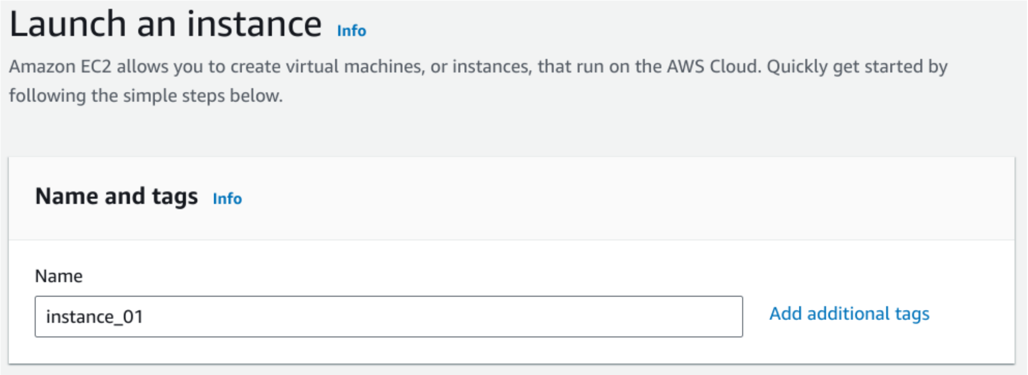
AWS Security

Day 3 - Assignment 12th July 2023

Assignment 1

Sharing AMI encrypted with KMS key between two AWS accounts.

Step 1 - Launch an EC2 instance in the first account.



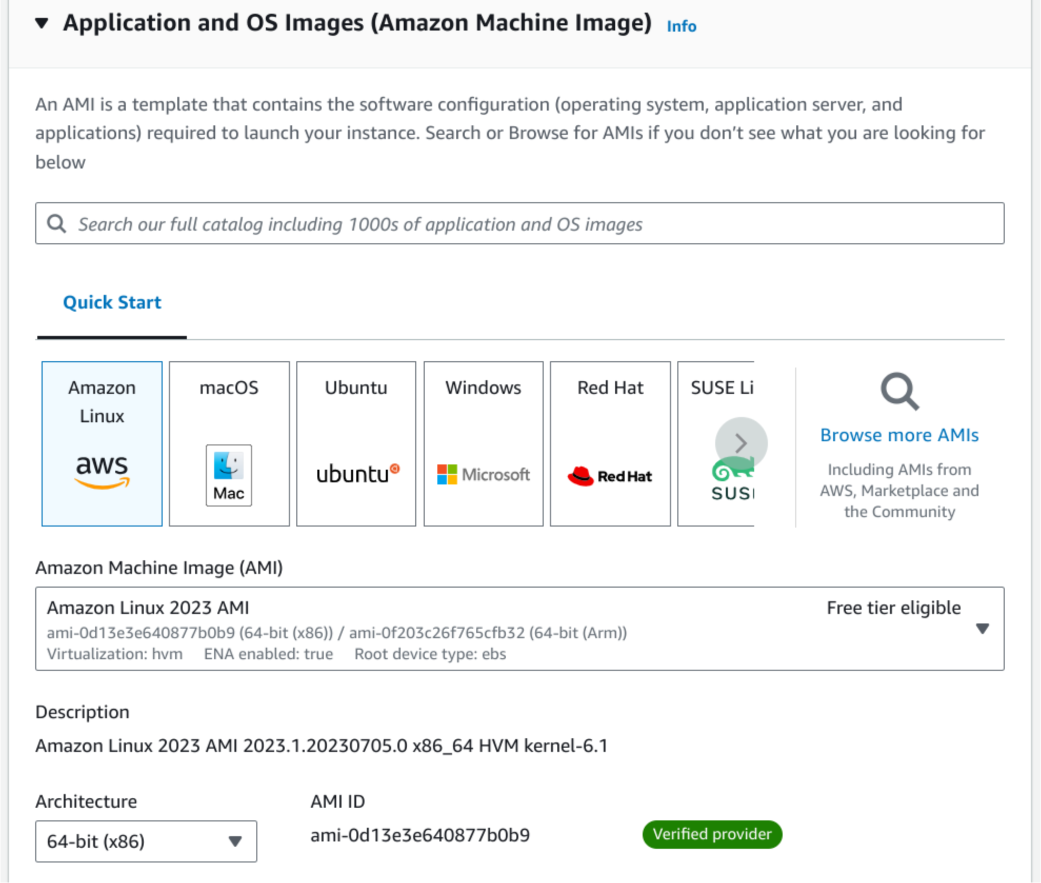
Launch an instance

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

Name

instance_01



Application and OS Images (Amazon Machine Image)

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

Amazon Machine Image (AMI)

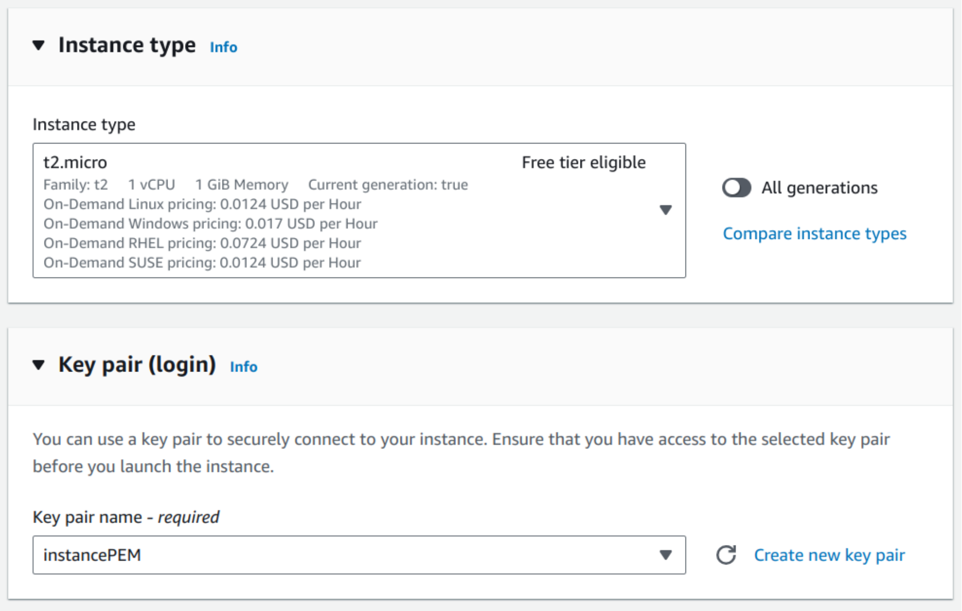
Amazon Linux 2023 AMI — Free tier eligible
ami-0d13e3e640877b0b9 (64-bit (x86)) / ami-0f203c26f765cfb32 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.1.20230705.0 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86)

AMI ID: ami-0d13e3e640877b0b9



▼ **Instance type** Info

Instance type

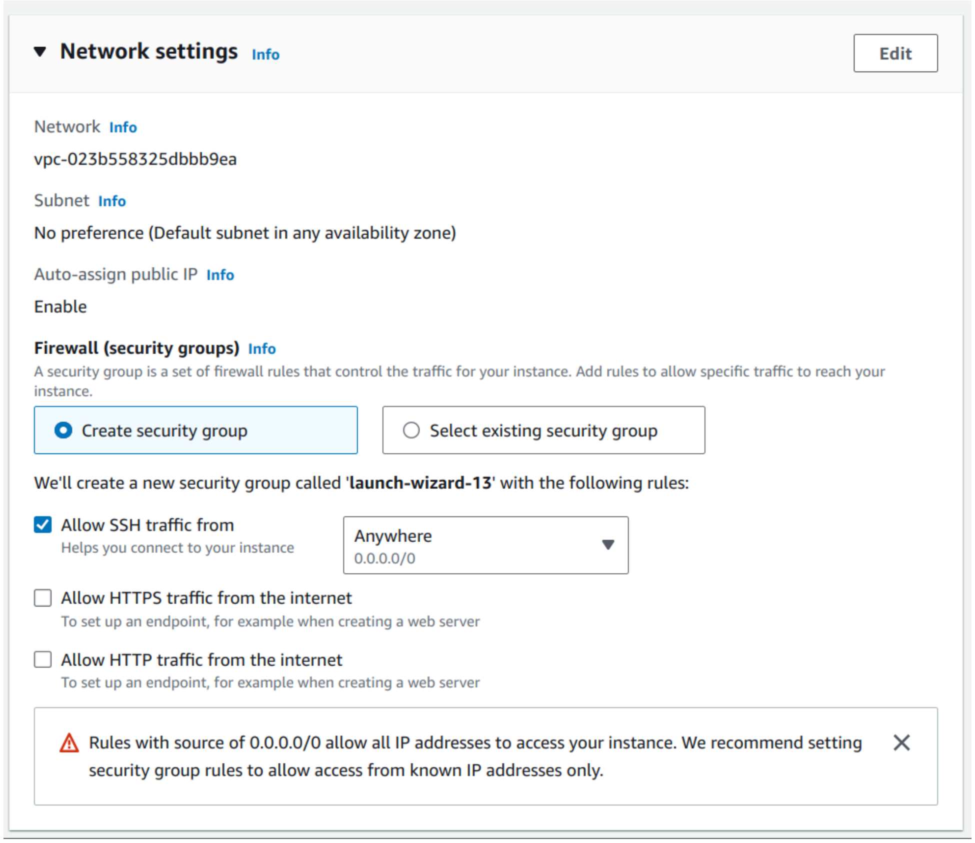
t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0124 USD per Hour
On-Demand Windows pricing: 0.017 USD per Hour
On-Demand RHEL pricing: 0.0724 USD per Hour
On-Demand SUSE pricing: 0.0124 USD per Hour

▼ **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*

instancePEM



▼ **Network settings** Info

Network Info
vpc-023b558325dbbb9ea

Subnet Info
No preference (Default subnet in any availability zone)

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

We'll create a new security group called '**launch-wizard-13**' with the following rules:

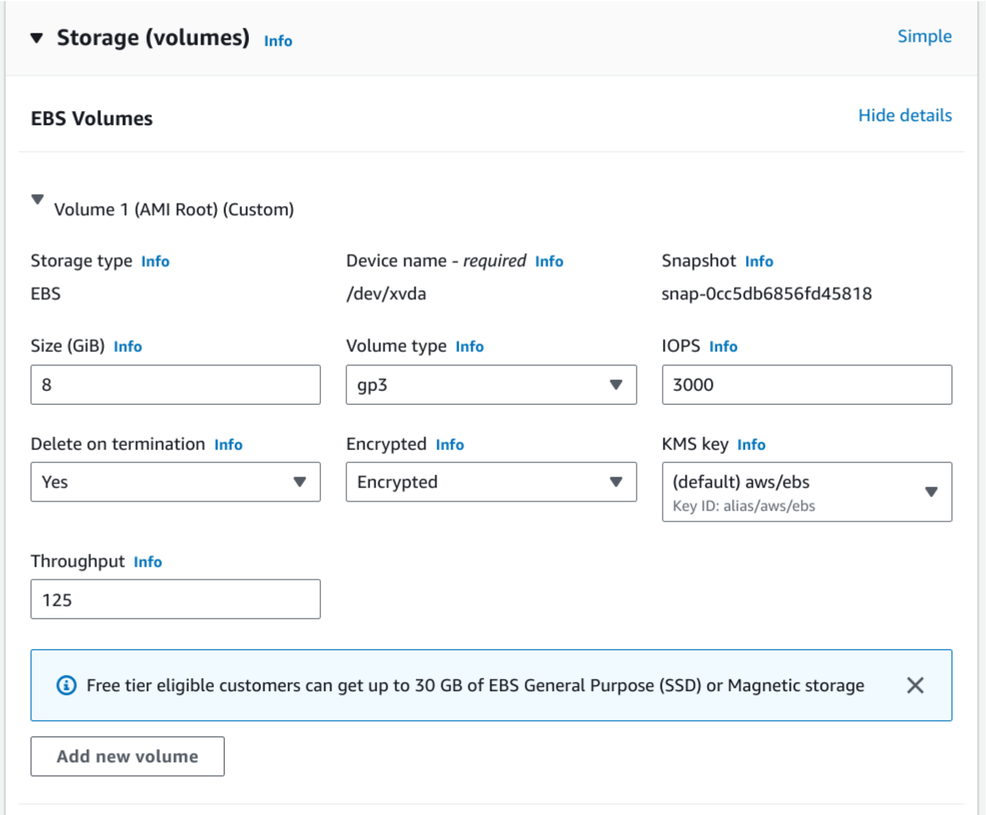
☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Encrypting the EBS volume attached to the instance, will create an encrypted AMI. Unencrypted AMI can be encrypted by creating an encrypted copy of it.



▼ Storage (volumes) Info — Simple

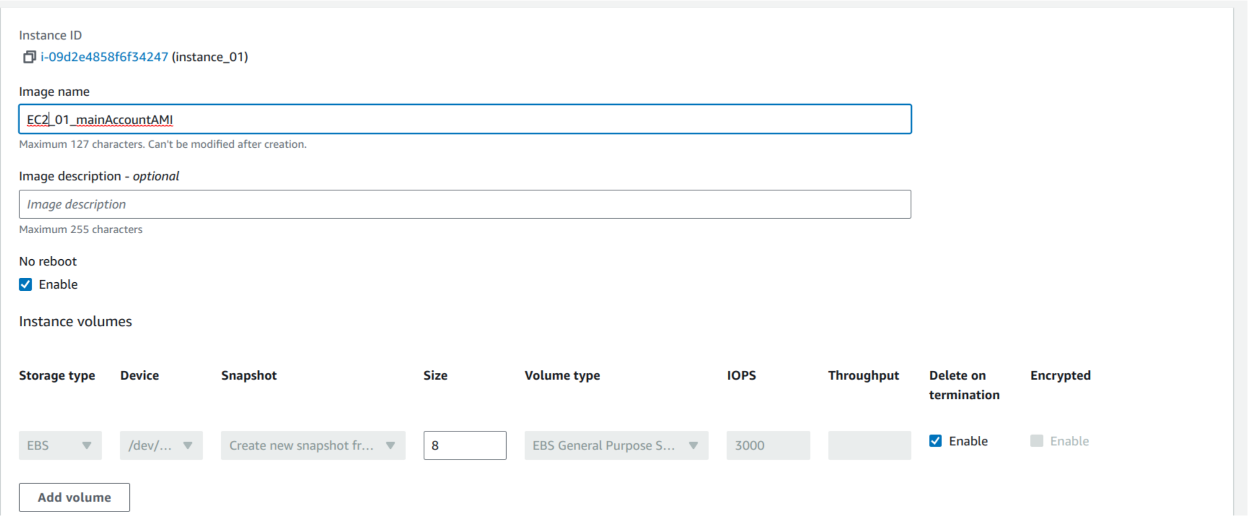
EBS Volumes — Hide details

▼ Volume 1 (AMI Root) (Custom)

Storage type Info EBS	Device name - *required* Info /dev/xvda	Snapshot Info snap-0cc5db6856fd45818
Size (GiB) Info 8	Volume type Info gp3	IOPS Info 3000
Delete on termination Info Yes	Encrypted Info Encrypted	KMS key Info (default) aws/ebs Key ID: alias/aws/ebs
Throughput Info 125		

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Step 2 - Create an image of the instance.



Instance ID
i-09d2e4858f6f34247 (instance_01)

Image name
EC2_01_mainAccountAMI
Maximum 127 characters. Can't be modified after creation.

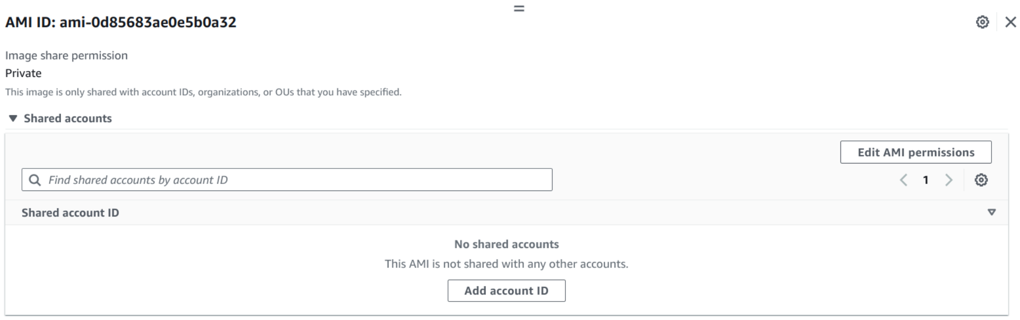
Image description - *optional*
Image description
Maximum 255 characters

No reboot
☑ Enable

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/…	Create new snapshot fr…	8	EBS General Purpose S…	3000		☑ Enable	□ Enable

Step 3 - Share the created AMI with another AWS account. Make sure that the AMI is encrypted.



AMI ID: ami-0d85683ae0e5b0a32

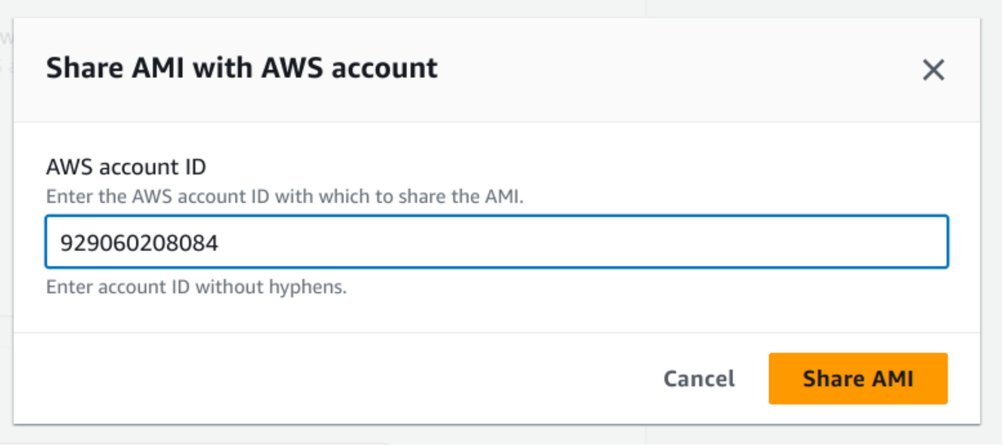
Image share permission
Private
This image is only shared with account IDs, organizations, or OUs that you have specified.

▼ Shared accounts

Find shared accounts by account ID

Shared account ID

No shared accounts
This AMI is not shared with any other accounts.



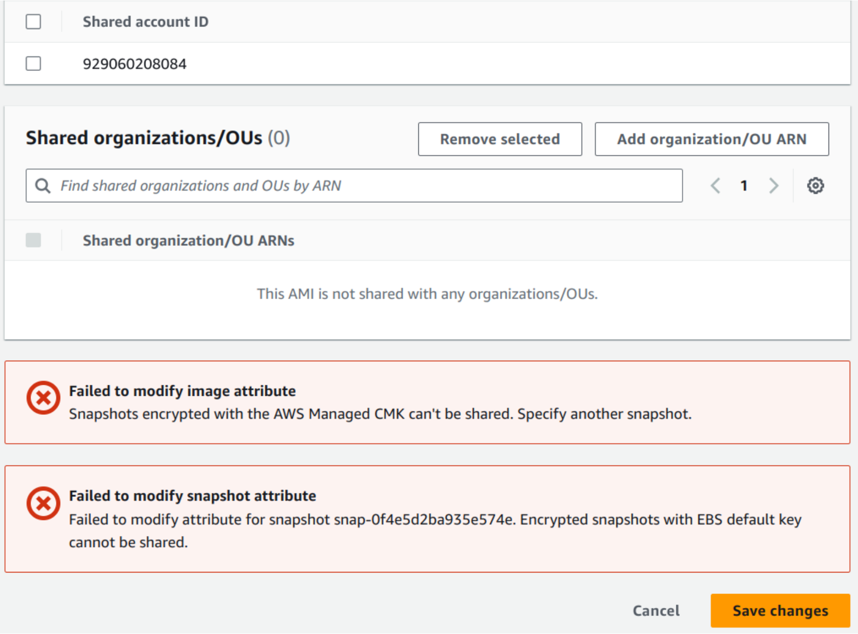
Share AMI with AWS account

AWS account ID
Enter the AWS account ID with which to share the AMI.

929060208084

Enter account ID without hyphens.

There is error sharing the AMI between accounts because EBS volumes encrypted using the KMS default key can not be shared with other accounts as default KMS keys are non shareable.



□ Shared account ID
□ 929060208084

Shared organizations/OUs (0)

Find shared organizations and OUs by ARN

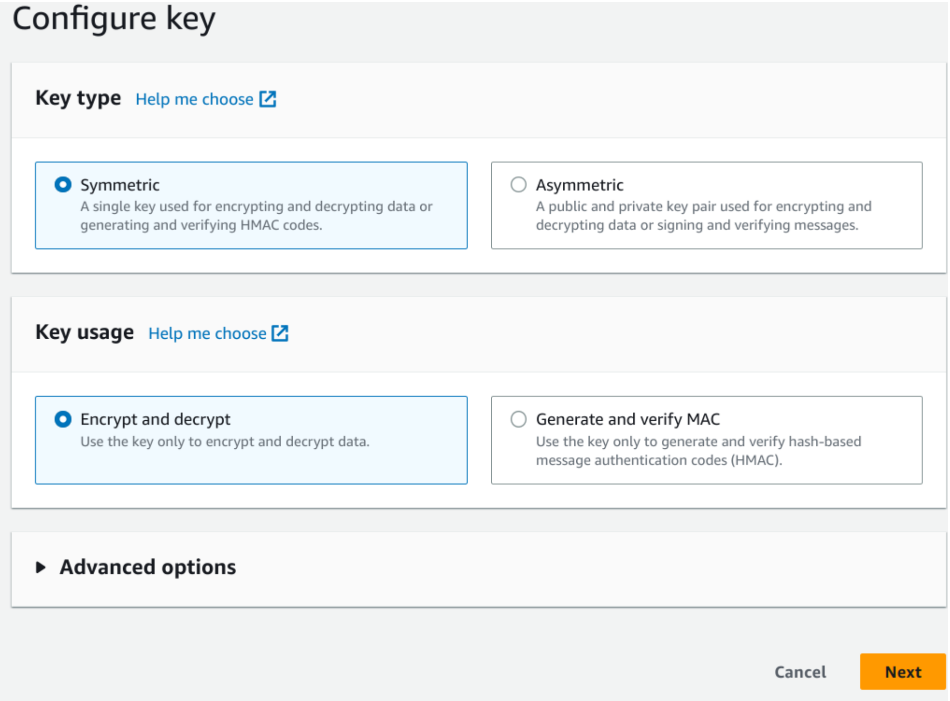
□ Shared organization/OU ARNs

This AMI is not shared with any organizations/OUs.

Failed to modify image attribute
Snapshots encrypted with the AWS Managed CMK can't be shared. Specify another snapshot.

Failed to modify snapshot attribute
Failed to modify attribute for snapshot snap-0f4e5d2ba935e574e. Encrypted snapshots with EBS default key cannot be shared.

Step 4 - Create a custom KMS key in KMS to encrypt the AMI.



Configure key

Key type Help me choose

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes.

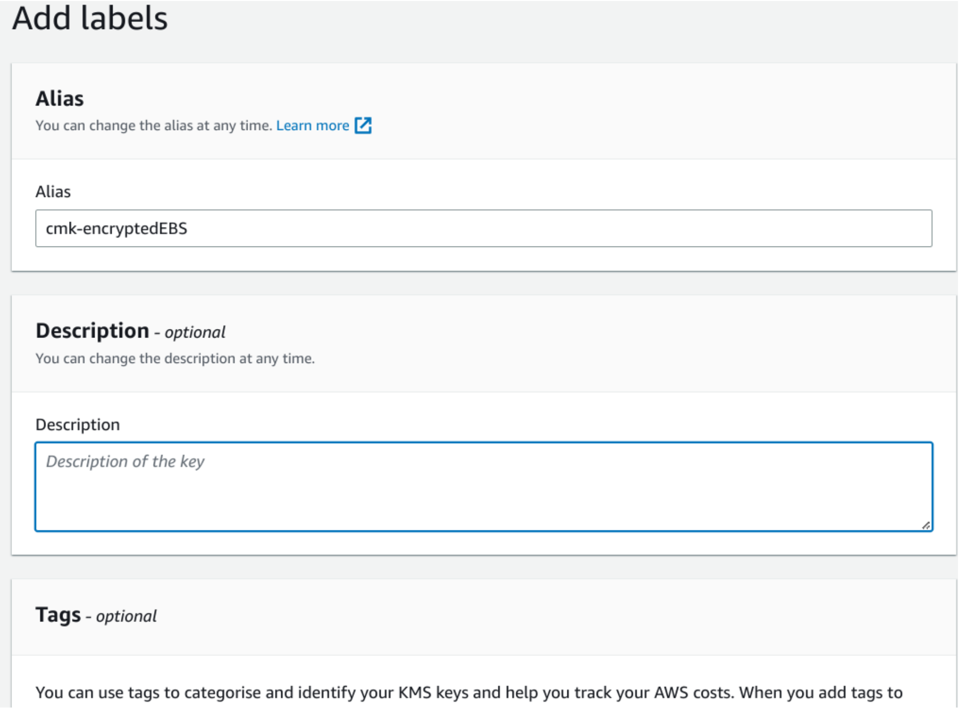
○ Asymmetric
A public and private key pair used for encrypting and decrypting data or signing and verifying messages.

Key usage Help me choose

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

▶ **Advanced options**



Add labels

Alias
You can change the alias at any time. Learn more

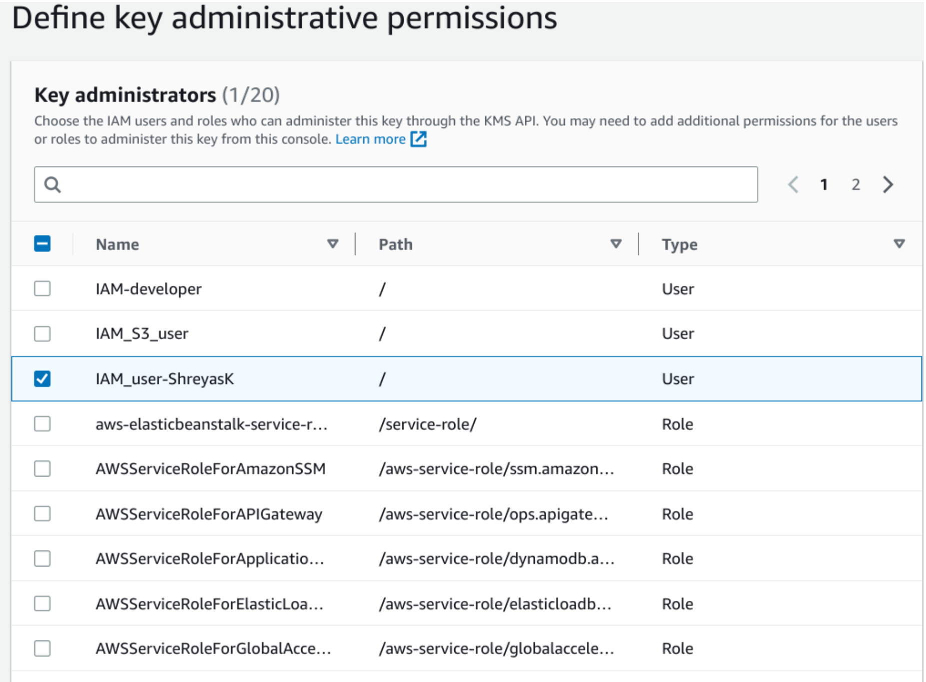
Alias: cmk-encryptedEBS

Description - *optional*
You can change the description at any time.

Description: *Description of the key*

Tags - *optional*

You can use tags to categorise and identify your KMS keys and help you track your AWS costs. When you add tags to

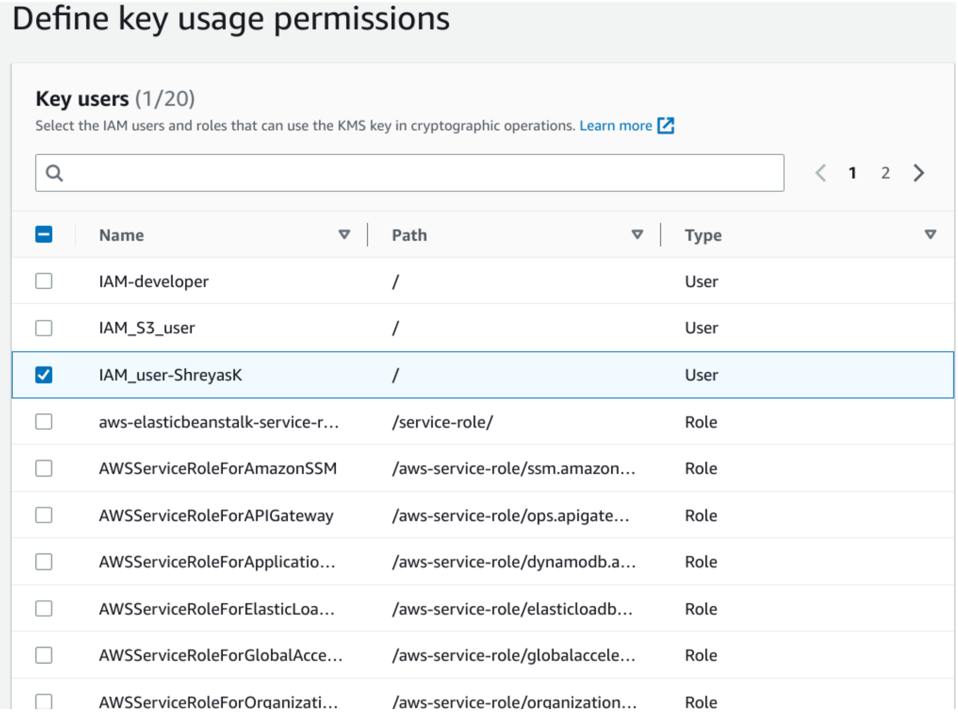


Define key administrative permissions

Key administrators (1/20)

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. Learn more

⊟	Name	Path	Type
☐	IAM-developer	/	User
☐	IAM_S3_user	/	User
☑	IAM_user-ShreyasK	/	User
☐	aws-elasticbeanstalk-service-r…	/service-role/	Role
☐	AWSServiceRoleForAmazonSSM	/aws-service-role/ssm.amazon…	Role
☐	AWSServiceRoleForAPIGateway	/aws-service-role/ops.apigate…	Role
☐	AWSServiceRoleForApplicatio…	/aws-service-role/dynamodb.a…	Role
☐	AWSServiceRoleForElasticLoa…	/aws-service-role/elasticloadb…	Role
☐	AWSServiceRoleForGlobalAcce…	/aws-service-role/globalaccele…	Role



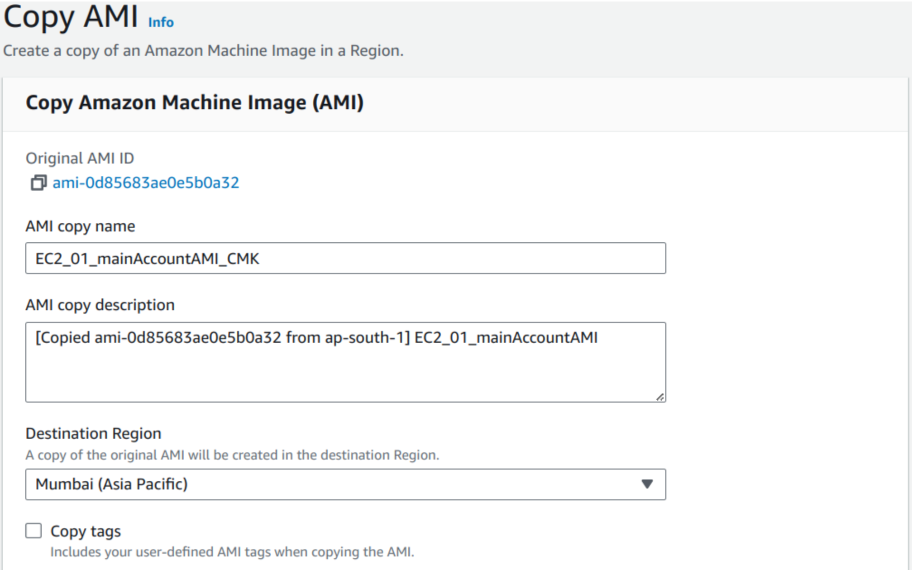
Define key usage permissions

Key users (1/20)

Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more

⊟	Name	Path	Type
☐	IAM-developer	/	User
☐	IAM_S3_user	/	User
☑	IAM_user-ShreyasK	/	User
☐	aws-elasticbeanstalk-service-r…	/service-role/	Role
☐	AWSServiceRoleForAmazonSSM	/aws-service-role/ssm.amazon…	Role
☐	AWSServiceRoleForAPIGateway	/aws-service-role/ops.apigate…	Role
☐	AWSServiceRoleForApplicatio…	/aws-service-role/dynamodb.a…	Role
☐	AWSServiceRoleForElasticLoa…	/aws-service-role/elasticloadb…	Role
☐	AWSServiceRoleForGlobalAcce…	/aws-service-role/globalaccele…	Role
☐	AWSServiceRoleForOrganizati…	/aws-service-role/organization…	Role

Step 5 - Create a copy of the AMI and select the custom KMS key created in the previous step for enabling encryption.



Copy AMI

Create a copy of an Amazon Machine Image in a Region.

Copy Amazon Machine Image (AMI)

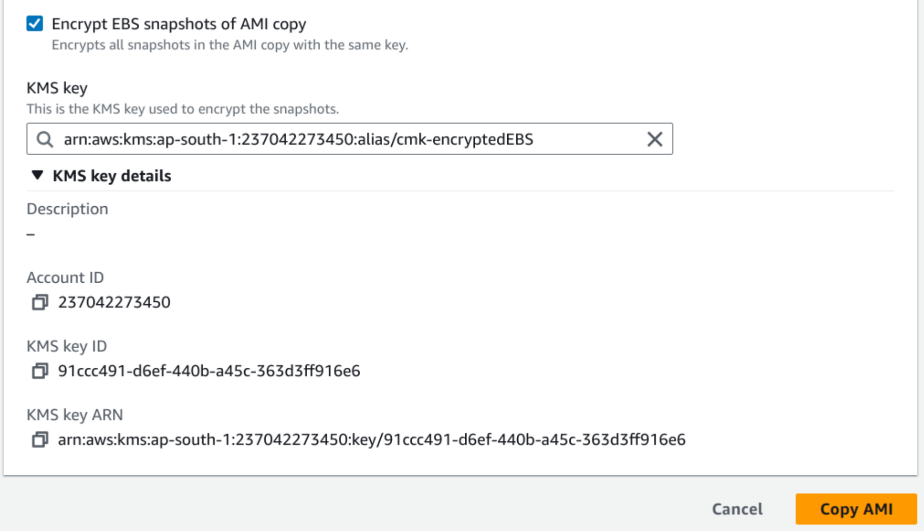
Original AMI ID
ami-0d85683ae0e5b0a32

AMI copy name
EC2_01_mainAccountAMI_CMK

AMI copy description
[Copied ami-0d85683ae0e5b0a32 from ap-south-1] EC2_01_mainAccountAMI

Destination Region
A copy of the original AMI will be created in the destination Region.
Mumbai (Asia Pacific)

☐ Copy tags
Includes your user-defined AMI tags when copying the AMI.



☑ Encrypt EBS snapshots of AMI copy
Encrypts all snapshots in the AMI copy with the same key.

KMS key
This is the KMS key used to encrypt the snapshots.
arn:aws:kms:ap-south-1:237042273450:alias/cmk-encryptedEBS

▼ KMS key details

Description
–

Account ID
237042273450

KMS key ID
91ccc491-d6ef-440b-a45c-363d3ff916e6

KMS key ARN
arn:aws:kms:ap-south-1:237042273450:key/91ccc491-d6ef-440b-a45c-363d3ff916e6

Step 6 - Share with another account by adding the account Id of the target account.

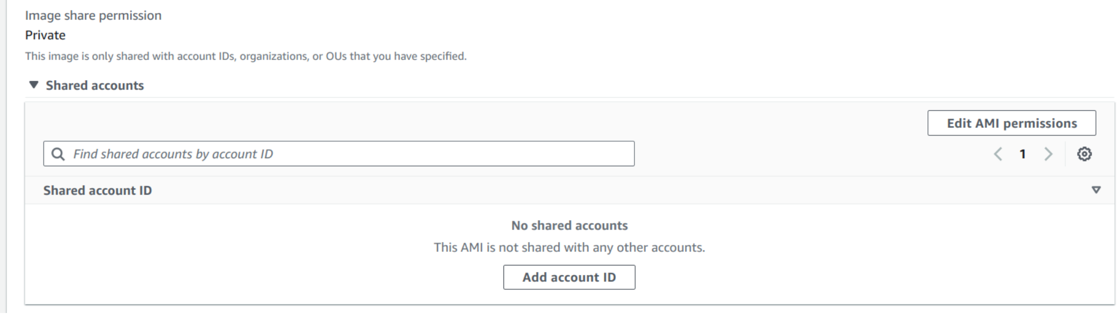
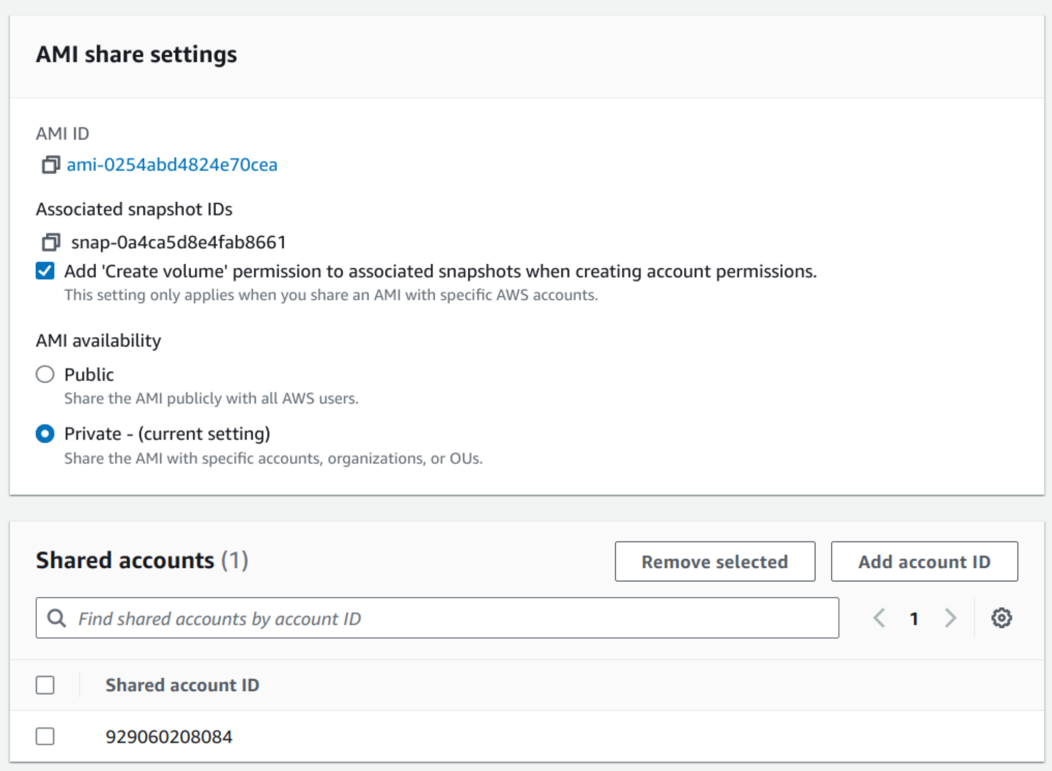


Image share permission
Private
This image is only shared with account IDs, organizations, or OUs that you have specified.

▼ Shared accounts

Shared account ID

No shared accounts
This AMI is not shared with any other accounts.



AMI share settings

AMI ID

ami-0254abd4824e70cea

Associated snapshot IDs

snap-0a4ca5d8e4fab8661

☑ Add 'Create volume' permission to associated snapshots when creating account permissions.
This setting only applies when you share an AMI with specific AWS accounts.

AMI availability

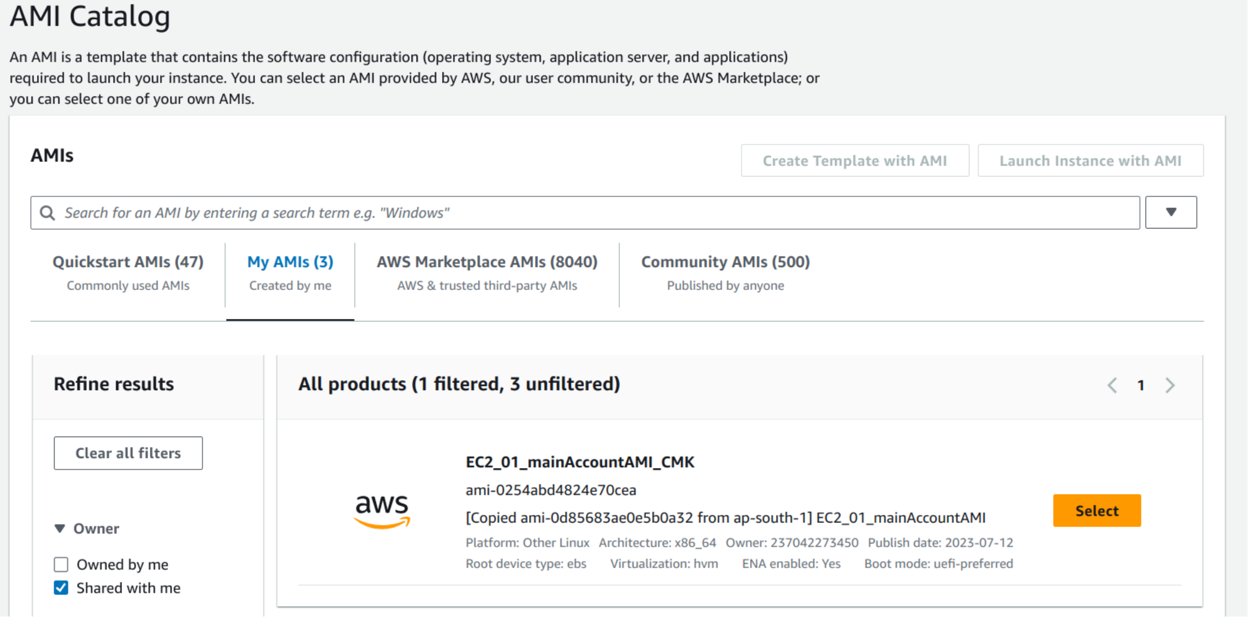
○ Public
Share the AMI publicly with all AWS users.

● Private - (current setting)
Share the AMI with specific accounts, organizations, or OUs.

Shared accounts (1)

□	Shared account ID
□	929060208084

Step 7 - Check if the AMI is visible in the target account. Here it is visible in the target account in the "shared with me" section.



AMI Catalog

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

AMIs

Owner

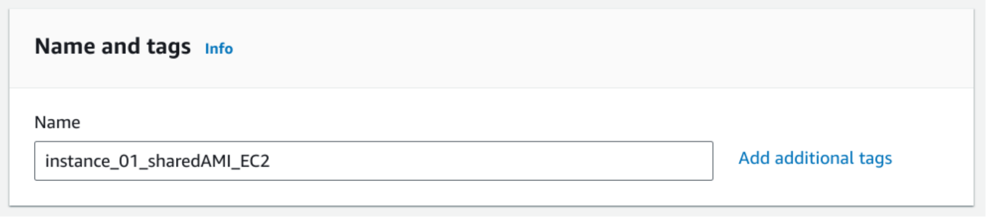
□ Owned by me

☑ Shared with me

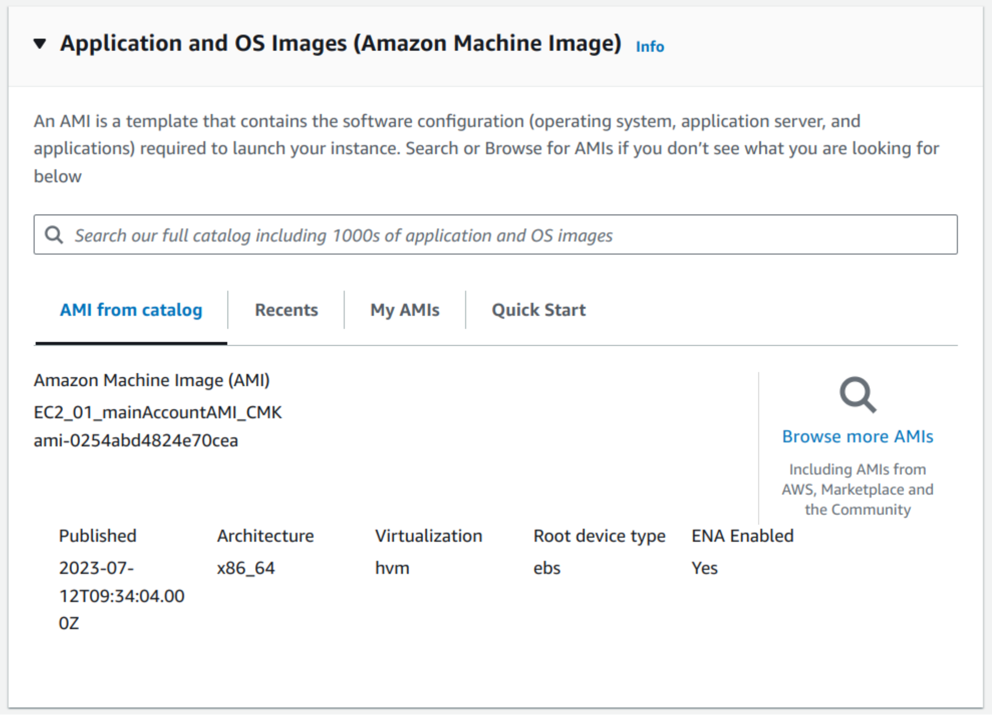
All products (1 filtered, 3 unfiltered)

EC2_01_mainAccountAMI_CMK
ami-0254abd4824e70cea
[Copied ami-0d85683ae0e5b0a32 from ap-south-1] EC2_01_mainAccountAMI
Platform: Other Linux Architecture: x86_64 Owner: 237042273450 Publish date: 2023-07-12
Root device type: ebs Virtualization: hvm ENA enabled: Yes Boot mode: uefi-preferred

Step 8 - Try to launch an instance using this AMI in the target account.


Name and tags Info

Name: instance_01_sharedAMI_EC2


Application and OS Images (Amazon Machine Image) Info

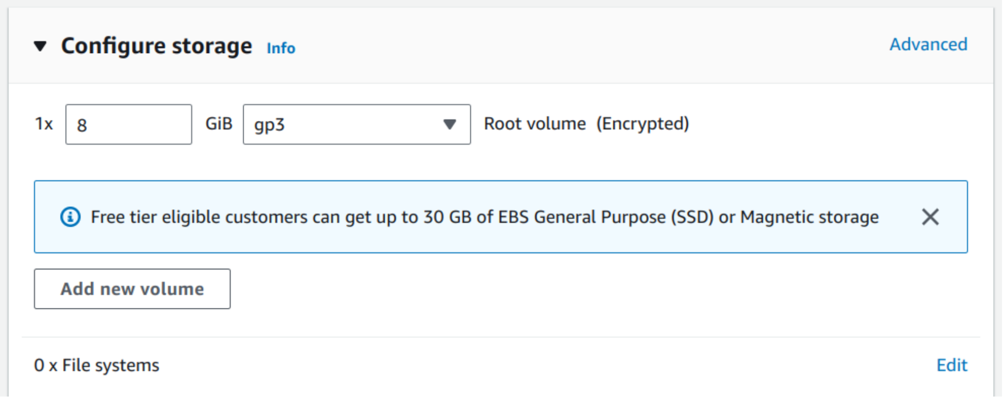
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)
EC2_01_mainAccountAMI_CMK
ami-0254abd4824e70cea

Published	Architecture	Virtualization	Root device type	ENA Enabled
2023-07-12T09:34:04.000Z	x86_64	hvm	ebs	Yes

The EBS volume is encrypted here by default because the AMI is encrypted.

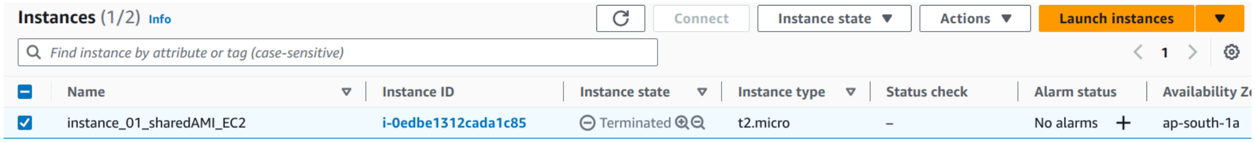

Configure storage Info

1x 8 GiB gp3 Root volume (Encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

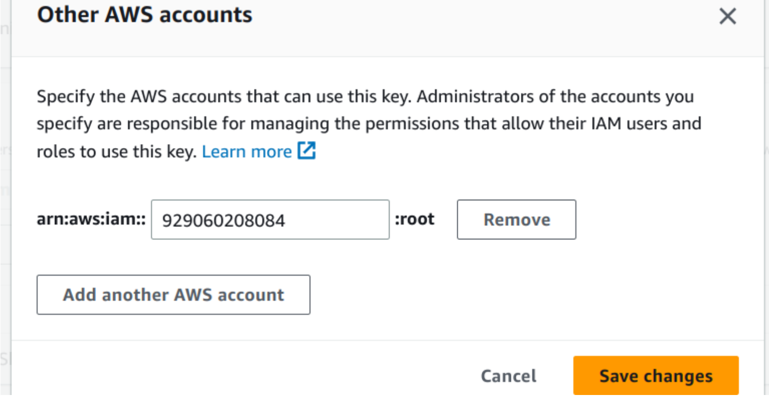
0 x File systems

Step 9 - The instance could not start and automatically terminated. Because the target account user does not have permission to access the KMS key in the source account which is used to encrypt the AMI.



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zo
☑	instance_01_sharedAMI_EC2	i-0edbe1312cada1c85	Terminated	t2.micro	–	No alarms	ap-south-1a

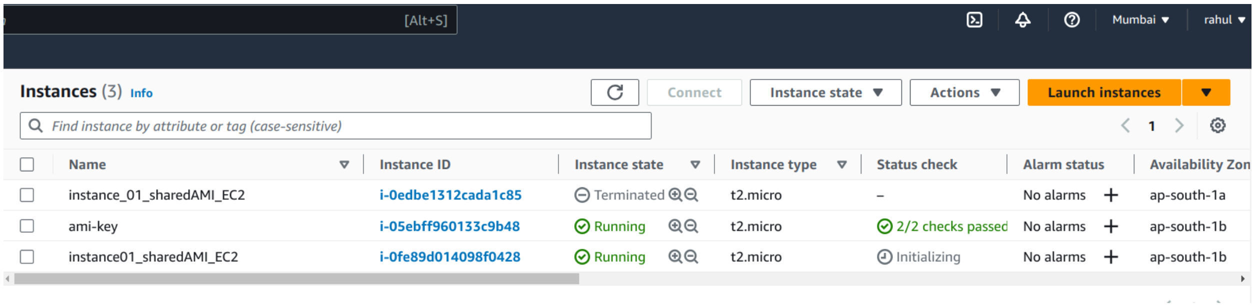
Step 10 - Change the configuration of the KMS key created in earlier steps. Specify the account or user which can access the KMS key.



Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more

arn:aws:iam:: 929060208084 :root

Step 11 - Launch another EC2 instance in the target account with the shared AMI. After giving access permission to the target account for the KMS key, the instance is launched and is running successfully.

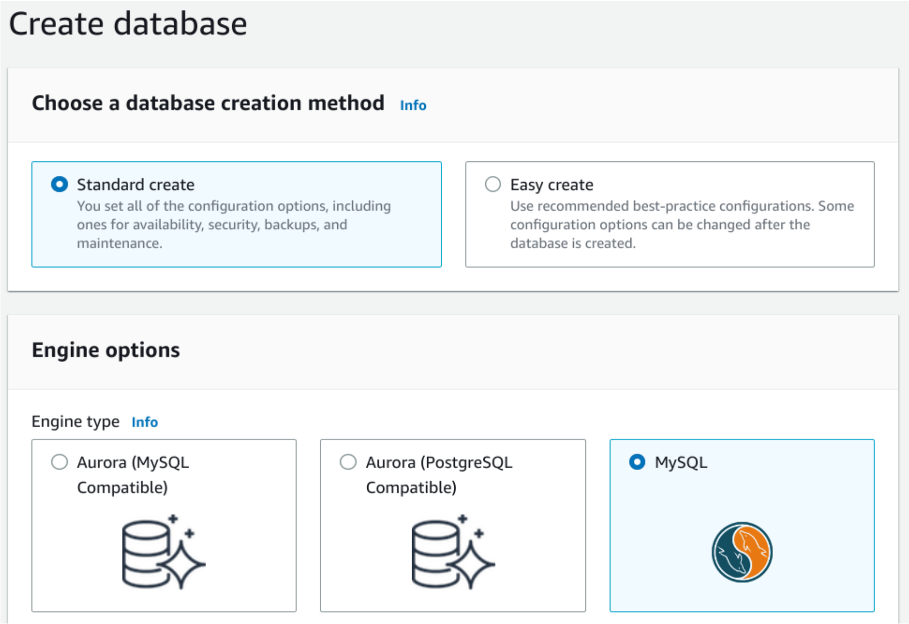


□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zon
□	instance_01_sharedAMI_EC2	i-0edbe1312cada1c85	Terminated	t2.micro	–	No alarms	ap-south-1a
□	ami-key	i-05ebff960133c9b48	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b
□	instance01_sharedAMI_EC2	i-0fe89d014098f0428	Running	t2.micro	Initializing	No alarms	ap-south-1b

Assignment 2

Store RDS database credentials in secrets manager.

Step 1 - Launch a RDS instance.



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.

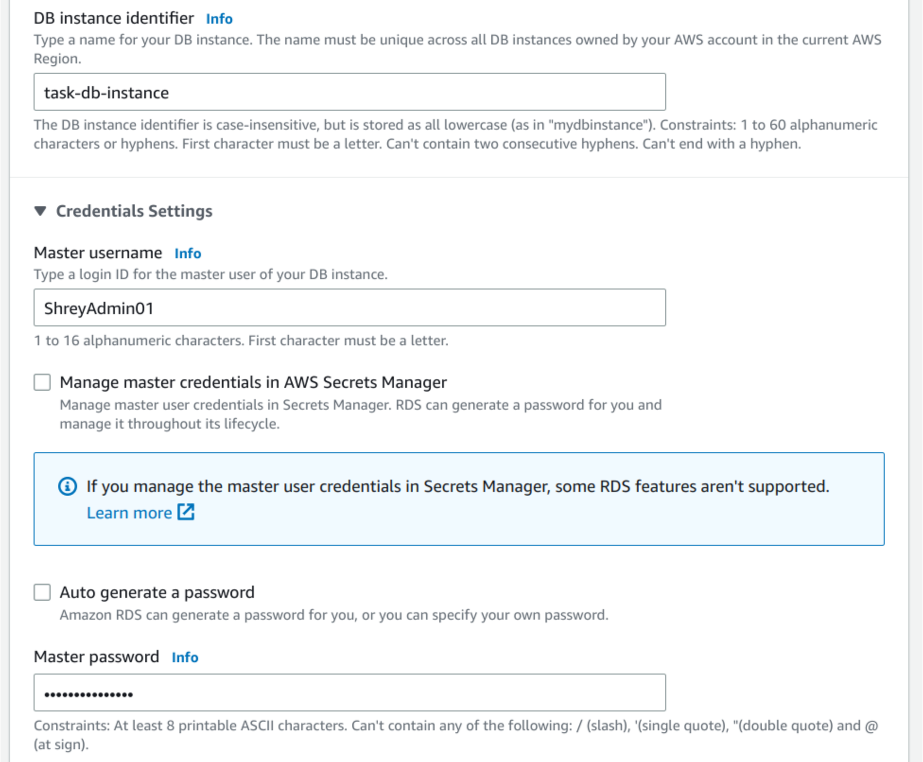
Engine options

Engine type Info

○ Aurora (MySQL Compatible)

○ Aurora (PostgreSQL Compatible)

● MySQL



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.

task-db-instance

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.

ShreyAdmin01

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.

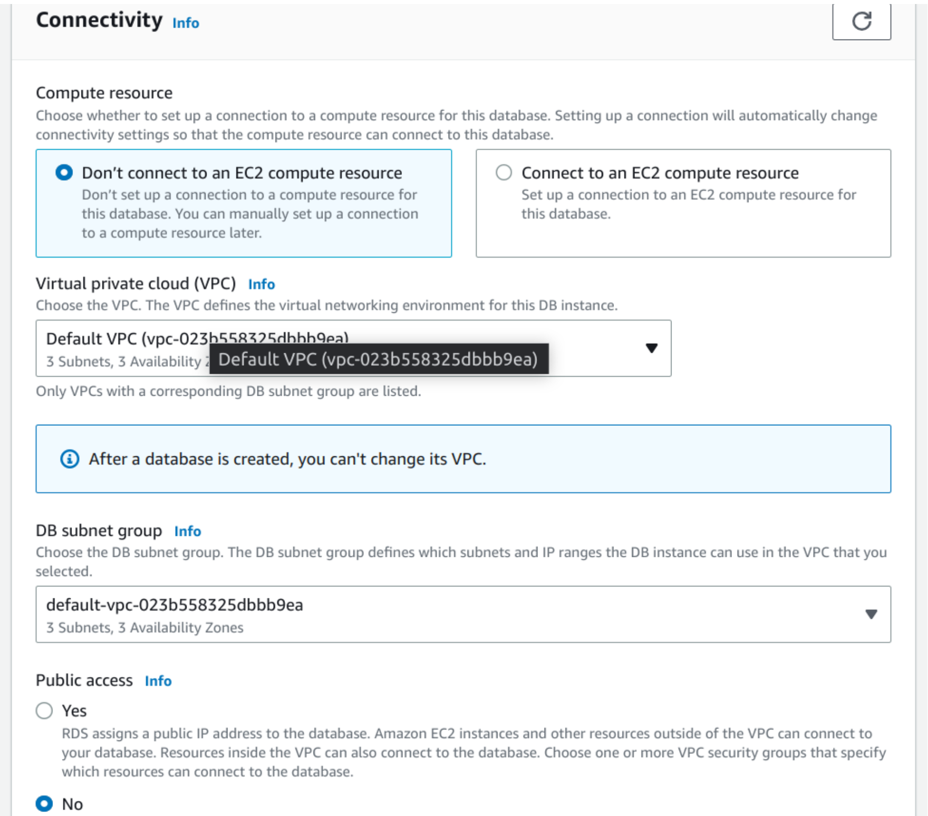
ⓘ If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
Learn more

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

Master password Info

•••••••••••••••

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).



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.

Virtual private cloud (VPC) Info

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

Default VPC (vpc-023b558325dbbb9ea)
3 Subnets, 3 Availability Z

Default VPC (vpc-023b558325dbbb9ea)

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

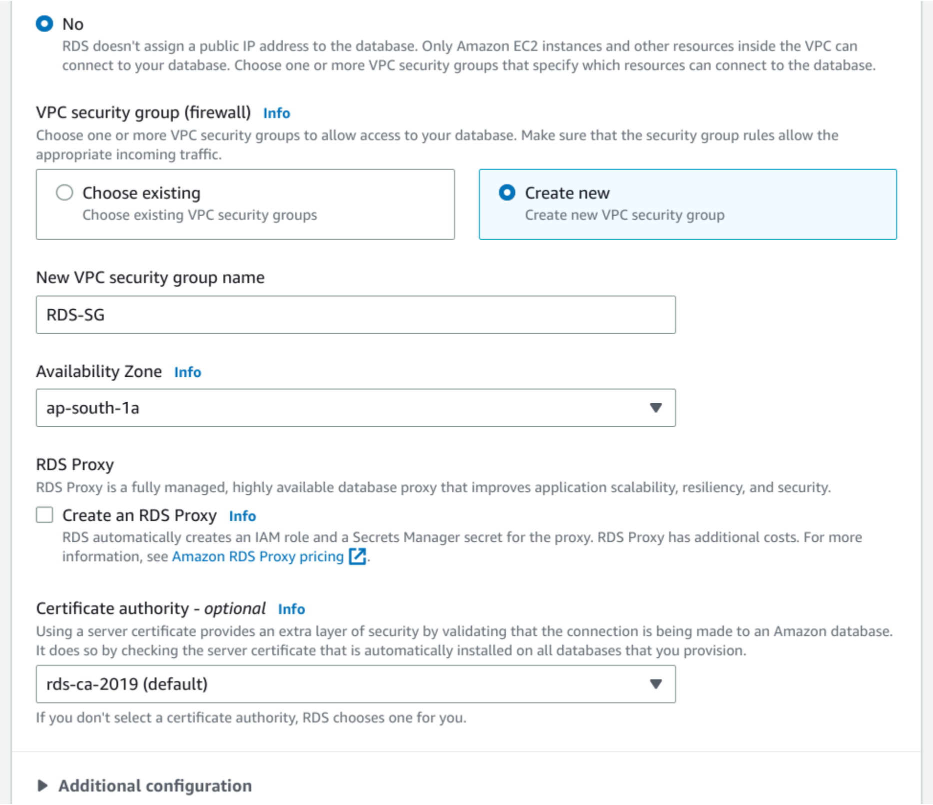
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

default-vpc-023b558325dbbb9ea
3 Subnets, 3 Availability Zones

Public access Info

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

● No



● No
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

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

New VPC security group name

RDS-SG

Availability Zone Info

ap-south-1a

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

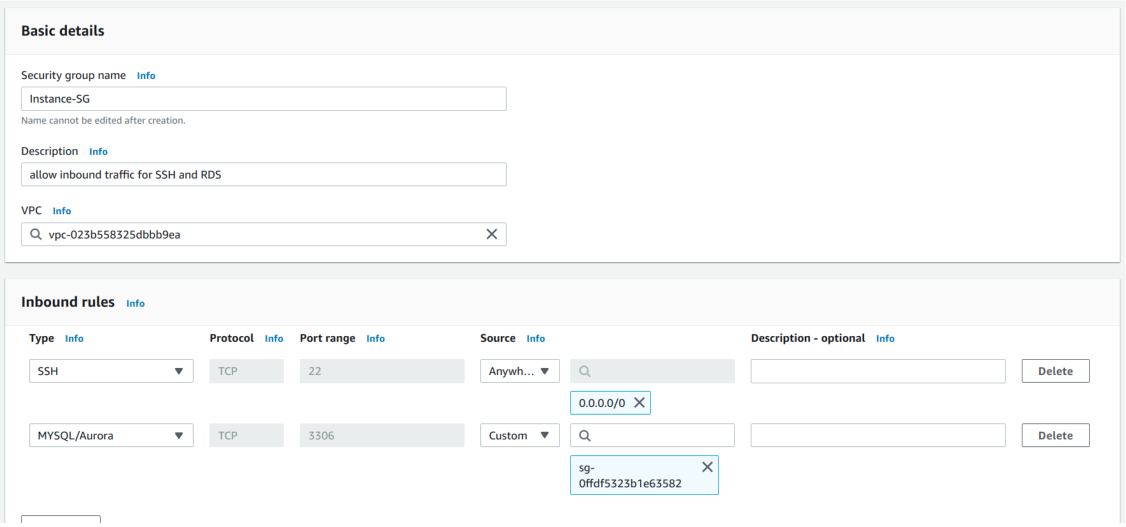
Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-2019 (default)

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

▶ **Additional configuration**

Step 2 - Create a security group for instance and allow “SSH” on port 22 and “MySql/Aurora” on port 3306, set source to RDS security group to allow the RDS instance to connect with the instance.



Basic details

Security group name: Instance-SG

Name cannot be edited after creation.

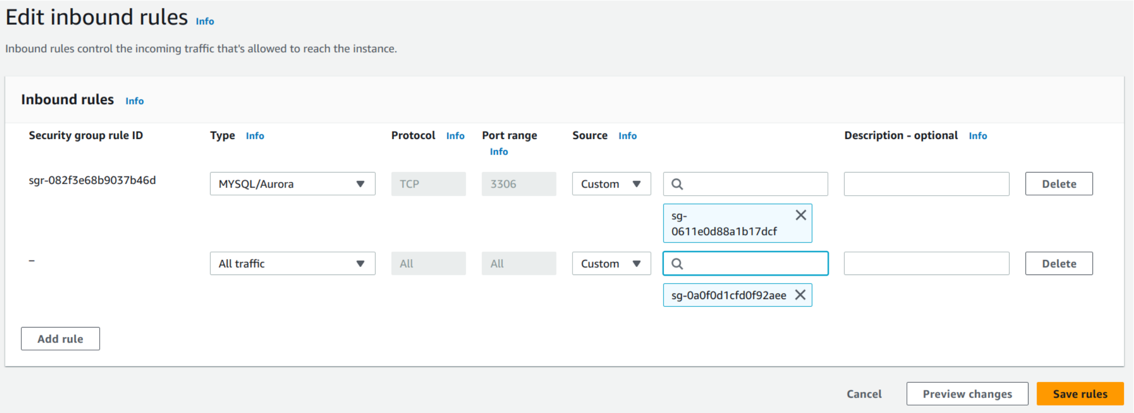
Description: allow inbound traffic for SSH and RDS

VPC: vpc-023b558325dbbb9ea

Inbound rules

Type	Protocol	Port range	Source		Description - optional
SSH	TCP	22	Anywh...	0.0.0.0/0	
MYSQL/Aurora	TCP	3306	Custom	sg-0ffdf5323b1e63582	

Step 3 - Configure the Security group associated with the RDS instance to allow inbound traffic from the EC2 instance’s security group.



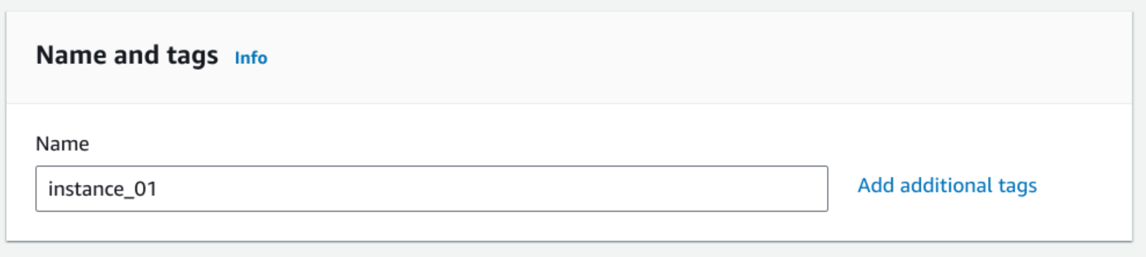
Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules

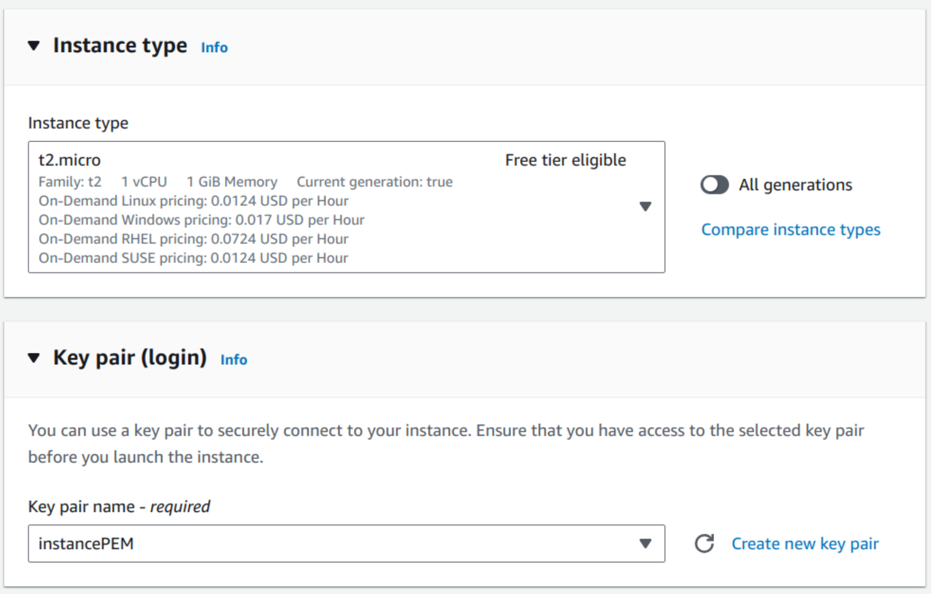
Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-082f3e68b9037b46d	MYSQL/Aurora	TCP	3306	Custom	sg-0611e0d88a1b17dcf	
–	All traffic	All	All	Custom	sg-0a0f0d1cfd0f92aee	

Step 4 - Launch an EC2 instance and attach the previously created security group.



Name and tags

Name: instance_01



▼ **Instance type** Info

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0124 USD per Hour
On-Demand Windows pricing: 0.017 USD per Hour
On-Demand RHEL pricing: 0.0724 USD per Hour
On-Demand SUSE pricing: 0.0124 USD per Hour

All generations

Compare instance types

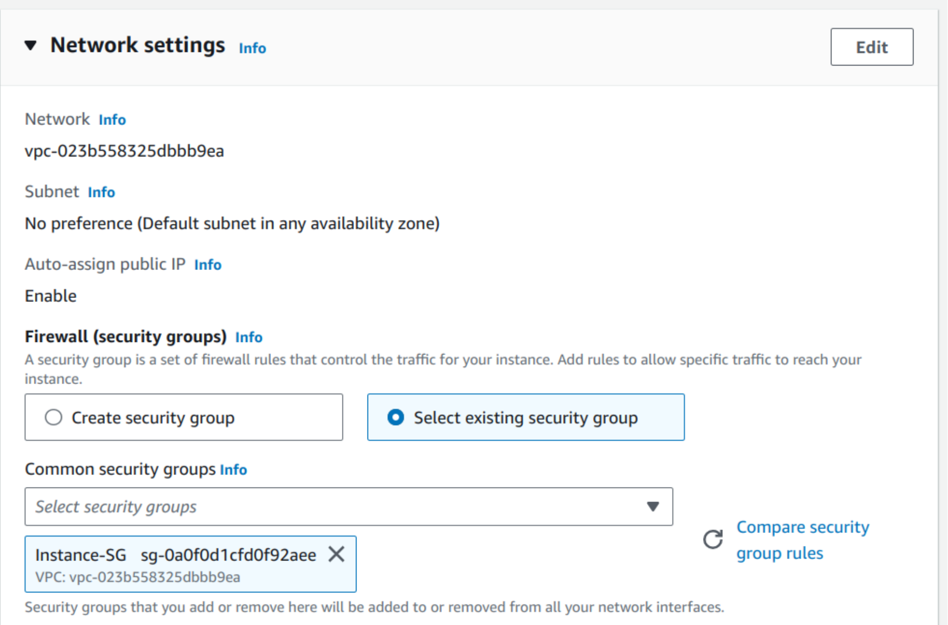
▼ **Key pair (login)** Info

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*

instancePEM

Create new key pair



▼ **Network settings** Info

Edit

Network Info
vpc-023b558325dbbb9ea

Subnet Info
No preference (Default subnet in any availability zone)

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

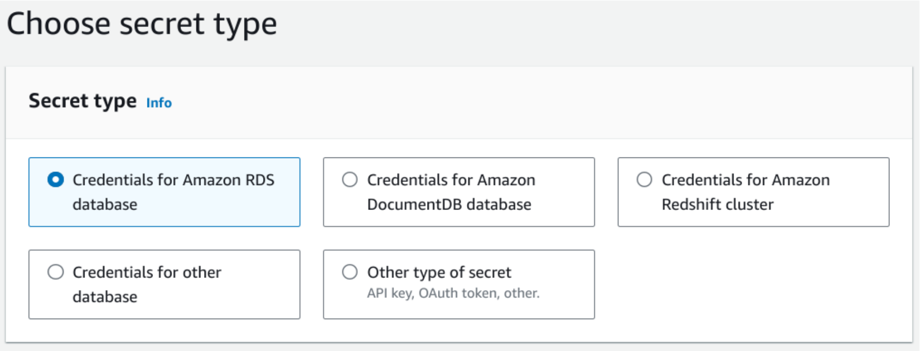
Select security groups

Instance-SG sg-0a0f0d1cfd0f92aee ✕
VPC: vpc-023b558325dbbb9ea

Compare security group rules

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

Step 5 - Add the RDS database credentials to AWS secrets manager.



Choose secret type

Secret type Info

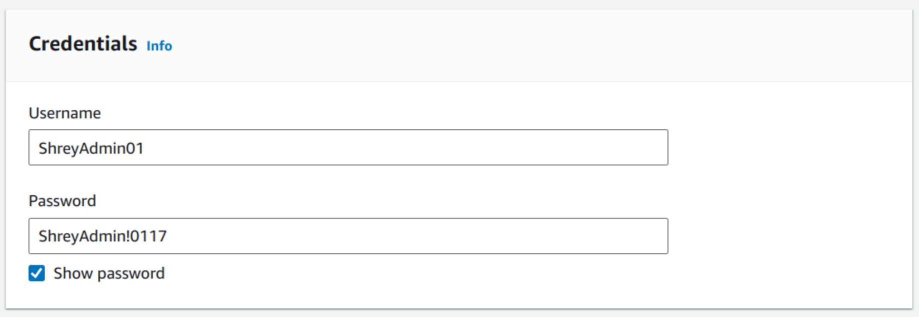
● Credentials for Amazon RDS database

○ Credentials for Amazon DocumentDB database

○ Credentials for Amazon Redshift cluster

○ Credentials for other database

○ Other type of secret
API key, OAuth token, other.



Credentials Info

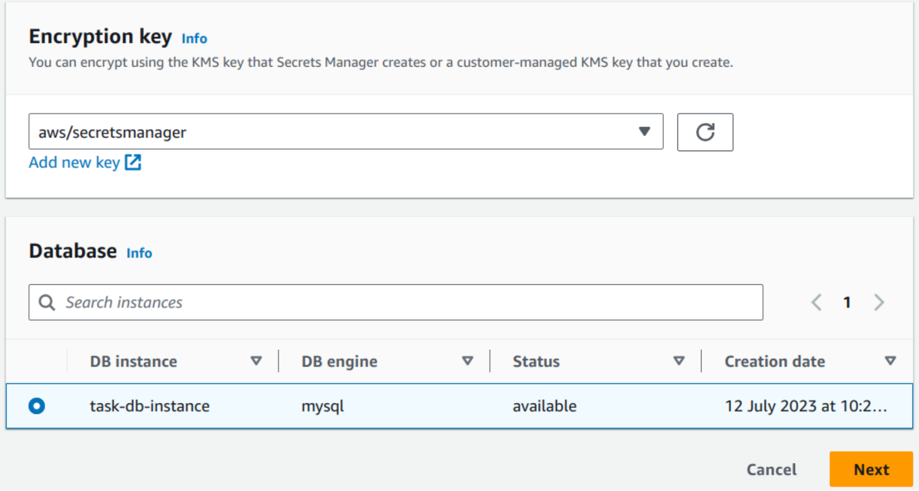
Username

ShreyAdmin01

Password

ShreyAdmin!0117

☑ Show password



Encryption key Info

You can encrypt using the KMS key that Secrets Manager creates or a customer-managed KMS key that you create.

aws/secretsmanager ▼

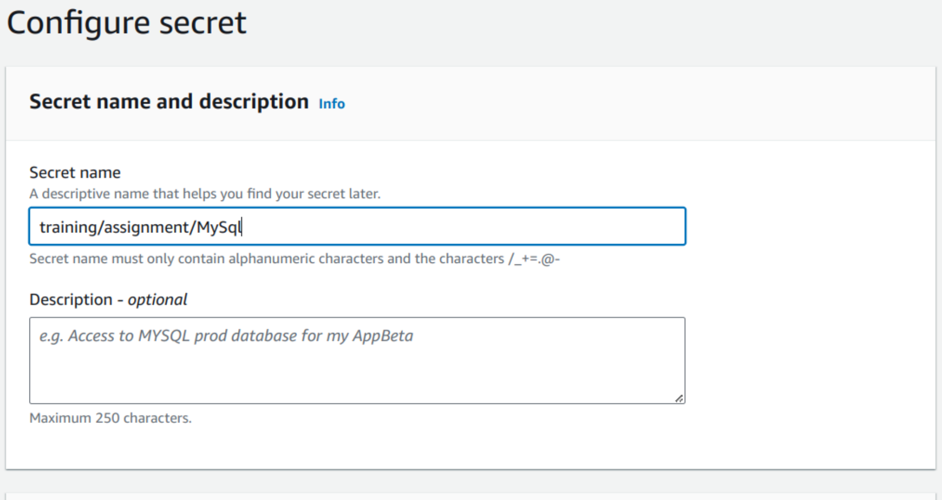
Add new key

Database Info

Search instances

< 1 >

	DB instance	DB engine	Status	Creation date
●	task-db-instance	mysql	available	12 July 2023 at 10:2…



Configure secret

Secret name and description Info

Secret name

A descriptive name that helps you find your secret later.

training/assignment/MySql

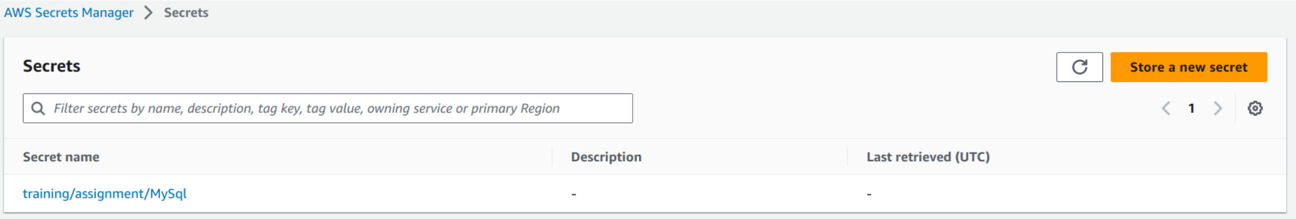
Secret name must only contain alphanumeric characters and the characters /_+=.@-

Description - *optional*

e.g. Access to MYSQL prod database for my AppBeta

Maximum 250 characters.

Secret is created successfully.



AWS Secrets Manager > Secrets

Secrets

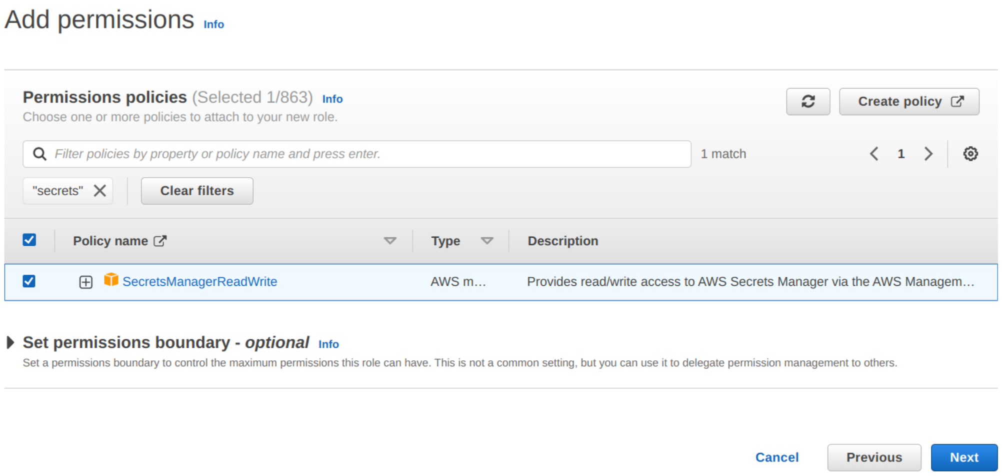
Filter secrets by name, description, tag key, tag value, owning service or primary Region

< 1 >

Secret name	Description	Last retrieved (UTC)
training/assignment/MySql	-	-

Step 6 - Attach IAM role to the instance to allow it to access secrets in the secret manager.

The policy “SecretsManagerReadWrite” allows the instance to access the secrets in the secrets manager.



Add permissions Info

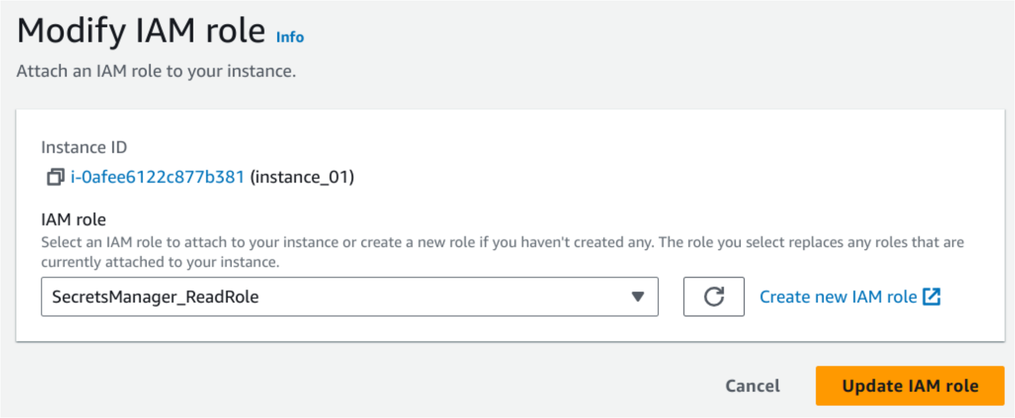
Permissions policies (Selected 1/863) Info

Choose one or more policies to attach to your new role.

☑	Policy name	Type	Description
☑	SecretsManagerReadWrite	AWS m…	Provides read/write access to AWS Secrets Manager via the AWS Managem…

Set permissions boundary - *optional* Info

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.



Modify IAM role Info

Attach an IAM role to your instance.

Instance ID

i-0afee6122c877b381 (instance_01)

IAM role

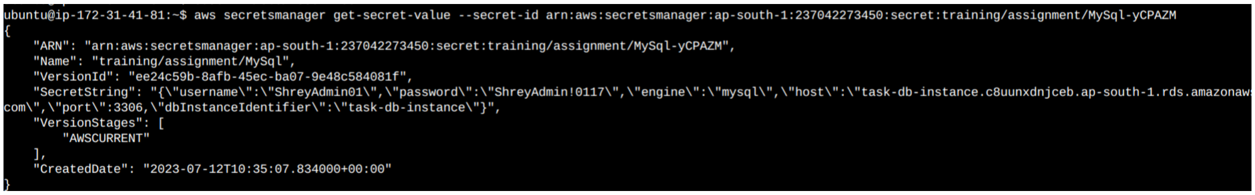
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

SecretsManager_ReadRole

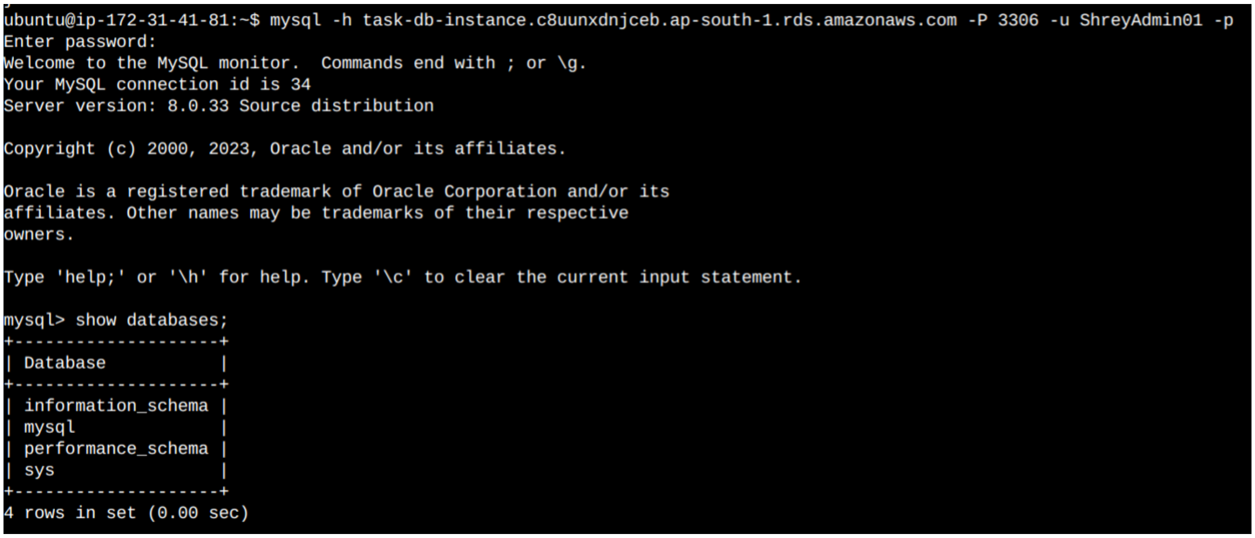
Step 7 - Connect to the EC2 instance and retrieve the credentials of the RDS instance stored in the secrets manager.

Run the “aws secretmanager get-secret-value” command with the Secret ARN value.

It returns the secret value that is the username and password of the database.



```
ubuntu@ip-172-31-41-81:~$ aws secretsmanager get-secret-value --secret-id arn:aws:secretsmanager:ap-south-1:237042273450:secret:training/assignment/MySql-yCPAZM
{
    "ARN": "arn:aws:secretsmanager:ap-south-1:237042273450:secret:training/assignment/MySql-yCPAZM",
    "Name": "training/assignment/MySql",
    "VersionId": "ee24c59b-8afb-45ec-ba07-9e48c584081f",
    "SecretString": "{\"username\":\"ShreyAdmin01\",\"password\":\"ShreyAdmin!0117\",\"engine\":\"mysql\",\"host\":\"task-db-instance.c8uunxdnjceb.ap-south-1.rds.amazonaw
com\",\"port\":3306,\"dbInstanceIdentifier\":\"task-db-instance\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2023-07-12T10:35:07.834000+00:00"
}
```



```
ubuntu@ip-172-31-41-81:~$ mysql -h task-db-instance.c8uunxdnjceb.ap-south-1.rds.amazonaws.com -P 3306 -u ShreyAdmin01 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 34
Server version: 8.0.33 Source distribution

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.00 sec)
```