



FlashGrid[®] Server for Oracle Database on Google Cloud

Deployment Guide

rev. 26.05-2026.07.14

Table of Contents

- 1 Introduction 3
 - 1.1 Key Components 3
 - 1.2 Infrastructure-as-Code Deployment 3
- 2 Prerequisites 4
 - 2.1 Service Account for Infrastructure Manager 4
 - 2.2 Uploading Oracle Installation Files to a Storage Bucket 4
 - 2.3 Preparing the VPC 4
- 3 Deploying FlashGrid Server 6
- 4 After Deploying 8
 - 4.1 Verifying a VM Instance Status 8
 - 4.2 OS User Accounts 8
 - 4.3 Finalizing Software Configuration 9
 - 4.4 Enabling Deletion Protection 9
 - 4.5 Installing an Additional Database Home 9
 - 4.6 Use of Anti-virus and Other Third-party Software 9
 - 4.7 Use of Automatic Configuration Tools 9
 - 4.8 Security Hardening 10
 - 4.9 Convert RHEL PAYG to BYOS License 10
- 5 Monitoring Instance Health 11
- 6 Before Going Live 11
- 7 Deleting a FlashGrid Server Deployment 11
- 8 Additional Documentation 12
- 9 Technical Support 12

1 Introduction

FlashGrid Server is an engineered cloud system for running Oracle Databases in public clouds. This guide provides step-by-step instructions for system and database administrators deploying FlashGrid Server with Oracle Database on Google Cloud.

1.1 Key Components

Key components of FlashGrid Server on Google Cloud:

- FlashGrid Storage Fabric software
- FlashGrid Cloud Area Network software
- Oracle Database: 19c, or 26ai
- Oracle Grid Infrastructure: 19c, or 26ai
- Operating Systems:
 - **Oracle Linux:** 9 (UEKR7)
 - **Red Hat Enterprise Linux (RHEL):** 8, or 9
- Compute Engine VM instance types:
 - **General-purpose:** c4-standard, c4-highcpu, c4-highmem, c4d-standard, c4d-highcpu, c4d-highmem, c3-standard, c3-highcpu, c3-highmem, c3d-standard, c3d-highcpu, c3d-highmem
 - **Memory-optimized:** m4-hypermem, m4-ultramem, m4-megamem, m3-ultramem, m3-megamem
- Disks: Hyperdisk Balanced and Balanced Persistent Disks

1.2 Infrastructure-as-Code Deployment

FlashGrid Server is delivered as Google Cloud Terraform modules that automate configuration of multiple components required for a database server. FlashGrid Launcher is an online tool that simplifies the deployment process by guiding through the server configuration parameters and generating Terraform modules.

2 Prerequisites

2.1 Service Account for Infrastructure Manager

If you use [Infrastructure Manager](#), create and configure a [service account](#), for example `for-infra-manager@your-project.iam.gserviceaccount.com`. Grant the service account the *Cloud Infrastructure Manager Agent* role and any additional roles required by the resources in your deployment, such as *Compute Admin* for Compute Engine resources.

2.2 Uploading Oracle Installation Files to a Storage Bucket

During software initialization Oracle installation files will be downloaded from a storage bucket. The list of files that must be placed in the storage bucket will be shown in FlashGrid Launcher. The same storage bucket can be used for deploying multiple instances. If any of the required Oracle files is missing or inaccessible, then the software initialization will fail.

Enabling public access to the bucket allows FlashGrid Launcher tool to verify that all required files are accessible. To enable public access, add *allUsers* with *Storage Object Viewer* (or *Storage Legacy Object Reader*) to the bucket permissions.

If allowing public access to the bucket is not possible then create the bucket with [uniform bucket-level access](#) enabled and create a [service account](#), for example `download-oracle-files@your-project.iam.gserviceaccount.com`. Grant that service account the *Storage Object Viewer* role on the bucket so the Compute Engine VM can download the required Oracle files. Then grant the Infrastructure Manager service account access as *Service Account User*:

- Open [Service Accounts](#) in Google Cloud Console IAM and select your project.
- Click on `download-oracle-files@your-project.iam.gserviceaccount.com`.
- Click on the *Principals with access* tab.
- Click *Grant Access*.
- Add `for-infra-manager@your-project.iam.gserviceaccount.com`.
- Select the *Service Account User* from the *Role* dropdown.
- Click *Save*.

You will specify both the storage bucket and the service account in FlashGrid Launcher.

2.3 Preparing the VPC

When creating a new instance, you have two options:

- **Automatically create a new VPC.**
This option is usually used for test systems isolated in their own sandbox VPCs. A VPC will be created together with the required subnet and firewall rules. By default, the VPC will be created with CIDR 10.100.0.0/16.
- **Create the instance in an existing VPC.**
This option is used for majority of production deployments where other systems (e.g. app servers) share the same VPC as the instance. In the FlashGrid Launcher tool you will need to provide name of the subnet where the system will be placed. Existing *Legacy* networks are not supported. Optionally you may provide [Network Tags and Secure Tag values](#). VPC firewall rules can use these as “target tags” to define which VMs a rule applies to; the rule then affects traffic to the VM’s primary internal IP on that VPC network. Secure tags are organization-level tag keys and values managed through Resource Manager and IAM.

If you use an existing VPC, make sure the following prerequisites are met before creating an instance:

- The VPC may have any CIDR that does not overlap with 192.168.0.0/16, for example 10.100.0.0/16. If you must use VPC with CIDR that overlaps with 192.168.0.0/16 then please request a customized configuration file from FlashGrid support.
- The VPC has a subnet in the target region.
- The subnet has [Private Google Access configured](#).
- Firewall rules allow ingress traffic on the following ports:
 - Inbound: TCP port 22 for SSH access to the instance
 - Inbound: TCP port 5901 if you choose to use VNC for creating a database using DBCA in GUI mode with direct connection (vs. SSH tunnel)
 - Inbound: TCP port 1521 for database client and application server access
 - Inbound access to the ports listed above must be allowed only from those source tags or IP ranges that require such access. Do not configure 0.0.0.0/0 as an allowed source in VPC firewall rules.
- FlashGrid Server VM is configured to use VPC's MTU settings. For the best performance, it's recommended to set the maximum transmission unit (MTU) of the VPC to 8896. However, ensure that these MTU settings do not interfere with other resources using the VPC.

3 Deploying FlashGrid Server

The FlashGrid Launcher tool simplifies instance deployment on Google Cloud Compute Engine by automating the following tasks:

- Creating and configuring VPC, subnet, and firewall rules (optional)
- Creating block storage volumes and launching Compute Engine VM instance
- Installing and configuring FlashGrid Cloud Area Network
- Installing and configuring FlashGrid Storage Fabric
- Installing and patching Oracle Grid Infrastructure software
- Configuring Grid Infrastructure
- Installing and patching Oracle Database software
- Creating ASM disk groups

To create an instance

1. Log in to [Google Cloud Console](#) with a user account that has the following privileges:
 - Compute Admin
 - Infra Manager Admin
 - Storage Admin
2. Open FlashGrid Launcher tool:
 - Start with one of the standard configurations at <https://www.flashgrid.io/products/flashgrid-for-oracle-db-on-google-cloud/>
 - or, if you have a custom configuration file, upload it at <https://2605.cloudprov.flashgrid.io/>
3. Configure parameters for the deployment
4. If verification passes, then click *Download Terraform* button to download Terraform configuration.
5. Extract the downloaded Terraform module and [upload the Terraform configuration to a Google Storage bucket](#).
Note: upload the extracted folder, **not** the downloaded archive file.
6. Go to the [new Terraform deployment](#) page in Infrastructure Manager.
7. Create a new deployment by supplying the Deployment ID, Region, and Service Account.
8. Set *Source of Terraform configuration* to *GCS*.
9. Set the Cloud Storage path (e.g. `gs://your-bucket/path-to-terraform-directory`) as the source for the Terraform configuration. Click *Continue*.
10. Fill in the Project ID in the *Terraform Details* section, then click the *Create Deployment* button to start the deployment.
11. Wait until creating the deployment completes.
Note: *Cloud Build Logs* may contain an error like

```
2025/10/16 16:27:15 [DEBUG] Loading disk type: hyperdisk-balanced
time="2025-10-16T16:27:15Z" level=error msg="error converting resource with address
module.flashgrid_cluster.google_compute_instance.cluster_instances["myhostname"] and type
google_compute_instance : The zonal field for resource disks cannot be empty."
```

This error is considered benign and can be safely ignored if the deployment is completed successfully without other issues.
12. SSH to the instance with your username.
13. The welcome message will show the current initialization status of the instance: in progress, failed, or completed.
14. If initialization is still in progress, then wait for it to complete (this includes Oracle software installation and configuration). You will receive a broadcast message when initialization completes or fails. Software initialization takes approximately 30 minutes, this includes Oracle software installation and configuration.

Note: for deploying FlashGrid Server with **SELinux** please refer to the Knowledge Base article [How to configure SELinux mode during system deployment](#).

4 After Deploying

4.1 Verifying a VM Instance Status

On an instance run `flashgrid-health-check` command to verify that the instance status is *Good* and all checks are passing.

```
[fg@myhostname ~]$ flashgrid-health-check

HealthCheck 20.9.1.57074 #7226b34d571618368a70c9af809e5f150f8c67ba
~~~~~
Check: ASM DiskGroup status
myhostname: OK

-----
  GroupName  Status  Mounted  Type    TotalMiB  FreeMiB  OfflineDisks  LostDisks  Resync  ReadLocal  Vote
-----
  DATA      Good    AllNodes  EXTERN  6144      6028     0              0          No     Enabled    N/A
  FRA        Good    AllNodes  EXTERN  6144      6040     0              0          No     Enabled    N/A
  GRID       Good    AllNodes  EXTERN  5120      5020     0              0          No     Disabled   N/A
-----

Check: Alerts in Storage Fabric logs in the last 7 days
myhostname: OK

Check: Available memory
myhostname: OK : avail mem: 27.7%

Check: Check db memory settings
myhostname: OK

Check: Check local listener for each db
myhostname: OK

Check: Check tnsnames.ora
myhostname: OK

Check: Flashgrid CLAN check
myhostname: OK

Check: Free system disk space
myhostname: OK : /u01: avail 66%, /: avail 90%

Check: Kernel taint check
myhostname: OK

Check: SF node status
myhostname: OK

Check: Swap disabled
myhostname: OK : Swap disabled

Check: System config file modifications
myhostname: OK

Check: System services
myhostname: OK

Check: Unexpected or 3rd party RPMs installed
myhostname: OK

Check: Unexpected or 3rd party services enabled
myhostname: OK
```

4.2 OS User Accounts

During software initialization the following OS user accounts are created:

- *fg* - the user account for running some of the FlashGrid Storage Fabric or FlashGrid Cloud Area Network utilities. The user *fg* has sudo rights.

- *grid* - Grid Infrastructure (GI) owner. GI environment variables are preconfigured.
- *oracle* - Database home owner. Database environment variables, except ORACLE_SID and ORACLE_UNQNAME, are preconfigured. After creating a database, you can configure ORACLE_SID and ORACLE_UNQNAME by editing `/home/oracle/.bashrc` file.

Note that no passwords are configured for any users. Also, password based SSH authentication is disabled in `/etc/ssh/sshd_config`. Key-based authentication is recommended for better security. Creating passwords for any user is not recommended.

User *fg* has sudo rights and allows switching to any other user without requiring a password (which is not configured by default). Example:

```
$ sudo su - grid
```

4.3 Finalizing Software Configuration

See the Knowledge Base article [Creating a Database](#) for instructions.

Note: ACFS support on RHEL may require an additional Oracle Clusterware patch. Please refer to Oracle [KB129209](#) for ACFS patch information.

4.4 Enabling Deletion Protection

If the instance is for production use, then it is strongly recommended to enable deletion protection for the Compute Engine VM instance. If you did not enable deletion protection in FlashGrid Launcher during deployment, follow the steps below to enable it now.

- Edit `main.tf` in the Terraform folder and set `deletion_protection = true`
- Upload the updated `main.tf` to the Google Cloud Storage bucket used by the deployment, choosing *Overwrite*.
- Open [Infrastructure Manager](#) and select the deployment that corresponds to the Compute Engine VM instance.
- Click *Edit* and then *Update* and wait until the deployment update completes.

4.5 Installing an Additional Database Home

In most cases manual installation of database software is not required. However, if you need to install an additional database home, then follow Oracle Database documentation for installing the database software.

4.6 Use of Anti-virus and Other Third-party Software

If anti-virus software must be used, then it is recommended to configure it in a way that avoids putting any files in quarantine. Automatic quarantine of files creates risk of the system downtime in case of a false positive detection on a critical system file on a Compute Engine VM instance.

Any proprietary kernel modules installed by third-party software create risks to reliable operation of the system. Such proprietary kernel modules are not tested or supported by FlashGrid, Red Hat, or Oracle. Proprietary kernel modules may consume kernel resources and may create instability, especially under high load. Symptoms may include kernel crashes, network disruptions, storage i/o disruptions, and server brown-out. If such reliability issue is encountered and no other root cause can be readily identified, FlashGrid support reserves the right to request removal of all proprietary kernel modules before continuing investigation.

4.7 Use of Automatic Configuration Tools

Automatic configuration tools (e.g. Ansible, Salt, etc.) must be used with extra care. Incorrect modification of a critical system file (e.g. `/etc/resolv.conf`) may cause system downtime. Note that many critical system configuration files

are protected with immutable attribute and have warnings in them. Do not remove the immutable attribute or allow automatic modification of such files unless absolutely necessary.

4.8 Security Hardening

The system is deployed using Linux images that have main security best practices implemented by default. The following steps are recommended, in case additional security hardening is required.

For applying a different hardening profile, the following steps are recommended:

- 1) Request FlashGrid support to review the list of required changes.
- 2) [Back up an instance](#).
- 3) Implement the required changes.
- 4) [Restart the instance](#).
- 5) Verify health of the system as user *fg*:

```
$ flashgrid-health-check
```

- 6) In case of errors, roll back the changes or restore the system from backup

4.9 Convert RHEL PAYG to BYOS License

If RHEL is used, a Compute Engine VM instance is provisioned with a RHEL PAYG license attached. To adopt BYOS, the RHEL license must be removed as per the [procedure documented by Google Cloud](#), following server deployment.

5 Monitoring Instance Health

The following methods of monitoring system health are available:

- *flashgrid-health-check* utility checks multiple items including database configuration, storage, OS kernel, config file modifications, errors in the logs, and other items that may affect health of the system or could help with troubleshooting. It is recommended for manual checks only.
- *FlashGrid Node Monitor* service is part of the *flashgrid-diags* package. It provides monitoring of various system health indicators, including CPU utilization, available memory, and clocks.
- Alerts about failures are recorded in system log and can be analyzed by 3rd-party tools.
- Email alerts can be configured in FlashGrid Launcher and sent to one or several email addresses. See the Knowledge Base article [Configuring email for FlashGrid notifications](#).
- *FlashGrid Node Monitor* can send alerts and diagnostic uploads via HTTP/HTTPS to a remote endpoint, with support for routing through an HTTP proxy. Node Monitor detects a condition, then sends either an email alert and/or an HTTP/REST request to a monitoring/alerting service.
- ASM disk group monitoring and alerting via Oracle Enterprise Manager.

6 Before Going Live

Before switching the system to live use (run commands as user *fg*):

1. Confirm that only minimally required access to the server is allowed in network security settings, and remove any unnecessary access
2. Verify health of the instance: `$ flashgrid-health-check`
3. Confirm that email alerts are configured and delivered: `$ flashgrid-node test-alerts`
4. Upload diags to FlashGrid support: `$ flashgrid-diags upload-all`
5. [Stop the instance](#) and [back it up](#).
6. Start the instance and do final check of the system health: `$ flashgrid-health-check`

7 Deleting a FlashGrid Server Deployment

To delete a FlashGrid server deployment

1. Disable VM deletion protection in Terraform if it was enabled:
 - Edit `main.tf` in the Terraform folder and set `deletion_protection = false`
 - Upload the updated `main.tf` to the Google Cloud Storage bucket used by the deployment, choosing *Overwrite*.
 - Open [Infrastructure Manager](#) and select the deployment that corresponds to the Compute Engine VM instance
 - Click *Edit* and then *Update* and wait until the deployment update completes.
2. Delete the deployment:
 - In [Infrastructure Manager](#), click *Delete* for the deployment and confirm the deletion.

8 Additional Documentation

[FlashGrid Server on Google Cloud Knowledge Base](#)

[FlashGrid Server on Google Cloud Backup Best Practices](#)

[FlashGrid Storage Fabric CLI Reference Guide](#)

[FlashGrid Cloud Area Network CLI Reference Guide](#)

9 Technical Support

For technical help with FlashGrid Server please open a [support request](#).

To expedite troubleshooting please also collect and upload diagnostic data to the secure storage used by FlashGrid support by running the following command as user *fg*:

```
$ flashgrid-diags upload-all
```

For reporting *emergency* type of issues that require immediate attention please also use the 24/7 telephone hotline: +1-650-641-2421 ext 7. Please note that use of the 24/7 hotline is reserved for emergency situations only.

Support Tiers and SLA details document: [FlashGrid Technical Support Services](#).

Copyright © 2016-2026 FlashGrid Inc. All rights reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document.

FlashGrid is a registered trademark of FlashGrid Inc. Google and Google Cloud are registered trademarks of Google LLC. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Red Hat is a registered trademark of Red Hat Inc. Other names may be trademarks of their respective owners.