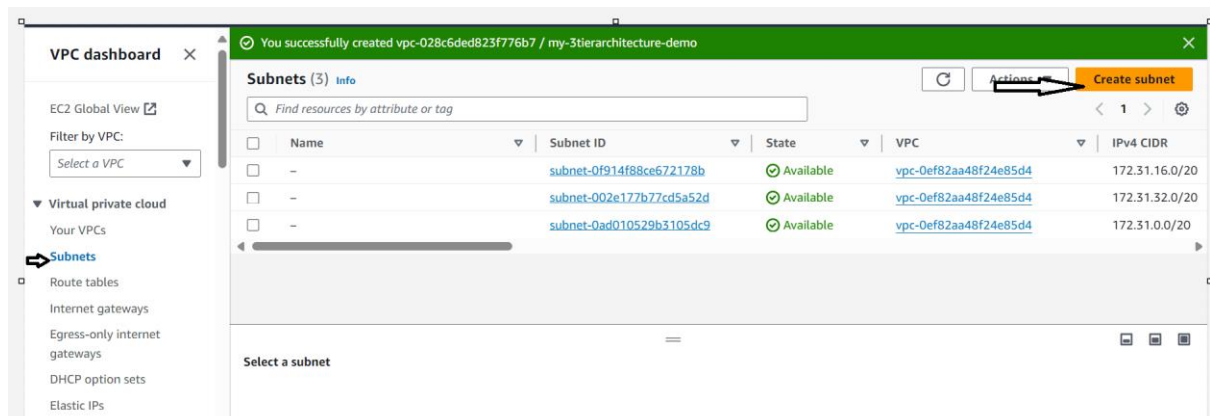
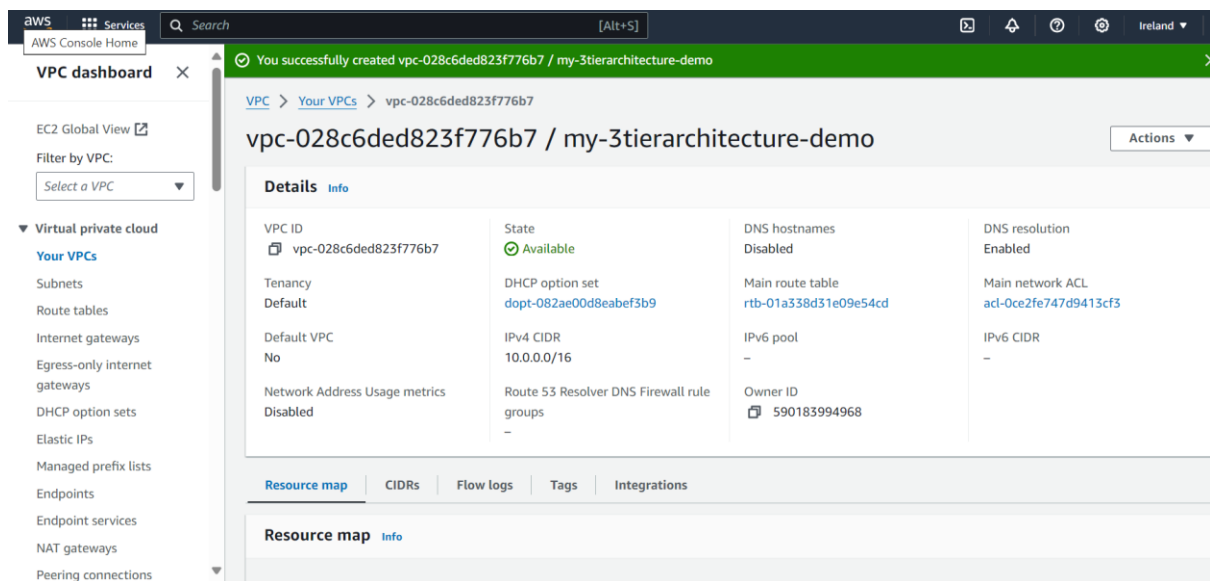


VPC and Subnets

VPC Creation

- Navigate to the VPC dashboard in the AWS console and navigate to **Your VPCs** on the left-hand side.



We will need six subnets across two availability zones. That means that three subnets will be in one availability zone, and three subnets will be in another zone. Each subnet in one availability zone will correspond to one layer of our three-tier architecture.

The screenshot shows the 'Create subnet' page in the AWS Management Console. It is divided into two main sections: 'VPC' and 'Subnet settings'.

VPC section:

- VPC ID:** A dropdown menu showing 'vpc-028c6ded823f776b7 (my-3tierarchitecture-demo)'. A red arrow points to this dropdown.
- Associated VPC CIDRs:** A text box showing '10.0.0.0/16'.

Subnet settings section:

- Subnet 1 of 1:**
- Subnet name:** A text box containing 'Public-Subnet-AZ1'. A red arrow points to this text box.
- Availability Zone:** A dropdown menu showing 'Europe (Ireland) / eu-west-1a'.
- IPv4 VPC CIDR block:** A dropdown menu showing '10.0.0.0/16'. A red arrow points to this dropdown.

Your final subnet setup should be similar to this. Verify that you have 3 subnets across 2 different availability zones.

The screenshot shows the 'Subnets (6)' page in the AWS Management Console. A green banner at the top states: 'You have successfully created 6 subnets: subnet-076d66175838cd5b4, subnet-089a2de9d522dc959, subnet-03c6faf85196eb446, subnet-09a93d92c694ab351, subnet-0ad5f7a514584c7e6, subnet-0fe21288b4b029b69'.

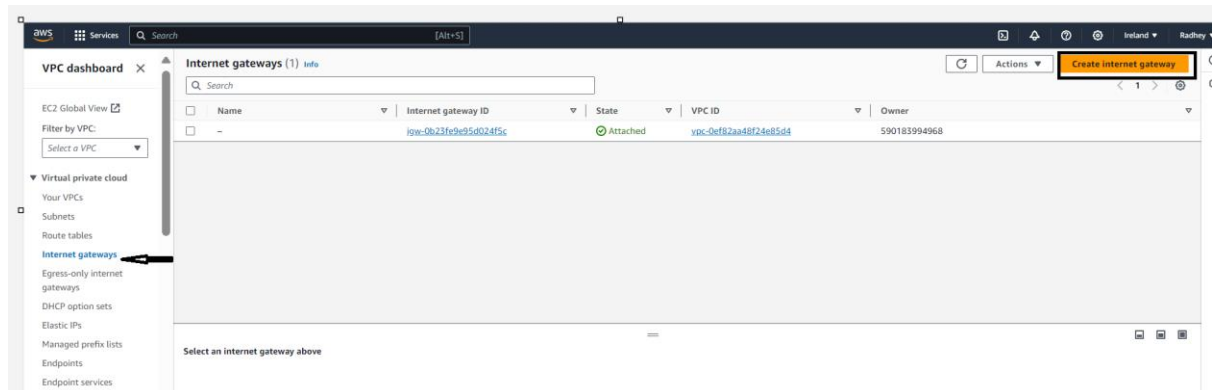
Below the banner is a table of subnets. The table has columns: Name, Subnet ID, State, VPC, IPv4 CIDR, IPv6, Available IPv4, and Availability Zone. The first three columns are highlighted with red boxes in the original image.

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6	Available IPv4	Availability Zone
Private-DB-Subnet-AZ2	subnet-0fe21288b4b029b69	Available	vpc-028c6ded823f776b7 my-...	10.0.5.0/24	-	251	eu-west-1b
Public-Subnet-AZ2	subnet-089a2de9d522dc959	Available	vpc-028c6ded823f776b7 my-...	10.0.1.0/24	-	251	eu-west-1b
Private-Subnet-AZ2	subnet-09a93d92c694ab351	Available	vpc-028c6ded823f776b7 my-...	10.0.3.0/24	-	251	eu-west-1b
Private-Subnet-AZ1	subnet-03c6faf85196eb446	Available	vpc-028c6ded823f776b7 my-...	10.0.2.0/24	-	251	eu-west-1a
Private-DB-Subnet-AZ1	subnet-0ad5f7a514584c7e6	Available	vpc-028c6ded823f776b7 my-...	10.0.4.0/24	-	251	eu-west-1a
Public-Subnet-AZ1	subnet-076d66175838cd5b4	Available	vpc-028c6ded823f776b7 my-...	10.0.0.0/24	-	251	eu-west-1a

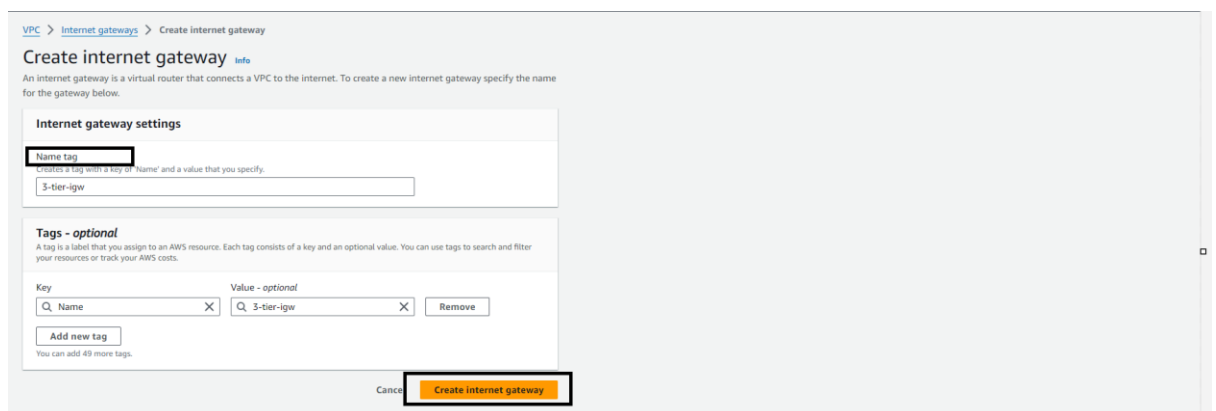
Internet Connectivity

Internet Gateway:

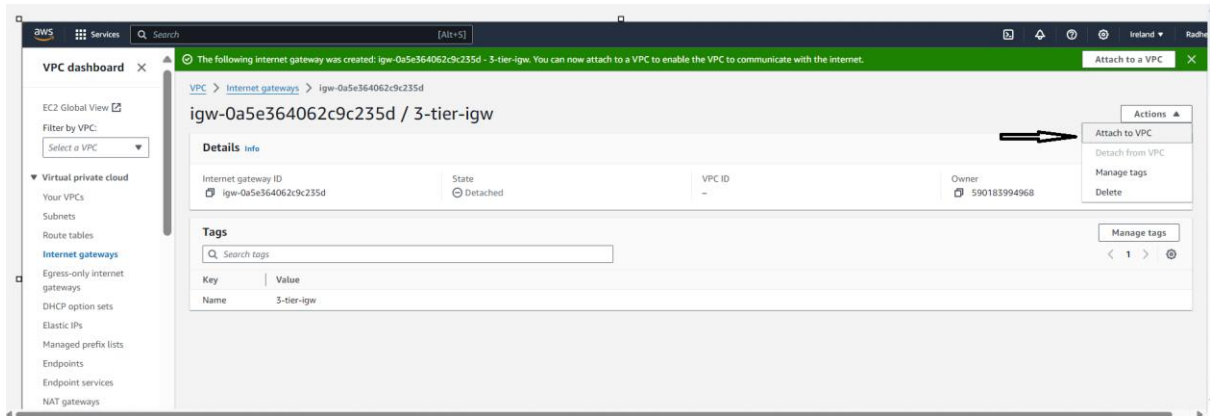
- In order to give the public subnets in our VPC internet access we will have to create and attach an Internet Gateway. On the left-hand side of the VPC dashboard, select Internet Gateway.



- Create your internet gateway by simply giving it a name and clicking Create internet gateway.

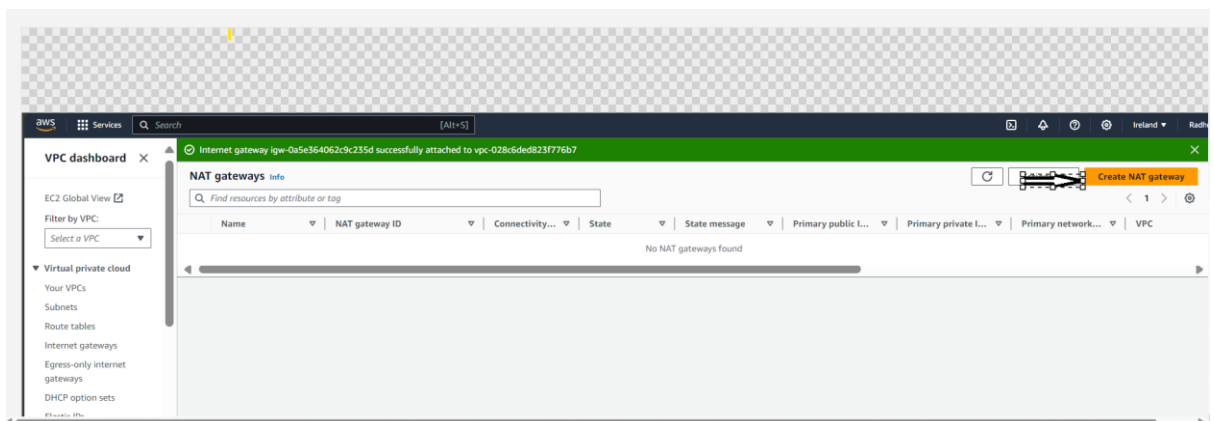


- After creating the internet gateway, attach it to your VPC that you create in the VPC and Subnet Creation step of the workshop. You have a couple options on how to do this, either with the creation success message or the Actions drop down.



NAT Gateway

- In order for our instances in the app layer private subnet to be able to access the internet they will need to go through a NAT Gateway. For high availability, you'll deploy one NAT gateway in each of your public subnets. Navigate to NAT Gateways on the left side of the current dashboard and click Create NAT Gateway.



- Fill in the Name, choose one of the public subnets you created in part 2, and then allocate an Elastic IP. Click Create NAT gateway.

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.
NGW-AZ1

Subnet
Select a subnet in which to create the NAT gateway.
subnet-07686617583cd5d4 (Public Subnet-AZ1)

Connectivity type
Select a connectivity type for the NAT gateway.
☒ Public
☐ Private

Elastic IP allocation ID - info
Assign an Elastic IP address to the NAT gateway.
elipalloc-00202be6e5195dcb1 Allocate Elastic IP

Additional settings info

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional
Name NGW-AZ1 Remove

Add new tag
You can add 49 more tags.

Cancel Create NAT gateway

- Repeat step 1 and 2 for the other subnet.

Routing Configuration

- Navigate to Route Tables on the left side of the VPC dashboard and click Create route table First, let's create one route table for the web layer public subnets and name it accordingly.

VPC dashboard

EC2 Global View ☒
Filter by VPC:
Select a VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints

Route tables (1) info

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
-	rtb-0aca3d15037b29796	-	-	Yes	vpc-0ef82aa48f24e85d4	590183994968

Create route table

Select a route table

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

PublicRouteTable

VPC
The VPC to use for this route table.

vpc-028c6ded823f776b7 (my-3tierarchitecture-demo)

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional

Q Name X Q PublicRouteTable X Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

- After creating the route table, you'll automatically be taken to the details page. Scroll down and click on the Routes tab and Edit routes.

VPC dashboard

EC2 Global View

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Route table rtb-0970b421cbd448223 | PublicRouteTable was created successfully.

VPC > Route tables > rtb-0970b421cbd448223

rtb-0970b421cbd448223 / PublicRouteTable

Actions

Details Info

Route table ID
rtb-0970b421cbd448223

Main
No

Explicit subnet associations
-

Edge associations
-

VPC
vpc-028c6ded823f776b7 | my-3tierarchitecture-demo

Owner ID
590183994968

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Both Edit routes

- Add a route that directs traffic from the VPC to the internet gateway. In other words, for all traffic destined for IPs outside the VPC CIDR range, add an entry that directs it to the internet gateway as a target. Save the changes.

VPC > Route tables > rtb-0970b421cbd448223 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="Internet Gateway"/>	-	No
	<input type="text" value="igw-0a5e364062c9c235d"/>		

- Edit the Explicit Subnet Associations of the route table by navigating to the route table details again. Select Subnet Associations and click Edit subnet associations.

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (0)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations			
You do not have any subnet associations.			

- Select the two web layer public subnets you created earlier and click **Save associations**.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6)

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	Private-DB-Subnet-AZ2	subnet-0fe21288b4b029b69	10.0.5.0/24	-	Main (rtb-01a338d31e09e54cd)
<input checked="" type="checkbox"/>	Public-Subnet-AZ2	subnet-089a2de9d522dc959	10.0.1.0/24	-	Main (rtb-01a338d31e09e54cd)
<input type="checkbox"/>	Private-Subnet-AZ2	subnet-09a95e92c694ab351	10.0.3.0/24	-	Main (rtb-01a338d31e09e54cd)
<input type="checkbox"/>	Private-Subnet-AZ1	subnet-03c6faf85196eb446	10.0.2.0/24	-	Main (rtb-01a338d31e09e54cd)
<input type="checkbox"/>	Private-DB-Subnet-AZ1	subnet-0ad5f7a514584c7e6	10.0.4.0/24	-	Main (rtb-01a338d31e09e54cd)
<input checked="" type="checkbox"/>	Public-Subnet-AZ1	subnet-076d66175838cd5b4	10.0.0.0/24	-	Main (rtb-01a338d31e09e54cd)

Selected subnets

- Now create 2 more route tables, one for each app layer private subnet in each availability zone. These route tables will route app layer traffic destined for outside the VPC to the NAT gateway in the respective availability zone, so add the appropriate routes for that.

VPC > Route tables > Create route table

Create route table info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

PrivateRouteTable-AZ1

VPC
The VPC to use for this route table.

vpc-028c6ded923f776b7 (my-3tierarchitecture-demo)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name X

Value - optional

Q PrivateRouteTable-AZ1 X Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

VPC > Route tables > rtb-0b482bef2241e678f > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0 X	NAT Gateway	-	No
	Q nat-034de7c48d2edee4b X		

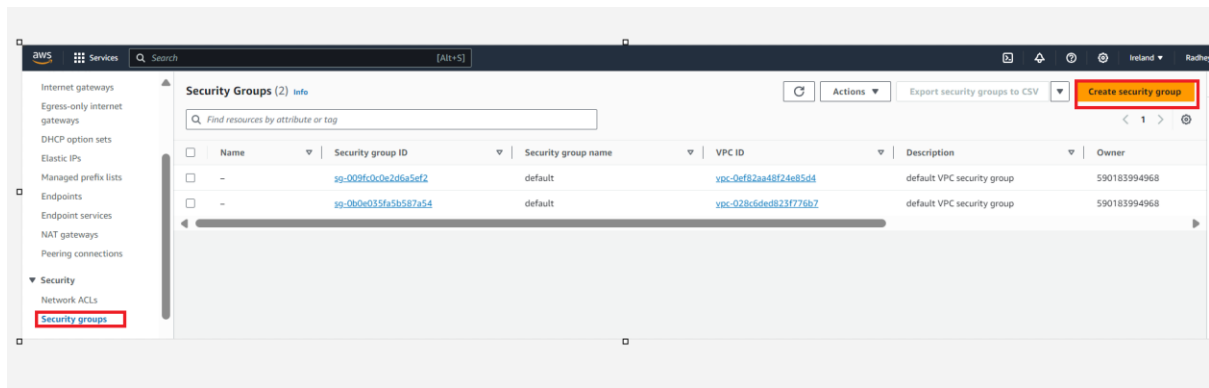
Add route

Cancel Preview Save changes

- Once the route tables are created and routes added, add the appropriate subnet associations for each of the app layer private subnets.

Security Groups

- Security groups will tighten the rules around which traffic will be allowed to our Elastic Load Balancers and EC2 instances. Navigate to Security Groups on the left side of the VPC dashboard, under Security.



- The first security group you'll create is for the public, internet facing load balancer. After typing a name and description, add an inbound rule to allow HTTP type traffic.

The screenshot shows the 'Create security group' form. In the 'Basic details' section, the 'Security group name' is 'Internet-Facing-LB-sg' and the 'Description' is 'External Load Balancer Security Group'. In the 'Inbound rules' section, a rule is being added with 'Type' set to 'HTTP', 'Protocol' set to 'TCP', 'Port range' set to '80', and 'Source' set to 'Anywhere-...' (0.0.0.0/0).

- The second security group you'll create is for the public instances in the web tier. After typing a name and description, add an inbound rule that allows HTTP type traffic from your internet facing load balancer security group you created in the previous step. This will allow traffic from your public facing load balancer to hit your instances.

The screenshot shows the 'Create security group' form. In the 'Basic details' section, the 'Security group name' is 'WebTier-sg' and the 'Description' is 'SG for the web tier'. In the 'Inbound rules' section, a rule is being added with 'Type' set to 'HTTP', 'Protocol' set to 'TCP', 'Port range' set to '80', and 'Source' set to 'Custom' (sg-044a8065bde141e).

- The third security group will be for our internal load balancer. Create this new security group and add an inbound rule that allows HTTP type traffic from your public instance security group. This will allow traffic from your web tier instances to hit your internal load balancer.

BASIC DETAILS

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Custom <input type="text" value="sg-04b1a4277bc087c2e"/>	<input type="text"/>

[Add rule](#) [Delete](#)

- The fourth security group we'll configure is for our private instances. After typing a name and description, add an inbound rule that will allow TCP type traffic on port 4000 from the internal load balancer security group you created in the previous step. This is the port our app tier application is running on and allows our internal load balancer to forward traffic on this port to our private instances.

BASIC DETAILS

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	4000	Custom <input type="text" value="sg-04b1a4277bc087c2e"/>	<input type="text"/>

[Add rule](#) [Delete](#)

- The fifth security group we'll configure protects our private database instances. For this security group, add an inbound rule that will allow traffic from the private instance security group to the MySQL/Aurora port (3306).

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
DBSG

Description [Info](#)
sg for our databases

VPC [Info](#)
vpc-028c6ded823f776b7 (my-3tierarchitecture-demo)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
MySQL/Aurora	TCP	3306	Custom sg-0bb964694d751e1f3 sg-0bb964694d751e1f3	<div></div> <div>Delete</div>

IAM EC2 Instance Role Creation

- Navigate to the IAM dashboard in the AWS console and create an EC2 role.

Identity and Access Management (IAM)

Dashboard
▼ Access management
User groups
Users
Roles
Policies
Identity providers
Account settings

[IAM](#) > Roles

Roles (2) [Info](#)
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

☐ Role name

☐ [AWSServiceRoleForSupport](#)

☐ [AWSServiceRoleForTrustedAdvisor](#)

Trusted entities

AWS Service: support (Service-Linker)

AWS Service: trustedadvisor (Service-Linker)

Roles Anywhere [Info](#)
Authenticate your non AWS workloads and securely provide access to AWS services.

Manage

- Select EC2 as the trusted entity.

Add permissions

Step 3
Name, review, and create

Trusted entity type

☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.
Use case

- When adding permissions, include the following AWS managed policies. You can search for them and select them. These policies will allow our instances to download our code from S3 and use Systems Manager Session Manager to securely connect to our instances without SSH keys through the AWS console.

- ✓ AmazonSSMManagedInstanceCore
- ✓ AmazonS3ReadOnlyAccess

Step 2
[Add permissions](#)

Step 3
Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
StierRole
Maximum 64 characters. Use alphanumeric and "+,=, @, -, _" characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-/[(){}\$%^&*!;':"<>~

Step 1: Select trusted entities [Edit](#)

Trust policy

```

1- [{
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "sts:AssumeRole"
8-       ],
9-       "Principal": {
10-        "Service": [
11-          "ec2.amazonaws.com"
12-        ]
13-      }
14-     ]
15-   }
16- ]

```

Step 2: Add permissions

Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonS3ReadOnlyAccess	AWS managed	Permissions policy
AmazonSSMManagedInstanceCore	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

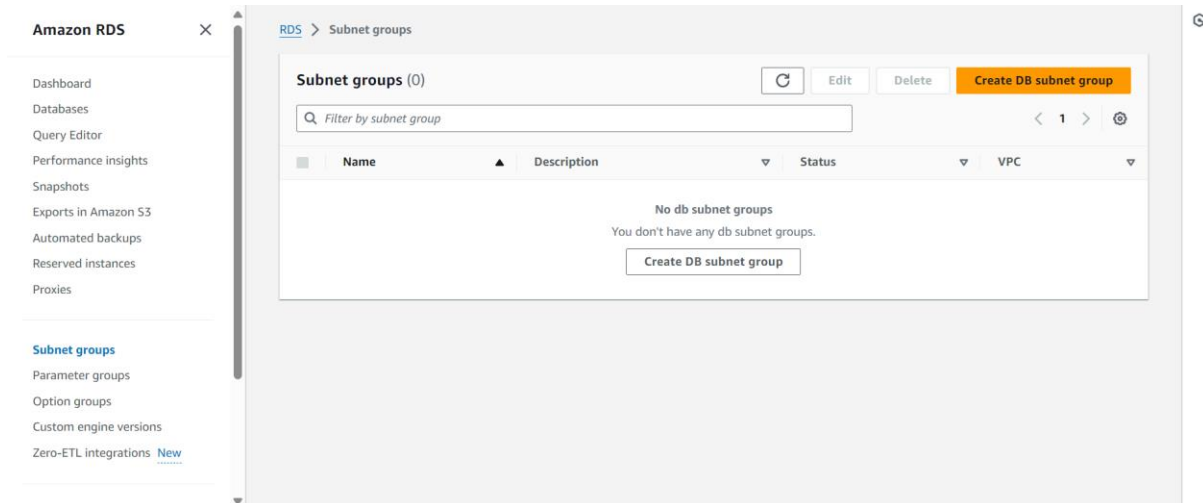
Create role

- Navigate to the S3 service in the AWS console and create a new S3 bucket.
- Give it a unique name, and then leave all the defaults as in. Make sure to select the region that you intend to run this whole lab in. This bucket is where we will upload our code later.

DATABASE DEPLOYMENT:

Subnet Groups

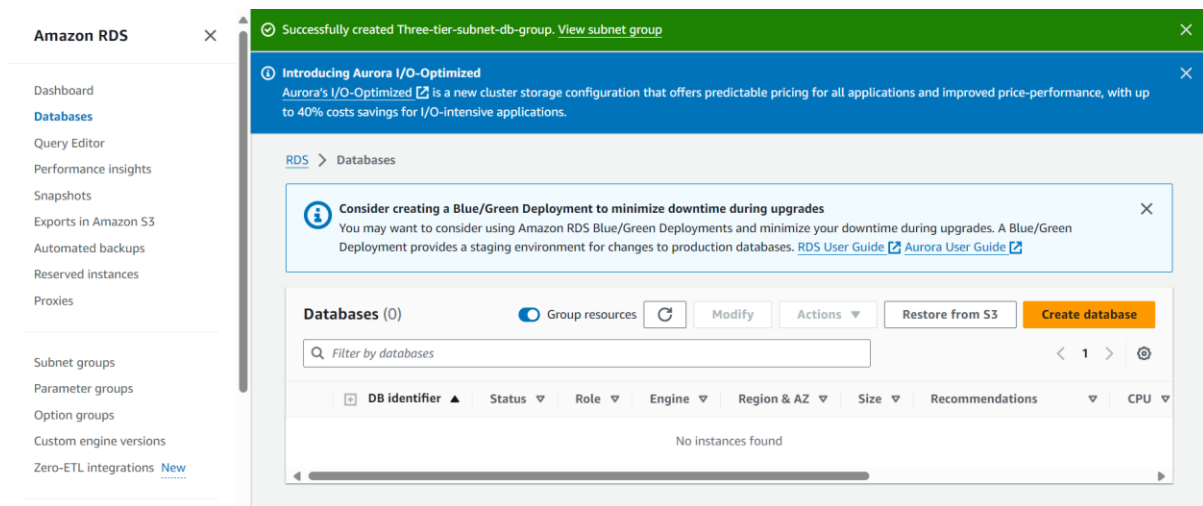
- Navigate to the RDS dashboard in the AWS console and click on Subnet groups on the left hand side. Click Create DB subnet group.



- Give your subnet group a name, description, and choose the VPC we created.

A screenshot of the 'Create DB subnet group' form in the AWS console. The form is titled 'Create DB subnet group' and includes a subtitle: 'To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.' The form contains three sections: 'Subnet group details', 'Name', and 'Description'. The 'Name' field is labeled 'Name' and has a warning: 'You won't be able to modify the name after your subnet group has been created.' The 'Description' field is labeled 'Description' and has a warning: 'You won't be able to modify the description after your subnet group has been created.' The 'VPC' field is labeled 'VPC' and has a warning: 'You won't be able to choose a different VPC identifier after your subnet group has been created.' The 'Name' field contains the text '3-tier-subnetdbgroup'. The 'Description' field contains the text 'subnet group for Database'. The 'VPC' field is a dropdown menu showing 'my-3tierarchitecture-demo (vpc-028c6ded823f776b7)'.

When adding subnets, make sure to add the subnets we created in each availability zone specifically for our database layer. You may have to navigate back to the VPC dashboard and check to make sure you're selecting the correct subnet IDs.



Create database


Choose a database creation method [Info](#)


☒ **Standard create**
You set all of the configuration options, including ones for availability, security, backups, and maintenance.


☐ **Easy create**
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**


Aurora MySQL-Compatible Edition

Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

Aurora MySQL 3.05.2 (compatible with MySQL 8.0.32) - default for major version 8.0

Parallel query is off by default. To enable it, use a DB instance parameter group with the `aurora_parallel_query` parameter enabled. [Learn more](#)

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.

Settings

DB cluster identifier [Info](#)

Enter a name for your DB cluster. The name must be unique across all DB clusters owned by your AWS account in the current AWS Region.

database-1

The DB cluster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). 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.

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.

admin

1 to 32 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

☐ Managed in AWS Secrets Manager - *most secure*
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

☒ Self managed
Create your own password or have RDS create a password that you manage.

☐ Auto generate password
Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / * @

Confirm master password [Info](#)

Aurora MySQL-
Compatible Edition

Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

Configuration options

Database instance, storage, and I/O charges vary depending on the configuration. [Learn more](#)

☒ Aurora Standard

- Cost-effective pricing for many applications with moderate I/O usage (I/O costs <25% of total database costs).
- Pay-per-request I/O charges apply. DB instance and storage prices don't include I/O usage.

☐ Aurora I/O-Optimized

- Predictable pricing for all applications. Improved price performance for I/O-intensive applications (I/O costs >25% of total database costs).
- No additional charges for read/write I/O operations. DB instance and storage prices include I/O usage.

Instance configuration

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

DB instance class [Info](#)

▼ Hide filters

☐ Include previous generation classes

☐ Serverless v2

☒ Memory optimized classes (includes r classes)

☐ Burstable classes (includes t classes)

db.r6g.2xlarge

8 vCPUs 64 GiB RAM Network: 4,750 Mbps

Aurora MySQL- Compatible Edition

Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

Multi-AZ deployment [Info](#)

☒ Create an Aurora Replica or Reader node in a different AZ (recommended for scaled availability)

Creates an Aurora Replica for fast failover and high availability.

☐ Don't create an Aurora Replica

Connectivity [Info](#)

Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

☒ Don't connect to an EC2 compute resource

Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

☐ Connect to an EC2 compute resource

Set up a connection to an EC2 compute resource for this database.

Network type [Info](#)

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

☒ IPv4

Your resources can communicate only over the IPv4 addressing protocol.

☐ Dual-stack mode

Your resources can communicate over IPv4, IPv6, or both.

Virtual private cloud (VPC) [Info](#)

Choose the VPC. The VPC defines the virtual networking environment for this DB cluster.

Aurora MySQL- Compatible Edition

Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

Choose the VPC. The VPC defines the virtual networking environment for this DB cluster.

my-3tierarchitecture-demo (vpc-028c6ded823f776b7)

6 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change its VPC.

DB subnet group [Info](#)

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB cluster can use in the VPC that you selected.

three-tier-subnet-db-group

2 Subnets, 2 Availability Zones

Public access [Info](#)

☐ Yes

RDS assigns a public IP address to the cluster. Amazon EC2 instances and other resources outside of the VPC can connect to your cluster. Resources inside the VPC can also connect to the cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

☒ No

RDS doesn't assign a public IP address to the cluster. Only Amazon EC2 instances and other resources inside the VPC can connect to your cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

VPC security group (firewall) [Info](#)

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

☒ Choose existing

Choose existing VPC security groups

☐ Create new

Create new VPC security group

Aurora MySQL- Compatible Edition

Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

Choose existing

Choose existing VPC security groups

Create new

Create new VPC security group

Existing VPC security groups

Choose one or more options

DBSG X

RDS Proxy

RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

Create an RDS Proxy

Info

RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).

Certificate authority - optional

Info

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-rsa2048-g1 (default)

Expires: May 20, 2061

If you don't select a certificate authority, RDS chooses one for you.

Additional configuration

Read replica write forwarding

Aurora MySQL- Compatible Edition

Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

Enhanced Monitoring

Additional configuration

Database options, encryption turned on, failover, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Estimated Monthly costs

DB instance	836.58 USD
Total	836.58 USD

This billing estimate is based on on-demand usage as described in [Amazon Aurora Pricing](#). Estimate does not consider reserved instance benefits and costs for instance storage, IOs, or data transfer.

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#).

You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

Cancel

Create database

Aurora MySQL- Compatible Edition

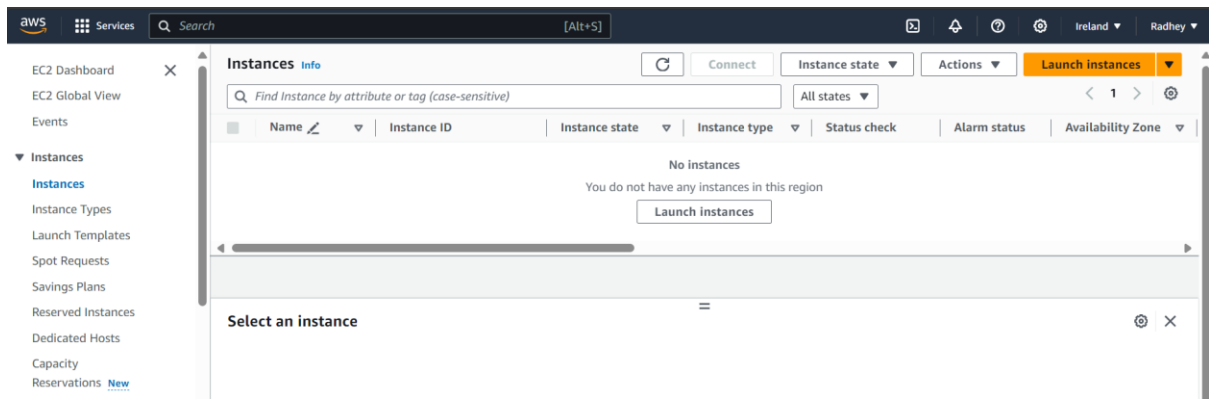
Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

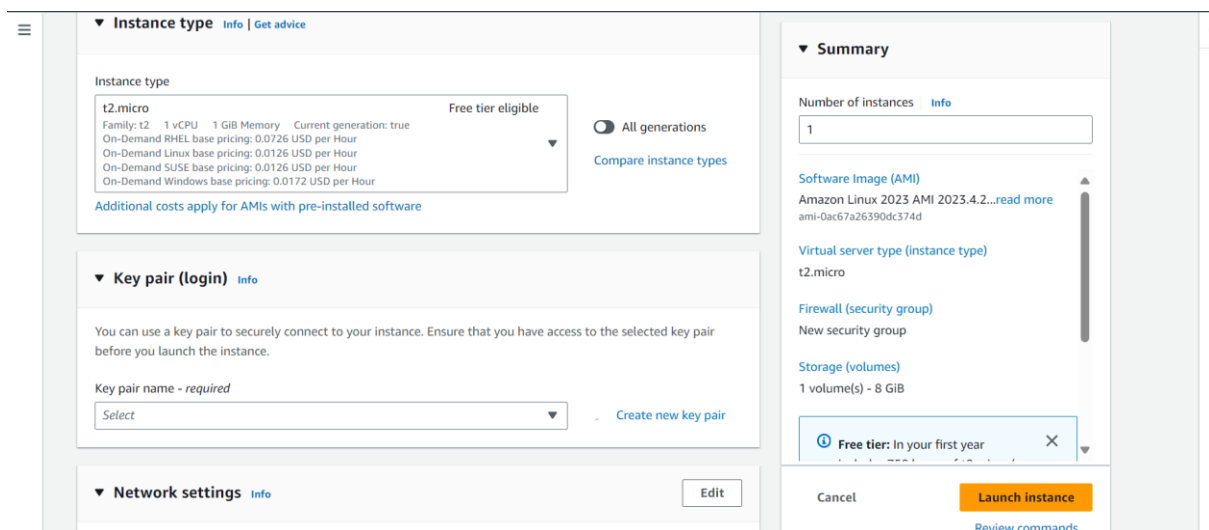
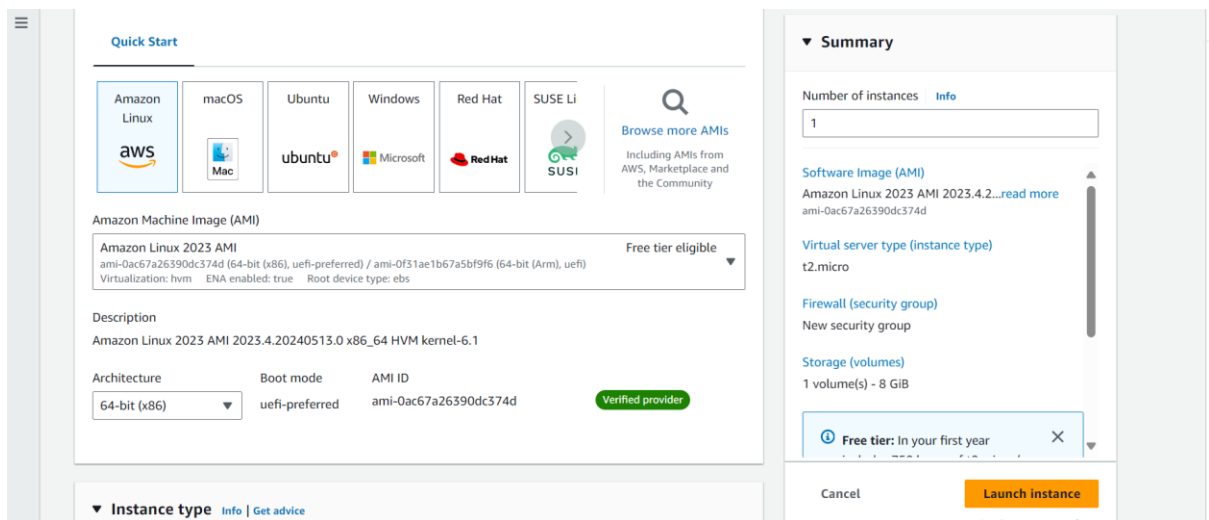
- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

App Instance Deployment

1. Navigate to the EC2 service dashboard and click on **Instances** on the left hand side. Then, click **Launch Instances**.



2. Select the first Amazon Linux 2 AMI



You can use a key pair to securely connect to your instance before you launch the instance.

Key pair name - required

Select

▼ Network settings

Info

Network

Info

vpc-0ef82aa48f24e85d4

Subnet

Info

No preference (Default subnet in any availability zone)

Auto-assign public IP

Info

Enable

Additional charges apply when outside of free tier allocation

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic to and from your instance.

Create security group

Key pair name

Key pairs allow you to connect to your instance securely.

3-tier

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA

RSA encrypted private and public key pair

☐ ED25519

ED25519 encrypted private and public key pair

Private key file format

☒ .pem

For use with OpenSSH

☐ .ppk

For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Cancel

Create key pair

VPC - required

Info

vpc-028c6ded823f776b7 (my-3tierarchitecture-demo)

10.0.0.0/16

Subnet

Info

subnet-03c6faf85196eb446

Private-Subnet-AZ1

VPC: vpc-028c6ded823f776b7

Owner: 590183994968

Availability Zone: eu-west-1a

IP addresses available: 251

CIDR: 10.0.2.0/24

Auto-assign public IP

Info

Disable

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

PrivateInstance-sg sg-0bb964694d751e1f3

VPC: vpc-028c6ded823f776b7

Compare security group rules

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

► Advanced network configuration

▼ Summary

Number of instances

Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.4.2...read more

ami-0ac67a26390dc374d

Virtual server type (instance type)

t2.micro

Firewall (security group)

PrivateInstance-sg

Storage (volumes)

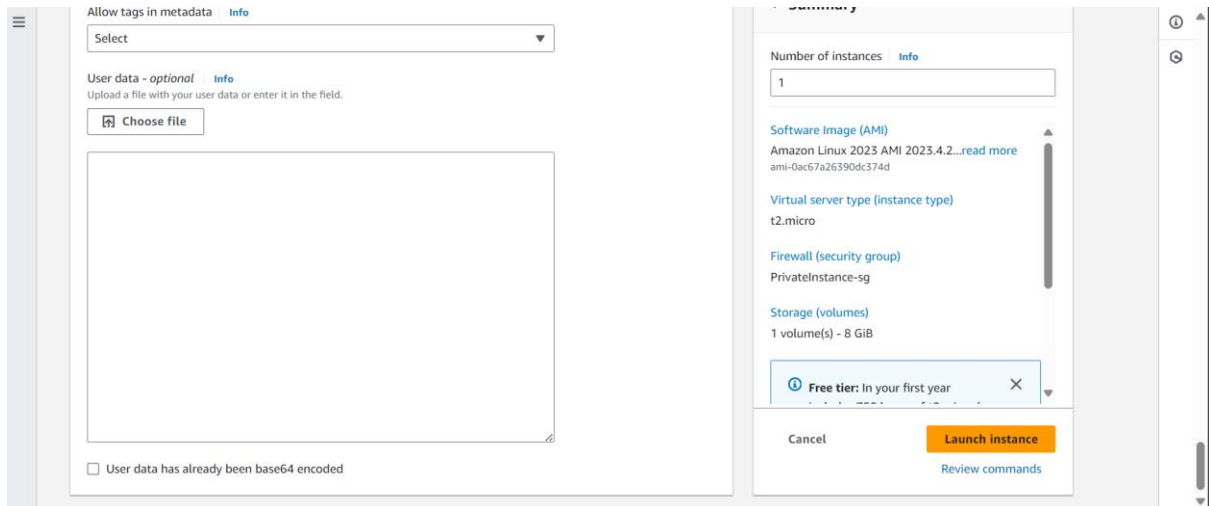
1 volume(s) - 8 GiB

Free tier: In your first year

Cancel

Launch instance

Review commands



Once the instance successfully Launched, login to EC2 insnstance and configure database and application and test Application Tier.

Internal Load Balancing and Auto Scaling