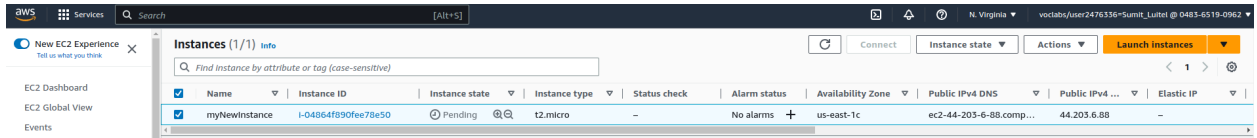
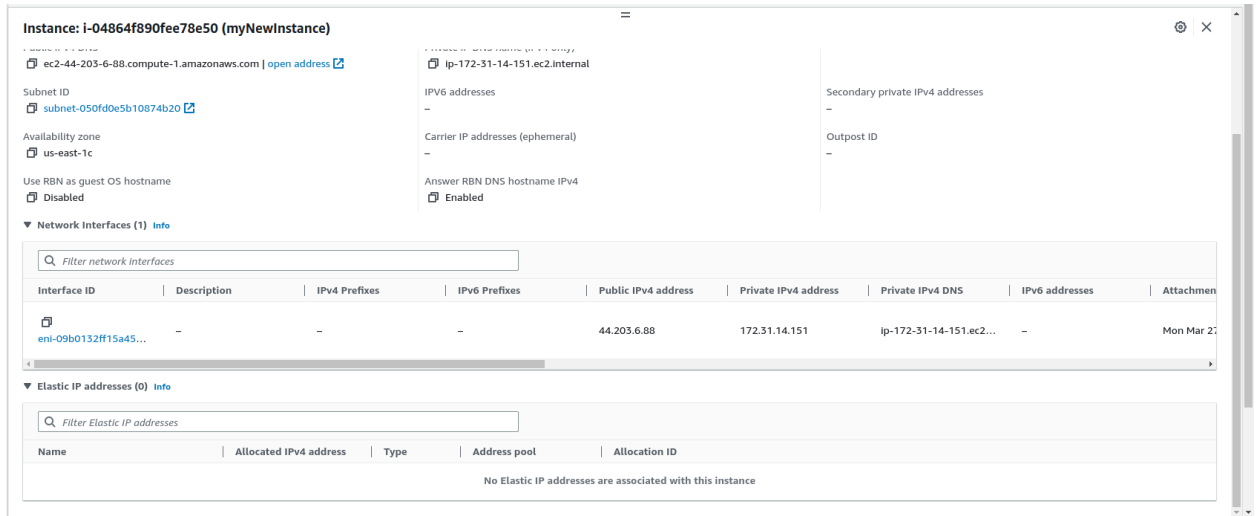


Lab 2:

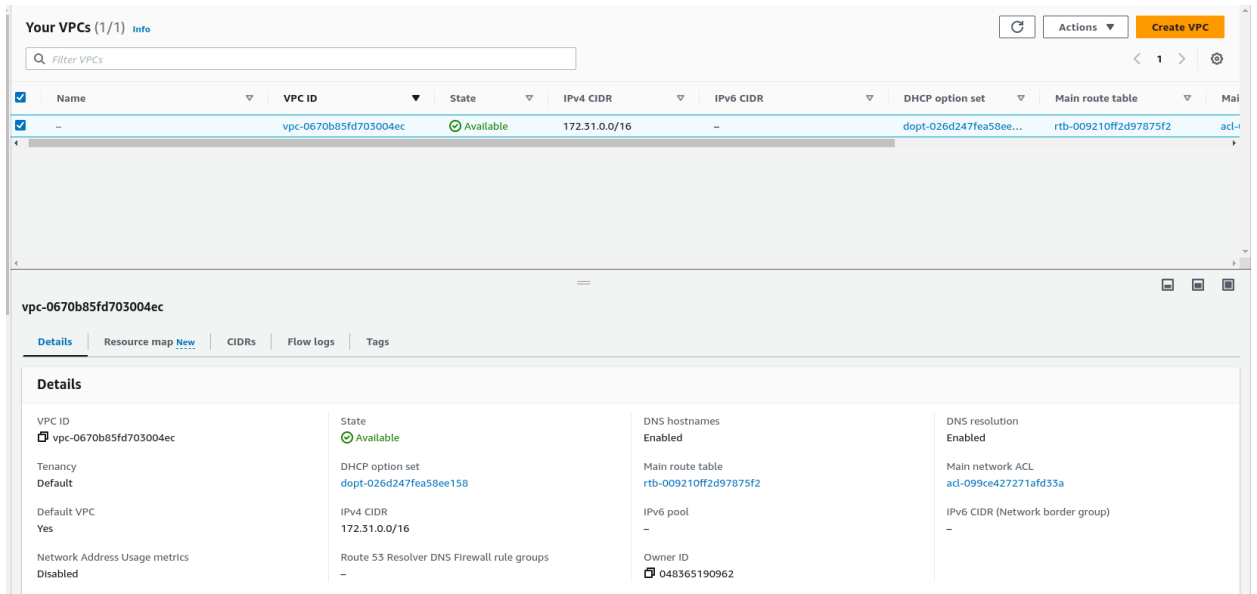
1. Launch a new instance in the default VPC in a particular subnet(AZ).
Note the different network resources attached to it.



The screenshot shows the AWS Management Console 'Instances' page. The instance 'myNewInstance' (ID: i-04864f890fee78e50) is in a 'Pending' state, running on a t2.micro instance type in the us-east-1c Availability Zone. It is associated with the ec2-44-203-6-88.compute-1 Public IPv4 DNS, the ec2-44-203-6-88.compute-1 Public IPv4 address, and the ec2-44-203-6-88.compute-1 Elastic IP address.

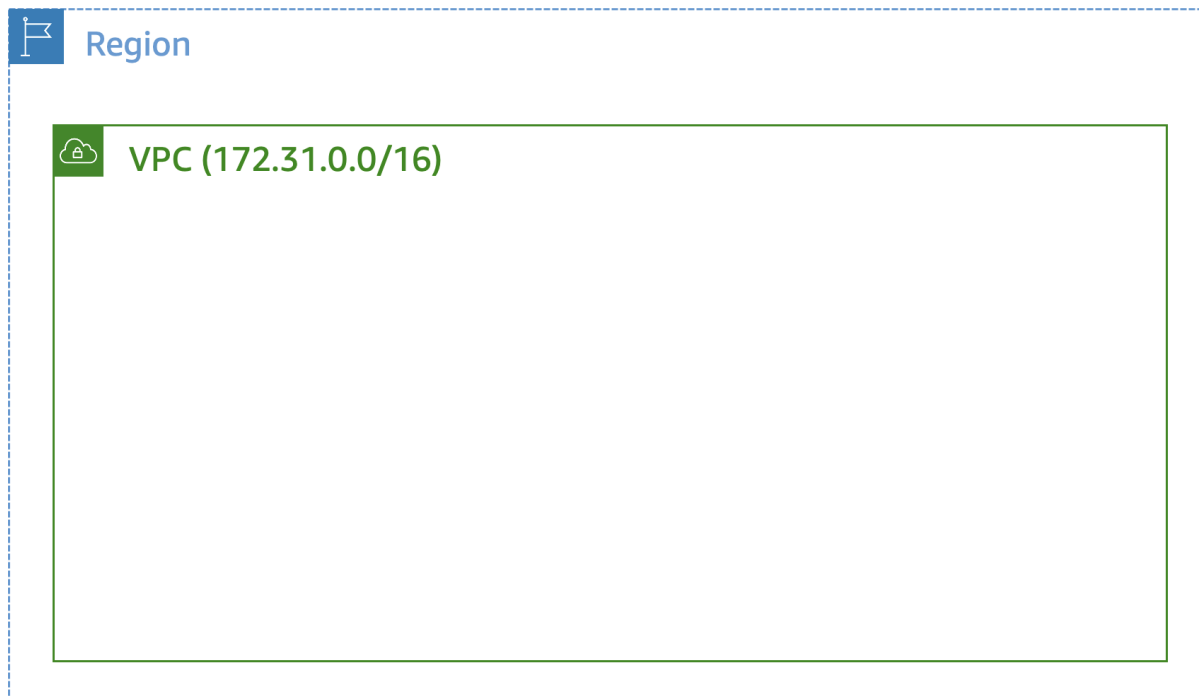


The screenshot shows the details of the instance 'myNewInstance'. The instance is associated with the subnet-050fd0e5b10874b20 Subnet ID, the us-east-1c Availability zone, and the ec2-44-203-6-88.compute-1 Public IPv4 DNS. The instance is associated with the ec2-44-203-6-88.compute-1 Public IPv4 address, the ec2-44-203-6-88.compute-1 Elastic IP address, and the ec2-44-203-6-88.compute-1 Elastic IP address.



The screenshot shows the details of the VPC 'vpc-0670b85fd703004ec'. The VPC is in an 'Available' state, with a VPC ID of vpc-0670b85fd703004ec, a VPC CIDR of 172.31.0.0/16, and a VPC IPv6 CIDR of -. The VPC is associated with the dopt-026d247fe58ee158 DHCP option set, the rtb-009210ff2d97875f2 Main route table, and the acl-099ce427271afd33a Main network ACL.

VPC deployed in AWS region.



CIDR - Classless Inter-Domain Routing (CIDR) is a range of IP addresses a network uses. A CIDR address looks like a normal IP address, except that it ends with a slash followed by a number. The number after the slash represents the number of addresses in the range. Example: **172.31.0.0/16**

This CIDR range includes all addresses from **172.31.0.0** through **172.31.255.255**, which is a total of **65,536 addresses**.

Public Subnet - A subnet is a subrange of IP addresses in the VPC. AWS resources can be launched into a specified subnet. Use a **public subnet** for resources that must be connected to the internet, and use a **private subnet** for resources that must remain isolated from the internet.

All of the default subnets are associated with the same VPC

Security group - A *security group* controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

VPC's internet gateway - An *internet gateway* allows communication between the resources in a VPC and the internet. Status - Attached meaning, Internet Gateway exists and that it is attached it to the default VPC.

Routes Table - Route table are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table. A subnet can be associated with only one route table at a time, but we can associate multiple subnets with the same route table.

2. Launch 3 instances, 2 in the same region and 1 in another region. Try to access the instances from the other using public and private IPS and note down which connections were successful.

(Hint: You can connect using http – by launching a webserver, or you can ping one server from another - by allowing ICMP protocol and executing ping command)

The screenshot shows the AWS Management Console interface for launching an EC2 instance. The breadcrumb navigation indicates the path: EC2 > Instances > Launch an instance. The main heading is "Launch an instance" with an "Info" link. Below this, a sub-header "Name and tags" contains a text input field with "Practice-Demo1" and an "Add additional tags" button. The "Application and OS Images (Amazon Machine Image)" section features a search bar and a "Quick Start" section with a carousel of AMI categories: Amazon Linux, macOS, Ubuntu (selected), Windows, Red Hat, and S. Below the carousel, the selected AMI is "Ubuntu Server 22.04 LTS (HVM), SSD Volume Type" with its ID and a "Free tier eligible" label. A description at the bottom states: "Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-02-08". On the right, the "Summary" section lists configuration details: "Number of Instances" (1), "Software Image (AMI)" (Canonical, Ubuntu, 22.04 LTS), "Virtual server type (Instance type)" (t2.micro), "Firewall (security group)" (New security group), and "Storage (volumes)" (1 volume(s) - 8 GiB). A "Free tier" notification box is also present. At the bottom right, there are "Cancel" and "Launch instance" buttons.

Services

Search

[Alt+S]

Connect

Instance state

Actions

Launch instances

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Instances (1) Info

Find instance by attribute or tag (case-sensitive)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	Practice-Demo1	i-0238f12b659ff8247	Running	t2.micro	-	No alarms +	us-east-1c	ec2-18-207-108-68.co...	18.207.108.68	-

Select an instance

Services

Search

[Alt+S]

Connect

Instance state

Actions

Launch instances

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Instances (1/1) Info

Instance sta

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input checked="" type="checkbox"/>	Practice-Demo1	i-0238f12b659ff8247	Running	t2.micro	-	No alarms +	us-east-1c	ec2-18-207-108-68.co...	18.207.108.68	-

Instance: i-0238f12b659ff8247 (Practice-Demo1)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

Instance summary Info

Instance ID

i-0238f12b659ff8247 (Practice-Demo1)

IPv6 address

-

Hostname type

IP name: ip-172-31-8-147.ec2.internal

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

18.207.108.68 [Public IP]

Public IPv4 address

18.207.108.68 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-172-31-8-147.ec2.internal

Instance type

t2.micro

VPC ID

vpc-0dc9737115ea6cf4e

Private IPv4 addresses

172.31.8.147

Public IPv4 DNS

ec2-18-207-108-68.compute-1.amazonaws.com | open address

Elastic IP addresses

-

AWS Compute Optimizer finding

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

Created 3 instances in the same region (N.virginia)

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Instances (1/3)

Instance sta

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	Practice-Demo1	I-0238f12b659ff8247	Running	t2.micro	2/2 checks passed	No alarms	us-east-1c	ec2-18-207-108-68.co...	18.207.108.68	-
<input checked="" type="checkbox"/>	Practice-Demo3	I-065c2a7a41b0a80d9	Running	t2.micro	-	No alarms	us-east-1a	ec2-3-80-221-98.comp...	3.80.221.98	-
<input type="checkbox"/>	Practice-Demo2	I-0ceb1bb761c4e191a	Running	t2.micro	Initializing	No alarms	us-east-1c	ec2-3-235-169-27.com...	3.235.169.27	-

Instance: i-065c2a7a41b0a80d9 (Practice-Demo3)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

Instance summary

Instance ID

I-065c2a7a41b0a80d9 (Practice-Demo3)

IPv6 address

-

Hostname type

IP name: ip-172-31-31-30.ec2.internal

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

3.80.221.98 [Public IP]

Public IPv4 address

3.80.221.98 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-172-31-31-30.ec2.internal

Instance type

t2.micro

VPC ID

vpc-0dc9737115ea6cf4e

Private IPv4 addresses

172.31.31.30

Public IPv4 DNS

ec2-3-80-221-98.compute-1.amazonaws.com | open address

Elastic IP addresses

-

AWS Compute Optimizer finding

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

EC2 > Instances > I-0238f12b659ff8247 > Connect to instance

Connect to instance

Connect to your instance I-0238f12b659ff8247 (Practice-Demo1) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

I-0238f12b659ff8247 (Practice-Demo1)

Public IP address

18.207.108.68

User name

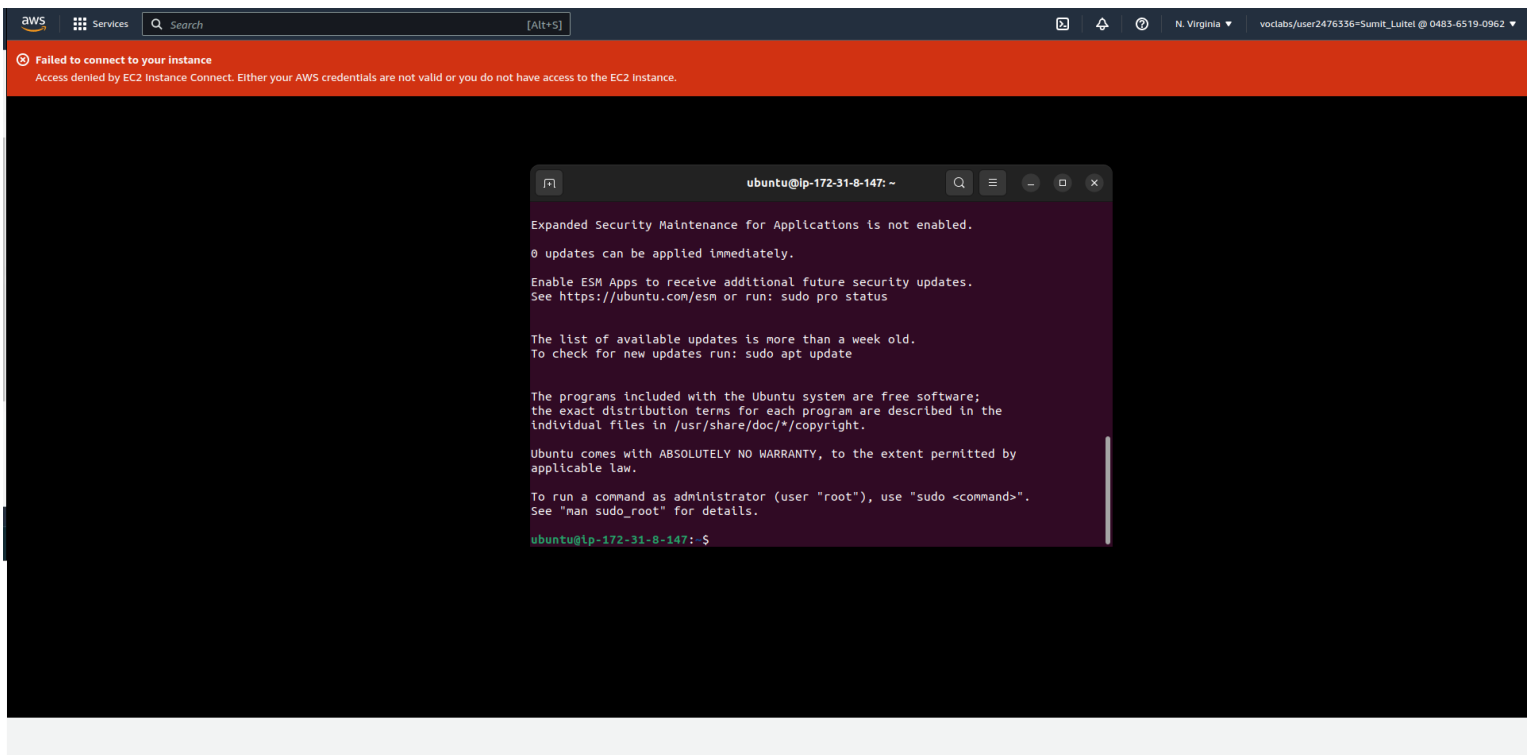
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ubuntu.

ubuntu

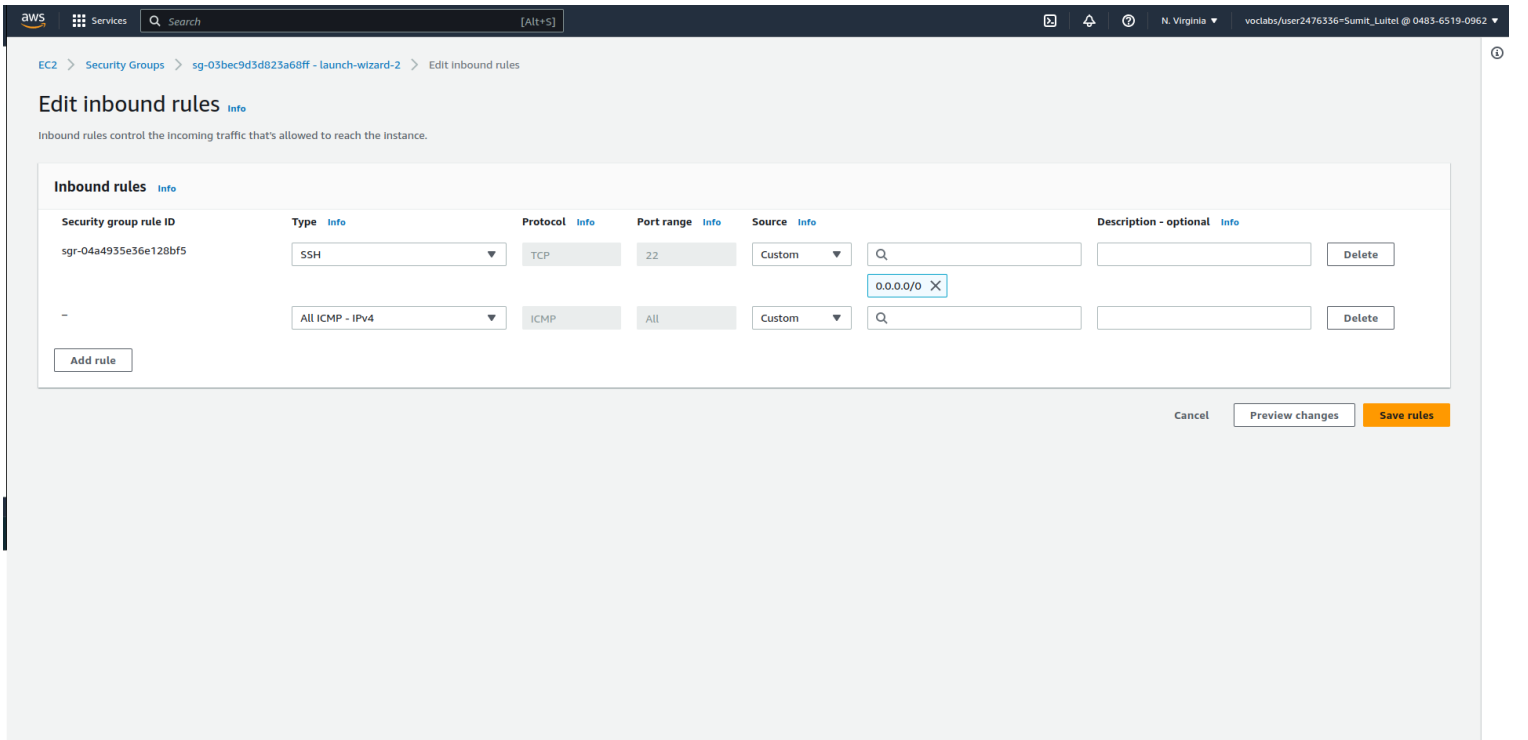
Note: In most cases, the default user name, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

Connect



- Add Inbound rule.
- Add ICMP Protocol in **Practice-Demo2**



- Ping the public IP

The screenshot displays the AWS Management Console interface. On the left, the navigation menu includes sections like 'New EC2 Experience', 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances', 'Images', 'Elastic Block Store', and 'Network & Security'. The main area shows the 'Instances (1/3)' page with a table of three instances: Practice-Demo3, Practice-Demo2 (selected), and Practice-Demo1. Below the table, the 'Details' tab for instance 'i-0ceb1bb761c4e191a' is open, showing fields like Instance ID, IP name, IPv6 address, Hostname type, Private IP DNS name, Instance type, VPC ID, and Subnet ID. A terminal window is overlaid on the right, showing a shell prompt 'ubuntu@ip-172-31-8-147: ~' and the command 'ping 172.31.4.190'. The terminal output shows 'PING 172.31.4.190 (172.31.4.190) 56(84) bytes of data.' followed by '111 packets transmitted, 0 received, 100% packet loss, time 112623ms'. Another terminal window shows 'ping 3.235.169.27' with successful results.

Name	Instance ID	Instance state	Instance type	Status
Practice-Demo3	i-065c2a7a41b0a80d9	Running	t2.micro	Success
Practice-Demo2	i-0ceb1bb761c4e191a	Running	t2.micro	Success
Practice-Demo1	i-0238f12b659ff8247	Running	t2.micro	Success

Instance: i-0ceb1bb761c4e191a (Practice-Demo2)

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

Instance summary Info

Instance ID: i-0ceb1bb761c4e191a (Practice-Demo2)

IPv6 address: -

Hostname type: IP name: ip-172-31-4-190.ec2.internal

Answer private resource DNS name: IPv4 (A)

Auto-assigned IP address: 3.235.169.27 [Public IP]

IAM Role: -

Public IPv4 address copied

3.235.169.27 | open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-4-190.ec2.internal

Instance type: t2.micro

VPC ID: vpc-0dc9737115ea6cf4e

Subnet ID: subnet-0e649d8778ddaa116

Private IPv4 addresses: 172.31.4.190

Public IPv4 DNS: ec2-3-235-169-27.compute-1.amazonaws.com | open address

Elastic IP addresses: -

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

Auto Scaling Group name: -

- Ping the private IP

Instances (1/3) Info

Find instance by attribute or tag (case-sensitive)

Instance state: **running** Clear filters

Name	Instance ID	Instance state	Instance type	Status
Practice-Demo3	i-065c2a7a41b0a80d9	Running	t2.micro	✓
Practice-Demo2	i-0ceb1bb761c4e191a	Running	t2.micro	✓
Practice-Demo1	i-0238f12b659ff8247	Running	t2.micro	✓

Instance: i-0ceb1bb761c4e191a (Practice-Demo2)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Info

Instance ID	i-0ceb1bb761c4e191a (Practice-Demo2)
IPv6 address	-
Hostname type	IP name: ip-172-31-4-190.ec2.internal
Answer private resource DNS name	IPV4 (A)
Auto-assigned IP address	3.235.169.27 [Public IP]
IAM Role	-
Public IPv4 address	3.235.169.27 open address
Instance state	Running
Private IP DNS name (IPv4 only)	ip-172-31-4-190.ec2.internal
Instance type	t2.micro
VPC ID	vpc-0dc9737115ea6cf4e
Subnet ID	subnet-0e649d8778ddaa116

```
ubuntu@ip-172-31-8-147: ~  
64 bytes from 3.235.169.27: icmp_seq=17 ttl=63 time=0.570 ms  
64 bytes from 3.235.169.27: icmp_seq=18 ttl=63 time=0.537 ms  
64 bytes from 3.235.169.27: icmp_seq=19 ttl=63 time=0.586 ms  
64 bytes from 3.235.169.27: icmp_seq=20 ttl=63 time=0.541 ms  
64 bytes from 3.235.169.27: icmp_seq=21 ttl=63 time=1.01 ms  
64 bytes from 3.235.169.27: icmp_seq=22 ttl=63 time=1.61 ms  
64 bytes from 3.235.169.27: icmp_seq=23 ttl=63 time=0.632 ms  
64 bytes from 3.235.169.27: icmp_seq=24 ttl=63 time=0.530 ms  
64 bytes from 3.235.169.27: icmp_seq=25 ttl=63 time=0.556 ms  
64 bytes from 3.235.169.27: icmp_seq=26 ttl=63 time=0.520 ms  
64 bytes from 3.235.169.27: icmp_seq=27 ttl=63 time=0.625 ms  
-  
--- 3.235.169.27 ping statistics ---  
27 packets transmitted, 27 received, 0% packet loss, time 26563ms  
rtt min/avg/max/mdev = 0.490/0.622/1.610/0.215 ms  
ubuntu@ip-172-31-8-147: ~$ ping 172.31.4.190  
PING 172.31.4.190 (172.31.4.190) 56(84) bytes of data.  
64 bytes from 172.31.4.190: icmp_seq=1 ttl=64 time=0.554 ms  
64 bytes from 172.31.4.190: icmp_seq=2 ttl=64 time=0.452 ms  
64 bytes from 172.31.4.190: icmp_seq=3 ttl=64 time=0.439 ms  
64 bytes from 172.31.4.190: icmp_seq=4 ttl=64 time=0.449 ms  
64 bytes from 172.31.4.190: icmp_seq=5 ttl=64 time=0.524 ms  
64 bytes from 172.31.4.190: icmp_seq=6 ttl=64 time=0.467 ms
```

Private IPv4 address copied

ec2-3-235-169-27.compute-1.amazonaws.com | [open address](#)

Public IPv4 DNS

ec2-3-235-169-27.compute-1.amazonaws.com | [open address](#)

Elastic IP addresses

-

AWS Compute Optimizer finding

[Opt-in to AWS Compute Optimizer for recommendations.](#) | [Learn more](#)

Auto Scaling Group name

-

Create new instance in new region (Oregon in example)

Instances (1) Info

Find instance by attribute or tag (case-sensitive)

Instance state: **running** Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
Practice-Demo3	i-016d5b81c1aa7f171	Running	t2.micro	Initializing	No alarms	us-west-2b	ec2-34-217-215-180.us...	34.217.215.180	-

Select an instance

Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

Instance state = running X Clear filters

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input checked="" type="checkbox"/>	Practice-Demo3	i-016d5b81c1aa7f171	Running	t2.micro	Initializing	No alarms	us-west-2b	ec2-34-217-215-180.us...	34.217.215.180	-

Instance: i-016d5b81c1aa7f171 (Practice-Demo3)

Details Security Networking Storage Status checks Monitoring Tags

▼ Instance summary Info

<p>Instance ID</p> <p>i-016d5b81c1aa7f171 (Practice-Demo3)</p> <p>IPv6 address</p> <p>-</p> <p>Hostname type</p> <p>IP name: ip-172-31-28-16.us-west-2.compute.internal</p> <p>Answer private resource DNS name</p> <p>IPv4 (A)</p> <p>Auto-assigned IP address</p> <p>34.217.215.180 [Public IP]</p>	<p>Public IPv4 address</p> <p>34.217.215.180 open address</p> <p>Instance state</p> <p>Running</p> <p>Private IP DNS name (IPv4 only)</p> <p>ip-172-31-28-16.us-west-2.compute.internal</p> <p>Instance type</p> <p>t2.micro</p> <p>VPC ID</p> <p>vpc-0824e103056f540b5</p>	<p>Private IPv4 addresses</p> <p>172.31.28.16</p> <p>Public IPv4 DNS</p> <p>ec2-34-217-215-180.us-west-2.compute.amazonaws.com open address</p> <p>Elastic IP addresses</p> <p>-</p> <p>AWS Compute Optimizer finding</p> <p>Opt-in to AWS Compute Optimizer for recommendations. Learn more</p>
---	---	--

Connection via SSH

EC2 > Instances > i-016d5b81c1aa7f171 > Connect to instance

Connect to your instance i-016d5b81c1aa7f171 (Practice-Demo3) using any of these options

EC2 Instance Connect Session Manager **SSH client** EC2 serial console

Instance ID

i-016d5b81c1aa7f171 (Practice-Demo3)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is oregondemo.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.


```
chmod 400 oregondemo.pem
```
4. Connect to your Instance using its Public DNS:


```
ec2-34-217-215-180.us-west-2.compute.amazonaws.com
```

Example:

```
ssh -i "oregondemo.pem" ubuntu@ec2-34-217-215-180.us-west-2.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.

Cancel

```
ubuntu@ip-172-31-28-16: ~
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-28-16:~$
```

- Can be connected to Public IP
- Cannot be connected to Private IP

Instances (1/3) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4	Elastic IP
Practice-Demo3	i-065c2a7a41b0a80d9	Terminated	t2.micro	-	No alarms	us-east-1a	-	-	-
Practice-Demo2	i-0ceb1bb761c4e191a	Running	t2.micro	2/2 checks passed	No alarms	us-east-1c	ec2-3-235-169-27.com...	3.235.169.27	-
Practice-Demo1	i-0238f12b659ff8247	Running	t2.micro	2/2 checks passed	No alarms	us-east-1c	ec2-18-207-108-68.co...	18.207.108.68	-

Instance: i-0ceb1bb761c4e191a (Practice-Demo2)

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

Instance summary Info

Instance ID: i-0ceb1bb761c4e191a (Practice-Demo2)

IPv6 address: -

Hostname type: -

IP name: ip-172-31-4-190.ec2.internal

Answer private resource DNS name: -

IPv4 (A): 3.235.169.27 [Public IP]

Auto-assigned IP address: 3.235.169.27 [Public IP]

IAM Role: -

Public IPv4 address copied

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-4-190.ec2.internal

Instance type: t2.micro

VPC ID: vpc-0dc9737115ea6cf4e

Subnet ID: subnet-0e649d8778ddaa116

Terminal Output:

```

ubuntu@ip-172-31-28-16: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-28-16: ~$ ping 34.217.215.180
PING 34.217.215.180 (34.217.215.180) 56(84) bytes of data.
^C
--- 34.217.215.180 ping statistics ---
28 packets transmitted, 0 received, 100% packet loss, time 27651ms

ubuntu@ip-172-31-28-16: ~$ ping 172.31.4.190
PING 172.31.4.190 (172.31.4.190) 56(84) bytes of data.
^C
--- 172.31.4.190 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13300ms

ubuntu@ip-172-31-28-16: ~$ ping 3.235.169.27
PING 3.235.169.27 (3.235.169.27) 56(84) bytes of data.
64 bytes from 3.235.169.27: icmp_seq=1 ttl=37 time=62.9 ms
64 bytes from 3.235.169.27: icmp_seq=2 ttl=37 time=63.0 ms
64 bytes from 3.235.169.27: icmp_seq=3 ttl=37 time=62.9 ms
64 bytes from 3.235.169.27: icmp_seq=4 ttl=37 time=62.9 ms
64 bytes from 3.235.169.27: icmp_seq=5 ttl=37 time=62.8 ms
  
```

AWS Compute Optimizer finding

[Opt-in to AWS Compute Optimizer for recommendations. | Learn more](#)

Auto Scaling Group name: -

3. Configuring a static website on Amazon S3

Amazon S3

Successfully created bucket "sumitexample.com"

To upload files and folders, or to configure additional bucket settings choose [View details](#).

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

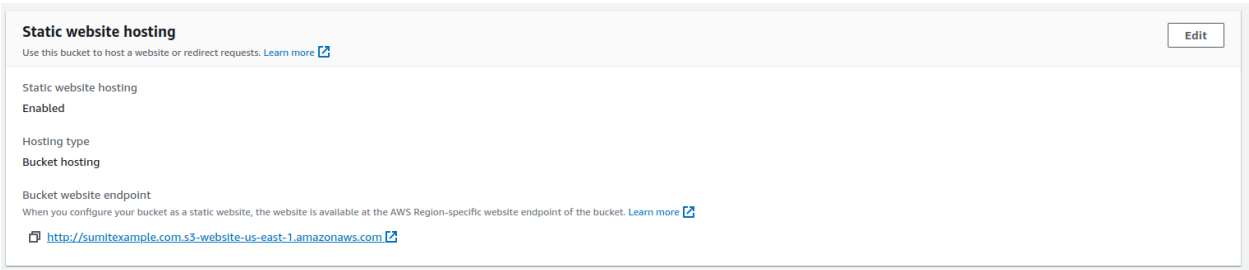
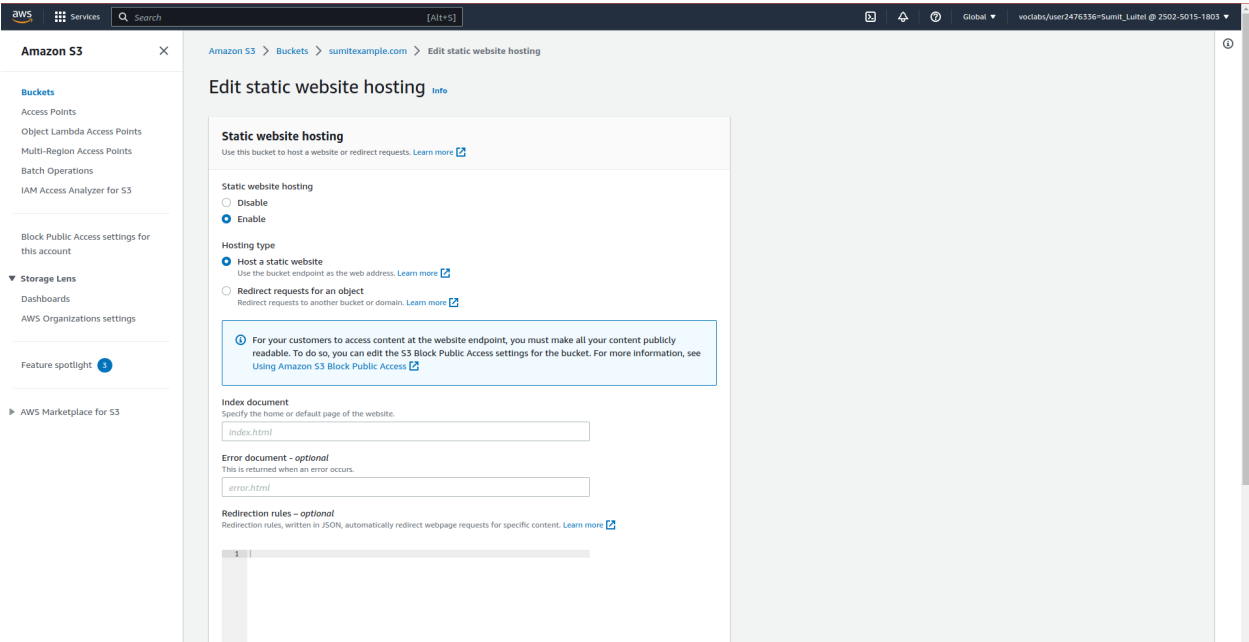
[View Storage Lens dashboard](#)

Buckets (1) Info

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name	AWS Region	Access	Creation date
sumitexample.com	US East (N. Virginia) us-east-1	Bucket and objects not public	March 26, 2023, 22:36:14 (UTC+05:45)



403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 13Z395XPP79AYMRK
- HostId: gXYvBSZXwnDIEAJYQ9gFwsReo3aJWg+z1WtbedIDr/SqRi9RkDFVDdYAwVuxCk/HjcVRBlQsc=

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets > sumitexample.com

sumitexample.com

Objects | Properties | Permissions | Metrics | Management | Access Points

Permissions overview

Access

Bucket and objects not public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

On

Individual Block Public Access settings for this bucket

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets > sumitexample.com > Edit Block public access (bucket settings)

Edit Block public access (bucket settings)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel Save changes

Successfully edited Block Public Access settings for this bucket.

Amazon S3 > Buckets > sumitexample.com

sumitexample.com

Objects | Properties | Permissions | Metrics | Management | Access Points

Permissions overview

Access

Objects can be public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

Off

Individual Block Public Access settings for this bucket

Amazon S3 > Buckets > sumitexample.com > Edit bucket policy

Edit bucket policy

Info

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN

arn:aws:s3:::sumitexample.com

Policy

1 {

2 "Version": "2012-10-17",

3 "Statement": [

4 {

5 "Sid": "PublicReadGetObject",

6 "Effect": "Allow",

7 "Principal": "*",

8 "Action": [

9 "s3:GetObject"

10],

11 "Resource": [

12 "arn:aws:s3:::sumitexample.com/*"

13]

14 }]

15 }

16 }

Edit statement

PublicReadGetObject

Remove

1. Add actions

Choose a service

Filter services

Included

S3

Available

AMP

API Gateway

API Gateway V2

ASC

Access Analyzer

Account

Activate

Alexa for Business

Amplify

2. Add a resource

Add

3. Add a condition (optional)

Add

Successfully edited bucket policy.

Amazon S3 > Buckets > sumitexample.com

sumitexample.com

Info

Publicly accessible

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Public

Upload succeeded
View details below.

Upload: status

Close

The information below will no longer be available after you navigate away from this page.

Summary

Destination

s3://sumitexample.com

Succeeded

1 file, 4.2 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 4.2 KB)

Find by name

Name

Folder

Type

Size

Status

Error

index.html

-

text/html

4.2 KB

Succeeded

-

Amazon S3 > Buckets > sumitexample.com

sumitexample.com

info

Publicly accessible

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

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](#)

Copy

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

☐

Name

Type

Last modified

Size

Storage class

☐

index.html

html

March 26, 2023, 22:46:27 (UTC+05:45)

4.2 KB

Standard

Static website hosting

Edit

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

Enabled

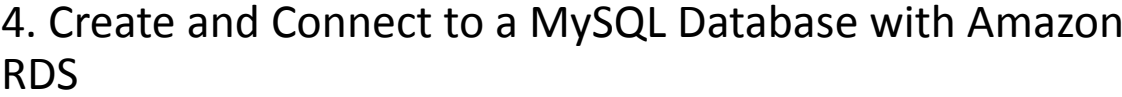
Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

http://sumitexample.com.s3-website-us-east-1.amazonaws.com



Choose a database creation method [Info](#)

- You set all of the configuration options, including ones for availability, security, backups, and maintenance.

- Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type [Info](#)

☐ Aurora (MySQL Compatible)



☐ Aurora (PostgreSQL Compatible)



☒ MySQL



☐ MariaDB



☐ PostgreSQL



☐ Oracle

ORACLE®

☐ Microsoft SQL Server



Templates

Choose a sample template to meet your use case.

☐ Production

Use defaults for high availability and fast, consistent performance.

☒ Dev/Test

This instance is intended for development use outside of a production environment.

☐ Free tier

Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.

[Info](#)

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

☐ **Multi-AZ DB Cluster - *new***

Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

☐ **Multi-AZ DB instance**

Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

☒ **Single DB instance**

Creates a single DB instance with no standby DB instances.

Settings

DB Instance Identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings



Master username [Info](#)

Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter.

☐ **Manage master credentials in AWS Secrets Manager**

Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

 If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
[Learn more](#) 

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

- ☐ Standard classes (includes m classes)
- ☐ Memory optimized classes (includes r and x classes)
- ☒ Burstable classes (includes t classes)

db.t3.micro

2 vCPUs 1 GiB RAM Network: 2,085 Mbps



☐ Include previous generation classes

Storage

Storage type [Info](#)

General Purpose SSD (gp2)

Baseline performance determined by volume size



Allocated storage [Info](#)

20

GIB

The minimum value is 20 GiB and the maximum value is 6,144 GiB

Provisioning less than 100 GiB of General Purpose (SSD) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) IO credit balance. [Learn more](#)

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

☒ Enable storage autoscaling

Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

Creating database [inventory-db](#)

View credential details

Your database might take a few minutes to launch.
How was your experience creating an Amazon RDS database? [Provide feedback](#)

RDS > Databases

Consider creating a Blue/Green Deployment to minimize downtime during upgrades

You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

Databases

Group resources

Modify

Actions

Restore from S3

Create database

Filter by databases

< 1 >

DB identifier	Role	Engine	Region & AZ	Size
inventory-db	Instance	MySQL Community	-	db.t3.micro

Successfully created database [inventory-db](#)

View connection details

How was your experience creating an Amazon RDS database? [Provide feedback](#)

RDS > Databases

Consider creating a Blue/Green Deployment to minimize downtime during upgrades

You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

Databases

Group resources

Modify

Actions

Restore from S3

Create database

Filter by databases

< 1 >

Role	Engine	Region & AZ	Size	Status	Actions	CPU	Current activity
Instance	MySQL Community	us-east-1a	db.t3.micro	Available	-	-	

Cannot connect to the server via VSCode.

Connect to server

Connection error! timeout expired

Error when following class session. Cannot Create a database.



Your request to create DB instance database-1 didn't work.



User: arn:aws:sts::699715469555:assumed-role/voclabs/user2476336=Sumit_Luitel is not authorized to perform: rds:CreateDBSubnetGroup on resource: arn:aws:rds:us-east-1:699715469555:subgrp:default-vpc-01174faeb576c62f4 because no identity-based policy allows the rds:CreateDBSubnetGroup action (Service: AmazonRDS; Status Code: 403; Error Code: AccessDenied; Request ID: 05afb44f-c2d5-4237-90b7-d96688d5fc85; Proxy: null)