

Foglight® for NetVault® 7.3.0 **User
and Administration Guide**



© 2024 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 trademark 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.

Foglight for NetVault User and Administration Guide
Foglight Version - 7.3.0
Cartridge Version - 7.3.0

Contents

| | |
|--|-----------|
| Understanding Foglight for NetVault | 5 |
| About Foglight for NetVault | 5 |
| Key benefits | 5 |
| Architecture | 6 |
| Getting Started | 6 |
| Creating a NetVault Agent | 6 |
| Managing certificates | 7 |
| Configuring data collection interval | 9 |
| Heat Map Analytics | 10 |
| Scatter Plot Analytics | 10 |
| Recommended additional reading | 11 |
| Using Foglight for NetVault | 12 |
| Monitoring NetVault Backup Servers | 12 |
| Summary - All Servers view | 12 |
| Individual Server Summary view | 13 |
| Monitoring NetVault Backup Clients | 17 |
| Summary - All Clients view | 17 |
| Individual Client Summary view | 18 |
| Monitoring NetVault Backup Policies | 19 |
| Summary - All Policies view | 19 |
| Individual Policy Summary view | 20 |
| Monitoring NetVault Backup Devices | 21 |
| Summary - All Devices view | 21 |
| Individual Device Summary view | 21 |
| Viewing NetVault Backup Jobs | 22 |
| About Us | 23 |
| We are more than just a name | 23 |
| Our brand, our vision. Together. | 23 |
| Contacting Quest | 23 |
| Technical support resources | 23 |

Understanding Foglight for NetVault

- [About Foglight for NetVault](#)
- [Key benefits](#)
- [Architecture](#)
- [Getting Started](#)

About Foglight for NetVault

Foglight® for NetVault®, by the means of NetVault Restful APIs, integrates Foglight for Virtualization Enterprise Edition (hereafter referred to as FVE) with the NetVault Server, and provides the following capabilities to effectively monitor large-scale NetVault deployments, including:

- Monitor NetVault infrastructure, including the NetVault Server and its affiliated clients.
- Provide and display a subset of status to FVE on demand, including Job status, Client status, Device/Storage status and statistics, and status of data being protected.
- Show NetVault reports and alarm notifications.

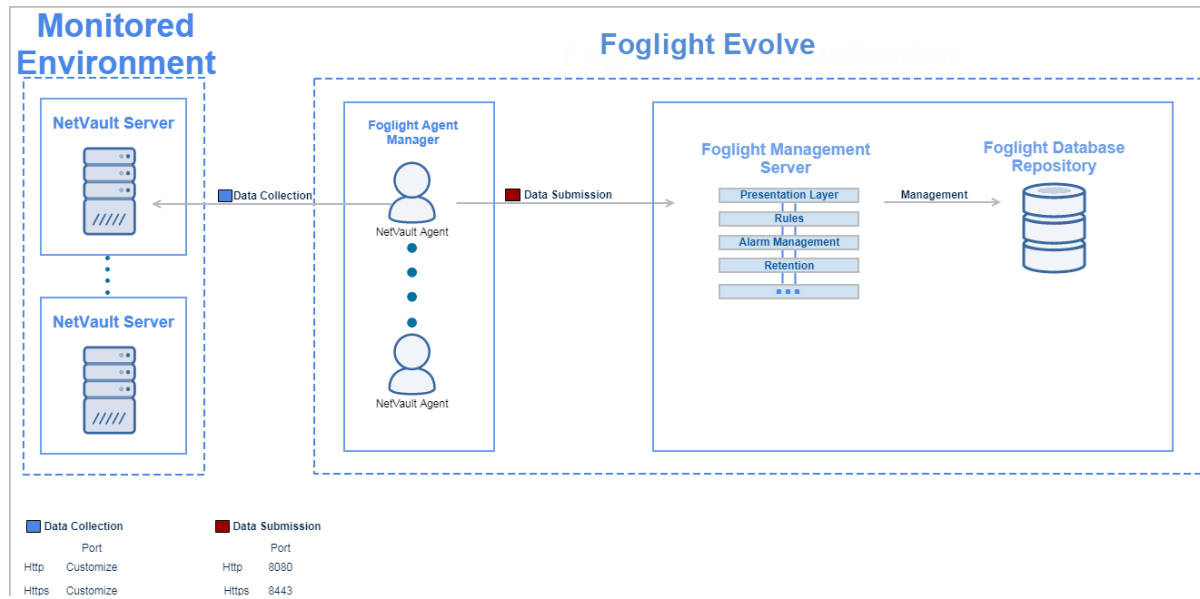
Key benefits

Foglight for NetVault offers these benefits for the customer environment:

- Better status visibility and monitoring for the complete NetVault environment.
- Single place to view the status and monitor multiple NetVault Servers and associated NetVault clients.
- Consolidated views of what is protected in a NetVault environment.
- Environment/equipment status and monitoring to help diagnose problems that can affect NetVault functionality and performance, especially where the cause of a problem is outside of NetVault control or visibility.
- Collection and display of historical status, events, performance, logs, and so on.
- More data and longer retention of data than what is stored by NetVault Servers.
- Better analysis of issues that require some history of data, for example:
 - Problems that were not noticed or reported until sometime after the occurrence.
 - Problems that are developed over time.
 - Problems that are sporadic or periodic.

Architecture

Figure 1. Components of Foglight for NetVault



Foglight for NetVault consists of three main components:

- Foglight Management Server and Foglight Database Repository — Responsible for managing, alerting, and viewing the collected data. Both components can be set to run on the same machine or reside on separate machines.
- Agent Manager — Hosts the monitoring NetVault agents.
- NetVault Backup Server — Provides the core services for protecting your data and administers backup and restore jobs for all assigned clients. Various types of physical and virtual storage devices can be locally attached to the server.

Getting Started

- [Creating a NetVault Agent](#)
- [Managing certificates](#)
- [Configuring data collection interval](#)
- [Heat Map Analytics](#)
- [Scatter Plot Analytics](#)
- [Recommended additional reading](#)

Creating a NetVault Agent

Each NetVault Agent monitors the assets inside the selected NetVault Backup environment. To enable the data collection for Foglight for NetVault, create a NetVault user with the “*Monitor Presets*” privilege, as well as grant this user with the access to the client groups and media groups that you want to monitor.

i | **NOTE:** Make sure to assign the minimum required privilege to your NetVault agent and the agent user; otherwise this agent can not start data collection.

i | **NOTE:** In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglIAM to use HTTPS. For more information, see [Managing certificates](#).

To create a NetVault agent:

- 1 Log in to the Foglight browser interface and make sure the left navigation panel is open.
- 2 On the navigation panel, under *Homes*, click **NetVault Environment**.
The **NetVault Environment** dashboard opens.
- 3 In the **NetVault Environment** dashboard, click **Administration**, and then click **Create Agent**.
The **NetVault Agent Wizard** dialog box opens.
- 4 **Select Agent Host:** Select the agent manager on which the new agent is to be deployed, and then click **Next**.
- 5 **NetVault Properties:** Specify the following values, and then click **Finish**.
 - **Server Address:** The IP address of the NetVault Server that hosts the agent instance.
 - **Port:** The port number used by the NetVault Server for listening to the connections from the agent instance (default: 8443).
 - **Use Https:** The option used to enable the agent connection using HTTPS (default: true).
 - **Login Username:** The name of the user that has the privileges required for connecting to the NetVault Server and retrieving information.
 - **Login Password:** The password of the user that has the privileges required for connecting to the NetVault Server and retrieving information.
 - **Error Event Keywords:** Keywords used to classify NetVault error events. Separate multiple keywords by comma.
 - **Warning Event Keywords:** Keywords used to classify NetVault warning events. Separate multiple keywords by comma.
 - **Collected Event Classes:** The option used to indicate which event classes will be collected by the agent instance. By default, all event classes available in the NetVault Server are checked.
 - **Collect Log Level:** The option used to indicate which logs will be collected by the agent instance. Warning and above is set by default.

The new NetVault Agent is created and its data will be shown on the **Monitoring** tab after a few minutes.

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-----  
XXXXXXXXXX=  
-----END CERTIFICATE-----
```

i **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
```

Configuring data collection interval

The default data collection interval of NetVault agents is set to 10 minutes by default. Foglight for NetVault enables you to change this collection interval as needed.

i | **NOTE:** Changing the data collection interval will take effect for all NetVault agents.

To configure the data collection interval:

- 1 On the navigation panel, under **Dashboards**, select **Administration > Agents > Agent Status**.
- 2 On the *Agent Status* dashboard, select the NetVault agent that you want to monitor, and then click **Edit Properties**.
- 3 In the *Edit Properties* dashboard, click **Edit** next to the *Collector Config* field.

i | **NOTE:** Quest highly recommends setting the *Collector Config* (also known as *Collection interval*) to a value that is larger than 10 minutes and is multiples of 10 minutes; otherwise the NetVault agent might not collect metrics from the NetVault Server.

The screenshot shows a web interface with two main sections. The top section is titled 'Event Configuration' and contains three input fields: 'Error event keywords, multiple words split with comma.' with the value 'error', 'Warning event keywords, multiple words split with comma.' with the value 'warning', and 'Collect Class Name' with a dropdown arrow. An 'Edit' button is to the right of these fields. The bottom section is titled 'Data Collection Scheduler' and contains a dropdown menu for 'Collector Config' with the value 'defaultSchedule' and an 'Edit' button. A red circle highlights the 'Data Collection Scheduler' section.

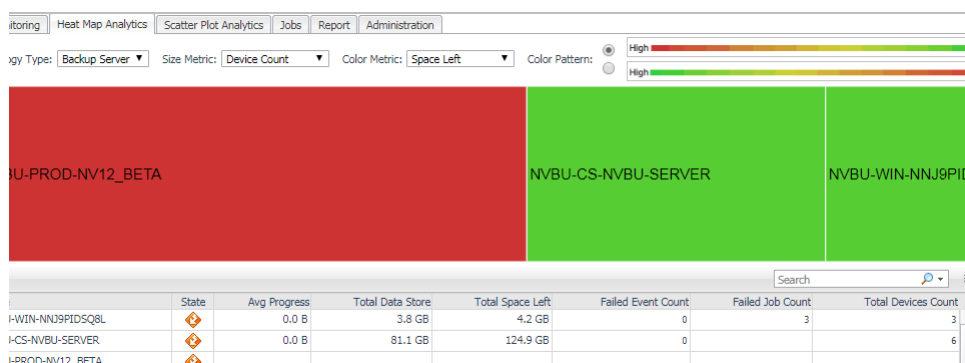
Heat Map Analytics

Heat Map is a two-dimensional representation of data in which values are represented by colors. Showing collected metrics with elaborate heat maps allows you to understand complex data sets and the monitored NetVault environment well. Heat maps will be refreshed automatically when you change either of the following fields:

- **Topology Type:** Indicates the monitored topology object, including Backup Server, Backup Client, Device Library, and Job.
- **Size Metric:** Populates a rectangle based upon the selected metrics. For example, if you select *Data Stored* from the Size Metric drop-down list, the rectangle area will be populated based on the data stored in the topology object.
- **Rendering related metrics:** For example, if you select *Space Available* and Red to Green, the rectangle of the topology object that has more available spaces will be rendered in red.
 - **Color Metric:** Renders the color of rectangle based upon the selected metrics.
 - **Color Pattern:** Offers two patterns, Red to Green (larger value shows in red) or Green to Red (larger value shows in green).

Figure 2 shows an example of heat map. This sample diagram represents the NVBU-PROD-NV12_BETA has the maximum amounts of devices and remaining spaces while NVBU-WIN-NNJ9 has the minimum amount. If you switch the Color Pattern, then NVBU-PROD-NV12_BETA will turn to green and NVBU-WIN-NNJ9 will show in red.

Figure 2. Sample Heat Map



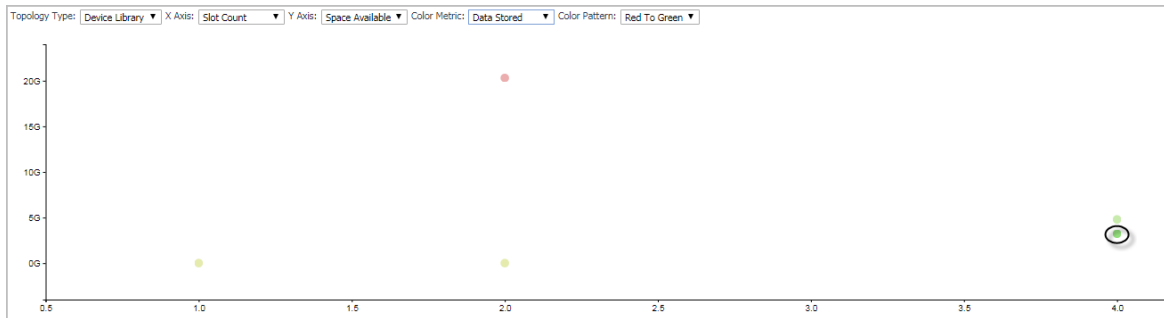
Scatter Plot Analytics

Scatter Plot is used to display values in points using two variables for a set of data. The points are color-coded also, Color Metric can be used to display one additional variable. The points on the chart will be refreshed automatically when you change either of the following fields:

- **Topology Type:** Indicates the monitored topology object, including Backup Server, Backup Client, Device Library, and Job.
- **X Axis:** Indicates which metrics will be plotted on X axis.
- **Y Axis:** Indicates which metrics will be plotted on Y axis.
- **Rendering related metrics:** For example, if you select *Space Available* and Red to Green, the rectangle of the topology object that has more available spaces will be rendered in red.
 - **Color Metric:** Renders the color of rectangle based upon the selected metrics.
 - **Color Pattern:** Offers two patterns, Red to Green (larger value shows in red) or Green to Red (larger value shows in green).

Figure 3 shows an example of Scatter Plot analytics. The green point on lower-bottom represents the following: its Slot Count is 4, its Space Available is less than 5G, and it has the minimum amount of data stored as this point shows in green.

Figure 3. Sample Scatter Plot



Recommended additional reading

As tasks on the Report dashboard and the Administration dashboard are commonly used throughout Foglight and FVE products, Quest recommends that you read the following guides to understand both dashboards and the relevant tasks.

- Chapter “*Explore the Agent Status dashboard*” in the *Foglight Administration and Configuration Guide*.
- Chapter “*Reporting on Your Enterprise*” in the *Foglight User Guide*.

In addition to the above guides, Quest also recommends that you read through the *Quest NetVault Backup Administrator’s Guide*, to get a comprehensive understanding about Quest NetVault Backup.

Using Foglight for NetVault

- [Monitoring NetVault Backup Servers](#)
- [Monitoring NetVault Backup Clients](#)
- [Monitoring NetVault Backup Policies](#)
- [Monitoring NetVault Backup Devices](#)
- [Viewing NetVault Backup Jobs](#)

Monitoring NetVault Backup Servers

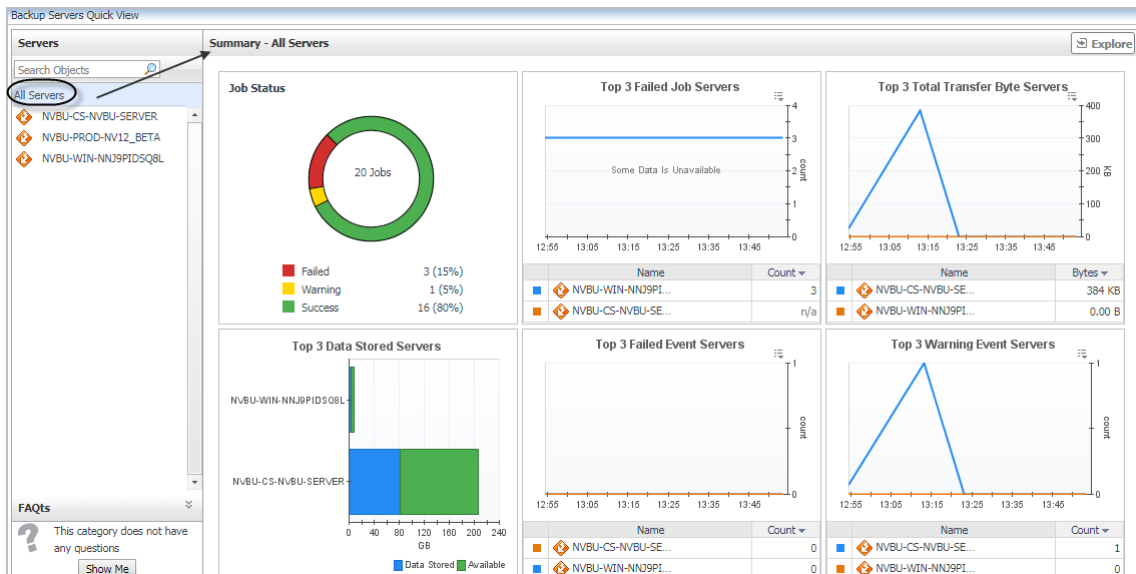
The *Backup Servers Quick View*, which appears after clicking **Monitoring > Servers**, shows the data collected about the selected NetVault environment. This view consists of the following two panes:

- The **Servers** tree view, which appears on the left of *Backup Servers Quick View*, lists the NetVault Servers existing in the monitored NetVault environment.
- The [Summary - All Servers view](#), which appears on the right after you click the **All Servers** node in the **Servers** tree view.
Or
The [Individual Server Summary view](#), which appears on the right after you select an individual server node in the **Servers** tree view.

Summary - All Servers view

The **Summary - All Servers** view appears on the right when you select **All Servers** in the **Servers** tree view.

Figure 4. Summary - All Servers view



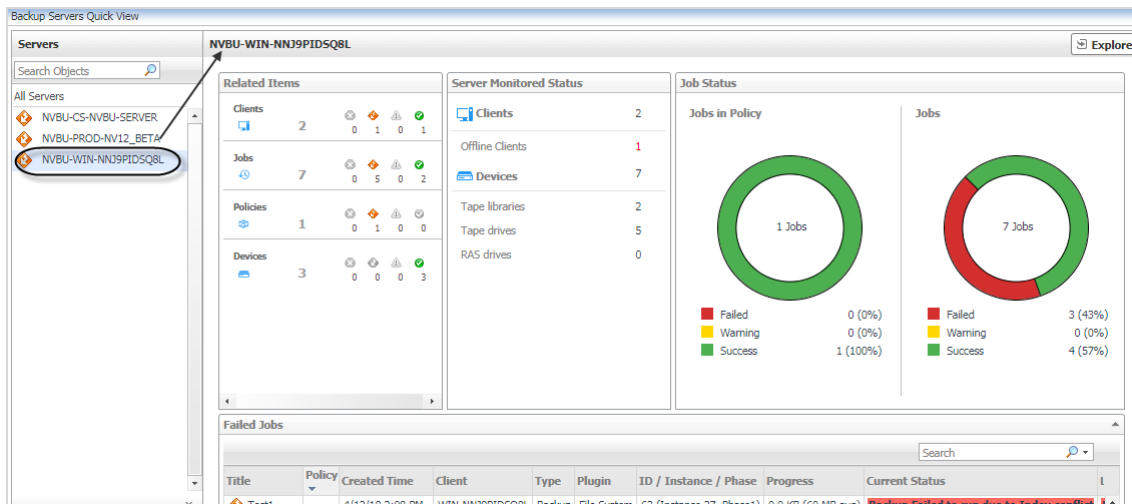
The **Summary - All Servers** view displays the following data:

- **Job Status:** Displays the number and status (Failed, Warning, or Success) of Jobs existing in all NetVault Backup Servers available in the monitored environment.
- **Top 3 Failed Job Servers:** Based upon the failed job counts, lists the NetVault Backup Servers in descending order.
- **Top 3 Total Transfer Bytes:** Based upon the value of transfer bytes, lists the top three NetVault Backup Servers.
- **Top 3 Data Stored:** Based upon the value of stored data, lists the NetVault Backup Servers in ascending order.
- **Top 3 Failed Events:** Based upon the number of failed events, lists the top three NetVault Backup Servers.
- **Top 3 Warning Events:** Based upon the number of warning events, lists the top three NetVault Backup Servers.

Individual Server Summary view

The **Individual Server Summary** view appears on the right when you select a server in the **Servers** tree view.

Figure 5. Individual Server Summary view



The **Individual Server Summary** view displays the following data:

- **Related Items:** Shows the number of Clients/Jobs/Policies/Devices that are affiliated with this NetVault Backup Server.
- **Server Monitored Status:** Shows the number of total and online Clients/Devices, and the number of Healthy/Warning/Error Jobs.
- **Job Status:**
 - **Jobs in Policy:** Displays the number and status (Failed, Warning, or Success) of Jobs existing in the policy.
 - **Jobs:** Displays the number and status (Failed, Warning, or Success) of Jobs existing in this NetVault Backup Server.
- **Failed Jobs:** Displays the detailed information about all failed jobs happened in this NetVault Backup Server.

Click **Explore** on the upper right of the **Individual Server Summary** view to open the **Server Explorer** view, which shows more detailed information about this NetVault Backup Server.

Server Explorer view

The **Server Explorer** view opens when you click **Explore** in the **Individual Server Summary** view, which includes the following tabs:

- **Server Summary tab:** This tab shows the same with **Individual Server Summary** view.
- **Server Performance tab**
- **Server Dependency tab**

Server Performance tab

The **Server Performance** tab displays the resource utilization for the selected NetVault Server over a selected period of time, which includes the following:

- **CPU:** Shows the CPU utilization summary for the selected NetVault Server based on its total capacity during a selected time period.
- **Memory:** Shows the physical memory utilization summary for the selected NetVault Server, broken into the amounts of memory that is swapped to disk, actively used, and allocated, all during a selected time period.
- **Storage:** Shows the disk utilization summary for the selected NetVault Server during a selected time period.

- **Network:** Shows the network utilization summary for the selected NetVault Server, including the average rate of network throughput, and the amounts of data sent to and received from the network.
- **Alarms:** Displays a list of alarms generated against the NetVault Server selected in the **Servers** tree view. Use this view to quickly identify any potential problems related to a specific NetVault Server.

Troubleshooting: No data displayed in the Server Performance tab

If the Host is not in the same domain with the Foglight Agent Manager on which the NetVault agent is running, there will be no data displayed in the *Server Performance* tab. In this case, do the following:

- 1 Browse to open the *hosts* file under *C:\Windows\System32\drivers\etc*.
- 2 Add the following line in the *hosts* file, then save and close.

<IP address of the host> <Machine ID of the host>

- 3 In the *Server Performance* tab, click **Add OS Monitor -> Single Host** on the top right.

The **Add Monitored Host** dialog box appears.

- 4 **Host and Agent Manager:** Specify the name or IP address of the host to be monitored, select an Agent Manager and OS type, and then click **Next**.

- 5 **Agent Properties:** Specify the following agent properties, and then click **Next**.

- **Agent Name:** Type the fully qualified host name of the machine on which the monitored the host specified in step 4.
- **Collect Top N Process Details:** Select this option if you want to collect top N server details from the monitored NetVault environment.
- **Use Ping to validate host availability:** Select this option if you want to enable the host availability validation using ping command.
- **Top CPU Processes:** Type a positive integer, for example, 5. This means the agent will collect top five NetVault Servers with the highest CPU utilization.
- **Top Memory Processes:** Type a positive integer, for example, 5. This means the agent will collect top five NetVault Servers with the highest memory utilization.
- **Top IO Processes:** Type a positive integer, for example, 5. This means the agent will collect top five NetVault Servers with the highest data transfer rates.
- **Collect Process Metrics:** Select this option if you want to collect process metrics from the monitored NetVault environment.
- **Aggregate Program Instances Data:** Select this option if you want to aggregate the data of program instances.
- **Collect Metrics:** Select *CPU, Disk, Memory, Network*, some of them, or all of them, as required.
- **Excluded Drives:** Select a list in which you want to specify the drives that you want to exclude from monitoring. You can select or clone an existing list, and edit it, as required. The default list is *defaultExcludedDrives*. Lists can be shared between multiple agent instances.

For each entry in the list, set its properties as follows:

- **Host Name Expression:** The name of one or more hosts that you want to exclude from monitoring. To specify multiple hosts, you must use regular expressions.
- **Drive Name Expression:** The name of one or more drives that you want to exclude from monitoring. To specify multiple drives, you must use regular expressions.
- **Process Availability Config:** Select a list in which you want to configure the process availability. You can select or clone an existing list, and edit it, as required. The default list is *defaultProcessAvailabilityConfig*. Lists can be shared between multiple agent instances.

For each entry in the list, set its properties as follows:

- **Process Name:** The name of process that you want to configure its availability.
- **Command Line:** The command line used to validate the process availability.

- *Expected Process Count*: The amount of expected process.
- *Include mounted remote filesystems*: Select this option if you want to include one or more mounted remote FileSystems.
- *Filesystem Type Config*: Select a list in which you want to configure the process availability. You can select or clone an existing list, and edit it, as required. The default list is *defaultProcessAvailabilityConfig*. Lists can be shared between multiple agent instances.

For each entry in the list, set its properties as follows:

- *Process Name*: The name of process that you want to configure its availability.
 - *Command Line*: The command line used to validate the process availability.
 - *Expected Process Count*: The amount of expected process.
- *Service Metrics*
 - *Collect Service Metrics*: Select either of the following: *Collect all services*, *Do not collect service*, *Collect only specified services*.
 - *Services to Monitor*: This option takes effect only when *Collect only specified services* is selected above. Select a service list that you want to collect.
- *Log Settings*
 - *Collect Log Events*: Select this option if you want to collect log events from the monitored NetVault environment.
 - *EventLog Backlog Hours*: Type a positive integer, for example, 1. This means the last one-hour log events will be saved.
 - *Event Logs To Monitor*: Select a list that includes the log classes to be collected. You can select or clone an existing list, and edit it, as required. The default list is *defaultEventLogs*. Lists can be shared between multiple agent instances.
 - *Event Log Filter*: Select a list of log filters. You can select or clone an existing list, and edit it, as required. The default list is *defaultEventFilter*. Lists can be shared between multiple agent instances.
 - *Event Log Severity*: Select a list of log severity. You can select or clone an existing list, and edit it, as required. The default list is *defaultEventSeverityMap*. Lists can be shared between multiple agent instances.
- *Collector Configuration*: This option is also known as *Data Collection Scheduler*. The default list is *defaultScheduler*.

For each entry in the list, set its properties as follows:

- *Name*: Contains the name of the default collector.
- *Interval*: Contains the length of the default collection interval.
- *Unit*: Contains the time unit for measuring the default collection interval: *milliseconds*, *seconds*, *minutes*, *hours*, or *days*.
- *Fast-Mode Interval*: Contains the length of the collection interval when the agent is running in fast mode.
- *Fast-Mode Unit*: Contains the time unit for measuring the collection interval when the agent is running in fast mode: *milliseconds*, *seconds*, *minutes*, *hours*, or *days*.
- *Fast-Mode Max Count*: Contains the maximum count of entries when the agent is running in fast mode.

6 *Credential Verification*: select one of the following options:

- *Do not configure a credential*: Select this option if you want to configure the credential for this resource at a later time.

- *Add host(s) to a new credential:* Select this option if you want to add the host to a new credential. This option is suitable if none of the existing credentials have the connection details needed to access the new host.

Then follow on-screen instructions to complete the credential verification.

- *Add host(s) to an existing credential:* Select this option if you want to add the host to an existing credential. This option is suitable if an existing credential has the security data needed to access the new host, but you need to edit its resource mappings to include this host.

Then follow on-screen instructions to complete the credential verification.

7 *Summary:* Review the information provided about the host and the monitoring agent, and click **Finish**.

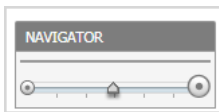
Server Dependency tab

A typical NetVault environment consists of many interrelated components. Understanding the dependencies between specific components in your monitored environment and the levels of resources they consume allows you to better understand resource-related issues, potentially affecting the stability of your system. This can help you predict the impact a potential outage may have.

The *Server Dependency* tab visualizes the relationships between the objects in your environment through an interactive dependency map. The map illustrates how different components relate to each other, and the levels of the available resources available to them. The *Server Dependency* tab provides a quick and easy way to view components grouped by device.

In a large multi-component environment, dependency maps are likely complex and may not fit your screen. The **NAVIGATOR** in the bottom-right corner allows you to easily set the zoom level by dragging the slider into the appropriate position. In addition,

Figure 6. Navigator



To find out more about an object appearing in the dependency map, click the object icon. A dwell appears, displaying more details about that object. The type and range of information appearing in the dialog box depends on the selected object's type.

Monitoring NetVault Backup Clients

The *Backup Clients Quick View*, which appears after clicking **Monitoring > Client**, shows the data collected about the selected NetVault environment. This view consists of the following two panes:

- The **Clients** tree view, which appears on the left of *Backup Clients Quick View*, lists the NetVault Clients existing in the monitored NetVault environment.
- The [Summary - All Clients view](#), which appears on the right after you click the **All Clients** node in the **Clients** tree view.

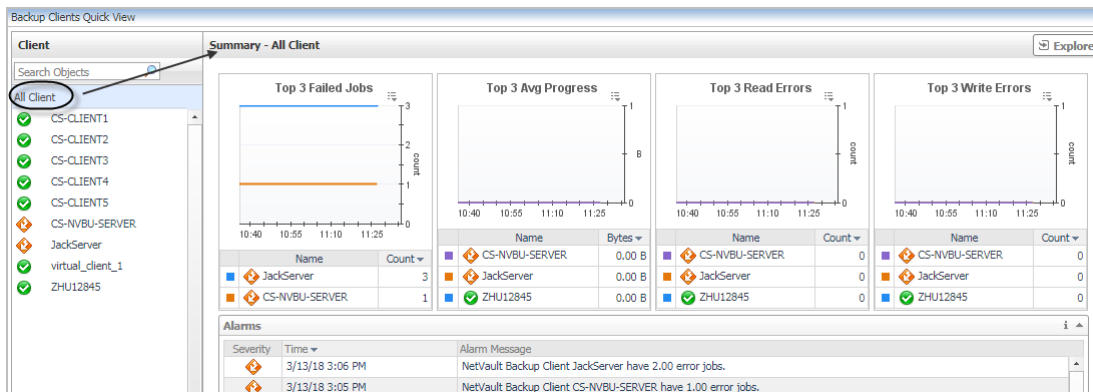
Or

The [Individual Client Summary view](#), which appears on the right after you select an individual client node in the **Clients** tree view.

Summary - All Clients view

The **Summary - All Clients** view appears on the right when you select **All Clients** in the **Clients** tree view.

Figure 7. Summary - All Clients view



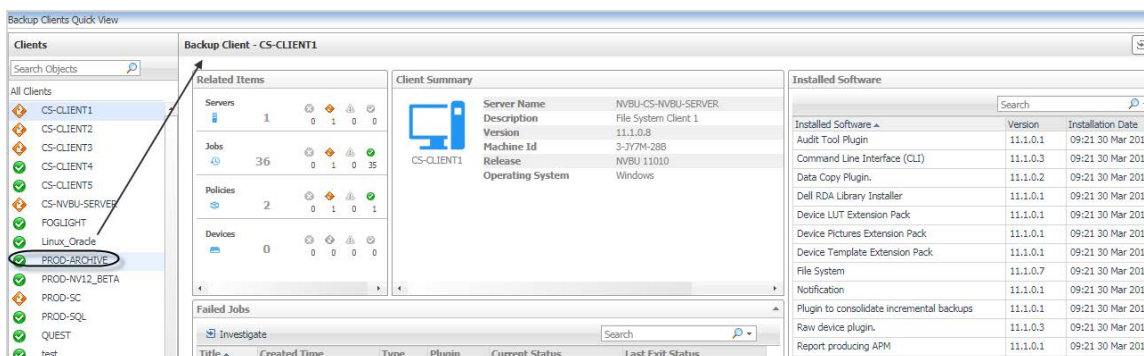
The **Summary - All Clients** view displays the following data:

- **Top 3 Failed Jobs:** Lists the top three NetVault Backup Clients with the highest amount of failed jobs during the selected time range.
- **Top 3 Avg Progress:** Lists the top three NetVault Backup Clients with the highest network transfer data to or from the network during the selected time range.
- **Top 3 Read Errors:** Lists the top three NetVault Backup Clients with the highest read errors during the selected time range.
- **Top 3 Write Errors:** Lists the top three NetVault Backup Clients with the highest write errors during the selected time range.
- **Alarms:** Lists the alarms generated against the monitored NetVault environment.

Individual Client Summary view

The **Individual Client Summary** view appears on the right when you select a client in the **Clients** tree view.

Figure 8. Individual Client Summary view



The **Individual Client Summary** view displays the following data:

- **Related Items:** Shows the number of Servers/Jobs/Policies/Devices that are affiliated with this NetVault Backup Client.
- **Client Summary:** Shows the physical information about this NetVault Backup Client.
- **Installed Software:** Lists the name and installation date of all software installed on this NetVault Backup Client.
- **Failed Jobs:** Displays the detailed information about all failed jobs happened in this NetVault Backup Client.

Click **Explore** on the upper right of the **Individual Client Summary** view to open the **Client Explorer** view, which shows more detailed information about this NetVault Backup Client.

Client Explorer view

The **Client Explorer** view opens when you click **Explore** in the **Individual Client Summary** view, which includes the following tabs:

- **Client Summary tab:** This tab shows the same with **Individual Client Summary** view.
- **Client Performance tab:** This tab shows the same with **Server Performance** tab.
- **Client Dependency tab:** This tab shows the same with **Server Dependency** tab.

Monitoring NetVault Backup Policies

The **Backup Policies Quick View**, which appears after clicking **Monitoring > Policy**, shows the data collected about the selected NetVault environment. This view consists of the following two panes:

- The **Policies** tree view, which appears on the left of **Backup Policies Quick View**, lists the NetVault Backup Policies existing in the monitored NetVault environment.
- The **Summary - All Policies** view, which appears on the right after you click the **All Policies** node in the **Policies** tree view.

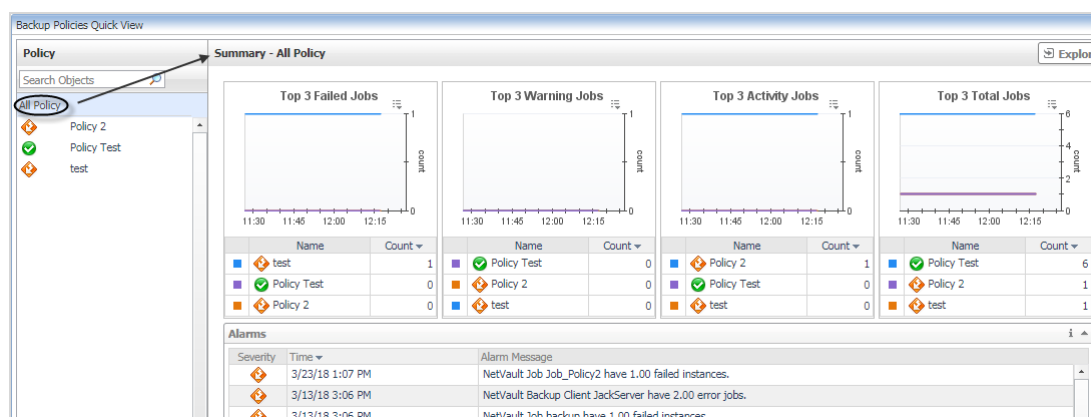
Or

The **Individual Policy Summary** view, which appears on the right after you select an individual Policy node in the **Policies** tree view.

Summary - All Policies view

The **Summary - All Policies** view appears on the right when you select **All Policies** in the **Policies** tree view.

Figure 9. Summary - All Policies view



The **Summary - All Policies** view displays the following data:

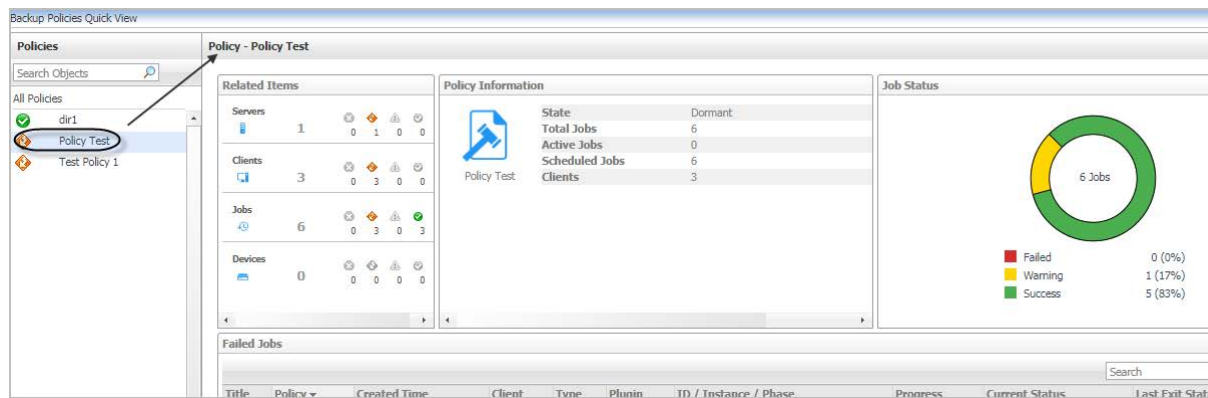
- **Top 3 Failed Jobs:** Lists the top three NetVault Backup Policies with the highest amount of failed jobs during the selected time range.
- **Top 3 Warning Jobs:** Lists the top three NetVault Backup Policies with the highest amount of warning Jobs during the selected time range.

- *Top 3 Activity Jobs*: Lists the top three NetVault Backup Policies with the highest amount of Activity Jobs during the selected time range.
- *Top 3 Total Jobs*: Lists the top three NetVault Backup Policies with the highest amount of Jobs during the selected time range.
- *Alarms*: Lists the alarms generated against the monitored NetVault environment.

Individual Policy Summary view

The **Individual Policy Summary** view appears on the right when you select a policy in the **Policies** tree view.

Figure 10. Individual Policy Summary view



The **Individual Policy Summary** view displays the following data:

- *Related Items*: Shows the number of Servers/Jobs/Clients/Devices that are affiliated with this NetVault Backup Policy.
- *Policy Information*: Shows the Status, Total Jobs, Active Jobs, Scheduled Jobs, and Clients about this NetVault Backup Policy.
- *Job Status*: Displays the number and status (Failed, Warning, or Success) of Jobs existing in this NetVault Backup Policy.
- *Failed Jobs*: Displays the detailed information about all failed jobs happened in this NetVault Backup Policy.

Click **Explore** on the upper right of the **Individual Policy Summary** view to open the **Policy Explorer view**, which shows more detailed information about this NetVault Backup Client.

Policy Explorer view

The *Policy Explorer* view opens when you click **Explore** in the *Individual Policy Summary view*, which includes the *Summary* tab that presents the following information of this NetVault Backup Policy:

- *Title*: Shows the title of this Backup Policy.
- *Policy*: Shows the name of this Backup Policy.
- *Created Time*: Shows the date and time when this Backup Policy is created.
- *Client*: Shows the name of the Client on which this Backup Policy is running.
- *Type*: Shows the type of this Backup Policy.
- *Plugin*: Shows the name of the plug-in to which this Backup Policy is specific.
- *ID/Instance/Phase*: Shows the amount of ID, instance, and phase.
- *Progress*: Shows the transfer byte in KB.

- **Current Status:** Shows the current status message of this Backup Policy.
- **Last Exit Status:** Shows the status message when this Backup Policy exits last time.

Monitoring NetVault Backup Devices

The *Backup Devices Quick View*, which appears after clicking **Monitoring > Device**, shows the data collected about the selected NetVault environment. This view consists of the following two panes:

- The **Devices** tree view, which appears on the left of *Backup Devices Quick View*, lists the NetVault Devices existing in the monitored NetVault environment.
- The **Summary - All Devices view**, which appears on the right after you click the **All Devices** node in the **Devices** tree view.

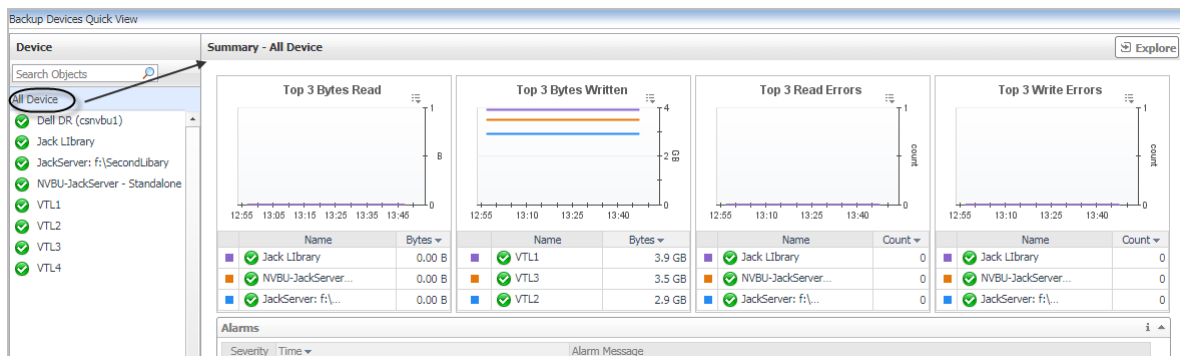
Or

The **Individual Device Summary view**, which appears on the right after you select an individual device node in the **Devices** tree view.

Summary - All Devices view

The **Summary - All Device** view appears on the right when you select **All Devices** in the **Devices** tree view.

Figure 11. Summary - All Devices view



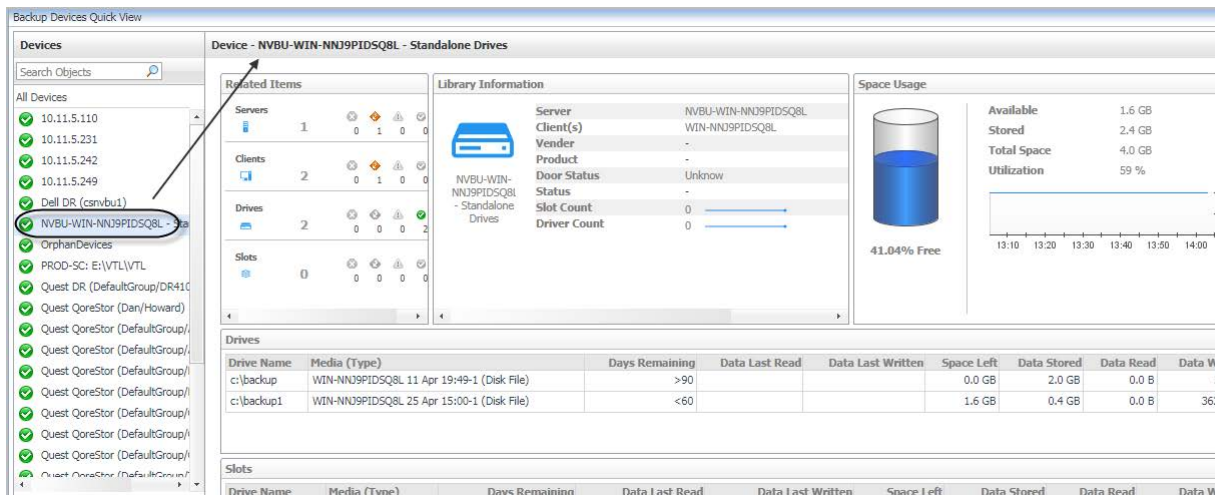
The **Summary - All Devices** view displays the following data:

- **Top 3 Bytes Read:** Lists the top three NetVault Backup Devices with the highest amount of Bytes read to the device during the selected time range.
- **Top 3 Bytes Written:** Lists the top three NetVault Backup Clients with the highest amount of Bytes written to the device during the selected time range.
- **Top 3 Read Errors:** Lists the top three NetVault Backup Devices with the highest read errors during the selected time range.
- **Top 3 Write Errors:** Lists the top three NetVault Backup Devices with the highest write errors during the selected time range.
- **Alarms:** Lists the alarms generated against the monitored NetVault environment.

Individual Device Summary view

The **Individual Device Summary** view appears on the right when you select a client in the **Devices** tree view.

Figure 12. Individual Device Summary view



The **Individual Device Summary** view displays the following data:

- **Related Items:** Shows the number of Servers/Clients/Drivers/Slots that are affiliated with this NetVault Backup Device.
- **Library Information:** Shows the following physical information about this NetVault Backup Device.
 - Server: Server name.
 - Client: Client to which the device is attached.
 - Vendor: Vendor name.
 - Product: Library type.
 - Door Status: Device status (online or offline).
 - Slot Count: Number of slots.
 - Drive Count: Number of drives.
- **Space Usage:** Shows the storage usage of this NetVault Backup Device.
- **Drives:** Shows the detailed information of all drives attached to this NetVault Backup Device.
- **Slots:** Displays the detailed information about all Slots attached to this NetVault Backup Device.

Viewing NetVault Backup Jobs

The *Jobs View*, which appears after clicking the *Jobs* tab, shows the Job-related information from the selected NetVault environment. This view consists of the following two tabs:

- The *All Jobs* tab — This tab includes the *All Jobs* table showing the following details for all Jobs collected from the monitored NetVault environment: name of Job, policy name, Job type, plug-in details of a job, selection set, next runtime, and advanced options.
- The *Failed Jobs* tab — This tab includes the following:
 - The *Failed Jobs* line chart shows the number of failed jobs existing in the monitored NetVault environment.
 - The *Failed Jobs* table shows the following details for all failed Jobs collected from the monitored NetVault environment: Job title, Policy name, Job created time, Client name, Job type, plug-in name, amount of ID/Instance/Phase, transfer bytes, current status message, and last exit status message.

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/>.

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.