

The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "TOOL BOX", "PENTESTING", "RED TEAM", "HACKER", "TRAINING", "ACCESS POINT", "PATV", "WORLD-CLASS TRAINERS", "TEAM LABS", "PENTESTER ACADEMY", "ATTACK DEFENSE LABS", "COURSES", "ACCESS POINT", "PENTESTER", "TOOL BOX", "WORLD-CLASS TRAINERS", "TRAINING", "PENTESTER ACADEMY", "ATTACK DEFENSE LABS", "COURSES", "ACCESS POINT", "PENTESTER", "TOOL BOX", "WORLD-CLASS TRAINERS", "TRAINING". The words "ATTACK" and "DEFENSE" are the largest and are colored red and dark blue respectively, while the others are in shades of gray. Below the word cloud, the text "by PentesterAcademy" is written in a black, sans-serif font.

Name	EC2 Unencrypted EBS disks
URL	https://attackdefense.com/challengedetails?cid=2452
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:

Step 1: Click on the lab link button to get access credentials. Login to aws console.

Access Credentials to your AWS lab Account

Login URL	https://854627651693.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	mark
Password	Ad4V8cMTkeYRA5a3

Step 2: Navigate to the EC2 dashboard and click on instances.

New EC2 Experience
Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances **New**

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances **New**

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs **New**

AMI Catalog

Resources

EC2 Global view

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

Instances (running)	1	Dedicated Hosts	0	Elastic IPs	0
Instances	1	Key pairs	0	Load balancers	0
Placement groups	0	Security groups	2	Snapshots	0
Volumes	2				

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

Launch instance

To get started, launch an Amazon EC2 Instance, which is a virtual server in the cloud.

Launch instance

Migrate a server

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

Refresh

AWS Health Dashboard

Region
US East (N. Virginia)

Status
 This service is operating normally

Zones

Step 3: Click on instance id and find the storage details.

New EC2 Experience
Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances **New**

Instance Types

Launch Templates

Instances (1) Info

Search

Refresh

Connect

Instance state

Actions

Launch instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
	-	i-04ba122db82b92ac3	Running	t2.small	2/2 checks passed	No alarms	us-east-1d	ec2-44-203-4-197.com...	44.203.4.197	-

Step 4: Click on storage.

Details | Security | Networking | **Storage** | Status checks | Monitoring | Tags

▼ Root device details

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

▼ Block devices

Filter block devices

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termination
vol-0103b344ceb3cbe1c	/dev/xvda	8	Attached	Fri Jul 29 2022 03:16:10 GM...	No	-	Yes
vol-027bb486afe93adab	/dev/xvdf	4	Attached	Fri Jul 29 2022 03:16:10 GM...	No	-	No

▼ Recent root volume replacement tasks

Filter tasks

Task ID	Task state	Start time	Completion time	Tags
No recent replace root volume tasks				

Replace root volume

Step 5: Try to connect with the instance.

EC2 > Instances > i-04ba122db82b92ac3

Instance summary for i-04ba122db82b92ac3 Info

Updated less than a minute ago

Connect Instance state Actions

<p>Instance ID</p> <p>i-04ba122db82b92ac3</p> <p>IPv6 address</p> <p>-</p> <p>Hostname type</p> <p>IP name: ip-10-0-0-164.ec2.internal</p> <p>Answer private resource DNS name</p> <p>-</p> <p>Auto-assigned IP address</p> <p>44.203.4.197 [Public IP]</p> <p>IAM Role</p> <p>-</p>	<p>Public IPv4 address</p> <p>44.203.4.197 open address</p> <p>Instance state</p> <p>Running</p> <p>Private IP DNS name (IPv4 only)</p> <p>ip-10-0-0-164.ec2.internal</p> <p>Instance type</p> <p>t2.small</p> <p>VPC ID</p> <p>vpc-0adbcdd854447502 (vpc-network)</p> <p>Subnet ID</p> <p>subnet-0a21b6b146ebadc36 (subnet)</p>	<p>Private IPv4 addresses</p> <p>10.0.0.164</p> <p>Public IPv4 DNS</p> <p>ec2-44-203-4-197.compute-1.amazonaws.com open address</p> <p>Elastic IP addresses</p> <p>-</p> <p>AWS Compute Optimizer finding</p> <p>User: am:aws:iam::854627651693:user/mark is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * with an explicit deny in a service control policy</p> <p>Retry</p> <p>Auto Scaling Group name</p> <p>-</p>
--	--	---

Try to connect instance with EC2 Instance connect.

EC2 > Instances > i-04ba122db82b92ac3 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-04ba122db82b92ac3 using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

 i-04ba122db82b92ac3

Public IP address

 44.203.4.197

User name

root

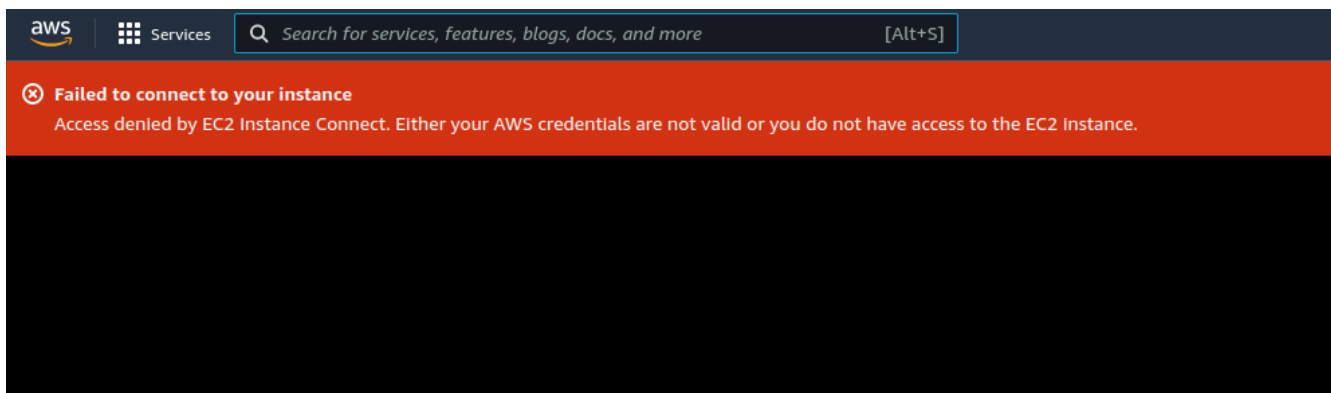
Connect using a custom user name, or use the default user name root for the AMI used to launch the instance.

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.

Cancel

Connect

User does not have access to the instance.



Key pair is not created. So the connection to EC2 instance with the SSH client is not possible.

Connect to instance [Info](#)


Connect to your instance i-04ba122db82b92ac3 using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console






No associated key pair

This instance is not associated with a key pair. Without a key pair, you can't connect to the instance through SSH.


You can connect using EC2 Instance Connect with just a valid username. You can connect using Session Manager if you have been granted the necessary permissions.


Instance ID

 [i-04ba122db82b92ac3](#)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is `id_rsa`
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 `chmod 400 id_rsa`
4. Connect to your instance using its Public DNS:
 `ec2-44-203-4-197.compute-1.amazonaws.com`

Example:

 `ssh -i "id_rsa" root@ec2-44-203-4-197.compute-1.amazonaws.com`



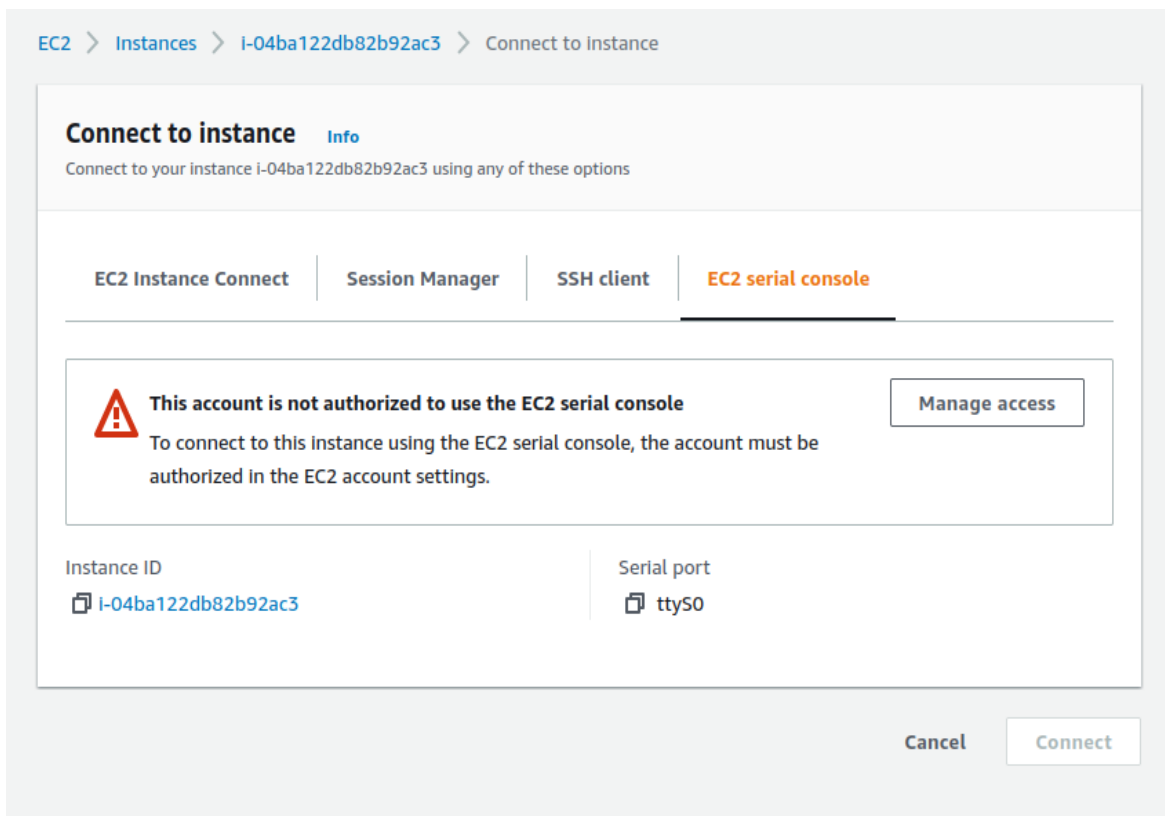
Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

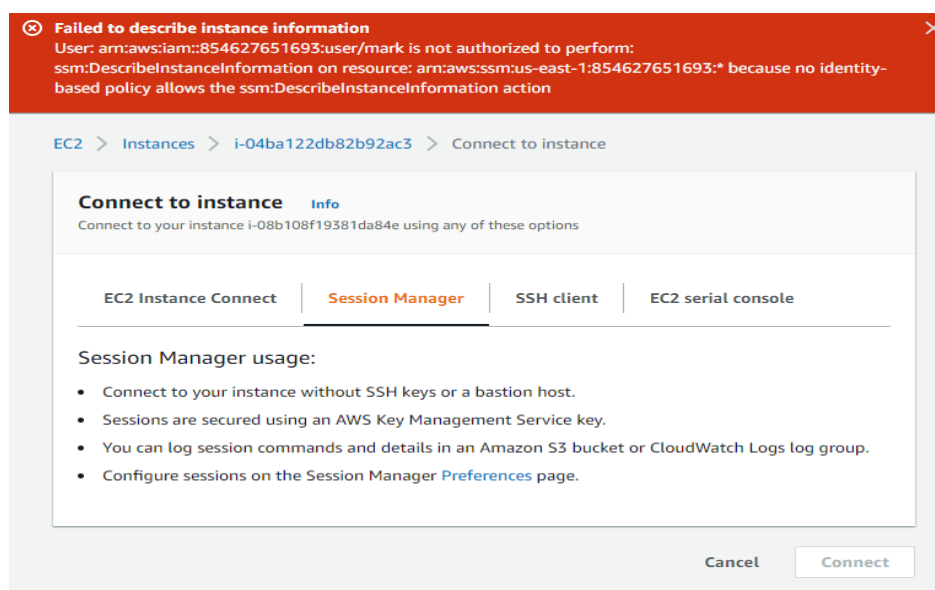
EC2 serial console is not authorized to connect with the instance.

©PentesterAcademy.com

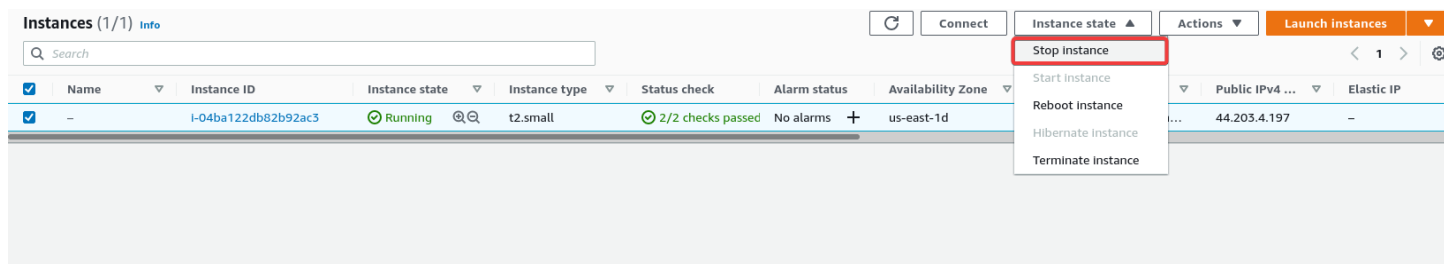
www.attackdefense.com



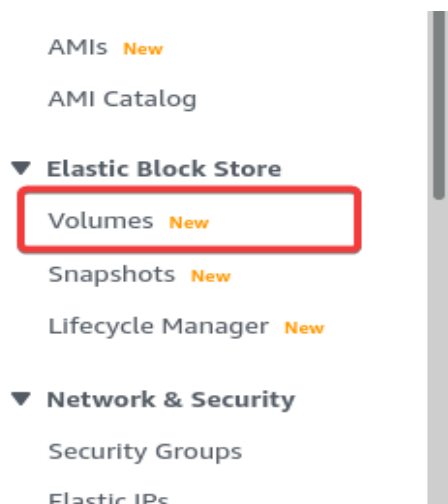
SSM is not authorized to connect with the instance. So this states that there is no access to the instance. Thus we cannot check the data inside volumes.



Step 6: Stop the running instance.



Step 7: Navigate to volumes.



Step 8: Detach the additionally attached volume from the instance.

Volumes (1/2)

Search

	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created
<input checked="" type="checkbox"/>	-	vol-027bb486afe93adab	gp2	4 GiB	100	-	snap-0347a7e...	2022/07/29 03:16 GMT-4
<input type="checkbox"/>	-	vol-0103b344ceb3cbe1c	gp2	8 GiB	100	-	snap-07a47aa...	2022/07/29 03:16 GMT-4

Actions

- Modify volume
- Create snapshot
- Create snapshot lifecycle policy
- Delete volume
- Attach volume
- Detach volume**
- Force detach volume
- Manage auto-enabled I/O
- Manage tags

Step 9: Click on detach.

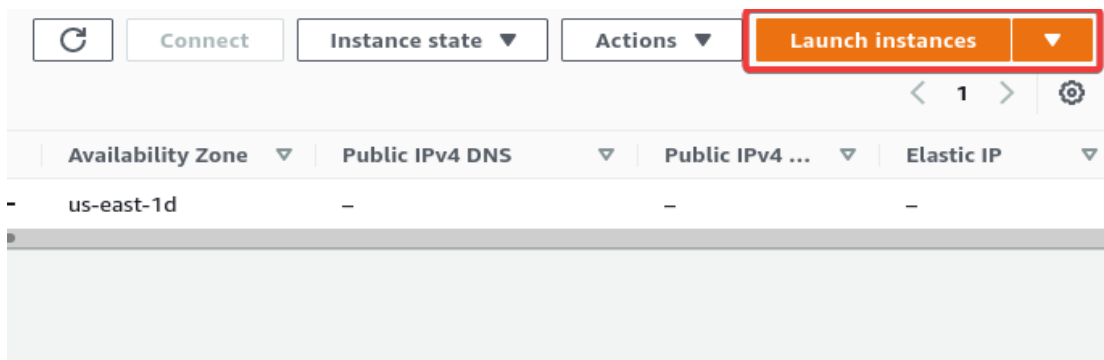
Detach vol-027bb486afe93adab?

After you detach a volume, you might still be charged for volume storage. If you no longer need the volume, delete it to stop incurring charges.

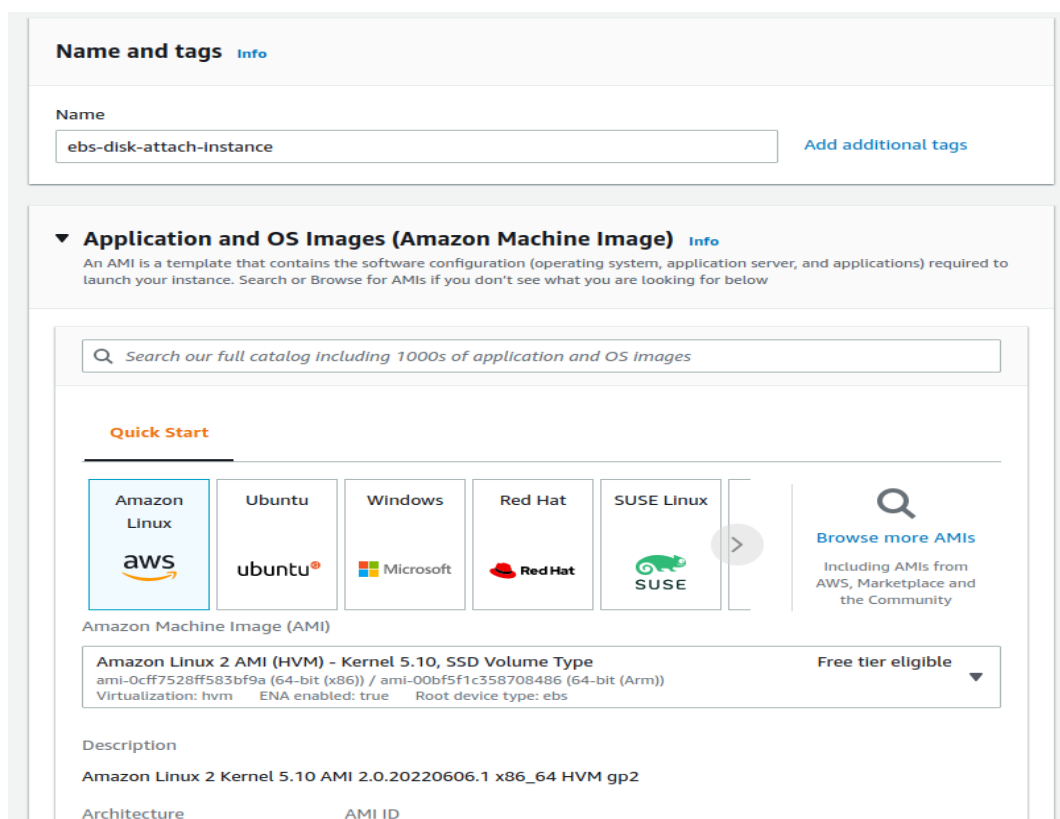
Are you sure that you want to detach volume vol-027bb486afe93adab?

Cancel Detach

Step 10: Now create a new instance and attach the detached volume and retrieve the data from it. Navigate back to the instance and click on launch instance.



Step 11: Set a name and select amazon Linux as AMI.



Step 12: Set instance type to t2.micro and proceed without key pair.

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible

[Compare instance types](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Proceed without a key pair (Not recommended)

Default value ▼

[Create new key pair](#)

Step 13: Select "SSHAccess" as the security group.

▼ Network settings [Get guidance](#)

Edit

Network [Info](#)

vpc-0adbcedd854447502 | vpc-network

Subnet [Info](#)

subnet-0a21b6b146ebadc36 | subnet

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups [Info](#)

Select security groups ▼

SSHAccess sg-0867f0bab3eada4ee ✕

VPC: vpc-0adbcedd854447502

[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Step 14: Leave other settings as default and click on Launch instance.

©PentesterAcademy.com

www.attackdefense.com

EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

ebs-disk-attach-Instance

Add additional tags

▼ 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

Quick Start

Amazon Linux

aws

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

▼ Summary

Number of Instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0cff7528ff583bf9a

Virtual server type (instance type)

t2.micro

Firewall (security group)

SSHAcess

Storage (volumes)

1 volume(s) - 8 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, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the Internet.

Cancel

Launch instance

Successfully initiated the launch of instance. Now click on View all instances.

EC2 > Instances > Launch an instance

✓ Success

Successfully initiated launch of instance (i-0e552306371326790)

▶ Launch log

Next Steps

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier)

How to connect to your instance

Your instance is launching and it might be a few minutes until it is in the running state, when it will be ready for you to use

Click View Instances to monitor your instance's status. Once your instance is in the 'running' state, you can connect to it from the Instances screen. Find out how to connect to your instance

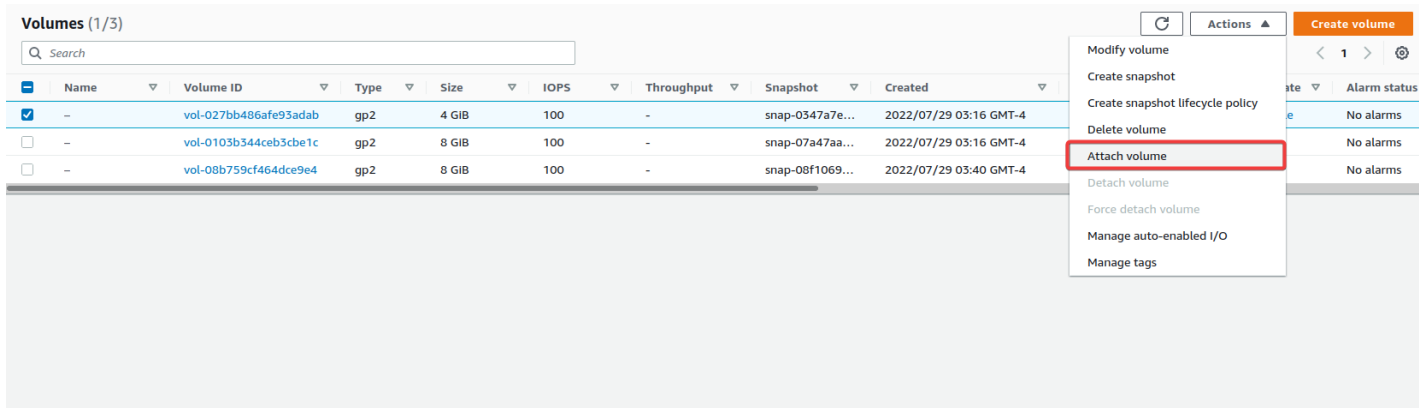
View more resources to get you started

View all instances

©PentesterAcademy.com

www.attackdefense.com

Step 15: Navigate back to volumes and select the detached volume. Click on attach from the actions drop-down.



Volumes (1/3)

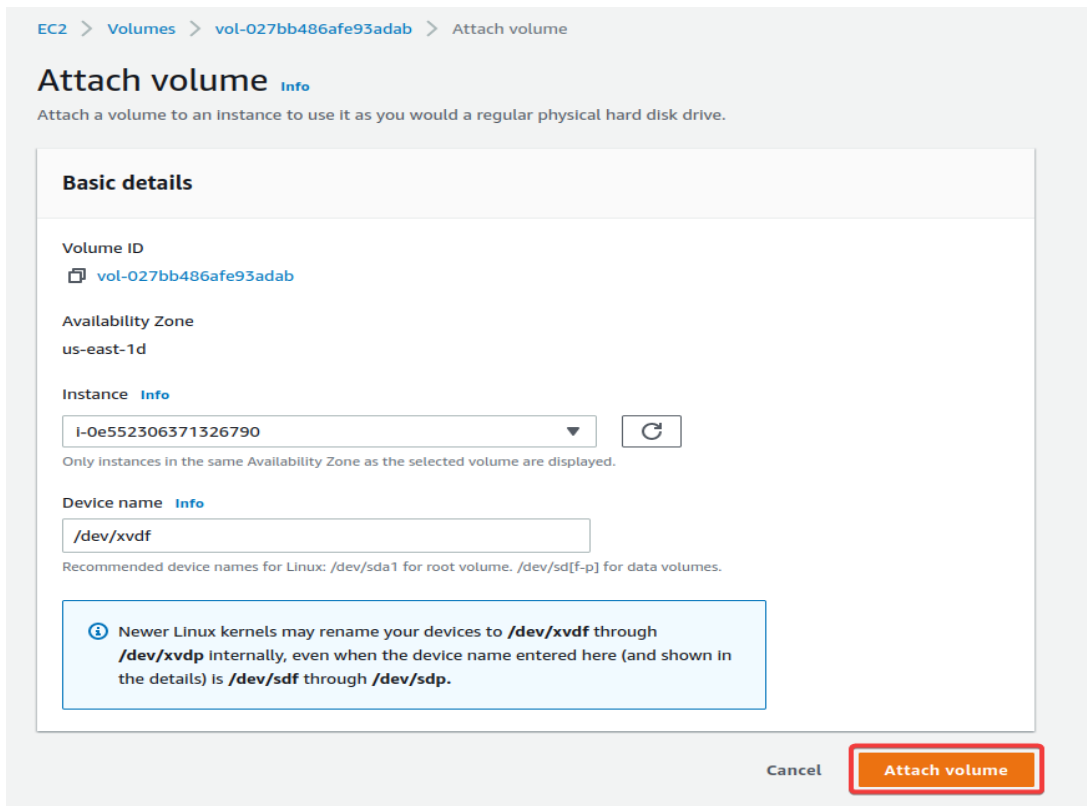
Search

	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created
<input checked="" type="checkbox"/>	-	vol-027bb486afe93adab	gp2	4 GiB	100	-	snap-0347a7e...	2022/07/29 03:16 GMT-4
<input type="checkbox"/>	-	vol-0103b344ceb3cbe1c	gp2	8 GiB	100	-	snap-07a47aa...	2022/07/29 03:16 GMT-4
<input type="checkbox"/>	-	vol-08b759cf464dce9e4	gp2	8 GiB	100	-	snap-08f1069...	2022/07/29 03:40 GMT-4

Actions

- Modify volume
- Create snapshot
- Create snapshot lifecycle policy
- Delete volume
- Attach volume**
- Detach volume
- Force detach volume
- Manage auto-enabled I/O
- Manage tags

Step 16: Attach the volume with the newly created instance.



EC2 > Volumes > vol-027bb486afe93adab > Attach volume

Attach volume [Info](#)

Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID
 vol-027bb486afe93adab

Availability Zone
us-east-1d

Instance [Info](#)
I-Oe552306371326790

Only instances in the same Availability Zone as the selected volume are displayed.

Device name [Info](#)
/dev/xvdf

Recommended device names for Linux: /dev/sda1 for root volume. /dev/sd[f-p] for data volumes.

Newer Linux kernels may rename your devices to **/dev/xvdf** through **/dev/xvdp** internally, even when the device name entered here (and shown in the details) is **/dev/sdf** through **/dev/sdp**.

Cancel **Attach volume**

Now the volumes will list in the storage section of EC2 instance.

Details | Security | Networking | **Storage** | Status checks | Monitoring | Tags

▼ Root device details

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

▼ Block devices

Filter block devices

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termination
vol-08b759cf464dce9e4	/dev/xvda	8	Attached	Fri Jul 29 2022 03:40:30 GM...	No	-	Yes
vol-027bb486afe93adab	/dev/xvdf	4	Attached	Fri Jul 29 2022 03:42:38 GM...	No	-	No

▼ Recent root volume replacement tasks

Filter tasks

Task ID	Task state	Start time	Completion time	Tags
No recent replace root volume tasks				

Replace root volume

Step 17: Navigate back to instances and try to connect with the created instance using EC2 instance connect.

EC2 > Instances > i-0e552306371326790

Instance summary for i-0e552306371326790 (ebs-disk-attach-instance) Info

Updated less than a minute ago

Connect Instance state Actions

Instance ID i-0e552306371326790 (ebs-disk-attach-instance)	Public IPv4 address 3.80.194.134 open address	Private IPv4 addresses 10.0.0.241
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-3-80-194-134.compute-1.amazonaws.com open address
Hostname type IP name: ip-10-0-0-241.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-0-241.ec2.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding User: arn:aws:iam::854627651693:user/mark is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * with an explicit deny in a service control policy Retry
Auto-assigned IP address 3.80.194.134 [Public IP]	VPC ID vpc-0adbcdd854447502 (vpc-network)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-0a21b6b146ebad36 (subnet)	

Details | Security | Networking | **Storage** | Status checks | Monitoring | Tags

Click on connect.

EC2 > Instances > i-0e552306371326790 > Connect to instance

Connect to instance

[Info](#)

Connect to your instance i-0e552306371326790 (ebs-disk-attach-instance) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

 i-0e552306371326790 (ebs-disk-attach-instance)


Public IP address

 3.80.194.134

User name

ec2-user

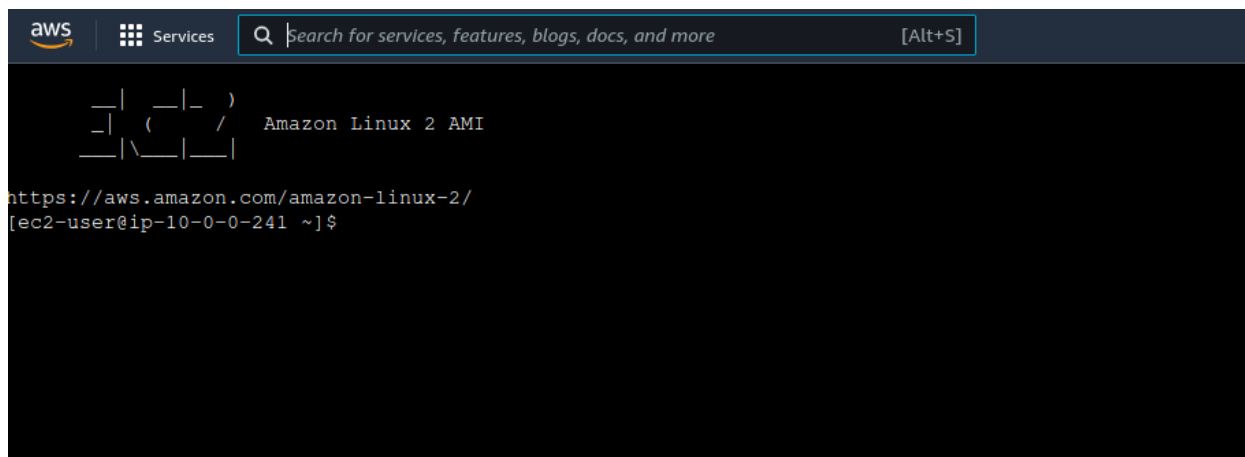
Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

 **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.

Cancel

Connect

Successfully connected to the instance.



Step 18: List the available volumes.

Command: lsblk



Step 19: Check the file system of the attached disk.

Command: sudo file -s /dev/xvdf


```
[ec2-user@ip-10-0-0-241 ~]$ sudo file -s /dev/xvdf
/dev/xvdf: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
[ec2-user@ip-10-0-0-241 ~]$
```

Step 20: Create a mount point directory for the volume and mount the volume at that directory. Now this will mount the data present inside the volume to the data folder in the root.


Command: `sudo mkdir /data`
`sudo mount /dev/xvdf /data`

```
[ec2-user@ip-10-0-0-241 ~]$ sudo mkdir /data
[ec2-user@ip-10-0-0-241 ~]$ sudo mount /dev/xvdf /data
[ec2-user@ip-10-0-0-241 ~]$
```

Step 21: Retrieve the flag.

Command: `ls /data`
`cat /data/flag`

```
[ec2-user@ip-10-0-0-241 ~]$ ls /data
flag
[ec2-user@ip-10-0-0-241 ~]$ cat /data/flag
1a0c77264e3e32c9e5cd777cd55f8c83
[ec2-user@ip-10-0-0-241 ~]$
```



Flag: 1a0c77264e3e32c9e5cd777cd55f8c83

References:

1. AWS EC2 documentation (<https://docs.aws.amazon.com/ec2/index.html>)