FlashGrid® Cloud Cluster

for Oracle RAC on AWS

Deployment Guide

rev. 21.08-2021.09.15

Table of Contents

1 Introduction

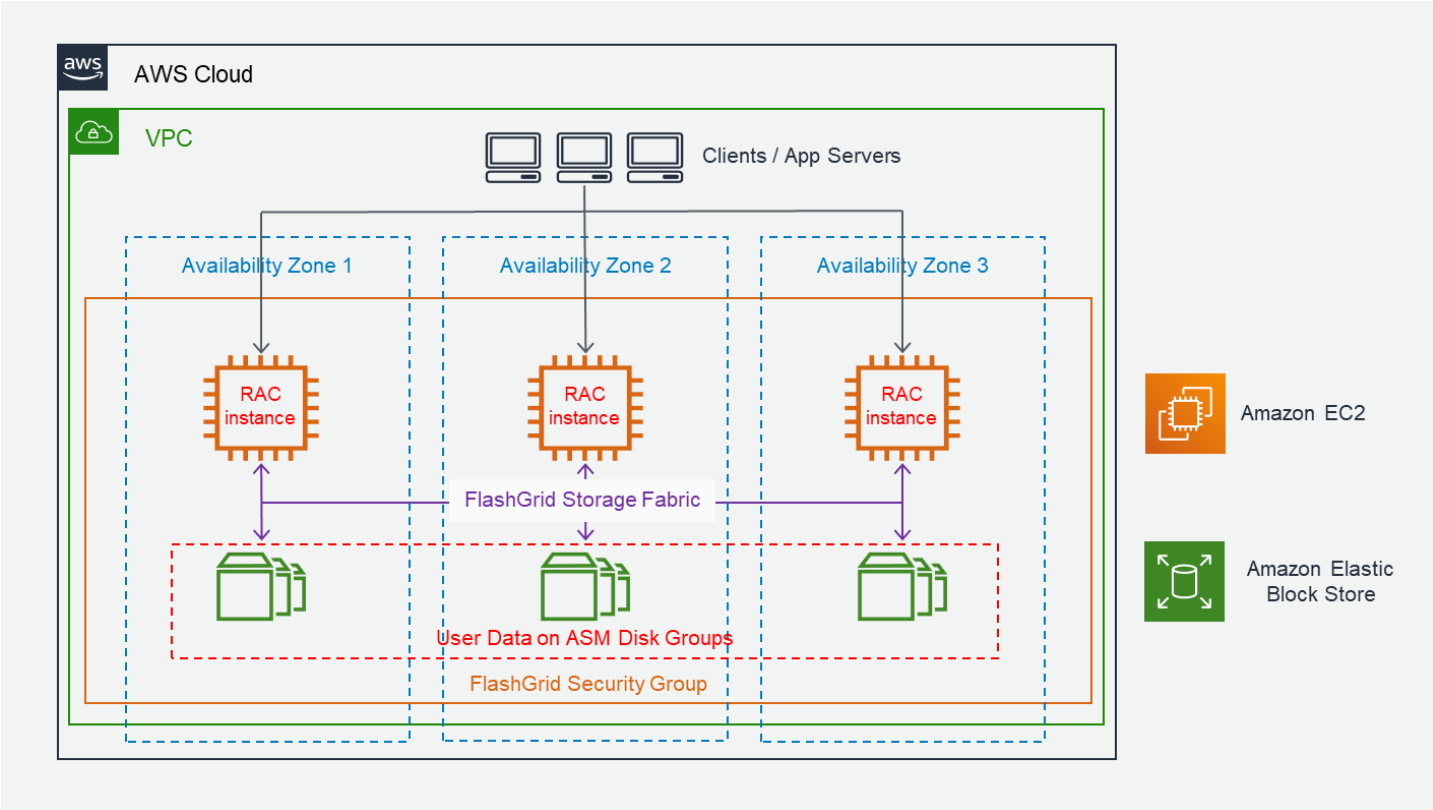
FlashGrid Cloud Cluster is an engineered cloud system that enables active-active database high availability infrastructure in public clouds. This guide provides step-by-step instructions for system and database administrators deploying FlashGrid Cloud Cluster with Oracle RAC on AWS cloud.

Additional information about the FlashGrid Cloud Cluster architecture is available in the following white paper: *"Mission-Critical Databases in the Cloud. Oracle RAC on Amazon EC2 Enabled by FlashGrid® Cloud Cluster."*

1.1 Key Components

Key components of FlashGrid Cloud Cluster 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: version 19c
- Operating System: Oracle Linux 7 or 8, Red Hat Enterprise Linux (RHEL) 7 or 8
    - Note: ACFS support with OL 8 / RHEL 8 requires the additional Oracle Clusterware patch 32848142.
- Amazon EC2 instances: r5, r5b, r5n, r4, m4, m5, m5n, c5, c5n, i3, i3en, x1, x1e, z1d, u-6tb1, u9-tb1, u12-tb1
- Disks: EBS GP3 volumes or local SSDs



FlashGrid Cloud Cluster Network Diagram

1.2 High Availability Architecture

By leveraging Oracle RAC active-active database clustering and synchronous data mirroring across nodes and AZs, FlashGrid Cloud Cluster enables near-zero (seconds) Recovery Time Objective (RTO) and zero Recovery Point Objective (RPO) in case of a failure of a single node instance, of a single EBS volume, or in case of one AZ failure.

If the cluster has 3+ database nodes, then two simultaneous database node failures can be tolerated without causing loss of database service.

Standard Oracle Client functionality provides mechanisms for application failover from a failed node, including Transparent Application Failover (TAF)

1.3 Infrastructure-as-Code Deployment

FlashGrid Cloud Cluster is delivered as an AWS CloudFormation template that automates 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 CloudFormation templates.

2 Prerequisites

2.1 Required Knowledge

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

2.2 Getting access to FlashGrid Cloud Cluster AMI from AWS Marketplace

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

To get access to the FlashGrid Cloud Cluster AMI

1. Open FlashGrid Cloud Cluster product page in AWS Marketplace:
   - Oracle Linux 7 based AMI
   - Oracle Linux 8 based AMI
   - RHEL 7 based AMI
   - RHEL 8 based AMI
2. Click ***Continue*** button
3. Select ***Manual Launch*** tab
4. Click ***Accept Software Terms*** button

Software fees charged through AWS Marketplace include FlashGrid Cloud Cluster software license and 24x7 Mission-Critical support plan. The fees are charged per cluster node 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 cluster 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 Cluster Launcher tool. The same S3 bucket can be used for deploying multiple clusters.

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

- Enabling public access to each file for the duration of cluster deployment
  OR
- Assigning the cluster node 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 cluster 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 cluster parameters in the FlashGrid Cloud Cluster 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 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, placement group(s), and security groups. 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. You will need to provide the VPC ID in the FlashGrid Cloud Cluster Launcher tool and subnet IDs 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 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 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 each of the availability zones used for the cluster nodes.
- 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 instances, then the VPC must have Internet Gateway configured.
- The VPC has a security group with the following ports open for inbound traffic:
  - 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 the FlashGrid Cloud Cluster Launcher tool.
  - 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
  - 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 Cluster

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

- Creating and configuring EC2 VPC, subnets, security group (optional)
- Creating EBS volumes and launching EC2 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 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 Cluster Launcher tool:
    - Start with one of the standard configurations at https://www.flashgrid.io/products/flashgrid-for-oracle-rac-on-aws
    - or, if you have a custom configuration file, upload it at https://2108-cluster.cloudprov.flashgrid.io/
3. Configure parameters of the cluster
4. Click *Validate Configuration* button
5. If verification passes then click *Launch Cluster* 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(s), and a security group.
9. Click *Next*
10. On the *Options* page:
    - If you added tags in FlashGrid Cloud Cluster Launcher, then **do not** add the same tags in CloudFormation Manager
    - If the cluster 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 cluster node instances
16. SSH to the first (as it was specified on the cluster configuration page) cluster node 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 initialization status of the cluster: in progress, failed, or completed.

18. 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 used to SSH to the VMs with the SSH key that was selected when creating the cluster 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 (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

4.4 Enabling termination protection

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

- Enable instance termination protection for each cluster node instance.
- Enable termination protection for the CloudFormation stack.

4.5 Installing database software (RAC One Node or additional database home)

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

4.6 Use of anti-virus 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.

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

Cluster nodes are deployed using RHEL or Oracle Linux 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://support.flashgrid.io/hc/en-us/articles/1500011214461
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: `$ 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. Apply the latest FlashGrid, OS, and Oracle software and security updates:
   - https://support.flashgrid.io/hc/en-us/articles/4405044508695-Updating-FlashGrid-software-and-Linux-kernel-using-FlashGrid-Cloud-Cluster-Node-Update-package
   - https://support.flashgrid.io/hc/en-us/articles/4405037723415-Updating-OS
   - https://support.flashgrid.io/hc/en-us/articles/4405037064855-Applying-Grid-Infrastructure-and-Database-patches
2. Confirm that only minimally required access is allowed in the security groups used by the cluster node instances. Remove unnecessary access.
3. Verify health of the cluster: `$ sudo flashgrid-health-check`
4. Confirm that email alerts are configured and delivered: `$ flashgrid-node test-alerts`
5. Upload diags to FlashGrid support: `$ sudo flashgrid-diags upload-all`
6. Stop the cluster and back up all cluster nodes: https://support.flashgrid.io/hc/en-us/articles/4404887221655-Shutting-down-entire-cluster
7. 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 instance termination protection for each cluster node 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 cluster.
5. If any EBS volumes were added after deploying the cluster, those volumes must be deleted separately.
6. If any AMI images or volume snapshots were created after deploying the cluster, those AMIs and snapshots must be deleted separately.

8 Additional Documentation

Knowledge Base: https://support.flashgrid.io/hc/en-us/categories/1500001538041-FlashGrid-Cluster-on-AWS

Backup and Restore Best Practices on AWS: https://support.flashgrid.io/hc/en-us/articles/1500011214461

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 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.