flashgrid

FlashGrid® Cluster

for Oracle Database and Oracle RAC on Google Cloud

Deployment Guide

rev. 26.03-2026.07.08

Table of Contents

1 Introduction

FlashGrid Cluster is an engineered cloud system that enables active-active database high availability infrastructure in public clouds. This guide provides step-by-step instructions for system and database administrators deploying FlashGrid Cluster with Oracle RAC on Google Cloud Compute Engine VMs.

Key components of FlashGrid Cluster on Google Cloud:

- FlashGrid Storage Fabric software
- FlashGrid Cloud Area Network software
- Oracle Database: 19c
  Note: For installing a legacy DB version 11.2.0.4, 12.1.0.2, or 12.2.0.1, deploy with the current version of FlashGrid Launcher and install database home manually. (Supported on RHEL8 only. Access to Tier1 Oracle patches is required.)
- Oracle Grid Infrastructure: 19c
- Operating System:
  - **Oracle Linux**: 9 (UEKR7)
  - **Red Hat Enterprise Linux (RHEL):** 8, or 9
- Compute Engine VM 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

FlashGrid Cluster is delivered as Google Cloud Terraform modules that automate configuration of multiple components required for a database cluster. FlashGrid Launcher is an online tool that simplifies the deployment process by guiding through the cluster 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 cluster, you have two options:

- **Automatically create a new VPC.**
  This option is usually used for a test cluster isolated in its own sandbox VPC. A new 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 cluster 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 cluster. In the FlashGrid Launcher tool you will need to provide name of the subnet where the cluster 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 a cluster:

- 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 a 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 and Outbound: All traffic between cluster nodes.
    - Inbound: TCP ports 1521, 1522 for SCAN and Local Listener access to the database nodes from app servers and other database clients. These are default port numbers that can be changed in the FlashGrid Launcher tool.
    - Inbound: TCP port 22 for SSH access to the cluster nodes.
    - 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 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 Cluster nodes are 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 a Cluster

The FlashGrid Launcher tool simplifies deployment of Oracle RAC clusters 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 VM instances for all nodes in the cluster
- Installing and configuring FlashGrid Cloud Area Network
- Installing and configuring FlashGrid Storage Fabric
- Installing and patching Oracle Grid Infrastructure software
- Configuring Grid Infrastructure cluster
- Installing and patching Oracle Database software
- Creating ASM disk groups

To create a cluster

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-rac-on-gcp/
    - or, if you have a custom configuration file, upload it at https://2603.cloudprov.flashgrid.io/
3. Configure parameters of the cluster.
4. Click *Validate Configuration* button.
5. If verification passes, then click *Download Terraform* button to download Terraform configuration.
6. 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.
7. Go to the new Terraform deployment page in Infrastructure Manager.
8. Create a new deployment by supplying the Deployment ID, Region, and Service Account.
9. Set *Source of Terraform configuration* to *GCS*.
10. Set the Cloud Storage path (e.g. `gs://your-bucket/path-to-terraform-directory`) as the source for the Terraform configuration. Click *Continue*.
11. Fill in the Project ID in the *Terraform Details* section, then click the *Create Deployment* button to start the deployment.
12. Wait until creating the deployment completes.
    Note: *Cloud Build Logs* may contain errors like
    ```
    2025/10/16 04:05:39 [DEBUG] Loading disk type: hyperdisk-balanced
    time="2025-10-16T04:05:39Z" level=error msg="error converting resource with address
    module.flashgrid_cluster.google_compute_instance.cluster_instances[\"myrac2n-68f06d03-rac1\"] 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.
13. SSH to the first (as it was specified on the cluster configuration page) cluster node with your username.
14. The welcome message will show the current initialization status of the cluster: in progress, failed, or completed.
15. 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. Cluster initialization takes 1 to 2 hours depending on configuration.

Note: for deploying FlashGrid Cluster with ***SELinux*** please refer to the following knowledge base article:
https://support.flashgrid.io/hc/en-us/articles/26368224225687

4 After Deploying a Cluster

4.1 Verifying Cluster Status

On any of the cluster nodes run `flashgrid-cluster` command to verify that the cluster status is *Good* and that all checks are passing.

```
[fg@rac1 ~]$ flashgrid-cluster
FlashGrid Cluster version 25.10.10.62253.97ab59d0
Storage Fabric version 25.10.10.18166 #4515c8fdbf95ff6a917082a33310138f90001bec
Thu Oct 16 05:16:31 2025 +0000
License: Active, Expires 2026-01-15
Licensee: Company_test
Support plan: Demo
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
FlashGrid running: OK
Clocks check: OK
Configuration check: OK
Network check: OK

Querying nodes: rac1, rac2, racq ...

Cluster Name: myrac2n
Cluster status: Good
-------------------------------------------------------------
Node  Status  ASM_Node  Storage_Node  Quorum_Node  Failgroup
-------------------------------------------------------------
rac1  Good    Yes       Yes           No           RAC1
rac2  Good    Yes       Yes           No           RAC2
racq  Good    No        No            Yes          RACQ
-------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------
GroupName  Status  Mounted   Type    TotalMiB  FreeMiB  OfflineDisks  LostDisks  Resync  ReadLocal  Vote
-------------------------------------------------------------------------------------------------------------
DATA       Good    AllNodes  NORMAL  20480     20120    0             0          No      Enabled    None
FRA        Good    AllNodes  NORMAL  20480     20120    0             0          No      Enabled    None
GRID       Good    AllNodes  NORMAL  12288     11464    0             0          No      Enabled    3/3
-------------------------------------------------------------------------------------------------------------
[fg@rac1 ~]$
```

4.2 OS User Accounts

During cluster 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. It also has key-based passwordless SSH configured between all nodes of the cluster, which makes it easy to move between the nodes.
- *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 on each database node.

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
```

Users *fg*, *grid*, and *oracle* have key-based SSH access configured between the nodes of the cluster. The corresponding key pairs are generated automatically during cluster initialization. For example, if you are logged in to *node1* as user *fg* then you can SSH into *node2* by simply running `'ssh node2'` without entering a password or providing a key.

4.3 Finalizing Cluster Configuration

See knowledge base articles for performing the following steps:

1. Creating a database: https://support.flashgrid.io/hc/en-us/articles/1500011215081
2. Connecting clients to a database: https://support.flashgrid.io/hc/en-us/articles/1500011176122

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 cluster is intended for production use, we strongly recommend enabling deletion protection for each 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 cluster.
- 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 cluster downtime in case of a false positive detection on a critical system file on multiple nodes of the cluster.

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, node evictions, and cluster 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`) on multiple cluster nodes may cause cluster 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

For applying security hardening to the OS using CIS aligned security profiles, see https://support.flashgrid.io/hc/en-us/articles/5883226799639

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 all cluster nodes: https://support.flashgrid.io/hc/en-us/articles/1500011175542
3) Implement the required changes on all nodes.
4) Restart the entire cluster: https://support.flashgrid.io/hc/en-us/articles/4404882268951
5) Verify health of the cluster as user *fg*:

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

6) In case of errors, roll back the changes or restore the nodes from backup.

4.9 Convert RHEL PAYG to BYOS License

If RHEL is used, cluster VM instances are provisioned with a RHEL PAYG license attached to each Compute Engine VM instance. To adopt BYOS, the RHEL license must be removed as per the procedure documented by Google Cloud, following cluster deployment.

5 Monitoring Cluster Health

The following methods of monitoring cluster health are available:

- *flashgrid-cluster* utility displays status of the storage subsystem (FlashGrid Storage Fabric and ASM) and its main components. The utility can be used in monitoring scripts. It returns a non-zero value if status of the cluster is *Warning* or *Critical*.
- *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 cluster 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 cluster to live use (run commands as user *fg*):

1. Verify health of the cluster: `$ flashgrid-health-check`
2. Confirm that email alerts are configured and delivered: `$ flashgrid-node test-alerts`
3. Upload diags to FlashGrid support: `$ flashgrid-diags upload-all`
4. Stop the cluster and back up all cluster nodes: https://support.flashgrid.io/hc/en-us/articles/4404887221655
5. Start the cluster and do final check of the cluster health: `$ flashgrid-health-check`

7 Deleting a Cluster

To delete a cluster

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 cluster.
   - 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

Knowledge Base: https://support.flashgrid.io/hc/en-us/categories/1500001520262

Backup Best Practices on Google Cloud: https://support.flashgrid.io/hc/en-us/articles/1500011175542

FlashGrid Storage Fabric CLI Reference Guide: https://support.flashgrid.io/hc/en-us/articles/1500011214681

FlashGrid Cloud Area Network CLI Reference Guide: https://support.flashgrid.io/hc/en-us/articles/1500011214661

9 Technical Support

For technical help with FlashGrid Cluster please open a support request at https://www.flashgrid.io/support/

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: https://www.flashgrid.io/docs/FlashGrid_technical_support_services.pdf