

Foglight® Hybrid Cloud Manager for Google
Cloud 1.9.0

User and Administration Guide



© 2020 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 Where next meets now 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 LLC 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. Tevtron, the Tevtron logo, and CitraTest are registered trademarks of Tevtron, 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.

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

Foglight Hybrid Cloud Manager for Google Cloud User and Administration Guide
Updated - December 2020
Foglight Version - 5.9.8
Software Version - 1.9.0

Contents

Using Foglight Hybrid Cloud Manager for Google Cloud	6
Installation requirements	6
Getting Started	7
Generating Google Cloud Service Account File	7
Getting the BigQuery Table ID	8
Service Account Permissions	9
Creating a Google Cloud Agent	11
Dashboard location and UI elements	13
Service selector	14
Actions bar	14
Menu bar	15
Quick view	15
Monitoring Tab	16
Projects	17
Project Explorer view	17
Regions	18
Region Explorer view	19
Instance Groups	19
Instance Group Explorer view	20
VM Instances	21
VM Instance Explorer view	22
Rule Configuration Tab	23
Rules view	23
Enabling/Disabling rule(s)	24
Adding a custom rule	25
Removing custom rule(s)	25
Reports Tab	27
Available report templates	27
Usage & Quotas Tab	29
Administration Tab	30
Agents related commands	30
Editing agent properties	31
Managing certificates	32
Syntax Conventions	32
Managing certificates for FglIAM	33
Managing certificates for FMS in FIPS-compliant mode	34
Cost Tab	37
Cost - Overview	37
Cost - Google Cloud view	38

Cost - Admin view	38
About Us	39
Technical support resources	39

Using Foglight Hybrid Cloud Manager for Google Cloud

Foglight® Hybrid Cloud Manager for Google Cloud helps visually monitor and manage Google Cloud platform.

The Foglight Hybrid Cloud Manager for Google Cloud User and Administration Guide is intended for users who belong to the Administrators group of Google Cloud and have been assigned either of System Administrator or Advanced Operator role.

The section introduces you to the Foglight Hybrid Cloud Manager for Google Cloud environment and provides you with essential information.

For more information, see the following topics:

- [Installation requirements](#)
- [Getting Started](#)
- [Dashboard location and UI elements](#)

Installation requirements

Foglight Hybrid Cloud Manager for Google Cloud comes installed on Foglight Evolve.

Foglight Hybrid Cloud Manager for Google Cloud requires the following cartridges for data collection:

- 1 *vUsage-Feedback-5_8_3.car*
- 2 *DRP-5.8.3.car*
- 3 *Cloud-Manager-1.9.0.car*
- 4 *CommonAnalytics-5_8_3.car*
- 5 *Optimizer-5.8.3.car*
- 6 *GoogleCloudAgent-1.9.0.car*

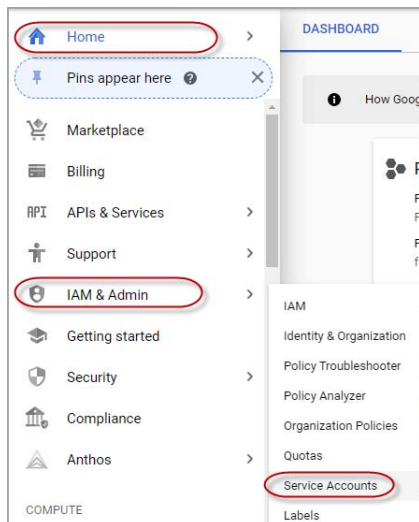
While Foglight Evolve comes with these cartridges pre-installed and enabled, a stand-alone Foglight release requires that these components be installed on the Foglight Management Server. The sequence of cartridge installation is important because of their dependencies. For more information about installing Foglight Hybrid Cloud Manager for Google Cloud, and for details about system requirements and version compatibility, see the *Foglight Hybrid Cloud Manager Release Notes*.

Getting Started

Generating Google Cloud Service Account File

To create and generate a Google Cloud Service Account file through the Google Cloud console:

- 1 Go to the *Google Cloud Platform console*: <https://console.cloud.google.com/>.
- 2 Go to menu **Home > IAM & Admin > Service Accounts**.








- 3 Locate the Service account and click  in the **Actions** column. Click **Create key**.

Service accounts for project "Foglight"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter table	Email	Status	Name ↑	Description	Key ID	Actions
	 foglight@appspot.gserviceaccount.com	✓	App Engine default service account		e2484343-30ba7ae379fae08c8042e10ed7cde363	 Edit Disable Create key Delete
	 billing-service@foglight-iam.gserviceaccount.com	✓	billingService		No keys	
	 billing-serviceaccount@foglight-iam.gserviceaccount.com	✓	billingServiceAccount		fa3882cedc1a7fe1489555d417bd34a7472c7989	
	 143707343931-compute@developer.gserviceaccount.com	✓	Compute Engine default service account		No keys	

- 4 Click **Create** on the popup page and save the private key in a JSON file.

Create private key for "service-account"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

☒ JSON
Recommended

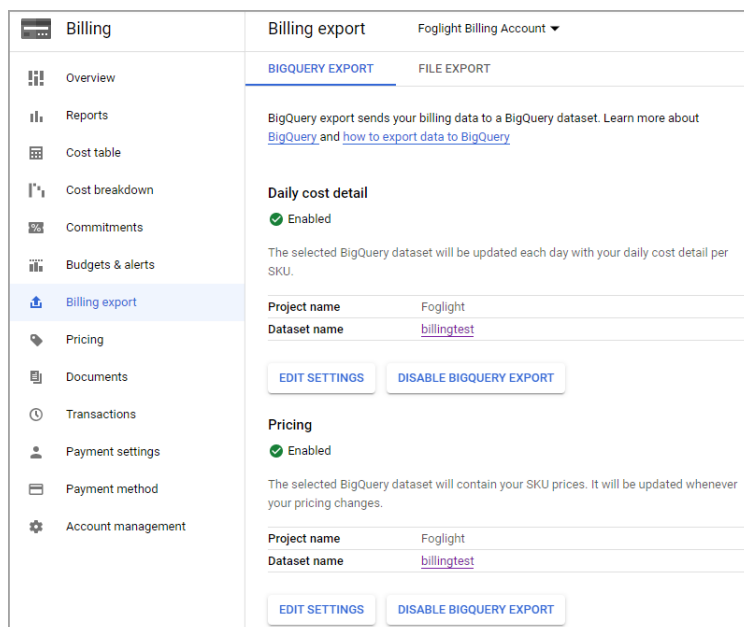
☐ P12
For backward compatibility with code using the P12 format

CANCEL CREATE

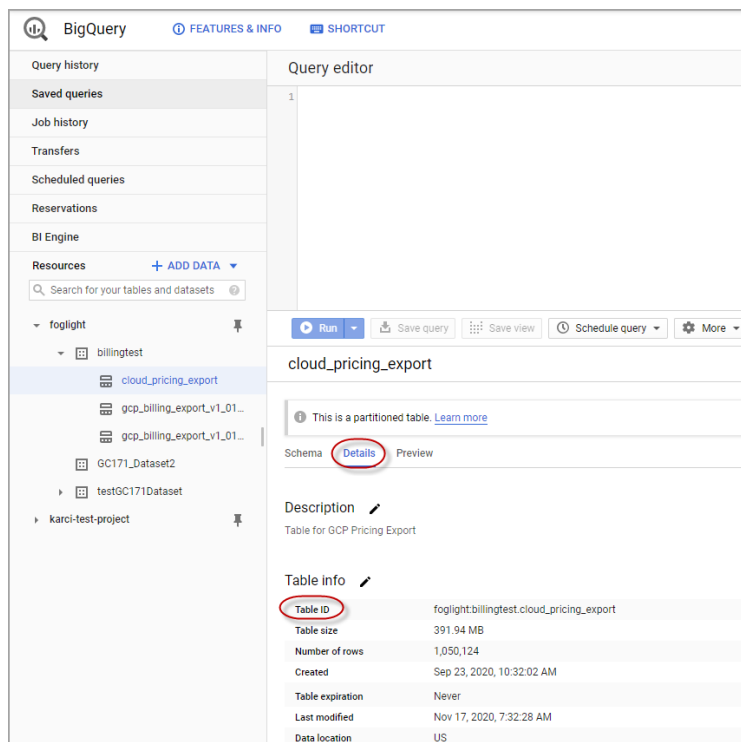
Getting the BigQuery Table ID

To get the **BigQuery Table ID** from **Google Cloud Platform console**:

- 1 Go to the **Google Cloud Platform console**: <https://console.cloud.google.com/>.
- 2 Choose **Billing** on the navigation bar, and then choose **Billing export**.



- 3 Click the target **Dataset name** and drill down to the dataset in the **BigQuery** page. Click **Details** and get the **Table ID**.



Service Account Permissions

Foglight uses service account to monitor Google Cloud. Each RESTful API provided by Google cloud requires that the service account has corresponding permissions.

- For Compute Engine monitoring:
The *viewer* roles are required.
- For Cost monitoring, the following roles are required:
 - *Billing Account Viewer*
 - *Bigquery user*
 - *Bigquery dataViewer*
- For Automatically install stackdriver, the following roles are required:
 - *compute.osAdminLogin*
 - *iam.serviceAccountUser*
 - *compute.instanceAdmin.v1*
 - *compute.osLogin*
 - *compute.securityAdmin*

i | **NOTE:** For a list of the supported operating systems of automatically install stackdriver, refer to https://cloud.google.com/monitoring/agent#supported_operating_systems.

To granting permissions to the service account, do either of the following:

- Grant permissions manually.
Manually grant roles to service account for each project and billing account.
- Grant permissions by script.
 - Use the gcloud CLI, which is a part of the Google Cloud SDK, to grant permissions automatically.
 - a Install the gcloud CLI from <https://cloud.google.com/sdk/docs/downloads-interactive> and run 'gcloud beta auth application-default login' to initialize it.
 - b Get the script at directory:
`{foglight_home}\fglam\agents\GoogleCloudAgent\{google_cloud_version}\script`
 - c Execute the grantProjectRoleToServiceAccount script to grant a specified project role or all projects role to the service account. The script includes two parameters:
 - **param 1** is mandatory. `-s` defined as String type and represents the service account.
 - **param 2** is optional. `-p` defined as String Array type and represents the projects you want to monitor. The script will grant all projects role to the service account if this param is not specified.

Refer to the below two examples for different operating systems:

- For Windows (PowerShell):

```
Example 1: .\grantProjectRoleToServiceAccount.ps1 -s  
XXXX@foglight.iam.gserviceaccount.com -p  
@('foglight','db','windows')
```

```
Example 2: .\grantProjectRoleToServiceAccount.ps1 -s  
XXXX@foglight.iam.gserviceaccount.com
```

- For Linux (Bash):

```
Example 1: bash grantProjectRoleToServiceAccount.sh -s  
XXXX@foglight.iam.gserviceaccount.com -p "foglight,db"
```

Example 2: `bash grantProjectRoleToServiceAccount.sh -s XXXX@foglight.iam.gserviceaccount.com`

- d Execute the `grantBillingAccountRoleToServiceAccount` script to grant the specified billing account role or all billing account roles to the service account. The script includes two parameters:

- **param 1** is mandatory. `-s` defined as String type and represents your service account.
- **param 2** is optional. `-b` defined as String Array type and represents the billing account you want to monitor. The script will grant all billing accounts role to the service account if this param is not specified.

Refer to the below two examples for different operating systems:

- For Windows (PowerShell):

Example 1: `.\grantBillingAccountRoleToServiceAccount.ps1 -s XXXX@foglight.iam.gserviceaccount.com -b @('015A1D-A50154-232131','015A1D-A50154-232133')`

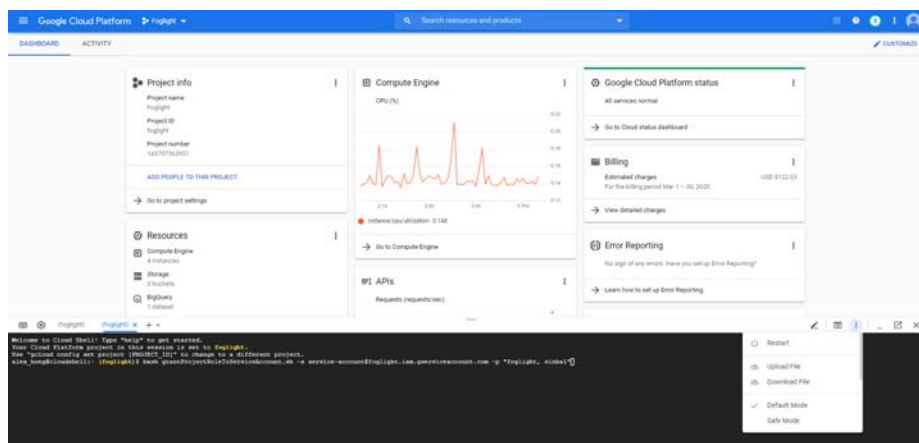
Example 2: `.\grantBillingAccountRoleToServiceAccount.ps1 -s XXXX@foglight.iam.gserviceaccount.com`

- For Linux (Bash):

Example 1: `bash grantBillingAccountRoleToServiceAccount.sh -s XXXX@foglight.iam.gserviceaccount.com -b "015A1D-A50154-232131,0196A2-C4659B-3461DA"`

Example 2: `bash grantBillingAccountRoleToServiceAccount.sh -s XXXX@foglight.iam.gserviceaccount.com`

- If you don't want to install the Google Cloud SDK, execute the Bash script at *Google Cloud Shell*:
 - a Open the Google Cloud shell through the follow link: <https://cloud.google.com/shell>
 - b Get the script at directory: `{foglight_home}\fglam\agents\GoogleCloudAgent\{google_cloud_version}\script`
 - c Upload the `grantProjectRoleToServiceAccount.sh` file to the console.



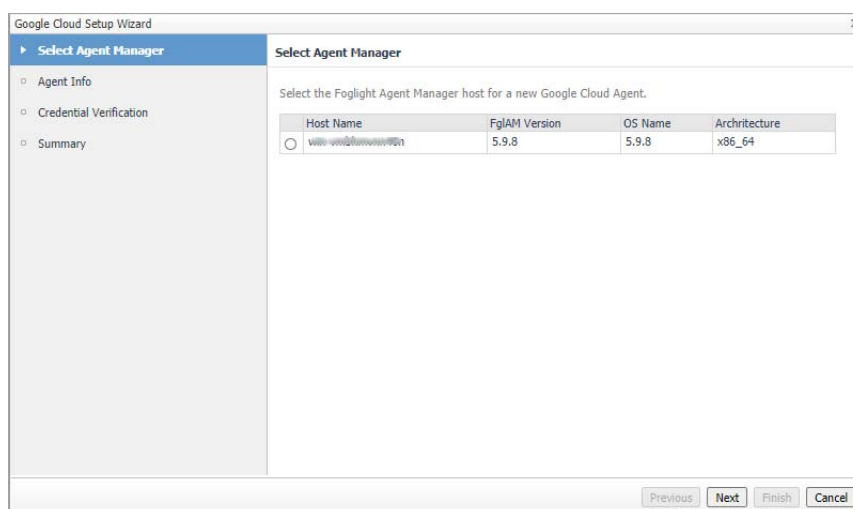
- d Execute the Bash script.

Creating a Google Cloud Agent

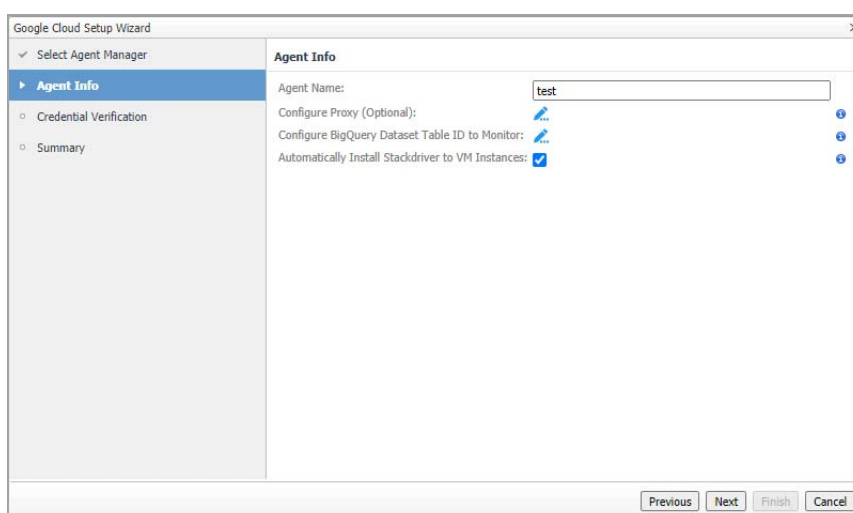
To create a Google Cloud agent:

- 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 **Cloud Manager**.
The **Cloud Manager** dashboard opens.
- 4 In the **Cloud Manager** dashboard, click **Google Cloud > Administration**, and then click **Add** or **Create Google Cloud Agent**.

A **Google Cloud Setup Wizard** dialog box opens.



- 5 In the *Select Agent Manager* view, select the agent manager on which the new agent is to be deployed, and then click **Next**.



- 6 In the *Agent Info* view, specify the following values, and then click **Next**.
 - *Agent Name*

Specify a name for the agent.

- *Configure Proxy (Optional)*

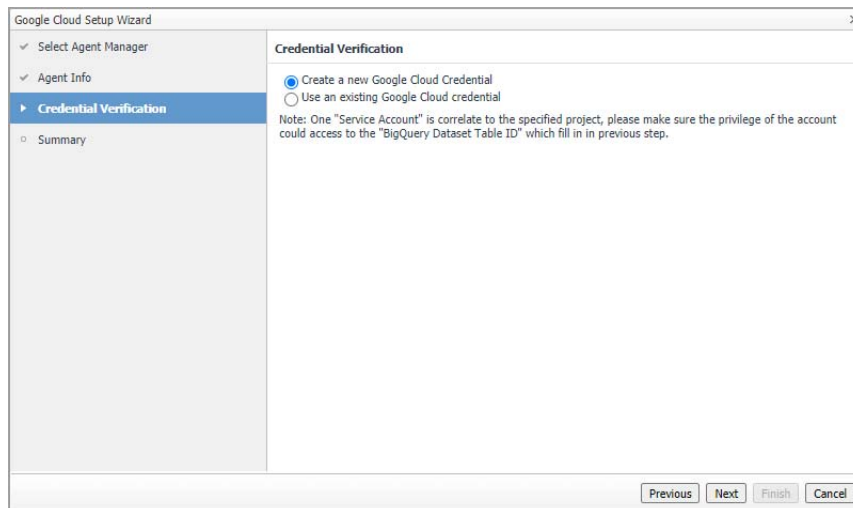
Configure the proxy setting when the Agent Host requires a proxy connection to the Internet. For more details, see [Configure Proxy \(Optional\)](#): on page 31.

- *Configure BigQuery Dataset Table ID to Monitor*

Enter the *BigQuery Table ID* according to the *Google Cloud Platform console*. To get the BigQuery Table ID from *Google Cloud Platform console*, see [Getting the BigQuery Table ID](#) on page 8 for more information.

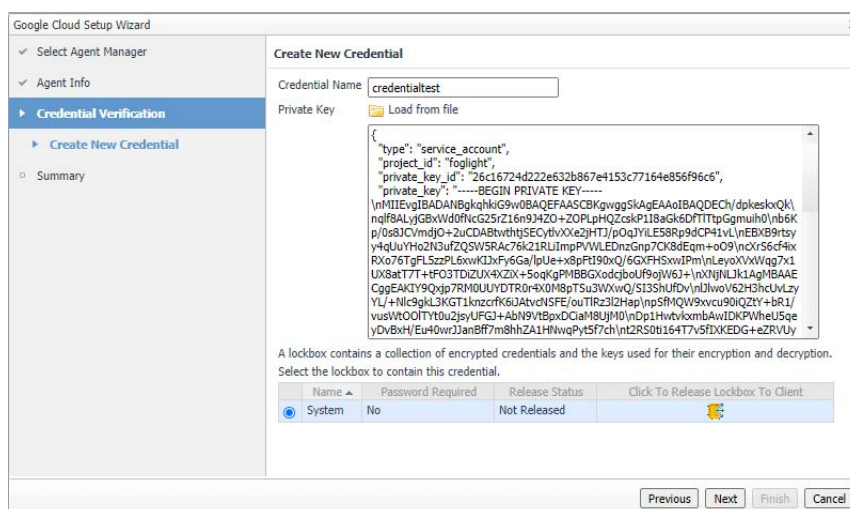
- *Automatically Install Stackdriver to VM Instances*

This option is selected by default. Install stackdriver agent to collect memory metrics.

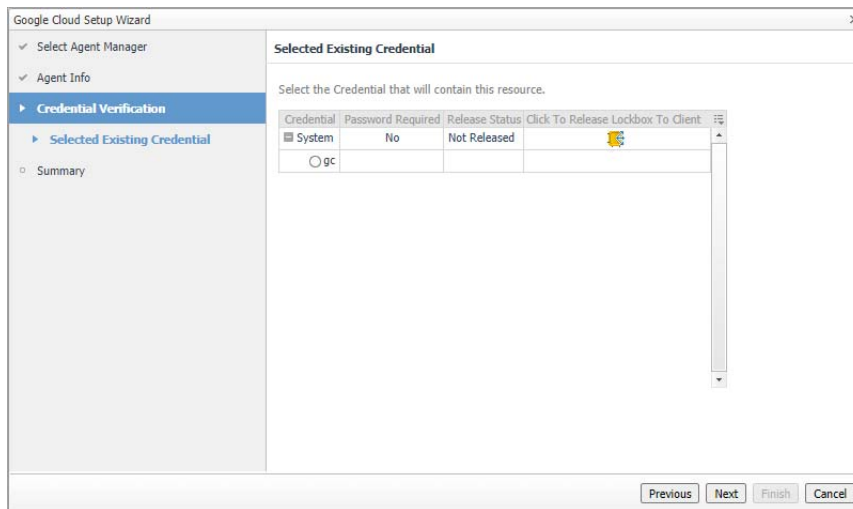


7 In the *Credential Verification* view, do either of the following:

- Choose *Create a new Google Cloud Credential* and click **Next**. A *Create New Credential* dialog box appears.
 - a Specify a *Credential Name*.
 - b Click **Load from file** to upload the JSON file generated from Google Cloud Platform console. See [Generating Google Cloud Service Account File](#) on page 7 for more information.
 - c Select the lockbox to contain the credential.



- Choose *Use an existing Google Cloud credential* and click **Next**. Select an existing credential and click **Next**.



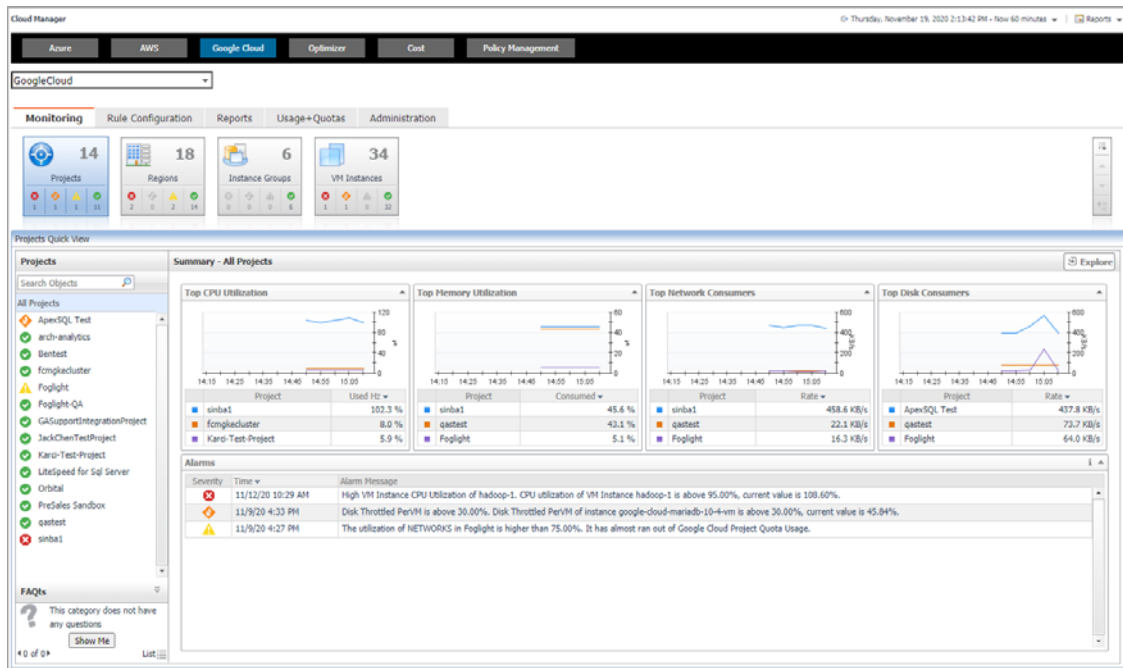
- 8 A *Summary* view appears and click **Finish**.
- 9 A popup message indicates that the new Google Cloud agent is created successfully. The agent list table refreshes to display the newly-created agent.

Dashboard location and UI elements

After installing Foglight Hybrid Cloud Manager for Google Cloud, the **Cloud Manager** entry appears under *Homes*.

To access the **Cloud Manager** 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 **Cloud Manager**, and then click **Google Cloud**.
The **Cloud Manager** dashboard opens.



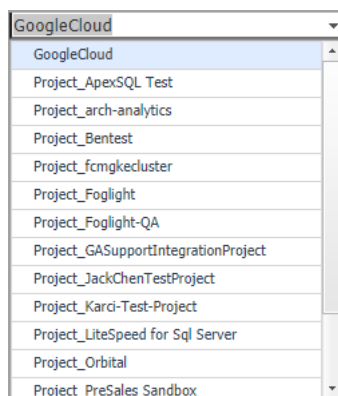
The **Cloud Manager** dashboard consists of the following UI elements:

- [Service selector](#)
- [Actions bar](#)
- [Menu bar](#)
- [Quick view](#)

Service selector

The Service selector is located at the top of the dashboard and allows you to select the Google Cloud environment you monitored.

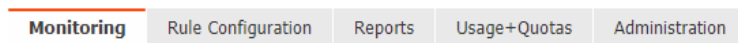
Figure 1. Service Selector



Actions bar

The actions bar at the top of the Cloud Manager dashboard contains the [Monitoring Tab](#), the [Rule Configuration Tab](#), the [Reports Tab](#), the [Usage & Quotas Tab](#), and [Administration Tab](#).

Figure 2. Actions bar



Menu bar

The Menu bar contains the following tiles: [Projects](#), [Regions](#), [Instance Groups](#), and [VM Instances](#).

Figure 3. Menu bar



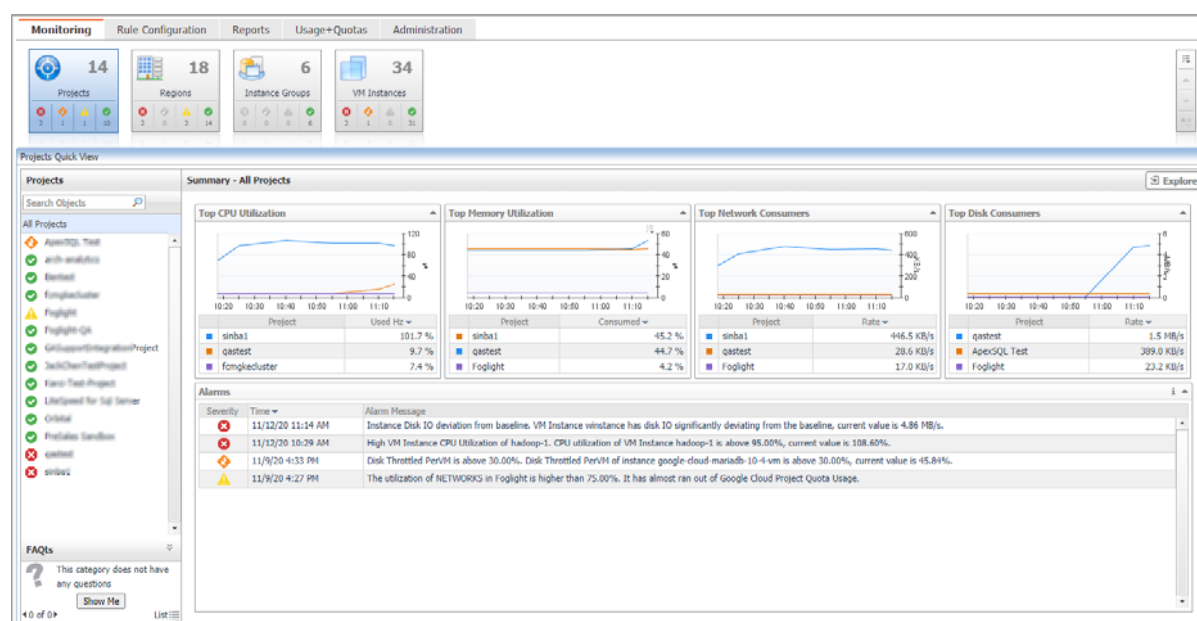
Quick view

The quick view is located on the lower part of the **Cloud Manager** dashboard, which is updated based on the tab selected on the Menu bar or the Actions bar.

Monitoring Tab

When navigating to the **Cloud Manager** dashboard for the first time, the **Monitoring** tab appears. The **Monitoring** tab allows you to select a monitoring object or a group of objects, such as projects, regions, instances groups, or VM instances, and review the data associated with your selection.

Figure 4. Monitoring dashboard



To access the Monitoring 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 **Cloud Manager**, and then click **Google Cloud**.
The **Cloud Manager** dashboard opens
- 4 On the actions bar, click **Monitoring**.
- 5 Select the **projects**, **regions**, **instances groups**, or **VM instances** tile from the top left.

For more information, see the following topics:

- [Projects](#)
- [Regions](#)
- [Instance Groups](#)
- [VM Instances](#)

Projects

The **Projects** view shows the data collected for a specific or all Google Cloud projects.

Figure 5. Projects view



The **Projects Quick View** displays the following features:

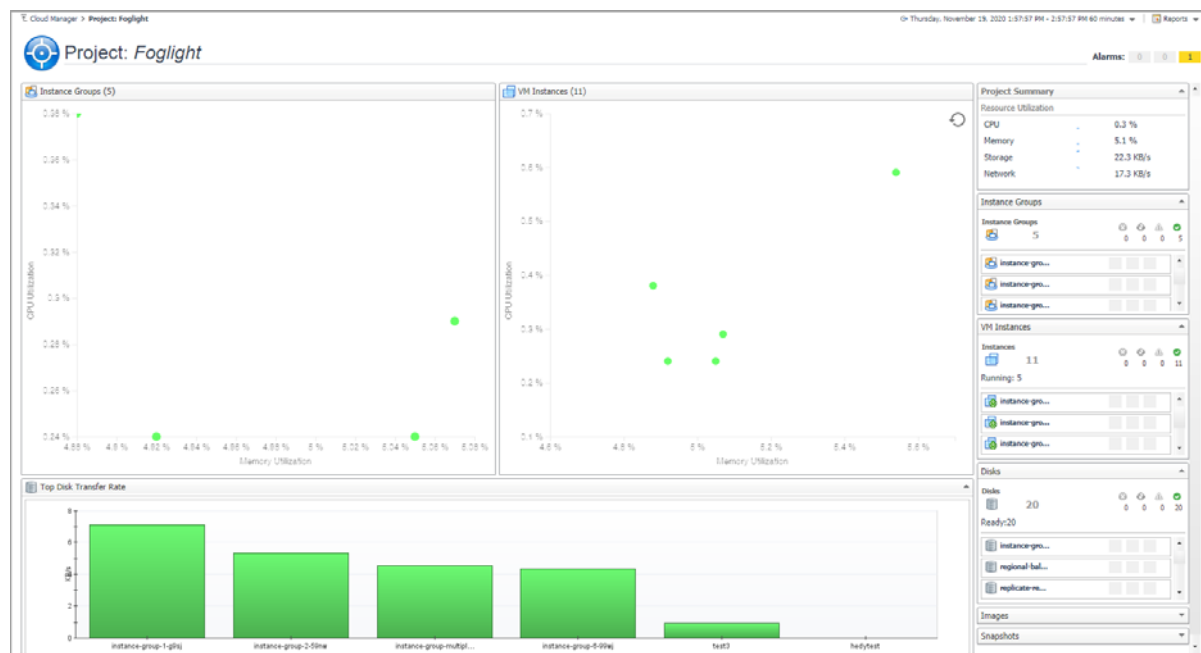
- **Projects tree view:** Shows all the projects under the selected service. Use the Projects tree view to switch between All Projects view and a single project view.
- **Summary - All Projects view:** Shows the projects with *Top CPU Utilization*, *Top Memory Utilization*, *Top Network Consumers*, and *Top Disk Consumers*.
- **A single Project view**
 - **Resource Information:** Shows the basic information for the selected project, including *Parent*, *Project Number*, *Default Network Tier*, *Default Service Account*, *XPN Project Status*, and *Life Cycle State*.
 - **Related Items:** Shows the relation and hierarchy for the selected project.
 - **Resource Utilization:** Shows the *CPU Utilization*, *Network Utilization*, *Memory Utilization*, and *Disk Utilization* for the selected project.
- **Alarms:** Shows all the alarms related to the selected project, or all the alarms related to the projects under the selected service.

Click **Explore** to open the **Project Explorer view**.

Project Explorer view

The *Project Explorer* view visually displays the detailed information of the project.

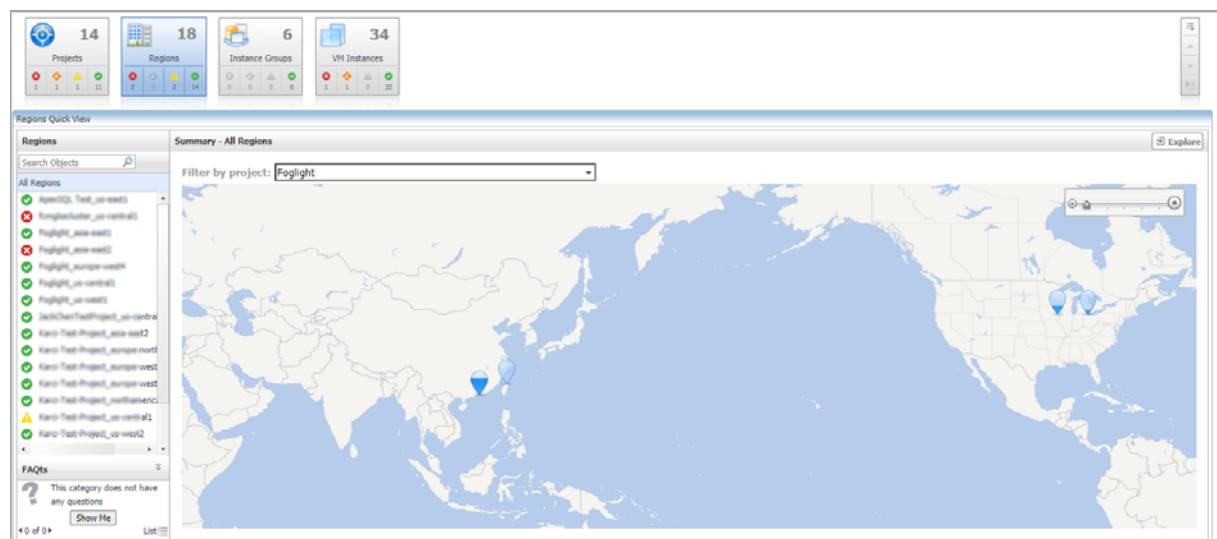
Figure 6. Projects Explorer view



Regions

The **Regions** view shows the data collected about a specific region or all Google Cloud regions.

Figure 7. Regions view



The **Regions Quick View** displays the following features:

- **Regions tree view:** Shows all the regions under the selected service. Use the Regions tree view to switch between All Regions view and a single region view.
- **Summary - All Regions view:** Choose different projects by *Filter by project* and view the region where the VM instances belongs to.

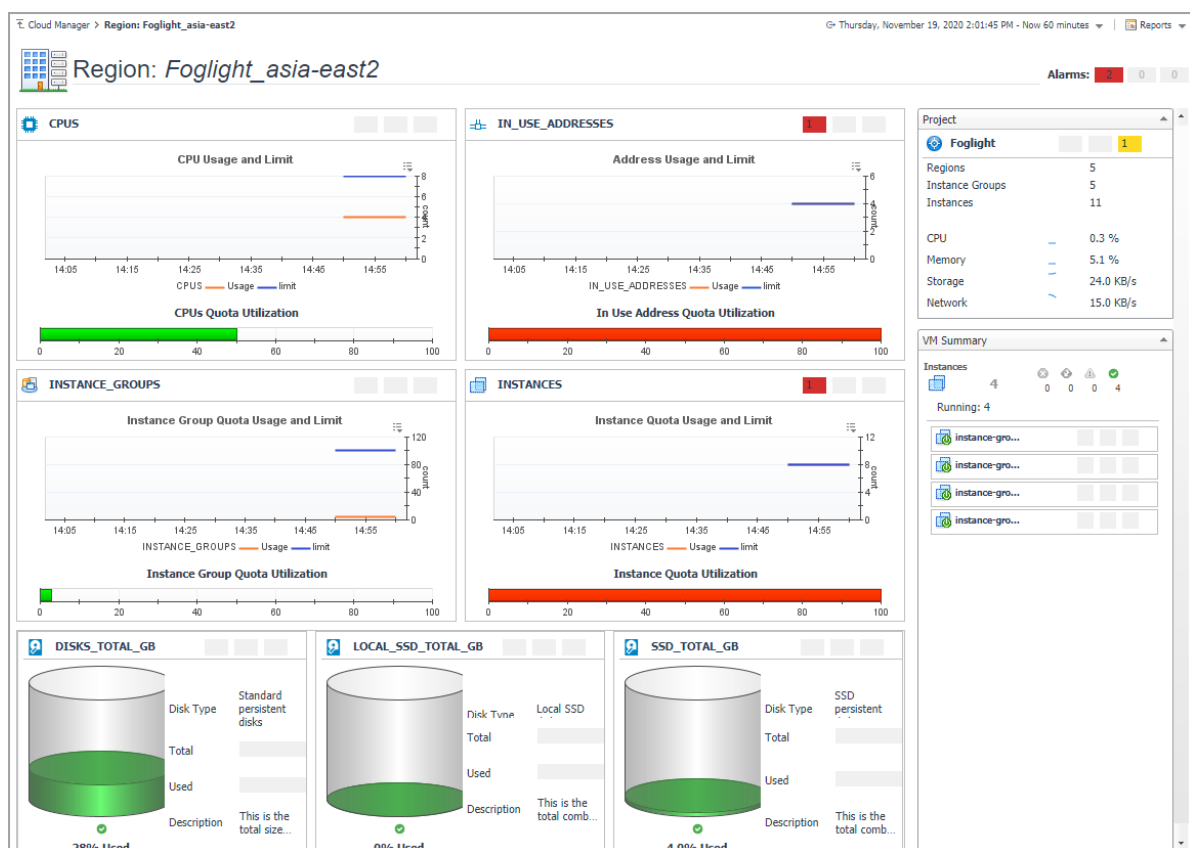
- A single **Region Details** view
 - **Related Items:** Shows the relation and hierarchy for the selected region.
 - **VM Instances** table: Shows the *Status*, *Name*, *CPU Utilization*, and *Memory Utilization* of the VM Instances for the selected region.
- **Alarms:** Shows all the alarms related to the selected region, or all the alarms related to the regions under the selected service.

Click **Explore** to open the **Region Explorer view**.

Region Explorer view

The *Region Explorer* view visually displays the detailed information of the region.

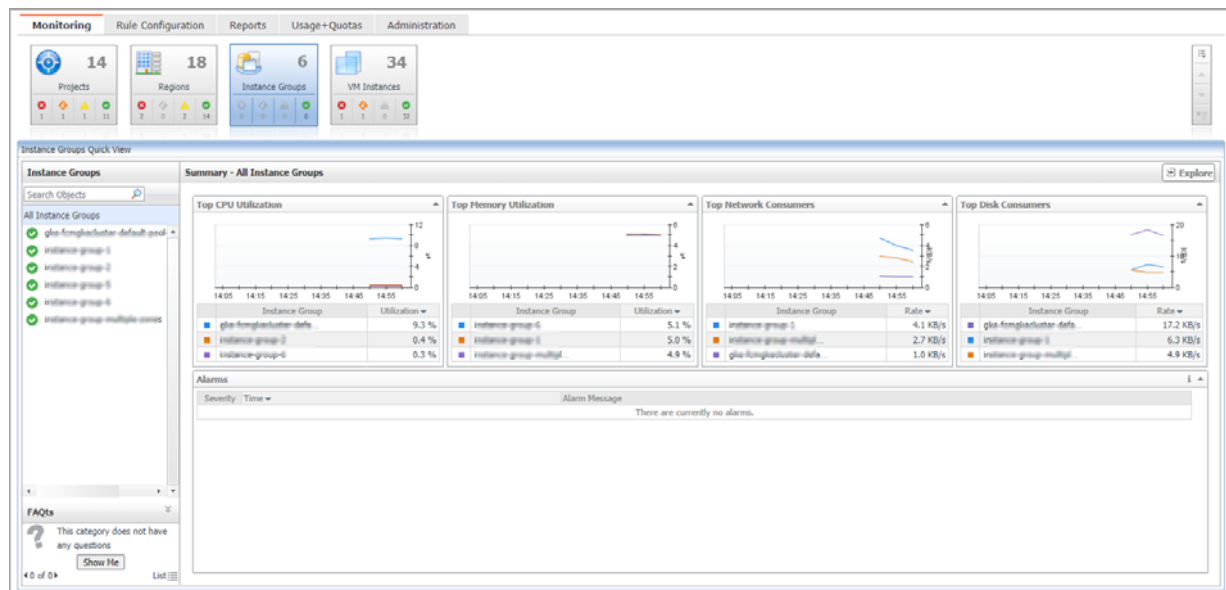
Figure 8. Region Explorer view



Instance Groups

The **Instance Groups** view shows the data collected for a specific or all Google Cloud instance groups.

Figure 9. Instance Groups view



The **Instance Groups Quick View** displays the following features:

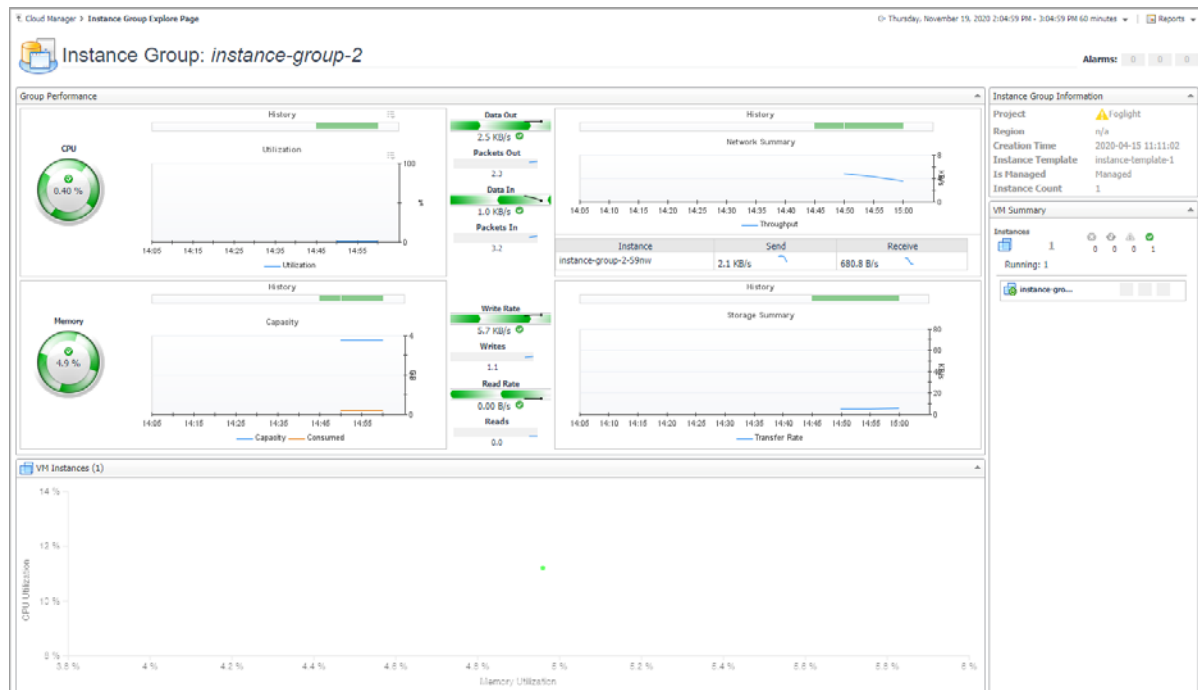
- **Instance Groups tree view:** Shows all the instance groups under the selected service. Use the Instance Groups tree view to switch between All Instance Groups view and a single Instance Group view.
- **Summary - All Instance Groups view:** Shows the instance groups with *Top CPU Utilization*, *Top Memory Utilization*, *Top Network Consumers*, and *Top Disk Consumers*.
- **A single Instance Group Summary view**
 - **Instance Group Information:** Shows the basic information for the selected instance group, including *Project name*, *Region*, *Creation time*, *Instance Template*, *Is Managed*, and *Instance Count*.
 - **Related Items:** Shows the relation and hierarchy for the selected instance group.
 - **Resource Utilization:** Shows the *CPU Utilization*, *Network I/O*, *Memory Utilization*, and *Disk I/O* for the selected instance group.
- **Alarms:** Shows all the alarms related to the selected instance group, or all the alarms related to the instance groups under the selected service.

Click **Explore** to open the [Instance Group Explorer view](#).

Instance Group Explorer view

The *Instance Group Explorer* view visually displays the detailed information of the instance group.

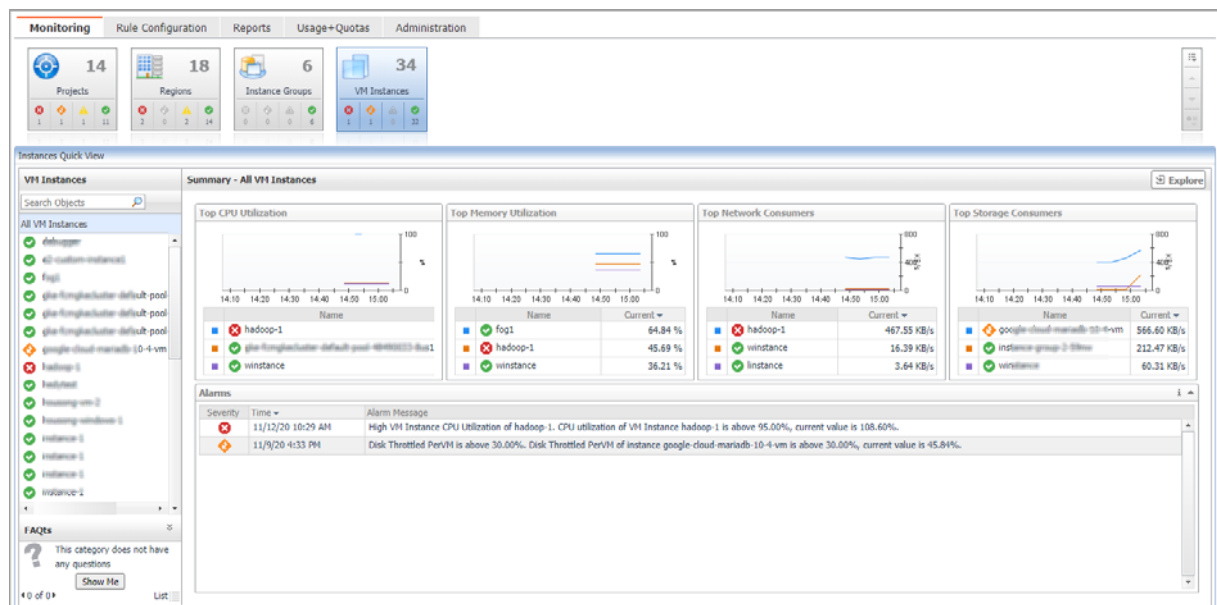
Figure 10. Instance Group Explorer view



VM Instances

The **VM Instances** view shows the data collected about a specific VM instance or all VM instances.

Figure 11. VM Instances view



The **VM Instances Quick View** displays the following features:

- **VM Instances tree view:** Shows all the VM instances under the selected service. Use the VM Instances tree view to switch between All VM Instances view and a single VM Instance view.

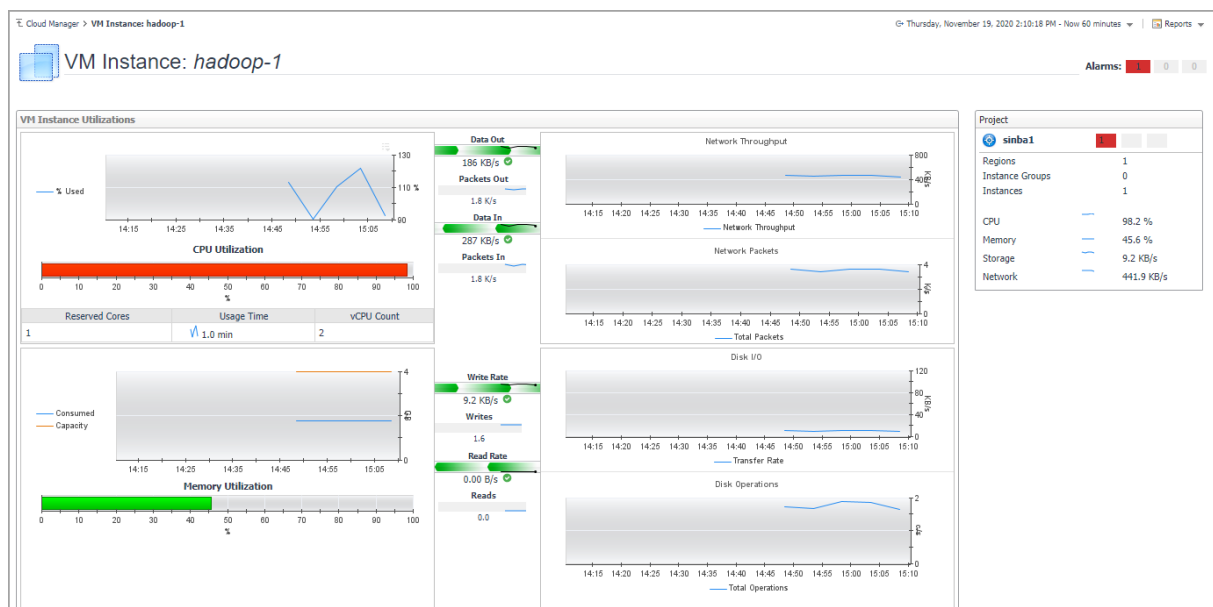
- **Summary - All VM Instances** view: Shows the VM instances with *Top CPU Utilization*, *Top Memory Utilization*, *Top Network Consumers*, and *Top Storage Consumers*.
- A single **VM Instance** view
 - **Resource Information:** Shows the basic information for the selected VM instance, including *Instance Group*, *CPU Platform*, *Status*, *Machine Type*, *Zone*, *Virtual Network*, *Internal IP*, and *External IP*.
 - **Related Items:** Shows the relation and hierarchy for the selected VM instance.
 - **Resource Utilization:** Shows the *CPU Utilization*, *Network I/O*, *Memory Utilization*, and *Disk I/O* for the selected VM instance.
- **Alarms:** Shows all the alarms related to the selected VM Instance, or all the alarms related to the VM Instances under the selected service.

Click **Explore** to open the **VM Instance Explorer** view.

VM Instance Explorer view

The *VM Instance Explorer* view visually displays the detailed information of the VM instance.

Figure 12. VM Instance Explorer view



Rule Configuration Tab

The **Rule Configuration** tab of the **Cloud Manager** dashboard contains links to rules and alarms tasks that you can use to manage Google Cloud rules and alarms.

Figure 13. Rule Configuration dashboard

Enabled	Rule	Fatal	Critical	Warning	Alarms	Applies To	Description
<input type="checkbox"/>	Google Cloud Agent Messages						This rule converts agent messages to Foglight alerts.
<input type="checkbox"/>	Google Cloud Billing Account Budget Over Spending						To monitor whether the cost trend has reached to the configured monthly budget.
<input type="checkbox"/>	Google Cloud Disk Throttled Bytes PerGB	50.0	30.0	10.0			Google Cloud Disk Throttled PerGB Checks
<input type="checkbox"/>	Google Cloud Disk Throttled Bytes PerVM	50.0	30.0	10.0			Google Cloud Disk Throttled PerVM Checks
<input type="checkbox"/>	Google Cloud Quota Utilization	95.0	85.0	75.0			Google Cloud Quota Usage Utilization Check
<input type="checkbox"/>	Google Cloud VM Instance CPU Utilization	95.0	85.0	75.0			Google Cloud VM Instance CPU Utilization Check
<input type="checkbox"/>	Google Cloud VM Instance Disk Transfer Rate						Google Cloud VM Instance Storage Transfer Rate Check
<input type="checkbox"/>	Google Cloud VM Instance Memory Utilization	95.0	85.0	75.0			Google Cloud VM Instance Memory Utilization Check
<input type="checkbox"/>	Google Cloud VM Instance Network Transfer Rate						Google Cloud VM Instance Network Transfer Rate Check

To access the Rule Configuration 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 **Cloud Manager**.
The **Cloud Manager** dashboard opens.
- 4 Click **Rule Configuration** in the actions bar.



For more information, see the following topics:

- [Rules view](#)
- [Enabling/Disabling rule\(s\)](#)
- [Adding a custom rule](#)
- [Removing custom rule\(s\)](#)

Rules view

By default, the following columns are displayed in the *Rules* view:


- **Enabled:** Indicates if the rule is enabled or disabled . You can sort the list of rules by state, by clicking the Enabled column.
- **Rule:** Contains the rule name. Click the rule name to start the workflow for viewing and editing rule details.
- Fatal , Critical , and Warning thresholds (multiple-severity rules only):

- For expressions that include one registry variable, these columns contain the current value of that variable. Click the value to edit it.
- For expressions that include multiple registry variables, the column contains an icon . Clicking that icon shows the list of referenced registry variables and their values. Click a value to edit it.
- For expressions that do not include any registry variables, this column contains an icon . Clicking that icon navigates to the **Edit Rule** dashboard.
- For rule states that do not have a conditional expression defined, this column is empty.
- **Alarms:** Contains the number of alarms (multiple-severity rules only) generated by the rule. Clicking that column shows a list of alarms indicating for each alarm its severity, when the alarm was generated, and the alarm message.
- **Applies to:** Shows the object name that is applied to this custom rule.
- **Description:** Contains the rule description.


Enabling/Disabling rule(s)

The *Rule Configuration* dashboard shows a list of existing rules and a set of rule management commands at the top of the list. Use the **Enable Rule** and **Disable Rule** buttons to activate or deactivate one or multiple rules at once.

To enable a rule:

- 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 **Cloud Manager**.
The **Cloud Manager** dashboard opens.
- 4 Click **Rule Configuration**.
The **Rule Configuration** dashboard opens.
- 5 On the *Rules* list, select one or more check boxes in the left-most column, and then click **Enable Rule**.
The *Enable Rules* dialog box opens.
- 6 In the *Enable Rules* dialog box, click **Yes**.
The *Rules* list refreshes with the rules' status updated automatically.

To disable a rule:

- 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 **Cloud Manager**.
The **Cloud Manager** dashboard opens.
- 4 Click **Rule Configuration**.
The **Rule Configuration** dashboard opens.
- 5 On the *Rules* list, select one or more check boxes in the left-most column, and then click **Disable Rule**.
The *Disable Rules* dialog box opens.

- 6 In the *Disable Rules* dialog box, click **Yes**.


The *Rules* list refreshes with the rules' status updated automatically.

Adding a custom rule

The *Rule Configuration* dashboard shows a list of existing rules and a set of rule management commands at the top of the list. Use the **Add Custom Rule** button to create a new rule as needed.

To customize a rule:

- 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 **Cloud Manager**.

The **Cloud Manager** dashboard opens.
- 4 Click **Rule Configuration**.

The **Rule Configuration** dashboard opens.
- 5 Click **Add Custom Rule** on the *Rules* table.

The *Create Custom Rule* dialog box opens.
- 6 In the *Create Custom Rule* dialog box, specify the following:
 - a Alarm Type:
 - a Type the name of custom rule in the *Name* field.
 - b Select an *Object Type*, and then select a metric from the *Metric* drop-down list. The value of *Metric* varies from the *Object Type*.
 - c Select either *Threshold* or *% Change*, and then specify the following values as needed.
 - *Threshold*: Specify *Condition*, *Time Period*, *Severity*, and then specify whether or not fire actions if the specified data attempts are reached. The value of *Condition* cannot be negative.
 - *% Change*: Specify *Condition*, *Time Period*, and *Severity Label*. The value of *Condition* cannot be negative.
 - b (Optional) Scope: Choose the objects to which you want to apply this rule. If no objects are selected in this step, the custom rule will apply to all objects which type is the *Object Type* specified in [Step 6](#).
 - c (Optional) Notifications: Click **Add New**, then the *Edit Notification Config - Dialog* box appears. In this dialog box, type the *E-mail Address* and *Description* as needed, and then click **Add**.
- 7 Click **Save**.

The *Rules* table refreshes automatically to show the newly added rule.


Removing custom rule(s)

The *Rule Configuration* dashboard shows a list of existing rules and a set of rule management commands at the top of the list. Use the **Remove Custom Rule** button to delete existing custom rule(s) as needed.

To remove a custom rule:

- 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 **Cloud Manager**.

The **Cloud Manager** dashboard opens.

- 4 Click **Rule Configuration**.

The **Rule Configuration** dashboard opens.

- 5 Click **Remove Custom Rule** on the *Rules* table.

The *Remove* dialog box opens.

- 6 Click **Yes**.

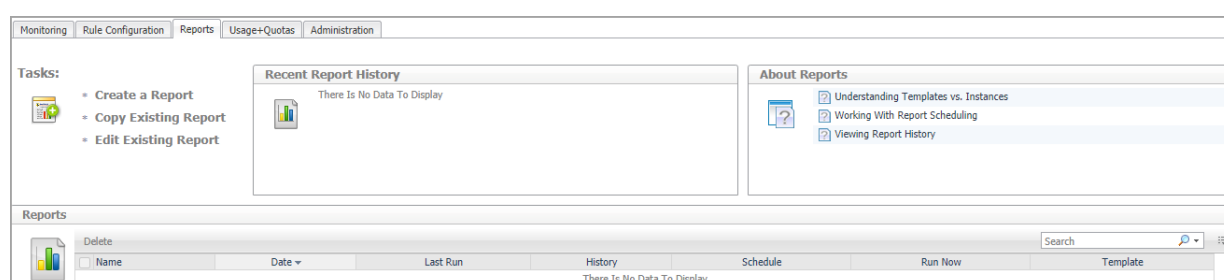
The *Rules* table refreshes automatically and removes the selected rule.

Reports Tab

Foglight Hybrid Cloud Manager for Google Cloud includes a report generation ability. This allows you to create reports using a set of predefined templates to report on the various aspects of your cloud environment. Foglight Hybrid Cloud Manager for Google Cloud includes a collection of predefined report templates.

You can generate, copy, and edit reports using the **Reports** tab on the *Reports* dashboard, or alternatively the *Reports* dashboard included with the Management Server.

Figure 14. Report dashboard



To access the Reports 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 **Cloud Manager**.
The **Cloud Manager** dashboard opens.
- 4 Click **Reports** in the actions bar.

For complete information about this tab, see the *Managing Capacity in Virtual Environments User Guide*. For more information about the *Reports* dashboard, see the *Foglight User Help*.

Available report templates

The following templates are available with Foglight Hybrid Cloud Manager for Google Cloud Cloud.

Table 1. Report templates

Report Template Name	This template can be used to generate a report that...
Cost-All Google Billing Accounts Summary Report	Summarizes the cost for all the Google Cloud Billing Accounts in the monitored environment.
Google Cloud Region Summary Report	Summarizes all regions at under your account, so that you could know all regions' performance.
Instance Group Performance by Service - Detail	Summarizes the detailed instance group performance by service.

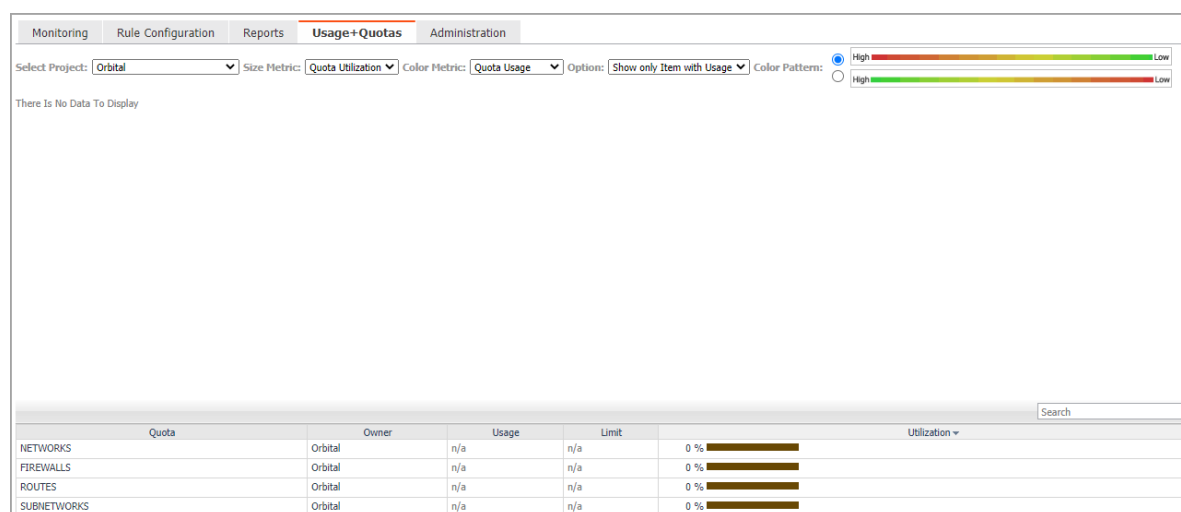
Table 1. Report templates

Report Template Name	This template can be used to generate a report that...
Instance Performance by Service - Detail	Summarizes the instance performance by service.
Project Performance by Service - Detail	Summarizes the project performance by service.
Project Summary Report	Summarizes the projects in the monitored environment.
VM Instance Performance Report	Summarizes the VM instance performance.


Usage & Quotas Tab

Foglight Hybrid Cloud Manager for Google Cloud allows you to view the subscription details by four filters, including *Quota*, *Owner*, *Usage*, *Limit*, and *Utilization*.

Figure 15. Usage & Quotas dashboard



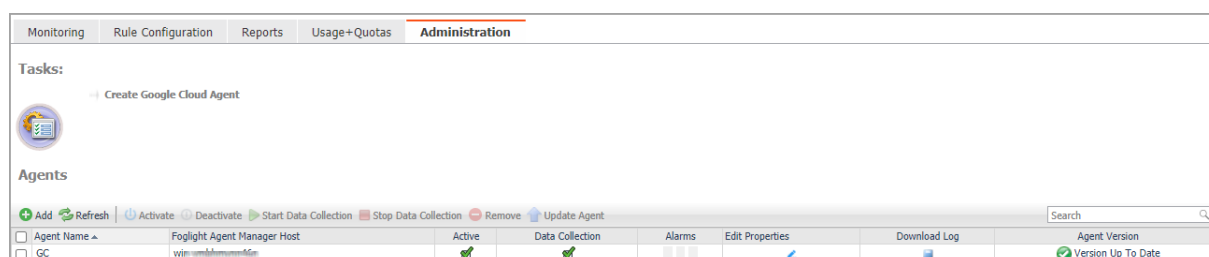
To access the Usage & Quotas dashboard:

- 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 **Cloud Manager**.
The **Cloud Manager** dashboard opens.
- 4 Click **Usage+Quotas** in the actions bar.

Administration Tab

The **Administration** tab of the **Cloud Manager** dashboard contains links to agent administration tasks that you can use to manage Google Cloud performance agents.

Figure 16. Administration dashboard



To access the Administration 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 **Cloud Manager**.
The **Cloud Manager** dashboard opens.
- 4 Click **Administration** in the actions bar.

For more information, see the following topics:

- [Agents related commands](#)
- [Agents related commands](#)
- [Creating a Google Cloud Agent](#)
- [Editing agent properties](#)

Agents related commands

The **Administration** dashboard 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 a Google Cloud Agent](#) on page 11.
- **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 Google Cloud platform 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 Google Cloud platform.
- **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 31.
- **Remove:** Deletes the selected agent instance.
- **Update Agent:** Updates the agent package to the latest version.

i 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**.

Editing agent properties

Google Cloud Agents collect data from Google Cloud platform and send it to the Management Server. The agents keep tracking of resource utilization metrics and alerts you when certain pre-defined thresholds are reached.

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

To edit the Google Cloud Performance 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 **Cloud Manager**.
Cloud Manager dashboard opens.
- 4 Click **Administration**.
The **Administration** dashboard opens.
- 5 Select the instance of the Google Cloud Agent properties that you want to modify, and then click **Edit Properties**.
- 6 In the **Edit Properties** dialog box, edit the following properties, as needed.
 - *Configure BigQuery Dataset Table ID to Monitor*
Enter the *BigQuery Table ID* according to the *Google Cloud Platform console*. To get the BigQuery Table ID from *Google Cloud Platform console*, see [Getting the BigQuery Table ID](#) on page 8 for more information.
 - *Configure Proxy (Optional):*
Configure the proxy setting when the Agent Host requires a proxy connection to the Internet.

- a Select the *Enable Proxy* check box to enable the proxy settings.
- b Input the host name or IP address for the *Proxy Server* and input the Proxy Port number.
- c If the proxy requires an authorization, select the *Authorization* check box, and input the Username and Password.

NOTE: In FIPS-compliant mode, if proxy settings are configured, you need to import the proxy server application root certificate into FMS KeyStore and FglAM. For more information, see [Managing certificates](#).

- d Select *Authorization*. Input Username and Password.
- *Automatically Install Stackdriver to VM Instances:* Select this option to install stackdriver agent to collect memory metrics.
 - *Click to Release Lockbox to Client:* Click the button to release the lockbox to client.
 - *Click to Edit Credential:* Click the button to update the JSON file for the service account.
 - *Add Google Cloud Agent to a new credential:* Create a new credential for the Google Cloud agent.
 - *Add Google Cloud Agent to an existing credential:* Assign the Google Cloud agent to an existing credential.
- 7 Click **Save**. The **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-----
XXXXXXXXXX=
-----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
```

Managing certificates for FMS in FIPS-compliant mode

Use the keytool utility shipped with Foglight to create, import, or export certificates. This utility can be found at: `<foglight_home>\jre\bin\keytool`.

The KeyStore Foglight used in FIPS-compliant mode is located at: `<foglight_home>/config/security/trust.fips.keystore` (default password: nitrogen)

Add a certificate in FIPS-compliant mode

Use the keytool command in FMS JRE located in `<foglight>/jre/bin`.

```
keytool -import -trustcacerts -alias "<alias>" -file "<certificate path>" -keystore
"<Foglight_home>/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen
```

- Validate the certificate and ensure the following:
 - It is not expired.
 - It is an X.509 format.

- Change the following before executing the command
 - <alias>: The alias is required and is used in the list and delete operations to refer to the certificate. It can be anything.
 - <Foglight_home>: The folder path where Foglight is installed.
 - <certificate path>: Your custom certificate path.

List installed certificates

```
keytool -list -keystore "<Foglight_home>/config/security/trust.fips.keystore" -
deststoretype BCFKS -provider
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen
```

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

Refer to the example output below:

```
Keystore type: BCFKS
Keystore provider: BCFIPS
Your keystore contains 151 entries
camerfirmachambersignca [jdk], Dec 18, 2019, trustedCertEntry,
Certificate fingerprint (SHA1):
4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C
entrust2048ca [jdk], Dec 18, 2019, trustedCertEntry
...
```

Delete a certificate

Remove a certificate referred to by an alias.

```
keytool -delete -alias <alias> -keystore
"<Foglight_home>/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen
```

A full example for managing certificate for FMS in FIPS-compliant mode

Add example certificate into FMS certificate store in FIPS-compliant mode

```
C:\Quest\Foglight\jre\bin>keytool -import -trustcacerts -alias "Evolve-Test" -file
"D:/Evolve-test.crt" -keystore
"C:/Quest/Foglight/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"C:/Quest/Foglight/server/core/bc-fips.jar" -storepass nitrogen

Owner: CN=CA, DC=ca, DC=local
Issuer: CN=CA, DC=ca, DC=local
Serial number: xxxx
Valid from: Sun Jan 06 23:07:06 CST 2019 until: Wed Apr 06 23:07:06 CST 2022
Certificate fingerprints:
...
```

Extensions:

...

Trust this certificate? [no]: yes

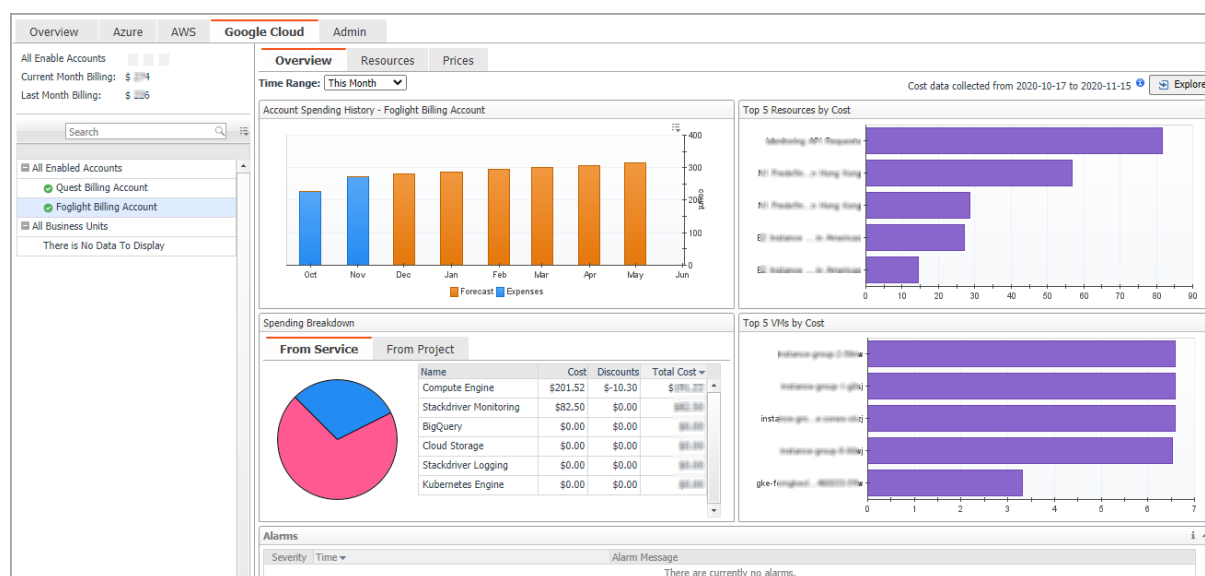
Certificate was added to keystore

Cost Tab

Click **Cost** on the top of the **Cloud Manager** dashboard to navigate to the **Cost** tab.

NOTE: Ensure that you have configured the cost metrics for account through the **Agent Properties** dialog box; otherwise there will be no data displayed on this tab. For more information about how to configure cost metrics, refer to the [Configure BigQuery Dataset Table ID to Monitor](#) on page 12.

Figure 17. Cost tab



To access the Cost tab:

- 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 **Cloud Manager**.
The **Cloud Manager** dashboard opens.
- 4 Click **Cost**. The **Cost** tab opens on the bottom of **Cloud Manager** dashboard.
- 5 Click **Google Cloud**.

Cost - Overview

The *Cost-Overview* includes the following elements:

- **Cost Summary:** Displays the Total Month-to-date cost, and cost by Azure, AWS, and Google Cloud platforms.

- **Cost Overview:** A stacked bar chart to display the Month-to-date Expenses and Forecast by Azure, AWS, Google Cloud platforms.

NOTE: The Month-to-date (MTD) indicates a period starting from the beginning of the current month till the end of the current date.

- **Infrastructure:** Displays an Infrastructure resource table across clouds.
 - Accounts Configured: The number of Azure subscriptions, AWS Accounts, or Google Cloud Billing Accounts.
 - Total VMs: The total number of VMs running in the Cloud platform.
- **Top 5 Business Units by Cost:** Aggregates the total cost for Business Units after users assign the AWS accounts, Azure Subscriptions, or Google Cloud Billing Accounts to a BU under **Cost > Admin**.
- **Cost Breakdown by Platforms:** Displays the Month-to-date cost by Azure, AWS, and Google Cloud platforms.

Cost - Google Cloud view

The *Cost - Google Cloud* view includes the following elements:

- Overview of all enabled Billing Accounts cost: Lists the enabled billing accounts, billing of the current month, and billing of the last month.
- Object tree view: Lists the enabled Billing Accounts and business units.
- Time Range Selector: Lists the time range for billing. The time bar of the Management Server does not take effects on the *Cost* dashboard.
- All Enabled Billing Accounts Spending History/Top 5 Billing Accounts by cost/Spending Breakdown: These three views will display the relevant cost information if you select *All Enabled Billing Accounts* or *All Business Units* from the object tree view.
- Billing Account Spending History/Top 5 Resources by Cost/Cost Breakdown By Service Type/Top 5 VMs by Cost: These four views will display the cost information of the selected billing account or business unit.
- Alarms: Lists all alarms against the selected billing account or business unit.
- Select Billing Account displays the Billing Account Overview, Resource cost, and SKU Prices.

Cost - Admin view

The *Cost - Admin* view includes the following:

- Google Cloud Accounts tab: Displays the overview of all billing accounts, including the billing account name, business unit, spending, monthly budget, last month billing, current month billing, and next month projection.
 - Set Monthly Budget: Updates monthly budget for the selected billing account.
 - Assign Business Unit: Assigns the select billing accounts to a Business Unit.
 - Remove from Business Units: Exits the selected business units.
- Business Units tab: Lists business units name, location, organization, and accounts.
 - Add Business Units: Creates a business unit, specifies Business Unit name, description, location, longitude, latitude, and assigns to a new organization or existing organization.
 - Delete Business Units: Deletes selected business units.
 - Assign Organization: Select the organization from the list for selected business units.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit <https://www.quest.com/>.

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.