



FortiADC - AWS 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>

NSE 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 AWS Deployment Guide

01-540-000000-20200214

TABLE OF CONTENTS

Change Log	4
Introduction	5
Before deploying the FortiADC-VM	6
Deploying the FortiADC-VM	10
Deploying FortiADC-VM for AWS	11
Example: Set VS on AWS in HA-VRRP mode	16
Bootstrapping the FortiADC-VM at initial boot-up using user data	21
Deploying Autoscaling on AWS	26
Planning & Prerequisites	28
Obtaining the deployment package	29
Deploying the CloudFormation templates	30
CFT parameters	33
Optional settings	40
Completing the deployment	42
Locating deployed resources	43
Verifying the deployment	47
Connecting to the primary FortiADC-VM	53
Configuring the FortiADC-VM for Autoscaling	58
Upgrading the deployment to apply firmware updates to the FortiADC instances	61
Configuring the Network Load Balancer	66
Attaching the FortiADC-VM instance to an existing Autoscaling group	69
Debug	74
Script	77
Importing the Amazon machine image	78
Important notes	86

Change Log

Date	Change Description
2023-02-03	Added Autoscale.
2020-04-08	Replaced cloud-init section with Bootstrapping the FortiADC-VM section
2020-02-14	Added cloud-init.
2019-10-01	Added Marketplace support.
2018-20-11	Second release.

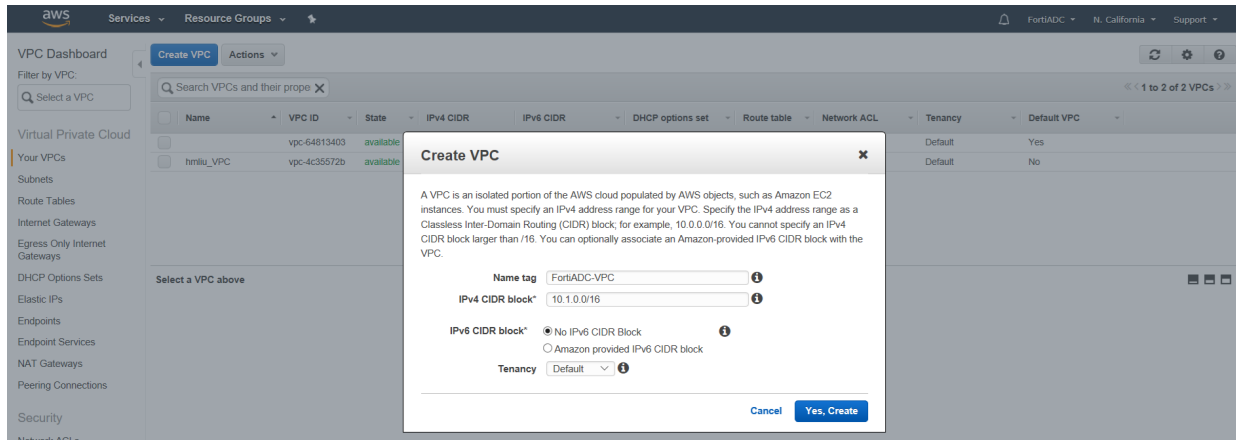
Introduction

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch virtual servers, configure security and networking, and manage storage.

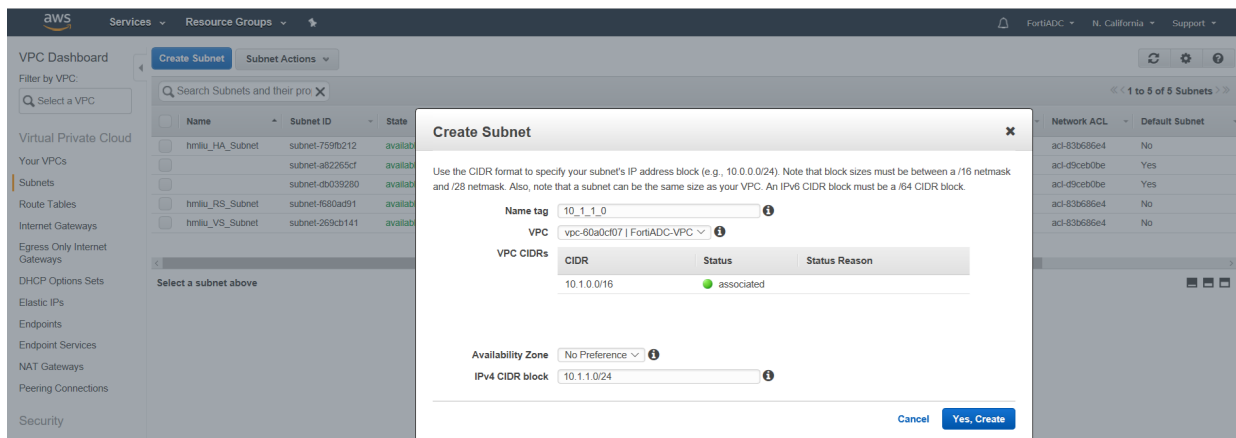
This guide shows how to deploy FortiADC-VM on AWS EC2.

Before deploying the FortiADC-VM

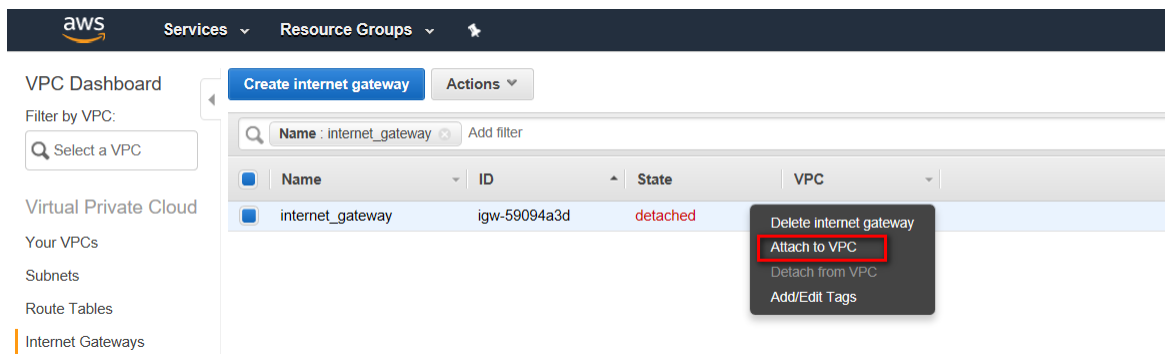
1. Create VPC and specify the IPv4 address range for your VPC



2. Create Subnet and specify your subnet's IP address block



3. Create internet gateway, and attach it to VPC



4. Create or use default route table, and configure "subnet associations" according to the actual network

The screenshot shows the AWS Management Console interface for the VPC Dashboard. The left sidebar lists various VPC resources, with 'Route Tables' highlighted. The main content area displays the 'FortiADC-VPC-Route-Table' (rtb-837f62e4) configuration. The 'Routes' tab is selected, showing a table of routes.

Name	Route Table ID	Explicitly Associated	Main	VPC
FortiADC-VPC-Route-Table	rtb-837f62e4	0 Subnets	Yes	vpc-60a0cf07 FortiADC-VPC

Below the table, the 'Routes' tab for 'rtb-837f62e4 | FortiADC-VPC-Route-Table' is shown. The 'Routes' sub-tab is active, displaying a table of routes.

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
0.0.0.0/0	igw-59094a3d	Active	No

5. Create security group, configure "Inbound Rules" and "Outbound Rules"

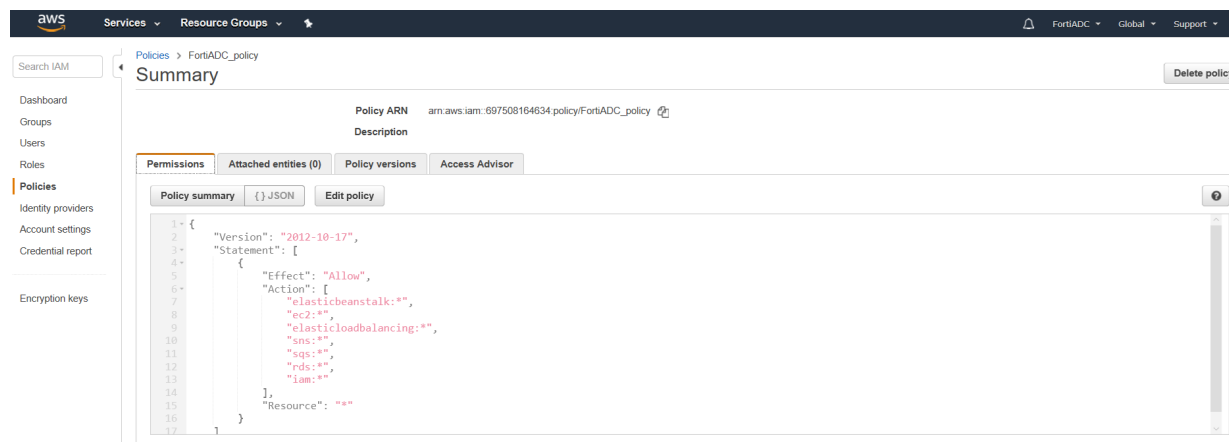
The screenshot shows the AWS Management Console interface for the Security Groups page. The left sidebar lists various VPC resources, with 'Security Groups' highlighted. The main content area displays the 'Security_Group_Allow_All' (sg-bf9768c7) configuration. The 'Inbound Rules' tab is selected, showing a table of inbound rules.

Name tag	Group ID	Group Name	VPC	Description
Security_Group_Allow_All	sg-bf9768c7	Security_Group_Allow...	vpc-60a0cf07 FortiADC-VPC	Security_Group_Allow_All

Below the table, the 'Inbound Rules' tab for 'sg-bf9768c7 | Security_Group_Allow_All' is shown. The 'Inbound Rules' sub-tab is active, displaying a table of inbound rules.

Type	Protocol	Port Range	Source	Description
ALL Traffic	ALL	ALL	0.0.0.0/0	

6. Create IAM policy



When switching to HA, it executes AWS API for migration of floating IP and reflection of public IP address.

An example of AWS permissions policy:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticbeanstalk:*",
        "ec2:*",
        "elasticloadbalancing:*",
        "sns:*",
        "sqs:*",
        "rds:*",
        "iam:*"
      ],
      "Resource": "*"
    }
  ]
}

```


7. Create role and attach permissions policies

Create role

1 2 3

Review

Provide the required information below and review this role before you create it.

Role name* FortiADC_Role

Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.

Role description FortiADC_Role

Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies FortiADC_policy [↗](#)

Deploying the FortiADC-VM

There are two ways to deploy FortiADC-VM on Amazon Web Services' Elastic Compute Cloud (Amazon EC2):

- Bring Your Own License (BYOL) — Requires a FortiADC-VM.
- On-demand — Provides a fully-licensed instance of FortiADC-VM, all FortiGuard services, and technical support on an hourly basis.

Both methods require an existing Amazon EC2 account and Amazon Virtual Private Cloud (Amazon VPC). You can deploy the FortiADC-VM for AWS using AWS Marketplace or from your own AMIs directly.

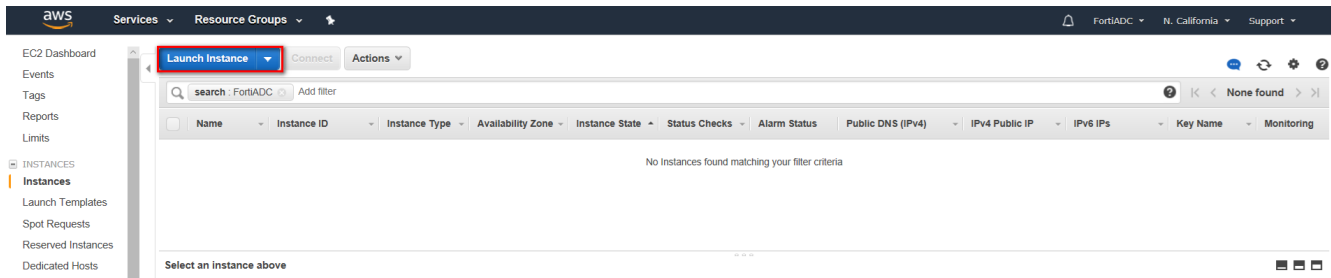


Starting from version 5.2.4, we suggest configuring the FortiADC from Amazon Marketplace.

Deploying FortiADC-VM for AWS

1. Login to AWS and ensure that you have a VPC (Virtual Private Cloud).

2. Go to the AWS Instances page and Launch Instance



3. Navigate to your choice of method for selecting the image: your AMIs or Marketplace



Marketplace is now recommended, as selecting the image through AMIs is more time-consuming.

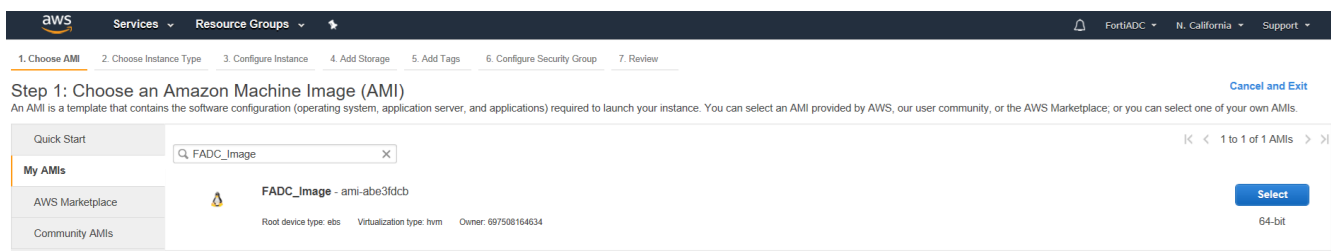
A. Marketplace

Go to Marketplace. **Launch Instance > Marketplace > Search for "FortiADC."**

Use the default image that is provided.

B. Use my AMIs

Please refer to [Importing the Amazon machine image on page 78](#) for uploading the image manually.



4. Select the appropriate region and EC2 instance type for your deployment. (suggest the over 4G memory)

Step 2: Choose an Instance Type
Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes

5. Configure Instance Details

Such as: Number of instances, Purchasing option, Network, Subnet, Auto-assign Public IP, IAM role, and more. (Role is required if in HA mode)

Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 2 [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network vpc-60a0cd07 | FortiADC-VPC [Create new VPC](#)

Subnet subnet-70341a17 | 10.1.1.0 | us-west-1b [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP Enable

IAM role FortiADC_Role [Create new IAM role](#)

Shutdown behavior Stop

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy Shared - Run a shared hardware instance
[Additional charges will apply for dedicated tenancy.](#)

T2 Unlimited ☐ Enable
[Additional charges may apply](#)

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-70341a17	Auto-assign	Add IP	

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

6. Add Storage

Notes: Root volume (suggested that you use a size of at least 1G).

After FortiADC-VM bootup, execute command “`execute formatlogdisk`”

If you change the size of the FortiADC-VM virtual hard disk after deployment, immediately run the following command: `execute formatlogdisk`. The `formatlogdisk` command clears logs from the virtual hard disk.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-00cb30ea5ce9fb97f	2	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensit)	30	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

7. Configure Security Group

You can create a new security group or select from an existing one.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

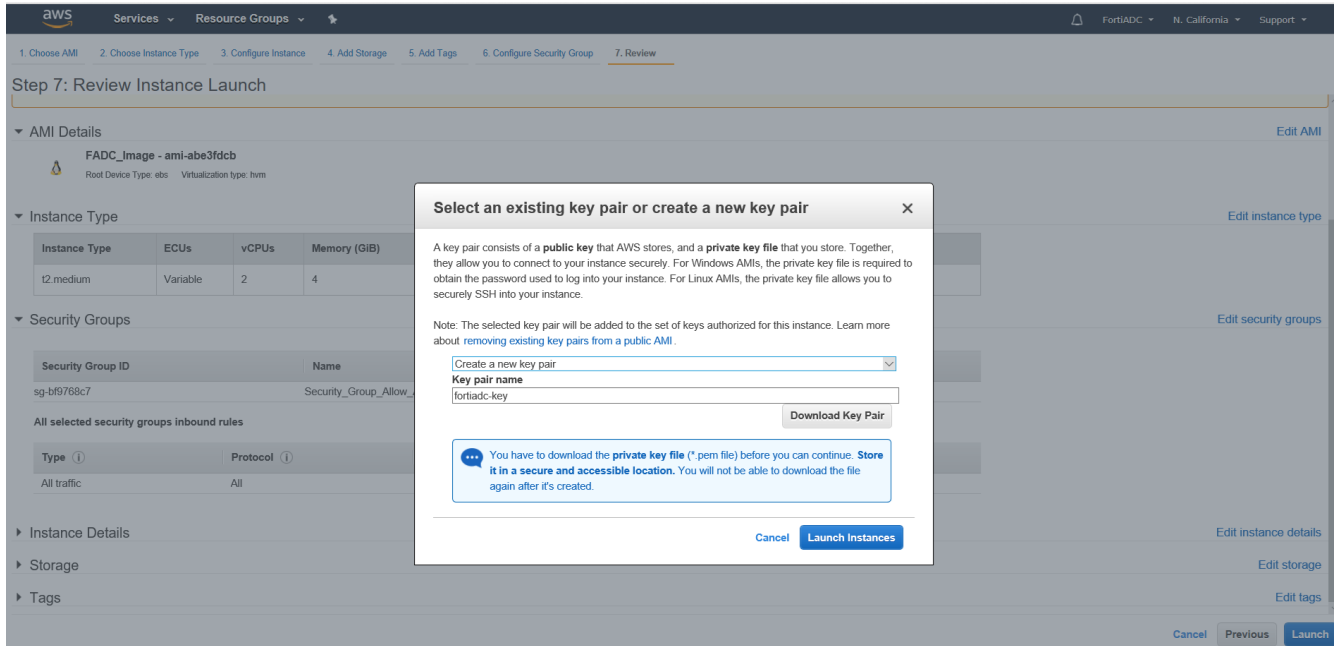
Security Group ID	Name	Description	Actions
sg-53b8492b	default	default VPC security group	Copy to new
sg-bf9768c7	Security_Group_Allow_All	Security_Group_Allow_All	Copy to new

Inbound rules for sg-bf9768c7 (Selected security groups: sg-bf9768c7)

Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	

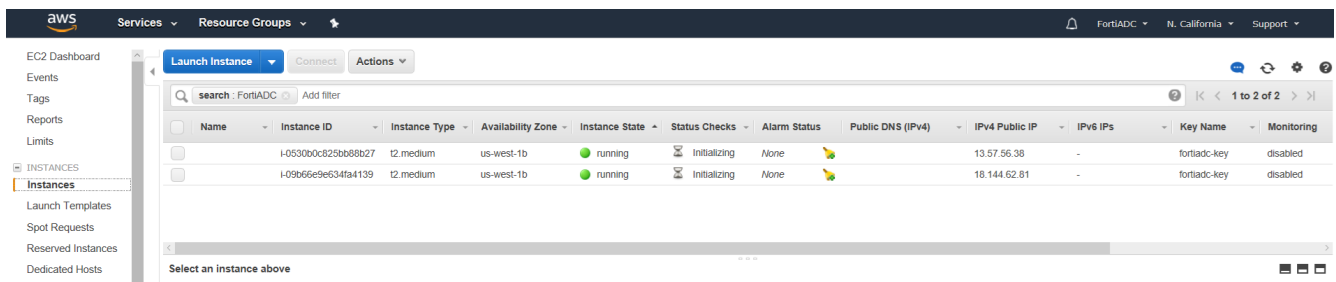
8. Create a new key pair and download it

Use the instructions provided under Key Pair. Creating a key pair allows you to access the command-line interface via SSH.



9. Click “Launch Instances”.

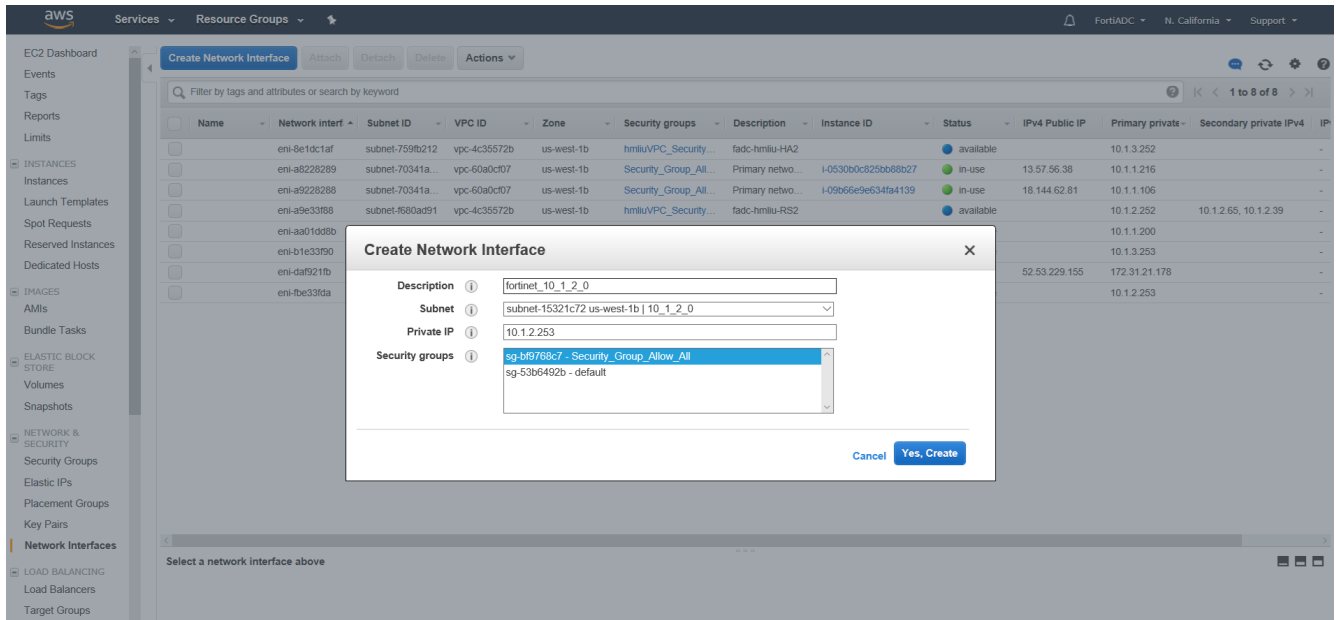
10. Navigate to the "Instances" page, check instance state.



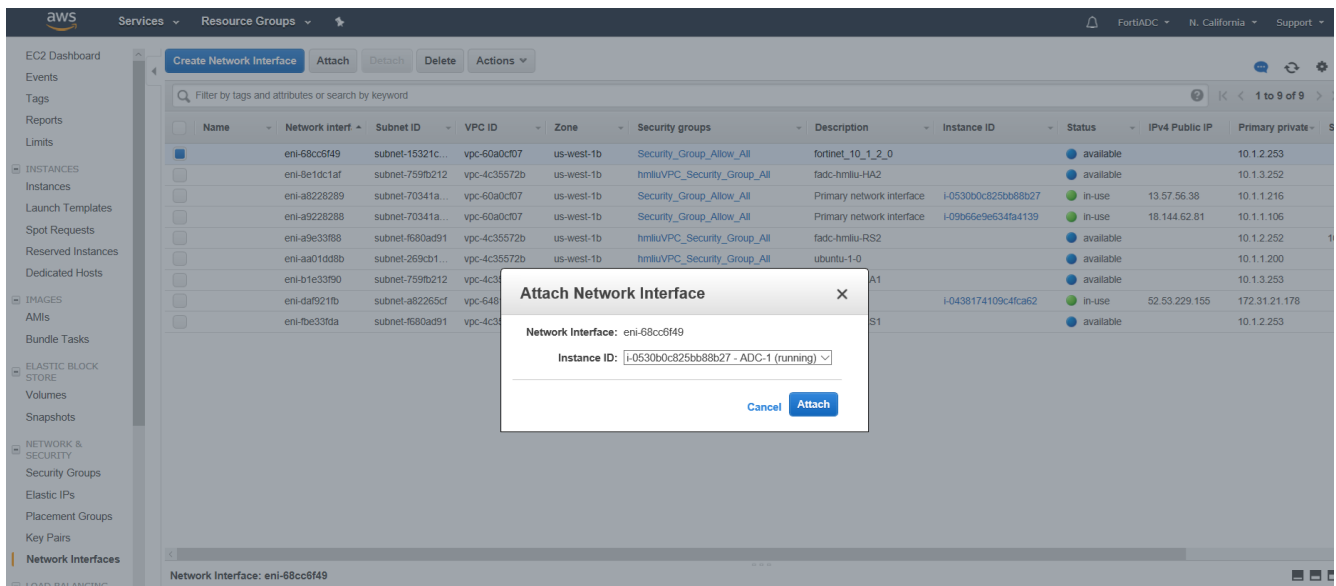
11. You can connect to the command-line interface (CLI) using SSH or telnet connection, or connect to the web UI using the HTTP or HTTPS. The default admin password is the AWS instance ID.

12. Create interface for FortiADC-VM

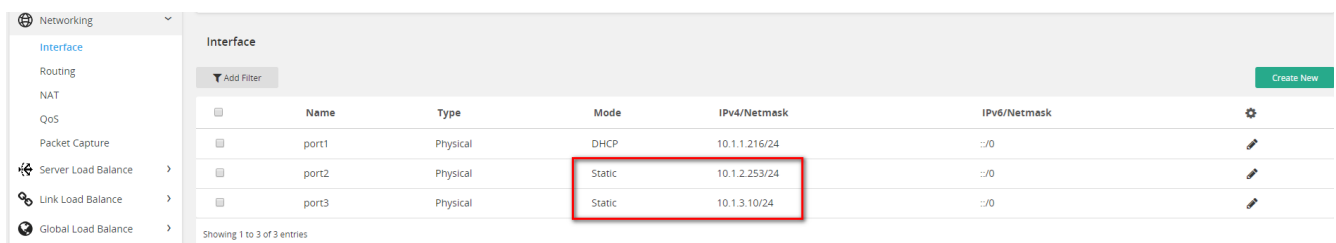
Step 1 : Navigate to the EC2 "Network Interface" page, create network interface, select subnet and security group, configure private IP.



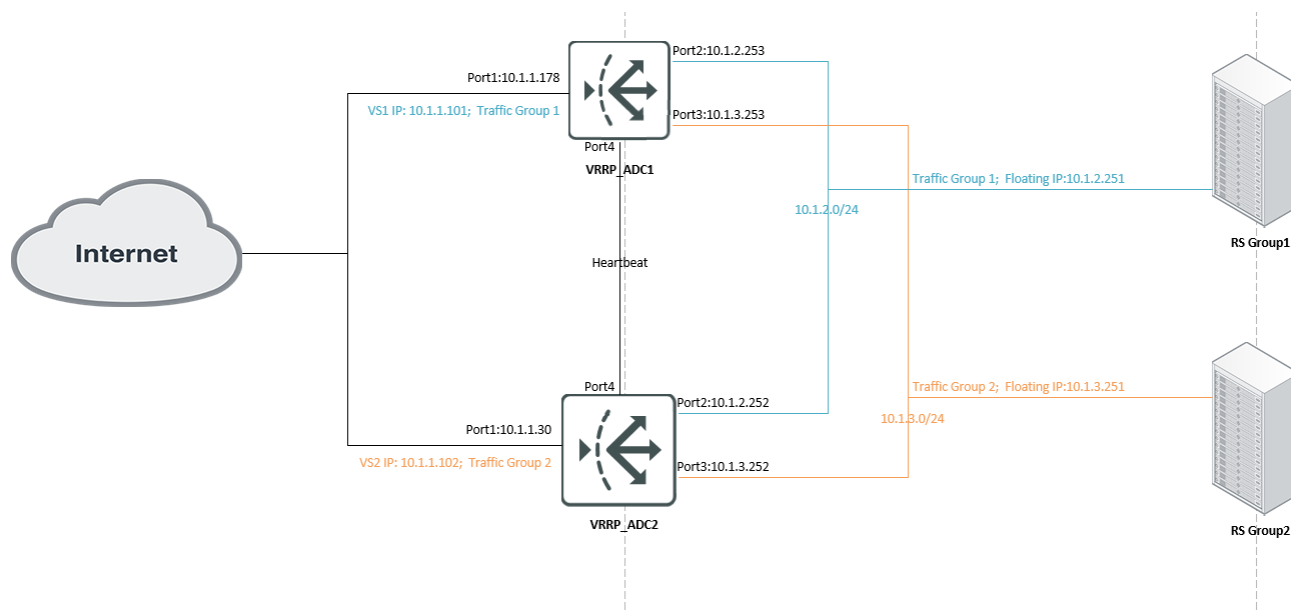
Step 2: Attach interface to FortiADC-VM instance.



Step 3: Reboot FortiADC-VM. After that, configure static IP for new interface.



Example: Set VS on AWS in HA-VRRP mode



Configure HA on ADC1

```
config system ha
  set mode active-active-vrrp
  set hbdev port4
  set datadev port4
  set group-name vrrp
  set l7-persistence-pickup enable
  set l4-persistence-pickup enable
  set l4-session-pickup enable
  set hb-type unicast
  set local-address 10.1.4.253
  set peer-address 10.1.4.252
end
```

Configure HA on ADC2

```
config system ha
  set mode active-active-vrrp
  set hbdev port4
  set datadev port4
  set local-node-id 1
  set group-name vrrp
  set priority 2
  set config-priority 50
  set l7-persistence-pickup enable
  set l4-persistence-pickup enable
```



```
set l4-session-pickup enable
set hb-type unicast
set local-address 10.1.4.252
set peer-address 10.1.4.253
end
```

Configure Traffic-Group on ADC

```
config system traffic-group
    edit "traffic_group_1"
        set failover-order 0 1
        set preempt enable
    next
    edit "traffic_group_2"
        set failover-order 1 0
        set preempt enable
    next
end
```

Configure VS on ADC

```
config load-balance real-server
edit "10_1_2_201"
    set ip 10.1.2.201
    next
    edit "10_1_3_201"
        set ip 10.1.3.201
        next
    end
config load-balance pool
    edit "RS_2_0"
        set health-check-list LB_HLTHCK_ICMP
        set real-server-ssl-profile NONE
    config pool_member
    edit 1
        set pool_member_cookie rs1
        set real-server 10_1_2_201
        next
    end
    next
    edit "RS_3_0"
        set real-server-ssl-profile NONE
        config pool_member
    edit 1
        set pool_member_cookie rs1
        set real-server 10_1_3_201
        next
    end
    next
    end

config load-balance virtual-server
    edit "VS1"
        set type 17-load-balance
        set interface port1
```

```
        set ip 10.1.1.101
        set load-balance-profile LB_PROF_HTTP
        set load-balance-method LB_METHOD_ROUND_ROBIN
        set load-balance-pool RS_2_0
        set traffic-group traffic_group_1
    next
    edit "VS2"
    set interface port1
    set ip 10.1.1.102
    set load-balance-profile LB_PROF_TCP
    set load-balance-method LB_METHOD_ROUND_ROBIN
    set load-balance-pool RS_3_0
    set traffic-group traffic_group_2
next
end
```

Configure Floating IP on ADC

ADC1:

```
config system interface
    edit "port2"
        set vdom root
        set ip 10.1.2.253/24
        set allowaccess ping
        config ha-node-ip-list
        end
        set traffic-group traffic_group_1
        set floating enable
        set floating-ip 10.1.2.251
    next
    edit "port3"
        set vdom root
        set ip 10.1.3.253/24
        set allowaccess ping
        config ha-node-ip-list
        end
        set traffic-group traffic_group_2
        set floating enable
        set floating-ip 10.1.3.251
    next
end
```

ADC2:

```
config system interface
    edit "port2"
        set vdom root
        set ip 10.1.2.252/24
        set allowaccess ping
        config ha-node-ip-list
        end
        set traffic-group traffic_group_1
        set floating enable
```

```

    set floating-ip 10.1.2.251
next
edit "port3"
    set vdom root
    set ip 10.1.3.252/24
    set allowaccess ping
config ha-node-ip-list
end
    set traffic-group traffic_group_2
    set floating enable
    set floating-ip 10.1.3.251
next
end

```

Configure on AWS

1. Ensure that the gateway of RS is a floating IP.
2. Assign VS IP and floating IP to AWS-EC2_ADC network interface.

In this example, you should assign VS IP 10.1.1.101 to ADC1 eth0; assign VS IP 10.1.1.102 to ADC2 eth0; assign floating IP 10.1.2.251 to ADC1 eth1; assign floating IP 10.1.2.251 to ADC2 eth2.

3. Allocate Elastic IP and bind with VS IP. User can access the VS through the public IP.

In this example, you should allocate elastic IP for VS1 IP 10.1.1.101 and VS2 IP 10.1.1.102.

aws Services Resource Groups

Addresses > Associate address

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (13.57.116.122)

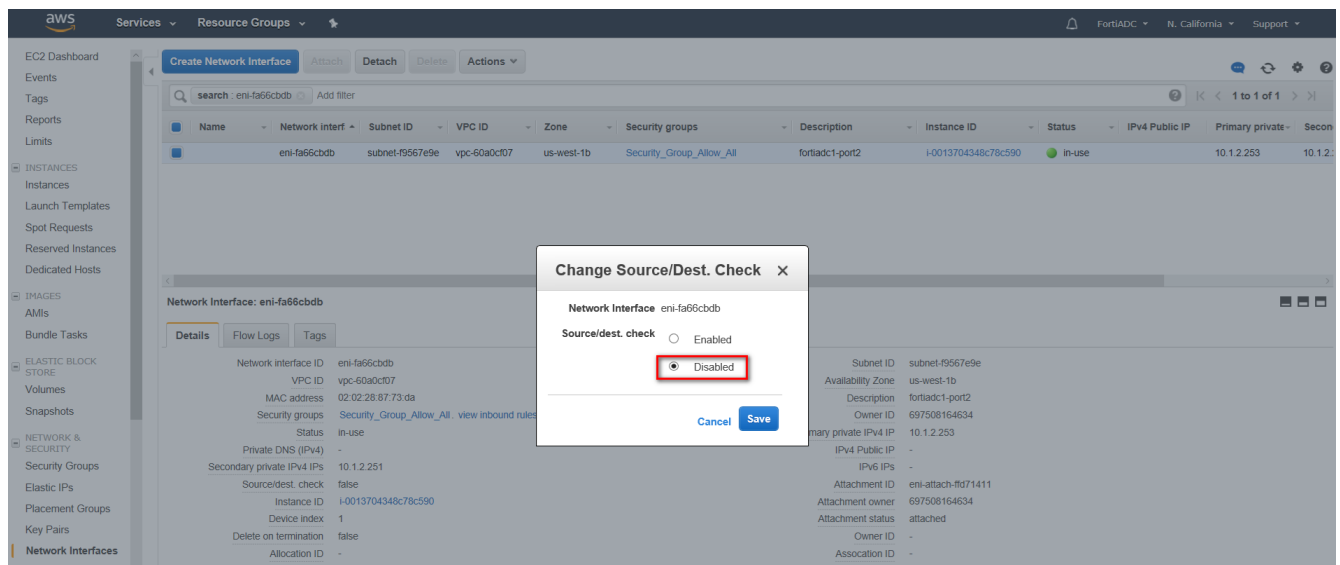
Resource type ☐ Instance ☒ Network interface

Network interface eni-c170dde0

Private IP 10.1.1.101

Reassociation ☒ Allow Elastic IP to be reassociated if already attached

4. For L4_DNAT_VS or L7 VS enabled "client-address", you must disable "Source/Dest. Check" on AWS_EC2_ADC interface, which connects to RS.



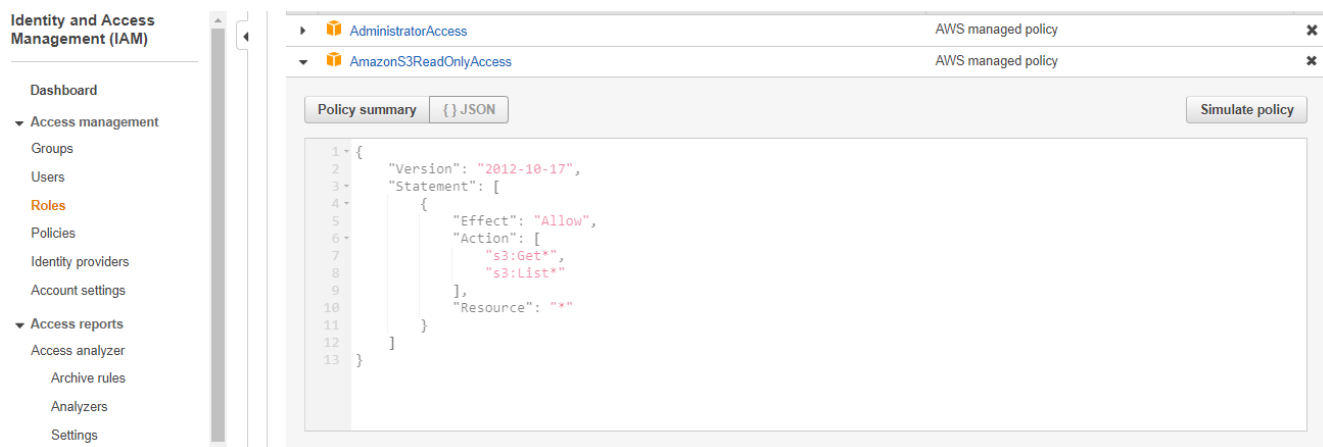
Bootstrapping the FortiADC-VM at initial boot-up using user data

If you are installing and configuring your applications on Amazon EC2 dynamically at instance launch time, you will typically need to pull and install packages, deploy files, and ensure services are started. The following bootstrapping instructions help simplify, automate, and centralize FortiADC-VM deployment directly from the configuration scripts stored in AWS S3. This is also called "cloud-init".

Setting up IAM roles

IAM roles need S3 bucket read access. This example applies the existing AmazonS3ReadOnlyAccess policy to the role by adding the following code or selecting S3ReadOnlyAccess from the policy list in adding to the role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "*"
    }
  ]
}
```



If you need further instructions, please refer to the AWS documentation on [IAM Roles for Amazon EC2](#)

Creating S3 buckets with license and firewall configurations

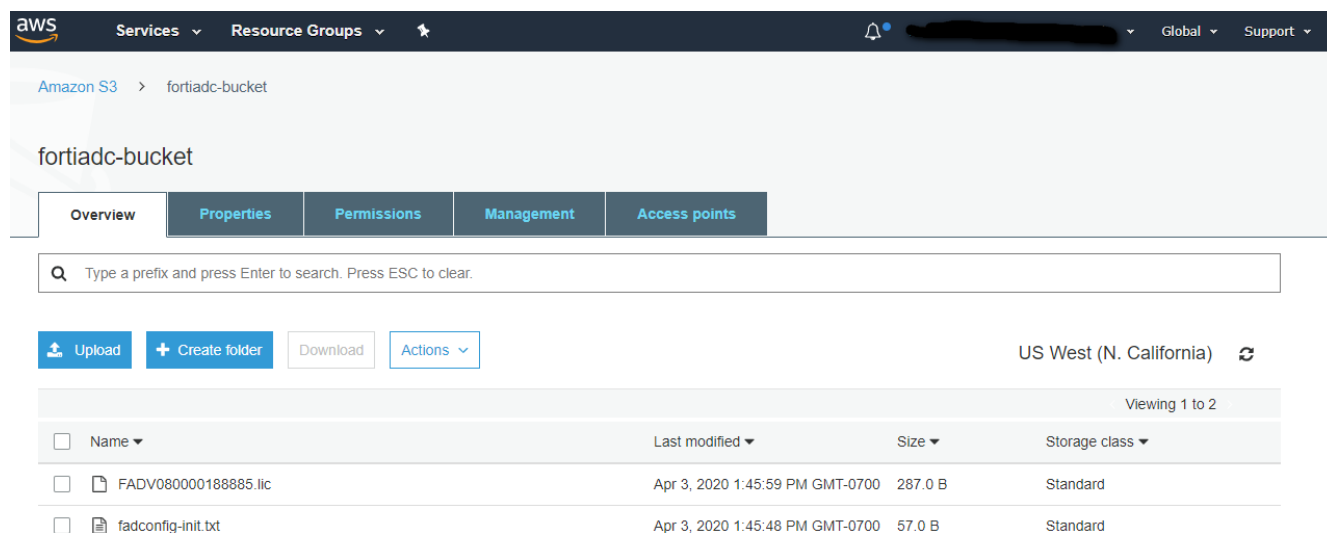
1. On the AWS console, create an Amazon S3 bucket at the root level for the bootstrap files.
2. Upload the license file and configuration files(s) to the S3 bucket. In this example, one license file and configuration files are uploaded. For example, let's have the following FortiADC CLI command statement in the config file:

```
config system global
```

```
set hostname fadcloudinit
end
```

This is to set a hostname as part of initial configuration at first launch.

```
{
  "bucket" : "fortiadc-bucket",
  "region" : "us-west-1",
  "license" : "/FADV080000188885.lic",
  "config" : "/fadconfig-init.txt"
}
```



The screenshot shows the AWS S3 console interface for a bucket named 'fortiadc-bucket'. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a user profile. The breadcrumb trail shows 'Amazon S3 > fortiadc-bucket'. Below the bucket name, there are tabs for 'Overview', 'Properties', 'Permissions', 'Management', and 'Access points'. A search bar is present with the placeholder text 'Type a prefix and press Enter to search. Press ESC to clear.' Below the search bar, there are buttons for 'Upload', 'Create folder', 'Download', and 'Actions'. The region is set to 'US West (N. California)'. A table lists the contents of the bucket, showing two files: 'FADV080000188885.lic' and 'fadconfig-init.txt'. The table has columns for 'Name', 'Last modified', 'Size', and 'Storage class'.

Name	Last modified	Size	Storage class
FADV080000188885.lic	Apr 3, 2020 1:45:59 PM GMT-0700	287.0 B	Standard
fadconfig-init.txt	Apr 3, 2020 1:45:48 PM GMT-0700	57.0 B	Standard

Launching the instance using roles and user data

Follow the normal procedure to launch the instance from the AWS marketplace. When selecting the VPC subnet, the instance must be with the role that was created and specify the information about the license file and configuration file from the AWS S3 bucket previously configured under **Advanced Settings**.

The screenshot shows the AWS Management Console interface for the 'Step 3: Configure Instance Details' of an EC2 instance launch. The console is in the 'N. California' region. The 'Number of instances' is set to 1. The 'Purchasing option' is 'On-Demand'. The 'Network' is 'vpc-60a0cf07 | FortiADC-VPC' and the 'Subnet' is 'subnet-2b2a024c | 10_1_4_0 | us-west-1b'. The 'Auto-assign Public IP' is 'Enable'. The 'Placement group' is 'Add instance to placement group'. The 'Capacity Reservation' is 'Open'. The 'IAM role' is 'FortiADC_Role'. The 'Advanced Details' section shows 'Metadata accessible' as 'Enabled', 'Metadata version' as 'V1 and V2 (token optional)', and 'Metadata token response hop limit' as '1'. The 'User data' field is highlighted with a red box and contains the following JSON configuration:

```
{
  "bucket": "fortiadc-bucket",
  "region": "us-west-1",
  "license": "/FADV080000188885.lic",
  "config": "/fadcconfig-init.txt",
}
```

The 'Review and Launch' button is visible at the bottom right of the console.

After launching the FortiADC-VM, open the console to verify that the VM is booting and utilizing the license file and configuration file that was provided.

[Instances](#) > Get instance screenshot

Get instance screenshot

Below is a screenshot of i-0af806ecbea6231d5 at 2020-04-03T16:21:52.695-07:00.

 Refresh

```
Partition /dev/xvdb ... Success

We'll now format the log disk. This could take up 20 min.
Let it finish, don't reboot

Format log disk /dev/xvdb1 ...Success
Warning: The system supports 10 ethernet interfaces but only 1 were found.
        If interfaces are changed outside of FortiADC-VM please ensure
        the FortiADC configuration is still valid.

FortiADC-XENAWS login: Configuration applied
License installed.
Serial Number: FADU080000188885

Ready to reload system.
VM license install succeeded.

The system is reloading.....
Warning: The system supports 10 ethernet interfaces but only 1 were found.
        If interfaces are changed outside of FortiADC-VM please ensure
        the FortiADC configuration is still valid.

fadcloudinit login: _
```

After logging in, use the **get system status** command to verify the license was activated and that the specified hostname was configured.


```
fadcloudinit # get system status
Version: FortiADC-XENAWS_v5.4.0_build0721.200124
VM Registration: Valid: License has been successfully authenticated with registration servers.
VM License File: License file and resources are valid.
VM Resources: 2 CPU/8 allowed, 7859 MB RAM, 29 GB Disk
Serial-Number: FADV080000188885
WAF Signature DB: 00001.00002
IP Reputation DB: 00001.00020
Geography IP DB: 00001.00036
Geography Regions: 00002.00024 (CN)
Regular Virus DB: 00001.00123
Extended Virus DB: 00000.00000
Extreme Virus DB: 00000.00000
AV Engine: 00006.00006
IPS-DB: 00006.00741
IPS-ETDB: 00000.00000
IPS Engine: 00004.00021
Bootloader Version: n/a
Hard Disk: Capacity 29 GB, Used 72 MB ( 0.24%), Free 29 GB
Log Size: 9 KB, 0%
Hostname: fadcloudinit
HA Configured Mode: standalone
HA Effective Mode: Standalone
Distribution: International
CM Agent status: (Disabled)
Uptime: 0 days 0 hours 11 minutes
Last Reboot: Fri Apr 03 16:20:08 PDT 2020
System Time: Fri Apr 03 16:31:33 PDT 2020
```

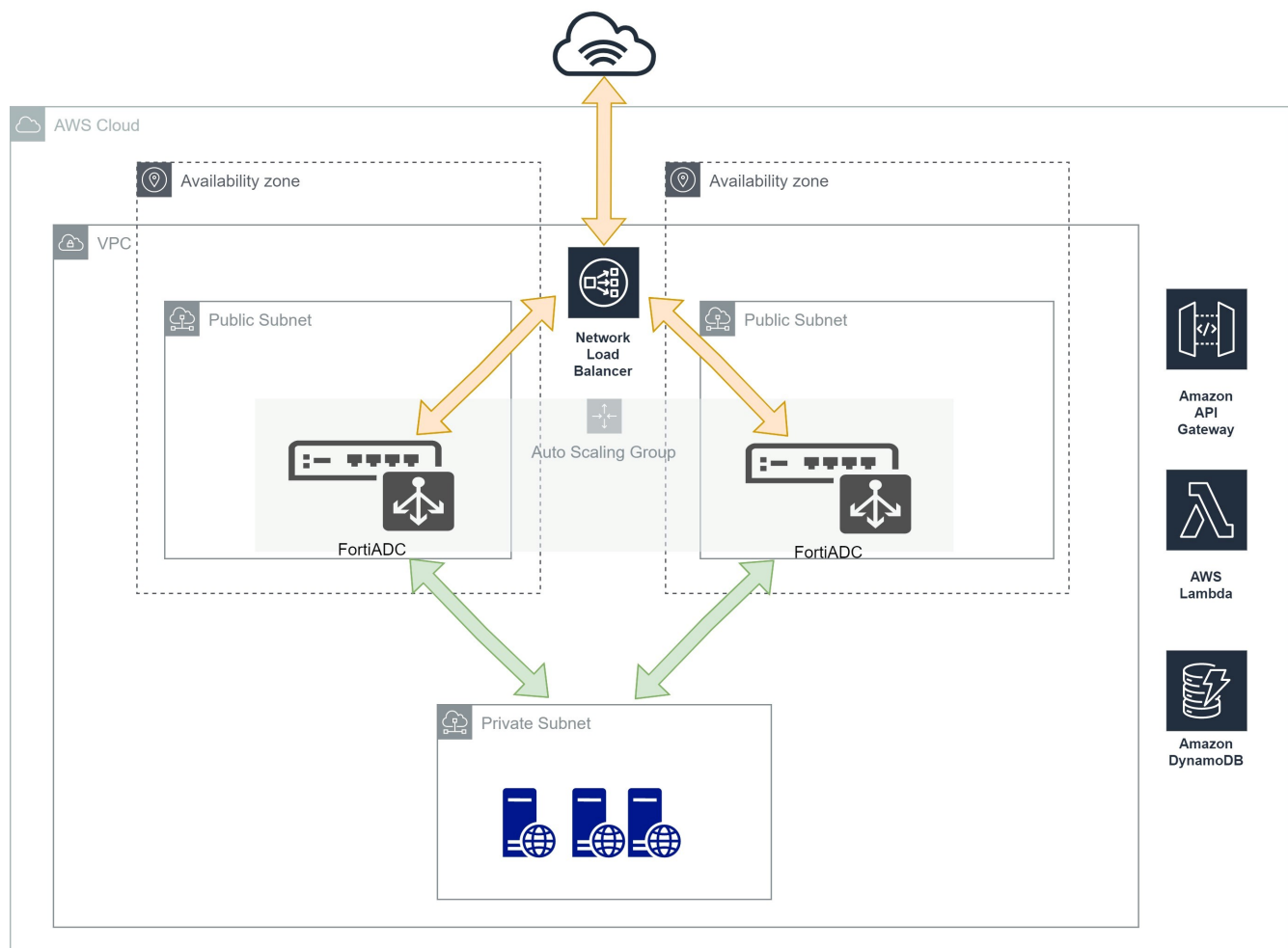
Deploying Autoscaling on AWS

You can deploy FortiADC virtual machines (VMs) to support Autoscaling on AWS. This requires a manual deployment incorporating AWS CloudFormation Templates (CFTs).

Multiple FortiADC-VM instances form an Autoscaling group (ASG) to provide highly efficient clustering at times of high workloads. FortiADC-VM instances can be scaled out automatically according to predefined workload levels. When a spike in traffic occurs, the Lambda script is invoked to automatically add FortiADC-VM instances to the ASG. Autoscaling is achieved by using FortiADC Cloud Autoscaling features such as system autoscale that synchronize operating system (OS) configurations across multiple FortiADC-VM instances at the time of scale-out events.

FortiADC Autoscale for AWS is available with FortiADC 7.2.0 and supports On-demand (PAYG) instances.

In this use case, you only need to configure on the primary FortiADC-VM, and the secondary FortiADC-VMs will automatically synchronize configurations.



FortiADC-VM Autoscale for AWS uses AWS CloudFormation Templates (CFTs) to deploy the following components:

- A highly available architecture that spans two Availability Zones (AZs).
- An Amazon Virtual Private Cloud (VPC) configured with public subnets according to AWS best practices, to provide you with your own virtual network on AWS.
- An Internet gateway to allow access to the Internet.
- In the public subnets, a FortiADC-VM host in an ASG complements AWS security groups to provide web filtering and threat detection to protect your services from cyber attacks.
- An externally facing network load balancer is created as part of the deployment process.
- An elastic IP to access the primary FortiADC-VM. When the primary role is transferred from one instance to another, the EIP will be associated with the new instance at the same time.
- An Amazon API Gateway, which acts as a front door by providing a Callback URL for the FortiADC-VM ASG. FortiADC-VMs use the API Gateway to send API calls and to process FortiADC Autoscaling tasks to synchronize configurations across multiple FortiADC-VM instances at the time of the Autoscaling scale-out event. This is currently only for internal use. There is no public access available.
- An AWS Lambda, which allows you to run certain scripts and code without provisioning servers. Fortinet provides Lambda scripts for running Autoscaling. Lambda functions are used to handle Autoscaling (launch/terminate instance based on the scale-out/scale-in policy), failover management (heartbeat check and primary election), CFT deployment, and configuration for other related components.
- An Amazon DynamoDB database that uses Fortinet-provided scripts to store information about Autoscaling condition states, including the primary node and health check state of each FortiADC-VM in the ASG group.

Planning & Prerequisites

Before you deploy FortiADC-VM Autoscaling on AWS, it is recommended that you become familiar with the following AWS services.

- [Amazon Elastic Cloud Compute \(Amazon EC2\)](#)
- [Amazon EC2 Autoscaling](#)
- [Amazon VPC](#)
- [AWS CloudFormation](#)
- [AWS Lambda](#)
- [Amazon DynamoDB](#)
- [Amazon API Gateway](#)
- [Amazon CloudWatch](#)
- [Amazon S3](#)

If you are new to AWS, go to the [Getting Started Resource Center](#) and the [AWS Training and Certification website](#).

It is expected that DevOps engineers or advanced system administrators who are familiar with the listed items deploy FortiADC Autoscale for AWS.

Technical Requirements

To start the deployment, you must have an AWS account. If you do not already have one, create one at <https://aws.amazon.com/> by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN. Your AWS account is automatically signed up for all AWS services. You are charged only for the services you use.

Log into your AWS account and verify the following:

- **IAM permissions** — Ensure that the AWS user deploying the template has sufficient permissions to perform the required service actions on resources. At a minimum, the following are required: **Service:** IAM; **Actions:** CreateRole; **Resource:** *. The FortiADC-VM Autoscaling for AWS template increases the security level of the deployment stack by narrowing down the scope of access to external resources belonging to the same user account as well as restricting access to resources within the deployment.
- **Region** — Use the region selector in the navigation bar to choose the AWS region where you want to deploy FortiADC-VM Autoscaling for AWS.
- **FortiADC subscription(s)** — Confirm that you have a valid subscription to the On-demand (PAYG) FortiADC as required for your deployment.
- **Key pair** — Ensure at least one Amazon EC2 [key pair](#) exists in your AWS account in the region where you plan to deploy FortiADC-VM Autoscaling for AWS. Make note of the key pair name.
- **Resources** — If necessary, request [service quota increases](#). This is necessary when you might exceed the default quotas with this deployment. The [Service Quotas console](#) displays your usage and quotas for some aspects of some services. For more information, see the AWS [documentation](#). The default instance type is **c5.2xlarge**.

Obtaining the deployment package

The FortiADC Autoscale for AWS deployment package is located in the [Fortinet GitHub project](#).

To obtain the deployment package:

1. From the [GitHub project release page](#), download the source code (.zip or .tar.gz) for the latest version.
2. Extract the source code into the project directory in your local workspace.
3. Create the directories and sub-directories, and place all the files under your S3 bucket using the same organizational structure as in the source code file.

Deploying the CloudFormation templates

There are two options available for deploying FortiADC-VM Autoscaling for AWS:

- Deployment into a new VPC (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, FortiADC-VMs, security groups, and other infrastructure components, and then deploys FortiADC-VM Autoscaling into this new VPC.
- Deployment into an existing VPC. This option provisions FortiADC-VM Autoscaling in your existing AWS infrastructure.



Incoming requests to the protected real servers in the private subnets will go through a connection that flows through the Internet gateway, network load balancer, and the FortiADC-VM ASG before reaching the protected real server. The protected real server returns the response using the same connection.

FortiADC-VM Autoscaling provides separate CFTs for these options. It also allows you to configure CIDR blocks, instance types, and FortiADC-VM settings.

To deploy the CloudFormation templates:

1. In the AWS Management Console, navigate to the S3 folder you uploaded files to in the previous section.
2. Click templates and select the appropriate entry template to start the deployment:
 - To deploy into a new VPC, use "workload-main.template".
 - To deploy into an existing VPC, use "workload-main-with-VPC.template"

Amazon S3 > Buckets > quickstart-fortinet-FortiADC > templates/

templates/ Copy S3 URI

Objects | Properties

Objects (8)

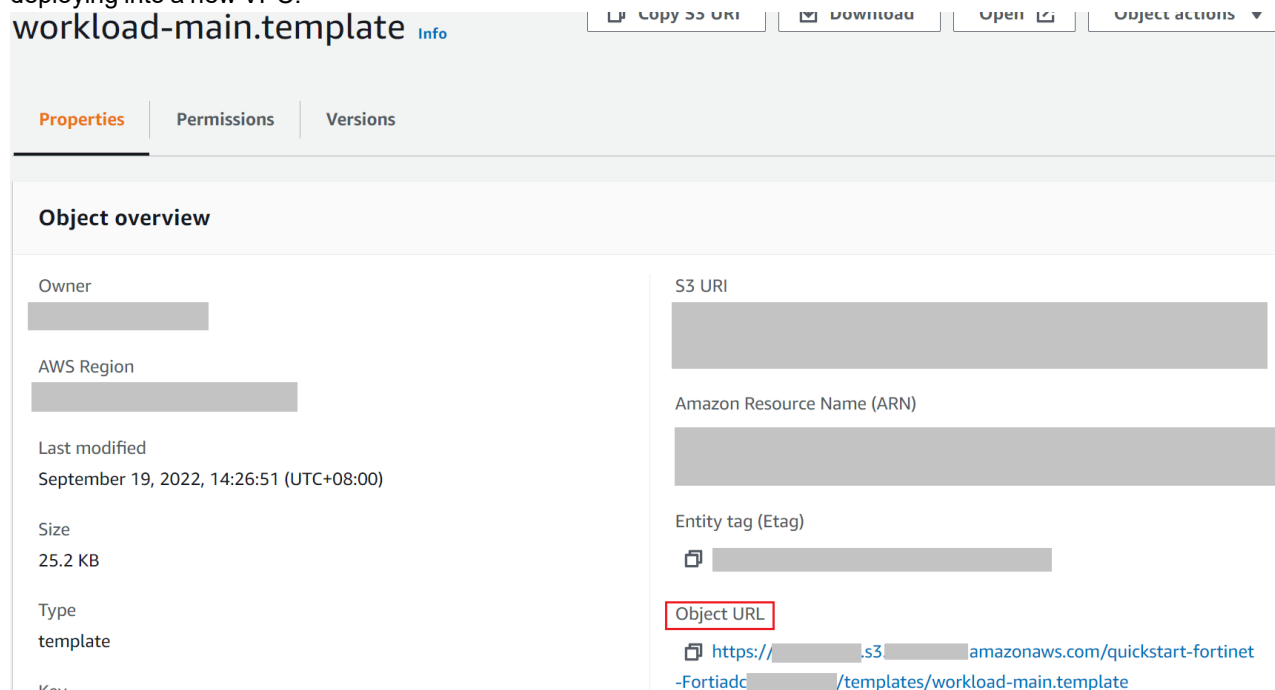
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Refresh
Copy S3 URI
Copy URL
Download
Open
Delete
Actions

Create folder
Upload

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	workload.template	template	September 19, 2022, 14:36:47 (UTC+08:00)	73.6 KB	Standard
<input type="checkbox"/>	workload-main.template	template	September 19, 2022, 14:26:51 (UTC+08:00)	25.2 KB	Standard
<input type="checkbox"/>	workload-main-with-VPC.template	template	September 19, 2022, 14:42:05 (UTC+08:00)	21.1 KB	Standard

3. Select the template and copy the **Object URL** for use in later steps. In our example, the template chosen is for deploying into a new VPC.



4. Go to **Services > Management & Governance > CloudFormation**.
5. Confirm the region you are in and then click **Create Stack > With new resources (standard)**.

6. Paste the **Object URL** from step 3 into the **Amazon S3 URL** field as shown:

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready

☐ Use a sample template

☐ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

☒ Amazon S3 URL

☐ Upload a template file

Amazon S3 URL

https://[redacted].s3.[redacted].amazonaws.com/quickstart-fortinet-Fortiadc-[redacted]/templates/workload-main.template

Amazon S3 template URL

S3 URL: [redacted] /quickstart-fortinet-Fortiadc-[redacted] /templates/workload-main.template

[View in Designer](#)

Cancel

Next

7. Click **Next**.
8. On the **Specify stack details** page, enter a stack name and review parameters for the template, providing values for parameters that require input. For details on each parameter, see the next section [cft parameters].

CFT parameters

After deploying the CFT, you must define the stack name and enter parameter values.

The following sections provide descriptions of the available parameters. Some parameters are specific to certain templates, and are only displayed when that template is selected.

After entering all the required parameters, click **Next** to continue.

Navigate to the list of parameters specific to your template:

- [Parameters for a new VPC deployment on page 33](#)
- [Parameters for an existing VPC deployment on page 36](#)

Parameters for a new VPC deployment

Network configuration

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	<i>Requires input</i>	List of Availability Zones to use for the subnets in the VPC. The FortiADC Autoscale solution uses two Availability Zones from your list and preserves the logical order you specify.
VPC CIDR (VPCCIDR)	10.0.0.0/16	Classless Inter-Domain Routing (CIDR) block for the FortiADC Auto Scale VPC.
Public subnet 1 CIDR (PublicSubnet1CIDR)	10.0.0.0/24	CIDR block for the public subnet located in Availability Zone 1 where FortiADC Autoscale instances will be deployed to.
Public subnet 2 CIDR (PublicSubnet2CIDR)	10.0.2.0/24	CIDR block for the public subnet located in Availability Zone 2 where FortiADC Autoscale instances will be deployed to.

FortiADC configuration

Parameter label (name)	Default	Description
Resource name prefix (CustomIdentifier)	fadcASG	A custom identifier as the resource name prefix. Can only contain uppercase letters, lowercase letters, and numbers. Maximum length is 10.
Fortiadc PAYG AMI Type (FortiadcPAYGAMIType)	FAD-PAYG-1gbps	FortiADC PAYG image type.
EC2 Instance type (FortiadcInstanceType)	c5.2xlarge	Instance type to launch as FortiADC-VM on-demand instances. <ul style="list-style-type: none"> • FAD-PAYG-100mbps, FAD-PAYG-500mbps, and FAD-PAYG-1gbps support the following EC2 Instance types: m5.large, m5.xlarge, m5.2xlarge, c5.large, c5.xlarge and c5.2xlarge • FAD-PAYG-5gbps and FAD-PAYG-10gbps support the

Parameter label (name)	Default	Description
		<p>following EC2 Instance types: m5.2xlarge, m5.4xlarge, m5.8xlarge, c5.2xlarge, c5.4xlarge, and c5.9xlarge</p> <p>For more information about instance types, see Amazon EC2 Instance Types.</p>
Admin port (FortiadcAdminPort)	8443	<p>A port number for FortiADC-VM administration.</p> <p>Select 8443 for HTTPS access.</p> <p>8080 port is reserved for HTTP access.</p> <p>10443 port is reserved for auto scaling configuration synchronization port.</p>
Admin CIDR block (FortiadcAdminCidr)	<i>Requires input</i>	<p>CIDR block for external admin management access.</p> <p>Note: 0.0.0.0/0 accepts connections from any IP address. It is recommend to use a constrained CIDR range to reduce the potential of inbound attacks from unknown IP addresses.</p>
Key pair name (KeyPairName)	<i>Requires input</i>	Amazon EC2 key pair for admin access.
FortiADC Elastic IP option (ElasticIPOption)	Use the Elastic IP specified in FortiADC Elastic IP or Name	<p>An Elastic IP can be used to access the primary FortiADC-VM. When the primary role is transferred from one instance to another, the EIP will be associated with the new instance at the same time. You can fill in the existing Elastic IP specified in FortiADC Elastic IP or Name, or let FortiADC generate a new one for you.</p>
FortiADC Elastic IP or Name (FortiadcElasticIP)	fadcASG-EIP	Specify the Elastic IP address or name, through which you can manage FortiADC. If you use an existing Elastic IP, fill it in here. If you create a new Elastic IP, give it a name so that you can find it easily in the AWS console.

FortiADC auto-scaling group configuration

Parameter label (name)	Default	Description
Instance lifecycle expiry (ExpireLifecycleEntry)	300	FortiADC-VM instance lifecycle expiry entry (in seconds). The range is 60 to 3600.
Desired capacity (FortiadcAsgDesiredCapacity)	2	The number of FortiADC instances the group should have at any time. Must keep at least 2 FortiADCs in the group for High Availability. Minimum is 2.
Minimum group size (FortiadcAsgMinSize)	2	Minimum number of FortiADC instances in the Auto-Scaling Group. Minimum is 2.
Maximum group size (FortiadcAsgMaxSize)	4	Maximum number of FortiADC instances in the Auto-Scaling Group. Minimum is 2.

Parameter label (name)	Default	Description
Health check grace period (FortiadcAsgHealthCheckGracePeriod)	300	The length of time (in seconds) that autoscaling waits before checking an instance's health status. Minimum is 60.
Scaling cooldown period (FortiadcAsgCooldown)	300	The ASG waits for the cooldown period (in seconds) to complete before resuming scaling activities. The range is 60 to 3600.
Scale-out threshold (FortiadcAsgScaleOutThreshold)	80	The average CPU threshold (in percentage) for the FortiADC-VM ASG to scale out (add) one instance. The range is 1 to 100. The value should be between Scale-in threshold and 100.
Scale-in threshold (FortiadcAsgScaleInThreshold)	25	The average CPU threshold (in percentage) for the FortiADC-VM ASG to scale in (remove) one instance. The range is 1 to 100. The value should be between 1 and Scale-out threshold .
Healthy threshold (FortiadcElbTgHealthyThreshold)	2	The number of consecutive health check failures required before considering a FortiADC-VM instance is unhealthy. Minimum is 2.
Health Check Timeout (FortiadcElbTgHCTimeout)	2	The amount of time in seconds, during which no response from a FortiADC instance means a failed health check. Minimum is 2.
Health Check Interval (FortiadcElbTgHCInterval)	5	The approximate amount of time in seconds between health checks of an individual FortiADC instance. Minimum is 5.

Load balancing configuration

Parameter label (name)	Default	Description
Web service traffic port (BalanceWebTrafficOverPort)	443	Receive HTTPS web service traffic through this port and load balance traffic to this port of FortiADC. The range is 1 to 65535.

AWS Quick Start configuration

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	<i>Requires input</i>	The name of the S3 bucket in which the FortiADC autoscaling deployment package is stored (for example: <code>aws-quickstart</code>). The Quick Start bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Quick Start S3 key prefix (QSS3KeyPrefix)	<i>Requires input</i>	The path of the FortiADC autoscaling deployment package in s3 (for example: <code>quickstart-fortinet-Fortiadc/</code>). The Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

Parameters for an existing VPC deployment

Network configuration

Parameter label (name)	Default	Description
VPC ID (VpcId)	<i>Requires input</i>	Select the existing VPC IDs where you want to deploy the ASG and related resources. The VPC must have the option DNS hostnames enabled, and subnets (Public/Private if needed) in different Availability Zones.
VPC CIDR (VPCCIDR)	<i>Requires input</i>	Classless Inter-Domain Routing (CIDR) block for the FortiADC Auto Scale VPC.
PublicSubnet1 (PublicSubnet1)	<i>Requires input</i>	Select a subnet in the VPC.
PublicSubnet2 (PublicSubnet2)	<i>Requires input</i>	Select another subnet in the VPC. The two subnets should be in different Availability Zones.

FortiADC configuration

Parameter label (name)	Default	Description
Resource name prefix (CustomIdentifier)	fadcASG	A custom identifier as the resource name prefix. Can only contain uppercase letters, lowercase letters, and numbers. Maximum length is 10.
Fortiadc PAYG AMI Typ (FortiadcPAYGAMIType)	FAD-PAYG-1gbps	FortiADC PAYG image type.
Instance type (FortiadcInstanceType)	c5.2xlarge	<p>Instance type to launch as FortiADC-VM on-demand instances.</p> <ul style="list-style-type: none"> FAD-PAYG-100mbps, FAD-PAYG-500mbps, and FAD-PAYG-1gbps support the following EC2 Instance types: m5.large, m5.xlarge, m5.2xlarge, c5.large, c5.xlarge and c5.2xlarge FAD-PAYG-5gbps and FAD-PAYG-10gbps support the following EC2 Instance types: m5.2xlarge, m5.4xlarge, m5.8xlarge, c5.2xlarge, c5.4xlarge, and c5.9xlarge <p>For more information about instance types, see Amazon EC2 Instance Types.</p>
Admin port (FortiadcAdminPort)	8443	<p>A port number for FortiADC-VM administration.</p> <p>Select 8443 for HTTPS access.</p> <p>8080 port is reserved for HTTP access.</p> <p>10443 port is reserved for auto scaling configuration synchronization port.</p>

Parameter label (name)	Default	Description
Admin CIDR block (FortiadcAdminCidr)	<i>Requires input</i>	CIDR block for external admin management access. Note: 0.0.0.0/0 accepts connections from any IP address. It is recommend to use a constrained CIDR range to reduce the potential of inbound attacks from unknown IP addresses.
Key pair name (KeyPairName)	<i>Requires input</i>	Amazon EC2 key pair for admin access.
FortiADC Elastic IP option (ElasticIPOption)	Use the Elastic IP specified in FortiADC Elastic IP or Name	An Elastic IP can be used to access the primary FortiADC-VM. When the primary role is transferred from one instance to another, the EIP will be associated with the new instance at the same time. You can fill in the existing Elastic IP specified in FortiADC Elastic IP or Name , or let FortiADC generate a new one for you.
FortiADC Elastic IP or Name (FortiadcElasticIP)	fadcASG-EIP	Specify the Elastic IP address or name, through which you can manage FortiADC. If you use an existing Elastic IP, fill it in here. If you create a new Elastic IP, give it a name so that you can find it easily in the AWS console.

FortiADC auto-scaling group configuration

Parameter label (name)	Default	Description
Instance lifecycle expiry (ExpireLifecycleEntry)	300	FortiADC-VM instance lifecycle expiry entry (in seconds). The range is 60 to 3600.
Desired capacity (FortiadcAsgDesiredCapacity)	2	The number of FortiADC instances the group should have at any time. Must keep at least 2 FortiADCs in the group for High Availability. Minimum is 2.
Minimum group size (FortiadcAsgMinSize)	2	Minimum number of FortiADC instances in the Auto-Scaling Group. Minimum is 2.
Maximum group size (FortiadcAsgMaxSize)	4	Maximum number of FortiADC instances in the Auto-Scaling Group. Minimum is 2.
Health check grace period (FortiadcAsgHealthCheckGracePeriod)	300	The length of time (in seconds) that autoscaling waits before checking an instance's health status. Minimum is 60.
Scaling cooldown period (FortiadcAsgCooldown)	300	The ASG waits for the cooldown period (in seconds) to complete before resuming scaling activities. The range is 60 to 3600.
Scale-out threshold (FortiadcAsgScaleOutThreshold)	80	The average CPU threshold (in percentage) for the FortiADC-VM ASG to scale out (add) one instance. The range is 1 to 100. The value should be between Scale-in threshold and 100.

Parameter label (name)	Default	Description
Scale-in threshold (FortiadcAsgScaleInThreshold)	25	The average CPU threshold (in percentage) for the FortiADC-VM ASG to scale in (remove) one instance. The range is 1 to 100. The value should be between 1 and Scale-out threshold .
Healthy threshold (FortiadcElbTgHealthyThreshold)	2	The number of consecutive health check failures required before considering a FortiADC-VM instance is unhealthy. Minimum is 2.
Health Check Timeout (FortiadcElbTgHCTimeout)	2	The amount of time in seconds, during which no response from a FortiADC instance means a failed health check. Minimum is 2.
Health Check Interval (FortiadcElbTgHCInterval)	5	The approximate amount of time in seconds between health checks of an individual FortiADC instance. Minimum is 5.

Load balancing configuration

Parameter label (name)	Default	Description
Web service traffic port (BalanceWebTrafficOverPort)	443	Receive HTTPS web service traffic through this port and load balance traffic to this port of FortiADC. The range is 1 to 65535.

AWS Quick Start configuration

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	<i>Requires input</i>	The name of the S3 bucket in which the FortiADC autoscaling deployment package is stored (for example: <code>aws-quickstart</code>). The Quick Start bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Quick Start S3 key prefix (QSS3KeyPrefix)	<i>Requires input</i>	The path of the FortiADC autoscaling deployment package in s3 (for example: <code>quickstart-fortinet-Fortiadc/</code>). The Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

Available instance types in each region

AWS has different support for instance types in each region. Refer to the [AWS documentation](#) to check whether or not your selected FortiADC instance type is supported in the deployment region and zone.

To see if the instance type is supported in your zone, enable **Available zones**.

Attribute columns

Choose instance type attributes to display as columns in the table

- ☒ Instance type (default)
- ☐ Instance family
- ☐ Instance size
- ☒ Availability zones
- ☐ Free-Tier eligible
- ☐ Bare metal
- ☐ Hypervisor
- ☒ vCPUs
- ☒ Architecture
- ☐ Cores
- ☐ Valid cores
- ☐ Threads per core

Cancel

Confirm

You can filter by instance types then search for your instance type (for example, c5.xlarge) to see its supported regions listed in the Availability zones field.

Instance types (1)

Instance type: c5.xlarge X

Clear filters

<input type="checkbox"/>	Instance type ▾	Availability zones ▾	vCPUs ▾	Architecture ▾	Memory (GiB) ▾
<input type="checkbox"/>	c5.xlarge	us-west-2a, us-west-2b, us-west-2c, us...	4	x86_64	8

Optional settings

After entering required parameters and clicking **Next**, you are directed to the **Configure stack options** page to specify optional settings.

Once you have configured optional settings, click **Next** to move forward in the deployment.

Tags

You can specify key-value pairs (tags) to apply to resources in your stack. For details, see the [AWS documentation](#).


Permissions

Under the **Permissions** section, you can specify an IAM role that AWS CloudFormation uses to create, modify, or delete resources in your stack. For details, see the [AWS documentation](#).

Advanced options

Under **Advanced** options, it is recommended that you disable the Stack creation option **Rollback on failure** to allow for a better troubleshooting experience. For details, see the [AWS documentation](#).


Advanced options

You can set additional options for your stack, like notification options and a stack policy. [Learn more](#) 

► Stack policy

Defines the resources that you want to protect from unintentional updates during a stack update.

► Rollback configuration

Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. [Learn more](#) 

► Notification options

▼ Stack creation options

Rollback on failure

Specifies whether the stack should be rolled back if stack creation fails.

☐ Enabled

☒ Disabled

Timeout

The number of minutes before a stack creation times out.

Termination protection

Prevents the stack from being accidentally deleted. Once created, you can update this through stack actions.

☒ Disabled

☐ Enabled

Completing the deployment

1. On the **Review** page, review and confirm the template settings, the stack details, and the stack options. Under **Capabilities**, select both check boxes to acknowledge that the template creates IAM resources and might require the ability to automatically expand macros.

Capabilities

i The following resource(s) require capabilities: [AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more.](#)

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources.

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

☒ I acknowledge that AWS CloudFormation might require the following capability:
CAPABILITY_AUTO_EXPAND

Cancel Previous Create change set **Create stack**

2. Click **Create stack** to deploy the stack.
The creation status is shown in the **Status** column. To see the latest status, refresh the view. It takes about 10 minutes to create the stack.
3. Monitor the status of the stack. Deployment has completed when each stack (including the main stack and all nested stacks) has a status of **CREATE_COMPLETE**.

Locating deployed resources

To locate a newly deployed resource, it is recommended to search for it using the ResourceTagPrefix (also referred to as the ResourceGroup Tag Key). Alternatively, the UniqueID can be used. For items that need a shorter prefix, the CustomIdentifier can be used. These keys are found on the Outputs tab as shown below. Note that the UniqueID is at the end of the ResourceTagPrefix.

Delete

Update

Stack actions ▼

Create stack ▼

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Outputs (3)

🔍 Search outputs

⚙️

Key ▲	Value ▼	Description ▼	Export name
CustomIdentifier	fadcASG	A custom identifier as resource name prefix on those resources that have a strict naming requirement.	-
ResourceTagPrefix	fadcASG-cc836360	The Value for the Tag Key 'ResourceGroup' on all resources deployed in this stack.	-
UniqueID	cc836360	An automatically generated random string as a unique ID for all resources in the deployment stack and nested stack.	-

This section includes steps on how to locate the following deployed resources:

- [VPC using the ResourceGroup Tag Key on page 44](#)
- [VPC subnets using the ResourceGroup Tag Key on page 44](#)
- [DynamoDB tables using the UniqueID on page 45](#)
- [Lambda Functions using the ResourceGroup Tag Key on page 45](#)
- [Log group using the Lambda function name on page 46](#)
- [Network Load Balancer using the ResourceGroup Tag Key on page 46](#)

VPC using the ResourceGroup Tag Key

To look up the newly deployed VPC using the ResourceGroup Tag Key:

1. In the AWS console, select **Services > Network & Content Delivery > VPC**.
2. In the left navigation tree, click **Your VPCs**.
3. Click the filter box and under **Tags**, select **ResourceGroup**.
4. Select your **ResourceTagPrefix** from the list of Tags. Your VPC will be displayed.

The screenshot shows the AWS VPC console. On the left, the navigation pane is open, showing 'Your VPCs' under 'Virtual private cloud'. The main content area is titled 'Your VPCs (1/1)' and includes a search bar 'Filter VPCs'. A filter box is open, showing 'ResourceGroup: fadcASG-cc836360' selected. Below the filter, a table lists VPCs. One VPC is shown with a checked checkbox, a minus sign in the 'N.' column, the ID 'vpc-...', state 'Ava...', and IPv4 CIDR '10.0.0.0/16'.

	N..	VPC ID	State	IPv4 CIDR
<input checked="" type="checkbox"/>	–	vpc-...	✓ Ava...	10.0.0.0/16

VPC subnets using the ResourceGroup Tag Key

To look up the newly deployed VPC subnets using the ResourceGroup Tag Key:

1. In the AWS console, select **Services > Network & Content Delivery > VPC**.
2. In the left navigation tree, click **VIRTUAL PRIVATE CLOUD > Subnets**.
3. Click the filter box and select **Tag Keys > ResourceGroup**.
4. Select your ResourceTagPrefix from the list of Tag Keys. Your VPC subnets will be displayed.

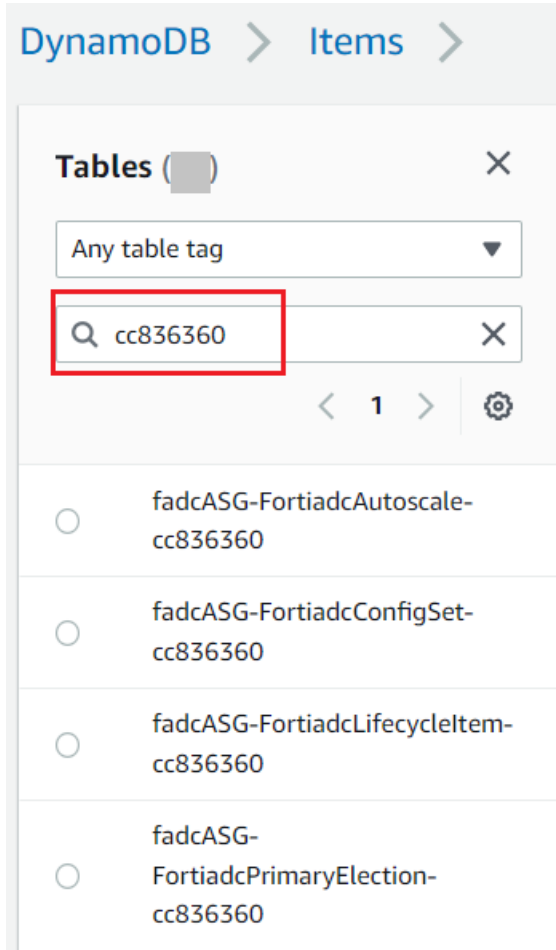
The screenshot shows the AWS Subnets console. On the left, the navigation pane is open, showing 'Subnets' under 'Virtual private cloud'. The main content area is titled 'Subnets (2)' and includes a search bar 'Filter subnets'. A filter box is open, showing 'ResourceGroup: fadcASG-cc836360' selected. Below the filter, a table lists subnets. Two subnets are shown, both with checked checkboxes, minus signs in the 'N.' column, subnet IDs 'subnet-...', state 'Ava...', VPC IDs 'vpc-...', and IPv4 CIDRs '10.0.0.0/24' and '10.0.2.0/24'.

	N..	Subnet ID	State	VPC	IPv4 CIDR
<input checked="" type="checkbox"/>	–	subnet-...	✓ Ava...	vpc-...	10.0.0.0/24
<input checked="" type="checkbox"/>	–	subnet-...	✓ Ava...	vpc-...	10.0.2.0/24

DynamoDB tables using the UniqueID

To look up the deployed DynamoDB tables using the UniqueID:

1. In the AWS console, select **Services > Database > DynamoDB**.
2. In the left navigation tree, click **Tables**.
3. Click the filter box and enter the **UniqueID**.
The DynamoDB tables will be displayed. The **Name** of each DynamoDB table will be in the format **<CustomIdentifier>-<table-name>-<UniqueID>**.

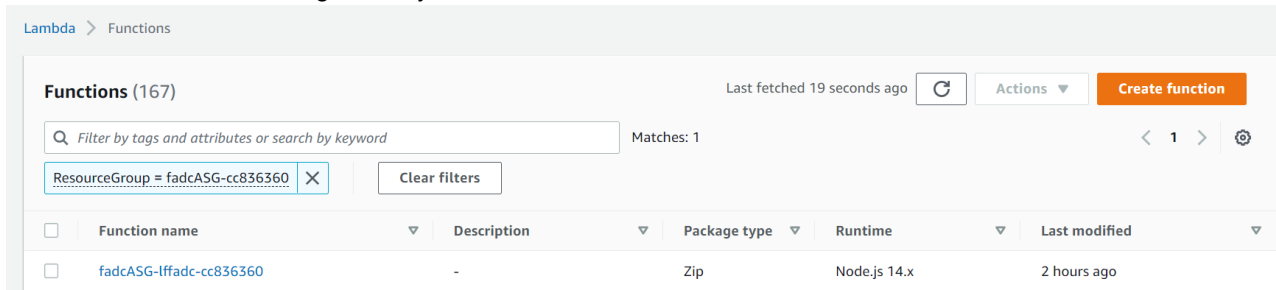


Lambda Functions using the ResourceGroup Tag Key

To look up the deployed Lambda Functions using the ResourceGroup Tag Key:

1. In the AWS console, select **Services > Compute > Lambda**.
2. In the left navigation tree, click **Functions**.
3. Click the filter box and enter the **ResourceGroup**.
The Lambda Functions will be displayed. Each **Function** name will be in the format **<CustomIdentifier>-<LambdaFunctionName>-<UniqueID>**.

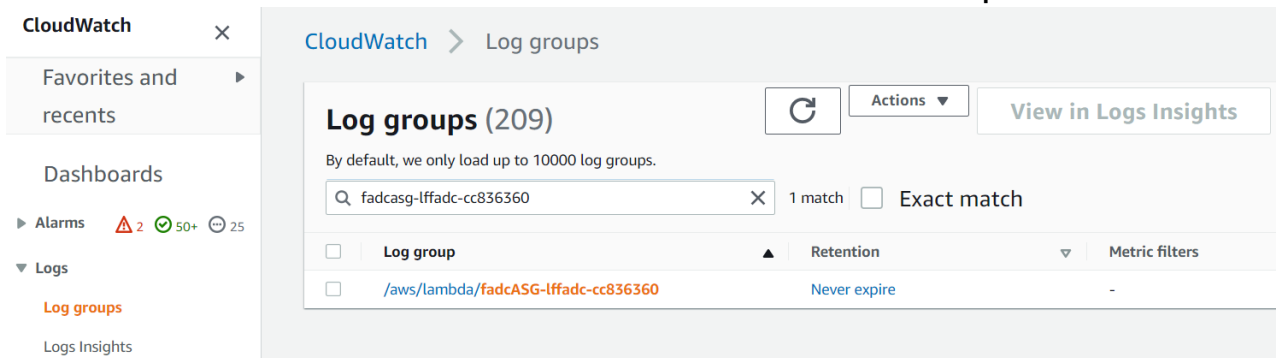
Click the **Function** name to go directly to the function.



Log group using the Lambda function name

To look up the deployed Log group using the Lambda function name:

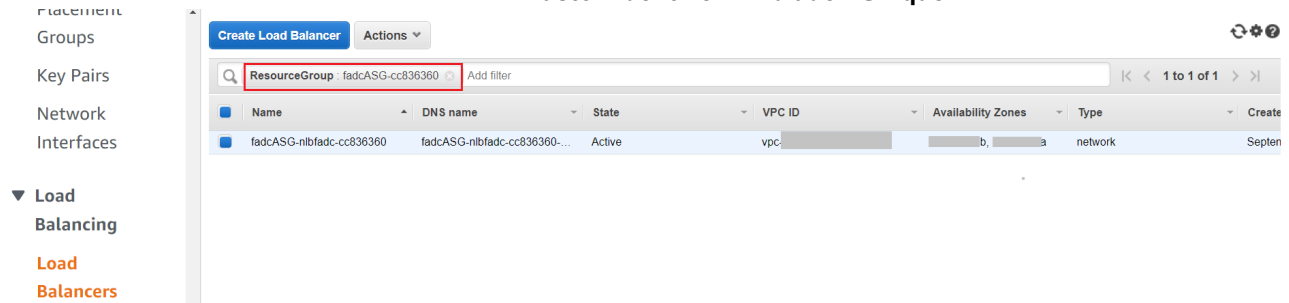
1. In the AWS console, select **Services > Management & Governance > CloudWatch**.
2. In the left navigation tree, click **Logs > Log Groups**.
3. Click the filter box and enter the **Lambda Function Name**.
The main Lambda Function name will be in the format **<CustomIdentifier>-lffadc-<UniqueID>**.



Network Load Balancer using the ResourceGroup Tag Key

To look up the deployed Network Load Balancer using the ResourceGroup Tag Key:

1. In the AWS console, select **Services > Compute**.
2. In the left navigation tree, click **Load Balancing > Load Balancer**.
3. Click the filter box and enter the **ResourceGroup**.
The Load balancer name will be in the format **<CustomIdentifier>-nlbfadc-<UniqueID>**.



Verifying the deployment

FortiADC-VM Autoscale creates an Auto Scaling group (ASG) with lifecycle events attached to the group. To verify the deployment, follow the steps below.

1. Verify that the ASG (with the name starting with fadcASG by default or the prefix you specified in **Resource name prefix**) was created after completion of the CloudFormation stack.

EC2 > Auto Scaling groups

Auto Scaling groups (1/5) Info

Refresh Edit Delete Create an Auto Scaling group

Q fadcASG X 2 matches < 1 > ⚙

	Name	Launch template/...	I...
<input checked="" type="checkbox"/>	fadcASG-FortiadcAutoScalingGroup-cc836360...	fadcASG-LaunchTemplate...	2


2. Navigate to the **Instance management** tab of the ASG.
You should see the instances with the "In-Service" lifecycle status. The number of instances should be the same as


the **Desired Capacity** that was specified in the CFT parameter.

EC2 > Auto Scaling groups > fadcASG-FortiadcAutoScalingGroup-cc836360

Details | Activity | Automatic scaling | **Instance management** | Monitoring

Instance refresh

Instances (2)  **Actions** ▼

< 1 > 

<input type="checkbox"/>	Instance ID ▼	Lifecycle ▼	Instance type ▼	Weighted
<input type="checkbox"/>	i-██████████...	InService	c5.2xlarge	-
<input type="checkbox"/>	i-██████████...	InService	c5.2xlarge	-

3. Navigate to the **Automatic scaling** tab of the ASG and execute a scale-out action.
The scale-out action should trigger a lifecycle event for instantiating a FortiADC instance. When the scale-out event



is completed, you should see the total number of instances in the ASG is increased by 1.

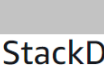
EC2 > Auto Scaling groups > fadcASG-FortiadcAutoScalingGroup-cc836360

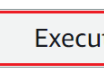
Details | Activity | **Automatic scaling** | Instance management | Monitoring


Instance refresh


Dynamic scaling policies (1/2) [Info](#)

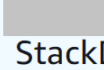
 Actions  Create dynamic scaling policy < 1 >

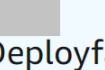
**StackD**

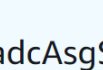
**Solution-**


**Solution-**



**StackDeployfadcAsgSolution-**

**StackDeployfadcAsgSolution-**

**StackDeployfadcAsgSolution-**



Policy type:
Simple scaling

Enabled or disabled?
Enabled

Execute policy when:
-StackDeployfadcAsgSolution-
-AlarmCpuUtilLow-
breaches the alarm threshold:
CPUUtilization < 25 for 1 consecutive
periods of 300 seconds for the metric
dimensions:
AutoScalingGroupName = fadcASG-
FortiadcAutoScalingGroup-cc836360

Take the action:
Remove 1 capacity units

And then wait:
300 seconds before allowing another
scaling activity

Policy type:
Simple scaling

Enabled or disabled?
Enabled

Execute policy when:
-StackDeployfadcAsgSolution-
-AlarmCpuUtilHigh-
breaches the alarm threshold:
CPUUtilization > 80 for 1 consecutive
periods of 300 seconds for the metric
dimensions:
AutoScalingGroupName = fadcASG-
FortiadcAutoScalingGroup-cc836360

Take the action:
Add 1 capacity units

And then wait:
300 seconds before allowing another
scaling activity

EC2 > Auto Scaling groups > fadcASG-FortiadcAutoScalingGroup-cc836360

Details | Activity | Automatic scaling | **Instance management** | Monitoring

Instance refresh

Instances (3) ⌂ Actions ▼

< 1 > ⚙

<input type="checkbox"/>	Instance ID ▼	Lifecycle ▼	Instance type ▼	Weighted capacity ▼
<input type="checkbox"/>	i-██████████...	InService	c5.2xlarge	-
<input type="checkbox"/>	i-██████████...	InService	c5.2xlarge	-
<input type="checkbox"/>	i-██████████...	InService	c5.2xlarge	-

Repeat the scale-in action as needed. Note that you must wait 300 seconds, as specified in the Scaling Cooldown period, between scale-out and scale-in actions.



4. Check the latest logs in the log group. You will see FortiADC-VM sending heartbeats by calling the /complete REST API to the lffadc Lambda function. The lffadc Lambda function checks whether the heartbeat is in time and


reports the healthy status in log.



CloudWatch > Log groups > /aws/lambda/fadcASG-lffadc-cc836360 > 2022/09/19/[\$LATEST]

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

☐ View as text  Actions  Create metric filter

 Filter events

2022-09-19 (1) > 2022-09-19 (2)  

Timestamp	Message
	There are older events to load. Load more .
2022-09-19T17:33:52.309+08:00	START RequestId: [REDACTED] Version: \$LATEST
2022-09-19T17:33:52.311+08:00	INFO Incoming event: {"resource":"/complete","path":"/complete","httpMethod":"POST","he...
2022-09-19T17:33:52.430+08:00	INFO found table fadcASG-FortiadcPrimaryElection-cc836360
2022-09-19T17:33:52.450+08:00	INFO found table fadcASG-FortiadcLifecycleItem-cc836360
2022-09-19T17:33:52.470+08:00	INFO found table fadcASG-FortiadcAutoscale-cc836360
2022-09-19T17:33:52.538+08:00	INFO called findCallingInstanceId: instance Id (i-[REDACTED]) found.
2022-09-19T17:33:52.538+08:00	INFO called findCallingInstanceId: instance Id (i-[REDACTED]) found.
2022-09-19T17:33:52.538+08:00	INFO called findHeartBeatInterval: interval (10) found.
2022-09-19T17:33:52.549+08:00	INFO called findFortiADCStatus: status not found
2022-09-19T17:33:52.687+08:00	INFO instance i-[REDACTED] is in ASG: fadcASG-FortiadcAutoScalingGroup-cc836360
2022-09-19T17:33:52.749+08:00	INFO Elected primary found: {"subnetId":"subnet-[REDACTED]","voteEndTime":166357...
2022-09-19T17:33:52.749+08:00	INFO calling getPrimaryInfo
2022-09-19T17:33:52.749+08:00	INFO i-090e33e73102d2fbf: calling describeInstance
2022-09-19T17:33:52.909+08:00	INFO i-090e33e73102d2fbf: called describeInstance, result: {"Reservations":[{"Groups":[...
2022-09-19T17:33:53.090+08:00	INFO heartBeatAllowLossCount is 5 heartBeatDelayAllowance is 60000
2022-09-19T17:33:53.090+08:00	INFO called getInstanceHealthCheck. (timestamp: 1663580032311, interval:10)healthcheck ...
2022-09-19T17:33:53.090+08:00	INFO i-[REDACTED]: calling describeInstance
2022-09-19T17:33:53.289+08:00	INFO i-[REDACTED]: called describeInstance, result: {"Reservations":[{"Groups":[...
2022-09-19T17:33:53.433+08:00	INFO heartBeatAllowLossCount is 5 heartBeatDelayAllowance is 60000
2022-09-19T17:33:53.433+08:00	INFO called getInstanceHealthCheck. (timestamp: 1663580032311, interval:10)healthcheck ...
2022-09-19T17:33:53.433+08:00	INFO instance (id:i-[REDACTED], ip: 10.0.2.154) health check (healthy, heartBeat...
2022-09-19T17:33:53.483+08:00	INFO called updateInstanceHealthCheck
2022-09-19T17:33:53.483+08:00	INFO hb record updated on (timestamp: 1663580033433, instance id:i-[REDACTED], i...
2022-09-19T17:33:53.483+08:00	INFO called findFortiADCCfgSyncPort: cfgsyncport not found or is not primary node
2022-09-19T17:33:53.526+08:00	INFO fadcCfgsyncport: 10443
2022-09-19T17:33:53.529+08:00	END RequestId: [REDACTED]

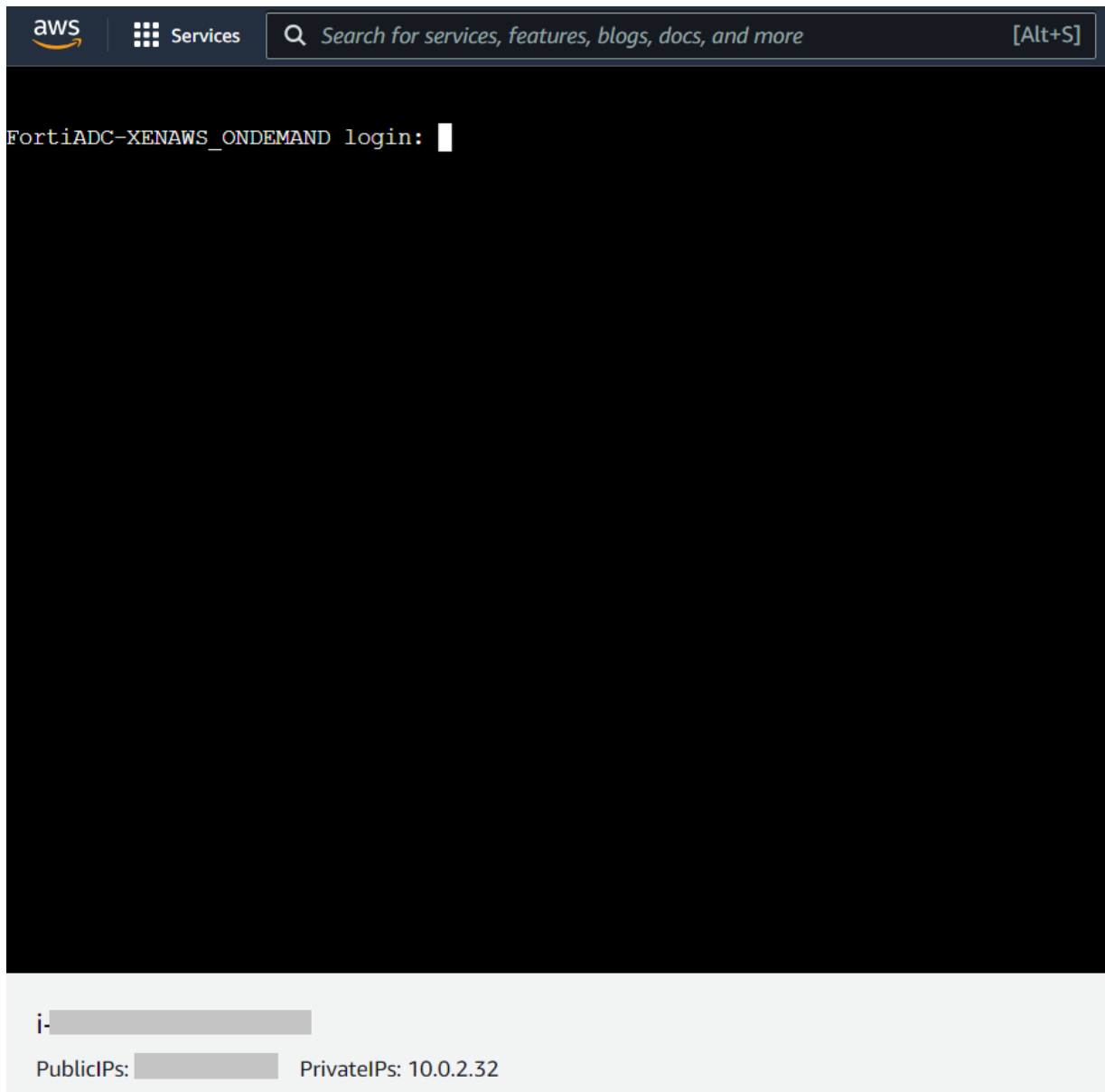
Connecting to the primary FortiADC-VM

If you have enabled the Elastic IP option in the CFT parameter, you can use the EIP to manage the primary FortiADC.

1. Identify the management IP address of the FortiADC.
If you choose to use an existing Elastic IP, the Elastic IP you entered is the management IP of the FortiADC.
If you choose to create a new Elastic IP, you need to search for the IP address created for you on the AWS Elastic IP console using the **FortiADC Elastic IP** or **Name** you have specified in the template.
Take note of the Elastic IP address for later steps.
2. Identify the Primary FortiADC in the ASG from the DynamoDB.
 - a. In the AWS console, go to **Services > Database > DynamoDB > Items**.
 - b. Locate the **FortiadcPrimaryElection** table and copy the **instanceld** for later steps.
For steps on how to locate the FortiadcPrimaryElection table, see [Locating deployed resources on page 43](#).
[DynamoDB](#) > [Items](#) > fadcASG-FortiadcPrimaryElection-cc836360

The screenshot shows the AWS DynamoDB console interface. The breadcrumb navigation is [DynamoDB](#) > [Items](#) > fadcASG-FortiadcPrimaryElection-cc836360. The table name is fadcASG-FortiadcPrimaryElection-cc836360. The 'Scan/Query items' section shows a 'Completed' status with 'Read capacity units consumed: 0.5'. Below this, the 'Items returned (1)' section displays a table with the following columns: asgName, instanceld, ip, subnetId, voteEndTime, voteState, and vpcId. The 'instanceld' column is highlighted with a red box, and its value is copied. The table has one item with the following data: asgName: fadcASG-FortiadcAut..., instanceld: i-..., ip: 10.0.2.32, subnetId: subnet-..., voteEndTime: 1663644267..., voteState: done, vpcId: vpc-...

- c. Navigate to the EC2 instance tab and paste the instanceld into the filter box.
 - d. Locate the primary instance from the filtered list.
3. Connect to the Primary node via the serial console, SSH or web browser.
 - Connect via the serial console:
In the **Primary Instance** tab, click **Connect > EC2 serial console**.



- Connect via SSH:
Use **admin** instead of root as the login user.

Connect to instance [Info](#)

Connect to your instance i-0d98f75c013fa0c53 using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is ytlai.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 `chmod 400 .pem`
4. Connect to your instance using its Public DNS:
 `ec2-..compute.amazonaws.com`

Example:

`ssh -i ".pem" root@ec2-..compute.amazonaws.com`

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

- Connect via web browser:
If you have not enabled the Elastic IP, take note of the public IP or FQDN of the primary FortiADC.

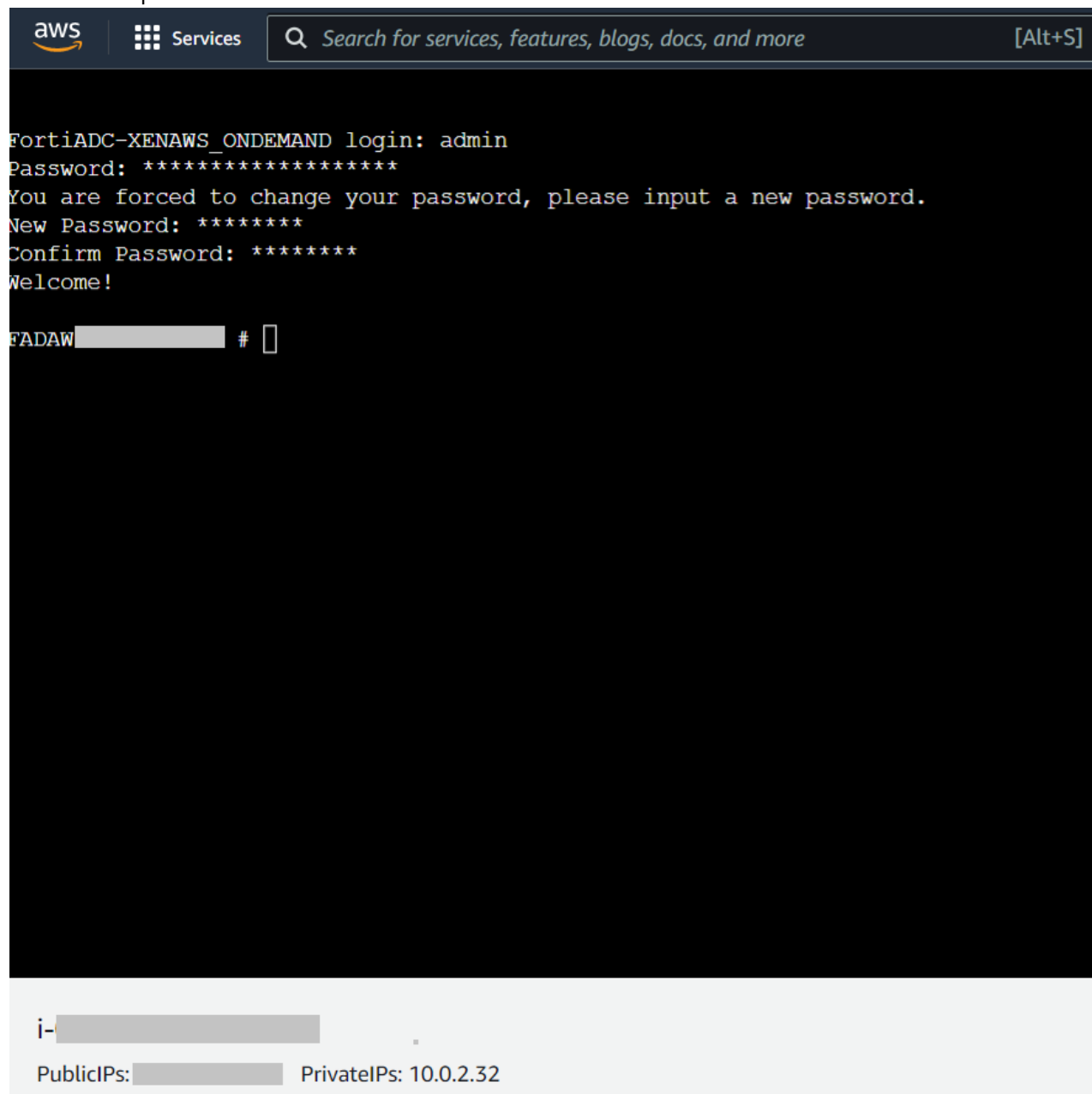
<p>Instance ID</p> <p> i-</p> <p>IPv6 address</p> <p>—</p>	<p>Public IPv4 address</p> <p> open address</p> <p>Instance state</p> <p> Running</p>	<p>Private IPv4 addresses</p> <p> 10.0.2.32</p> <p>Public IPv4 DNS</p> <p> ec2-..compute.amazonaws.com open address</p>
--	--	---

In your web browser, open an HTTPS session using the Public IP address, FQDN, or Elastic IP. Ensure to specify the HTTPS admin port (`https://<Public IP address or FQDN or Elastic IP>: 8443`).

You will see a certificate error message from your browser, which is normal because the default FortiADC certificate is self-signed and not recognized by browsers. Proceed past this error. At a later time, you can upload a publicly signed certificate to avoid this error.

4. Login to the FortiADC-VM with the default user name **admin**. The password is the instance ID by default and you will be required to change the password after you log into the FortiADC-VM.

See the example below for the serial console:



5. From the Web UI, navigate to **System > Cloud Auto Scaling**. You will see the auto-scaling configuration is automatically configured. On the primary FortiADC-VM, you can see the status of all secondary FortiADC-VMs, including hostname, serial number, AWS ec2 instance-id and the status.
If the status of the secondary FortiADC is **init**, it means the secondary FortiADC is connected and synchronized to the primary.

The screenshot shows the FortiADC Cloud Auto Scaling configuration page. The left sidebar has 'System' expanded and 'Cloud Auto Scaling' selected. The main panel shows configuration fields: Status (online), Update Interval (10), Role (Primary/Secondary), Sync Interface (port1), Sync Port (10443), and Callback URL (https://). Below these are 'Save' and 'Refresh' buttons. The 'Auto Scaling Group' section shows a table with one entry:

Host Name	Status	Serial Number	Instance ID	IP Address
FADAWS-7E	init	FADAWS-7E	i-	10.0.0.116

Showing 1 to 1 of 1 entries

If the status changes to **online**, it means the synchronization is done and the secondary FortiADC is ready to serve. If you want to connect to the secondary FortiADC to check configuration or log, please wait until its status becomes online.

This screenshot is similar to the previous one, but the status of the instance has changed to 'online'. The 'Status' field in the configuration panel is now 'online'. The table in the 'Auto Scaling Group' section also shows the status as 'online' (highlighted with a red box in the original image):

Host Name	Status	Serial Number	Instance ID	IP Address
FADAWS-7E	online	FADAWS-7E	i-	10.0.0.116

Showing 1 to 1 of 1 entries

Configuring the FortiADC-VM for Autoscaling

The autoscaling settings on FortiADC are automatically configured. You can view or change the configurations through **System > Cloud Auto Scaling** on the GUI or run `config system auto-scale` in CLI.

After AWS autoscaling resources are deployed, the function APP elects a server instance, the primary node. All clients (secondary nodes) will continuously communicate with the elected primary server. The primary node will later synchronize its configurations to all the clients.

When a new instance joins the cluster, it automatically inherits configurations from the primary node.

You only need to configure the settings on the primary node. The configuration will be automatically synchronized to all the secondary nodes.

Note: The configuration synchronization can be only triggered by Primary node.

The following provides steps on how to direct web traffic to FortiADC for threat detection. Please note that we would only be covering basic options, for more information on other options such as the web protection profile, see the FortiADC Administration Guide.

Basic steps:

1. [Create and configure a real server and real server pool on page 58.](#)
2. [Create and configure a virtual server on page 59](#)
3. [Test the connection between the FortiADC-VM and AWS on page 60.](#)

Create and configure a real server and real server pool

1. In the Primary FortiADC-VM, go to **Server Load Balance > Real Server Pool**.
2. Navigate to the **Real Server** tab and click **Create New** to create a new real server.

The screenshot displays the FortiADC web interface for configuring a Real Server. The left-hand navigation pane shows the 'Server Load Balance' menu item expanded, with 'Real Server Pool' selected. The main content area is titled 'Real Server' and contains the following configuration fields:

- Name:** A text input field containing 'real_server'.
- Server Type:** A set of tabs with 'Static' selected, and 'Dynamic Manual' and 'Dynamic Auto' as options.
- Status:** A set of tabs with 'Enable' selected, and 'Disable' and 'Maintain' as options.
- Type:** A set of tabs with 'IP' selected, and 'FQDN' as an option.
- Address:** A text input field that is currently empty.
- Address6:** A text input field containing '::'.

At the bottom right of the configuration panel, there are two buttons: a green 'Save' button and a white 'Cancel' button.

3. Navigate to the **Real Server Pool** tab and click **Create New** to create a new real server pool.

Real Server Pool

Name: server_pool

Address Type: IPv4 IPv6

Type: Static Dynamic

Health Check: ☒

Health Check Relationship: AND OR

Selected Items: LB_HLTHCK_HTTP

Available Items: Create New, LB_HLTHCK_ICMP, LB_HLTHCK_HTTPS, LB_HLTHCK_TCP_ECHO

Health Check List: Double-click to deselect. Drag to reorder.

Double-click to select.

Direct Route Mode: ☐

Real Server SSL Profile: NONE

Member

Delete + Create New + Add Filter

ID	Name	Address	Health Check	Port	
1	real_server		inherited	80	

Showing 1 to 1 of 1 entries 0 rows selected Show 25 entries

Save Cancel

Create and configure a virtual server

1. Go to **Server Load Balance > Virtual Server**.
2. In the **Virtual Server** tab, click **Create New** to create a new virtual server.
3. Configure the following settings:

Setting	Guideline
Profile	Select the LB_PROF_HTTPS profile.
Port	Enter the port number specified in the Web service traffic port CFT parameter.
Real Server Pool	Select the real server pool created previously.

Test the connection between the FortiADC-VM and AWS

1. Log in to AWS and select **Load Balancers** in EC2 service.
2. Locate the load balancer you have created. Take note of its DNS name.

Networks

Interfaces

Load Balancing

Load Balancers

Target Groups

Auto Scaling

Launch Configuration

ns

Auto Scaling Groups

Name

State

VPC ID

Availability Zones

Type

fadcASG-nlbfdc-cc836360	fadcASG-nlbfdc-cc836360-...	Active	vpc-	b, a	network
-------------------------	-----------------------------	--------	------	------	---------

Load balancer: fadcASG-nlbfdc-cc836360

Description

Listeners

Monitoring

Integrated services

Tags

Basic Configuration

Name

ARN

DNS name

State

Type

Scheme

IP address type

VPC

Availability Zones

fadcASG-nlbfdc-cc836360

fadcASG-nlbfdc-cc836360-...amazonaws.com
(A Record)

Active

network

internet-facing

ipv4

Edit IP address type

subnet-...-...b
IPv4 address: Assigned by AWS

subnet-...-...a

3. Enter the DNS name in your web browser to access your application.
The URL is constructed in the format **https://<dns name>:<port>**. For example, **https://xxxxx.amazonaws.com:443**.
You should be directed to your application homepage.

Upgrading the deployment to apply firmware updates to the FortiADC instances

When an auto scale-out event triggers a new FortiADC instance to deploy and join the ASG, the image version in the Launch Template must be aligned with the image version of the current FortiADC instance in the ASG. If the image versions between the Launch Template and the current FortiADC instance in the ASG is incompatible, the new FortiADC would not synchronize with the primary node.

The following provides steps to apply firmware updates to the FortiADC instances that the AWS Autoscaling deployment deployed.



Back up all FortiADC configurations prior to upgrading the FortiADC instances.

To upgrade the deployment:

1. Obtain the AMI ID for the desired FortiADC image version:
 - From the AWS marketplace — If the desired FortiADC image is available in the AWS marketplace, you can obtain the FortiADC AMI ID from the marketplace listing.
 - By importing the Amazon machine image — If the desired FortiADC is **not** available in the AWS marketplace, you can obtain the AMI ID by manually importing the Amazon machine image. For details, see [Importing the Amazon machine image on page 78](#).
2. Edit the launch template in the ASG to use the desired image version:
 - a. Go to **EC2 > Auto Scaling > Auto Scaling Groups**.
 - b. Select the desired scaling group. Search using the **Resource name prefix**, the default is **fadcASG**.
 - c. In **LAUNCH TEMPLATE**, select **Edit**.

- d. From the **Version** drop-down list, select the new version. In the example below, the Launch template is set to use the **Latest** version.

Launch template

Edit

Launch template fadcASG-LaunchTemplatefadcAutoscale-cc836360 lt- <div></div> <div> <div>Version</div> <div>Latest</div> </div>	AMI ID ami- <div></div>	Instance type c5.2xlarge
Description 720340	Security groups -	Security group IDs -
Request Spot Instances No	Key pair name <div></div>	Storage (volumes) /dev/sdb
	Create time Tue Aug 16 2022 07:39:10 GMT+0800 (Taipei Standard Time)	Created by <div></div>

- e. Click **Update**.

3. Create a new launch template version that references the new FortiADC version's AMI ID, so that autoscaling uses the new template version for new instances:

- a. Navigate to the launch template.
b. From the **Actions** menu, select **Modify Template (Create new version)**.

EC2 > Launch templates > fadcASG-LaunchTemplatefadcAutoscale-cc836360

Actions

Launch instance from template

Modify template (Create new version)

Delete template version

Set default version

Manage tags

Create Spot Fleet

Create Auto Scaling group

Delete template

Launch template name

fadcASG-LaunchTemplatefadcAutoscale-cc836360

Default version

1

Owner

c. Under **Application and OS Images**, paste the AMI ID that you obtained in step 1 in the searchbar or search under **My AMIs**.

FortiADC 7.2.0 AWS Deployment Guide
Fortinet Inc.

62

In this example, the AMI name is 720600.

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

AMI from catalog

Recents

My AMIs

Quick Start

☐ Don't include in

☒ Owned by me

☐ Shared with me

Q

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

720600

ami-

2022-09-26T08:00:52.000Z

Root device type: ebs

Virtualization: hvm

ENA enabled: true

▼

Description

720600

FortiADC 7.2.0 AWS Deployment Guide
Fortinet Inc.

63

d. Add the data storage and create the template version.

▼ **Storage (volumes)** [Info](#)

EBS Volumes [Hide details](#)

▶ Volume 1 (AMI Root) (2 GiB, EBS, General purpose SSD (gp2))
AMI Volumes are not included in the template unless modified

▼ Volume 2 (Custom) [Remove](#)

Storage type [Info](#)
EBS

Device name - required [Info](#)
/dev/sdb

Volume type [Info](#)
gp2

Size (GiB) [Info](#)
30

Snapshot [Info](#)
Don't include in ... ▼

IOPS [Info](#)
100 / 3000

Delete on termination [Info](#)
Yes ▼

Encrypted [Info](#)
Don't include in launch tem... ▼

KMS key [Info](#)
Don't include i... ▼

KMS keys are only applicable when encryption is set on this volume.

Software Image (AMI)
720600
ami-
Virtual server type (instance type)
c5.2xlarge
Firewall (security group)
Storage (volumes)
2 volume(s) - 32 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro) in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage.

Cancel [Create template version](#)

You will see the newly created launch template version.

Launch template version details [Actions](#) [Delete template version](#)

Version
2

Description
720600

Date created
2022-09-22T01:22:57.000Z

Created by

[Instance details](#) | [Storage](#) | [Resource tags](#) | [Network interfaces](#) | [Advanced details](#)

AMI ID
ami-

Instance type
c5.2xlarge

Availability Zone
-

Key pair name

Security groups
-

Security group IDs
sg-

4. Confirm the latest created launch template version has been associated in the ASG.

Launch template

Edit

Launch template fadcASG-LaunchTemplatefadcAutoscale-cc836360 lt- <div></div>	AMI ID ami- <div></div>	Instance type c5.2xlarge
<div> <div>Version</div> <div>Latest</div> <div>Description</div> <div>720600</div> </div>	Security groups -	Security group IDs -
Request Spot Instances No	Key pair name <div></div>	Storage (volumes) /dev/sdb
Create time Wed Oct 05 2022 11:17:03 GMT+0800 (Taipei Standard Time)	Created by <div></div>	

5. Manually apply the update to existing instances. Only the primary FortiADC need to be updated; the firmware updating will be triggered on the secondary FortiADC instance by the primary FortiADC. For details, see the [FortiADC Handbook on updating the firmware](#).

Configuring the Network Load Balancer

By default, a TCP listener is added to the external load balancer to allow the HTTPS traffic to be routed to the HTTPS target autoscaling group. You can add other listeners as needed, such as a listener for HTTP traffic.

To configure the network load balancer:

1. Locate the load balancer using the ResourceGroup Tag Key. For detailed steps, see [Locating deployed resources on page 43](#).

2. In the **Load balancer**, click the **Listeners** tab and click **Add Listener**.

Load balancer: fadcASG-nlb-fadc-cc836360

Listeners listen for connection requests using their protocol and port. You can add, remove, or update listeners and listener rules.

To view and edit listener attributes, select the listener and choose Edit.

Add listener Edit Delete

<input type="checkbox"/>	Listener ID	Security policy	SSL Certificate	ALPN policy	Default action
<input type="checkbox"/>	TCP : 443	N/A	N/A	N/A	forwarding to fadcASG-tg-fadc-cc836360

3. In the new listener, specify the port value for HTTP or HTTPS services respectively and click **Create target group** to create a target group for this listener.

In the example below, the new listener is configured for TCP using port 80 for HTTP services.

EC2 > Load balancers > fadcASG-nlbfdac-cc836360 : Add listener

Add listener

Listener details [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Protocol

TCP ▼

Port

80

1-65535

Default action [Info](#)

Forward to

Select a target group ▼



[Create target group](#)

Cancel

Add

4. In the new target group, configure the following **Basic configurations** and **Advanced health check settings**:

- Basic configurations — select **target type** as **Instances** and **Protocol** as **TCP**.
- Advanced health check settings — override the port with the FortiADC admin port (8443).

Select all the instances in the autoscaling group into the pending targets then create the target.

5. After the target is created, navigate back to the **Add listener** tab to associate the target with the listener.

EC2 > Load balancers > fadcASG-nlb fadc-cc836360 : Add listener

Add listener

Listener details [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Protocol : Port
 TCP : 80
 1-65535

Default action [Info](#)

Forward to fadcASG-port80-cc836360
 TCP ▼
 Target type: Instance, IPv4



[Create target group](#)

6. Add security group inbound rules in the security group to allow HTTP or HTTPS service traffic to be sent to FortiADC-VMs in the autoscaling group.

With these configurations, the HTTP and HTTPS traffic to the load balancer will be distributed among the FortiADC-VMs in the autoscaling group.

Load balancer: fadcASG-nlb fadc-cc836360

Description **Listeners** Monitoring Integrated services Tags

Listeners listen for connection requests using their protocol and port. You can add, remove, or update listeners and listener rules.

To view and edit listener attributes, select the listener and choose Edit.

Add listener

Edit

Delete

<input type="checkbox"/>	Listener ID	Security policy	SSL Certificate	ALPN policy	Default action
<input type="checkbox"/>	TCP : 80 [Dropdown]	N/A	N/A	N/A	forwarding to fadcASG-port80-cc836360
<input type="checkbox"/>	TCP : 443 [Dropdown]	N/A	N/A	N/A	forwarding to fadcASG-tgfadc-cc836360

Attaching the FortiADC-VM instance to an existing Autoscaling group

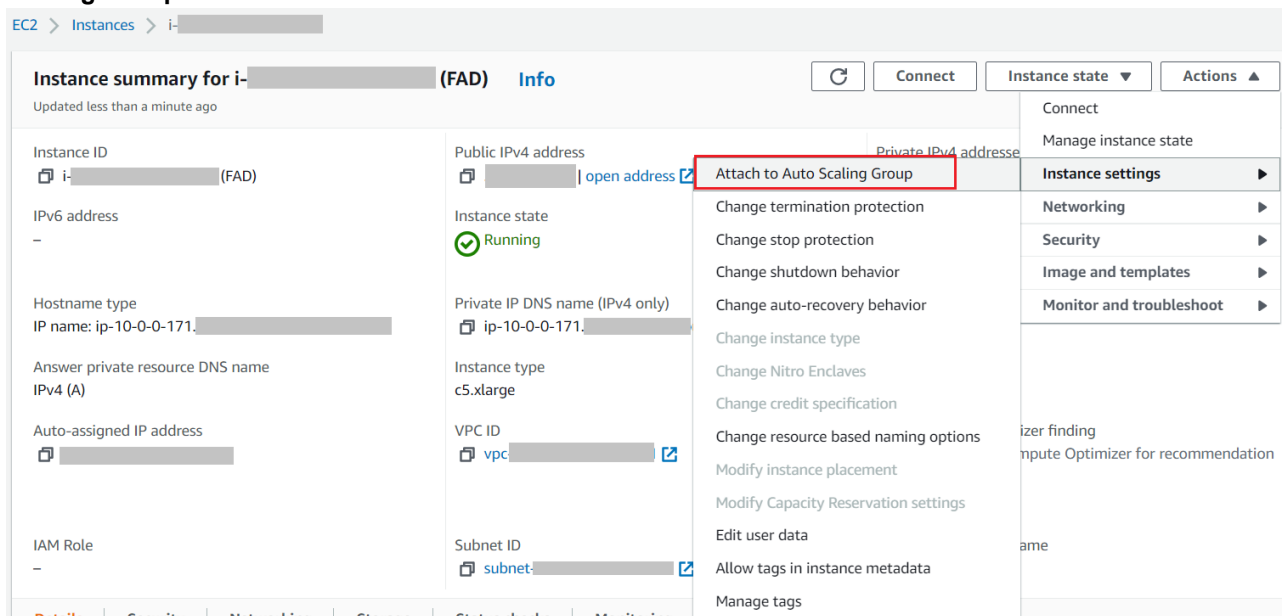
You can attach a FortiADC-VM (which can be licensed with PAYG or BYOL) to an existing autoscaling group.

Before you begin:

- Ensure the FortiADC-VM is in standalone mode.
- Ensure the image version of the FortiADC-VM is the same as the FortiADC-VMs in the ASG. If the image version is different, you will see the log from AWS CloudWatch or from FortiADC debug log. For details, see [debug].
- Check the rules of the network security group attached to the FortiADC-VM network interface card to ensure the inbound/outbound rules include the rules of the network security group of the FortiADC-VMs in the ASG.

To attach the FortiADC-VM instance to an existing ASG:

1. In the AWS console, go to **EC2 > Instances** and select the FortiADC-VM you want to add to the ASG.
2. In the FortiADC-VM instance, click the **Actions** drop-down and select **Instance settings > Attach to Auto Scaling Group**.



3. In the **Attach to Auto Scaling group** page, select the ASG to attach the FortiADC-VM to.

Attach to Auto Scaling group [Info](#)

Enable automatic scaling for an instance by attaching it to an Auto Scaling group.

Instance ID

i- (FAD)

Public IPv4 DNS

ec2- .compute.amazonaws.com

Auto Scaling Group

Choose an existing Auto Scaling group or enter a name to create a new Auto Scaling group.

fadcASG-FortiadcAutoScalingGroup-3f028160

When you attach an instance to a new Auto Scaling group, we create a new launch configuration and associate it with the Auto Scaling group.

4. Check the Instance page to see the FortiADC-VM instance is attached to the ASG.

EC2 > Instances > i- (FAD)

Instance summary for i- (FAD) [Info](#)

Updated less than a minute ago

<p>Instance ID</p> <p> i- (FAD)</p> <p>IPv6 address</p> <p>—</p> <p>Hostname type</p> <p>IP name: ip-10-0-0-171</p> <p>Answer private resource DNS name</p> <p>IPv4 (A)</p> <p>Auto-assigned IP address</p> <p></p> <p>IAM Role</p> <p>—</p>	<p>Public IPv4 address</p> <p> open address</p> <p>Instance state</p> <p> Running</p> <p>Private IP DNS name (IPv4 only)</p> <p> ip-10-0-0-171</p> <p>Instance type</p> <p>c5.xlarge</p> <p>VPC ID</p> <p> vpc- open address</p> <p>Subnet ID</p> <p> subnet- open address</p>	<p>Private IPv4 addresses</p> <p> 10.0.0.171</p> <p>Public IPv4 DNS</p> <p> ec2- .amazonaws.com</p> <p>open address</p> <p>Elastic IP addresses</p> <p>—</p> <p>AWS Compute Optimizer finding</p> <p> Opt-in to AWS Compute Optimizer for recommendation s.</p> <p>Learn more</p> <p>Auto Scaling Group name</p> <p>fadcASG-FortiadcAutoScalingGroup-3f028160</p>
--	---	--

5. After the FortiADC-VM is added into the ASG, you can see the desired capacity has increased by 1, and the minimum capacity remains the same value. In this case, the scale-in event may be triggered due to the CPU load in

average be lower than the set threshold. You can change the minimum capacity or make the new added instance under scale-in protection to prevent from any instances in ASG to be terminated.

Group details

Desired capacity	Auto Scaling group name
3	fadcASG- FortiadcAutoScalingGroup- 3f028160
Minimum capacity	Date created
2	Fri Oct 07 2022 17:21:16 GMT+0800 (Taipei Standard Time)
Maximum capacity	Amazon Resource Name (ARN)
4	

6. Configure the autoscale configuration on FortiADC-VM. If the ASG was previously empty, then configure the FortiADC-VM as the primary node, otherwise, configure it as the secondary.
If the FortiADC-VM is the primary node, you can get a Callback URL from the launch template.
 - a. Configure the FortiADC-VM to autoscaling primary role:
 - i. In the AWS console, go to **EC2 > Launch Templates** and locate the launch template by ResourceGroup tag.
 - ii. Click the **Details > Advanced details** tab and check the **User data**.
Take note of `config-url` and replace the API path `get-config` with `complete`.
In the example below, the Callback URL will be `https://xxxx.execute-api.us-west-`

2.amazonaws.com/prod/complete.

EC2 > **Launch templates** > fadcASG-LaunchTemplatefadcAutoscale-3f028160

User data

```
{
  "config-url": "https://[redacted].execute-api.us-west-2.amazonaws.com/prod/get-config",
  "productcode": ""
}
```

Base64-encoded user data has been decoded for readability.

- iii. Fill in the autoscaling configuration, set the role to primary and enable the status. Then, click **Save**.
- b. Configure the FortiADC-VM as the autoscaling secondary role.
 - i. Take note of the Callback URL from the Primary Cloud Auto Scaling configuration and the port1 interface IP of the primary node.
 - ii. Fill in the cloud autoscaling configuration and enable the status, then click **Save**.

FortiADC FortiADC-XENAWS HA: Standalone

Dashboard > Security Fabric > FortiView > **System** > Settings > **Cloud Auto Scaling**

High Availability

Traffic Group

Administrator

SNMP

Replacement Messages

AWS Scripting

Status ☒

Update Interval 10
Default: 10 Range: 10-120(second)

Role Primary **Secondary**

Primary IP 10.0.2.181
Example: 192.0.2.5

Sync Interface port1

Sync Port 10443
Default: 10443 Range: 1-65535

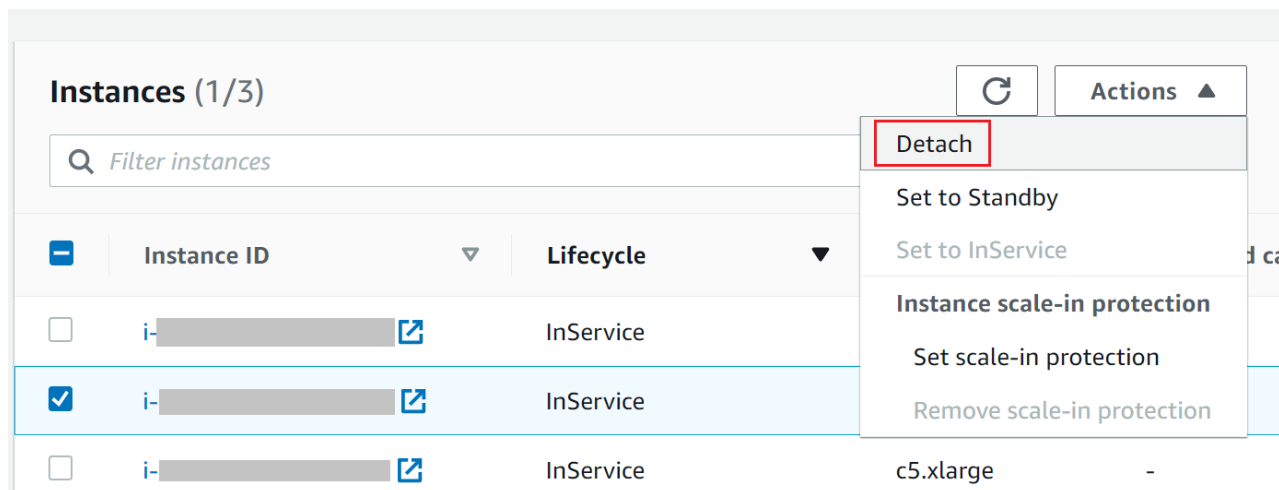
Callback URL https://[redacted].execute-api.us-west-2.amazonaws.com/prod/get-config

Save Refresh

- iii. Checking from the primary node, you should see this FortiADC-VM is connected. If not, please check debug.

7. Optionally, you can detach the FortiADC-VM if you do not need it.

On the AWS console, go to **EC2 > Auto Scaling Group** and locate the ASG. There, you can select the FortiADC-VM to be detached by clicking **Actions > Detach**.



After FortiADC-VM is successfully detached, the status of the autoscale configuration on FortiADC-VM is automatically disabled.

Debug

Debug information can either be accessed through the AWS CloudWatch or through the FortiADC CLI.

Logs are available from AWS CloudWatch where you can check if FortiADC-VMs in the ASG is sending the heartbeat callback on time, or whether FortiADC-VM maintains to be healthy. For steps on how to look up the logs and Dynamo DB records for the deployed resource, see [Locating deployed resources on page 43](#).

On FortiADC-VM, you can use CLI commands to look up the status of the cloud autoscaling daemon:

- Use the `debug cloud-autoscale autoscaled` command to see the heartbeat callback result and failover information if the primary election is triggered.

```
FADAWS # diagnose debug cloud-autoscale autoscaled
10.06 20:22:52 autoscale hb timer timeout
10.06 20:22:52 sync callback
10.06 20:22:53 sync action update start
10.06 20:22:53 sync action response primary ip: 10.0.2.231, config-sync-port: 10443, action: -1
10.06 20:22:53 timer timeout 10
10.06 20:23:03 autoscale hb timer timeout
10.06 20:23:03 sync callback
10.06 20:23:04 sync action update start
10.06 20:23:04 sync action response primary ip: 10.0.2.231, config-sync-port: 10443, action: -1
10.06 20:23:04 timer timeout 10
10.06 20:23:14 autoscale hb timer timeout
10.06 20:23:14 sync callback
10.06 20:23:15 sync action update start
10.06 20:23:15 sync action response primary ip: 10.0.2.231, config-sync-port: 10443, action: -1
10.06 20:23:15 timer timeout 10
10.06 20:23:25 autoscale hb timer timeout
10.06 20:23:25 sync callback
10.06 20:23:27 sync action update start
10.06 20:23:27 sync action response primary ip: 10.0.2.231, config-sync-port: 10443, action: -1
10.06 20:23:27 timer timeout 10
```

- Use the `diagnose debug cloud-autoscale autoscale-tunnel` command to see the synchronization between the primary and secondary FortiADCs. It will also show the crash log if it exists.
Primary FortiADC:

```
FADAWS [REDACTED] # diagnose debug cloud-autoscale autoscale-tunnel
Primary node log:
2022/10/06 20:07:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:08:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:09:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:10:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:11:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:12:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:13:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:14:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:15:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:16:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:17:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:18:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:19:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:20:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:21:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:22:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:23:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:24:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:25:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]
2022/10/06 20:26:51 libtunnel.go:374: Update Secondary node FADAWS [REDACTED]

Primary node crash log:
```

Secondary FortiADC:

```
FADAWS[REDACTED] # diagnose debug cloud-autoscale autoscale-tunnel
Secondary node log:
TRACE: 2022/10/06 20:23:51 client.go:123: Update info to Primary node :
{"hostname":"FADAWS[REDACTED]"}
TRACE: 2022/10/06 20:24:51 client.go:123: Update info to Primary node :
{"hostname":"FADAWS[REDACTED]"}
TRACE: 2022/10/06 20:25:51 client.go:123: Update info to Primary node :
{"hostname":"FADAWS[REDACTED]"}
TRACE: 2022/10/06 20:26:51 client.go:123: Update info to Primary node :
{"hostname":"FADAWS[REDACTED]"}
TRACE: 2022/10/06 20:27:51 client.go:123: Update info to Primary node :
{"hostname":"FADAWS[REDACTED]"}
TRACE: 2022/10/06 20:28:51 client.go:123: Update info to Primary node :
{"hostname":"FADAWS[REDACTED]"}
TRACE: 2022/10/06 20:29:51 client.go:123: Update info to Primary node :
{"hostname":"FADAWS[REDACTED]"}
TRACE: 2022/10/06 20:30:49 client.go:288: Relay seq num 4 len 93
TRACE: 2022/10/06 20:30:49 client.go:175: receive : {"cmd":"config user local \nedit user1 \nset pa
ssword [REDACTED] \nend \nend\nend\nend\nend\nend\nend\n"} 93
TRACE: 2022/10/06 20:30:49 client.go:187: Run cli cmd result :0
TRACE: 2022/10/06 20:30:49 client.go:159: resp seqnum: 4
TRACE: 2022/10/06 20:30:51 client.go:123: Update info to Primary node :
{"hostname":"FADAWS[REDACTED]"}
Secondary node crash log:
```

Script

FortiADC provides the method to execute any AWS API for users – Users can upload Python script to FortiADC (system > AWS Scripting page) with traffic group setting and execute this script on the FortiADC to which its traffic group belongs.

If two FortiADCs are in different traffic groups for HA-VRRP mode, they can execute script individually, and communicate with AWS when doing the HA switch.

Run script:

- Execute manually from GUI, upload scripts, choose traffic-group, click “Run”
- Traffic-group takes effect in new device and will execute scripts after doing HA switch

Command to check which traffic-group this device belongs: `get system traffic-group-status detail`

To execute AWS API, set the following on FortiADC:

```
config system aws
set region us-west-1 (set region name as need)
set accesskey XXXXXXXXXXXX (get from .csv file when create user on AWS)
set secretkey XXXXXXXXXXXX (get from .csv file when create user on AWS)
end
```

Example: This script modifies the default rout in the AWS route table, when the default traffic group works in the new ADC

```
#!/bin/sh
traffic_group=${TRAFFIC_GROUP_NAME}
eni_id="XXXXXXXXXX"
route_table_id="XXXXXXXXXX"
echo ${TRAFFIC_GROUP_NAME}
if [${traffic_group}="default"]
then
aws ec2 replace-route --route-table-id $route_table_id --destination-cidr-block 0.0.0.0/0 --
    network-interface-id $eni_id
else
echo "do noting"
fi
```

Importing the Amazon machine image

Step 1: Precondition

Install the AWS Command Line Interface and its dependencies on most Linux distributions with pip, a package manager for Python. Please refer to <https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html> for more information.

A. Use pip to install the AWS CLI.

```
$ pip install awscli --upgrade --user
```

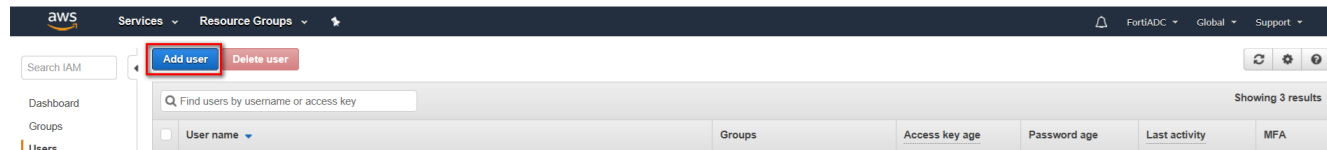
B. Verify that the AWS CLI installed correctly.

```
$ aws --version
```

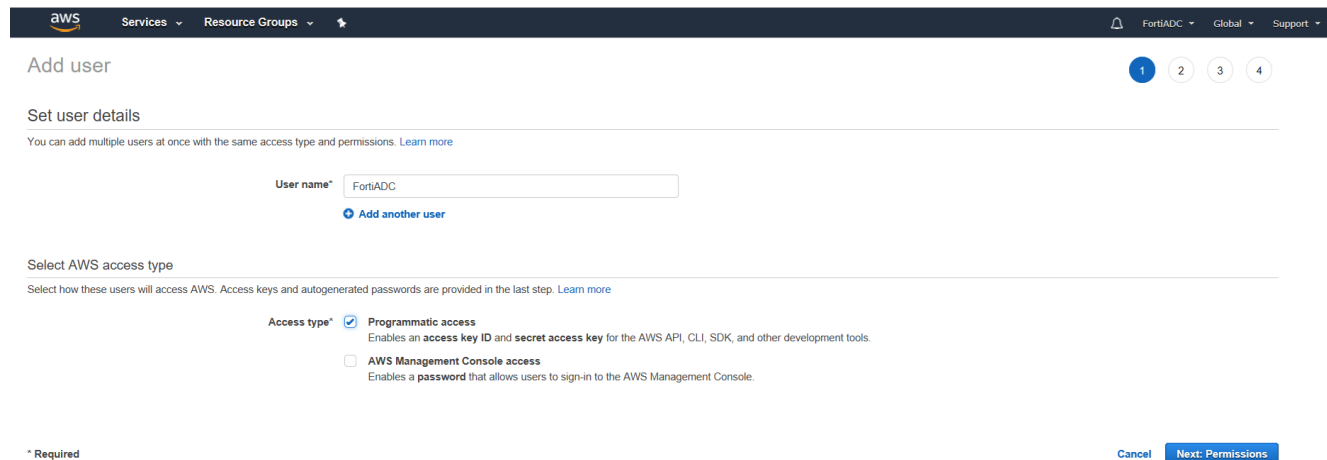
Step 2: Get IAM key

A. Navigate to <https://console.aws.amazon.com/iam>

B. Users -> Add user



C. Check the box Programmatic access



D. Check the box Administrators

Add user

Set permissions for FortiADC

Add user to group

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

Create group Refresh

Search

Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> Administrator	AdministratorAccess

E. After Created, download .csv file to get key

Add user

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://697508164634.signin.aws.amazon.com/console>

Download .csv

User	Access key ID	Secret access key
<input checked="" type="checkbox"/> FortiADC	AKIAI44QH8DHBVS7G	***** Show

Step 3: Configuring the AWS CLI

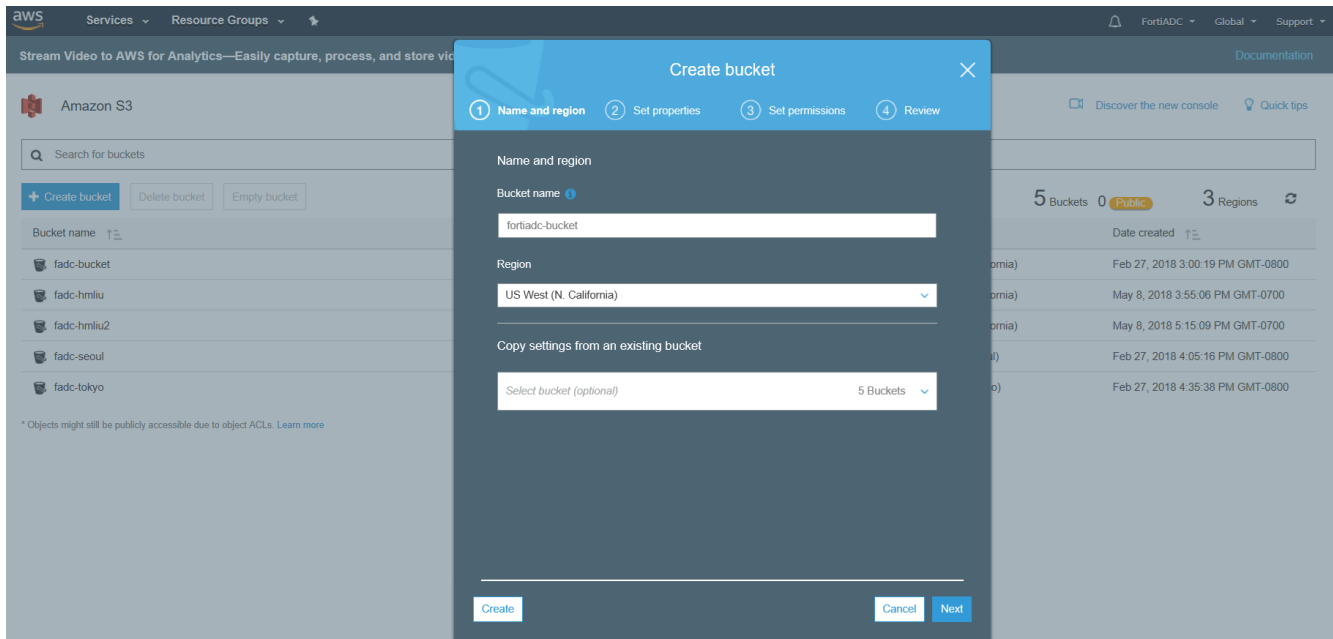
```
$ aws configure
AWS Access Key ID []:xxxxxxxxxxxx (get from Step 2.)
AWS Secret Access Key []:xxxxxxxxxxxx (get from Step 2.)
Default region name []:us-west-1 (Please refer below table for your region name)
Default output format []: json
```

Region Name	Region
US East (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka-Local)	ap-northeast-3
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
China (Beijing)	cn-north-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2
EU (Paris)	eu-west-3
South America (São Paulo)	sa-east-1

Step 4: Create S3 bucket

A. Navigate to <https://s3.console.aws.amazon.com/s3>

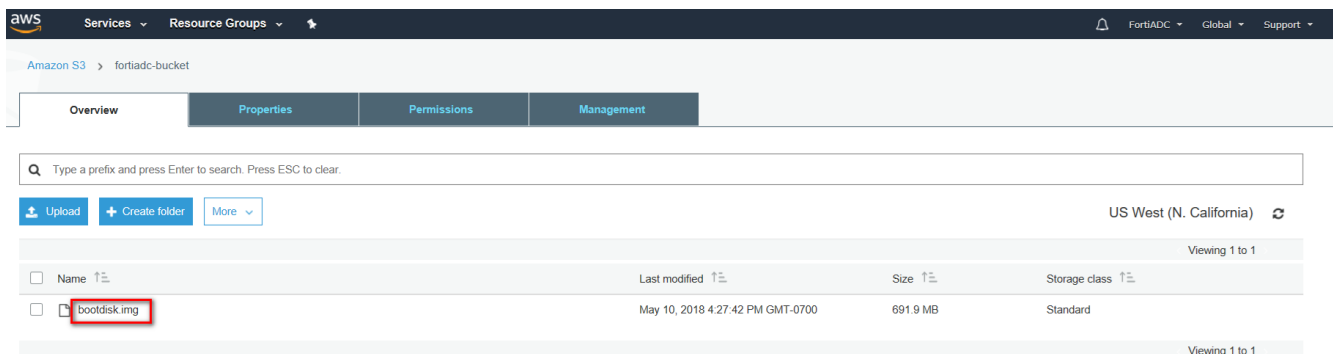
B. Create bucket



Step 5: upload image and create snapshot

A. Upload image

- unzip image.out.xenaws.zip to get bootdisk.img
- `aws s3 cp bootdisk.img s3://<your bucket name>`
- Check the upload success



B. To create the service role

- 1) Create trust-policy.json with the following policy:


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "vmie.amazonaws.com" },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:Externalid": "vmimport"
        }
      }
    }
  ]
}
```

2) Create a role named vmimport

If the role with name vmimport already exists, skip this step.

```
$ aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json
```

3) Create role-policy.json with the following policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::<your S3 bucket name>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::<your S3 bucket name>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

4) Attach the policy to the role created above

```
$ aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document
file://role-policy.json
```

C. Create snapshot

1) Create container.json with the following content:

```
{
  "Description": "FADC 5.1.0 image",
  "Format": "raw",
  "UserBucket": {
    "S3Bucket": "fortiadc-bucket", // S3Bucket:<your S3 bucket name>
    "S3Key": "bootdisk.img" // S3Key:<Your image name in S3 >
  }
}
```

2) import snapshot

```
$ aws ec2 import-snapshot --description "<description>" --disk-container
file://container.json
{
  "SnapshotTaskDetail": {
    "Status": "active",
    "Description": "FADC",
    "Format": "RAW",
    "DiskImageSize": 0.0,
    "UserBucket": {
      "S3Bucket": "fortiadc-bucket",
      "S3Key": "bootdisk.img"
    },
    "Progress": "3",
    "StatusMessage": "pending"
  },
  "Description": "FADC",
  "ImportTaskId": "import-snap-fh2q08gi"
}
```

You can check the progress using the following commands:

```
$ aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-fh2q08gi //
ImportTaskId
{
  "ImportSnapshotTasks": [
    {
      "SnapshotTaskDetail": {
        "Status": "active",
        "Description": "FADC",
        "Format": "RAW",
        "DiskImageSize": 725500928.0,
        "UserBucket": {
          "S3Bucket": "fortiadc-bucket",
          "S3Key": "bootdisk.img"
        },
        "Progress": "19",
```

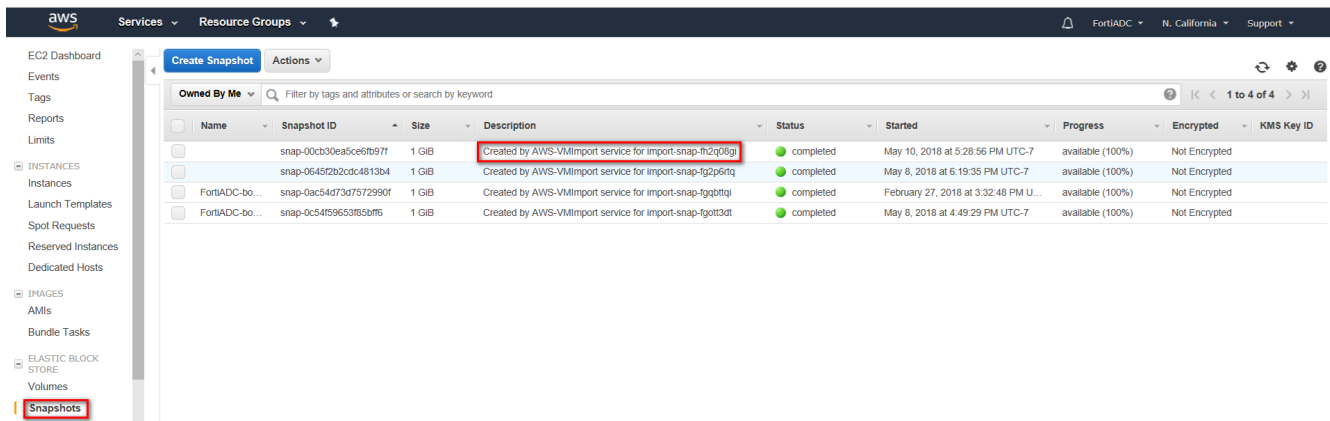
```

    "StatusMessage": "validated"
  },
  "Description": "FADC",
  "ImportTaskId": "import-snap-fh2q08gi"
}
]
}

$ aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-fh2q08gi
{
  "ImportSnapshotTasks": [
    {
      "SnapshotTaskDetail": {
        "Status": "completed",
        "Description": "FADC",
        "Format": "RAW",
        "DiskImageSize": 725500928.0,
        "UserBucket": {
          "S3Bucket": "fortiadc-bucket",
          "S3Key": "bootdisk.img"
        },
        "SnapshotId": "snap-00cb30ea5ce6fb97f"
      },
      "Description": "FADC",
      "ImportTaskId": "import-snap-fh2q08gi"
    }
  ]
}

```

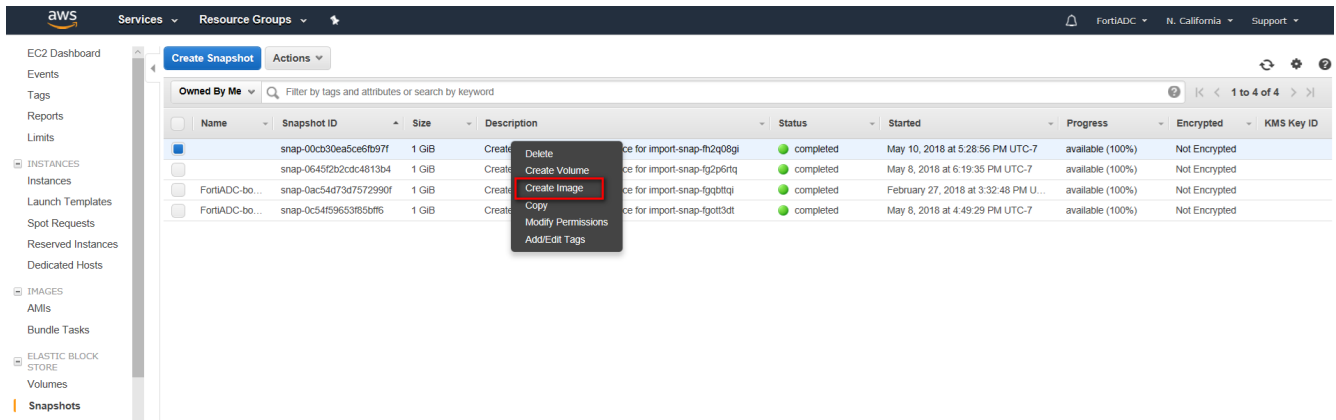
After "Status": "completed", you can find your snapshot in the navigation pane, under Elastic Block Store



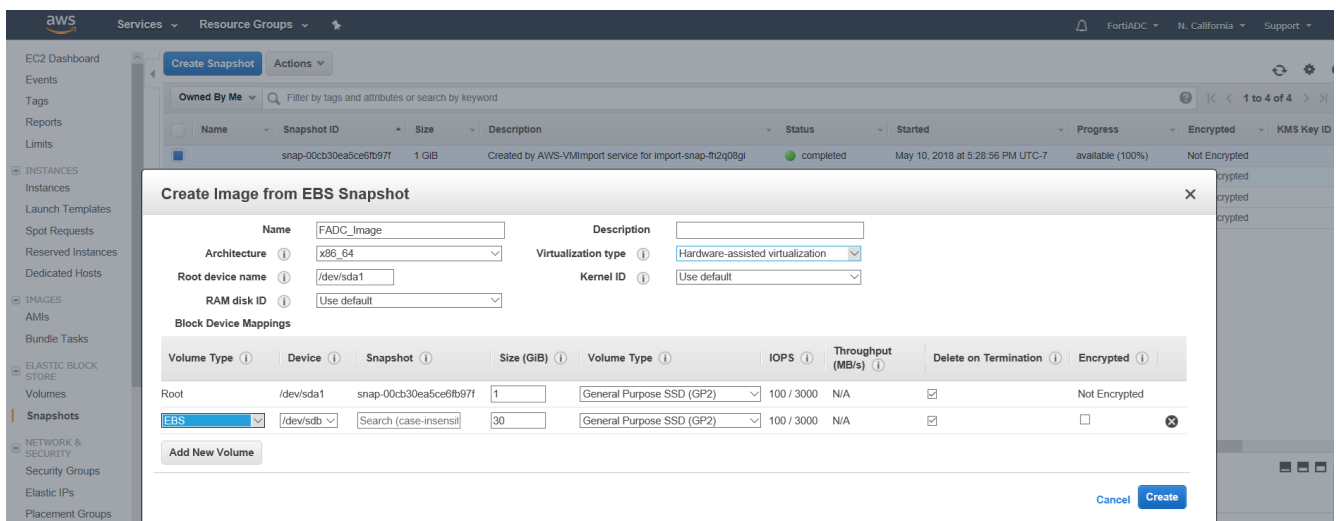
Name	Snapshot ID	Size	Description	Status	Started	Progress	Encrypted	KMS Key ID
	snap-00cb30ea5ce6fb97f	1 GiB	Created by AWS-VMimport service for import-snap-fh2q08gi	completed	May 10, 2018 at 5:28:56 PM UTC-7	available (100%)	Not Encrypted	
	snap-0645f2b2dc4813b4	1 GiB	Created by AWS-VMimport service for import-snap-fg2p6tq	completed	May 8, 2018 at 6:19:35 PM UTC-7	available (100%)	Not Encrypted	
FortiADC-bo...	snap-0ac5407367572990f	1 GiB	Created by AWS-VMimport service for import-snap-fggbttq	completed	February 27, 2018 at 3:32:48 PM U...	available (100%)	Not Encrypted	
FortiADC-bo...	snap-0c54f5965385b0f5	1 GiB	Created by AWS-VMimport service for import-snap-fgott3dt	completed	May 8, 2018 at 4:49:29 PM UTC-7	available (100%)	Not Encrypted	

Step 6: Create Amazon Machine Image (AMI)

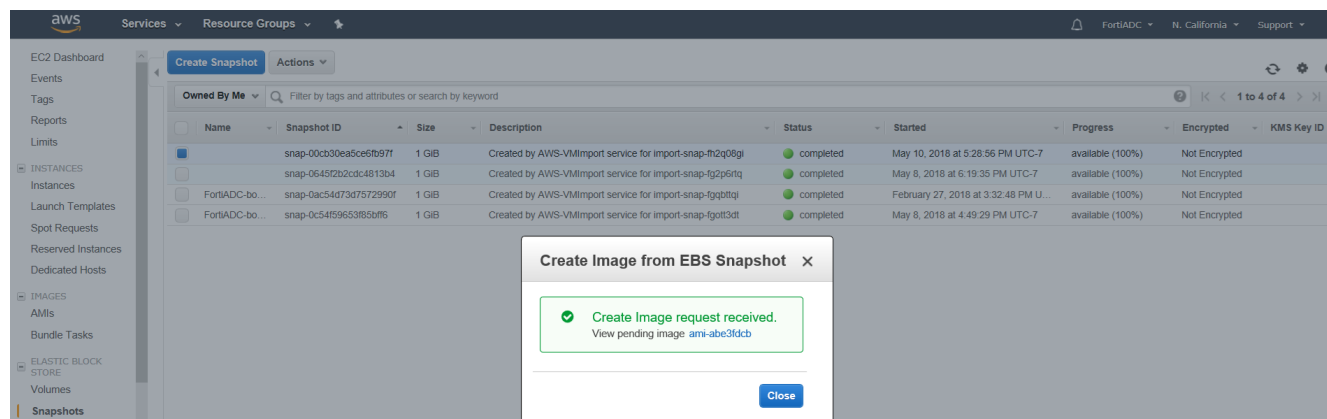
A. Right click on FortiADC-bootdisk and choose Create Image



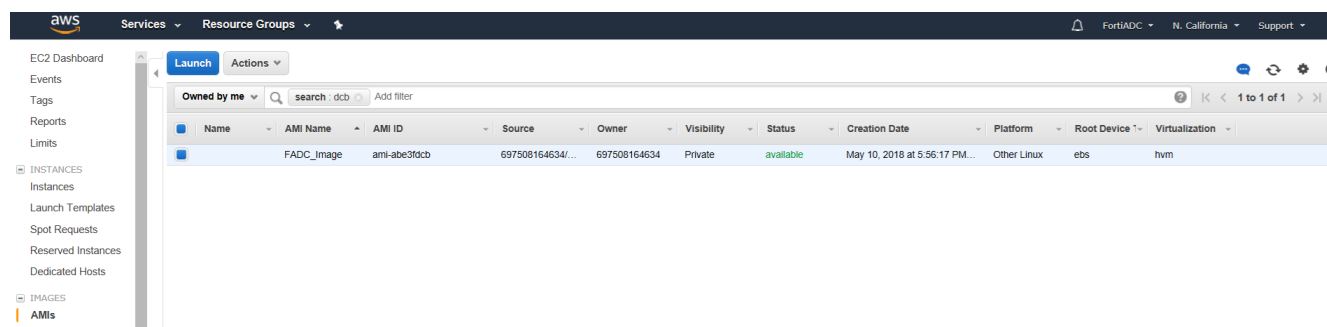
2. Fill name and set Virtualization type to virtual machine (HVM) and Add a New Volume with 30GB



3. Click Create



4. Under My AMIs you can find the one you just created



Important notes

1. In L4_VS DNAT mode or L7_VS mode enabled "client-address", you need to disable "Source/Dest. Check" on AWS_EC2_ADC interface, which connects to RS, and ensure that ADC is the gateway for RS.
2. Currently only supports VRRP group with no more than two ADCs.



FORTINET®



Copyright© 2023 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.