Quest®

Quest® Protect Dashboard 6.0.0

User and Administration Guide

© 2021 Quest Software Inc.

ALL RIGHTS RESERVED.

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

The information in this document is provided in connection with Quest Software 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 Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE 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 SOFTWARE 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 SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software 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 Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Android, Chrome, Google Play, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LCC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered trademarks of Motorola Trademark Holdings, LLC. The Trademark BlackBerry Bold is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Quest is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Ixia and the Ixia four-petal logo are registered trademarks or trademarks of Ixia. Opera, Opera Mini, and the O logo are trademarks of Opera Software ASA. Tevron, the Tevron logo, and CitraTest are registered trademarks of Tevron, LLC. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Vormetric is a registered trademark of Vormetric, Inc. Intel, Itanium, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Debian is a registered trademark of Software in the Public Interest, Inc. OpenStack is a trademark of the OpenStack Foundation. Amazon Web Services, the "Powered by Amazon Web Services" logo, and "Amazon RDS" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. Infobright, Infobright Community Edition and Infobright Enterprise Edition are trademarks of Infobright Inc. POLYCOM®, RealPresence® Collaboration Server, and RMX® are registered trademarks of Polycom, Inc. All other trademarks and registered trademarks are property of their respective

owners.

Legend

WARNING: **A WARNING icon indicates a potential for property damage, personal injury, or death.**

CAUTION: **A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Quest Protect Dashboard User and Administration Guide
Updated - May 2021
Foglight Version - 6.0.0
Software Version - 6.0.0

Contents

Using Quest Protect Dashboard 6
Installation requirements 6
Rapid Recovery Agent Configuration 7
Standard environments: Rapid Recovery Agent and Agent Manager configuration 7
Large environments: Rapid Recovery Agent and Agent Manager configuration 7
Minimum memory and CPU requirements 8
Veeam Agent Configuration 8
Standard environments: Veeam Agent and Agent Manager configuration 9
Large environments: Veeam Agent and Agent Manager configuration 9
Minimum memory and CPU requirements 10
Dashboard location and UI elements 10
Group selector 11
Menu bar 11
Quick view 12

Getting Started Tab - Rapid Recovery 13

Protected Status Tab - Rapid Recovery 15
Unprotected Virtual Machines table 15
Unmonitored Rapid Recovery Protected Virtual Machines table 16

Repositories Capacity Planning Tab - Rapid Recovery 17
Repositories table 17

Rapid Recovery Infrastructure Tab 19
Core Servers table 19
Rapid Recovery Agents table 20

Events Tab - Rapid Recovery 21
Tasks tab 22
Alerts tab 22
Journal tab 22

Getting Started Tab - Veeam 24

Protected Status Tab - Veeam 26
Unprotected Virtual Machines table 27
Unmonitored Veeam Protected Virtual Machines table 27

Repositories Capacity Planning Tab - Veeam 28
Repositories table 28

Veeam Infrastructure Tab 30
Backup Servers table 30
Veeam Protected VMs table 31

Jobs Tab - Veeam 32
Jobs table 32
Job Sessions view 33

Administration Tab 34
Agents related commands 34
Creating Rapid Recovery Agent 35
Creating Veeam Agent 36
Editing agent properties 38
Managing certificates 39
Syntax Conventions 39
Managing certificates for FglAM 39

Virtual Machine Automation 41
Automation of VM Protection 42
Automation of VM Replication 43
Automation of VM Standby 44

About Us 46
We are more than just a name 46
Our brand, our vision. Together. 46
Contacting Quest 46
Technical support resources 46

1

Using Quest Protect Dashboard

Quest® Protect Dashboard accelerates the performance of your entire virtual infrastructure, transforms the application experience for users, and helps you control license and hardware costs. Go way beyond simple Hyper-V and VMware monitoring by maximizing resource utilization and improving virtual application performance across hybrid environments.

- Reduce hardware and licensing costs by proactively predicting and budgeting for capital expenditures.
- Protect growing virtual environments automatically—systems, applications, and data.
- Recover from data loss or corruption in minutes with zero impact on your users, as if the outage never happened.

The *Quest Protect Dashboard User and Administration Guide* is intended for users who have access to Quest Protect Dashboard. To get access to the Quest Protect dashboard, the user should have at least one of the following User roles: System Administrator, Advanced Operator, Capacity Management Administrator, VMware Administrator, or VMware QuickView.

- To enable the data collection from Rapid Recovery Core Server, ensure that the user account belongs to Administrators group of Rapid Recovery Core Server.
- To enable the data collection from Veeam Backup Server, ensure the following:
    1. The enterprise-plus license of Veeam Backup Enterprise Manager has been installed.
    2. The user account used to monitor Veeam must be assigned with the Portal Administrator role of Veeam Backup Enterprise Manager.

This section introduces you to the Quest Protect environment, and provides you with essential information.

For more information, see the following topics:

- Installation requirements
- Rapid Recovery Agent Configuration
- Veeam Agent Configuration
- Dashboard location and UI elements

Installation requirements

Quest Protect Dashboard comes installed on Foglight® Evolve and can be installed on a Foglight Management Server.

Quest Protect Dashboard requires the following cartridges for data collection.

- *vUsage-Feedback-5_8_2.car*
- *DRP-5.8.2.car*
- *Protect_1.8.0.car*

While Foglight Evolve comes with these cartridges pre-installed and enabled, a stand-alone Foglight release requires that these components be installed on the Foglight Management Server. The sequence of cartridge installation is important because of their dependencies. For more information about installing Quest Protect

Dashboard, and for details about system requirements and version compatibility, see the *Quest Protect Dashboard* Release Notes.

Rapid Recovery Agent Configuration

The Rapid Recovery Agents collect data from your Rapid Recovery infrastructure and sends it to the Rapid Recovery Core Server. The agents keep track of resource utilization metrics and alerts you when certain predefined thresholds are reached.

Standard environments: Rapid Recovery Agent and Agent Manager configuration

On 64-bit hosts meeting the minimum system requirements, the embedded Agent Manager can be used to run Rapid Recovery Agents to monitor the Rapid Recovery Core Server that protects up to100 machines.

Table 1. Agent Manager configuration for Rapid Recovery Agent

	Minimum CPU	Minimum Memory	Minimum Host Memory	Total protected machines
Windows 64-bit	1	2.5GB	3GB	100
Linux 64-bit	1	2.5GB	3GB	100

Large environments: Rapid Recovery Agent and Agent Manager configuration

The Agent Manager JVM usually requires additional memory to monitor the Rapid Recovery Core Server that protects more than 100 virtual machines.

The following calculations are guidelines, not hard and fast rules. Memory requirements can vary greatly from installation to installation with similar machine counts. If insufficient memory is configured, the failure mode is easily recognizable: all agents on the Agent Manager host will go into a broken state after the agent(s) were activated for a short period of time, usually within 24 hours. In addition, the Agent Manager log will contain a line similar to the following: `Caused by: java.lang.OutOfMemoryError: Java heap space`

If this is the case, add memory greater than what is shown in the calculations below, in increments of 512 MB until the agents stabilize. As most of memory is consumed by events, the memory consumed by Rapid Recovery agents is calculated based on the amounts of events that have been generated in last 2 weeks. It is supposed that one protected machine generates 1500 events in last 2 weeks, and one event might consume 16.5 KB memory, then one protected machine would consume 16.5 x1500 = 20 MB. For example, if a Rapid Recovery Core Server protects 100 machines, this Rapid Recovery Core Server will consume 20 MB x100 =2000 MB (round up to 2 GB). Therefore it is strongly recommended to check the number of events that have been generated since last week. Use the following formula to calculate the required memory:

```
512 MB + 16.5 KB x events#
```

If you do not want to check the amounts of events, use the following formula to calculate the required memory based on the number of protected machines:

```
512 MB + 20 MB x protected machines#
```

The default setting for agents deployed on 64-bit systems is 2560 MB, which suffice this environment. Similarly, protecting 1000 machines requires 20512 MB of memory:

```
512 MB + 20 MB x 1000 = 20512 MB
```

Foglight Evolve Virtual Appliance comes pre-configured to support up to 100 protected machines. This requires the default Agent Manager settings to be changed.

To change the JVM memory settings:

1. Determine the amount of additional memory required. This will be the total from the last step above minus the default value of 2560 MB. In the example above, this is `20512 - 2560 = 17952 MB (round up to 17 GB).`
2. On the agent machine, open the *baseline.jvmargs.config* file for editing. The file is located in the *<Agent_Manager_home>/state/default/config* directory.
3. Add the following lines in the **Memory Settings** section:

   ```
   vmparameter.0 = "-Xms17g";

   vmparameter.1 = "-Xmx17g";
   ```

   Note: If this file has been previously edited, increment the numeric parameters accordingly.
4. Delete the existing deployed negotiation configuration settings directory: *<Agent_Manager_home>/state/default/config/deployments*

   Restart the Agent Manager for these settings to take effect.

CPU

CPU usage on the Agent Manager host is relatively low most of the time. However, usage peaks dramatically during the performance metric collection. This is normal and expected. CPU utilization consistently over 50% is an indication that additional processing power is required. As with memory, usage can vary between different installations with similar numbers of protected machines. The following guidelines should be followed:

Up to 100 machines	1 CPU
100+ machines	add 1 CPU per 100 machines -- round up when necessary

Minimum memory and CPU requirements

# of protected machines	Memory[1] Foglight JVM settings	# of CPUs
100	Xms|Xmx=1G	1
500	Xms|Xmx=4G	5
1000	Xms|Xmx=8G	10

1. Edit the Foglight Management Server JVM settings in the server.config file located under *Quest\Foglight\config*\. When running Foglight on a virtual machine, full memory needs be reserved at the hypervisor level.

Veeam Agent Configuration

The Veeam Agents collect data from your Veeam infrastructure and sends it to the Veeam Backup Server. The agents keep track of resource utilization metrics and alerts you when certain pre-defined thresholds are reached.

Standard environments: Veeam Agent and Agent Manager configuration

On 64-bit hosts meeting the minimum system requirements, the embedded Agent Manager can be used to run Veeam Agents to monitor the Veeam Enterprise Manager Server that protects up to400 machines.

Table 2. Agent Manager configuration for Veeam Agent

	Minimum CPU	Minimum Memory	Minimum Host Memory	Total protected machines
Windows 64-bit	1	2.5GB	3GB	400
Linux 64-bit	1	2.5GB	3GB	400

Large environments: Veeam Agent and Agent Manager configuration

The Agent Manager JVM usually requires additional memory to monitor the Veeam Enterprise Manager Server that protects more than 400 virtual machines.

The following calculations are guidelines, not hard and fast rules. Memory requirements can vary greatly from installation to installation with similar machine counts. If insufficient memory is configured, the failure mode is easily recognizable: all agents on the Agent Manager host will go into a broken state after the agent(s) were activated for a short period of time, usually within 24 hours. In addition, the Agent Manager log will contain a line similar to the following: `Caused by: java.lang.OutOfMemoryError: Java heap space`

If this is the case, add memory greater than what is shown in the calculations below, in increments of 512 MB until the agents stabilize. Use the following formula to calculate the required memory:

`512 MB + 5 MB x protected machines#`

According to the above formula, monitoring 400 virtual machines requires 2512 MB of memory: `512 MB + 5 MB * 400 = 2512 MB.`

The default setting for agents deployed on 64-bit systems is 2560 MB, which suffice this environment. Similarly, protecting 1000 machines requires 5512 MB of memory: `512 MB + 5 MB x 1000 = 5512 MB`

Foglight Evolve Virtual Appliance comes pre-configured to support up to 400 protected machines. This requires the default Agent Manager settings to be changed.

To change the JVM memory settings:

1. Determine the amount of additional memory required. This will be the total from the last step above minus the default value of 2560 MB. In the example above, this is `5512 – 2560 = 2952 MB (round up to 3GB).`
2. On the agent machine, open the *baseline.jvmargs.config* file for editing. The file is located in the *<Agent_Manager_home>/state/default/config* directory.
3. Add the following lines in the **Memory Settings** section:

   ```
   vmparameter.0 = "-Xms3g";
   ```

   ```
   vmparameter.1 = "-Xmx3g";
   ```

   Note: If this file has been previously edited, increment the numeric parameters accordingly.
4. Delete the existing deployed negotiation configuration settings directory: *<Agent_Manager_home>/state/default/config/deployments*

   Restart the Agent Manager for these settings to take effect.

CPU

CPU usage on the Agent Manager host is relatively low most of the time. However, usage peaks dramatically during the performance metric collection. This is normal and expected. CPU utilization consistently over 50% is an indication that additional processing power is required. As with memory, usage can vary between different installations with similar numbers of protected machines. The following guidelines should be followed::

Up to 400 machines	1 CPU
400+ machines	add 1 CPU per 400 machines -- round up when necessary

Minimum memory and CPU requirements

# of protected machines	Memory[1] Foglight JVM settings	# of CPUs
400	Xms|Xmx=1G	1
1000	Xms|Xmx=2G	3
2000	Xms|Xmx=4G	5

1. Edit the Foglight Management Server JVM settings in the server.config file located under *Quest\Foglight\config*\. When running Foglight on a virtual machine, full memory needs be reserved at the hypervisor level.

Dashboard location and UI elements

After installing Quest Protect Dashboard, the **Protection** entry appears under Homes.

To access the Protection dashboard:

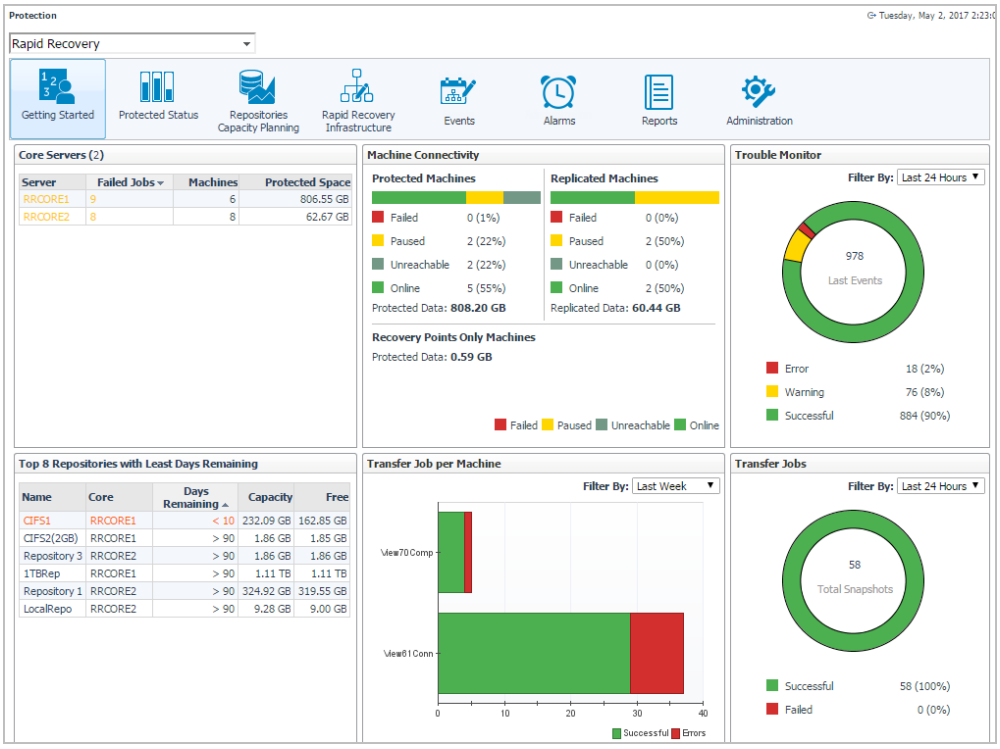
1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click Protection.

The **Protection** dashboard opens.



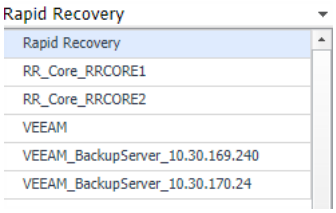
The **Protection** dashboard consists of the following UI elements:

- Group selector
- Menu bar
- Quick view

Group selector

The Group selector is located at the top of the dashboard and allows you to select the Protection environment that you monitored.

Figure 1. Group Selector

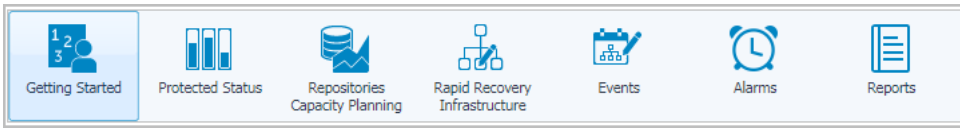


Menu bar

The Menu bar contains the following tabs:

- *Rapid Recovery*: *Getting Started Tab - Rapid Recovery*, *Protected Status Tab - Rapid Recovery*, *Repositories Capacity Planning Tab - Rapid Recovery*, *Rapid Recovery Infrastructure Tab*, *Events Tab - Rapid Recovery*, and *Administration Tab*
- *Veeam*: *Getting Started Tab - Veeam*, *Protected Status Tab - Veeam*, *Repositories Capacity Planning Tab - Veeam*, *Veeam Infrastructure Tab*, *Jobs Tab - Veeam*, and *Administration Tab*.

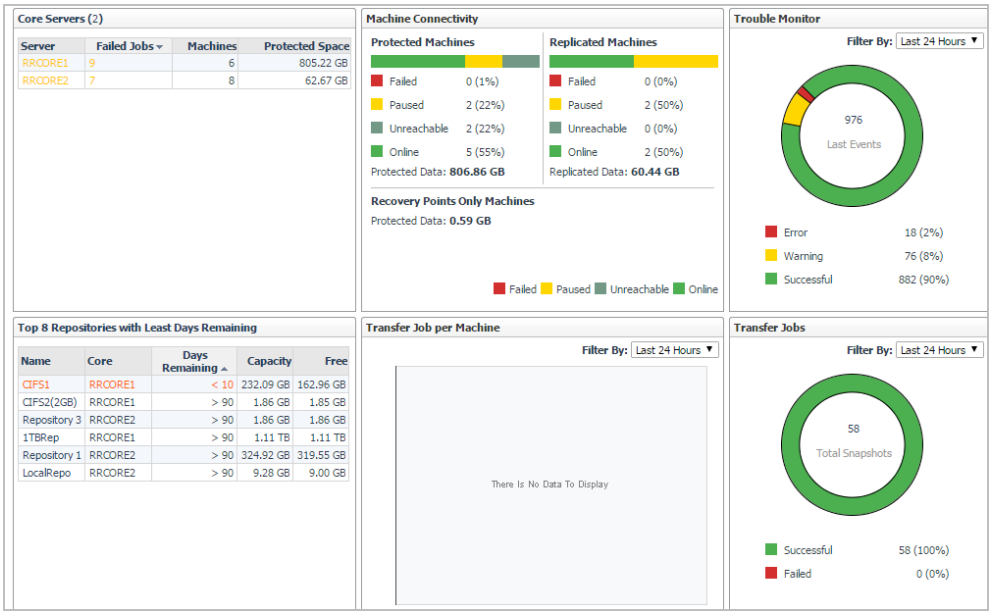
Figure 2. Menu bar



Quick view

The quick view is located on the lower part of the Protection dashboard, which is updated based on the tab selected on the menu bar.

Figure 3. Quick view

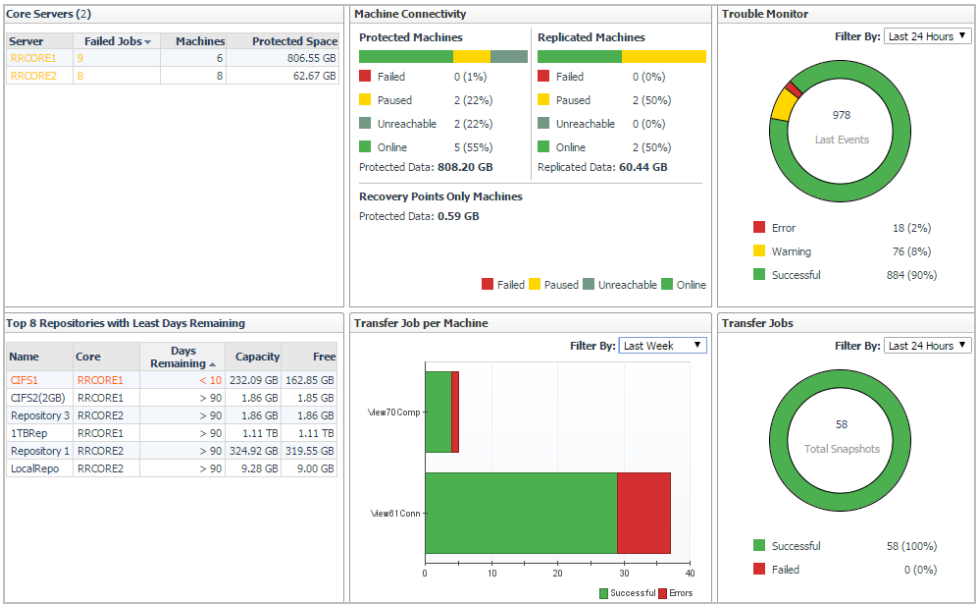


2

Getting Started Tab - Rapid Recovery

The **Getting Started** view of the Protection dashboard shows the data collected in the Rapid Recovery Core Servers.

Figure 4. Getting Started view



To access the Getting Started view:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.
5. On the menu bar, click the Getting Started tab.

   The Getting Started view appears at the bottom of the Protection dashboard.

The Getting Started view includes the following tables:

- *Core Servers*: This table lists the monitored Rapid Recovery Core Servers. Click this link to navigate to the Rapid Recovery Infrastructure Tab. For more information, see Rapid Recovery Infrastructure Tab on page 19.

- *Machine Connectivity*: This table shows the connectivity state of machines protected and replicated on the monitored Rapid Recovery core. It also shows connectivity for data on recovery points-only machine. For more information about recovery points-only machine, refer to the Rapid Recovery Help.
- *Trouble Monitor:* This table shows job activity, connections with the license portal, and transfer activity to detect early on the monitored Rapid Recovery core. The time range is configurable, defaulting to last 24 hours. Click this graph to navigate to the *Events* > *Journal* tab. For more information, see Journal tab on page 22.
- *Top 8 Repositories with Least Days Remaining*: This tables shows the top eight repositories with the least days remaining on the monitored Rapid Recovery core. Click this link to navigate to the Repositories Capacity Planning Tab - Rapid Recovery. For more information, see Repositories Capacity Planning Tab - Rapid Recovery on page 17.
- *Transfer Job per Machine*: This table shows, by protected machine of which the latest transfer job is failed, the number of successful and failed transfer jobs in the specified time range. This table shows the top ten machines with the most failed transfer job. The time range is configurable, defaulting to last 24 hours. Click this graph to navigate to the *Events* > *Tasks* tab. For more information, see Tasks tab on page 22.
- *Transfer Jobs*: This table shows all snapshot data transfers (including base images and incremental snapshots) that completed in the specified time range. The time range is configurable, defaulting to last 24 hours. Click this graph to navigate to *Events* > *Tasks* tab. For more information, see Tasks tab on page 22.

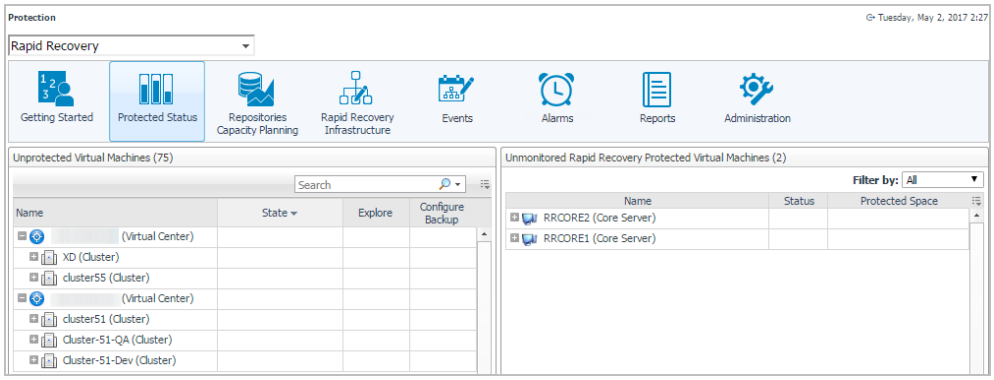
3

Protected Status Tab - Rapid Recovery

The **Protected Status** view of the Protection dashboard shows the unprotected virtual machines and unmonitored Rapid Recovery Protected virtual machines on the monitored Rapid Recovery Core. The Protected Status view includes the following two tables:

- Unprotected Virtual Machines: For more information, see Unprotected Virtual Machines table on page 15.
- Unmonitored Rapid Recovery Protected Virtual Machines: For more information, see Unmonitored Rapid Recovery Protected Virtual Machines table on page 16.

Figure 5. Protected Status view



To access the Protected Status view:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click Protection.

The **Protection** dashboard opens.

4 Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.

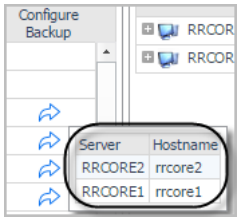
5 On the menu bar, click the Protected Status tab.

The Protected Status view appears at the bottom of the Protection dashboard.

Unprotected Virtual Machines table

The Unprotected Virtual Machines table shows a list of virtual machines that are monitored by the Foglight for VMware, but not backed up in the monitored Rapid Recovery environment.

Table 3. Description of the Unprotected Virtual Machines table

Data displayed	• **Name**. Shows the name of virtual machine. • **State**. Indicates whether the virtual machine is Powered On, Powered Off, or Suspended. • **Explore**. Shows the link to the Virtual Machine Explorer dashboard. • Configure Backup. Shows the link to the Rapid Recovery Core Server.
Where to go next	Drill down on: • **Explore**. Click to navigate to the VMware Explorer dashboard. For more information, refer to the Foglight for VMware User and Reference Guide. • **Configure Backup**. Click to allow user to choose Rapid Recovery Core server for backup. 

Unmonitored Rapid Recovery Protected Virtual Machines table

The Unmonitored Rapid Recovery Protected Virtual Machines table shows a list of virtual machines that have backup files on the Rapid Recovery Core Servers, but not monitored by the Foglight for VMware.

Table 4. Description of the Unmonitored Rapid Recovery Protected Virtual Machines table

Data displayed	• **Name**. Shows the display name of Rapid Recovery Core Server, cluster, or virtual machine. • **Status**. Indicates whether the machine connectivity is Online, Failed, Paused, or Unreachable. • **Protected Space**. Indicates the amount of protected storage space.

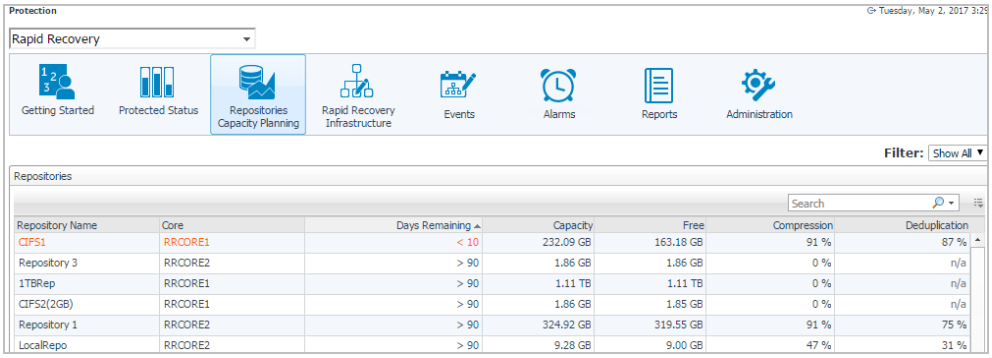
4

Repositories Capacity Planning Tab - Rapid Recovery

The **Repositories Capacity Planning** view of the Protection dashboard shows the information about repositories in which backup snapshot data captured from your monitored protection environment is stored and managed. The **Repositories Capacity Planning** view includes the following two elements:

- Repositories table: For more information, see Repositories table on page 17.
- Filter menu: Allows you to filter the repositories based on the following options: Show All (default option), 10 days, 30 days, 60 days, and 90 days.

Figure 6. Repositories Capacity Planning view



To access the Repositories Capacity Planning view:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click Protection.

The **Protection** dashboard opens.

4 Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.

5 On the menu bar, click the Repositories Capacity Planning tab.

The Repositories Capacity Planning view appears at the bottom of the Protection dashboard.

Repositories table

The Repositories table shows a list of central locations in which backup snapshot data captured from your monitored Rapid Recovery environment is stored and managed.

Table 5. Description of the Repositories table

Data displayed	• **Repository Name**. Shows the display name of repository. • **Core**. Shows the Core server in which the repository is stored and managed. • **Days Remaining**. Indicates when the storage gets fully occupied. • **Capacity**. Shows the total capacity on the storage. • **Free**. Shows the free capacity on the storage. • **Compression**. Shows the percentage of compression. • **Deduplication**. Shows the percentage of deduplication.

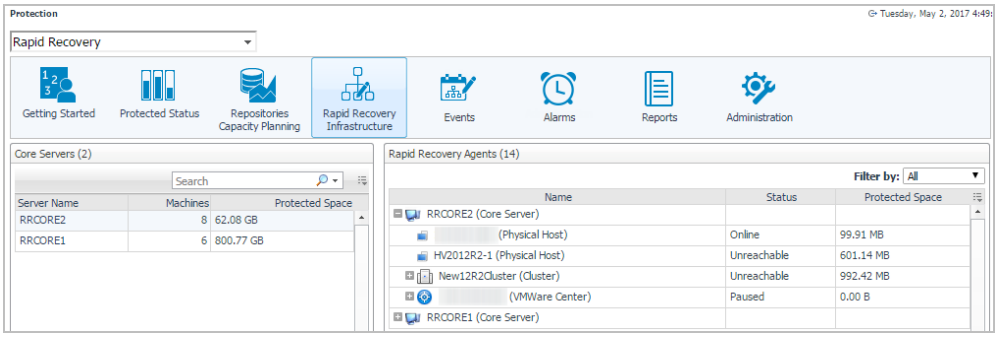
5

Rapid Recovery Infrastructure Tab

The **Rapid Recovery Infrastructure** view of the Protection dashboard shows the infrastructure of the service scoped Rapid Recovery Core servers. The **Rapid Recovery Infrastructure** view includes the following two tables:

- Core Servers: For more information, see Core Servers table on page 19.
- Rapid Recovery Agents: For more information, see Rapid Recovery Agents table on page 20.

Figure 7. Rapid Recovery Infrastructure view



To access the Rapid Recovery Infrastructure view:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click Protection.

The **Protection** dashboard opens.

4 Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.

5 On the menu bar, click the **Rapid Recovery Infrastructure** tab.

The **Rapid Recovery Infrastructure** view appears at the bottom of the Protection dashboard.

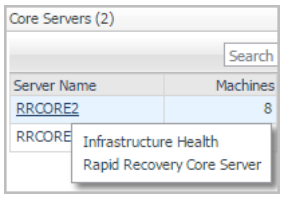
Core Servers table

The Core Servers table shows a list of core servers that exist in the monitored Rapid Recovery environment.

Table 6. Description of the Core Servers table

Data displayed	• **Server Name**. Shows the name of Rapid Recovery Core. • **Machines**. Shows the amount of machines in this Rapid Recovery Core. • **Protected Spaces**. Indicates the amount of storage space protected by this Rapid Recovery Core.

Table 6. Description of the Core Servers table

Where to go next	Drill down on: • **Server Name**. Click this column to show links to Infrastructure Health and Rapid Recovery Core Server. 

Rapid Recovery Agents table

The Rapid Recovery Agents table shows a list of agents that exist in the monitored Rapid Recovery environment.

Table 7. Description of the Rapid Recovery Agents table

Data displayed	• **Name**. Shows the name of Rapid Recovery Core Server or cluster. • **Status**. Indicates whether the machine connectivity is Online, Failed, Paused, or Unreachable. • **Protected Space**. Indicates the amount of protected storage space.

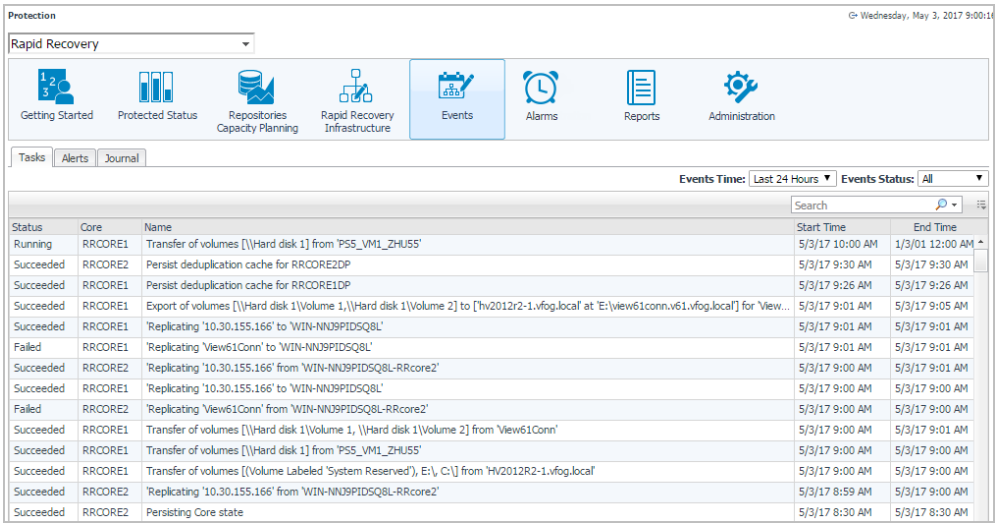
6

Events Tab - Rapid Recovery

The **Events** view of the Protection dashboard shows events for the Core, a specific protected or replicated machine in the monitored Rapid Recovery environment. The **Events** view includes the following three tabs:

- Tasks tab: A task is an event related to a job. A job is a process that the Rapid Recovery Core must perform. Each job has a current state, and a start and end time and date. Some tasks are initiated manually or scheduled by the user. Examples include forcing a snapshot, scheduling a backup, or performing a restore from a recovery point. Other tasks are automatic functions, such as running nightly jobs, or performing rollup using the default retention policy.
- *Alerts tab*: An alert is a priority event, such as an error, warning, or important informational message. If you request notifications of any specific events, these notifications appear in the Alerts subset.
- *Journal tab*: The Journal tab shows a complete list of all logged events (for the Core, or the selected machine, as appropriate). This list is more comprehensive, showing jobs, high priority events, and lower priority events. This category includes passive and non-job events (such as the Core starting successfully, or reporting status from the license portal).

Figure 8. Events view



To access the Events view:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click Protection.

The **Protection** dashboard opens.

4 Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.

5 On the menu bar, click the **Events** tab.

The **Events** view appears at the bottom of the Protection dashboard.

Tasks tab

A task is a job that the Rapid Recovery Core must perform, such as transferring data in a regularly scheduled backup, or performing a restore from a recovery point. The Tasks tab opens by default when navigating to the Events view.

The Tasks tab includes the following elements:

- Events Time: Allows you to filter events based on the following options: Last 1 Hour, Last 4 Hours, Last 12 Hours (default option), Last 48 Hours, This Week, and Last Week.
- Events Status: Allows you to filter events based on the following options: All (default option), Successful, and Failed.
- Tasks table:

Data displayed

- **Status**. Indicates whether this task is Succeeded or Failed.
- **Core**. Shows the display name of this Rapid Recovery Core.
- **Name**. Shows the task type for this protected machine. Examples include transfer of volumes, The task name. This field lists the task type for this protected machine. Examples include transfer of volumes, maintaining repository, rolling up, and so on.
- **Start Time**. Indicates the time when this task starts.
- **End Time**. Indicates the time when this task ends.

Alerts tab

An alert is a priority notification of an event. Any event for which you specifically requested notification appears in the list of alerts, along with errors, warnings, or important informational messages. To access the Alerts tab, click Alerts in the Events view.

The Alerts tab includes the following elements:

- Events Time: Allows you to filter alerts based on the following options: Last 1 Hour, Last 4 Hours, Last 12 Hours (default option), Last 48 Hours, This Week, and Last Week.
- Events Level: Allows you to filter alerts based on the following options: All (default option), Error, Info, and Warning.
- Alerts table:

Data displayed

- **Level**. Indicates whether this alert is Info, Warning, or Error.
- **Core**. Shows the display name of this Rapid Recovery Core.
- **Date**. Indicates the date when this alert occurs.
- **Message**. Shows the detailed message of this alert.

Journal tab

The journal lists all logged events. This list is comprehensive, including both job- and non-job-related events. It includes specific events for which you requested notification. The journal also lists passive events and status events from the Core, the license portal, and so on. To access the Journal tab, click Journal in the Events view. The Journal tab includes the following elements:

- Events Time: Allows you to filter journals based on the following options: Last 1 Hour, Last 4 Hours, Last 12 Hours (default option), Last 48 Hours, This Week, and Last Week.
- Events Level: Allows you to filter journals based on the following options: All (default option), Error, Info, and Warning.
- Journals table:

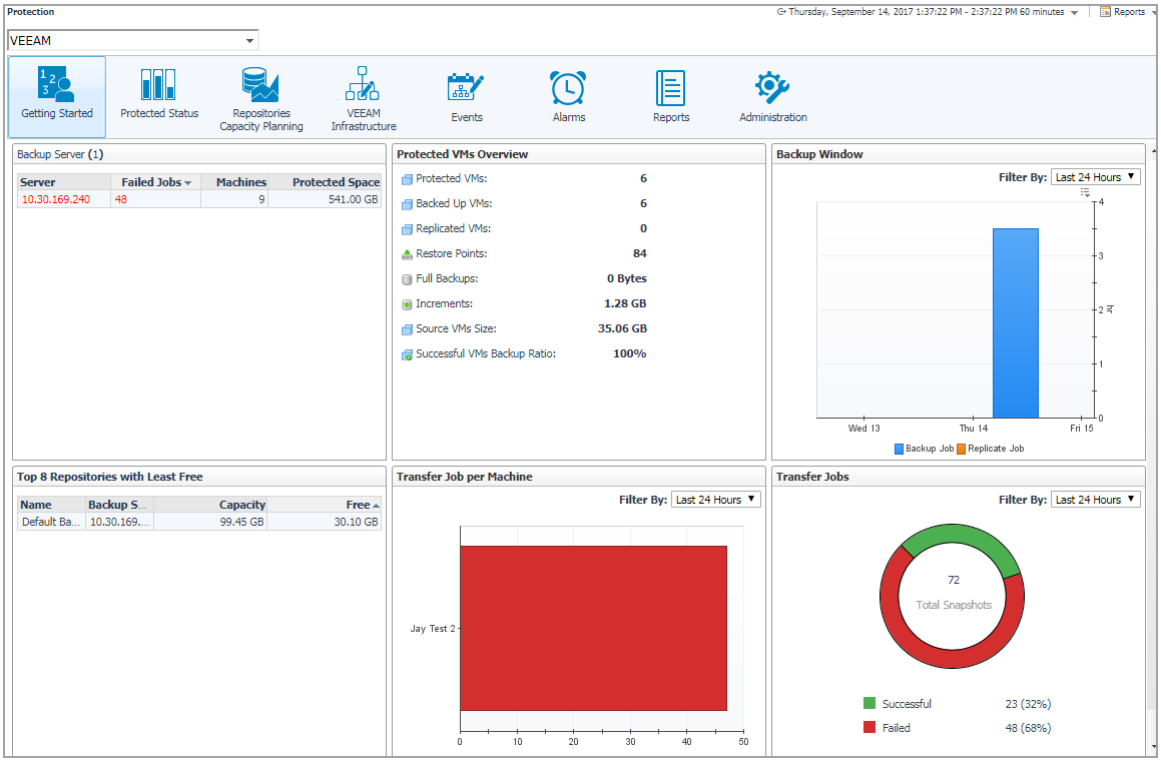
Data displayed

- **Level**. Indicates whether this journal is Info, Warning, or Error.
- **Core**. Shows the display name of this Rapid Recovery Core.
- **Date**. Indicates the date when this journal occurs.
- **Message**. Shows the detailed message of this journal.

Getting Started Tab - Veeam

The **Getting Started** view of the Protection dashboard shows the data collected in the Veeam Servers.

Figure 9. Getting Started view



To access the Getting Started view:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.
5. On the menu bar, click the Getting Started tab.

   The Getting Started view appears at the bottom of the Protection dashboard.

The Getting Started view includes the following tables:

- *Backup Servers*: This table lists the monitored Veeam Backup Core Servers. Click this link to navigate to the Veeam Infrastructure Tab. For more information, see Veeam Infrastructure Tab on page 30.

- *Protected VMs Overview*: This table presents the information about how your VMs are protected, number of protected VMs (backed up or replicated), number of restore points available, source VM size, full and incremental backup size, and successful backup sessions ratio on the monitored Veeam Backup Server. For more information about Veeam Backup Infrastructure, refer to the Veeam Help.
- *Backup Window:* This table shows the total duration of Backup and Replication jobs.
- *Top 8 Repositories with Least Free*: This tables shows the top eight repositories with the least days remaining on the monitored Veeam Backup server. Click this link to navigate to the Repositories Capacity Planning Tab - Veeam. For more information, see Repositories Capacity Planning Tab - Veeam on page 28.
- *Transfer Job per Machine*: This table shows, by protected machine of which the latest transfer job is failed, the number of successful and failed transfer jobs in the specified time range. This table shows the top ten machines with the most failed transfer job. The time range is configurable, defaulting to last 24 hours. Click this graph to navigate to the *Jobs* tab. For more information, see Jobs Tab - Veeam on page 32.
- *Transfer Jobs*: This table shows all snapshot data transfers (including base images and incremental snapshots) that completed in the specified time range. The time range is configurable, defaulting to last 24 hours. Click this graph to navigate to *Jobs* tab. For more information, see Jobs Tab - Veeam on page 32.

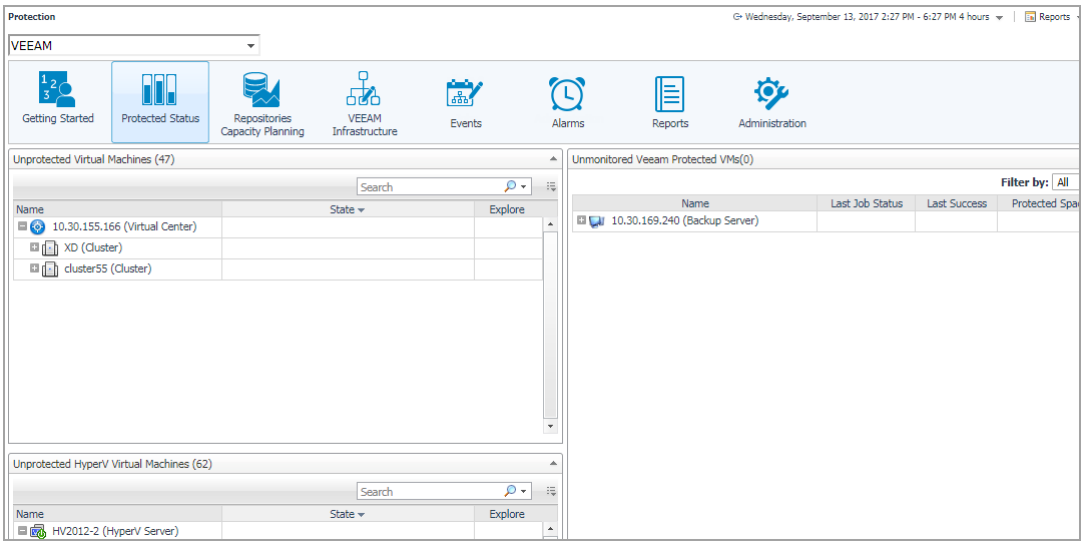
8

Protected Status Tab - Veeam

The **Protected Status** view of the Protection dashboard shows the unprotected virtual machines and unmonitored Veeam Protected virtual machines on the monitored Veeam Backup Servers. The Protected Status view includes the following two tables:

- Unprotected Virtual Machines: For more information, see Unprotected Virtual Machines table on page 27.
- Unmonitored Veeam Protected Virtual Machines: For more information, see Unmonitored Veeam Protected Virtual Machines table on page 27.

Figure 10. Protected Status view



To access the Protected Status view:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click Protection.

The **Protection** dashboard opens.

4 Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.

5 On the menu bar, click the Protected Status tab.

The Protected Status view appears at the bottom of the Protection dashboard.

Unprotected Virtual Machines table

The Unprotected Virtual Machines table shows a list of virtual machines that are monitored by the Foglight for VMware, but not backed up in the monitored Rapid Recovery environment.

Table 8. Description of the Unprotected Virtual Machines table

Data displayed	• **Name**. Shows the name of virtual machine. • **State**. Indicates whether the virtual machine is Powered On, Powered Off, or Suspended. • **Explore**. Shows the link to the Virtual Machine Explorer dashboard. • Configure Backup. Shows the link to the Rapid Recovery Core Server.
Where to go next	Drill down on: • **Explore**. Click to navigate to the VMware Explorer dashboard. For more information, refer to the Foglight for VMware User and Reference Guide.

Unmonitored Veeam Protected Virtual Machines table

The Unmonitored Veeam Protected Virtual Machines table shows a list of virtual machines that have backup files on the Veeam Backup Servers, but not monitored by the Foglight for VMware.

Table 9. Description of the Unmonitored Veeam Protected Virtual Machines table

Data displayed	• **Name**. Shows the display name of Veeam Backup Server, cluster, or virtual machine. • **Last Job Status**. Indicates whether the machine connectivity is last job is Success, Warning, or Failed. • **Last Success**. Indicates the time of last success job. • **Protected Space**. Indicates the amount of protected storage space.

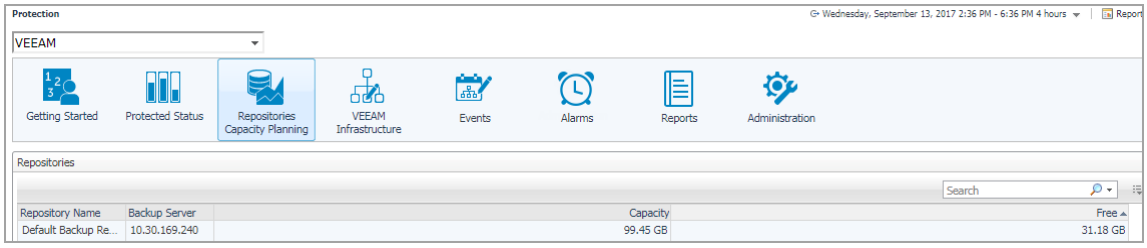
9

Repositories Capacity Planning Tab - Veeam

The **Repositories Capacity Planning** view of the Protection dashboard shows the information about repositories in which backup snapshot data captured from your monitored protection environment is stored and managed. The **Repositories Capacity Planning** view includes the following two elements:

- Repositories table: For more information, see Repositories table on page 28.
- Filter menu: Allows you to filter the repositories based on the following options: Show All (default option), 10 days, 30 days, 60 days, and 90 days.

Figure 11. Repositories Capacity Planning view



To access the Repositories Capacity Planning view:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.
5. On the menu bar, click the Repositories Capacity Planning tab.

   The Repositories Capacity Planning view appears at the bottom of the Protection dashboard.

Repositories table

The Repositories table shows a list of central locations in which backup snapshot data captured from your monitored Veeam environment is stored and managed.

Table 10. Description of the Repositories table

Data displayed	• **Repository Name**. Shows the display name of repository. • **Backup Server**. Shows the Backup Server in which the repository is stored and managed.

Table 10. Description of the Repositories table

- **Capacity**. Shows the total capacity on the storage.
- **Free**. Shows the free capacity on the storage.

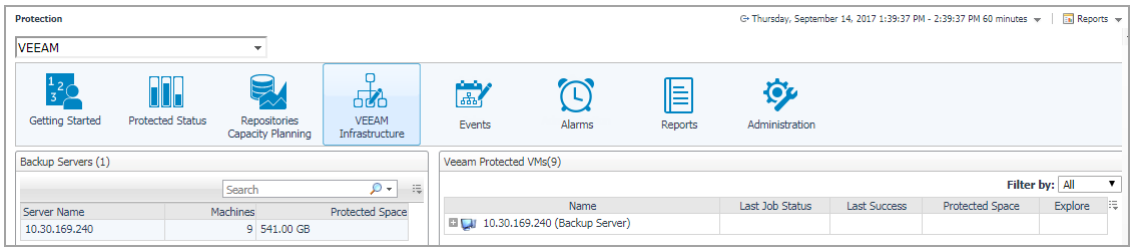
10

Veeam Infrastructure Tab

The **Veeam Infrastructure** view of the Protection dashboard shows the infrastructure of the service scoped Veeam Backup servers. The **Veeam Infrastructure** view includes the following two tables:

- Backup Servers: For more information, see Backup Servers table on page 30.
- Veeam Protected VMs: For more information, see Veeam Protected VMs table on page 31.

Figure 12. Veeam Infrastructure view



To access the Veeam Infrastructure view:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.
5. On the menu bar, click the **Veeam Infrastructure** tab.

   The **Veeam Infrastructure** view appears at the bottom of the Protection dashboard.

Backup Servers table

The Backup Servers table shows a list of core servers that exist in the monitored Veeam environment.

Table 11. Description of the Backup Servers table

Data displayed	• **Server Name**. Shows the name of Veeam Backup Server. • **Machines**. Shows the amount of machines in this Veeam Backup Server. • **Protected Spaces**. Indicates the amount of storage space protected by this Veeam Backup Server.

Veeam Protected VMs table

The Veeam Protected VMs table shows a list of agents that exist in the monitored Veeam environment.

Table 12. Description of the Veeam Protected VMs table

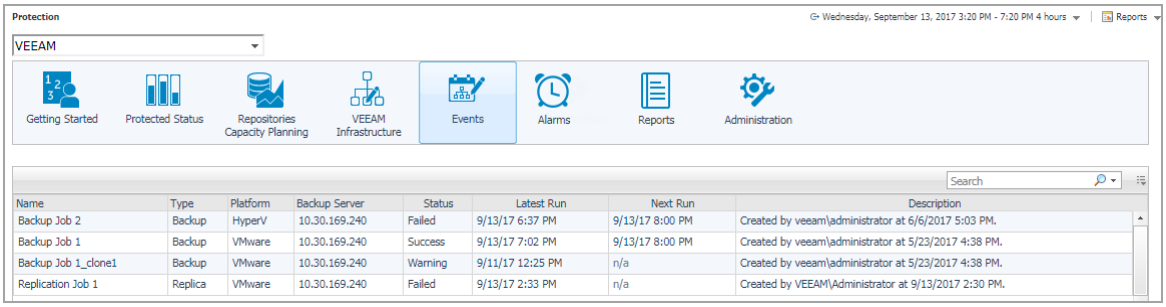
Data displayed	• **Name**. Shows the name of Veeam Backup Server or cluster. • **Last Job Status**. Indicates whether the last job is Success, Warning, or Failed • **Last Success**. Indicates the time of last success job. • **Protected Space**. Indicates the amount of protected storage space.
Where to go next	Drill down on: • **Explore**. Click to navigate to the *VMware Explorer* dashboard. For more information, refer to the *Foglight for VMware User and Reference Guide*.

11

Jobs Tab - Veeam

The **Jobs** view of the Protection dashboard shows backup jobs for the Backup Servers, a specific protected or replicated machine in the monitored Veeam environment.

Figure 13. Jobs view



To access the Job view:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.
5. On the menu bar, click the **Jobs** tab.

   The **Jobs** view appears at the bottom of the Protection dashboard.

A backup job is a configuration unit of the backup activity. The backup job defines when, what, how and where to back up. One backup job can be used to process one or several VMs.

The **Jobs** view includes the following elements:

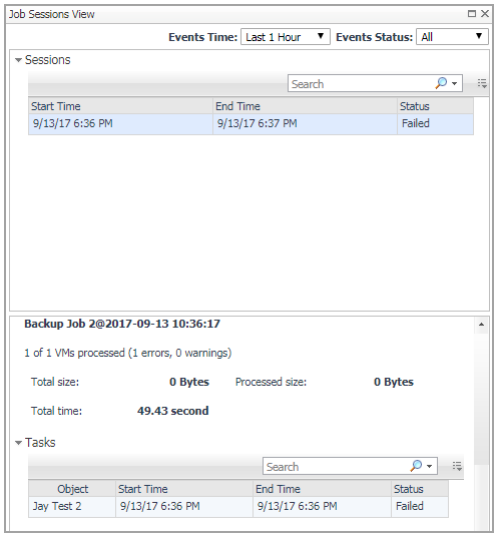
- Jobs table
- Job Sessions view

Jobs table

Table 13. Jobs table

Data displayed	• **Name**. Shows the name of Jobs. • **Type**. Indicates whether this job is backup job, or replication job.

Table 13. Jobs table

Where to go next	• **Platform**. Indicates whether this job is for HyperV, or VMware platform. • **Backup Server**. Shows the display name of this Veeam Backup Server. • **Latest Run**. Indicates when this job ran the last time. • **Next Run**. Indicates when this job will run the next time. • **Description**. Shows the description message of this job. • **Name**. Click this column to show the **Jobs Sessions View** dialog box. 

Job Sessions view

The *Jobs Sessions* view includes the following elements:

- **Events Time**: Allows you to filter events based on the following options: Last 1 Hour, Last 4 Hours, Last 12 Hours (default option), Last 48 Hours, This Week, and Last Week.
- **Events Status**: Allows you to filter events based on the following options: All (default option), Successful, and Failed.
- **Sessions table**:

Table 14. Sessions table

Data displayed	• **Start Time**. Shows the start time of this session. • **End Time**. Shows the end time of this session. • **Status**. Indicates whether the job is Success, or Failed.

- **Sessions Quick View**: The *Session Quick View* is updated based on the row selected on the sessions table. The *Session Quick View* shows numbers of VMs processed, total and processed size, and total time this session takes.
- **Tasks Table**:

Table 15. Tasks table

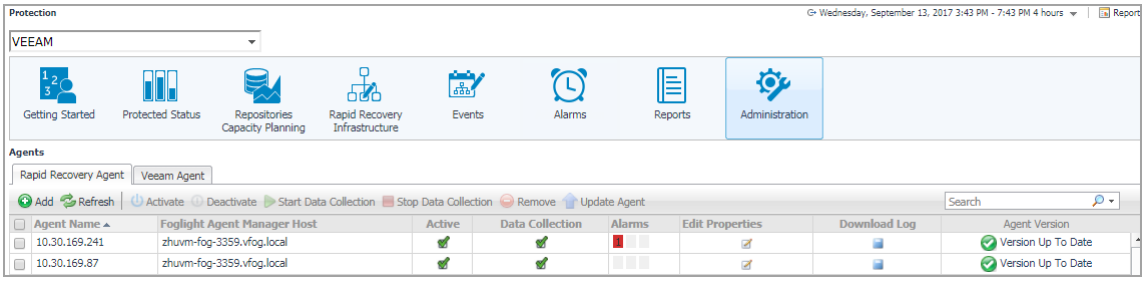
Data displayed	• **Object**. Shows the task name. • **Start Time**. Shows the start time of this task. • **End Time**. Shows the end time of this task. • **Status**. Indicates whether the job is Success, Warning, or Failed.

12

Administration Tab

The **Administration** view of the Protection dashboard contains links to agent administration tasks that you can use to manage Rapid Recovery or Veeam agents.Foglight-FVE-FSM-vApp-standard

Figure 14. Administration view



To access the Administration view:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.
5. On the menu bar, click the **Administration** tab.

   The **Administration** view appears at the bottom of the Protection dashboard.

For more information, see the following topics:

- Agents related commands
- Creating Rapid Recovery Agent
- Creating Veeam Agent
- Editing agent properties
- Managing certificates

Agents related commands

The **Administration view** shows a list of existing agent instances and a set of agent management commands at the top of the list. Use it to verify that your agents are collecting data from the monitored environment.

The following commands are available:

- **Add:** Starts a workflow for creating new agent instances. For more information, see Creating Rapid Recovery Agent on page 35. or For more information, see Creating Veeam Agent on page 36.
- **Refresh:** Refreshes the list of agent instances and their states.
- **Activate:** Activates one or more selected agent instances. Activating an agent instance starts the agent process on the machine on which the agent is installed.
- **Deactivate:** Deactivates one or more selected agent instances. Deactivating an agent stops the agent process on the machine on which the agent is installed.
- **Start Data Collection:** Starts the data collection for one or more selected agent instances. Starting an agent's data collection causes the agent to begin monitoring the Rapid Recovery Core and to send the collected metrics back to the Management Server.
- **Stop Data Collection:** Stops the data collection for one or more selected agent instances. Stopping an agent's data collection causes the agent to stop monitoring the Rapid Recovery Core.
- **Edit Properties:** Starts a workflow for editing the properties of one or more selected agent instances. Each agent comes with a set of properties that it uses to configure its correct running state. Editing agent properties on page 38.
- **Download Log**: Retrieves agent log files that describe the operations an agent process performs while it is running on the monitored host. Use agent logs to solve problems related to an agent's state or behavior. For example, if an agent instance fails to activate, you can use an agent log file to determine the cause of the problem.
- **Remove:** Deletes the selected agent instance.
- **Update Agent:** Updates the agent package to the latest version.

  IMPORTANT: Updating the agent package using this command generates the previously existing credentials. However, if you update the agent package by re-deploying its .gar file through the Agent Status page, the credentials need to be re-created. To do that, select an agent instance, click **Edit Properties**, and configure the required credentials on the **Credentials** tab of the **Edit Tab Manager** dialog box.

To perform any of the available commands, select one or more check boxes in the left-most column and click the appropriate button. For example, to start an agent's data collection, select the check box in the agent row and click **Start Data Collection**.

Creating Rapid Recovery Agent

The Rapid Recovery Agents collect data from your Rapid Recovery infrastructure and sends it to the Rapid Recovery Core Server. The agents keep track of resource utilization metrics and alerts you when certain pre-defined thresholds are reached.

NOTE: In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use HTTPs. For more information, see Managing certificates on page 39.

To create a Rapid Recovery Agent:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

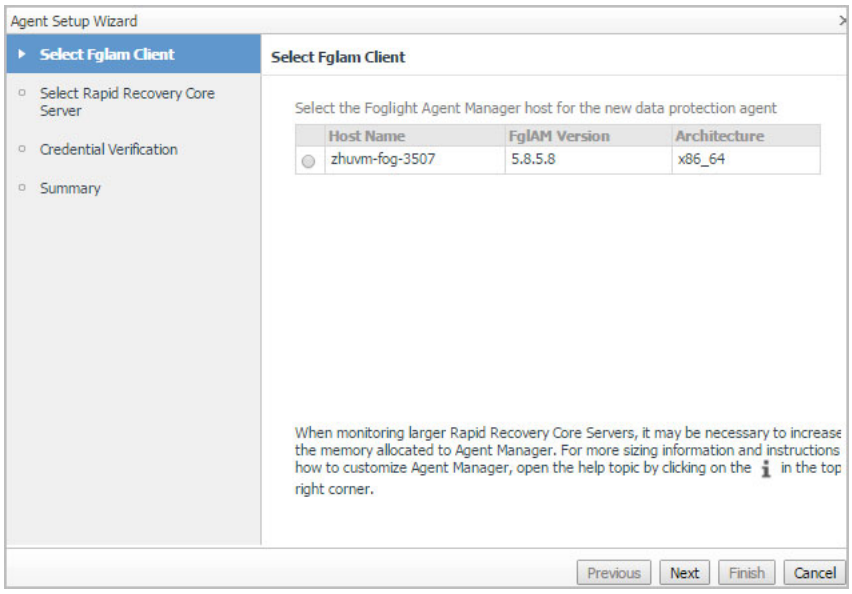
   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.

5 On the menu bar, click the **Administration** tab.

The **Administration** view appears at the bottom of the Protection dashboard.

6 In the **Administration** view, click Rapid Recovery Agent, and then click **Add**.

The **Agent Setup Wizard** dialog box opens.



7 In the *Select Fglam Client* step, select the agent manager on which the new agent is to be deployed, and then click **Next**.

8 In the *Select Rapid Recovery Core Server* step, specify the following values, as needed, then click **Next**.

- *Rapid Recovery Core Server:* The name or IP address of the computer on Rapid Recovery Core Server is running.
- *Port*: The HTTP port number used by the Rapid Recovery Core Server.

9 In the *Credential Verification* step, perform either of the following:

NOTE: The user credential must belong to the Administrators group of Rapid Recovery Core Server.

1 Select Add Rapid Recovery Core server to a new credential, then the **Create New Credential** view appears on the right. Specify the credential related information, and then click **Next**.

Or

2 Select Add Rapid Recovery Core server to an existing credential, then the **Selected Existing Credential** view appears on the right. Select an existing credential, and then click **Next**.

10 In the *Summary* step, confirm the agent information, and then click Finish.

The new Rapid Recovery Agent is created, and its data is to be monitored by Rapid Recovery after a few minutes.

Creating Veeam Agent

The Veeam Agents collect data from your Veeam infrastructure and sends it to the Veeam Backup Server. The agents keep track of resource utilization metrics and alerts you when certain pre-defined thresholds are reached.

NOTE: In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use HTTPs. For more information, see Managing certificates on page 39.

To create a Veeam Agent:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click Protection.

The **Protection** dashboard opens.

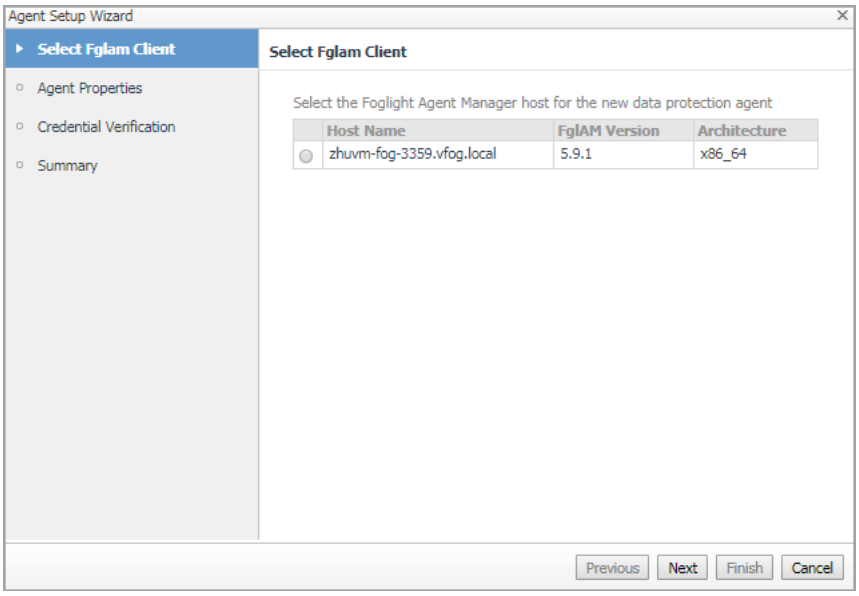
4 Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.

5 On the menu bar, click the **Administration** tab.

The **Administration** view appears at the bottom of the Protection dashboard.

6 In the **Administration** view, click **Veeam Agent**, and then click **Add**.

The **Agent Setup Wizard** dialog box opens.



7 In the *Select Fglam Client* step, select the agent manager on which the new agent is to be deployed, and then click **Next**.

8 In the *Agent Properties* step, specify the following values, as needed, then click **Next**.

- *Enterprise Manager:* The name or IP address of the computer on Veeam Backup Server is running.
- *Port*: The HTTP port number used by the Veeam Backup Server.

9 In the *Credential Verification* step, perform either of the following:

NOTE: The user credential must assign with either of the Portal Administrator, Restore Operator, or Portal User role.

1 Select Add Veeam Manager Server to a new credential, then the **Create New Credential** view appears on the right. Specify the credential related information, and then click **Next**.

Or

2 Select Add Veeam Manager server to an existing credential, then the **Selected Existing Credential** view appears on the right. Select an existing credential, and then click **Next**.

10 In the *Summary* step, confirm the agent information, and then click **Finish**.

The new Veeam Agent is created, and its data is to be monitored by Veeam Backup Server after a few minutes.

Editing agent properties

Default versions of these properties are installed with Foglight. However, you can edit the default shareable and agent properties, configure agent properties that apply only to a specific agent instance, and create edited clones of shareable properties that are used by a subset of agents of a certain type.

To edit the Rapid Recovery Agent properties:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.
5. On the menu bar, click the **Administration** tab.

   The **Administration** view appears at the bottom of the Protection dashboard.
6. Select the instance of the Rapid Recovery Agent which properties that you want to modify, and then click **Edit Properties.**
7. In the **Rapid Recovery Agent: Edit Properties** dialog box, edit the properties as needed, and then click **Save**.

   The **Rapid Recovery Agent: Edit Properties** dialog box closes and the list of agent instances automatically refreshes in the display area.

To edit the Veeam Agent properties:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click Protection.

   The **Protection** dashboard opens.
4. Use the Group selector located at the top of the dashboard to select the protection environment that you want to monitor.
5. On the menu bar, click the **Administration** tab.

   The **Administration** view appears at the bottom of the Protection dashboard.
6. Select the instance of the Veeam Agent which properties that you want to modify, and then click **Edit Properties.**
7. In the **Veeam Agent: Edit Properties** dialog box, edit the properties as needed, and then click **Save**.

   The **Veeam Agent: Edit Properties** dialog box closes and the list of agent instances automatically refreshes in the display area.

Managing certificates

Syntax Conventions

In order to successfully make use of the Foglight commands in your monitoring environment, review the syntax conventions before getting started. The syntax conventions are as follows:

- Generic examples follow the UNIX path structure that uses forward slashes '/' to separate directories.
- Platform-specific examples follow standard platform conventions. For example, UNIX-specific examples use forward slashes '/' as directory delimiters, while Windows examples use backslashes '\'.
- *<foglight_home>* is a placeholder that represents the path to the Foglight Management Server installation.
- *<foglight_agent_mgr_home>* is a placeholder that represents the path to the Foglight Agent Manager installation. This can be the location of the Foglight Agent Manager installation on a monitored host, or the home directory of the Foglight Agent Manager that comes embedded with the Foglight Management Server. For example:

  Path to the Foglight Agent Manager installation on a monitored host (Windows):

  C:\Quest\Foglight_Agent_Manager

  Path to the embedded Foglight Agent Manager installation (Windows):

  C:\Quest\Foglight\fglam
- Unless otherwise specified, Foglight commands are case-sensitive.

Managing certificates for FglAM

Foglight Evolve agents use Foglight Agent Manager (FglAM) to manage certificates for SSL encryption connection.

Prerequisite

All the certificate-related command line options require that FglAM be **up and running**.

Add a certificate

```
bin/fglam --add-certificate "user alias 1"=/path/to/certificate/file
```

- Validate the certificate and ensure the following:
  - It is not expired.
  - It is an X.509 format.
  - FglAM requires the Base64 format. To verify if the certificate file is encoded with Base64, open the certificate with a notepad and the certificate should be similar to the following example:

    ```
    -----BEGIN CERTIFICATE-----
    XXXXXXXX=
    -----END CERTIFICATE-----
    ```

    NOTE: If the certificate is not Base64 format, use openssl command to convert the certificate file into a Base64 file. Use either of the following commands depending on the source form:

    ```
    openssl x509 -inform DER -in xxx.cer -out xxx.crt
    ```

    or

    ```
    openssl x509 -inform PEM -in xxx.cer -out xxx.crt
    ```

- The `alias` is required and is used in the list and delete operations to refer to the certificate. It can be anything.

List installed certificates

```
bin/fglam --list-certificates
```

Print out a list of certificates and the aliases that refer to them.

Refer to the example output below:

```
List of installed certificates:
  Alias                Certificate Info
  -----                ----------------
  user alias 1        XXXX
```

Delete a certificate

Remove a certificate referred to by an `alias`.

```
bin/fglam --delete-certificate "user alias 1"
```

A full example for managing certificate for FglAM

- Add an example certificate into FglAM certificate store

  ```
  C:\Quest\Foglight\fglam\bin>fglam.exe --add-certificate "Evolve-test"="D:/Evolve-test.crt"
  …
  2020-02-27 16:31:01.000 INFO  [native] Certificate added: Certificate from
    D:\Evolve-test.crt added as Evolve-test
  ```

- List the example certificate in the FglAM certificate store

  ```
  C:\Quest\Foglight\fglam\bin>fglam.exe --list-certificate
  …
    Alias                       Certificate
    -----                       -----------
    Evolve-test                         Issuer:
                                  CN: XXX
  ```

- Delete the example certificate from the FglAM certificate store

  ```
  C:\Quest\Foglight\fglam\bin>fglam.exe --delete-certificate "Evolve-test"
  …
  2020-02-27 16:28:21.000 INFO  [native] Certificate deleted: Certificate
    Evolve-test deleted
  ```

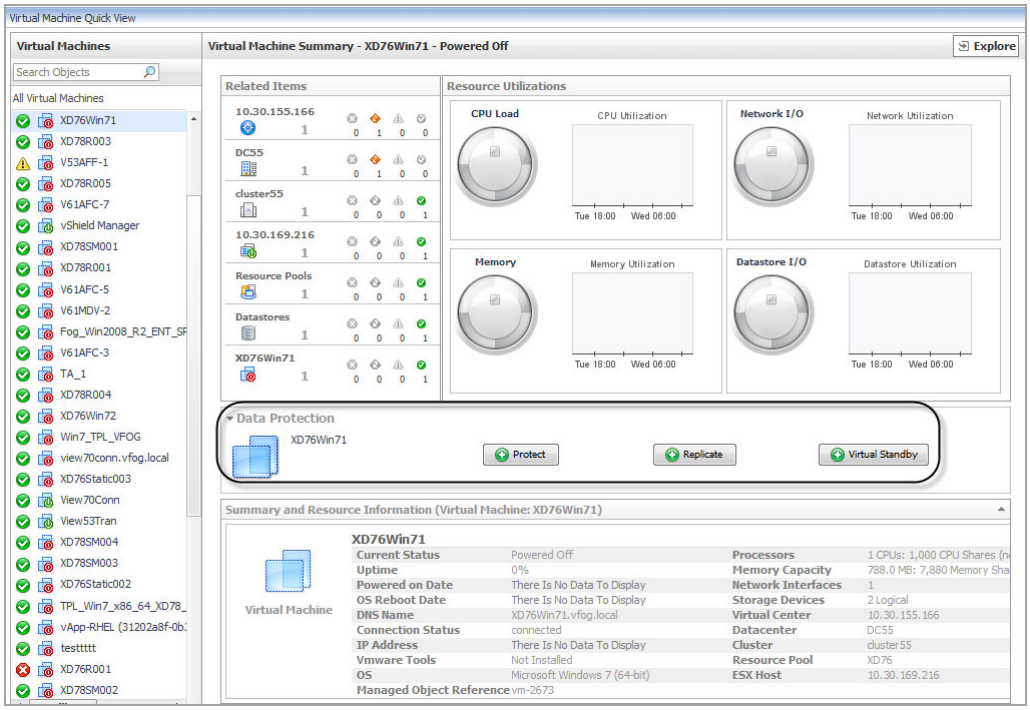
13

Virtual Machine Automation

The Protect Virtual Machine Automation provides you with an approach to perform the Protect, Replicate, and Virtual Standby operations on virtual machines from either of the following dashboards, without interfacing with the Rapid Recovery console.

- *VMware Environment* > *Virtual Machine Quick View*
- *VMware Environment* > *VMware Explorer*
- *Hyper-V Environment* > *Virtual Machine Quick View*
- *Hyper-V Environment* > *Hyper-V Explorer*

Figure 15. VM Automation view



To access the VM Automation view:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▸ on the left.
3. On the navigation panel, under *Homes*, click **VMware Environment** or **Hyper-V Environment.**

   The **VMware Environment** or **Hyper-V Environment** dashboard opens.
4. Select a Virtual Machine from the *Monitoring* > *Virtual Machine Quick View* > *Virtual Machines* tree view.

   The **VM Automation (Data Protection)** view appears in the middle of *Virtual Machine Summary* view.

The Protect Virtual Machine Automation includes the following three options:

- Automation of VM Protection: The automation of VM protection is only available for VMware virtual machines. For more information, see Automation of VM Protection on page 42.
- Automation of VM Replication: The virtual machines must be protected before performing the VM replication automation. For more information, see Automation of VM Replication on page 43.
- Automation of VM Standby: The virtual machines must be protected before performing the VM standby automation. For more information, see Automation of VM Standby on page 44.

Automation of VM Protection

The *VMware VM Protection Setup Wizard* guides you through the procedure for identifying virtual machines that you want to protect. This wizard also enables you to customize the schedule for performing the protection automation.

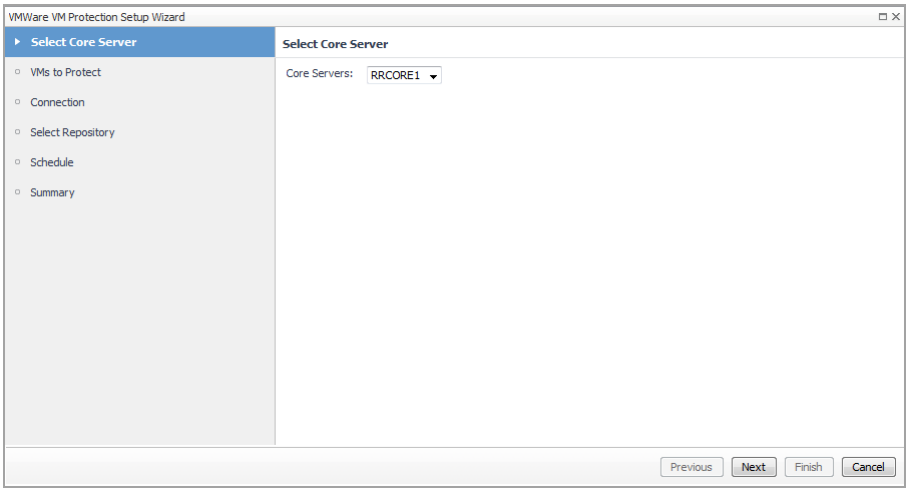
To perform the automation of VM protection:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **VMware Environment** or **Hyper-V Environment.**

   The **VMware Environment** or **Hyper-V Environment** dashboard opens.
4. Select a Virtual Machine that you want to protect from the *Monitoring* > *Virtual Machine Quick View* > *Virtual Machines* tree view.

   The **VM Automation (Data Protection)** view appears in the middle of *Virtual Machine Summary* view.
5. Click **Protect**. The *VMware VM Protection Setup Wizard* opens.
6. In the *Select Core Server* step, select a Core Server from the drop-down list, and then click **Next**.



7. In the *VMs to Protect* step, select VMs from the left vCenter table, click >> to move selected VMs to the right table, and then click **Next**.
8. In the *Connection* step, specify the port number as needed, and then click **Next**.
9. In the *Select Repository* step, select a repository from the *Core Repositories* drop-down list, and then click **Next**.
10. In the *Schedule* step, select either of the following schedule options, and then click **Next**:
    - *Default protection*: The automation will be performed hourly for all volumes.

- *Periods*: The automation will be performed on specified weekdays or weekends.
- *Daily protection time*: The automation will be performed on a daily basis.

11 In the *Summary* step, review all configurations and click **Finish**.

The selected VM will be added into *Protect Rapid Recovery Protected VMs* list and *Rapid Recovery Core Server* list after the VM protection automation is complete. The first time when a VM protection is added, its snapshot with the customized schedule will be transferred to the repository on the Rapid Recovery Core. You might need to wait for a while to see the VM's status update and to collect data back to Foglight from Rapid Recovery server.

Automation of VM Replication

The replicate is the process of copying recovery points from one Rapid Recovery Core and transmitting them to another Rapid Recovery Core for disaster recovery purposes. The process requires a paired source-target relationship between two or more cores. The *VM Replication Wizard* guides you through the procedure for identifying virtual machines that you want to replicate.

To perform the automation of VM replication:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click **VMware Environment** or **Hyper-V Environment**.

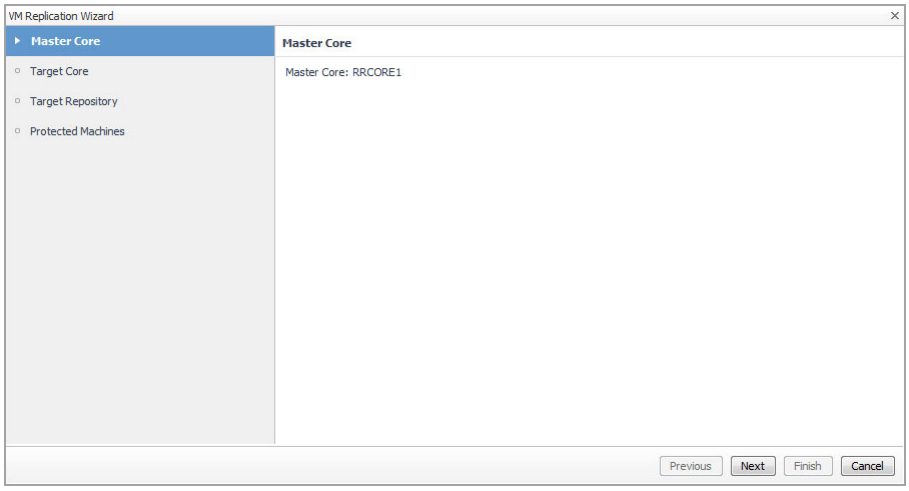
The **VMware Environment** or **Hyper-V Environment** dashboard opens.

4 Select a Virtual Machine that you want to protect from the *Monitoring* > *Virtual Machine Quick View* > *Virtual Machines* tree view.

The **VM Automation (Data Protection)** view appears in the middle of *Virtual Machine Summary* view.

5 Click **Replicate**. The *VM Replication Wizard* opens.

6 In the *Master Core* step, click **Next**.



7 In the *Target Core* step, select the target Core Server, and then click **Next**.

NOTE: If there is no available target Core, go to *Rapid Recovery Console* > *Replication* and add a target Core in the selected Master Core manually.

8 In the *Target Repository* step, select a repository, and then click **Next**.

9 In the *Protected Machines* step, select other virtual machines that you want to replicated as needed, and then click **Finish**.

The selected VMs will be added into target Core after the VM replication automation is complete. The replication pane contains summary information about the replicated machine, including the replication name, the state of replication, progress, and available space. You might need to wait for a while to see the VM's status update and to collect data back to Foglight from Rapid Recovery server.

Automation of VM Standby

The *VM Virtual Standby Wizard* guides you through the procedure for performing a virtual standby of continual export of recovery point data from a protected machine to a virtual machine in any supported VM format.

To perform the automation of VM standby:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

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

3 On the navigation panel, under *Homes*, click **VMware Environment** or **Hyper-V Environment**.

The **VMware Environment** or **Hyper-V Environment** dashboard opens.

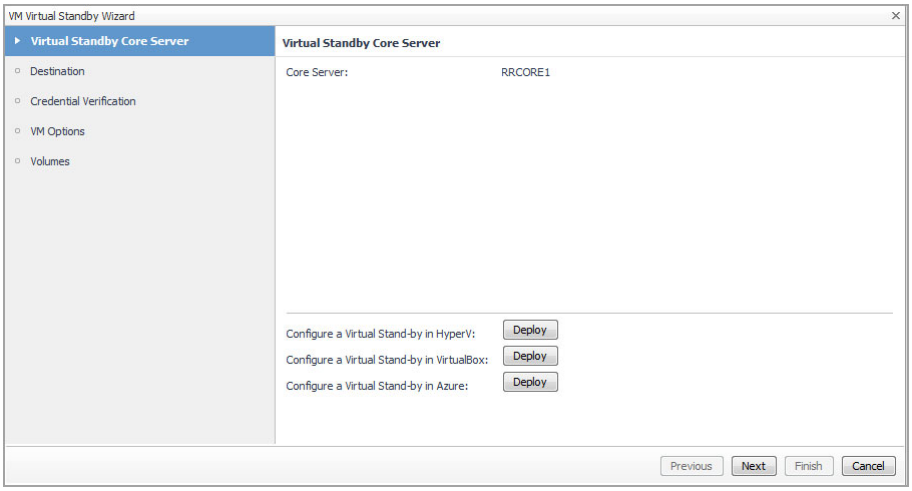
4 Select a Virtual Machine that you want to protect from the *Monitoring* > *Virtual Machine Quick View* > *Virtual Machines* tree view.

The **VM Automation (Data Protection)** view appears in the middle of *Virtual Machine Summary* view.

5 Click **Virtual Standby**. The *VM Virtual Standby Wizard* opens.

6 In the *Virtual Standby Core Server* step, verify the Core Server information, and then click **Next**.

NOTE: Currently only the virtual standby deployment in VMware is supported. If you need to deploy a virtual standby on Hyper-V/VirtualBox/Azure, go to the Rapid Recovery console.



7 In the *Destination* step, specify the host name and port number, and then click **Next**.

8 In the *Credential Verification* step, select new credential or an existing credential, and then click **Next**.

9 In the *VM Options* step, specify the following values, and then click **Next**.

- Resource Pool: Select a resource pool from the drop-down list.
- VM Configuration location: Select a data store from the drop-down list.
- Virtual machine name: Specify the name for the Virtual Machine.

- Amount of RAM (MB): Select either of the following to specify the amount of memory usage for the virtual machine:
  - Use the same amount of RAM as source machine
  - Use a specific amount of RAM, and then specify the amount in MB. The minimum amount is 1024 MB and the maximum allowed by the application is 65536 MB.
- Number of processors: The number of processors (CPUs) that is required for the exported virtual machine. The minimum is 1.
- Cores per processor: The number of cores that is required for each processor. The minimum is 1.
- Disk Provisioning: Select the type of disk provisioning:
  - Thin. Thin provisioning creates a virtual disk the size of the used space on the original volumes, rather than the entire volume size. For example, if the original volume is 1 TB, but contains only 2 GB of used space, Rapid Recovery creates a virtual disk of 2 GB.
  - Thick. Thick provisioning creates a new disk or volume that is the same size as the original volume from the protected server, even if only a portion of the original volume is being used. For example, if the volume is 1 TB large but contains 2 GB of used space, Rapid Recovery creates a virtual disk of 1 TB.
- Disk mapping: Specify the type of disk mapping as appropriate (Automatic, Manual, or with VM).
- Version: Select the version of the virtual machine.

10 In the *Volumes* step, select the volumes that you want to export, and then click **Next**.

11 On the *summary* step, click **Finish** to close the wizard and to start the export.

You can monitor the export process on Rapid Recovery console > Virtual standby Export Queue after the VM standby automation is complete. You might need to wait for a while to see the VM's status update and to collect data back to Foglight from Rapid Recovery server.

About Us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.