ATTACK DEFENSE

by PentesterAcademy

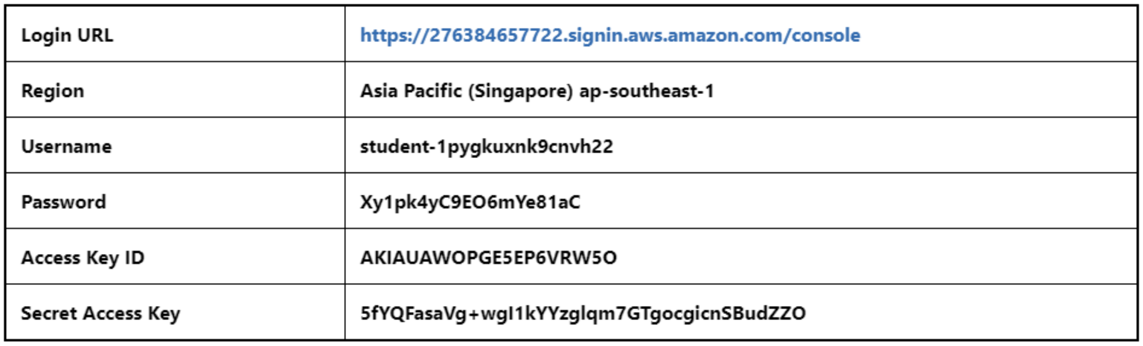
Name	EC2 Enumeration
URL	https://attackdefense.com/challengedetails?cid=2424
Type	AWS Cloud Security : EC2

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

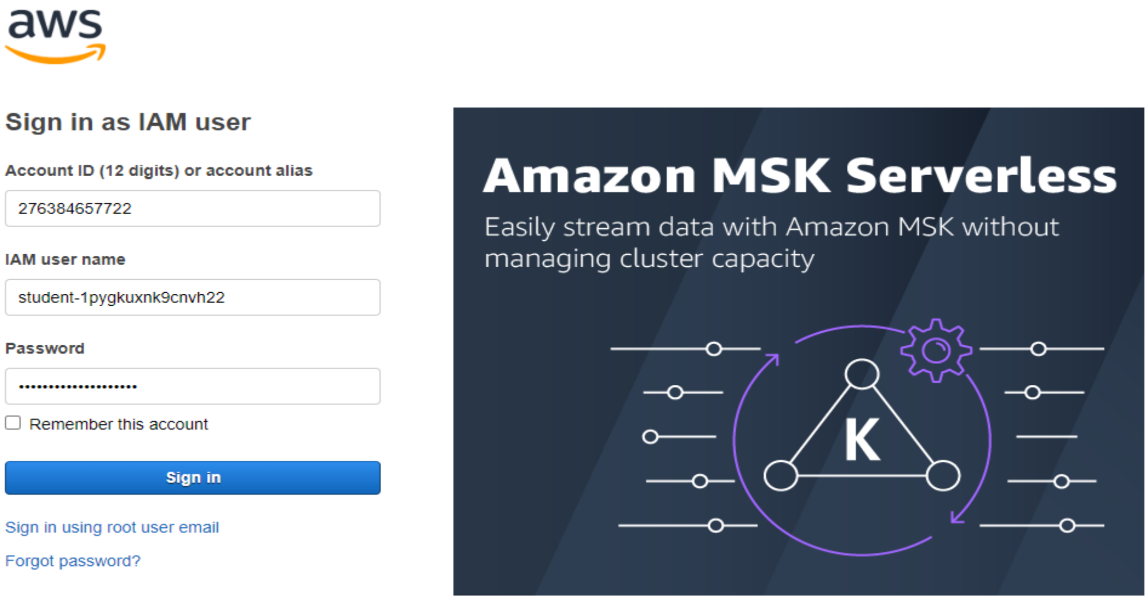
Console Based Enumeration

Step 1: Click on the lab link button to get access to the AWS lab credentials.



Login URL	https://276384657722.signin.aws.amazon.com/console
Region	Asia Pacific (Singapore) ap-southeast-1
Username	student-1pygkuxnk9cnvh22
Password	Xy1pk4yC9EO6mYe81aC
Access Key ID	AKIAUAWOPGE5EP6VRW5O
Secret Access Key	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

Step 2: Sign in to the AWS console.



Sign in as IAM user

Account ID (12 digits) or account alias

276384657722

IAM user name

student-1pygkuxnk9cnvh22

Password

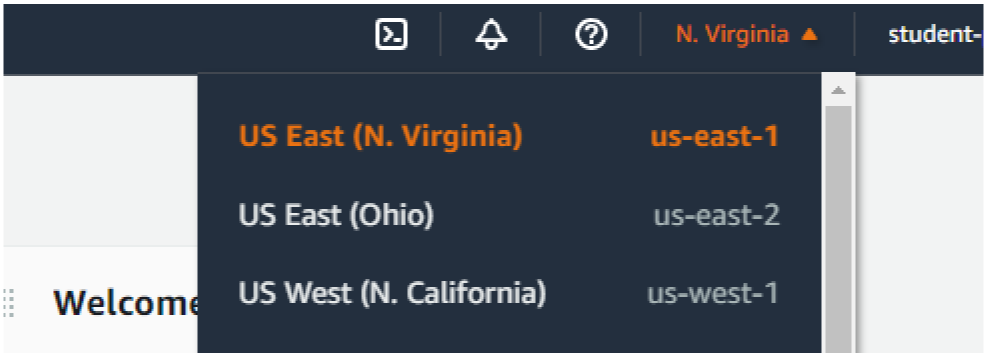
••••••••••••••••••••

□ Remember this account

Sign in
Sign in using root user email
Forgot password?
Amazon MSK Serverless
Easily stream data with Amazon MSK without managing cluster capacity
K

Step 3: Search for the EC2 Dashboard and navigate to it.

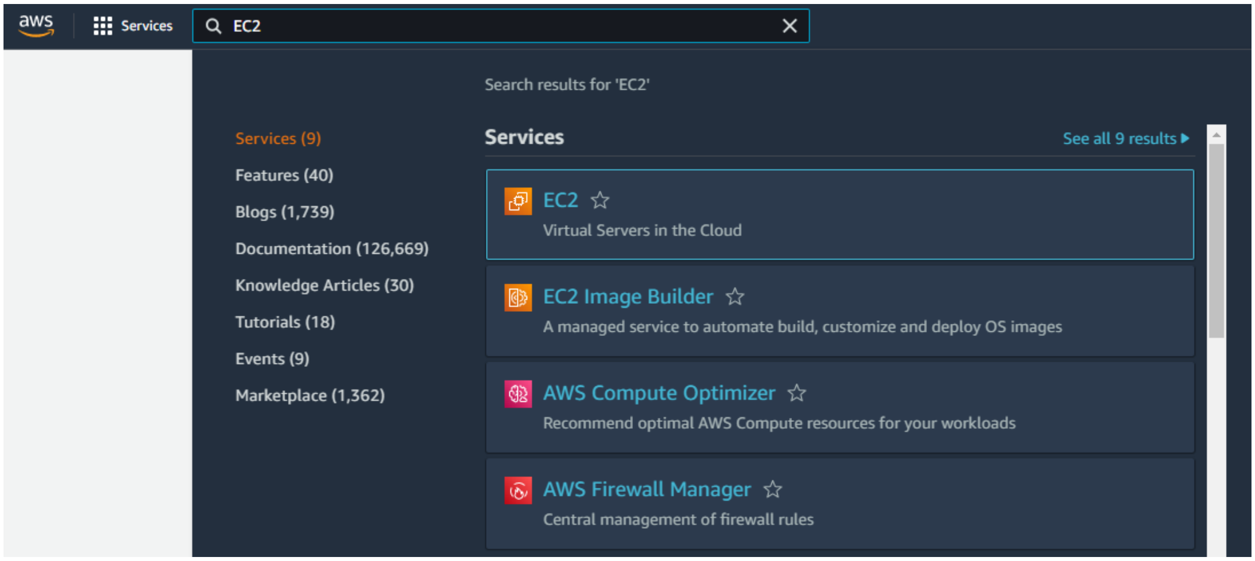
Note: Change the region to “us-east-1”, if it is not selected by default.



US East (N. Virginia) us-east-1

US East (Ohio) us-east-2

US West (N. California) us-west-1



Search results for 'EC2'

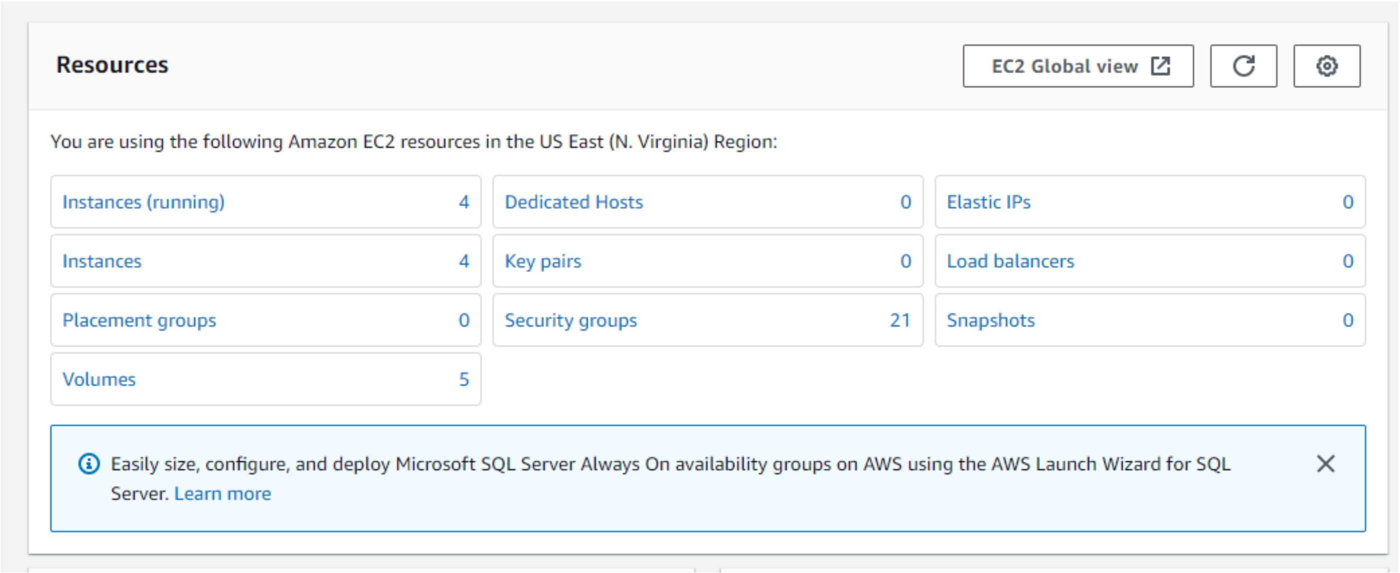
EC2 ☆
Virtual Servers in the Cloud

EC2 Image Builder ☆
A managed service to automate build, customize and deploy OS images

AWS Compute Optimizer ☆
Recommend optimal AWS Compute resources for your workloads

AWS Firewall Manager ☆
Central management of firewall rules

Step 4: Navigate to the instances page from the dashboard by clicking instances under the resources.

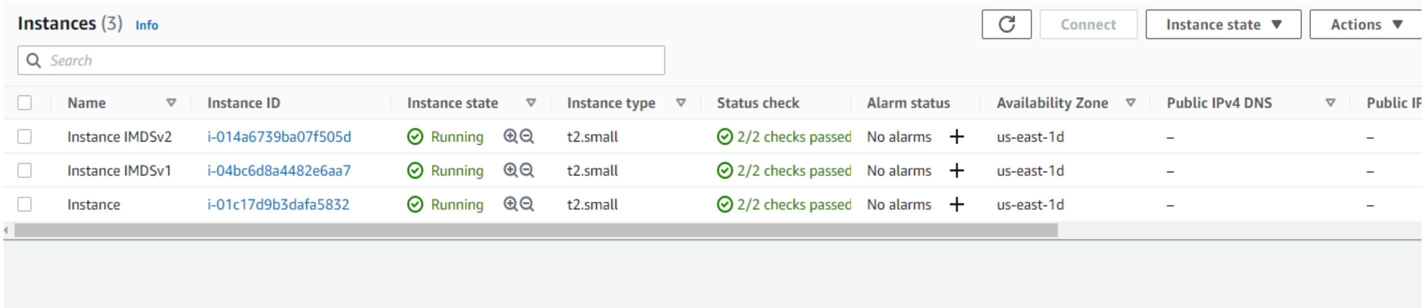


You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	4	Dedicated Hosts	0	Elastic IPs	0
Instances	4	Key pairs	0	Load balancers	0
Placement groups	0	Security groups	21	Snapshots	0
Volumes	5				

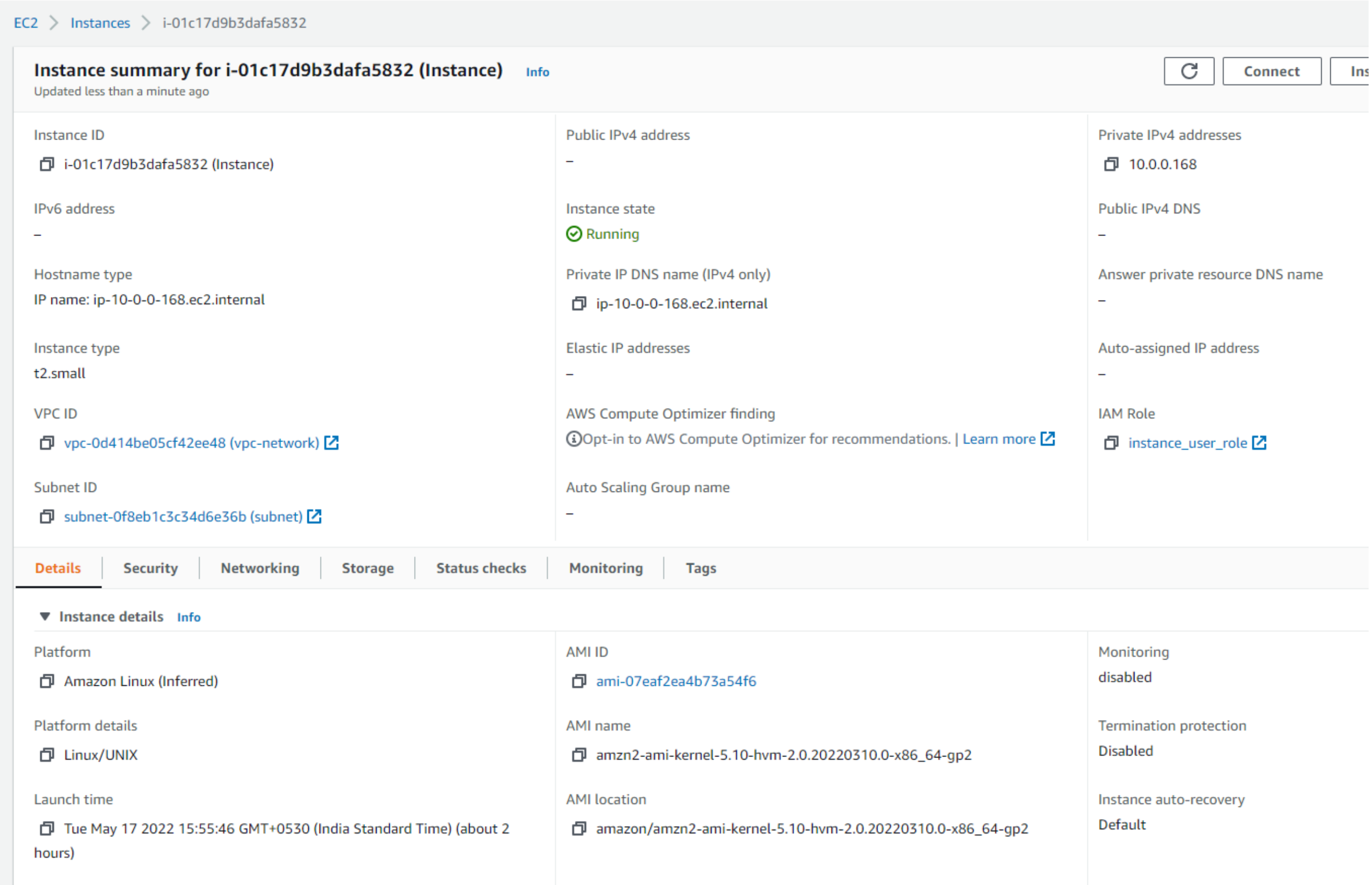
Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Step 5: Under Instances is a list of the EC2 instances deployed in the account. Click on Instance id with the name "Instance".



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
□	Instance IMDSv2	i-014a6739ba07f505d	✓ Running	t2.small	✓ 2/2 checks passed	No alarms +	us-east-1d	–	–
□	Instance IMDSv1	i-04bc6d8a4482e6aa7	✓ Running	t2.small	✓ 2/2 checks passed	No alarms +	us-east-1d	–	–
□	Instance	i-01c17d9b3dafa5832	✓ Running	t2.small	✓ 2/2 checks passed	No alarms +	us-east-1d	–	–

The details of the instance deployed are mentioned here.



Instance summary for i-01c17d9b3dafa5832 (Instance) Info

Updated less than a minute ago

Instance ID
i-01c17d9b3dafa5832 (Instance)

Public IPv4 address
–

Private IPv4 addresses
10.0.0.168

IPv6 address
–

Instance state
✓ Running

Public IPv4 DNS
–

Hostname type
IP name: ip-10-0-0-168.ec2.internal

Private IP DNS name (IPv4 only)
ip-10-0-0-168.ec2.internal

Answer private resource DNS name
–

Instance type
t2.small

Elastic IP addresses
–

Auto-assigned IP address
–

VPC ID
vpc-0d414be05cf42ee48 (vpc-network)

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role
instance_user_role

Subnet ID
subnet-0f8eb1c3c34d6e36b (subnet)

Auto Scaling Group name
–

▼ Instance details Info

Platform
Amazon Linux (Inferred)

AMI ID
ami-07eaf2ea4b73a54f6

Monitoring
disabled

Platform details
Linux/UNIX

AMI name
amzn2-ami-kernel-5.10-hvm-2.0.20220310.0-x86_64-gp2

Termination protection
Disabled

Launch time
Tue May 17 2022 15:55:46 GMT+0530 (India Standard Time) (about 2 hours)

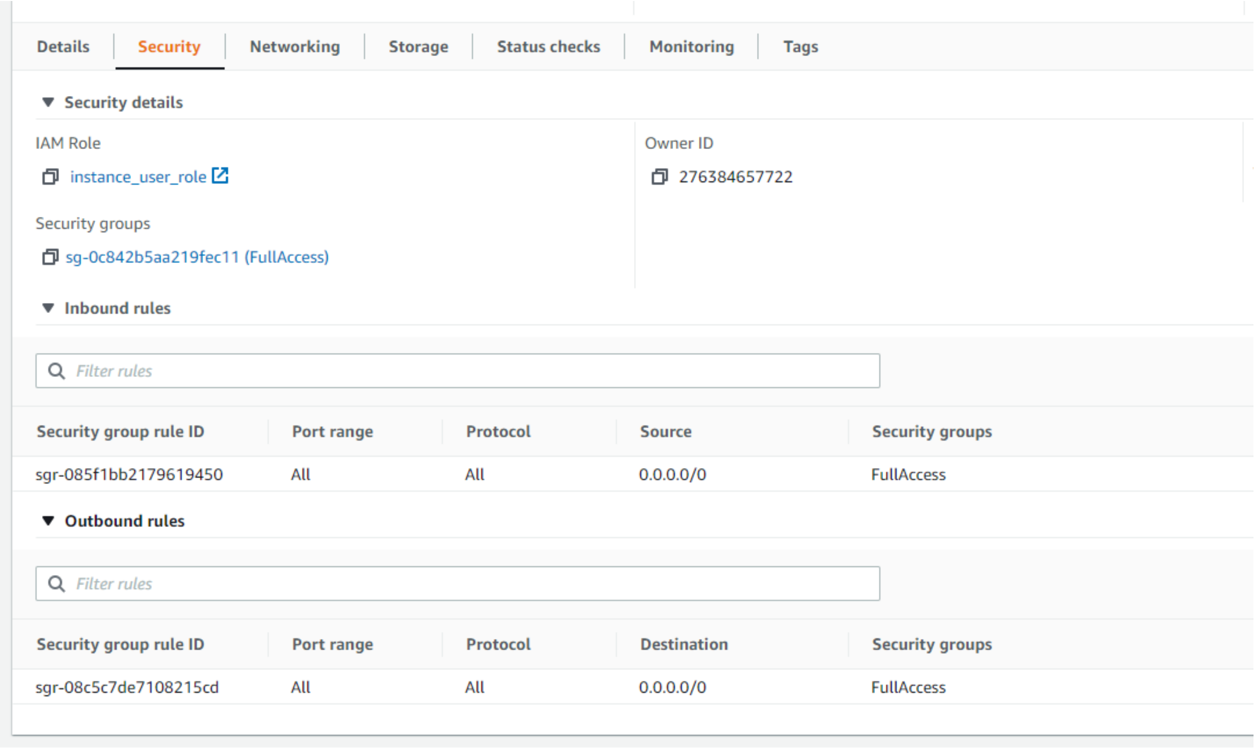
AMI location
amazon/amzn2-ami-kernel-5.10-hvm-2.0.20220310.0-x86_64-gp2

Instance auto-recovery
Default

Step 6: Click on security to see the security details of the instance.

A security group acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance. When you launch an instance, you can specify one or more security groups. If you don't specify a security group, Amazon EC2 uses the default security group.

In this instance, the security group provided is giving full access to the incoming and outgoing traffic.



IAM Role: instance_user_role

Owner ID: 276384657722

Security groups: sg-0c842b5aa219fec11 (FullAccess)

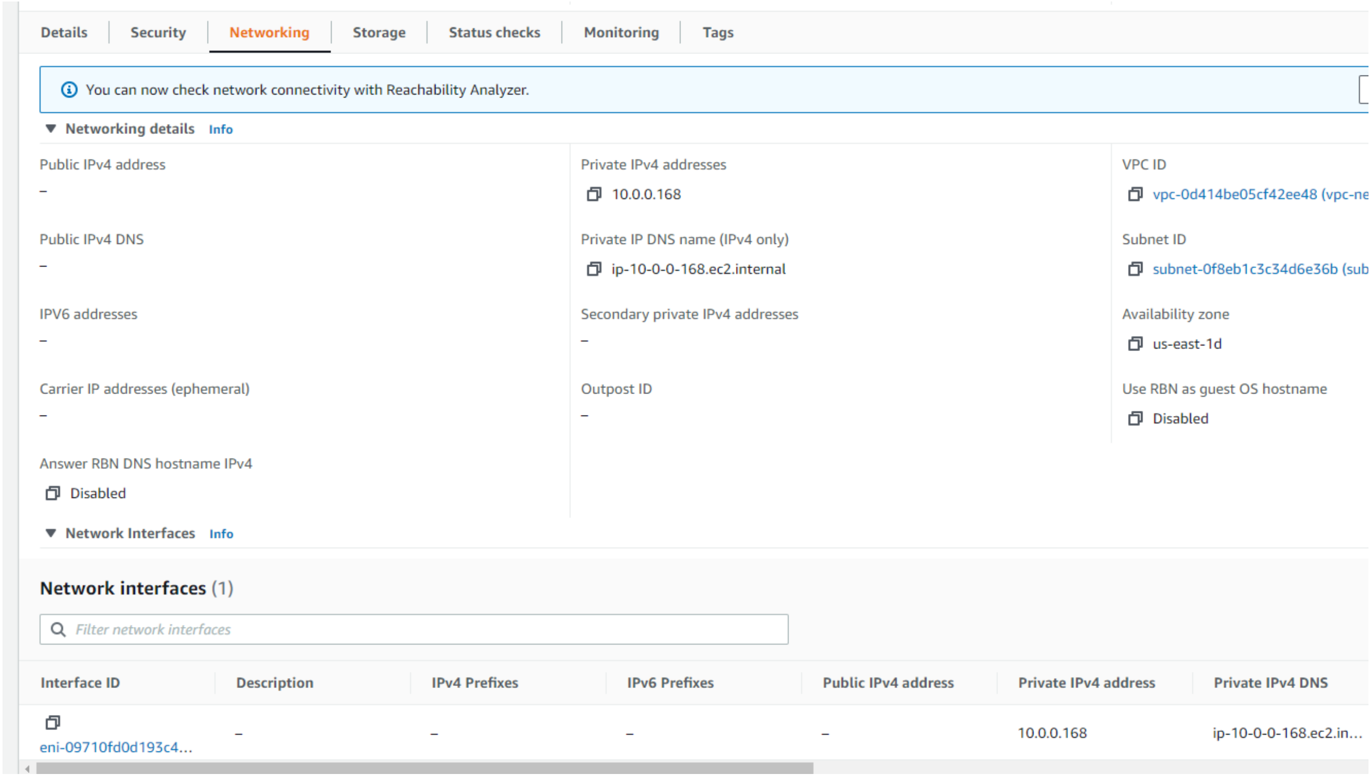
Security group rule ID	Port range	Protocol	Source	Security groups
sgr-085f1bb2179619450	All	All	0.0.0.0/0	FullAccess

Security group rule ID	Port range	Protocol	Destination	Security groups
sgr-08c5c7de7108215cd	All	All	0.0.0.0/0	FullAccess

Step 7: Click on Networking to see the Networking details of the instance.

When you launch an instance, you can select a subnet from the VPC. The instance is configured with a primary network interface, which is a logical virtual network card.

For this instance, public IP is disabled, so this instance only has a private ipv4 address.



You can now check network connectivity with Reachability Analyzer.

▼ Networking details Info

Public IPv4 address
–

Public IPv4 DNS
–

IPV6 addresses
–

Carrier IP addresses (ephemeral)
–

Answer RBN DNS hostname IPv4
Disabled

Private IPv4 addresses
10.0.0.168

Private IP DNS name (IPv4 only)
ip-10-0-0-168.ec2.internal

Secondary private IPv4 addresses
–

Outpost ID
–

VPC ID
vpc-0d414be05cf42ee48 (vpc-ne

Subnet ID
subnet-0f8eb1c3c34d6e36b (sub

Availability zone
us-east-1d

Use RBN as guest OS hostname
Disabled

▼ Network Interfaces Info

Network interfaces (1)

Filter network interfaces

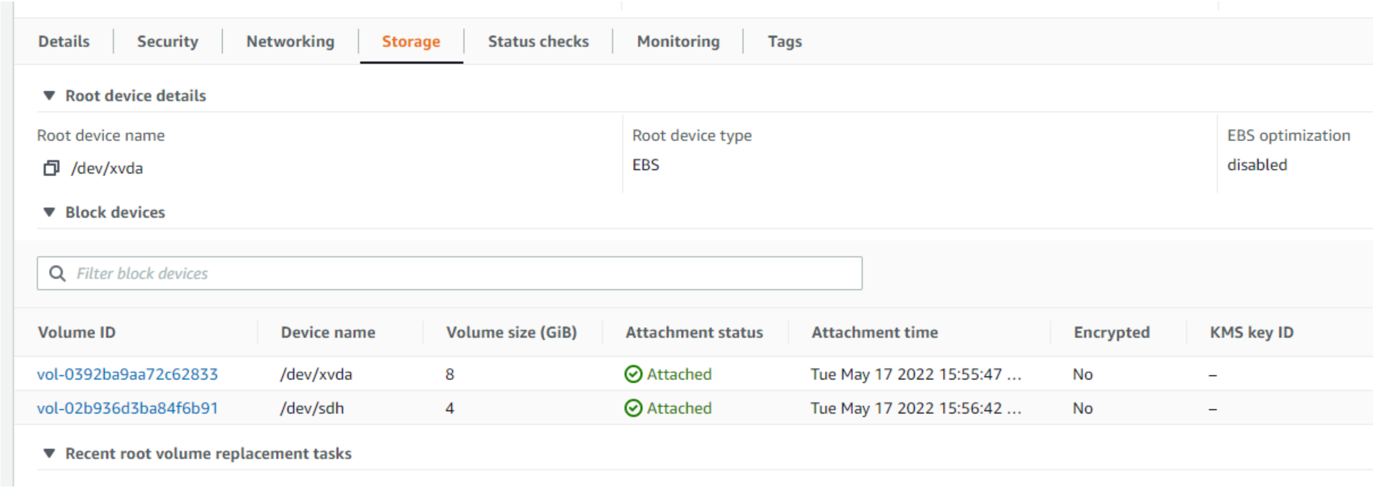
Interface ID	Description	IPv4 Prefixes	IPv6 Prefixes	Public IPv4 address	Private IPv4 address	Private IPv4 DNS
eni-09710fd0d193c4...	–	–	–	–	10.0.0.168	ip-10-0-0-168.ec2.in...

Step 8: Click on Storage to see the Storage details of the instance.

Here you can see two storage volumes attached with this instance which is also called EBS.

EBS volume is a durable, block-level storage device that you can attach to your instances. After you attach a volume to an instance, you can use it as you would use a physical hard drive. EBS volumes are flexible.

For current-generation volumes attached to current-generation instance types, you can dynamically increase size, modify the provisioned IOPS capacity, and change volume type on live production volumes.



▼ Root device details

Root device name	Root device type	EBS optimization
/dev/xvda	EBS	disabled

▼ Block devices

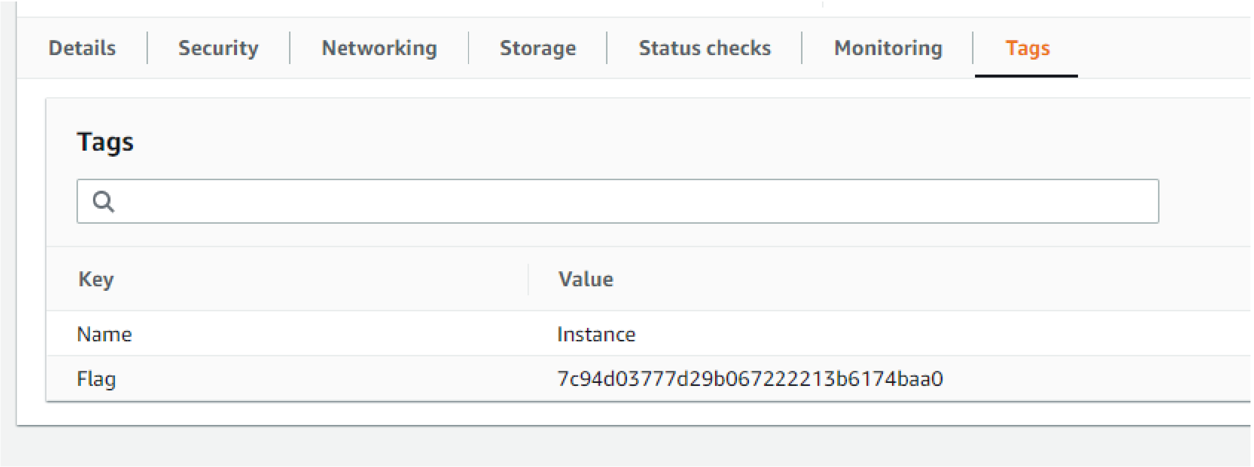
Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
vol-0392ba9aa72c62833	/dev/xvda	8	✓ Attached	Tue May 17 2022 15:55:47 ...	No	–
vol-02b936d3ba84f6b91	/dev/sdh	4	✓ Attached	Tue May 17 2022 15:56:42 ...	No	–

▼ Recent root volume replacement tasks

Step 9: Click on Tags to see the tags attached with this instance.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type

Got the flag from this instance successfully.

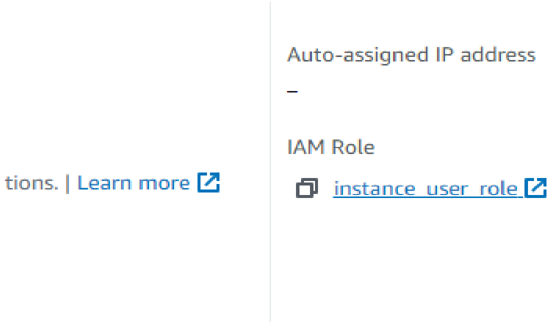


Tags

Key	Value
Name	Instance
Flag	7c94d03777d29b067222213b6174baa0

Flag: 7c94d03777d29b067222213b6174baa0

Step 10: Click on IAM Role attached with this instance.



tions. | Learn more

Auto-assigned IP address

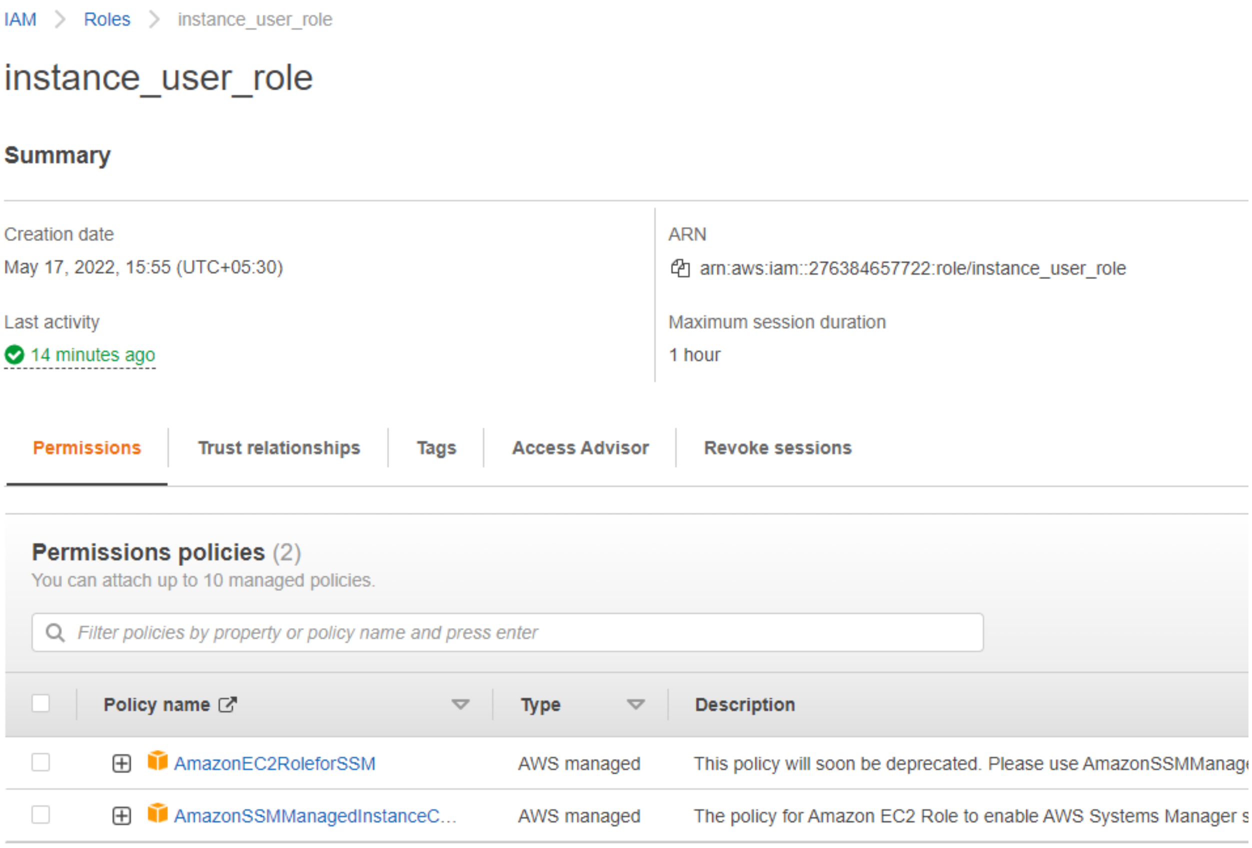
–

IAM Role

instance_user_role

An instance profile is a container for an IAM role that you can use to pass role information to an EC2 instance when the instance starts.

Here you can see the attached policies.



IAM > Roles > instance_user_role

instance_user_role

Summary

Creation date

May 17, 2022, 15:55 (UTC+05:30)

Last activity

14 minutes ago

ARN

arn:aws:iam::276384657722:role/instance_user_role

Maximum session duration

1 hour

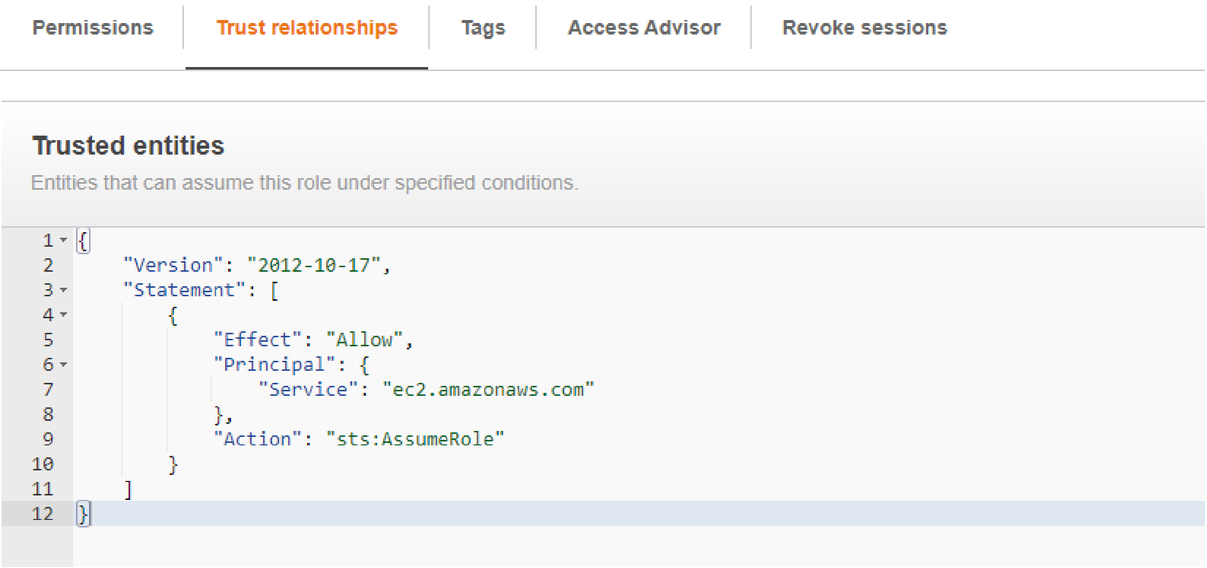
Permissions policies (2)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

□	Policy name	Type	Description
□	AmazonEC2RoleforSSM	AWS managed	This policy will soon be deprecated. Please use AmazonSSMManag
□	AmazonSSMManagedInstanceC...	AWS managed	The policy for Amazon EC2 Role to enable AWS Systems Manager s

Step 11: Click on Trust relationships to see the trust policy. A trust policy is a JSON policy document in which you define the principles that you trust to assume the role.

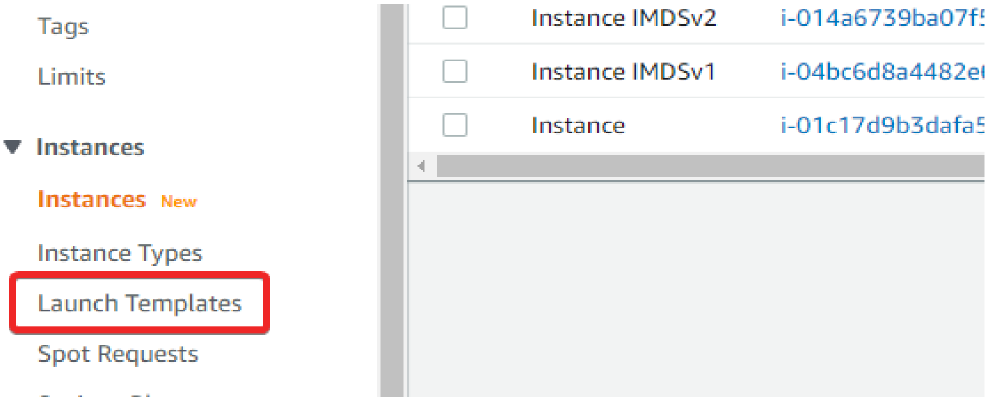


Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

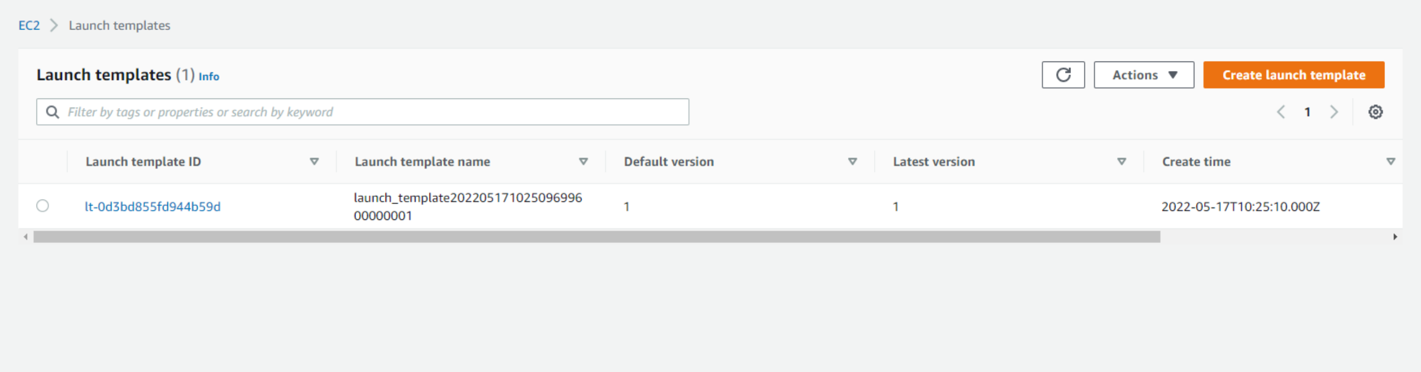
Step 12: Click on launch templates from the side panel.



□	Instance IMDSv2	i-014a6739ba07f5
□	Instance IMDSv1	i-04bc6d8a4482e(
□	Instance	i-01c17d9b3dafa5

Step 13: Click on launch template id to see the launch template details.

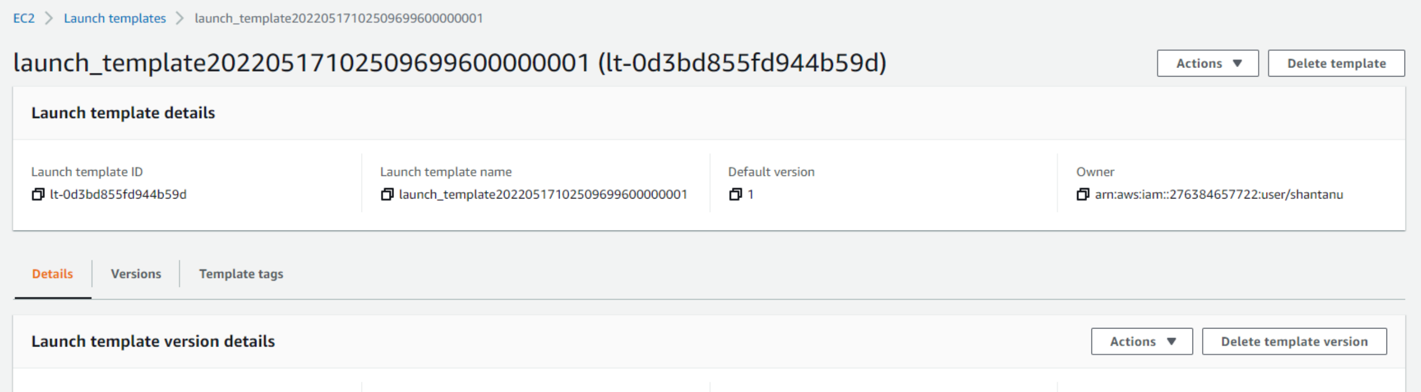
Launch templates are used to store launch parameters so that you do not have to specify them every time you launch an instance. When you launch an instance using the Amazon EC2 console, an AWS SDK, or a command-line tool, you can specify the launch template to use.



Launch templates (1) Info

	Launch template ID	Launch template name	Default version	Latest version	Create time
○	lt-0d3bd855fd944b59d	launch_template202205171025096996 00000001	1	1	2022-05-17T10:25:10.000Z

Here you can find the details of the launch template.



launch_template20220517102509699600000001 (lt-0d3bd855fd944b59d)

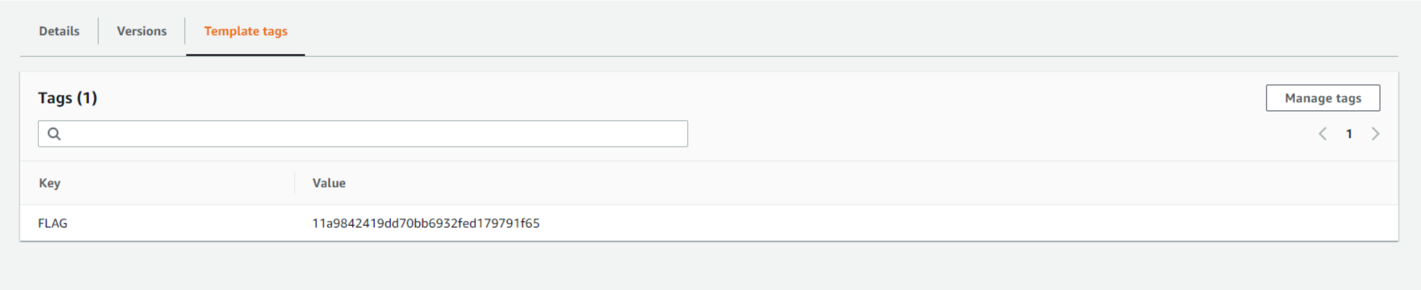
Launch template details

Launch template ID	Launch template name	Default version	Owner
lt-0d3bd855fd944b59d	launch_template20220517102509699600000001	1	arn:aws:iam::276384657722:user/shantanu

Launch template version details

Step 14: Click on Template tags in the launch template.

Got the flag from the launch template successfully.

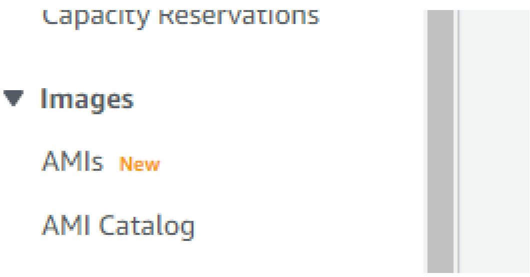


Tags (1)

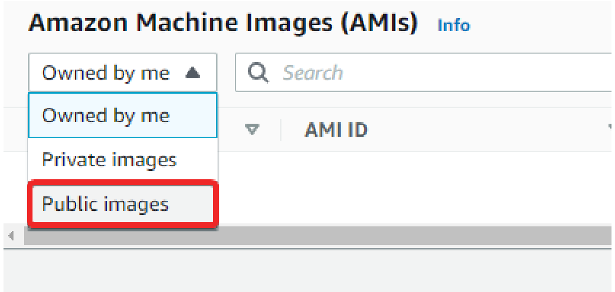
Key	Value
FLAG	11a9842419dd70bb6932fed179791f65

Flag: 11a9842419dd70bb6932fed179791f65

Step 15: Click on the AMIs from the side panel.

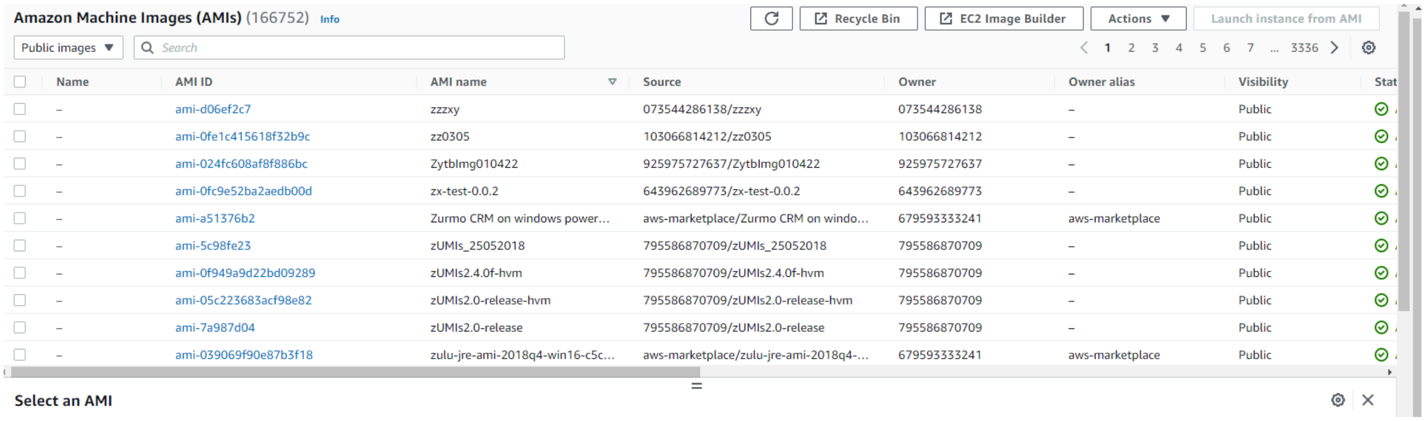


Step 16: Change “Owned by me” to “Public images” in the AMI section. This will list all the public images inside AWS in this section.



Step 17: Select any AMI from the list and click on AMI id.

AMI is a template that contains a software configuration. From an AMI, you launch an instance, which is a copy of the AMI running as a virtual server in the cloud. Your instances keep running until you stop, hibernate, terminate them, or until they fail. If an instance fails, you can launch a new one from the AMI.



□	Name	AMI ID	AMI name	Source	Owner	Owner alias	Visibility	Stat
□	–	ami-d06ef2c7	zzzxy	073544286138/zzzxy	073544286138	–	Public	✓
□	–	ami-0fe1c415618f32b9c	zz0305	103066814212/zz0305	103066814212	–	Public	✓
□	–	ami-024fc608af8f886bc	ZytbImg010422	925975727637/ZytbImg010422	925975727637	–	Public	✓
□	–	ami-0fc9e52ba2aedb00d	zx-test-0.0.2	643962689773/zx-test-0.0.2	643962689773	–	Public	✓
□	–	ami-a51376b2	Zurmo CRM on windows power...	aws-marketplace/Zurmo CRM on windo...	679593333241	aws-marketplace	Public	✓
□	–	ami-5c98fe23	zUMIs_25052018	795586870709/zUMIs_25052018	795586870709	–	Public	✓
□	–	ami-0f949a9d22bd09289	zUMIs2.4.0f-hvm	795586870709/zUMIs2.4.0f-hvm	795586870709	–	Public	✓
□	–	ami-05c223683acf98e82	zUMIs2.0-release-hvm	795586870709/zUMIs2.0-release-hvm	795586870709	–	Public	✓
□	–	ami-7a987d04	zUMIs2.0-release	795586870709/zUMIs2.0-release	795586870709	–	Public	✓
□	–	ami-039069f90e87b3f18	zulu-jre-ami-2018q4-win16-c5c...	aws-marketplace/zulu-jre-ami-2018q4-...	679593333241	aws-marketplace	Public	✓

Select an AMI

Here you can see the details of the AMI.

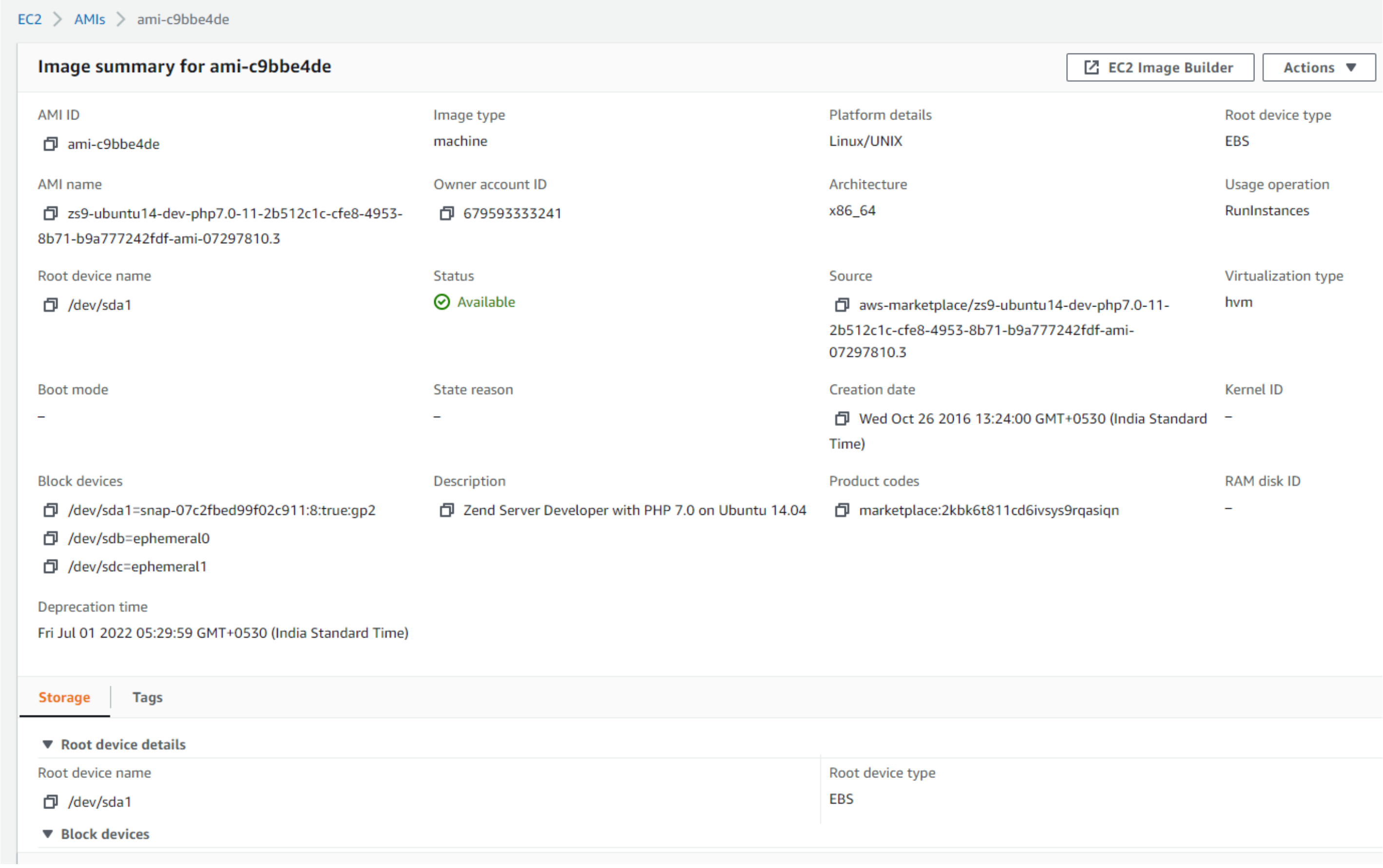


Image summary for ami-c9bbe4de

AMI ID: ami-c9bbe4de

Image type: machine

Platform details: Linux/UNIX

Root device type: EBS

AMI name: zs9-ubuntu14-dev-php7.0-11-2b512c1c-cfe8-4953-8b71-b9a777242fdf-ami-07297810.3

Owner account ID: 679593333241

Architecture: x86_64

Usage operation: RunInstances

Root device name: /dev/sda1

Status: Available

Source: aws-marketplace/zs9-ubuntu14-dev-php7.0-11-2b512c1c-cfe8-4953-8b71-b9a777242fdf-ami-07297810.3

Virtualization type: hvm

Boot mode: –

State reason: –

Creation date: Wed Oct 26 2016 13:24:00 GMT+0530 (India Standard Time)

Kernel ID: –

Block devices:
/dev/sda1=snap-07c2fbed99f02c911:8:true:gp2
/dev/sdb=ephemeral0
/dev/sdc=ephemeral1

Description: Zend Server Developer with PHP 7.0 on Ubuntu 14.04

Product codes: marketplace:2kbk6t811cd6ivsys9rqasiqn

RAM disk ID: –

Deprecation time: Fri Jul 01 2022 05:29:59 GMT+0530 (India Standard Time)

▼ Root device details

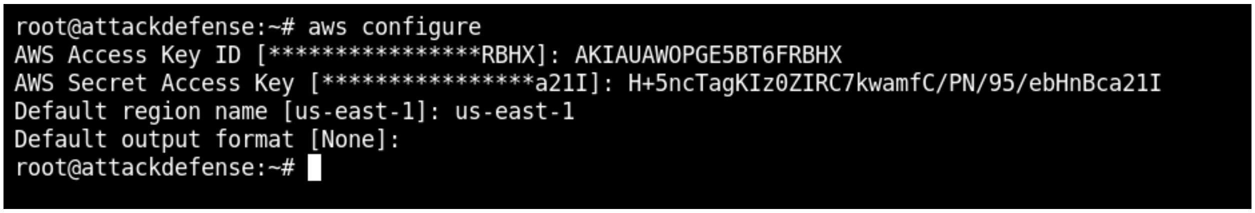
Root device name: /dev/sda1

Root device type: EBS

▼ Block devices

Step 18: Configure AWS CLI to use the provided credentials.

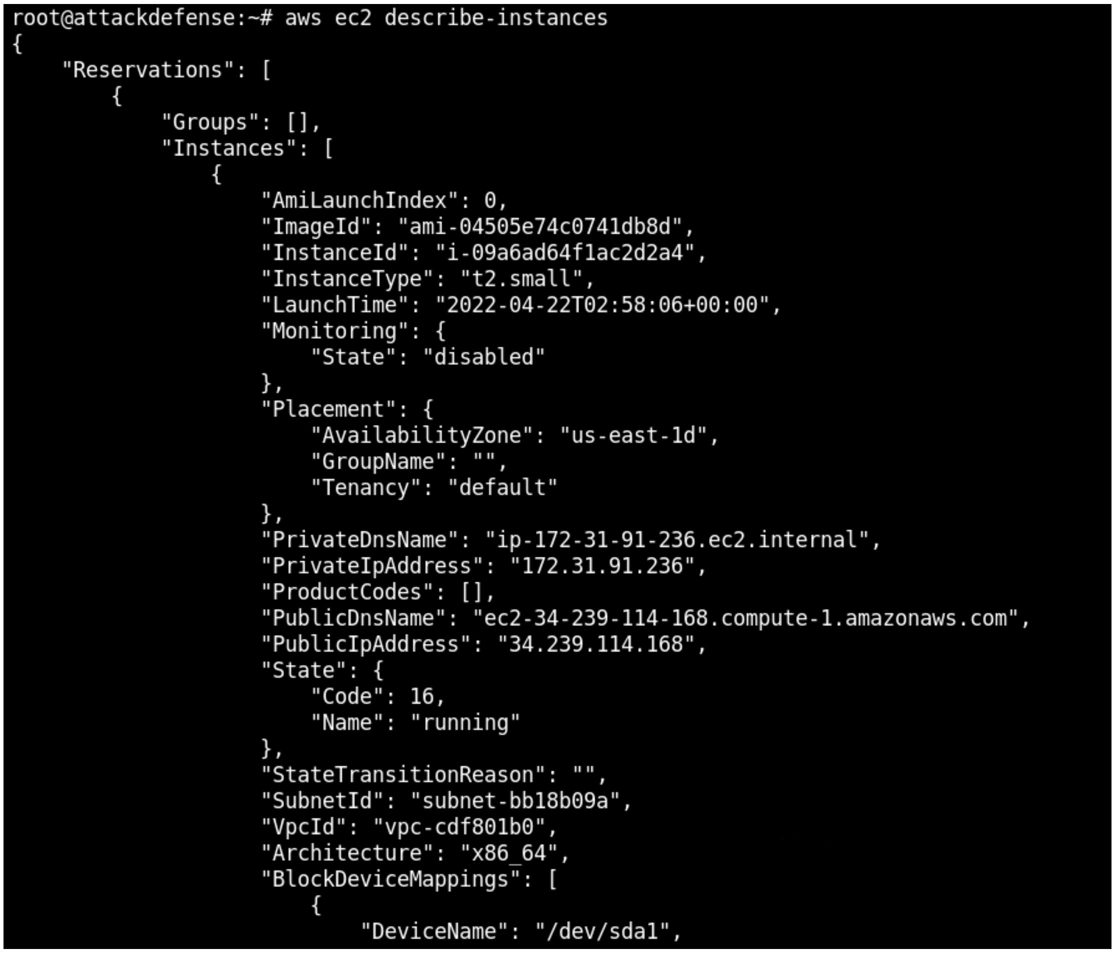
Command: aws configure



```
root@attackdefense:~# aws configure
AWS Access Key ID [****************RBHX]: AKIAUAWOPGE5BT6FRBHX
AWS Secret Access Key [****************a21I]: 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
Default region name [us-east-1]: us-east-1
Default output format [None]:
root@attackdefense:~# █
```

Step 19: Describe instances. The output includes information for all instances.

Command: aws ec2 describe-instances

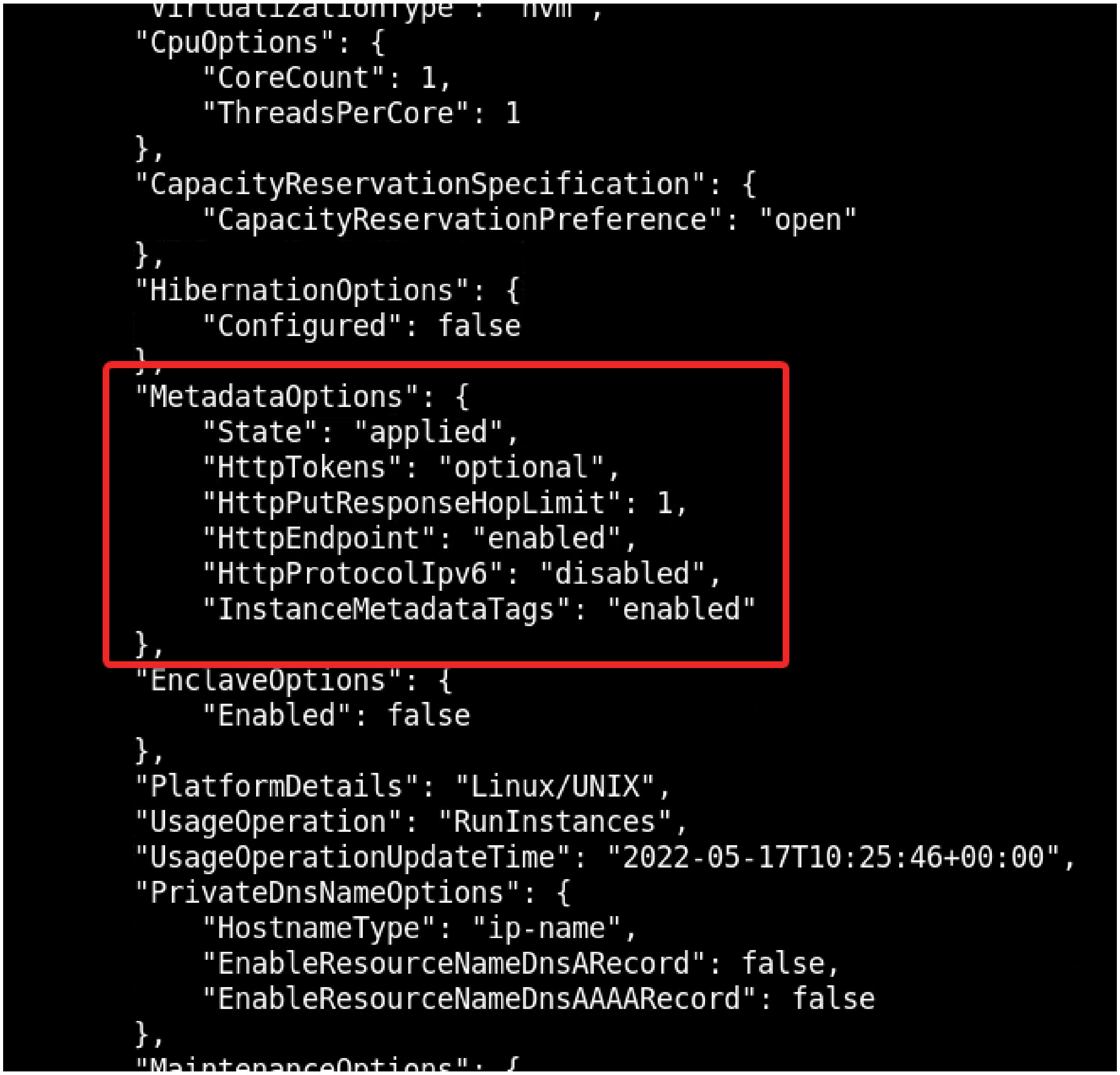


```
root@attackdefense:~# aws ec2 describe-instances
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-04505e74c0741db8d",
                    "InstanceId": "i-09a6ad64f1ac2d2a4",
                    "InstanceType": "t2.small",
                    "LaunchTime": "2022-04-22T02:58:06+00:00",
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "Placement": {
                        "AvailabilityZone": "us-east-1d",
                        "GroupName": "",
                        "Tenancy": "default"
                    },
                    "PrivateDnsName": "ip-172-31-91-236.ec2.internal",
                    "PrivateIpAddress": "172.31.91.236",
                    "ProductCodes": [],
                    "PublicDnsName": "ec2-34-239-114-168.compute-1.amazonaws.com",
                    "PublicIpAddress": "34.239.114.168",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "StateTransitionReason": "",
                    "SubnetId": "subnet-bb18b09a",
                    "VpcId": "vpc-cdf801b0",
                    "Architecture": "x86_64",
                    "BlockDeviceMappings": [
                        {
                            "DeviceName": "/dev/sda1",
```

Step 20: Describe the specified instance with IMDS v1.

Command: aws ec2 describe-instances --instance-ids i-04bc6d8a4482e6aa7

In this instance, HttpTokens is set to “optional” which means it is having metadata service version 1.

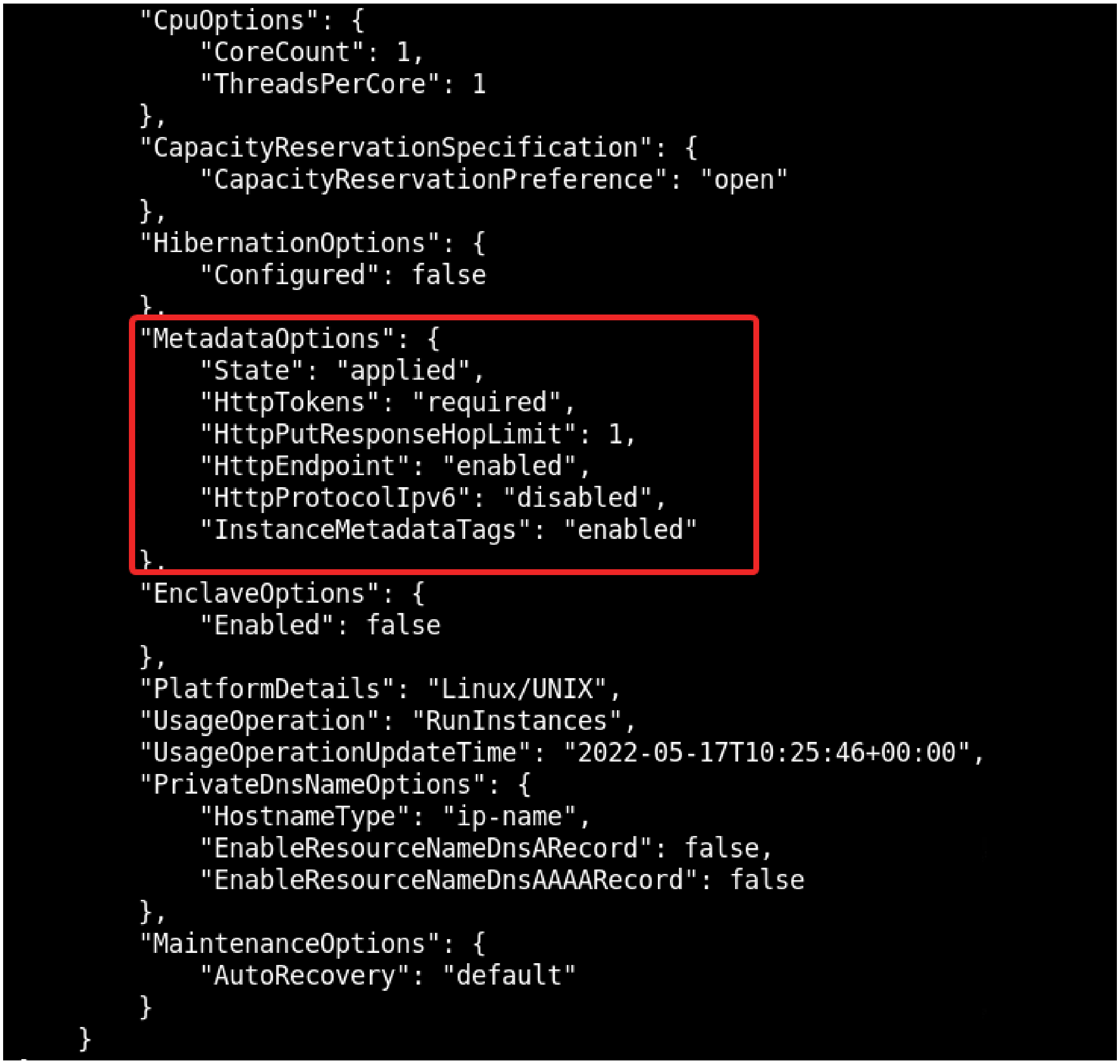


```
        "VirtualizationType": "hvm",
        "CpuOptions": {
            "CoreCount": 1,
            "ThreadsPerCore": 1
        },
        "CapacityReservationSpecification": {
            "CapacityReservationPreference": "open"
        },
        "HibernationOptions": {
            "Configured": false
        },
        "MetadataOptions": {
            "State": "applied",
            "HttpTokens": "optional",
            "HttpPutResponseHopLimit": 1,
            "HttpEndpoint": "enabled",
            "HttpProtocolIpv6": "disabled",
            "InstanceMetadataTags": "enabled"
        },
        "EnclaveOptions": {
            "Enabled": false
        },
        "PlatformDetails": "Linux/UNIX",
        "UsageOperation": "RunInstances",
        "UsageOperationUpdateTime": "2022-05-17T10:25:46+00:00",
        "PrivateDnsNameOptions": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
        },
        "MaintenanceOptions": {
```

Step 21: Describe the specified instance with IMDS v2.

Command: aws ec2 describe-instances --instance-ids i-014a6739ba07f505d

In this instance, HttpTokens is set to “required” which means it is having metadata service version 2.



```
        "CpuOptions": {
            "CoreCount": 1,
            "ThreadsPerCore": 1
        },
        "CapacityReservationSpecification": {
            "CapacityReservationPreference": "open"
        },
        "HibernationOptions": {
            "Configured": false
        },
        "MetadataOptions": {
            "State": "applied",
            "HttpTokens": "required",
            "HttpPutResponseHopLimit": 1,
            "HttpEndpoint": "enabled",
            "HttpProtocolIpv6": "disabled",
            "InstanceMetadataTags": "enabled"
        },
        "EnclaveOptions": {
            "Enabled": false
        },
        "PlatformDetails": "Linux/UNIX",
        "UsageOperation": "RunInstances",
        "UsageOperationUpdateTime": "2022-05-17T10:25:46+00:00",
        "PrivateDnsNameOptions": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
        },
        "MaintenanceOptions": {
            "AutoRecovery": "default"
        }
    }
```

References:

1. AWS EC2 documentation (https://docs.aws.amazon.com/ec2/index.html)
2. AWS CLI (https://docs.aws.amazon.com/cli/latest/reference/)