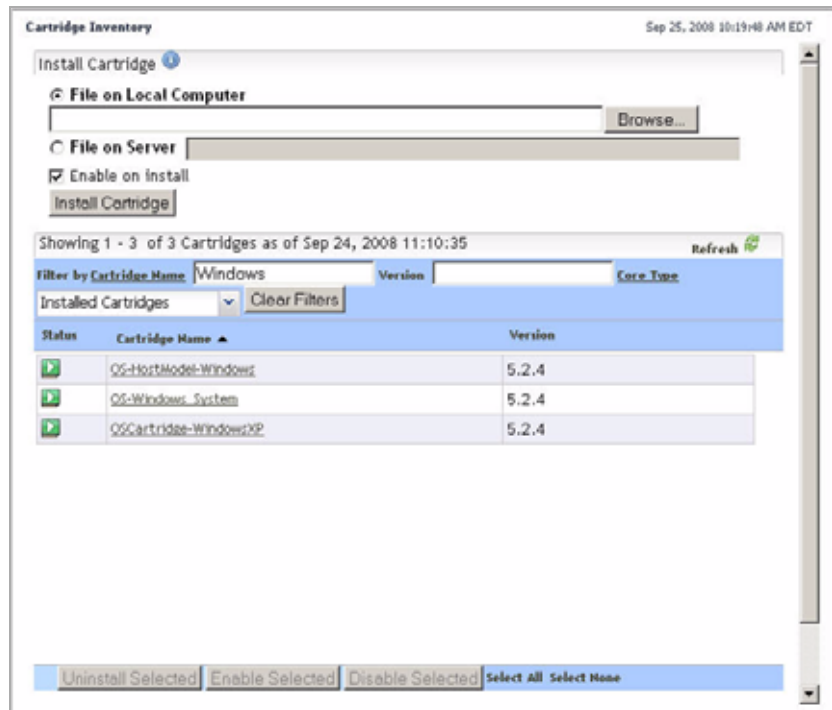
To clear the filters, click **Clear Filters**.

The Cartridge Inventory dashboard refreshes, showing the list of all cartridges.

From here, you can proceed to any of the following procedures:

Installing Cartridges

Installation is the first step in adding a cartridge to the vFoglight Management Server. A cartridge file has the extension *.car*. Installing the CAR file causes the Management Server to be aware of all cartridges in the CAR file.

Use the Cartridge Inventory dashboard to install a single cartridge at a time. To install multiple cartridges at the same time, use the cartridge:install command. For complete information about this command, see the *Command-Line Reference Guide*.

You can only install those cartridges that are listed in your vFoglight license. Trying to install a non-licensed cartridge results in error. For information on how to find out whether your license includes a particular cartridge, see Chapter 2, "Viewing License Capabilities" on page 72.

A cartridge must also be enabled before it is added to the Management Server. You can enable a cartridge upon or after installation. See "Enabling Cartridges" on page 157 for instructions on enabling cartridges after installation.

To install a cartridge:

Note   This procedure continues from "Accessing the Cartridge Inventory Dashboard" on page 150.

---

1   In the Cartridge Inventory dashboard, in the **Install Cartridge** area, complete one of the following steps:

   • If the CAR resides in a location that you can access from your local computer, specify the path and name of the CAR file.

      Ensure that the **File on Local Computer** option is selected. Click **Browse** and navigate to the CAR file using the file browser that appears.

      The **File on Local Computer** box refreshes, showing the full path to the CAR file.

   or

   • If the CAR file resides on the computer hosting the vFoglight Management Server specify its path and name.

      Select the **File on Server** option, and in the box to its right, type the path and file name. The path should be relative to the vFoglight Management Server installation directory.

For example, if the name of the CAR file is *Virtual-VMware.car*, and it resides in the *<vfoglight_home>/cartridge* directory on the vFoglight Management Server computer, in the **File on Server** box, type the following:

```
cartridge/Virtual-VMware-5_2_3.car
```

2   **Optional**. To enable the cartridge immediately after its installation, select the **Enable on install** check box.

Alternatively, you can enable the cartridge at a later time. To do that, ensure that the **Enable on install** check box is cleared, and follow the instructions in "Enabling Cartridges" on page 157 after the cartridge installation.

3   Click **Install Cartridge**.

A status bar appears in the Cartridge Inventory dashboard, indicating the installation progress.

If the installation succeeds, a message appears in the upper-left corner of the **Install Cartridge** area.
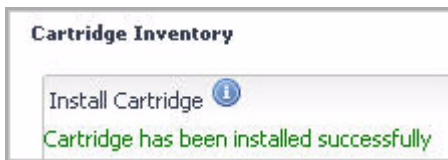
4   **Important**. In the list of installed cartridges, in the upper-right corner, click Refresh.

The list refreshes, showing the newly-installed cartridge.

Note   You can only install those cartridges that are listed in your vFoglight license. Trying to install a non-licensed cartridge results in error. For information on how to find out whether your license includes a particular cartridge, see Chapter 2, "Viewing License Capabilities" on page 72.

5   Observe the list of installed cartridges.

The **Status** column contain icons that indicate if a cartridge is enabled [icon], enabled pending dependency [icon], partially enabled [icon], or disabled [icon].

If you chose not to enable the cartridge immediately after the installation in step 2, you can do that at a later time. For instructions, see "Enabling Cartridges" on page 157.

From here, you can proceed to "Enabling Cartridges" on page 157.

Enabling Cartridges

Enabling a cartridge completes the process of adding it to the vFoglight Management Server by making the cartridge's components available for use by the Management Server.

A cartridge can be in one of the following states:

- Enabled
- Enabled, pending dependency
- Disabled
- Partially enabled

Use the Enable Selected button on the Cartridge Inventory dashboard to enable one or more cartridges, as outlined below.

To enable a cartridge:

Note   This procedure continues from "Installing Cartridges" on page 155.

---

1   In the Cartridge Inventory dashboard, select one or more disabled cartridges in the table that you want to enable.

    The **Status** column contain icons that indicate if a cartridge is enabled [icon], enabled pending dependency [icon], partially enabled [icon], or disabled [icon].

    Tip   To select multiple cartridges, press the CTRL or SHIFT key while selecting the rows containing the cartridges that you want to enable.

2   Click the **Enable Selected** button at the bottom of the Cartridge Inventory dashboard.

    If the operation is successful, a message appears above the cartridge list.

Requested operation was successfully completed

3 In the Cartridge Inventory dashboard, observe the **Status** column of the cartridges that you enabled.

The **Status** column of each newly-enabled cartridge contains an icon (▶) indicating that the operation was successful.

Disabling Cartridges

A cartridge can be in one of the following states:

• Enabled

• Enabled, pending dependency

• Disabled

• Partially enabled

Disabling a cartridge causes its components to no longer be available for use by the vFoglight Management Server. A disabled cartridge remains installed on the Management Server.

For example, you could disable a cartridge to temporarily disable its functionality but keep the *.car* file installed on the Management Server.

Note   If you are installing a new version of a cartridge, vFoglight will detect and automatically disable the older version.

Use the Disable Selected button on the Cartridge Inventory dashboard to disable one or more cartridges, as outlined below.

To disable a cartridge:

Note   This procedure continues from "Accessing the Cartridge Inventory Dashboard" on page 150.

---

1 In the Cartridge Inventory dashboard, in the cartridge table, select one or more enabled cartridges that you want to disable.

The **Status** column contain icons that indicate if a cartridge is enabled ![icon], enabled pending dependency ![icon], partially enabled ![icon], or disabled ![icon].

> **Tip** To select multiple cartridges, press the CTRL or SHIFT key while selecting the rows containing the cartridges that you want to disable.

2 Click the **Disable Selected** button at the bottom of the Cartridge Inventory dashboard.

The **Cartridge Confirmation** dialog box appears.

The list of cartridges that appears in the **Cartridge Confirmation** dialog box reflects your cartridge selection.

3 In the **Cartridge Confirmation** dialog box, click **OK**.

The **Cartridge Confirmation** dialog box closes. If the operation is successful, a message appears above the cartridge list.

4 In the Cartridge Inventory dashboard, observe the **Status** column of the cartridges that you disabled.

The **Status** column of each newly-disabled cartridge contains an icon (![icon]) indicating that the operation was successful.

Uninstalling Cartridges

Uninstalling a cartridge removes the files for that cartridge from the directory for the vFoglight Management Server.

A CAR file can contain multiple cartridges. When you remove all of the cartridges that come in a CAR file, the CAR file will be deleted.

Caution If you remove a cartridge while the agents that were included in that cartridge are deployed and actively collecting data, it can cause communication problems between the agents and the vFoglight Management Server.

For example, the agents may not be able to connect to the Management Server. If they are still able to connect, the Management Server will likely not be able to recognize the data that they send.

To remove a cartridge:

Note This procedure continues from ".

---

1   In the Cartridge Inventory dashboard, select one or more cartridges that you want to remove.

The **Status** column contain icons that indicate if a cartridge is enabled ▶, enabled pending dependency ▪ , partially enabled ▪ , or disabled ▫ .

Tip   To select multiple cartridges, press the CTRL or SHIFT key while selecting the rows containing the cartridges that you want to remove.

2   Click the **Uninstall Selected** button in the lower-left corner of the Cartridge Inventory dashboard.
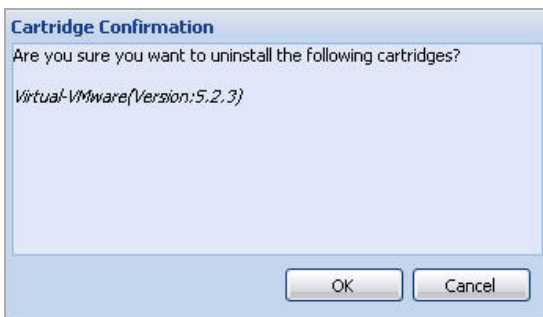
The **Cartridge Confirmation** dialog box appears.

The list of cartridges that appears in the **Cartridge Confirmation** dialog box reflects your cartridge selection.

3 In the **Cartridge Confirmation** dialog box, click **OK**.

The **Cartridge Confirmation** dialog box closes. If the operation is successful, a message appears above the cartridge list.

Requested operation was successfully completed

4 In the Cartridge Inventory dashboard, observe the list of cartridges.

The cartridges that you removed no longer appear in the list.

Downloading Agent Components

There are two types of agent components that you can download using this dashboard:

- *Executable agent installers.* Some cartridges include one or more executable agent installers. The agent installers that are available for download are listed on the Components for Download dashboard. You can use the controls on this page to download agent installers from the Management Server to a remote machine.

  Caution Read and follow any documentation provided with the agent installers.

- *Agent packages*. Other types of cartridges include agent packages that can be deployed and activated using the Agent Status dashboard. For more information about agent management in the Administration module, see "Managing Agents" on page 165.

Use the Components for Download dashboard to view information about existing components and to download them. For more information on how to use the Cartridge Inventory dashboard, refer to the following sections:

- "Accessing the Cartridge Inventory Dashboard" on page 150
- "Downloading Components" on page 163

Accessing the Components for Download Dashboard

The Components for Download dashboard allows you to view information about existing components and to download them.

To download agent components:

Note This procedure continues from "

---

1   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Cartridges > Components for Download**.

    The Components for Download dashboard appears in the display area, showing a list of agent components that are available for download.
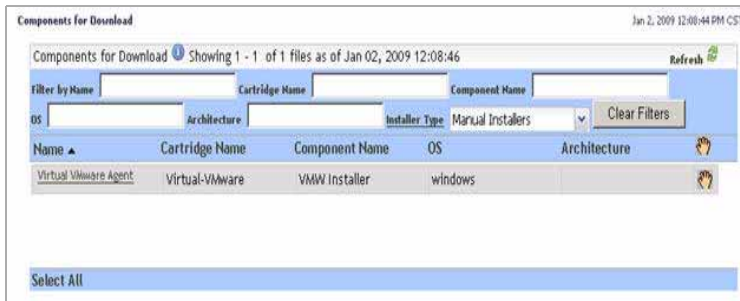
    If the row containing an agent installer shows the Manual Installer icon (🖐) in the Manual Installer column (🖐), this indicates that you need to run the agent installer manually on the monitored host after downloading it to the monitored host. For complete information on how to manually install an agent component, see your cartridge documentation.

3   **Newly-installed cartridges**. In the Components for Download list, in the upper-right corner, click Refresh 🔄.

    The list of components refreshes, showing any components that come with newly-installed cartridges that are available for download.

4   View information about one or more agent components.

    Move the mouse pointer over the **Name** column in the row containing the component about which you want to view information.

    A dwell appears, showing the component information.

```
Name: Virtual VMware Agent(Version:5.2.3)
File Name: setup.exe
Cartridge Name: Virtual-VMware(Version:5.2.3)
Component Name: VMW Installer(Version:5.2.3)
OS: windows(Version:N/A)
Architecture: N/A
Installer Locale: N/A
Installer Type: Manual Installer
```

5 To sort the list of components, click any of the **Name**, **Cartridge Name**,
   Component Name, **OS**, **Architecture**, or the Manual Installer icon ( ) column
   headings as required.

6 To filter the list of cartridges, use one or more of the following boxes above the
   component table:

   • **Name**: Type the component name for which you want to filter.

   • **Cartridge Name**: Type the cartridge name for which you want to filter.

   • **Component Name**: Type the component name for which you want to filter.

   • **OS**: Type the OS name for which you want to filter.

   • **Architecture**: Type the architecture name for which you want to filter.

   • **Installer Type**: Click and select **All Installers** or **Manual Installers** as
     required.

   For example, to list only the agent components that can be installed on monitored
   hosts that are running AIX, in the **OS** box, type aix.

   The Components for Download dashboard refreshes, showing the list of
   components whose name matches the filter pattern.

   To clear the filters, click **Clear Filters**.

   The Components for Download dashboard list refreshes, showing the list of all
   components.

From here, you can proceed to "Downloading Components" on page 163.

Downloading Components

Use the Name column on the Components for Download dashboard to download agent
components, as outlined below.

To download an agent component:

Note   This procedure continues from "Accessing the Components for Download Dashboard" on
page 161.

---

1   In the Components for Download dashboard, click the **Name** column of the row
containing the agent component that you want to download.

Your Web browser displays a dialog box that allows you to open or save the
support bundle.
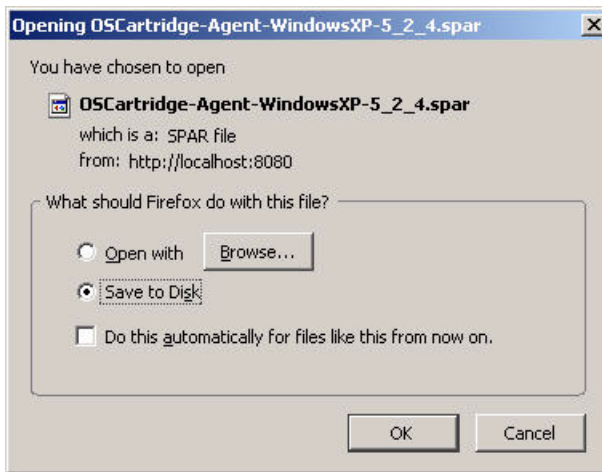
Note   The appearance of the above dialog may be different, depending on the type and
version of your Web browser.

2   Save the file to disk.

5

Managing Agents

This chapter introduces you to vFoglight agents and provides information on how to install and manage them. It contains the following sections:

Note In order to complete each of the procedures in this chapter, your user account must belong to a group with the Administration role. For more information about users, groups, and roles, see "Managing Users and Security" on page 105.

This chapter contains the following sections:

About vFoglight Agents

A vFoglight agent monitors a specific part of your environment, such as a VirtualCenter, application, or server.

There are two categories of agents: agents that run remotely (on a monitored host) and touchless agents, which monitor remote systems from within the vFoglight Management Server.

Each cartridge that you install on the vFoglight Management Server includes one or more agent types. When you install a cartridge and deploy its agent package that include those types to one or more monitored hosts, you can create agent instances and initiate their data collection.

Agents collect data from your monitored environment and send it to the Management Server. Agents can monitor the availability and performance of network services, operating systems, log files, file systems, disk space and utilization, top processes, custom applications, application servers, and Web servers. vFoglight also includes internal agents that monitor vFoglight components and services.

Note   In vFoglight, the vFoglight Agent Manager is used to manage agent instances and their communication with the vFoglight Management Server. Some monitoring environments use the vFoglight Client, which is an older version of the agent manager. While vFoglight supports both types of agent managers, some commands and dashboards may display slightly different type of information. This chapter contains samples of command-line output and screen captures that illustrate a monitoring environment that uses the vFoglight Agent Manager. For information on those interfaces in environments that use the vFoglight Client, see "Appendix: vFoglight Client Reference" on page 497.

Managing Agent Properties by Type

When an agent connects to the vFoglight Management Server, it is provided with sets of properties that it uses to configure its correct running state. vFoglight stores agent properties in the vFoglight Management Server. Any passwords that are defined in agent properties, and stored in the database, are encrypted. This feature is useful in situations when a database password is defined in agent properties, you have different types of databases and their administrators in your environment, such as the vFoglight database and a production database. Having a database password encrypted prevents those database administrators that do not interface with vFoglight from accessing the vFoglight database.

Default versions of these properties are installed with the cartridge in which the agents are included. You can edit the default properties, create sets of properties that apply only to a specific agent instance, and create edited clones of property sets that are used by a subset of the agents of a certain type.

There are two types of agent properties:

- *Primary*. They are included in the agent component and their settings can be specific to the agent type or the agent instance. Each agent comes with a set type-specific properties. You can edit them for a particular agent instance, leave them unchanged, or apply their settings to all agent instances of the same type. If you do not change agent properties for an instance, vFoglight uses the default properties that come with that agent type.

- *Secondary*. They are in list form. The value of each secondary property can be set to one or more lists. You will recognize a list-based property by the Edit and Clone buttons that appear next to it.

List property

Lists that come with an agent type are type-specific and as such global in nature, which means that any changes to them affect all instances of that agent type. To override this behavior, you can create an instance-specific list by cloning a global list and assigning the cloned list to one or more agent instances. Any changes to this list affect only those agent instances to which the list is assigned.

Examples of situations in which you may want to clone a list include the following scenarios:

- You want a set of default agent properties to use different lists at different times. For example, you may want to create a clone of a list and configure it to have different settings during testing.
- You want to use lists with different settings in different agent instances.

You can view and edit type-specific agent properties using the Agent Properties dashboard. For complete information, refer to the following sections:

-

Note If you remove an agent after deploying it, its properties will be unavailable in the Agent Properties dashboard.

Accessing the Agent Properties Dashboard

Use the Agent Properties dashboard to view and edit type-specific agent properties, both primary and secondary.

To access the Agent Properties dashboard:

Note This procedure continues from "

---

1 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Agents > Agent Properties**.

The Agent Properties dashboard appears in the display area.
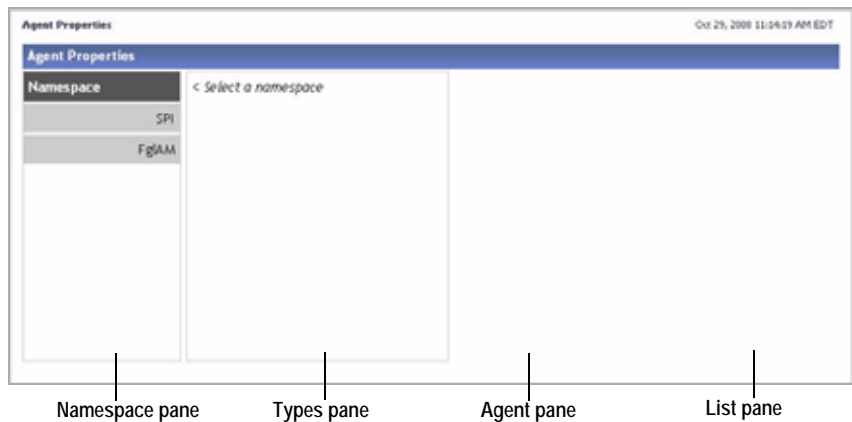
Namespace pane   Types pane   Agent pane   List pane

Note   For a sample screen capture of this dashboard in a monitoring environment that uses the vFoglight Client, see "Agent Properties dashboard" on page 501.

The Agent Properties dashboard contains three panes:

- **Namespace**: Contains a list of vFoglight adapters that allow the agent to communicate with the vFoglight Management Server. The majority of vFoglight agents use the vFoglight Agent Manager and the SPI adapter. Other agents come with their own agent adapter. For example, the Java EE cartridge has its own agent adapter.

- **Types**: Lists agent types for a selected agent adapter.

  Note   This pane is initially blank.

- **Agent**: Lists type-specific agent properties for a selected agent type.

  Note   This pane is initially blank.

- **List**: Shows list entries when editing a secondary property.

  Note   This pane is initially blank.

3   Select an agent adapter.

In the Agent Properties dashboard, in the **Adapter** pane, click an agent adapter.

The **Types** pane refreshes, showing the agent types that use the selected agent adapter to communicate with the vFoglight Management Server.
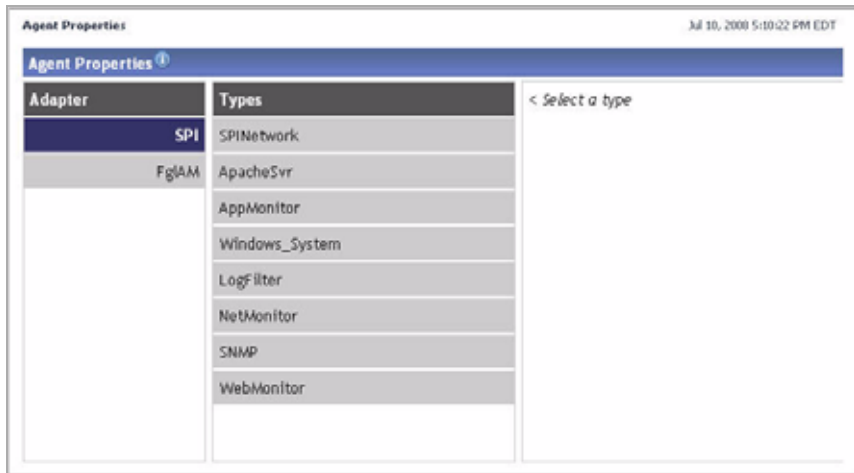
4 Select an agent type.

In the Agent Properties dashboard, in the **Type** pane, click an agent type.

The Agent pane refreshes, showing the agent properties for the selected agent type.
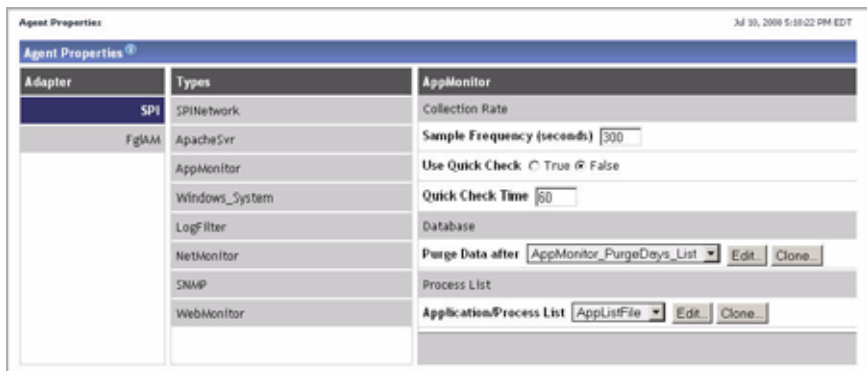
5 Observe agent properties.

A list-based property has the **Edit** and **Clone** buttons to its right.

List property

A primary property appears as a box or an option.

Primary properties
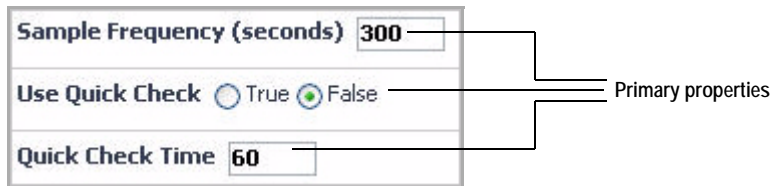
For complete information about any agent properties that appear in the Agent pane, refer to your cartridge documentation.

Editing Type-Specific Agent Properties

The Agent pane of the Agent Properties dashboard contains simple (primary) properties and list-based properties.

List property

Primary properties
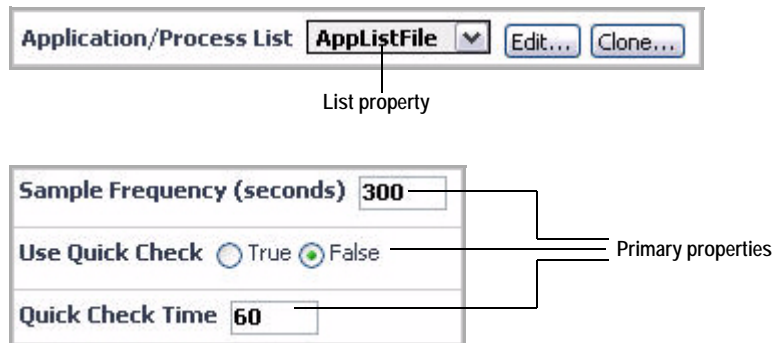
For more information on agent properties in vFoglight, see "Managing Agent Properties by Type" on page 167.

You can edit a primary property simply by specifying the desired value or option for the selected agent type. Editing list-based properties is somewhat different in that it allows you to either edit an existing list, or copy a list and make edits to it.

For instructions on how to edit agent properties, see the following sections:

•

Editing primary type-specific properties

Use the Agent pane of the Agent Properties dashboard to edit primary type-specific properties, as outlined below.

To edit a primary type-specific property:

Note   This procedure continues from "Accessing the Agent Properties Dashboard" on page 168.

---

1   In the Agent Properties dashboard, in the Agent pane, locate the primary property that you want to edit.

   Note   Use caution when modifying type-specific agent properties, as these settings can apply to multiple agents.

   A primary property appears as a box or an option.
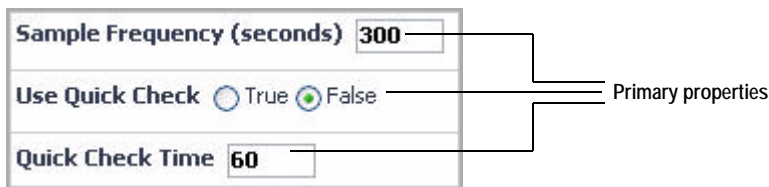
2   Edit the property as required.

   Note   All text boxes on the Agent Properties dashboard have a limit of 64 characters.

   The name and value of the edited property appears red on the Agent pane to indicate the change. Additionally, a **Save** button appears in the lower-right corner of the Agent pane.

3 Click the **Save** button.

The Agent pane refreshes.

Cloning lists in secondary properties

Each secondary property can have one or more lists to which it can be set. Cloning a list allows you to create multiple instances of the same list and assign them to different agent instances as required. This type of configuration creates potentially instance-specific lists, overriding the default behavior of lists in which they are shared amongst agent instances.

When you clone a list, its selection of rows and fields remains unchanged. You can alter it if required at a later time. For more information, see "Editing lists in secondary properties" on page 174.

Use the Clone button on the Agent pane to clone lists that are assigned to secondary agent properties, as outlined below.

To clone a secondary property:

Note This procedure continues from "" on page 168.

---

1 In the Agent Properties dashboard, in the Agent pane, locate the secondary property that you want to clone.

2 Click the **Clone** button to the right of the box that contains the property value.

A dialog box appears.

Clone name: AppMonitor_PurgeDays_
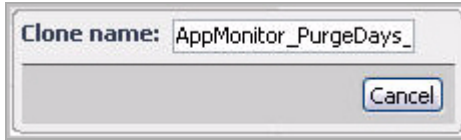
Cancel

3 In the dialog box, in the **Clone name** box, specify the name of the cloned list either by editing the value that appears.

As you edit the list name, a **Clone** button appears in the dialog box to the left of the **Cancel** button.

Clone name: lonitor_PurgeDays_List2
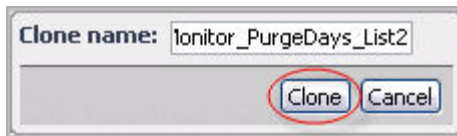
Clone Cancel

4 Click the **Clone** button that appears to the left of the **Cancel** button in the dialog box.

The dialog box closes and the secondary property refreshes, with its value set to the newly-cloned list. The property name and list name appear red in the Agent pane to indicate the change.

Purge Data after AppMonitor_PurgeDays_List2

5 Save your changes to the agent properties.

In the Agent pane, in the lower-right corner, click the **Save** button.

The Agent pane refreshes.

Editing lists in secondary properties

Editing a list involves changing the value of its entries, adding new entries, or deleting existing ones. This feature is useful in situations when you clone a list and need to use its modified clones in certain agent configurations.

Use this type of approach when you want to use different lists at different times, or to assign different versions of the same list to agent instances of the same agent type.

Use the Edit button on the Agent pane to edit lists that are assigned to secondary agent properties, as outlined below.

Caution Changes made to lists can affect multiple agents.

To edit a list for a secondary property:

Note This procedure continues from "Accessing the Agent Properties Dashboard" on page 168.

---

1 In the Agent Properties dashboard, in the Agent pane, locate the secondary property that you want to edit.

2 Click the **Edit** button to the right of the box that contains the property value.

   Caution Secondary agent properties can apply to multiple agents. If you want to edit a cloned list that is instance-specific, ensure that you select that list in the property box before clicking the **Edit** button.

   The List pane refreshes, showing the contents of the selected list.

AppMonitor_PurgeDays_List2	
Foglight Table	**Purge Days**
AgentMsgs	3
AppAvailability	14
ApplicationTotals	90
ProcessDetail	14
ProcessTotals	14
	Add new row

3 To edit an entry in the list, complete the following steps.

   a Double-click the row containing that entry.

   A dialog box appears.
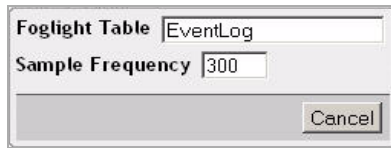
Foglight Table	EventLog
Sample Frequency	300
	Cancel

Note   The appearance of the dialog box depends on the nature and complexity of the list entry.

Note   All text boxes have a limit of 64 characters.

b   Edit the entry in the dialog box and click the **OK** button that appears.

As you edit the list entry, its name and value appear red in the dialog box to indicate the change.

Sample Frequency	350

c   To save your changes, click the **Save** button that appears in the dialog box.

The dialog box closes and the List pane refreshes, showing the newly-edited value.

4   To add a row to the list, complete the following steps.

a   In the List pane, click the **Add new row** button in the lower-right corner.

A dialog box appears.
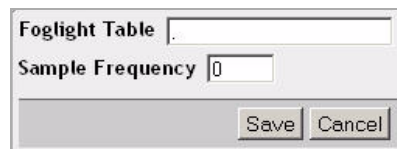
Foglight Table	.
Sample Frequency	0
	Save Cancel

Note   The appearance of the dialog box depends on the nature and complexity of the list entry.

b   Edit the entry in the dialog box.

As you edit the list entry, its name and value appear red in the dialog box to indicate the change.

Sample Frequency 350

    c To save your changes, click the **Save** button that appears in the dialog box.

       The dialog box closes and the List pane refreshes, showing the newly-added entry.

5 To delete one or more rows from the list, complete the following steps.

    a In the List pane, select the rows containing the entries that you want to delete from the list.

       To select multiple entries, press the CTRL key while clicking rows.

    b Click the **Delete selected row(s)** button that appears in the lower-right corner.

       The newly-deleted rows are removed from the list.

Removing cloned lists from secondary properties

Use the Remove button on the Agent pane to delete lists that are assigned to secondary agent properties, as outlined below.

You can only remove cloned lists. Any lists that are included with vFoglight cannot be deleted.

To delete a secondary property:

Note This procedure continues from "Accessing the Agent Properties Dashboard" on page 168.

---

1 In the Agent Properties dashboard, in the Agent pane, locate the list that you want to delete.

In the Agent pane, the **Remove** button appears to the right of the **Clone** button, indicating that the selected list is cloned and can be removed.

Purge Data after AppMonitor_PurgeDays_List2 ▾ Edit... Clone... Remove...

2 Click **Remove**.

    Caution Secondary agent properties can apply to multiple agents. If you want to edit a cloned list that is instance-specific, ensure that you select that list in the property box before clicking the **Edit** button.

A message box appears, asking you to confirm the delete operation.

> Delete AppMonitor_PurgeDays_List2 ?
>
> [Remove] [Cancel]
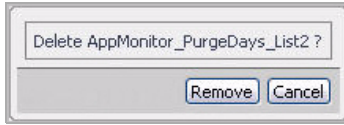
3 Click **Remove** in the message box.

The message box closes and the list is removed from the collection of lists that are available for selection from the secondary property. The property from which you removed the secondary list appears red, indicating unsaved edits.

> **Purge Data after** AppMonitor_PurgeDays_List ▾

4 Save your changes to the agent properties.

In the Agent pane, in the lower-right corner, click the **Save** button.

The Agent pane refreshes.

•

Assigning Blackouts to Agent Instances

A schedule defines a period of time during which an action occurs. Blackout schedules prevent agents from collecting data. You can use an existing schedule or create another one if required. For more information about schedules, see Chapter 8, "Using Schedules" on page 395.

An agent blackout is a scheduled event during which the agent does not collect data for set intervals. For example, you might want to set the times when regularly scheduled maintenance is performed on a server as the blackout period for the agents that run on that server.

Use the Agent Blackouts dashboard to manage agent blackouts.

To manage agent blackouts:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow ▸ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Agents > Agent Blackouts**.

    The Agent Blackouts dashboard appears in the display area, listing all agent instances.
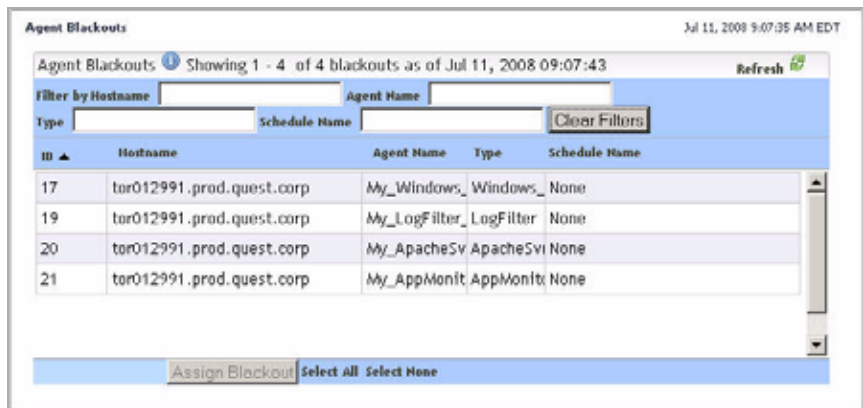
3 To sort the list by their ID, host name, instance name, agent type, or schedule name, click the **ID**, **Hostname**, **Agent Name**, **Type**, or **Schedule Name** column headings as required.

4 To filter the list of agents by the host name, instance name, agent type, or schedule name, use the **Hostname**, **Agent Name**, **Type,** or **Schedule Name** boxes at the top of the Agent Blackouts list.

For example, to list only the hosts whose agent type contains "Windows", in the **Type** box, type Windows.

The Agent Blackouts list refreshes, showing the agent instances whose name matches the filter pattern.
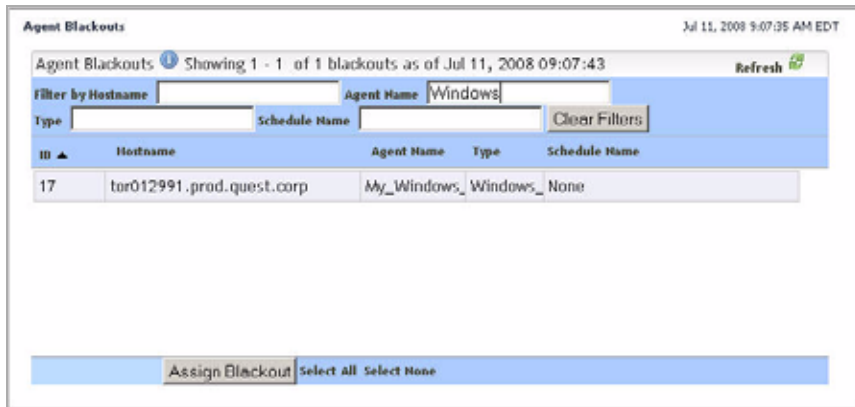
To clear the filters, click **Clear Filters**.

The Agent Blackouts dashboard refreshes, showing the list of all agents.
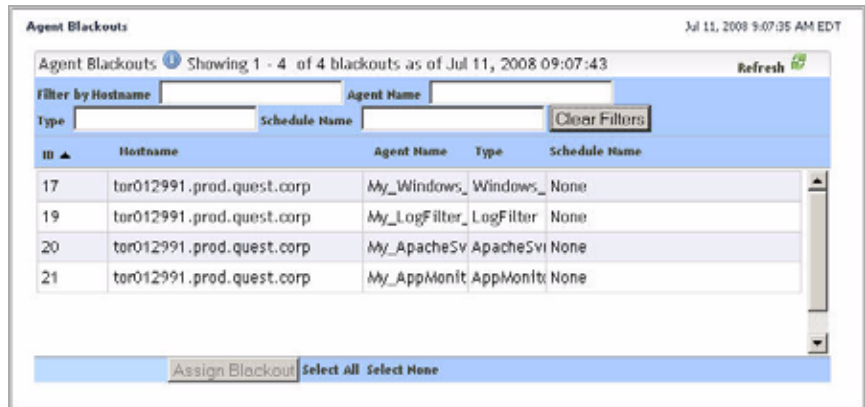
To clear the filters, click **Clear Filters**.

5 Assign or remove a blackout schedule for an agent.

   a Select the row containing that agent.

   b Click the **Assign Blackout** button at the bottom.

     The **Selected Agents** dialog box appears.
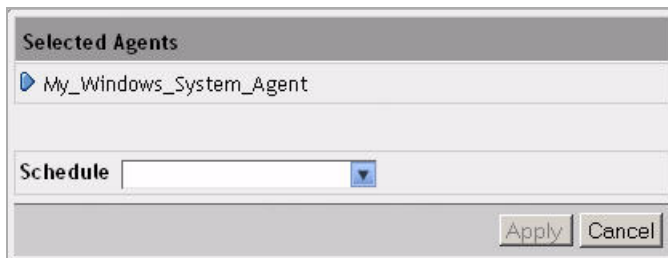
   c Choose a blackout schedule for the selected agent.

     Click **Schedule**.

     A list of all available schedules appears.

The list reflects the entries in Manage Schedules dashboard. For more information, see "Managing Schedules" on page 397.

To remove a schedule, select **None** in the list.

To assign a schedule, select any other entry in the list, as required. For example, to black out the selected agent on the first day of each month, select **First day of month**.

6 Click **Apply**.

The **Selected Agents** dialog box closes and the Agent Blackouts dashboard refreshes, showing the schedule assignment in the **Schedule Name** column.

6
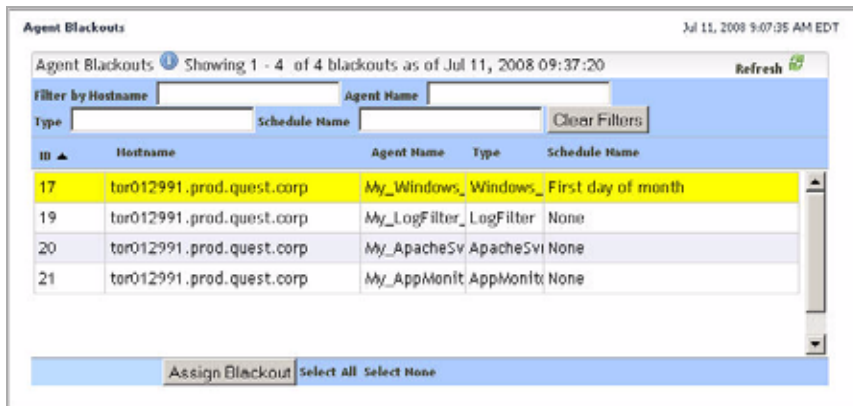
Working with vFoglight Rules and Registry

This chapter introduces you to vFoglight rules and registry and provides information on how to create and manage these entities. It contains the following sections:

Note	In order to complete each of the procedures in this chapter, your user account must belong to a group with the Administration role. For more information about users, groups, and roles, see "Managing Users and Security" on page 105.

This chapter contains the following sections:

About Rules, Registry, and Topology in vFoglight

vFoglight collects data about your system and dynamically builds topology models at run-time. A topology model organizes the data in a way that represents the logical and physical relationship between items in your monitored environment and provides the context for the collected metrics. Each topology model includes one or more topology types, and each type has an associated set of metrics. Topology objects are instances of a topology type. For example, a Host model may contain Processor, Host, and Memory topology types; a specific CPU would be an instance of the Processor topology type. For more information on data and topology models, see Chapter 7, "Working with Data" on page 327.

A registry variable can have a global value that is available to all topology types and objects as well as multiple values that are associated with specific topology types or objects. If required, these values can be configured to change at certain times. For more information, see "Working with vFoglight Registry Variables" on page 184.

A rule is associated with a topology type and can be configured to run against specific topology objects. Rule definitions can include registry variables, raw metrics, derived metrics, and topology object properties. At run-time, vFoglight creates topology objects and initiates rules to run against these objects, using registry variables, metrics, and object properties as thresholds for alarm generation, as specified in rule definitions. For more information, see "Working with Rules" on page 223.

Working with vFoglight Registry Variables

vFoglight registry variables can be used in rule conditions, expressions, and actions. They are stored in the vFoglight registry. A registry variable can have a global value that is available to all topology types and objects. It can also have multiple additional values associated with specific topology types or objects, or calendar dates. In addition, these values can be configured to change at certain times.

You create new registry variables, assign values to registry variables, and manage registry variables using the dashboards that come with the Administration module. Because registry variables can have multiple values that are tied to the topology or dates, you can see verify their values and see how they are affected by these parameters.

For complete information, see the following sections:

- "Managing Registry Variables" on page 185
- "Creating Registry Variables" on page 195

- "Editing Registry Variables" on page 200
- "Viewing Registry Values" on page 209
- "Example: Assigning Multiple Values to a Registry Variable" on page 216
- "Example: Using Performance Calendars" on page 216
- "Example: Assigning Host-Specific Email Addresses of vFoglight System Administrators" on page 217

Managing Registry Variables

The Manage Registry Variables dashboard allows you to create new registry variables, assign values to registry variables, and manage registry variables. For complete information, see the following sections:

- "Working with vFoglight Registry Variables" on page 184
- "Accessing the Manage Registry Variables dashboard" on page 185
- "Editing permissions of registry variables" on page 188
- "Copying registry variables" on page 191
- "Deleting registry variables" on page 193
- "Viewing and editing variable definitions" on page 194

Accessing the Manage Registry Variables dashboard

The Manage Registry Variables dashboard includes a list of the registry variables that exist in your monitoring environment and includes an interface for adding and deleting registry variables.

To access the Manage Registry Variables dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Manage Registry Variables**.

   The Manage Registry Variables dashboard appears in the display area.

3 To sort the list of variables by their name or type, click the **Variable Name** or **Type** column headings as required.

4 **Optional**. Filter the list of variables.

- To show only the variables whose name matches a text pattern, type that pattern into the **Variable Name** box at the top of the list.

  The Manage Registry Variables dashboard refreshes, showing only the variables whose name matches the text pattern.

- To show only the variables that are associated with specific topology types, click **By Topology** at the top of the list and select the topology type for which you want to filter from the list that appears.

  The Manage Registry Variables dashboard refreshes, showing only the variables that have one or more values scoped to the selected topology type.

- To show only the variables that have a global default value set, click **By Global Default** and select **Defined** from the list that appears.

  The Manage Registry Variables dashboard refreshes, showing only the variables that have a global default value.

- To show only the variables that do not have a global default value set, click **By Global Default** and select **Undefined** from the list that appears.
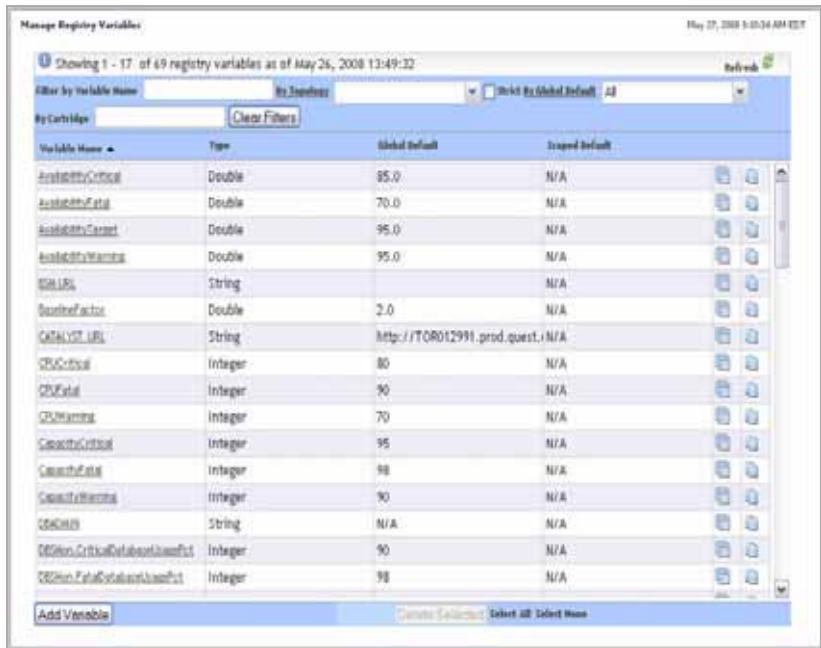
The Manage Registry Variables dashboard refreshes, showing only the variables that do not have a global default value.

- To show only the variables that come with a specific cartridge, in the **By Cartridge** box, type the cartridge name.

  The Manage Registry Variables dashboard refreshes, showing only the variables that come with the cartridge whose name that matches the expression.

- To clear the filters, click **Clear Filters**.

  The Manage Registry Variables dashboard refreshes, showing the list of all variables.

From here, you can proceed to any of the following procedures:

- "Editing permissions of registry variables" on page 188
- "Copying registry variables" on page 191
- "Deleting registry variables" on page 193

Editing permissions of registry variables

vFoglight allows you to control access to registry variables. For each variable you can grant or deny read, write, or control access to roles or users. For more information about security concepts in vFoglight, see Chapter 3, "Managing Users and Security" on page 105.

vFoglight employs the following behavior when it comes to permissions for registry variables:

- If no one has a permission to the registry variable, everyone has a permission.

- If one has a permission to the registry variable, others with undefined permission do not have any permission.

- Final permission is based on a combination of the role, user, and registry variable defined on the server side.

Use the Edit Permissions button ( ) on the Manage Registry Variables dashboard to navigate to the Edit Permissions for Registry Variable area, that allows you to add or edit permissions to roles and users, as outlined below. The Edit Permissions for Registry Variable area contains two tables that show the permissions for each vFoglight user or role.
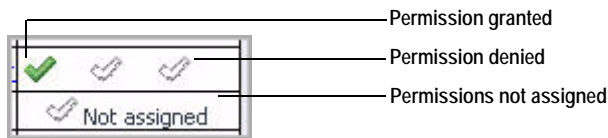
To add permissions for a registry variable:

1 In the Manage Registry Variables dashboard, in the row containing the variable whose permissions you want to edit, click the Edit Permissions for Registry Variable button ( ).

    The Edit Permissions for Registry Variable area appears in the display area.

2 To add permissions to a variable, complete the following steps.

    a Click the role or user to which you want to assign permissions.

        Tip   The Not Assigned icons in the **Permissions** columns indicate that the role has no permissions assigned to it.

    The **Add Role Permission** or **Add User Permission** dialog box appears.

b In the dialog box that appears, use the **Read**, **Write**, and **Control** check boxes to assign permissions as required, and click **Save**.

The dialog box closes and the selected entry refreshes, showing three check marks in the **Permission** columns, one for each of the read, write, and control permissions.

Permission granted

Permission denied

3 To edit or delete permissions for a variable, complete the following steps.

a Click the role or user whose permissions you want to edit.

Tip Three check marks in the **Permissions** columns indicate that the role already has permissions assigned to it.

The **Edit Role Permission** or **Edit User Permission** dialog box appears.

b To edit the permissions, ensure that the **Edit** option is selected and use the **Read**, **Write**, and **Control** check boxes as required.

To delete the permissions, select the **Delete** option.

c Click **Save**.

The dialog box closes and the selected entry refreshes, showing the newly-edited permissions.

Copying registry variables

Use the Copy Registry Variable button on the Manage Registry Variables dashboard to copy a registry variable, as outlined below.

To copy a registry variable:

Note This procedure continues from "" on

---

1 In the Manage Registry Variables dashboard, in the row containing the variable that you want to copy, click the Copy Registry Variable button ( ).

The **Copy Registry Variable** dialog box appears.
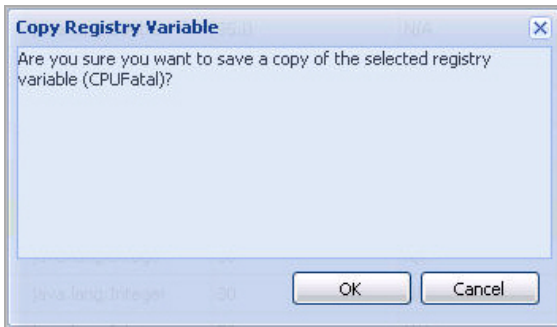
2 In the **Copy Registry Variable** dialog box, click **OK**.

The **Copy Registry Variable** dialog box closes and another dialog box appears, asking you to specify the name of the destination variable.

3 Type the name of the variable and click **OK**.

Note You must use a unique name.

The dialog box closes and the **Edit Registry Variable** pane appears in the display area.

4 If required, edit the newly-copied variable.

For more information, see "Editing Registry Variables" on page 200.

Deleting registry variables

Use the Delete Selected button on the Manage Registry Variables dashboard to delete a
registry variable, as outlined below.

Note   When a registry variable is deleted, all references to that variable in rule conditions and
expressions become invalid. This may cause the rule to fail to evaluate. If this occurs, you
must manually modify the rule condition or expression.

To delete a registry variable:

Note   This procedure continues from "Accessing the Manage Registry Variables dashboard" on
page 185.

1   In the Manage Registry Variables dashboard, select the row containing the variable that you want to delete.

2   Click the **Delete Selected** button at the bottom.

The **Registry Variable Confirmation** dialog box appears.
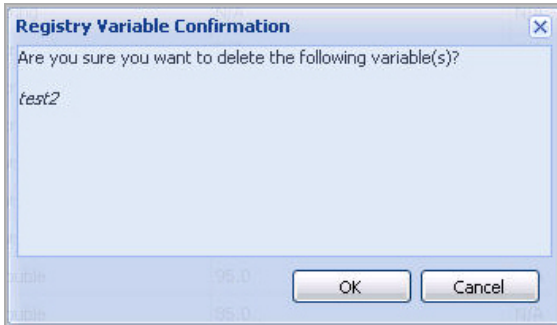
3   In the **Registry Variable Confirmation** dialog box, click **OK**.

The **Registry Variable Confirmation** dialog box closes.

4   Observe the Manage Registry Variables dashboard.

The newly-deleted variable no longer shows in the list.

Viewing and editing variable definitions

To view or edit variable definitions:

> **Note**   This procedure continues from "Accessing the Manage Registry Variables dashboard" on page 185.

1   In the Manage Registry Variables dashboard, click the **Variable Name** column of the row containing the variable whose definitions you want to view.

The **Edit Registry Variable** view appears in the display area.

2 Observe the variable definitions.

3 Edit the variable if required.

   For complete instructions, see "Specifying values" on page 201.

Creating Registry Variables

vFoglight allows you to create registry variables using the Create Registry Variable dashboard. You can access this dashboard from the navigation panel, or through the Manage Registry Variables dashboard.

To create a registry variable:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1 Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

2 Open the Create Registry Variable dashboard by completing one of the following steps:

• On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Manage Registry Variables**.

In the Manage Registry Variables dashboard that appears in the display area, click the **Add Variable** button in the lower-left corner.

or

• On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Create Registry Variable**.

The Create Registry Variable dashboard appears in the display area.

Create Registry Variable	Apr 23, 2008 11:13:55 PM EDT
Create Registry Variable	Registry Variable Added

Step 1: Create Registry Variable ⓘ

Registry Variable Name:

Description/Comments:

Registry Value Type: Boolean ▾

Cancel | Add

3 Specify the name, description, and data type for the variable using the following boxes:

• **Registry Variable Name**: The name of the variable.

> **Note** The registry variable name cannot be longer than two hundred and fifty (250) characters and cannot be the same as the name of an existing registry variable.
>
> In addition, the name cannot be changed once the registry variable has been added. This is because registry variables are referred to by their names in rule conditions and expressions and changing them would invalidate these references. However, you can copy a registry variable and give the copy a different name.

- **Description/Comments**: Any comments about the variable or its usage.
- **Registry Value Type**: The data type of the variable. There are 6 possible data types to which a variable can be set, as listed below.

   Note   The registry variable type cannot be changed once the registry variable has been added.

Registry Value Type	Description	Example
Boolean	A boolean value: `true` or `false`.	`true`
String	A text string.	`This message was generated by vFoglight.`
Integer	An integer value between -2^{31} and 2^{31} -1. For example, valid values include `235` and `-10000`.	`6825`
Double	A decimal value. For example, valid values include `34.1234`, `35e3` (meaning 35,000.0) or `1.2E-2` (meaning 0.012).	`95.0`

Registry Value Type	Description	Example
Timestamp	Contains a date and time. For example, valid values include `06/12/06`, `2006-06-21 15:30:21.0`, `June 7, 2006 3:08:21 PM`. Invalid date or time formats cannot be saved to the database and any attempts to save them result in an error. If the time is not provided, or the values are invalid, vFoglight treats the time as midnight. Prior to saving the value of a Timestamp variable, vFoglight converts it to the following format: `yyyy-mm-dd hh:mm:ss.ds` Once the value is converted, vFoglight stores it in the database.	`2008-08-10 23:15:16.0`

Registry Value Type	Description	Example
PasswordValue	A password value. Prior to storing the value of the PasswordValue data type in the registry, vFoglight encrypts it and saves the encrypted value in the database. This is useful in cases where you need to secure password values when passing it to command or remote command actions. For example, you create a registry variable of the PasswordValue type, `MyPassword`, and set its value to `demo123`. vFoglight encrypts the registry value, then stores it encrypted in the database (for example, `43-119-184-240-170-150-124-218-30-112-216-76-197-233-188-206`). In a function call `registry("MyPassword")`, vFoglight retrieves the registry value from the database in its encrypted form, which secures the password value.	`demo123`

4 Click **Add**.

5 A confirmation message appears in the display area, informing you that the variable has been created.
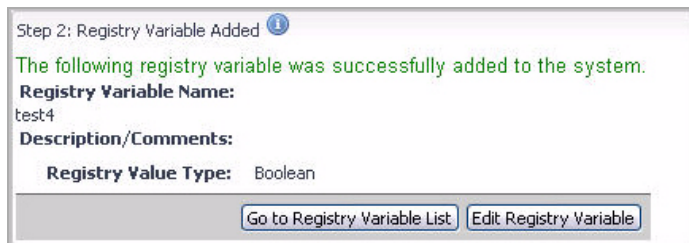
6 To verify if the variable appears in the Manage Registry Variables dashboard, click **Go to Registry Variable List**.

To edit the newly-created variable, click **Edit Registry Variable**. For information on how to edit registry variables, see "Editing Registry Variables" on page 200.

Editing Registry Variables

You can edit a newly-created or an existing variable and assign it a global default value, associate values with specific topology types or objects, or configure performance calendars for each value.

For instructions, see the following sections:

- "Getting started with variable definitions" on page 200
- "Specifying values" on page 201
- "Using performance calendars" on page 204
- "Scoping variables to topology types or object instances" on page 206

Getting started with variable definitions

Once you create a variable, you can proceed to add comments to it and edit its settings as required.

You cannot edit the name of a registry variable after it has been created. This is because registry variables are referred to by name in rule conditions and expressions; changing their names would invalidate these references. Additionally, you cannot edit the value type of a registry variable after it has been created.

To get started with editing variable definitions:

Note This procedure continues from "Accessing the Manage Registry Variables dashboard" on page 185 or "Creating Registry Variables" on page 195.

1 In the Manage Registry Variables dashboard, click the **Variable Name** column of the row containing the variable whose definitions you want to view.

The **Edit Registry Variable** view appears in the display area.

> **Note** The name and value type of a registry variable cannot be changed after the variable creation. Registry variables are referred to by their names in rule conditions and expressions and changing them would invalidate these references. However, you can copy a registry variable and give the copy a different name.

2 **Optional**. Add or edit the existing comments in the **Description/Comments** box and then click **Save** on the right.

From here, you can proceed to "Specifying values" on page 201

Specifying values

A registry variable can have a global value and multiple scoped values (that is, values that are associated with specific topology types or objects). Each of these values has a default setting. For example, if the variable's type is Integer, the global default value would be set to a specific integer. However, you can also configure the setting for each value to vary over time by adding schedules and alternate values to the value's performance calendars. A performance calendar specifies an alternative value which is only in effect during the span(s) of time set by a schedule. All of the schedules that have been created are available for use with registry variables. See "Example: Assigning

The values that you assign to a variable must be consistent with the data type that you specify at variable creation time. For example, if you selected Integer as the data type, type 10 when specifying the value, not ten.

To specify values for a variable:

Note   This procedure continues from "Getting started with variable definitions" on page 200 or "Viewing and editing variable definitions" on page 194.

---
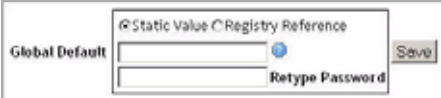
1   Specify a default value for the variable using the options in the **Global Default area**.

There are two types of options you can specify:

• **Static Value**: This value does not change over time.

When you select this option, specify the value of the registry variable in the **Global Default** area. The value you provide must be compatible with the variable's data type that you set at variable creation. The appearance of the Global Default area depends on the type of data you can use, as indicated in the table below. For example, if the data type is Boolean, instead of typing true or false, select the appropriate value from the list that appears.

Data Type	Global Default Area	To specify the value
Boolean		Click the box and select **true** or **false** from the list that appears.

Data Type	Global Default Area	To specify the value
String Long Integer Double Timestamp		Type the value in the box, making sure that the value is compatible with the data type. For example, if the variable is of a String type, type a text string.
Password Value		Type the password into each box.

For more information about different data types you can use, see "Creating Registry Variables" on page 195

- **Registry Variable Reference**: This value references another registry variable.

  When you select this option, the **Global Default** area refreshes, allowing you to select from available registry variables whose data type matches the data type of the registry variable that you are editing. For example, if the data type is Long, clicking the box in the **Global Default** area shows a list containing the registry variables of the Long type that exist in your configuration.
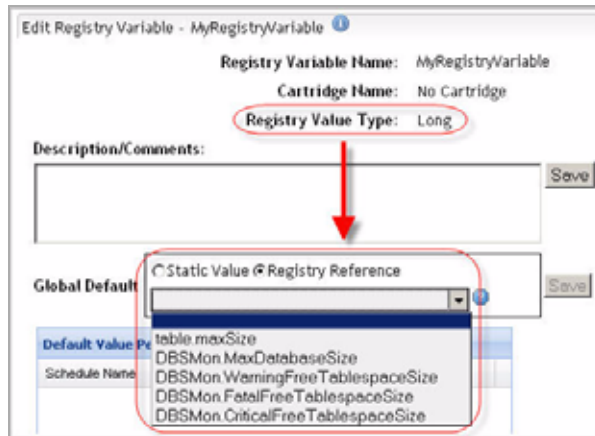
> **Note** The value that you specify in this field applies to all topology types and objects other than those that you specify in the **Registry Values** table, as described in "Scoping variables to topology types or object instances" on page 206. It is effective at all times except at the times set in the schedules added to the **Default Value Performance Calendar**, as described in "Using performance calendars" on page 204.

2   Click **Save** to save the global default value.

From here, you can proceed to "Using performance calendars" on page 204.

Using performance calendars

If you want the default value to change over time, add one or more schedules to the performance calendar and specify the value for each schedule. See "Example: Using Performance Calendars" on page 216 for an example of how to use this feature.

The vFoglight Management Server evaluates the schedules in the performance calendar in the order they are listed, starting with the first one. Changing their order affects the behavior of the actions that are associated with the variable whose value is set by the schedule-based entries in the performance calendar.

For example, if there are two schedule entries in the performance calendar that overlap in time but have two different values, the first entry listed takes precedence, causing one or more actions that are associated with that variable to make use of that entry for the duration of the schedule.

Working with vFoglight Rules and Registry
Working with vFoglight Registry Variables
205

To add schedules to a performance calendar:

Note   This procedure continues from "Specifying values" on page 201.

---

1   Choose a schedule.

Click **Schedule Name** and select a schedule from the list that appears.

The list reflects the existing schedules. For information on how to add schedules to vFoglight, see Chapter 8, "Using Schedules" on page 395.

2   Specify the value for the newly-selected schedule.
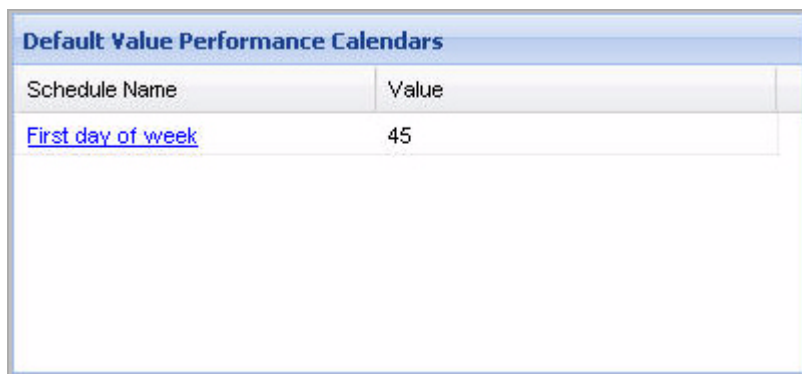
Similar to the global default value, there are two options you can specify: **Static Value** and **Registry Variable Reference**.

Use the **Value** box to specify the value with which you want to replace the default value during the period defined by the schedule.

Note   The value you specify here should match the data type of the variable. For example, if the variable is a boolean, you can set it to `true` or `false`.

3   Click **Add**.

The schedule and alternate value appear in the **Default Value Performance Calendars** table, as specified.

Default Value Performance Calendars	
Schedule Name	Value
First day of week	45

4   If required, add more schedules to the list and ensure that their order is valid.

Caution   The vFoglight Management Server evaluates schedule-based values in the order that they are listed, starting with the first one. Changing their order affects the output of actions that are associated with the value that is associated with their schedule entries.

To move a threshold bound up or down, in the **Default Value Performance Calendar** table, in the **Schedule Name** column, use the Move up the selected performance calendar (⬆) or Move down the selected performance calendar (⬇) buttons as required.

From here, you can proceed to "Scoping variables to topology types or object instances" on page 206.

Scoping variables to topology types or object instances

The way you define registry variables can help you to reduce the number of rules that need to be created and managed by allowing you to create a single rule that can be applied to several topology types or objects.

If you want to scope the registry variable to topology types or objects, and add schedule-specific values to it, add one or more values to the Registry Values table.

To scope the registry value to a topology type or object:

Note This procedure continues from "Using performance calendars" on page 204.

1 Click **Add Registry Value** at the bottom.

The **Create Registry Value—Step 1** view appears in the display area.

2   Click **Topology Type** and select a type from the list that appears.

3   **Optional**. Narrow down your scope to a particular object

Click **Topology Object** and select an object from the list that appears.

4   Specify the default value that you want the variable to use when scoping on the newly-specified topology type or object.

In the Default Value area, select the **Static Value** or **Registry Variable Reference** option and use the **Value** box to specify the default value.

5   Click **Add**.

The **Create Registry Value—Step 2** view appears in the display area.
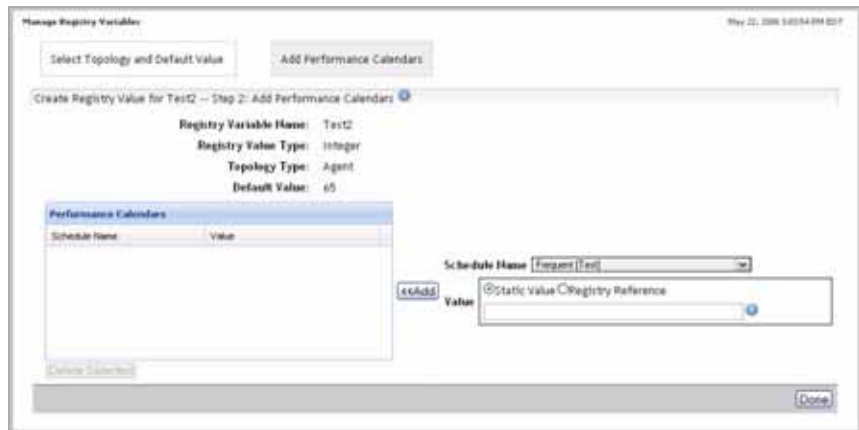
6   **Optional**. If you want the default value to change over time, add one or more schedules to the **Default Value Performance Calendars** table and specify the value for each schedule.

To add a schedule to the performance calendar, complete the following steps.

a   Choose a schedule.

Click **Schedule Name** and select a schedule from the list that appears.

The list reflects the existing schedules. For information on how to add schedules to vFoglight, see Chapter 8, "Using Schedules" on page 395.

b   Specify the value for the newly-selected schedule.

Similar to the global default value, there are two options you can specify: **Static Value** and **Registry Variable Reference**.

Use the **Value** box to specify the value with which you want to replace the default value during the period defined by the schedule.

c Click **Add**.

The schedule and alternate value appear in the **Default Value Performance Calendars** table, as specified.

Default Value Performance Calendars	
Schedule Name	Value
First day of week	45

d Click **Done**.

In the Edit Registry Variable pane, the **Registry Value** table refreshes, showing the newly-added registry value scoped to a topology type or object, as specified.

Registry Values		
Topology Type	Topology Object Name	Scoped Default
Agent		65
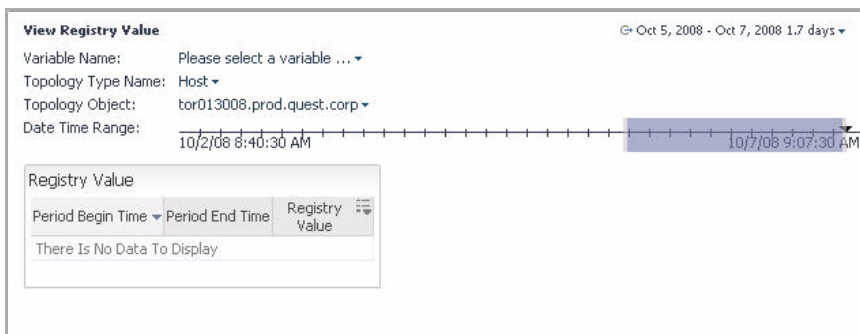
Viewing Registry Values

A registry variable can have a global value that is available to all topology types and objects. It can also have multiple additional values associated with specific topology types or objects, or calendar dates. To find out what is the value of a registry variable for a particular topology type or object, and, if applicable, during a specific time period, use the Check Registry Value dashboard.

To view the values of a registry variable:

   1   Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

   2   On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Check Registry Value**.

   The Check Registry Value dashboard appears in the display area, showing the **View Registry Variable** view.

   3   The dashboard shows the following information:

   •   **Variable Name**: The name of the registry variable whose value you want to view.

   •   **Topology Type Name**: The topology type with which the registry value is associated.

   •   **Topology Object**: The object instance of the specified topology type with which the registry value is associated.

   •   **Date Time Range**: The date and time range for which you want to look up the registry value.

- **Registry Value**: The value to which the variable is set during a specified date and time range. If there are multiple time ranges during which the registry value changes, the table shows the registry value for each range.

4 Specify the name of the variable whose values you want to view.

For example, we will look at the SYSADMIN variable that is scoped to two topology object instances and two different performance calendars.

Note By default, the SYSADMIN variable has no scoped values. They have been created for the purpose of this exercise. For an example of how you can scope a registry variable to multiple topology objects, see "Example: Assigning Multiple Values to a Registry Variable" on page 216.

a In the **View Registry Variable** view, click the link that appears on the right of **Variable Name**.

The **Registry Variable** list appears, showing the registry variables that exist in your vFoglight environment.

Registry Variable ▲
AvailabilityCritical
AvailabilityFatal
AvailabilityTarget
AvailabilityWarning
BaselineFactor
BSM URL
CapacityCritical
CapacityFatal
CapacityWarning
CATALYST_URL
CollisionRateCritical
CollisionRateWarning
CPUCritical
CPUFatal
CPUWaitCritical
CPUWaitWarning
CPUWarning
DBADMIN
DBSMon.CriticalDatabaseUsagePct
DBSMon.CriticalFreeTablespaceSize

Note The list does not include the registry variables that contain password values.

    b In the **Registry Variable** list, scroll down until you find **SYSADMIN** and select that entry.

5 Select the topology type to which the SYSADMIN variable is scoped.

    a In the **View Registry Variable** view, click the link that appears on the right of **Topology Type Name**.

       The **Topology Type** list appears, showing all topology types that exist in your vFoglight environment.

Topology Type ▲
Agent
AgentHealthState
AgentState
AggregateModelInstance
AggregateModelRoot
AIX_Host
AlarmChangeType
AlarmRuleBasedView
AlarmSeverity
ApacheSvr_ReqCodes
ApacheSvr_ReqTypes
ApacheSvr_Stats
ApacheSvr_Transactions
ApacheSvrAgent
ApacheSvrAgent_F4Table
ApplicationTier
ApplicationTopology
ApplicationTopologyModel
AppMonitor_AgentMsgs
AppMonitor_AppAvailability

    b In the **Topology Type** list, scroll down until you find **Host** and select that entry.

6 Select the object instance of the selected topology type to which the SYSADMIN variable is scoped.

    a In the **View Registry Variable** view, click the link that appears on the right of **Topology Object**.

       The **Topology Object** list appears, showing the object instances of the selected topology type.

    b In the **Topology Object** list, select an object instance.

7 Specify the date and time range during which you want to see the registry values.

In the **View Registry Variable** view, on the right of **Date Time Range**, drag the edges of the Zonar to set the range. For more information about the Zonar, see the *vFoglight User Guide*.

The **Registry Value** table refreshes, showing different registry values for different date and time periods.

8 **Optional**. Reduce the number of columns that appear in the audit log table.

    a In the audit log table, in the **Operation Name (Name)** column, click the **Show/Hide columns** button.

Show/Hide columns

The **Show columns** dialog box appears.

Show columns

☑ Period Begin Time

☑ Period End Time

☑ Registry Value

[Apply]   [Cancel]

Actions

Export as CSV...
Export as PDF...

Since all of the four columns appear in the **Registry Value** table by default, all of the check boxes that correspond to the columns appear selected.

b To hide a column, in the **Show columns** dialog box, clear the corresponding check box.

or

To show a column, clear the corresponding check box.

For example, to display only the time at which the value was set and the value, ensure that the **Period Begin Time** and **Registry Value** check boxes are selected, and clear the **Period End Time** check box.

c Click **Apply**.

The audit log table refreshes, showing only the selected columns.

Period Begin Time	Registry Value
10/14/08 5:06 PM	mary@abc.com
10/18/08 12:00 AM	kevin@abc.com
10/20/08 12:00 AM	mary@abc.com

9 **Optional**. Print the list of audit logs to a file.

a In the audit log table, in the **Operation Name (Name)** column, click the **Show/Hide columns** button.

Show/Hide columns

Period Begin Time	Period End Time	Registry Value
10/14/08 5:06 PM	10/18/08 12:00 AM	mary@abc.com

The **Show columns** dialog box appears.
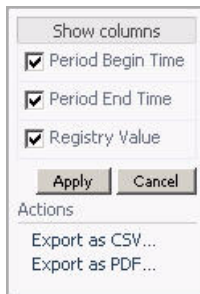
b In the **Show Columns** dialog box, under **Actions**, click one of the following links:

Export as CSV, to export the table contents to a Comma Separated Values (CSV) file.

Export as PDF, to export the table contents to a PDF file.

Important If you previously show or hide one or more columns in the audit table, this layout is reflected in the exported file. For example, if you display only the time at which the value was set and the registry value, only the **Period Begin Time** and **Registry Value** columns are exported to a file.

When exporting the table contents to a PDF file, the PDF output appears in a new tab or window (depending on the type and version of your Web browser).

When exporting the table contents to a CSV file, a dialog box appears, allowing you open the exported file, or to save it to disk.
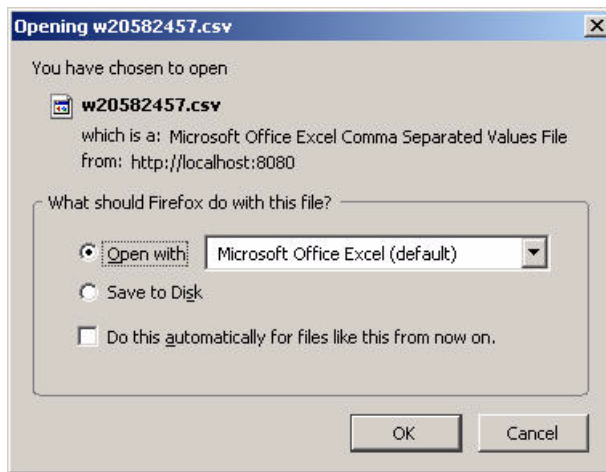
Note The appearance of the above dialog box may be different, depending on the type
and version of your Web browser.

10 Change the object instance and the date and time range.

The **Registry Value** table refreshes, showing the values scoped to the selected
object instance and date and time range.

Registry Value			
Period Begin Time	Period End Time	Registry Value	
10/15/08 3:05 PM	10/18/08 12:00 AM	pete@xyz.com	
10/18/08 12:00 AM	10/20/08 12:00 AM	ron@xyz.com	
10/20/08 12:00 AM	10/21/08 3:43 PM	pete@xyz.com	

11 View the logic that determines a registry value that appears in the list.

Click a row containing a registry value.

The **Registry Lookup Path** dialog box appears, showing the variable name,
scoped topology type and object (if applicable), and the time period during which
the selected value is valid.

```
Registry Lookup Path                              ×
Variable Name: SYSADMIN
Topology Type Name: Host
Topology Object: tor013008.prod.quest.corp
Period: 10/15/08 3:05 PM - 10/18/08 12:00 AM
        topology type: object              value
Host: tor013008.prod.quest.corp      pete@xyz.com
```

Example: Assigning Multiple Values to a Registry Variable

You have several groups of servers in your monitored environment. You want an email to be sent to the system administrator if one of the servers becomes unavailable, but a different administrator is responsible for each group. Instead of creating a different rule with a different email action for each group, you create a registry variable called *Administrator* and then assign it a different value (the email address of the appropriate administrator) for each group of servers. You then create a single simple rule that fires if any of the servers become unavailable and which uses the *Administrator* variable in the rule's email action.

Example: Using Performance Calendars

Creating a performance calendar for a variable's values allows you to cause rules to behave differently at different times.

Note   If the schedule used in a performance calendar is deleted, the performance calendar will automatically be deleted as well.

There is a simple rule that applies to the servlets in your application; an alarm fires if the request response time for a servlet exceeds the threshold set in the rule condition. This threshold is a registry variable called *ResponseTimeTooLong*; it is scoped to the topology type *J2EEServlet* and its default scoped value is 8 seconds.

However, you know that at certain times of day response times for servlet instances are expected to exceed this threshold. At these times, the acceptable response time can be as long as 15 seconds.

You can use registry variable performance calendars to account for this and avoid having the rule fire as a result of false positives. You create a schedule called *EndOfDay*

that is set to the recur daily at the times when it is acceptable for response times for the servlet instances to exceed eight seconds. You then navigate to the *Manage Registry Variables* dashboard, and select the variable *ResponseTimeTooLong*. You leave the variable's scoped value for servlets at its default setting of 8 seconds but add the schedule *EndOfDay* to the list of *Performance Calendars* for the variable, set the replacement value to the alternative threshold of 15 seconds and then save your changes.

Example: Assigning Host-Specific Email Addresses of vFoglight System Administrators

The vFoglight Management Server includes the global registry variable SYSADMIN that allows you to set the email address of the vFoglight System Administrator. Larger monitoring environments have different system administrators that manage different parts of vFoglight. For example, you can have a different system administrator looking after each monitored host. Monitored hosts in the vFoglight data model exist as object instances of the topology type Host. vFoglight registry variables can have topology-scoped variables associated with particular topology types and/or their object instances. This feature allows you to assign host-specific email addresses of different vFoglight administrators using the SYSADMIN registry variable. In this example, there are two monitored hosts and each host has a designated system administrator, as listed below.

Host	Administrator's email
HostA	joe@xyzdomain.com
HostB	larry@pdqdomain.com

To assign host-specific email addresses:

Note This procedure continues from "Getting Started with the Administration Module" on page 32.

1 Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Manage Registry Variables**.

   The Manage Registry Variables dashboard appears in the display area.
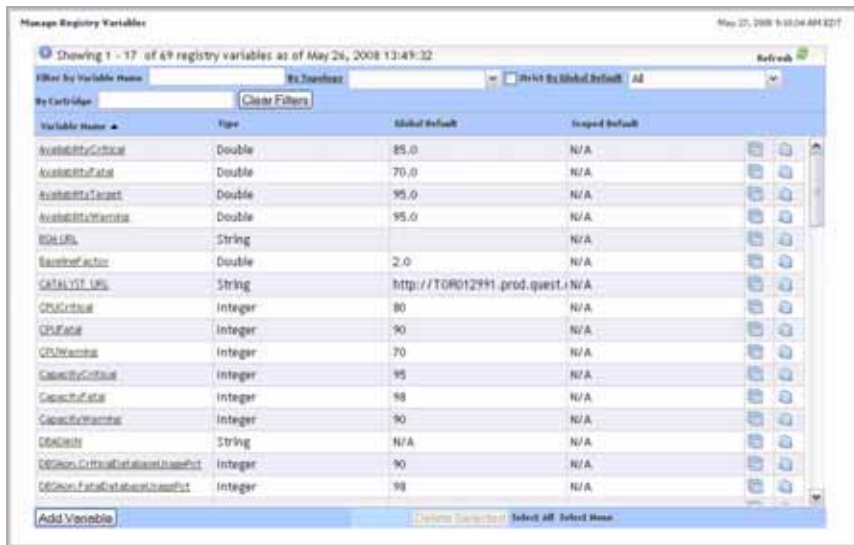
3 On the Manage Registry Variables dashboard, locate the row containing the SYSADMIN variable.

> **Tip** You can filter the list of variables using filters. At the top of the Manage Registry Variables dashboard, in the **Filter By Variable Name** box, type *SYSADMIN*. The Manage Registry Variables dashboard refreshes, showing only the *SYSADMIN* variable.
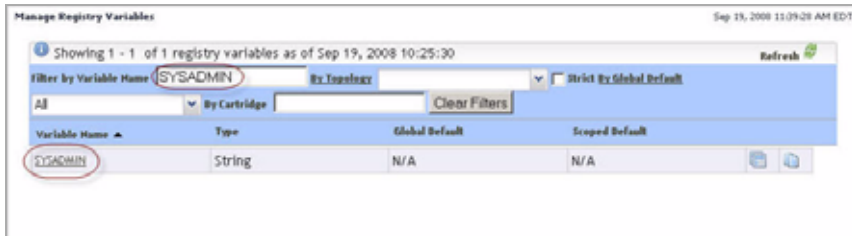
4 Open the SYSADMIN variable for editing.

Click the **Variable Name column** of the row containing **SYSADMIN** entry.

The Manage Registry Variables dashboard refreshes, showing the **Edit Registry Variable** view.

5 Assign an email address to each monitored host by adding two host-specific values to the SYSADMIN variable.

To add a topology-scoped value to the registry variable, complete the following steps.

a At the bottom of the **Edit Registry Variable** view, click **Add Registry Value**.

The Manage Registry Variables dashboard refreshes, showing the **Create Registry Value—Step 1** view.

b Set the scope of the SYSADMIN variable to the Host type.

In the **Create Registry Value—Step 1** view, on the right of **Topology Type**, click **Select Type**.

In the list that appears, under **Core**, select **Host**.

c Narrow down the scope of the value by setting the value scope to a particular instance of the Host type.

On the right of **Topology Object**, click **All Objects**

In the list that appears, select a monitored host.

d Specify the email address of the system administrator that is responsible for that host.

In the **Default Value** area, ensure that the **Static Value** option is selected.

In the box at the bottom of the **Default Value** area, type the administrator's email address.

e At the bottom of the **Create Registry Value—Step 1** view, click **Add**.

The Manage Registry Variables dashboard refreshes, showing the **Create Registry Value—Step 2** view.

f In the bottom-right, click **Done**.

The Manage Registry Variables dashboard refreshes, showing the newly-added value in the **Registry Values** table.

To add another email address, scoped to the other monitored host, repeat step a to step f.

When you add the second topology-scoped value, the Registry Values table shows two entries, one for each host.

Registry Values		
Topology Type	Topology Object Name	Scoped Default
Host	HostA.MyDomain.com	joe@xyzdomain.com
Host	HostB.MyDomain.Com	larry@pdqdomain.com

Working with Rules

vFoglight allows you to create flexible rules that can be applied to complex, interrelated data from multiple sources within your distributed system. You can associate several different actions with a rule, configure a rule so that it does not fire repeatedly, and associate a rule with schedules that define when it should and should not be evaluated.

The following list introduces you to the concepts and terms related to rules.

- *Rule*. A rule is a piece of business logic that links a condition with a result. The result may be linked to actions. There are two types of rules in vFoglight: simple rules and multiple-severity rules. A rule includes a scope, conditions, expressions, messages, and actions.

- *Rule Scope*. The scope of a rule defines the set of topology objects against which it will run. The scope object is the object on which alarms will appear in the vFoglight interface.

- *Simple Rule*. A simple rule runs user-defined actions when the condition for that rule is met. Simple rules do not create alarms and unlike multiple-severity rules (see below), they don't have severity levels. A simple rule is logic that is triggered by data. See "Defining rule types" on page 250 for more information.

- *Multiple-Severity Rule*. A multiple-severity rule is a more complex type of rule that can include up to five levels of severity. These levels are described in more detail in "Defining rule types" on page 250. This type of rule always creates an alarm when the condition associated with one of its severity levels is met.

- *Severity State*. A severity state is the highest severity condition of a multiple-severity rule that evaluated to true.

- *Fire Prevention*. A group of settings that prevent actions and alarms from firing repeatedly for a rule.

- *Effective Period*. A scheduled period during which a rule is active.

- *Blackout Period*. A scheduled period during which a rule is inactive.

- *Monitoring Data*. Data that has been collected from your monitored environment by the agents and transformed into a standard format for use by the vFoglight Management Server. Monitoring data includes both metrics and topology object properties.

- *Function*. Rule conditions and expressions are matched against monitoring data. Functions cause calculations to be performed on the data specified in conditions and expressions, allowing the data to be modified before it is matched.

- *Registry Variable*. A variable stored in the vFoglight registry that can be used in rule conditions, actions, and expressions. The value of a registry variable can be configured to change over time. Variables can be scoped to specific topology types or objects.

- *Metric*. A metric is a value measured over time. There are two types of metrics in vFoglight: raw and derived. Every metric is scoped to a topology type (and may be scoped to one or more specific topology objects of that type).

- *Raw Metric*. A raw metric is simply collected from your monitored environment. That is, it is not calculated from other metrics.

- *Derived Metric*. A derived metric is calculated from one or more (raw or derived) metrics. Derived metrics can be created in the vFoglight Administration Module.

- *Topology Object Property.* Data collected from your monitored environment that describes a topology object.

You can create new rules, define existing or newly-created rules, and manage rules using the dashboards that come with the Administration module. vFoglight comes with a set of core rules. Each cartridge has their own collection of rules. For information about core vFoglight rules, see "Core vFoglight Rules" on page 305. For details about cartridge-based rules, see your cartridge documentation.

For information about rule-related operations that you can perform in the Administration module, see the following sections:

- "Managing Rules" on page 225
- "Creating Rules" on page 246
- "Defining Rules" on page 248
- "Defining Conditions, Alarms, and Actions" on page 254
- "Associating Rules with Schedules" on page 299
- "Defining Alarm and Action Behavior" on page 302
- "Defining Rule-Level Variables" on page 303
- "Core vFoglight Rules" on page 305
- "Example: Creating a Multiple-Severity Rule Scoped to an EJB Instance" on page 311
- "Example: Creating a Simple Rule" on page 313
- "Example: Creating Multiple-Severity Rules with a Topology Scope" on page 314

Managing Rules

The Manage Rules dashboard contains a table that lists all of the simple rules and multiple-severity rules that are currently defined, the scope of each rule, and the cartridge with which each rule is associated (if applicable).

This dashboard also includes controls for filtering the list of rules by cartridge; for adding, copying, deleting, and editing rules; and for suspending rule alarms and actions.

For instructions on how to use the Manage Rules dashboard, see the following sections:

Accessing the Manage Rules dashboard

The Manage Rules dashboard includes a list of the rules that exist in your monitoring environment and allows you to add or delete rules and perform other rule management operations.

To access the Manage Rules dashboard:

Note   This procedure continues from " or ".

---

1   Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Manage Rules**.

The Manage Rules dashboard appears in the display area.
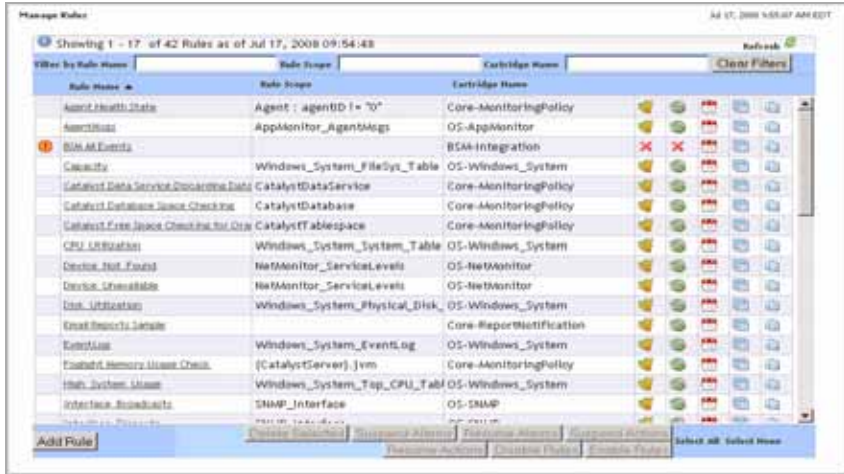
3 Newly-installed cartridges. In the upper-right corner, click Refresh.

The list of rules refreshes, showing any rules that come with newly-installed cartridges.

4 To sort the list of variables by their name, scope or the name of the cartridge name to which they belong, click the **Rule Name**, **Rule Scope**, or **Cartridge Name** column headings as required.

5 Optional. Filter the list of rules.

• To show only the rules whose name matches a particular text pattern, in the **Rule Name** box at the top, type the text pattern.

The Manage Rules dashboard refreshes, showing only the rules whose name matches the specified text pattern.

• To show only the rules whose scope name matches a particular text pattern, in the **Rule Scope** box at the top, type the text pattern.

The Manage Rules dashboard refreshes, showing only the rules whose scope matches the specified text pattern.

- To show only the rules that belong to a particular cartridge, in the **Cartridge Name** box at the top, type the cartridge name.

  The Manage Rules dashboard refreshes, showing only the rules that come with the specified cartridge.

- To clear the filters, click **Clear Filters**.

  The Manage Rules dashboard refreshes, showing the list of all rules.
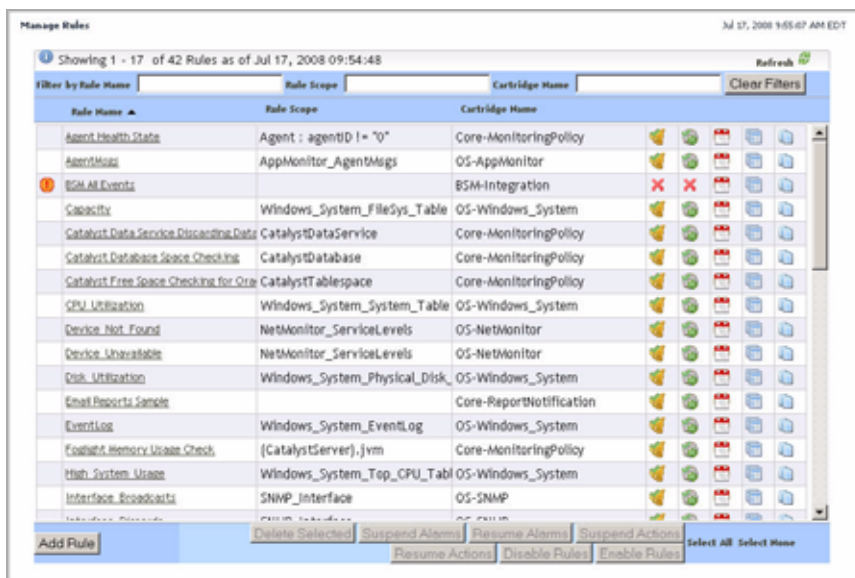
From here, you can proceed to any of the following procedures:

- "Editing rule permissions" on page 228
- "Copying rules" on page 231
- "Deleting rules" on page 233
- "Disabling or enabling rules" on page 234
- "Suspending or resuming alarms" on page 236
- "Suspending or resuming actions" on page 238
- "Viewing rule schedules" on page 240
- "Viewing a rule summary" on page 241

- "Viewing and editing rule definitions" on page 245

Editing rule permissions

vFoglight allows you to control access to rules. For each rule you can grant or deny read, write, or control access to roles or users. For more information about security concepts in vFoglight, see Chapter 3, "Managing Users and Security" on page 105.

vFoglight employs the following behavior when it comes to rule permissions:

- If no one has a permission to the rule, everyone has a permission.
- If one has a permission to the rule, others with undefined permission do not have any permission.
- Final permission is based on a combination of the role, user, and rule defined on the server side.

Use the Edit Permissions button ( ) on the Manage Rules dashboard to navigate to the Edit Permissions for Rule area, that allows you to add or edit permissions to roles and users, as outlined below. The Edit Permissions for Rules area contains two tables that show the permissions for each vFoglight user or role.
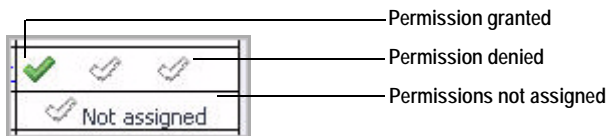
To add permissions for a rule:

Note This procedure continues from "Accessing the Manage Rules dashboard" on page 225.

1 In the Manage Rules dashboard, in the row containing the rule whose permissions you want to edit, click the **Edit Permissions for Rule** button ( ).

The Edit Permissions for Rules area appears in the Manage Rules dashboard.

2 To add permissions to a rule, complete the following steps.

    a Click the role or user to which you want to assign permissions.

        Tip   The Not Assigned icons in the **Permissions** columns indicate that the role has no permissions assigned to it.

    The **Add Role Permission** or **Add User Permission** dialog box appears.

b In the dialog box that appears, use the **Read**, **Write**, and **Control** check boxes to assign permissions as required, and click **Save**.

The dialog box closes and the selected entry refreshes, showing three check marks in the **Permission** columns, one for each of the read, write, and control permissions.

- Permission granted
- Permission denied

3 To edit or delete permissions for a rule, complete the following steps.

a Click the role or user whose permissions you want to edit.

Tip Three check marks in the **Permissions** columns indicate that the role already has permissions assigned to it.

The **Edit Role Permission** or **Edit User Permission** dialog box appears.

b To edit the permissions, ensure that the **Edit** option is selected and use the **Read**, **Write**, and **Control** check boxes as required.

c To delete the permissions, select the **Delete** option

d Click **Save**.

The dialog box closes and the selected entry refreshes, showing the newly-edited permissions.

Copying rules

Use the Copy Rule button on the Manage Rules dashboard to copy a rule, as outlined below.

To copy a rule:

Note   This procedure continues from "" on page 225.

---

1 In the Manage Rules dashboard, in the row containing the rule that you want to copy, click the Copy Rule button (🗗).

The **Rule Confirmation** dialog box appears.

Rule Confirmation

Are you sure you want to save a copy of the selected rule (Console)?

OK   Cancel
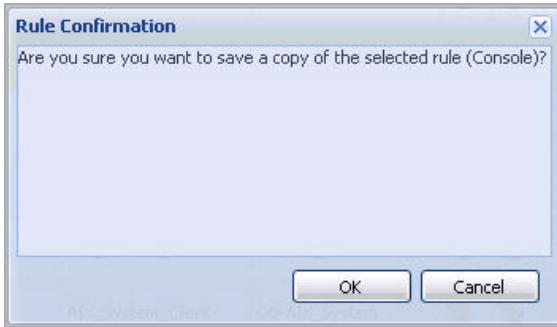
2 In the **Rule Confirmation** dialog box, click **OK**.

The **Rule Confirmation** dialog box closes and the Edit Rule area appears in the Manage Rules dashboard, allowing you to edit the newly-copied rule.
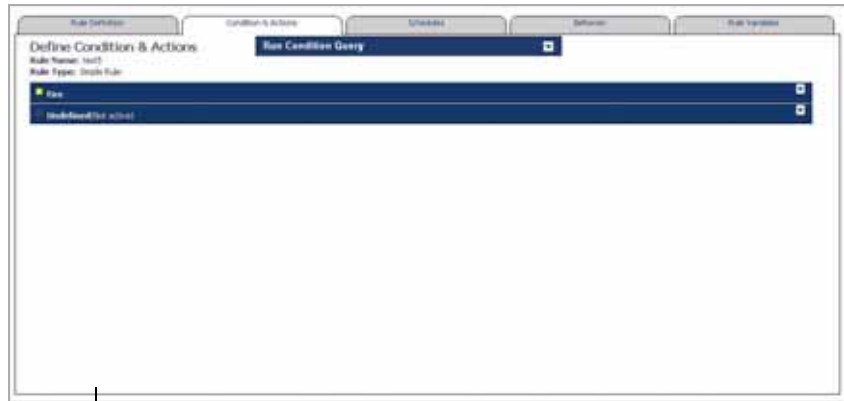
Simple rule

Multiple-severity rule

Note   The appearance of the Edit Rule area depends on the severity levels of the newly-copied rule as indicated in the above illustration. For more information about rule severity levels, see "Adding severity-level variables" on page 256

3 If required, edit the newly-copied rule.

For more information, see "Defining Rules" on page 248.

Deleting rules

Use the Delete Selected button on the Manage Rules dashboard to delete a rule, as outlined below.

To delete a rule:

Note   This procedure continues from ".

---

   1 In the Manage Rules dashboard, select the row containing the rule that you want to delete.

   2 Click the **Delete Selected** button at the bottom.

     The **Delete Rule Confirmation** dialog box appears.

   3 In the **Delete Rule Confirmation** dialog box, click **OK**.

     The **Delete Rule Confirmation** dialog box closes.

   4 Observe the Manage Registry Variables dashboard.

     The newly-deleted rule no longer shows in the list.

Disabling or enabling rules

In some cases you may need to enable or disable a rule. For example, if a rule monitors a host that needs to taken offline for system maintenance, you can disable that rule temporarily to avoid triggering its actions while the monitored host is unavailable. Use the Manage Rules dashboard to drill down to the rule that you want to disable or enable, and then use the Disable Rules or Enable Rules buttons on the Manage Rules dashboard to change the rule state.

To disable a rule:

Note   This procedure continues from ".

---

1 In the Manage Rules dashboard, select the row containing the rule that you want to disable.

Tip To select multiple rules, press the CTRL or SHIFT key while selecting the rows containing the rules that you want to disable.

2 Click the **Disable Rules** button at the bottom.

The **Delete Rule Confirmation** dialog box appears.

3 In **Delete Rule Confirmation** dialog box, click **OK**.

The **Delete Rule Confirmation** dialog box closes and the Manage Rules dashboard refreshes, showing a Rule is currently disabled icon (🔴) in the row containing the newly-disabled rule.

4 Place the mouse pointer over the Rule is currently disabled icon (🔴) icon.

A tool tip appears, indicating that the rule is disabled.

To enable a rule:

Note This procedure continues from "

1 In the Manage Rules dashboard, select the row containing the disabled rule that you want to enable.

Note A Rule is currently disabled icon (🔴) appears in the row containing a rule that has been disabled.

Tip To select multiple rules, press the CTRL or SHIFT key while selecting the rows containing the rules that you want to enable.

2 Click the **Enable Rules** button at the bottom.

The **Delete Rule Confirmation** dialog box appears.

Delete Rule Confirmation

Are you sure you want to enable following rules?

Agent Health State

OK   Cancel

3 In **Delete Rule Confirmation** dialog box, click **OK**.

The **Delete Rule Confirmation** dialog box closes and the Manage Rules dashboard refreshes, no longer showing the Rule is currently disabled icon (🔴) in the row containing the newly-enabled rule.

Suspending or resuming alarms

You can configure a rule to stop generating alarms for a specified length of time (beginning immediately). It can be useful to suspend alarms in many situations, such as when one or more servers are being brought offline for system maintenance.

Note vFoglight stops both generating and clearing alarms for a rule during the period when its alarms are suspended.

To suspend alarms for a rule:

Note This procedure continues from "Accessing the Manage Rules dashboard" on page 225.

1 In the Manage Rules dashboard, select the row containing the rule whose alarms you want to suspend.

2 Click the **Suspend Alarms** button at the bottom.

The **Temporarily Suspend Rule Alarms** dialog box appears.

Temporarily Suspend Rule Alarms

For: 10 minutes ▼ Go Cancel
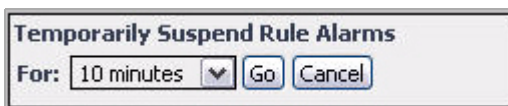
3 Specify the time period for which you want to suspend alarms.

In the **Temporarily Suspend Rule Alarms** dialog box, click **For** and select the time period as required, then click **Go**.

The **Temporarily Suspend Rule Alarms** dialog box closes and the Manage Rules dashboard refreshes, showing a warning icon in the row containing the rule with newly-suspended alarms.

Note The warning icon indicates different types of states a rule may be in. For example, it appears when a rule is disabled, or when its alarms or actions are suspended. Placing the mouse pointer over the icon shows more details about the rule state.

4 Place the mouse pointer over the warning icon.

A tool tip appears, indicating that alarms are currently suspended for the rule.

To resume alarms for a rule:

Note This procedure continues from "" on page 225.

1 In the Manage Rules dashboard, select the row containing the rule whose alarms you want to resume.

2 Click the **Resume Alarms** button at the bottom.
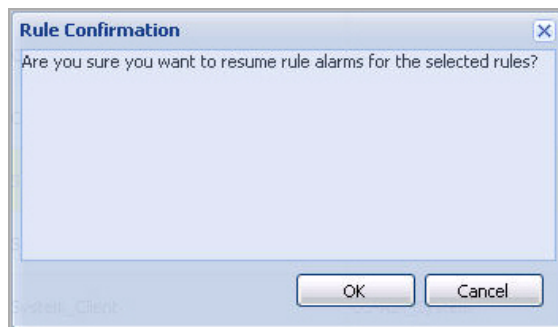
The **Rule Confirmation** dialog box appears.

3 Click **OK.**

The **Rule Confirmation** dialog box closes and the Manage Rules dashboard refreshes.

4 In the Manage Rules dashboard, observe the row containing the rule whose alarms you resumed.

The absence of the warning icon indicates that the alarms for the rule are no longer suspended.

If a warning icon appears in the row containing the rule with newly-resumed alarms, place the mouse pointer over the icon. The tool tip that appears no longer indicates that the rule's alarms are suspended.

Note The warning icon indicates different types of states a rule may be in. For example, it appears when a rule is disabled, or when its alarms or actions are suspended. Placing the mouse pointer over the icon shows more details about the rule state.

Suspending or resuming actions

You can configure a rule to stop performing actions for a specified length of time (beginning immediately). It can be useful to suspend alarms in many situations, such as when one or more servers are being brought offline for system maintenance.

To suspend actions for a rule:

Note This procedure continues from "" on .

1 In the Manage Rules dashboard, select the row containing the rule whose actions you want to suspend.

2 Click the **Suspend Actions** button at the bottom.

The **Temporarily Suspend Rule Actions** dialog box appears.

3 Specify the time period for which you want to suspend actions.

In the **Temporarily Suspend Rule Actions** dialog box, click **For** and select the time period as required, then click **Go**.

A message appears, indicating the actions will be suspended for the selected amount of time. Click **Save**.

The **Temporarily Suspend Rule Actions** dialog box closes and the Manage Rules dashboard refreshes, showing a warning icon in the row containing the rule with newly-suspended actions.

> **Note** The warning icon indicates different types of states a rule may be in. For example, it appears when a rule is disabled, or when its alarms or actions are suspended. Placing the mouse pointer over the icon shows more details about the rule state.

4 Place the mouse pointer over the warning icon.

A tool tip appears, indicating that actions are currently suspended for the rule.

To resume actions for a rule:

> **Note** This procedure continues from "Accessing the Manage Rules dashboard" on page 225.

1 In the Manage Rules dashboard, select the row containing the rule whose actions you want to resume.

2 Click the **Resume Actions** button at the bottom.
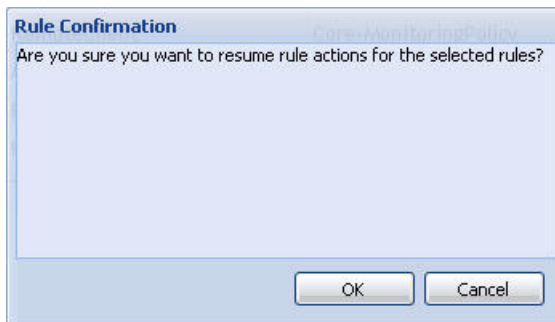
The **Rule Confirmation** dialog box appears.

3 Click **OK.**

The **Rule Confirmation** dialog box closes and the Manage Rules dashboard refreshes.

4 In the Manage Rules dashboard, observe the row containing the rule whose actions you resumed.

The absence of the warning icon indicates that the actions for the rule are no longer suspended. If a warning icon appears in the row containing the rule with newly-resumed actions, place the mouse pointer over the icon. The tool tip that appears no longer indicates that the rule's actions are suspended.

> **Note** The warning icon indicates different types of states a rule may be in. For example, it appears when a rule is disabled, or when its alarms or actions are suspended. Placing the mouse pointer over the icon shows more details about the rule state.

Viewing rule schedules

A rule can be associated with one or more schedules during which it is active (effective schedules) or inactive (blackout schedules). Use the Schedule button on the Manage Rules dashboard to view the schedules that are assigned to a rule or edit schedule assignments as required.

To view a rule's schedules:

> **Note** This procedure continues from ".

1 In the Manage Rules dashboard, click the Schedules icon (🗓) in the row containing the rule whose schedules you want to view.

The Edit Rule area appears in the Manage Rules dashboard with the **Schedules** tab open.
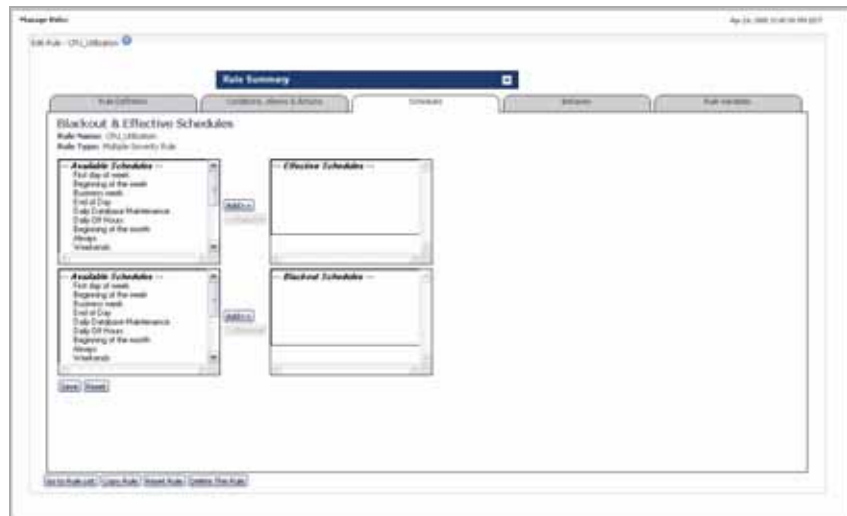
2   If required, edit the rule schedules.

For more information, see "Associating Rules with Schedules" on page 299.

Viewing a rule summary

The Edit Rule view includes a summary pane that allows you to quickly review a rule's settings and drill down to the appropriate tab if required. The Rule Summary pane includes the following information:

- The rule name
- The name of the cartridge the rule belongs to, if applicable
- The rule type
- The type of the rule trigger
- The rule scope, if applicable
- Whether or not the rule alarms are active
- Whether or not the rule actions are active
- Whether or not the rule is active
- The rule's alarm and action behavior
- The rule's alarm description

- Conditional expressions, alarm messages, and actions for each severity level
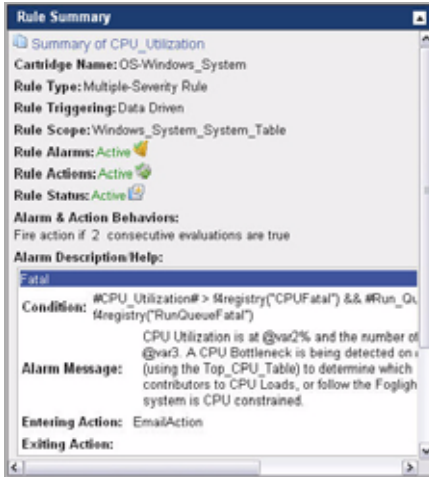
To view a rule summary:

Note   This procedure continues from ".

---

1 In the Manage Rules dashboard, click the **Rule Name** column of the row containing the rule that you want to enable or disable

The **Edit Rule** view appears in the display area.
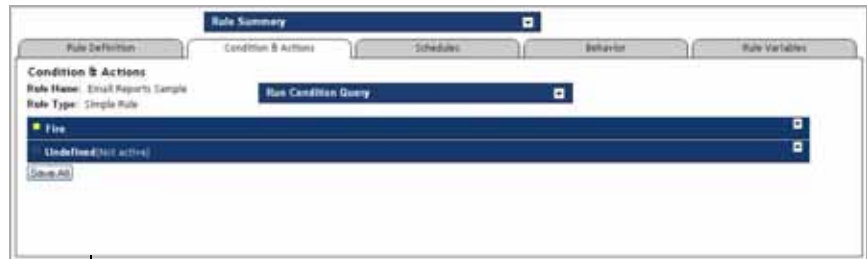
Simple rule

Multiple-severity rule

Note   The appearance of the Edit Rule view depends on the severity levels of the newly-copied rule as indicated in the above illustration. For more information about rule severity levels, see "Defining rule types" on page 250.

2 Open the **Rule Summary** pane by clicking the Roll Down button (▣) on the **Rule Summary** bar.

The **Rule Summary** pane expands in the display area.

> **Note**   The appearance of the **Rule Summary** pane depends on the rule type, its severity
> levels, and other settings. In the above illustration, the rule whose settings appear in
> the Rule Summary pane is active.

3 Observe the rule summary.

The **Rule Summary** pane includes links to other areas in the **Edit Rule** view and
Manage Rules dashboard that allow you to quickly edit the rule settings if
required.

4 Move the mouse pointer over the **Rule Summary** pane.

Hovering over a control that allows drill-down actions shows a tooltip that
describes the nature of the drill-down action.

For example, move the mouse pointer over **Rule Triggering** in the **Rule
Summary** pane.

A tooltip appears.

5 **Optional**. Edit the rule settings.

For example, to edit the rule's alarm and action behavior, in the **Rule Summary**
pane, click Alarm & Action Behaviors.

The **Behavior** tab opens in the **Edit Rule** view.

Viewing and editing rule definitions

To view or edit rule definitions:

Note   This procedure continues from "Accessing the Manage Rules dashboard" on page 225.

---

1 In the Manage Rules dashboard, click the **Rule Name** column of the row containing the rule whose definitions you want to view.

   The **Edit Rule** view appears in the display area.
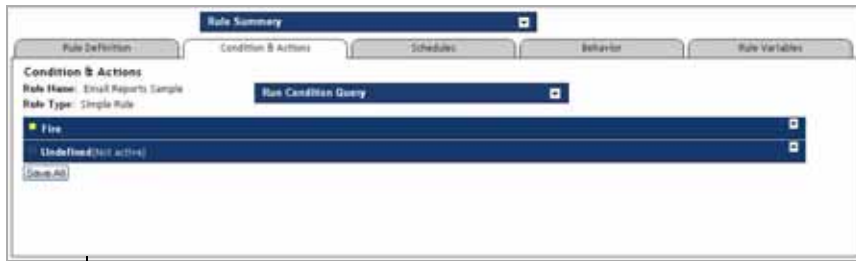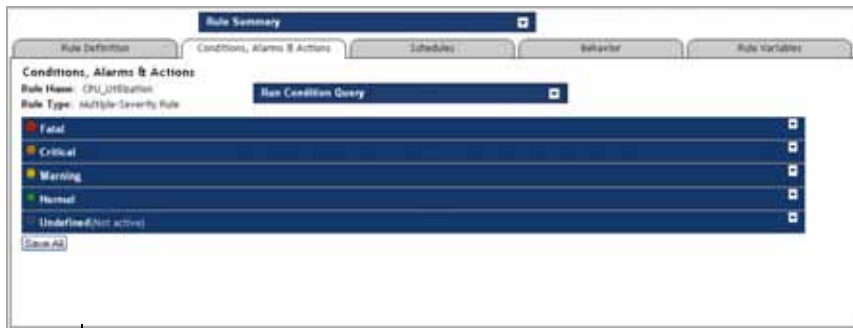
Simple rule

Multiple-severity rule

Note The appearance of the Edit Rule area depends on the severity levels of the newly-copied rule as indicated in the above illustration. For more information about rule severity levels, see "Defining rule types" on page 250.

2 Observe the rule definitions.

3 Edit the rule definitions as required.

For complete instructions, see "Defining Rules" on page 248.

Creating Rules

Creating rules allows you to customize how vFoglight notifies you of the status of your monitored system and to specify what actions should be performed when the status changes.

vFoglight allows you to create rules using the Create Rule dashboard. You can access this dashboard from the navigation panel, or through the Manage Rules dashboard.

To create a rule:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

2   Open the Create Rule dashboard by completing one of the following steps:

   • On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Manage Rules**.

     In the Manage Registry Variables dashboard that appears in the display area, click the **Add Rule** button in the lower-left corner.

   or

   • On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Create Rule**.

   The rule definitions appears in the display area with the **Rule Definition** tab open.
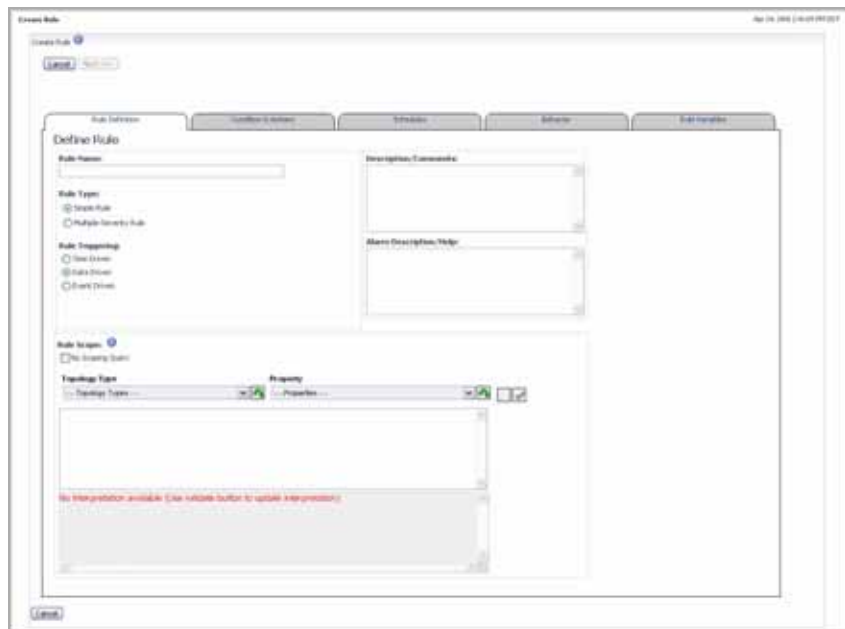
From here, you can proceed to "Defining Rules" on page 248.

Defining Rules

Rule definitions can consist of any if the following components:

- *Registry Variables*. A registry variable can be used in rule conditions, expressions, and actions. Registry variables are stored in the vFoglight registry. A registry variable can have a global value that is available to all topology types and objects. It can also have multiple additional values associated with specific topology types or objects. In addition, these values can be configured to change at certain times.

- *Metrics*. A metric is a specified value that is measured over time. In vFoglight, each metric is associated with a topology type or with a specific topology object. There are two types of metrics in vFoglight:

  - *Raw Metrics*. Raw metrics are collected by the agents directly from your monitored environment and sent to the vFoglight Management Server.

  - *Derived Metrics*. Derived metrics are calculated from one or more (raw or derived) metrics. They are scoped to a topology type and can optionally be scoped to specific objects of that type. Many derived metrics will automatically be included with vFoglight and its cartridges, and additional derived metrics can be created from the vFoglight Administration Module.

    Note Derived metrics are listed on the Manage Derived Metrics dashboard in the Administration module (Data > Manage Derived Metrics). However, no distinction is made between raw metrics and derived metrics in other locations in vFoglight or in the vFoglight Administration Module.

- *Topology Object Properties*. Topology object properties describe a topology object. These properties are collected by vFoglight from your monitored environment, generally from the configuration data for the object.

Both simple rules and multiple-severity rules include a scope, conditions, expressions, messages, and actions. Once you create a rule, you can assign values to it, associate values with specific topology types or objects, or configure performance calendars for each value.

For an example of how to define a simple rule, see "Example: Creating a Simple Rule" on page 313.

For instructions, see the following sections:

- "Getting started with rule definitions" on page 249

Getting started with rule definitions

Once you create a rule, you can add comments to it and edit its settings as required.

To get started with rule definitions:

Note   This procedure continues from "Copying rules" on page 231, "Viewing and editing rule definitions" on page 245, or "Creating Rules" on page 246.

---

1   Provide a descriptive name for the rule.

In the **Rule Definition** tab, in the **Rule Name** box, type the rule name.

Important. The following rule names are reserved and should not be used:

- • `foglight_rule_name`
- • `foglight_rule_comments`
- • `foglight_rule_domain_query`
- • `foglight_rule_id`
- • `foglight_monitored_host_name`
- • `foglight_monitoring_agent_name`
- • `foglight_rule_alarm_link`
- • `foglight_scoping_id`

Note   The `foglight_monitored_host_name` and `foglight_monitoring_agent_name` variables are only available for rules with scoping queries.

2   **Optional**. Describe the rule.

In the **Description/Comments** box, type the rule description.

3   **Optional**. Add information about the nature of the alert message.

In the **Alarm/Description** box, type the information about the alert that is generated by the rule.

From here, you can proceed to "Defining rule types" on page 250.

Defining rule types

There are two types of rules in vFoglight. Each rule type of is associated with a topology type and can be scoped to one or more specific topology objects. Those types are:

- *Simple rules*. A simple rule has a single condition, and can be in one of three states:

  - *Fire*
  - *Undefined*
  - *Normal*

  If its condition is met, the state of the rule is set to Fire and any actions that are associated with this state are performed. If the condition is not met, the rule remains in the Normal state. If the rule's condition cannot be evaluated because data is missing or unavailable, the state of the rule is set to Undefined and any actions that are associated with this state are performed.

  The condition for a simple rule is regularly evaluated against monitoring data. Therefore, the state of the rule can change if the data changes. For example, if a set of monitoring data matches a simple rule's condition, the rule enters the Fire state. If the next set does not match the condition, the rule exits the Fire state and enters the Normal state. You can configure a simple rule to perform one or more actions upon entering and/or exiting each state.

- *Multiple-Severity rules*. A multiple-severity rule is a more complex type of rule that can have up to five severity levels:

  - *Undefined*
  - *Fatal*
  - *Critical*
  - *Warning*
  - *Normal*

  When you create a multiple-severity rule, you must specify a condition for at least one severity level (Fatal, Critical, or Warning).

  As with simple rules, the conditions for a multiple-severity rule are regularly evaluated against monitoring data. All conditions in a rule are evaluated; the severity state is set to the highest level for which the condition evaluates to true. If none of the conditions are met, the severity state is set to Normal. If a condition cannot be evaluated because data is missing or unavailable, the state is set to Undefined.

An alarm is generated each time a multiple-severity rule enters a new state. In addition, you can configure a multiple-severity rule to perform one or more actions upon entering and/or exiting each state.

To define the rule type:

Note   This procedure continues from "Getting started with rule definitions" on page 249.

• Select the rule type.

  In the **Rule Definition** tab, select one of the following **Rule Type** options:

  • **Simple Rule**
  • **Multiple-Severity Rule**

From here, you can proceed to "Triggering rules" on page 251.

Triggering rules

The type of the trigger that you select determines when the rule's conditions are evaluated against the data that is collected from your monitored environment. You configure a rule to have one of the following triggers:

• *Data-Driven Trigger.* If a rule has a data-driven trigger, one or more if its conditions will be evaluated every time that new data associated with one or more topology types or objects to which the rule applies is sent to the vFoglight Management Server. This option is selected as the default trigger.

• *Time-Driven Trigger.* A time-driven trigger causes one or more of rule's conditions to be evaluated once per pre-defined interval. By default time-driven rules are only evaluated if data for the evaluation of the condition is available.

  For details on how to write conditions for data-driven and event-driven rules, see "Defining conditions for data-driven and time-driven rules" on page 263.

• *Event- Driven Trigger.* An event-driven trigger causes one or more of rule's conditions to be evaluated every time a pre-defined event occurs. There are two types of events that can act as rule triggers:

  • *AlarmSystemEvent.* Multiple-severity rules generate system events when a rule severity level is reached. Alarm-based system events allow you to monitor alarm-related system events.

  • *ReportGeneratedEvent.* Report generation creates events. You can monitor those events as required and use them to trigger report-related events.

For details on how to write conditions for event-driven rules, see "Defining conditions for event-driven rules" on page 267.

To assign a time-driven trigger:

Note This procedure continues from "Defining rule types" on page 250.

---

1 In the **Rule Definition** tab, under **Rule Triggering**, select the **Time Driven** option.

The **Rule Definition** tab refreshes, showing a set of **Recurrence Interval** boxes on the right.

2 Specify the recurrence interval for the trigger in the *hh:mm:ss* format.

3 To make time driven rules evaluate on each time interval, regardless of the existence of data, select the **Trigger Without Data** check box.

> **Note** For details on how to write conditions for time-driven rules, see "Defining conditions for data-driven and time-driven rules" on page 263.

To assign a data -driven trigger:

Note This procedure continues from "Defining rule types" on page 250.

• In the **Rule Definition** tab, under **Rule Triggering**, ensure that the **Data Driven** option is selected.

> **Note** For details on how to write conditions for data-driven rules, see "Defining conditions for data-driven and time-driven rules" on page 263.

To assign an event-driven trigger:

Note This procedure continues from "Defining rule types" on page 250.

---

1 In the **Rule Definition** tab, under **Rule Triggering**, select the **Event Driven** option.

The **Rule Definition** tab refreshes, showing the **Event Name** box on the right.

```
Rule Triggering:
○ Time Driven
○ Data Driven    Event Name   [AlarmSystemEvent        ▼]
● Event Driven
```

2 Specify the event that you want to use as the rule trigger.

Click **Event Name** and select one of the following events:

- **AlarmSystemEvent**
- **ReportGeneratedEvent**

Note   For details on how to write conditions for event-driven rules, see "Defining conditions for event-driven rules" on page 267.

From here, you can proceed to "Defining the rule scope" on page 253.

Defining the rule scope

The scope of a rule defines the set of topology objects against which it runs. A rule must be scoped to a topology type and can optionally be scoped to specific topology objects of that type. If a rule is not scoped to specific objects, it applies to all instances of that type. The scope object is the object on which alarms will appear in the vFoglight interface. The rule scope is specified using the query language.

A rule can apply to a topology type or to one or more objects of that type. You can change the scope of a rule (the topology type or specific topology object(s) to which it applies) after its creation.

For detail information on how to scope a rule or derived metric to one or more topology objects, see "Using the Query Language" on page 473.

Caution   You may need to reconfigure the rule's condition(s) if you change its scope: the metrics, registry variables, and topology object properties specified in the existing condition(s) may not be available for the new topology type or object(s).

To get started with specifying a rule scope:

Note   This procedure continues from "Triggering rules" on page 251.

- In the **Rule Definition** tab, use the Rule Scope area to scope the rule to one or more topology objects.

    For detail instructions, see "Setting the Scope for a Rule or Derived Metric" on page 474.

From here, you can proceed to "Defining Conditions, Alarms, and Actions" on page 254.

Defining Conditions, Alarms, and Actions

Simple rules have a single condition only, and can be in one of three states: *Fire, Undefined*, or *Normal*. If the condition is met, the state of the rule is set to Fire and any actions that are associated with this state are performed. If the condition is not met, the rule remains in the Normal state. If the rule's condition cannot be evaluated because data is missing or unavailable, the state of the rule is set to Undefined. The condition for a simple rule is regularly evaluated against monitoring data. Therefore, the state of the rule can change if the data changes.

Multiple-severity rules can have up to five severity levels: *Undefined*, *Fatal*, *Critical*, *Warning*, or *Normal*. When you create a multiple-severity rule, you must specify a condition for one or more of the following severity levels Fatal, Critical, or Warning. When you edit multiple-severity rules, you write a condition for each specified severity level.

Unlike simple rules, that can have only one condition associated with their Fire state, multiple-severity rules can have a conditional expression associated with each severity (Warning, Critical, and/or Fatal) along with an alarm message associated with that conditional expression. This is because simple rules do not generate alarms. They fire when the condition for their Fire state is met. On the other hand, multiple-severity rules generate alarms each time they enter a severity state.

As with simple rules, the conditions for a multiple-severity rule are regularly evaluated against monitoring data. All conditions in a rule are evaluated; the severity state is set to the highest level for which the condition evaluates to True. If none of the conditions are met, the severity state is set to Normal. If a condition cannot be evaluated because data is missing or unavailable, the state is set to Undefined.

For complete information about simple and multiple-severity rules, see "Defining rule types" on page 250.
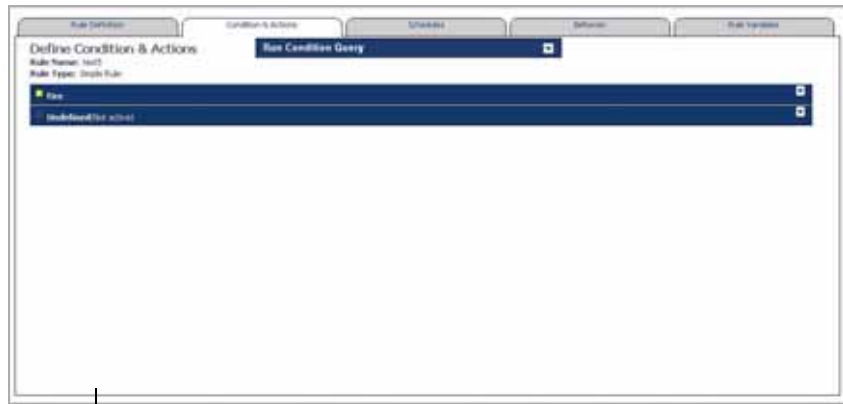
Simple rule

Multiple-severity rule

If you plan to make use of this feature, you need to add those variables before writing conditional expressions.

For instructions, see the following sections:

- "Adding severity-level variables" on page 256
- "Writing conditions" on page 261
- "Copying conditions in multiple-severity rules" on page 276
- "Defining actions" on page 278

Adding severity-level variables

Each severity-level can have its own set of variables that you can use in alarm messages. Unlike registry variable that are global in nature, severity-level variables are only accessible to the severity level in which you define them. There are two types of severity-level variables:

- *Expressions*. An expression is used to retrieve data. It can contain a registry variable or a function.

- *Messages*. A message is typically a text string that can include other severity-level variables, displaying dynamically-supplied data about your monitored system.

For example:

Severity-Level Variables		
Name	Value	Type
var1	scope.get(**"agent/host/name"**)	Expression
var2	#CPU_Utilization#	Expression
var3	#Run_Queue_Length#	Expression
Text	@var1: CPU Utilization	Message
Subject	CPU Utilization is at @var2% and the number of process in the run queue is @var3. A CPU Bottleneck is being detected on @var1. Check the top processes (using the Top_CPU_Table) to determine which processes are the greatest contributors to CPU Loads, or follow the vFoglight online help to find out if the system is CPU constrained. Please use the following URL to obtain alarm details. @foglight_rule_alarm_link	Message

In the above example, the `Text` and `Subject` variables make use of the expression-type variables, `var1`, `var2`, and `var3`. Furthermore, the `Text` and `Subject` variables can be used in an alarm message in an email action that sends that information to a specified recipient when the rule generates an alarm.

If you are defining a simple severity rule, you can add one set of severity-level variables. Multiple-severity rules allow you to add one set of variables to each severity level that you want to define.

Additionally, you can create rule-level variables and reference them in expressions defined in different severity levels within the same rule. For more information, see "Defining Rule-Level Variables" on page 303. For details on vFoglight registry variables, see "Working with vFoglight Registry Variables" on page 184.

To add a severity-level variable:

Note   This procedure continues from "Defining the rule scope" on page 253.

---

1 Open the **Conditions, Alarms, and Actions** tab (multiple-severity rules) or **Conditions and Actions** tab (simple rules).

   If you are defining a simple rule, the **Conditions & Actions** tab opens.

   If you are defining a multiple-severity rule, the **Conditions, Alarms & Actions** tab opens.

Note For more information about rule severity levels, see "Adding severity-level variables" on page 256.

2 Choose the alarm level for which you want to define the severity-level variables.

If you are defining a simple rule, click **Fire**.

If you are defining a multiple-severity rule, click one of the following bars:

- **Fatal**
- **Critical**
- **Warning**

A pane containing the severity-level condition definitions expands under the severity bar with the **Condition** tab open.
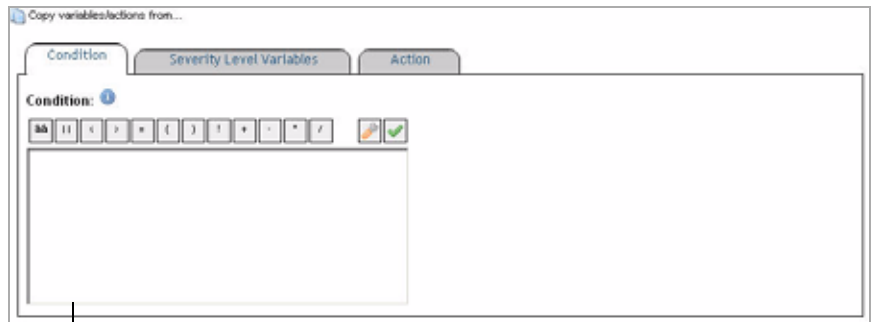
Simple rule
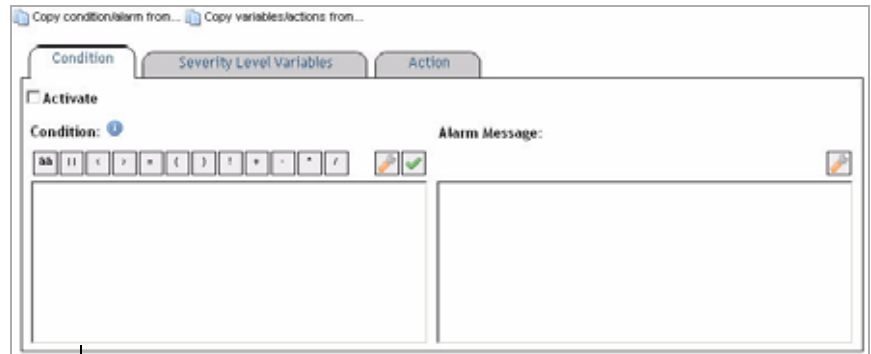
Multiple-severity rule

3 Open the **Severity Level Variables** tab.

The **Severity Level Variables** tab appears in the severity-level definition pane.
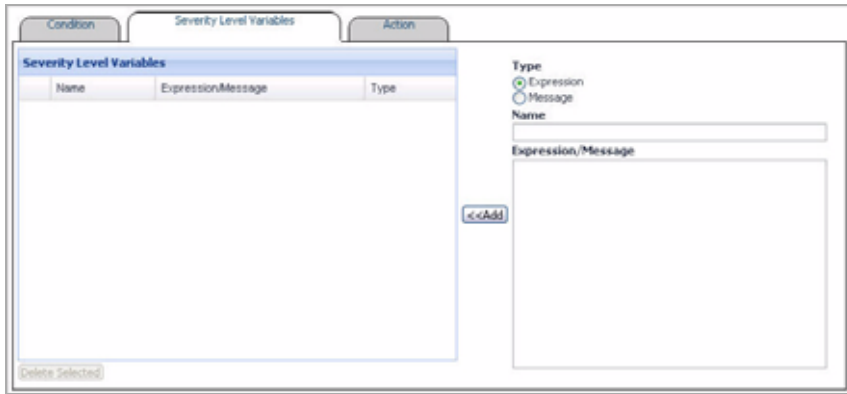
4 Define the type of the severity variable by selecting one of the following **Type** options on the right:

- **Expression**
- **Message**

5 Name the severity-level variable.

In the **Name** box, type the name of the variable.

Important. The following names are reserved and should not be used:

- `foglight_severity_level`
- `foglight_severity_level_name`

6 Specify the variable value.

Expressions can contain registry variable or functions while messages are text strings that can make use of the existing severity-level variables.

For example:
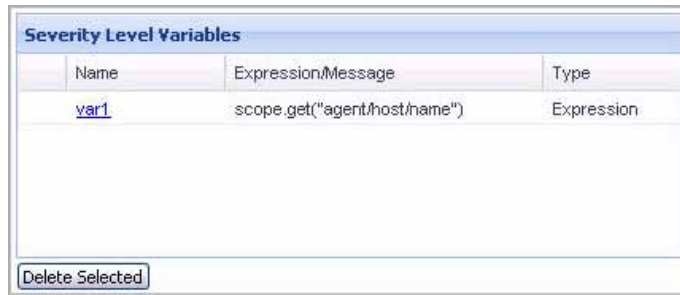
Severity-Level Variables		
Name	Value	Type
var1	scope.get(**"**agent/host/name**"**)	Expression
Text	@var1: CPU Utilization	Message

In the **Expression/Message** box, type the value of the variable.

7 Click **Add**.

The **Severity Level Variables** pane refreshes, showing the newly-added variable.

Severity Level Variables		
Name	Expression/Message	Type
var1	scope.get("agent/host/name")	Expression

Delete Selected

To delete a severity-level variable from the list, select the row containing that variable in the **Severity Level Variables** pane, and click **Delete Selected**.

From here, you can proceed to "Writing conditions" on page 261.

Writing conditions

A condition is the part of a rule that is evaluated against monitoring data. When it evaluates to True, the rule is said to fire, causing any actions that are associated with the rule or severity level to be performed.

When you create a simple rule, you specify a single condition for it. You can edit this condition after you create the rule. When you create a multiple-severity rule, you must specify a condition for one or more of its severity levels, *Fatal*, *Critical*, and *Warning*, along with an alarm message that is associated with each condition.

- *Conditional Expression*. A conditional expression can be either true or false. They can reference registry variables, Groovy functions, and metrics associated with the one or more topology types or their topology objects to which the rule applies.

  Additionally, conditional expressions can reference properties of topology objects that are related (within the hierarchy of the topology model) to one or more topology objects to which the rule is scoped. For example, the condition for a simple rule that is associated with a specific JVM can reference properties of the server on which the JVM is running (such as the server name), or properties of the cluster to which the server belongs.

Furthermore, event-driven rules can retrieve data generated by report- and alarm-related events.

Expressions can be simple—for example, an expression can consist only of a metric name—but they can also be defined using very complex syntax. See "Examples" on page 481 for examples of expressions.

Conditional expressions make use of the query language. See "Using the Query Language in Rule Conditions or Derived Metric Expressions" on page 480 for detailed information about the query language in vFoglight.

- *Alarm Message*. vFoglight generates an alarm message when the conditional expression associated with a multiple-severity rule evaluates to True. An alarm message is typically a text string that can include other severity-level variables, displaying dynamically-supplied data about your monitored system.

  Important Simple rules do not generate alarms. They fire when the condition for their Fire state is met. On the other hand, multiple-severity rules generate alarms each time they enter a severity state.

For information on how to write conditions, see the following sections:

- "Expression scope" on page 262
- "Copying conditions in multiple-severity rules" on page 276
- "Defining conditions for data-driven and time-driven rules" on page 263
- "Defining conditions for event-driven rules" on page 267

Expression scope

Expressions and messages can be set with one of two distinct scopes:

- *Rule-scoped expressions and messages*. They can be referenced by the actions set for the *Fire* and *Undefined* states of a simple rule and for all severity levels (*Fatal*, *Critical*, *Warning*, *Normal*, and *Undefined*) in a multiple-severity rule.

  Note It is a best practice that rule-scoped expressions are used until there is a need for more finely scoped expressions.

- *Severity-scoped expressions and messages*. They can only be referenced by the actions set for the specific rule level at which the message is defined. For example, if an expression is defined for the *Fatal* level of a multiple-severity rule, it can only be referenced by the actions that are set for that severity level.

Note In addition to rule-level expressions and severity-level expressions, vFoglight also includes pre-defined system expressions. For example, there is a pre-defined expression that refers

to each severity level. System expressions are listed in the vFoglight Administration Module.

Defining conditions for data-driven and time-driven rules

When you write conditions for data-driven or time-driven rules, you can make use of variables, topology object metrics, and Groovy functions.

To define a condition for a data-driven or time-driven rule:

Note   This procedure continues from "

1   In the **Conditions and Actions** tab (simple rules) or **Conditions, Alarms & Actions** tab (multiple-severity rules), open the **Conditions** tab.

The **Condition** tab opens in the display area.

Simple rule

Multiple-severity rule

Important The appearance of the Condition tab depends on the rule type. In addition to the condition editor, multiple-severity rules also include an alarm editor that allows you to compose an alarm message associated with each severity state (Warning, Critical, and/or Fatal).

Unlike simple rules, that can have only one condition associated with their Fire state, multiple-severity rules can have a conditional expression associated with each severity (Warning, Critical, and/or Fatal) along with an alarm message associated with that conditional expression.

This is because simple rules do not generate alarms. They fire when the condition for their Fire state is met. On the other hand, multiple-severity rules generate alarms each time they enter a severity state.

For complete information about the differences between simple rules and multiple-severity rules, see "Defining rule types" on page 250.

2 Write the conditional expression.

In the **Condition** tab, use the **Condition** area to write the conditional expression.

You can type the condition directly into the **Condition** box, or use the operator controls and the Condition Editor to add logical operators, registry variables, metrics, or Groovy functions. For complete information about inserting operators or using the Condition editor, see "Specifying a Rule Condition or Derived Metric Expression" on page 481.

Caution   If you change the metrics, registry variables, or topology object properties that are referenced in the condition, ensure that the new items are available for the topology type or object(s) to which the rule is scoped.

Important   To separate multiple lines in conditional expressions, use a semicolon followed by a carriage return. In conditional expressions consisting of a single line, using a semicolon to end the line is optional. For example:

Multi-line expressions

Example A

Correct

```
println @event.dump();
@event.get("report/name") == "MyReport";
```

Incorrect

```
println @event.dump()
@event.get("report/name") == "MyReport";
```

Note   The first line is missing a semicolon which causes the expression to result in an error.

Single-line expressions

Example B

Correct

```
println @event.dump();
```

Example C

Correct

```
println @event.dump()
```

> **Note** Using a semicolon to end the line in a single-line expression is optional, therefore both expressions are valid.

3 Multiple-severity rules. Activate the condition by selecting the **Activate** check box.

You must activate the condition for a severity level in a multiple-severity rule before you can save it. If the **Activate** check box is cleared when you click **Save**, the condition that you specified will be discarded, as will any expressions or actions that you set in the sub-tabs of the tab for that severity level.

> **Caution** Do not clear the **Activate** check box if you want to temporarily disable a rule. To temporarily deactivate the alarms and actions for an entire rule, follow the instructions in "Suspending or resuming alarms" on page 236. You can also configure the behavior of the alarms and actions for the rule. See "Defining Alarm and Action Behavior" on page 302 for more information.

4 Multiple-severity rules. Define the alarm message associated with the newly-defined condition.

In the **Alarm** box, type the alarm message.

5 Multiple-severity rules (Optional). To reference a rule-level variable or a system variable in the alarm message, in the **Alarm Message** box, click the location to which you want to add the variable, and then click the Alarm Message Editor button (🖉) above the **Alarm Message** box.

The **Alarm Message Editor** dialog box appears.

Alarm Message Editor

Name	Expression/Message	Type
AgentId	scope.get(\"agentID\")	E
AgentName	scope.get(\"name\")	E
HealthStateName	scope.get(\"healthState\").get(\"n...	E

Insert   Close

- To add a rule-level variable, in the **Alarm Message Editor** dialog box, on the **Rule Variables** tab, select the rule-level variable and click **Insert**.
- To add a system variable, on the **System Variables** tab, select the system variable and click **Insert**.

The newly-added variable appears in the **Alarm Message** box.

When you finish adding variables to the alarm message, close the **Alarm Message** box by clicking **Close**.

6 Save the newly-defined rule condition by clicking the **Save** button above the **Condition** tab.

From here, you can proceed to "Defining actions" on page 278.

Defining conditions for event-driven rules

When you write conditions for event-driven rules, in addition to variables, topology object metrics, and Groovy functions, you can use events and their properties to trigger rule actions.

Event-driven rules allow you to monitor the events generated every time a pre-defined event occurs. There are two types of events that can act as rule triggers:

- *AlarmSystemEvent*

  Multiple-severity rules generate system events when a rule severity level is reached. Alarm-based system events allow you to monitor alarm-related system

events and use the following properties in rule conditions in order to trigger event-driven rules:

Property	Data Type	Description
alarmID	String	Contains the ID of the alarm that generates the event.
alarmLink	String	Contains the URL to the alarm.
clearedTime	Date	Specifies the time at which the alarm is cleared.
change	AlarmChangeType	Specifies the alarm change type: Fire, Clear, or Acknowledge.
createdTime	Date	Specifies the time at which the alarm is created.
isAcknowledged	Boolean	Determines if the event is acknowledged. It can be set to True or False.
isCleared	Boolean	Determines if the event is cleared. It can be set to True or False.
message	String	Contains the alarm message.
ruleComments	String	Contains any comments associated with the rule that generates the alarm.
ruleID	String	Contains the ID of the rule that generates the alarm.
ruleName	String	Contains the name of the rule that generates the alarm.

Property	Data Type	Description
severityLevel	Integer	Contains a number that identifies the severity level: • 0: Undefined • 1: Normal • 2: Warning • 3: Critical • 4: Fatal
severityName	String	Contains one of the following values that identify the severity level: Undefined, Normal, Warning, Critical, or Fatal.
sourceID	String	Contains the ID of the source data object that generates the event.
sourceName	String	Contains the name of the source data object that generates the event.
userDefinedData	DataObject	Contains a data object that includes any additional information about the alarm. This data can be used when creating event-related dashboards. For more information about creating dashboards, see the *vFoglight User Guide*.

- *ReportGeneratedEvent*

    Report generation creates system events. You can monitor these events and their properties in order to trigger event-driven rules:

Property	Data Type	Description
createdTime	Date	Specifies the time at which the event is created.
report	Report	Contains an object of the Report type. For complete information about creating and scheduling reports in vFoglight, see the *vFoglight User Guide*.

In addition to the ReportGeneratedEvent object properties you can reference the Report object properties when writing rule conditions for a rule triggered by a report generation event. The following table lists the Report object properties, their data types, and descriptions.

Property	Data Type	Description
dateRun	Date	The date on which the report is run.
emailRecipients	String	The email recipients to which the report is to be sent.
errorMessage	String	An error message associated with the report.
isEnabled	Boolean	Specifies whether the report generation is enabled.
name	String	The report name.
numResultsRetained	Integer	The number of records in that are retained in the report.
reportId	String	The report ID.
scheduleId	String	The ID of the schedule that is associated with the report.

Property	Data Type	Description
scheduleName	String	The name of the schedule that is associated with the report.
size	Integer	The report size in bytes.
templateId	String	The ID of the template used to create the report.
templateName	String	The name of the template used to create the report.
user	String	The name of the vFoglight user who created the report.

To define a condition for an event-driven rule:

Note   This procedure continues from "Adding severity-level variables" on page 256.

1 On the **Conditions and Actions** tab (simple rules) or **Conditions, Alarms & Actions** tab (multiple-severity rules), open the **Conditions** tab.

The **Condition** tab opens in the display area.

Simple rule

Multiple-severity rule

> **Important** The appearance of the Condition tab depends on the rule type. In addition to the condition editor, multiple-severity rules also include an alarm editor that allows you to compose an alarm message associated with each severity state (Warning, Critical, and/or Fatal).
>
> Unlike simple rules, that can have only one condition associated with their Fire state, multiple-severity rules can have a conditional expression associated with each severity (Warning, Critical, and/or Fatal) along with an alarm message associated with that conditional expression.
>
> This is because simple rules do not generate alarms. They fire when the condition for their Fire state is met. On the other hand, multiple-severity rules generate alarms each time they enter a severity state.
>
> For complete information about the differences between simple rules and multiple-severity rules, see "Defining rule types" on page 250.

2 Write the conditional expression.

In the **Condition** tab, use the **Condition** area to write the conditional expression. using the following syntax:

```
some_value.equals(@event.get("[report/]property");
```

Where

- **report** indicates that you want to use the ReportGeneratedEvent in the conditional expression.

- *property* is the name of the event property that you want to use in the comparison. For a complete list of event properties and the information they contain, see "AlarmSystemEvent" on page 267 or "ReportGeneratedEvent" on page 269.

- *some_value* contains the value that is to be compared with the specified property value.

  Caution The data type of the value you specify here must match the data type of the property with which you compare this value.

For example, to write a condition that triggers an event-driven rule to fire when vFoglight generates a report whose name is System Resources, write the following expression:

```
@event.get("report/name") == "System Resources";
```

Report attachments are not stored in ReportGeneratedEvent object properties. To retrieve a report attachment in a rule condition, use the following syntax:

```
byte[] a_pdf_object =
    server.get("ReportingService").getReportData(@event.get
    ("report/reportId"));
```

Where *a_pdf_object* is the name of the report file that you want to retrieve.

Important To separate multiple lines in conditional expressions, use a semicolon followed by a carriage return. In conditional expressions consisting of a single line, using a semicolon to end the line is optional. For example:

Multi-line expressions

Example A

Correct

```
println @event.dump();
@event.get("report/name") == "MyReport";
```

Incorrect

```
println @event.dump()
@event.get("report/name") == "MyReport";
```

> **Note** The first line is missing a semicolon which causes the expression
> to result in an error.

Single-line expressions

Example B

Correct

```
println @event.dump();
```

Example C

Correct

```
println @event.dump()
```

> **Note** Using a semicolon to end the line in a single-line expression is optional,
> therefore both expressions are valid.

3 Multiple-severity rules. Activate the condition by selecting the **Activate** check box.

You must activate the condition for a severity level in a multiple-severity rule before you can save it. If the **Activate** check box is cleared when you click **Save**, the condition that you specified will be discarded, as will any expressions or actions that you set in the sub-tabs of the tab for that severity level.

> **Caution** Do not clear the **Activate** check box if you want to temporarily disable a multiple-severity rule. To temporarily deactivate the alarms and actions for an entire rule, follow the instructions in "Suspending or resuming alarms" on page 236. You can also configure the behavior of the alarms and actions for the rule. See "Defining Alarm and Action Behavior" on page 302 for more information.

4 Multiple-severity rules. Define the alarm message associated with the newly-defined condition.

In the **Alarm** box, type the alarm message.

5 **Multiple-severity rules (Optional)**. To reference a rule-level variable or a system variable in the alarm message, in the **Alarm Message** box, click the location to which you want to add the variable, and then click the Alarm Message Editor button ( ) above the **Alarm Message** box.

The **Alarm Message Editor** dialog box appears.

- To add a rule-level variable, in the **Alarm Message Editor** dialog box, on the **Rule Variables** tab, select the rule-level variable and click **Insert**.

  The **Rule Variables** tab lists all of the rule-level variables, including expressions and messages.

- To add a system variable, on the **System Variables** tab, select the system variable and click **Insert**.

  The newly-added variable appears in the **Alarm Message** box.

  When you finish adding variables to the alarm message, close the **Alarm Message** box by clicking **Close**.

6 Save the newly-defined rule condition by clicking the **Save** button above the **Condition** tab.

From here, you can proceed to

Copying conditions in multiple-severity rules

In some cases you may need to copy the conditions from an existing severity level of the same rule. A condition is comprised of a conditional expression and an alarm message, both of which are copied when required. For more information about conditional expressions and alarm messages, see "Writing conditions" on page 261.

Copying a condition can be useful in situations when the conditional expressions of different severities are similar, so instead of writing and validating them for each severity level you can copy an existing expression and modify it as required.

While you are in the edit rule mode, any unsaved changes to the conditional expressions or alarm messages that you want to copy will be carried over to the destination condition. For example, if you edit a conditional expression for the Warning condition of a rule without saving it, and then proceed to copy that condition in the Critical pane, the unsaved edits of the Warning condition will be carried over to the Critical condition.

To copy a condition from an existing severity level:

Note   This procedure continues from "Adding severity-level variables" on page 256.

1   On the **Conditions, Alarms & Actions** tab, open the **Conditions** tab.

The **Condition** tab opens in the display area.

2   Choose the severity level from which you want to copy the conditional expression.

> **Caution**   You can only copy the conditions from those severity levels that are already defined. Attempting to copy a condition for a rule that has no conditions defined results in an error.

    a   Click the **Copy condition/alarm** button above the **Condition** tab.

        A list appears, showing those severity levels for which the conditions have been defined. For example, if you are defining a condition for the Critical severity, and the conditions for the Fatal and Warning levels have already been defined, the list shows two options: **Fatal** and **Warning**, as illustrated below.
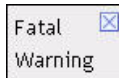
        Caution   Attempting to copy a condition for a rule that has no conditions defined results in error.

    b   Select the severity level whose condition you want to copy.

        The Condition tab refreshes, showing the newly copied conditional expression and alarm message in the Condition and Alarm Message boxes.
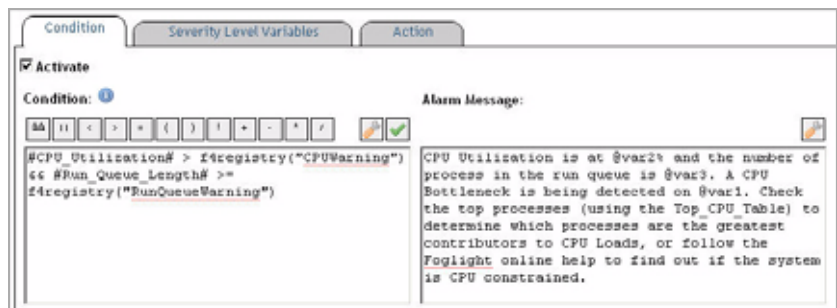
3   **Optional**. Edit the conditional expression and the alarm message, if required. For instructions, see one of the following sections:

- "Defining conditions for data-driven and time-driven rules" on page 263
- "Defining conditions for event-driven rules" on page 267

4   Save your changes to the rule condition by clicking the **Save** button above the **Condition** tab.

From here, you can proceed to "Defining actions" on page 278.

Defining actions

An action is a particular operation that is performed when a rule enters or exits a state (for example, when a rule condition is met).

Multiple actions can be associated with simple rules as well as with each severity level in a multiple-severity rule. Actions can be added to a rule after it is created.

For examples on how to add actions to a rule severity level, see "Example: Configuring Rule Action Parameters" on page 314 and "Example: Implementing Command Actions in Rules" on page 322.

vFoglight action types

There are two types of actions in vFoglight:

- *Entering*. It causes the action to be performed when a simple rule or a severity level in a multiple-severity rule enters the state in which the condition for that rule or severity level is met.

  It is a best practice that *Entering* actions be used by default.

- *Exiting*. It causes the action to be performed when a simple rule or a severity level in a multiple-severity rule exits the state in which the condition for that rule or severity level is met.

  Use of the *Exiting* action should be restricted to cases where an action specific to the state is needed. For example, if an *Entering* action starts a script, then the *Exiting* action may stop the script.

vFoglight actions

The actions available in vFoglight are as follows:

- *BSM Actions*. They send alarm data to vFoglight Service Discovery Dashboards.

- *SNMP Trap Actions*. They cause alarms to be forwarded as SNMP traps to a management system that supports SNMP (such as Tivoli® NetView®, Micromuse NetCool® or HP® Vantage Point) when the rule fires. Various parameters can be set for sending the SNMP trap, including the community, the trap type, and the host and port for the monitoring service.

- *Email Actions*. They cause email messages to be sent to a specified recipient when the rule fires. For more information about viewing the settings related to email actions and configuring email actions in vFoglight, see "Viewing email settings and configuring email actions" on page 279.

- *Command Actions.* They cause an external action to be executed on the machine hosting the vFoglight Management Server. For example, a *Command* action may run the executable that starts a service. Various parameters can be set for this action. The mandatory parameter is COMMAND_LINE which is the executable command and one or more arguments. Optionally, you can also set OS environment variables (separated by an exclamation mark).

- *Remote Command Actions*. They cause an external action to be executed on a remote platform. Various parameters can be set for this action including a mandatory parameter is COMMAND_LINE.

- *Script Actions*. They cause an arbitrary script to be run when the rule fires. This is to be used for any integration not available through built-in actions. Various parameters can be set for this action, such as script name (mandatory), scoping topology ID, scripting object ID, and arguments associated with the script. The ten arguments (0-9) must be mapped directly to the script, and it is the responsibility of the user to assure the parameters match the script in number and in type. There is currently no validation facility for script actions.

For a list of parameters that are supported in each action type, refer to "About action parameters" on page 288.

Viewing email settings and configuring email actions

The report engine uses email actions to send reports to email recipients or email alarm-related messages to vFoglight administrators when certain thresholds are reached. When you add a scheduled report and specify its email recipients using the Report Manager dashboard, vFoglight uses the default mail parameters, set by the vFoglight registry with the mail. prefix, to send the report to the specified recipients at a rate set in the associated schedule.

Alternatively, you may need to edit the default email-related settings that control mail connection and mail socket by creating two new registry variables, mail.connection.timeout and mail.socket.timeout, and assigning them the appropriate value in seconds.

For complete information about creating reports and the Report Manager dashboard, see the *vFoglight User Guide*. For information on where to find the global settings that vFoglight uses for sending emails, see "Mail (Global Settings)" on page 61.

In some situations you may need to filter the reports before sending them to email recipients. You can do that by editing the Fire condition of the rule Email Reports Sample as required. For instructions on how to write rule conditions, see "Writing conditions" on page 261.

To view email settings in vFoglight:

Note This procedure continues from "Accessing the vFoglight Configuration Dashboard" on page 67.

• In the vFoglight Configuration dashboard, locate the **Mail (Global Settings)** view.

Mail (Global Settings)	
Connection Timeout	Not Globally Configured
From	Not Globally Configured
SMTP Host	Not Globally Configured
SMTP Port	Not Globally Configured
Recipient	Not Globally Configured
Socket Timeout	Not Globally Configured
User	Not Globally Configured

The **Mail (Global Settings)** view contains email settings that are used by vFoglight when sending messages to specified recipients, such as the connection time-out, default email sender, host name, port number, recipient's email address, socket time-out, and the user logging into the email server used by vFoglight. For complete information about the settings in the **Mail (Global Settings)** view, see "Mail (Global Settings)" on page 61.

These settings need to be configured after the installation. For details, proceed to To configure email actions in vFoglight:.

To configure email actions in vFoglight:

Note This procedure continues from "Accessing the Manage Registry Variables dashboard" on page 185.

1 On the Manage Registry Variables dashboard, locate the following variables: **mail.from**, **mail.host**, **mail.password**, **mail.port**, **mail.receipient**, **mail.transport.protocol**, and **mail.user**.

Tip You can filter the list of variables using filters. At the top of the Manage Registry Variables dashboard, in the **Filter By Variable Name** box, type *mail*. The Manage Registry Variables dashboard refreshes, showing only the registry variables that start with the *mail* prefix.
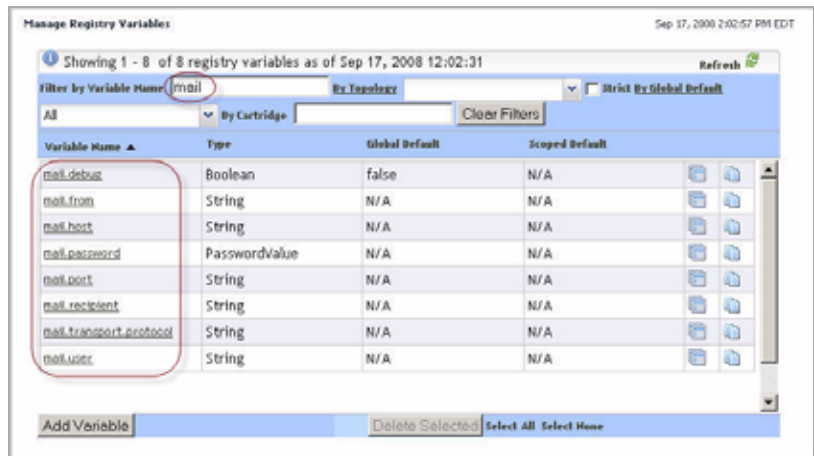
2 Set the global default values of the following `mail.` variables:

- **mail.from**: The default email address used by the vFoglight Management Server from which emails are sent.

- **mail.host**: The default email host used by the vFoglight Management Server from which emails are sent.

- **mail.password**: The default password for logging into the email server.

- **mail.port**: The default port number of the email server used by the vFoglight Management Server from which emails are sent.

- **mail.receipient**: The default email address used by the vFoglight Management Server to which emails are sent.

- **mail.transport.protocol**: The default mail transport protocol (for example, SMTP, POP3, IMAP4, or others).

- **mail.user**: The default user name that the vFoglight Management Server uses for logging into the email server.

To set the global value of a registry variable, complete the following steps:

a On the Manage Registry Variables dashboard, click the **Variable Name** column of the registry variable whose global default value you want to edit. For example, to edit the value of the `mail.host` variable, click **mail.host**.

The **Edit Registry Variable** view appears in the Manage Registry Variables dashboard, showing the settings of the `mail.host` variable.

In the **Edit Registry Variable** view, in the **Global Default** area, type the global default value that you want to assign to the variable.

For example, to configure the mail.host variable, type the name of the default email host that you want the vFoglight Management Server to use for sending emails.

b On the right of the **Global Default** area, click **Save**.

A message appears in the upper-left corner, indicating success.
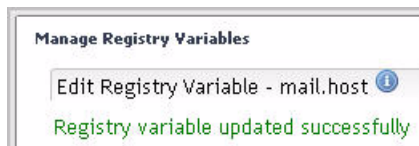
c Return to the list of registry variables in the Manage Registry Variables dashboard by clicking the **Go to Registry Variable List** button at the bottom.

The Manage Registry Variables dashboard refreshes, and the row containing the newly-edited variable appears selected in the list.

Variable Name ▲	Type	Global Default	Scoped Default		
mail.debug	Boolean	false	N/A		
mail.from	String	jnikic@sitraka.com	N/A		
mail.host	String	MyEmailHost.com	N/A		

For complete information on how to edit a registry variable, see "Editing Registry Variables" on page 200.

3   Optional. Configure the mail connection and mail socket time-outs.

The default values are 20 seconds for the connection and 10 seconds for the socket time-out. To use different values, create the following registry variable values and assign them the appropriate integer value in seconds: `mail.socket.timeout` and `mail.connection.timeout`.

To create a vFoglight registry variable, complete the following steps:

a   On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Create Registry Variable**.

The Create Registry Variable dashboard appears in the display area, showing the **Step 1: Create Registry Variable** view.

b Specify the name and data type for the variable using the following boxes:

Registry Variable Name: The name of the variable:
`mail.connection.timeout` when specifying the connection time-out or
`mail.socket.timeout` for the socket time-out.

Registry Value Type: Click the box and select **Integer** from the list that
appears.

c Click **Add**.

The Create Registry Variable dashboard refreshes, showing the **Step 2:
Registry Variable Added** view.

> **Create Registry Variable**   Sep 23, 2008 3:00:30 PM EDT
>
> | Create Registry Variable | Registry Variable Added |
>
> Step 2: Registry Variable Added ⓘ
>
> The following registry variable was successfully added to the system.
> **Registry Variable Name:**
> mail.connection.timeout
> **Description/Comments:**
>
> **Registry Value Type:**   Integer
>
> Go to Registry Variable List | Edit Registry Variable
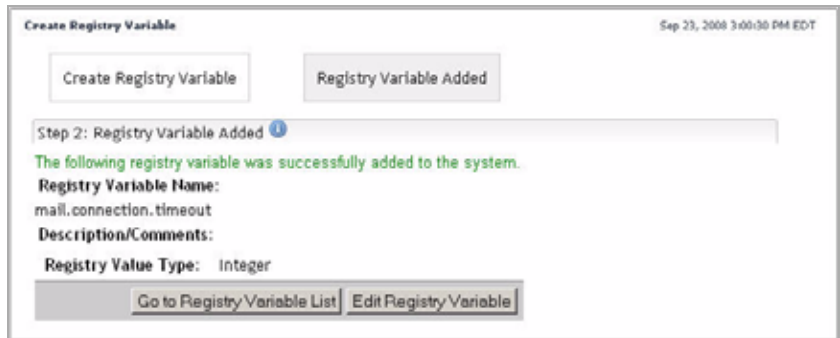
d Edit the newly-created registry variable.

In the **Step 2: Registry Variable Added** view, click **Edit Registry Variable**.

The Create Registry Variable dashboard refreshes, showing the **Edit Registry Variable** view.
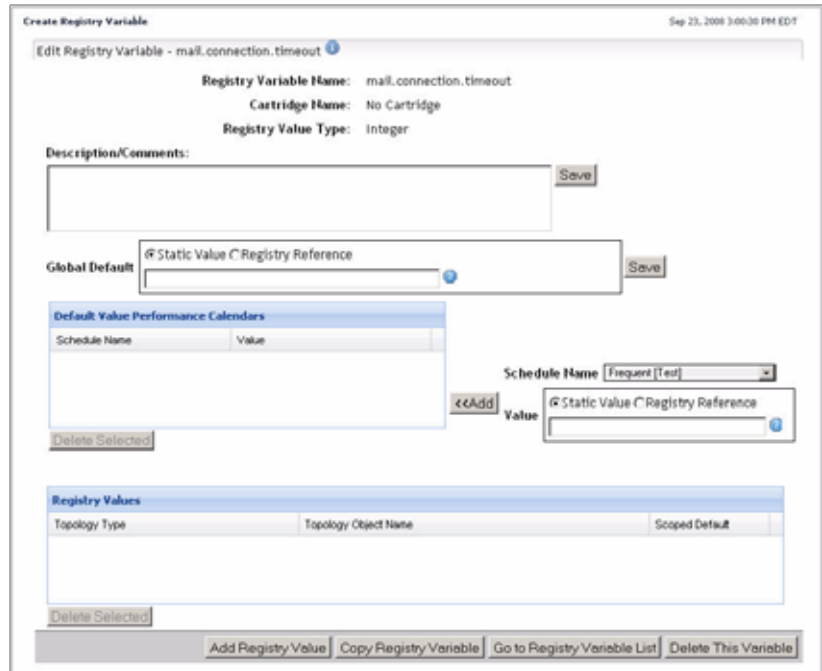
    e Specify the length of the time-out.

       In the **Edit Registry Variable** view, in the **Global Default** area, ensure that the **Static Value** option is selected and type the number of seconds in the box.

    f Save your changes.

       On the right of the **Global Default** area, click **Save**.

       A message appears in the upper-left corner, indicating success.

    g Return to the list of registry variables in the Manage Registry Variables dashboard by clicking the **Go to Registry Variable List** button at the bottom.

       The Manage Registry Variables dashboard refreshes, and the row containing the newly-edited variable appears selected in the list.

       For complete information on how to edit a registry variable, see "Editing Registry Variables" on page 200.

Important In some situations you need to create or receive email alerts that contain a URL to the browser interface. To ensure the URL points to the computer on which the vFoglight Management Server is running, ensure that the CATALYST_URL registry variable contains the correct computer name and port number.

For example: http://MyHost.MyDomain.com:8080/

Adding actions to rules

An action is a particular operation that is performed when a rule enters and/or exits a state (for example, when a rule condition is met). You can associate multiple actions can be with simple rules as well as with each severity level in a multiple-severity rule. You can add actions to a rule after it is created.

To add an action to a rule:

---

1   In the **Conditions and Actions** tab (simple rules) or **Conditions, Alarms & Actions** tab (multiple-severity rules), open the **Action** tab.

    The **Action** tab appears in the display area.
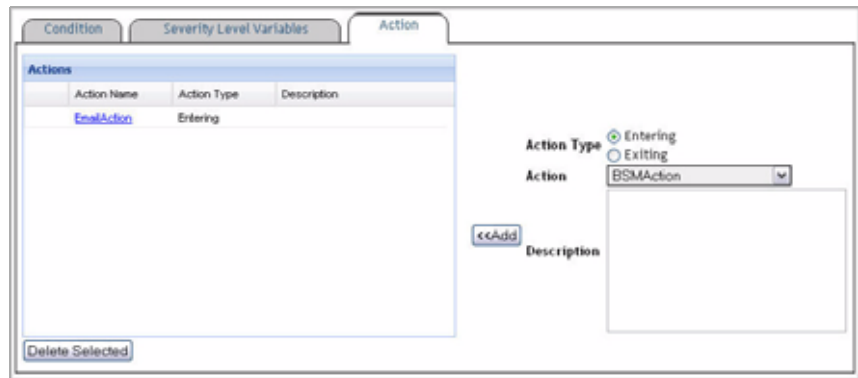
2   Define the action type by selecting one of the following **Action Type** options on the right:

   • **Entering**

   • **Exiting**

   See "vFoglight action types" on page 278 for more information.

3   Specify the action.

    Click **Action** and select an action from the list that appears.

    See "vFoglight actions" on page 278 for more information.

4   **Optional**. Add information about the selected action.

    In the **Description** box, type the action description.

5   Click **Add**.

    The Action tab shows a list of parameters associated with the newly-selected action.

From here, you can edit the action parameters as required. For details, see "About action parameters" on page 288.

About action parameters

Each rule action has a set of parameters associated with it. Some action parameters are mandatory while others are optional. When you add an action to a rule, you must configure the action's mandatory parameters in order for it to be executed when the rule reaches the severity level for which the action is defined.

When specifying an action parameter you can make use of vFoglight registry variables, rule-level variables, or specify a custom value. The data type of the specified value must match the action parameter's data type.

Note To successfully configure an action, you must ensure that all of the actions's mandatory parameters are specified.

The following table lists rule actions and their parameters.

Parameter	Required?	Description
BSM Actions		
Alarm system event	Yes	Alarm system event generated by vFoglight.
BSM URL	Yes	URL of the BSM system to which to post the data.
Event Attributes	No	Optional event attributes to pass to BSM.
Managed Control Attributes	No	Optional component attributes to pass to BSM.
Technology Level Agreement Attributes	No	Optional Technology Level Agreement attributes to pass to BSM.
Command Actions		

Parameter	Required?	Description
COMMAND_LINE	Yes	The command that you want to run on the command line along with its options and arguments if applicable. **Note** If the command is not accessible from the *<foglight_home>* directory, you need to specify its path.
ENVIRONMENT_VARIABLES	No	A list of environment variables separated by exclamation marks '!'.
Email Actions		
mail.attachement	No	Email attachment.
mail.attachement.file.name	Yes	The file name of the email attachment.
mail.attachement.mime.type	Yes	The attachment's MIME type.
mail.bcc	No	Blind CC list. Uses a comma as a separator.
mail.cc	No	Mail CC list. Uses a comma as a separator.
mail.content.type	Yes	Can be set to text/plain or text/html.
mail.message	No	Message body.
mail.recipient	Yes	Recipient's email address. It overrides the value set by the global mail.recipient registry variable. For more information about this variable, see "Viewing email settings and configuring email actions" on page 279.

Parameter	Required?	Description
mail.subject	No	Mail subject line
Remote Command Actions		
COMMAND_LINE	Yes	The command that you want to run remotely along with its options and arguments if applicable.
ENVIRONMENT_VARIABLES	No	A list of environment variables separated by exclamation marks '!'.
HostName	Yes	The name of the host computer on which the command is to be executed.
MatchAll	No	A flag indicating whether to run the command on all hosts that match the selection criteria. The false default runs the command on the first matching host only.
PlatformInfo	No	The target platform specification.
RemoteInstallationId	No	Target installation ID. This information is useful if there are multiple remote agents that support remote command execution.
RemoteWorkingDir	No	Working directory on the remote machine.

Parameter	Required?	Description
UseRegExp	No	Indicates whether the values specified by the HostName, PlatformInfo, and RemoteInstallationId parameters are regular expressions.
Script Actions		
Argument 1–10	No	Parameters to pass to the script.
Scoping object id	No	The ID of the scoping object.
Script name	Yes	The name of the script.
		Caution The rule runs the script from the *<foglight_home>/scripts* directory. If you place your script elsewhere in the file system, include the script path.
SNMP Trap Actions		
CommunityString	Yes	SNMP community string.
TargetAddress	Yes	Trap target address.
TargetPort	Yes	Trap target port.

The following rules apply to the command syntax for Command and Remote Command actions:

- The executable command must point to a path which can be understood and executed by the native operating system (such as a a Windows batch file or a binary executable file). For example:

Correct

```
C:\hello.bat
perl C:\hello.pl
\\my_domain\my_server\my_group\my_user_account\hello.bat
```

Incorrect

```
P:\hello.bat (where P: is a mapped drive)
```

Only those commands that point to a specific batch file on a physical drive produce a command output in the Command Prompt window. That is because command actions invoked by a script do not read back from the stream nor print the command output to the console, waiting for the command to finish. In the above examples, only `C:\hello.bat` generates a command-line output.

- The executable command should be separated from the arguments by one or more space characters, and the arguments should similarly be separated by one or more space characters.

- If the executable or an argument contains one or more space characters, it should be quoted with double quotation marks ("). Command actions do not recognize single quotation marks. Do not use a back slash (\) as an escape character for single or double quotation marks as it has no effects in command actions. For example:

Correct

```
arg1 arg2 arg3
"arg one" arg2
```

Incorrect

```
'arg three here'
"arg \"one"
```

- If the command or an argument is quoted and has to contain one or more double quotes, the embedded double quotation mark must be escaped by using two adjacent quotes ("") or using a back slash and quote (\"), whichever is suitable to the underlying OS.

- Triple quotes (""") are recognized as one quotation mark. This is useful in dealing with Windows batch files.

- Triple quotes are not allowed in a quoting context.

About rule system variables

There are trigger-specific rule variables that can be used in conditional expressions of rules with certain trigger types. Each variable contains the information relative to the rule in which it is used. For example, if you create a rule *RuleA* and use the rule-level variable `foglight_rule_name` as a parameter in an action that you add to *RuleA*, that parameter uses the actual rule name, *RuleA* .

Rules in vFoglight can be triggered by data, time, or events. Different trigger types, such as time, data, and event triggers, have different rule-level variables available to them. For example, in an event-driven rule you can reference the properties of the system alarm event that triggers the rule directly.

The following table lists all of the rule-level variables and indicates their availability in different trigger types.

Variable	Description	Trigger Type		
		Time	**Data**	**Event**
event	System event	Yes	No	No
event_foglight_rule_alarm_link	Link for the alarm causing the event	Yes	No	No
event_foglight_rule_comments	The comments for the rule causing the event	Yes	No	No
event_foglight_rule_id	The ID of the rule causing the event	Yes	No	No
event_foglight_rule_name	The name of the rule causing the event	Yes	No	No
event_foglight_severity_level	The severity level (0-4) causing the event	Yes	No	No
event_foglight_severity_level_name	Name of the severity level causing the event	Yes	No	No
event_scope	Event scope	Yes	No	No
foglight_rule_alarm_link	Link for the alarm	Yes	Yes	Yes
foglight_rule_comments	Comments for the rule	Yes	Yes	Yes
foglight_rule_domain_query	Rule domain query	Yes	Yes	Yes
foglight_rule_id	Rule ID	Yes	Yes	Yes

Variable	Description	Trigger Type		
		Time	**Data**	**Even t**
foglight_rule_name	Rule name	Yes	Yes	Yes
foglight_scoping_id	ID of the topology object	Yes	Yes	Yes

For more information on rule trigger types, see "Triggering rules" on page 251.

Note	vFoglight prevents you from creating a rule variable with the same name as a system variable. However, the variable name can change if you change the trigger type. In this instance, a warning icon will appear in the Rule Variables and Severity Level Variables listings.

Editing action parameters

To edit an action parameter:

Note	This procedure continues from "Adding actions to rules" on page 286.

1 In the **Action** tab, in the **Actions** pane, click the **Action Name** column of the row containing the action whose parameter you want to edit.

The action definitions appear in the display area.

Note The above screen capture shows a list of parameters for a command action. Each action has a different set of parameters associated with it. For more information, see the table listing preceding this procedure.

2 Observe the **Type** column of the row containing the parameter that you want to edit.

> **Caution** The **Type** column shows the parameter's data type. When changing the parameter value, ensure that the value you specify matches that data type.

Each action comes with its own set of action parameters. For more information, see "About action parameters" on page 288.

3 In the **Action Parameters** pane, in the row containing the parameter that you want to edit, click the **Default** link of that appears in the row's **Value** column.

The **Action Parameter Editor** dialog box appears.
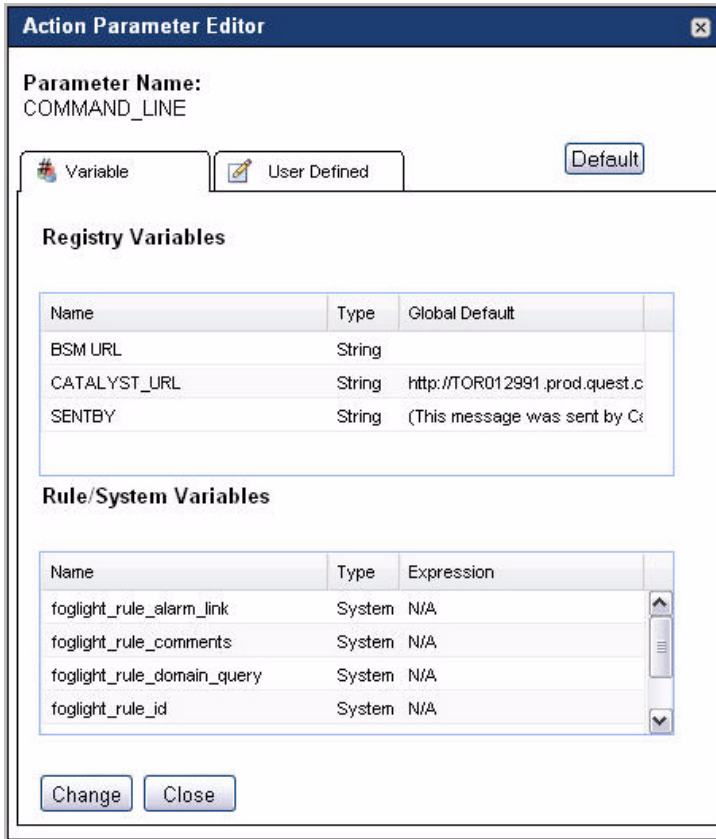
4 Specify the parameter value by completing one of the following steps in the
Action Parameter Editor dialog box.

> **Caution** When specifying the parameter value, ensure that the value you specify matches
> the parameter's data type. For more information, see step 2.

• Set the parameter to a vFoglight registry variable.

In the **Variable** tab, in the **Registry Variables** table, select the row containing
the vFoglight registry variable to which you want to set the parameter.

• Set the parameter to a rule system variable.

In the **Variable** tab, in the **Rule/System Variables** table, select the row containing the rule system variable to which you want to set the parameter. The list of available variables depends on the rule trigger type.

For complete information about rule system variables, see "About rule system variables" on page 292. For details on rule triggers, see "Triggering rules" on page 251.

• Set the parameter to a custom value.

Open the **User Defined** tab and type a value for the action parameter.

5 Click **Change**.

The **Action Parameter Editor** dialog box closes and the **Action Parameters** table refreshes, showing the newly-modified parameter value in the **Value** column of the parameter's row.

6 When you finish making changes to the action parameters, click **Go to Action List** to return to the list of actions.

The **Actions** pane refreshes, showing the newly-edited action.

Actions		
Action Name	Action Type	Description
CommandAction	Entering	
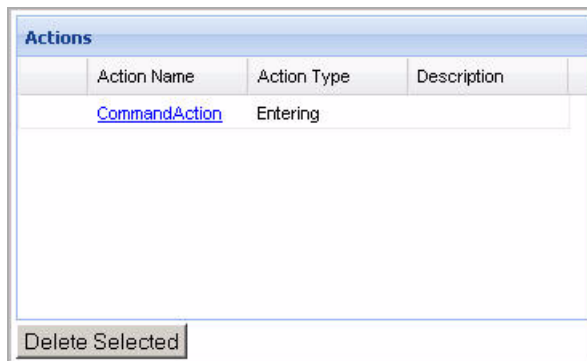
Delete Selected

To delete an action from the list, select the row containing that action in the **Actions** pane, and click **Delete Selected**.

From here, you can proceed to "Associating Rules with Schedules" on page 299.

Copying severity-level variables and actions in multiple-severity rules

In some cases you may need to copy the severity-level variables and actions from an existing severity level of the same rule. Each severity level can have its own actions and severity-level variables. For more information about severity-level actions and

variables, see "Adding severity-level variables" on page 256 and "Defining actions" on page 278.

While you are in the edit rule mode, any unsaved changes to the severity-level variables or actions that you want to copy will be carried over to the destination severity. For example, if you edit an action for the Warning condition of a rule without saving it, and then proceed to copy that action in the Critical pane, the unsaved edits of the Warning action will be carried over to the Critical severity.

Copying severity-level actions and variables can be useful in situations when those definitions are identical or, in some cases, are similar. Instead of writing and validating them for each severity level you can copy existing ones and modify them as required.

To copy variables and actions from an existing severity level:

Note   This procedure continues from "Defining the rule scope" on page 253.

1   On the **Conditions, Alarms & Actions** tab, open the **Conditions** tab.

    The **Condition** tab opens in the display area.
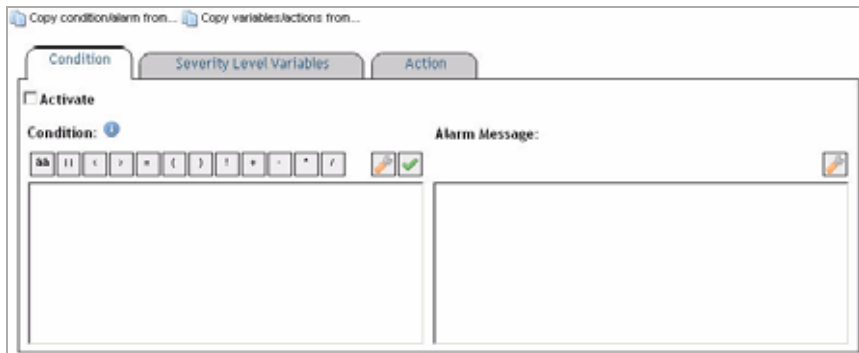
2   Choose the severity level from which you want to copy the conditional expression.

    Caution   You can only copy the conditions from those severity levels that are already defined. Attempting to copy a condition for a rule that has no conditions defined results in error.

    a   Click the **Copy variables/actions** button above the **Condition** tab.

        A list appears, showing those severity levels for which the conditions have been defined. For example, if you are defining a condition for the Critical

severity, and the conditions for the Fatal and Warning levels have already been defined, the list shows two options: **Fatal** and **Warning**, as illustrated below.

```
Fatal      ⊠
Warning
```
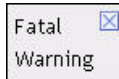
> **Caution**   Attempting to copy a condition for a rule that has no conditions defined results
> in error.

   b   Select the severity level whose condition you want to copy.

   The Condition tab refreshes.

3   Verify the settings of the newly-copied severity-level variables and actions in the **Severity Level Variables** and **Action** tabs.

4   **Optional**. Edit the newly-copied severity-level variables and actions, if required. For instructions, see one of the following sections:

   •   "Adding severity-level variables" on page 256
   •   "Defining actions" on page 278

5   Save your changes to the rule condition by clicking the **Save** button above the **Condition** tab.

From here, you can proceed to "Defining actions" on page 278.

Associating Rules with Schedules

Once you have defined one or more conditions for a rule, you can associate the rule with a schedule either as an effective period or as a blackout period.

An effective period is a schedule during which you want a rule to be evaluated. For example, you might want to set your company's hours of operation as the effective period for a rule.

You can also set blackout periods for a rule. A blackout is a schedule during which evaluation of the rule is suspended for set intervals. For example, you might want to set the times when regularly scheduled maintenance is performed on a server as the blackout period for a rule.

If a rule has no schedules associated with it, then it is always active. If you only add effective schedules to a rule, then it is automatically inactive at all times other than those specified by the effective schedules. Conversely, if you only add blackout schedules to a

rule, then it is automatically active at all times other than those specified by the blackout schedules.

If you add both effective and blackout schedules to a rule, then it will be active only at the times specified by the effective schedules minus the times specified by the blackout schedules. This is because blackout schedules take precedence over effective schedules. For example, suppose you add two schedules to a rule: an effective schedule that runs Monday to Friday, 9 am to 5 pm, and a blackout schedule that runs every Tuesday from 10am to 11am. The rule will be active every Monday, Wednesday, Thursday and Friday from 9 am to 5 pm but will only be active from 9am to 10am and from 11am to 5pm on Tuesdays.

To associate a rule with schedules:

Note   This procedure continues from "Defining conditions for data-driven and time-driven rules" on page 263.

---

1 Open the **Schedules** tab.

The **Schedules** tab opens in the display area.

2 Assign effective schedules.

a In the list that appears in the upper-left corner, select one or more schedules that you want to assign as effective schedules.

The list shows all schedules that exist in vFoglight. For information on how to add or remove schedules, see Chapter 8, "Using Schedules" on page 395.

b Click **Add** on the right of the list.

The **Effective Schedules** list on the right refreshes, showing the newly-added schedules.

3 Assign blackout schedules.

   a In the list that appears in the lower-left corner, select one or more schedules that you want to assign as blackout schedules.

      Note The list shows all schedules that exist in vFoglight. For information on how to add or remove schedules, see Chapter 8, "Using Schedules" on page 395.

   b Click **Add** on the right of the list.

      The **Blackout Schedules** list on the right refreshes, showing the newly-added schedules.
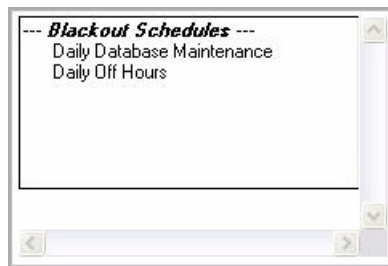
      Note Adding the **Always** entry to the list of blackout schedules does not create a black out for the rule. It has no effect on the rule's blackout schedule.

The same set of schedules are listed as *Available Schedules* for use as effective schedules and blackout schedules. Do not add the same schedule as both an effective schedule and a blackout schedule. If you do so, the schedule will only count as a blackout schedule (because blackout schedules take precedence over effective schedules).

From here, you can proceed to "" on page 302.

Defining Alarm and Action Behavior

vFoglight allows you to configure a rule so that its actions and alarms (multiple-severity rules only) do not fire repeatedly. Defining the behavior of rule alarms and actions can help you avoid being overwhelmed with alerts when a rule condition is met many times within a short period.

To define alarm and action behavior:

Note   This procedure continues from "" on page 299.

1 Open the **Behavior** tab.

The **Behavior** tab opens in the display area.

Simple rule

Multiple-severity rule

2 Configure the desired options for the behavior of rule alarms and actions and select the check boxes that correspond with these options.

Defining Rule-Level Variables

In addition to vFoglight registry variables and severity-level variables, you can define rule-level variables. If you are creating or editing a multiple-severity rule, you can define a rule level variable and reference it in expressions of different severities in the rule definition.

There are two types of rule-level variables:

- *Expressions*. An expression is used to retrieve data. It can contain a registry variable or a function.

- *Messages*. A message is typically a text string that can include other severity-level variables, displaying dynamically-supplied data about your monitored system.

For example:

Severity-Level Variables		
Name	Value	Type
var1	scope.get(**"**agent/host/name**"**)	Expression
var2	#CPU_Utilization#	Expression
var3	#Run_Queue_Length#	Expression
Text	@var1: CPU Utilization	Message
Subject	CPU Utilization is at @var2% and the number of process in the run queue is @var3. A CPU Bottleneck is being detected on @var1. Check the top processes (using the Top_CPU_Table) to determine which processes are the greatest contributors to CPU Loads, or follow the vFoglight online help to find out if the system is CPU constrained. Please use the following URL to obtain alarm details. @foglight_rule_alarm_link	Message

For more information about vFoglight registry variables, see "Working with vFoglight Registry Variables" on page 184. For details on severity-level variables, see "Adding severity-level variables" on page 256.

To define a rule-level variable:

Note   This procedure continues from "

---

1   Open the **Rule Variables** tab.

The **Rule Variables** tab opens in the display area.

2   Define the type of the rule-level variable by selecting one of the following **Type** options on the right:

   • **Expression**

   • **Message**

3   Name the severity-level variable.

   In the **Name** box, type the name of the variable.

   Important. The following names are reserved and should not be used:

   • `foglight_severity_level`

   • `foglight_severity_level_name`

   Note   You cannot give the same name to more than one expression or message in the same scope. If you give the same name to two expressions or messages in different scopes, only the severity-scoped one will appear in the **Rule Variables** table.

4   Specify the variable value.

   Expressions can contain registry variables or functions while messages are text strings that can make use of the existing severity-level variables.
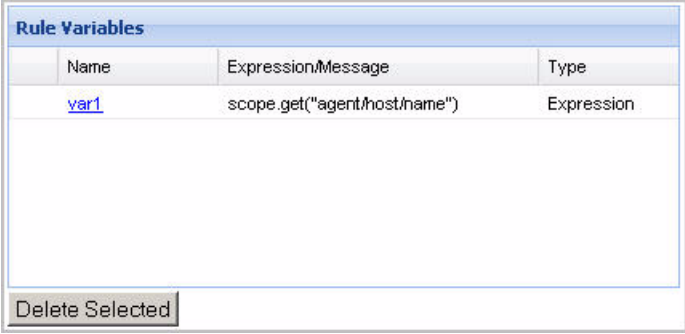
For example:

Severity-Level Variables		
Name	Value	Type
var1	scope.get(**"agent/host/name"**)	Expression
Text	@var1: CPU Utilization	Message

In the **Expression/Message** box, type the value of the variable.

5 Click **Add**.

The **Rule Variables** pane refreshes, showing the newly-added variable.

Rule Variables		
Name	Expression/Message	Type
var1	scope.get("agent/host/name")	Expression

Delete Selected

To delete a rule-level variable from the list, select the row containing that variable in the **Rule Variables** pane, and click **Delete Selected**.

Core vFoglight Rules

The vFoglight Management Server includes some built-in rules that monitor the health of your application server environment.

Overview of rules

vFoglight allows you to create flexible rules that can be applied to complex, interrelated data from multiple sources within your distributed system. You can associate several

different actions with a rule, configure a rule so that it does not fire repeatedly, and associate a rule with schedules to define when it should and should not be evaluated.

Different types of data can be used in rules, including registry variables, raw metrics, derived metrics, and topology object properties.

There are two types of rules in vFoglight: simple rules and multiple-severity rules. A simple rule has a single condition, and can be in one of three states: *Fire*, *Undefined*, or *Normal*. A multiple-severity rule can have up to five severity levels: *Undefined*, *Fatal*, *Critical*, *Warning*, and *Normal*.

Rule conditions are regularly evaluated against monitoring data (metrics and topology object properties collected from your monitored environment and transformed into a standard format). Therefore, the state of the rule can change if the data changes. For example, if a set of monitoring data matches a simple rule's condition, the rule enters the *Fire* state. If the next set does not match the condition, the rule exits the *Fire* state and enters the *Normal* state.

A rule condition is a type of expression that can be true or false. When it evaluates to true, the rule is said to fire, causing any actions that are associated with the rule or severity level to be performed. You can configure a rule to perform one or more actions upon entering or exiting each state. When a multiple-severity rule fires, an alarm also appears in vFoglight.

For more information see "Working with Rules" on page 223.

Core vFoglight rules

Rules in this section:

- Agent Health State Rule
- BSM All Events Rule
- Catalyst Data Service Discarding Data Rule
- Catalyst Database Space Checking Rule
- Catalyst Free Space Checking for Oracle Tablespaces Rule
- DiagnosticAgentDiscovery
- Email Reports Sample Rule
- vFoglight Agent Type License Checker
- vFoglight Memory Usage Check Rule
- vFoglight Topology Size Limit Reached

- Remote Agent Manager State Rule

- ServiceLevelEvaluation – FMSServiceSLP Rule

Agent Health State Rule

Purpose

This rule monitors the health of all agents in the monitoring environment.

Scope

Agent : agentID != "0"

Rule Definition

Conditions	State
An agent is down	Warning
An agent's health is in decline	Critical

BSM All Events Rule

Purpose

This rule sends all alarms from vFoglight to the Service Discovery and Dashboards product.

Scope

None

Catalyst Data Service Discarding Data Rule

Purpose

This rule monitors the observations and generates alarm if the Data Service starts discarding any observations. This can happen when the vFoglight Management Server is overloaded, or when there is a difference or the difference in the system time between the monitored system and the vFoglight Management Server.

Scope

CatalystDataService

Rule Definition

Conditions	State
The Data Service discards one or more observations within a 15 minute interval	Warning

Catalyst Database Space Checking Rule

Purpose

This rule monitors the size of the database.

Scope

CatalystDatabase

Rule Definition

Conditions	State
The size of the vFoglight database exceeds 75% of the maximum database size.	Warning
The size of the vFoglight database exceeds 90% of the maximum database size.	Critical
The size of the vFoglight database exceeds 98% of the maximum database size.	Fatal

Catalyst Free Space Checking for Oracle Tablespaces Rule

Purpose

This rule checks the space that is currently available to the Oracle database against the thresholds defined in the vFoglight registry by the following variables:

- DBSMon.WarningFreeTablespaceSize
- DBSMon.CriticalFreeTablespaceSize
- DBSMon.FatalFreeTablespaceSize

Database administrators should provide values for these thresholds in order to get notified when the database starts growing out of bounds.

Scope

CatalystTablespace

Rule Definition

Conditions	State
The size that is available to the Oracle database exceeds the threshold of set by the `DBSMon.WarningFreeTablespaceSize` registry variable.	Warning
The size that is available to the Oracle database exceeds the threshold of set by the `DBSMon.CriticalFreeTablespaceSize` registry variable.	Critical
The size that is available to the Oracle database exceeds the threshold of set by the `DBSMon.FatalFreeTablespaceSize` registry variable.	Fatal

DiagnosticAgentDiscovery

Purpose

This periodically looks for new agent instances that are connecting to the vFoglight Management Server. It rebuilds the topology if it detects new agents.

Scope

CatalystServer

Email Reports Sample Rule

Purpose

This rule directs all scheduled reports to their email recipients. A scheduled report can have one or more email recipients.

Scope

None

vFoglight Agent Type License Checker

Purpose

Checks whether the CPU count of an agent type exceeds the licensed number of agents.

Scope

AgentTypeLicense

vFoglight Memory Usage Check Rule

Purpose

This rule checks the memory that is available to vFoglight.

Scope

(CatalystServer).jvm

vFoglight Topology Size Limit Reached

Purpose

Checks if any attempts to create topology objects are failing because the topology size limit has been reached. This number is defined by the foglight.limit.instances registry variable whose global default value is set to 10000. You can change this value as required. For more information, see "Editing Registry Variables" on page 200.

Scope

CatalystTopologySizeConstraintService

Remote Agent Manager State Rule

Purpose

This rule checks whether all instances of the vFoglight Agent Manager are connected to the vFoglight Management Server.

Scope

RemoteClient

Rule Definition

Conditions	State
An instance of the vFoglight Agent Manager is disconnected	Warning

ServiceLevelEvaluation – FMSServiceSLP Rule

Purpose

vFoglight monitors each service (either implicit or user-defined) for service level compliance. The ServiceLevelEvaluation – FMSServiceSLP rule checks the availability of each service and raises an alarm if the availability is lower than the a predefined threshold during a period of one hour.

Scope

FSMServiceLevelPolicy

Rule Definition

Conditions	State
An average availability during one hour period is below 95%.	Warning
An average availability during one hour period is below 85%.	Critical
An average availability during one hour period is below 70%.	Fatal

Example: Creating a Multiple-Severity Rule Scoped to an EJB Instance

This section provides an example of a multiple-severity rule and describes the process of creating it.

There is a specific EJB instance (called *EJB_Instance1*) in the application *MyApplication* that you want to monitor; you would like to be alerted when the number of rollbacks per minute exceeds a certain threshold.

To configure vFoglight to monitor *EJB_Instance1*, you launch the vFoglight Administration Module and create a multiple-severity rule that is scoped to this specific topology object and that has conditions set for the *Fatal*, *Critical*, and *Warning* levels.

Launching the Create Rule dashboard

To begin the process of creating the rule, in vFoglight, in the Administration module, open the Create Rule dashboard by choosing **Rules & Notifications > Create Rule** from the navigation panel.

Setting basic rule properties

In the Rule Definition area of the Create Rule dashboard, you name the rule
`EJB_Instance1-Rollbacks` and add comments about the purpose of this rule. You
select **Multiple-Severity Rule** as the **Rule Type**. Since you want this rule to be
evaluated every time that metrics associated with *EJB_Instance1* are sent to the
vFoglight Management Server, you leave the **Trigger Type** at its default setting, **Data
Driven**.

Scoping the rule

Having set the basic rule properties, you scope the rule to the specific topology object
that you want to monitor. First, you select **WebLogicEJBInstance** from the **Topology
Type** box and then click the **Append** button (🔼) to the right of the menu to insert the
name of this topology type into the **Rule Scope** box. After inserting the name of the
topology type, you must manually type a space in the **Rule Scope** box, followed by the
word `where`, followed by another space. Next, you specify the EJB instance and
application in this box using the query language.

Since you want this rule to apply to a specific EJB instance (`EJB_Instance1`), you
specify it by name in the **Rule Scope** box. To do so, you select the topology type
property **name** from the **Property** drop-down menu. You then place the cursor in the
Rule Scope box where you want your selection to be inserted and click the **Append**
button (🔼) to the right of the **Property** menu. After inserting the property **name**, you
manually specify the value for the property as follows:

```
name="EJB_Instance1"
```

You want to specify another property after the instance name, so you manually type a
space in the **Rule Scope** box, followed by the word `and`, followed by another space
after `name="EJB_Instance1"`.

You then specify the application name in the **Rule Scope** box using the following
syntax:

```
ejb.application.name="MyApplication"
```

When you finish editing the information in this box, the rule scope is specified as
follows:

```
WebLogicEJBInstance where name="EJB_Instance1" and
ejb.application.name="MyApplication"
```

You click the **Validate Scope** button (✅) to ensure that the topology type is valid and that you used the correct syntax in the **Rule Scope** box. The rule scope is successfully validated, so you click **Next** to navigate to the Condition, Alarms & Actions tab.

Specifying conditions

After scoping the rule to `EJB_Instance1` in `MyApplication`, you specify the conditions for the rule on the Condition, Alarms & Actions tab.

To start the process of setting the condition for the Fatal severity level, you click the header for this level on the Condition, Alarms & Actions tab.

You had previously created a derived metric called `transactionRollbackRate`: you derived this metric from the raw metric `transactionsRolledBackTotalCount` so that it returns a rate (the total number of transactions that are rolled back per minute).

On the **Condition** sub-tab for the Fatal level, you click the **Condition Editor** button (🔧) to launch the Condition Editor. You switch to the **Metric/Property** tab, select **transactionRollbackRate** from the **Choose Metric Value** list, and click **Select** to insert it into the **Condition** box. You then type >10 in this box after the metric name.

When you finish editing the information in the **Condition** box, the condition is specified as follows:

```
#transactionRollbackRate#>10
```

You repeat this process for the Critical and Warning levels, specifying the conditions for these levels as `#transactionRollbackRate#>8` and `#transactionRollbackRate#>6`, respectively.

You click **Finish** when you have specified the conditions for all three severity levels. You review the settings for the rule on the **Rule Added** area and then click the **Go to Rule List** button. The new rule is listed on the Manage Rules dashboard.

Example: Creating a Simple Rule

A simple rule is scoped to the topology type `JVM` and has the condition `#threads_started#>10`. This means that the rule will enter the Fire state when any instance of the `JVM` topology type returns a started-threads count greater than 10.

The rule includes an expression called `ThreadsNum`. The value of this expression is the metric `#threads_started#`, the same metric that is used in the rule's condition. In turn, this expression is referenced in a message called `ProblemSynopsis` whose value is `Threads started count is too high: @ThreadsNum`.

An entering Email action is set for this rule. This action uses the `ProblemSynopsis` message as the text of the email that is sent when the rule enters the Fire state.

- "Example: Creating Multiple-Severity Rules with a Topology Scope" on page 314
- "Example: Configuring Rule Action Parameters" on page 314
- "Example: Creating Rules with Different Topology Types" on page 315
- "Example: Implementing Command Actions in Rules" on page 322

Example: Creating Multiple-Severity Rules with a Topology Scope

You want to monitor processor objects on a particular server (called `Server1`) based on the metric `percentUserTime`. You create a multiple-severity rule to monitor these objects, and scope the rule to the `Processor` topology type. To cause this rule to apply to the server that you are interested in, you specify in the scope that the rule should apply to the `Processor` topology object whose `host name` property is `Server1`:

```
Processor where host.name="Server1"
```

You want to include all three severity levels (Fatal, Critical, and Warning) in the rule. You set these levels' conditions as follows:

- **Fatal:** `#percentUserTime#>15`
- **Critical:** `#percentUserTime#>10`
- **Warning**: `#percentUserTime#>5`

Example: Configuring Rule Action Parameters

You want to define rule actions for a rule severity level: a remote command action on a monitored host and a script action on the vFoglight Management Server.

To configure a rule's action parameters:

Note   The information in this procedure assumes that you have a good understanding of the rule editing workflow. For step-by-step instructions on how to add actions to a rule and edit their parameters, see "Defining actions" on page 278.

---

1   Verify that the script is accessible by the rule. To do that, copy your script to the *<vfoglight_home>/scripts* directory on the vFoglight Management Server.

2   Open the rule for editing and navigate to the **Action** tab of the severity level for which you want to define the actions.

3   Add an entering ScriptAction and edit its parameters.

    a   If your script has one or more arguments, use the `Argument 1-10` parameters to specify the arguments' value.

    b   If you want the script to run against a particular topology object, use the `Script object id` parameter to specify the object's ID.

    c   Use the `Script name` parameter to specify the script name.

4   Return to the **Action** tab.

5   Add an entering Remote Command Action that is to be executed on a monitored host and edit its parameters.

    a   Use the `HostName` parameter to specify the name of the monitored host machine.

    b   Use the `RemoteWorkingDir` parameter to specify the absolute path on the remote host in which you want the command to run.

    c   Use the `COMMAND_LINE` parameter to specify the command that you want to run remotely along with any options or arguments if applicable.

6   Return to the **Action** tab and save your changes to the rule.

When the rule enters the severity state that includes newly-defined actions it executes those actions as specified.

Example: Creating Rules with Different Topology Types

In this example, you will create two rules, Processor Load and Host Processor Load. For the purpose of this example, the Processor Load rule is scoped to the `Processor` topology type that monitors the utilization of all `Processor` objects instances in the topology model, and fires when the utilization for a processor reaches 90% in a 24-hour period. For instructions on how to create this rule, see "To scope a rule to the Processor type:" on page 316.

Unlike the Processor Load rule that monitors all instances of the Processor type. the Host Processor Load rule is scoped to the `Host` type that monitors all of the `Processor` instances for a particular `Host` object, and fires if all of the `Processor` objects for the scoped `Host` object reach the utilization of 90%. For instructions on how to create this rule, see "To scope a rule to the Host type:" on page 322.

The following diagram illustrates the scope of each of the rules that you are about to create from the topology model perspective.
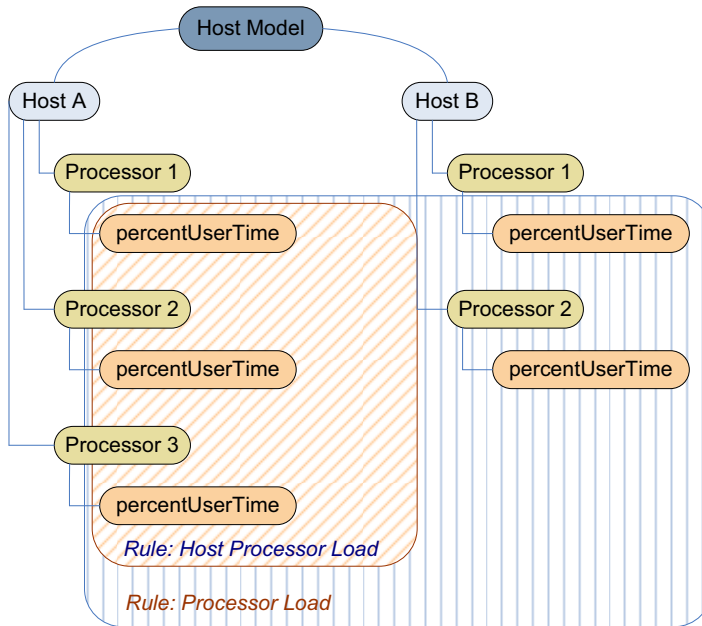
To scope a rule to the Processor type:

    1 Create a simple, data-driven rule with the `Processor` scope.

        a Ensure that the navigation panel is open.

            To open the navigation panel, click the right-facing arrow ▶ on the left.

        b On the navigation panel, under **Dashboards**, choose **Administration > Rules & Notifications > Create Rule**.

            The Create Rule dashboard appears in the display area with the **Rule Definition** tab open.
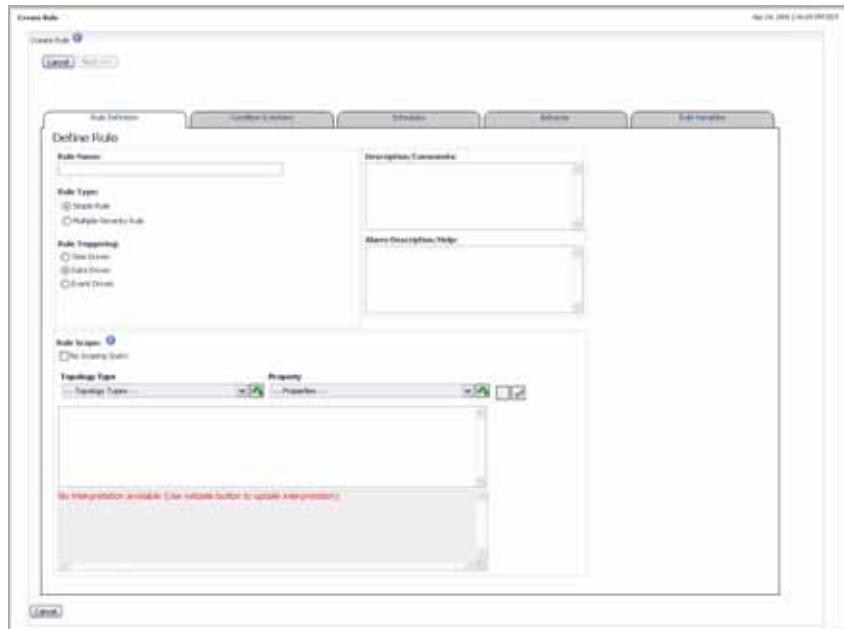
c In the Create Rule dashboard, in the **Rule Definition** tab, in the **Rule Name** box, type the rule name. For example, Processor Load.

d Under **Rule Type**, select the **Simple Rule** option.

e Under **Rule Triggering**, select the **Data Driven** option.

2 Scope the rule to the Processor topology type.

    a In the **Rule Definition** tab, in the **Rule Scope** pane, ensure that the **No Scoping Query** check box is clear.

    b Click **Topology Type** and select **Core > Processor** from the list that appears.

    c Click the Append button (🔼) to the right of the **Topology Type** box.

    The box immediately below the **Topology Type** box, showing the newly-selected Processor type.

    d Validate the topology scope by clicking the Validate Rule Scope button (✅) to the right of the **Property** box.

    A confirmation message appears above the **Topology Type** box while the name of the Processor type appears in the box at the bottom.

3 Write a condition that triggers the rule each time the utilization of a Processor type reaches 90% using the Processor's percentUserTime metric.

a In the Create Rule dashboard, open the **Conditions and Actions** tab.

b Expand the condition editing pane by clicking the **Fire** bar.
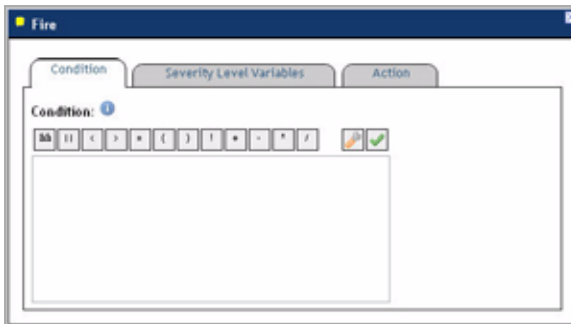
c Click the Condition Editor button ().

The **Condition Editor** dialog box appears.
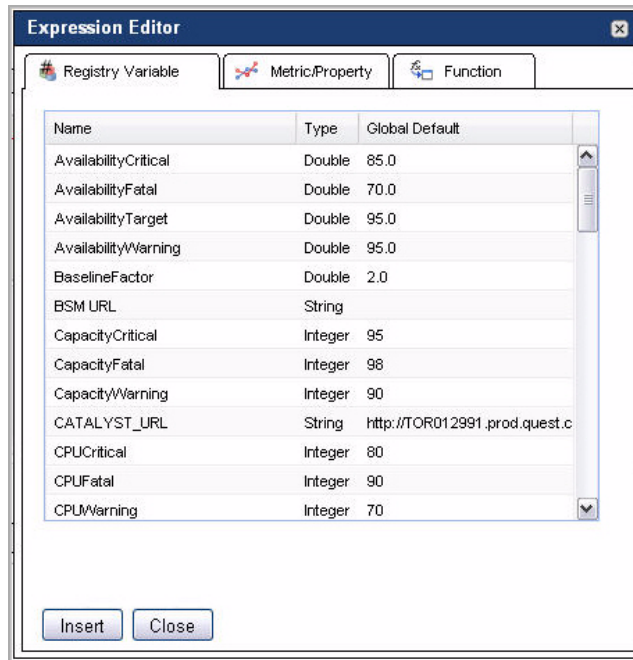
d In the **Condition Editor** dialog box, open the **Metric/Property** tab.
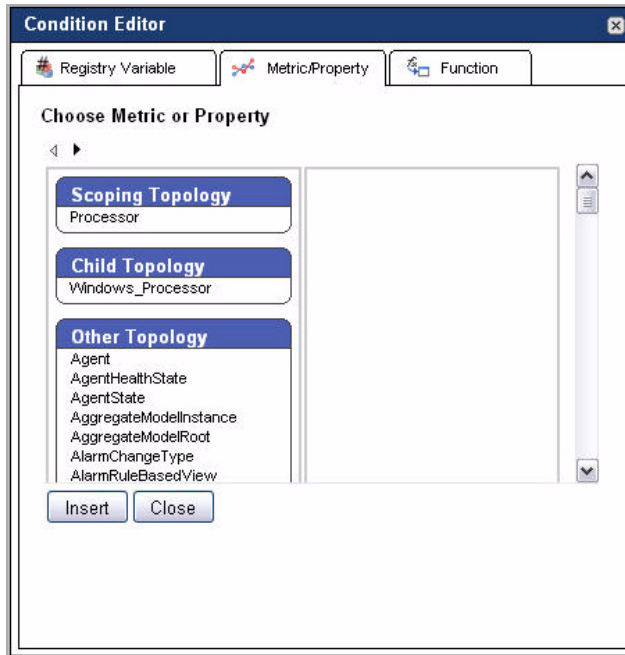
e   On the **Metric/Property** tab, in the left pane, in the **Scoping Topology** area, click **Processor**.

    Tip   The **Scoping Topology** area shows the rule scope, Processor, that you defined in step 1.

f   The pane on the right refreshes, showing the instances and metrics for the selected Processor type.
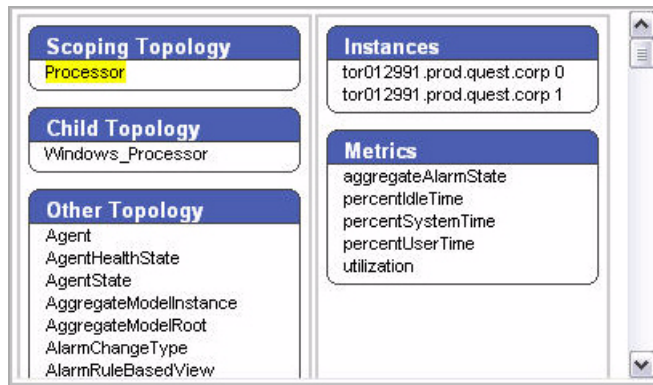
g In the **Metrics** area, select **percentUserTime** and click **Insert**.

The **Condition** box in the display area refreshes, showing the newly-selected metric.
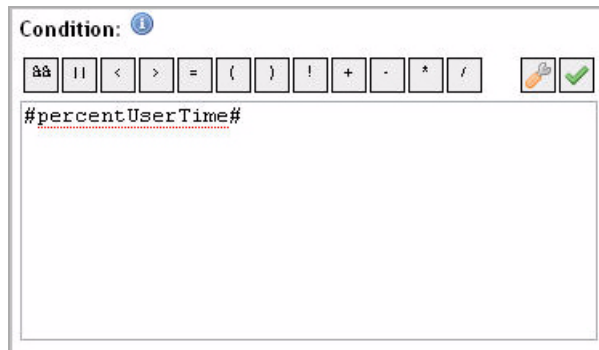
h Edit the condition as follows:

```
#percentUserTime# > 0.9
```

i Click the Validate button (✓) above the **Condition** box.

A success message appears above the **Condition** box.

4 Refine the newly-created condition by adding a time constraint to it and a Groovy function that retrieves a maximal value of the metric over a 24-hour period.

Edit the condition as follows:

```
max(#percentUserTime for 24h#) > 0.9
```

5 Click **Finish**.

To scope a rule to the Host type:

Note The information in this procedure assumes that you have a good understanding of the rule creation workflow. For step-by-step instructions on how to scope a rule to a topology type or use the Condition Editor, see the above procedure, "To scope a rule to the Processor type:" on page 316.

---

1 Create a simple, data-driven rule.

2 Scope the rule to the Host topology type.

3 Write a condition that generates an alarm each time the utilization of all of the scoped host's processors are utilized over 90% using the Processor's percentUserTime metric for each Processor object that is within the rule scope, set to the Host type (see step 1).

For example:

```
min(#percentUserTime from Processor where host = $scope#)
    > 0.9
```

4 Save your changes.

Example: Implementing Command Actions in Rules

In this example, you will define a command action that calls a shell script and defines a set of environment variables containing information about the agent instances in your monitoring environment. Next, you will write the shell script that will print the content of the command action variables to an output file.
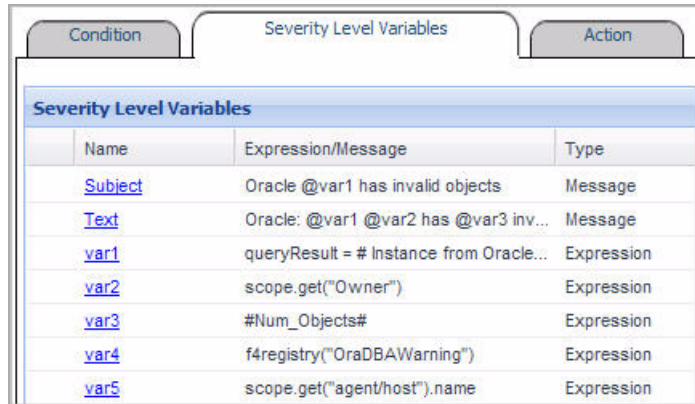
When you save your changes, the command action calls the shell script, which populates the output file with agent-related information whenever the rule condition is met.

Alternatively, a command action can issue a command directly without referencing it in a script by calling the command line directly.

To integrate a command action with a shell script:

1 Locate a rule that you want to associate with a command action and open it for editing.

2 In the **Edit Rule** view, open the severity level to which you want to add a command action.

3 In the severity level area, open the **Severity Level Variables** tab, and add severity-level variables that contain the information that you want to print to an output file. For example:

Condition	Severity Level Variables	Action

Severity Level Variables

Name	Expression/Message	Type
Subject	Oracle @var1 has invalid objects	Message
Text	Oracle: @var1 @var2 has @var3 inv...	Message
var1	queryResult = # Instance from Oracle...	Expression
var2	scope.get("Owner")	Expression
var3	#Num_Objects#	Expression
var4	f4registry("OraDBAWarning")	Expression
var5	scope.get("agent/host").name	Expression

The above example shows seven different severity-level variables:

- `Subject`, `Text`: Define the text that appears in the alarm message.

- `var1`: Retrieves the result of a query.

  For example, the expression
  `queryResult = #Instance from OracleHost_Processes#` returns the value of the Instance field of the OracleHost_Processes table.

- `var2`, `var5`: Retrieve the value of a topology property that exists in the rule scope using the `scope` variable and its `get` function.

  For example, the expression `scope.get("agent/host").name` obtains the name of a monitored host that is being monitored by an `agent` object instance that exists in the rule scope.

- `var3`: Retrieves the value of a property of the scoped topology type.

  For example, the expression `#Num_Objects#` retrieves the value of the `#Num_Objects#` property of the scoped topology type.

- `var4`: Retrieves the value of a vFoglight registry variable.

For example, the expression f4registry(**"OraDBAWarning"**) retrieves the value of the OraDBAWarning registry variable.

4   Open the **Action** tab and add an entering command action.

5   Define the action parameters as follows:

- COMMAND_LINE: Specify the absolute path and name of the shell script that you want the command action to call.

- ENVIRONMENT_VARIABLES: Type a list of the variables that you defined in step 3, using the following syntax to specify a variable:

      output_data=@variable

   Tip   Use the exclamation mark '!' to separate variables.

For example:

Condition	Severity Level Variables	Action		

Action: CommandAction
Action Type: Entering
Description:

Action Parameters

Name	Default Value	Required	Type	Value	Parameter Description
COMMAND_LINE	Undefined	mandatory	String	/opt/quest/test.sh	Executable command and arguments
ENVIRONMENT_VARIABLES	Undefined	optional	String	P1=@var1!P2=@var2!P3=@var3! P4=@var4!P5=@var5!@P6=@var6	Exclamation mark separated environment variables i.e. var1=name1! var2=name2!

Go to Action List

6   Save your changes.

7   Create the shell script, ensuring that its name and location match the one you set in the COMMAND_ACTION action parameter (see step 5).

8   Add a line to the shell script using the following command syntax:

```
/bin/echo ${variable_1}:${variable_2}:...:${variable_n} >
    output_file_path_and_name
```

For example:

```
/bin/echo ${P1}:${P2}:${P3}:${P4}:${P5} >
    /opt/quest/out.txt
```

   Tip   Alternatively, to issue the command directly without referencing it in a script as instructed in step 7, use the COMMAND_ACTION's value to specify the command.

When the rule meets the condition that includes the newly-defined command action, it writes the information to the output file. Here is a sample of what that output may look like:

```
jorcl:PUBLIC:19.0:root@localhost:
    melscv-w2k3-fdb.melsales.dev.mel.au.qsft
```

For complete information on how to add actions to rules, see "Defining actions" on page 278.

- •

7

Working with Data

This chapter introduces you to vFoglight data management entities on how to create and manage these entities. It contains the following sections:

| Note | In order to complete each of the procedures in this chapter, your user account must belong to a group with the Administration role. For more information about users, groups, and roles, see "Managing Users and Security" on page 105. |

This chapter contains the following sections:

About Data Management in vFoglight

vFoglight models retain collected data and transform it into nodes, adding configuration data to each node as properties, and attaching metric data to appropriate nodes as metrics. Each metric is associated with a topology type or with a specific topology object. In some cases you will need to create custom topology types that suit your monitoring needs. For more information, see "Adding Topology Types" on page 329.

There are two types of metrics in vFoglight:

- *Raw metrics*. They include the metrics collected directly from monitored hosts.

- *Derived metrics*. They are calculated from one or more raw or derived metrics. Derived metrics are scoped to a topology type or its objects. You can create and manage derived metrics using the Administration module. Derived metrics are useful in situations when you need to reuse metric expressions in rules. For more information on how to manage and create derived metrics, see "Working with Derived Metrics" on page 332.

In vFoglight, retention policies allow you to define time periods where monitoring data can be sampled, aggregated, or purged from your system. Topology objects inherit retention policies from its topology type. vFoglight allows you to alter retention policies for one or more topology types as required. For more information, see "Managing Retention Policies" on page 372.

In addition to adding derived metrics and topology types, and altering the retention policy for a topology type, vFoglight allows you to assign threshold levels to metrics. This feature is useful in case you need to reference these levels in rules or derived metrics. For more information on how to create and manage thresholds, see "Working with Thresholds" on page 353.

Adding Topology Types

vFoglight transforms monitoring data into models. A model is a set of objects and relationships designed to represent a monitored resource and its parts. Topology describes the logical and physical relationships between data nodes in a model. At run-time, vFoglight dynamically builds topology models based on data about your system that is collected by vFoglight agents. Topology models provide the context for the metrics sent by the agents to the vFoglight Management Server. The set of topology types that exist in your environment depends on your monitoring needs, reflected in the type and nature of cartridges that you use for data collection. If you need additional topology types, you can add them to vFoglight as required using the Adding Topology Types dashboard.

Use the XML syntax when defining a topology type. For example:

```
<type name="ApacheSvr_Transactions" extends="F4Table">
<property name="IntervalTransactions" type="Metric"
   is-containment="true" />
<property name="TransactionRate" type="Metric"
   is-containment="true" />
<property name="TransactionTag" type="String"
   is-identity="true" />
<property name="TransactionThroughput" type="Metric"
   is-containment="true" />
<property name="TransactionThroughputRate" type="Metric"
   is-containment="true" />
</type>
```

Important Topology types can only be removed by uninstalling the cartridge that contains the types that you want to delete.

To add topology types:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

1   Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Data > Add Topology Type**.

   The Add Topology Type dashboard appears in the display area.

3 To add one or more topology types that are defined in an XML file accessible by your local machine, complete one of the following steps in the **Import From File** area of the Add Topology Type dashboard.

  • Ensure that the **File on Local Computer** option is selected. Then click **Browse**, and navigate to the topology file in the file browser that appears.

    The file browser closes and the **File on Local Computer** option refreshes to show the absolute path and name of the topology file.

  or

  • Select the **File on Local Computer** option, and in the box to the right, type the absolute path and name of the topology file

    Windows example:

    ```
    C:\Vizioncore\vFoglight\topology.xml
    ```

4 To add one or more topology types that are defined in an XML file accessible by the machine on which the vFoglight Management Server is running, complete the following steps.

  a Select the **File Location on Server** option.

    b In the **File Location on Server** box, type the path and name of the topology file. Use either an absolute path or a path relative to the installation directory of the vFoglight Management Server.

> **Note** Use the back slash character '\' as a directory separator.

For example, both of the following lines point to the same topology file:

```
C:\Vizioncore\vFoglight\topology\topology.xml
```

```
topology\topology.xml
```

5 To define one or more topology types using the text editor in the Add Topology Type dashboard, in the **Import From Text** area, type the topology definition that you want to add between the `<types>` and `</types>` tags.

For example:

```
<!DOCTYPE types SYSTEM "../dtd/topology-types.dtd">
   <types>
      <type name="MyHost" extends="Host">
         <property name="MyAlarmTotalCount" type="Integer"
            is-containment="true" />
         <property name="MyDomainName" type="String"
            is-containment="true" />
      </type>
      <type name="MyAgent" extends="Agent">
         <property name="AgentName" type="String"
            is-containment="true" />
         <property name="MyAnnotations" type="String"
            is-containment="true" />
      </type>
   </types>
```

Validate the topology definition by clicking **Validate**.

The **Alert** message box appears, indicating that the topology definition is valid.

```
Alert                                                    ×
Successful
The XML topology type is valid and can be imported.
```

> **Note** The validation process is limited. Your XML may appear to be valid and still fail on import.

6 Close Click **Import Topology**.

The **Alert** message box appears, this time indicating that the topology import was successful.

```
Alert                                              ✕
Successful
Topology Type Successfully Imported, affecting 2 types.
```

Working with Derived Metrics

vFoglight transforms collected data into nodes. It adds configuration and metric data to each node as properties and metrics, respectively. A metric is a specific value that is measured over time. Each metric is associated with a topology type or with a specific topology object.

There are two types of metrics in vFoglight:

- *Raw Metrics*. Raw metrics are collected directly from your monitored environment by the agents and sent to the vFoglight Management Server.

- *Derived Metrics*. Derived metrics are calculated from one or more (raw or derived) metrics. They are scoped to a topology type and can optionally be scoped to specific objects of that type. Many derived metrics come included with vFoglight and its cartridges. If required, you can create derived metrics and add them to your environment.

There are many reasons why it can be useful to create derived metrics. For example, creating derived metrics can make creating and managing rules simpler by allowing you to reuse metric expressions (metrics and functions performed on metrics). For more examples, see the following sections:

- "Example: Creating and Managing Multiple Rules with the Same Scope" on page 351

- "Example: Using a Single Derivation with Multiple Scoping or Multiple Derivations" on page 352

- "Example: Optimizing Performance" on page 353

You create new derived metrics and manage the existing ones using the dashboards that come with the Administration module. For complete information, see the following sections:

- "Managing Derived Metrics" on page 333

Managing Derived Metrics

The Manage Derived Metrics dashboard contains a list of all derived metrics showing their name and scope. The derived metrics that exist in your vFoglight environment appear on the Manage Derived Metrics dashboard. However, there is no distinction between raw and derived metrics in other locations on the Administration module.

This dashboard also includes controls for filtering the list of derived metrics by the metric name, scope, or cartridge. For instructions on how to use the Manage Derived Metrics dashboard, see the following sections:

Accessing the Manage Derived Metrics dashboard

The Manage Derived Metrics dashboard includes a list of the derived metrics that exist in your monitoring environment and allows you to add or delete derived metrics and perform other metric management operations.

To access the Manage Derived Metrics dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Data > Manage Derived Metrics**.

    The Manage Derived Metrics dashboard appears in the display area.

3 To sort the list of derived metrics by their name or scope, click the **Derived Metric Name** or **Derived Metric Scope** column headings as required.

4 **Optional**. Filter the list of derived metrics.

- To show only the derived metrics whose name matches a particular text pattern, in the **Derived Metric Name** box at the top, type the text pattern.

  The Manage Derived Metrics dashboard refreshes, showing only the derived metrics whose name matches the specified text pattern.

- To show only the derived metrics whose scope matches a particular text pattern, in the **Derived Metric Scope** box at the top, type the text pattern.

  The Manage Derived Metrics dashboard refreshes, showing only the derived metrics whose scope matches the specified text pattern.

- To show only the derived metrics that belong to a particular cartridges, in the **Cartridge Name** box at the top, type the cartridge name.

  The Manage Derived Metrics dashboard refreshes, showing only the rules that come with the specified cartridge.

- To clear the filters, click **Clear Filters**.

The Manage Derived Metrics dashboard refreshes, showing the list of all variables.

From here, you can proceed to any of the following procedures:

- "Editing permissions of derived metrics" on page 335
- "Copying derived metrics" on page 339
- "Deleting derived metrics" on page 341
- "Viewing and editing derived metrics" on page 341

Editing permissions of derived metrics

vFoglight allows you to control access to derived metrics. For each derived metric you can grant or deny read, write, or control access to roles or users. For more information about security concepts in vFoglight, see Chapter 3, "Managing Users and Security" on page 105.

vFoglight employs the following behavior when it comes to permissions of derived metrics:

- If no one has a permission to the derived metric, everyone has a permission.

- If one has a permission to the derived metric, others with undefined permission do not have any permission.

- Final permission is based on a combination of the role, user, and derived metric defined on the server side.

Use the Edit Permissions button ( ) on the Manage Derived Metrics dashboard to navigate to the Edit Permissions for Derived Metric area, that allows you to add or edit permissions to roles and users, as outlined below. The Edit Permissions for Derived Metric area contains two tables that show the permissions for each vFoglight user or role.

Permission granted
Permission denied
Permissions not assigned
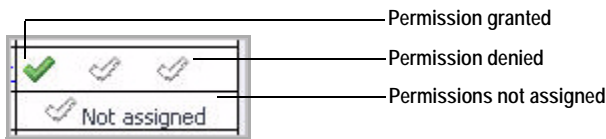
To add permissions for a derived metric:

Note   This procedure continues from "Accessing the Manage Derived Metrics dashboard" on page 333.

1   In the Manage Derived Metrics dashboard, in the row containing the rule whose permissions you want to edit, click the Edit Permissions for Derived Metric button ( ).

The Edit Permissions for Derived Metric area appears in the Manage Derived Metrics dashboard.
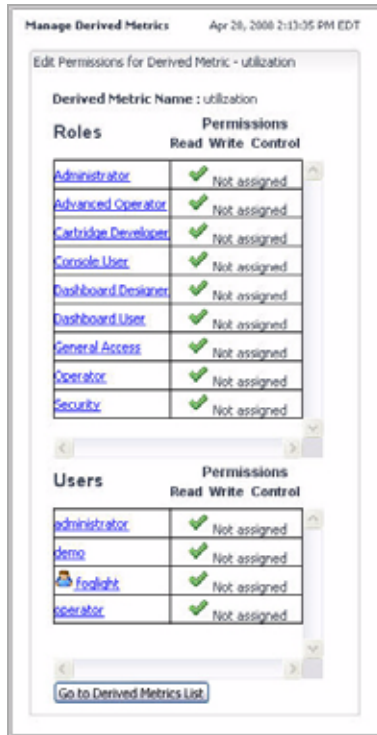
2 To add permissions to a derived metric, complete the following steps.

   a Click the role or user to which you want to assign permissions.

   Tip The Not Assigned icons in the **Permissions** columns indicate that the role has no permissions assigned to it.

   The **Add Role Permission** or **Add User Permission** dialog box appears.

Add Role Permission
Role Name: Advanced Operator
☑ Read
☑ Write
☑ Control
[Save] [Cancel]

Add User Permission
User Name: demo
☑ Read
☑ Write
☑ Control
[Save] [Cancel]

b In the dialog box that appears, use the **Read**, **Write**, and **Control** check boxes to assign permissions as required, and click **Save**.

The dialog box closes and the selected entry refreshes, showing three check marks in the **Permission** columns, one for each of the read, write, and control permissions.

Permission granted

Permission denied

3 To edit or delete permissions for a rule, complete the following steps.

   a Click the role or user whose permissions you want to edit.

     Tip Three check marks in the **Permissions** columns indicate that the role already has permissions assigned to it.

   The **Edit Role Permission** or **Edit User Permission** dialog box appears.

b To edit the permissions, ensure that the **Edit** option is selected and use the **Read**, **Write**, and **Control** check boxes as required.

c To delete the permissions, select the **Delete** option

d Click **Save**.

The dialog box closes and the selected entry refreshes, showing the newly-edited permissions.

Copying derived metrics

Use the Copy Derived Metric button on the Manage Derived Metrics dashboard to copy a derived metric, as outlined below.

To copy a derived metric:

Note   This procedure continues from "" on

1 In the Manage Derived Metrics dashboard, in the row containing the derived metric that you want to copy, click the Copy Derived Metric button ( ).

The **Copy Derivation** dialog box appears.
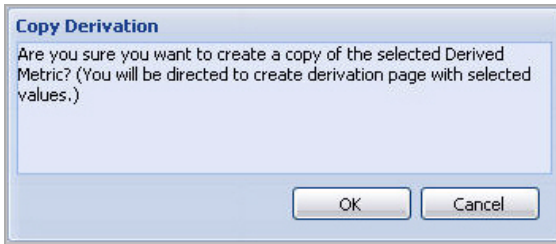
2 In the **Copy Derivation** dialog box, click **OK**.

The **Copy Derivation** dialog box closes and the **Create Derived Metric** view appears in the display area.
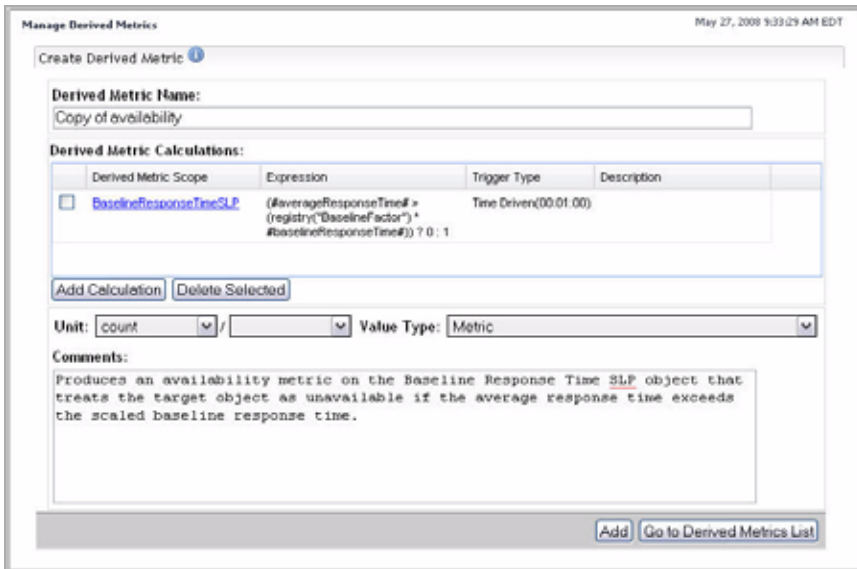
3 Provide a unique name for the destination metric.

In the **Create Derived Metric** view, in the **Derived Metric Name** box, type the name of the derived metric.

4 If required, edit the settings of the newly-copied derived metric.

For more information, see "Defining Derived Metrics" on page 344.

Deleting derived metrics

Use the Delete Selected button on the Manage Derived Metrics dashboard to delete a derived metric, as outlined below.

To delete a derived metric:

Note   This procedure continues from "Accessing the Manage Derived Metrics dashboard" on page 333.

1   In the Manage Derived Metrics dashboard, select the row containing the derived metric that you want to delete.

2   Click the **Delete Selected** button at the bottom.

The **Delete Derivation** dialog box appears.
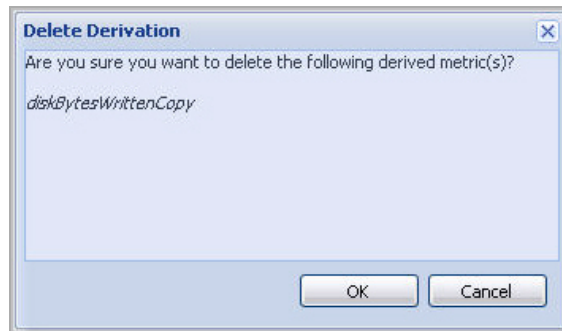
3   In the **Delete Derivation** dialog box, click **OK**.

The **Delete Derivation** dialog box closes.

4   Observe the Manage Derived Metrics dashboard.

The newly-deleted derived metrics no longer shows in the list.

Viewing and editing derived metrics

To view or edit derived metric:

Note   This procedure continues from "Accessing the Manage Derived Metrics dashboard" on page 333.

1 In the Manage Derived Metrics dashboard, click the **Derived Metric Name** column of the row containing the derived metrics whose definitions you want to view.

The **Edit Derived Metric** view appears in the Manage Derived Metrics dashboard.

2 Observe the metric definitions.

3 Edit the derived metric as required.

For complete instructions, see "Adding calculations to derived metrics" on page 344.

Creating Derived Metrics

vFoglight allows you to create derived metrics using the Create Derived Metric dashboard. You can access this dashboard from the navigation panel, or through the Manage Derived Metrics dashboard.

When you create a derived metric, vFoglight changes the topology type to which the derived metric is scoped by associating a new metric property to that topology type.

To create a derived metric:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow 🔺 on the left.

2   Open the Create Derived Metric dashboard by completing one of the following steps:
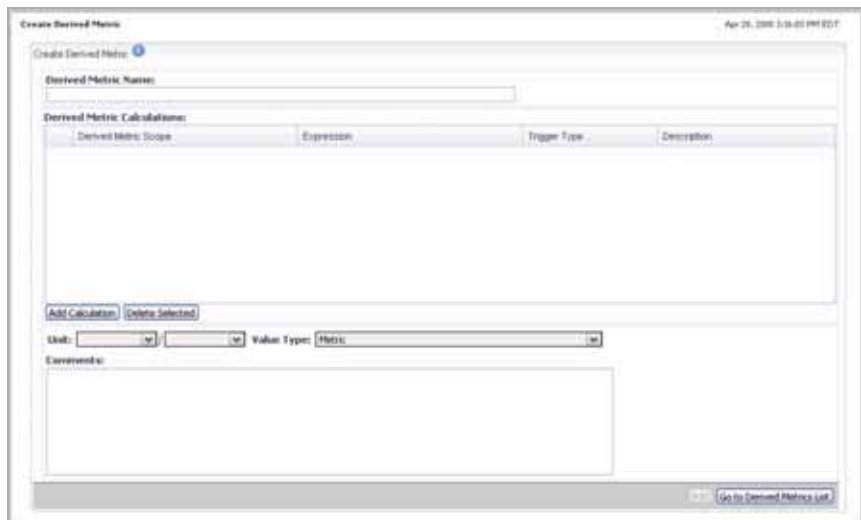
    • On the navigation panel, under **Dashboards**, choose **Administration > Data > Manage Derived Metrics**.

      In the Manage Derived Metrics dashboard that appears in the display area, click the **Add Derived Metric** button in the lower-left corner.

    or

    • On the navigation panel, under **Dashboards**, choose **Administration > Data > Create Derived Metric**.

    The Create Derived Metric dashboard appears in the display area.

From here, you can proceed to "Defining Derived Metrics" on page 344.

Defining Derived Metrics

Derived metrics are calculated from one or more (raw or derived) metrics. They must be scoped to a topology type and can optionally be scoped to specific objects of that type. If a rule or derived metric is not scoped to specific objects, it applies to all objects of that type. Many derived metrics are included with vFoglight and its cartridges. You can also create customized derived metrics from within the Administration module.

For instructions, see the following sections:

- "Getting started with derived metric definitions" on page 344
- "Adding calculations to derived metrics" on page 344
- "Triggering derived metrics" on page 348
- "Setting the value type" on page 350

Getting started with derived metric definitions

Once you create a derived metric, you can add name it and proceed to edit its settings as required.

To get started with derived metric definitions:

Note   This procedure continues from "Creating Derived Metrics" on page 342.

- Provide a descriptive name for the derived metric.

  In the Create Derived Metric dashboard, in the **Derived Metric Name** box, type the name that you want to assign to the derived metric.

From here, you can proceed to "Adding calculations to derived metrics" on page 344.

Adding calculations to derived metrics

The scope of a derived metric defines the set of topology objects against which vFoglight calculates it. A derived metric is scoped to a topology type and can optionally be scoped to specific topology objects of that type. If a derived metric is not scoped to specific objects, it applies to all instances of that type. You specify the derived metric scope using the query language. You can change the scope of a derived metric (the topology type or one or more specific topology objects of that type to which it applies) after its creation.

The vFoglight Management Server processes the derived metric calculation in the order they are listed, starting with the first one. Changing their order affects the behavior of the actions that are associated with the derived metric.

For example, if there are two calculations whose conditions evaluate to True, the first calculation listed takes precedence, causing one or more actions that are associated with that metric to be generated before the next one.

For detail information on how to scope a rule or derived metric to one or more topology objects, see "Using the Query Language" on page 473.

To get started with adding calculations to a derived metric:

Note This procedure continues from "Getting started with derived metric definitions" on page 344 or "Viewing and editing derived metrics" on page 341.

---

1 **New derived metrics.** In the **Derived Metric Calculations** area, click **Add Calculation**.

The display area refreshes, showing the **Derived Metric Scope** and **Expression** areas that allow you to define the scope for the derived metric.

2 Use the **Derived Metric Scope** and **Expression** areas to specify the scope of the derived metric.

> **Caution** If you change the topology type or object(s) to which the derived metric is scoped, you may need to reconfigure the derived metric expression: the metrics specified in the existing expression may not be available for the new topology type or object.
>
> Likewise, if you change the metrics that are specified in the Expression field, ensure that the new metrics are available for the topology type or object(s) to which the derived metric is scoped.

For detail instructions, see "Setting the Scope for a Rule or Derived Metric" on page 474.

3 When you finish adding calculations to derived metrics, ensure that their order is valid.

> **Caution** The vFoglight Management Server evaluates derived metric calculations in the order that they are listed, starting with the first one. Changing their order affects the output of actions that are associated with those calculations.

To move a threshold bound up or down, in the **Derived Metric Calculations** table, in the **Derived Metric Scope** column, use the Move up (▲) or Move down (▼) buttons as required.

4 Specify the unit of the derived metric.

Use one or a combination of the two **Unit** boxes under the **Derived Metric Calculations** list to specify the unit. Each box contains the following choices:

- **billion**
- **billionth**
- **bit**
- **byte**
- **count**
- **day**
- **exabyte**
- **gigabyte**
- **hour**
- **kilobyte**
- **megabyte**
- **microsecond**
- **million**
- **millionth**
- **millisecond**
- **minute**
- **month**
- **nanosecond**
- **percent**
- **petabyte**
- **second**
- **terabyte**

- **thousand**
- **thousandth**
- **trillion**
- **trillionth**
- **year**

For example, to set the unit of the derived metric to a number of days per month, click the left **Unit** box, and select **day** from the list that appears, then click the right **Unit** box and select **month**, as illustrated bellow.

5 Define the data type of the derived metric.

A derived metric take over the form of a metric or an observation type. Click **Value Type** and select one of the following values, as required:

- **AgentStateObservation**
- **AlarmStateObservation**
- **CatalystPersistencePolicyRollupObservation**
- **HostTopCPUProcessObservation**
- **HostTopIOProcessObservation**
- **HostTopMemoryProcessObservation**
- **Metric**
- **RequestTraces**
- **SPIDefaultObservation**
- **StringListObservation**
- **StringObservation**

> **Caution** The derived metric data types that you define at metric creation time cannot be changed.

6 **Optional**. Add comments about the newly-created derived metric.

From here, you can proceed to "Triggering derived metrics" on page 348.

Triggering derived metrics

An instance of a derived metric is created when its definition is triggered. A derived metric is configured to have one of the following triggers:

- *Schedule-Driven Derived Metric*. A schedule-driven derived metric is evaluated based on a schedule created in the Administration Module. See Chapter 8, "Using Schedules" on page 395 for information about schedules.

  There are three trigger timing options for schedule-driven derived metrics:

  - *Enter and Exit*. Causes the derived metric to be evaluated when the period defined by the schedule begins and ends.
  - *Enter only*. Causes the derived metric to be evaluated when the period defined by the schedule begins.
  - *Exit only*. Causes the derived metric to be evaluated when the period defined by the schedule ends.

- *Time-Driven Derived Metrics*. A time-driven trigger causes the derived metric to be evaluated once per pre-defined interval.

- *Data-Driven Derived Metrics*. If a derived metric has a data-driven trigger, it will be evaluated every time that data that is used in the expression for the derived metric is sent to the vFoglight Management Server.
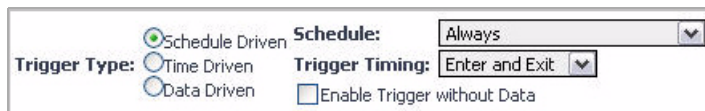
To assign a schedule -driven trigger:

Note This procedure continues from "Adding calculations to derived metrics" on page 344.

1 In the **Expression** area, under **Trigger Type**, select the **Schedule Driven** option.

   The **Expression** area refreshes, showing a set of controls on the right.

2 Choose the schedule during which you want the derived metric to be triggered.

   Click **Schedule** and select a schedule from the list that appears.

   Note The list shows all schedules that exist in vFoglight. For information on how to add or remove schedules, see Chapter 8, "Using Schedules" on page 395.

3 Select the trigger timing option to specify the point in time in which vFoglight evaluates the derived metric in relation with the newly-specified schedule.

   Click **Trigger Timing** and select one of the following options from the list that appears:

• **Enter and Exit**
• **Enter only**
• **Exit only**

4 To enable the trigger without data, select the **Enable Trigger without Data** check box.

5 Save your changes.

To assign a time -driven trigger:

Note This procedure continues from "Adding calculations to derived metrics" on page 344.

---

1 In the **Expression** area, under **Trigger Type**, select the **Schedule Driven** option.

The **Expression** area refreshes, showing a set of controls on the right.

2 Specify the recurrence interval for the trigger in the *hh:mm:ss* format.

3 To enable the trigger without data, select the **Enable Trigger without Data** check box.

4 Save your changes.

To assign a data -driven trigger:

Note This procedure continues from "Adding calculations to derived metrics" on page 344.

---

1 In the **Expression** area, under **Trigger Type**, select the **Data Driven** option.

2 Save your changes.

From here, you can proceed to "Setting the value type" on page 350.

Setting the value type

Once you define the scope and trigger of the derived metric, you can specify the value type for the derived metric. The value type for a derived metric dictates the appearance of the derived metric. You can set the derived type to a metric, and specify its unit of measurement, or to an observation.

To set the value type for a derived metric:

Note   This procedure continues from "" on page 348.

---

1   In the area immediately below the **Derived Metric Calculations** list, click **Value Type** and select **Metric** from the list that appears.

2   Select the units of measurement.

   Use one or both of the **Unit** boxes on the left of **Unit Type** as required.

   For example, **percent** or **count / second**.

   Note   You cannot change the value type of a derived metric unless you also change the name of the derived metric.

   You can change the unit of measurement for a derived metric, but only to a compatible unit. For example, you could change the unit from **megabyte** to **kilobyte**, but you could not change it from **megabyte** to **percent** without also changing the name of the derived metric.

To set the value type to an observation:

Note   This procedure continues from "" on page 348.

---

1   In the area immediately below the **Derived Metric Calculations** list, ensure that both of the **Unit** boxes are blank.

2   Specify the observation that you want to use as the value type for the derived metric.

   Click **Value Type** on the right and select an observation from the list that appears.

3   **Optional**. Add comments about the value type.

   Type your comments in the **Comments** box.

4   Save your changes.

   Click **Add** (when creating a new derived metric) or **Save** (when editing an existing metric).

Example: Creating and Managing Multiple Rules with the Same Scope

If you need to create multiple rules that are scoped to the same topology type and that use the same metric expressions in their conditions, you can make the process of

creating rules simpler and more efficient by creating a derived metric scoped to the same topology type and using it in these rules' conditions. See "Examples" on page 490 for an example.

In addition, creating a derived metric could help you manage these rules. For example, if the metric expression used in the rules' conditions needed to be calculated differently, you could simply edit the expression for the derived metric instead of editing multiple conditions.

Example: Using a Single Derivation with Multiple Scoping or Multiple Derivations

Derivation definitions will allow multiple scoping query/expression pairs under a single definition. For each topology object, the expression paired with the first scoping query which matches the object will be calculated. This allows you to override a derivation definition based on the scoping query where multiple derivations definitions exist.

Use the following guidelines to decide when to use one derivation with multiple scopes, or when to use multiple derivation definitions:

- Choose a single derivation definition when you need the overriding behavior. If you have a subset of a topology object type that requires a derivation to be calculated differently, use a single derivation definition with additional scope/expression pairs.
For example, you have a derivation `freeMemory` for topology type `OS`, with a subtype `Unix` that requires a different `freeMemory` calculation. Define a single derivation `freeMemory` create two scope/expression pairs (one for `OS` and the other for `Unix`).

- Choose a multiple derivation definition when you are using the same observation name for unrelated scoping queries.
For example, if you have a derivation `freeMemory` for the types `OS` and `JVM`, create two separate derivations to avoid coupling the definitions.

- Choose multiple derivation definitions when you have alternate ways of calculating the same observation for the same topology objects. If you keep the calculations in the same derivation definition, only the first calculation in the list will take affect.

Example: Optimizing Performance

Derived metrics can also help you optimize performance by reducing the number of calculations that need to be performed at run-time. For example, if there are multiple rules that need to use the same complex metric expression in their conditions, creating a derived metric with this expression and using it in these rules' conditions would have a positive impact on performance: the calculation specified in the metric expression would only need to be performed each time an instance of the derived metric is created instead of each time the rule is evaluated.

Working with Thresholds

Threshold levels in metrics are useful in situations when you need to reference a specific metric value multiple times, for example in derived metrics or rules.

You create new thresholds metrics and manage the existing ones using the dashboards that come with the Administration module. For complete information, see the following sections:

- "Managing Thresholds" on page 353
- "Creating Thresholds" on page 361
- "Defining Thresholds" on page 362

Managing Thresholds

The Manage Threshold dashboard allows you to create new registry variables, assign values to registry variables, and manage registry variables. For complete information, see the following sections:

- "Accessing the Manage Thresholds dashboard" on page 353
- "Editing threshold permissions" on page 355
- "Deleting thresholds" on page 359
- "Viewing and editing thresholds" on page 360

Accessing the Manage Thresholds dashboard

The Manage Thresholds dashboard includes a list of the thresholds that exist in your monitoring environment and includes mechanisms for adding and deleting thresholds.

To access the Manage Thresholds dashboard:
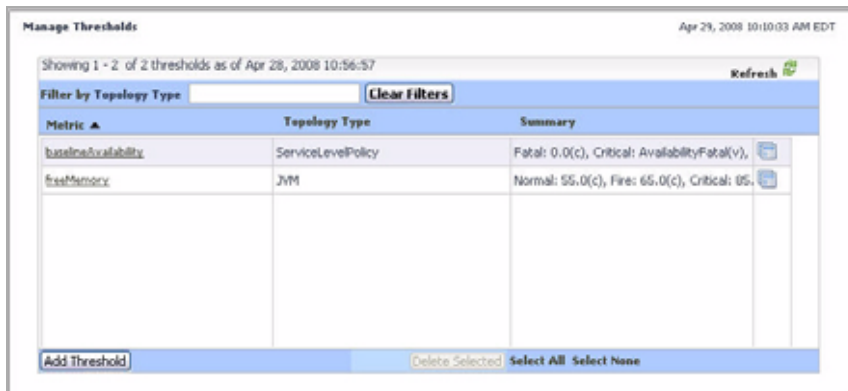
Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

1 Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▸ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Data > Manage Thresholds**.

   The Manage Thresholds dashboard appears in the display area.

3 To sort the list of thresholds by the metric in which they are defined or the topology type that is used to define the metric, click the **Metric** or **Topology Type** column headings as required.
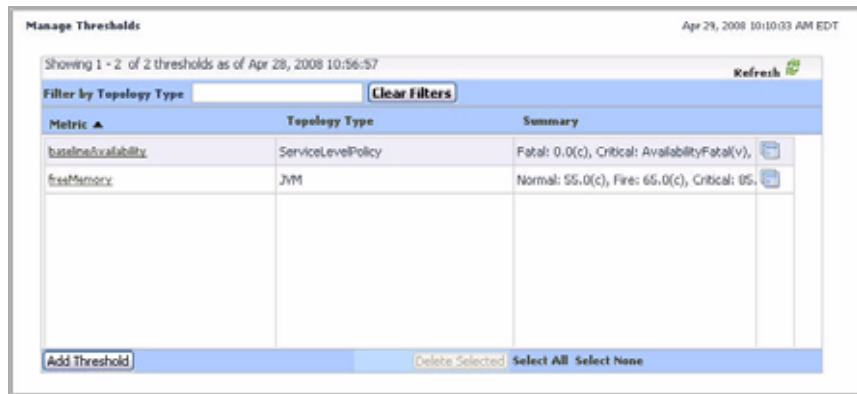
4 **Optional**. Filter the list of thresholds using the topology type as the filter.

   In the **Topology Type** box at the top, type the name of the topology type.

   The Manage Thresholds dashboard refreshes, showing only the thresholds that are defined for the specified topology type.

   To clear the filter, click **Clear Filters**.

   The Manage Thresholds dashboard refreshes, showing the list of all thresholds.

From here, you can proceed to any of the following procedures:

- "Editing threshold permissions" on page 355
- "Deleting thresholds" on page 359
- "Viewing and editing thresholds" on page 360

Editing threshold permissions

vFoglight allows you to control access to thresholds. For each threshold you can grant
or deny read, write, or control access to roles or users. For more information about
security concepts in vFoglight, see Chapter 3, "Managing Users and Security" on
page 105.

vFoglight employs the following behavior when it comes to threshold permissions:

- If no one has a permission to the threshold, everyone has a permission.
- If one has a permission to the threshold, others with undefined permission do not
  have any permission.
- Final permission is based on a combination of the role, user, and threshold
  defined on the server side.

Use the Edit Permissions for Threshold button ( ) on the Manage Thresholds
dashboard to navigate to the Edit Permissions for Threshold area, that allows you to add
or edit permissions to roles and users, as outlined below. The Edit Permissions for
Threshold area contains two tables that show the permissions for each vFoglight user or
role.

Permission granted
Permission denied
Permissions not assigned
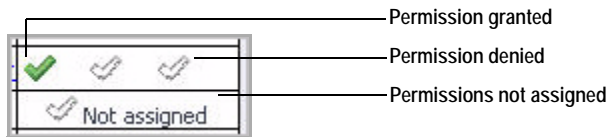
To add permissions for a threshold:

Note   This procedure continues from "Accessing the Manage Thresholds dashboard" on page 353.

  1 In the Manage Thresholds dashboard, in the row containing the variable whose permissions you want to edit, click the Edit Permissions for Threshold button ( ).

The Edit Permissions for Threshold area appears in the Manage Thresholds dashboard.

2 To add permissions to a threshold, complete the following steps.

    a Click the role or user to which you want to assign permissions.

        Tip The Not Assigned icons in the **Permissions** columns indicate that the role does not have permissions assigned to it.

    The **Add Role Permission** or **Add User Permission** dialog box appears.

Add Role Permission
Role Name: Advanced Operator
☑ Read
☑ Write
☑ Control
[Save] [Cancel]

Add User Permission
User Name: demo
☑ Read
☑ Write
☑ Control
[Save] [Cancel]

b In the dialog box that appears, use the **Read**, **Write**, and **Control** check boxes to assign permissions as required, and click **Save**.

The dialog box closes and the selected entry refreshes, showing three check marks in the **Permission** columns, one for each of the read, write, and control permissions.

Permission granted

Permission denied

3 To edit or delete permissions for a threshold, complete the following steps.

a Click the role or user whose permissions you want to edit.

Tip Three check marks in the **Permissions** columns indicate that the role already has permissions assigned to it.

The **Edit Role Permission** or **Edit User Permission** dialog box appears.

b To edit the permissions, ensure that the **Edit** option is selected and use the **Read**, **Write**, and **Control** check boxes as required.

c To delete the permissions, select the **Delete** option

d Click **Save**.

The dialog box closes and the selected entry refreshes, showing the newly-edited permissions.

Deleting thresholds

Use the Delete Selected button on the Manage Thresholds dashboard to delete a threshold, as outlined below.

Note   When a threshold is deleted, all references to that threshold in rule conditions or derived metric expressions become invalid. This may cause a rule to fail to evaluate. If this occurs, you must manually modify the rule condition or expression.

To delete a threshold:

Note   This procedure continues from "" on .

---

1 In the Manage Thresholds dashboard, select the row containing the threshold that you want to delete.

2 Click the **Delete Selected** button at the bottom.

The **Delete Threshold** dialog box appears.

Delete Threshold

Are you sure you want to delete thresholds defined for the following "metric / topology type"?

freeMemory / JVM

OK   Cancel
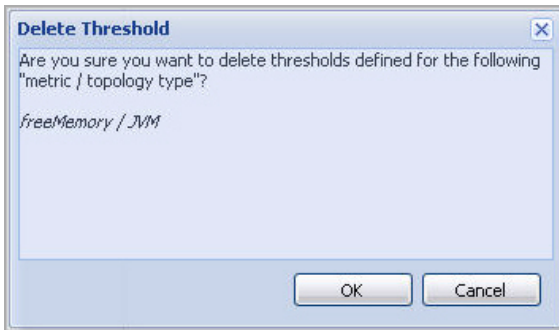
3 In the **Delete Threshold** dialog box, click **OK**.

The **Delete Threshold** dialog box closes.

4 Observe the Manage Thresholds dashboard.

The newly-deleted threshold no longer appears in the list.

Viewing and editing thresholds

To view or edit a threshold:

Note   This procedure continues from "Accessing the Manage Thresholds dashboard" on page 353.

---

1 In the Manage Thresholds dashboard, click the **Metric** column of the row containing the threshold whose definitions you want to view.

The **Edit Threshold** view appears in the Manage Thresholds dashboard.
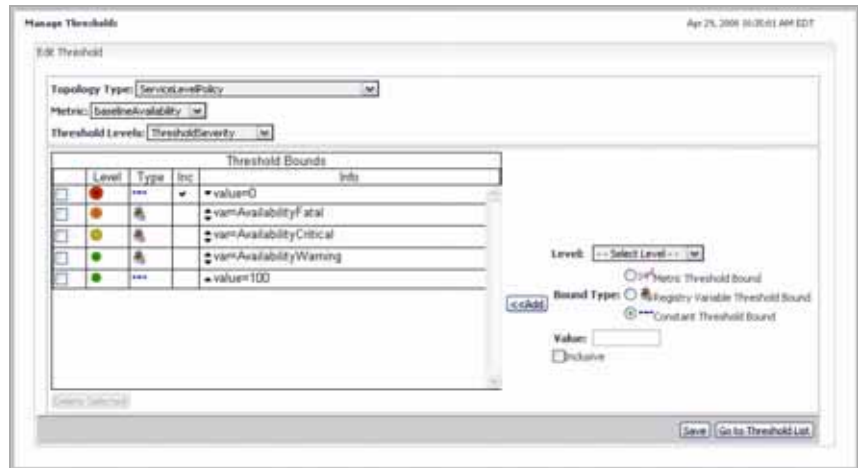
2 Observe the threshold definitions.

3 Edit the threshold as required.

For complete instructions, see "Adding bounds to metric threshold levels" on page 364.

Creating Thresholds

You can add new thresholds to vFoglight using the Create Threshold dashboard. You can access this dashboard from the navigation panel, or through the Manage Thresholds dashboard.

To create a threshold:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---
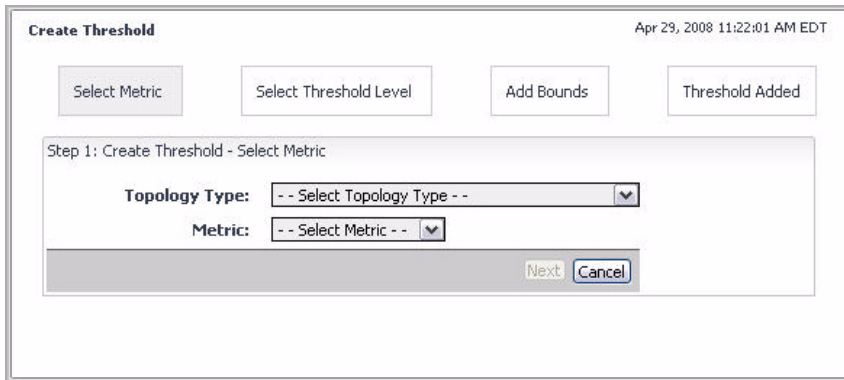
1 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2 Open the Create Threshold dashboard by completing one of the following steps:

• On the navigation panel, under **Dashboards**, choose **Administration > Data > Manage Thresholds**.

In the Manage Thresholds dashboard that appears in the display area, click the **Add Threshold** button in the lower-left corner.

or

- On the navigation panel, under **Dashboards**, choose **Administration > Data > Create Threshold**.

The Create Threshold dashboard appears in the display area.

From here, you can proceed to "Defining Thresholds" on page 362.

Defining Thresholds

Defining thresholds involves several steps. Once you get started with threshold creation, you need to select the topology type and the metrics using that type for which you want to define thresholds. Furthermore, you need to specify threshold levels and bounds, and finally, view the threshold summary.

For instructions, see the following sections:

- "Selecting metrics and threshold levels" on page 363
- "Adding bounds to metric threshold levels" on page 364

Selecting metrics and threshold levels

To select a metric and its threshold level:

Note   This procedure continues from "" on page 361.

---

1   Choose the topology type of the metric whose thresholds you want to set.
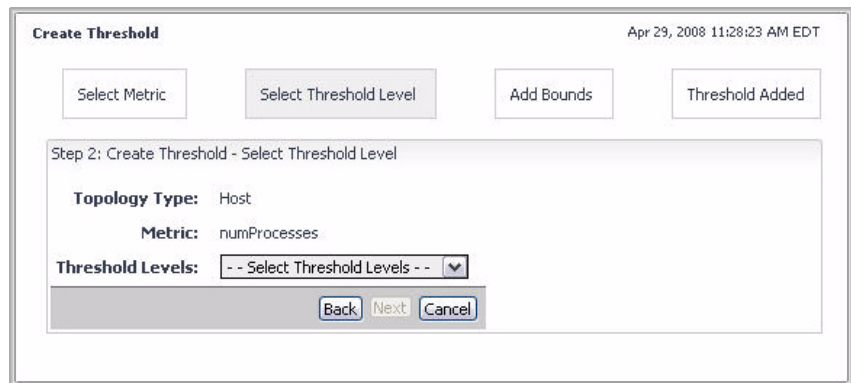
In the Create Threshold dashboard, in the **Step 1: Create Threshold - Select Metric** area, click **Topology Type** and select the topology type from the list that appears.

2   Choose the metric whose thresholds you want to set.

Click **Metric** and select the metric from the list that appears.

3   Click **Next**.

The **Step 2: Create Threshold - Select Threshold Level** area appears in the Create Threshold dashboard.

In the **Step 2: Create Threshold - Select Threshold Level** area, click Threshold Levels and choose one of the following predefined threshold levels:

- **AgentHealthState**
- **AgentState**
- **AlarmChangeType**
- **AlarmSeverity**
- **CatalystServiceState**

- **ThresholdSeverity**

4 Click **Next**.

The **Step 3: Create Threshold - Add Bounds** area appears in the Create Threshold dashboard.
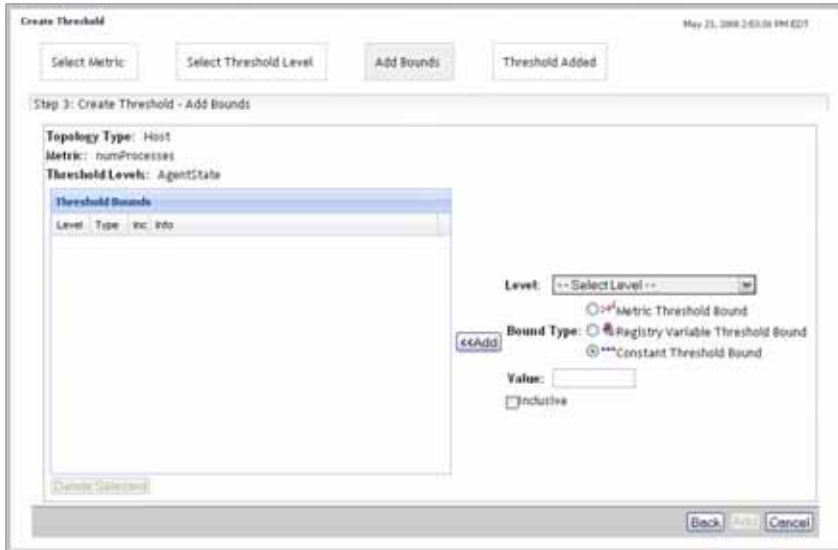
From here, you can proceed to "Adding bounds to metric threshold levels" on page 364.

Adding bounds to metric threshold levels

A metric threshold level can have a number of different levels one or more of sub-levels, as listed in the following table:

Threshold Level	Threshold Sub-Level
AgentHealthState	OK
	Running Unexpectedly
	Broken
	Agent Info Not Present

Threshold Level	Threshold Sub-Level
AgentState	Unknown
	Stopped
	Starting
	Stopping
	Running
	Collecting data
	Running but not collecting data
AlarmChangeType	Fire
	Clear
	Acknowledge
AlarmSeverity	Undefined
	Normal
	Fire
	Warning
	Critical
	Fatal

Threshold Level	Threshold Sub-Level
CatalystServiceState	Stopped
	Stopping
	Starting
	Started
	Failed
	Destroyed
	Created
	Unregistered
	Registered
ThresholdSeverity	Normal
	Critical
	Fatal

You can have one or more threshold bounds in a threshold level. There are three different types of threshold bounds:

- *Metric Threshold Bound*. Severity level is bound to another metric.
- *Registry Variable Threshold Bound*. Severity level is bound to a registry variable.
- *Constant Threshold Bound*. Severity level is bound to a fixed value.

The vFoglight Management Server evaluates threshold bounds in the order that they are listed, starting with the first one. Changing their order affects the output of actions that are associated with those threshold levels.

For example, if a threshold level includes several threshold bounds that reference standard vFoglight severity levels in the ascending order such as Normal, Warning, Critical, and Fatal, and you change their order in the list to Normal, Critical, Warning, and Fatal, the Warning, the bound that is associated with the Warning level evaluates to True only after the evaluation of the Critical level.

To bind a threshold level to a metric:

---

1   Select the severity type of the threshold level.

Click **Level** and select a threshold level from the list that appears.

2   Select the **Metric Threshold Bound** option.

The display area refreshes, showing a set of controls that allow you to define the metric to which you want to bind the severity level.

3   Click **Metric** and select a metric from the list that appears.

4   **Optional**. Specify the standard deviation from the value that the selected metric contains.

In the **Number of Standard Deviation** box, type the standard deviation.

5   If you want vFoglight to acknowledge that the threshold is reached when the threshold level exceeds the value of the binding metric, ensure that the **Inclusive** check box is cleared.

If you want vFoglight to acknowledge that the threshold is reached when the threshold level reaches the value of the binding metric, check the **Inclusive** check box.

6   Click the **Add** button on the right of the **Bound Type** options.

The newly-created metric threshold bound appears in the **Threshold Bounds** table.

To bind a threshold level to a registry variable:

Note   This procedure continues from "Selecting metrics and threshold levels" on page 363 or
"Viewing and editing thresholds" on page 360.
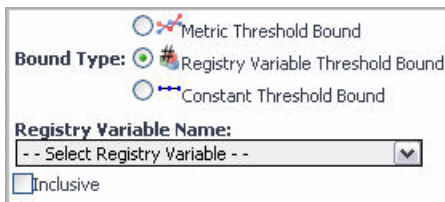
---

  1 Select the severity type of the threshold level.

       Click **Level** and select a severity level from the list that appears.

  2 Select the **Registry Variable Threshold Bound** option.

       The **Registry Variable Name** box appears below the **Bound Type** options,
allowing you to specify the registry variable to which you want to bind the
severity level.

  3 Click **Registry Variable Name** and select a variable from the list that appears.

  4 If you want vFoglight to acknowledge that the threshold is reached when the
threshold level exceeds the value of the binding registry variable, ensure that the
Inclusive check box is cleared.

       If you want vFoglight to acknowledge that the threshold is reached when the
threshold level reaches the value of the binding registry variable, check the
Inclusive check box.

  5 Click the **Add** button on the right of the **Bound Type** options.

The newly-created registry variable threshold bound appears in the **Threshold Bounds** table.

To bind a threshold level to a constant value:

---

1 Select the severity type of the threshold level.

   Click **Level** and select a severity level from the list that appears.

2 Select the **Constant Threshold Bound** option.

   The **Value** box appears below the **Bound Type** options, allowing you to specify the constant value to which you want to bind the severity level

   .

3 Specify the value to which you want to bind the threshold level.

   In the **Value** box, type that value. This can be a positive or a negative value, depending on the metric range.

4 If you want the vFoglight to acknowledge that the threshold is reached when the threshold level exceeds the value of the binding registry variable, ensure that the **Inclusive** check box is cleared.

If you want vFoglight to acknowledge that the threshold is reached when the threshold level reaches the value of the binding registry variable, check the **Inclusive** check box.

5   Click the **Add** button on the right of the **Bound Type** options.

The newly-created registry variable threshold bound appears in the **Threshold Bounds** table.

Threshold Bounds			
Level	Type	Inc	Info
Collecting data	←→		value=85

To save your changes:

Note   This procedure continues from any of the following sections:

---

1   Ensure that the order of the bounds in the threshold bounds is valid.

Caution   The vFoglight Management Server evaluates threshold bounds in the order that they are listed, starting with the first one. Changing their order affects the output of actions that are associated with that threshold level.

To move a threshold bound up or down, in the **Threshold Bounds** table, in the **Info** column, use the Move up this bound (▲) or Move down this bound (▼) buttons as required.

2   Complete one of the following steps:

- **Existing thresholds.** Click **Save**.

   A list appears in the display area, showing the newly-added threshold bounds for the selected threshold level.
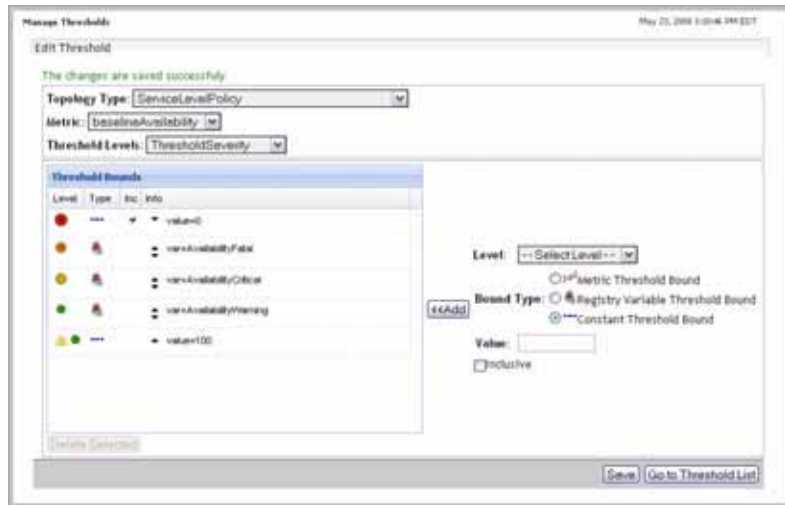
or

• **New thresholds.** Click **Add**.

A list appears in the display area, showing the threshold bounds for the selected threshold level.
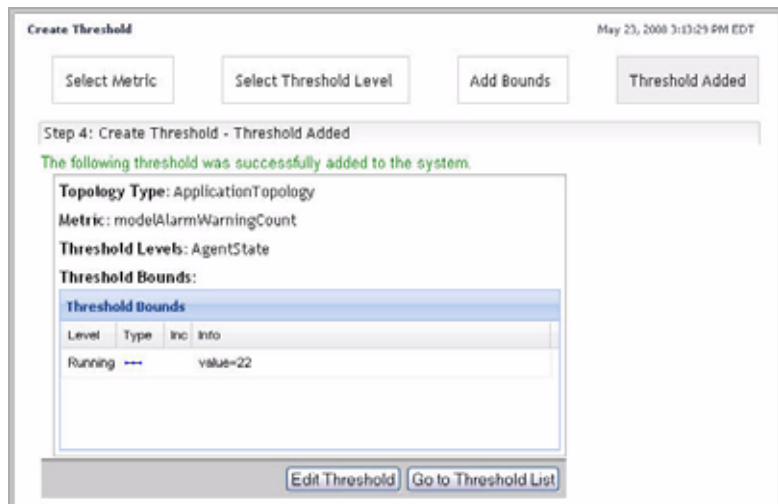
Observe the Manage Thresholds dashboard.

The newly-added threshold appears in the list.

Managing Retention Policies

Topology is a representation of—and a way of understanding—the logical and physical relationship between items in your monitored environment. At run-time, vFoglight dynamically builds topology models using the monitoring data about your system that is collected by vFoglight agents. A model is a set of objects and relationships designed to represent a monitored resource and its parts. vFoglight models retain collected data and transform it into nodes, adding configuration data to each node as properties, and attaching metric data to appropriate nodes as metrics. Topology models provide the context for the metrics sent by the agents to the vFoglight Management Server.

Retention policies allow you to define time periods where monitoring data can be sampled, aggregated, or purged from your system. All topology objects in vFoglight form a hierarchy whose root is the super-type `TopologyObject`. Retention policies are inherited from the object's type. These policies may be overwritten, in which case the modification applies to all child types in the hierarchy.

In addition to retention policies, the collected data has additional life-cycle properties that are defined in the `storage-config.xml` file that is located in the directory *<vfoglight_home>/config*. For example, according to the default retention policy for `TopologyObject`, all data is rolled up to 15 minute periods after the age of 15 minutes, then rolled up to one-hour periods after the age of four hours, and finally rolled up to four-hour periods after the age of five days. Furthermore, the default settings in `storage-config.xml` dictate that the 15-minute interval data is kept for three days and is converted to one-hour interval data, while one-hour interval data is kept for two weeks and then converted to four-hour interval data.

If there is no existing retention policy for a topology type, that type inherits the retention policy from its parent type. If no policies exist within the entire hierarchy, the type inherits the policy from the `TopologyObject` type. Conversely, setting a retention policy for a topology type completely overwrites any policy it inherits from a super-type, and is applied to all sub-types of that topology type. For an example of how to configure a retention policy in cases where data storage is limited, see "Example: Addressing Data Storage Concerns" on page 390

You create new retention policies and manage the existing ones using the Manage Retention Policies dashboard. For complete information, see the following sections:

About Retention Policy Mechanisms

While it is theoretically possible to create any retention policy that you desire in vFoglight, the design of the system constrains the easy-to-accomplish retention policies to a narrow range of options. Specifically, the database design of vFoglight provides a structure that is capable of holding data in three different buckets, called generations, that are defined in *<vfoglight_home>/config/storage-config.xml*. Each generation has a predefined period of time in which it retains data. Without modification to the generations, there are specific rules that must be followed when assigning retention policies to ensure that you get the results you are expecting.

This section provides information on the key mechanisms involved in retention policies and rules for defining retention policies that work effectively with the default database configuration.

For complete information, see the following sections:

About database generations

Generations refer to the database structures that hold long-term data. For any given metric, each generation can hold one aggregation level of data (for example, raw, hourly averages, 4 hour averages, and so on). Out of the box, there are three generations, each holding data for:

• *Generation 1*: Data for 0 – 3 days

• *Generation 2*: Data for 3 – 14 days

- *Generation 3*: Indefinite

Because data is constrained to those buckets, retention policies must are also constrained to a set of rules. In general, you can create retention policies that:

- Have 3 retention policies (including a purge), where:
  - The first retention policy sets the granularity of data stored for 3 days in generation 1.
  - The second sets the granularity of data stored for 14 days in generation 2
  - The third sets the granularity of data that live indefinitely (until a purge) in generation 3
- Have 2 retention policies (including a purge), where:
  - The first retention policy sets the granularity of data stored for up to 14 days in generation 1 and/or generation 2
  - The second sets the granularity of data that live indefinitely (until a purge) in generation 3
- Have 1 retention policy (including a purge), where
  - The first retention policy sets the granularity of data that will live indefinitely (until a purge) in generation 1, 2 or 3.

How vFoglight populates database generations

Moving data from memory to the database

The data service periodically writes data from the short-term memory cache to generation 1. The frequency by which data are written is defined in the first retention policy (for more information, see "How retention policies interact with database generations" on page 375). This interval should not exceed 15 minutes to prevent the vFoglight Management Server memory from growing too large.

Database roll-ups

A nightly roll-up job aggregates data and writes those data to generations 2 and 3. The roll-up is only done once daily, according to the time set in the Daily Database Maintenance schedule. For more information about schedules in vFoglight, see Chapter 8, "Using Schedules".

How retention policies interact with database generations

Both mechanisms for populating the repository (from memory to the database, database roll-ups) use the retention policies defined in the Retention Policies Dashboard as the guidelines for how they store data.

A retention policy is the set of definitions, for a given object, that indicate how data is stored. Each definition within a policy contains two parameters:

- *Age*: Specifies the age at which the data is eligible for a roll-up
- *Roll-up period*: Specifies the period of time over which the data is aggregated

Policies can be set at an object level; however, retention policies also adhere to the object inheritance capabilities. If a policy has not been explicitly assigned to an object, it inherits a value from a higher level in the model. The top-level object is TopologyObject.

The policy that is applied to TopologyObject, and therefore any object which does not have explicitly assigned policies, is as follows:

Policy		**Translates to**
Age	15 minutes	After 15 minutes, store 15 minute average data to Generation 1 (where they are stored for three days)
Roll-up	15 minutes	
Age	4 hours	Data older than four hours is eligible for roll-up (they are actually only rolled up once a day during the database roll-up) to one-hour averages and persisted into Generation 2 (where they are stored for 14 days)
Roll-up	1 hour	
Age	5 days	Data older than 5 days old is eligible for Roll-up (they are actually only rolled up once per day during the database roll-up) to four-hour averages and persisted into Generation 3 indefinitely
Roll-up	4 hours	

The illustration below shows the interaction between the TopologyObject retention policy and the default generation definitions.
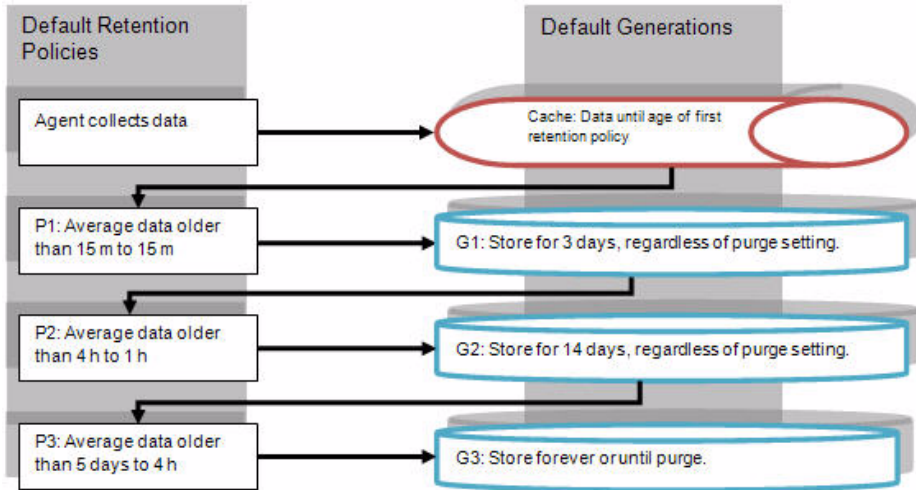
Individual cartridges frequently have their own policies which must be examined on individual object level to understand that retention policy behavior.

Developing a retention policy: Example

While the browser interface does not prevent you from setting policies that are in conflict with the generations, setting policies that are outside of these boundaries does not yield the expected results. Instead, the retention policy engine find the most optimal scheme for your data (ensuring that the lowest granularity is written to Generation 1 and that longest duration data are written to Generation 3).

The table shows how to configure retention policies, at 1, 2 or 3 levels of aggregation, following the specifications below.

	Acceptable age values	Acceptable roll-up values	Explanation
Three-level policy (including a purge)			
Level 1	<= 15 minutes	<= 15 minutes	Data is persisted at the roll-up interval defined in the Level 1 policy for three days.

	Acceptable age values	**Acceptable roll-up values**	**Explanation**
Level 2	> 15 minutes and < 3 days	Any roll-up greater than Level 1	The age date for the Level 2 policy must be less than or equal to three days. Data is persisted at the roll-up interval defined in the Level 2 policy for 14 days.
Level 3	> Level 2 setting and < 14 days	Any roll-up greater than Level 2	The age date for the Level 3 policy must be less than or equal to 14 days. Data is persisted at this roll-up interval indefinitely. A purge policy defines a minimum length of time that data must persist before it is truncated.
Purge Policy	> Level 3 setting	Purge	Data is never purged from the system before the age value of the purge policy. Data may, however, be retained for longer than the setting as the system waits to find an acceptable time to purge data.

Two-level policy (including a purge)

	Acceptable age values	**Acceptable roll-up values**	**Explanation**
Level 1	<= 15 minutes	<= 15 minutes	Data is persisted at the roll-up interval defined in the Level 1 policy for either three or 14 days, depending on the age of the Level 2 setting. If the age of the Level 2 setting is less than or equal to three days, then the data is persisted for three days. If the age of the Level 2 setting is between three and 14 days, the data is persisted for 14 days.

	Acceptable age values	**Acceptable roll-up values**	**Explanation**
Level 2	<= 14 days	Any roll-up greater than Level 1	The age date for the Level 2 policy must be less than or equal to 14 days. Data is persisted at this roll-up interval indefinitely. A purge policy defines a minimum length of time that data must persist before it is truncated.
Purge Policy	> Level 2 setting	Purge	Data is never purged from the system before the age value of the purge policy. Data may, however, be retained for longer than the setting as the system waits to find an acceptable time to purge data.

One-level policy (including a purge)

Level 1	<= 15 minutes	<= 15 minutes	Data is persisted at the roll-up interval defined in the Level 1 policy indefinitely. A purge policy will define a minimum length of time that data must persist before it is truncated.
Purge Policy	> 15 minutes	Purge	Data is never purged from the system before the age value of the purge policy. Data may, however, be retained for longer than the setting as the system waits to find an acceptable time to purge data.

Accessing the Manage Retention Policies Dashboard

Use the Manage Retention Policies dashboard to create and edit retention policies for topology types and properties of topology types. Each policy specifies one or more time periods after which data is rolled up and the granularity of the roll-up.

In the Manage Retention Policies dashboard, the Age column specifies the amount of time allotted for data collection. The Roll-up Period defines the granularity of the collection period. For example, if Age is defined as one minute, and the Roll-up Period is defined as five minutes, any data older than one minute is eligible to be aggregated into the five-minute roll-up period.

Caution   The first period in the retention policy specifies the aggregation that is performed before the raw data is persisted. Therefore, the Age determines how long raw samples remain in memory before being persisted. In order to constrain the server's memory usage, the Age specified for the first roll up period should not be too large. Settings larger than 30 minutes should be carefully considered.

Caution   The Roll-up Period of the first retention policy period determines the amount of the initial aggregation. If you do not want any aggregation to be performed, this can be set to 0 ms. If not set to zero, this setting should not be too small, as it increases the amount of processing performed by the server. A setting smaller than 30 seconds should be carefully considered.

For metrics, the aggregation retains the count, minimum, maximum, sum, average, and standard deviation of the aggregated values. For other observation types, aggregation is a sampling process that retains the latest value per time slice.

The default roll-up period is 15 minutes; therefore any raw data older than 15 minutes is rolled up to the next period.

To access the Manage Retention Policies dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▸ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Data > Manage Retention Policies**.

   The Manage Retention Policies dashboard appears in the display area.

3 To sort the list of retention policies by the topology type to which they apply, click the **Topology Type - Property Name** column heading as required.

4 **Optional**. Filter the retention policies by the subset of topology types for any installed cartridges in your monitoring environment. Use this filter to search for, isolate, and apply policies on the basis of each individual case.

In the **Filter** area, click **By Cartridge** and select the cartridge from the list that appears.

The Manage Retention Policies dashboard refreshes, showing only those topology types that exist in the specified cartridge.

Example. If you have the OS Cartridge installed and you want to look up the retention policy for the `Windows_System_Top_CPU_Table`, use the agent name, `OS-Windows_System`, as the filter.

The list of topology types refreshes, showing the tables that come with the selected agent, including the `Windows_System_Top_CPU_Table`.

From here, you can proceed to any of the following procedures:

- "Deleting Retention Policies" on page 381
- "Viewing the Hierarchy of Topology Types in the Database Schema" on page 383
- "Editing Retention Policies" on page 386
- "Creating Retention Policies" on page 388

Deleting Retention Policies

Use the Delete Selected button on the Manage Retention Policies dashboard to delete the retention policy associated with a particular topology object, as outlined below.

To delete a retention policy:

> **Note** This procedure continues from "Accessing the Manage Retention Policies Dashboard" on page 378.

1 In the Manage Retention Policies dashboard, in the row containing the topology type whose retention policies you want to delete, select the check box on the left of the **Topology Type - Property Name** column.

2 Click the **Delete Selected** button at the bottom.

Your Web browser displays a dialog box that allows you to proceed or with or cancel the delete operation.

> **Note** The appearance of the above dialog may be different, depending on the type and version of your Web browser.

3 Confirm the delete operation.

4 Observe the Manage Retention Policies dashboard.

The newly-deleted retention policies no longer appears in the list.

Viewing the Hierarchy of Topology Types in the Database Schema

Before you get started with editing retention policies, you need to identify the correct topology type whose retention policies you want to edit. When you set a retention policy for a topology type, the ancestors of that topology type inherit the newly-set retention policy. It is therefore important to identify the ancestors of the topology type before editing its retention policies.

The Manage Retention Policies dashboard lists all of the available topology types that exists in the database schema and their properties but does not provide information on their position in the schema, such as their ancestors, descendants, or object instances. To identify the ancestors of a particular topology type, use the Schema Browser dashboard. In addition to topology type ancestors, the Schema Browser dashboard can show the properties, descendants, and instances for each topology type. For complete information about the Schema Browser dashboard, see the *vFoglight User Guide*.
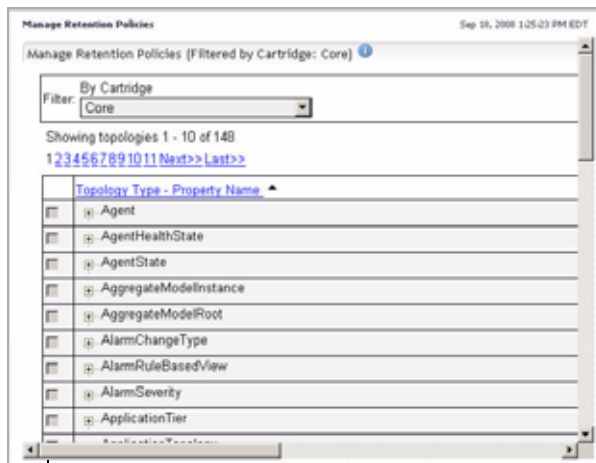
List of topology types in the Manage Retention Policies Dashboard
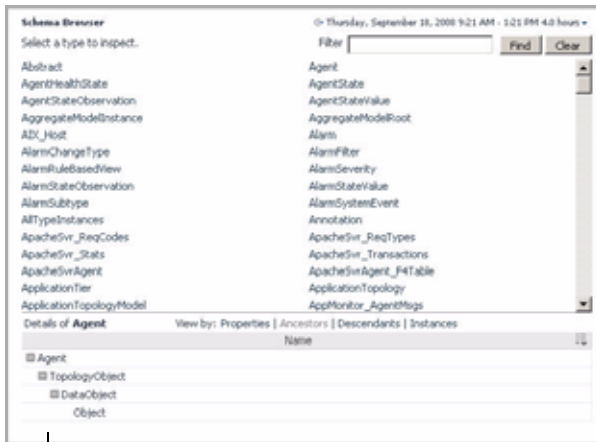
Ancestors of a topology type in the Schema Browser

To view the hierarchy of a topology type:

    1 Ensure that the navigation panel is open.

       To open the navigation panel, click the right-facing arrow ▶ on the left.

    2 On the navigation panel, under **Dashboards**, choose **vFoglight > Schema > Schema Browser**.

       The Schema Browser dashboard appears in the display area, and the Schema Selector appears in the navigation panes
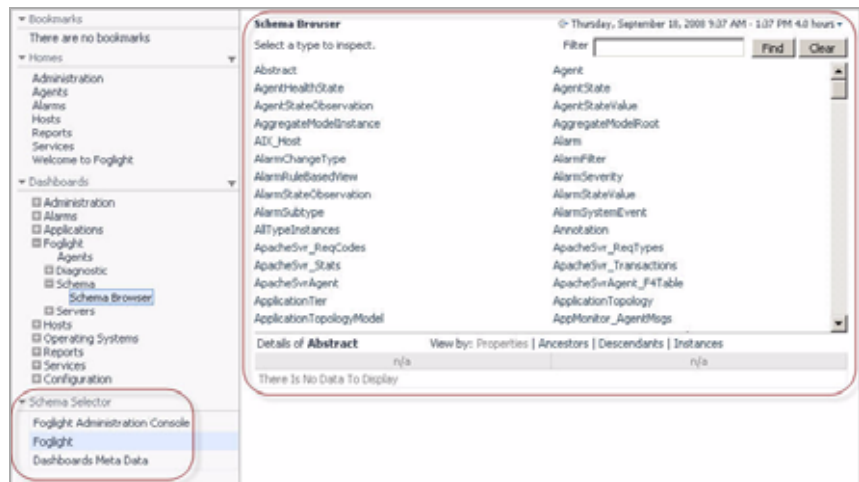
3 Ensure that the Schema Browser shows the core topology types.

On the navigation panel, under **Schema Selector**, verify if the **vFoglight** entry is selected.
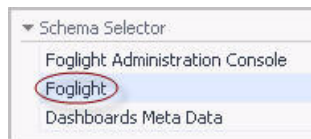
4 Observe the list of topology types that appear in the Schema Browser dashboard.

5 Select a topology type in the upper pane of the Schema Browser and review its details in the lower pane.

For example, to look at the details of the Alarm topology type, in the list appearing in the upper pane, click the **Alarm** entry.

The lower pane shows the details of the Alarm topology type.

Details of **Alarm**	View by: Properties | Ancestors | Descendants | Instances
Name	**Type Name**
uniqueId	String
sourceID	String
sourceName	String
ruleId	String
ruleName	String
createdByLocalRule	Boolean
severity	AlarmSeverity
topologyObject	TopologyObject
message	String

To find out the ancestors of the selected topology type, at the top of the lower pane, on the right of **View by**, click **Ancestors**.

The lower pane refreshes, showing the ancestors of the selected topology types.

Details of **Alarm**	View by: Properties | Ancestors | Descendants | Instances
Name	
⊟ Alarm	
⊟ DataObject	
Object	

When you find out the hierarchy of the topology type whose retention policies you want to edit, you can proceed to "Editing Retention Policies" on page 386. For additional complete information about the Schema Browser dashboard, see the *vFoglight User Guide*.

Editing Retention Policies

The Manage Retention Policies dashboard allows you to edit an existing retention policy period. The following example shows how you can edit the super-type TopologyObject to change the default retention policies for all observations in your system.

Note   If the retention policy is inherited from another policy, you have to click the topology type to invoke the *Edit* Reten*tion Policy Period* dialog. Use the mouse to roll over the period listings to see if the policy is inherited, and from which Topology Type the policy is inherited.

To edit the default retention policy period:
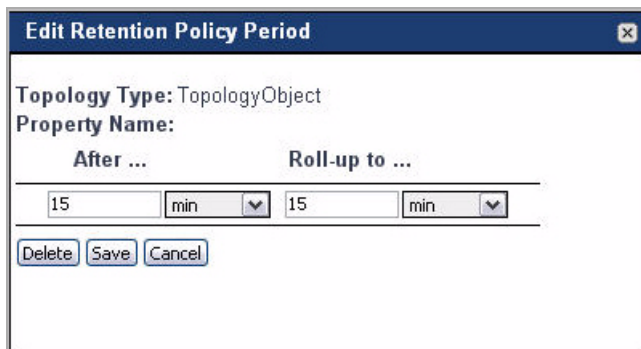
1 In the Manage Retention Policies dashboard, locate the TopologyObject type.

2 Review the default retention policies for the TopologyObject type.

Expand the **TopologyObject** node to see the default policy periods.

A set of policies appears under the **TopologyObject** node.

TopologyObject		
	15min	15min
	4hours	1hours
	5days	4hours

3 Edit the age of a retention policy period.

Choose a period and click its **Age** column.

The **Edit Retention Policy Period** dialog box appears.

4 Edit the existing data sampling period.

In the **Edit Retention Policy Period** dialog box, in the **After** column, specify the duration and the measurement unit of the data sampling period. For example: 16 min.

5 Edit the existing roll-up period or configure the retention policy to purge the data.

In the **Roll-up to** column, specify the duration and the measurement unit of the roll-up period. For example: 1 hour.

If you want the data to purge after the retention period, click the box on the right and select **purge** from the list that appears.

6 Click **Save**.

The **Edit Retention Policy Period** dialog box closes and a message appears in the upper-left, indicating the success of the edit operation.
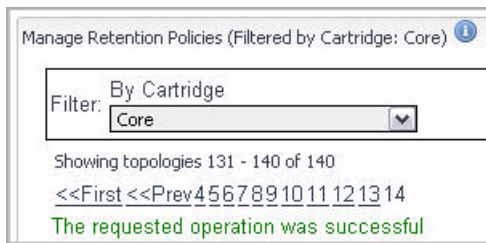
7 Observe the Manage Retention Policies dashboard.

The newly-edited retention and roll-up periods appear in the list.

Creating Retention Policies

You can create new retention policies for the topology types listed in the table on the Manage Retention Policies dashboard.

To create a retention policy:

Note This procedure continues from "Accessing the Manage Retention Policies Dashboard" on page 378.

---

1 In the Manage Retention Policies dashboard, click the topology type to which you want to assign a retention policy.

The **Add Retention Policy** dialog box appears.

2   Add a data sampling period.

In the **Add Retention Policy** dialog box, in the **After** column, specify the duration and the measurement unit of the data sampling period. For example: 20 min.

3   Add a roll-up period or configure the retention policy to purge the data.

In the **Roll-up to** column, specify the duration and the measurement unit of the roll-up period. For example: 1 hour.

If you want the data to purge after the retention period, click the box on the right and select **purge** from the list that appears.

4   To add another retention period, click the plus button ().

Another row appears in the table, allowing you to specify another set of data sampling and retention periods.

Specify the data sampling and roll-up or purging parameters periods for the newly-added retention period using the controls in the **After** and **Roll-up to** columns.

To delete a retention period from the table, use the red Delete button (⊗).

5 Click **Save**.

The **Edit Retention Policy Period** dialog box closes and a message appears in the upper-left, indicating the success of the edit operation.
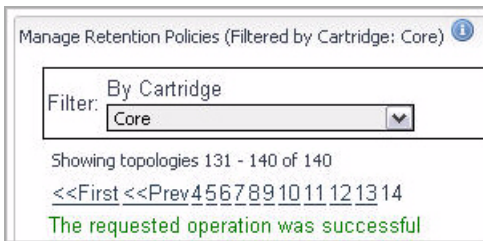
6 Observe the Manage Retention Policies dashboard.

The newly-edited data sampling and roll-up periods appear in the list.

Example: Addressing Data Storage Concerns

If you have data storage concerns, you may want to increase the default aggregation periods or purge times. For example, the following settings will create a large data set:

```
after 15 minutes - roll up to 15 minutes
after 1 year - purge
```

The following example uses a one-day granularity, and therefore a smaller data set is retained:

```
after 15 minutes - roll up to 15 minutes
after 1 week - roll up to 1 day
```

```
after 1 year - purge
```

Note	If the roll-up period is less than one day, the roll-up period must be a multiple of the previous roll-up period value.

Note	You cannot define two identical data sampling periods for the same topology type or property.

Enabling the Collection of Data with Older Timestamps

By default, the vFoglight Management Server accepts only the data that is collected within one hour from the moment it is received. The one-hour window allows the server to accept the data that agents collect during such short-term disruptions. When the connection with the server is lost, vFoglight agents continue to collect and store data from monitored hosts, and forward that data to the server when the connection is restored without any additional configuration of the agents or agent manager components.

This feature is useful in situations when an agent temporarily loses a connection with the server. However, in some situations, such as a longer-term network outage, you may need to increase the one-hour time window to prevent the vFoglight Management Server to discard the data with timestamps that are older than one hour.

The length of that time window can be controlled with a virtual machine (VM) option, `foglight.data_service.max_past_timestamp_delta`. Add this option to the configuration file *<vfoglight_home>/config/foglight.config* to change the length of the store-and-forward period in milliseconds.

Any data with older timestamps that is received and accepted by the vFoglight Management Server triggers data-driven rules and derived metrics. Time-driven rules do not re-evaluate data with older timestamps, even if that data meets their conditions and would cause them to fire if collected in real-time. For more information about rule triggers, see Chapter 6, "Triggering rules" on page 251.

To enable the collection of data with older timestamps:

1   On the computer on which the vFoglight Management Server is installed, locate the *<vfoglight_home>/config/foglight.config* file and open it for editing.

2   In the *foglight.config* file, locate the following line of code:

```
# Uncomment the following lines starting with option0 to
   adjust VM settings
```

Following the above line is a list of VM options, some of which may or may not be used. A default installation does not have any of the VM options set:

```
#
# foglight.vm.option0 = "";
# foglight.vm.option1 = "";
# ...
# foglight.vm.option99 = "";
#
```

3 Find an unused VM option and set it to a desired length in milliseconds.

   a Remove the comment marker from the beginning of the line.

   b Insert the `foglight.data_service.max_past_timestamp_delta` option and the length of the store and forward period between the quotation marks.

     For example, to set the store and forward period to 8 hours, you should set the `foglight.data_service.max_past_timestamp_delta` option to 28,800,000 milliseconds:

     8 hours = 8 hours * 60 minutes * 60 seconds * 1,000 = 28,800,000 milliseconds

  For example:

```
foglight.vm.option0="-Dfoglight.data_service.
    max_past_timestamp_delta=28800000";
```

4 Save your changes.

   Important In order for the changes to take effect, you need to restart the vFoglight Management Server.

8

Using Schedules

This chapter introduces you to vFoglight schedules and provides information on how to create and manage them. It contains the following sections:

Note   In order to complete each of the procedures in this chapter, your user account must belong to a group with the Administration role. For more information about users, groups, and roles, see "Managing Users and Security" on page 105.

This chapter contains the following sections:

About Schedules

A schedule is a calendar entry. A schedule consists of one or more schedule items. Each schedule item is effectively a sub-schedule: it includes a start date (and can include an end date), a time range during which it runs, a recurrence pattern (once, periodically, daily, weekly, monthly, or yearly), and range of recurrence.

You use schedules to set effective periods and blackout periods for rules and agents. For more information, see Chapter 6, "Associating Rules with Schedules" on page 299 and Chapter 5, "Assigning Blackouts to Agent Instances" on page 179. Additionally, you can create schedule-driven derived metrics and configure the values for registry variables to change at certain times based on schedules. See Chapter 7, "Triggering derived metrics" on page 348 and Chapter 6, "Using performance calendars" on page 204 for more information.

If a schedule only includes one schedule item, then that item is the schedule. If a schedule includes multiple schedule items, then they collectively form the schedule. For example, if you wanted a schedule to run indefinitely from 10:00 am to 11:00 am daily and on the first day of the month from 8:00 am to 6:00 pm, but also every Saturday from 11:00 am to 4:00 pm in May, add a schedule item for each of these time spans to the schedule.

You can create new schedules and manage the existing ones using the dashboards that come with the Administration module. For complete information, see the following sections:

- "Managing Schedules" on page 397
- "Creating Schedules" on page 407

Managing Schedules

The Manage Schedules dashboard allows you to manage existing schedules, assign permissions to schedules, and other features. For complete information, see the following sections:

- "Accessing the Manage Schedules Dashboard" on page 397
- "Editing Schedule Permissions" on page 399
- "Copying Schedules" on page 402
- "Deleting Schedules" on page 404
- "Viewing Schedule Definitions" on page 405
- "Viewing and Editing Schedules" on page 406

Accessing the Manage Schedules Dashboard

The Manage Schedules dashboard includes a list of the schedules that exist in your monitoring environment and includes an interface for adding and deleting schedules.

To access the Manage Schedules dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Schedules > Manage Schedules**.

   The Manage Schedules dashboard appears in the display area.

Manage Schedules   Apr 30, 2008 9:25:14 AM EDT

ⓘ Showing 1 - 18 of 18 schedules as of Apr 30, 2008 10:25:49   Refresh ↻

Schedule Name	Next Scheduled Time ▲		
Frequent [Test]	Wed Apr 30, 2008 10:25 EDT	▤	▢
Always	Wed Apr 30, 2008 10:25 EDT	▤	▢
Business hours	Wed Apr 30, 2008 10:25 EDT	▤	▢
Business week	Wed Apr 30, 2008 10:25 EDT	▤	▢
Hourly	Wed Apr 30, 2008 11:00 EDT	▤	▢
End of Day	Wed Apr 30, 2008 17:00 EDT	▤	▢
Beginning of the day	Thu May 01, 2008 00:00 EDT	▤	▢
First day of month	Thu May 01, 2008 00:00 EDT	▤	▢
Beginning of the month	Thu May 01, 2008 00:00 EDT	▤	▢
Daily Off Hours	Thu May 01, 2008 00:00 EDT	▤	▢
Monthly Off Hours	Thu May 01, 2008 00:00 EDT	▤	▢
Daily Database Maintenance	Thu May 01, 2008 02:00 EDT	▤	▢
Start of Day	Thu May 01, 2008 08:00 EDT	▤	▢
Weekends	Sat May 03, 2008 00:00 EDT	▤	▢
First day of week	Mon May 05, 2008 00:00 EDT	▤	▢
Weekly Off Hours	Mon May 05, 2008 00:00 EDT	▤	▢
Beginning of the week	Mon May 05, 2008 00:00 EDT	▤	▢
Quarterly Off Hours	Tue Jul 01, 2008 00:00 EDT	▤	▢

[Add Schedule]   [Delete Selected] **Select All Select None**

3 To sort the list of variables by their name or next scheduled time, click the
Schedule Name or **Next Scheduled Time** column headings as required.

From here, you can proceed to any of the following procedures:

Editing Schedule Permissions

vFoglight allows you to control access to a schedule. For each schedule you can grant or deny read, write, or control access to roles or users. For more information about security concepts in vFoglight, see Chapter 3, "Managing Users and Security" on page 105.

vFoglight employs the following behavior when it comes to schedule permissions:

• If no one has a permission to the schedule, everyone has a permission.

• If one has a permission to the schedule, others with undefined permission do not have any permission.

• Final permission is based on a combination of the role, user, and schedule defined on the server side.

Use the Edit Permissions button ( ) on the Manage Schedules dashboard to navigate to the Edit Permissions for Schedule area, that allows you to add or edit permissions to roles and users, as outlined below. The Edit Permissions for Schedule area contains two tables that show the permissions for each vFoglight user or role.
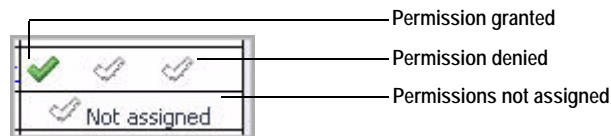
To add permissions for a schedule:

Note   This procedure continues from "Accessing the Manage Schedules Dashboard" on page 397.

1 In the Manage Schedules dashboard, in the row containing the schedule whose permissions you want to edit, click the Edit Permissions for Schedule button ( ).

The Edit Permissions for Schedule area appears in the Manage Schedules dashboard.

2 To add permissions to a schedule, complete the following steps.

    a Click the role or user to which you want to assign permissions.

        Tip The Not Assigned icons in the **Permissions** columns indicate that the role has no permissions assigned to it.

    The **Add Role Permission** or **Add User Permission** dialog box appears.

b In the dialog box that appears, use the **Read**, **Write**, and **Control** check boxes to assign permissions as required, and click **Save**.

The dialog box closes and the selected entry refreshes, showing three check marks in the **Permission** columns, one for each of the read, write, and control permissions.

Permission granted

Permission denied
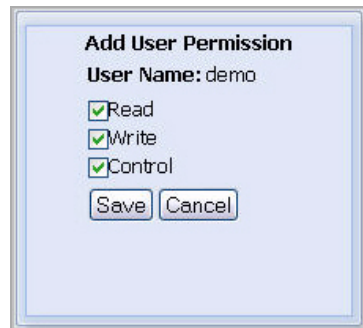
3 To edit or delete permissions for a schedule, complete the following steps.

   a Click the role or user whose permissions you want to edit.

      Tip Three check marks in the **Permissions** columns indicate that the role already has permissions assigned to it.

   The **Edit Role Permission** or **Edit User Permission** dialog box appears.
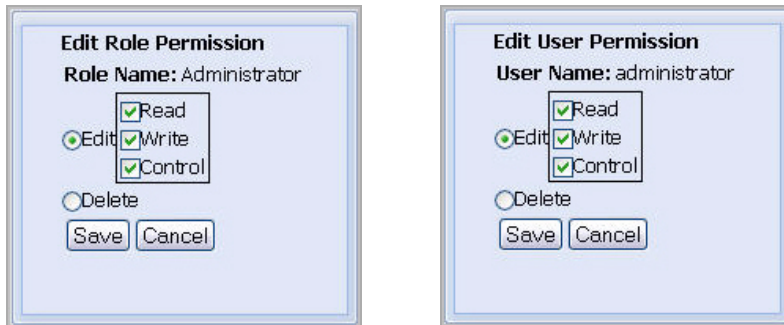
b To edit the permissions, ensure that the **Edit** option is selected and use the **Read**, **Write**, and **Control** check boxes as required.

c To delete the permissions, select the **Delete** option.

d Click **Save**.

The dialog box closes and the selected entry refreshes, showing the newly-edited permissions.

Copying Schedules

Use the Copy Schedule button on the Manage Schedules dashboard to copy a schedule, as outlined below.

To copy a schedule:

Note   This procedure continues from "Accessing the Manage Schedules Dashboard" on page 397.

1 In the Manage Schedules dashboard, in the row containing the schedule that you want to copy, click the Copy Schedule button (▣).

The **Copy Schedule** dialog box appears.
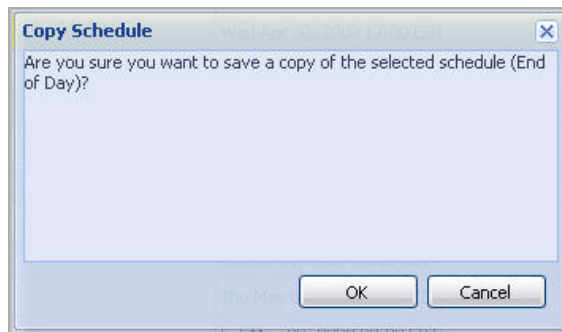
The dialog box closes and the **Edit Schedule** view appears in the Manage Schedules dashboard.
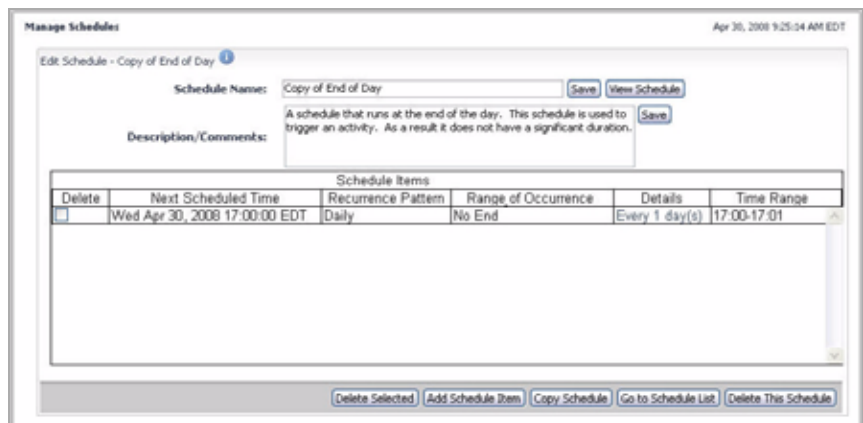
2 If required, edit the newly-copied schedule.

For more information, see "Viewing and Editing Schedules" on page 406.

Deleting Schedules

Use the Delete Selected button on the Manage Schedules dashboard to delete a schedule, as outlined below.

Note   When a schedule is deleted, all references to that schedule are removed as well; any performance calendars that are based on that schedule are removed and the deleted schedule is removed from the list of effective and blackout schedules for rules.

To delete a schedule:

Note   This procedure continues from "" on page 397.

---

1   In the Manage Schedules dashboard, select the row containing the schedule that you want to delete.

2   Click the **Delete Selected** button at the bottom.

The **Schedule Delete Confirmation** dialog box appears.
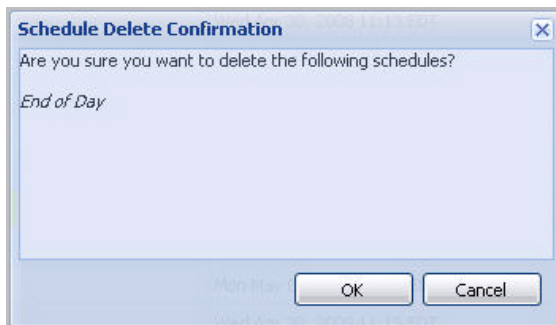
3   In the **Schedule Delete Confirmation** dialog box, click **OK**.

The **Schedule Delete Confirmation** dialog box closes.

4   Observe the Manage Schedules dashboard.

The newly-deleted schedule no longer appears in the list.

Viewing Schedule Definitions

To view schedule definitions:
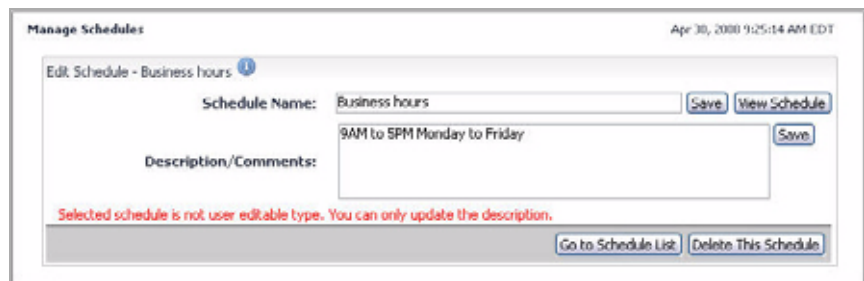
Note   This procedure continues from "Accessing the Manage Schedules Dashboard" on page 397.

---

1 In the Manage Schedules dashboard, click the **Schedule Name** column of the row containing the schedule whose definitions you want to view.

The **Edit Schedule** view appears in the Manage Schedules dashboard.

2 View the definitions of the selected schedule.

In the **Edit Schedule** view, click the **View Schedule** button in the upper-right corner.

The **Business Hours** dialog box appears.
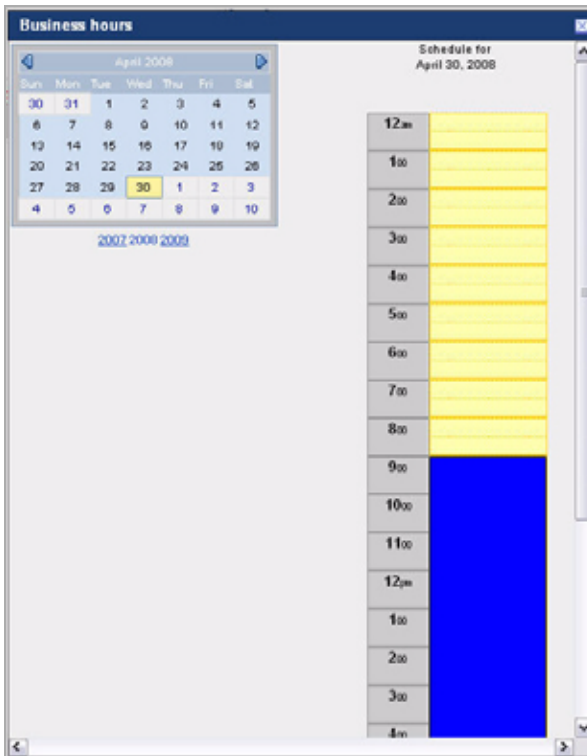
3 Observe the schedule definitions for a selected date.

In the **Business Hours** dialog box, use the calendar in the upper-left corner to select a date.

On the right, the schedule for the selected date refreshes, showing the schedule's effective hours in blue.

When you finish observing schedule definitions, close the **Business Hours** dialog box.

Viewing and Editing Schedules

You can edit the existing schedules by adding or removing recurrence patterns to it as required. For example, if you have a schedule that runs indefinitely from 10:00 am to 11:00 am daily and on the first day of the month from 8:00 am to 6:00 pm, but you want

to edit it to also run every Saturday from 11:00 am to 4:00 pm in May, add a schedule item for each of these time spans to the schedule.

To view and edit a schedule:

Note This procedure continues from "" on .

---

1 In the Manage Schedules dashboard, click the schedule that you want to edit.

   The **Edit Schedule** view appears in the Manage Schedules dashboard.

2 Observe the schedule definitions.

3 Edit the schedule definitions as required.

   For complete instructions, see "" on .

Creating Schedules

vFoglight allows you to create schedules using the Create Schedule dashboard. You can access this dashboard from the navigation panel, or through the Manage Schedules dashboard. When you create a schedule, you can use it in rule, derived metric, and agent definitions as required.

Creating a schedule involves several steps. Once you get started with schedule creation, you need to define the start date and recurrence pattern. For instructions, see the following sections:

- "Accessing the Create Schedule Dashboard" on page 408
- "Getting Started with Schedule Definitions" on page 409
- "Adding or Removing Schedule Items" on page 410
- "Defining Schedule Items" on page 415

Accessing the Create Schedule Dashboard

To access the Create Schedule dashboard:

Note This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2 Open the Create Schedule dashboard by completing one of the following steps:

- On the navigation panel, under **Dashboards**, choose **Administration > Schedules > Manage Schedules**.

    In the Manage Schedules dashboard that appears in the display area, click the **Add Schedule** button in the lower-left corner.

or

- On the navigation panel, under **Dashboards**, choose **Administration > Schedules > Create Schedules**.

The Create Schedule dashboard appears in the display area, showing the **Step 1: Create Schedule - Schedule Name and Description** view.

From here, you can proceed to "Getting Started with Schedule Definitions" on page 409.

Getting Started with Schedule Definitions

To get started with schedule definitions:

Note   This procedure continues from "Accessing the Create Schedule Dashboard" on page 408.

---

1   Specify the schedule name.

    In the Create Schedule dashboard, in the **Schedule Name** box, type the name that you want to assign to the schedule.

2   **Optional**. Add information that describes the schedule.

    In the **Description/Comments** box, type the schedule description or comments as required. For example:

    ```
    A schedule that runs at the end of the day. This schedule is
    used to trigger an activity. As a result it does not have a
    significant duration.
    ```

3   Click **Next**.

The **Step 2: Create Schedule - Details of Schedule** view appears in the Create Schedule dashboard.

From here, you can proceed to "Adding or Removing Schedule Items" on page 410.

Adding or Removing Schedule Items

A schedule can contain one or more items, each describing a recurrence pattern. For example, if you wanted a schedule to run indefinitely from 10:00 am to 11:00 am daily and on the first day of the month from 8:00 am to 6:00 pm, but also every Saturday from 11:00 am to 4:00 pm in May, add a schedule item for each of these time spans to the schedule.

When you create a schedule, you have to specify at least one schedule item and its recurrence pattern. You can edit the schedule at a later time by adding or removing schedule items as required.

To add a schedule item to a newly-created schedule that has no other schedule items:

Note   This procedure continues from "Getting Started with Schedule Definitions" on page 409.

- In the Create Schedule dashboard, in the **Step 2: Create Schedule - Details of Schedule** view, specify the start date, end date and duration (if applicable), and the range of occurrence, as required.

For complete information on how to define a schedule item, see "Defining Schedule Items" on page 415.

To add a schedule item to a newly-created schedule that already contains schedule items:

Note   This procedure continues from "Defining Schedule Items" on page 415.

1   Open the schedule for editing.

In the **Step 3: Create Schedule - Schedule Added** view, click **Edit Schedule**.
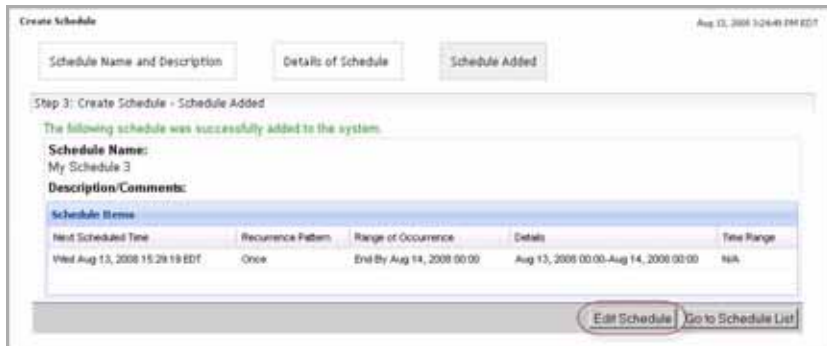
The **Edit Schedule** view appears.

2 In the **Edit Schedule** view, click **Add Schedule Item** in the lower-right corner.
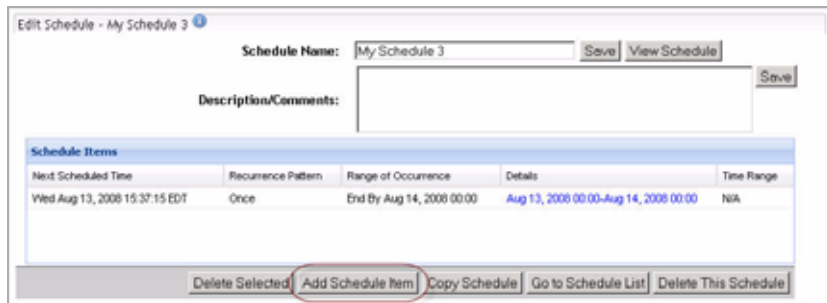
The **Edit Schedule -> Add Schedule Item** view appears, allowing you to define another schedule item.

For complete information on how to define a schedule item, see "Defining Schedule Items" on page 415.

To add a schedule item to an existing schedule:

Note   This procedure continues from "Viewing and Editing Schedules" on page 406.

---

1   In the **Edit Schedule** view, click **Add Schedule Item** in the lower-right corner.

To delete a schedule item:

Note   This procedure continues from "Viewing and Editing Schedules" on page 406 or "Defining Schedule Items" on page 415.

---

1   In the **Edit Schedule** view, select the row containing the schedule item that you want to delete and click **Delete Selected**.

The **Schedule Confirmation** dialog box appears, asking you to confirm the delete operation.

2   In the **Schedule Confirmation** dialog box, click **OK**.

The **Edit Schedule** view refreshes, no longer showing the newly-deleted schedule item in the list.

Defining Schedule Items

There are six types of patterns that you can define in a schedule item, as listed below.

Pattern	Allows you to create pattern that	For instructions, see
Once	Starts at a specified date and time, for a specified duration, and ends at a defined end date and time	"To define a schedule item that occurs once:" on page 416
Periodical	Starts at a specified time and date for a certain duration, repeats at specified time periods, with or without a defined end date and time	"To define a schedule item that occurs periodically:" on page 419
Daily	Starts at a specified time and date, runs for a whole day or a fraction of a day, repeats at a regular interval of days, with or without a defined end date and time	"To define a schedule item that occurs periodically:" on page 419
Weekly	Starts at a specified time and date, runs for a whole day or a fraction of a day, repeats at a regular interval of weeks on one or more days of the week, with or without a defined end date and time	"To define a schedule item that occurs weekly:" on page 427
Monthly	Starts at a specified time and date, runs for a whole day or a fraction of a day, repeats at a regular interval of months on one or more days of the week, with or without a defined end date and time	"To define a schedule item that occurs monthly:" on page 433

Pattern	Allows you to create pattern that	For instructions, see
Yearly	Starts at a specified time and date, runs for a whole day or a fraction of a day, repeats at a regular interval of years on one or more days of the week each month, with or without a defined end date and time	"To define a schedule item that occurs yearly:" on page 440
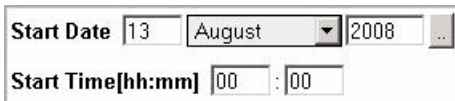
To define a schedule item that occurs once:

Note

---

1 In the **Recurrence Pattern** area, ensure that the **Once** option is selected.

2 Specify the start date and time of the recurrence pattern using the controls that appear above the **Recurrence Pattern** area.

Start Date	13	August ▼	2008	...
Start Time[hh:mm]	00	:	00	

a Use the **Start Date** boxes to specify the day, month and year of the start date.

Alternatively, click the Calendar button on the right and use the calendar controls that appear to specify the start date.

Tip The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

b Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

> **Tip** The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.
>
> The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

3 Specify the date and time after which the schedule item ends using the controls in the **Range of Occurrence** area.

> **Note** In the **Range of Occurrence** area, the **No End** option appears disabled while the **End By Date** option is enabled and selected. This is because a schedule item that occurs once must have an end date.

a Use the **End Date** boxes to specify the day, month and year of the start date.

> **Tip** The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

Alternatively, click the Calendar button on the right and use the calendar controls that appear to specify the end date.

   b Use the **End Time [hh:mm]** boxes to specify the hour and minute of the end time.

     Tip The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

         The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

4 Save the changes to the schedule item.

- **New schedules.** In the lower-right corner, click **Add**.
- **Existing schedules.** In the lower-right corner, click **Save**.

The **Schedule Items** table refreshes, showing the newly-added schedule item.

5 Add one or more schedule items if required.

For details, see "Adding or Removing Schedule Items" on page 410.

To define a schedule item that occurs periodically:

Note This procedure continues from "Adding or Removing Schedule Items" on page 410.

---

1 In the **Recurrence Pattern** area, select the **Periodical** option.

The view refreshes, showing a set of controls that allow you to define a schedule item that occurs periodically.

2 Specify the start date and time, and the duration of the recurrence pattern using the controls that appear above the **Recurrence Pattern** area.

a Use the **Start Date** boxes to specify the day, month and year of the start date.

Alternatively, click the Calendar button on the right and use the calendar controls that appear to specify the start date.

Tip The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

b Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

> **Tip** The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.
>
> The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

c Use the **Duration [hh:mm]** boxes to specify the hour and minute of the start time.

> **Tip** The Hour box accepts any positive values.
>
> The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

3 Specify the recurrence pattern.

In the **Recurrence Pattern** area, use the **Every [hh:mm]** boxes to specify the hour and minute of the start time.

> **Important** The recurrence period must be longer than the duration specified in step 2. For example, if the duration of the schedule item is three hours, the recurrence periods should occur at intervals that are longer than three hours.

> **Tip** The Hour box accepts any positive values.
>
> The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

4 Specify the date and time after which the schedule item ends using the controls in the **Range of Occurrence** area.

- To specify an end date, in the **Range of Occurrence** area, ensure that the **End By Date** option is selected, and specify the end date and time using the **End Date** and **End Time [hh:mm]** boxes as required.

    Tip   Use the Calendar button on the right and use the calendar controls that appear to specify the start date.

    Tip   The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

    The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

- To have the schedule item recurring at the recurrence pattern specified in step 3 without an end date, in the **Range of Occurrence** area, select the **No End** option.

    The **Range of Occurrence** area refreshes, no longer showing the controls for specifying the end date.

5 Save the changes to the schedule item.

- **New schedules.** In the lower-right corner, click **Add**.
- **Existing schedules.** In the lower-right corner, click **Save**.

The **Schedule Items** table refreshes, showing the newly-added schedule item.

6 Add one or more schedule items if required.

For details, see "Adding or Removing Schedule Items" on page 410.

To define a schedule item that occurs daily:

Note   This procedure continues from "Adding or Removing Schedule Items" on page 410.

---

1 In the **Recurrence Pattern** area, select the **Periodical** option.

The view refreshes, showing a set of controls that allow you to define a schedule item that occurs on a daily basis.

2   Specify the start date of the recurrence pattern.

Use the **Start Date** boxes to specify the day, month and year of the start date.

Alternatively, click the Calendar button on the right and use the calendar controls that appear to specify the start date.

Tip   The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

3   Specify the duration of the schedule item.

•   If you want the schedule to occur for a part of the day, complete one of the following steps.

• Specify the start time and end time of the schedule item.

   • Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

Tip   The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

   The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

   • Select the **End Time [hh:mm]** option and specify the hour and minute of the end time.

Note   The **Duration [hh:mm]** boxes appear disabled when you specify the **End Time [hh:mm]** option.

   The end time should occur after the start time.

Tip   The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

   The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

or

• Specify the start time and duration of the schedule item.

- Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

Tip The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

- Select the **Duration [hh:mm]** option and specify the hour and minute of the duration time.

Note The **End Time [hh:mm]** boxes appear disabled when you specify the **Duration [hh:mm]** option.

Tip The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

or

- If you want the schedule to occur for the entire day, select the **Whole Day** check box.

The **Start Time [hh:mm]**, **End Time [hh:mm]**, and **Duration [hh:mm]** boxes appear disabled.

vFoglight
Administration and Configuration Guide

4 Specify the recurrence pattern.

In the **Recurrence Pattern** area, use the **Every** box to specify the number of days at which the schedule recurs.

Tip The **Every** box accepts any positive values.

5 Specify the date and time after which the schedule item ends using the controls in the **Range of Occurrence** area.

- To specify an end date, in the **Range of Occurrence** area, ensure that the **End By Date** option is selected, and specify the end date and time using the **End Date** and **End Time [hh:mm]** boxes as required.

    Tip Use the Calendar button on the right and use the calendar controls that appear to specify the start date.

    Tip The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

    The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

- To have the schedule item recurring at the recurrence pattern specified in step 4 without an end date, in the **Range of Occurrence** area, select the **No End** option.

  The **Range of Occurrence** area refreshes, no longer showing the controls for specifying the end date.

```
Range of Occurrence
⊙ No End
○ End By Date
```

6 Save the changes to the schedule item.

- **New schedules.** In the lower-right corner, click **Add**.
- **Existing schedules.** In the lower-right corner, click **Save**.

The **Schedule Items** table refreshes, showing the newly-added schedule item.

Create Schedule				Aug 14, 2008 11:04:31 AM EDT
Edit Schedule - My Schedule ⓘ				
Changes have been saved				
Schedule Name:	My Schedule		Save	View Schedule
Description/Comments:				Save

Schedule Items				
Next Scheduled Time	Recurrence Pattern	Range of Occurrence	Details	Time Range
Thu Aug 14, 2008 23:59:00 EDT	Daily	End By Aug 15, 2008 00:00	Every 1 day(s)	23:56 hour(s) from 23:59

| Delete Selected | Add Schedule Item | Copy Schedule | Go to Schedule List | Delete This Schedule |

7 Add one or more schedule items if required.

To define a schedule item that occurs weekly:

Note

1 In the **Recurrence Pattern** area, select the **Weekly** option.

The view refreshes, showing a set of controls that allow you to define a schedule item that occurs on a weekly basis.

2 Specify the start date of the recurrence pattern.

Use the **Start Date** boxes to specify the day, month and year of the start date.

Alternatively, click the Calendar button on the right and use the calendar controls that appear to specify the start date.

Tip The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

3 Specify the duration of the schedule item.

- If you want the schedule to occur for a part of the day, complete one of the following steps.

  • Specify the start time and end time of the schedule item.

    • Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

    Tip   The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

    • Select the **End Time [hh:mm]** option and specify the hour and minute of the end time.

    Note   The **Duration [hh:mm]** boxes appear disabled when you specify the **End Time [hh:mm]** option.

    The end time should occur after the start time.

    Tip   The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

or

  • Specify the start time and duration of the schedule item.

• Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

Tip The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

• Select the **Duration [hh:mm]** option and specify the hour and minute of the duration time.

Note The **End Time [hh:mm]** boxes appear disabled when you specify the **Duration [hh:mm]** option.

Tip The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

or

• If you want the schedule to occur for the entire day, select the **Whole Day** check box.

The **Start Time [hh:mm]**, **End Time [hh:mm]**, and **Duration [hh:mm]** boxes appear disabled.

4 Specify the recurrence pattern.

In the **Recurrence Pattern** area, use the **Every** box to specify the number of weeks at which the schedule occurs.

Tip   The **Every** box accepts any positive values.

Select one or more check boxes that represent the days of the week on which the schedule occurs.

For example, to have the schedule occurring on Mondays and Wednesdays for four weeks in a row, in the **Every** box, type 4, and select the **Monday** and **Wednesday** check boxes, as illustrated bellow.

Every 4   week(s) on
☑Monday ☐Tuesday ☑Wednesday ☐Thursday
☐Friday ☐Saturday ☐Sunday

5 Specify the date and time after which the schedule item ends using the controls in the **Range of Occurrence** area.

Range of Occurrence

○No End   **End Date**   15   August   ▼ 2008   ..
◉End By Date **End Time[hh:mm]** 00 : 00

- To specify an end date, in the **Range of Occurrence** area, ensure that the **End By Date** option is selected, and specify the end date and time using the **End Date** and **End Time [hh:mm]** boxes as required.

    Tip Use the Calendar button on the right and use the calendar controls that appear to specify the start date.

    Tip The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

    The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

- To have the schedule item recurring at the recurrence pattern specified in step 4 without an end date, in the **Range of Occurrence** area, select the **No End** option.

    The **Range of Occurrence** area refreshes, no longer showing the controls for specifying the end date.

6 Save the changes to the schedule item.

- **New schedules.** In the lower-right corner, click **Add**.
- **Existing schedules.** In the lower-right corner, click **Save**.

The **Schedule Items** table refreshes, showing the newly-added schedule item.

7   Add one or more schedule items if required.

    For details, see "Adding or Removing Schedule Items" on page 410.

To define a schedule item that occurs monthly:

Note   This procedure continues from "Adding or Removing Schedule Items" on page 410.

---

1   In the **Recurrence Pattern** area, select the **Monthly** option.

    The view refreshes, showing a set of controls that allow you to define a schedule item that occurs that occurs on a monthly basis.

2 Specify the start date of the recurrence pattern.

Use the **Start Date** boxes to specify the day, month and year of the start date.

Alternatively, click the Calendar button on the right and use the calendar controls that appear to specify the start date.

Tip The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

3 Specify the duration of the schedule item.

- If you want the schedule to occur for a part of the day, complete one of the following steps.

  • Specify the start time and end time of the schedule item.

    • Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

    Tip The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

    • Select the **End Time [hh:mm]** option and specify the hour and minute of the end time.

    Note The **Duration [hh:mm]** boxes appear disabled when you specify the **End Time [hh:mm]** option.

    The end time should occur after the start time.

    Tip The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

or

  • Specify the start time and duration of the schedule item.

• Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

Tip The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

• Select the **Duration [hh:mm]** option and specify the hour and minute of the duration time.

Note The **End Time [hh:mm]** boxes appear disabled when you specify the **Duration [hh:mm]** option.

Tip The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

or

• If you want the schedule to occur for the entire day, select the **Whole Day** check box.

The **Start Time [hh:mm]**, **End Time [hh:mm]**, and **Duration [hh:mm]** boxes appear disabled.

4 Specify the recurrence pattern.

- To have the schedule occurring on a specified day of the month, at the rate of one or more months, in the **Recurrence Pattern** area, ensure that the **By Date** option is selected, and then specify the day of the month and the rate at which it occurs.

  Tip The **Day** box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

  The **every** box accepts any positive values.

  For example, to have the schedule occurring on the fifth day of every second month, in the **Day** box, type 5, and in the **every** box, type 2, as illustrated bellow.

- To have the schedule occurring on one or more days of the week, at a rate of one or more months, in the **Recurrence Pattern** area, select the **By Week** option.

  The **Recurrence Pattern** area refreshes, showing a set of the controls that allow you to specify the pattern.

  Specify the week of the month, the day of the week and the rate at which it occurs.

  Tip The **every** box accepts any positive values.

  For example, to have the schedule occurring on the second Tuesday of every third month, click **First** and select **Second** from the list that appears. Then, select the **Tuesday** check box, and in the **every** box, type 3, as illustrated below.

In the **Recurrence Pattern** area, use the **Every** box to specify the number of weeks at which the schedule occurs.

Tip   The **Every** box accepts any positive values.

5   Specify the date and time after which the schedule item ends using the controls in the **Range of Occurrence** area.

•   To specify an end date, in the **Range of Occurrence** area, ensure that the **End By Date** option is selected, and specify the end date and time using the **End Date** and **End Time [hh:mm]** boxes as required.

Tip   Use the Calendar button on the right and use the calendar controls that appear to specify the start date.

Tip   The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

- To have the schedule item recurring at the recurrence pattern specified in step 4 without an end date, in the **Range of Occurrence** area, select the **No End** option.

  The **Range of Occurrence** area refreshes, no longer showing the controls for specifying the end date.

Range of Occurrence
⊙ No End
○ End By Date

6 Save the changes to the schedule item.

- **New schedules.** In the lower-right corner, click **Add**.
- **Existing schedules.** In the lower-right corner, click **Save**.

The **Schedule Items** table refreshes, showing the newly-added schedule item.

Create Schedule Aug 14, 2008 12:09:28 PM EDT

Schedule Name and Description	Details of Schedule	Schedule Added

Step 3: Create Schedule - Schedule Added

The following schedule was successfully added to the system.

Schedule Name:
My Schedule

Description/Comments:

Schedule Items

Next Scheduled Time	Recurrence Pattern	Range of Occurrence	Details	Time Range
Sun Sep 14, 2008 00:00:00 EDT	Monthly	End By Sep 15, 2008 00:00	Day 14 of every 1 month(s)	00:00 hour(s) from 00:00

Edit Schedule   Go to Schedule List

7 Add one or more schedule items if required.

For details, see "Adding or Removing Schedule Items" on page 410.

To define a schedule item that occurs yearly:

Note   This procedure continues from "

---

1 In the **Recurrence Pattern** area, select the **Yearly** option.

The view refreshes, showing a set of controls that allow you to define a schedule item that occurs on a yearly basis.

2 Specify the start date of the recurrence pattern.

Use the **Start Date** boxes to specify the day, month and year of the start date.

Alternatively, click the Calendar button on the right and use the calendar controls that appear to specify the start date.

Tip   The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

3 Specify the duration of the schedule item.

- If you want the schedule to occur for a part of the day, complete one of the following steps.

  • Specify the start time and end time of the schedule item.

    • Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

    Tip The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

    • Select the **End Time [hh:mm]** option and specify the hour and minute of the end time.

    Note The **Duration [hh:mm]** boxes appear disabled when you specify the **End Time [hh:mm]** option.

    The end time should occur after the start time.

    Tip The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

    The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

  or

  • Specify the start time and duration of the schedule item.

- Use the **Start Time [hh:mm]** boxes to specify the hour and minute of the start time.

Tip   The Hour box accepts the values between 0 and 23. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

- Select the **Duration [hh:mm]** option and specify the hour and minute of the duration time.

Note   The **End Time [hh:mm]** boxes appear disabled when you specify the **Duration [hh:mm]** option.

Tip   The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 24; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

or

- If you want the schedule to occur for the entire day, select the **Whole Day** check box.

The **Start Time [hh:mm]**, **End Time [hh:mm]**, and **Duration [hh:mm]** boxes appear disabled.

4 Specify the recurrence pattern.

- To have the schedule occurring on a specified day of the month, at the rate of one or more months, in the **Recurrence Pattern** area, ensure that the **By Date** option is selected, and then specify the day of the month and the rate at which it occurs.

  Tip The **Day** box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

  For example, to have the schedule occurring on the sixth day of every April month, click the Month box and select **April** from the list that appears, and in the Day box, type 6, as illustrated bellow.

- To have the schedule occurring on a particular day of the week, in the **Recurrence Pattern** area, select the **By Week** option.

  The **Recurrence Pattern** area refreshes, showing a set of the controls that allow you to specify the pattern.

  Specify the week of the month, the day of the week and the month on which the schedule occurs.

  For example, to have the schedule occurring every third Thursday in November, click **First** and select **Third** from the list that appears. Then, select the **Thursday** check box, click the Month box on the right and select **November** from the list that appears, as illustrated below.

5 Specify the date and time after which the schedule item ends using the controls in the **Range of Occurrence** area.

- To specify an end date, in the **Range of Occurrence** area, ensure that the **End By Date** option is selected, and specify the end date and time using the **End Date** and **End Time [hh:mm]** boxes as required.

  Tip Use the Calendar button on the right and use the calendar controls that appear to specify the start date.

  Tip The Day box accepts the values between 1 and 31. Any positive values outside that range are automatically adjusted to 31; negative values are not accepted.

  The Hour box accepts the values between 0 and 24. Any positive values outside that range are automatically adjusted to 23; negative values are not accepted.

The Minute box accepts the values between 0 and 59. Any positive values outside that range are automatically adjusted to 59; negative values are not accepted.

- To have the schedule item recurring at the recurrence pattern specified in step 4 without an end date, in the **Range of Occurrence** area, select the **No End** option.

  The **Range of Occurrence** area refreshes, no longer showing the controls for specifying the end date.

  ```
  Range of Occurrence
  ⊙No End
  ○End By Date
  ```

6 Save the changes to the schedule item.

- **New schedules.** In the lower-right corner, click **Add**.
- **Existing schedules.** In the lower-right corner, click **Save**.

The **Schedule Items** table refreshes, showing the newly-added schedule item.

7 Add one or more schedule items if required.

For details, see "Adding or Removing Schedule Items" on page 410.

9

Working with vFoglight Tooling

This chapter introduces you to the Tooling dashboards and provides information on how to build script agents and use the query tool. It contains the following sections:

Note In order to complete each of the procedures in this chapter, your user account must belong to a group with the Administration role. For more information about users, groups, and roles, see "Managing Users and Security" on page 105.

This chapter contains the following sections:

About vFoglight Tooling

The vFoglight Management Server collects data from your monitored system and organizes that data into a topology model. Each topology model is comprised of nodes. The nodes and their relationship in the topology model represent the logical and physical structure of the entities in your monitored environment. Furthermore, each topology model includes a set of topology types to describe the nodes, or topology objects, in that model.

The topology types that exist in your environment depend on the nature and complexity of your monitoring environment and the type of vFoglight cartridges and their agents that you use to collect information from monitored hosts.

In addition to a wide offering of vFoglight cartridges for a number of different environment types, your business scenario may require additional custom agents. vFoglight allows you to add one or more script-based custom agents to address your unique monitoring needs. For more information, see "Building Script Agents" on page 448.

Furthermore, vFoglight uses the query language that allows you to drill through the topology model and select topology objects as required. You interact with the query language when specifying rule conditions, derived metrics, and other vFoglight entities. You can take advantage of the query language to select a range of topology objects and run a script against those objects to retrieve instant results. For more information, see "Retrieving Data with Queries and Scripts" on page 467.

Building Script Agents

Custom script agents interact with the vFoglight Agent Manager through the vFoglight collector executable. You can use any scripting language to write your scripts. Script-based custom agents output to standard output (stdout) and the vFoglight collector reads the data and retransmits it to the vFoglight Agent Manager.

There are two types of Script Agents:

• *Type 1 scripts*. The vFoglight collector calls these scripts every time they need to collect data. In Type 1 scripts, the collector executes the script, then stands by for a time period specified in the agent properties. When the standby period ends, the collector becomes active and reruns the script. Type 1 scripts are useful for collecting data that does not require calculations from multiple collection periods.

For a sample of a Type 1 script, see "Example: Type 1 Script" on page 466.

- *Type 2 scripts*. These scripts control their own collection frequency cycle. In Type 2 scripts, the vFoglight collector executes the script and remains open. The script controls the standby period instead of the agent properties. Type 2 scripts perform data calculations before the data enters the database and measure changes between collection periods.

  For a sample of a Type 2 script, see "Example: Type 2 Script" on page 466.

Building a script agent involves several steps. First, you need to write an agent script using a particular syntax, upload it using the Build Script Agent dashboard. The upload process automatically builds the agent package. Next, you deploy that agent package to the vFoglight Agent Manager, create one or more agent instances as required, and edit agent properties if required. For complete instructions, see the following sections:

Looking at the Script Syntax

When writing a script to create a custom agent, use the following syntax:

```
TABLE table_name
    START_SAMPLE_PERIOD
        field_name[.type[.{id|obs}]][:unit]=value
        …
    END_SAMPLE_PERIOD
    …
END_TABLE
…
```

Note   The ellipsis '…' indicates that you can repeat the level.

A Canonical Data Transformation (CDT) dynamically converts the output data into the appropriate format (such as topology types and observations) that exist in the collection model. This mechanism dictates the syntax of the line of the code that specifies the field

data immediately following the START_SAMPLE_PERIOD command, as shown in the above syntax block:

```
START_SAMPLE_PERIOD
    field_name[.type[.{id|obs}]][:unit]=value
```

The following table describes the script elements, some of which appears in the above block.

Script Element	Definition
END_SAMPLE_PERIOD	Sends the current collection sample to the database and completes the transaction.
END_TABLE	Closes the table.
field_name	Contains the name of the field under which to store the observation.
id	Indicates that the property should be treated as an identity.
LOG message	Sends a status message to vFoglight Agent Manager logs with message specifying the message.
LOG severity message	Sends an error message to vFoglight Agent Manager logs with message specifying the message and severity set to one of the following values: **FATAL**, **WARNING**, or **CRITICAL**.
NEXT_SAMPLE	Sends multiple rows of field data in a single transaction.
obs	Indicates that the specified topology type is an observation (such as StringObservation).
SLEEP sample_freq	In Type 2 scripts, this element ends the script and instructs the collector to wait for the specified time before executing the script again.
	Note In NT operating systems, use the rapssleep command, as those systems do not have a sleep facility: **rapssleep** %sample_freq%

Script Element	Definition
START_SAMPLE_PERIOD	Starts the data collection for the specified table and inserts field data using the line of code that immediately follows this command.
TABLE *table_name*	Opens the table with *table_name* specifying the name of the table. If an identity field is declared, append it to the table name.
type	Specifies the topology type if it is not a metric.
unit	Contains the name of the measurement unit to use for metrics. If a unit is not specified, vFoglight uses "count" as the unit by default.

When you finish writing the agent script, you can proceed to "Accessing the Build Script Agent Dashboard" on page 451.

Accessing the Build Script Agent Dashboard

When you finish your script, navigate to the Build Script Agent dashboard. The Build Script Agent dashboard allows you to upload an agent script to the vFoglight Management Server.

To access the Build Script Agent dashboard:

Note

1 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow ▶ on the left.

2 On the navigation panel, under **Dashboards**, choose **Administration > Tooling > Build Script Agent**.

The Build Script Agent dashboard appears in the display area.

From here, you can go to "Uploading Agent Scripts and Building Agent Packages" on page 452.

Uploading Agent Scripts and Building Agent Packages

Once you finish your script and get started with the Build Script Agent dashboard, you can upload your script to the vFoglight Management Server and build the agent package.

To upload an agent script:

> **Note** This procedure continues from "Accessing the Build Script Agent Dashboard" on page 451.

1 Ensure that your agent script is valid and complete.

For information about the script syntax, see "Looking at the Script Syntax" on page 449.

2 Locate your agent script.

In the Build Script Agent dashboard, click **Browse**.

Navigate to your script using the file browser that appears. When you close the file browser and return to the Build Script Agent dashboard, the **Upload Script** box refreshes, showing the path and name of the script file while the **Script Version** boxes show the version number.

3 Ensure that the version number of the script agent that you are about to upload is correct.

To change the version number, use the **Script Version** boxes as required.

4 Upload the script and build the agent.

Click **Submit**.

The **Build Script Agent** dialog box appears, asking you to confirm the build operation.

The **Build Script Agent** dialog box shows that the agent you are about to create includes two components: an agent component and a cartridge component. That is because in vFoglight each agent requires a cartridge component that contains topology definitions and default agent properties while the agent component acts as a data collector. When you create script-based agents, the name and version number of the agent component are identical to the name and version number of the cartridge component.

5 In the **Build Script Agent** dialog box, click **Confirm**.

Note vFoglight checks the collection of the existing cartridge list and displays a warning message if duplicate cartridges exist. If it finds a cartridge with the same name and version, the **Confirm** button appears disabled and a warning message appears. If a cartridge with the same name but different version exists, a warning message appears but the **Confirm** button is enabled. In this case, vFoglight disables the existing cartridge during the installation of the new cartridge.

The **Build Script Agent** dialog box closes. A progress bar in the Build Script Agent dashboard indicates that the upload operation is in progress. After a few moments, the **Build Script Agent** dialog box reappears, indicating the success of the build operation.

6   In the **Build Script Agent** dialog box, click **Move to Agent Listing**.

The **Agent Status** area appears in the Build Script Agent dashboard.
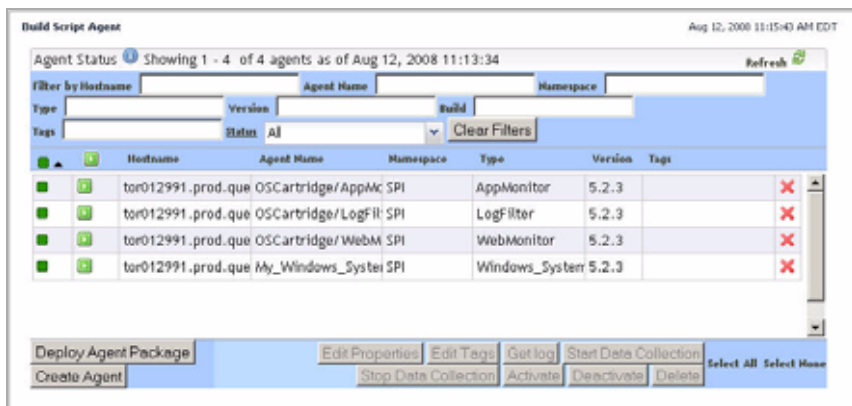
From here, you can proceed to "Deploying Script Agent Packages" on page 454.

Deploying Script Agent Packages

When you successfully upload the agent script and build the agent package, you can deploy that package to the vFoglight Agent Manager. Package deployment is identical to the process you use to deploy any other agent package. One thing you need to pay attention to is the package name and version: use the same name and version number that you specify when uploading and building the package.

Use the Agent Status area in the Build Script Agent dashboard to deploy a script agent. Alternatively, you can deploy the package using the command line. To deploy a script agent package:

1 On the Build Script Agent dashboard, in the lower-left corner of the **Agent Status** area, click **Deploy Agent Package**.

The **Agent Status** area appears in the Build Script Agent dashboard.

The **Deploy Agent Package** dialog box appears.

2 Specify the monitored host to which you want to deploy the agent package.

Note In order to select the agent adapter, the adapter must be up and running on the monitored host.

In the **Deploy Agent Package** dialog box, click **Host** and select the monitored host to which you want to deploy the agent package.

3 Select the script agent package.

Click **Package** and select the script agent package that you created in "Uploading Agent Scripts and Building Agent Packages" on page 452 from the list that appears.
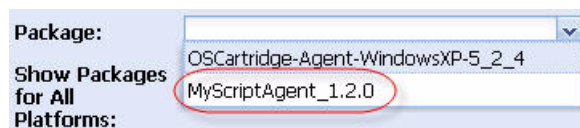
For example: `MyScriptAgent-1.2.0`

4 Click **Deploy**.

The **Deploy Agent Package** dialog box refreshes, showing the status of the deployment operation.
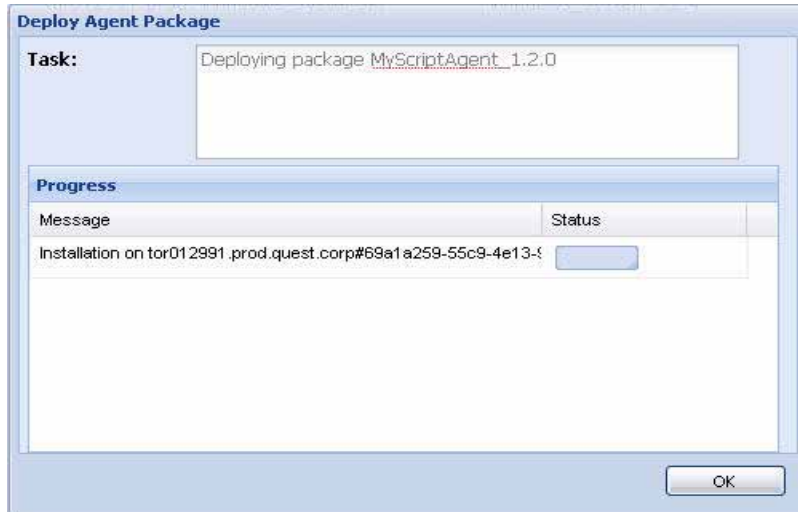
After a few moments, in the **Deploy Agent Package** dialog box, in the **Status** column of the **Progress** table, a green check mark appears, indicating a success of the deployment operation.
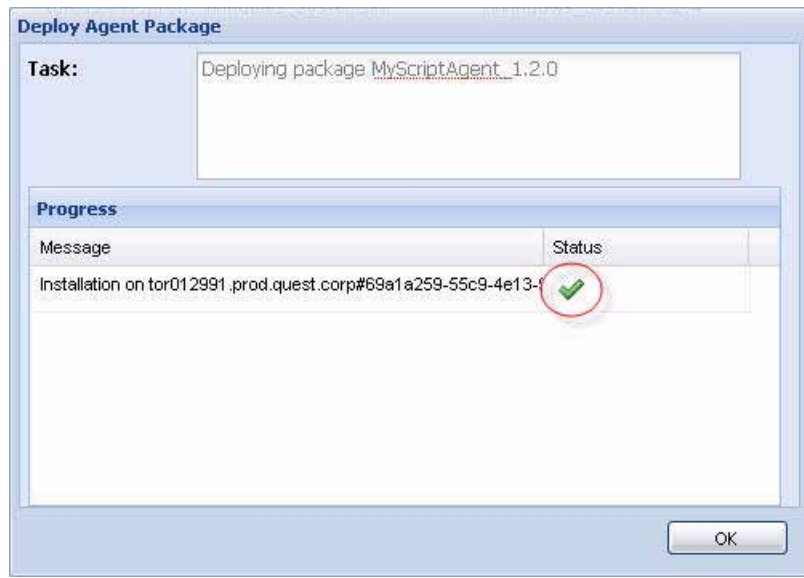
5 Click **OK** to close the **Deploy Agent Package** dialog box.

From here, you can proceed to "Creating and Activating Script Agent Instances" on page 457.

Creating and Activating Script Agent Instances

Once you have successfully deployed the package containing the script agent, you can create one or more instances of your custom script agent. Instance creation is identical to the process you use to create agent instances of any other type. However, you need to ensure that the agent type you choose matches the one you build and deploy.

Use the Agent Status area in the Build Script Agent dashboard to create one or more instances of your script agent. Alternatively, you can create agent instances using the command line.

To create and activate a script agent instance:

Note   This procedure continues from "Deploying Script Agent Packages" on page 454.

---

1 In the Build Script Agent dashboard, in the Agent Status area, click the **Create Agent** button in the lower-left corner.

The **Create Agent** dialog box appears.
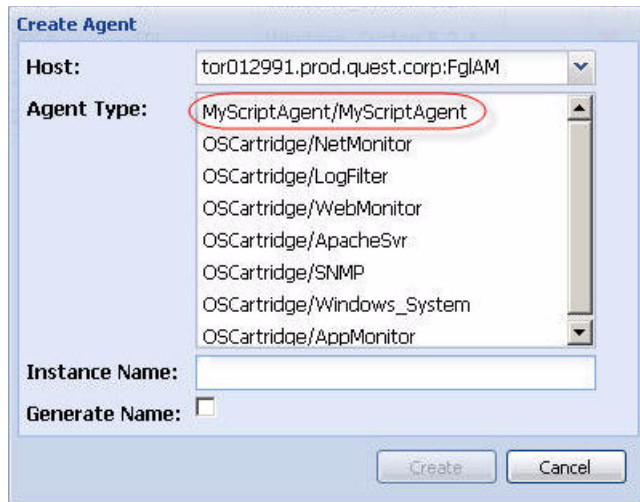
2 Specify the host that you want to monitor with the script-based agent instance that you are about to create.

Note In order to select the host, the vFoglight Agent Manager must be up and running on the monitored host.

In the **Create Agent** dialog box, click **Host** and select the monitored host computer.

The Agent Type box refreshes, showing a list of agent types that can be created on the selected host. The script agent package that you deployed to the monitored host in "Deploying Script Agent Packages" on page 454 appears in the list.

The list reflects the cartridges that have been installed, enabled, and deployed to the monitored host.

3 Select the script agent to use as a type for the agent instance you are about to create.

> **Note** You can only create instances of those agents whose types have already been deployed to the monitored host.

In the **Agent Type** box, click script agent type whose package you deployed in "Deploying Script Agent Packages" on page 454.

For example, **MyScriptAgent/MyScriptAgent**.

4 Specify the name of the agent instance that you are about to create.

- To assign a specific name to the agent instance, in the **Instance Name** box, type that name. For example, MyAgent.
- To assign a generic name, select the **Generate Name** check box.

5 Click **Create**.

The **Create Agent** dialog box closes and the **Create Agent Results** dialog box appears, showing the status of the operation.
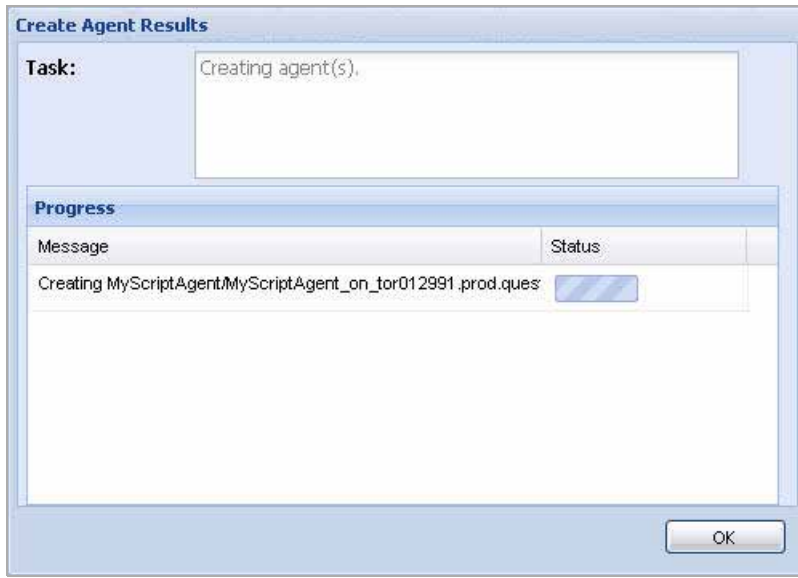
After a few moments, in the **Create Agent Results** dialog box, in the **Status** column of the **Progress** table, a green check mark appears, indicating a success of the operation.
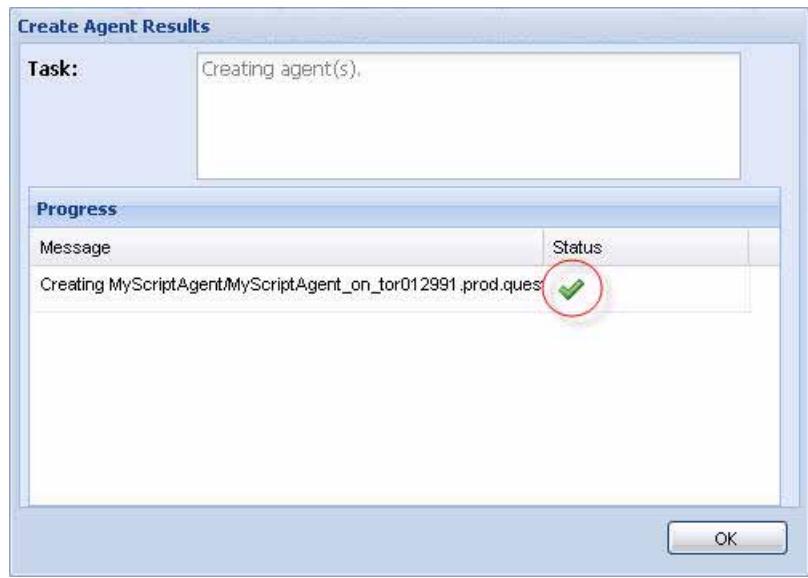
The Agent Status dashboard, refreshes, showing the newly-created agent instance.

6   Activate the newly-added script agent instance.

   a   In the **Agent Status** area, select the row containing the script agent instance and click **Activate**.

       The **Agent Operation** dialog box appears, showing the status of the activation process.
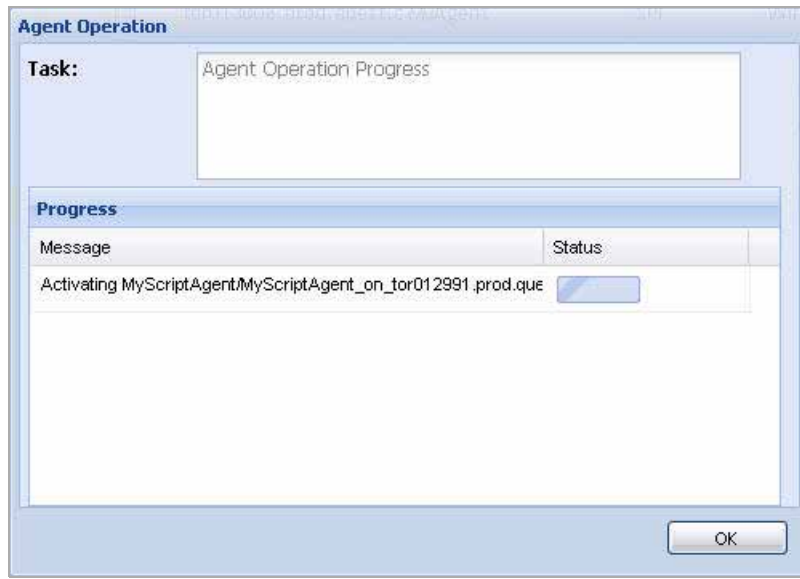
After a few moments, in the **Agent Operation** dialog box, in the **Status** column of the **Progress** table, a green check mark appears, indicating a success of the operation.
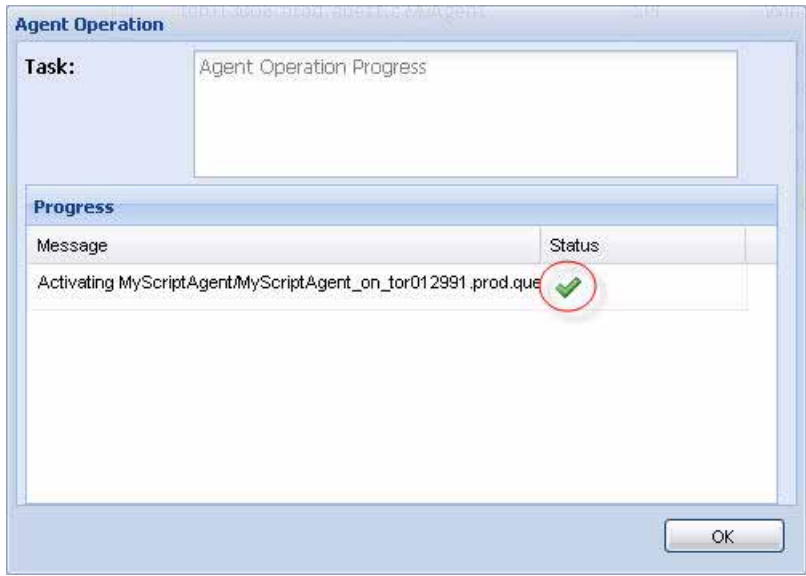
b   In the **Agent Operation** dialog box, click **OK**.

The **Agent Operation** dialog box closes and the **Agent Status** area refreshes, showing the Activated icon (■) and Collecting Data icon (▶) in the row containing the script agent indicating that the agent is active and collecting data.
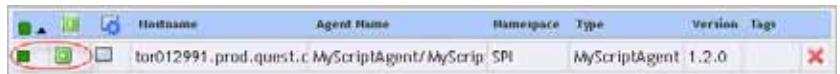
Note   It may take some time for the Activated (■) and Collecting Data (▶) icons to appear even if activation of the agent was successful.

The Activated icon appears when the Management Server has confirmed that the agent has started and is running.

If the activation command was executed successfully but the agent fails after starting, the Activated icon will not appear.

Editing Script Agent Properties

In some cases you might need to edit the properties of the newly-created script agent. For example, Type 1 script agents control their standby periods using agent properties. For more information, see "Building Script Agents" on page 448 and "Example: Type 1 Script" on page 466.

Use the Agent Status area in the Build Script Agent dashboard to begin editing agent properties.

To edit the properties of a script agent:

Note   This procedure continues from "Deploying Script Agent Packages" on page 454.

---

1   On the Build Script Agent dashboard, in the **Agent Status** area, select the row containing the script agent whose properties you want to edit.

2   Click the **Edit Properties** button at the bottom.

The Build Script Agent dashboard refreshes, showing the properties of the selected script agent instance.
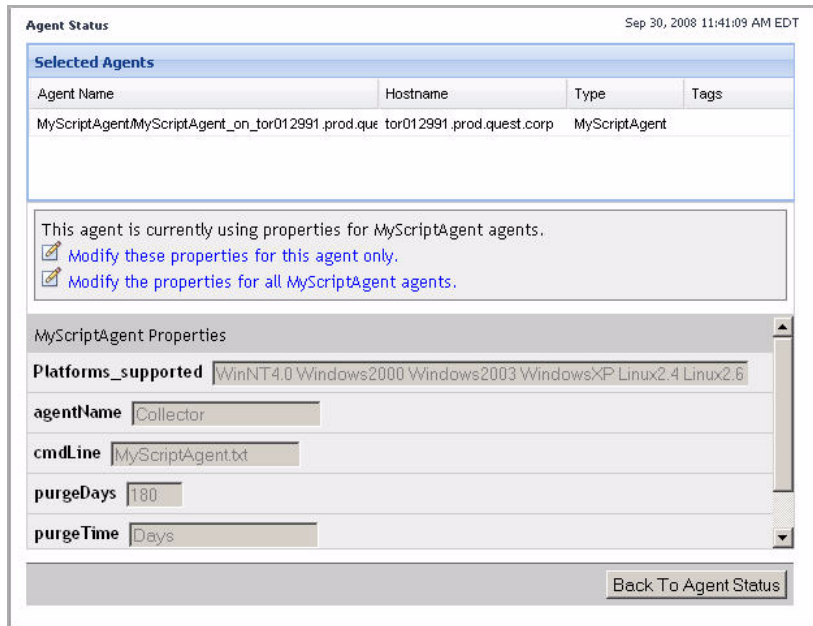
Note The type and range of script agent properties depends on the script that you used to build the agent.

3 Click **Modify these properties for this agent only**.

The boxes in the agent properties area become enabled for editing.
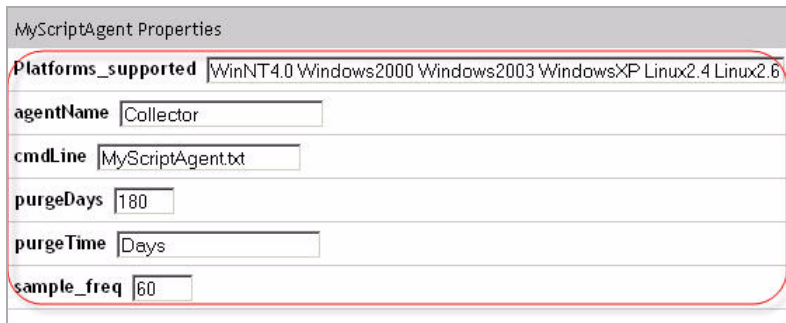
4 In the agent properties area, edit the script agent properties as required.

5 Save your changes.

Click **Save**.

The Build Script Agent dashboard refreshes, showing a list of all agent instances.

Example: Type 1 Script

The following is an example of a Type I script:

```
@echo off
if not "%ECHO%"=="" echo %ECHO%
if not "%OS%"=="Windows_NT" goto EXIT
if "%sample_freq%"=="" set sample_freq=60
echo LOG Start collecting data for NT at %sample_freq% seconds
echo TABLE NT
echo START_SAMPLE_PERIOD
echo FooId.String.id = Bar
echo stringProp.String = This is a non-identity string property.
echo intProp.Integer = 30
echo countMetric = 40
echo timeMetric:second = 50
echo rateMetric:count/second = 50
echo fancyMetric:[4 kilobyte] = 50
echo intWithUnit.Integer:[minute] = 60
echo stringObs.StringObservation.obs = Hello World
echo END_SAMPLE_PERIOD
echo START_SAMPLE_PERIOD
echo FooId.String.id = Another Bar
echo stringProp.String = This is a non-identity string property.
echo intProp.Integer = 31
echo countMetric = 41
echo timeMetric:second = 51
echo rateMetric:count/second = 51
echo fancyMetric:[4 kilobyte] = 51
echo intWithUnit.Integer:minute = 61
echo stringObs.StringObservation.obs = abc
echo END_SAMPLE_PERIOD
echo END_TABLE
```

Example: Type 2 Script

The following is an example of a Type II script:

```
@echo off
if not "%ECHO%"=="" echo %ECHO%
if not "%OS%"=="Windows_NT" goto EXIT
if "%sample_freq%"=="" set sample_freq=60
echo LOG Start collecting data for NT at %sample_freq% seconds
:Loop
echo LOG New sample is available
echo TABLE NT
echo START_SAMPLE_PERIOD
echo FooId.String.id = Bar
echo stringProp.String = This is a non-identity string property.
echo intProp.Integer = 30
echo countMetric = 40
echo timeMetric:second = 50
echo rateMetric:count/second = 50
echo fancyMetric:[4 kilobyte] = 50
echo intWithUnit.Integer:[minute] = 60
echo stringObs.StringObservation.obs = Hello World
echo END_SAMPLE_PERIOD
echo START_SAMPLE_PERIOD
echo FooId.String.id = Another Bar
echo stringProp.String = This is a non-identity string property.
echo intProp.Integer = 31
echo countMetric = 41
echo timeMetric:second = 51
echo rateMetric:count/second = 51
echo fancyMetric:[4 kilobyte] = 51
echo intWithUnit.Integer:minute = 61
echo stringObs.StringObservation.obs = abc
echo END_SAMPLE_PERIOD
echo END_TABLE
"../bin/rapssleep" %sample_freq%
goto :Loop
:EXIT
```

Retrieving Data with Queries and Scripts

vFoglight query language allows you to drill down through the topology model in your
monitoring environment and retrieve data objects as required. The query language
allows you to select one or more topology objects and run scripts against them to

retrieve desired results. For more information about the query language and its syntax, see "Using the Query Language" on page 473.

You may be required to run scripts at the request of Vizioncore Support or for other maintenance functions. You can also test sample scripts from this window. This tool has no restrictions, but is recommended for advanced users.

Use the Script Editor dashboard to display the instances of particular topology types in your monitoring environment, and drill down through their objects to see detailed information on each type. For instructions, see the following sections:

- "Accessing the Script Editor Dashboard" on page 468
- "Selecting Topology Objects" on page 469
- "Retrieving Data" on page 472

Accessing the Script Editor Dashboard

The Script Editor dashboard allows you to select topology objects that exist in your monitoring environment and retrieve information about those objects.

To access the Script Editor dashboard:

Note   This procedure continues from "Getting Started with the Administration Module" on page 32.

---

1   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow ▶ on the left.

2   On the navigation panel, under **Dashboards**, choose **Administration > Tooling > Script Editor**.

    The Script Editor dashboard appears in the display area.
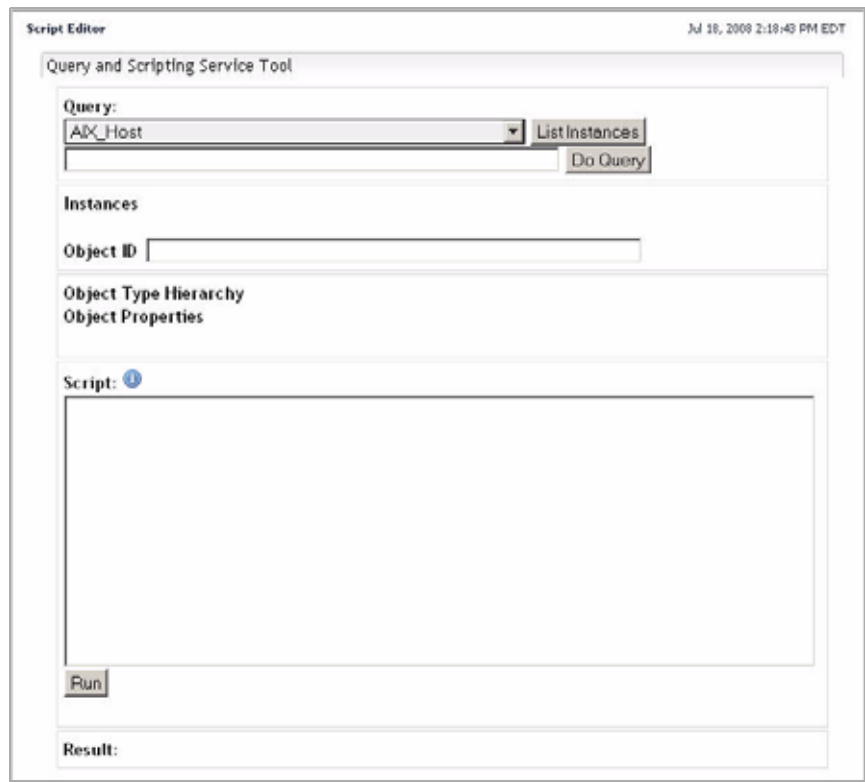
From here, you can go to "Selecting Topology Objects" on page 469.

Selecting Topology Objects

Once you access the Script Editor dashboard, you can use it to select the objects of a particular topology type and view the data that they contain. When you select topology objects, use the Query button to display the following information about a selected topology type:

- Instances
- Instance names
- Object IDs

- Object type hierarchies
- Object properties, including:
  - Unique ID
  - Object ID
  - ID
  - Version
  - Effective start date

To select topology objects:

Note   This procedure continues from "Accessing the Script Editor Dashboard" on page 468.

---

1   Select a topology type whose objects you want to query.

In the Script Editor dashboard, click **Query**, and select a topology type from the list that appears. For example, to select all objects of the Host topology type, select **Host**.

2   List all instances of the selected topology type.

Click **List Instances**.

The **Instances** area refreshes, showing all instances of the selected topology type and also any objects whose type is inherited from the selected topology type. For example, if you selected the Host topology type, the **Instances** area lists all object instances of that type, showing the following information for each topology object:

- Topology object ID
- Topology type
- Instance name.

Topology object ID   Topology type   Instance name
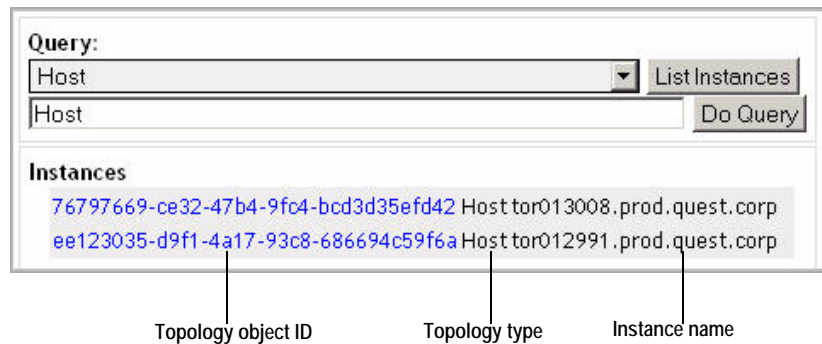
3   View information about one of the listed topology objects.

In the **Instances** box, click a topology object ID.

The **Object ID**, **Object Type Hierarchy**, and **Object Properties** boxes refresh, showing the information about the selected topology object instance.
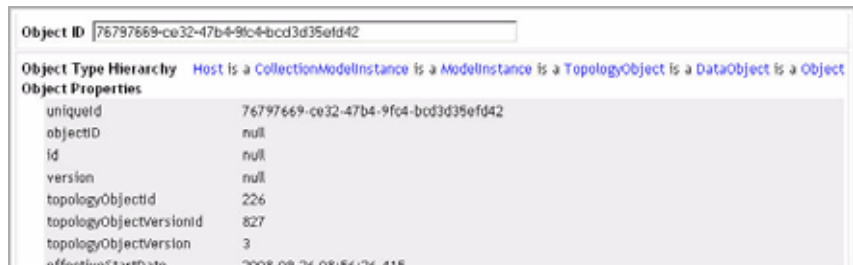
The **Object Type Hierarchy** area displays the hierarchical relationship between the selected topology type and its parent types. The parent types appear as selectable items in the hierarchical listing. If you click on any of the parent types, the **Instances** box refreshes, showing the entire set of instances for the parent type.

4   Observe the object properties.

Use the scroll bar on the right to view the values contained in the object properties.

From here, you can go to "Retrieving Data" on page 472.

Retrieving Data

Once you retrieve information about one or more topology objects, you can run scripts against a selected topology object and retrieve the data that it contains as required.

The Script Editor dashboard allows you to write and run scripts using the vFoglight query language and process scoping queries against one or more topology objects that exist in your monitoring system.

The query language allows you to specify the scope for a rule or derived metric. A rule or derived metric must be scoped to a topology type and can optionally be scoped to specific instances (topology objects) of that type. The expression that sets the rule or derived metric scope is called a scoping query. For more information about the query language, see "Using the Query Language" on page 473.

To retrieve data:

Note   This procedure continues from "Selecting Topology Objects" on page 469.

---

   1   Using the Groovy language, write a script to retrieve information about the selected object. For information about the Groovy language, see"Using the Query Language" on page 473.

       In the Script Editor dashboard, in the **Script** box, type your script.

   2   Run your script.

       Click **Run**.

       The **Result** area refreshes, showing the data retrieved as a result of your script.

10

Using the Query Language

A query language is used in vFoglight to set the scope for rules and derived metrics, to create rule conditions and expressions, to reference expressions in messages, and to create derived metric expressions.

This appendix contains the following sections:

Using the Query Language to Set the Rule or Derived Metric Scope

The scope of a rule defines the set of topology objects against which it will run. The scope of a derived metric defines the set of topology objects to which it applies. A rule or derived metric must be scoped to a topology type and can optionally be scoped to specific instances of that type (topology objects). If a rule or derived metric is not scoped to specific objects, it applies to all objects of that type.

You specify the scope for a rule or derived metric using the query language. The expression that sets the rule or derived metric scope is called a scoping query.

Setting the Scope for a Rule or Derived Metric

vFoglight provides controls that allow you to insert the topology type, specific topology objects, properties of the topology type, and syntactic elements of the scoping query into the scoping expression.

You can use the controls described below to build the scoping query. You can also specify all or part of the rule or derived metric scope manually. See "Specifying the scoping query manually" on page 479 for examples of the syntax that must be used in a scoping query.

Note   The **Rule Scope** and **Derived Metric Scope** fields are case-sensitive.

Inserting topology types

A rule or derived metric can be scoped to a topology type.

To insert the topology type into a scoping query:

   1   Click **Topology Type** and select a topology type from the list that appears.

   2   Click the Append button ( ) to the right of the **Topology Type** box.

       The name of the newly-selected topology type appears in the box immediately below the **Topology Type** box.

   3   Complete one of the following steps.

- Scope down to a property of the selected topology type by proceeding to "Inserting topology type property names" on page 475.

or

- Validate the rule scope by clicking the Validate Scope button (✓) to the right of the **Property** box.

  If the scope is valid, a confirmation message appears above the **Topology Type** box while the name of the newly-selected topology type appears in the box at the bottom.

Note You must select a topology type before you can use the **Property** drop-down menu or launch the **Scoping Query Editor**.

Inserting topology type property names

You can optionally specify that a rule or derived metric be scoped to instances to the selected topology type with a particular property value.

To insert a topology type property name into a scoping query:

Note This procedure continues from "Inserting topology types" on page 474.

---

1 In the box immediately below the **Topology Type** and **Property** boxes that already contains the topology type name, edit the logical expression that matches the rule scope.

   For example, if you want to write a query for the instances of the selected topology type with a property that contains a a particular value, edit the logical expression as follows:

   ```
   TopologyType where property = "value"
   ```

   Where *TopologyType* is the topology type you selected in "Inserting topology types" on page 474.

   For more information about the query language syntax, see "Specifying the scoping query manually" on page 479.

2 Specify the property name you want to query.

   a In the above expression, select property.

   b Click **Property** and select the property name from the list that appears.

   c Click the Append button (⬆) to the right of the **Property** box.

The name of the newly-selected property appears in the expression immediately below the **Property** box.

3 Specify the property value for which you want to query.

In the above expression, select value and replace it with the property value.

4 Validate the scope by clicking the Validate Scope button (✓) on the right.

If the scope is valid, a confirmation message appears above the **Topology Type** box while the name of the newly-edited expression appears at the bottom.

Note You can also use the controls in the **Scoping** Query **Editor** to build a scoping query that uses the correct syntax and then insert it into the **Rule Scope** or **Derived Metric Scope** field. See Restricting the scope to topology objects below for instructions.

Restricting the scope to topology objects

When you select a topology type, use the Scoping Query Editor dialog box to narrow down the scope for a rule or derived metric. The controls in this dialog allow you to select an instance of a topology type insert them into the scoping expression as required.

To open the Scoping Query Editor dialog box:

Note This procedure continues from "Inserting topology types" on page 474.

---

1 Click the Scoping Query Editor button (🔧).

The **Scoping Query Editor** dialog box appears.
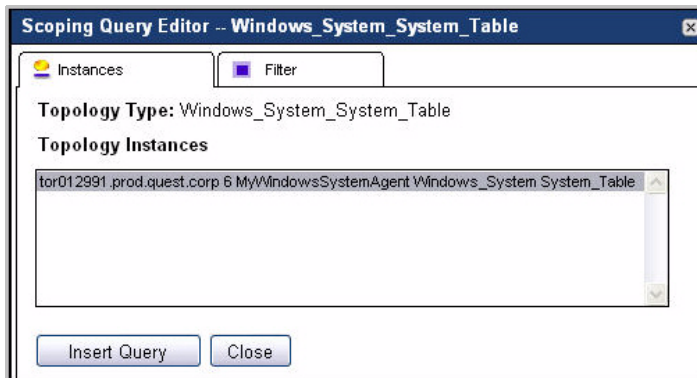
From here, you can proceed to any of the following procedures:

Inserting topology object instances

When you specify a topology type, you can select an object instance of that type and insert it into the scoping query using the Scoping Query Editor dialog box.

To insert a topology object into the scoping query:

Note This procedure continues from

---

1 In the **Scoping Query Editor** dialog box, ensure that the **Instances** tab is open.

2 Select a topology object instance.

   In the **Topology Instances** box, select the object instance.

3 In the display area, in the box immediately below the **Topology Type** and **Property** boxes, place the cursor where you want to insert the new segment of the scoping query.

   If that box is empty, a complete scoping query (including the topology type you selected) will be inserted into it.

4 In the **Scoping Query Editor** dialog box, click **Insert Query**.

   The **Scoping Query Editor** dialog box closes and the scoping query (or scoping query segment) appears in the box immediately below the **Topology Type** and **Property** boxes.

5 Validate the scope by clicking the Validate Scope button (✓) on the right.

   If the scope is valid, a confirmation message appears above the **Topology Type** box while the name of the newly-edited expression appears at the bottom with the topology type instance referenced with its uniqueID property.

Filtering through topology type properties

When you specify a topology type, you can select an object instance of that type using the type's property values as a filter and insert the instances whose properties match the filter into the scoping query using the **Scoping** Query Editor dialog box.

To specify topology type properties:

> **Note** This procedure continues from "Restricting the scope to topology objects" on page 476.

1 In the **Scoping Query Editor** dialog box, click the **Filter** tab.

The **Filter** tab opens in the **Scoping Query Editor** dialog box, allowing you to create a logical expression containing up to three comparison expressions that are connected with "AND" or "OR" logical operators.
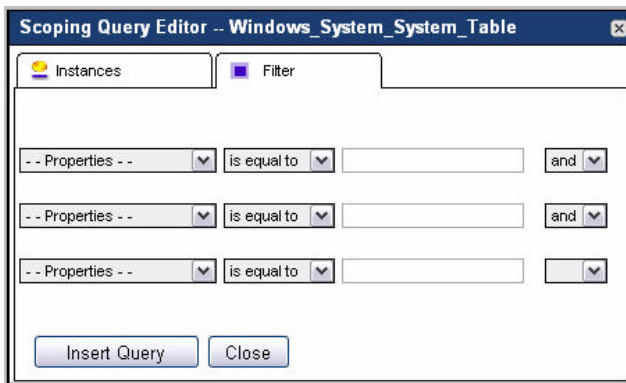
2 To specify a comparison expression, complete the following steps.

a In the **Filter** tab, click **Properties** and select a property.

b Click **is equal to** on the right and select a logical operator from the list that appears: **is equal to**, **is not equal to**, **is like**, or **is not like**.

c In the box to the right of the one containing the newly-selected logical operator, type the property value that you want to use in the filter.

3 If you do not want to add more comparison expressions to the filter, click **and** on the right and select the blank entry.

4 If you want to add more expressions to the filter, repeat step 2 and set the logical operators at the end of each line as required.

> **Note** If you need to define more than three expressions in the filter, you can add them after closing the **Scoping** Query Editor dialog box.

5 Click **Insert Query**.

The **Scoping Query Editor** dialog box closes and the scoping query (or scoping query segment) appears in the box immediately below the **Topology Type** and **Property** boxes.

6 Validate the scope by clicking the Validate Scope button (✓) on the right.

If the scope is valid, a confirmation message appears above the **Topology Type** box while the name of the newly-edited expression appears at the bottom with the topology type instance referenced with its `uniqueID` property.

Specifying the scoping query manually

You can use the syntax shown in one of the examples below to manually specify all or part of the scoping query in the box immediately below the **Topology Type** and **Property** boxes.

Note   In addition to the examples shown below, there are many different ways of specifying a scoping query. These examples are simply provided as guidelines with regard to the query language syntax.

Examples

- You can scope the rule or derived metric to a specific, named topology object by using the syntax

  ```
  <TopologyType> where name ="<Object>"
  ```

  where `TopologyType` is the name of the topology type of which `Object` is an instance and `Object` is the specific instance to which you want the rule or derived metric to be scoped.

- You can scope the rule or derived metric to multiple similarly-named topology objects of a certain type by using syntax similar to

  ```
  <TopologyType> where name like "%<Object>"
  ```

  where `TopologyType` is the name of the topology type of which the topology objects with names like `Object` are instances. In the example shown above, the % wildcard causes the rule or derived metric to be scoped to all topology objects (of the specified type) with names that end with what you specify in place of `Object`.

- You can cause the rule or derived metric to be scoped to all topology objects of a specific type except for a single, named instance by using the syntax

  ```
  <TopologyType> where name ! ="<Object>"
  ```

where `TopologyType` is the name of the topology type of which `Object` is an instance and `Object` is the specific instance to which you do not want the rule or derived metric to be scoped.

• You can cause the rule or derived metric to be scoped to all topology objects of a specific type except those that have names like that of a certain instance by using the syntax

```
<TopologyType> where name ! like "%<Object>%"
```

where `TopologyType` is the name of the topology type of which the instances with names like `Object` are instances. In the example shown above, the % wildcards cause the rule or derived metric to be scoped to all topology objects (of the specified type) with names that do not include what you specify in place of `Object`.

• You can cause the rule or derived metric to be scoped to all topology objects of a specific type except two named instances by using the syntax

```
<TopologyType> where name != "<Object1>" or name !=
    "<Object2>"
```

where `TopologyType` is the name of the topology type of which `Object1` and `Object2` are instances; `Object1` and `Object2` are the instances to which the rule or derived metric will not be scoped.

Using the Query Language in Rule Conditions or Derived Metric Expressions

A condition is the part of a rule that is evaluated against monitoring data. When creating a simple rule or when configuring a severity level for a multiple-severity rule, you must specify a condition using the query language.

The query language is also used to specify the expression for a derived metric. The derived metric is calculated based on this expression.

About the Query Language in Rule Expressions and Messages

You can create expressions and messages in the **Expression/Message** box on the **Rule Variables** tab or the **Severity Level Variables** tab for a rule severity level.

Expressions must be specified using the query language, and the syntax `@expressionName` must be used to reference expressions in messages.

Tip   If you want to include an email address in a message, simply use the @ symbol twice. For example:
Send email to administrator@@example.com

Note   The expressions that you can reference in a message vary depending on the scope of the message. See Chapter 6, "Adding severity-level variables" on page 256 for details.

You can also reference registry variables in expressions using the syntax `registry("registryVariableName")`.

Examples

- You are editing a simple rule that is scoped to the topology type `JVM`; the condition for the rule is `#threads_started#>10`. You want to create a message (to use as the text of the email that is sent when the rule fires) that includes the value of the `#threads_started#` metric at the time when the rule fires.

  Using the controls on the **Severity Level Variables** tab of the **Fire** tab, you create an expression called `threadsNum` whose value is `#threads_started#`. You then create a message called `ProblemSynopsis`. The value that you set for this message is:

  ```
  Threads started count is too high: @threadsNum
  ```

  In this message, the at sign '@' is used to reference the `threadsNum` expression. When the message shown above is included in the email, `@threadsNum` will be replaced by the number of threads that were started at the time when the rule fired.

- There is a registry variable called `CPUFatal` whose value is `90` for the topology object to which the rule you are editing is scoped. You want to reference this variable in the alarm message for the rule's Fatal severity level, so you create an expression called `CPU` whose definition is `registry("CPUFatal")`. You then reference this expression in the rule's alarm message: `CPU usage is at @CPU%`.

Specifying a Rule Condition or Derived Metric Expression

vFoglight provides controls above the **Condition** field (for a rule) or the **Expression** field (for a derived metric) that allow you to insert elements into the condition or

expression that are either part of the query language or have been formatted to use the query language syntax. The process of writing expressions is described in the following sections:

- "Inserting operators" on page 482
- "Editing conditions and expressions" on page 482
- "Validating conditions or expressions" on page 490

Inserting operators

The available operators are listed along the top of the **Condition** and **Expression** boxes. These operators are part of the query language.

To insert an operator into a rule condition or derived metric expression:

1 Place the cursor in the **Condition** or **Expression** box where you want to insert the operator.

2 Click the button for that operator.

Editing conditions and expressions

The Condition Editor (rules) and Expression Editor (derived metrics) dialog boxes allow you to insert registry variables, metrics, and Groovy functions into rule conditions or derived metric expression.

To get started with editing conditions or expressions:

Note This procedure continues from "Inserting operators" on page 482.

- Click the Condition Editor (rules) or Expression Editor (derived metrics) button ( ).

  The **Condition Editor** (rules) or **Expression Editor** (derived metrics) dialog box appears.
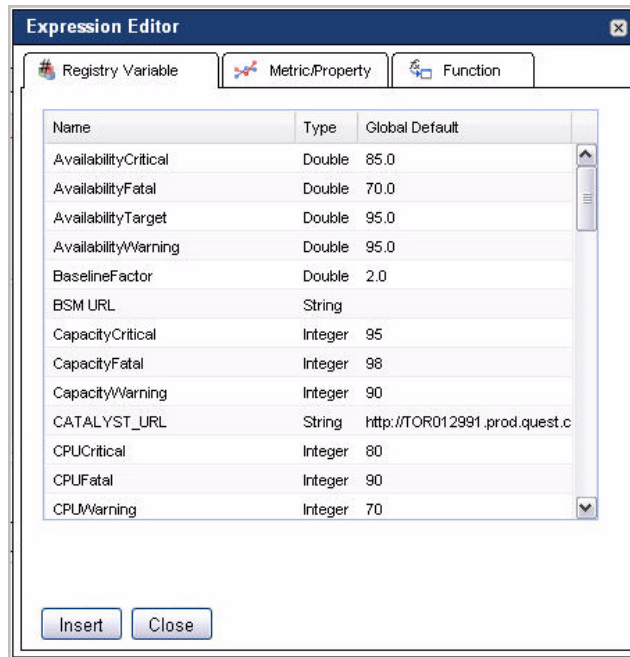
From here, you can proceed to any of the following procedures:

- "Inserting registry variables" on page 483
- "Inserting metrics and topology object properties" on page 484
- "Inserting Groovy functions" on page 487

Inserting registry variables

Caution	Although you can insert a registry variable into a derived metric expression, it is not recommended that you do so.
	Using a registry variable in a derived metric expression could lead to unpredictable and confusing results since the resulting metric might change its definition at different points in time.

The Registry Variable tab in the Condition Editor (rules) and Expression Editor (derived metrics) dialog box lists the registry variables that are available based on the rule or

derived metric scope. Each registry variable's type and global default value also appear in this table.

Note   The list of registry variables displayed in this table is based on the list shown on the *Manage Registry Variables* dashboard (Administration > Rules & Notifications > Manage Registry Variables). This table is empty if no registry variables are available for the associated topology type.

To insert a registry variable into the rule condition or derived metric expression:

Note   This procedure continues from "Editing conditions and expressions" on page 482.

---

    1 In the display area, place the cursor in the **Condition** box (rules) or **Expression** box (derived metrics) where you want to insert the variable.

    2 In the **Condition Editor** (rules) or **Expression Editor** (derived metrics) dialog box, ensure that the **Registry Variable** tab is open.

    3 In the **Registry Variable** tab, select a variable from the list, and click **Insert**.

       The dialog box closes and the **Condition** (rules) or **Expression** (derived metrics) box refreshes, showing the newly-added variable.

From here, you can proceed to "Validating conditions or expressions" on page 490.

Inserting metrics and topology object properties

The Metric/Property tab in the Condition Editor (rules) and Expression Editor (derived metrics) dialog box lists the metrics and topology object properties that are available based on the scope of the rule or derived metric. This tab allows you to navigate through lists of topologies, metrics, and instances associated with the rule.

The initial view of this tab lists three groups of topology types:

- **Scoping Topology**: Shows a single scoping topology type included in this category. If the rule or derived metric is not scoped, this area is empty.

- **Child Topology**: Lists the descendents of the scoped topology type.

- **Other Topology**: Lists the following topology types:

  - Core vFoglight topologies

  - All topology types that belong to the same cartridge containing the rule or derived metric whose condition or expression you are editing. If the rule or derived metric does not belong to a cartridge, this area includes all topology types without a cartridge association.

• Parent types of the scoping topology type that descend from
  `TopologyObject`.

To insert a metric or property into a rule condition or derived metric expression:

Note This procedure continues from "Editing conditions and expressions" on page 482.

1 In the display area, place the cursor in the **Condition** box (rules) or **Expression**
   box (derived metrics) where you want to insert the metric.

2 In the **Condition Editor** (rules) or **Expression Editor** (derived metrics) dialog
   box, click the **Metric/Property** tab.

   The **Metric/Property** tab shows lists three groups of topology types: **Scoping
   Topology**, **Child Topology**, and **Other Topology**.
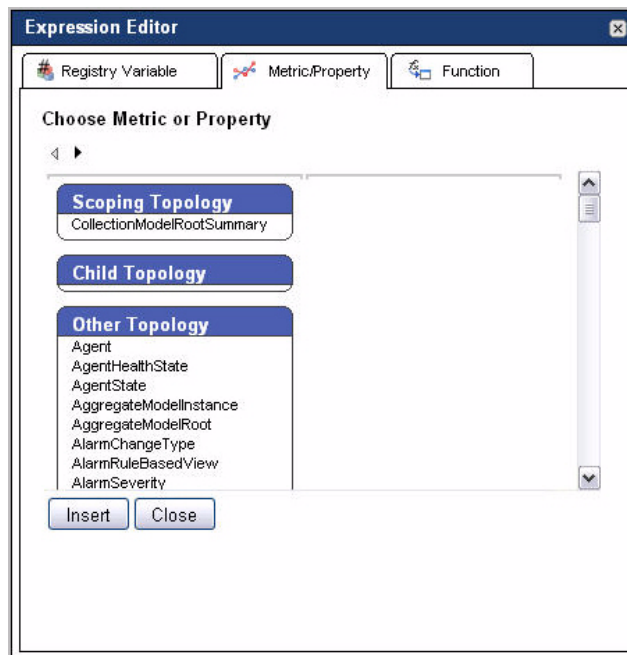
3 Choose a topology type and display its metrics and instances.

   Select a topology type from one of the following panes **Scoping Topology**, **Child
   Topology**, or **Other Topology**.

The **Metric/Property** tab refreshes, showing the instances and metrics for the selected topology type.
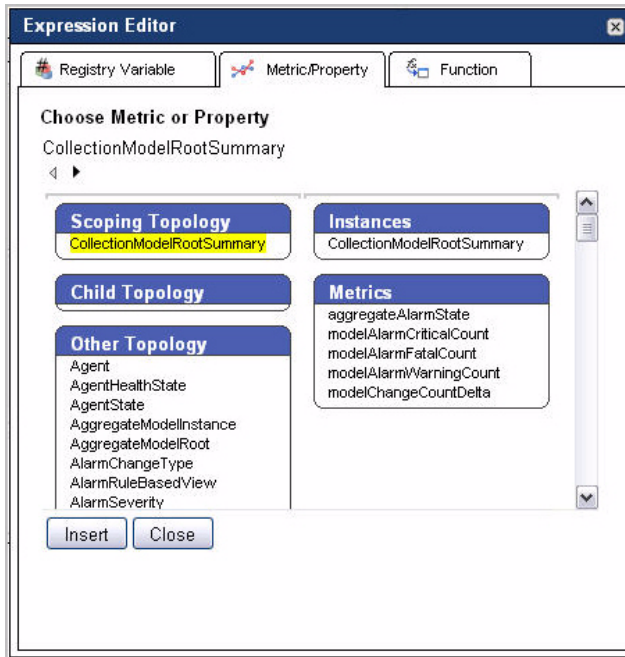
4 Choose a metric or an instance.

The **Metric/Property** tab displays only two columns at a time, causing the initial list of topology types to shift to the left. Use the arrow buttons in the upper-left to navigate through the window. A breadcrumb trail displays the metrics and properties you have chosen

• To select a metric, in the **Metrics** pane, click the metric.

Note If you choose a metric, you cannot navigate further in this dialog box.

or

• To select an instance, in the **Instances** pane, click the instance name.

The **Metric/Property** tab refreshes, showing the list of properties for the selected instance.
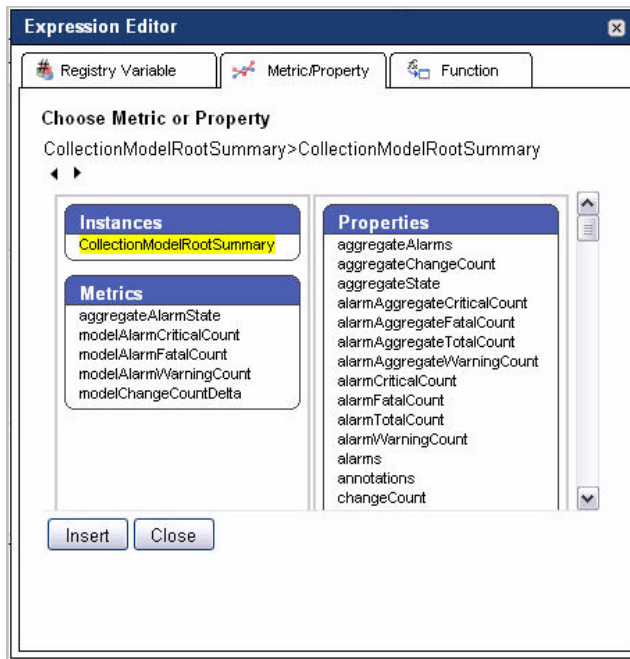
In the Properties pane, select the property that you want to add to the condition (rules) or expression (derived metrics).

    a Choose a property from the list.

  5 Click the **Insert** button.

The dialog box closes and the **Condition** (rules) or **Expression** (derived metrics) box refreshes, showing the newly-selected instance or metric.

From here, you can proceed to "Validating conditions or expressions" on page 490.

Inserting Groovy functions

The Function tab in the Condition Editor (rules) and Expression Editor (derived metrics) dialog box includes controls for inserting Groovy functions into rule conditions or derived metric expressions. It lists the functions that you can use in conditions and expressions. The functions that you see on this tab are defined in the vFoglight database. For a full list of functions and their descriptions, see "Using Functions with Conditions and Expressions" on page 491.

To insert a Groovy function into a rule condition or derived metric expression:

> **Note** This procedure continues from "Editing conditions and expressions" on page 482.

1 In the display area, place the cursor in the **Condition** box (rules) or **Expression** box (derived metrics) where you want to insert the function.

2 In the **Condition Editor** (rules) or **Expression Editor** (derived metrics) dialog box, click the **Function** tab.

   The **Function** tab opens in the dialog box.
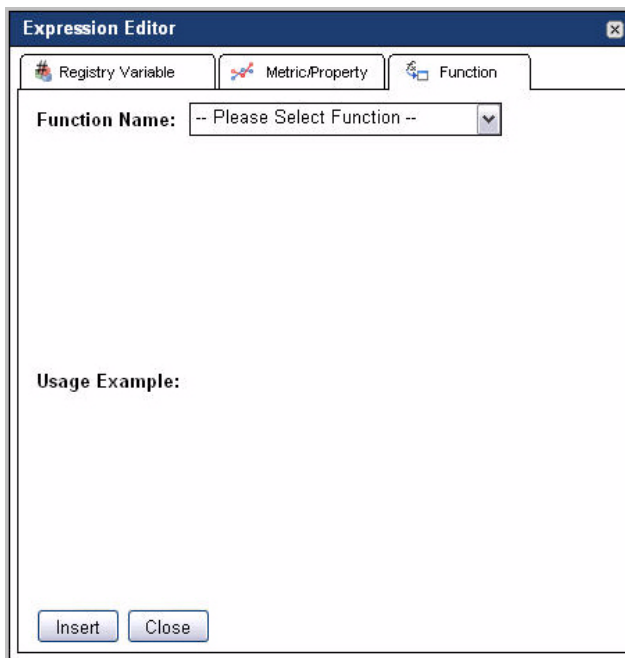
3 Choose the Groovy function that you want to add to your condition or expression.

   Click **Function Name** and select a function from the list.

   The **Function** tab refreshes, allowing you to specify the arguments for the selected function and shows usage examples.
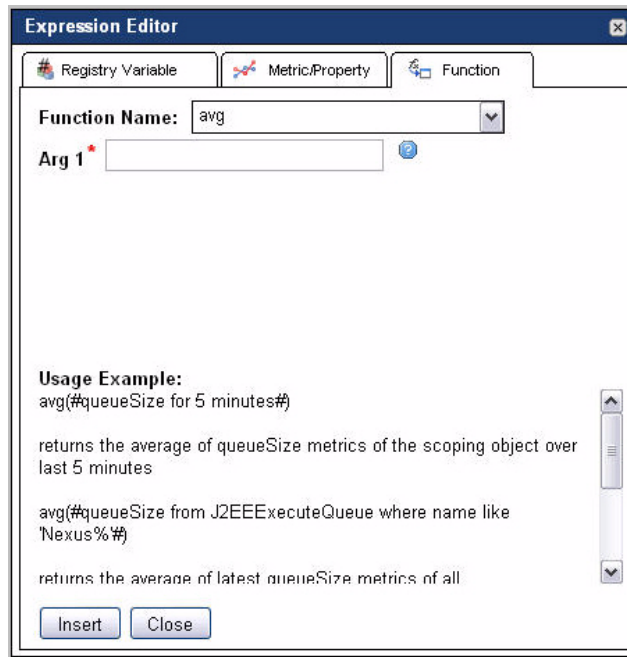
4 Specify the function arguments as required using one or more **Arg** boxes.

The first argument represents the object on which the function will be performed, such as a metric (specified using the format #metric#) or a topology object within the rule or derived metric scope (specified as scope). See "Using Functions with Conditions and Expressions" on page 491 for more information.

> **Tip** Hover the cursor over the question mark icon (⊙) next to one of the argument fields to make a tooltip appear. This tooltip states which type of parameter is expected for that field.

5 Click the **Insert** button.

The dialog box closes and the **Condition** (rules) or **Expression** (derived metrics) box refreshes, showing the newly-added function.

From here, you can proceed to "Validating conditions or expressions" on page 490T

Validating conditions or expressions

When you have finished editing the rule condition or derived metric expression, you can validate its syntax.

To validate a condition or expression:

Note This procedure continues from ".

- Click the Validate button (✅) above the **Condition** (rules) or **Expression** (derived metrics) box.

If the syntax is correct, a success message appears above the **Condition** (rules) or **Expression** (derived metrics) box.

Examples

- You are configuring the Critical severity level for an existing rule that scoped to all requests with names that include the element *jdbc* (the rule scope is `RequestType where name like "%jdbc%"`). You want an alarm to be fired for this level if the average execution time (over the last hour) for a request in the rule scope exceeds the limit set by the registry variable `ExecuteTimeCritical`.

  You select the rule from the Manage Rules dashboard to open it for editing and use the fields and controls on the **Critical** pane to create the condition for this severity level.

  After launching the **Condition Editor** dialog box, open the **Function** tab and select **avg** from the **Function Name** box. You then specify the argument for the selected function in the **Arg1** field. For example, specify the execution time as an argument for this function by typing `#executionTime for 1 hour#` in the **Arg1** field. Then click **Insert** to insert the function. The function and its parameter appear in the **Condition** field.

  To complete the condition, you need to insert the appropriate operator and the registry variable. You place the cursor at the end of the condition and insert the the greater than '>' operator. In the **Condition Editor** dialog box, you switch to the **Registry Variable** tab, select **ExecuteTimeCritical** from the list, and click **Insert**. The condition appears as follows:

  ```
  avg(#executionTime for 1
      hour#)>registry("ExecuteTimeCritical")
  ```

- You are creating a number of rules, each of which is scoped to a different EJB instance. You know that you need to configure the conditions for many of these

rules to perform the same function (rate) on the same metric (#passivationCount#). Instead of doing this manually for each rule, you decide to create a derived metric that you can use in all of these rules' conditions.

You use the fields and controls on the Create Derived Metric dashboard (**Data > Create Derived Metric**) to create a derived metric expression that calculates the passivation rate for EJBs.

After launching the **Expression Editor** dialog box, you open the **Function** tab and select **rate** from the **Function Name** box. You then specify the argument for this function in the **Arg1** field. For example, specify the passivation count as an argument for this function by typing #passivationCount# in the **Arg1** field. Then click **Insert** to insert the function. The function and its parameter appear in the **Condition** field.

```
rate(#passivationCount#)
```

Using Functions with Conditions and Expressions

Derived metric expressions and rule conditions and expressions are matched against monitoring data. vFoglight can perform functions on this data. Functions cause calculations to be performed on the data specified in conditions and expressions, allowing the data to be modified before it is matched.

Most of the default functions available with vFoglight cause calculations to be performed on metrics. In addition, the functions alarmCount, changeSummary, descendents, findObservationEntries, getContainedObjects, and getObservationTrend cause values to be returned for topology objects (based on a specified scope). In most cases, you specify scope as the parameter for one of these functions; using the scope variable causes the function to be performed on the topology objects included in the rule or derived metric scope. However, there may be situations in which you want to specify an alternate scope. See "Advanced scripting example" on page 495 for more information.

The following functions are supported by vFoglight for use with rule conditions and expressions and derived metric expressions:

- alarmCount: Returns the current number of alarms for each topology object referenced by this function's scope parameter.

- avg: Calculates an average (arithmetic mean) from metric values.

  If you are calculating an average for multiple topology objects, vFoglight will calculate an average from the metric values for each object, then calculate a second average from the averages for the objects.

- `changeSummary`: Returns the list of topology property changes for each topology object referenced by this function's scope parameter over the specified time period (supplied in milliseconds).

- `checkObservationAlarms`: Returns a list of all log entry objects with a particular severity.

- `checkUserPermission`: Check the permissions assigned to a user.

- `compareStrings`: Compares two text strings.

- `count`: calculates the number of observations. An observation can be either a metric or a property of a topology object.

- `createObservationAlarms`: Returns a list of all log entry objects with a particular severity.

- `currentUserHasAdvancedOperationsRole`:

- `delta`: calculates the difference between the maximum value of the two most recent samples of a single metric. The delta function is used with metrics whose unit of measurement is count.

- `delta_rate`: calculates the rate per second of the delta.

- `descendents`: returns the set of topology objects that are directly or indirectly contained by each topology object referenced by this function's scope parameter.

- `f4registry`: Returns the value of a given registry variable for the current scoping object.

- `findObservationEntries`: Returns a list of log entry objects with a specified set of properties.

- `generateUUID`:

- `getAlarmSeverities`: Retrieves a list of alarm severities for a given object.

- `getAllMonitoredComponents`: Returns all monitored components in the definition of the scoping object.

- `getContainedComponentsPropertyName`:

- `getContainedObjects`: returns the set of topology objects of the specified type that are directly contained by each topology object referenced by this function's scope parameter.

- `getImpactedServices`: Returns a list of impacted services.

- `getInstalledAgentList`: Returns a list of installed agents for the given vFoglight Agent Manager ID.

- `getMonitoredComponentRuleInfoList`: Returns a list of rules that are scoped to a monitored component.

- `getObservationTrend`: Returns an observation trend.

- `getPropertyObject`: Returns the value of property for the topology object with the given ID.

- `getPropertyValueAtGivenTimesOfGivenTopologyObjects`: Returns the values of a given property for a list of `TopologyObjects` at a given list of times.

- `getPropertyValuesOfTopologyObjectAtGivenTimes`: Returns the values of a given property for a list of `TopologyObjects` at a given time.

- `getRuleAlarmSeveritiesConfigured`: Returns the existing alarm severities that are configured for a rule.

- `getRuleBasedView`: Returns a rule-based view.

- `getRuleBasedViewInput`: Returns a rule-based view input.

- `getRuleBasedViewName`: Returns a rule-based view name.

- `getRuleComment`: Returns a rule comment.

- `getRuleInfoUsingId`: Returns a rule comment given an ID.

- `getSeverityConditions`: Returns a list of severity conditions for a rule.

- `getTopologyPropertyValue`: Returns the value of a topology property for a scoping object at a given date and time

- `help`: Returns a list of supporting information such as scripts or methods as specified by the parameter.

- `histogram`: keeps a histogram to measure the distribution of metric values (for example, for a set of topology objects or for a single object over a specified period of time).

- `isNotNull`: Determines whether a given data object is set to null.

- `last`: Returns a `com.quest.nitro.service.scripting.ObservedDataQueryResult` object which contains the latest metrics for the scoping object if there are any observations made during a given period.

- `max`: Calculates a maximum from metric values.

- `metricDifference`: Returns the difference percentile between two given metric values.

- `min`: calculates a minimum from metric values.

- **period**: calculates the total length of a period of time from a series of metrics and returns a value in seconds.

- **positive_delta**: Returns the difference between the maximal values of the most recent two metric values for a scoping object.

- **positive_delta_rate**: Returns the difference between the maximal values of the most recent two metric values for a scoping object divided by the time period in seconds of the more recent metric value.

- **rate**: calculates the rate of a metric value per second.

- **returnIncludeOrExcludeGivenABoolean**: Determines whether to include or exclude the object given a boolean value.

- **returnObjectsSatisfyingNameFilter**: Returns a given number of objects whose name matches a string pattern specified by the parameter.

- **returnObjectsSatisfyingTypeNameFilter**: Returns a given number of objects whose name matches a string pattern specified by the parameter.

- **stddev**: Calculates the standard deviation from multiple metric values.

- **sum**: Calculates the sum of metric values.

- **updateHostModel**: Updates the Host Model.

Examples

- You are creating a multiple-severity rule that applies to requests for a specific JSP. You want this rule to generate a Warning alarm when there are more than ten requests of this type per second.

  In the **Condition** box on the **Condition** tab of the rule's **Warning** pane, you specify the following:

  ```
  rate(#count#)>10
  ```

- You are creating a simple rule that applies to JDBC requests. You want this rule to fire an alarm if the metric #requestResponseTime# returns values greater than 750 milliseconds more than 10% of the time over the period of an hour.

  In the **Condition** box for the rule's Fire state, you specify a condition similar to the following:

  ```
  metric = #requestResponseTime for 1 hour#
  histo = histogram(metric, [10, 50, 250, 500, 750])
  if (histo[5]/count(metric)>0.1)
      {return true;}
  else
  ```

```
          {return false;}
```

Advanced scripting example

In most cases, you use the `scope` variable as a parameter for the functions `alarmCount`, `descendents`, and `getContainedObjects`. However, there may be a situation in which you need to create a condition or expression that uses one of these functions but want the function to be performed on an object outside of the rule or derived metric scope.

For example, if you wanted to compare the alarm count for objects within the scope of a rule with the alarm count for a specific server that is not within this scope, you could specify a condition using the following syntax:

```
alarmCount(scope) > alarmCount(#!CatalystServer where name =
"Server_IP:1099"#.getTopologyObjects()[0])
```

Where *Server_IP* is the IP address of the server. For example:

```
alarmCount(scope) > alarmCount(#!CatalystServer where name =
"10.4.112.155:1099"#.getTopologyObjects()[0])
```

Note   In the example shown above, the exclamation point '**!**' implies that the argument passed to the `alarmCount` function is a topology object property and not a metric.

Using the Query Language FAQ

This section provides answers to the following FAQs:

- "How do I reference a topology object property in an expression?" on page 495
- "How do I export metrics from the command line?" on page 496

How do I reference a topology object property in an expression?

If the rule is scoped to the topology object that has that property, you can reference the property using the `scope` variable. This variable contains a reference to the topology object against which the expression runs.

For example, you are interested in the property `filesystemName`, you can use the following in an expression to obtain the property value:

```
"File system " + scope.get("filesystemName") + " is now full"
```

If you want to reference the topology object from within a string or embedded query, you must prefix the scope variable with the dollar sign '$'. For example:

```
"File system $scope is now full"
```

or

```
#Filesystem where name = $scope.get("filesystemName")#
```

How do I export metrics from the command line?

The fglcmd tool includes a command that allows you to export metric observations to a file using a metric query. The metricexport command can be used to export metrics to a CSV or XML file.

For example, the following command exports the values of the Process metric collected in the past two hours to a CSV file.

```
C:\Vizioncore\vFoglight\bin>fglcmd -usr foglight -pwd foglight
   -cmd util:metricexport -output_format csv -metric_query
   "Processes from Windows_System_System_Table for 2
   hours" -f my_metric_query.csv
```

For complete details on how to configure fglcmd, and about the util:metricexport command, see the *Command-Line Reference Guide*.

A

Appendix: vFoglight Client Reference

While the new versions of vFoglight use the vFoglight Agent Manager to communicate with vFoglight agents, previous versions used the vFoglight Client. The Administration module and vFoglight command-line interface support both technologies, however, some dashboards in the browser interface as well as vFoglight commands can provide slightly different type of data in monitoring environments that still use the vFoglight Client for agent communication. This appendix shows examples of dashboards and command-line output in an environment that uses the vFoglight Client.

This appendix contains the following sections:

Starting the vFoglight Client

To start the vFoglight Client:

- To start the vFoglight Client, you run the spid executable that is located in the vFoglight Client installation directory. Alternatively, to start the Client on Windows platforms, choose **Start > Programs > Vizioncore > vFoglight SPID 5.2.4 > Start SPID**.

For more information, refer to the *Installation and Setup Guide*.

Note For information on how to start the vFoglight Agent Manager, see "Getting Started with the Administration Module" on page 32.

Viewing the Content of a vFoglight Client Support Bundle

When you create a client support bundle using the support_bundle command, vFoglight saves this data in a ZIP file in the *<vfoglight_home>/support/<user_name>* directory on the computer hosting the vFoglight Client. For more information about this command, see the *Command-Line Reference Guide*.

Client support bundles contain diagnostic data about a vFoglight Client.

To view the content of a client support bundle:

Note This procedure continues from "Managing Support Bundles" on page 75.

---

1 Locate the client support bundle whose content you want to view.

Each client support bundle is contained in a ZIP file in the *<vfoglight_home>/ support/<user_name>* directory on the computer hosting the vFoglight Client.

2 Extract the contents of the ZIP file containing the client support bundle to a local directory.

3 Observe the file structure.

Each client support bundle consists of the following files and directories:

config/

    spid/

        <VERSION>/

            <CACHE>/

                SPI/

                    SPI/

                        <AGENT_NAME>/

                            SPI.xml   SPID configuration file

                SPINetwork/

                    SPINetwork

                        <AGENT_NAME>/

                            Orb.xml   JacORB configuration

                            OrbInitRefs.xml   FMS server location details

logs/

    <CARTRIDGE>/

        <VERSION>/

            logs/   All log files from all deployed agents (OSCartridge, SPID, Oracle, SQL2005, etc) are in this folder.
Additional logs may be present in other directories, depending on the agent and/or platform

manifests/	OPTIONAL (may be present for specific platforms)
<CARTRIDGE>_file_manifest.txt	A file manifest for every cartridge deployed to this SPID installation
osfiles/	OPTIONAL (may be present for specific platforms)
*	Various OS configuration files like *"/etc/hosts"*, depending on the OS platform.

Note For information about the content of vFoglight Agent Manager support bundles, see
"Viewing Audit Information" on page 82.

Browser Interface

This section contains sample screen captures that appear in monitoring environments that use the vFoglight Client for agent communication with the vFoglight Management Server. It includes screen captures for the following dashboards:

- "Agent Properties dashboard" on page 501
- "Agent Status dashboard" on page 502
- "Agent Adapters dashboard" on page 502

Agent Properties dashboard
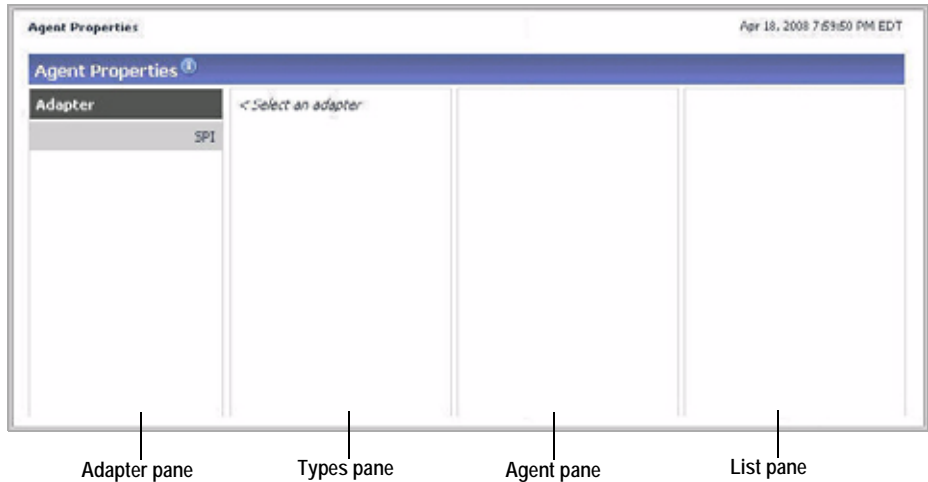
| Adapter pane | Types pane | Agent pane | List pane |

Note   For a sample screen capture of this dashboard in a monitoring environment that uses the vFoglight Agent Manager, see "Accessing the Agent Properties Dashboard" on page 168.

Agent Status dashboard

The Agent Status dashboard shows an entry for the SPINetwork agent that comes with the vFoglight Client.

Agent Adapters dashboard

Command-Line Interface

This section contains **fglcmd** examples and their command-line output that appears when the agent instances in your monitoring environment use the vFoglight Client for communication with the vFoglight Management Server. It includes the following sections:

- "Deploying agent packages" on page 503
- "Creating agent instances" on page 504
- "Retrieving agent logs" on page 505
- "vFoglight Client IDs" on page 506
- "Installer IDs" on page 507

For more information about **fglcmd** and the command-line output that is generated in environments that use the vFoglight Agent Manager for managing agent instances, see the *Command-Line Reference Guide*.

Deploying agent packages

Important The procedure below assumes that the have access to and have configured the **fglcmd** package on the computer you are using to deploy agent packages. For complete instructions, see the *Command-Line Reference Guide.*

To deploy an agent package using the command line:

1 Open a Command Prompt window and navigate to the directory on your computer that contains the uncompressed **fglcmd** package. For example, *<vfoglight_home>/bin.*

   Note For complete information on how to get started with **fglcmd**, see the Command-Line Reference Guide.

2 List the agent packages that are available to the vFoglight Client using the following command syntax:

   ```
   fglcmd -usr user_name -pwd password -cmd agent:types
       -clientname SPI://myhost.mydomain.corp:0
   ```

   An output similar to the following appears, listing all vFoglight Clients and the agent types that are available to them.

   ```
   Client ID: myhost.mydomain#SPI://
   myhost.mydomain.corp:0
   Installer ID: myhost.mydomain#SPI://
   ```

```
myhost.mydomain:0#SpiInstaller/admin
   Agent Package ID: OSCartridge-Windows2003-5.2.4-
      AgentPackage
   Agent Package Cartridge Name: OSCartridge-
      Windows2003
   Agent Package Cartridge Version: 5.2.4
```

3 Review the above output and record the ID of the agent package that you want to deploy.

4 Deploy the agent package using the following command syntax:

fglcmd -usr *user_name* **-pwd** *password* **-cmd**
agent:deploy -packageid
*cartridge_name-cartridge_version-***AgentPackage**
-host *myhost.mydomain.corp*

An output similar to the following appears:

```
Successfully installed package cartridge_name-
   cartridge_version-AgentPackage on
   myhost.mydomain.corp#SPI://
   myhost.mydomain.corp:0#SpiInstaller/admin
```

Creating agent instances

Important The procedure below assumes that the have access to and have configured the **fglcmd** package on the computer you are using to create agent instances. For complete instructions, see the *Command-Line Reference Guide.*

To create an agent instance using the command line:

1 Open a Command Prompt window and navigate to the directory on your computer that contains the uncompressed **fglcmd** package. For example, *<vfoglight_home>/bin.*

Note For complete information on how to get started with **fglcmd**, see the Command-Line Reference Guide.

2 List the agent types that are available to the vFoglight Client using the following command syntax:

fglcmd -usr *username* **-pwd** *password* **-cmd agent:packages**
   -clientname *myhost.mydomain.corp*

An output similar to the following appears, listing all agent types that are available to the specified vFoglight Client.

```
Client ID: myhost.mydomain.corp#SPI://
```

```
            myhost.mydomain.corp:0
    Client Name: SPI://myhost.mydomain.corp:0
    Agent Types:
        NetMonitor
        Windows_System
        WebMonitor
        AppMonitor
        LogFilter
        SNMP
        ApacheSvr
        TerminalServer
```

3 Review the above output and record the type of the agent whose instance you want to create.

4 Create an agent instance using the following command syntax:

> **fglcmd -usr** *username* **-pwd** *password* **-cmd**
>   **agent:create -name** *instance_name* **-type** *agent_type*

If successful, this command does not generate any output.

Retrieving agent logs

Important The procedure below assumes that the have access to and have configured the **fglcmd** package on the computer you are using to retrieve agent logs. For complete instructions, see the *Command-Line Reference Guide.*

To retrieve an agent log using the command line:

1 Open a Command Prompt window and navigate to the directory on your computer that contains the uncompressed **fglcmd** package. For example, *<vfoglight_home>/bin.*

> **Note** For complete information on how to get started with **fglcmd**, see the Command-Line Reference Guide.

2 List the agent log files using the following command syntax:

> **fglcmd -usr** *username* **-pwd** *password* **-cmd agent:logs**
>   **-host** *myhost*

An output similar to the following appears, listing all log files that exist on the specified host.

> *Client ID: tor013008.prod.quest.corp#SPI://*
> *   tor013008.prod.quest.corp:0*
> *Client Name: SPI://tor013008.prod.quest.corp:0*

```
Host Name: tor013008.prod.quest.corp
50 log files found.
OSCartridge\5.2.0\logs\AIX_Console_My_AIX_Console_Agent
    _2008-01-21_095227_001.log
OSCartridge\5.2.0\logs\AIX_MPStat_My_AIX_MPStat_Agent_
    2008-01-21_094945_001.log
OSCartridge\5.2.0\logs\AIX_System_My_AIX_System_Agent_
    2008-01-21_095149_001.log
OSCartridge\5.2.0\logs\ApacheSvr_ApacheSvr_
    2008-01-16_102536_001.log
OSCartridge\5.2.0\logs\ApacheSvr_My_ApacheSvr_Agent_
    2008-01-16_114450_001.log
```

3 Review the above output and record the log file that you want to retrieve.

4 Transfer that log file into a local directory using the following command syntax:

> **fglcmd -usr** *username* **-pwd** *password* **-cmd**
>   **agent:getlog -log** *path_and_name_of_log_file* **-f**
>   *path_and_name_of_destination_file*

If successful, this command does not generate any output.

Note If you pull agent logs into the <vfoglight_home>/logs directory, they will be packaged
as part of the server support bundle. For more information about server support
bundles, see Chapter 2, "Managing Support Bundles" on page 75.

vFoglight Client IDs

Some commands (for example agent:create) require a vFoglight Agent Manager ID
as a parameter. vFoglight Agent Manager IDs identify agent management processes on
remote machines. For agents managed by the vFoglight Agent Manager, vFoglight
Agent Manager IDs identify instances of the vFoglight Agent Manager. Since it is
possible to have several process managers on a monitored host, vFoglight Agent
Manager IDs are more complex than host names.

The vFoglight Agent Manager IDs use the following syntax:

```
<hostname>#SPI://HostName:0/MS
<hostname>#SPI://HostName:0
```

vFoglight Agent Manager IDs for running agent managers can be obtained by executing
the agent:packages command:

```
C:\Vizioncore\vFoglight\bin>fglcmd -usr foglight -pwd foglight
    -cmd agent:types -host MyHost
Client ID: MyHost#SPI://MyHost:0/MS
Client Name: MS
```

```
Agent Types:
----------------------------------
Client ID: MyHost#SPI://MyHost:0
Client Name: SPI://MyHost:0
Agent Types:
    Windows_System
    WebMonitor
    AppMonitor
    LogFilter
----------------------------------
```

Installer IDs

Installer IDs help deploy new agent packages to remote hosts. Installer IDs identify agent managers that are capable of installing agent packages on a remote machine. It is possible to have several such installers within one vFoglight Agent Manager, so installer IDs are more complex than vFoglight Agent Manager IDs.

The vFoglight Agent Manager installer ID uses the following syntax:

HostName#SPI://*HostName*:0#SpiInstaller/admin

In general, each remote installer is capable of handling an agent package of one type. The type of agent package is specified in the respective cartridge manifest file, but is not visible directly through the command line interface. However, agent package types affect the results of the agent:packages command. Given a vFoglight Agent Manager ID as a parameter, the agent:packages command checks the installers that are available on the vFoglight Agent Manager and returns IDs for all agent packages that can be handled by at least one installer on the vFoglight Agent Manager.

```
C:\Vizioncore\vFoglight\bin>fglcmd -usr foglight -pwd foglight
    -cmd agent:packages -clientid
    tor012991.prod.quest.corp#cf238d96-3a56-45d6-a33e-
    b88bb7d4ff55
```

```
Client ID: tor012991.prod.quest.corp#cf238d96-3a56-45d6-a33e-
    b88bb7d4ff55
Installer ID: tor012991.prod.quest.corp#cf238d96-3a56-45d6-a33e-
    b88bb7d4ff55#FglAM:tor012991.prod.quest.corp/cf238d96-3a56-
    45d6-a33e-b88bb7d4ff55/installer
    Agent Package ID: OSCartridge-WindowsXP-5.2.4-OSCartridge-
        Agent-WindowsXP-windows-/5\.1.*/-ia32,x86_64
    Agent Package Cartridge Name: OSCartridge-WindowsXP
    Agent Package Cartridge Version: 5.2.4
    Agent Package OS: windows
```

```
    Agent Package OS Version: /5\.1.*/
    Agent Package OS Architecture: ia32,x86_64
----------------------------------
```

```
C:\Vizioncore\vFoglight\bin>fglcmd -usr foglight -pwd foglight
    -cmd agent:packages -clientid MyHost.#SPI://MyHost:0
Installer ID: MyHost#SPI://MyHost:0#SpiInstaller/admin
Agent Package ID: C:\<foglight_home>\dist\tmp\cartridge.exploded\
    OSCartridge-usrnsupported-WindowsXP-5_1 HEAD_3/20/
090208_0630\I
    nstallers-5_1 HEAD_3/20/090208_0630\OSCartridge-Agent-
WindowsXP
    .zip
Agent Package Cartridge Name: OSCartridge-usrnsupported-WindowsXP
Agent Package Cartridge Version: 5.2.4 HEAD_3/20/090208_0630
----------------------------------
```

Index