Azure Administration Guide

FortiAnalyzer 7.2

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

March 25, 2024
FortiAnalyzer 7.2 Azure Administration Guide
05-720-0792221-20240325

TABLE OF CONTENTS

About FortiAnalyzer for Azure

FortiAnalyzer-VM for Azure delivers centralized logging, analytics, and reporting features. As an Azure 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 disclosure of security breaches.

Highlights of FortiAnalyzer for Azure include the following:

- Graphical summary reports provide network-wide reporting of events, activities, and trends occurring on FortiGates 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 FortiGates 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 a specific operation, 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.

FortiAnalyzer supports backing up FortiAnalyzer Azure VMs using Azure's enhanced backup policy. For more information, see the Microsoft documentation.

FortiAnalyzer 7.2 supports Azure Stack Hub.

Instance type support

FortiAnalyzer supports the following instance types on Azure.

Supported instances on the Azure marketplace listing may change without prior notice.

FortiAnalyzer has a minimum requirement of 4 vCPU and 8GB of RAM on an instance. For v7.2.2 and later, the minimum requirement for RAM is increased to 16 GB.

Instance Types of A- and D-series may no longer appear as deployable at the time you install the FortiAnalyzer virtual machine (VM) via the Azure Marketplace.

For up-to-date information on each instance type, see the following links:

- Sizes for virtual machines in Azure
- General purpose virtual machine sizes
- Previous generations of virtual machine sizes

The following table shows all instance types currently supported on FortiAnalyzer:

Instance Type	vCPU	RAM (GB)
Dsv2 Series		
Standard_DS4_v2	8	28
Standard_DS5_v2	16	56
Dv3 Series		
Standard_D4_v3	4	16
Standard_D8_v3	8	32
Standard_D16_v3	16	64
Standard Dav4 Series		
Standard_D4a_v4	4	16
Standard_D8a_v4	8	32
Standard_D16a_v4	16	64
Standard_D32a_v4	32	128
Standard_D48a_v4	48	192
Standard_D64a_v4	64	256
Standard_D96a_v4	96	384
Standard Dasv4 Series		
Standard_D4as_v4	4	16
Standard_D8as_v4	8	32
Standard_D16as_v4	16	64
Standard_D32as_v4	32	128
Standard_D48as_v4	48	192
Standard_D64as_v4	64	256
Standard_D96as_v4	96	384
Dasv4 Series		
D4as_v4	4	16
D8as_v4	8	32
D16as_v4	16	64

Instance Type	vCPU	RAM (GB)
D32as_v4	32	128
D48as_v4	48	192
D64as_v4	64	256
D96as_v4	96	384

Previous Generation Instance Types	vCPU	RAM (GB)
Previous Generation		
Standard_A6 (retiring soon)	4	28
Standard_A7 (retiring soon)	8	56
Standard_A8_v2	8	16
Standard_D4	8	28
Standard_DS4	8	28

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.

You can deploy FortiAnalyzer-VM using different CPU and RAM sizes and launch it on various private and public platforms.

Licensing

You must have a license to deploy FortiAnalyzer for Azure.

- Order type on page 6
- Creating a support account on page 7
- Registering and downloading your license on page 7

Order type

On Azure, FortiAnalyzer is only available in a bring your own license (BYOL) order type.

BYOL includes perpetual, subscription, and Flex-VM licensing. 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 provides the same ordering practice across all private and public clouds, no matter the platform. You must activate a license the first time you access the instance from the GUI or the CLI before you start using FortiAnalyzer.

Creating a support account

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 FortiAnalyzer and cannot proceed to configure FortiAnalyzer.

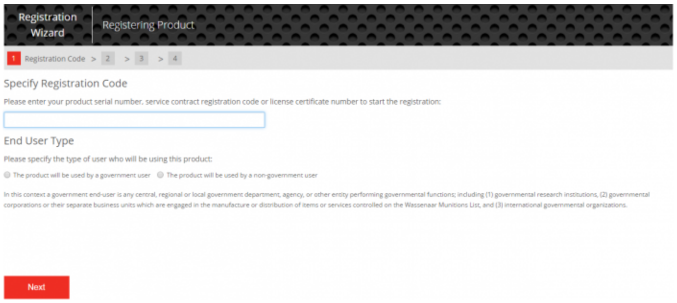
Registering and downloading your license

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. After you purchase a license or obtain an evaluation license (one per account) , you will receive a PDF with an activation code.

For Flex-VM, the VM is activated by token instead of an uploaded license file. For more information, see the Flex-VM Administration Guide.

To register your license:

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. In the *Specify Registration Code* field, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.



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.

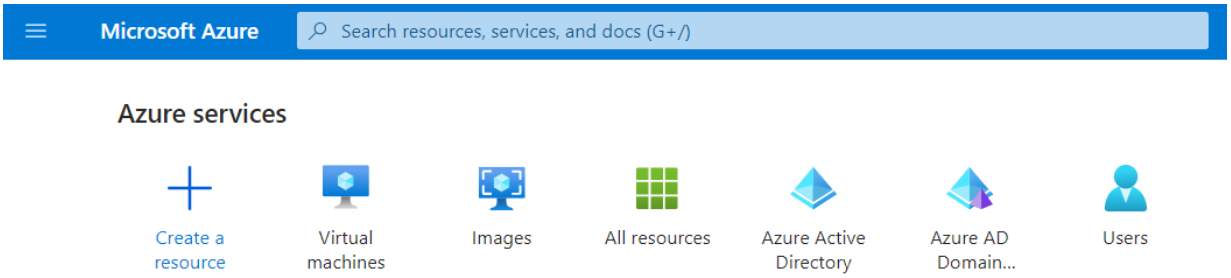
3. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiAnalyzer-VM.
4. After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiAnalyzer-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Deploying a FortiAnalyzer-VM on Azure

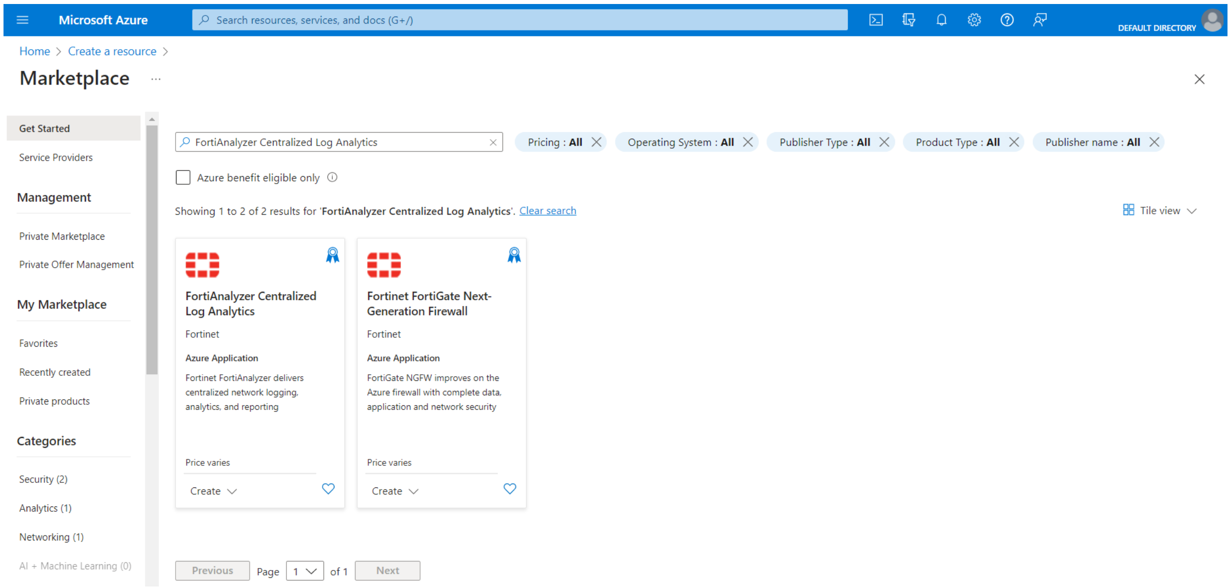
Creating a FortiAnalyzer-VM

To create FortiAnalyzer-VM on Azure:

1. Find the FortiAnalyzer-VM in the Microsoft Azure Portal:
   a. Log into the Microsoft Azure Portal and click *Create a resource*.



   b. Search for FortiAnalyzer Centralized Log Analytics and select it from the search results.



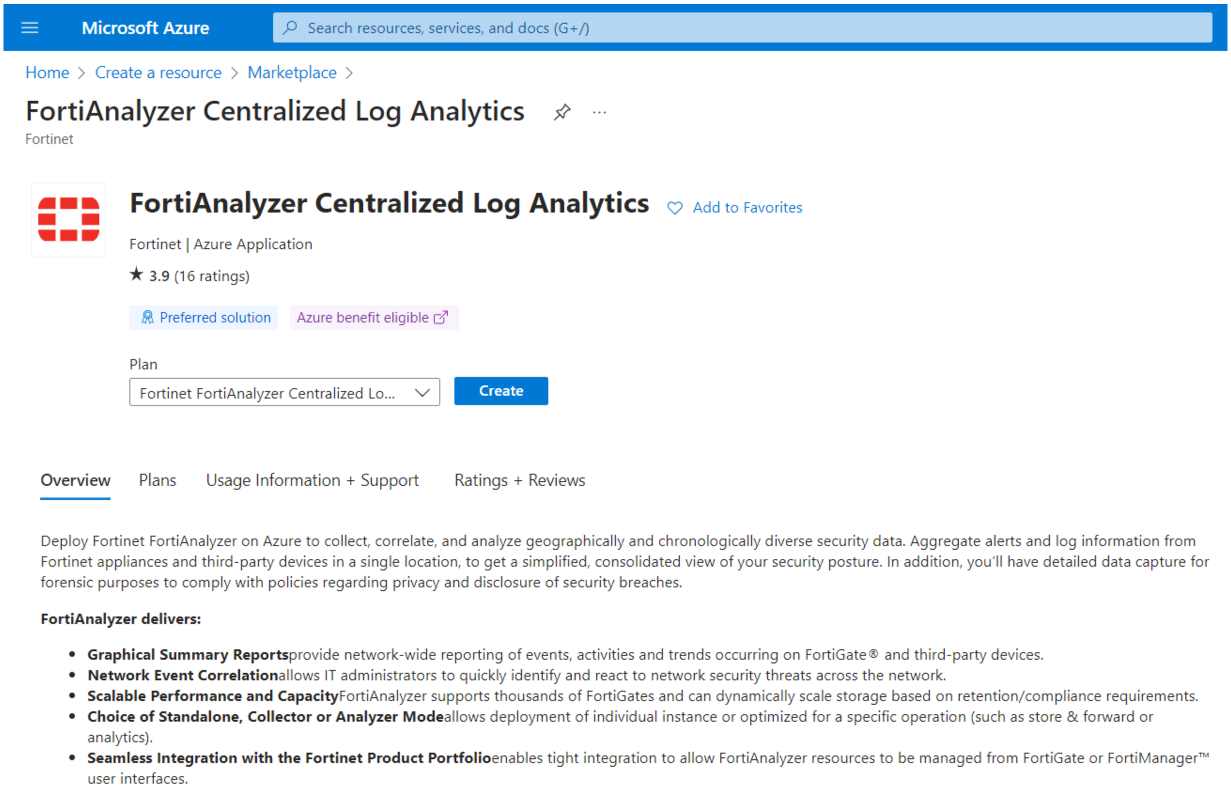
FortiAnalyzer Centralized Log Analytics

□ Azure benefit eligible only

Showing 1 to 2 of 2 results for 'FortiAnalyzer Centralized Log Analytics'. Clear search

FortiAnalyzer Centralized Log Analytics
Fortinet
Azure Application
Fortinet FortiAnalyzer delivers centralized network logging, analytics, and reporting

Fortinet FortiGate Next-Generation Firewall
Fortinet
Azure Application
FortiGate NGFW improves on the Azure firewall with complete data, application and network security


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Marketplace >
Add to Favorites
Preferred solution
Azure benefit eligible
Create
Overview
Plans
Usage Information + Support
Ratings + Reviews

FortiAnalyzer Centralized Log Analytics
Fortinet

FortiAnalyzer Centralized Log Analytics

Fortinet | Azure Application

★ 3.9 (16 ratings)

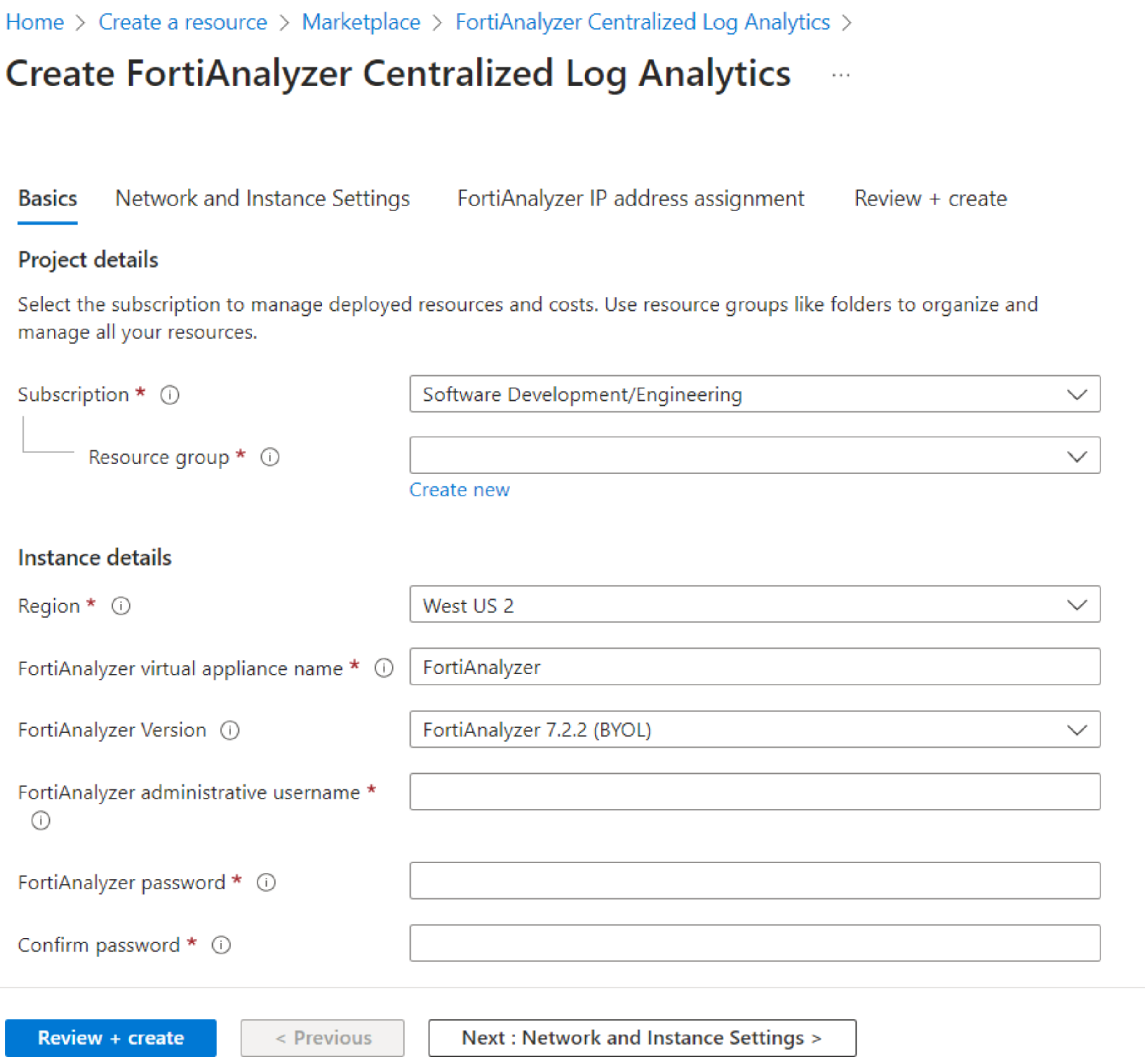
Plan
Fortinet FortiAnalyzer Centralized Lo...

Deploy Fortinet FortiAnalyzer on Azure 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 posture. In addition, you'll have detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of security breaches.

FortiAnalyzer delivers:

- **Graphical Summary Reports**provide network-wide reporting of events, activities and trends occurring on FortiGate® and third-party devices.
- **Network Event Correlation**allows IT administrators to quickly identify and react to network security threats across the network.
- **Scalable Performance and Capacity**FortiAnalyzer supports thousands of FortiGates and can dynamically scale storage based on retention/compliance requirements.
- **Choice of Standalone, Collector or Analyzer Mode**allows deployment of individual instance or optimized for a specific operation (such as store & 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.

2. Click *Create*.
3. Configure the *Basics* section:



Home > Create a resource > Marketplace > FortiAnalyzer Centralized Log Analytics >

Create FortiAnalyzer Centralized Log Analytics ...

Basics | Network and Instance Settings | FortiAnalyzer IP address assignment | Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ	Software Development/Engineering
Resource group * ⓘ	 Create new

Instance details

Region * ⓘ	West US 2
FortiAnalyzer virtual appliance name * ⓘ	FortiAnalyzer
FortiAnalyzer Version ⓘ	FortiAnalyzer 7.2.2 (BYOL)
FortiAnalyzer administrative username * ⓘ	
FortiAnalyzer password * ⓘ	
Confirm password * ⓘ	

a. Select the appropriate *Subscription* from the dropdown list. You may have only one option here. Ensure your organization's subscription allows you to purchase the product.

b. Select the *Resource group*. You can either create a new resource group or select an existing one.

c. Select the appropriate *Region* for the deployment.

d. Enter a FortiAnalyzer-VM name in the *FortiAnalyzer instance name* field.

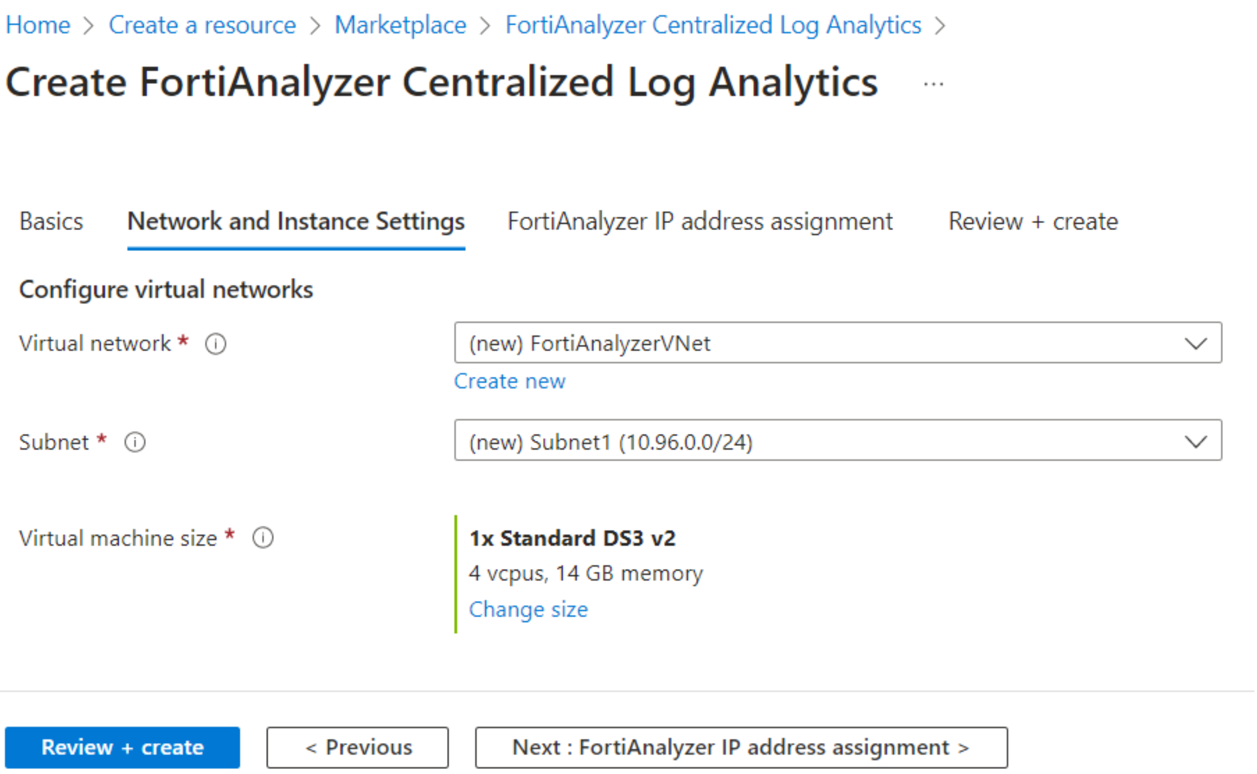
e. Under *FortiAnalyzer Version*, select the desired version.

f. Set a *FortiAnalyzer administrative username*. This name cannot be *admin* or *root*.

g. Enter a *FortiAnalyzer password* for the new account and confirm the password. For security reasons, it is not possible to reset this password through the Microsoft Azure portal, so make sure that you remember the password.

h. Click *Next: Network and Instance Settings*.

4. Configure the *Network and Instance Settings* section:



Home > Create a resource > Marketplace > FortiAnalyzer Centralized Log Analytics >

Create FortiAnalyzer Centralized Log Analytics ...

Basics
Network and Instance Settings
FortiAnalyzer IP address assignment
Review + create

Configure virtual networks

Virtual network * (new) FortiAnalyzerVNet

Subnet * (new) Subnet1 (10.96.0.0/24)

Virtual machine size * **1x Standard DS3 v2** 4 vcpus, 14 GB memory

Change size
Review + create
< Previous
Next : FortiAnalyzer IP address assignment >

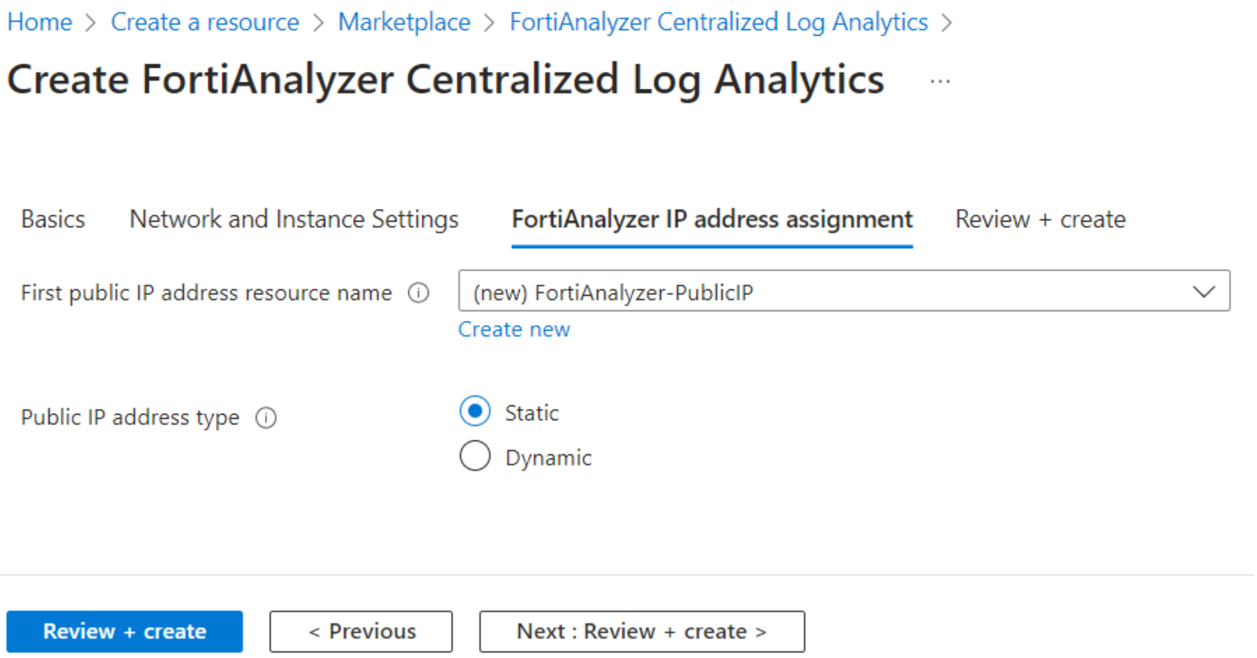
a. Select the *Virtual network*. You can either create a new virtual network (VNet) or select an existing one.

b. Select the *Subnet* where the FortiAnalyzer-VM will be deployed.

c. In *Virtual machine size*, select the appropriate VM size for your deployment. In the Microsoft Azure Marketplace, the FortiAnalyzer-VMs come in a variety of sizes. Each VM size within each series has different limits for the amount of memory, number of NICS, maximum number of data disks, size of cache, and maximum IOPS and bandwidth.

d. Click *Next: FortiAnalyzer IP address assignments*.

5. Configure the *FortiAnalyzer IP address assignments* section:


Home > Create a resource > Marketplace > FortiAnalyzer Centralized Log Analytics >
Basics
Network and Instance Settings
FortiAnalyzer IP address assignment
Review + create
Create new
Review + create
< Previous
Next : Review + create >

Create FortiAnalyzer Centralized Log Analytics

First public IP address resource name: (new) FortiAnalyzer-PublicIP

Public IP address type: ● Static ○ Dynamic

a. Select *First public IP address resource name*. You can either create a new public IP address or select an existing one.
b. In the *Public IP address type* field, select *Dynamic* or *Static*. It usually fine to accept the default value.
c. Click *Next: Review + create*.

6. Wait for validation to pass, then click *Create*. If an error occurs at this stage, resolve it or contact Microsoft support.

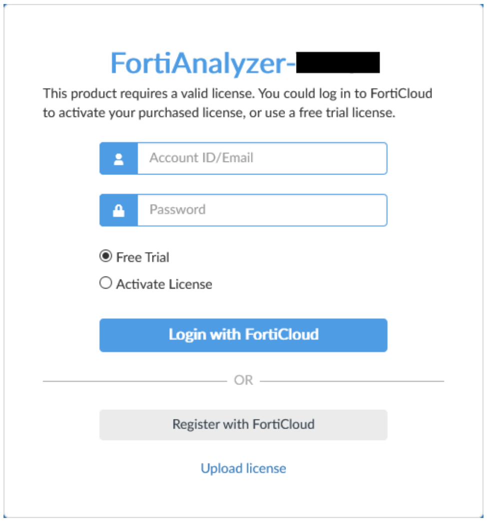
   Azure deploys the FortiAnalyzer-VM and displays a success message upon completion. The deployment may take 30 minutes or longer to complete.

> FortiAnalyzer-VM requires a minimum disk size of 500GB. By default, a log disk of 1 TB is automatically allocated to a FortiAnalyzer-VM instance.

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.

2. Take one of the following actions:

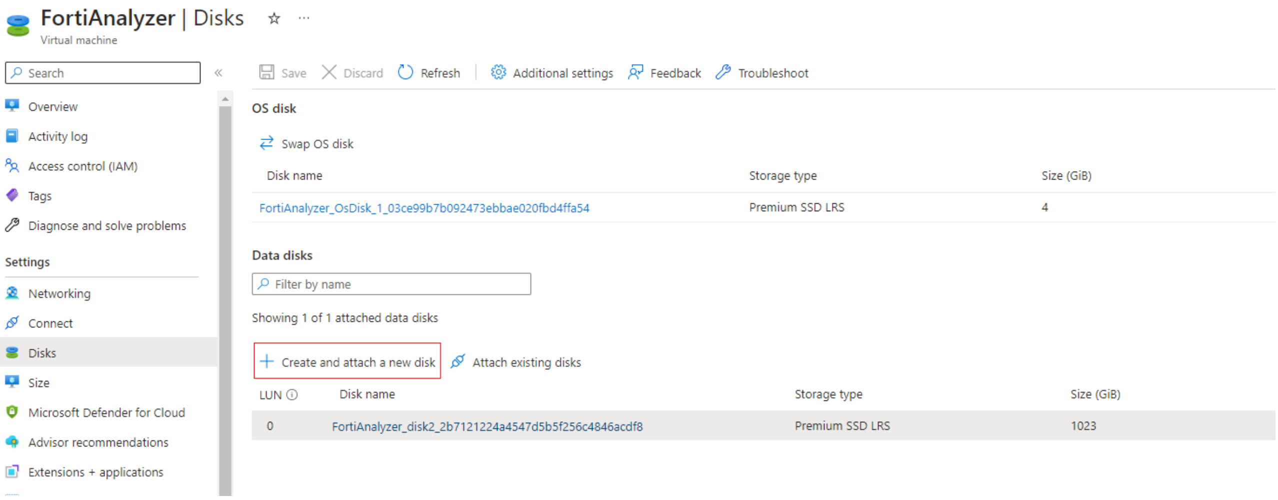
Action	Description
Free Trial	If a valid license is not associated with the account, you can start a free trial license. 1. Select *Free Trial*, and click *Login with FortiCloud*. 2. Use your FortiCloud account credentials to log in, or create a new account. FortiAnalyzer connects to FortiCloud to get 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 7.2 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. 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 configured *FortiWeb administrative username* and *FortiAnalyzer password*.

Adding a disk to the FortiAnalyzer-VM for logging (optional)

In the future or depending on your license requirements, you may need to add more disks to your FortiAnalyzer-VM instances.

1. In the Azure portal, under the FortiAnalyzer Virtual machine *Settings* > *Disks*, click *Create and attach new disk*.



OS disk

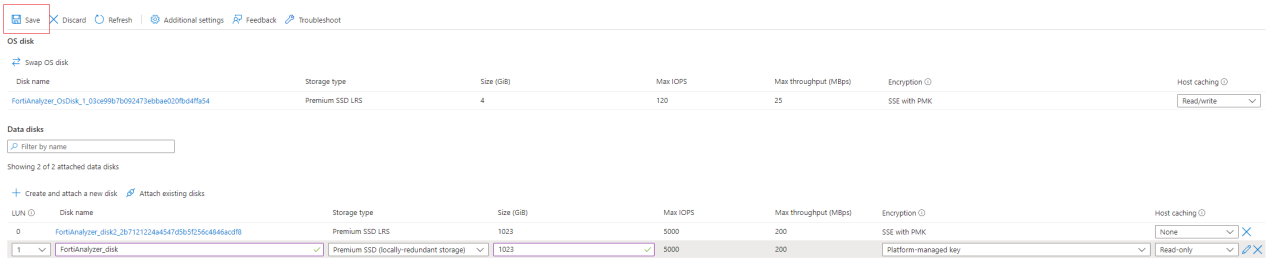
Disk name	Storage type	Size (GiB)
FortiAnalyzer_OsDisk_1_03ce99b7b092473ebbae020fbd4ffa54	Premium SSD LRS	4

Data disks

Showing 1 of 1 attached data disks

LUN ⓘ	Disk name	Storage type	Size (GiB)
0	FortiAnalyzer_disk2_2b7121224a4547d5b5f256c4846acdf8	Premium SSD LRS	1023

2. Input the required parameters (*Disk name*, *Storage type*, *Size*, and *Encryption type*) and click *Save*.



OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (MBps)	Encryption ⓘ	Host caching ⓘ
FortiAnalyzer_OsDisk_1_03ce99b7b092473ebbae020fbd4ffa54	Premium SSD LRS	4	120	25	SSE with PMK	Read/write

Data disks

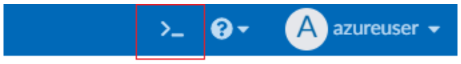
Showing 2 of 2 attached data disks

LUN ⓘ	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (MBps)	Encryption ⓘ	Host caching ⓘ
0	FortiAnalyzer_disk2_2b7121224a4547d5b5f256c4846acdf8	Premium SSD LRS	1023	5000	200	SSE with PMK	None
1	FortiAnalyzer_disk	Premium SSD (locally-redundant storage)	1023	5000	200	Platform-managed key	Read-only

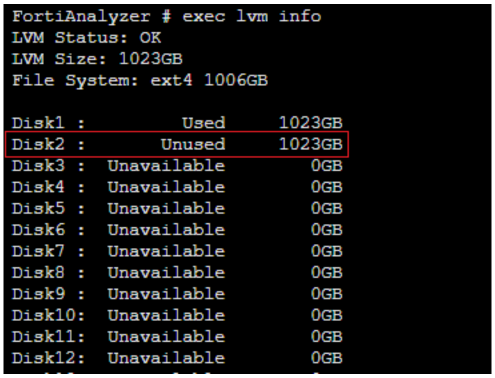
Refer to Azure Managed Disks Overview for details about Azure disks.

On Azure VMs, data may be lost from temporary disks during a maintenance event or when powering off. Therefore, temporary disks (typically /dev/sdb) cannot be used and will not appear under `exec lvm info` in the CLI for FortiAnalyzer-VM. For more information, see Azure managed disks overview.

3. Log into the FortiAnalyzer-VM management GUI console.
4. Open the CLI console.

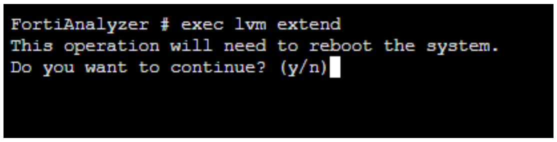


5. In the command prompt window, enter `exec lvm info`. The newly added disk appears as `Unused`.



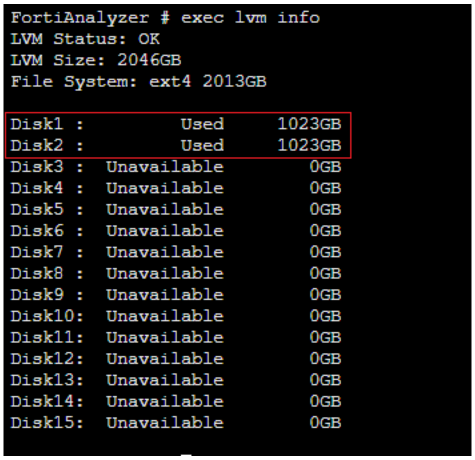
```
FortiAnalyzer # exec lvm info
LVM Status: OK
LVM Size: 1023GB
File System: ext4 1006GB

Disk1 :         Used     1023GB
Disk2 :       Unused     1023GB
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
```

6. Enter `exec lvm extend` to incorporate the disk to the FortiAnalyzer system. Entering `y` reboots the instance.



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

7. Navigate to the FortiAnalyzer dashboard. You will see now that the available disk size has changed. You can also run `exec lvm info` again in the CLI to see that the additional disk is now in use.

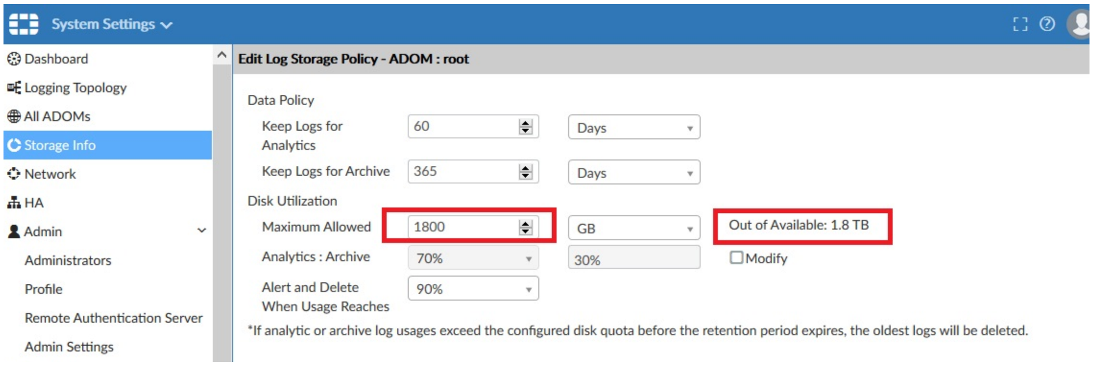


```
FortiAnalyzer # exec lvm info
LVM Status: OK
LVM Size: 2046GB
File System: ext4 2013GB

Disk1 :         Used     1023GB
Disk2 :         Used     1023GB
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
```

   The FortiAnalyzer system reserves a certain portion of disk space for system use and unexpected quota overflow. The remaining space is available for allocation to devices. Reports are stored in the reserved space. The following describes the reserved disk quota relative to the total available disk size (other than the root device):

   - Small disk (equal to 500 GB): reserves 20% or 50 GB of disk space, whichever is smaller.
   - Medium disk (less than or equal to 1 TB): reserves 15% or 100 GB of disk space, whichever is smaller.
   - Medium to large disk (less than or equal to 5 TB): reserves 10% or 200 GB of disk space, whichever is smaller.
   - Large disk (less than 5 TB): reserves 5% or 300 GB of disk space, whichever is smaller.

8. Configure the consumable disk space for logging. 200 GB is reserved. Therefore, 1.8 TB is available for consumption out of the 2 TB of disks.



Edit Log Storage Policy - ADOM : root

Data Policy

Keep Logs for Analytics: 60 Days

Keep Logs for Archive: 365 Days

Disk Utilization

Maximum Allowed: 1800 GB — Out of Available: 1.8 TB

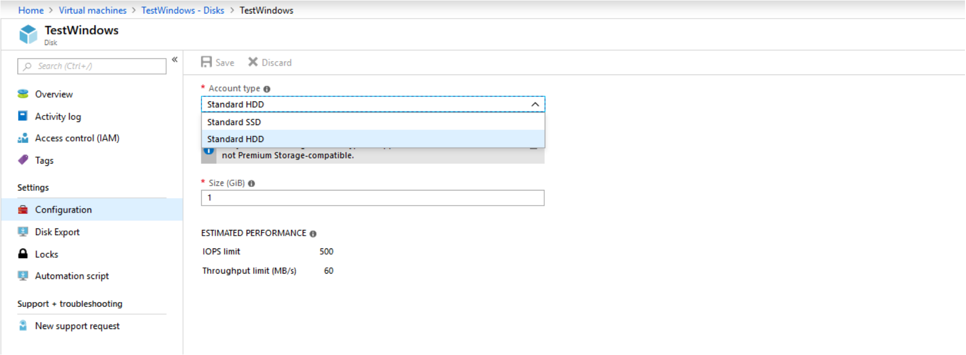
Analytics : Archive: 70% 30% □Modify

Alert and Delete When Usage Reaches: 90%

*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

Changing a disk type on the FortiAnalyzer-VM (optional)

1. Sign in to the *Azure portal*.
2. Select the FortiAnalyzer-VM from the list of *Virtual Machines*.
3. Stop the VM by selecting *Stop* at the top of the VM *Overview* pane, and wait for the VM to stop.
4. In the navigation pane for the VM, select *Disks*.
5. Select the disk that is to be converted.
6. Select *Configuration*.
7. Select the *Account Type* dropdown and choose the new disk type.
   For example, select *Standard SSD*.



* Account type: Standard HDD (options: Standard SSD, Standard HDD)

not Premium Storage-compatible.

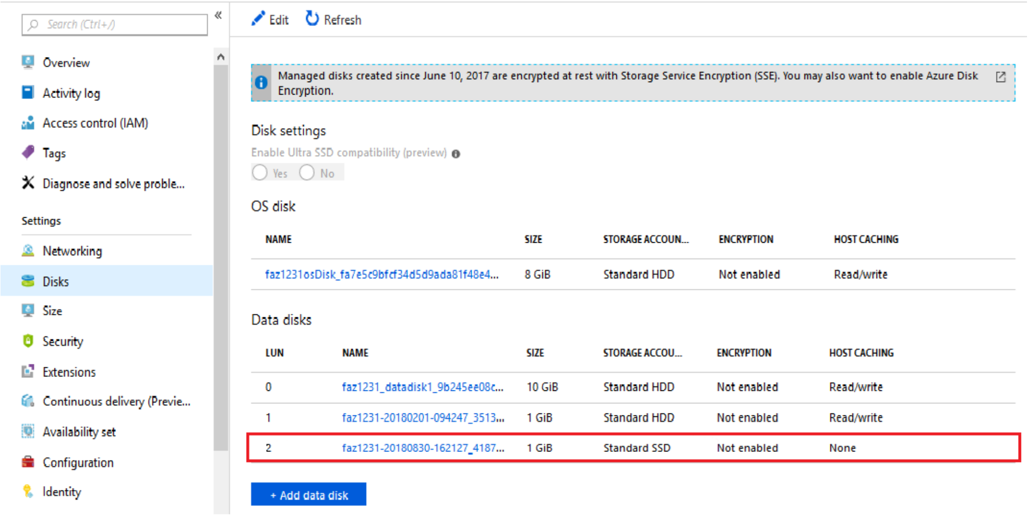
* Size (GiB): 1

ESTIMATED PERFORMANCE

IOPS limit 500

Throughput limit (MB/s) 60

8. Select *Save*.
   The new disk type is displayed in the FortiAnalyzer-VM *Disks* pane.



Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption.

Disk settings

Enable Ultra SSD compatibility (preview)

○ Yes ○ No

OS disk

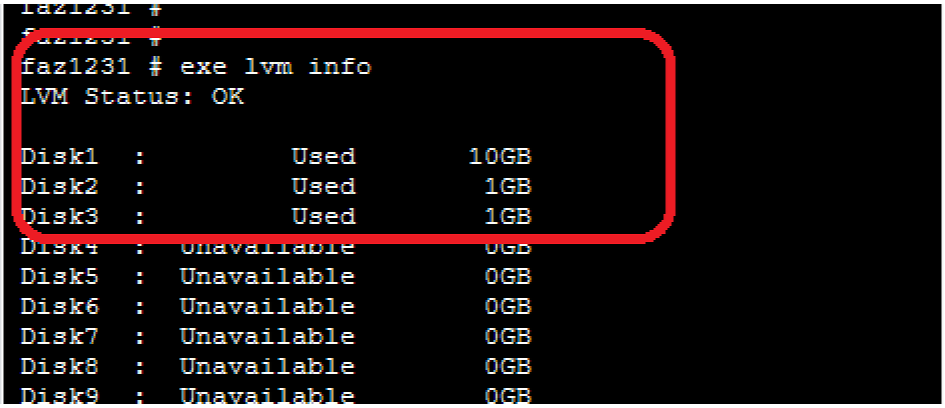
NAME	SIZE	STORAGE ACCOUN...	ENCRYPTION	HOST CACHING
faz1231osDisk_fa7e5c9bfcf34d5d9ada81f48e4...	8 GiB	Standard HDD	Not enabled	Read/write

Data disks

LUN	NAME	SIZE	STORAGE ACCOU...	ENCRYPTION	HOST CACHING
0	faz1231_datadisk1_9b245ee08c...	10 GiB	Standard HDD	Not enabled	Read/write
1	faz1231-20180201-094247_3513...	1 GiB	Standard HDD	Not enabled	Read/write
2	faz1231-20180830-162127_4187...	1 GiB	Standard SSD	Not enabled	None

+ Add data disk

9. Once the disk type has been changed, you can check the status of your FortiAnalyzer LVM with the CLI command: *exe lvm info*.



```
faz1231 #
faz1231 #
faz1231 # exe lvm info
LVM Status: OK

Disk1   :        Used       10GB
Disk2   :        Used        1GB
Disk3   :        Used        1GB
Disk4   :  Unavailable       0GB
Disk5   :  Unavailable       0GB
Disk6   :  Unavailable       0GB
Disk7   :  Unavailable       0GB
Disk8   :  Unavailable       0GB
Disk9   :  Unavailable       0GB
```

HA for FortiAnalyzer on Azure

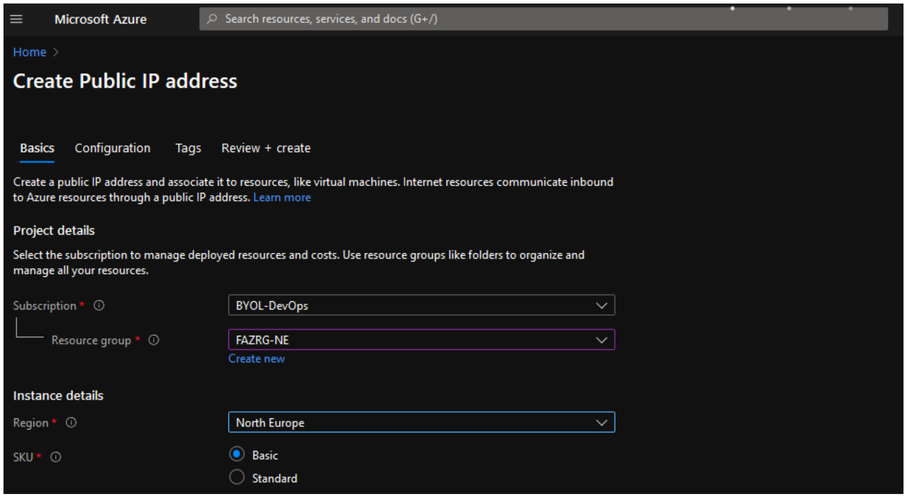
The following topics provide an overview of how to deploy FortiAnalyzer in high availability (HA) mode on Azure:

1. Deploying FortiAnalyzer HA instances on Azure on page 18
2. Configuring FortiAnalyzer HA on page 20

Deploying FortiAnalyzer HA instances on Azure

To deploy FortiAnalyzer instances on Azure:

1. In the Azure GUI, create the FortiAnalyzer instances in one Resource Group in the same or different subnets. Different VNET is currently not supported as the Public IP being assigned is regional resource.



Create Public IP address

Create a public IP address and associate it to resources, like virtual machines. Internet resources communicate inbound to Azure resources through a public IP address. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : BYOL-DevOps

Resource group * : FAZRG-NE

Instance details

Region * : North Europe

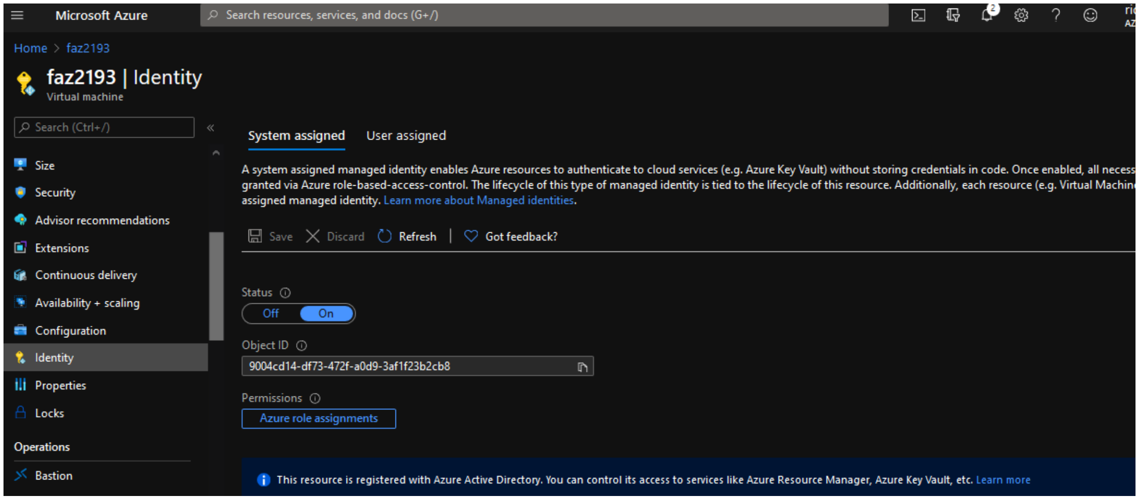
SKU * : ● Basic ○ Standard

2. In the same Resource Group, create a Static Public IP to be used as the Virtual IP (VIP) of the FortiAnalyzer HA. Alternatively, a Secondary Internal IP can also be used as the VIP if necessary.
While creating the External IP, ensure that *SKU* is *Basic* and *Tier* is *Regional*, and the location is the same as that of the FortiAnalyzer instances.

For a more secure deployment, use *Standard* as the Public IP SKU. For further configuration information, see Azure Public IP and Azure Network Security Groups.

The External VIP is assigned to an instance when its mode is transitioned to Primary by the fazutil to call Azure APIs from within the instance.

3. For each FortiAnalyzer instance, navigate to the instance, go to *Settings* > *Identity*, and set *System assigned* to *ON*.



A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Once enabled, all necess granted via Azure role-based-access-control. The lifecycle of this type of managed identity is tied to the lifecycle of this resource. Additionally, each resource (e.g. Virtual Machin assigned managed identity. Learn more about Managed identities.

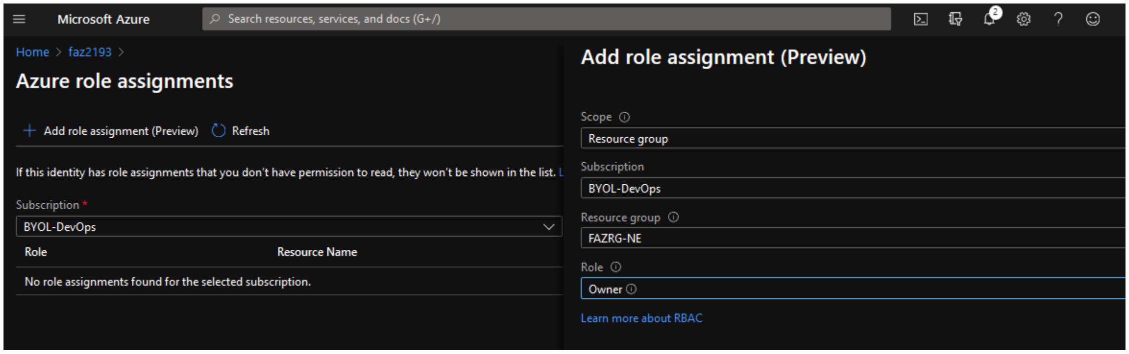
Status: Off [✓ On]

Object ID: 9004cd14-df73-472f-a0d9-3af1f23b2cb8

Permissions: Azure role assignments

This resource is registered with Azure Active Directory. You can control its access to services like Azure Resource Manager, Azure Key Vault, etc. Learn more

4. Under *Azure role assignments*, add a role capable of editing the VM with the *Scope* set as *Resource Group*.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > faz2193 >
Azure role assignments
Add role assignment (Preview)
Refresh
Add role assignment (Preview)
Learn more about RBAC

If this identity has role assignments that you don't have permission to read, they won't be shown in the list.

Subscription *: BYOL-DevOps

Role	Resource Name
No role assignments found for the selected subscription.	

Scope: Resource group

Subscription: BYOL-DevOps

Resource group: FAZRG-NE

Role: Owner

5. On the *Azure Network Security Group*, 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)

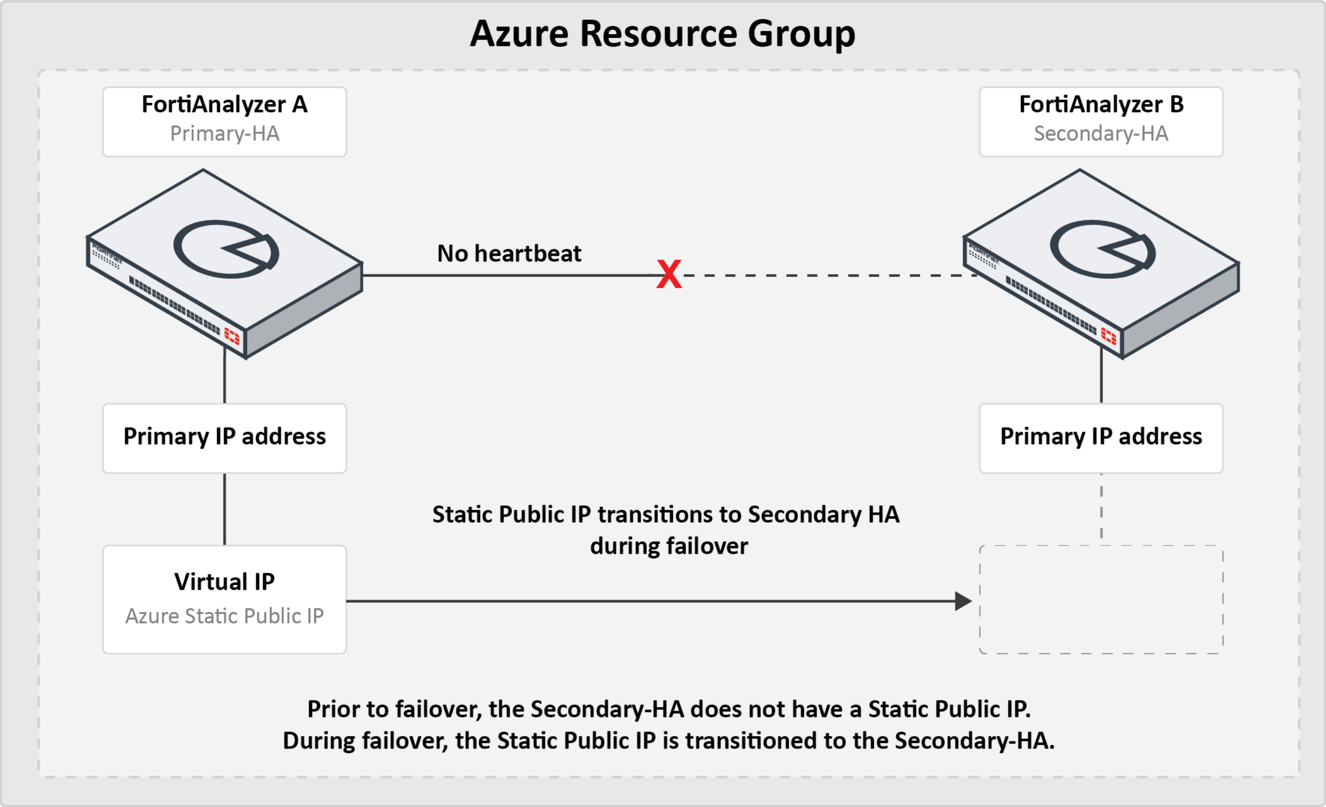
You can now configure the HA settings in FortiAnalyzer. See Configuring FortiAnalyzer HA on page 20.

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 Static Public 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.

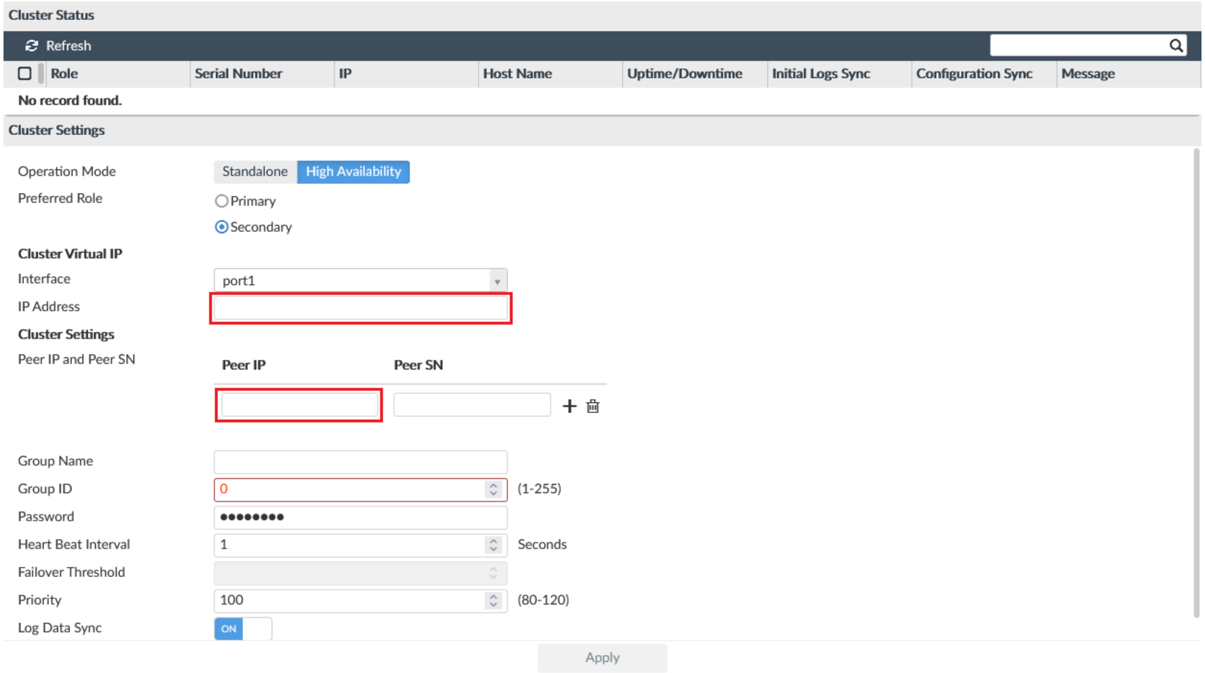
Prior to failover, the Secondary-HA (FortiAnalyzer-B) is not configured with a Static Public IP address.


Azure Resource Group
FortiAnalyzer A
Primary-HA
FortiAnalyzer B
Secondary-HA
No heartbeat
X
Primary IP address
Primary IP address
Static Public IP transitions to Secondary HA during failover
Virtual IP
Azure Static Public IP
Prior to failover, the Secondary-HA does not have a Static Public IP.
During failover, the Static Public 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 *Cluster Virtual IP*.



☐ Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync	Message
No record found.							

Operation Mode: Standalone / [✓ High Availability]

Preferred Role: ○ Primary ● Secondary

Cluster Virtual IP

Interface: port1

IP Address:

Cluster Settings

Peer IP and Peer SN

Peer IP	Peer SN

Group Name:

Group ID: 0 (1-255)

Password: ●●●●●●●●

Heart Beat Interval: 1 Seconds

Failover Threshold:

Priority: 100 (80-120)

Log Data Sync: ON

2. Import the Azure Root CA to FortiAnalyzer. In order for the fazutil to call the Azure API successfully, you must import the Azure Cloud CA certificate to each FortiAnalyzer instance.
   For more information on the CA used by Microsoft Entra ID (formerly Azure AD), see https://learn.microsoft.com/en-us/azure/security/fundamentals/azure-CA-details.
   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
2022-04-11	Initial release.
2022-09-15	Updated Instance type support on page 4.
2023-03-07	Updated Instance type support on page 4.
2023-04-28	Updated: • Creating a FortiAnalyzer-VM on page 8. • Instance type support on page 4. • Order type on page 6. • Creating a support account on page 7. • Registering and downloading your license on page 7.
2023-05-02	Updated Adding a disk to the FortiAnalyzer-VM for logging (optional) on page 14.
2023-10-26	Updated Configuring FortiAnalyzer HA on page 20.
2023-10-31	Updated About FortiAnalyzer for Azure on page 4.
2023-11-14	Updated Instance type support on page 4.
2023-12-21	Updated Instance type support on page 4.
2024-03-08	Updated Deploying FortiAnalyzer HA instances on Azure on page 18.
2024-03-20	Updated Adding a disk to the FortiAnalyzer-VM for logging (optional) on page 14.
2024-03-25	Updated About FortiAnalyzer for Azure on page 4.

www.fortinet.com