



flashgrid

FlashGrid[®] Server for Oracle Database on Azure

Deployment Guide

rev. 24.11-2024.12.10

Table of Contents

- 1 Introduction 3
- 2 Prerequisites 3
- 3 Deploying FlashGrid Server 4
- 4 After Deploying 5
 - 4.1 Verifying the status 5
 - 4.2 Verifying synchronization of clocks 5
 - 4.3 OS user accounts 6
 - 4.4 Finalizing system configuration 6
 - 4.5 Adding a protection lock 6
 - 4.6 Installing an additional database home 6
 - 4.7 Use of anti-virus and other third-party software 7
 - 4.8 Use of automatic configuration tools 7
 - 4.9 Security hardening 7
- 5 Monitoring FlashGrid Server Health 8
- 6 Before Going Live 8
- 7 Deleting a System 9
- 8 Additional Documentation 9
- 9 Contacting Technical Support 9

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 Azure cloud.

Key components of FlashGrid Server on Azure:

- FlashGrid Storage Fabric software
- FlashGrid Cloud Area Network software
- FlashGrid Diagnostics software
- FlashGrid Health Checker 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:** 7, 8, or 9
 - **Red Hat Enterprise Linux:** (RHEL) 8, or 9
- Azure VMs:
 - **General purpose:** Dsv5
 - **Memory optimized:** Ebsv5, Esv5, Mbsv3, Msv3
- Disks: Premium SSD, Premium SSD v2

FlashGrid Server is delivered as Azure Resource Manager templates that automate configuration of multiple components required for a database. FlashGrid 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 a FlashGrid Server:

- **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 Launcher. The corresponding storage account must have access for *'All networks'* enabled in *'Firewall and virtual networks'* settings.
- **Microsoft.Storage** service endpoint configured for the VNet. Having the storage service endpoint allows access to the storage container from the VM. If Microsoft.Storage service endpoint is not added, and a public IP is not assigned then system 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 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 FlashGrid Server

The FlashGrid 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 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 Launcher tool:
 - Start with one of the standard configurations at <https://www.flashgrid.io/products/flashgrid-for-oracle-db-on-azure>
 - or, if you have a custom configuration file, upload it at <https://2411.cloudprov.flashgrid.io/upload>
2. Configure parameters for the deployment
3. Click *Validate Configuration* button
4. If verification passes then click *Launch FlashGrid* 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. If you did not provide an SSH key, select *Use existing key stored in Azure in SSH public key source* and specify a stored key.
9. Check *'I agree to the terms and conditions state above'*
10. Click *Purchase*
11. Open list of Notifications (bell icon) and click *'Deployment in progress...'*
12. Wait until the deployment status changes to *Succeeded*
13. 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
14. SSH to the VM as user *az-admin*
15. The welcome message will show the current software initialization status: in progress, failed, or completed.
16. 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.

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 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. Creating a database: <https://support.flashgrid.io/hc/en-us/articles/1500011215081>
2. Connecting clients: <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.

4.5 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 an additional database home

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 and other third-party 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.

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 Linux. 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.

4.8 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 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 the system: <https://support.flashgrid.io/hc/en-us/articles/1500011175562-FlashGrid-Server-non-clustered-on-Azure-Backup-Best-Practices>
- 3) Implement the required changes
- 4) Restart the system: <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 FlashGrid 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 as user *fg*:

```
$ 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 *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 to live use (run commands as user *fg*):

1. Verify health of the VM: `$ 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 VM and back it up: <https://support.flashgrid.io/hc/en-us/articles/1500011175562-FlashGrid-Server-non-clustered-on-Azure-Backup-Best-Practices>
5. Start the VM and do a final health check: `$ 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

Knowledge Base: <https://support.flashgrid.io/hc/en-us/categories/1500001538081-FlashGrid-Server-on-Azure>

Backup and Restore Best Practices in Azure: <https://support.flashgrid.io/hc/en-us/articles/1500011175562>

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 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.

Copyright © 2016-2024 FlashGrid Inc. All rights reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document.

FlashGrid is a registered trademarks of FlashGrid Inc. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Red Hat is a registered trademark of Red Hat Inc. Microsoft and Azure are registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.