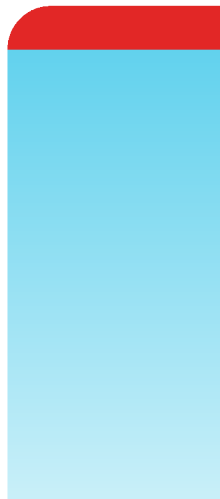


Azure Administration Guide

FortiAnalyzer 7.0



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 8, 2024

FortiAnalyzer 7.0 Azure Administration Guide

05-700-704744-20240308

TABLE OF CONTENTS

About FortiAnalyzer for Azure	4
Instance type support	4
Models	6
Licensing	6
Order types	6
Creating a support account	6
Registering and downloading your license	7
Deploying a FortiAnalyzer-VM on Azure	8
Creating a FortiAnalyzer-VM	8
Connecting to the FortiAnalyzer-VM	13
Adding a disk to the FortiAnalyzer-VM for logging (optional)	14
Changing a disk type on the FortiAnalyzer-VM (optional)	16
HA for FortiAnalyzer on Azure	18
Deploying FortiAnalyzer HA instances on Azure	18
Transition of secondary IP address during failover topography	19
Configuring FortiAnalyzer HA	20

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.

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.



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

Instance Type	vCPU	RAM (GB)
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
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 types on page 6](#)
- [Creating a support account on page 6](#)
- [Registering and downloading your license on page 7](#)

Order types

On Azure, there is only one order type available for FortiAnalyzer: BYOL. Currently pay as you go/on-demand (PAYG) is not listed.

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 the publicly available price list, which is updated quarterly, lists prices. BYOL licensing 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 features.

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

See [Creating a support account on page 6](#). Also see *Support* on the FortiAnalyzer BYOL [marketplace product page](#).

Creating a support account

FortiAnalyzer for Azure supports BYOL licensing models.

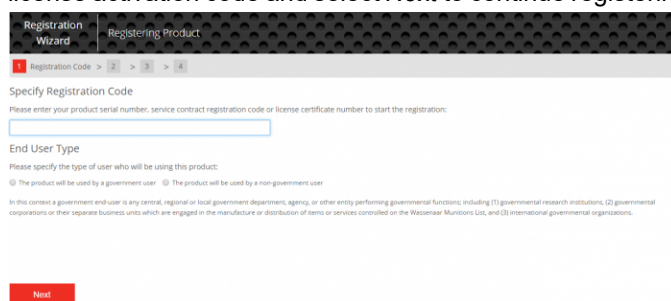
For BYOL, you typically order a combination of products and services, including support entitlement.

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 FortiAnalyzer and cannot proceed to configure FortiAnalyzer. See [Registering and downloading your license on page 7](#).

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 (60-day term), 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. 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.

The screenshot shows the 'Registration Wizard' interface. At the top, there's a dark header with 'Registration Wizard' and 'Registering Product'. Below this is a progress bar with four steps: 1. Registration Code (active), 2. End User Type, 3. License Agreement, and 4. Summary. The main content area is titled 'Specify Registration Code' and includes the instruction: 'Please enter your product serial number, service contract registration code or license certificate number to start the registration:'. There is a text input field below this instruction. Underneath the input field is the 'End User Type' section, which asks 'Please specify the type of user who will be using this product:' and provides two radio button options: 'The product will be used by a government user' and 'The product will be used by a non-government user'. A small disclaimer is visible at the bottom of the form. A red 'Next' button is located at the bottom right of the form.

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

1. Find FortiAnalyzer-VM in the [Microsoft Azure Portal](#):
 - a. Log into the Microsoft Azure Portal and click *Create a resource*.
 - b. Find *FortiAnalyzer Centralized Log Analytics* and click *GET IT NOW*.
2. Under *Select a deployment model*, ensure that *Resource Manager* is selected. Select *Create*.
3. Configure the *Basics* section:
 - a. Set a FortiAnalyzer-VM name in the *FortiAnalyzer virtual appliance name* field.
 - b. Under *Version*, select *BYOL*.
 - c. Set a *FortiAnalyzer administrative username*. This name cannot be admin or root.
 - d. Choose 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.
 - e. 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.
 - f. Create a new *Resource group*. Currently, it is not possible to select an existing resource group for a Microsoft Azure Marketplace template set, so you must create a new one.
 - g. Set a *Location* for the VM. Click *OK*.

The screenshot displays the 'Basics' configuration page for creating a FortiAnalyzer VM in the Microsoft Azure Portal. The left sidebar shows a five-step process: 1. Basics (selected), 2. Network and Instance Settings, 3. FortiAnalyzer IP address assignment, 4. Summary, and 5. Buy. The main configuration area includes the following fields and options:

- FortiAnalyzer virtual appliance name:** A text box containing 'FortiAnalyzer'.
- FortiAnalyzer Version:** A dropdown menu with 'FortiAnalyzer 6.0.0 (BYOL)' selected and 'FortiAnalyzer 5.6.3 (BYOL)' as an alternative option.
- FortiAnalyzer administrative username:** An empty text box.
- FortiAnalyzer password:** An empty text box.
- Confirm password:** An empty text box.
- Subscription:** A dropdown menu showing 'BYOL-DevOps'.
- Resource group:** Radio buttons for 'Create new' (selected) and 'Use existing'.
- Location:** A dropdown menu showing 'West US'.

An 'OK' button is located at the bottom right of the configuration area.

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

- Select *Virtual network*. You can either create a new virtual network (VNet) or select an existing one.
- In the *Address space* field, accept the default values or specify your own. Click *OK*.

The screenshot shows the 'Create virtual network' dialog in the Azure portal. The dialog is divided into two main sections: 'Network and Instance Settings' and 'Choose virtual network'.

Network and Instance Settings:

- Virtual network:** (new) FortiAnalyzerVNet
- Subnet:** Configure subnets
- Virtual machine size:** 1x Standard D2 v2

Choose virtual network:

- A message states: "No virtual networks found in the selected subscription and location 'Korea Central'."
- A button labeled "Create new" is visible.
- A "No results" message is displayed.

Create virtual network details:

- Name:** FortiAnalyzerVNet
- Address space:** 10.24.0.0/16 (10.24.0.0 - 10.24.255.255 (65536 addresses))

The dialog includes a sidebar with navigation steps: 1 Basics (Done), 2 Network and Instance Settings (active), 3 FortiAnalyzer IP address assign..., 4 Summary, and 5 Buy. An "OK" button is at the bottom right.

5. In the *Subnet* section, the *Subnet name* and *Subnet address prefix* are pre-defined and you should not need to change the default values. Click *OK*.

The screenshot shows the 'Subnet' configuration dialog in the Azure portal. The dialog is divided into two main sections: 'Network and storage settings' and 'Subnet'.

Network and storage settings:

- Virtual network:** (new) FortiAnalyzerVNet
- Subnet:** Configure subnets
- Virtual machine size:** 1x Standard D2 v2
- Storage account:** Configure required settings

Subnet details:

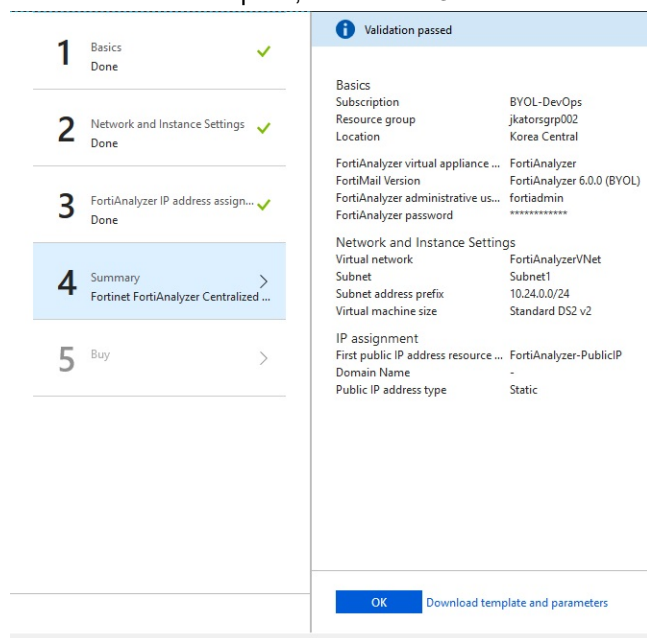
- Subnet name:** Subnet1
- Subnet address prefix:** 10.26.0.0/24

The dialog includes a sidebar with navigation steps: 1 Basics (Done), 2 Network and Storage Settings (active), 3 FortiAnalyzer IP address assign..., 4 Summary, and 5 Buy. An "OK" button is at the bottom right.

6. In the *Virtual machine size* section, 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. Click **OK**.

7. Configure the *FortiAnalyzer IP address assignments* section:
- Select *First public IP address resource name*. In the *Name* field, set a name for the public IP address of the FortiAnalyzer.
 - In the *Public IP address type* field, select *Dynamic* or *Static*. Click **OK**.
 - In the *SKU* field, select *Basic* or *Standard*. Click **OK**.

8. Wait for validation to pass, then select **OK**. If an error occurs at this stage, resolve it or contact Microsoft support.



Validation passed	
Basics	
Subscription	BYOL-DevOps
Resource group	jkatorsgrp002
Location	Korea Central
FortiAnalyzer virtual appliance ...	
FortiAnalyzer	FortiAnalyzer
FortiMail Version	FortiAnalyzer 6.0.0 (BYOL)
FortiAnalyzer administrative us...	fortiadmin
FortiAnalyzer password	*****
Network and Instance Settings	
Virtual network	FortiAnalyzerVNet
Subnet	Subnet1
Subnet address prefix	10.24.0.0/24
Virtual machine size	Standard DS2 v2
IP assignment	
First public IP address resource ...	FortiAnalyzer-PublicIP
Domain Name	-
Public IP address type	Static

OK Download template and parameters



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.

9. Select *Purchase* to buy the FortiAnalyzer-VM instance from Microsoft Azure. Once the FortiAnalyzer-VM is deployed, you will see a “Deployment succeeded” message. The deployment may take 30 minutes or longer to complete.

Purchase

FortiAnalyzer Centralized Log Analytics
by Fortinet
[Terms of use](#) | [privacy policy](#)

Deploying this template will result in various actions being performed, which may include the deployment of one or more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings.

Current retail prices for Azure resources are set forth [here](#) and may not reflect discounts applicable to your Azure subscription.

Prices for Marketplace offerings are set forth [here](#), and the legal terms associated with any Marketplace offering may be found in the Azure portal; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Template deployment is intended for advanced users only. If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.

Terms of use

By clicking "Purchase," I (a) agree to the legal terms and privacy statement(s) provided above as well as the legal terms and privacy statement(s) associated with each Marketplace offering that will be deployed using this template, if any; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); (c) agree that Microsoft may share my contact information and transaction details with any third-party sellers of the offering(s); and (d) give Microsoft permission to share my contact information so that the provider of the template can contact me regarding this product and related products. Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Purchase

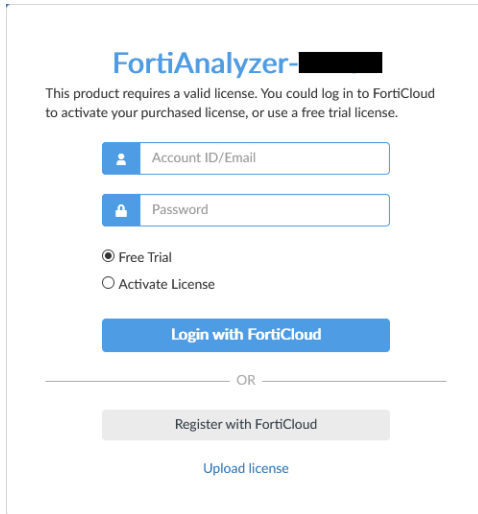


The terms of use you see at the time of your deployment may differ from the screenshot above.

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.



The login dialog box for FortiAnalyzer-VM. It features the FortiAnalyzer logo at the top. Below the logo, a message states: "This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license." There are two input fields: "Account ID/Email" and "Password". Below these fields are two radio buttons: "Free Trial" (selected) and "Activate License". A blue button labeled "Login with FortiCloud" is positioned below the radio buttons. Below this button is a horizontal line with "OR" in the center. Underneath the line is a gray button labeled "Register with FortiCloud". At the bottom, there is a blue link labeled "Upload license".

2. Take one of the following actions:

Action	Description
Free Trial	<p>If a valid license is not associated with the account, you can start a free trial license.</p> <ol style="list-style-type: none"> 1. Select <i>Free Trial</i>, and click <i>Login with FortiCloud</i>. 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. <p>For more information, see the FortiAnalyzer 7.0.0 VM Trial License Guide.</p>
Activate License	<p>If you have a license file, you can activate it .</p> <ol style="list-style-type: none"> 1. Select <i>Activate License</i>, and click <i>Login with FortiCloud</i>. 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	<ol style="list-style-type: none"> 1. Click <i>Browse</i> to upload the license file, or drag it onto the field. 2. Click <i>Upload</i>. After the license file is uploaded, the system will restart to verify it. This may take a few moments. <div>  <p>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 <i>Asset Managmeent > Products > Product List</i>, then click the product serial number.</p> </div>

- 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.

- Create and configure an additional empty disk as below.

Create managed disk

* Name: jkato-newdisk002 ✓

* Subscription: BYOL-DevOps

* Resource group: ☒ Create new ☐ Use existing
jkatorgrp002 ✓

* Location: Korea Central

Availability zone: None

No availability zones are available for the location you have selected. To view locations that support availability zones, go to aka.ms/zonedregions.

* Account type: Standard HDD

* Source type: None (empty disk)

* Size (GiB): 1023 ✓

ESTIMATED PERFORMANCE

IOPS limit: 500

Throughput limit (MB/s): 60

[Create](#) [Automation options](#)

- Attach it to the FortiAnalyzer-VM and click **Save**.

FortiAnalyzer - Disks

Virtual machine

Search (Ctrl+F)

Save Discard Refresh

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.

OS disk

NAME	SIZE	STORAGE ACCOUNT ...	ENCRYPTION	HOST CACHING
FortiAnalyzer_OsDisk_1_dd3750ce3ba24c9aba3bf2cebd2...	2 GiB	Premium SSD	Not enabled	Read/write

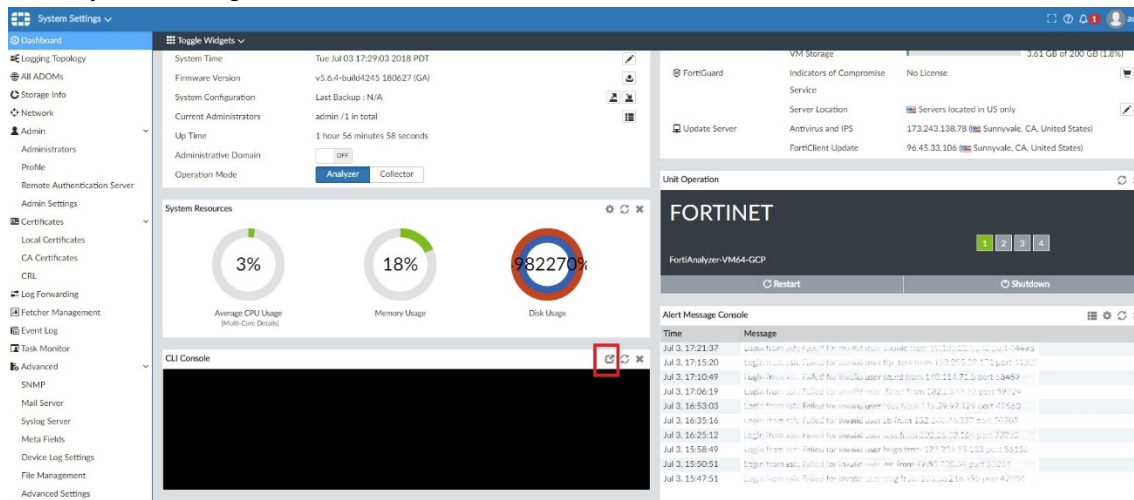
Data disks

LUN	NAME	SIZE	STORAGE ACCOUNT ...	ENCRYPTION	HOST CACHING
0	FortiAnalyzer_disk2_7b339ba895af4fe9...	1023 GiB	Premium SSD	Not enabled	None
1	jkato-newdisk002	1023 GiB	Standard HDD	Not enabled	None

[+ Add data disk](#)

Refer to [Azure Managed Disks Overview](#) for details about Azure disks.

- Log into the FortiAnalyzer-VM management GUI console.

4. Go to *System Settings*. Invoke the CLI console.5. In the command prompt window, enter `exec lvm info`. The newly added disk appears as Unused.

```
FortiAnalyzer #
FortiAnalyzer # exec lvm info
LVM Status: OK

Disk1 :      Used      1072GB
Disk2 :      Unused    1072GB
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

FortiAnalyzer #
```

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

```
FortiAnalyzer # exec lvm extend
Disk2 will be added to LVM.
This operation will need to reboot the system.
Do you want to continue? (y/n) y
```

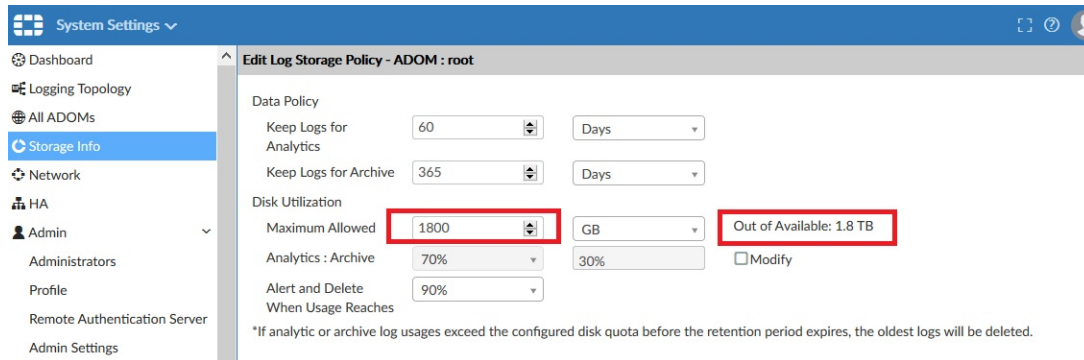
7. Navigate to the FortiAnalyzer dashboard. You will see now that the available disk size has changed. You can also run `exec lvm info` again in the CLI to see that the additional disk is now in use.

```
FortiAnalyzer # exec lvm info
LVM Status: OK

Disk1 :      Used      1072GB
Disk2 :      Used      1072GB
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
```

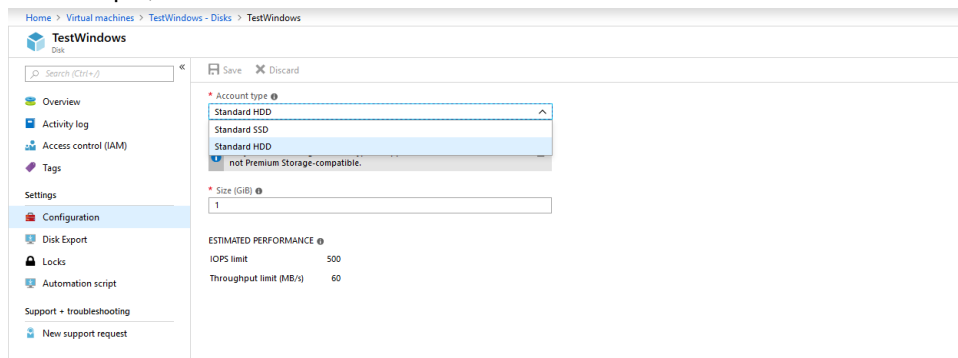
The FortiAnalyzer system reserves a certain portion of disk space for system use and unexpected quota overflow. The remaining space is available for allocation to devices. Reports are stored in the reserved space. The following describes the reserved disk quota relative to the total available disk size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

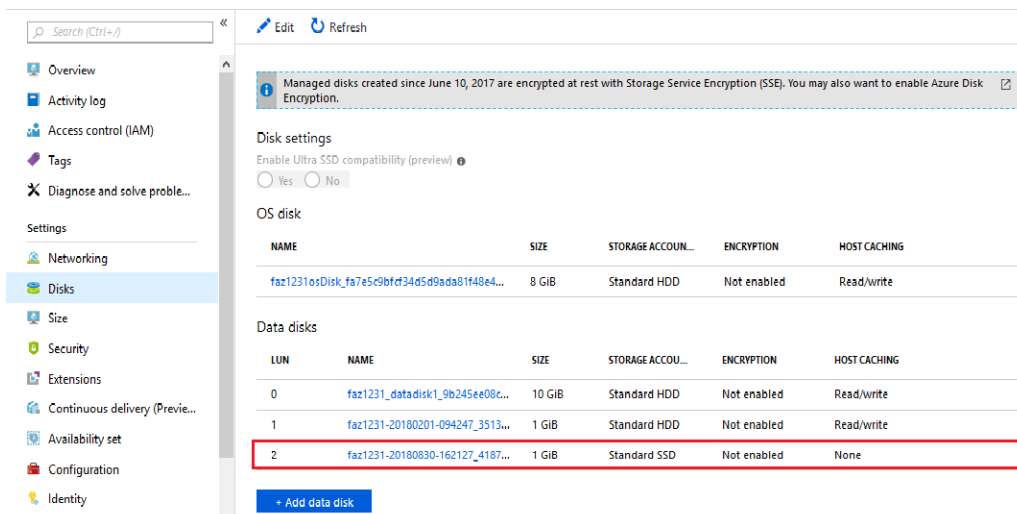


Changing a disk type on the FortiAnalyzer-VM (optional)

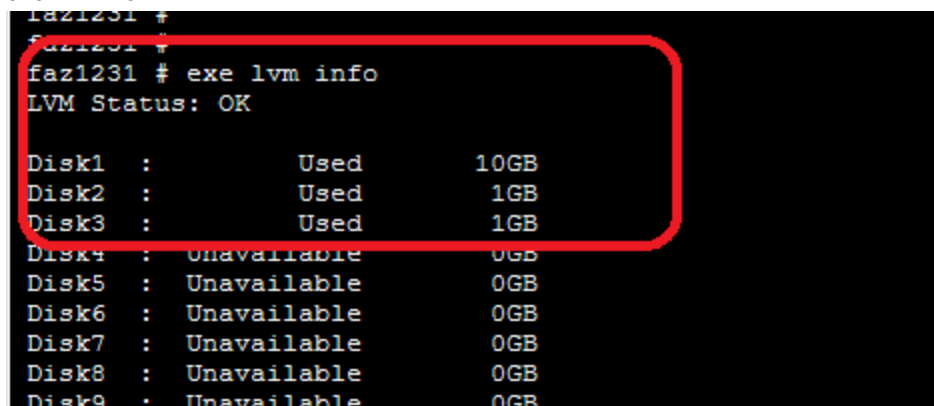
1. Sign in to the *Azure portal*.
2. Select the FortiAnalyzer-VM from the list of *Virtual Machines*.
3. Stop the VM by selecting *Stop* at the top of the VM *Overview* pane, and wait for the VM to stop.
4. In the navigation pane for the VM, select *Disks*.
5. Select the disk that is to be converted.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



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



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



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.

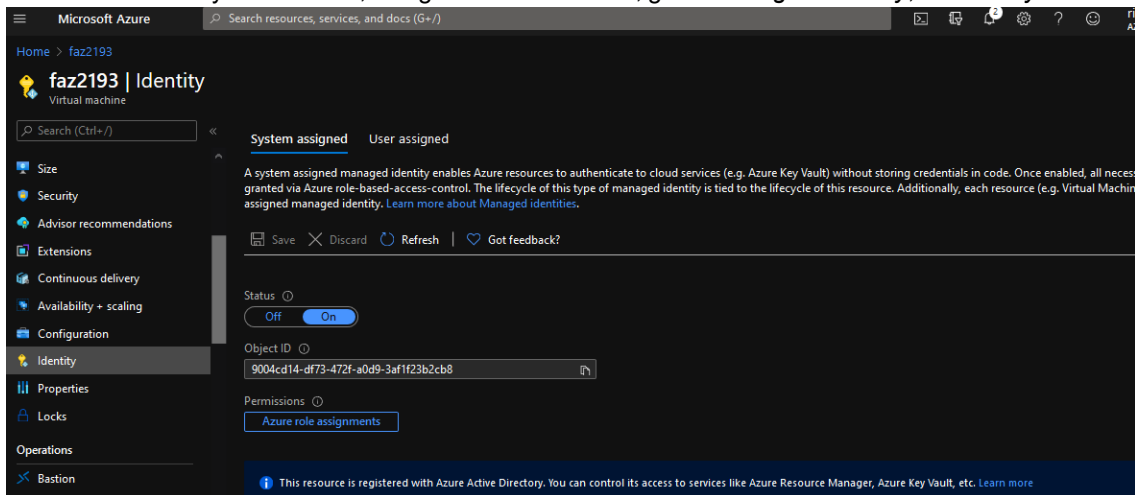
2. In the same Resource Group, create a Static Public IP to be used as the Virtual IP (VIP) of the FortiAnalyzer HA. Alternatively, a Secondary Internal IP can also be used as the VIP if necessary. While creating the External IP, ensure that *SKU* is *Basic* and *Tier* is *Regional*, and the location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



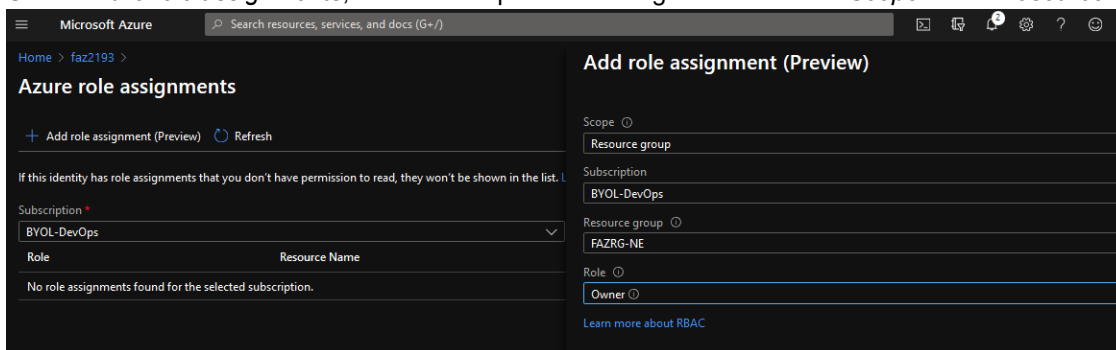
For a more secure deployment, use *Standard* as the Public IP SKU. For further configuration information, see [Azure Public IP](#) and [Azure Network Security Groups](#).

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*.



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



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)

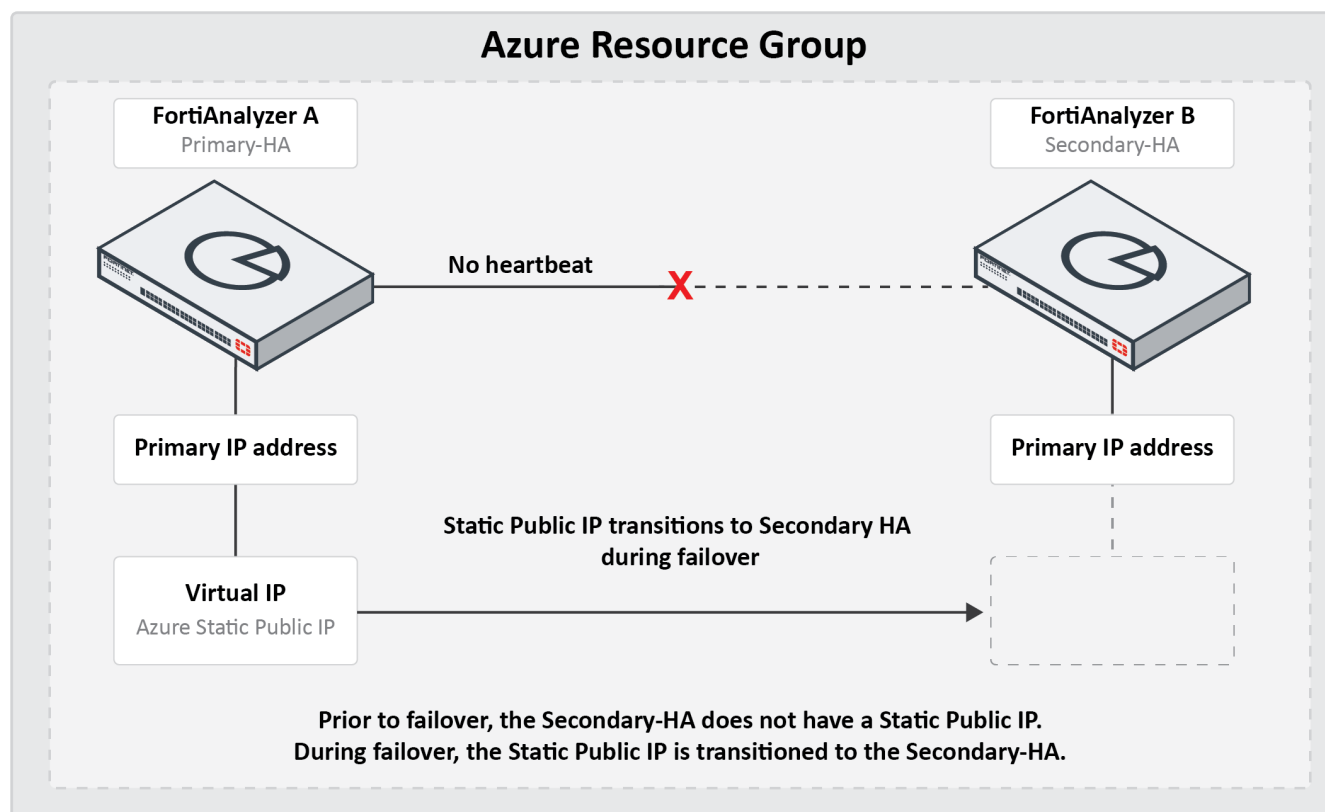
You can now configure the HA settings in FortiAnalyzer. See [Configuring FortiAnalyzer HA on page 20](#).

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.



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*.

Cluster Status

Refresh

<input type="checkbox"/> Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync	Message
No record found.							

Cluster Settings

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
<input type="text"/>	<input type="text"/> +

Group Name:

Group ID: 0 (1-255)

Password:

Heart Beat Interval: 1 Seconds

Failover Threshold:

Priority: 100 (80-120)

Log Data Sync: ☒ ON

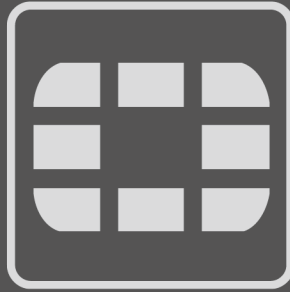
Apply

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*.



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



FORTINET®



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.