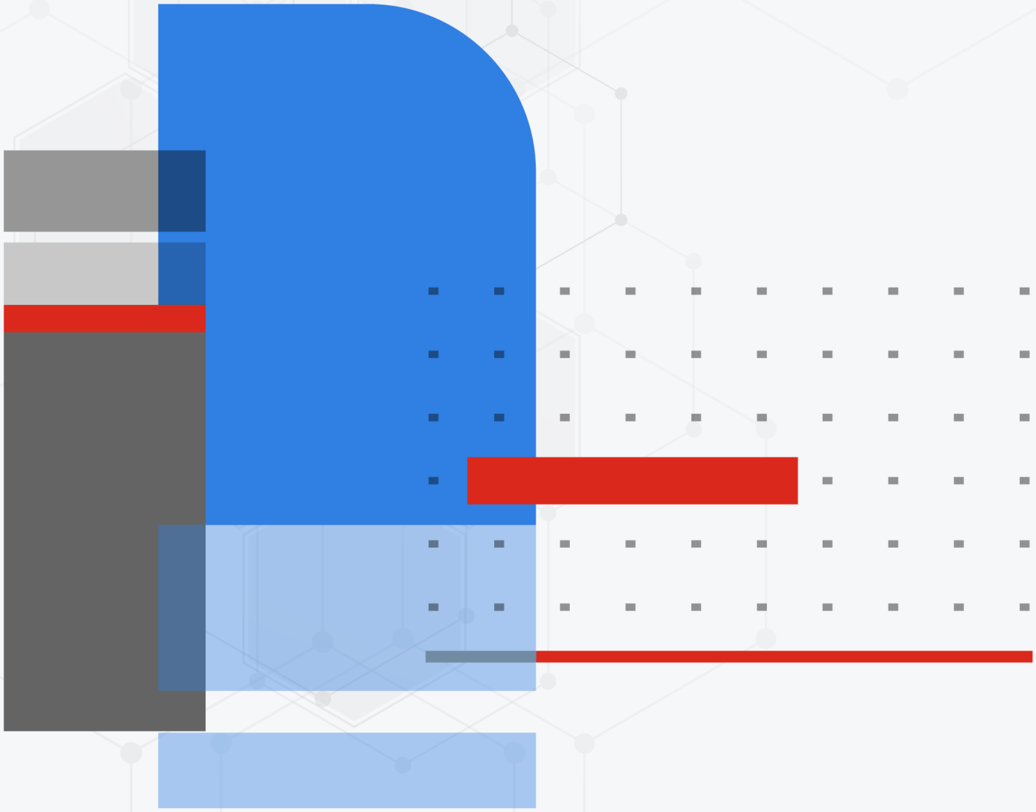
GCP Administration Guide

FortiAnalyzer 7.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 18, 2025
FortiAnalyzer 7.4 GCP Administration Guide
05-740-910387-20251218

TABLE OF CONTENTS

About FortiAnalyzer for GCP

FortiAnalyzer-VM for GCP delivers centralized logging, analytics, and reporting features. As a GCP VM instance, FortiAnalyzer allows you to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location to get a simplified, consolidated view of your security position. In addition, you will have detailed data capture for forensic purposes to comply with policies regarding privacy and security breach disclosures.

Highlights of FortiAnalyzer for GCP include the following:

- Graphical summary reports provide network-wide reporting of events, activities, and trends occurring on FortiAnalyzers and third-party devices.
- Network event correlation enables IT administrators to quickly identify and react to security threats across the network.
- Scalable performance and capacity supports thousands of FortiAnalyzers and can dynamically scale storage based on retention and compliance requirements.
- Choice of standalone, collector, or analyzer mode allows deployment of individual instances or optimization for specific operations, such as store and forward or analytics.
- Seamless integration with the Fortinet product portfolio enables tight integration to allow FortiAnalyzer resources to be managed from FortiGate or FortiManager user interfaces.

When deploying Fortinet products on a cloud platform, it is critical to understand that you are responsible for all costs incurred from the resources you use. This includes but is not limited to the following: CPU, memory, storage volumes, snapshots, data transfers, and network bandwidth.

Once your deployment is live, services may automatically generate temporary files, system logs, or additional volumes and snapshots. These can consume disk space and lead to unexpected charges.

To avoid surprise costs, it is your responsibility to do the following:

- Regularly check which services and features are active in your cloud environment.
- Monitor disk usage and be aware of what triggers new volume or snapshot creation.
- Set appropriate usage limits, quotas, and budget alerts.
- Configure disk space threshold alarms and act promptly when notified.

Each cloud provider has different tools for managing and monitoring these settings. Refer to GCP’s documentation to configure alerts, budgets, and usage controls appropriately.

Machine type support

You can deploy FortiAnalyzer for GCP as VM instances. Supported machine types may change without notice. Currently FortiAnalyzer supports standard machine types, high memory machine types, and high CPU machine types with minimum 2 vCPUs and 7.5 GB of RAM and maximum 96 vCPUs and 624 GB of RAM in the predefined machine type lineup. You can also customize the combination of vCPU and RAM sizes within this range. You can find more details on predefined machine types here.

Starting in 7.2.2, the minimum recommended VM configuration is increased to 16GB memory and 4 vCPU.

Latest supported machine types can be seen under machine type selection if you try to launch FortiAnalyzer from the marketplace listing or Compute Engine portal.

Models

FortiAnalyzer-VM is licensed based on the amount of logging per day and storage capacity. Refer to price lists and order SKUs available through your resellers/distributors. These are also referred to as bring your own license (BYOL) models.

FortiAnalyzer-VM can be deployed using different CPU and RAM sizes and launched on various private and public cloud platforms.

Licensing

You must have a license to deploy FortiAnalyzer for GCP. The following sections provide information on licensing FortiAnalyzer for GCP:

- Order types on page 5
- Creating a support account on page 6
- Registering and downloading licenses on page 6

Order types

FortiAnalyzer for GCP supports only Bring Your Own License (BYOL). There is no Pay As You Go/On-Demand (PAYG) subscription available yet.

BYOL is annual perpetual licensing, as opposed to PAYG, which is an hourly subscription available with marketplace-listed products. BYOL licenses are available for purchase from resellers or your distributors, and prices are listed in the publicly available price list that is updated quarterly. BYOL licensing provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

Creating a support account

FortiAnalyzer-VM for GCP supports BYOL licensing models.

For BYOL, you typically order a combination of products and services, including support entitlement.

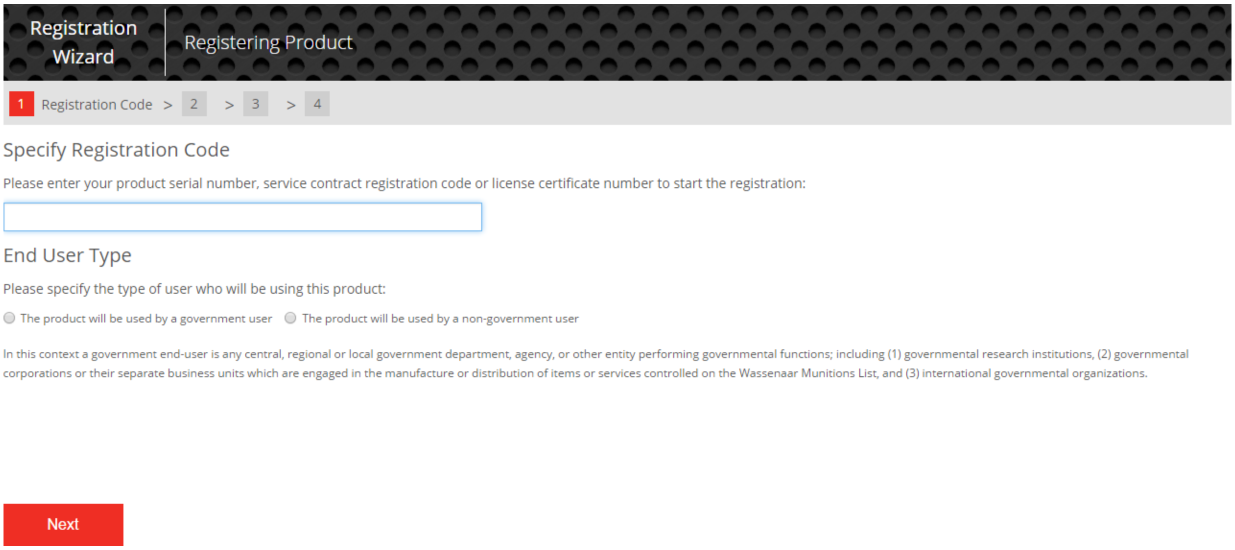
You must create a FortiCare support account and obtain a license to activate the product through the FortiCare support portal. If you have not activated the license, you will see the license upload screen when logging into the FortiAnalyzer and cannot proceed to configure the FortiAnalyzer. See Registering and downloading licenses on page 6.

Registering and downloading licenses

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. If you don't have a partner, contact gcpsales@fortinet.com for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license, you will receive a PDF with an activation code.

1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. Go to *Asset > Register/Renew* to start the registration process.



Specify Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration:

End User Type

Please specify the type of user who will be using this product:

○ The product will be used by a government user ○ The product will be used by a non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

3. In the *Specify Registration Code* field, enter your license activation code, then select *Next* to continue registering the product.
4. Enter your details in the other fields as required.
5. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiAnalyzer-VM.
   After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiAnalyzer-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Deploying FortiAnalyzer on GCP

Deploying a FortiAnalyzer on GCP consists of the following steps:

1. FortiAnalyzer-VM marketplace deployment on page 7
2. Registering and downloading your license on page 13
3. Connecting to the FortiAnalyzer-VM on page 14
4. Adding a disk to the FortiAnalyzer-VM for logging on page 15

FortiAnalyzer-VM marketplace deployment

FortiAnalyzer-VM requires a minimum disk size of 500GB.

Deleting the FortiAnalyzer-VM instance after deployment does not delete the log disk. However, deleting the entire deployment from the Solution Deployment section deletes all resources that the deployment created, including the log disk.

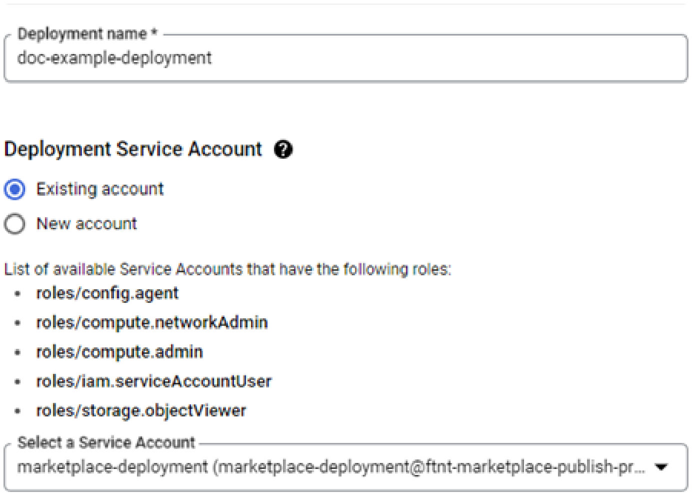
Do not rerun a broken deployment. Terraform state lock is enabled by default and you cannot disable it from the marketplace GUI. Delete the broken deployment and create a new deployment instead.

To prepare a service account:

For information about creating a service account, see Create service accounts in the Google Cloud documentation.

Deploying a FortiAnalyzer-VM requires the following permissions and roles:

- roles/config.agent
- roles/compute.networkAdmin
- roles/compute.admin
- roles/iam.serviceAccountUser
- roles/storage.objectViewer



Deployment name *
doc-example-deployment

Deployment Service Account

● Existing account
○ New account

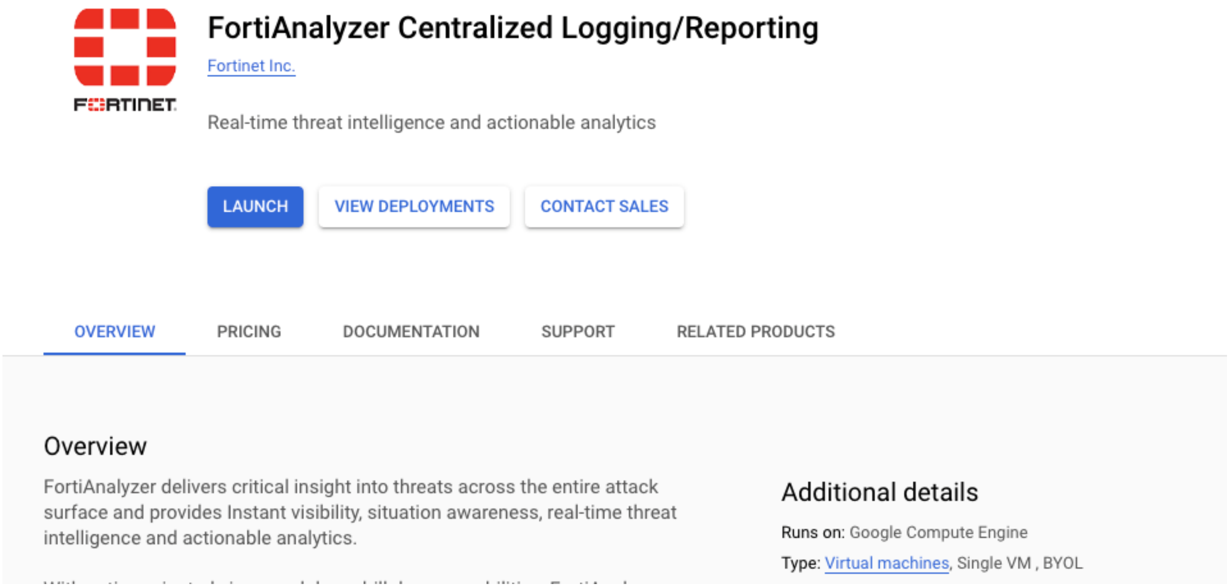
List of available Service Accounts that have the following roles:

- roles/config.agent
- roles/compute.networkAdmin
- roles/compute.admin
- roles/iam.serviceAccountUser
- roles/storage.objectViewer

Select a Service Account
marketplace-deployment (marketplace-deployment@ftnt-marketplace-publish-pr...

To perform initial deployment of the FortiAnalyzer-VM:

1. In Google Cloud Marketplace, find *FortiAnalyzer Centralized Logging/Reporting*.



FortiAnalyzer Centralized Logging/Reporting

Fortinet Inc.

Real-time threat intelligence and actionable analytics

Overview

FortiAnalyzer delivers critical insight into threats across the entire attack surface and provides Instant visibility, situation awareness, real-time threat intelligence and actionable analytics.

Additional details

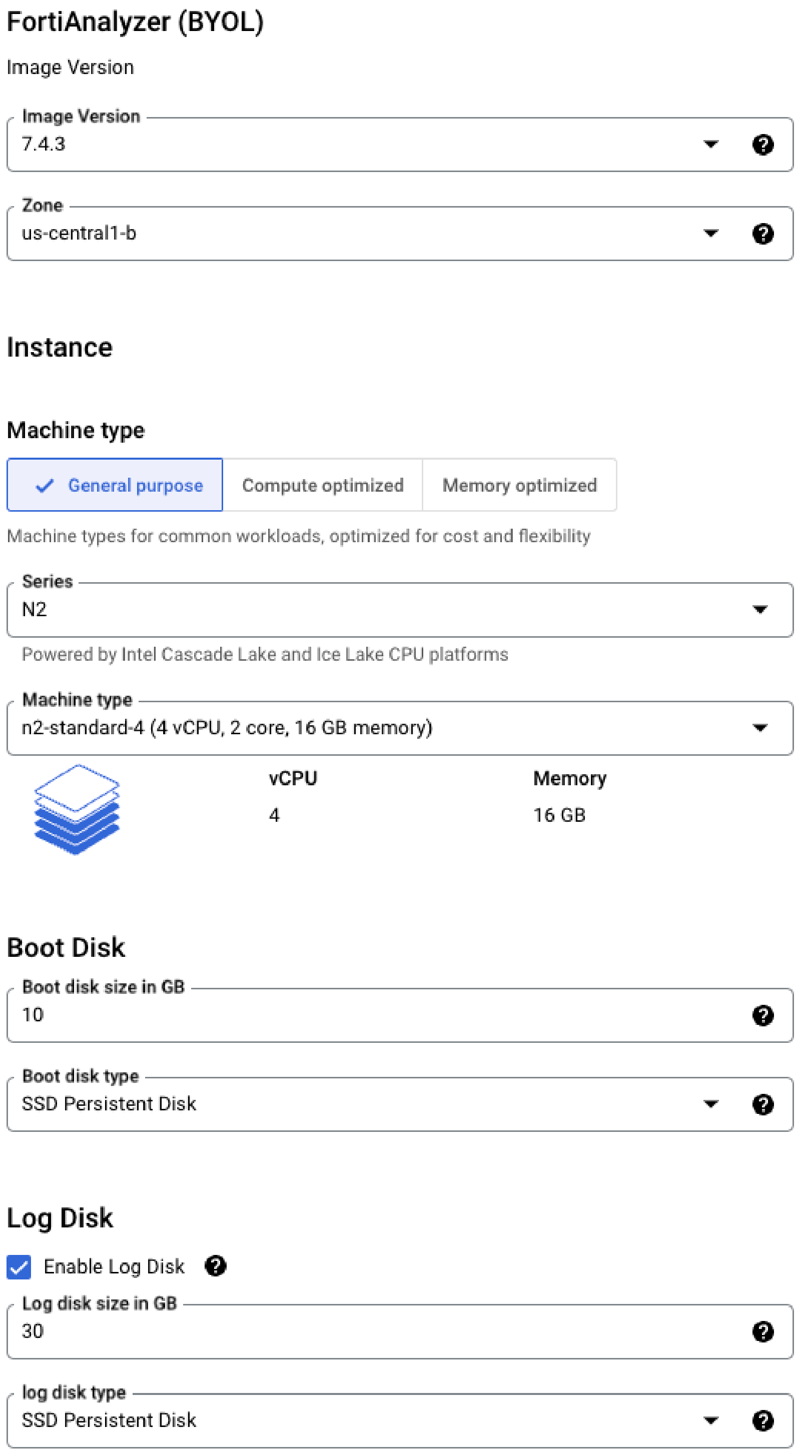
Runs on: Google Compute Engine

Type: Virtual machines, Single VM , BYOL

2. Click *LAUNCH*.
3. Configure the variables as required:

Deployment name	Enter the name of the FortiAnalyzer-VM to appear in the Compute Engine portal.
Deployment Service Account	Select *Existing account*.
Image Version	Select the FortiAnalyzer version. The latest version is the default.
Instance	

Zone	Select the zone to deploy the FortiAnalyzer to.
Machine type	Select the required instance type.
Boot Disk	
Boot disk size in GB	Leave as-is at 10 GB. Note you must add additional disks for logging in later steps.
Boot disk type	Select the boot disk type.
Log Disk	
Enable Log Disk	Enable *Enable Log Disk*.
Log disk size in GB	Enter the desired log disk size. The minimum system requirement is 500 GB. To add additional disks for logging in later steps, see Adding a disk to the FortiAnalyzer-VM for logging on page 15.
Log disk type	Select the log disk type.
Networking Currently, the Cloud Launcher solution supports one network interface.	
Network	Select the network located in the selected zone.
Subnetwork	Select the subnet where the FortiAnalyzer resides.
External IP	Select *Ephemeral*. You will need to access the FortiAnalyzer management GUI via this public IP address.
Firewall	Leave all options selected, or allow at least HTTPS traffic if the strictest security is allowed in your network as the first setup. You can change firewall settings later, as needed.
Enable IP Forward	Enable the VM to forward packets.



FortiAnalyzer (BYOL)

Image Version

Image Version: 7.4.3

Zone: us-central1-b

Instance

Machine type

☑ General purpose | Compute optimized | Memory optimized

Machine types for common workloads, optimized for cost and flexibility

Series: N2

Powered by Intel Cascade Lake and Ice Lake CPU platforms

Machine type: n2-standard-4 (4 vCPU, 2 core, 16 GB memory)

vCPU	Memory
4	16 GB

Boot Disk

Boot disk size in GB: 10

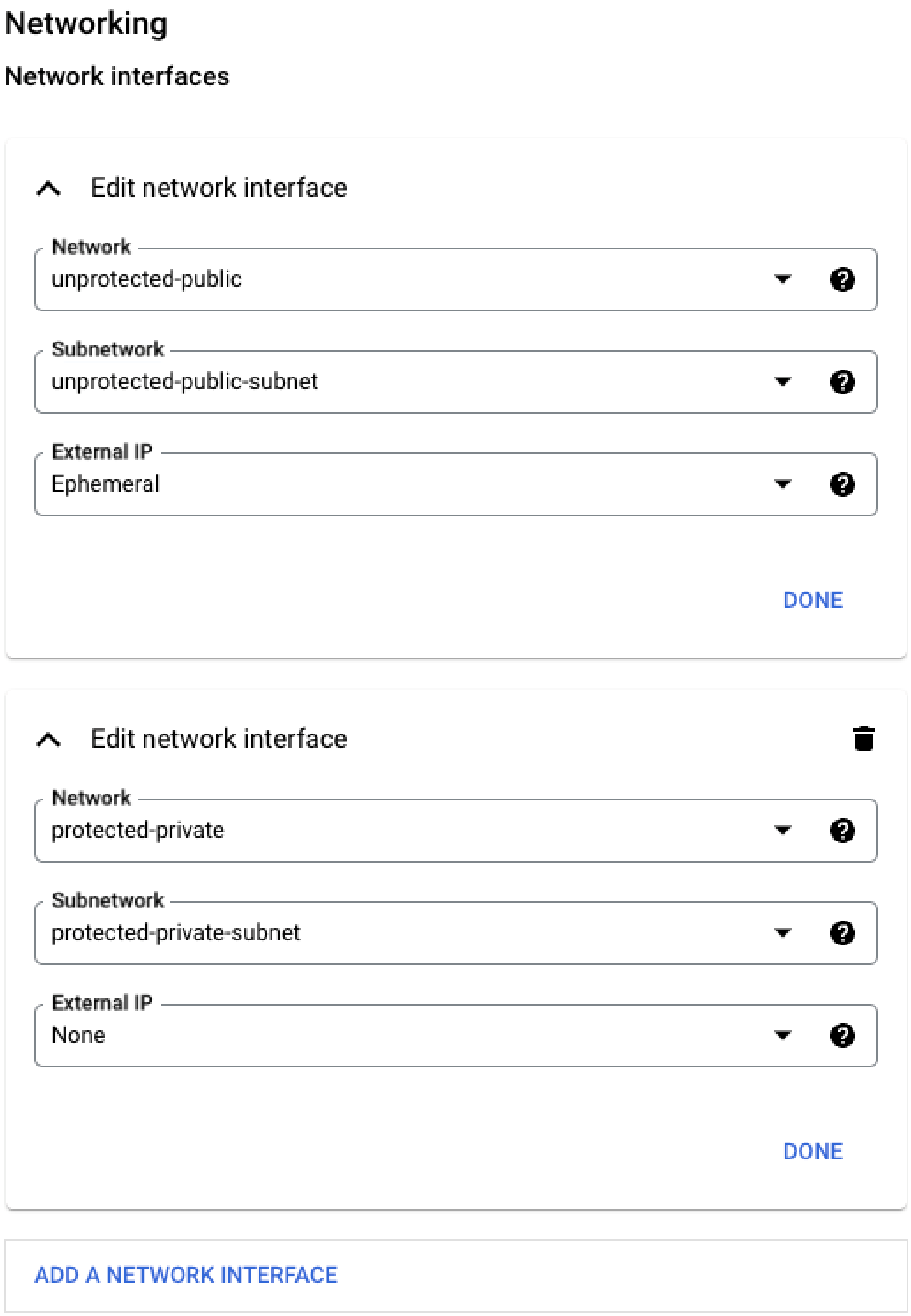
Boot disk type: SSD Persistent Disk

Log Disk

☑ Enable Log Disk

Log disk size in GB: 30

log disk type: SSD Persistent Disk



Networking

Network interfaces

Edit network interface

Network: unprotected-public

Subnetwork: unprotected-public-subnet

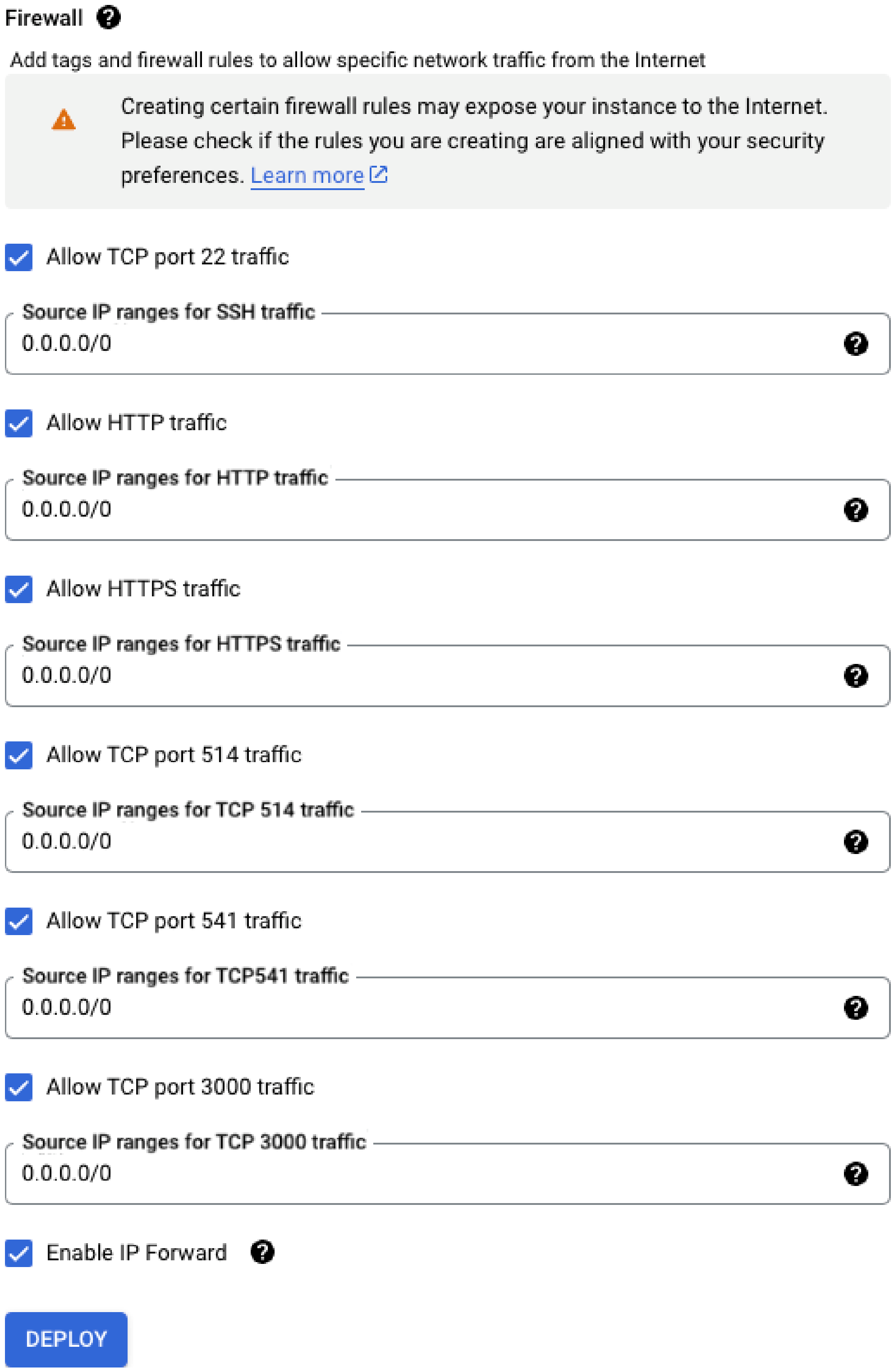
External IP: Ephemeral

Edit network interface

Network: protected-private

Subnetwork: protected-private-subnet

External IP: None



Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

Creating certain firewall rules may expose your instance to the Internet. Please check if the rules you are creating are aligned with your security preferences. Learn more

☑ Allow TCP port 22 traffic

Source IP ranges for SSH traffic: 0.0.0.0/0

☑ Allow HTTP traffic

Source IP ranges for HTTP traffic: 0.0.0.0/0

☑ Allow HTTPS traffic

Source IP ranges for HTTPS traffic: 0.0.0.0/0

☑ Allow TCP port 514 traffic

Source IP ranges for TCP 514 traffic: 0.0.0.0/0

☑ Allow TCP port 541 traffic

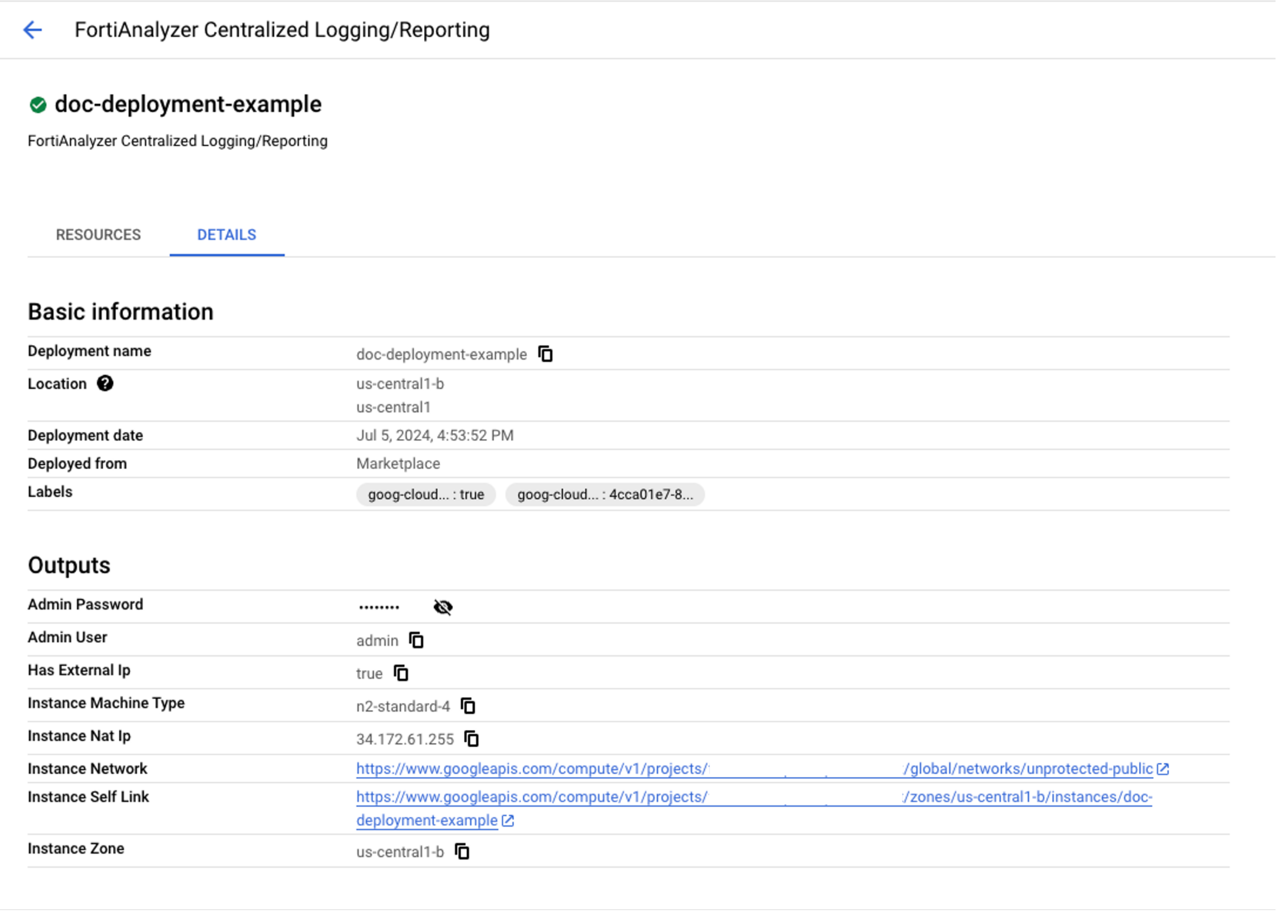
Source IP ranges for TCP541 traffic: 0.0.0.0/0

☑ Allow TCP port 3000 traffic

Source IP ranges for TCP 3000 traffic: 0.0.0.0/0

☑ Enable IP Forward

4. Click *Deploy*. When deployment is complete, the screen appears as below.



FortiAnalyzer Centralized Logging/Reporting

doc-deployment-example

FortiAnalyzer Centralized Logging/Reporting

Basic information

Deployment name	doc-deployment-example
Location	us-central1-b us-central1
Deployment date	Jul 5, 2024, 4:53:52 PM
Deployed from	Marketplace
Labels	goog-cloud... : true goog-cloud... : 4cca01e7-8...

Outputs

Admin Password	••••••••
Admin User	admin
Has External Ip	true
Instance Machine Type	n2-standard-4
Instance Nat Ip	34.172.61.255
Instance Network	https://www.googleapis.com/compute/v1/projects/ /global/networks/unprotected-public
Instance Self Link	https://www.googleapis.com/compute/v1/projects/ /zones/us-central1-b/instances/doc-deployment-example
Instance Zone	us-central1-b

Registering and downloading your license

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. If you don't have a partner, contact gcpsales@fortinet.com for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license (60-day term), you will receive a PDF with an activation code.

To register and download your license:

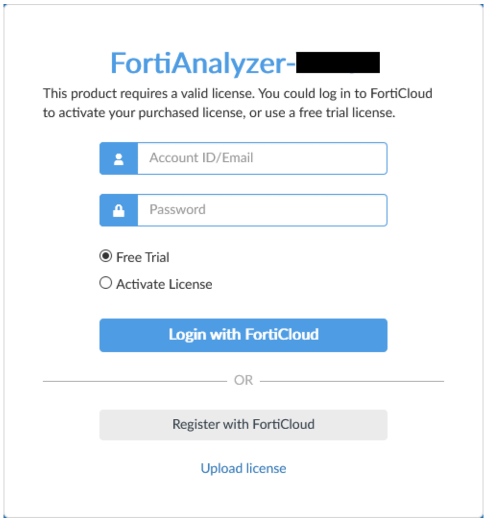
1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. In *Asset Management*, click *Register Product*, or click the *Register More* button.
3. Enter your registration code, and confirm the other details required for registration including your end user type.
4. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiAnalyzer-VM.

After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiAnalyzer-VM, if you get an error that the license is invalid, wait 30 minutes and try again.
For more information, see the FortiCloud Asset Management Administration Guide.

Connecting to the FortiAnalyzer-VM

To activate a license for FortiAnalyzer VM:

1. Connect to the FortiAnalyzer using your browser.
   The login dialog box is displayed.



FortiAnalyzer-[redacted]

This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license.

● Free Trial
○ Activate License

2. Take one of the following actions:

Action	Description
Free Trial	If a valid license is not associated with the account, you can start a free trial license. **1.** Select *Free Trial*, and click *Login with FortiCloud*. **2.** Use your FortiCloud account credentials to log in, or create a new account. FortiAnalyzer connects to FortiCloud to get the trial license. The system will restart to apply the trial license. **3.** Read and accept the license agreement. For more information, see the *FortiAnalyzer 7.4 VM Trial License Guide*.
Activate License	If you have a license file, you can activate it . **1.** Select *Activate License*, and click *Login with FortiCloud*. **2.** Use your FortiCloud account credentials to log in. FortiAnalyzer connects to FortiCloud, and the license agreement is displayed. **3.** Read and accept the license agreement.
Upload License	**1.** Click *Browse* to upload the license file, or drag it onto the field.

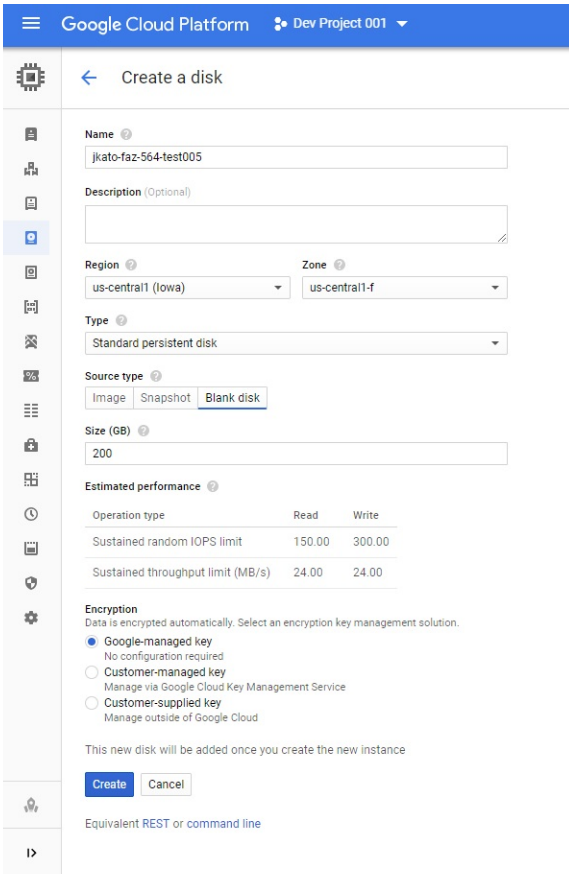
Action	Description
	2. Click *Upload*. After the license file is uploaded, the system will restart to verify it. This may take a few moments. To download the license file, go to the Fortinet Technical Support site (https://support.fortinet.com/), and use your FortiCloud credentials to log in. Go to *Asset Managmeent* > *Products* > *Product List*, then click the product serial number.

3. Once registration is complete, log into the FortiAnalyzer-VM with the username *admin* and the supplied temporary password. From the previous step, there is a temporary admin password automatically generated on the Google Cloud.

Adding a disk to the FortiAnalyzer-VM for logging

You are required to add another disk to store logs.

1. Log into the GCP Compute Engine.
2. Go to the *Disks* page.
3. Create a blank disk in the same zone where the FortiAnalyzer-VM resides. Disk size varies depending on the license.



Create a disk

Name
jkato-faz-564-test005

Description (Optional)

Region
us-central1 (Iowa)

Zone
us-central1-f

Type
Standard persistent disk

Source type
Image | Snapshot | Blank disk

Size (GB)
200

Estimated performance

Operation type	Read	Write
Sustained random IOPS limit	150.00	300.00
Sustained throughput limit (MB/s)	24.00	24.00

Encryption
Data is encrypted automatically. Select an encryption key management solution.

● Google-managed key
No configuration required

○ Customer-managed key
Manage via Google Cloud Key Management Service

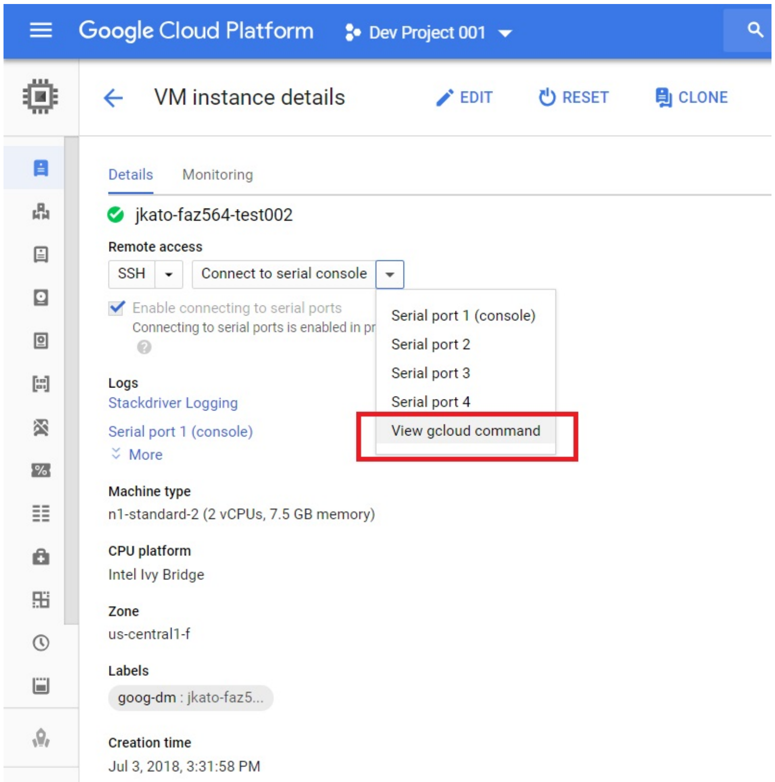
○ Customer-supplied key
Manage outside of Google Cloud

This new disk will be added once you create the new instance

Create | Cancel

Equivalent REST or command line

4. Click *Create*. Ensure the disk appears in the *Disks* list.
5. You must attach the disk to the FortiAnalyzer-VM instance. Navigate to the FortiAnalyzer-VM instance and start the gcloud command.



jkato-faz564-test002

Remote access

☑ Enable connecting to serial ports

Connecting to serial ports is enabled in pr

Logs

Stackdriver Logging

Serial port 1 (console)

More

Machine type

n1-standard-2 (2 vCPUs, 7.5 GB memory)

CPU platform

Intel Ivy Bridge

Zone

us-central1-f

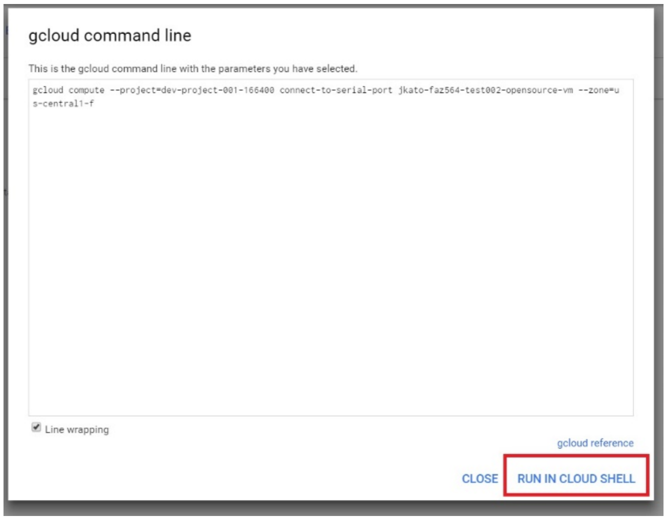
Labels

goog-dm : jkato-faz5...

Creation time

Jul 3, 2018, 3:31:58 PM

6. Click *RUN IN CLOUD SHELL*.



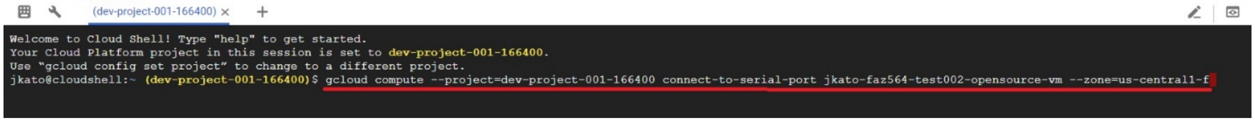
gcloud command line

This is the gcloud command line with the parameters you have selected.

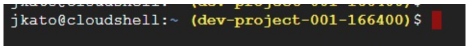
```
gcloud compute --project=dev-project-001-166400 connect-to-serial-port jkato-faz564-test002-opensource-vm --zone=u
s-central1-f
```

☑ Line wrapping

7. Delete the lines that appear in the command line.



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to dev-project-001-166400.
Use "gcloud config set project" to change to a different project.
jkato@cloudshell:~ (dev-project-001-166400)$ gcloud compute --project=dev-project-001-166400 connect-to-serial-port jkato-faz564-test002-opensource-vm --zone=us-central1-f
```



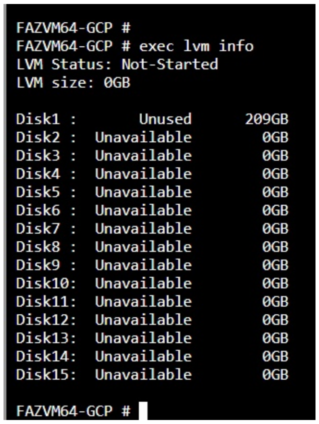
```
jkato@cloudshell:~ (dev-project-001-166400)$
```

8. Enter the following command:
```
gcloud compute instances attach-disk [INSTANCE_NAME] --disk [DISK_NAME]
```

For example, the above instance has the instance name “jkato-faz564-test002” and disk name “jkato-faz-564-test005". In this case, the command is as follows:

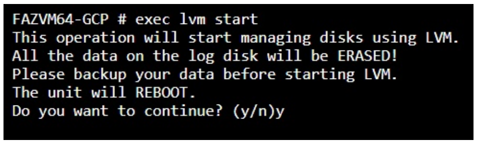
```
gcloud compute instances attach-disk jkato-faz564-test002 --disk jkato-faz-564-test005
```

9. After attaching the disk, log into the FortiAnalyzer-VM management GUI.
10. In the GUI, open the CLI from the icon in the banner.
11. In the command line window, enter `exec lvm info`. The recently added disk is shown as *Unused*.



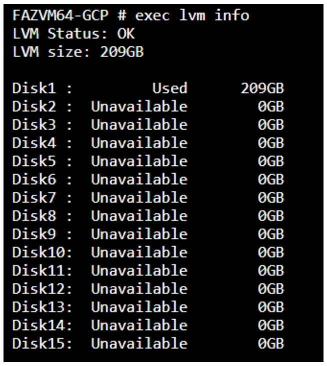
```
FAZVM64-GCP #
FAZVM64-GCP # exec lvm info
LVM Status: Not-Started
LVM size: 0GB

Disk1 :       Unused      209GB
Disk2 :  Unavailable        0GB
Disk3 :  Unavailable        0GB
Disk4 :  Unavailable        0GB
Disk5 :  Unavailable        0GB
Disk6 :  Unavailable        0GB
Disk7 :  Unavailable        0GB
Disk8 :  Unavailable        0GB
Disk9 :  Unavailable        0GB
Disk10:  Unavailable        0GB
Disk11:  Unavailable        0GB
Disk12:  Unavailable        0GB
Disk13:  Unavailable        0GB
Disk14:  Unavailable        0GB
Disk15:  Unavailable        0GB

FAZVM64-GCP #
```

12. Enter `exec lvm start` to start LVM disk management. Enter y to continue. The system reboots.



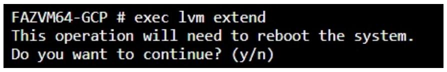
```
FAZVM64-GCP # exec lvm start
This operation will start managing disks using LVM.
All the data on the log disk will be ERASED!
Please backup your data before starting LVM.
The unit will REBOOT.
Do you want to continue? (y/n)y
```

13. Rebooting causes the connection to the CLI console and the management GUI to be lost. Repeat steps 9 to 11. The disk now appears as *Used*.



```
FAZVM64-GCP # exec lvm info
LVM Status: OK
LVM size: 209GB

Disk1 :         Used      209GB
Disk2 :  Unavailable        0GB
Disk3 :  Unavailable        0GB
Disk4 :  Unavailable        0GB
Disk5 :  Unavailable        0GB
Disk6 :  Unavailable        0GB
Disk7 :  Unavailable        0GB
Disk8 :  Unavailable        0GB
Disk9 :  Unavailable        0GB
Disk10:  Unavailable        0GB
Disk11:  Unavailable        0GB
Disk12:  Unavailable        0GB
Disk13:  Unavailable        0GB
Disk14:  Unavailable        0GB
Disk15:  Unavailable        0GB
```

14. Run `exec lvm extend`. This incorporates the disk into the FortiAnalyzer system.

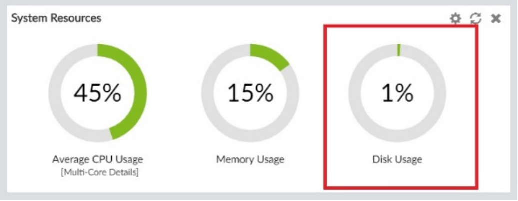


```
FAZVM64-GCP # exec lvm extend
This operation will need to reboot the system.
Do you want to continue? (y/n)
```

15. To add more disks later, follow steps 4 to 6 in Technical Note: Extending disk space in FortiAnalyzer VM / FortiManager VM.

VM platforms may automatically restart or prompt you to restart when resizing an active VM. As a precaution to prevent database corruption and preserve data in FortiAnalyzer, it is best to backup the logs and perform a graceful shutdown before resizing. For more information, see the FortiAnalyzer Best Practices Guide.

16. Go to the *Dashboard*. You will now have sufficient disk space.



Deploying FortiAnalyzer-VM using Google Cloud SDK

You can deploy FortiAnalyzer-VM (bring your own license (BYOL)) by using the Google Cloud SDK on your local PC. This is a method of deploying FortiAnalyzer-VM on GCP outside of the marketplace product listing and without creating an instance on the Google Cloud Compute Portal.

For details, see Cloud SDK.

> This deployment method only applies for BYOL.

This deployment consists of the following steps:

1. Obtaining the deployment image on page 20
2. Uploading the deployment image to Google Cloud on page 20
3. Creating a FortiAnalyzer custom image on page 21
4. Deploying a FortiAnalyzer-VM instance on page 22

Obtaining the deployment image

To obtain the deployment image:

1. Sign in to FortiCloud.
2. Go to *Support > VM Images*.
3. From the *Select Product* dropdown list, select *FortiAnalyzer*.
4. From the *Select Platform* dropdown list, select *Google*.
5. Download the deployment package file. The deployment package file is named “FAZ_VM64_GCP-vX-buildXXXX-FORTINET.out.gcp.tar.gz”, where *vX* is the major version number and *XXXX* is the build number.

Uploading the deployment image to Google Cloud

To upload the FortiAnalyzer deployment image to Google Cloud:

1. Log into Google Cloud.
2. Go to *Storage > Browser*.

3. Create a new bucket or go to an existing bucket.
4. Upload the newly downloaded deployment file.

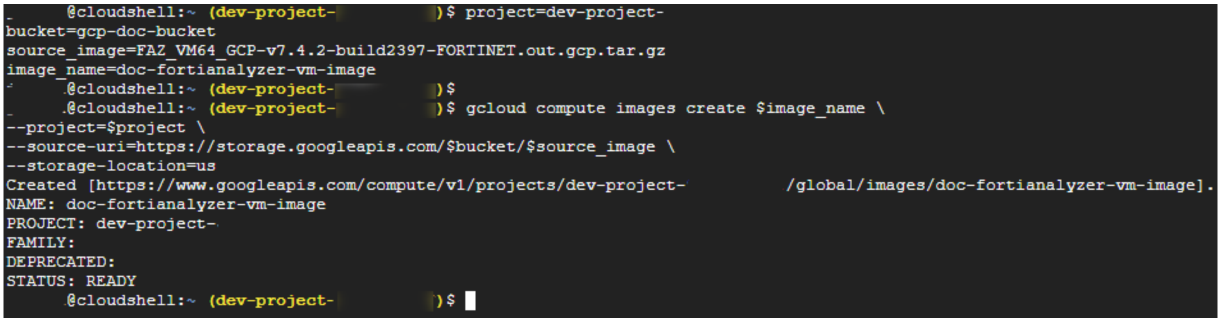
Creating a FortiAnalyzer custom image

This process uses environment variables with the GCloud SDK CLI commands.

To create a FortiAnalyzer custom image:

1. Obtain and place the latest FortiAnalyzer-VM 7.4 image in your desired bucket:
   a. Download the FortiAnalyzer-VM image from the Fortinet Support site. For more information, see Obtaining the deployment image on page 20.
   b. Place the obtained image in your desired bucket. For more information, see Uploading the deployment image to Google Cloud on page 20.
2. Create a custom image via the Google Cloud CLI SDK. Assign environment variables with your project ID, the bucket where you placed the FortiAnalyzer-VM image, and the image name. This example uses the full name of the file downloaded from the Fortinet Support site in the image variable:

```
project=<your project id>
bucket=<name of your bucket>
source_image=<source image, e.g. FAZ_VM64_GCP-v7.4.2-build2397-FORTINET.out.gcp.tar.gz>
image_name=doc-FortiAnalyzer-vm-image

gcloud compute images create $image_name \
--project=$project \
--source-uri=https://storage.googleapis.com/$bucket/$source_image \
--storage-location=us
```



```
[redacted]@cloudshell:~ (dev-project-[redacted])$ project=dev-project-
bucket=gcp-doc-bucket
source_image=FAZ_VM64_GCP-v7.4.2-build2397-FORTINET.out.gcp.tar.gz
image_name=doc-fortianalyzer-vm-image
[redacted]@cloudshell:~ (dev-project-[redacted])$
[redacted]@cloudshell:~ (dev-project-[redacted])$ gcloud compute images create $image_name \
--project=$project \
--source-uri=https://storage.googleapis.com/$bucket/$source_image \
--storage-location=us
Created [https://www.googleapis.com/compute/v1/projects/dev-project-[redacted]/global/images/doc-fortianalyzer-vm-image].
NAME: doc-fortianalyzer-vm-image
PROJECT: dev-project-
FAMILY:
DEPRECATED:
STATUS: READY
[redacted]@cloudshell:~ (dev-project-[redacted])$
```

Deploying a FortiAnalyzer-VM instance

The networks in this example are already setup. Use existing networks and subnets or create them prior to running the commands in this document. Edit all GCP environment-specific variables to fit your GCP environment. This guide assumes familiarity with Linux distributions and Google Cloud CLI already installed and configured for your project and GCP environment. For information about installing the Google Cloud CLI SDK, see Install the gcloud CLI.

This process uses environment variables with the GCloud SDK CLI commands. The custom image creation process is referenced to create the FortiAnalyzer-VM Instance.

To deploy a FortiAnalyzer-VM instance:

1. Define environment variables:

```
project=<your project id>
```

```
zone=us-central1-a
```

```
serviceaccount=<your service account>
```

```
image_name=doc-FortiAnalyzer-vm-image
```

```
image=projects/$project/global/images/$image_name
```

2. Edit and run the following commands in GCP:

```
gcloud compute instances create doc-fortianalyzer-vm \
```

```
--project=$project \
```

```
--zone=$zone \
--machine-type=n2d-standard-2 \
```

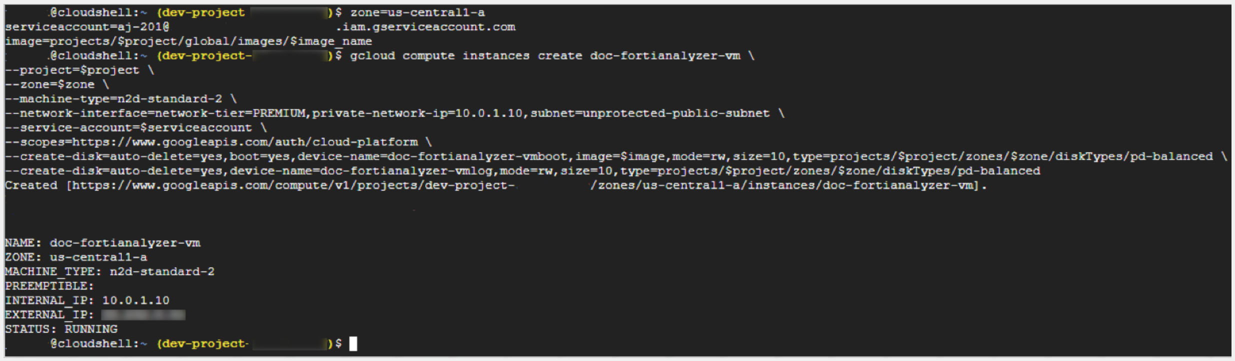
```
--network-interface=network-tier=PREMIUM,private-network-ip=10.0.1.10,subnet=unprotected-public-subnet \
```

```
--service-account=$serviceaccount \
```

```
--scopes=https://www.googleapis.com/auth/cloud-platform \
```

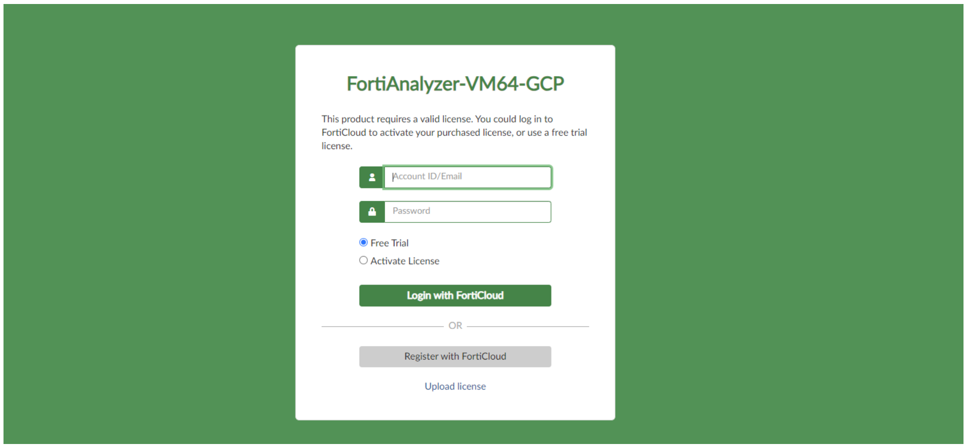
```
--create-disk=auto-delete=yes,boot=yes,device-name=doc-fortianalyzer-vmboot,image=$image,mode=rw,size=10,type=projects/$project/zones/$zone/diskTypes/pd-balanced \
```

```
--create-disk=auto-delete=yes,device-name=doc-fortianalyzer-vmlog,mode=rw,size=10,type=projects/$project/zones/$zone/diskTypes/pd-balanced
```



```
      @cloudshell:~ (dev-project [redacted])$ zone=us-central1-a
serviceaccount=aj-201@                    .iam.gserviceaccount.com
image=projects/$project/global/images/$image_name
      @cloudshell:~ (dev-project-[redacted])$ gcloud compute instances create doc-fortianalyzer-vm \
--project=$project \
--zone=$zone \
--machine-type=n2d-standard-2 \
--network-interface=network-tier=PREMIUM,private-network-ip=10.0.1.10,subnet=unprotected-public-subnet \
--service-account=$serviceaccount \
--scopes=https://www.googleapis.com/auth/cloud-platform \
--create-disk=auto-delete=yes,boot=yes,device-name=doc-fortianalyzer-vmboot,image=$image,mode=rw,size=10,type=projects/$project/zones/$zone/diskTypes/pd-balanced \
--create-disk=auto-delete=yes,device-name=doc-fortianalyzer-vmlog,mode=rw,size=10,type=projects/$project/zones/$zone/diskTypes/pd-balanced
Created [https://www.googleapis.com/compute/v1/projects/dev-project-          /zones/us-central1-a/instances/doc-fortianalyzer-vm].


NAME: doc-fortianalyzer-vm
ZONE: us-central1-a
MACHINE_TYPE: n2d-standard-2
PREEMPTIBLE:
INTERNAL_IP: 10.0.1.10
EXTERNAL_IP: [redacted]
STATUS: RUNNING
      @cloudshell:~ (dev-project-[redacted])$
```

3. Obtain the newly deployed FortiAnalyzer-VM instance ID by running the following command: `gcloud compute instances describe doc-FortiAnalyzer-vm –zone=$zone | grep id`. For more information, see Get the ID of a VM instance.
4. Access the newly deployed FortiAnalyzer-VM using the public IP address from step 2's output and the instance ID from step 4 as the password. You can apply a license using the FortiAnalyzer GUI.



FortiAnalyzer-VM64-GCP

This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license.

Account ID/Email

Password

● Free Trial
○ Activate License

HA for FortiAnalyzer on GCP

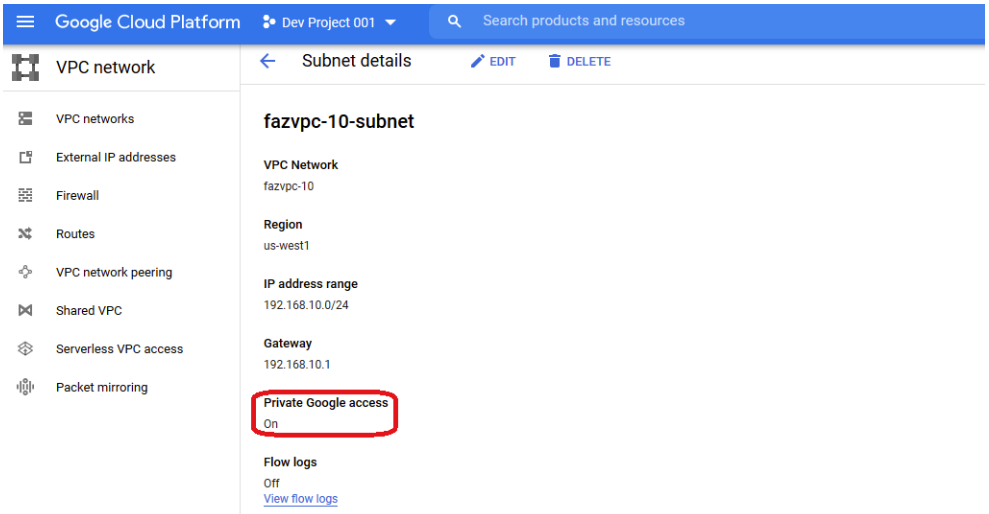
The following topics provide an overview of how to deploy FortiAnalyzer in high availability (HA) mode on GCP:

1. Deploying FortiAnalyzer HA instances on GCP on page 24
2. Configuring FortiAnalyzer HA on page 26

Deploying FortiAnalyzer HA instances on GCP

To deploy FortiAnalyzer instances on GCP:

1. In GCP, create the FortiAnalyzer instances in one Region in the same or different subnets.
   The subnets must have the *Private Google access* option enabled in the *Subnet details* menu.



fazvpc-10-subnet

VPC Network
fazvpc-10

Region
us-west1

IP address range
192.168.10.0/24

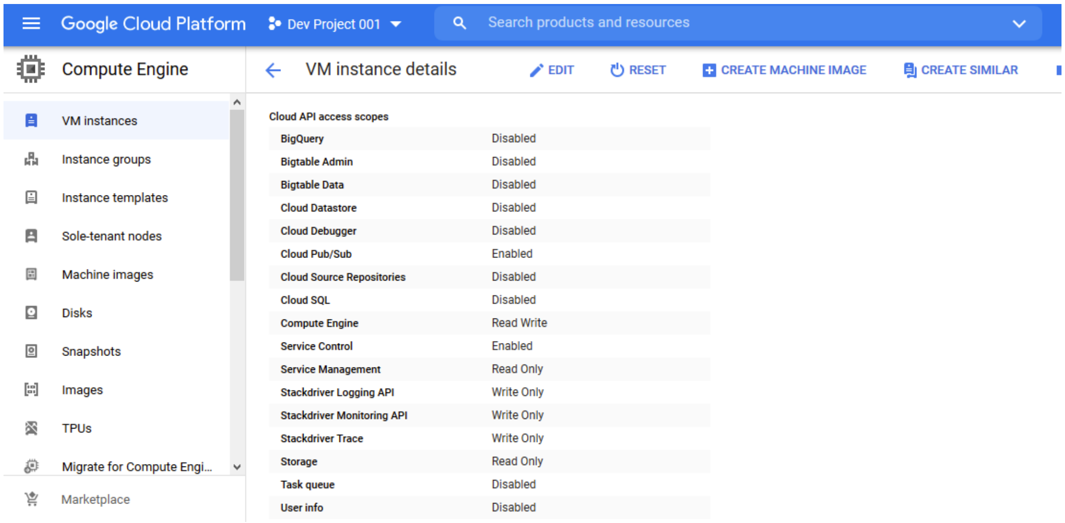
Gateway
192.168.10.1

Private Google access
On

Flow logs
Off

2. Allocate a Static IP address to be used as the virtual IP (VIP) of the FortiAnalyzer HA.
   - While creating the External IP, ensure that the *Static IP Network Service Tier* is *Premium* and the region is the same as that of the FortiAnalyzer instances.

   The External VIP is assigned to an instance when its mode is transitioned to Primary by the fazutil to call Google APIs from within the instance.
3. Assign the required permissions in IAM for the service account associated with each of the FortiAnalyzer instances.
4. Also ensure that the *Cloud API access scopes* for *Compute Engine* in each instance is set to *Read Write*.



Cloud API access scopes

BigQuery	Disabled
Bigtable Admin	Disabled
Bigtable Data	Disabled
Cloud Datastore	Disabled
Cloud Debugger	Disabled
Cloud Pub/Sub	Enabled
Cloud Source Repositories	Disabled
Cloud SQL	Disabled
Compute Engine	Read Write
Service Control	Enabled
Service Management	Read Only
Stackdriver Logging API	Write Only
Stackdriver Monitoring API	Write Only
Stackdriver Trace	Write Only
Storage	Read Only
Task queue	Disabled
User info	Disabled

Ensure that all the *Google Cloud Platform Quotas* under *ListGroup* have the necessary allocation as this may cause HA to fail otherwise.

5. On a *GCP Firewall Policy*, create an inbound rule that allows traffic for the following ports between the primary and secondary units:

Protocol	Port	Purpose
Other*	112	To allow the keepalived adverts from the primary.
TCP	514	To allow initial log sync.
TCP	5199	To allow for configuration sync.

* 112 VRRP (Virtual Router Redundancy Protocol), Common Address Redundancy Protocol (not IANA assigned)

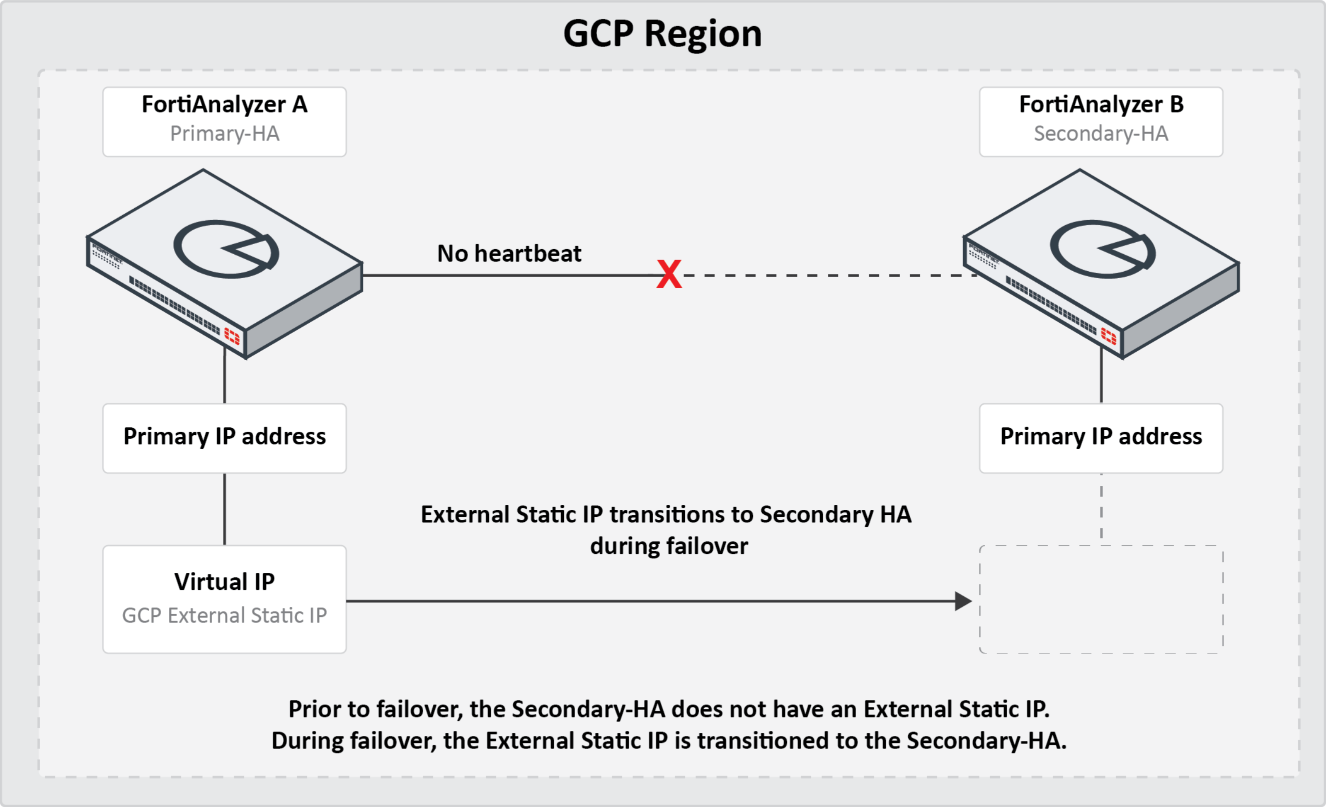
You can now configure the HA settings in FortiAnalyzer. See Configuring FortiAnalyzer HA on page 26.

Transition of secondary IP address during failover topography

In the example below, FortiAnalyzer-A is the Primary-HA and FortiAnalyzer-B is the Secondary-HA.

During failover, FortiAnalyzer-B becomes the new Primary unit. The External Static IP is transitioned from FortiAnalyzer-A to FortiAnalyzer-B, and can be accessed from the internet using the same IP. The addresses does not change during transition.

Prior to failover, the Secondary-HA (FortiAnalyzer-B) is not configured with a External Static IP address.


GCP Region
FortiAnalyzer A
Primary-HA
FortiAnalyzer B
Secondary-HA
No heartbeat
Primary IP address
Primary IP address
External Static IP transitions to Secondary HA during failover
Virtual IP
GCP External Static IP
Prior to failover, the Secondary-HA does not have an External Static IP.
During failover, the External Static IP is transitioned to the Secondary-HA.

Configuring FortiAnalyzer HA

To configure FortiAnalyzer HA:

1. On FortiAnalyzer, configure high availability at *System Settings > HA*.
   See the FortiAnalyzer Administration Guide for more information on configuring HA.
   When configuring HA, use the primary private IP as the *Peer IP* and the External Static IP as the *VIP*.
2. Import the Google Root CA to FortiAnalyzer. In order for the fazutil to call the Google API successfully, you must import the Google Cloud CA certificates to each FortiAnalyzer instance.
   For more information on Google Trust Services, see https://pki.goog/repository/.
   a. Go to *System Settings > Certificates > CA Certificates*.
   b. Click *Import*.
   c. Browse to the file location and select it, or drag-and-drop it into the pop-up window.
   d. Click *OK*.

Change log

Date	Change description
2023-05-15	Initial release.
2023-05-18	Updated FortiAnalyzer-VM marketplace deployment on page 7.
2023-11-14	Updated Machine type support on page 4.
2024-03-08	Updated Deploying FortiAnalyzer HA instances on GCP on page 24.
2024-03-27	Added Deploying FortiAnalyzer-VM using Google Cloud SDK on page 20
2024-07-18	Updated FortiAnalyzer-VM marketplace deployment on page 7.
2025-05-23	Updated Adding a disk to the FortiAnalyzer-VM for logging on page 15.
2025-06-17	Updated About FortiAnalyzer for GCP on page 4.
2025-07-24	Updated About FortiAnalyzer for GCP on page 4.
2025-12-18	Updated Deploying FortiAnalyzer HA instances on GCP on page 24.

www.fortinet.com