FortiADC - AWS Deployment Guide

Version 7.0.0

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

FORTINET®

January 28, 2022
FortiADC 7.0.0 AWS Deployment Guide
01-540-000000-20200214

TABLE OF CONTENTS

Change Log

Date	Change Description
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.

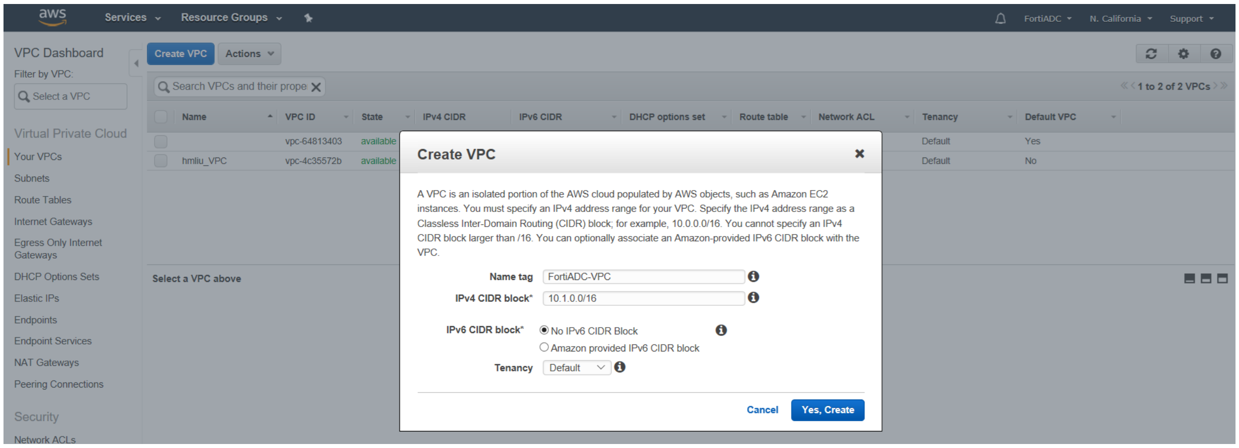
Introduction

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



Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
	vpc-64813403	available						Default	Yes
hmliu_VPC	vpc-4c35572b	available						Default	No

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag: FortiADC-VPC

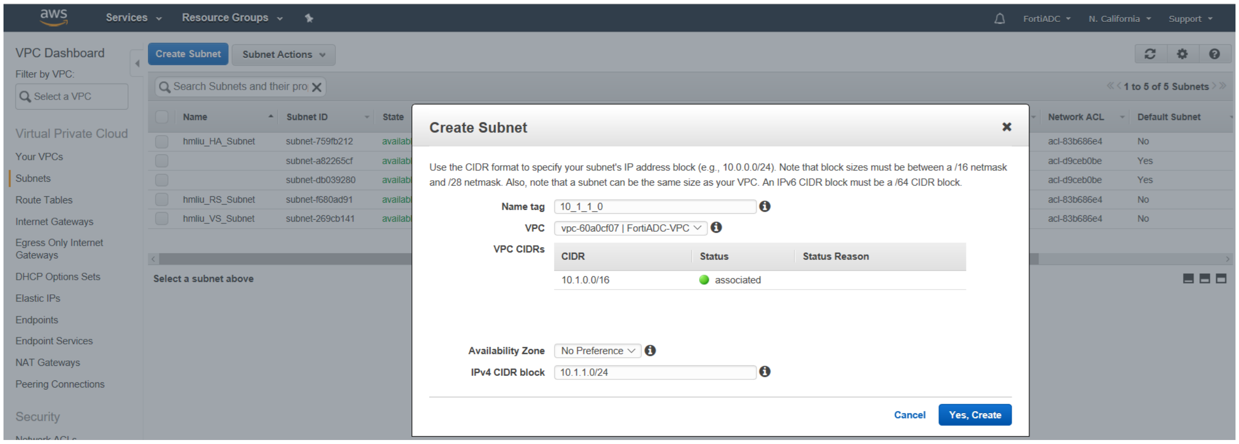
IPv4 CIDR block*: 10.1.0.0/16

IPv6 CIDR block*: ● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block

Tenancy: Default

Cancel | Yes, Create

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



Name	Subnet ID	State	Network ACL	Default Subnet
hmliu_HA_Subnet	subnet-759fb212	availab	acl-83b686e4	No
	subnet-a82265cf	availab	acl-d9ceb0be	Yes
	subnet-db039280	availab	acl-d9ceb0be	Yes
hmliu_RS_Subnet	subnet-f680ad91	availab	acl-83b686e4	No
hmliu_VS_Subnet	subnet-269cb141	availab	acl-83b686e4	No

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: 10_1_1_0

VPC: vpc-60a0cf07 | FortiADC-VPC

VPC CIDRs:

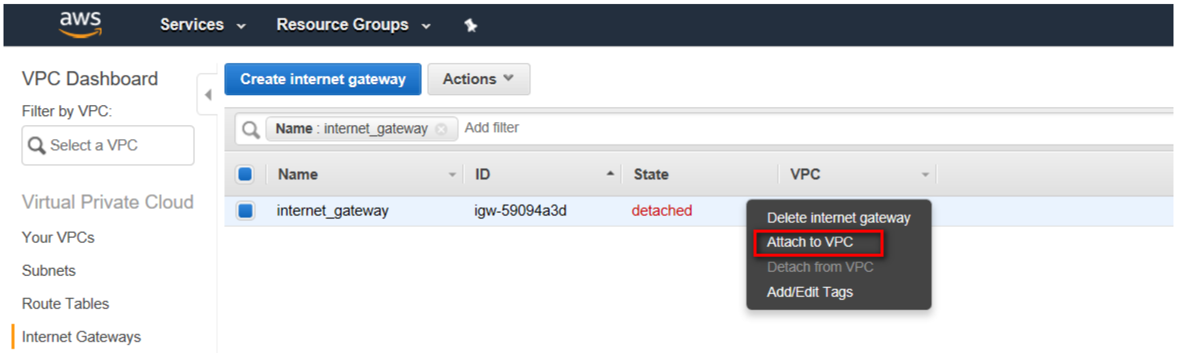
CIDR	Status	Status Reason
10.1.0.0/16	● associated	

Availability Zone: No Preference

IPv4 CIDR block: 10.1.1.0/24

Cancel | Yes, Create

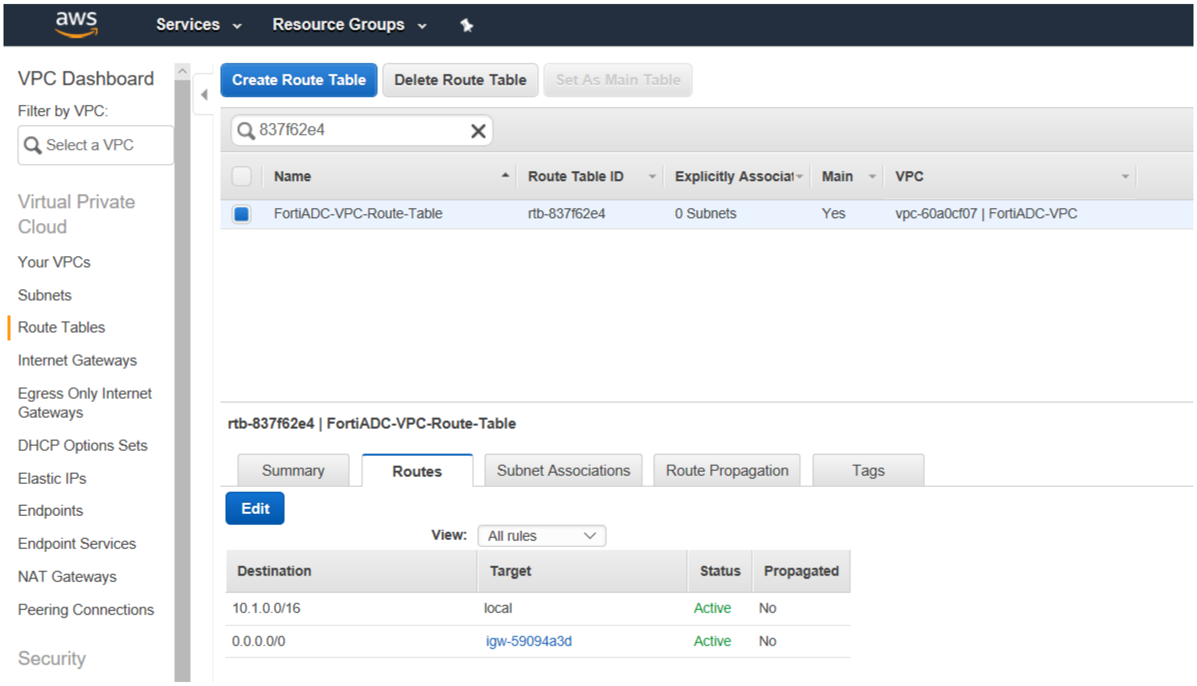
3. Create internet gateway, and attach it to VPC



Name : internet_gateway

Name	ID	State	VPC
internet_gateway	igw-59094a3d	detached	

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



837f62e4

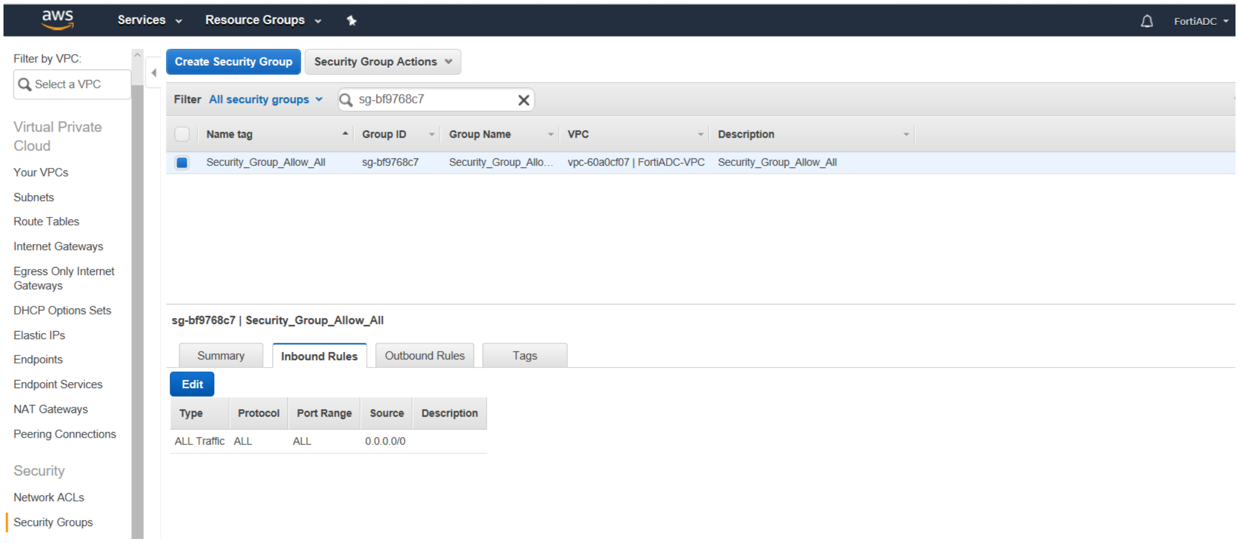
	Name	Route Table ID	Explicitly Associat	Main	VPC
☑	FortiADC-VPC-Route-Table	rtb-837f62e4	0 Subnets	Yes	vpc-60a0cf07 | FortiADC-VPC

rtb-837f62e4 | FortiADC-VPC-Route-Table

View: All rules

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"



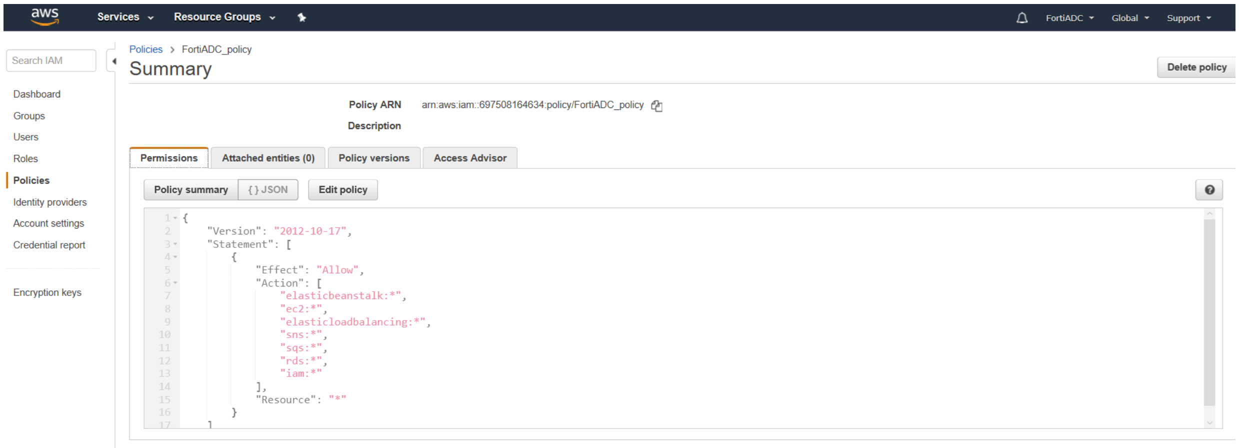
Filter All security groups sg-bf9768c7

	Name tag	Group ID	Group Name	VPC	Description
☑	Security_Group_Allow_All	sg-bf9768c7	Security_Group_Allo...	vpc-60a0cf07 | FortiADC-VPC	Security_Group_Allow_All

sg-bf9768c7 | Security_Group_Allow_All

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

6. Create IAM policy



Policy ARN arn:aws:iam::697508164634:policy/FortiADC_policy

Description

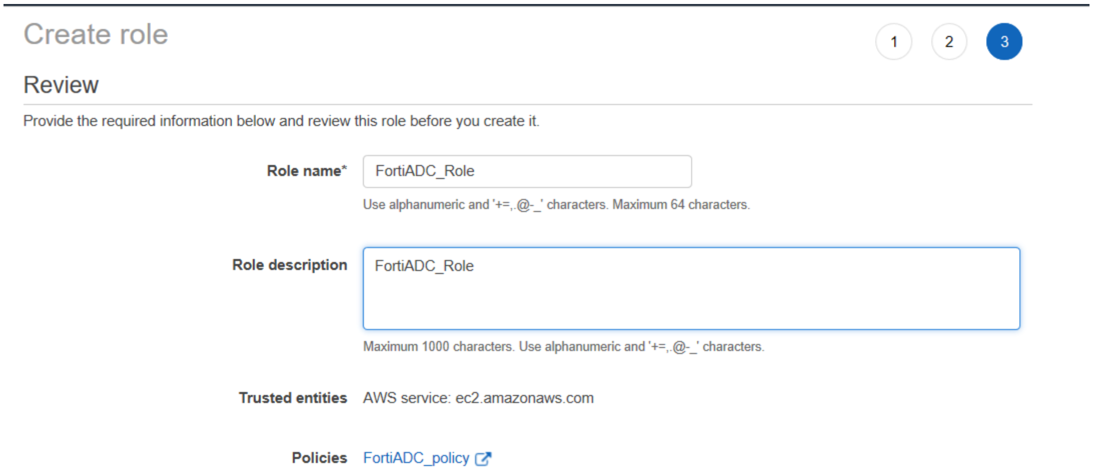
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticbeanstalk:*",
                "ec2:*",
                "elasticloadbalancing:*",
                "sns:*",
                "sqs:*",
                "rds:*",
 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

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

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.

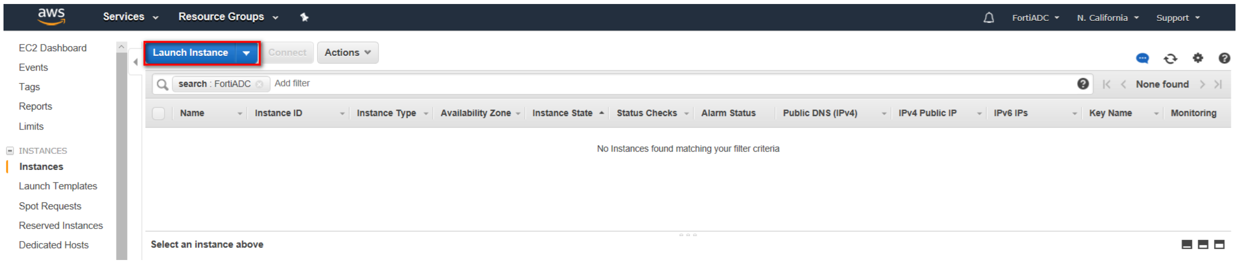
Both methods require an existing Amazon EC2 account and Amazon Virtual Private Cloud (Amazon VPC). You can deploy the FortiADC-VM for AWS using AWS Marketplace or from your own AMIs directly.

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



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring

No Instances found matching your filter criteria

Select an instance above

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.

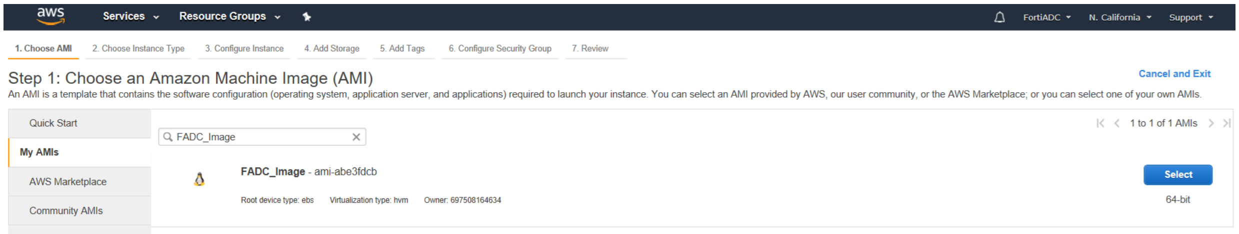
A. Marketplace

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 25 for uploading the image manually.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

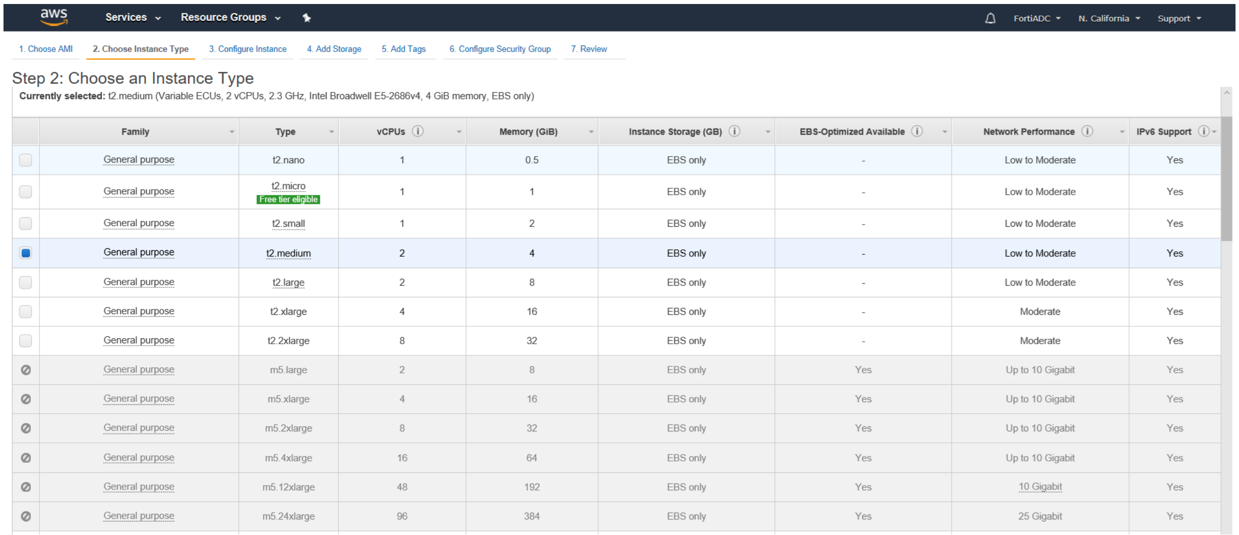
FADC_Image

FADC_Image - ami-abe3fdcb

Root device type: ebs Virtualization type: hvm Owner: 697508164634

64-bit

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



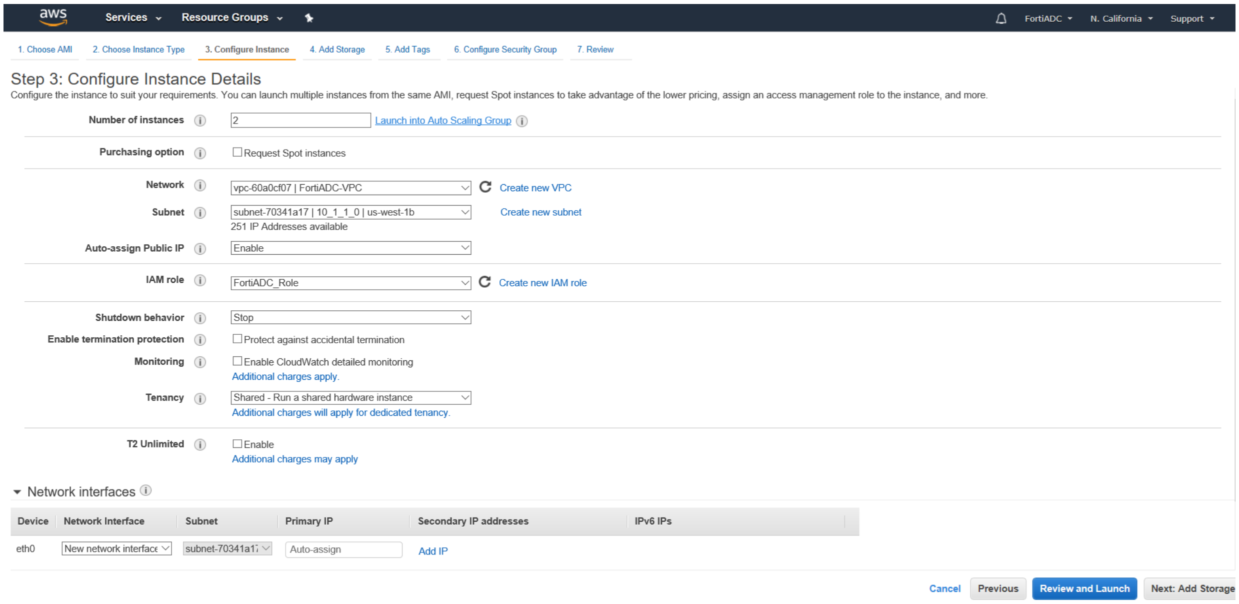
Step 2: Choose an Instance Type

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
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
■	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
⊘	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
⊘	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
⊘	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
⊘	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
⊘	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
⊘	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
Purchasing option	□ Request Spot instances
Network	vpc-60a0cf07 | FortiADC-VPC
Subnet	subnet-70341a17 | 10_1_1_0 | us-west-1b 251 IP Addresses available
Auto-assign Public IP	Enable
IAM role	FortiADC_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

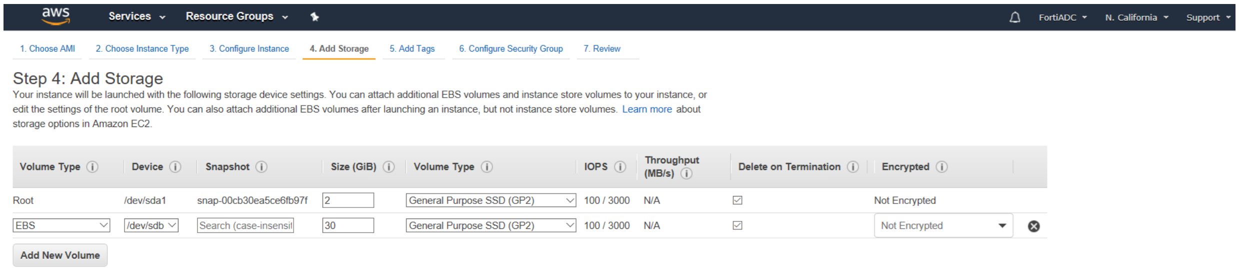
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-70341a17	Auto-assign	Add IP	

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.



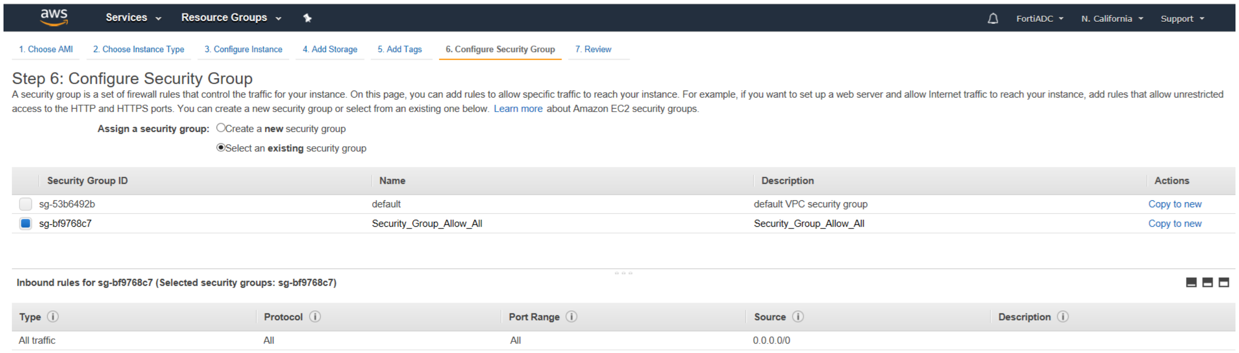
Step 4: Add Storage

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-00cb30ea5ce6fb97f	2	General Purpose SSD (GP2)	100 / 3000	N/A	☑	Not Encrypted	
EBS	/dev/sdb	Search (case-insensit	30	General Purpose SSD (GP2)	100 / 3000	N/A	☑	Not Encrypted	⊗

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

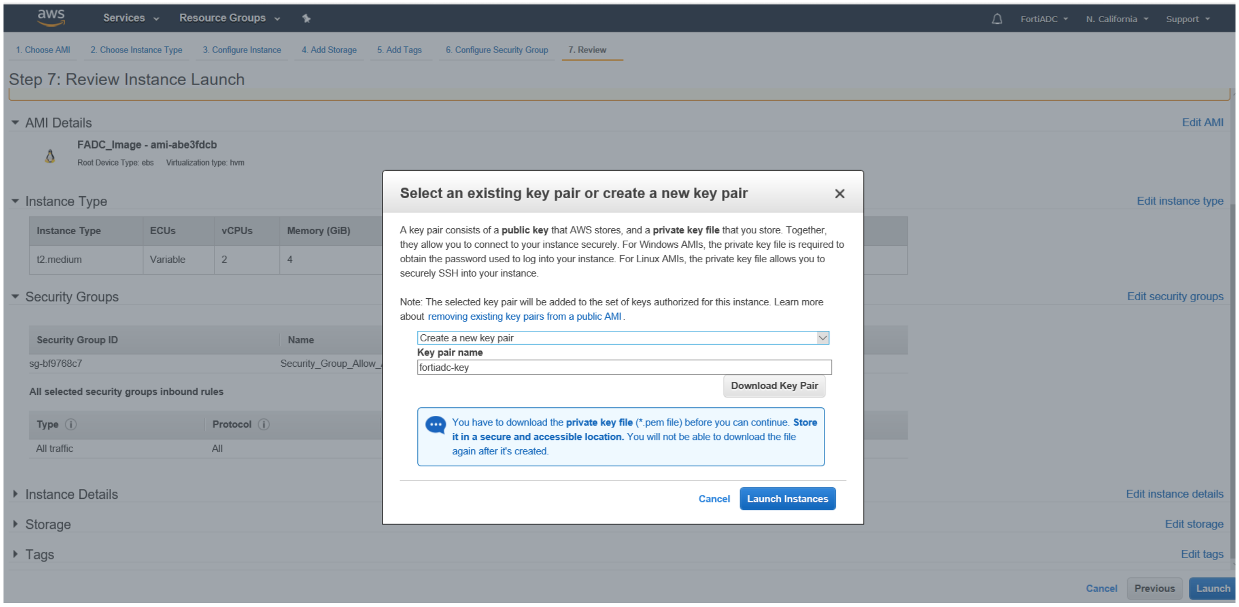
	Security Group ID	Name	Description	Actions
□	sg-53b6492b	default	default VPC security group	Copy to new
■	sg-bf9768c7	Security_Group_Allow_All	Security_Group_Allow_All	Copy to new

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.



Step 7: Review Instance Launch

AMI Details

FADC_Image - ami-abe3fdcb

Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)
t2.medium	Variable	2	4

Security Groups

Security Group ID	Name
sg-bf9768c7	Security_Group_Allow_

All selected security groups inbound rules

Type	Protocol
All traffic	All

Instance Details

Storage

Tags

Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name

fortiadc-key

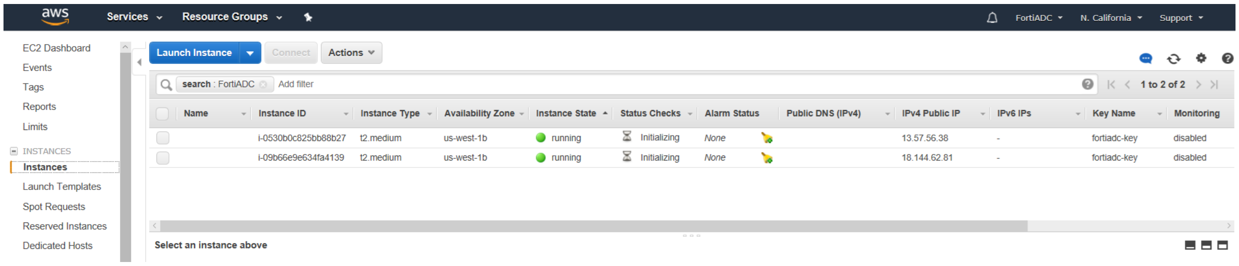
Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel Launch Instances

9. Click “Launch Instances”.

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



search : FortiADC

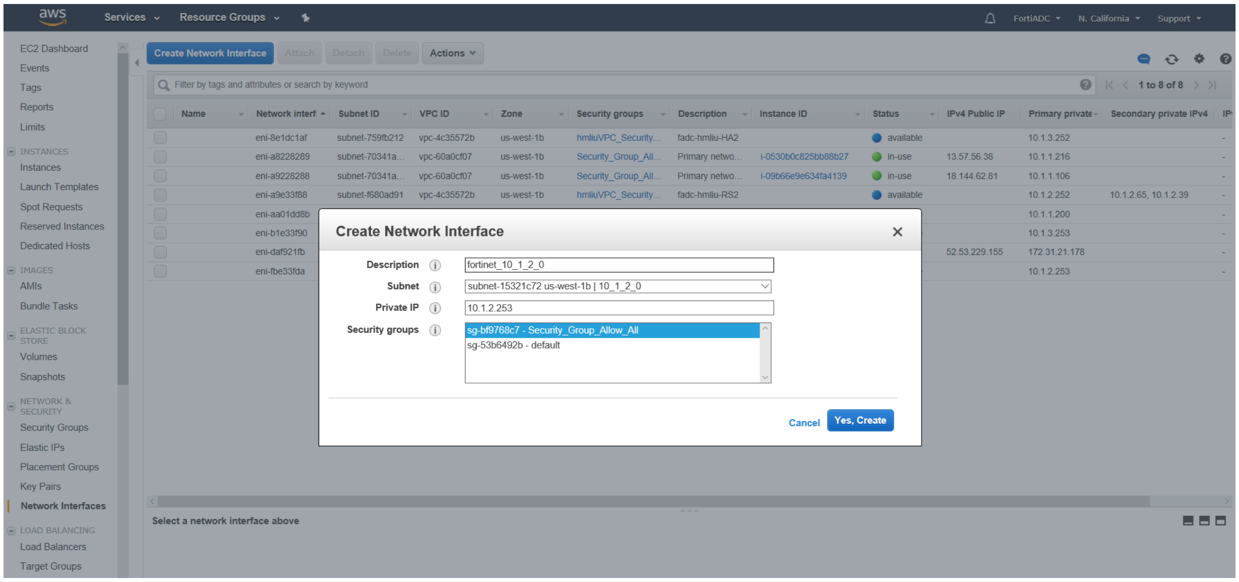
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring
	i-0530b0c825bb88b27	t2.medium	us-west-1b	● running	Initializing	None		13.57.56.38	-	fortiadc-key	disabled
	i-09b66e9e634fa4139	t2.medium	us-west-1b	● running	Initializing	None		18.144.62.81	-	fortiadc-key	disabled

Select an instance above

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.



Name	Network interf	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID	Status	IPv4 Public IP	Primary private	Secondary private IPv4	IP
	eni-8e1dc1af	subnet-759fb212	vpc-4c35572b	us-west-1b	hmliuVPC_Security…	fadc-hmliu-HA2		available		10.1.3.252		-
	eni-a8228289	subnet-70341a…	vpc-60a0cf07	us-west-1b	Security_Group_All…	Primary netwo…	i-0530b0c825bb88b27	in-use	13.57.56.38	10.1.1.216		-
	eni-a9228288	subnet-70341a…	vpc-60a0cf07	us-west-1b	Security_Group_All…	Primary netwo…	i-09b66e9e634fa4139	in-use	18.144.62.81	10.1.1.106		-
	eni-a9e33f88	subnet-f680ad91	vpc-4c35572b	us-west-1b	hmliuVPC_Security…	fadc-hmliu-RS2		available		10.1.2.252	10.1.2.65, 10.1.2.39	-
	eni-aa01dd8b									10.1.1.200		-
	eni-b1e33f90									10.1.3.253		-
	eni-daf921fb								52.53.229.155	172.31.21.178		-
	eni-fbe33fda									10.1.2.253		-

Create Network Interface

Description: fortinet_10_1_2_0

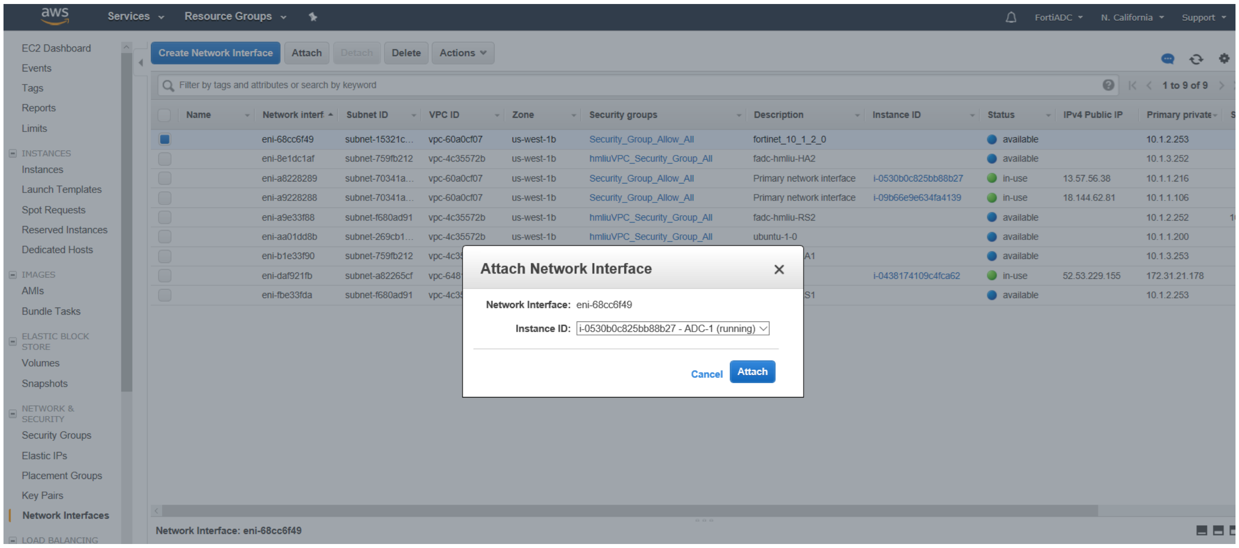
Subnet: subnet-15321c72 us-west-1b | 10_1_2_0

Private IP: 10.1.2.253

Security groups: sg-bf9768c7 - Security_Group_Allow_All; sg-53b6492b - default

Cancel | Yes, Create

Step 2：Attach interface to FortiADC-VM instance.



Name	Network interf	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID	Status	IPv4 Public IP	Primary private	S
	eni-68cc6f49	subnet-15321c…	vpc-60a0cf07	us-west-1b	Security_Group_Allow_All	fortinet_10_1_2_0		available		10.1.2.253	
	eni-8e1dc1af	subnet-759fb212	vpc-4c35572b	us-west-1b	hmliuVPC_Security_Group_All	fadc-hmliu-HA2		available		10.1.3.252	
	eni-a8228289	subnet-70341a…	vpc-60a0cf07	us-west-1b	Security_Group_Allow_All	Primary network interface	i-0530b0c825bb88b27	in-use	13.57.56.38	10.1.1.216	
	eni-a9228288	subnet-70341a…	vpc-60a0cf07	us-west-1b	Security_Group_Allow_All	Primary network interface	i-09b66e9e634fa4139	in-use	18.144.62.81	10.1.1.106	
	eni-a9e33f88	subnet-f680ad91	vpc-4c35572b	us-west-1b	hmliuVPC_Security_Group_All	fadc-hmliu-RS2		available		10.1.2.252	1
	eni-aa01dd8b	subnet-269cb1…	vpc-4c35572b	us-west-1b	hmliuVPC_Security_Group_All	ubuntu-1-0		available		10.1.1.200	
	eni-b1e33f90	subnet-759fb212	vpc-4c3			A1		available		10.1.3.253	
	eni-daf921fb	subnet-a82265cf	vpc-648				i-0438174109c4fca62	in-use	52.53.229.155	172.31.21.178	
	eni-fbe33fda	subnet-f680ad91	vpc-4c3			S1		available		10.1.2.253	

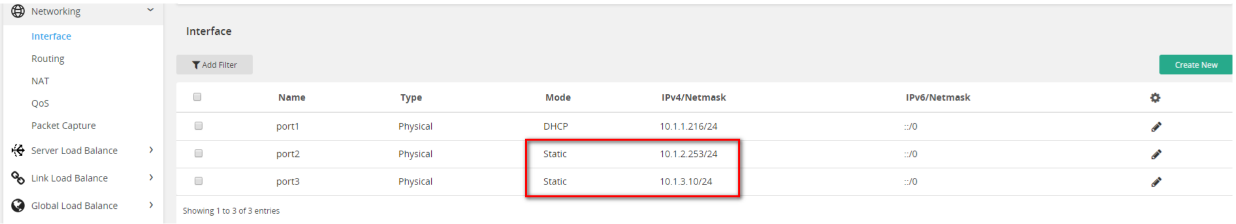
Attach Network Interface

Network Interface: eni-68cc6f49

Instance ID: i-0530b0c825bb88b27 - ADC-1 (running)

Cancel | Attach

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

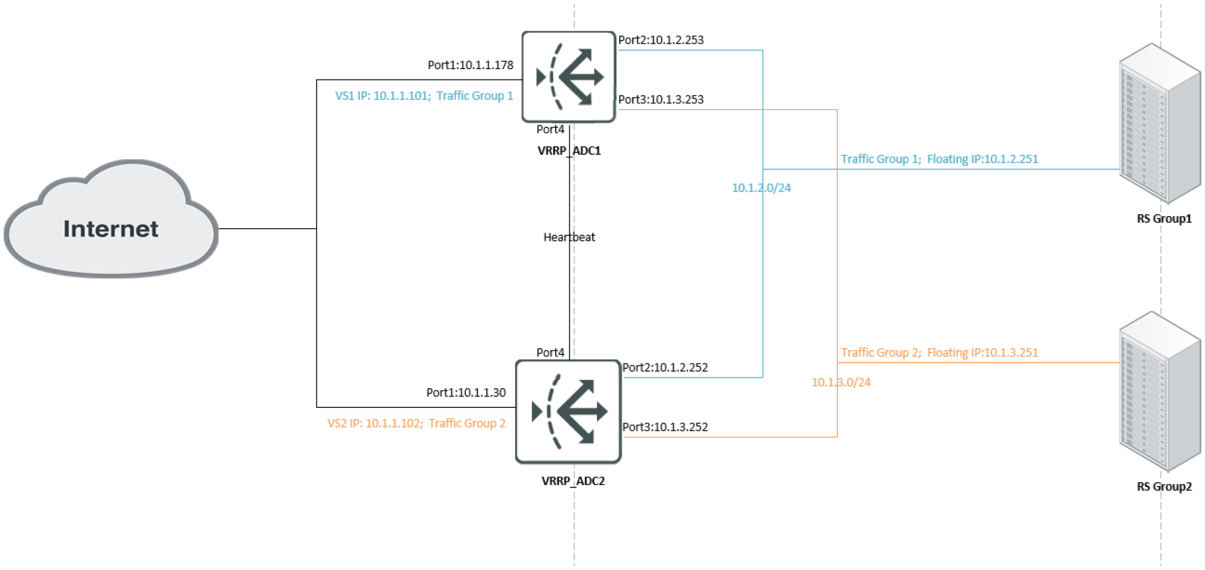


Interface

Name	Type	Mode	IPv4/Netmask	IPv6/Netmask
port1	Physical	DHCP	10.1.1.216/24	::/0
port2	Physical	Static	10.1.2.253/24	::/0
port3	Physical	Static	10.1.3.10/24	::/0

Showing 1 to 3 of 3 entries

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 l7-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

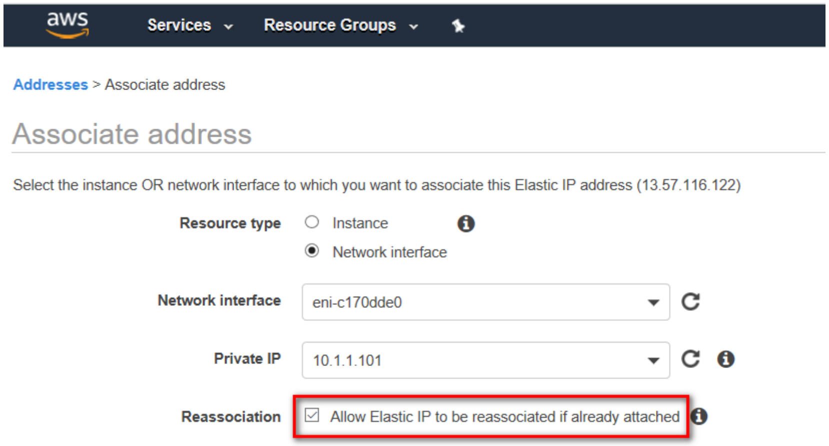
1. Ensure that the gateway of RS is a floating IP.

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.



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

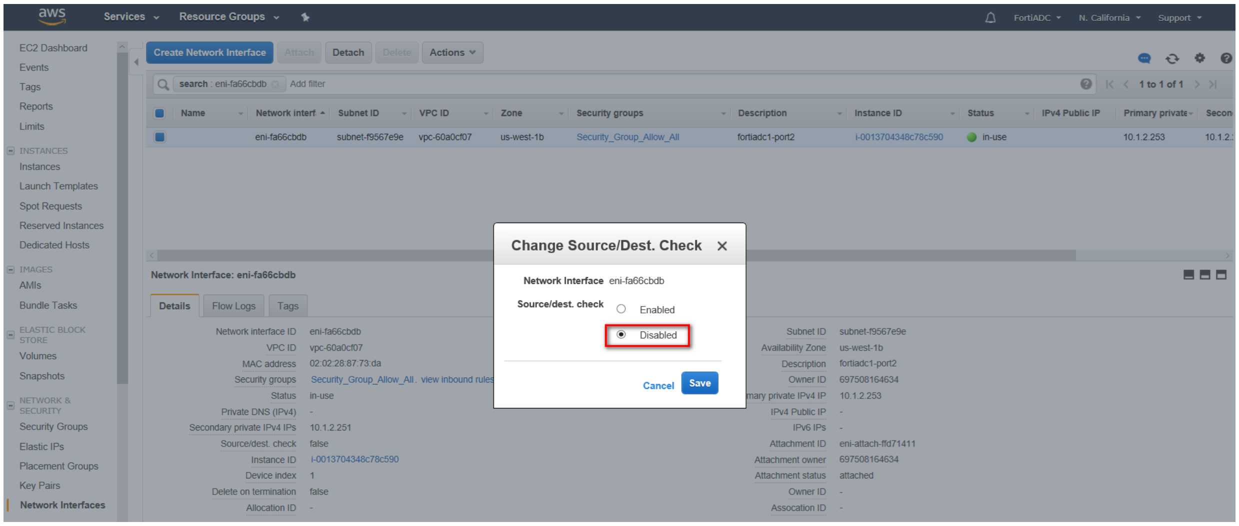
Resource type ○ Instance ● Network interface

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.



search : eni-fa66cbdb

Name	Network interf	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID	Status	IPv4 Public IP	Primary private	Secon
	eni-fa66cbdb	subnet-f9567e9e	vpc-60a0cf07	us-west-1b	Security_Group_Allow_All	fortiadc1-port2	i-0013704348c78c590	● in-use		10.1.2.253	10.1.2.:

Network Interface: eni-fa66cbdb

Network interface ID	eni-fa66cbdb	Subnet ID	subnet-f9567e9e
VPC ID	vpc-60a0cf07	Availability Zone	us-west-1b
MAC address	02:02:28:87:73:da	Description	fortiadc1-port2
Security groups	Security_Group_Allow_All . view inbound rules	Owner ID	697508164634
Status	in-use	mary private IPv4 IP	10.1.2.253
Private DNS (IPv4)	-	IPv4 Public IP	-
Secondary private IPv4 IPs	10.1.2.251	IPv6 IPs	-
Source/dest. check	false	Attachment ID	eni-attach-ffd71411
Instance ID	i-0013704348c78c590	Attachment owner	697508164634
Device index	1	Attachment status	attached
Delete on termination	false	Owner ID	-
Allocation ID	-	Assocation ID	-

Change Source/Dest. Check ×

Network Interface eni-fa66cbdb

Source/dest. check ○ Enabled ● Disabled

Cancel Save

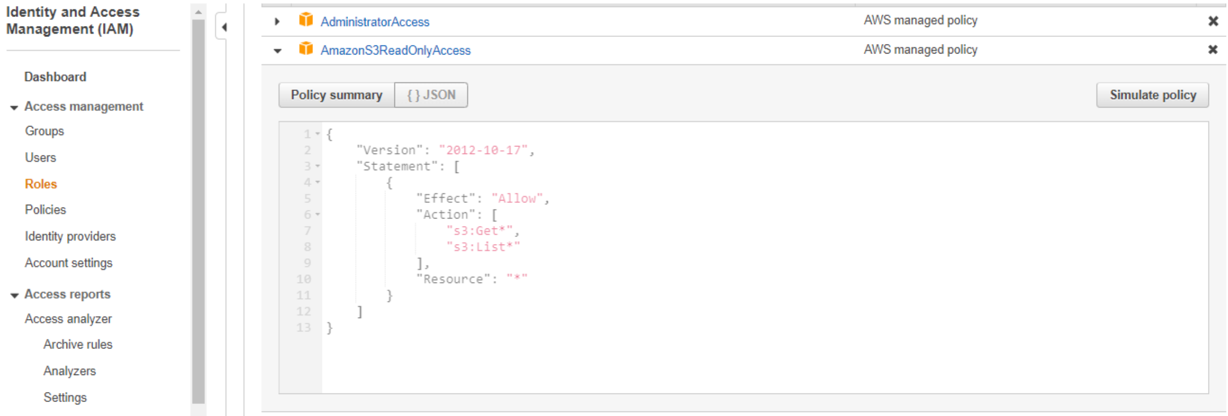
Bootstrapping the FortiADC-VM at initial boot-up using user data

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": "*"
      }
   ]
}
```



AdministratorAccess	AWS managed policy
AmazonS3ReadOnlyAccess	AWS managed policy

```
{
    "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

.

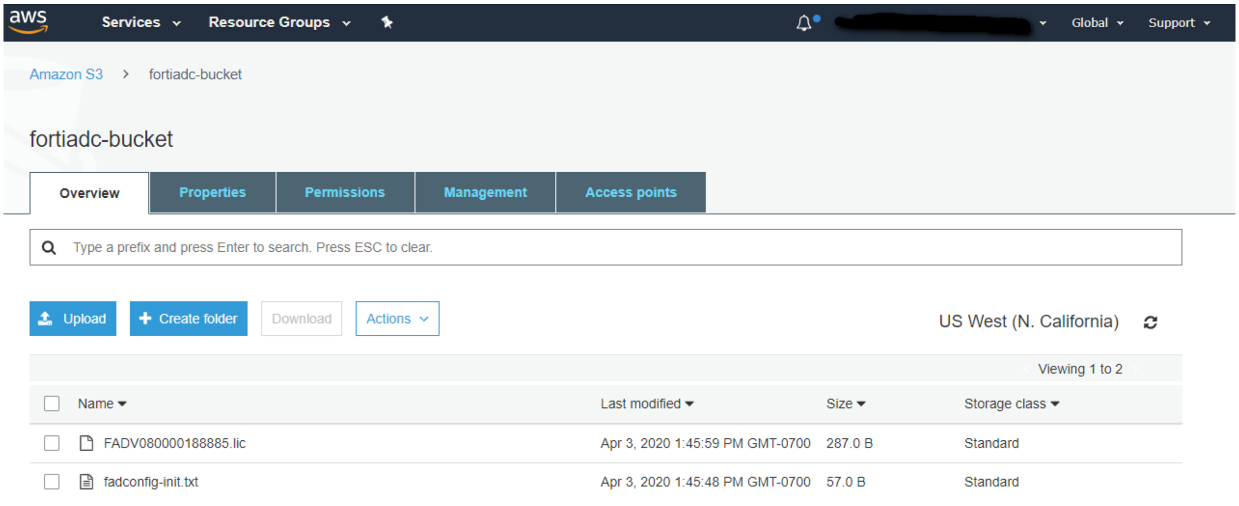
Creating S3 buckets with license and firewall configurations

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.

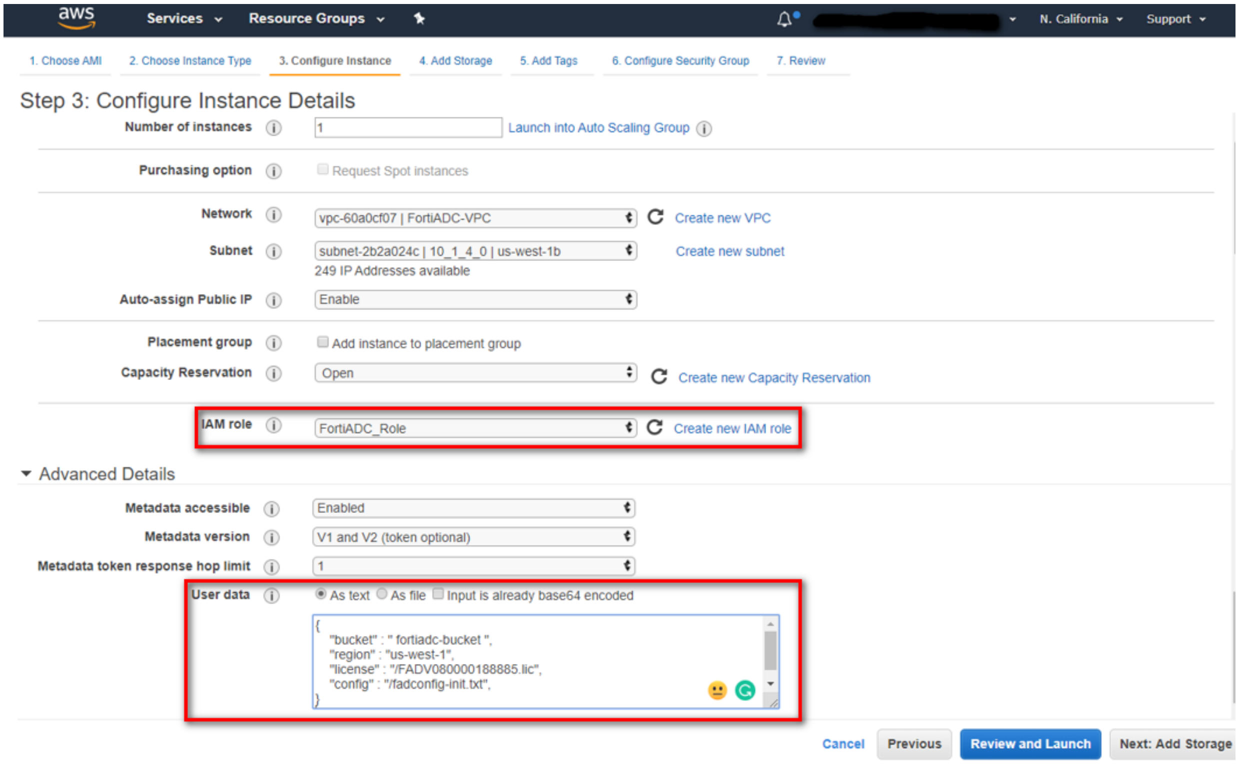
```
{
   "bucket" : "fortiadc-bucket",
   "region" : "us-west-1",
   "license" : "/FADV080000188885.lic",
   "config" : "/fadconfig-init.txt"
}
```



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**.



Step 3: Configure Instance Details

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-60a0cf07 | FortiADC-VPC — Create new VPC

Subnet: subnet-2b2a024c | 10_1_4_0 | us-west-1b — Create new subnet
249 IP Addresses available

Auto-assign Public IP: Enable

Placement group: □ Add instance to placement group

Capacity Reservation: Open — Create new Capacity Reservation

IAM role: FortiADC_Role — Create new IAM role

Advanced Details

Metadata accessible: Enabled

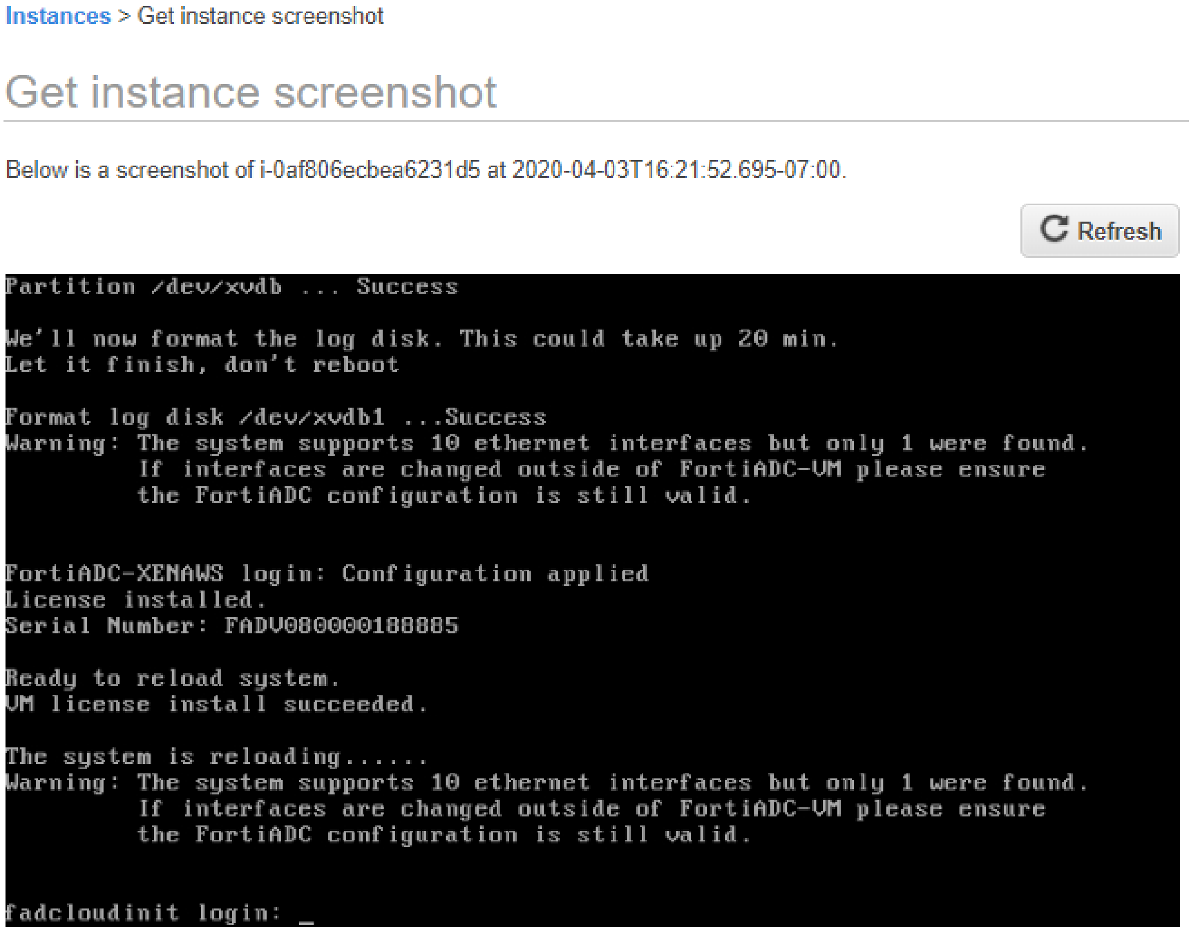
Metadata version: V1 and V2 (token optional)

Metadata token response hop limit: 1

User data: ● As text ○ As file □ Input is already base64 encoded

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

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.



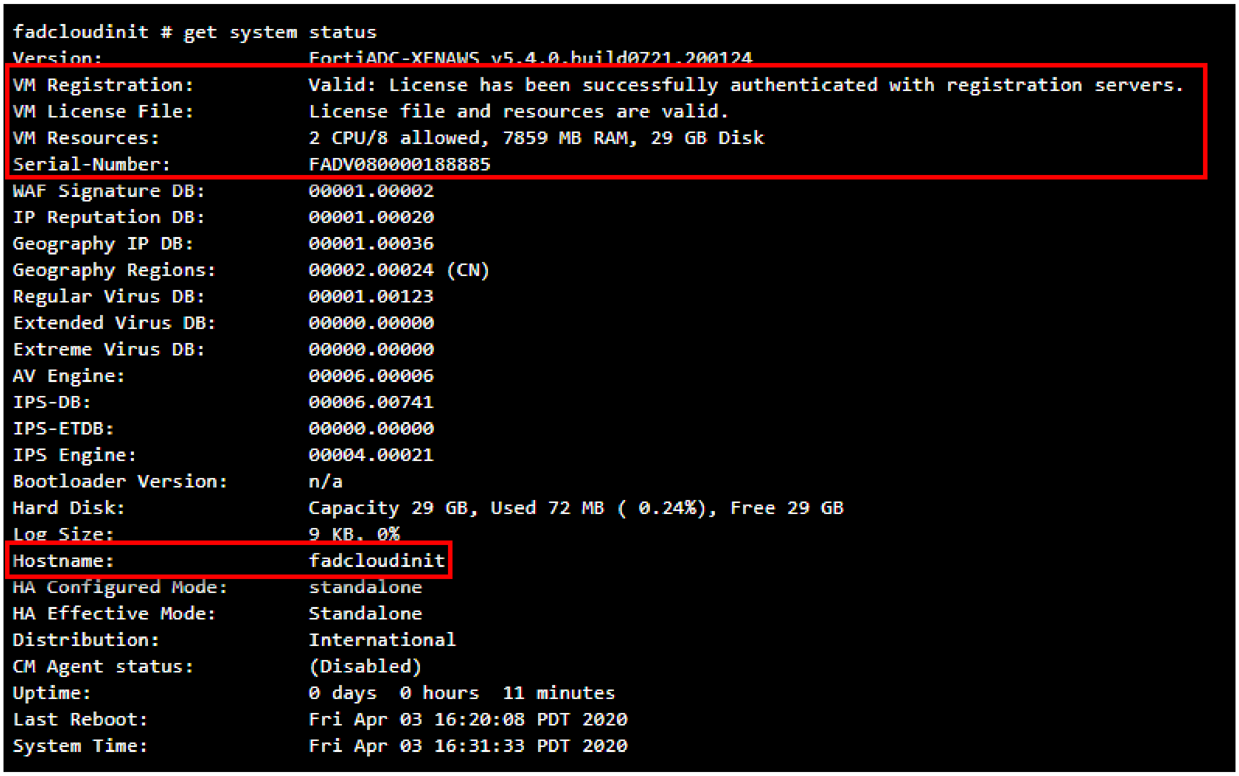
Instances > Get instance screenshot

Get instance screenshot

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

```
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: FADV080000188885

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
```

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 XXXXXXXXXX (get from .csv file when create user on AWS)
set secretkey XXXXXXXXXX (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
```

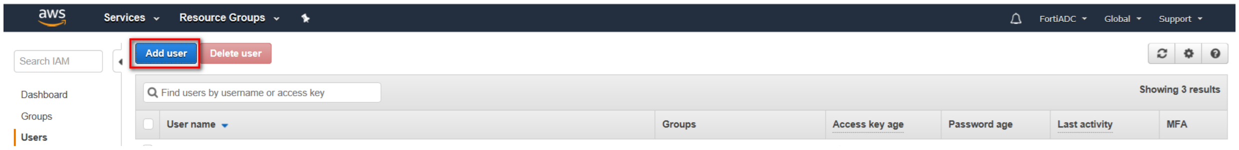
B. Verify that the AWS CLI installed correctly.

```
$ aws --version
```

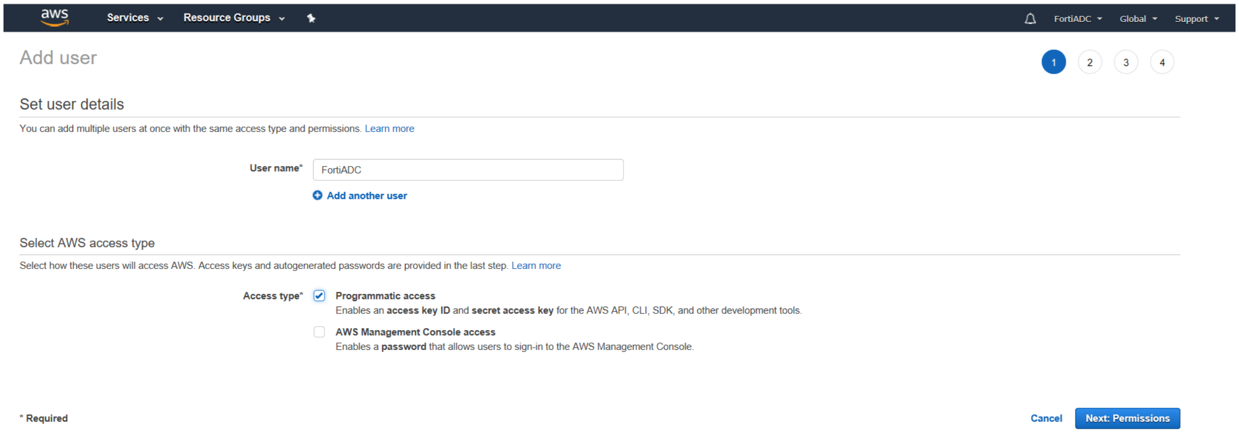
Step 2: Get IAM key

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

B. Users -> Add user



C. Check the box Programmatic access



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* FortiADC

Select AWS access type

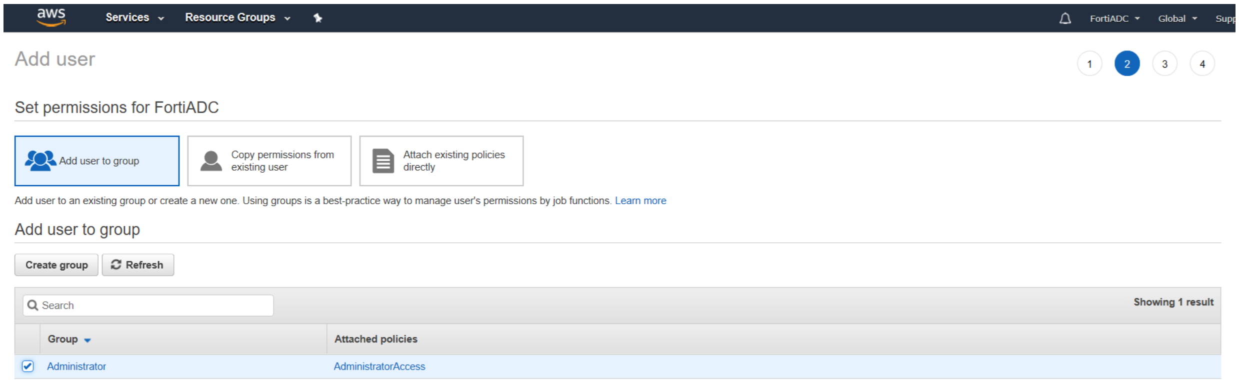
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

D. Check the box Administrators



Add user

Set permissions for FortiADC

Add user to group
Copy permissions from existing user
Attach existing policies directly

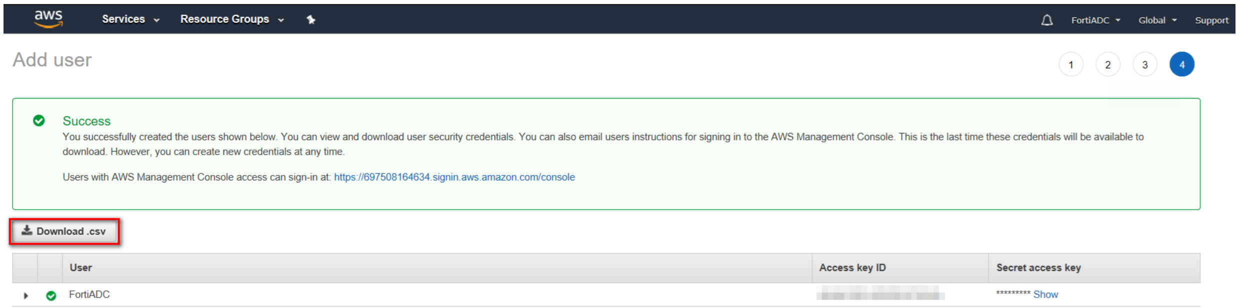
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

Showing 1 result

	Group	Attached policies
☑	Administrator	AdministratorAccess

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



Add user

Success

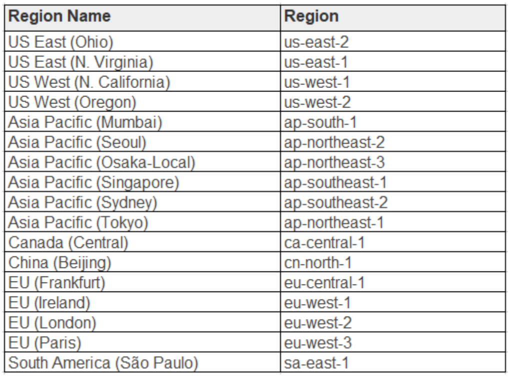
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any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

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

	User	Access key ID	Secret access key
▸ ✓	FortiADC	[redacted]	******** 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
```

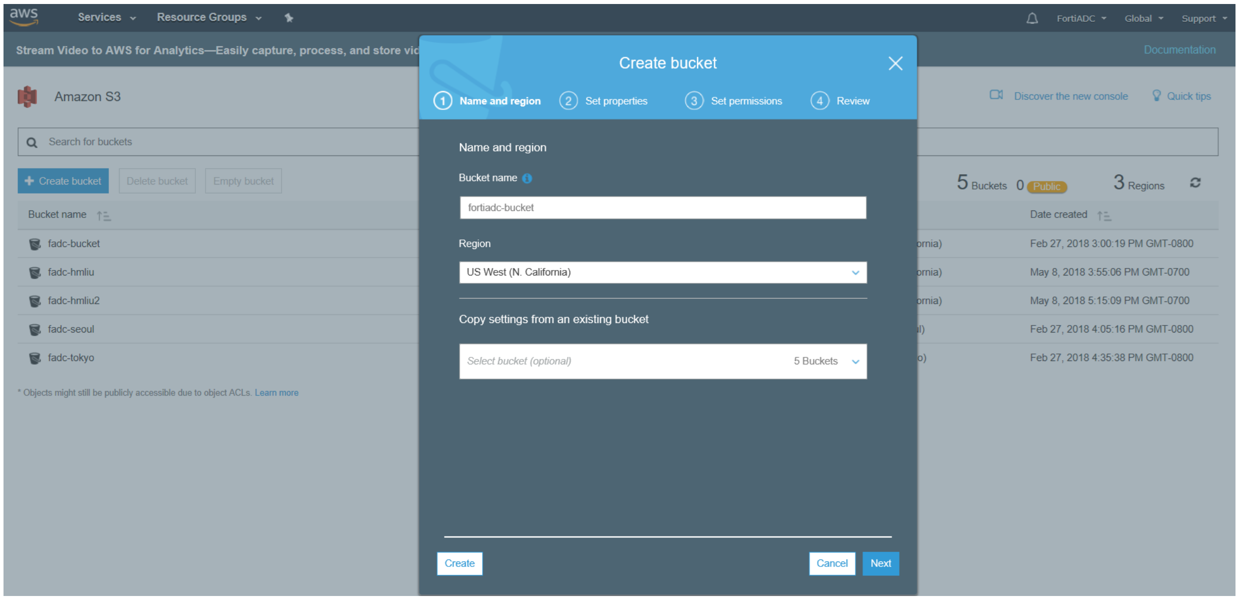


Region Name	Region
US East (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka-Local)	ap-northeast-3
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (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



Name and region

Bucket name: fortiadc-bucket

Region: US West (N. California)

Copy settings from an existing bucket

Select bucket (optional) 5 Buckets

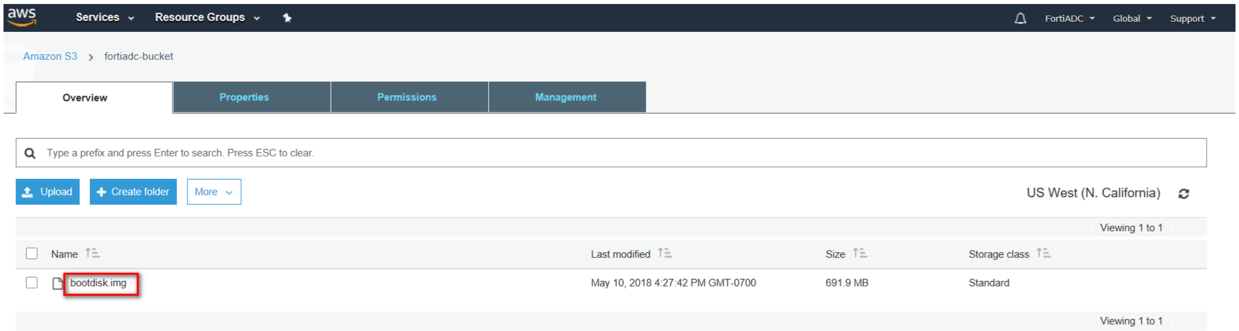
Bucket name		Date created
fadc-bucket	ornia)	Feb 27, 2018 3:00:19 PM GMT-0800
fadc-hmliu	ornia)	May 8, 2018 3:55:06 PM GMT-0700
fadc-hmliu2	ornia)	May 8, 2018 5:15:09 PM GMT-0700
fadc-seoul	l)	Feb 27, 2018 4:05:16 PM GMT-0800
fadc-tokyo	o)	Feb 27, 2018 4:35:38 PM GMT-0800

* Objects might still be publicly accessible due to object ACLs. Learn more

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



US West (N. California)

Viewing 1 to 1

Name	Last modified	Size	Storage class
bootdisk.img	May 10, 2018 4:27:42 PM GMT-0700	691.9 MB	Standard

Viewing 1 to 1

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:GetBucketLocation",
   "s3:GetObject",
   "s3:ListBucket"
],
   "Resource":[
   "arn:aws:s3:::fortiadc-bucket", // arn:aws:s3:<your S3 bucket name>
   "arn:aws:s3:::fortiadc-bucket/*" // 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

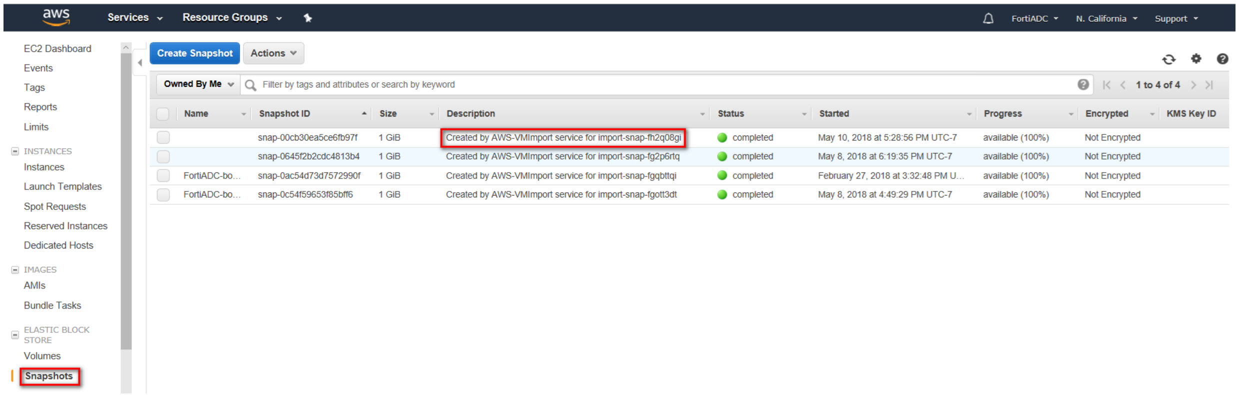
```
$ aws ec2 import-snapshot --description "<description>" --disk-container
     file://container.json
{
"SnapshotTaskDetail": {
"Status": "active",
"Description": "FADC",
"Format": "RAW",
"DiskImageSize": 0.0,
"UserBucket": {
"S3Bucket": "fortiadc-bucket",
"S3Key": "bootdisk.img"
},
"Progress": "3",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

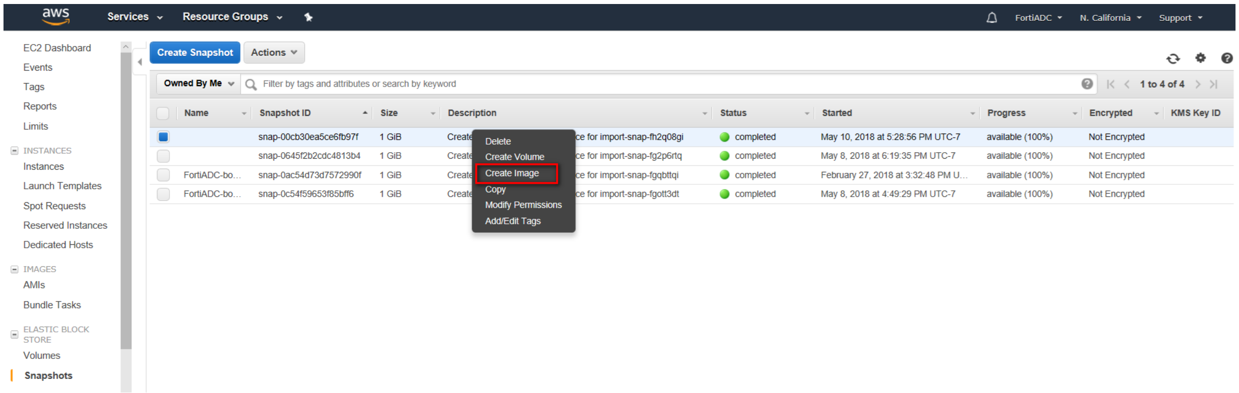
After "Status": "completed", you can find your snapshot in the navigation pane, under Elastic Block Store



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-0645f2b2cdc4813b4	1 GiB	Created by AWS-VMImport service for import-snap-fg2p6rtq	completed	May 8, 2018 at 6:19:35 PM UTC-7	available (100%)	Not Encrypted	
FortiADC-bo...	snap-0ac54d73d7572990f	1 GiB	Created by AWS-VMImport service for import-snap-fgqbttqi	completed	February 27, 2018 at 3:32:48 PM U...	available (100%)	Not Encrypted	
FortiADC-bo...	snap-0c54f59653f85bff6	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	

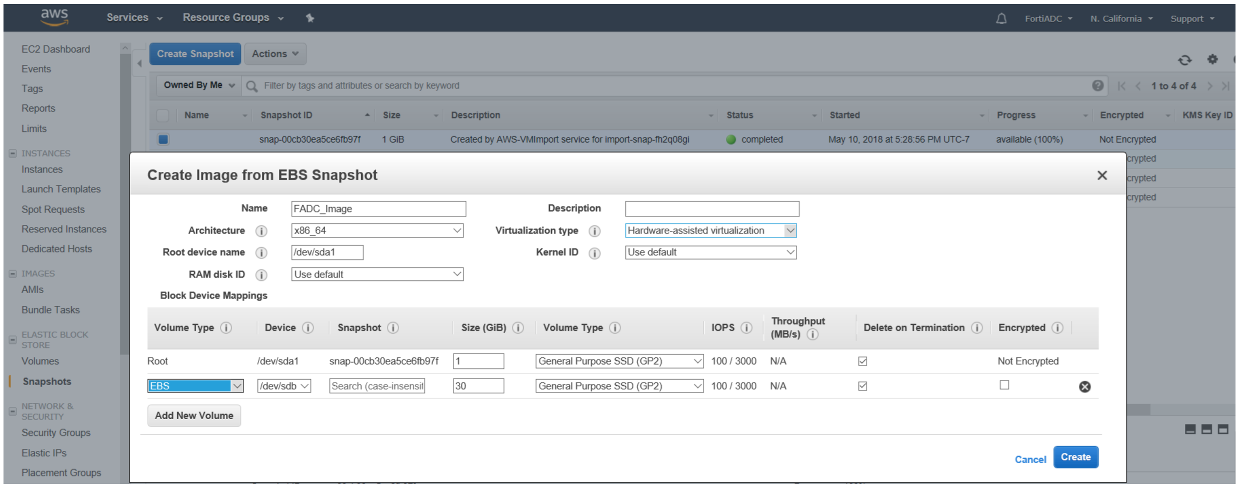
Step 6: Create Amazon Machine Image (AMI)

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



Name	Snapshot ID	Size	Description	Status	Started	Progress	Encrypted	KMS Key ID
	snap-00cb30ea5ce6fb97f	1 GiB	Create ce for import-snap-fh2q08gi	completed	May 10, 2018 at 5:28:56 PM UTC-7	available (100%)	Not Encrypted	
	snap-0645f2b2cdc4813b4	1 GiB	Create ce for import-snap-fg2p6rtq	completed	May 8, 2018 at 6:19:35 PM UTC-7	available (100%)	Not Encrypted	
FortiADC-bo...	snap-0ac54d73d7572990f	1 GiB	Create ce for import-snap-fgqbttqi	completed	February 27, 2018 at 3:32:48 PM U...	available (100%)	Not Encrypted	
FortiADC-bo...	snap-0c54f59653f85bff6	1 GiB	Create ce for import-snap-fgott3dt	completed	May 8, 2018 at 4:49:29 PM UTC-7	available (100%)	Not Encrypted	

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



	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	

Create Image from EBS Snapshot

Name: FADC_Image
Description:
Architecture: x86_64
Virtualization type: Hardware-assisted virtualization
Root device name: /dev/sda1
Kernel ID: Use default
RAM disk ID: Use default

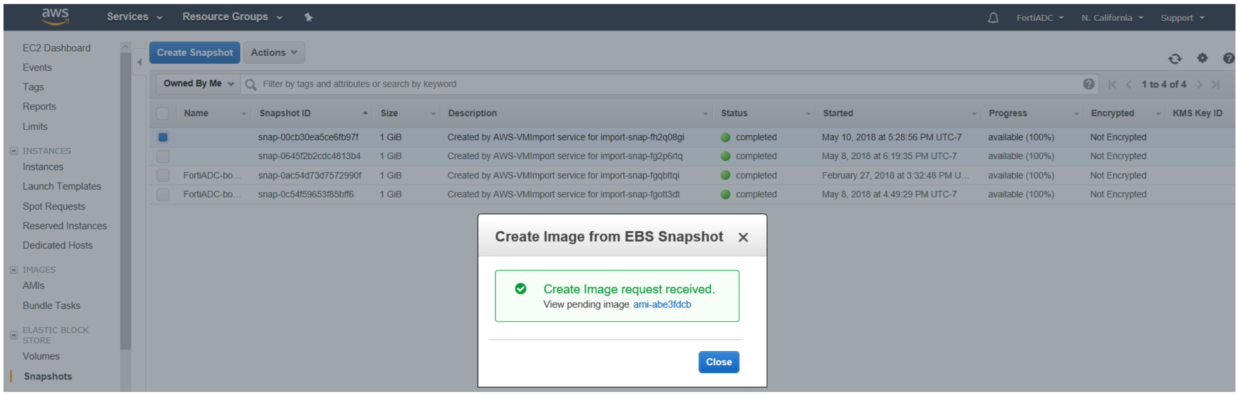
Block Device Mappings

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted	
Root	/dev/sda1	snap-00cb30ea5ce6fb97f	1	General Purpose SSD (GP2)	100 / 3000	N/A	☑	Not Encrypted	
EBS	/dev/sdb	Search (case-insensit	30	General Purpose SSD (GP2)	100 / 3000	N/A	☑	□	⊗

Add New Volume

Cancel Create

3. Click Create



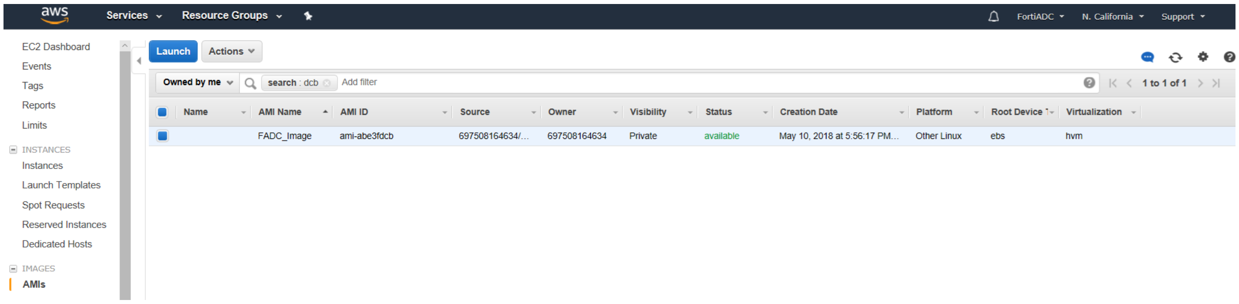
	Name	Snapshot ID	Size	Description	Status	Started	Progress	Encrypted	KMS Key ID
■		snap-00cb30ea5ce6fb97f	1 GiB	Created by AWS-VMImport service for import-snap-fh2q08gi	● completed	May 10, 2018 at 5:28:56 PM UTC-7	available (100%)	Not Encrypted	
□		snap-0645f2b2cdc4813b4	1 GiB	Created by AWS-VMImport service for import-snap-fg2p6rtq	● completed	May 8, 2018 at 6:19:35 PM UTC-7	available (100%)	Not Encrypted	
□	FortiADC-bo...	snap-0ac54d73d7572990f	1 GiB	Created by AWS-VMImport service for import-snap-fgqbttqi	● completed	February 27, 2018 at 3:32:48 PM U...	available (100%)	Not Encrypted	
□	FortiADC-bo...	snap-0c54f59653f85bff6	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	

Create Image from EBS Snapshot

Create Image request received.
View pending image ami-abe3fdcb

Close

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



	Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform	Root Device T	Virtualization
■		FADC_Image	ami-abe3fdcb	697508164634/...	697508164634	Private	available	May 10, 2018 at 5:56:17 PM...	Other Linux	ebs	hvm

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.