FortiADC - Azure Deployment Guide

Version 7.2.0

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

FORTINET VIDEO GUIDE
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 CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 3, 2023
FortiADC 7.2.0 Azure Deployment Guide
01-544-677187-20230203

TABLE OF CONTENTS

Change Log

Date	Change Description
May 27, 2022	Initial release

Introduction

Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers. This document explains how to create a virtual FortiADC instance in Microsoft Azure, and how to pair FortiADC HA on Azure using the ARM template.

Deploying FortiADC-VM on Azure Cloud Platform

There are two methods to configure the FortiADC instance on Azure. The first is an automatic method in Marketplace, the second is by using a user uploaded image.

A. Automatically upload the image

Starting from 5.2.4 we suggest configuring the ADC instance from Marketplace.

1. Go to **Azure > Marketplace >** Search for "FortiADC".

2. Click **Create**.

You have created a FortiADC instance using a default image, which is automatically of the newest version. Now, in this document, you can skip to 4. Create virtual machine on page 9, under "B. Configure the FortiADC Instance using the user uploaded image."

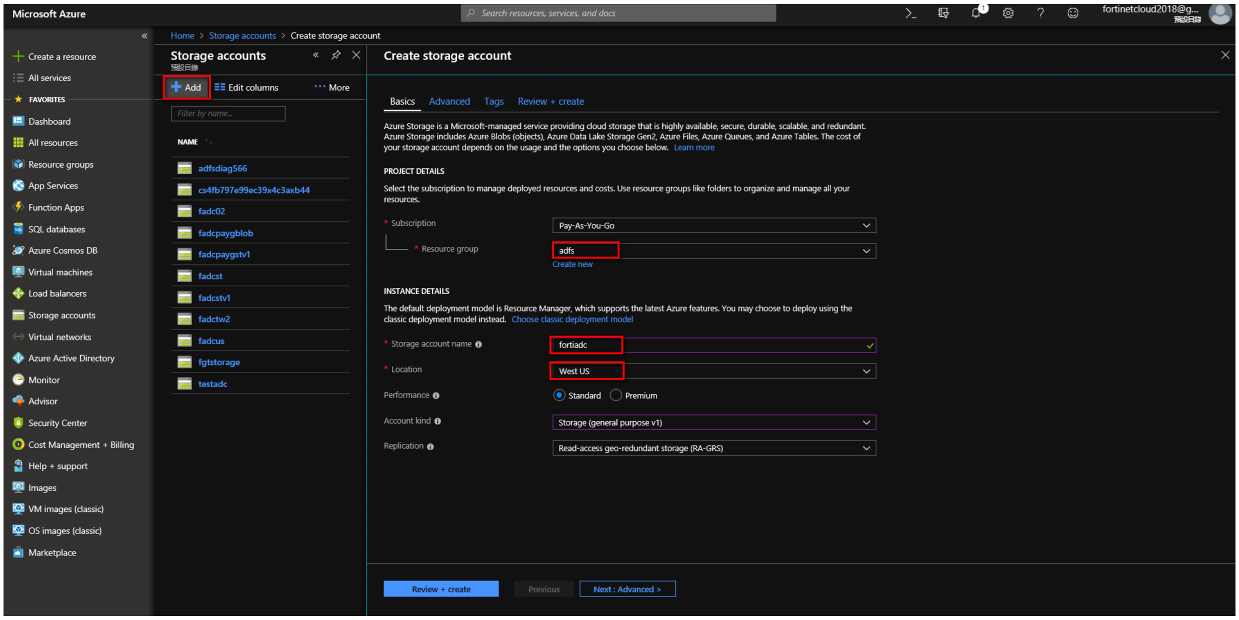
B. Configure the FortiADC Instance using the user uploaded image

1. Upload boot.vhd to blobb

Download FortiADC image from https://support.fortinet.com. Such as:

FAD_AZURE-V500-buildXXXX-FORTINET.out.azure.zip

Unzip it. You will find the file boot.vhd. Navigate to Home > **Storage accounts.** Create a storage account, select “Resource”, write “Storage account name”, select “Location."



Create storage account

Basics | Advanced | Tags | Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. 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: Pay-As-You-Go

* Resource group: adfs

Create new

INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. Choose classic deployment model

* Storage account name: fortiadc

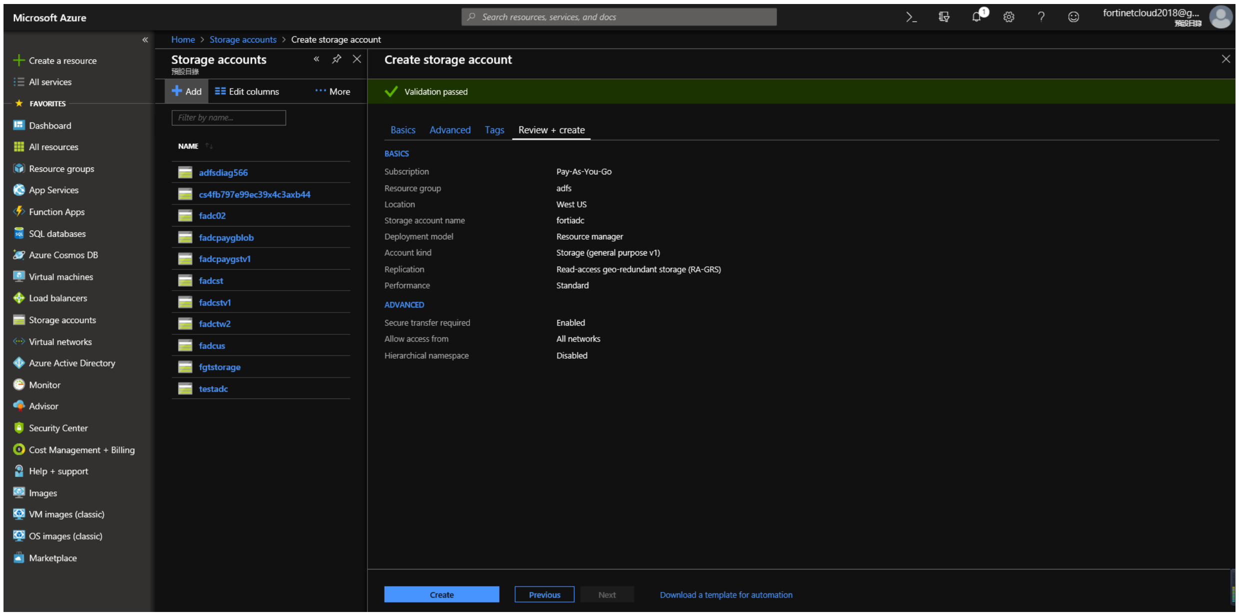
* Location: West US

Performance: ● Standard ○ Premium

Account kind: Storage (general purpose v1)

Replication: Read-access geo-redundant storage (RA-GRS)

Create storage account



Create storage account

✓ Validation passed

Basics | Advanced | Tags | Review + create

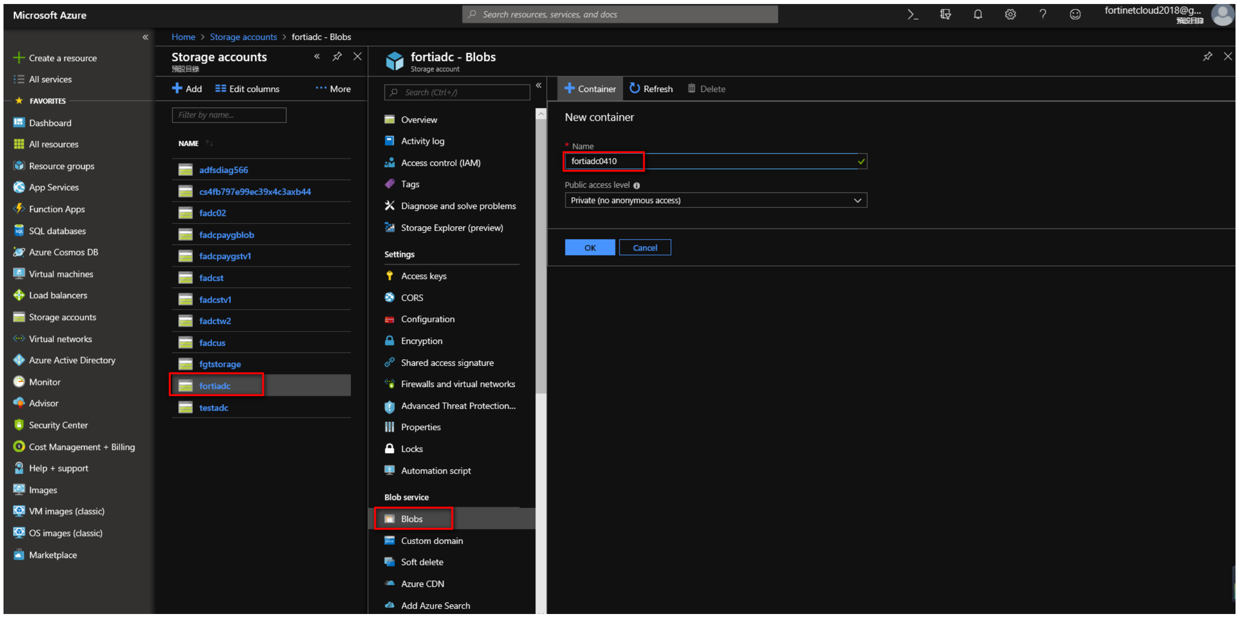
BASICS

Subscription	Pay-As-You-Go
Resource group	adfs
Location	West US
Storage account name	fortiadc
Deployment model	Resource manager
Account kind	Storage (general purpose v1)
Replication	Read-access geo-redundant storage (RA-GRS)
Performance	Standard

ADVANCED

Secure transfer required	Enabled
Allow access from	All networks
Hierarchical namespace	Disabled

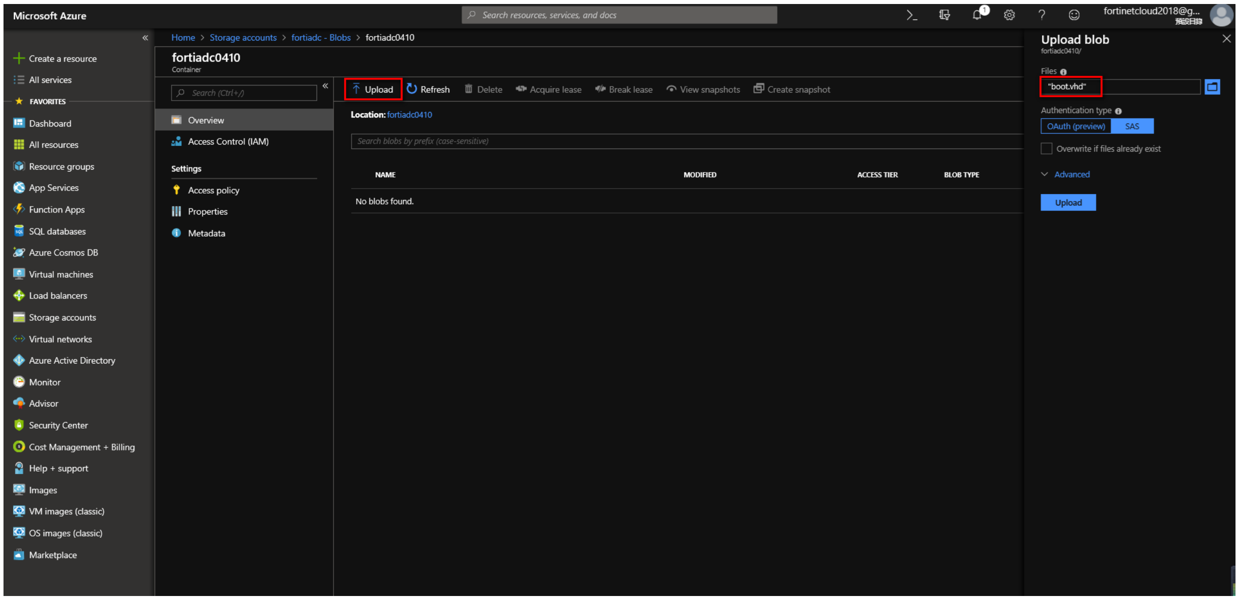
In the newly created **storage account**, add a new **container**, then upload the file boot.vhd.



New container

* Name: fortiadc0410

Public access level: Private (no anonymous access)



Location: fortiadc0410

NAME	MODIFIED	ACCESS TIER	BLOB TYPE
No blobs found.			

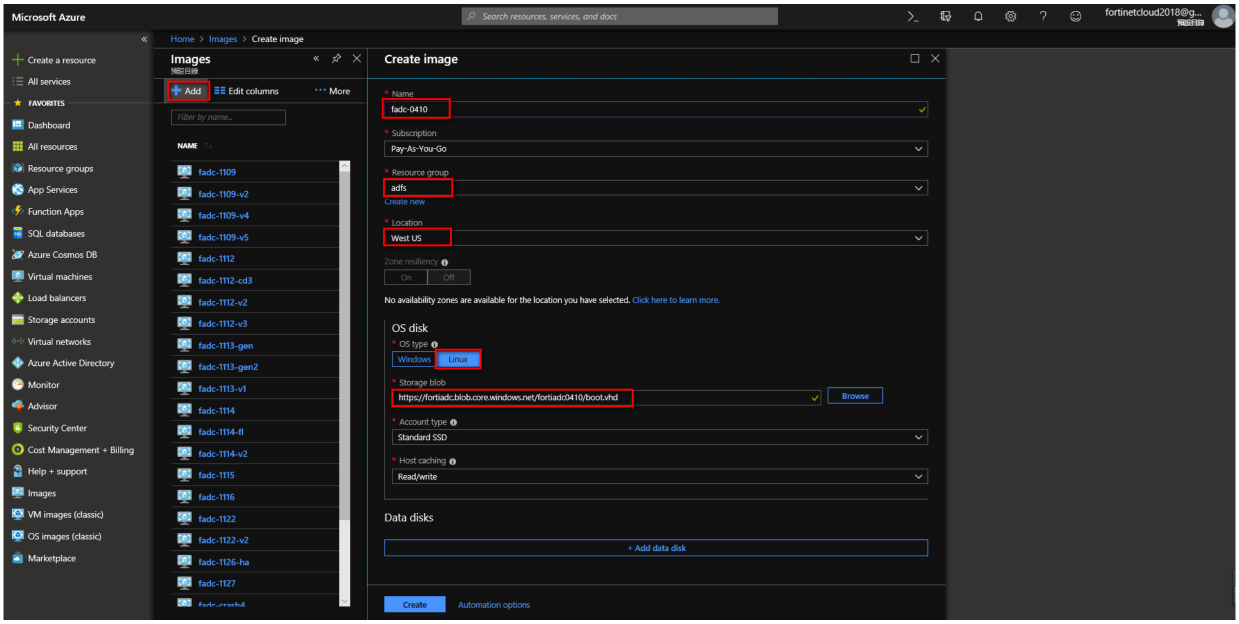
Files: "boot.vhd"

Authentication type: OAuth (preview) SAS

□ Overwrite if files already exist

2. Create image from boot.vhd.

Navigate to **Home > Images > Create image.** Write in a name, select a resource group, choose a location, **set the OS type to Linux**, select the previous file boot.vhd. Then select account type as **Host Caching**.



Create image

- Name: fadc-0410
- Subscription: Pay-As-You-Go
- Resource group: adfs
- Location: West US
- Zone resiliency: On / Off

No availability zones are available for the location you have selected. Click here to learn more.

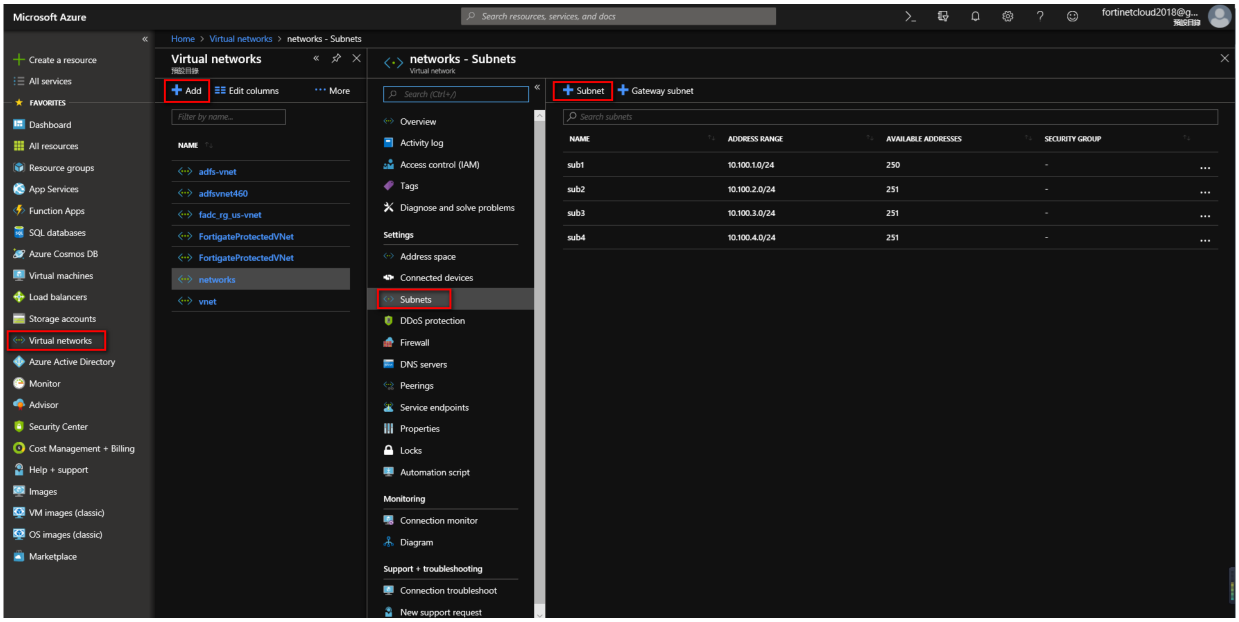
OS disk

- OS type: Linux
- Storage blob: https://fortiadc.blob.core.windows.net/fortiadc0410/boot.vhd
- Account type: Standard SSD
- Host caching: Read/write

Data disks

3. Create virtual networks

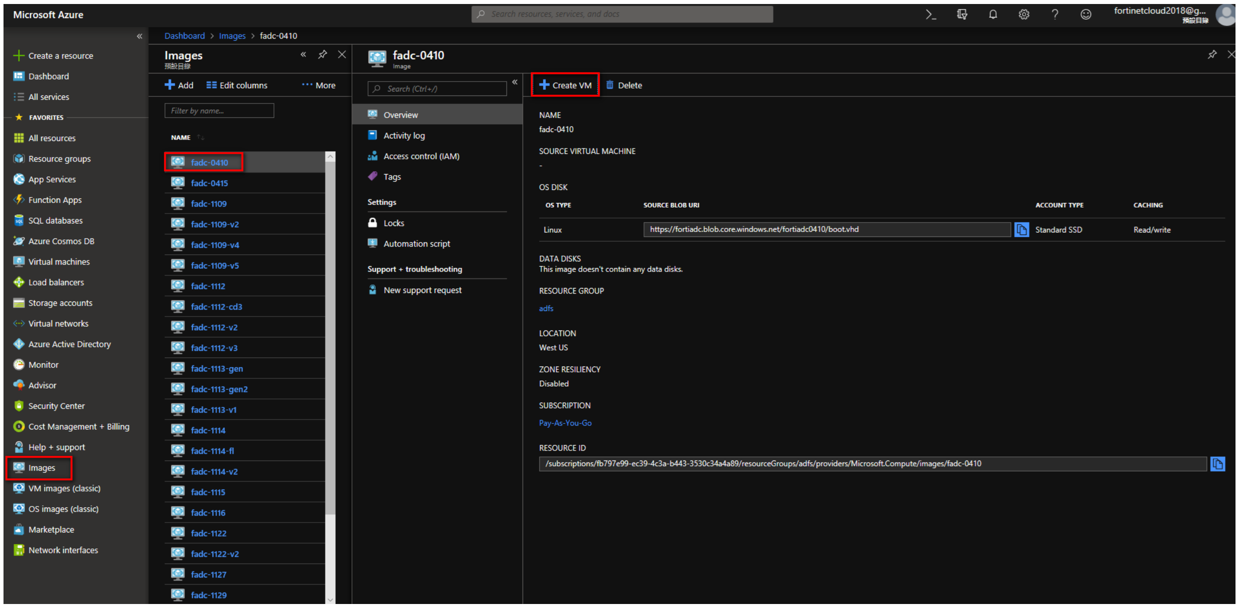
Navigate to **Home > Virtual Networks**, click **Add** to create a virtual network, then add a subnet.



NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
sub1	10.100.1.0/24	250	-
sub2	10.100.2.0/24	251	-
sub3	10.100.3.0/24	251	-
sub4	10.100.4.0/24	251	-

4. Create virtual machine

You can go to the Virtual Machine page to create a VM, though you can also go from the image itself to create a VM. Navigate to the Images page, choose the image you want, then click Create VM.



NAME
fadc-0410

SOURCE VIRTUAL MACHINE
-

OS DISK

OS TYPE	SOURCE BLOB URI	ACCOUNT TYPE	CACHING
Linux	https://fortiadc.blob.core.windows.net/fortiadc0410/boot.vhd	Standard SSD	Read/write

DATA DISKS
This image doesn't contain any data disks.

RESOURCE GROUP
adfs

LOCATION
West US

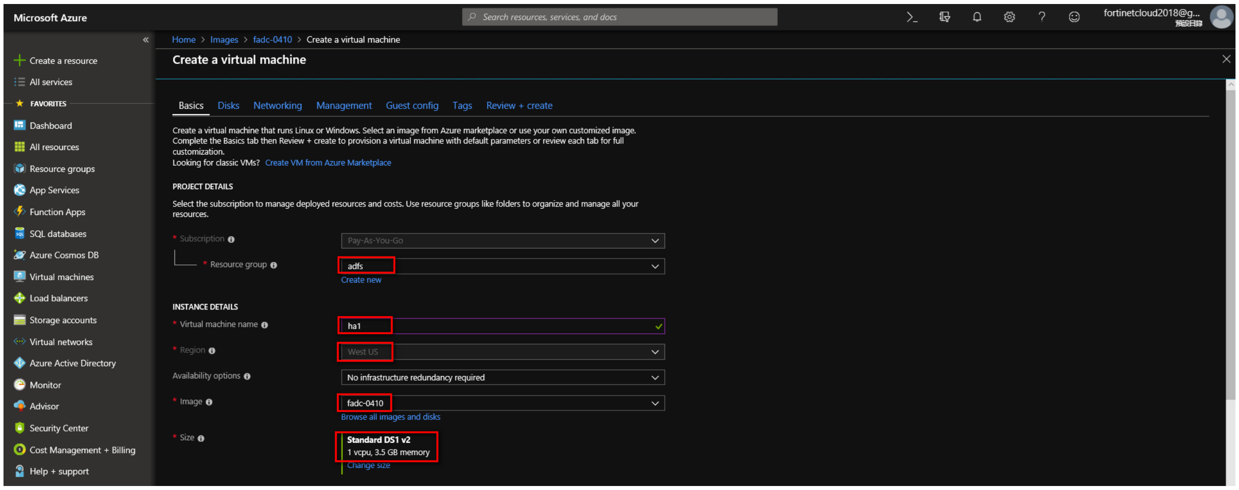
ZONE RESILIENCY
Disabled

SUBSCRIPTION
Pay-As-You-Go

RESOURCE ID
/subscriptions/fb797e99-ec39-4c3a-b443-3530c34a4a89/resourceGroups/adfs/providers/Microsoft.Compute/images/fadc-0410

Choose “Resource group”, write in “Virtual machine name”, choose “Region”, determine the “Image." It's recommended you choose a size that supports at least 2 VCPUs. Also, your memory cannot be lower than 4GB.

For Authentication type, choose “password," determine the Username and Password. For Public inbound ports select **Allow select ports**. For select inbound ports, choose HTTP, HTTPS, SSH.



Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace

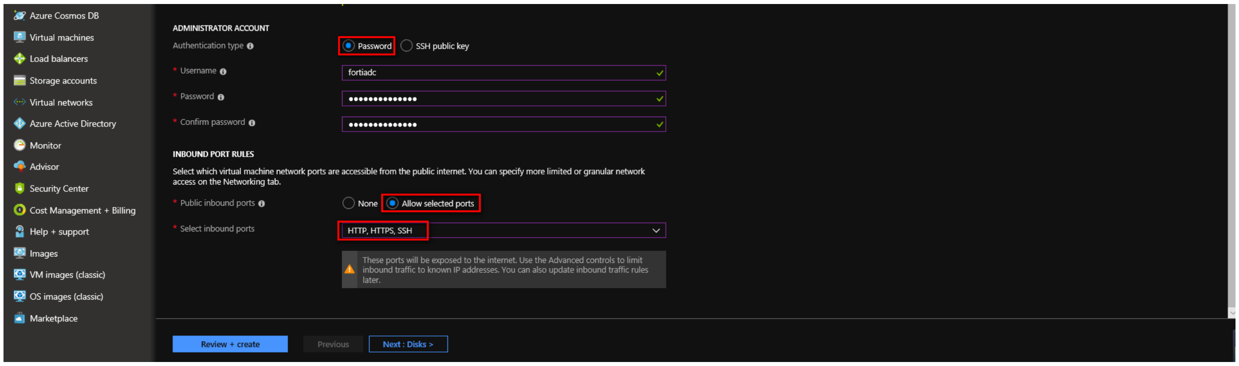
PROJECT DETAILS

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

* Subscription: Pay-As-You-Go
* Resource group: adfs
Create new

INSTANCE DETAILS

* Virtual machine name: ha1
* Region: West US
Availability options: No infrastructure redundancy required
* Image: fadc-0410
Browse all images and disks
* Size: **Standard DS1 v2**
1 vcpu, 3.5 GB memory
Change size



ADMINISTRATOR ACCOUNT

Authentication type: ● Password ○ SSH public key
* Username: fortiadc
* Password: ••••••••••••••
* Confirm password: ••••••••••••••

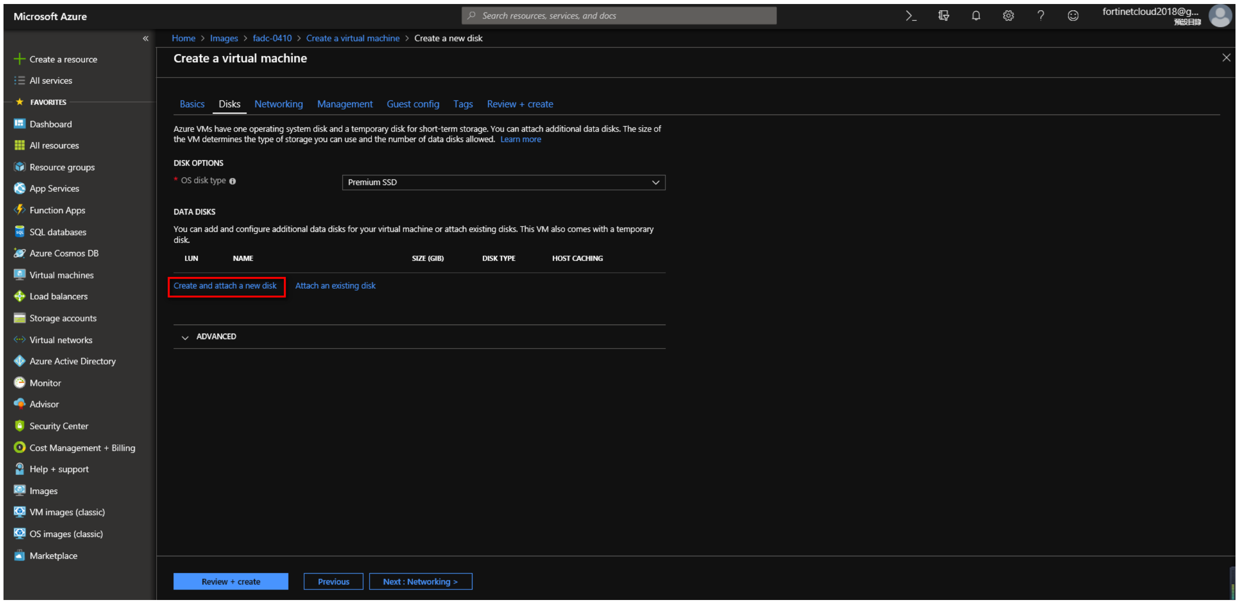
INBOUND PORT RULES

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports: ○ None ● Allow selected ports
* Select inbound ports: HTTP, HTTPS, SSH

These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

Create a log disk for the VM.



Create a virtual machine

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

DISK OPTIONS

* OS disk type: Premium SSD

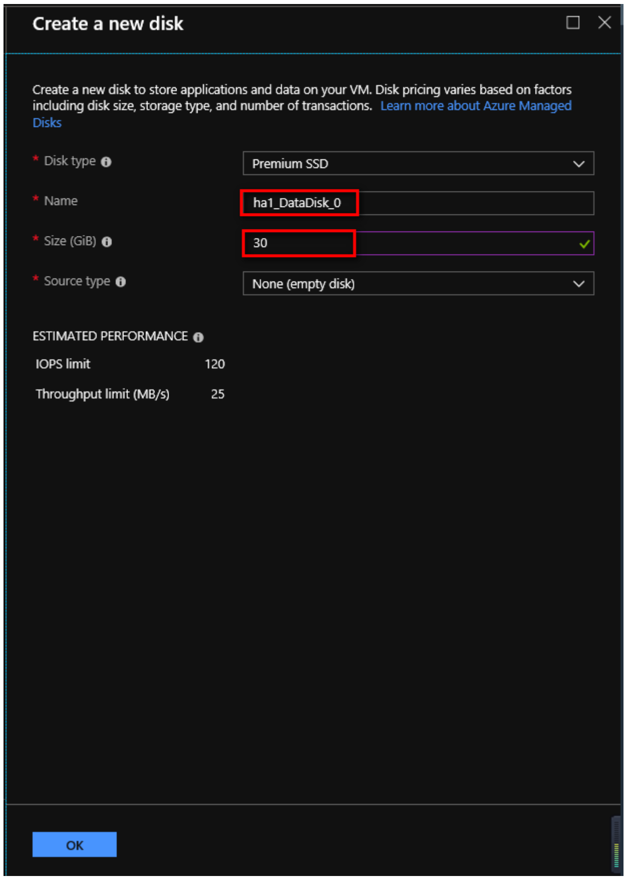
DATA DISKS

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	NAME	SIZE (GIB)	DISK TYPE	HOST CACHING

Create and attach a new disk   Attach an existing disk

ADVANCED



Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. Learn more about Azure Managed Disks

* Disk type: Premium SSD

* Name: ha1_DataDisk_0

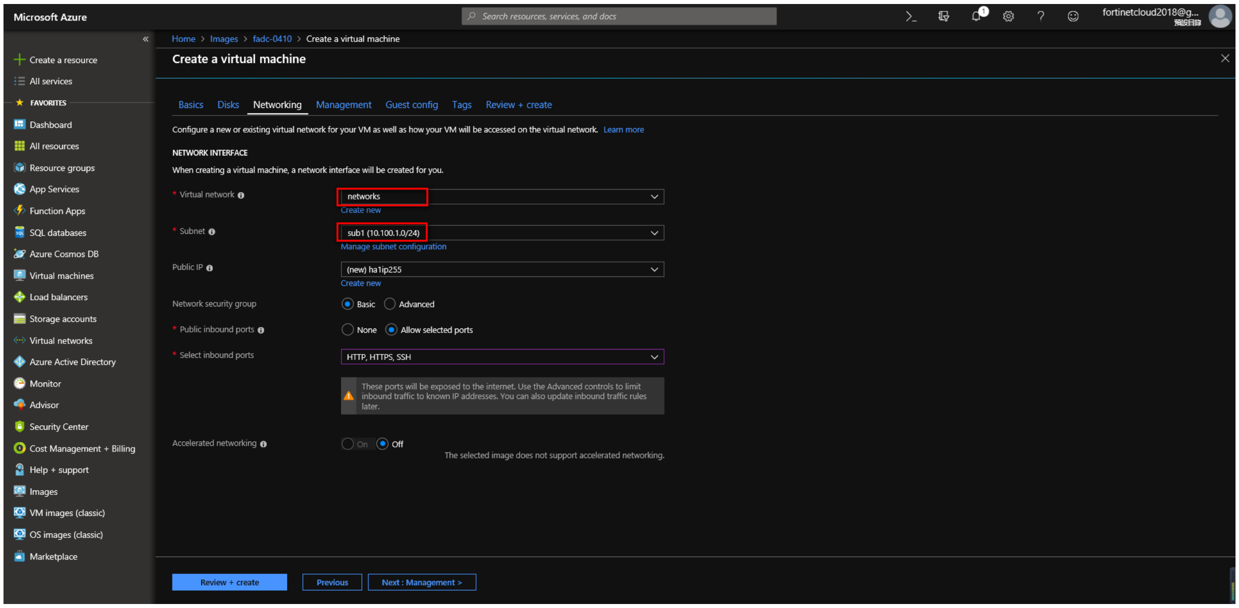
* Size (GiB): 30

* Source type: None (empty disk)

ESTIMATED PERFORMANCE

IOPS limit	120
Throughput limit (MB/s)	25

Configure Networking, select the network and subnet. After creating the VM, you can also add interfaces according to your needs.



Create a virtual machine

Configure a new or existing virtual network for your VM as well as how your VM will be accessed on the virtual network. Learn more

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

* Virtual network: networks (Create new)

* Subnet: sub1 (10.100.1.0/24) (Manage subnet configuration)

Public IP: (new) ha1ip255 (Create new)

Network security group: ● Basic ○ Advanced

* Public inbound ports: ○ None ● Allow selected ports

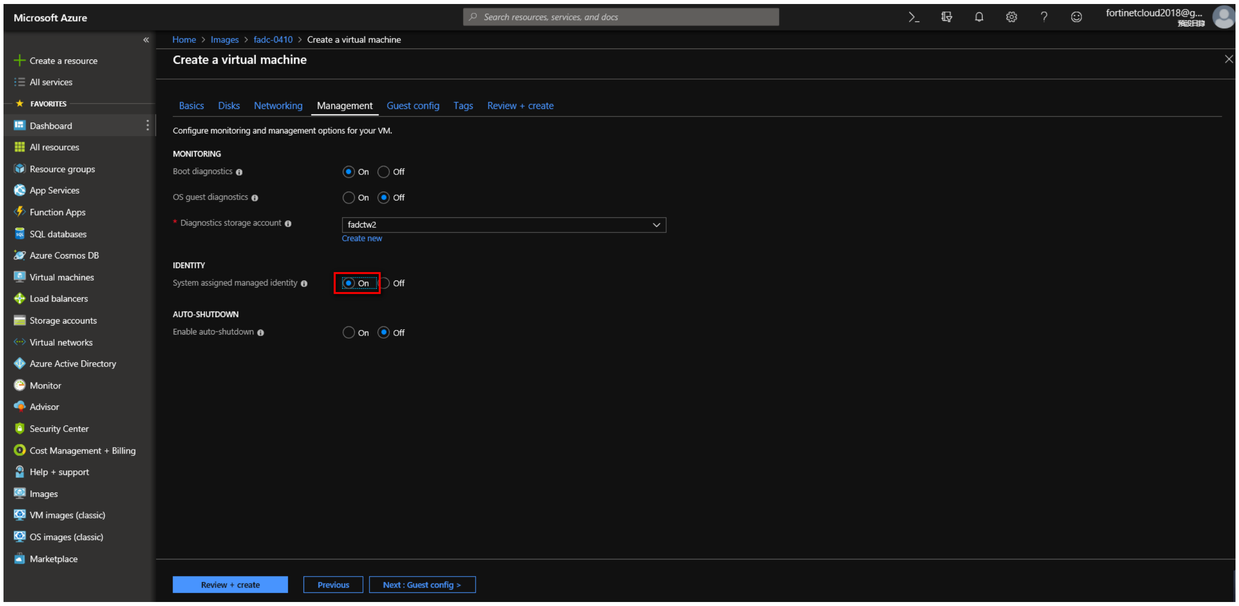
* Select inbound ports: HTTP, HTTPS, SSH

These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

Accelerated networking: ○ On ● Off

The selected image does not support accelerated networking.

Go to VM Management, enable identity for access token.



Create a virtual machine

Configure monitoring and management options for your VM.

MONITORING

Boot diagnostics: ● On ○ Off

OS guest diagnostics: ○ On ● Off

* Diagnostics storage account: fadctw2 (Create new)

IDENTITY

System assigned managed identity: ● On ○ Off

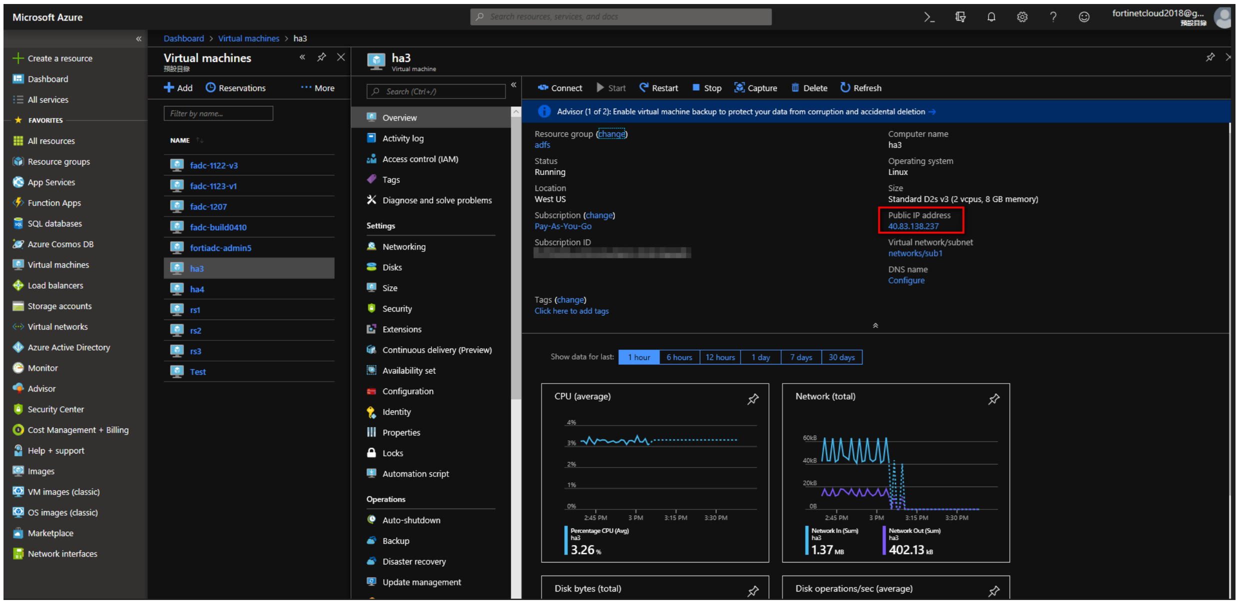
AUTO-SHUTDOWN

Enable auto-shutdown: ○ On ● Off

Afterwards, click “Review + create” to create the virtual machine.

5. Access the FortiADC

In the FortiADC VM, find the public IP address. In a browser, navigate to http://<public_IP_address>. Use the VM username that you previously created; you cannot use the default username 'admin.' Of course you can also go through SSH or HTTPS to access the public IP of the FortiADC.



Advisor (1 of 2): Enable virtual machine backup to protect your data from corruption and accidental deletion →

Resource group (change)
adfs

Status
Running

Location
West US

Subscription (change)
Pay-As-You-Go

Subscription ID
[redacted]

Tags (change)
Click here to add tags

Computer name
ha3

Operating system
Linux

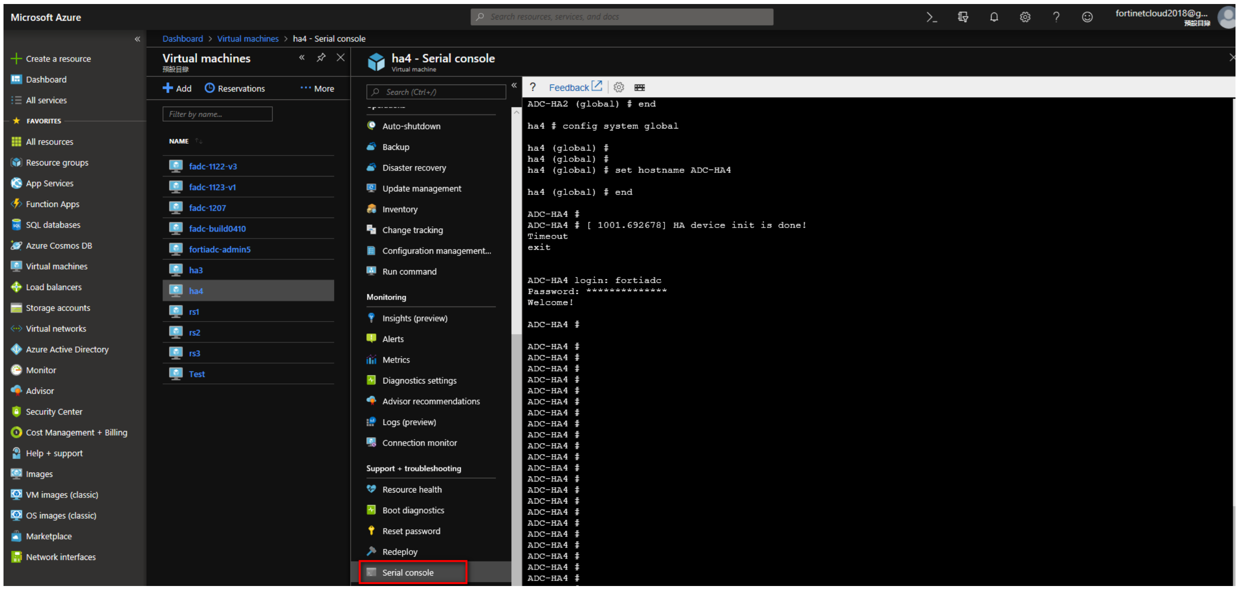
Size
Standard D2s v3 (2 vcpus, 8 GB memory)

Public IP address
40.83.138.237

Virtual network/subnet
networks/sub1

DNS name
Configure

You can also use Connect to serial, to access the FortiADC.



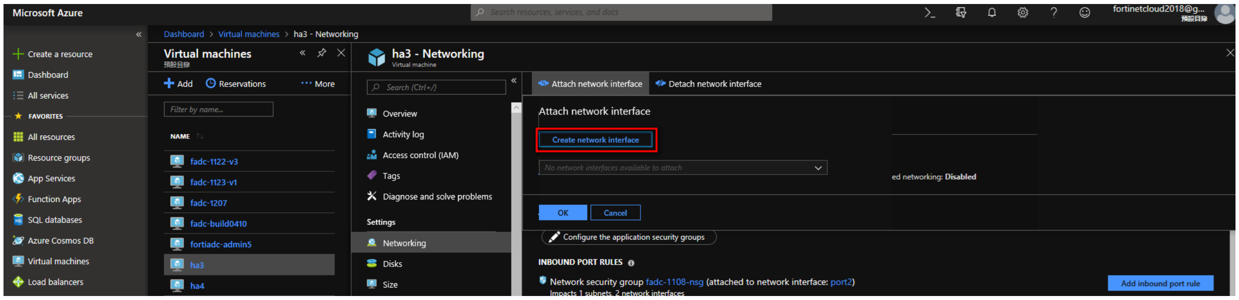
```
ADC-HA2 (global) # end

ha4 # config system global

ha4 (global) #
ha4 (global) #
ha4 (global) # set hostname ADC-HA4

ha4 (global) # end

ADC-HA4 #
ADC-HA4 # [ 1001.692678] HA device init is done!
Timeout
exit


ADC-HA4 login: fortiadc
Password: **************
Welcome!

ADC-HA4 #

ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
ADC-HA4 #
```

6. Add interface and attach it to the FortiADC VM

Test > Networking > Attach network interface.

First you need to know how big the VM size is, that way you know how many network interfaces you can create. To create network interface, and then to stop the VM, go to **Attach Interface**

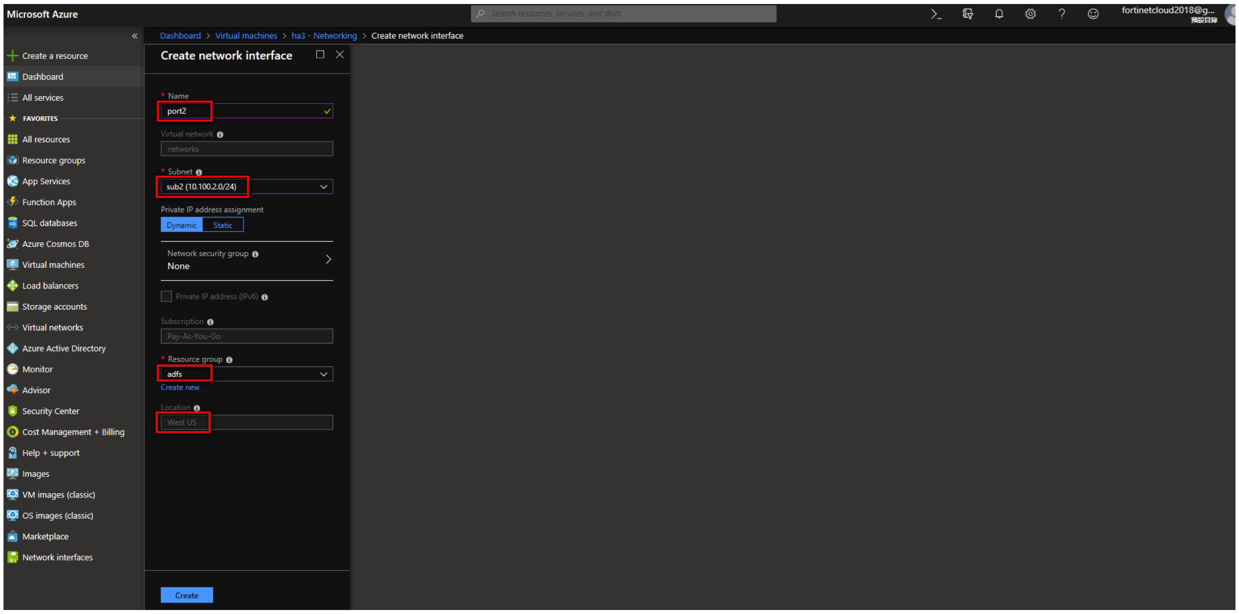
Create network interface



Attach network interface

No network interfaces available to attach

Network security group fadc-1108-nsg (attached to network interface: port2)
Impacts 1 subnets, 2 network interfaces


Microsoft Azure
Dashboard > Virtual machines > ha3 - Networking > Create network interface
Create network interface
Create new
Create

* Name: port2

Virtual network: networks

* Subnet: sub2 (10.100.2.0/24)

Private IP address assignment: Dynamic | Static

Network security group: None

□ Private IP address (IPv6)

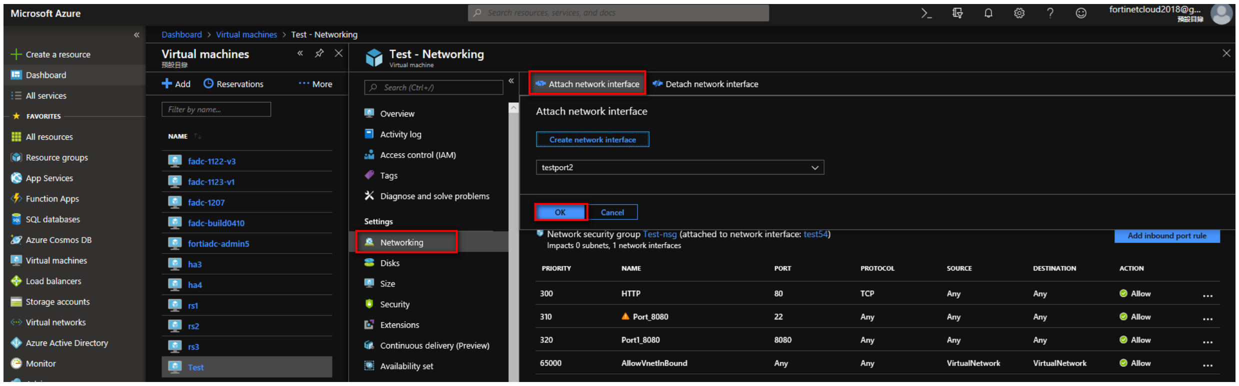
Subscription: Pay-As-You-Go

* Resource group: adfs

Location: West US

Attach interface

Stop VM, enter the “Networking” tab, click “Attach network interface”, and then click OK on the port you want attached.



Attach network interface

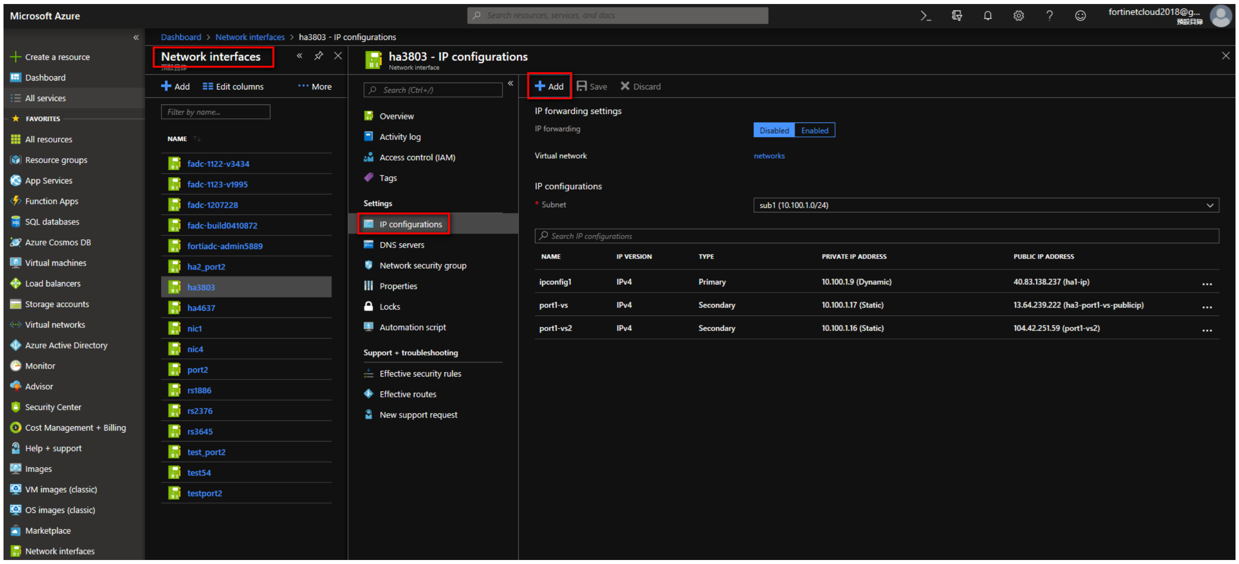
testport2

Network security group Test-nsg (attached to network interface: test54)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	HTTP	80	TCP	Any	Any	✓ Allow
310	⚠ Port_8080	22	Any	Any	Any	✓ Allow
320	Port1_8080	8080	Any	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow

7. Making a secondary IP for the FortiADC VS

Navigate to Network interface page, choose add Seconday IP, go back to IP configurations, click“add” to add a Seconday IP.



IP forwarding settings

IP forwarding: Disabled | Enabled

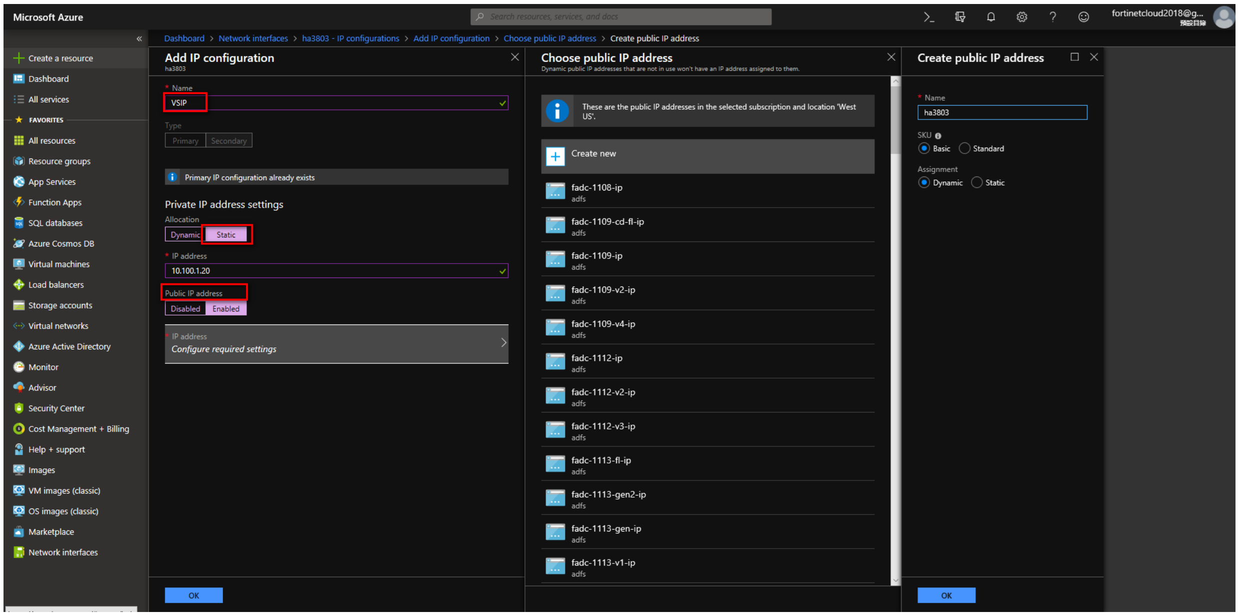
Virtual network: networks

IP configurations

* Subnet: sub1 (10.100.1.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
ipconfig1	IPv4	Primary	10.100.1.9 (Dynamic)	40.83.138.237 (ha1-ip)
port1-vs	IPv4	Secondary	10.100.1.17 (Static)	13.64.239.222 (ha3-port1-vs-publicip)
port1-vs2	IPv4	Secondary	10.100.1.16 (Static)	104.42.251.59 (port1-vs2)

Write Seconday IP Name. For Private IP address it’s suggested you select “Static." Create a Public IP address as needed. If you want the VS to access outside IP’s, you need a public IP. If it’s only for the FortiADC NAT source pool, or if you are using a floating IP, you only need to create private IP addresses.


Microsoft Azure
Dashboard > Network interfaces > ha3803 - IP configurations > Add IP configuration > Choose public IP address > Create public IP address
OK
OK

Add IP configuration

ha3803

* Name: VSIP

Type: Primary | Secondary

Primary IP configuration already exists

Private IP address settings

Allocation: Dynamic | Static

* IP address: 10.100.1.20

Public IP address: Disabled | Enabled

* IP address: Configure required settings

Choose public IP address

Dynamic public IP addresses that are not in use won't have an IP address assigned to them.

These are the public IP addresses in the selected subscription and location 'West US'.

+ Create new

- fadc-1108-ip adfs
- fadc-1109-cd-fl-ip adfs
- fadc-1109-ip adfs
- fadc-1109-v2-ip adfs
- fadc-1109-v4-ip adfs
- fadc-1112-ip adfs
- fadc-1112-v2-ip adfs
- fadc-1112-v3-ip adfs
- fadc-1113-fl-ip adfs
- fadc-1113-gen2-ip adfs
- fadc-1113-gen-ip adfs
- fadc-1113-v1-ip adfs

Create public IP address

* Name: ha3803

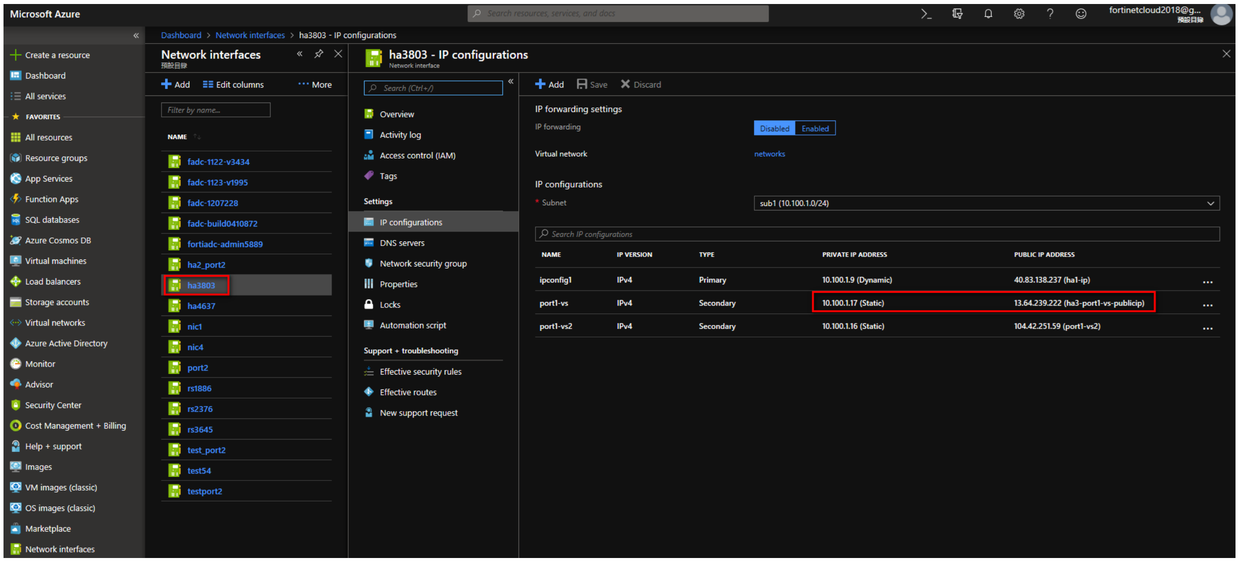
SKU: ● Basic ○ Standard

Assignment: ● Dynamic ○ Static

Example 1

10.100.1.17 is configured on FortiADC VS, 13.64.239.222 is the FortiADC VS's way of accessing the public IP. Client can then use IP 13.64.239.222 to access the VS.

Add 10.100.1.17 to Azure port, and create a public IP.



IP forwarding settings

IP forwarding: Disabled | Enabled

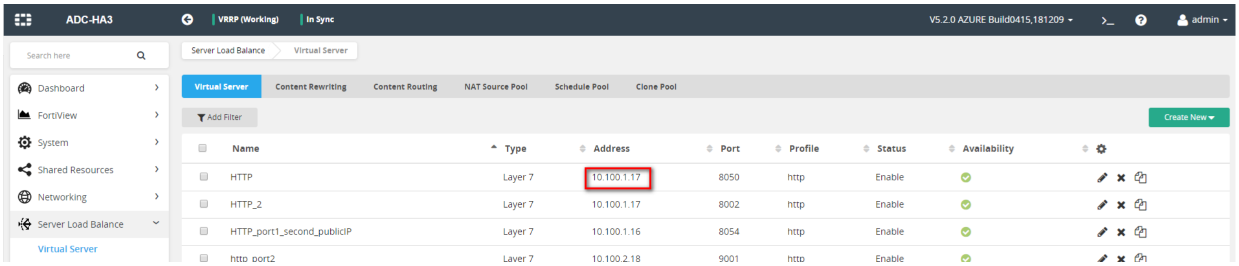
Virtual network: networks

IP configurations

* Subnet: sub1 (10.100.1.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
ipconfig1	IPv4	Primary	10.100.1.9 (Dynamic)	40.83.138.237 (ha1-ip)
port1-vs	IPv4	Secondary	10.100.1.17 (Static)	13.64.239.222 (ha3-port1-vs-publicip)
port1-vs2	IPv4	Secondary	10.100.1.16 (Static)	104.42.251.59 (port1-vs2)

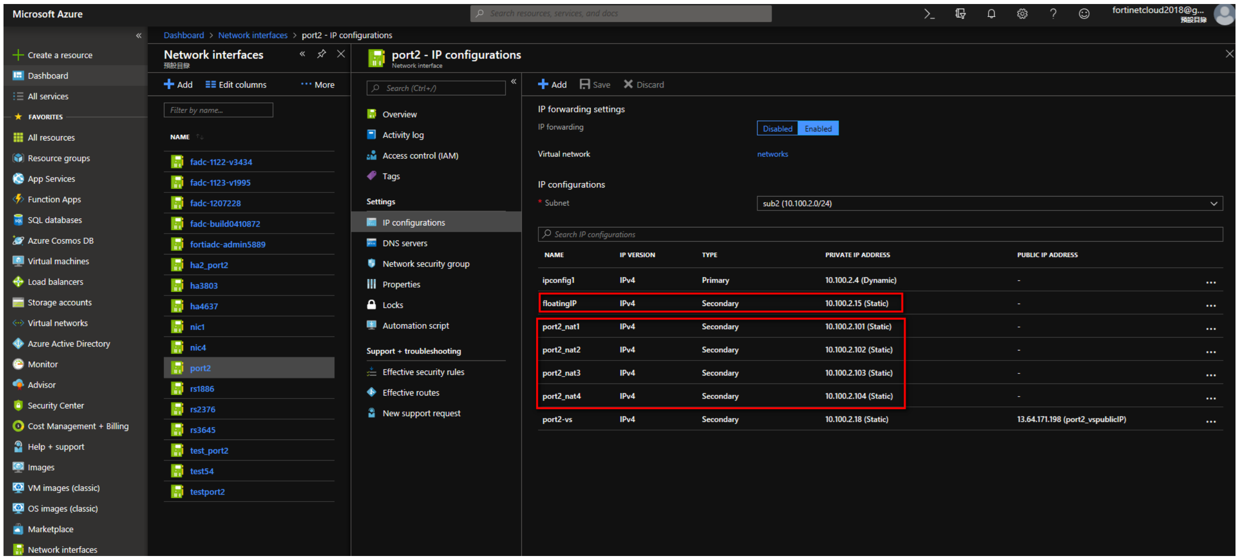
FortiADC VS IP: 10.100.1.17



Name	Type	Address	Port	Profile	Status	Availability
HTTP	Layer 7	10.100.1.17	8050	http	Enable	✓
HTTP_2	Layer 7	10.100.1.17	8002	http	Enable	✓
HTTP_port1_second_publicIP	Layer 7	10.100.1.16	8054	http	Enable	✓
http_port2	Layer 7	10.100.2.18	9001	http	Enable	✓

Example 2

If the FortiADC has a floating IP, you also need to put the floating IP into Azure’s corresponding port; if the FortiADC is using NAT Source Pool, you also need to put the NAT Pool IP to the corresponding port in Azure.



IP forwarding settings

IP forwarding: Disabled | Enabled

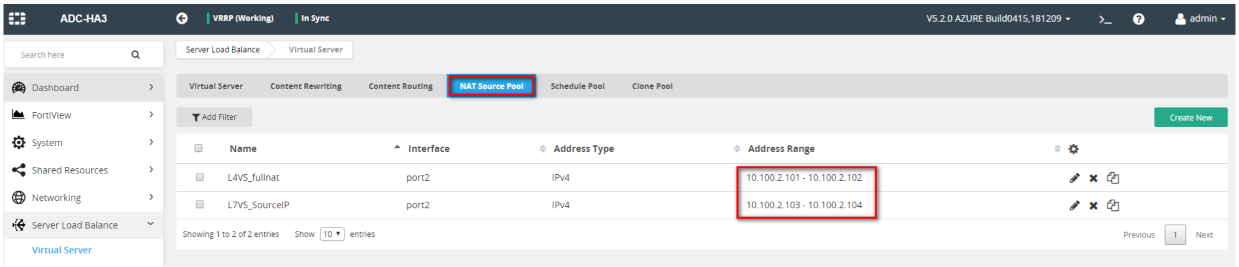
Virtual network: networks

IP configurations

* Subnet: sub2 (10.100.2.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
ipconfig1	IPv4	Primary	10.100.2.4 (Dynamic)	-
floatingIP	IPv4	Secondary	10.100.2.15 (Static)	-
port2_nat1	IPv4	Secondary	10.100.2.101 (Static)	-
port2_nat2	IPv4	Secondary	10.100.2.102 (Static)	-
port2_nat3	IPv4	Secondary	10.100.2.103 (Static)	-
port2_nat4	IPv4	Secondary	10.100.2.104 (Static)	-
port2-vs	IPv4	Secondary	10.100.2.18 (Static)	13.64.171.198 (port2_vspublicIP)

FortiADC NAT Source Pool

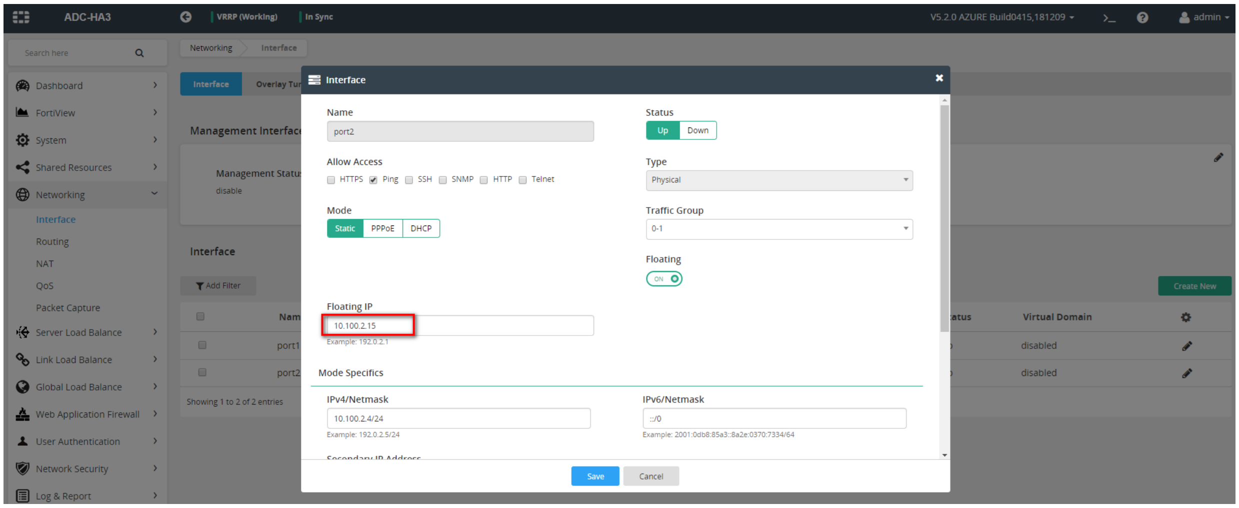


Server Load Balance > Virtual Server

Name	Interface	Address Type	Address Range
L4VS_fullnat	port2	IPv4	10.100.2.101 - 10.100.2.102
L7VS_SourceIP	port2	IPv4	10.100.2.103 - 10.100.2.104

Showing 1 to 2 of 2 entries Show 10 entries

FortiADC Floating IP



Interface

Name: port2

Status: Up Down

Allow Access: □ HTTPS ☑ Ping □ SSH □ SNMP □ HTTP □ Telnet

Type: Physical

Mode: Static PPPoE DHCP

Traffic Group: 0-1

Floating: ON

Floating IP: 10.100.2.15
Example: 192.0.2.1

Mode Specifics

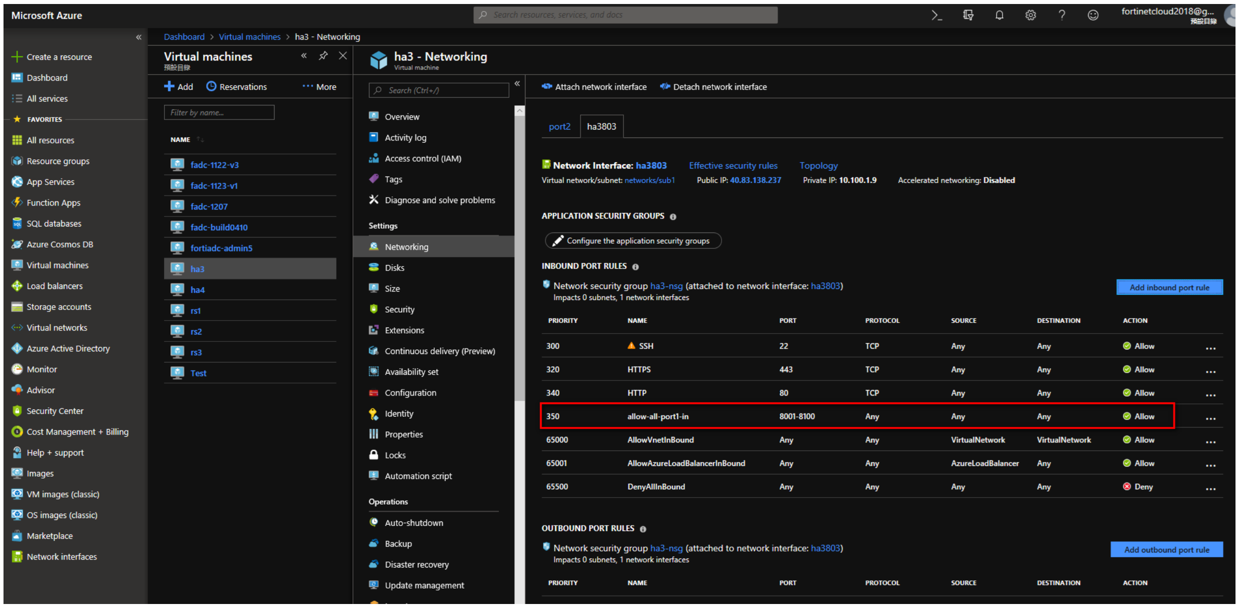
IPv4/Netmask: 10.100.2.4/24
Example: 192.0.2.5/24

IPv6/Netmask: ::/0
Example: 2001:0db8:85a3::8a2e:0370:7334/64

Secondary IP Address

8. Create a rule for Azure interface

According to the VS's protocol and port, in Azure's corresponding port you must create a rule; for example if the port is 8050 (as shown below), you need to create a rule on Azure so that the user can access the VS.



Network Interface: ha3803
Virtual network/subnet: networks/sub1 Public IP: 40.83.138.237 Private IP: 10.100.1.9 Accelerated networking: Disabled

APPLICATION SECURITY GROUPS

INBOUND PORT RULES

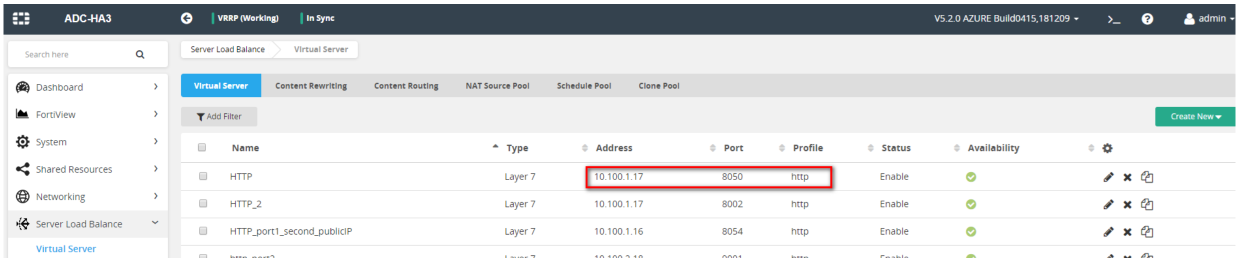
Network security group ha3-nsg (attached to network interface: ha3803)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	SSH	22	TCP	Any	Any	Allow
320	HTTPS	443	TCP	Any	Any	Allow
340	HTTP	80	TCP	Any	Any	Allow
350	allow-all-port1-in	8001-8100	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

OUTBOUND PORT RULES

Network security group ha3-nsg (attached to network interface: ha3803)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION



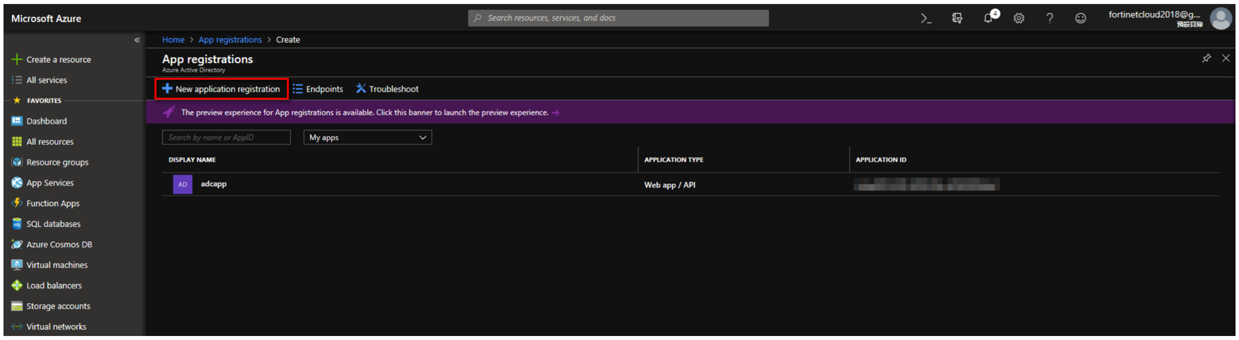
Name	Type	Address	Port	Profile	Status	Availability
HTTP	Layer 7	10.100.1.17	8050	http	Enable	✓
HTTP_2	Layer 7	10.100.1.17	8002	http	Enable	✓
HTTP_port1_second_publicIP	Layer 7	10.100.1.16	8054	http	Enable	✓

9. Requires access token to use Azure RestAPI

If using FortiADC's HA-VRRP, FortiADC needs to use the Azure rest API, and then you need to make the following configurations:

9.1 Create Azure App

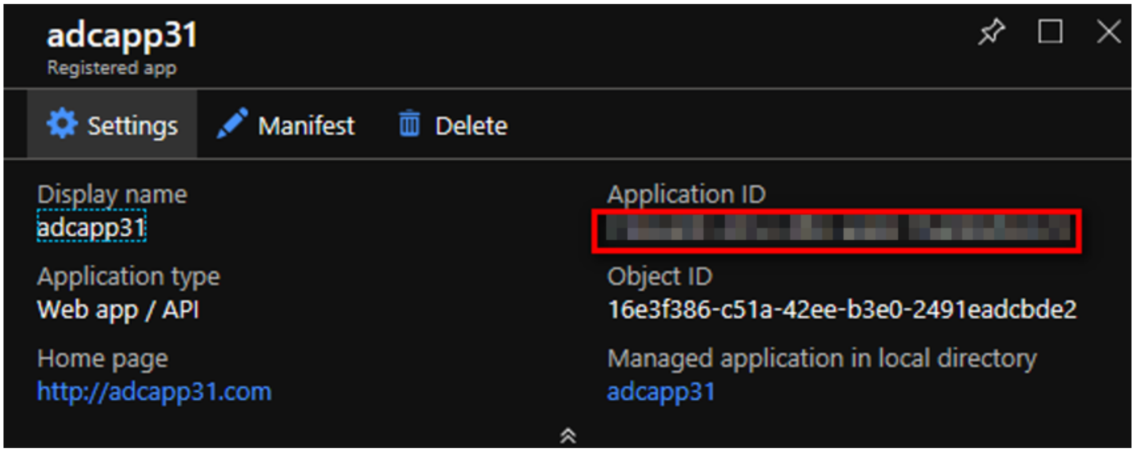
Write in the Name Application type, choosing "Web app / API", and write in the Sign-on URL.



The preview experience for App registrations is available. Click this banner to launch the preview experience. →

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
AD adcapp	Web app / API	[redacted]

Client ID：Application ID is the Client ID



Display name
adcapp31

Application type
Web app / API

Home page
http://adcapp31.com

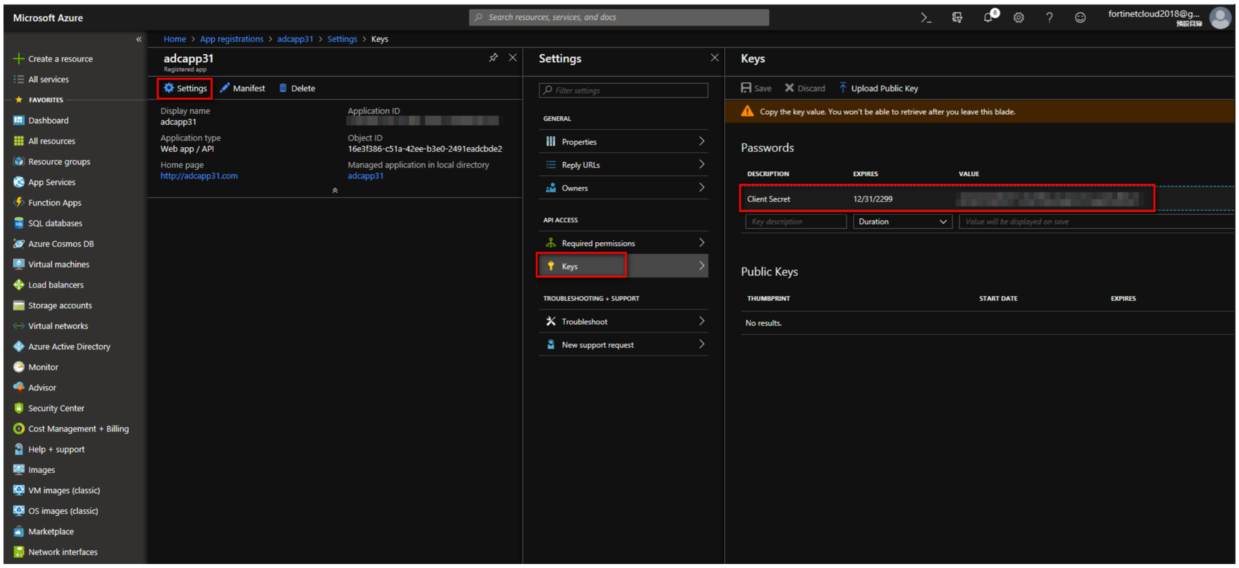
Application ID
[redacted]

Object ID
16e3f386-c51a-42ee-b3e0-2491eadcbde2

Managed application in local directory
adcapp31

Creating a Client Secret

Click "settings", enter the "Keys" tab. In "Key description" go to"Client Secret", selecting "Expires." Then save; it will automatically create "Value." This created "Value" is the Client Secret. **Copy the client secret for future use on the FortiADC.**



Home > App registrations > adcapp31 > Settings > Keys

adcapp31
Registered app

Display name: adcapp31
Application ID: [redacted]
Application type: Web app / API
Object ID: 16e3f386-c51a-42ee-b3e0-2491eadcbde2
Home page: http://adcapp31.com
Managed application in local directory: adcapp31

Keys

Copy the key value. You won't be able to retrieve after you leave this blade.

Passwords

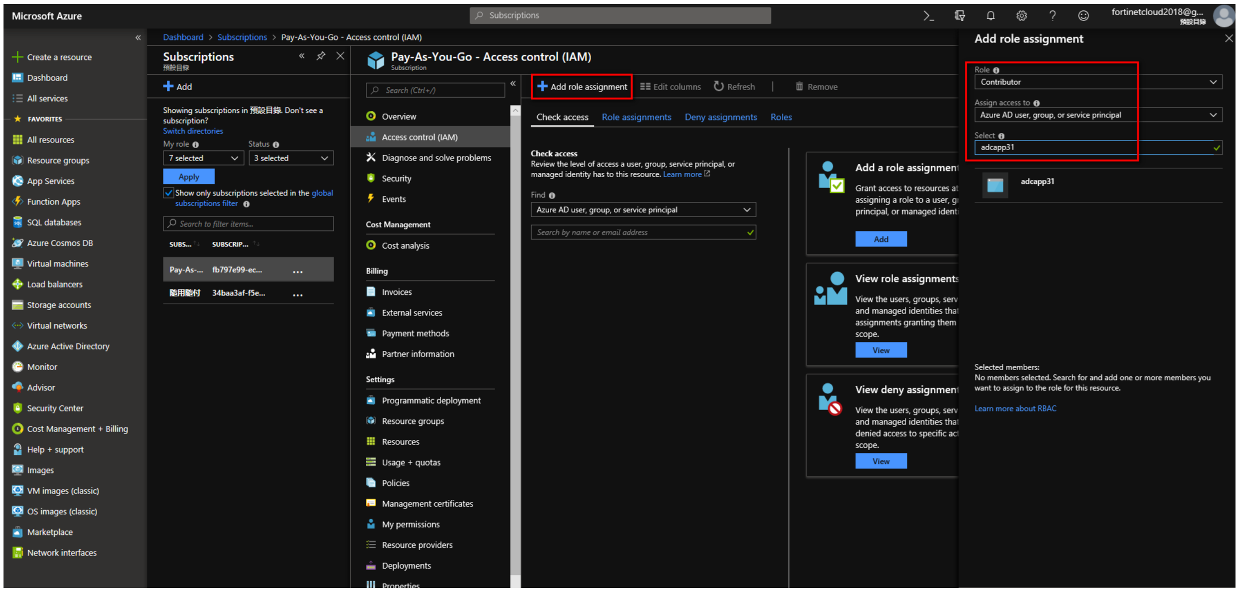
DESCRIPTION	EXPIRES	VALUE
Client Secret	12/31/2299	[redacted]
Key description	Duration	Value will be displayed on save

Public Keys

THUMBPRINT	START DATE	EXPIRES
No results.		

Add role to subscription. Choose Contributor to get R/W access to Azure service.

Navigate to **Home > Subscriptions**. Choose Subscription, such as Pay-As-You-Go, enter Access control (IAM). Add role assignment, choosing “Contributor." Assign access to choose “Azure AD user,group,or service principal." **Use the Azure app you just created**.



Dashboard > Subscriptions > Pay-As-You-Go - Access control (IAM)

Pay-As-You-Go - Access control (IAM)
Subscription

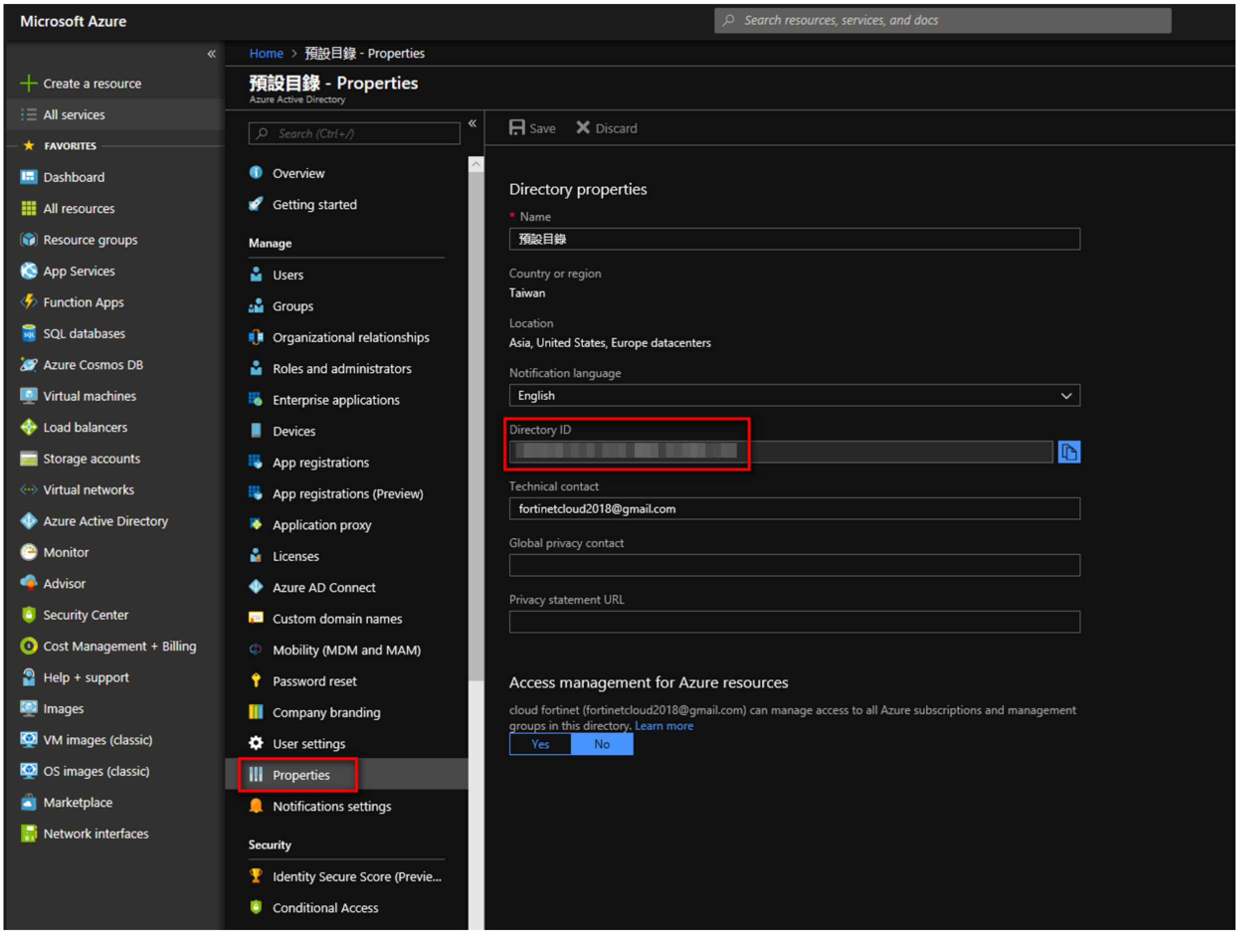
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Find: Azure AD user, group, or service principal

Add role assignment
Role: Contributor
Assign access to: Azure AD user, group, or service principal
Select: adcapp31

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.
Learn more about RBAC

Tenant ID:

Navigate to Home > Properties, copy the Tenant ID.



Directory properties

* Name: 預設目錄

Country or region: Taiwan

Location: Asia, United States, Europe datacenters

Notification language: English

Directory ID: [redacted]

Technical contact: fortinetcloud2018@gmail.com

Global privacy contact:

Privacy statement URL:

Access management for Azure resources

cloud fortinet (fortinetcloud2018@gmail.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more

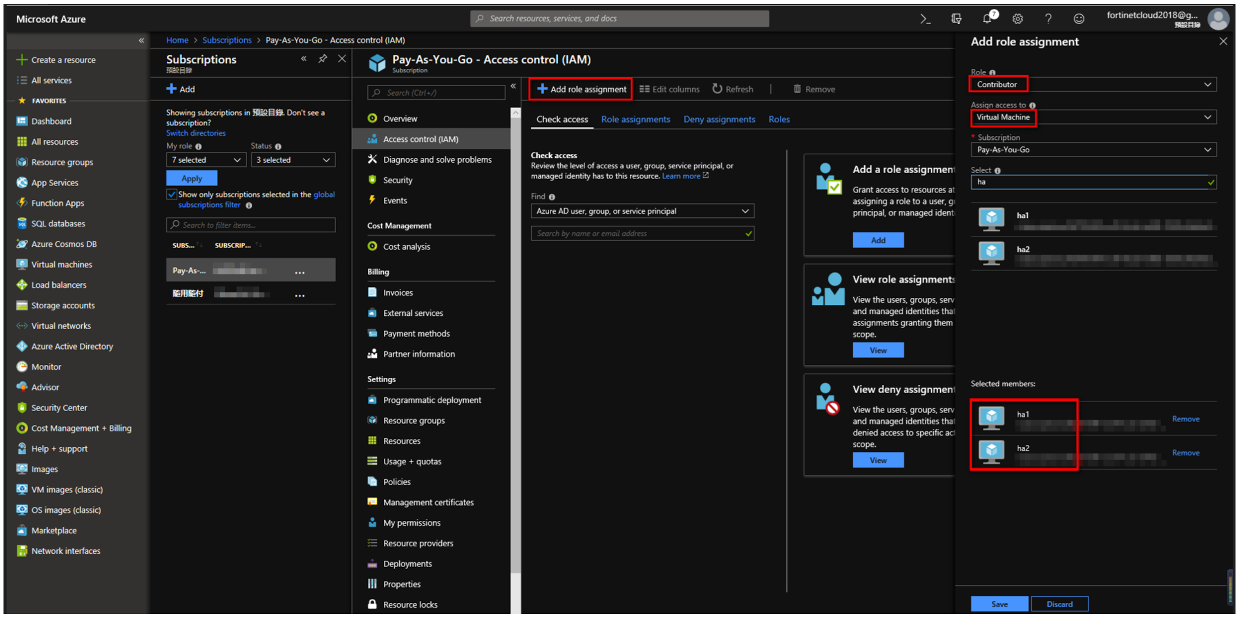
Yes No

Config Client ID, Client Secret and Tenant ID on FortiADC:

```
config system azure
   set tenant-id XXXXXXXXXXXXXXXXXXXXX
   unset subscription-id
   set client-id XXXXXXXXXXXXXXXXXXXXXXXXXXX
   set client-secret XXXXXXXXXXXXXXXXXXXXXXXXXXXX
   set azure-region global
   unset resource-group
end
```

9.2 Grant access to the managed identity

Choose the Role as Contributor, and assign access to the Virtual Machine. Then select the FortiADC's that use the Rest API.



Role: Contributor

Assign access to: Virtual Machine

Subscription: Pay-As-You-Go

Select: ha

ha1

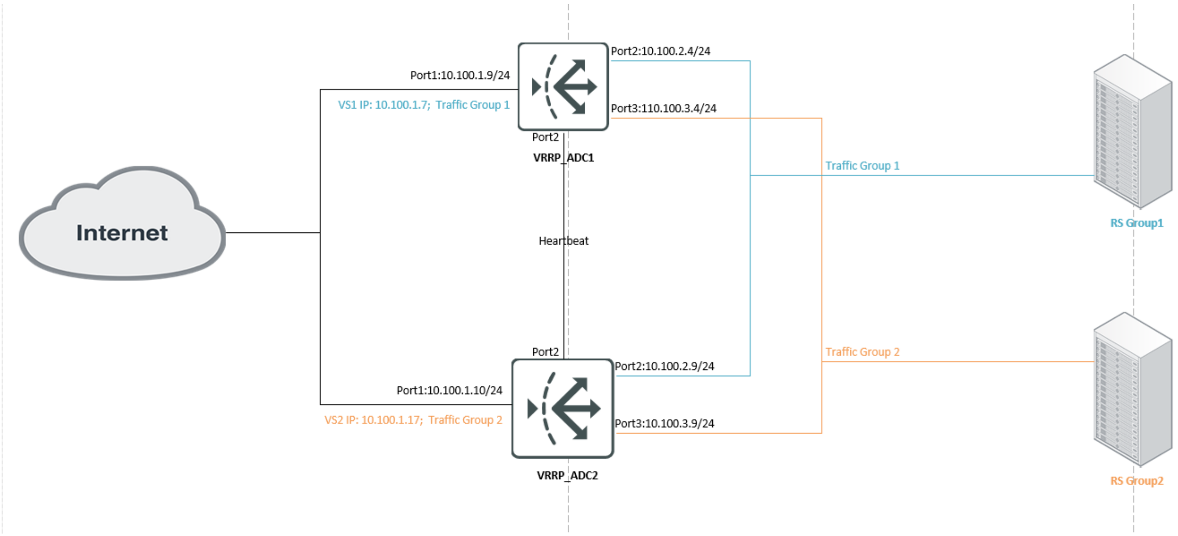
ha2

Selected members:

ha1

ha2

Example: Set VS on Azure in HA-VRRP mode



Configure HA on FortiADC1

```
config system ha
set mode active-active-vrrp
set hbdev port2
set datadev port2
set group-id 31
set local-node-id 1
set group-name azure_group
set config-priority 200
set override enable
set l7-persistence-pickup enable
set l4-persistence-pickup enable
set l4-session-pickup enable
set hb-type unicast
set local-address 10.100.2.4
set peer-address 10.100.2.9
end
```

Configure HA on FortiADC2

```
config system ha
set mode active-active-vrrp
set hbdev port2
set datadev port2
set group-id 31
set group-name azure_group
set override enable
set l7-persistence-pickup enable
set l4-persistence-pickup enable
set l4-session-pickup enable
set hb-type unicast
set local-address 10.100.2.9
set peer-address 10.100.2.4
end
```

Configure Traffic-Group on FortiADC

```
config system traffic-group
   edit "0-1"
   set failover-order 0 1
   set preempt enable
next
   edit "1-0"
   set failover-order 1 0
   set preempt enable
next
end
```

Configure tenant-id client-id and client secret on FortiADC

```
config system azure
   set tenant-id 0483fd85-be76-4370-8880-e4ab864c
   set client-id 4cdad0f5-4f28-42f8-8f3e-b5561
   set client-secret ENC cLzCNMaHqye1rLx0Ys8BPlwz9Oeb9QWyO0CJ70hSwZy7
end
```

Configure VS on FortiADC

```
config load-balance real-server
   edit "RS1"
   set ip 10.100.2.6
   next
   edit "RS2"
   set ip 10.100.3.6
   next
end

config load-balance pool
```

```
   edit "Pool_1"
   set real-server-ssl-profile NONE
   config pool_member
   edit 1
   set pool_member_cookie rs1
   set real-server RS1
   next
end
next
   edit "Pool_2"
   set real-server-ssl-profile NONE
   config pool_member
   edit 1
   set pool_member_cookie rs1
   set real-server RS2
   next
end
next
end

config load-balance virtual-server
   edit "L7_HTTP_Public"
   set type l7-load-balance
   set interface port1
   set ip 10.100.1.7
   set port 8003
   set load-balance-profile HTTP
   set load-balance-method LB_METHOD_ROUND_ROBIN
   set load-balance-pool Pool_1
   set traffic-log enable
   set traffic-group 0-1
   set fortiview enable
next

edit "L7_HTTP_Public_Secondary"
   set type l7-load-balance
   set interface port1
   set ip 10.100.1.17
   set port 8003
   set load-balance-profile HTTP
   set load-balance-method LB_METHOD_ROUND_ROBIN
   set load-balance-pool Pool_2
   set traffic-log enable
   set traffic-group 1-0
   set fortiview enable
next
end
```

Important notes

1. In L4_VS DNAT mode or L7_VS mode enabled "client-address", make sure FortiADC is the gateway for RS.
2. If you want to use L4_VS DNAT, you have to go to the outgoing port in Azure and enable IP forwarding, because the RS source IP is not the same as the FortiADC outgoing port IP.
3. Does not support HA-AP and HA-AA mode.
4. Only supports HA-VRRP group with two FortiADC's currently.
5. If you configure L4VS “NAT Source Pool” or SNAT “Translation to IP Address”, Floating IP etc, you must add these IP's to the instance interface via secondary IP on Azure.
6. If you manually change the FortiADC’s configuration, for example by changing VS IP, second IP, floating IP, NAT Source Pool, or changing the VS traffic group, you must make the corresponding changes on Azure.
7. It is suggested that you use a static IP on Azure, because in the case of an FortiADC HA failover the dynamic IP may change, so the Azure IP and the FortiADC IP will not be the same.
8. VS IP, Floating IP, NAT Source Pool cannot be the same as the interface primary IP, because in the case of an FortiADC HA failover there may be issues.
9. You have to use log disk, otherwise some functions cannot be used correctly, like VRRP.
10. FortiADC's HSM client, Luna HSM version 7.2 or higher, is compatible with Azure HSM.