Rackspace Managed Services for Google Cloud Platform Product Guide

Release 2018-03-02-15:58

March 02, 2018

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, but 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*.

CHAPTER

FOUR

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 and management charges, as described below.

4.1 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.

4.2 Monthly Management Fees

Your 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, we will prorate the monthly management fee for the remainder of the month based on the date we began management.

4.3 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.

4.4 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.

CHAPTER

FIVE

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.

5.1 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.

5.2 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*.

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. Do not remove this account or alter its 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.

5.3 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

SIX

SECURITY

6.1 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.

6.1.1 Racker Authentication

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

6.1.2 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.

6.1.3 Encryption at Rest

All sensitive data is encrypted at rest.

6.1.4 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.

6.1.5 Activity Logging

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

6.2 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, 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

6.3 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*.

6.3.1 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

SEVEN

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.

7.1 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.

7.1.1 Runway Service Level

For projects at the Runway service level, Rackspace only provides support for billing and account management issues. If you need support for the Google services running in your project, you must either upgrade to the Aviator service level or establish a support relationship directly with Google. Contact your Technical Account Manager for additional details regarding both options.

7.2 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.