flashgrid

FlashGrid® Cloud Cluster
for Oracle RAC on GCP

Deployment Guide

rev. 20.10-2020.12.30

Table of Contents

1 Introduction

FlashGrid Cloud 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 Cloud Cluster with Oracle RAC on Google Cloud Platform.

Key components of FlashGrid Cloud Cluster 20.10 for GCP:

- FlashGrid Storage Fabric: ver. 20.08
- FlashGrid Cloud Area Network: ver. 20.10
- FlashGrid Diagnostics: ver. 20.09
- FlashGrid Health Checker ver. 20.09
- Oracle Database: ver. 19c, 18c, 12.2.0.1, 12.1.0.2, or 11.2.0.4.
- Oracle Grid Infrastructure: ver. 19c. (Versions 18c and 12.2.0.1 available on request)
- Operating System: Oracle Linux 7, Red Hat Enterprise Linux 7
- GCP Compute Engine VM types:
    - n1-standard, n1-hugemem
    - n2-standard, n2-hugemem
    - m1-ultramem, m1-megamem
- Disks: SSD Persistent disks

FlashGrid Cloud Cluster is delivered as GCP Deployment Manager templates that automate configuration of multiple components required for a database cluster. FlashGrid Cloud Cluster Launcher is an online tool that simplifies the deployment process by guiding through the cluster configuration parameters and generating Deployment Manager templates.

2 Prerequisites

2.1 Uploading Oracle Installation Files to a Storage Bucket

During cluster 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 Cloud Cluster Launcher. The same storage bucket can be used for deploying multiple clusters. If any of the required Oracle files is missing or inaccessible then the cluster initialization will fail.

Enabling public access to the bucket allows FlashGrid Cloud Cluster 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 *Bucket Policy Only*, create a service account *FlashGrid Cloud Cluster VM*, and add this service account to the bucket's permissions with *Storage Object Viewer* role. This will allow the cluster node VMs to download the required Oracle files. You can find the default compute engine service account in IAM console.

2.2 Preparing the VPC

When creating a new cluster you have two options:

- **Automatically create a new VPC.**
  This option is usually used for test clusters isolated in their own sandbox VPCs. A VPC will be created together with the required subnets 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 Cloud Cluster Launcher tool you will need to provide name of the subnet where the cluster will be placed. Existing *Legacy* networks are not supported.

If using an existing VPC then make sure that the following pre-requisites 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 have to 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. Without *Private Google Access* configured enabling *External IPs* is required for access to the storage bucket with Oracle files.
- Firewall rules allow ingress traffic on the following ports:
  - UDP ports 4801, 4802, 4803 and TCP 3260 between the cluster node VMs (cluster initialization will fail if any of these ports are not open)
  - 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 FlashGrid Cloud Cluster Launcher.
  - TCP port 22 for SSH access to the cluster nodes
  - TCP port 5901 if you choose to use VNC for creating a database using DBCA in GUI mode

3 Deploying a Cluster

The FlashGrid Cloud Cluster Launcher tool simplifies deployment of Oracle RAC clusters on GCP by automating the following tasks:

- Creating and configuring VPC, subnet, and firewall rules (optional)
- Creating EBS volumes and launching VMs 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 GCP Console with a user account that has the following privileges:
   - Compute Admin
   - Deployment Manager Editor
2. Open FlashGrid Cloud Cluster Launcher tool:
   - Start with one of the standard configurations at https://www.flashgrid.io/skycluster-for-gcp
   - or, if you have a custom configuration file, upload it at https://2010-skycluster.cloudprov.flashgrid.io/
3. Configure parameters of the cluster
4. Click *Validate Configuration* button
5. If verification passes then click *Generate Template* button
6. Copy the cloud shell command and run it in Google Cloud Shell to create the cluster deployment
7. Wait until creating the deployment completes
8. SSH to the first (as it was specified on the cluster configuration page) cluster node with your user name
9. The welcome message will show the current initialization status of the cluster: in progress, failed, or completed.
10. 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.

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 all checks are passing.

```
[fg@rac1 ~]$ flashgrid-cluster
FlashGrid 18.07.10.46032 #95f2b5603f206af26482ac82386b1268b283fc3c
License: via Marketplace Subscription
Support plan: 24x7
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
FlashGrid running: OK
Clocks check: OK
Configuration check: OK
Network check: OK

Querying nodes: quorum, rac1, rac2 ...

Cluster Name: myrac
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           QUORUM
-------------------------------------------------------------

-----------------------------------------------------------------------------------------------------
GroupName   Status   Mounted    Type     TotalMiB   FreeMiB   OfflineDisks   LostDisks   Resync   ReadLocal   Vote
-----------------------------------------------------------------------------------------------------
GRID        Good     AllNodes   NORMAL   12588      3376      0              0           No       Enabled     3/3
DATA        Good     AllNodes   NORMAL   2048000    2048000   0              0           No       Enabled     None
FRA         Good     AllNodes   NORMAL   1024000    1024000   0              0           No       Enabled     None
-----------------------------------------------------------------------------------------------------
```

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 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. Changing temporary ASM passwords: https://kb.flashgrid.io/asm-password
2. Creating a database: https://kb.flashgrid.io/createdb
3. Connecting clients to a database: https://kb.flashgrid.io/connect-clients

4.4 Enabling deletion protection

If the cluster is for production use then it is strongly recommended to enable deletion protection for each VM.

4.5 Use of anti-virus software

If anti-virus software has to 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.

4.6 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.

4.7 Security hardening

Cluster nodes are deployed using RHEL 7 or Oracle Linux 7 images that have main security best practices implemented by default. The following steps are recommended, in case additional security hardening is required:

1) Request FlashGrid support to review the list of required changes.
2) Back up all cluster nodes: https://www.kb.flashgrid.io/backup-restore/backup-best-practices-on-gcp
3) Implement the required changes on all nodes.
4) Restart the entire cluster: https://kb.flashgrid.io/maintenance/maintenance-gcp#restarting-the-entire-cluster
5) Verify health of the cluster: `$ sudo flashgrid-health-check`
6) In case of errors, roll back the changes or restore the nodes from backup.

5 Monitoring Cluster Health

The following methods of monitoring cluster 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 cluster or could help with troubleshooting. It is recommended for manual checks only.
- *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*.
- Alerts about failures are recorded in system log and can be analyzed by 3rd-party tools.
- Email alerts can be sent to one or several email addresses.
- ASM disk group monitoring and alerting via Oracle Enterprise Manager.

To test email alerts

1. On all nodes (including quorum node) run

   `$ flashgrid-node test-alerts`

2. Check that test alert emails were received from all cluster nodes at each of the configured email addresses.

To modify the list of email alert recipients

As user fg@ on any database node run

   `$ flashgrid-cluster set-email-alerts name1@host1 name2@host2 ...`

Note that by default the *From* address is set to *flashgrid@localhost.localdomain*. This will ensure that delivery failure notifications are sent to root's mailbox on the originating node, which can help with troubleshooting delivery issues. It is recommended to add this address to the whitelist of senders on the receiving email server and in the email clients.

6 Before Going Live

Before switching the cluster to live use:

1. Verify health of the cluster: `$ sudo flashgrid-health-check`
2. Confirm that email alerts are configured and delivered: `$ flashgrid-node test-alerts`
3. Upload diags to FlashGrid support: `$ sudo flashgrid-diags upload-all`
4. Stop the cluster and back up all cluster nodes:
   https://www.kb.flashgrid.io/backup-restore/backup-best-practices-on-gcp
5. Start the cluster and do final check of the cluster health: `$ sudo flashgrid-health-check`

7 Deleting a cluster

To delete a cluster

1. Disable VM deletion protection for each cluster node if it was enabled
2. Open *Deployment Manager* console
3. Select deployment corresponding to the cluster
4. Click *Delete*

---

8 Additional Documentation

Maintenance Tasks on GCP: https://www.kb.flashgrid.io/maintenance/maintenance-gcp

Backup and Restore Best Practices on GCP: https://www.kb.flashgrid.io/backup-restore/backup-best-practices-on-gcp

Troubleshooting: https://www.kb.flashgrid.io/troubleshooting

FlashGrid Storage Fabric CLI Reference Guide: https://www.kb.flashgrid.io/cli-ref/sf-cli

FlashGrid Cloud Area Network CLI Reference Guide: https://www.kb.flashgrid.io/cli-ref/clan-cli

9 Contacting Technical Support

For technical help with FlashGrid Cloud 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:

```
$ sudo 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.