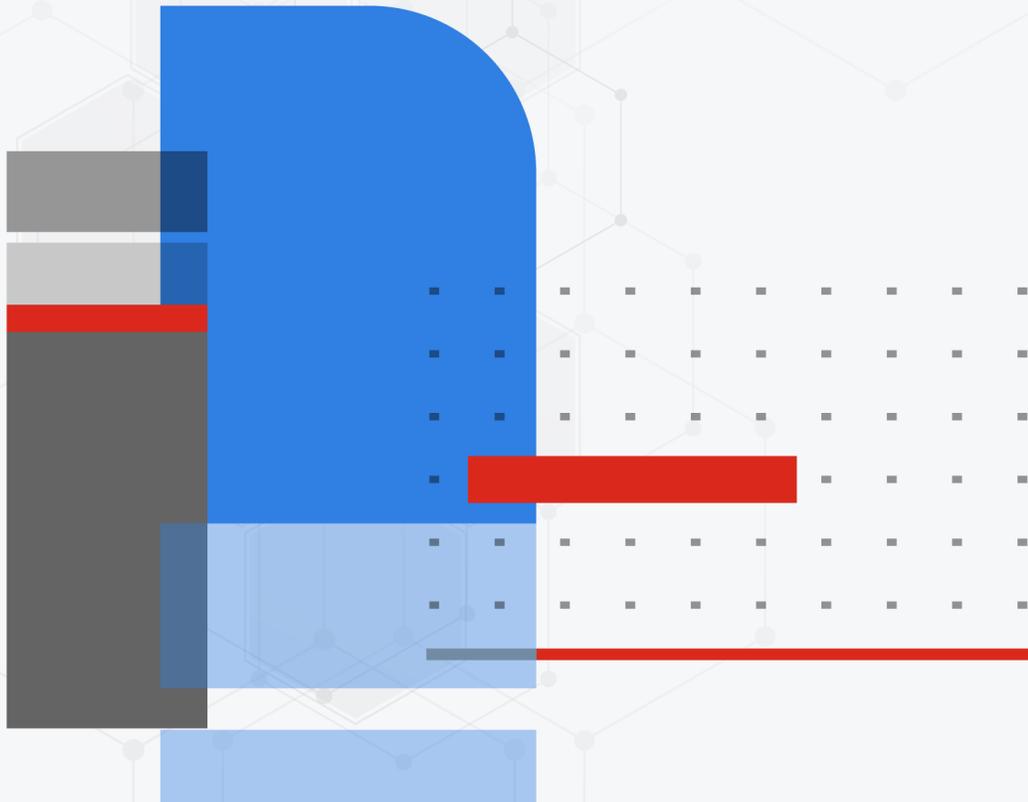


OpenStack Integration Guide

FortiADC 7.6.1



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



June 8, 2022

FortiADC 7.6.1 OpenStack Integration Guide

01-544-677187-20220608

TABLE OF CONTENTS

Change Log	4
Introduction	5
Implementation	6
FortiADC Octavia driver and agent in OpenStack environment	6
Deploying a FortiADC-VM instance in an OpenStack environment	7
Deployment	20
Installation requirements	22
Installation procedures	23
Validation	26
Key Considerations for Integrating FortiADC with OpenStack	29

Change Log

Date	Change Description
10/16/2019	Second update, adding deploy FortiADC-VM in an OpenStack environment.
03/28/2018	First update, adding notes to the Important Notes section.
01/19/2018	Initial release.
10/10/2024	Openstack 2023.2 Octavia support.

Introduction

This document discusses the integration of FortiADC with OpenStack, providing detailed instructions on installing the FortiADC Octavia Driver and Agent on OpenStack, as well as creating virtual load balancers on FortiADC through the OpenStack Octavia service.

A strong understanding of OpenStack and the Octavia setup is required to successfully install and run the Fortinet drivers and agents.

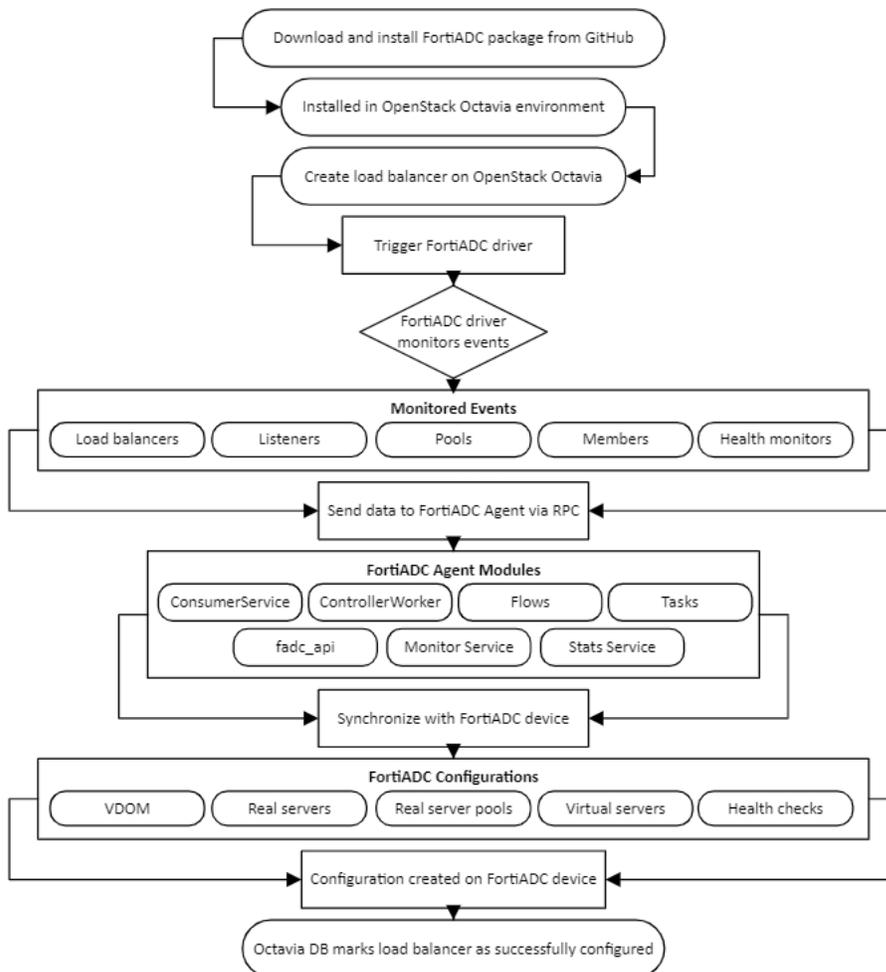
For more information about OpenStack, visit:

- OpenStack Community Forum at <https://www.openstack.org/community/>
- OpenStack Documentation at <https://docs.openstack.org/2023.2/index.html>

Implementation

FortiADC Octavia driver and agent in OpenStack environment

The diagram below illustrates the implementation of the FortiADC Octavia driver and agent within an OpenStack environment.



Deploying a FortiADC-VM instance in an OpenStack environment

Deploying a FortiADC-VM instance in an OpenStack environment

1. Creating boot and log images

In **Project > Compute > Images**, use the Image File options to navigate to Image Details and select the boot.qcow2 and data.qcow2 file you extracted from the FortiADC-VM KVM software package. For **Format**, select **QCOW2-QEMU Emulator**.

Create Image

Image Details

Specify an image to upload to the Image Service.

Image Name*
adc-boot

Image Description

Image Source

Source Type
File

File*
Browse... boot.qcow2

Format*
QCOW2 - QEMU Emulator

Image Requirements

Kernel
Choose an image

Ramdisk
Choose an image

Architecture

Minimum Disk (GB)
0

Minimum RAM (MB)
0

Image Sharing

Visibility
Public Private

Protected
Yes No

Images

Q Click here for filters.

Displaying 6 items

<input type="checkbox"/>	Owner	Name ^
<input type="checkbox"/>	> demo	adc-boot
<input type="checkbox"/>	> demo	adc-data

2. Creating Volume

To create the volume FortiADC-VM uses for its boot and log disk, navigate to **Project > Volumes > Volumes**. This step may take a while.

Create Volume

Volume Name:

Description:

Volume Source:

Use image as a source:

Type:

Size (GiB) *:

Availability Zone:

Description: Volumes are block devices that can be attached to instances.

Volume Type Description: **lvmdriver-1**
No description available.

Volume Limits

Total Gibibytes: 405 of 1,000 GiB Used

Number of Volumes: 12 of 30 Used

Create Volume ✕

Volume Name
adc-data

Description

Volume Source
Image

Use image as a source
adc-data (29.6 MB)

Type
lvmdriver-1

Size (GiB) *
30

Availability Zone
nova

Description:
Volumes are block devices that can be attached to instances.

Volume Type Description:
lvmdriver-1
No description available.

Volume Limits

Total Gibibytes 407 of 1,000 GiB Used

Number of Volumes 13 of 30 Used

Volumes

Displaying 14 items

<input type="checkbox"/>	Name	Description	Size
<input type="checkbox"/>	adc-data	-	30GiB
<input type="checkbox"/>	adc-boot	-	2GiB

3. Creating Flavor

To specify the size of the instance, go to the OpenStack dashboard, navigate to **Admin > Compute > Flavors** and click **Create Flavor**. Complete the flavor settings.

We suggest selecting a compute flavor that has a minimum of 8 GB of memory.

Admin / Compute / Flavors

Flavors

Displaying 16 items

<input type="checkbox"/>	Flavor Name	VCPUs	RAM	Root Disk	Ephemeral Disk	Swap Disk
<input type="checkbox"/>	adc-basis	1	4GB	2GB	0GB	0MB

4. Creating Network

Navigate to **Project > Network > Networks**. In the network creation wizard, complete the network and subnet settings to create Network, 10 Subnets and Ports.

Create Network ✕

Network Subnet Subnet Details

Network Name

Create a new network. In addition, a subnet associated with the network can be created in the following steps of this wizard.

Enable Admin State ⓘ

Shared

Create Subnet

Create 'subnet1' when creating Network.

Create Network ✕

Network **Subnet** Subnet Details

Subnet Name

Network Address Source

Network Address

IP Version

Gateway IP

Disable Gateway

Creates a subnet associated with the network. You need to enter a valid "Network Address" and "Gateway IP". If you did not enter the "Gateway IP", the first value of a network will be assigned by default. If you do not want gateway please check the "Disable Gateway" checkbox. Advanced configuration is available by clicking on the "Subnet Details" tab.

Create Network ✕

Network Subnet **Subnet Details**

Enable DHCP

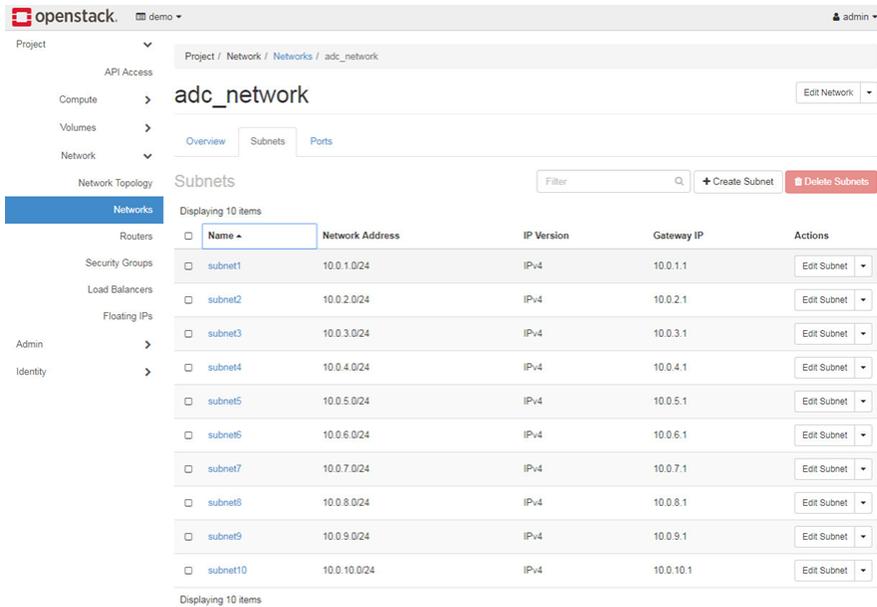
Specify additional attributes for the subnet.

Allocation Pools

DNS Name Servers

Host Routes

Click on the created network and create 9 more subnets.



Click Ports tab and then create 10 ports in different subnets for FortiADC interfaces.

Create Port ✕

Name

Enable Admin State

Device ID

Device Owner

Specify IP address or subnet

Subnet

MAC Address

Port Security

Description:
 You can create a port for the network. If you specify device ID to be attached, the device specified will be attached to the port created.

Project / Network / Networks / adc_network

adc_network

Overview Subnets Ports

Ports

Displaying 11 items

Name	Fixed IPs	MAC Address	Attached Device	Status	Admin State	Actions
(6543660-74af)	<ul style="list-style-type: none"> 10.0.1.100 10.0.10.100 10.0.2.100 10.0.3.100 10.0.4.100 10.0.5.100 10.0.6.100 10.0.7.100 10.0.8.100 10.0.9.100 	fa:16:3e:15:97:42	network:dhcp	Active	UP	Edit Port
adc-port1	10.0.1.105	fa:16:3e:d7:a8:99	Detached	Down	UP	Edit Port
adc-port2	10.0.2.106	fa:16:3e:61:cc:ef	Detached	Down	UP	Edit Port
adc-port3	10.0.3.109	fa:16:3e:81:0d:11	Detached	Down	UP	Edit Port
adc-port4	10.0.4.101	fa:16:3e:22:a8:63	Detached	Down	UP	Edit Port
adc-port5	10.0.5.107	fa:16:3e:79:7c:1b	Detached	Down	UP	Edit Port
adc-port6	10.0.6.109	fa:16:3e:92:d4:20	Detached	Down	UP	Edit Port
adc-port7	10.0.7.103	fa:16:3e:6d:c7:91	Detached	Down	UP	Edit Port
adc-port8	10.0.8.104	fa:16:3e:04:df:0e	Detached	Down	UP	Edit Port
adc-port9	10.0.9.110	fa:16:3e:24:1a:48	Detached	Down	UP	Edit Port
adc-port10	10.0.10.105	fa:16:3e:14:be:91	Detached	Down	UP	Edit Port

Displaying 11 items

Configure **Security Group** in **Project > Network > Security Groups** to allow all.

Project / Network / Security Groups

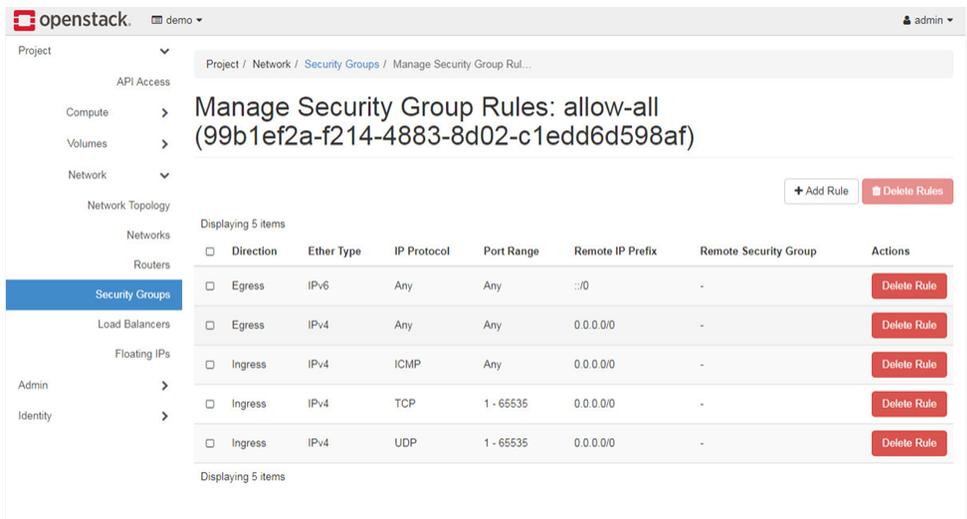
Security Groups

Filter Create Security Group Delete Security Groups

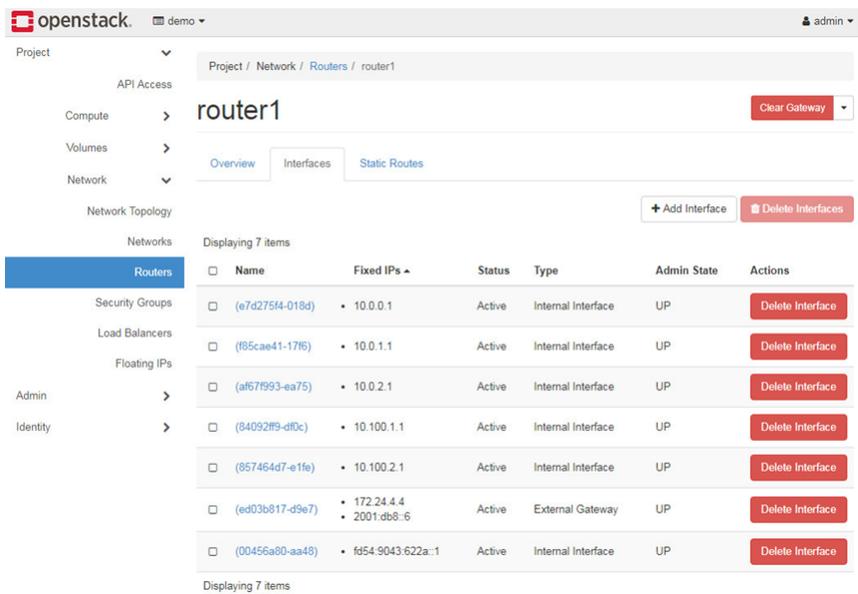
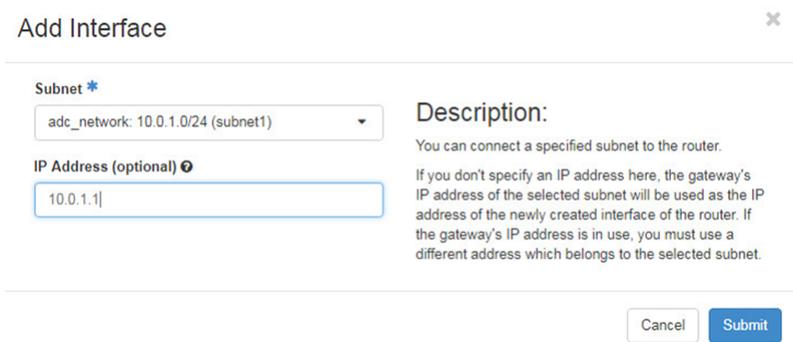
Displaying 2 items

Name	Security Group ID	Description	Actions
allow-all	99b1e12a-f214-4883-8d02-c1edd6d598af		Manage Rules
default	bdc336b-3f70-4958-81fc-4dd21b4748ed	Default security group	Manage Rules

Displaying 2 items



To the router, add subnets which need to be forwarded to the public network in **Project > Network > Routers**.



Allocate Floating IP in **Project > Network > Floating IPs**.

Allocate Floating IP ✕

Pool *
public

Description:
Allocate a floating IP from a given floating IP pool.

Project Quotas
Floating IP 0 of 50 Used

openstack demo admin

Project / Network / Floating IPs

Floating IPs

Allocate IP To Project Release Floating IPs

Displaying 1 item

IP Address	Mapped Fixed IP Address	Pool	Status	Actions
<input type="checkbox"/> 172.24.4.12	-	public	Down	Associate

Displaying 1 item

Admin Identity

5. Creating Instance

Create Instance in **Project > Compute > Instances**.

Launch Instance ✕

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *
adc1

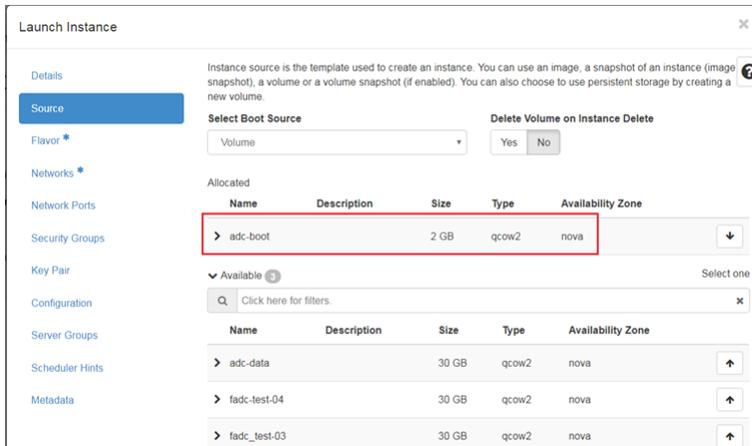
Availability Zone
nova

Count *
1

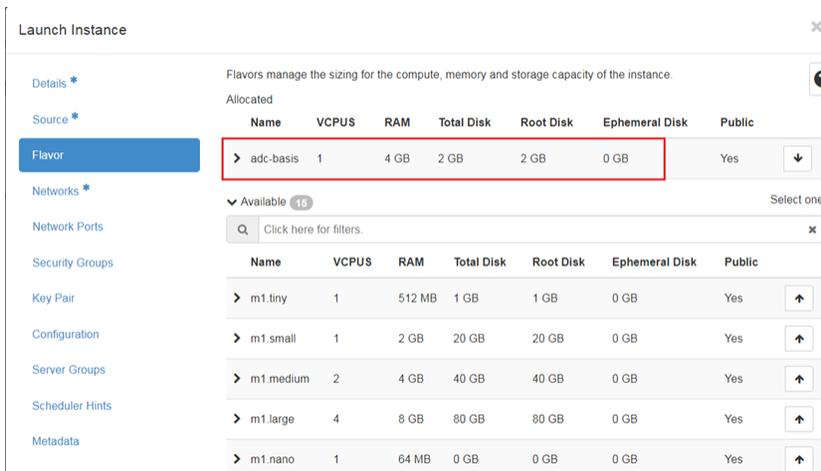
Total Instances (10 Max)
10%

0 Current Usage
1 Added
9 Remaining

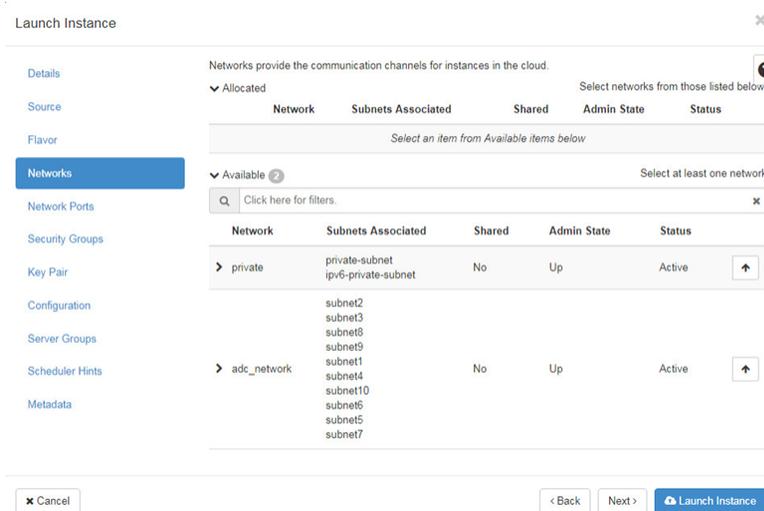
Select created boot disk in Volume.



Select created flavor.



Do not select Networks. Add created Network Ports instead.



Deploying a FortiADC-VM instance in an OpenStack environment

Launch Instance ✕

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Ports provide extra communication channels to your instances. You can select ports instead of networks or a mix of both. ?

▼ Allocated **10** Select ports from those listed below.

	Name	IP	Admin State	Status	
↕ 1	> adc-port1	10.0.1.105 on subnet: subnet1	Up	Down	⌵
↕ 2	> adc-port2	10.0.2.106 on subnet: subnet2	Up	Down	⌵
↕ 3	> adc-port3	10.0.3.109 on subnet: subnet3	Up	Down	⌵
↕ 4	> adc-port4	10.0.4.101 on subnet: subnet4	Up	Down	⌵
↕ 5	> adc-port5	10.0.5.107 on subnet: subnet5	Up	Down	⌵
↕ 6	> adc-port6	10.0.6.109 on subnet: subnet6	Up	Down	⌵
↕ 7	> adc-port7	10.0.7.103 on subnet: subnet7	Up	Down	⌵
↕ 8	> adc-port8	10.0.8.104 on subnet: subnet8	Up	Down	⌵
↕ 9	> adc-port9	10.0.9.110 on subnet: subnet9	Up	Down	⌵
↕ 10	> adc-port10	10.0.10.105 on subnet: subnet10	Up	Down	⌵

▼ Available **0** Select one

🔍 Filter

Name	IP	Admin State	Status
No available items			

✕ Cancel < Back Next > Launch Instance

Configure Security Groups and then click "Launch Instance".

Launch Instance ✕

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Select the security groups to launch the instance in. ?

▼ Allocated **1**

Name	Description
> allow-all	

▼ Available **1** Select one or more

🔍 Click here for filters.

Name	Description
> default	Default security group

✕ Cancel < Back Next > Launch Instance

Because only boot disk can be configured during instance creation, attach data disk is needed for the FortiADC instance.

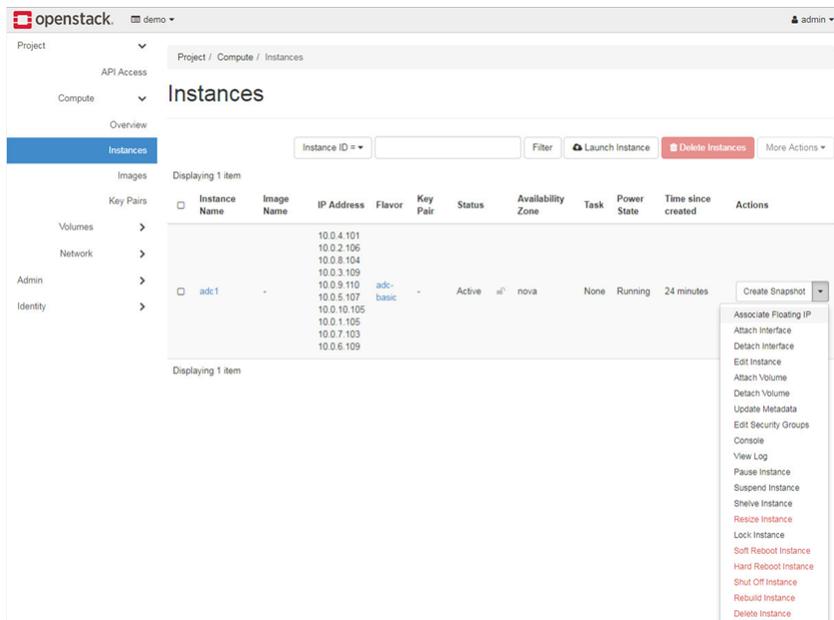
Deploying a FortiADC-VM instance in an OpenStack environment

The screenshot shows the OpenStack dashboard interface. The main content area displays a table of instances. The instance 'adc1' is selected, and the 'Actions' dropdown menu is open, showing various options including 'Attach Volume'.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions	
adc1	-	10.0.4.101 10.0.2.106 10.0.8.104 10.0.3.109 10.0.9.110 10.0.5.107 10.0.10.105 10.0.1.105 10.0.7.103 10.0.6.109	adc-basic	-	Active	all	nova	None	Running	2 minutes	Create Snapshot Associate Floating IP Attach Interface Detach Interface Edit Instance Attach Volume Detach Volume Update Metadata Edit Security Groups Console View Log Pause Instance Suspend Instance Shelve Instance Resize Instance Lock Instance Soft Reboot Instance Hard Reboot Instance Shut Off Instance Rebuild Instance Delete Instance

The 'Attach Volume' dialog box is shown. The 'Volume ID' field is highlighted with a red box and contains the value 'adc-data (e95edc16-b1ae-4d78-8772-5bc15be3...)'. The 'Description' field contains the text 'Attach Volume to Running Instance.' The dialog has 'Cancel' and 'Attach Volume' buttons.

Assign Floating IP 172.24.4.x in public network to Instance.



The associated port needs to be in the subnet whose gateway was added in Router in the previous step.

Manage Floating IP Associations

IP Address * Select the IP address you wish to associate with the selected instance or port.

172.24.4.12 +

Port to be associated * -

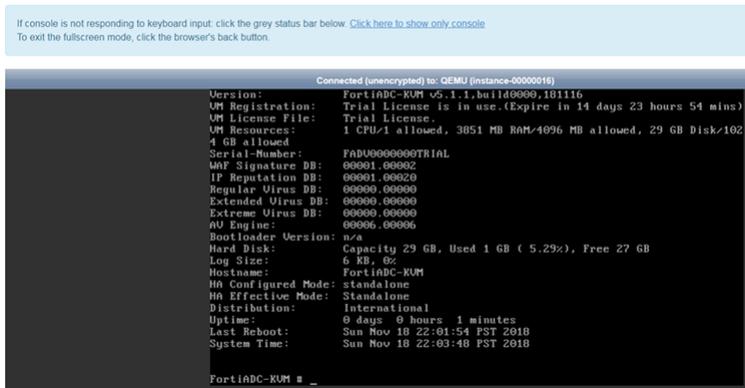
adc1: 10.0.1.105

Cancel Associate

6. Connect to console

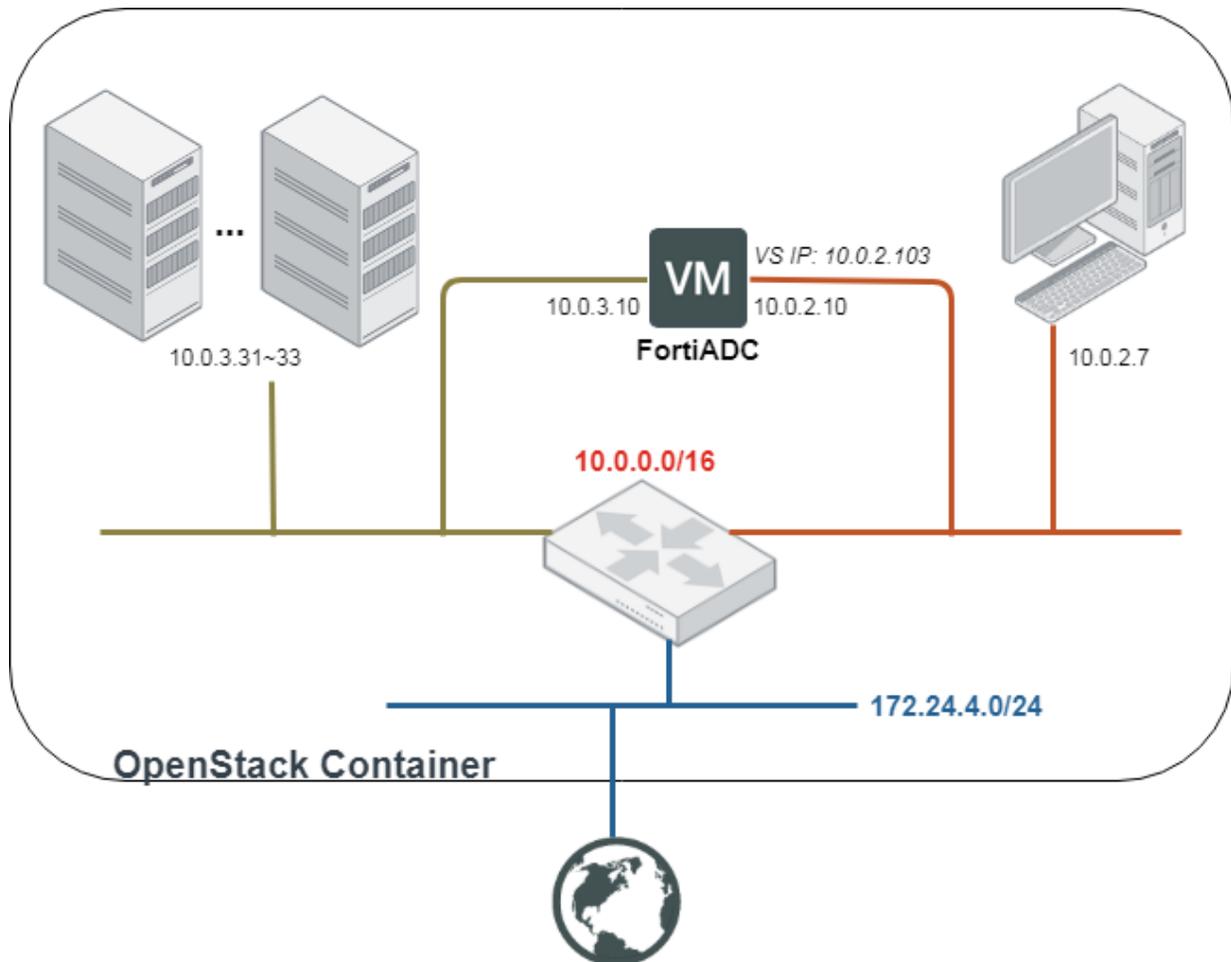
Remember to reboot FortiADC Instance after attaching data volume.

Instance Console



Deployment

FortiADC can only be deployed within an OpenStack container environment.



The following are example configurations deployed on FortiADC through Octavia:

Configuring a virtual server:

```
config load-balance virtual-server
  edit "09e01bbc-4076-44ea-8d0e-558ab6503655"
    set type l7-load-balance
    set ip 10.0.2.103
    set load-balance-profile LB_PROF_HTTP
    set load-balance-persistence LB_PERSIS_HASH_SRC_ADDR
    set load-balance-method LB_METHOD_ROUND_ROBIN
    set load-balance-pool 3ed56621-9825-494a-9246-452e591f913e
  next
end
```

Configuring a real server pool:

```
config load-balance pool
  edit "3ed56621-9825-494a-9246-452e591f913e"
    set health-check-ctrl enable
    set health-check-list 7baa43a4-633b-4f35-af0d-02f9aedd9422
    set real-server-ssl-profile NONE
  config pool_member
    edit 1
      set pool_member_cookie rs1
      set real-server 38a40738-becf-4736-a16b-d3b131275f31
    next
    edit 2
      set pool_member_cookie rs2
      set real-server 0cc6107e-8848-4f39-80e3-873a788b9000
    next
    edit 3
      set pool_member_cookie rs3
      set real-server fef07534-ef8e-48a3-89d3-1db551b952a9
    next
  end
next
end
```

Configuring real servers:

```
config load-balance real-server
  edit "38a40738-becf-4736-a16b-d3b131275f31"
    set ip 10.0.3.31
  next
  edit "0cc6107e-8848-4f39-80e3-873a788b9000"
    set ip 10.0.3.32
  next
  edit "fef07534-ef8e-48a3-89d3-1db551b952a9"
    set ip 10.0.3.33
  next
end
```

Installation requirements

FortiADC-OpenStack integration requires the following software packages:

- OpenStack 2023.2 release
- Octavia 2023.2
- FortiADC 7.4.3
- fadc-octavia-provider: 1.0.0

Installation procedures

Follow the steps below to install the FortiADC software package in your OpenStack environment.

Step 1: Verify your OpenStack environment

Ensure that the system is running OpenStack version 2023.2 with Octavia properly installed and configured.

Step 2: Download and extract the fadc-octavia-provider

1. Download the `fadc-octavia-provider.tar.gz` file from <https://github.com/fortinet/fortiadc-openstack>.
2. Extract the contents in your OpenStack installation environment using the command: `tar -zxvf fadc-octavia-provider.tar.gz`.

Step 3: Install the FortiADC Driver and Agent

1. Install the driver and agent:

If the openstack installed on python virtual environment, it needs to go to virtual environment to install package.
Run the `./install.sh` to install both driver and agent.

2. Modify `octavia.conf` in `/etc/octavia/`:

```
enabled_provider_drivers = amphora:The Octavia Amphora driver.,octavia:Deprecated  
alias of the Octavia Amphora driver.,ovn:Octavia OVN driver.,fortiadc_  
driver:fortiadc driver.  
default_provider_driver = fortiaadc_driver
```

Restart uwsgi service. It can enable Fortiadc driver.

Step 4: Start the FortiADC Agent

1. Configure the FortiADC Agent:

The package includes an example configuration file named `fadc_octavia_example.conf`. Copy this file to `/etc/octavia/fadc_octavia.conf` and modify it with the appropriate values.

Please ensure that the content of the `fadc_devices` section remains in JSON format after making any changes.

```
fadc_devices = [  
    {  
        "fadc_FQDN": "172.24.4.223",  
        "fadc_username": "admin",  
        "fadc_password": "fortinet",  
        "fadc_vdom_network_mapping": "port2",
```

```

        "fadc_bind_vip_port_id": "69dd6263-203f-46ed-835d-327b9f0baf8d",
        "fadc_vdom_network_allowAccess": {"port2":"http ping telnet
https"},
        "fadc_vdom_network_ip": {"port2":"10.20.2.23/24"},
        "fadc_vdom_default_gw": "10.20.2.1",
        "fadc_vs_dev_intf": "port2",
        "fadc_vs_packet_forward_method": "FullNAT",
        "fadc_vs_persistency": "LB_PERSIS_HASH_SRC_ADDR",
        "fadc_get_stats_interval": "2",
        "fadc_vs_nat_pool": ["10.20.2.190", "10.20.2.199"],
        "fadc_vs_nat_intf": "port2",
        "fadc_healthcheck_port": "80",
        "certificate_verify": false,
        "projects": [
            "fe6cb031d610420394ba134f670488a6"
        ]
    }
}
]

```

2. Install the FortiADC Agent Service:

Locate the FortiADC agent path by executing the command: `which fortiadc_agent` in the environment where the `fadc-octavia-provider` package is installed.

Then, run the installation script with the following command:

```
sudo ./install_service.sh /path/to/fortiadc_agent
```

To verify that the service has started successfully, use the command:

```
ps -ef | grep fortiadc_agent
```

FortiADC Configuration Parameters for Deployment within an OpenStack Container:

Parameter	Description
Debug	
<code>debug_mode</code>	Enable or disable debug messages for <code>fadc_api</code> . True = enable False = disable
Device information	
<code>fadc_FQDN</code>	The FortiADC's IP address that OpenStack uses to communicate with it.
<code>fadc_username</code>	The FortiADC global user log-in name. Note: The default password is <code>admin</code> .
<code>fadc_password</code>	The FortiADC log-in password. Note: It's blank (no password) by default.
Network	
<code>fadc_vdom_network_</code>	The interfaces assigned to the virtual domain.

Parameter	Description
mapping	
<code>fadc_bind_vip_port_id</code>	The bind virtual interface port ID.
<code>fadc_vdom_network_allowAccess</code>	The applications that the interface allows to access. The value can be HTTPS, HTTP, SNMP, SSH, Ping, and Telnet.
<code>fadc_vdom_network_ip</code>	The IP addresses of the assigned interfaces.
<code>fadc_default_gw</code>	The static route with destination 0.0.0.0/0 in the VDOM.
Virtual server	
<code>fadc_vs_dev_intf</code>	The virtual server interface.
<code>fadc_vs_persistency</code>	The name of the persistence profile in the virtual server.
<code>fadc_vs_packet_forward_method</code>	The packet-forwarding method in Layer-4 virtual servers. It can be NAT or FullNAT. Note: This applies to Layer-4 virtual servers only.
<code>fadc_vs_nat_pool</code>	The IP address range of the NAT source pool. Note: This applies to Layer-4 virtual servers with NAT only.
<code>fadc_vs_nat_intf</code>	The interface of the NAT source pool. Note: This applies to Layer-4 virtual servers with NAT only.
<code>fadc_get_stats_interval</code>	The amount of data shown on the FortiADC's FortiView page: <ul style="list-style-type: none"> • 0=One hour's worth of data • 1=Six hours' worth of data • 2=One day's worth of data • 3=One week's worth of data • 4=One month's worth of data • 5=One year's worth of data
Health check monitor port	
<code>fadc_healthcheck_port</code>	The port number for FortiADC to create healthcheck profiles. The default is 80. Valid values range from 0 to 65535. Note: This applies to HTTP, HTTPS, and TCP only.

Validation

After completing the installation of `fadc-octavia-provider 1.0.0`, the next step is to validate the installation to ensure everything is functioning correctly.

To validate your installation:

Step 1: Create a load balancer in OpenStack.

From the OpenStack GUI, select Project > Network > Load Balancers to open the Create Load Balancer page, and then follow the tabs on the left to configure the load balancer.

1. Click the Load Balancer Details tab to configure the load balancer.

The screenshot shows the 'Create Load Balancer' page in the OpenStack GUI. The 'Load Balancer Details' tab is selected. The form contains the following fields:

- Name:** Load Balancer 1
- Description:** Create on GUI
- IP address:** 10.0.2.103
- Subnet:** subnet2

At the bottom of the form, there are buttons for 'Cancel', '< Back', 'Next >', and 'Create Load Balancer'.

2. Click the Listener Details tab to configure the listener.
Load balancers listen for requests on multiple ports, each of which is specified by a listener.

The screenshot shows the 'Create Load Balancer' page in the OpenStack GUI, with the 'Listener Details' tab selected. The form contains the following fields:

- Name:** Listener 1
- Description:** Create Load Balancer
- Protocol:** HTTP
- Port:** 80

At the bottom of the form, there are buttons for 'Cancel', '< Back', 'Next >', and 'Create Load Balancer'.

- Click Pool Details to configure the server pool.
A server pool contains a list of members(servers) that serve content through the load balancer.

Create Load Balancer ✕

Load Balancer Details

Listener Details

Pool Details

Pool Members

Monitor Details *

Provide the details for the pool. ?

Name

Description

Method *

✕ Cancel
< Back
Next >
Create Load Balancer

- Click Pool Members to add servers to the server pool.
Pool members are servers that handle traffic behind a load balancer. Each member is identified by the IP address and port it uses to serve traffic.

Create Load Balancer ✕

Load Balancer Details

Listener Details

Pool Details

Pool Members

Monitor Details *

Add members to the load balancer pool. ?

▼ Allocated Members 3

IP Address *	Subnet *	Port *	Weight	
<input type="text" value="10.0.3.31"/>	<input type="text" value="subnet3"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	<input type="button" value="Remove"/>
<input type="text" value="10.0.3.32"/>	<input type="text" value="subnet3"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	<input type="button" value="Remove"/>
<input type="text" value="10.0.3.33"/>	<input type="text" value="subnet3"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	<input type="button" value="Remove"/>

▼ Available Instances

Name	IP Address	
adc0	10.100.9.10...	<input type="button" value="Add"/>
Client1	10.100.4.101...	<input type="button" value="Add"/>
Server2	10.100.5.102...	<input type="button" value="Add"/>
Server3	10.100.5.103...	<input type="button" value="Add"/>
Server1	10.0.3.31...	<input type="button" value="Add"/>
adc1	10.0.4.101...	<input type="button" value="Add"/>

✕ Cancel
< Back
Next >
Create Load Balancer

- Click Monitor Details to configure the health monitor.
Health monitors keep track of the health of pool members. They divert traffic away from members that are

offline or non-responsive.

For the monitor type **HTTP**, it is recommended to select **HEAD** instead of **GET**. The suggested HTTP health monitor settings are as follows:

Create Load Balancer
✕

[Load Balancer Details *](#)

[Listener Details *](#)

[Pool Details *](#)

[Pool Members](#)

Monitor Details

Provide the details for the health monitor.

Create Health Monitor

Yes
No

Name	Type *	Max Retries Down *
<input type="text"/>	<input type="text" value="HTTP"/>	<input type="text" value="3"/>
Delay (sec) *	Max Retries *	Timeout (sec) *
<input type="text" value="5"/>	<input type="text" value="1"/>	<input type="text" value="4"/>
HTTP Method	Expected Codes	URL Path
<input type="text" value="HEAD"/>	<input type="text" value="200"/>	<input type="text" value="/"/>
Admin State Up		
Yes No		

✕ Cancel
< Back
Next >
Create Load Balancer

Ensure that the Timeout value is set to be less than the Interval value for optimal FortiADC performance.

Step 2: Verify the load balancer configuration in FortiADC.

If your configuration of the load balancer in OpenStack is successful, the project ID that you created in OpenStack should show up in the Name column of the Virtual Domain page on the FortiADC GUI . In other words, the OpenStack project ID becomes the name of the virtual domain in FortiADC.

To verify your load balancer configuration:

1. Log into your FortiADC GUI.
2. Make sure that your Project ID in OpenStack appears in the Name column of the Virtual Domain page.

Key Considerations for Integrating FortiADC with OpenStack

The following key considerations must be kept in mind when integrating FortiADC with OpenStack.

Monitor Configuration for Load Balancer:

- When configuring the monitor details in OpenStack, ensure that the **Timeout** value is set lower than the **Interval** value for optimal performance.

Network Interface Changes:

- If the network interfaces of a FortiADC instance change in OpenStack, you must enable the `retrieve_physical_hwaddr` setting for the physical ports via the CLI, then reboot the FortiADC appliance. This ensures that FortiADC correctly updates the MAC addresses for the physical ports.
- By default, `retrieve_physical_hwaddr` is not enabled. If network ports are changed in an OpenStack VM, access the FortiADC console and manually enable this setting for the modified ports.

Algorithm Support:

- FortiADC does not support `SOURCE_IP` as an `lb_algorithm` and will default to the Round Robin (RR) algorithm instead.

Virtual Server Creation:

- You cannot create a virtual server if `fadc_vs_persistency` is not supported in the virtual server profile specified in the `fadc_octavia.conf` configuration file.

FortiADC and OpenStack Octavia Value Range Differences:

- **Connection limit:** Starts at `-1` in Octavia, but at `0` in FortiADC. Setting Octavia to `0` or `-1` will set the FortiADC connection limit to `0`.
- **Pool Member Weight:** Octavia allows a weight range of `0-256`, while FortiADC allows `1-256`. FortiADC will not change the current weight if configured to `0`.
- **Delay and Timeout:** FortiADC's delay and timeout range is `1-3600`, and the **Timeout** value must be less than the **Interval**. Octavia does not have this restriction.

Octavia Agent Capabilities:

- The FortiADC Octavia agent does not support High Availability (HA).
- It only supports Layer 7 (L7) HTTP/HTTPS and Layer 4 (L4) TCP for load balancer creation.

L4 TCP Packet Forwarding:

- L4 TCP supports two packet forwarding methods: **DNAT** and **Full NAT**. Configure `fadc_vs_packet_forward_method` to specify the packet forwarding method for the L4 virtual server. Acceptable values are

NAT or FullNAT.

NAT Pool for L4 TCP Full NAT:

- A NAT pool is supported exclusively in L4 TCP with Full NAT. Use the following format to define the NAT pool:

```
fadc_vs_nat_pool = ['172.24.4.130', '172.24.4.135'] # Address range from
172.24.4.130 to 172.24.4.135
```

The parameter `fadc_vs_nat_intf` can be set to specify the interface for the NAT source pool. These parameters apply only to the TCP listener (L4 TCP) with Full NAT packet forwarding.

Address Pair Limits:

- The maximum number of allowed address pairs for a single network port is 10. This means users can create up to 9 load balancers on one ADC port, excluding configurations for the NAT source pool.

Manual Address Pair Configuration for L4 Full NAT:

- When using L4 Full NAT with a NAT source pool, the IP addresses in the pool must be manually added to the allowed address pairs on the ADC port.

Security Rules for Load Balancers:

- Security rules for load balancers must be added manually, or you can disable port security on the specific port or the entire network.

Reboot After Adding Data Disk:

- After deploying FortiADC in OpenStack and adding a data disk, reboot the instance to update its hardware information.



www.fortinet.com

Copyright© 2025 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 Chief Legal Officer, 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.