FlashGrid® Cloud Server

for Oracle Database on AWS

Deployment Guide

rev. 21.08-2021.09.07

Table of Contents

1 Introduction

FlashGrid Cloud Server is an engineered cloud system that enables database infrastructure in public clouds. This guide provides step-by-step instructions for system and database administrators deploying FlashGrid Cloud Server with Oracle database on AWS cloud.

1.1 Key Components

Key components of FlashGrid Cloud Server 21.08 for AWS:

- FlashGrid Storage Fabric: ver. 21.08
- FlashGrid Cloud Area Network: ver. 21.08
- FlashGrid Diagnostics: ver. 21.08
- FlashGrid Health Checker ver. 21.08
- Oracle Database: ver. 19c, 18c, 12.2.0.1, 12.1.0.2, or 11.2.0.4.
- Oracle Grid Infrastructure: ver. 19c.
- Operating System: Oracle Linux 7, Red Hat Enterprise Linux 7
- Amazon EC2 instances: R5, R5B, R5D, R4, M5, M5D, M4, i3, i3en, X1, X1E, Z1D, High Memory
- Disks: EBS GP2, GP3 volumes or local SSDs

1.2 Infrastructure-as-Code Deployment

FlashGrid Cloud Server is delivered as an AWS CloudFormation template that automates configuration of multiple components required for a database. FlashGrid Cloud Server Launcher is an online tool that simplifies the deployment process by guiding through the system configuration parameters and generating CloudFormation templates.

2 Prerequisites

2.1 Required Knowledge

Working knowledge of the following AWS services is required for successful deployment of FlashGrid Cloud Server on AWS: EC2, VPC, EBS, CloudFormation, S3, IAM, Marketplace

2.2 Getting access to FlashGrid Cloud Server AMI from AWS Marketplace

To be able to create an instance, your AWS account must have an active subscription to the selected FlashGrid Cloud Server AMI. Otherwise deployment will fail when creating VM instances. The FlashGrid Cloud Server AMIs are based on either Oracle Linux 7 or RHEL 7.

To get access to the FlashGrid Cloud Server AMI

1. Open FlashGrid Cloud Server product page in AWS Marketplace:
   - Oracle Linux 7 based AMI
   - RHEL 7 based AMI
2. Click ***Continue to Subscribe*** button
3. Click ***Accept Terms*** button

Software fees charged through AWS Marketplace include FlashGrid Cloud Server software license and 24x7 Mission-Critical support plan. The fees are charged per instance and depend on the selected EC2 instance type and size. *Hourly* and *Annual* subscription models are available. Pricing information is available on the AWS Marketplace product pages – see the two links above.

2.3 Uploading Oracle installation files to S3

During instance initialization Oracle installation files will be downloaded from an S3 bucket. The list of files that must be placed in the S3 bucket will be shown by the FlashGrid Cloud Server Launcher tool. The same S3 bucket can be used for deploying multiple instances.

Two options are available for allowing access to the files in the S3 bucket for the instances:

- Enabling public access to each file for the duration of instance deployment
  OR
- Assigning the instances an IAM role that has permissions for accessing files in the bucket

To allow public access to the files in S3

1. Create an S3 bucket/folder for uploading the installation files
2. Upload the required files to the S3 bucket/folder
3. In S3 Management Console navigate to the bucket and the folder to see the list of files
4. Select all files
5. Click *More -> Make Public*
6. You can disable public access after the software completes initialization

To use an IAM role for access to the files in S3

1. Create an S3 bucket/folder for uploading the installation files
2. Upload the required files to the S3 bucket/folder
3. In *IAM Management Console* create a new policy named ***GetOracleFilesFromS3*** that allows ***s3:GetObject*** action on all uploaded files. See an example below.
4. In *IAM Management Console* create a new role named ***GetOracleFilesFromS3*** and attach the ***GetOracleFilesFromS3*** policy to it.
5. Use the ***GetOracleFilesFromS3*** role when configuring instance parameters in the FlashGrid Cloud Server Launcher tool.

Example of an IAM policy:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
          "Sid": "Stmt1508867055000",
          "Effect": "Allow",
          "Action": [
               "s3:GetObject"
           ],
           "Resource": [
                "arn:aws:s3:::mybucket/mydirectory/*"
            ]
        }
     ]
}
```

Additional information about IAM and IAM best practices is available at:

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

2.4 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 security groups. 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. You will need to provide the VPC ID in the FlashGrid Cloud Server Launcher tool and subnet ID and security group IDs in the CloudFormation Manager.

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 have to use VPC with CIDR that overlaps with 192.168.0.0/16 then please request a customized configuration file from FlashGrid Cloud Server technical support.
- The VPC has a subnet in the availability zone used for the instance.
- The VPC has an S3 endpoint configured (required unless public IPs can be enabled for access to S3)
- If you choose to enable Public IPs on the VM instance, then the VPC must have Internet Gateway configured.
- The VPC has a security group with the following ports open for inbound traffic:
  - TCP port 22 for SSH access to the instance
  - TCP port 5901 if you choose to use VNC for creating a database using DBCA in GUI mode
  - 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.

3 Deploying a FlashGrid Cloud Server Instance

The FlashGrid Cloud Server Launcher tool simplifies instance deployment in AWS by automating the following tasks:

- Creating and configuring EC2 VPC, subnet, security group (optional)
- Creating EBS volumes and launching an EC2 instance
- Installing and configuring FlashGrid Cloud Server software
- 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 AWS Management Console with a user account that has the following privileges:
    - AWSCloudFormationFullAccess
    - AmazonEC2FullAccess
    - AmazonVPCFullAccess (required only if creating a new VPC)
2. Open FlashGrid Cloud Server Launcher tool:
    - Start with one of the standard configurations at https://www.flashgrid.io/products/flashgrid-for-oracle-db-on-aws/
    - or, if you have a custom configuration file, upload it at https://2108-server.cloudprov.flashgrid.io
3. Configure parameters for the deployment
4. Click *Validate Configuration* button
5. If verification passes then click *Launch FlashGrid Cloud Server* button, which will take you to AWS CloudFormation Manager
6. Click *Next*
7. Select your SSH key
8. If using an existing VPC, then select subnet and security group.
9. Click *Next*
10. On the *Options* page:
    - If you added tags in FlashGrid Cloud Server Launcher then **do not** add the same tags in CloudFormation Manager
    - If the instance is for production use then expand the *Advanced* options and enable *Termination Protection*
11. Click *Next*
12. Click *Create*
13. Wait until the status of the stack changes to *CREATE_COMPLETE*
14. If creating the stack fails:
    a) Check for the cause of the failure on the *Events* tab
    b) Correct the cause of the error
    c) Delete the failed stack
    d) Repeat the steps for creating a new stack
15. Use EC2 Management Console to get IP addresses of the instance
16. SSH to the instance as user fg@
    Note: If you selected to create a new VPC and connecting through a public IP address then need to edit security group attached to the database nodes. In the rule for SSH allow access from your client system IP.
17. The welcome message will show the current software initialization status: in progress, failed, or completed.

18. If software initialization is still in progress then wait for it to complete. You will receive a broadcast message when software initialization completes or fails. Software initialization takes approximately 30 minutes, this includes Oracle software installation and configuration.

4 After Deploying an Instance

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 used to SSH to the VM with the SSH key that was selected when creating the instance configuration. It can also be used for running FlashGrid Storage Fabric or FlashGrid Cloud Area Network utilities. The user *fg* has sudo rights.
- *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 an instance.

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: https://support.flashgrid.io/hc/en-us/articles/1500011176122

4.4 Enabling termination protection

If termination protection was not enabled when creating the instance and if the instance is for production use then it is strongly recommended to enable termination protection:

- Enable instance termination protection
- Enable termination protection for the CloudFormation stack

4.5 Installing database software

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

4.6 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 system downtime in case of a false positive detection on a critical system file on the instance.

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

An instance is 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 Cloud Server support to review the list of required changes
2) Back up an instance: https://support.flashgrid.io/hc/en-us/articles/1500011214581
3) Implement the required changes
4) Restart the instance: https://support.flashgrid.io/hc/en-us/articles/440488745832
5) Verify health of the instance: `$ sudo flashgrid-health-check`
6) In case of errors, roll back the changes or restore the instance from backup

5 Monitoring Instance Health

The following methods of monitoring instance 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 instance 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@ 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 instance to live use:

1. Apply the latest FlashGrid, OS, and Oracle software and security updates:
   - https://support.flashgrid.io/hc/en-us/articles/4404881233943
   - https://support.flashgrid.io/hc/en-us/articles/4404886257431
   - https://support.flashgrid.io/hc/en-us/articles/4405037064855
2. Confirm that only minimally required access is allowed in the security groups used by the database server EC2 instance. Remove unnecessary access.
3. Verify health of the instance: `$ sudo flashgrid-health-check`
4. Confirm that email alerts are configured and delivered: `$ flashgrid-node test-alerts`
5. Upload diags to FlashGrid Cloud Server support: `$ sudo flashgrid-diags upload-all`
6. Stop the instance and back it up: https://support.flashgrid.io/hc/en-us/articles/1500011214581
7. Start the instance and do final check of the instance health: `$ sudo flashgrid-health-check`

7 Deleting an Instance

To delete an instance

1. Disable instance termination protection if it was enabled
2. Open AWS CloudFormation Manager console
3. Disable termination protection for the corresponding CloudFormation stack if it was enabled
4. Delete the stack corresponding to the instance
5. If any EBS volumes were added after deploying the instance, those volumes must be deleted separately
6. If any AMI images or volume snapshots were created after deploying the instance, those AMIs and snapshots must be deleted separately

8 Additional Documentation

Knowledge Base: https://support.flashgrid.io/hc/en-us/categories/1500001538061-FlashGrid-Server-on-AWS

Backup and Restore Best Practices: https://support.flashgrid.io/hc/en-us/articles/1500011214581-FlashGrid-Server-non-clustered-on-AWS-Backup-Best-Practices

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 Contacting Technical Support

For technical help with FlashGrid Cloud 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 Cloud Server 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.