flashgrid

FlashGrid® Server

for Oracle Database on Google Cloud

Deployment Guide

rev. 24.11-2024.12.10

Table of Contents

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, 18c, 12.2.0.1, 12.1.0.2, or 11.2.0.4
- Oracle Grid Infrastructure: 19c
- Operating Systems:
  - **Oracle Linux**: 9
  - **Red Hat Enterprise Linux** (RHEL) 8, or 9
- Compute Engine VM types:
  - **General-purpose:** c3-standard, c3-highmem, c3-highcpu, c3d-standard, c3d-highmem, c3d-highcpu, c4-standard, c4-highmem, c4-highcpu
  - **Memory-optimized:** m3-ultramem, m3-megamem
- Disks: Hyperdisk Balanced and Balanced Persistent Disks

1.2 Infrastructure-as-Code Deployment

FlashGrid Server is delivered as Google Cloud Deployment Manager templates 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 Deployment Manager templates.

2 Prerequisites

2.1 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 *Bucket Policy Only*, create a service account *FlashGrid VM*, and add this service account to the bucket's permissions with *Storage Object Viewer* role. This will allow the server VM 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 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 subnets 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.

If using an existing VPC then make sure that the following pre-requisites 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. 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:
  - Inbound and Outbound: All traffic between members of the security group.
  - 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 security groups or IP ranges that require such access. Do not configure *Anywhere* or *0.0.0.0/0* as allowed sources.
- 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 VM
- 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 GCP Console with a user account that has the following privileges:
    - Compute Admin
    - Deployment Manager Editor
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://2411.cloudprov.flashgrid.io/
3. Configure parameters for the deployment
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 system deployment
7. Wait until creating the deployment completes
8. SSH to the instance with your username
   Note: If you selected to create a new VPC and connecting through a public IP address then need to edit VPC Network attached to the instance. In the *Firewall Rules* section select the rule corresponding to *tcp:22,* edit it, and add your client system IP to the *Source IP ranges* field.
9. The welcome message will show the current initialization status of the instance: 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. Software initialization takes approximately 30 minutes, this includes Oracle software installation and configuration.

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

4 After Deploying

4.1 Verifying an 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 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 the additional Oracle Clusterware patch. Please refer to Oracle Doc ID 1369107.1 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 VM.

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 VM.

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: https://support.flashgrid.io/hc/en-us/articles/4404887458327
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

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.
- 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. Trigger sending test alerts:

   ```
   $ flashgrid-node test-alerts
   ```

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

To modify the list of email alert recipients

As user *fg* on a database instance 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 system to live use (run commands as user *fg*):

1. Verify health of the instance: `$ 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 instance and back it up.
5. Start the instance and do final check of the system health: `$ flashgrid-health-check`

7 Deleting an instance

To delete an instance

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

8 Additional Documentation

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

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

Support Tiers and SLA details: https://www.flashgrid.io/docs/FlashGrid_technical_support_services.pdf

9 Contacting Technical Support

For technical help with FlashGrid Server 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.