Rackspace Managed Services for Google Cloud Platform Product Guide

Release 2019-07-12-14:41

July 12, 2019

CONTENTS

IMPORTANT: This is a PDF version of the Product Guide, and is intended to be used for point-in-time offline reference purposes only. The authoritative version of this document lives online at https://manage.rackspace.com/gcp/docs and will contain the latest updates.

This Product Guide is designed to provide a detailed look at how Rackspace delivers our **Managed Services for Google Cloud Platform** offering.

For general information on the offering, please visit https://www.rackspace.com/gcp.

To sign up, visit https://cart.rackspace.com/gcp.

CHAPTER

ONE

GETTING STARTED

It is easy to get started experiencing Rackspace Managed Services for Google Cloud Platform.

1.1 Create your Rackspace account

The first step is to create your Rackspace account. Visit https://cart.rackspace.com/gcp and follow the instructions to establish your account.

1.2 Log in with Google

After you have created your Rackspace account, navigate to the Managed Services for Google Cloud Platform Control Panel. Once you've logged in, click the "Log in with Google" button to establish a link between your Rackspace account and Google.

After linking your accounts, you'll be prompted to select the Google organization that you want Rackspace to manage. Note that a Google organization can only be associated with a single Rackspace account, and all projects you wish for us to manage must belong to that organization. You must have the Organization Admin role in your Google organization to complete this process, which ensures that only an authorized user completes this one-time linking. If you require management of projects in more than one Google organization, consider creating a second Rackspace account or migrating the projects to a single Google organization.

If you do not already have a Google organization, create one by following Google's instructions for Creating and Managing Organizations. If you need assistance with this process, please contact your *support team*.

Once you've selected your Google organization, you can then select the GCP project(s) that you would like us to manage. Initially, all projects will be set to the Runway *service level*. You can contact your Technical Account Manager if you want to establish an Aviator service level GCP project.

CHAPTER

TWO

GCP PROJECTS

Each Rackspace account can house one or more GCP projects from the same Google organization. We generally recommend provisioning a GCP project per application deployment phase (e.g. development, staging, and production), thereby allowing you to assign different users in your company access to the appropriate GCP projects without complex IAM policies. In this example, developers could be granted access to provision Compute Engine instances, Cloud SQL databases, etc. in your development and staging projects, but be restricted to read access of the resources in your production project.

In addition to being a strong permission boundary, GCP projects also provide a convenient construct for tracking expenses, since by default, both GCP and Rackspace charges are grouped by GCP project. For example, if 4 separate GCP projects are used called app1-dev, app1-prod, app2-dev, app2-prod, it is very easy to see how much is being spent on each application environment.

Lastly, using separate GCP projects per environment gives you the flexibility to select different Rackspace service levels for each environment, since Rackspace service levels are applied at the GCP project level. For example, you may opt for the Runway service level on your development project while using the Aviator service level for your production project.

2.1 Offboarding

While we hope to serve you for life, should you ever decide that you no longer require Rackspace's management of your GCP project we can work with you to transition your account to a direct relationship with GCP. You would retain access to all GCP resources, but would lose access to Rackspace tooling as well as Rackspace's GCP expertise and service. If you are considering making this change, please *contact your Technical Account Manager* for further assistance.

CHAPTER

THREE

SERVICE LEVELS

Rackspace Managed Services for Google Cloud Platform combines tooling and automation with human experts to deliver a world-class experience. We offer two service levels, Runway and Aviator, which are selected for each GCP project we support.

- Runway: "I want access to Rackspace tooling, the ability to request on-demand support for a fee, and will manage my GCP project myself."
- Aviator: "I want Rackspace to operate and manage my GCP project for me or with me."

For details on what is included in each service level, including details on levels of support for each GCP service, download our `Rackspace Managed Services for Google Cloud Platform Service Overview`.

3.1 Aviator Response Time SLAs

Rackspace will respond to your Aviator support requests submitted to us via ticket in the following timeframes. For Aviator projects, all requests should be made directly to Rackspace and we will escalate to Google directly, if needed.

- Emergency: If Rackspace Infrastructure monitoring and alerting services determines your GCP Services are inaccessible from the public internet, which may result in the inability to complete business transactions, our initial response to emergency monitoring alarms will occur within fifteen minutes.
- Urgent: If your GCP Services are functioning improperly or at less than optimal performance and the failure is impacting business transactions, our initial response is 60 minutes.

If at any time you need to escalate a Support request on your account, please *contact us*.

3.2 Runway Response Time SLAs

Rackspace will respond to your Runway support requests submitted via a ticket within 4 hours of submission.

- Runway project tickets related to billing or account issues are included in the Runway service offering.
- Runway project tickets related to Google Cloud Platform infrastructure or other categories of issues are considered on-demand support and require payment of a service fee for Rackspace to address.

CHAPTER

FOUR

SERVICE BLOCKS

Rackspace knows that our customers have varying needs at different stages of their cloud journey. That's why we provide a set of support offers that solve for your needs at any stage of your cloud lifecycle. Our services include architecture help, access to experts to solve your problems, security assistance, 24x7x365 management, cost governance, and other value-added services - all backed by GCP certified engineers and architects.

Our offers allow you to customize your experience with the ability to choose the service options to match your needs. These offers are described below.

4.1 Platform Essentials

Platform Essentials is a prerequisite for all other GCP service blocks. Platform Essentials includes:

- GCP Support powered by Google Certified Rackers and backed by GCP Enterprise Support
- Unified billing for all your Rackspace platforms and other Managed Public Cloud Accounts
- Access to the Fanatical Support for GCP Control Panel to manage your GCP projects, your users, and their permissions

Platform Essentials customers receive 24x7x365 guidance and support on their GCP project. Rackspace will respond to support requests submitted via tickets in the following timeframes:

- Urgent: Production System Outage / Significant Business Impact [60 Minute Response Time]
- High: Production System Impaired / Moderate Business Impact [4 Hour Response Time]
- Normal: Issues and Requests / Minimal Business Impact [12 Hour Response Time]
- Low: General Information, Questions, and Guidance [24 Hour Response Time]

All requests should be made directly to Rackspace and we will escalate to GCP, if needed.

4.2 Architect & Deploy

With the Rackspace Architect & Deploy service block, our experts apply best practices to design and deploy public cloud infrastructure that meets your business needs while minimizing costs, maximizing availability, security and performance, and enabling you to outsource ongoing management activities to Rackspace. The Architect & Deploy offer includes:

- A Technical Onboarding Manager to coordinate end-to-end activities and project manage your GCP deployment
- A Solutions Architect to understand your requirements and create a high-level proposal document for your approval

- A Build Engineer who will build and deploy the environment as per the design document
- Design Document: A document describing the detailed solution design. This document will be shared, and your approval of the design is required prior to deploying the solution
- GCP Environment: The deployed solution running in GCP

4.3 Manage & Operate

With tooling, automation, monitoring and 24x7x365 access to certified cloud specialists for day-to-day operational support and management, Manage & Operate allows you and your team to rest easy knowing Rackspace has your back. Manage & Operate includes access to additional tooling like Passport (instance access request control tool) and Watchman (turns monitoring alerts to tickets for Rackers to address). Your Rackspace technical support professionals will help you resolve issues quickly and effectively any day of the year, any time of the day. Manage & Operate includes:

- Named Account Manager to coordinate escalations, follow GCP technical issues through to resolution, and help focus on the GCP technical operations of the account
- Access to 24x7x365 Technical Operations staffed around the clock and around the globe to help when you experience an issue with your GCP infrastructure
- 24x7x365 management of your environment
- Operating System management
- Configuration of Rackspace infrastructure standard monitoring that is integrated with the Rackspace ticketing system

In addition to the response time SLAs of Cloud Foundation, Manage & Operate customers have access to:

- Emergency: Business-Critical System Outage / Extreme Business Impact detected by Monitoring [15 Minute Response Time]

Architect & Deploy is a pre-requisite for any customers selecting Manage & Operate.

4.4 Complex Cloud Operations

As a business matures or their cloud spend increases, operating GCP can become more complex. Complex Cloud Operations will help you manage this complexity with Rackspace experts that have worked with other similarly complex cloud deployments. Whether you desire a deeper technical relationship to drive outcomes or need assistance handling your architecture's complexity, Complex Cloud Operations can assist.

Complex Cloud Operations is offered in three tiers of support:

- Bronze: Lead Cloud Engineer shared between 10 customers
- Silver: Lead Cloud Engineer shared between 4 customers
- Gold: Lead Cloud Engineer shared between 2 customers
- Platinum: Lead Cloud Engineer dedicated to your account

Rackspace will recommend a tier of support (Bronze, Silver or Gold) based on customer complexity and requirements. Quarterly, customers will work with their resources to scope what available capabilities will be delivered based on level of commitment and customer requirements. Potential activities include:

- ITIL problem management of recurring incidents
- Architecture diagrams of existing infrastructure

- Creation/Maintenance of basic post-deployment infrastructure configuration management scripts
- Review recommendations around Security, Availability, Performance, and GCP Trusted Advisor with remediation plan
- Implement cost saving recommendations by terminating idle or unused resources, right-sizing resources, updating previous generation resources
- Participate in Customer Change Advisory Boards and Stand-Ups
- Training sessions on relevant public cloud topics
- Well-Architected Reviews on different parts of your deployment
- In-Depth Roadmap Reviews for Rackspace Offers and Cloud Products
- Big Data, Serverless, and Container experts

Please talk to your Account Manager if you are interested in learning more about the service block offers.

CHAPTER

FIVE

BILLING

When you signup for Managed Services for Google Cloud Platform, Rackspace will become your reseller of GCP services. This means that all billing of both infrastructure and management charges is provided through a consolidated Rackspace bill, and you do not have to maintain a payment relationship for those projects with Google directly. The credit card you provided when signing up for your Rackspace account will be automatically billed for both your GCP infrastructure, management charges and on-demand support fees, as described below.

5.1 Billing Cycles

Google bills for all infrastructure on a calendar month basis. GCP charges for the previous month's usage are typically finalized by the 10th day of each month. After the charges are finalized by Google, both infrastructure and management charges are added to your Rackspace account and will appear on your next Rackspace bill. Each line item will include the month in which the charges were incurred. Your Rackspace bill is created the 15th of each month, unless you are using an account originally created for the Rackspace Public Cloud, in which case you will be billed based on the anniversary date the account was created.

5.2 Monthly Management Fees

Monthly management fees for each Aviator GCP project will be billed at the rate agreed upon during the project's onboarding. During your first month of management for each GCP project, your monthly management fee is prorated based on the start date of management.

5.3 On-Demand Support Fees

On-Demand support fees for a Runway project ticket are estimated and scoped up front for each ticket by the support team. The fee needs to be agreed to before work begins. Agreed upon fees are included in the upcoming billing cycle.

On-Demand support fee is structured as a cost for the ticket and a cost for the time spent on the ticket. Time is billed in 30 minute increments, rounded up.

5.4 Viewing your Invoices

To view your invoices, login to the Managed Services for Google Cloud Platform Control Panel, select the Account dropdown at the top right corner, and select Billing Overview.

The primary account holder will receive an email any time a payment is processed, indicating that a new invoice is available for review.

5.5 Modifying your Payment Method

If you need to update the credit card or ACH (eCheck - United States only) details that you have on file, login to the Managed Services for Google Cloud Platform Control Panel, select the Account dropdown at the top right corner, and select Billing Overview. From there, you'll find a link to update your payment details.

5.6 Native GCP Project Billing Account Access

All GCP projects under Rackspace management are associated with a single Rackspace owned GCP billing account for your organization. Rackspace automatically grants billing account access to the user who linked the organization with billing:admin rights. This user can manage who else in the organization has access to native GCP billing features.

5.6.1 Managing Access & Payment Contacts

- Please review Overview of Billing Access Control and use GCP's IAM & admin panel to manage access
- Please see the Change Payments Contacts and Notifications for documentation on managing who received budget alerts and payment notifications

5.6.2 Native GCP Billing panel features

- View GCP infrastructure usage reports by visiting the Billing section of the Google Cloud console and clicking on the *Reports* link in the sidebar.
- Set Budget Alerts on GCP infrastructure usage by visiting the Billing section of the Google Cloud console and clicking on the *Budgets & alerts* link in the sidebar.
- Export detailed infrastructure usage reports as flat files or setup recurring BigQuery export by visiting the Billing section of the Google Cloud console and clicking on the *Billing export* link in the sidebar.
- Visualize usage over time with Data Studio provides information on how to use Data Studio to get more detailed insights on usage

5.6.3 Warnings and Notes

Users with Billing:Admin access rights are able to make changes that can impact your service.

- Please do not modify your Rackspace supported project's billing account assignment. Doing so will impact your service; please Contact Us if you wish to change your service level.
- Please do not add Rackspace's billing account to projects that have not been linked through Rackspace's web cloud management tool. If you do this your project will not be properly linked. To address please link the project through the Managed Services for Google Cloud Platform Control Panel .

CHAPTER

SIX

ACCESS AND PERMISSIONS

Controlling access and permissions to the Rackspace and GCP control planes (APIs and UIs) along with the resources you deploy at GCP are a critical part of the overall security of your environment.

6.1 Rackspace Account Permissions

You can grant other members of your company access to Billing and Payments and Support Ticketing by clicking the Account dropdown in the top right corner of the Managed Services for Google Cloud Platform Control Panel and selecting User Management. From there, you can add and manage existing users, selecting which parts of the Rackspace Control Panel they should have access to.

6.2 GCP Project Permissions

GCP project permissions are managed via Google Cloud Identity and Access Management. If you have questions regarding the permissions you should grant users in your company, contact a member of your *support team*.

6.3 Identity/IAM

Both Google and Rackspace encourage the use of the least permissive model for IAM. In essence, access should only be granted where necessary to accomplish tasks. Due to our Google Deployment Manager (GDM) based infrastructure-as-code deployment model, minimizing users beyond the account used to allow Rackspace access for management is suggested. Using GDM to deploy infrastructure means user accounts with permission to manually create/destroy resources in Google Cloud Platform (GCP) is not supported, and instead the GDM templates should be updated and used to deploy the infrastructure changes.

The top-down permissions model used by Google means users granted organizational access have permissions that override more granular permissions applied at service levels, for example. Rackspace's policy to avoid granting access unless necessary, and then grant it at the most granular level possible is necessary to ensure unintentional access is not granted.

In order to ensure that your aviator projects meet this permissions model, Rackspace may periodically audit the permissions being passed to the project and require adjustments to to utilize the least permissive model.

Rackspace will add a service account with the Project Owner role to each of your GCP projects that we manage: automation@rackspace-mgcp.iam.gserviceaccount.com. Additionally, we will grant resource-observer@rackspace-mgcp.iam.gserviceaccount.com the Viewer role on all Aviator projects. Do not remove these accounts or alter their permissions in any way without first consulting with your *support team*. We will also temporarily add accounts from the gcp.rackspace.com domain as Rackers and automation need access to your projects, so do not remove those accounts or alter their permissions.

6.4 Google Organization Permissions

Rackspace will also add our automation@rackspace-mgcp.iam.gserviceaccount.com service account with the Project Creator role on your Google organization, allowing both you and us to create additional projects for new applications, as needed.

CHAPTER

SEVEN

SECURITY

7.1 Rackspace Shared Management Services

Rackspace takes the security of our shared management services and the Managed Services for Google Cloud Platform Control Panel extremely seriously. All infrastructure is deployed leveraging the same set of best practices that we apply to customer projects. The following sections provide a sample of some of the key security focus areas.

7.1.1 Racker Authentication

All Rackspace employees must leverage two-factor authentication for all access to customer account data and customer environments.

7.1.2 Racker Privileges

The level of privileges each Racker has to our Managed Services for Google Cloud Platform management systems is tightly controlled based on job role and is periodically reviewed to ensure that each Racker has the minimum level of permissions required to adequately perform their job duties. All privilege changes require management approval and are also logged for later review.

7.1.3 Encryption at Rest

All sensitive data is encrypted at rest.

7.1.4 Encryption in Transit

All communication between services that make up our shared management system are encrypted during transit using SSL. Our customer and Racker UIs and APIs are only accessible via HTTPS.

7.1.5 Activity Logging

Stackdriver Logging allows you to view audit logs associated with admin and data access events on Google Cloud Platform.

7.2 Permissions

We use a service account with the following permissions to deliver our services to you:

- Organization: *Project Creator*, which allows us to create additional projects in your Organization upon your request
- Runway Projects: *browser*, *billing.projectManager*, *serviceusage.serviceUsageAdmin*, and *servicemanagement.admin* roles. (note that this does not give us the ability to provision or deprovision resources on your projects)
- Aviator Projects: *Owner* permissions, which allow us to share full administrative control with you

7.3 GCP Security

Review Google Cloud Platform Security for more information regarding Google's security practices.

If you have questions regarding any aspect of the security of your environment, please *contact a member of your Support team*.

7.3.1 Security Updates

Google Cloud Platform Security Bulletins are available from Google.

From time to time, Rackspace will provide additional detail or guidance to our customers for specific security incidents. We will publish such value-add security updates below.

Rackspace Response to Meltdown and Spectre

On January 3, 2018, Rackspace was made aware of CPU architecture vulnerabilities associated with Intel, AMD, ARM and other providers. Information about this vulnerability has been provided by Google and is available within the following Google posts:

- https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html
- https://blog.google/topics/google-cloud/what-google-cloud-g-suite-and-chrome-customers-need-know-about-industry-wide-cpu-vulnerability/

These issues were originally uncovered by Google's Project Zero. Their research findings show that an unauthorized party may read sensitive information in the system's memory such as passwords, encryption keys, or sensitive information open in applications.

The remainder of this update is addressed to our Fanatical Support for GCP customers specifically. For updates about our other Rackspace supported hosting environments, please refer to the Rackspace blog.

Overview

Details about the security vulnerabilities can be found in CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754. Google's security bulletin regarding these vulnerabilities can be found here.

There is not a single fix There is no single fix for all three security vulnerabilities. Many vendors have patches available for one or more of these attacks.

Google Cloud Platform (GCP) Response Within Google Cloud Platform, the vulnerability affects two components: the underlying GCP resources and the Google Cloud Services (GCE, GKE, Dataproc, etc.) that run on those resources. Google has confirmed that they have mitigated underlying GCP resources impacted by the vulnerability. For the remaining Google Cloud Services impacted by this vulnerability, Google has recommended that customers take further action.

Next Steps For Aviator supported projects, your Rackspace Cloud Engineering team will coordinate with you to define the next steps needed to mitigate this vulnerability. We are analyzing your current project(s) to understand the scope of work required and will contact you within the next 24 hours.

For projects that are not supported by Rackspace Managed Services (i.e., Runway projects), we recommend that customers undertake mitigation steps per the documentation provided by Google in the security links provided above. We also recommend that you regularly review the Google Cloud security website.

For any further information, please contact your Rackspace team.

Change Log

Date	Description
2018/01/05 14:03 CST	Initial revision of this security update

CHAPTER

EIGHT

SUPPORT

There are multiple ways to receive Fanatical support for your GCP projects. A helpful Racker is always just a phone call or ticket away. We are available live 24x7x365.

8.1 Tickets

The primary way you interact with a Racker is by creating a ticket in the Managed Services for Google Cloud Platform Control Panel. Once logged in, click the Support button in the black bar at the top of the screen and follow the links to create a new ticket or view an existing ticket.

Our automated systems will also create tickets for events on your GCP project(s) that require either your attention or the attention of a Racker.

Any time a ticket is updated, you will receive an email directing you back to the Control Panel to view the latest comments.

8.2 Runway Service Level

Runway projects offer 24x7x365 support.

Billing and account management issues are included in the Runway service offering. All other issues are treated as on-demand support and are charged a fee per ticket to address.

If you need 24x7x365 support for the Google services running in your project and have frequent support needs you should upgrade to the Aviator service level. Contact your Technical Account Manager for additional details.

8.3 Phone

Would you prefer to speak to a live Racker? Give our team a call at 800-961-4454 (US) or 0800-988-0300 (UK) and we'll be happy to assist you. Additional international contact numbers are available on our Contact Us page.

8.4 Monitoring

Rackspace uses Stackdriver Metrics to capture performance metric data for GCP infrastructure components. Stackdriver includes a large number of standard metrics via the default agent, and can also be used to monitor third party applications and services via a variety of additional agents.

Stackdriver metrics for installed agents are always captured, and are subject to retention periods based on the Stackdriver tier purchased by the user (currently this is the same for all tiers). Customers who desire longer metric retention can opt for data to be copied to an external location, e.g. Google Cloud Storage or BigQuery. Dashboards can be generated in the Stackdriver web interface to explore stored metric data, and Alert and Notification Policies can be created to inform users via a variety of means as to emergent conditions.

Rackspace deploys standard alerts for Aviator customers using common GCP components like Compute Engine and Cloud SQL. These may be customized with the cooperation of the MGCP operations team.

Rackspace configures a set of webhook notification targets in Stackdriver, one for each Rackspace ticket severity level. When an alert is posted to one of these webhooks, the data is received by a Rackspace system called Watchman. Watchman groups alerts into appropriate tickets according to the infrastructure involved and the corresponding alert policies. Rackspace operations personnel then respond to these alerts based on customer runbooks.

8.5 Logging

Stackdriver Logging can be used to capture system and application logs in GCP. Log capture is not currently configured by default for Aviator customers, but can be activated with the cooperation of the MGCP operations team.

Logs are retained for 30 days by default, and may be archived to Google Cloud Storage and/or analyzed with BigQuery. Log-based metrics can also be used to trigger alerts via Stackdriver Monitoring.