FlashGrid® Cloud Server

for Oracle Database on Azure

Deployment Guide

rev. 20.10-2020.12.30

Table of Contents

1 Introduction

FlashGrid Cloud Server 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 Server with Oracle Database on Azure cloud.

Key components of FlashGrid Cloud Server 20.09 for Azure:

- 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
- Operating System: Oracle Linux 7, Red Hat Enterprise Linux 7
- Azure VMs: DSv2, DSv3, ESv3, DSv4, ESv4, M, GS, Ls_v2.
- Disks: Premium SSD or local NVMe SSD

FlashGrid Cloud Server is delivered as Azure Resource Manager templates that automate 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 software configuration parameters and generating Azure Resource Manager templates.

2 Prerequisites

The following prerequisites are required for automated deployment of an Oracle Database system in Azure using FlashGrid Cloud Server Launcher:

- **Azure Storage Blob Container** with Oracle installation files that will be downloaded to the system during software initialization. The list of files that must be placed in the Storage Container will be shown in FlashGrid Cloud Server Launcher. The corresponding storage account must have access for *'All networks'* enabled in *'Firewall and virtual networks'* settings.
- **Enabled Service Endpoints** when deploying in an existing VNet. Enabling service endpoints allows access to the storage container from the VM. If Service Endpoints are disabled and public IPs not assigned, then software initialization will fail because downloading Oracle files from the VM will not be possible.
- **Azure subscription with sufficient quotas** for creating the required VM type and sufficient number and size of Premium Managed Disks.
- **SSH key pair** that will be used for accessing the VM. Use of passwords instead of the key pair is not supported. To create a new key pair use *ssh-keygen* in Linux or *puttygen* in Windows. In the FlashGrid Cloud Server Launcher tool you will need to provide the public key that will be placed on the VM. Example of a valid public key pair format:

  ```
  ssh-rsa <PublicKeyBody>
  ```

3 Deploying a FlashGrid Cloud Server on Azure

The FlashGrid Cloud Server Launcher tool simplifies provisioning of Oracle Database system in Azure by automating the following tasks:

- Creating cloud infrastructure: VM, storage, and optionally network
- Installing and configuring FlashGrid Cloud Server software
- Installing, configuring, and patching Oracle Grid Infrastructure
- Installing and patching Oracle Database software
- Creating ASM disk groups

To create a VM

1. Open FlashGrid Cloud Server Launcher tool:
    - Start with one of the standard configurations at https://flashgrid.io/skybase-for-oracle-on-azure/
    - or, if you have a custom configuration file, upload it at https://2010-skybase.cloudprov.flashgrid.io
2. Configure parameters for the deployment
3. Click *Validate Configuration* button
4. If verification passes then click *Launch FlashGrid Cloud Server* button, which will take you to Azure Resource Manager
5. Select *Resource group -> Create new*. By having the system in a separate resource group you can later delete all infrastructure by simply deleting the resource group.
6. Enter a name for the new resource group that will contain the infrastructure. A name matching the system name is recommended.
7. Select your target location (region)
8. Check *'I agree to the terms and conditions state above'*
9. Click *Purchase*
10. Open list of Notifications (bell icon) and click *'Deployment in progress…'*
11. Wait until the deployment status changes to *Succeeded*
12. If the deployment fails:
    a) Check for the cause of the failure in the *Operation details*
    b) Correct the cause of the error
    c) Delete the failed resource group
    d) Repeat the steps for creating a new resource group
13. SSH to the VM as user ***az-admin@***
14. The welcome message will show the current software initialization status: in progress, failed, or completed.
15. If software 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.

4 After Deploying

4.1 Verifying the status

On the VM run `flashgrid-health-check` command to verify that the status is *Good* and all checks are passing.

```
[az-admin@myhostname ~]$ sudo flashgrid-health-check
HealthCheck 20.9.1.51823.test #43fdf490ae61edb4febd0f6f378fb56dfc6a3036
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Check: ASM DiskGroup status
   myhostname: OK
      ------------------------------------------------------------------------------------------------------------
      GroupName  Status  Mounted   Type    TotalMiB  FreeMiB  OfflineDisks  LostDisks  Resync  ReadLocal  Vote
      ------------------------------------------------------------------------------------------------------------
      DATA       Good    AllNodes  EXTERN  11264     11172    0             0          No      Enabled    N/A
      FRA        Good    AllNodes  EXTERN  12288     12196    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: 32.8%

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 67%, /: avail 95%

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 Verifying synchronization of clocks

Chrony service is used for synchronizing a VM clock with external NTP servers. Without active clock synchronization service the clocks are likely to get out of sync.

To check status of CHRONYD service

```
$ sudo chronyc sources
```

Example:

```
[az-admin@myhostname ~]$ sudo chronyc sources
210 Number of sources = 4
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* time1.google.com              1   6   177    58  -2383us[-4178us] +/-   12ms
^+ time2.google.com              1   6   177    58   -164us[ -164us] +/-   12ms
^+ time3.google.com              1   6   177    58  -1798us[-1798us] +/-   11ms
^+ time4.google.com              1   6   177    57   -165us[ -165us] +/- 9051us
```

Note that the '*' character shows which NTP server is currently used for synchronization. Normally this should be one of the external NTP servers. If it shows that VM is used for synchronization, then this means that the external NTP servers are not accessible.

Public NTP servers, e.g. *timeX.google.com*, can be used only if public IPs are enabled on the VM (not recommended in production use for security reasons) or if NAT is configured in the network. If needed, the list of NTP servers can be modified in `/etc/chrony.conf` after the software is configured.

4.3 OS user accounts

During software initialization the following OS user accounts are created:

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

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.

Users *az-admin* and *fg* have sudo rights and allows switching to any other user without requiring a password (which is not configured by default). Example:

```
$ sudo su - grid
```

4.4 Finalizing system 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

4.5 Adding a protection lock

It is strongly recommended to add a lock to the resource group to protect it against accidental deletion or modification.

4.6 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.

4.7 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 downtime in case of a false positive detection on a critical system file on the VM.

4.8 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.

4.9 Security hardening

The system 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 support to review the list of required changes
2) Back up the system: https://kb.flashgrid.io/backup-restore/backup-and-restore-skybase-for-oracle-on-azure
3) Implement the required changes
4) Restart the system: https://kb.flashgrid.io/maintenance/maintenance-skybase-for-oracle-on-azure
5) Verify health of the system: `$ sudo flashgrid-health-check`
6) In case of errors, roll back the changes or restore the system from backup

5 Monitoring FlashGrid Cloud Server 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. On all nodes (including quorum node) run

   $ `flashgrid-node test-alerts`

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

To modify the list of email alert recipients

As user az-admin@ 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 to live use:

1. Verify health of the VM: `$ sudo flashgrid-health-check`
2. Confirm that email alerts are configured and delivered: `$ flashgrid-node test-alerts`
3. Upload diags to FlashGrid Cloud Server support: `$ sudo flashgrid-diags upload-all`
4. Stop the VM and back it up: https://kb.flashgrid.io/backup-restore/backup-and-restore-skybase-for-oracle-on-azure
5. Start the VM and do a final health check: `$ sudo flashgrid-health-check`

7 Deleting a System

To delete a system

1. Delete any protection lock(s) for the resource group
2. Delete the resource group corresponding to the system

8 Additional Documentation

Maintenance Tasks in Azure: https://kb.flashgrid.io/maintenance/maintenance-skybase-for-oracle-on-azure

Backup and Restore Best Practices in Azure: https://kb.flashgrid.io/backup-restore/backup-and-restore-skybase-for-oracle-on-azure

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 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:

```
$ 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.