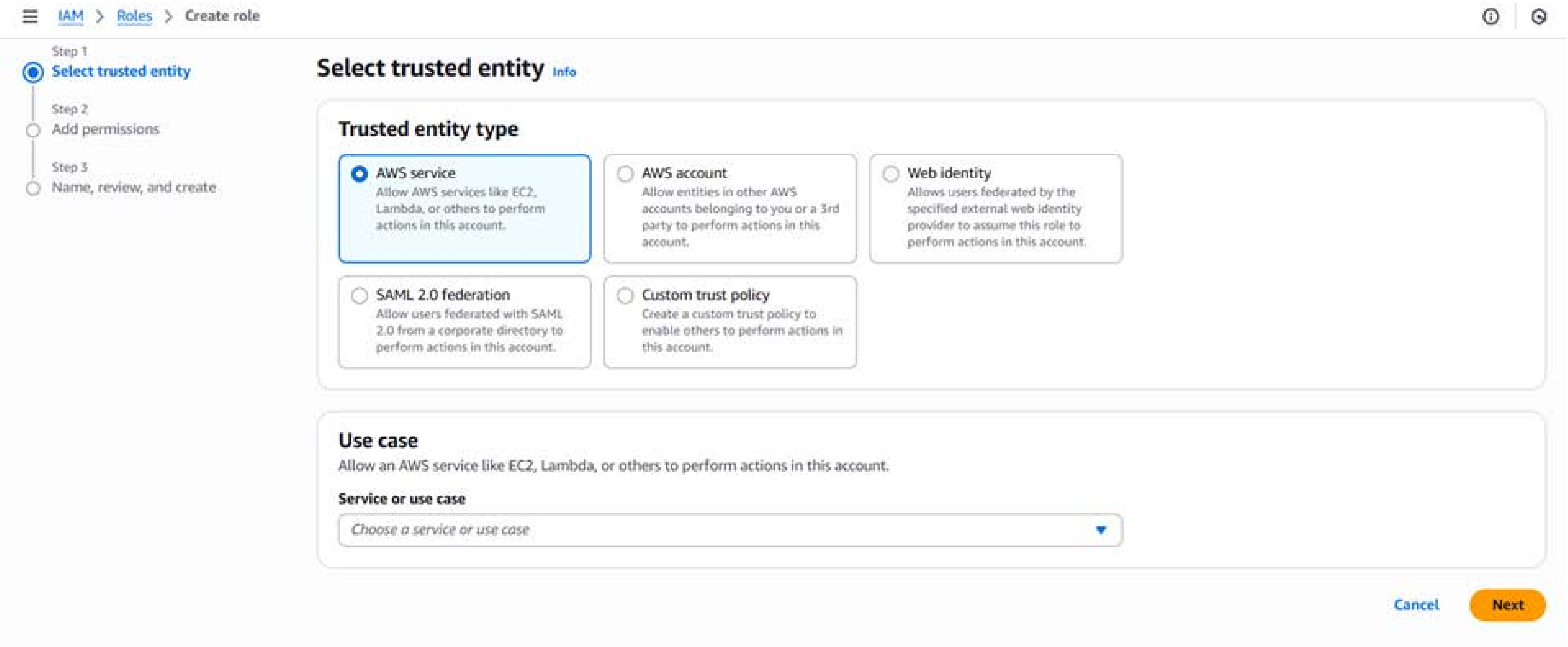
Второе задание



IAM > Roles > Create role

Step 1
● Select trusted entity

Step 2
○ Add permissions

Step 3
○ Name, review, and create

Select trusted entity Info

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.

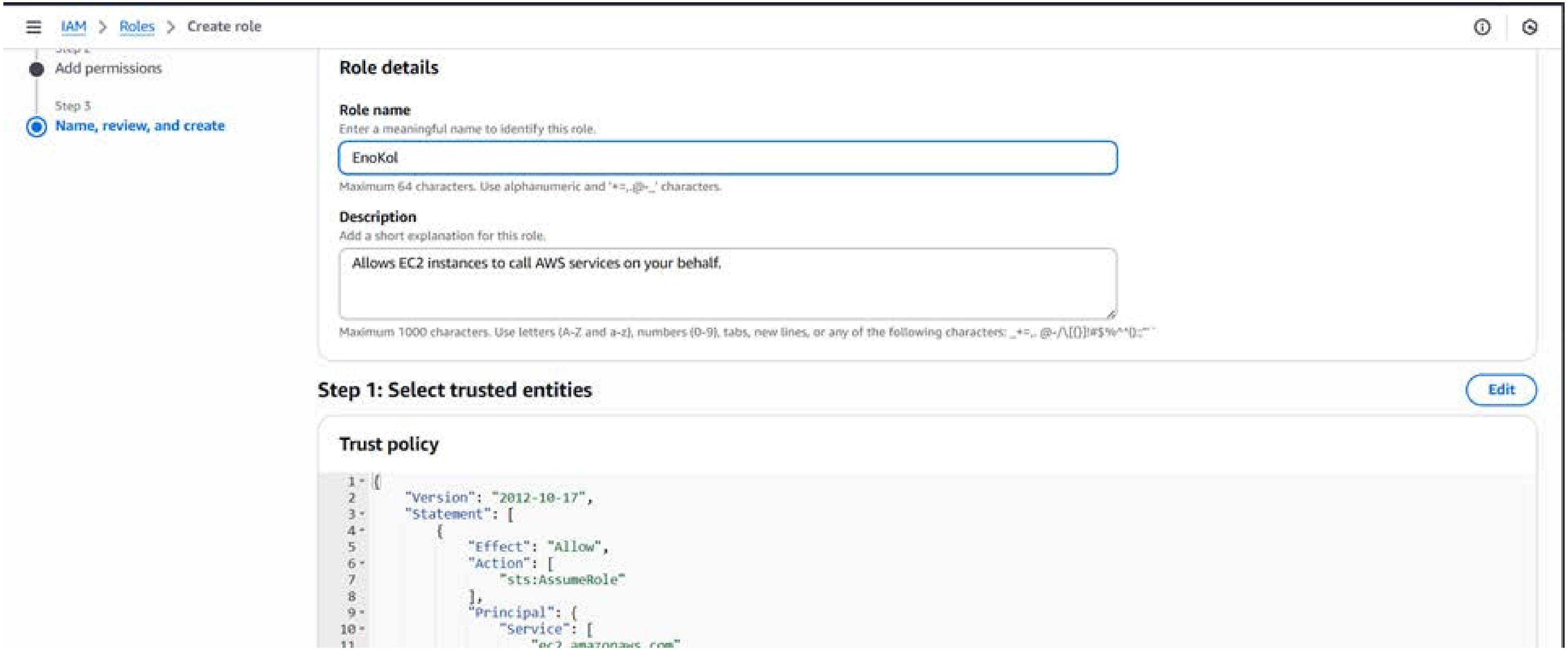
Use case

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

Service or use case

Choose a service or use case ▼

Cancel Next



Role details

Role name

Enter a meaningful name to identify this role.

EnoKol

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

Add a short explanation for this role.

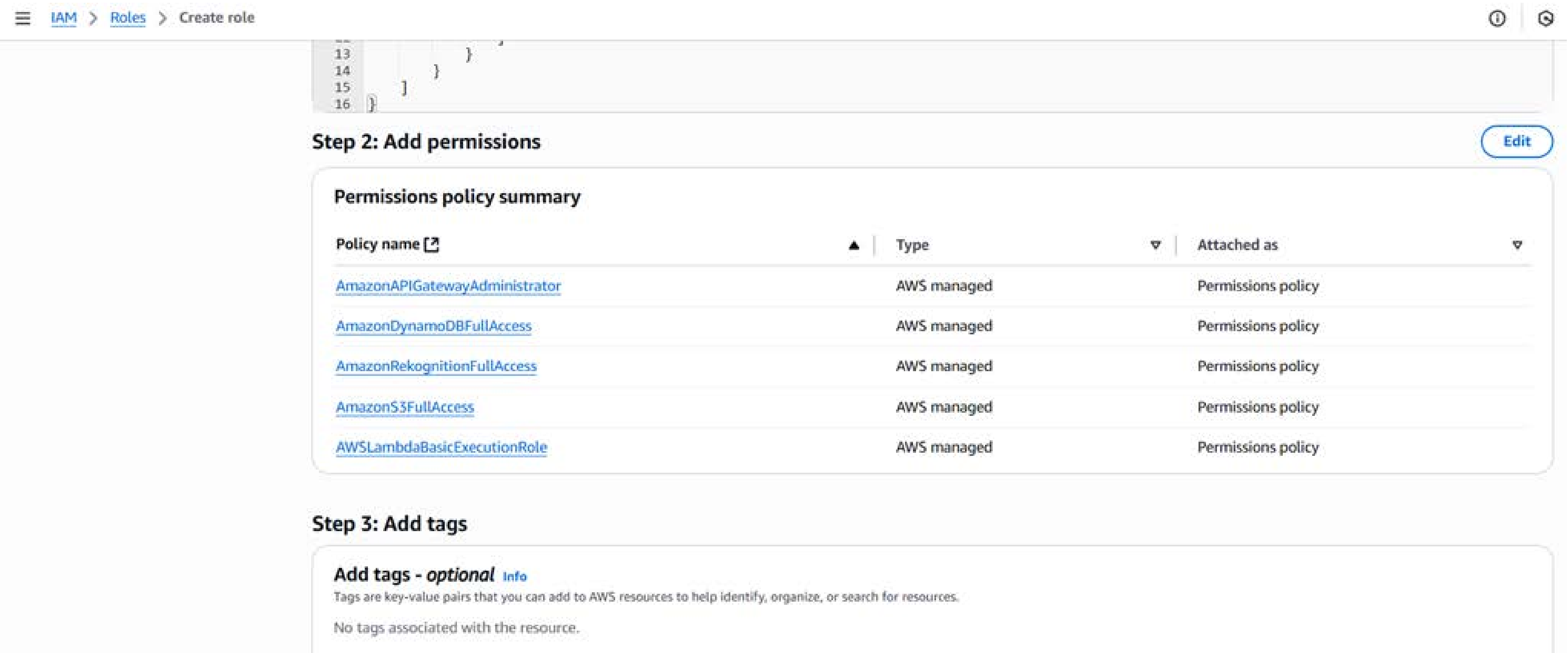
Allows EC2 instances to call AWS services on your behalf.

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

Trust policy

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



```
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

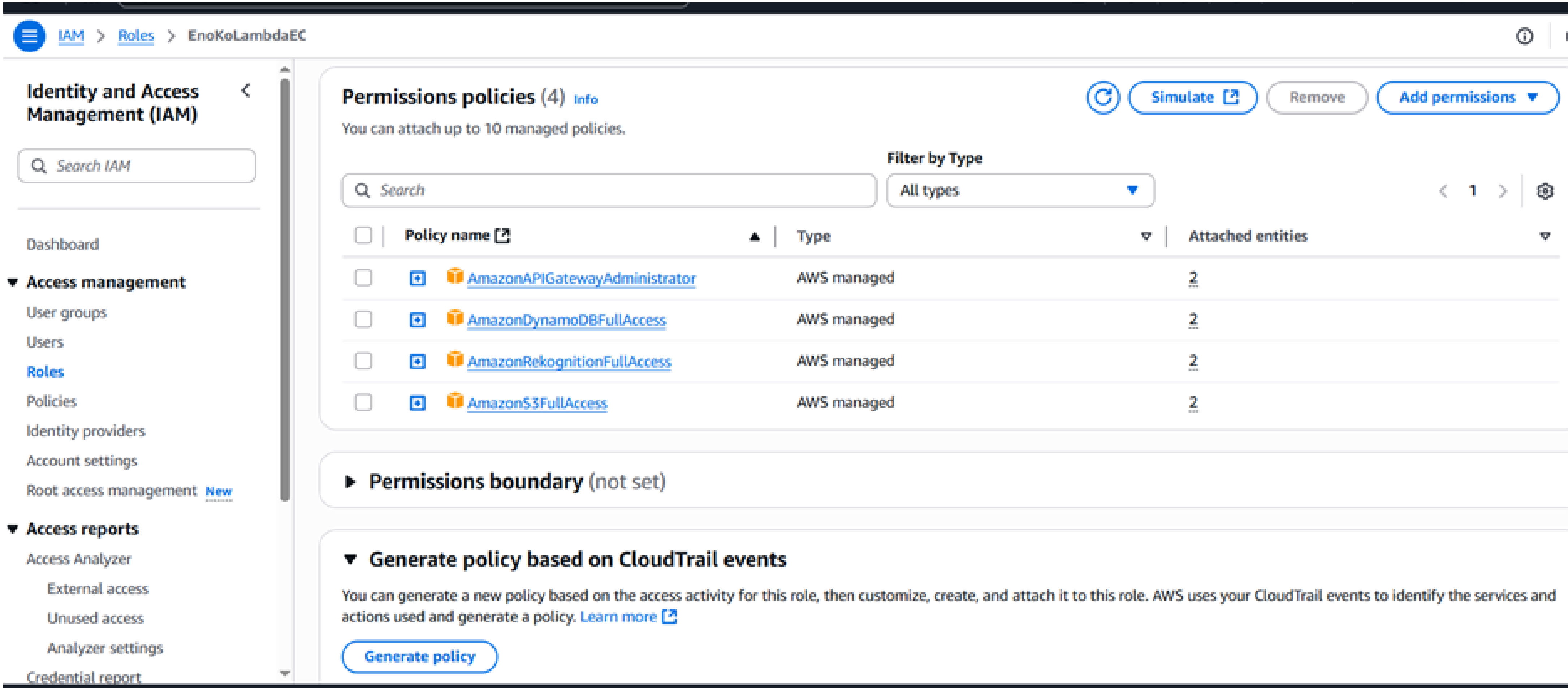
Policy name	Type	Attached as
AmazonAPIGatewayAdministrator	AWS managed	Permissions policy
AmazonDynamoDBFullAccess	AWS managed	Permissions policy
AmazonRekognitionFullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy
AWSLambdaBasicExecutionRole	AWS managed	Permissions 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.



Permissions policies (4) Info

You can attach up to 10 managed policies.

□	Policy name	Type	Attached entities
□	AmazonAPIGatewayAdministrator	AWS managed	2
□	AmazonDynamoDBFullAccess	AWS managed	2
□	AmazonRekognitionFullAccess	AWS managed	2
□	AmazonS3FullAccess	AWS managed	2

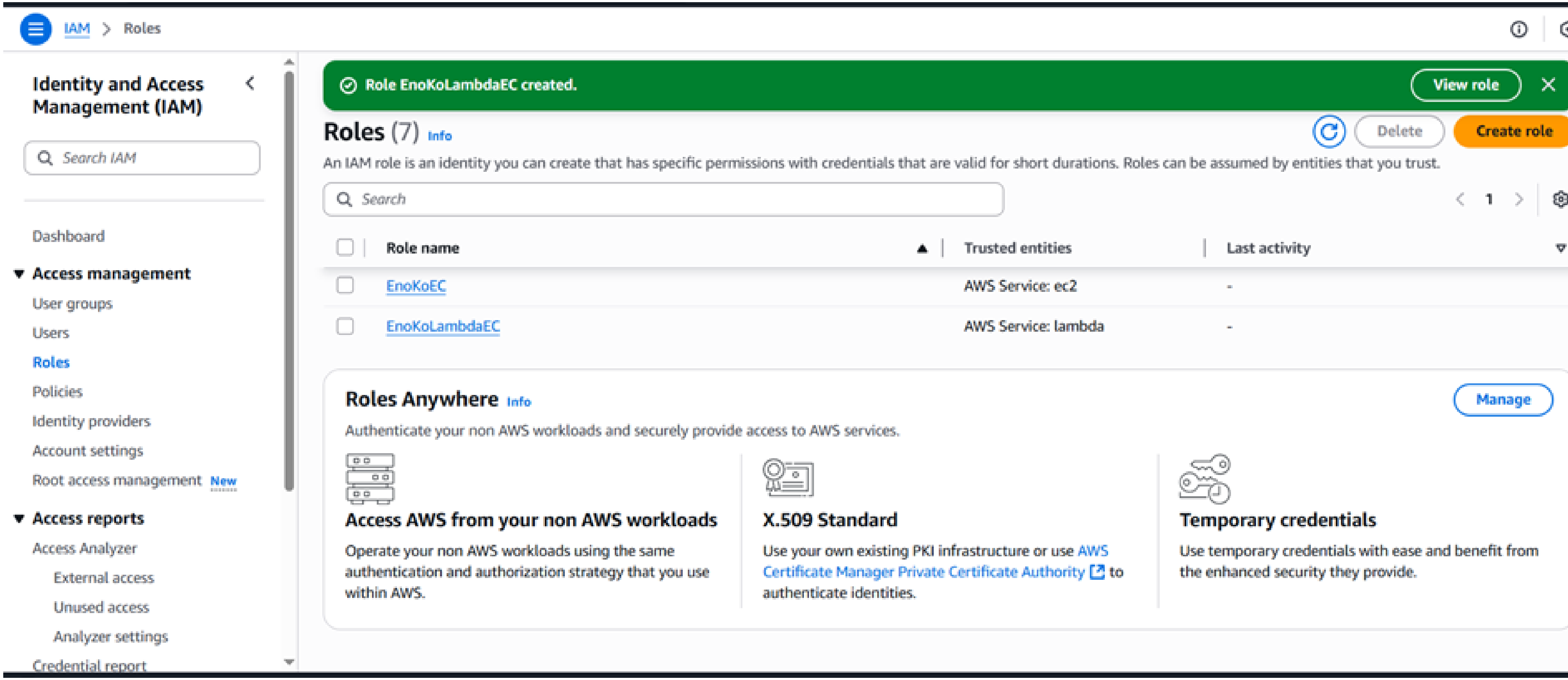
▶ **Permissions boundary** (not set)

▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

Generate policy

Нужно создать две роли



Role EnoKoLambdaEC created.

Roles (7) 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	Trusted entities	Last activity
□	EnoKoEC	AWS Service: ec2	-
□	EnoKoLambdaEC	AWS Service: lambda	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

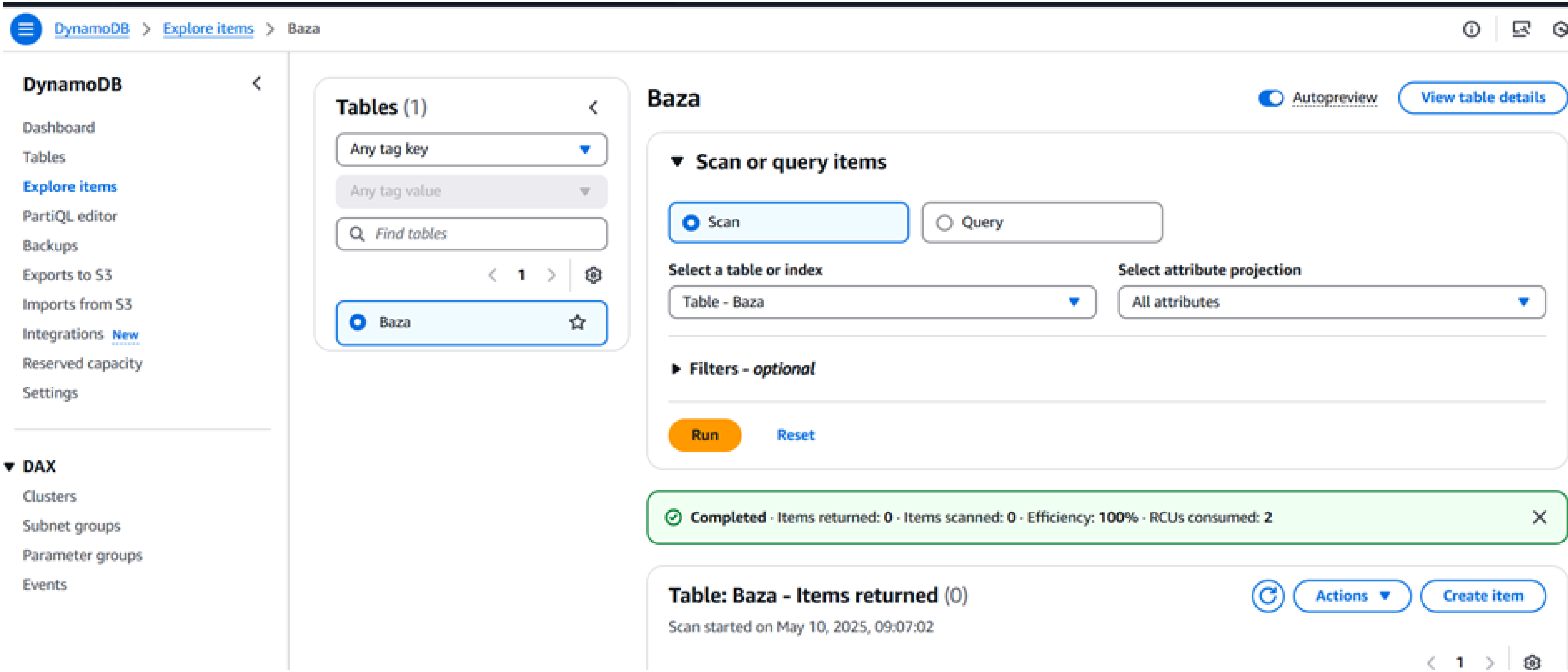
X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

База создается также как и первом задании



Baza

Scan or query items

● Scan ○ Query

Select a table or index: Table - Baza

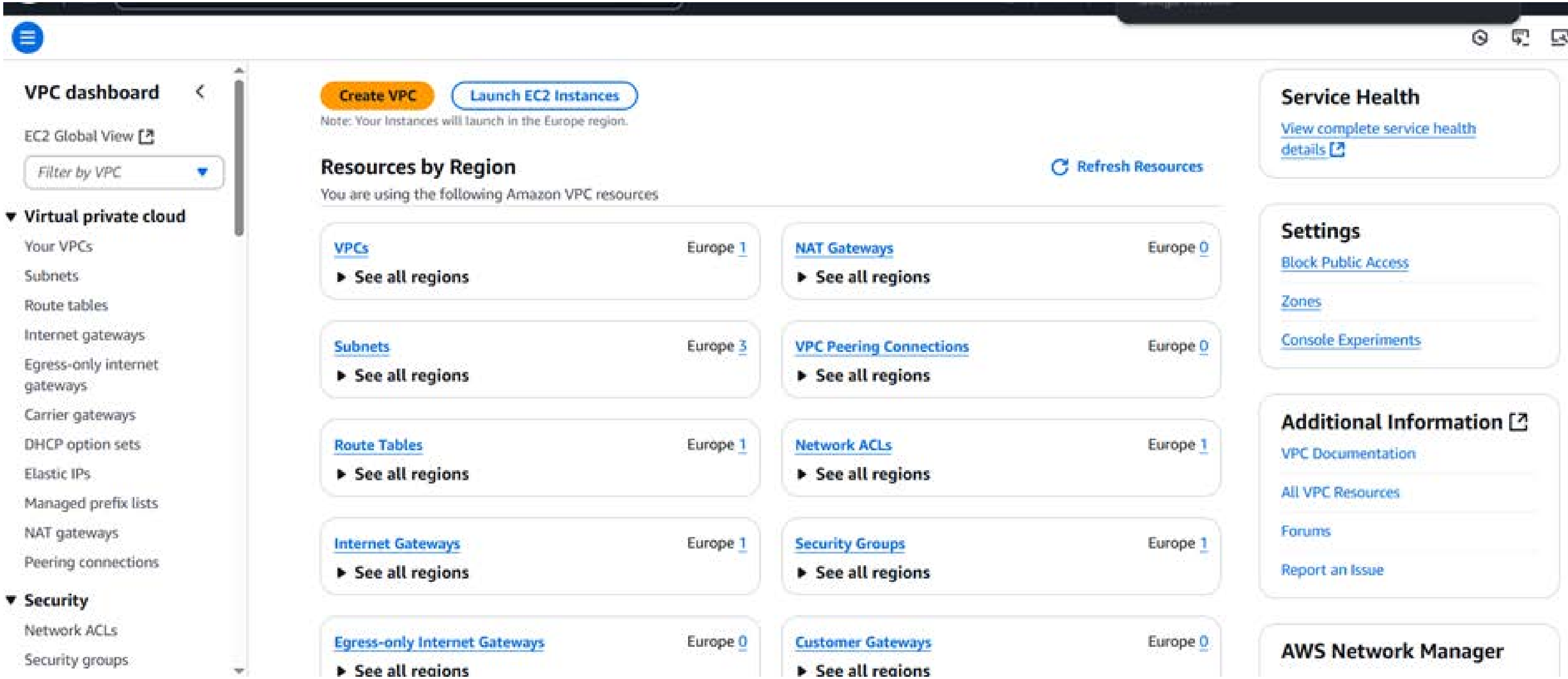
Select attribute projection: All attributes

Filters - *optional*

Completed · Items returned: 0 · Items scanned: 0 · Efficiency: 100% · RCUs consumed: 2

Table: Baza - Items returned (0)

Scan started on May 10, 2025, 09:07:02



VPC dashboard

EC2 Global View

Filter by VPC

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

▼ Security

Network ACLs

Security groups

Create VPC

Launch EC2 Instances

Note: Your Instances will launch in the Europe region.

Resources by Region

Refresh Resources

You are using the following Amazon VPC resources

VPCs Europe 1
▶ See all regions

NAT Gateways Europe 0
▶ See all regions

Subnets Europe 3
▶ See all regions

VPC Peering Connections Europe 0
▶ See all regions

Route Tables Europe 1
▶ See all regions

Network ACLs Europe 1
▶ See all regions

Internet Gateways Europe 1
▶ See all regions

Security Groups Europe 1
▶ See all regions

Egress-only Internet Gateways Europe 0
▶ See all regions

Customer Gateways Europe 0
▶ See all regions

Service Health

View complete service health details

Settings

Block Public Access

Zones

Console Experiments

Additional Information

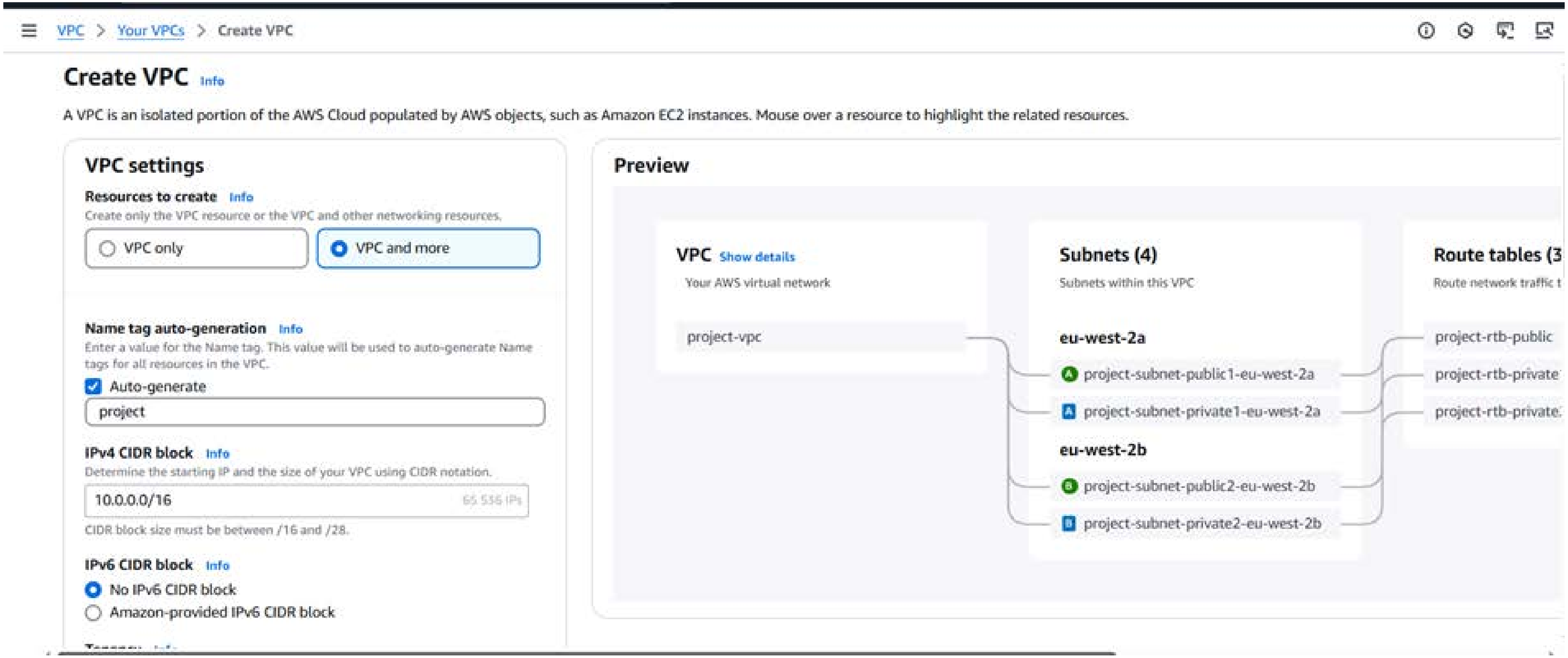
VPC Documentation

All VPC Resources

Forums

Report an Issue

AWS Network Manager



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
○ VPC only
● VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
project

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

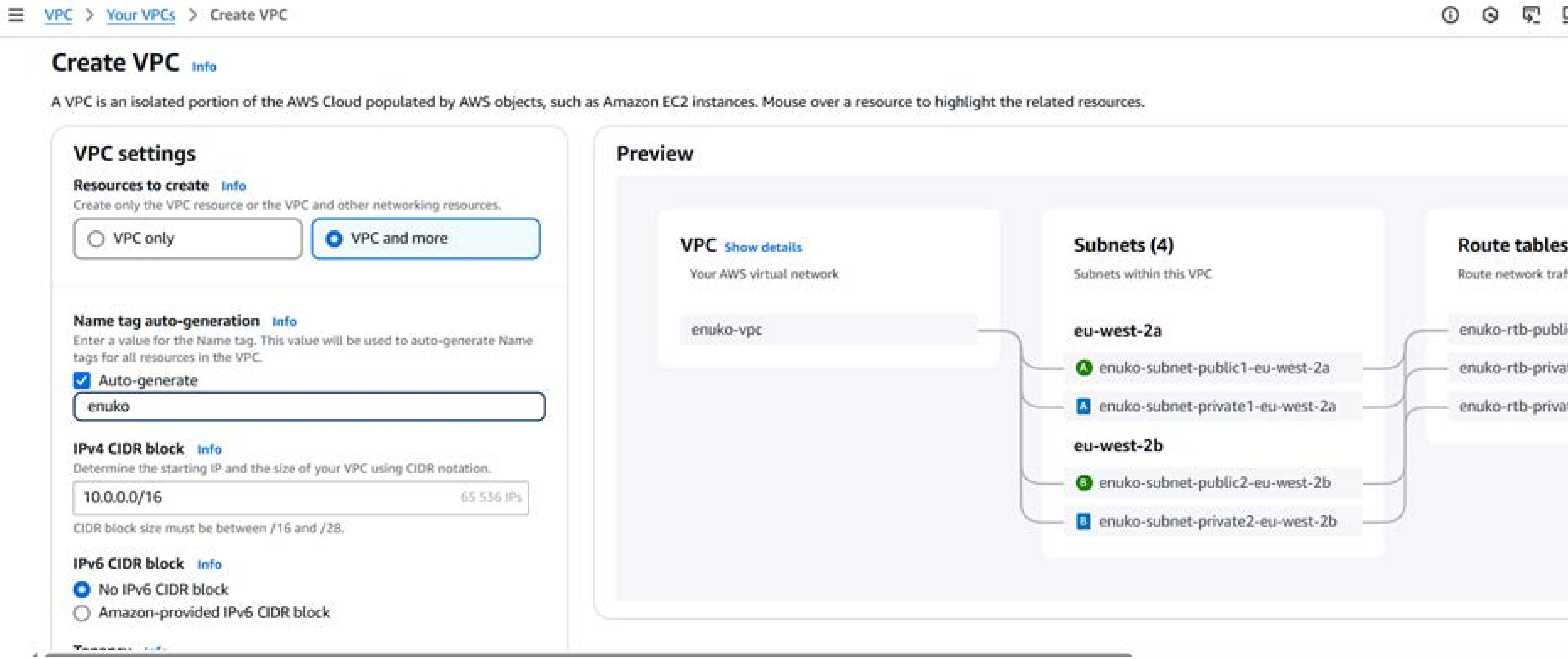
Tenancy Info

Preview

VPC Show details
Your AWS virtual network
project-vpc

Subnets (4)
Subnets within this VPC
eu-west-2a
project-subnet-public1-eu-west-2a
project-subnet-private1-eu-west-2a
eu-west-2b
project-subnet-public2-eu-west-2b
project-subnet-private2-eu-west-2b

Route tables (3
Route network traffic t
project-rtb-public
project-rtb-private
project-rtb-private



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

○ VPC only ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

enuko

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65 536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

● No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

Tenancy Info

Preview

VPC Show details

Your AWS virtual network

enuko-vpc

Subnets (4)

Subnets within this VPC

eu-west-2a

A enuko-subnet-public1-eu-west-2a

A enuko-subnet-private1-eu-west-2a

eu-west-2b

B enuko-subnet-public2-eu-west-2b

B enuko-subnet-private2-eu-west-2b

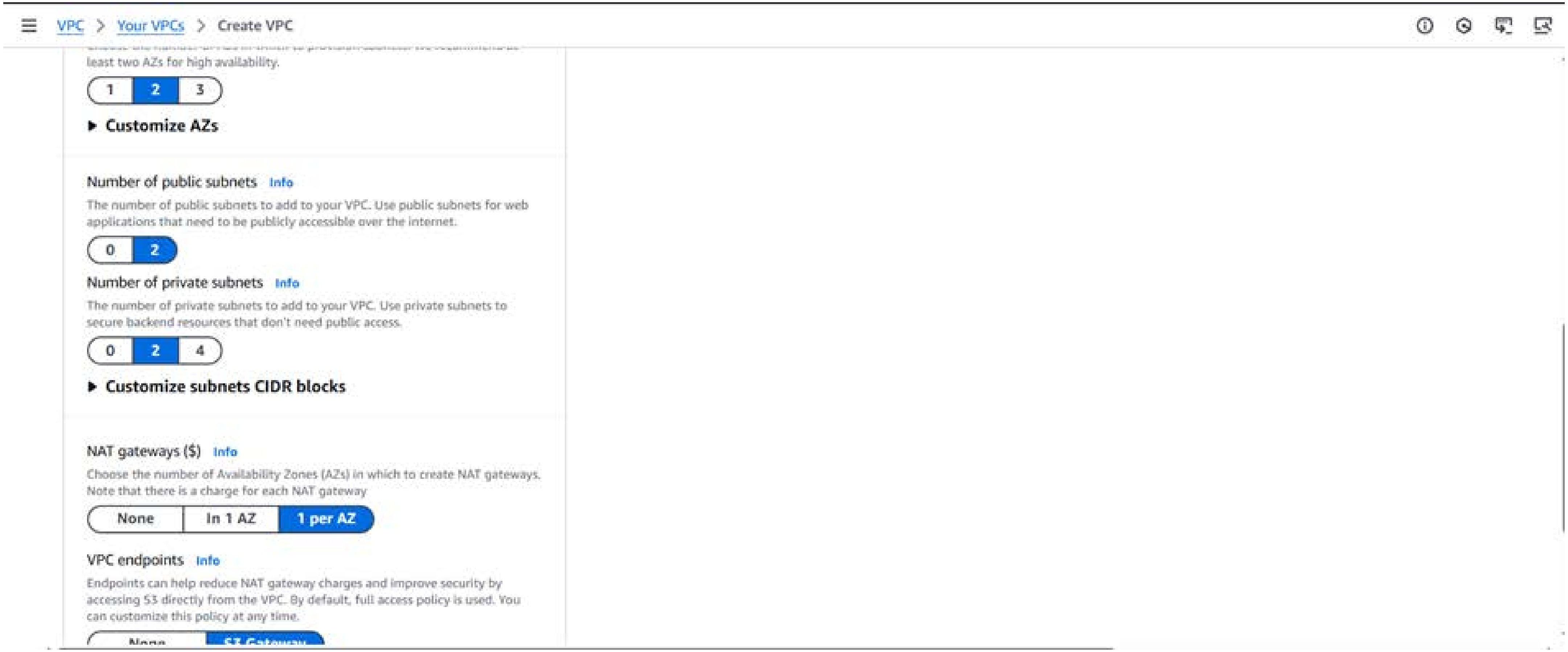
Route tables

Route network traf

enuko-rtb-publi

enuko-rtb-privat

enuko-rtb-privat



least two AZs for high availability.

1 [✓ 2] 3

▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 [✓ 2]

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 [✓ 2] 4

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

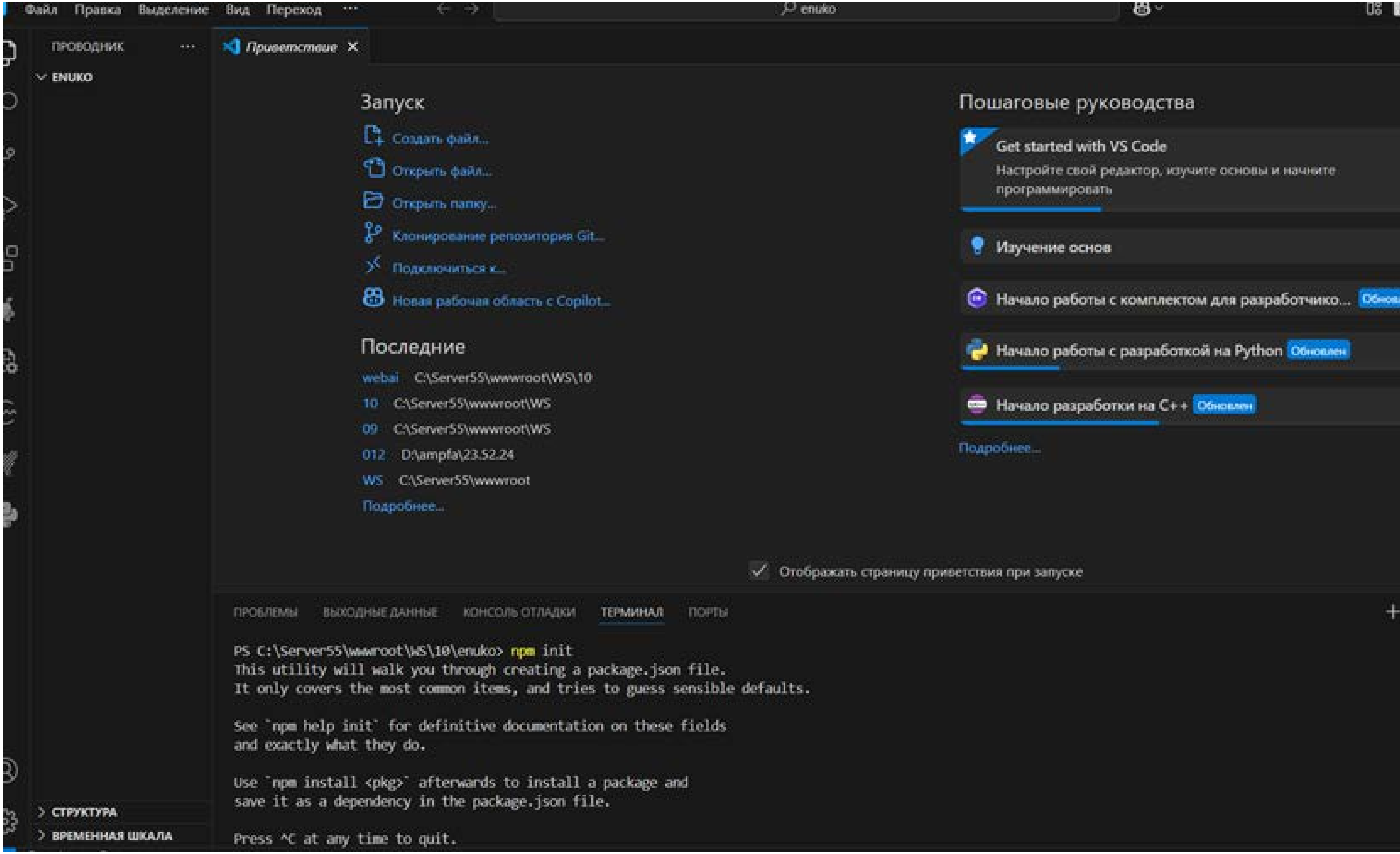
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None In 1 AZ [✓ 1 per AZ]

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

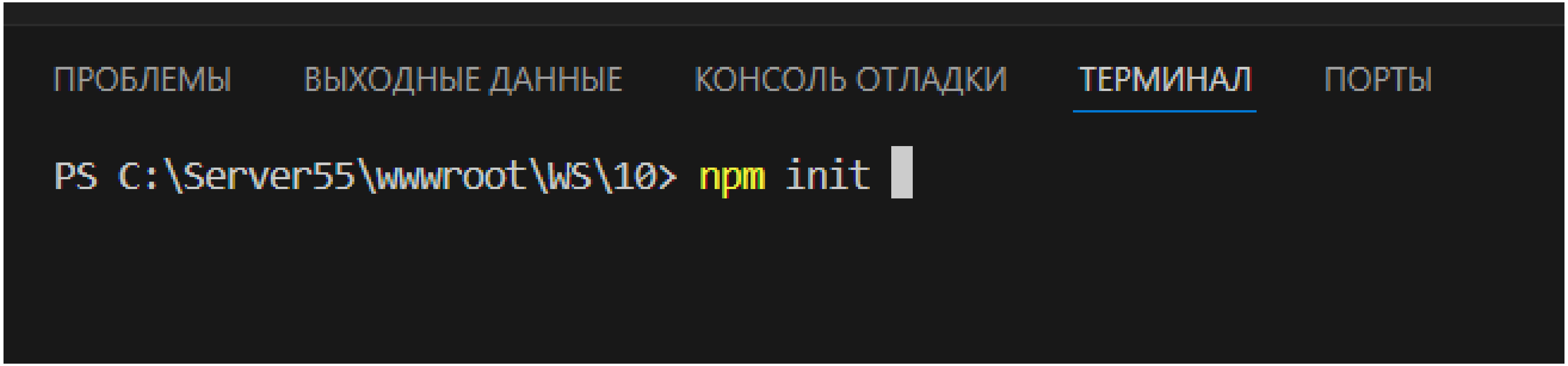
None [✓ S3 Gateway]


Файл Правка Выделение Вид Переход ···
enuko
ПРОВОДНИК ···
ENUKO
Приветствие ✕
Запуск
Создать файл...
Открыть файл...
Открыть папку...
Клонирование репозитория Git...
Подключиться к...
Новая рабочая область с Copilot...
Последние
webai C:\Server55\wwwroot\WS\10
10 C:\Server55\wwwroot\WS
09 C:\Server55\wwwroot\WS
012 D:\ampfa\23.52.24
WS C:\Server55\wwwroot
Подробнее...
Пошаговые руководства
Get started with VS Code
Изучение основ
Начало работы с комплектом для разработчико... Обнов
Начало работы с разработкой на Python Обновлен
Начало разработки на C++ Обновлен
Подробнее...
СТРУКТУРА
ВРЕМЕННАЯ ШКАЛА
ПРОБЛЕМЫ ВЫХОДНЫЕ ДАННЫЕ КОНСОЛЬ ОТЛАДКИ ТЕРМИНАЛ ПОРТЫ

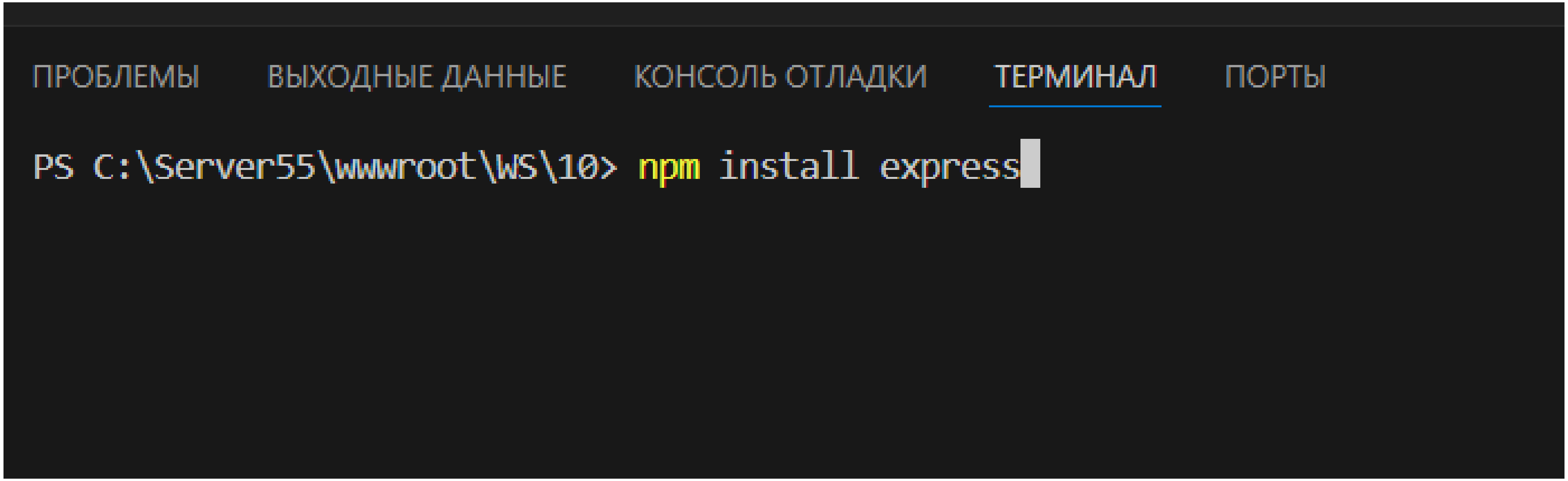
Настройте свой редактор, изучите основы и начните программировать

☑ Отображать страницу приветствия при запуске

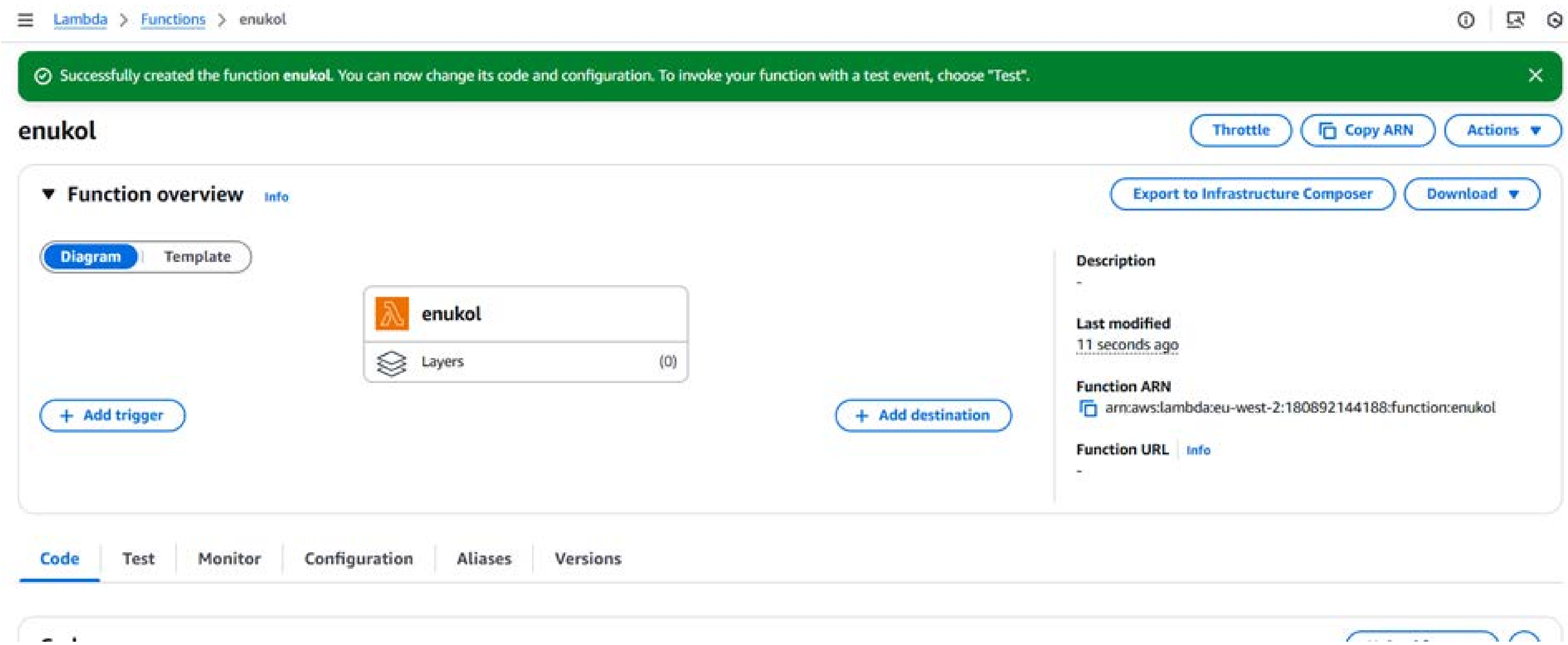
```
PS C:\Server55\wwwroot\WS\10\enuko> npm init
This utility will walk you through creating a package.json file.
It only covers the most common items, and tries to guess sensible defaults.

See `npm help init` for definitive documentation on these fields
and exactly what they do.

Use `npm install <pkg>` afterwards to install a package and
save it as a dependency in the package.json file.

Press ^C at any time to quit.
```



```
PS C:\Server55\wwwroot\WS\10> npm init
```



```
PS C:\Server55\wwwroot\WS\10> npm install express
```



Successfully created the function **enukol**. You can now change its code and configuration. To invoke your function with a test event, choose "Test".

enukol

▼ Function overview

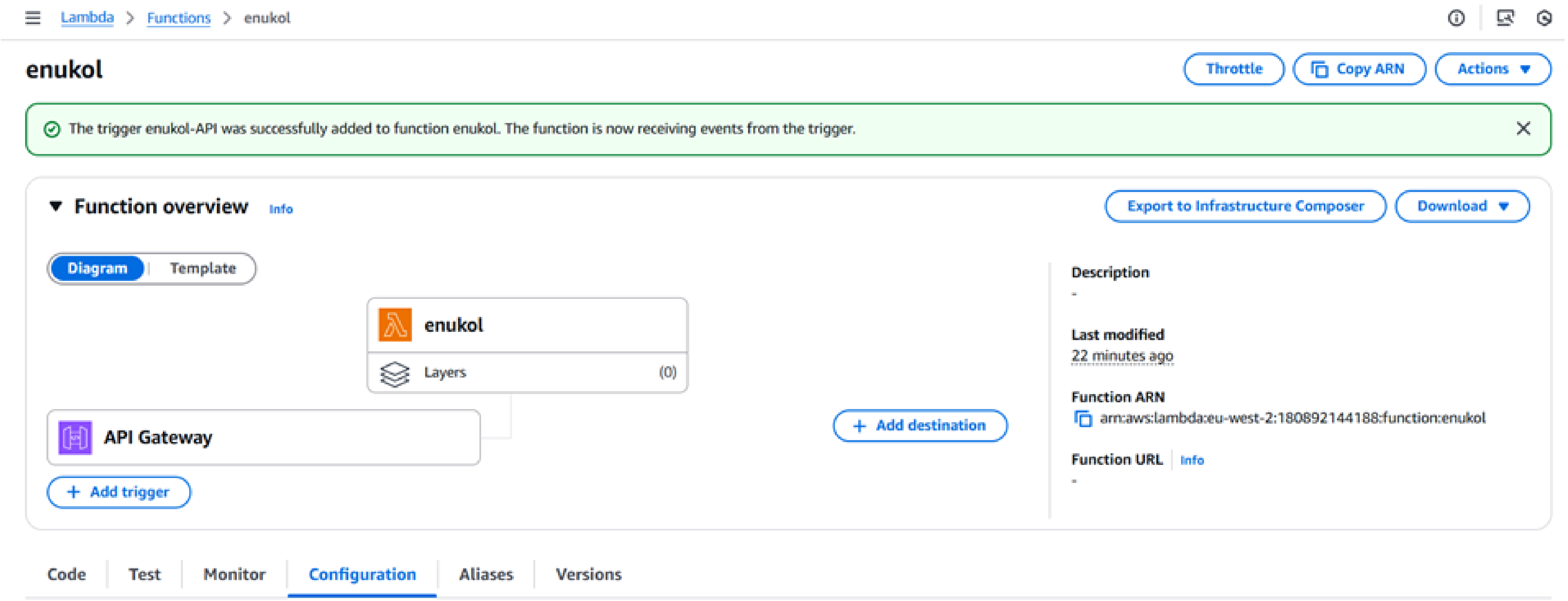
enukol

Description
-

Last modified
11 seconds ago

Function ARN
arn:aws:lambda:eu-west-2:180892144188:function:enukol

Function URL
-



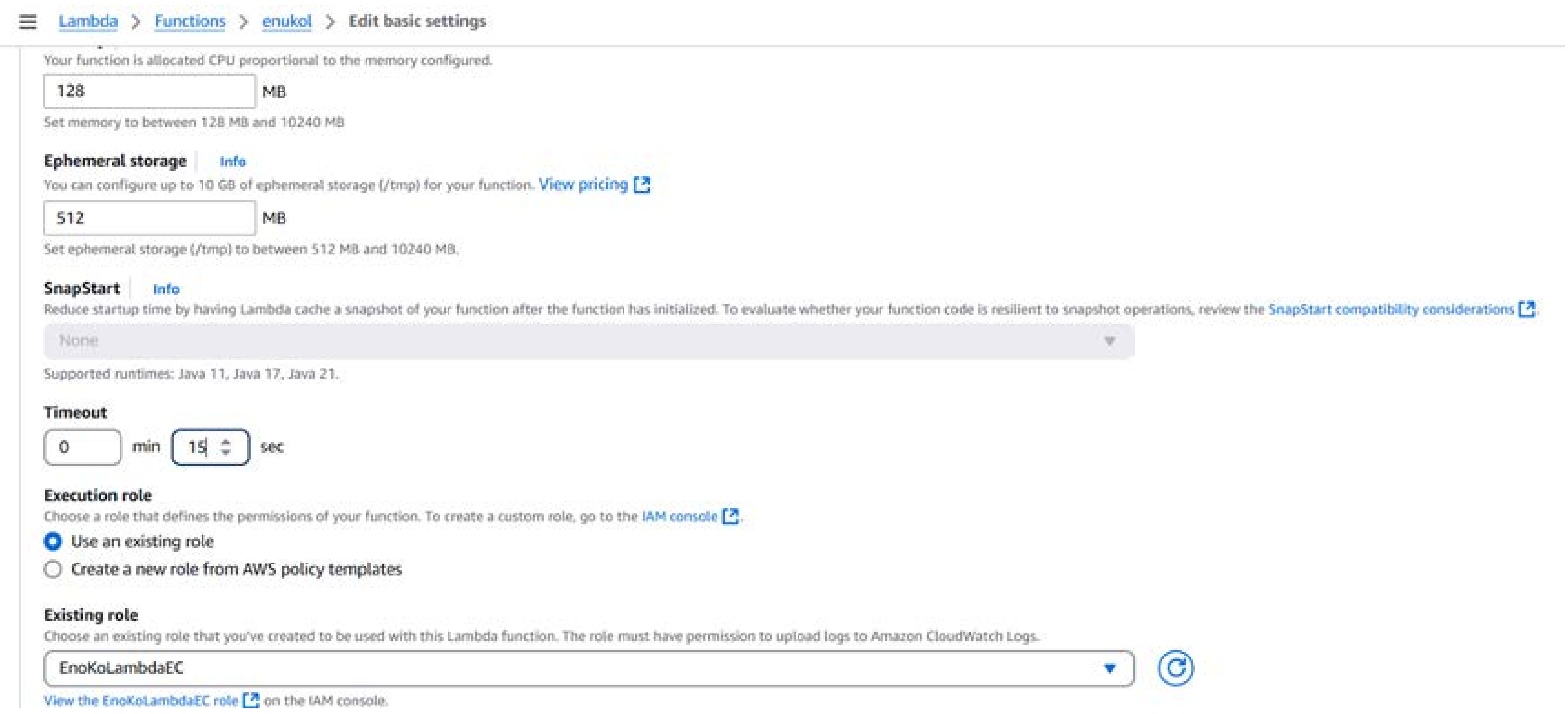
The trigger enukol-API was successfully added to function enukol. The function is now receiving events from the trigger.

Description
-

Last modified
22 minutes ago

Function ARN
arn:aws:lambda:eu-west-2:180892144188:function:enukol

Function URL Info
-



Lambda > Functions > enukol > Edit basic settings

Your function is allocated CPU proportional to the memory configured.

128 MB

Set memory to between 128 MB and 10240 MB

Ephemeral storage Info

You can configure up to 10 GB of ephemeral storage (/tmp) for your function. View pricing

512 MB

Set ephemeral storage (/tmp) to between 512 MB and 10240 MB.

SnapStart Info

Reduce startup time by having Lambda cache a snapshot of your function after the function has initialized. To evaluate whether your function code is resilient to snapshot operations, review the SnapStart compatibility considerations.

None ▼

Supported runtimes: Java 11, Java 17, Java 21.

Timeout

0 min 15 sec

Execution role

Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.

● Use an existing role

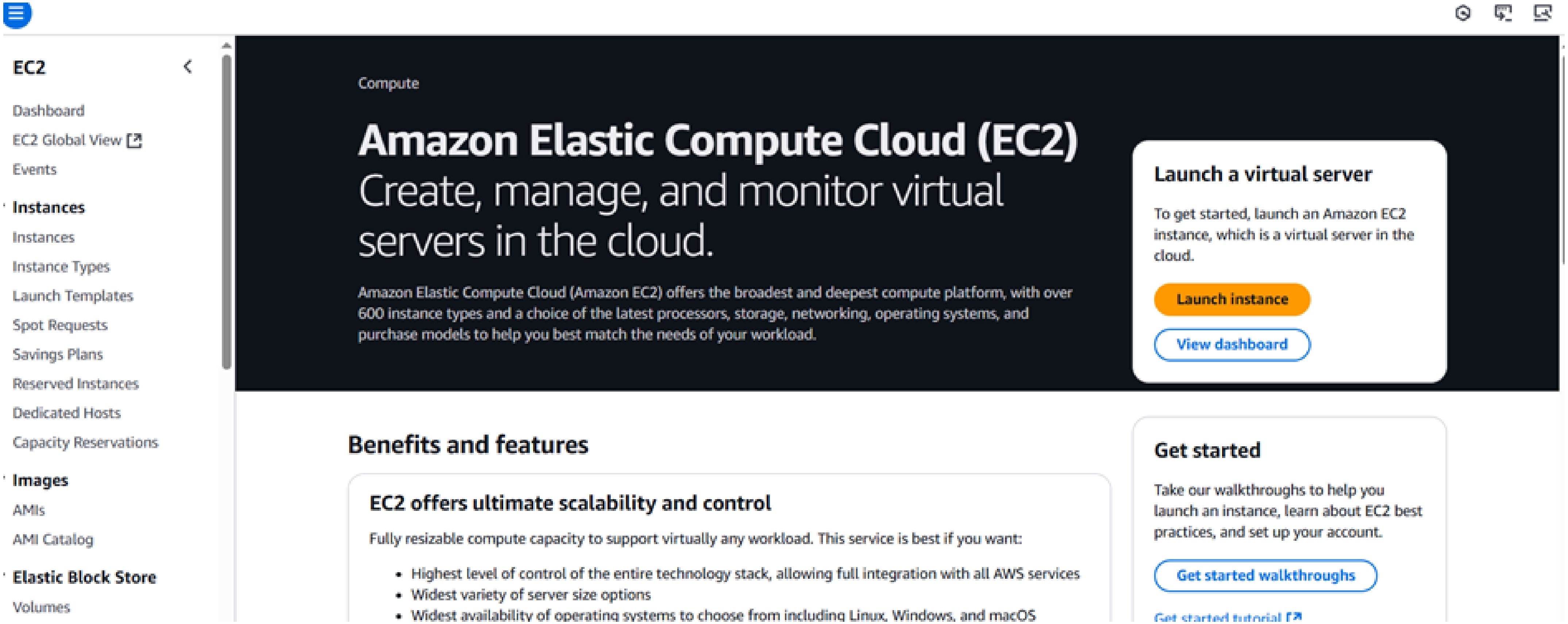
○ Create a new role from AWS policy templates

Existing role

Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

EnoKoLambdaEC ▼

View the EnoKoLambdaEC role on the IAM console.



EC2

Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Compute

Amazon Elastic Compute Cloud (EC2)

Create, manage, and monitor virtual servers in the cloud.

Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 600 instance types and a choice of the latest processors, storage, networking, operating systems, and purchase models to help you best match the needs of your workload.

Launch a virtual server

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

Benefits and features

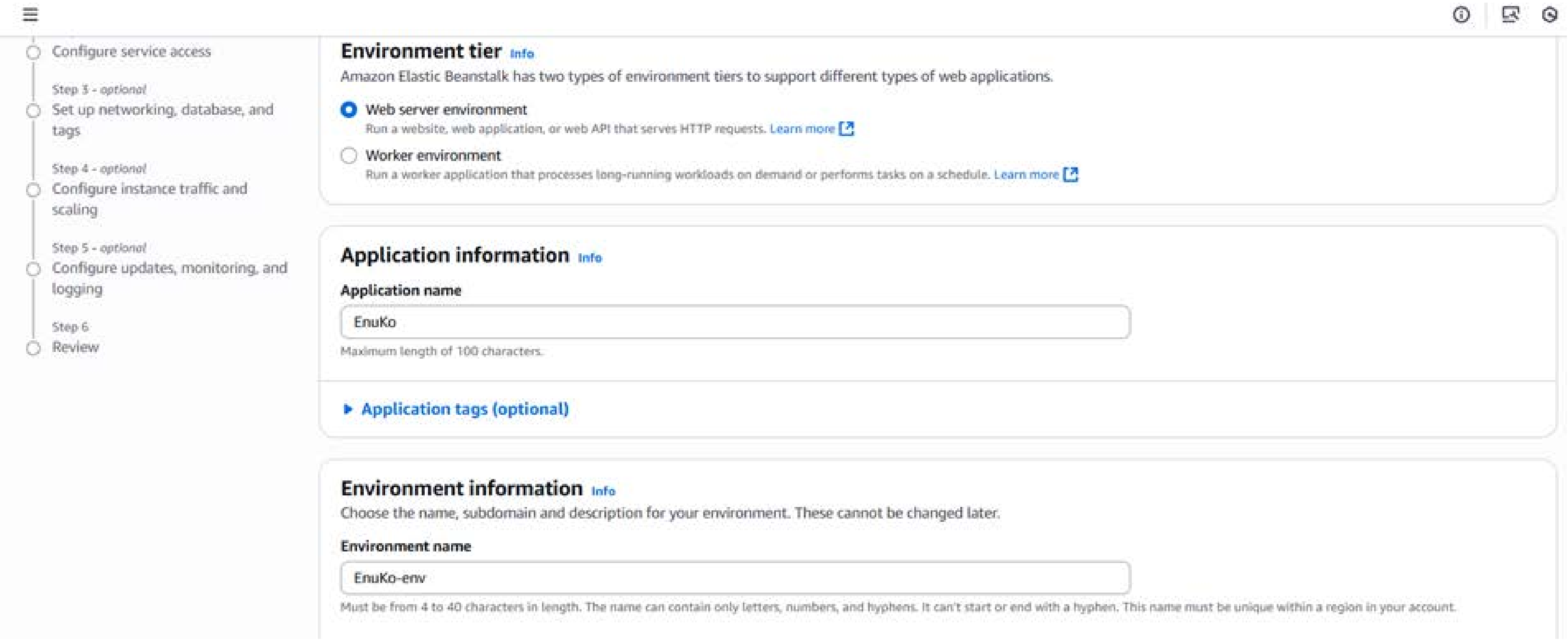
EC2 offers ultimate scalability and control

Fully resizable compute capacity to support virtually any workload. This service is best if you want:

- Highest level of control of the entire technology stack, allowing full integration with all AWS services
- Widest variety of server size options
- Widest availability of operating systems to choose from including Linux, Windows, and macOS

Get started

Take our walkthroughs to help you launch an instance, learn about EC2 best practices, and set up your account.



Configure service access

Step 3 - *optional*
○ Set up networking, database, and tags

Step 4 - *optional*
○ Configure instance traffic and scaling

Step 5 - *optional*
○ Configure updates, monitoring, and logging

Step 6
○ Review

Environment tier Info

Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications.

● Web server environment
Run a website, web application, or web API that serves HTTP requests. Learn more

○ Worker environment
Run a worker application that processes long-running workloads on demand or performs tasks on a schedule. Learn more

Application information Info

Application name

EnuKo

Maximum length of 100 characters.

▶ Application tags (optional)

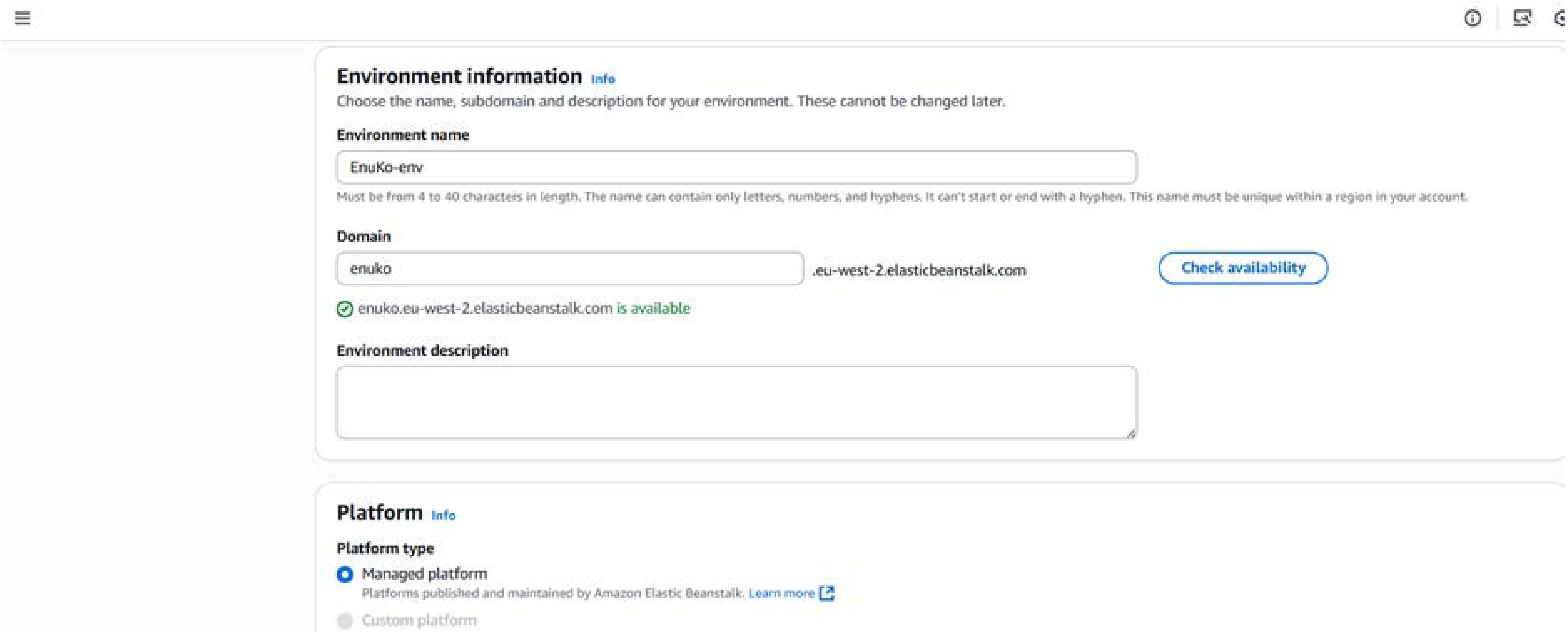
Environment information Info

Choose the name, subdomain and description for your environment. These cannot be changed later.

Environment name

EnuKo-env

Must be from 4 to 40 characters in length. The name can contain only letters, numbers, and hyphens. It can't start or end with a hyphen. This name must be unique within a region in your account.



Environment information

Choose the name, subdomain and description for your environment. These cannot be changed later.

Environment name

EnuKo-env

Must be from 4 to 40 characters in length. The name can contain only letters, numbers, and hyphens. It can't start or end with a hyphen. This name must be unique within a region in your account.

Domain

enuko .eu-west-2.elasticbeanstalk.com

✓ enuko.eu-west-2.elasticbeanstalk.com is available

Environment description

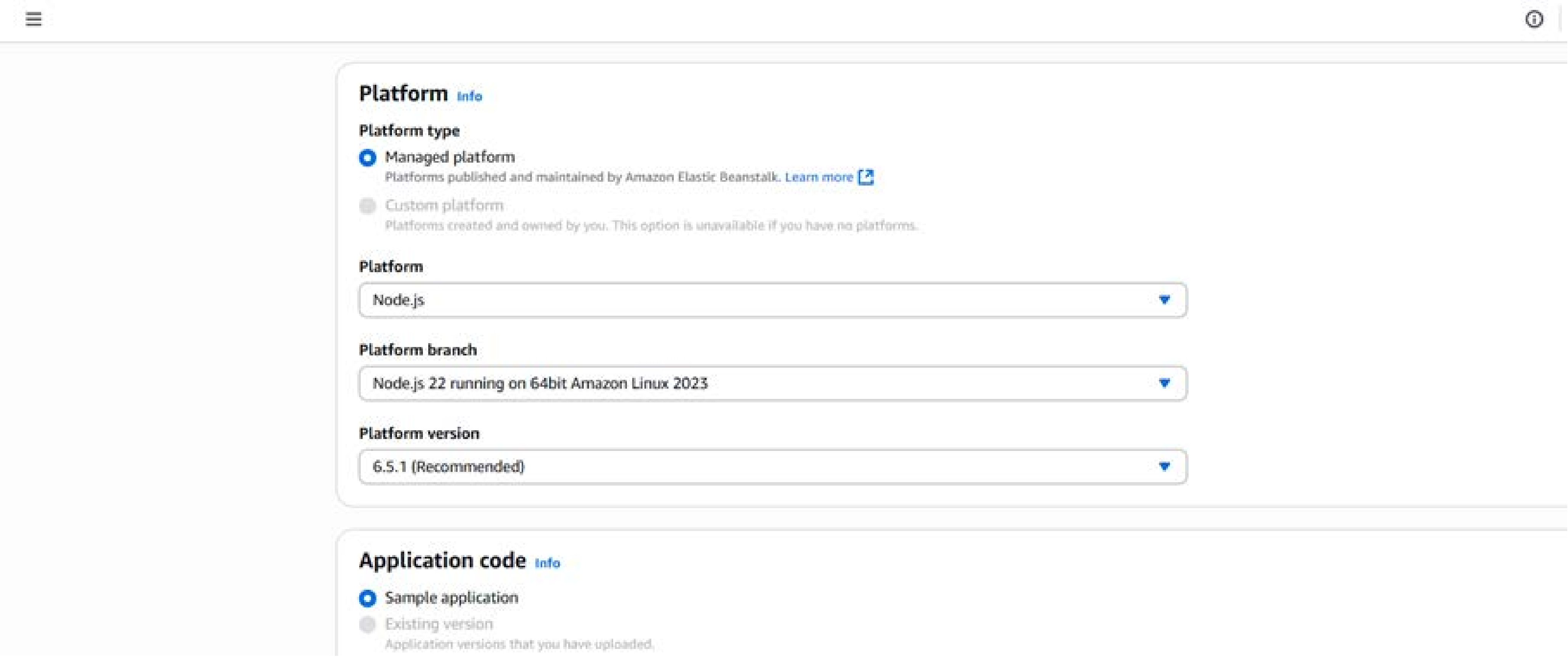
Platform

Platform type

● Managed platform

Platforms published and maintained by Amazon Elastic Beanstalk. Learn more

○ Custom platform



Platform Info

Platform type

● Managed platform
Platforms published and maintained by Amazon Elastic Beanstalk. Learn more

○ Custom platform
Platforms created and owned by you. This option is unavailable if you have no platforms.

Platform
Node.js ▼

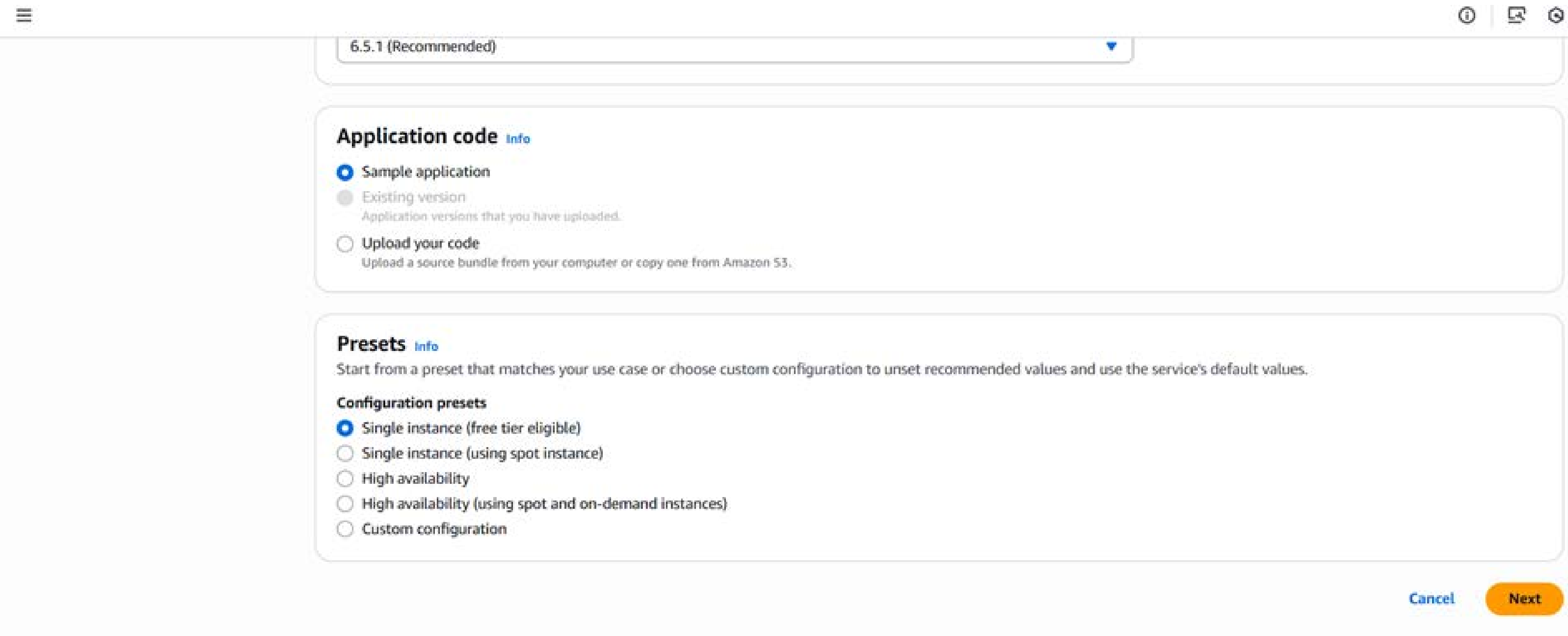
Platform branch
Node.js 22 running on 64bit Amazon Linux 2023 ▼

Platform version
6.5.1 (Recommended) ▼

Application code Info

● Sample application

○ Existing version
Application versions that you have uploaded.



6.5.1 (Recommended) ▼

Application code Info

● Sample application

○ Existing version

Application versions that you have uploaded.

○ Upload your code

Upload a source bundle from your computer or copy one from Amazon S3.

Presets Info

Start from a preset that matches your use case or choose custom configuration to unset recommended values and use the service's default values.

Configuration presets

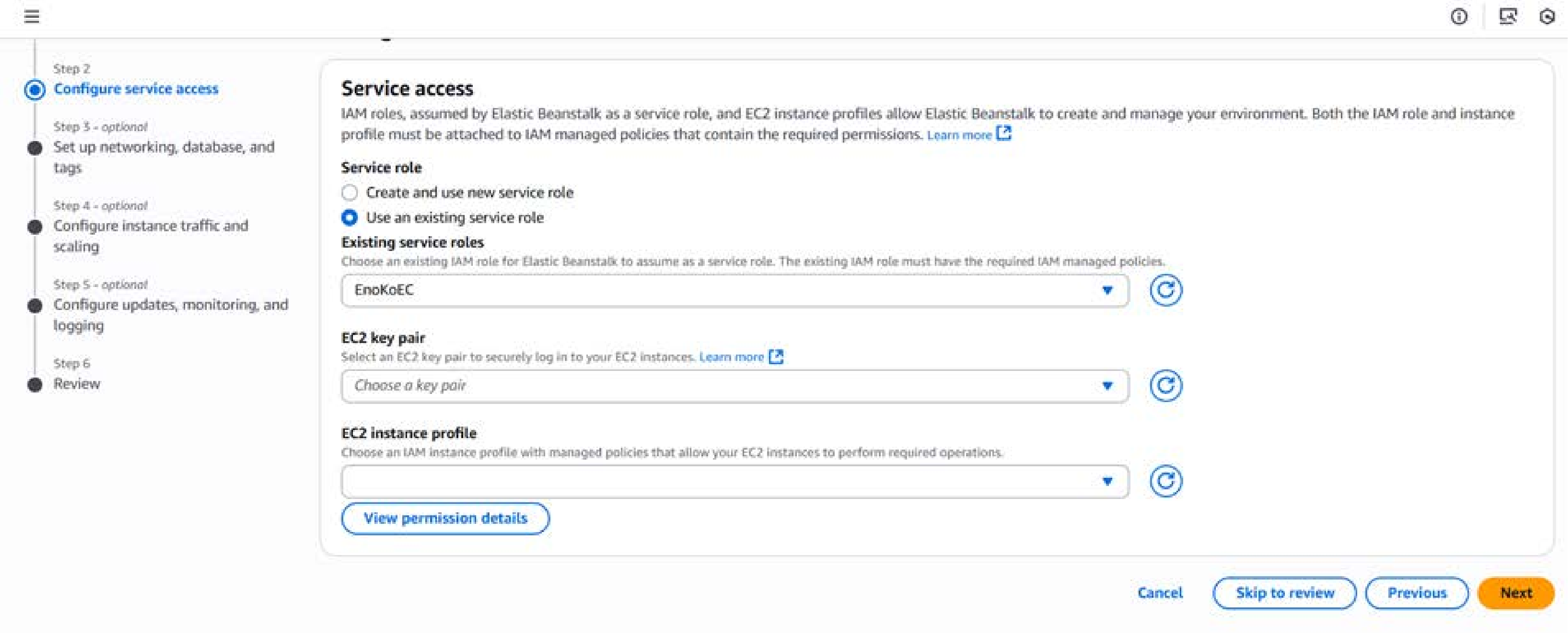
● Single instance (free tier eligible)

○ Single instance (using spot instance)

○ High availability

○ High availability (using spot and on-demand instances)

○ Custom configuration



Step 2
Configure service access
Step 3 - *optional*
Set up networking, database, and tags
Step 4 - *optional*
Configure instance traffic and scaling
Step 5 - *optional*
Configure updates, monitoring, and logging
Step 6
Review

Service access

IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions. Learn more

Service role

○ Create and use new service role

● Use an existing service role

Existing service roles

Choose an existing IAM role for Elastic Beanstalk to assume as a service role. The existing IAM role must have the required IAM managed policies.

EnoKoEC ▼

EC2 key pair

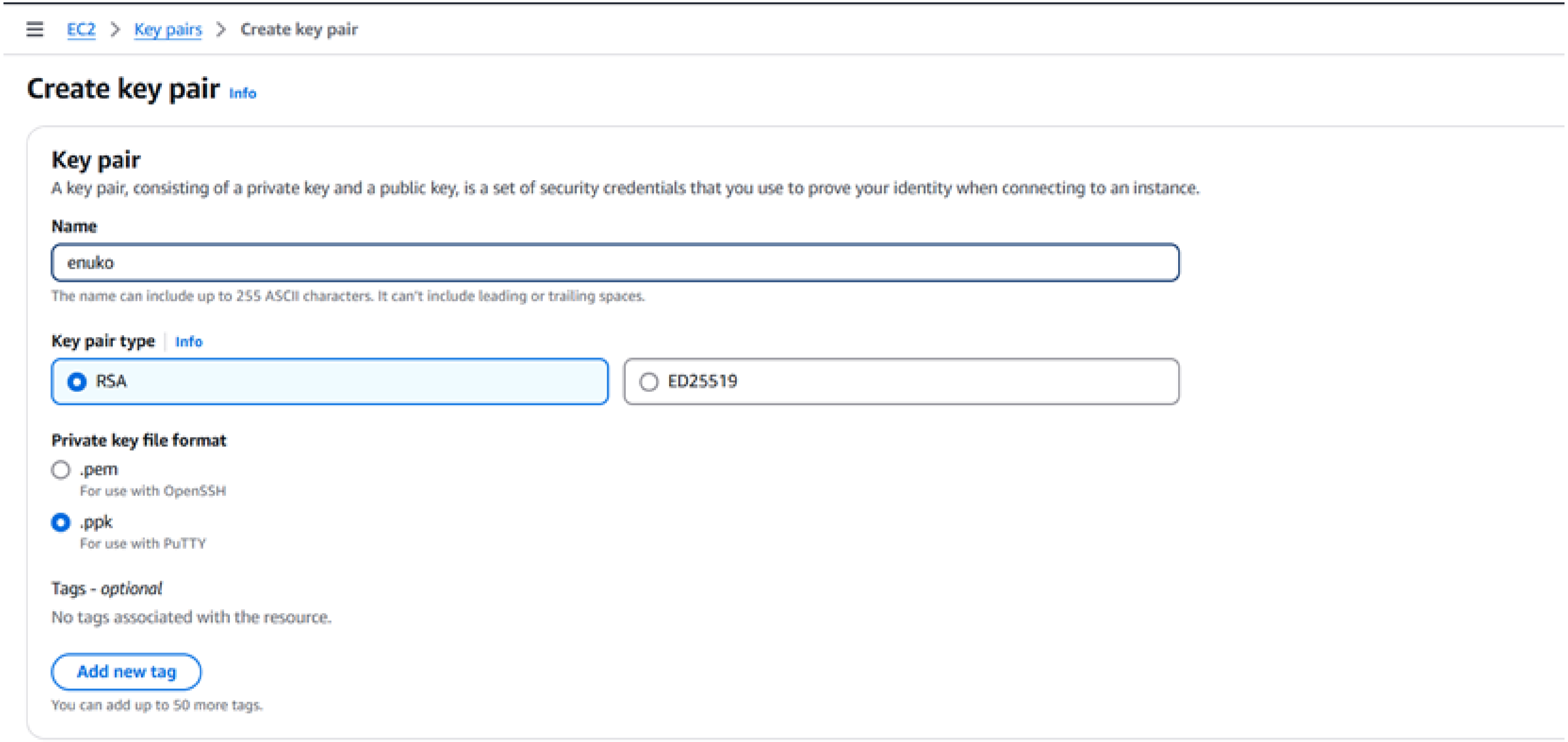
Select an EC2 key pair to securely log in to your EC2 instances. Learn more

Choose a key pair ▼

EC2 instance profile

Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

▼



Create key pair

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

enuko

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

Key pair type

● RSA ○ ED25519

Private key file format

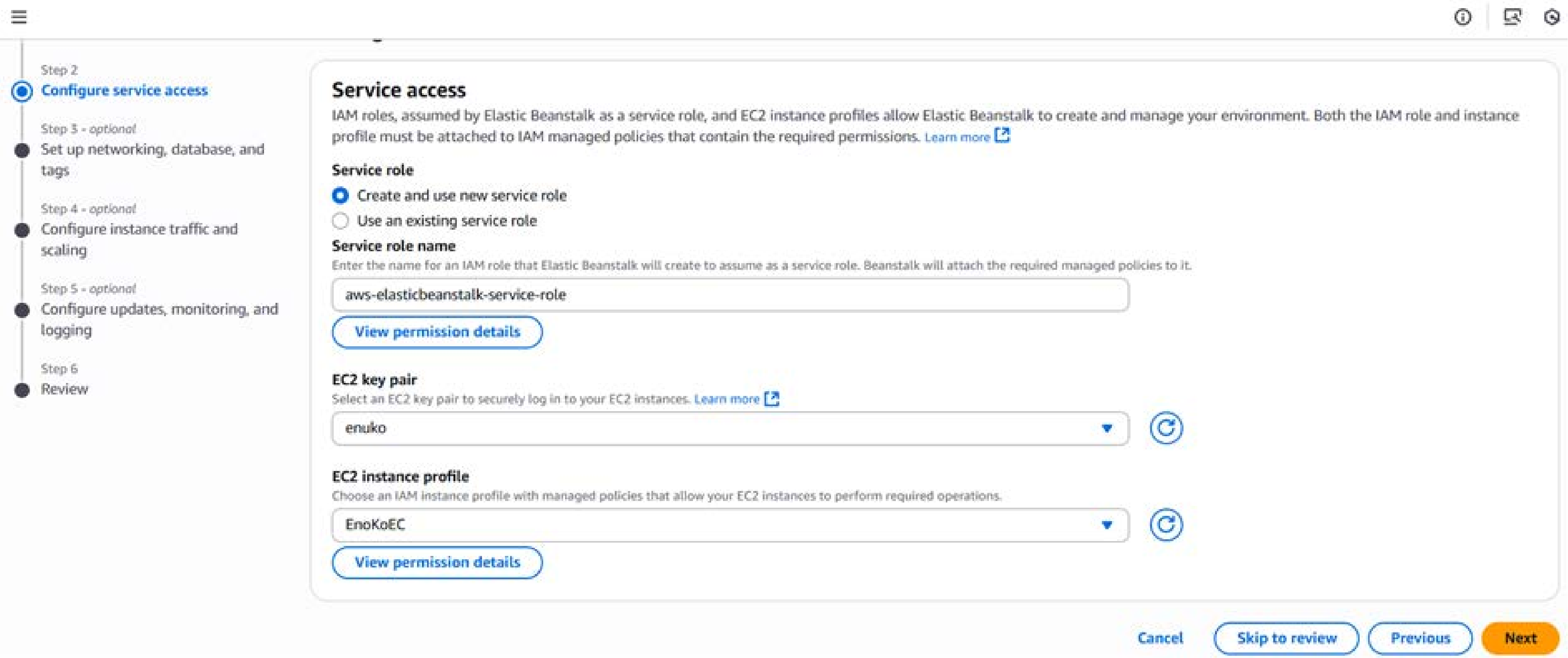
○ .pem
For use with OpenSSH

● .ppk
For use with PuTTY

Tags - *optional*

No tags associated with the resource.

You can add up to 50 more tags.



Step 2
● Configure service access

Step 3 - *optional*
● Set up networking, database, and tags

Step 4 - *optional*
● Configure instance traffic and scaling

Step 5 - *optional*
● Configure updates, monitoring, and logging

Step 6
● Review

Service access

IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions. Learn more

Service role

● Create and use new service role

○ Use an existing service role

Service role name

Enter the name for an IAM role that Elastic Beanstalk will create to assume as a service role. Beanstalk will attach the required managed policies to it.

aws-elasticbeanstalk-service-role

EC2 key pair

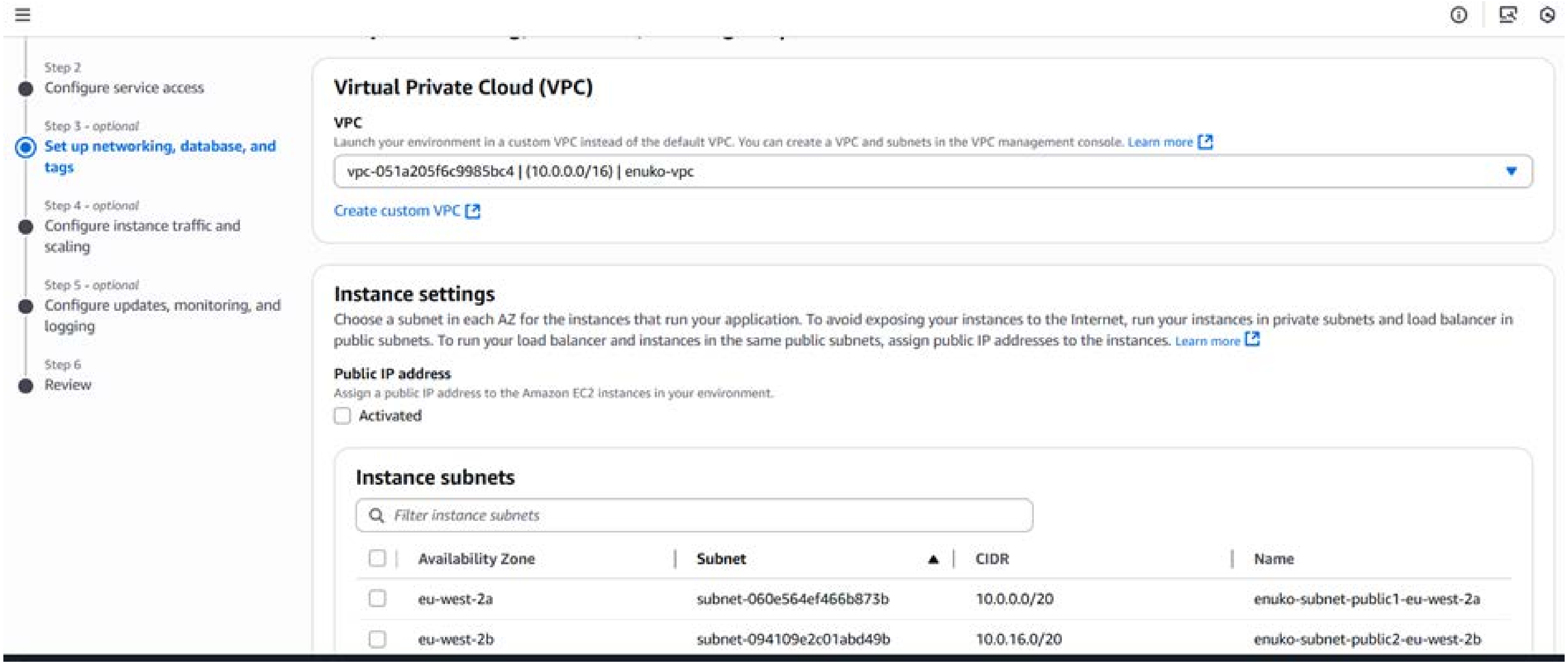
Select an EC2 key pair to securely log in to your EC2 instances. Learn more

enuko

EC2 instance profile

Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

EnoKoEC



Step 2
Configure service access

Step 3 - *optional*
Set up networking, database, and tags

Step 4 - *optional*
Configure instance traffic and scaling

Step 5 - *optional*
Configure updates, monitoring, and logging

Step 6
Review

Virtual Private Cloud (VPC)

VPC

Launch your environment in a custom VPC instead of the default VPC. You can create a VPC and subnets in the VPC management console. Learn more

vpc-051a205f6c9985bc4 | (10.0.0.0/16) | enuko-vpc

Create custom VPC

Instance settings

Choose a subnet in each AZ for the instances that run your application. To avoid exposing your instances to the Internet, run your instances in private subnets and load balancer in public subnets. To run your load balancer and instances in the same public subnets, assign public IP addresses to the instances. Learn more

Public IP address

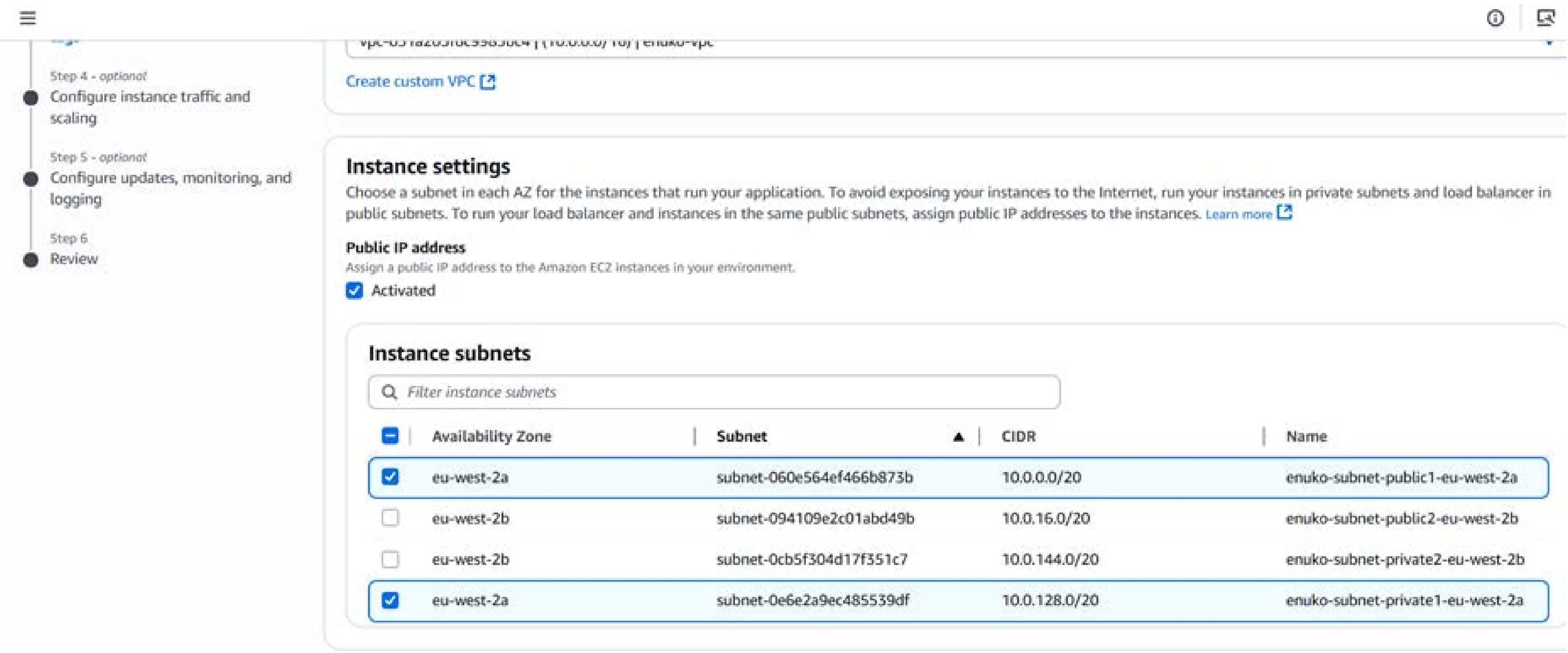
Assign a public IP address to the Amazon EC2 instances in your environment.

□ Activated

Instance subnets

Filter instance subnets

□	Availability Zone	Subnet ▲	CIDR	Name
□	eu-west-2a	subnet-060e564ef466b873b	10.0.0.0/20	enuko-subnet-public1-eu-west-2a
□	eu-west-2b	subnet-094109e2c01abd49b	10.0.16.0/20	enuko-subnet-public2-eu-west-2b



vpc-031a203fdc9983bc4 | (10.0.0.0/16) | enuko-vpc

Create custom VPC

Step 4 - *optional*
● Configure instance traffic and scaling

Step 5 - *optional*
● Configure updates, monitoring, and logging

Step 6
● Review

Instance settings

Choose a subnet in each AZ for the instances that run your application. To avoid exposing your instances to the Internet, run your instances in private subnets and load balancer in public subnets. To run your load balancer and instances in the same public subnets, assign public IP addresses to the instances. Learn more

Public IP address

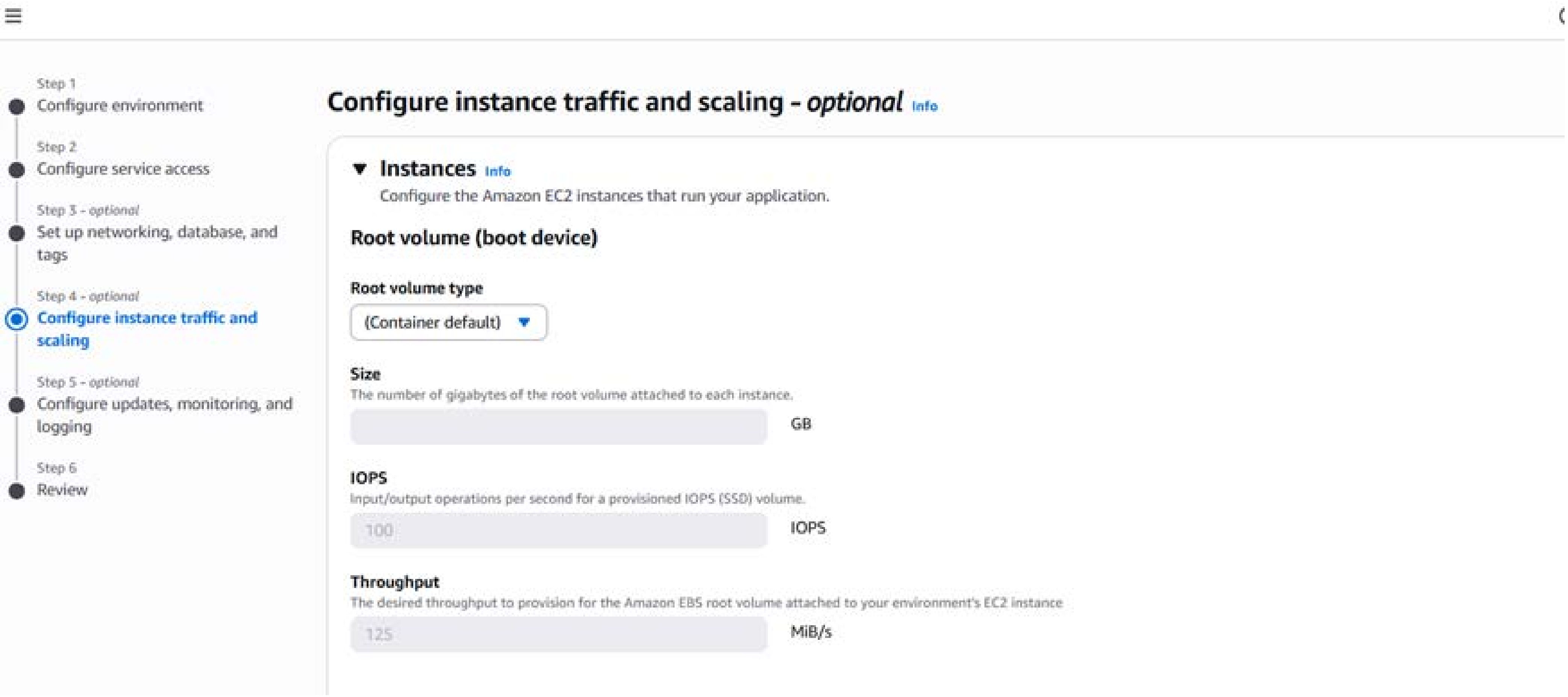
Assign a public IP address to the Amazon EC2 instances in your environment.

☑ Activated

Instance subnets

Filter instance subnets

	Availability Zone	Subnet ▲	CIDR	Name
☑	eu-west-2a	subnet-060e564ef466b873b	10.0.0.0/20	enuko-subnet-public1-eu-west-2a
□	eu-west-2b	subnet-094109e2c01abd49b	10.0.16.0/20	enuko-subnet-public2-eu-west-2b
□	eu-west-2b	subnet-0cb5f304d17f351c7	10.0.144.0/20	enuko-subnet-private2-eu-west-2b
☑	eu-west-2a	subnet-0e6e2a9ec485539df	10.0.128.0/20	enuko-subnet-private1-eu-west-2a



Step 1
● Configure environment

Step 2
● Configure service access

Step 3 - *optional*
● Set up networking, database, and tags

Step 4 - *optional*
◉ **Configure instance traffic and scaling**

Step 5 - *optional*
● Configure updates, monitoring, and logging

Step 6
● Review

Configure instance traffic and scaling - *optional* Info

▼ Instances Info

Configure the Amazon EC2 instances that run your application.

Root volume (boot device)

Root volume type

(Container default) ▼

Size

The number of gigabytes of the root volume attached to each instance.

GB

IOPS

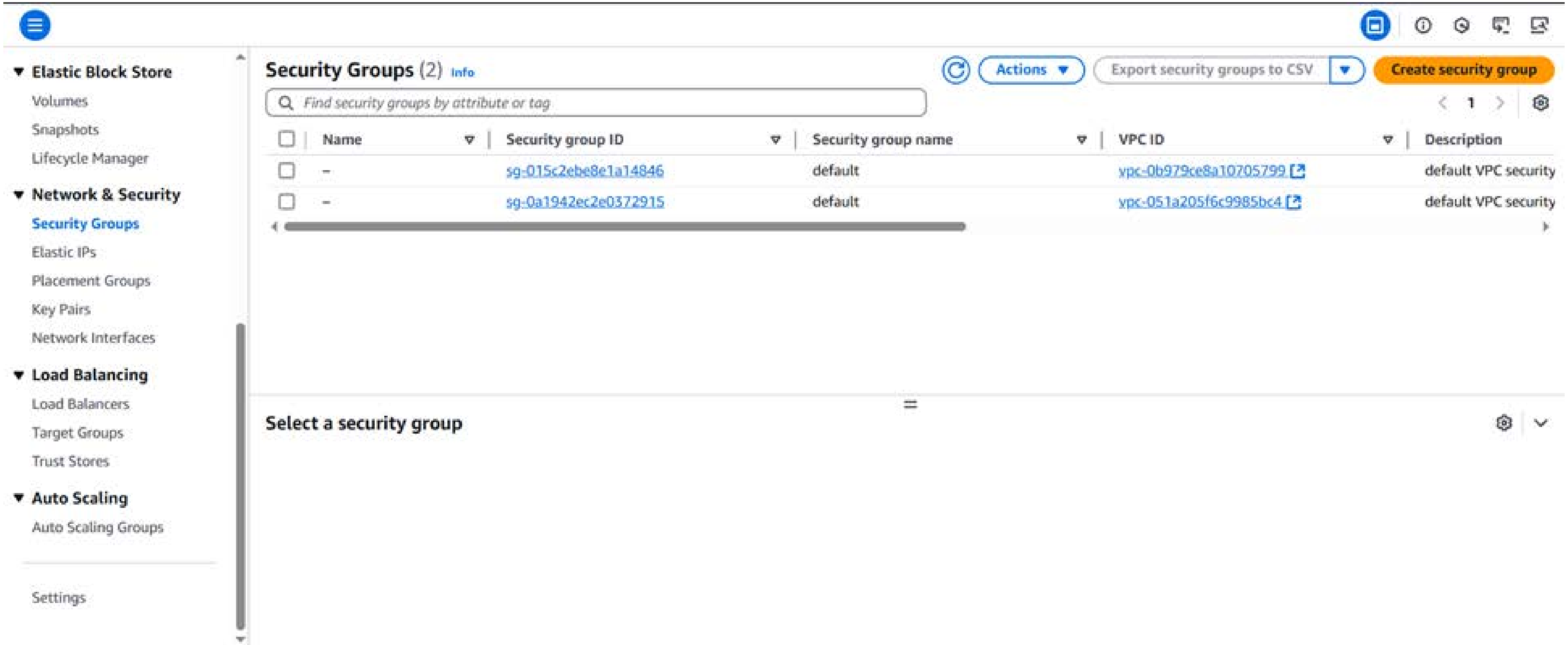
Input/output operations per second for a provisioned IOPS (SSD) volume.

100 IOPS

Throughput

The desired throughput to provision for the Amazon EBS root volume attached to your environment's EC2 instance

125 MiB/s

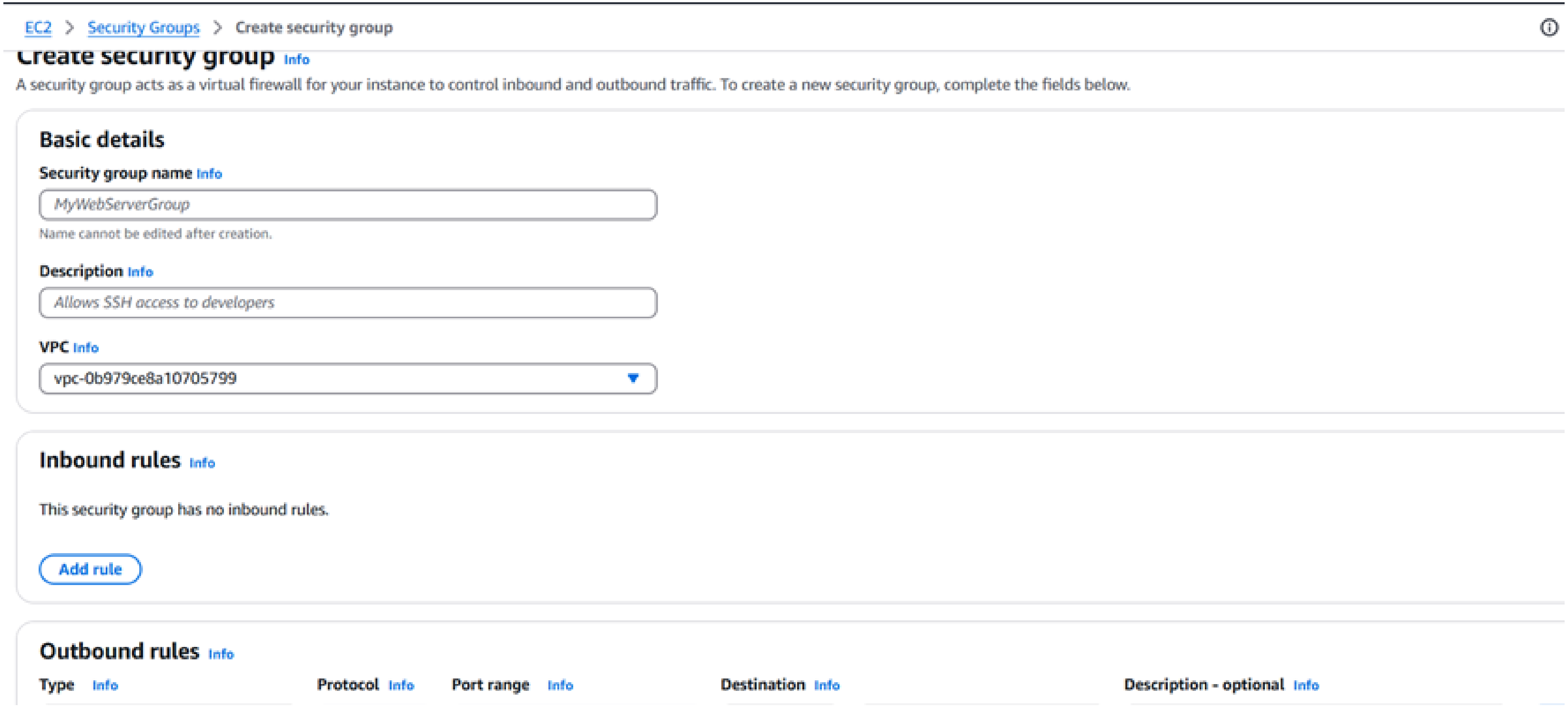


Security Groups (2)

Find security groups by attribute or tag

□	Name	Security group ID	Security group name	VPC ID	Description
□	–	sg-015c2ebe8e1a14846	default	vpc-0b979ce8a10705799	default VPC security
□	–	sg-0a1942ec2e0372915	default	vpc-051a205f6c9985bc4	default VPC security

Select a security group



EC2 > Security Groups > Create security group

Create security group Info

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

MyWebServerGroup

Name cannot be edited after creation.

Description Info

Allows SSH access to developers

VPC Info

vpc-0b979ce8a10705799

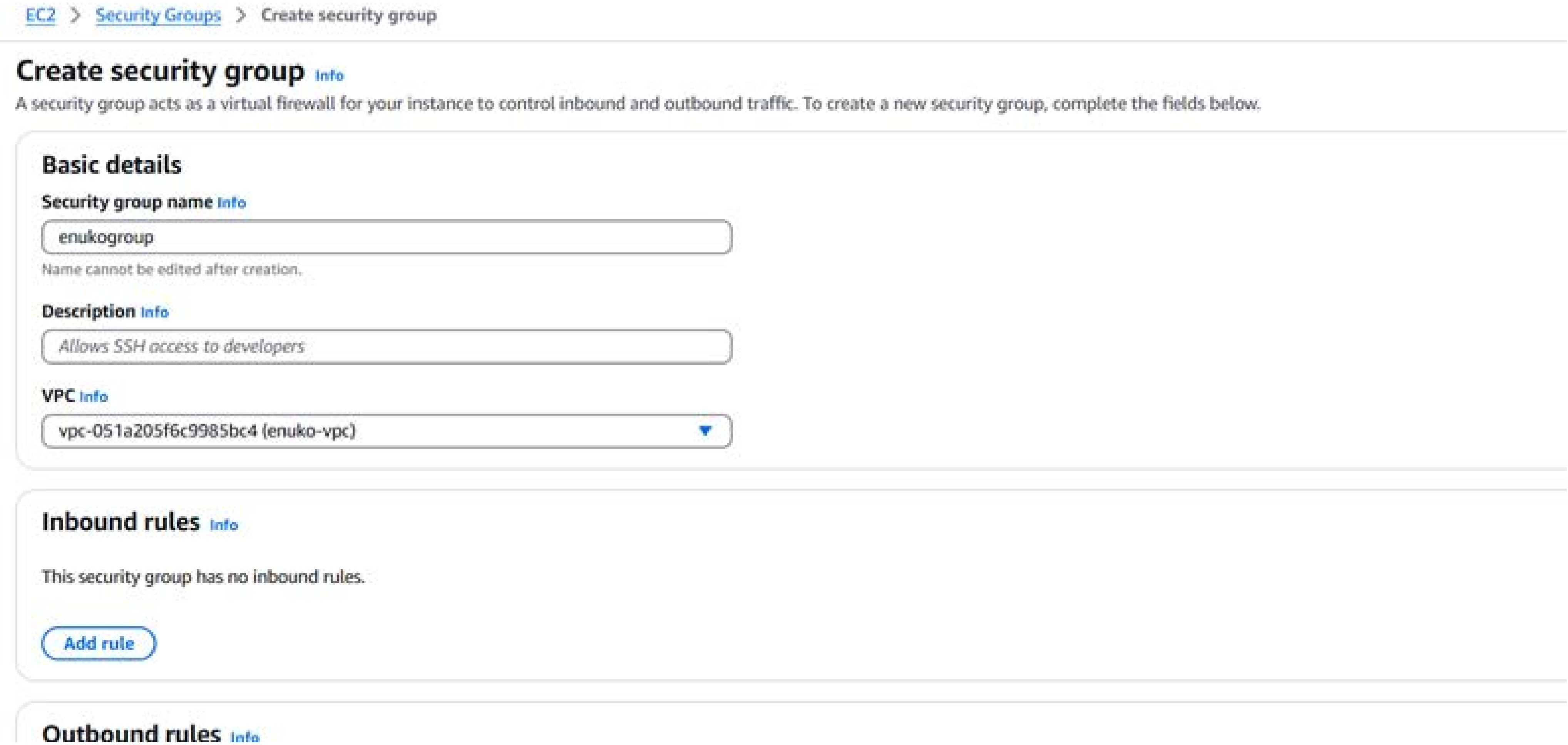
Inbound rules Info

This security group has no inbound rules.

Add rule

Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info



Create security group Info

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

enukogroup

Name cannot be edited after creation.

Description Info

Allows SSH access to developers

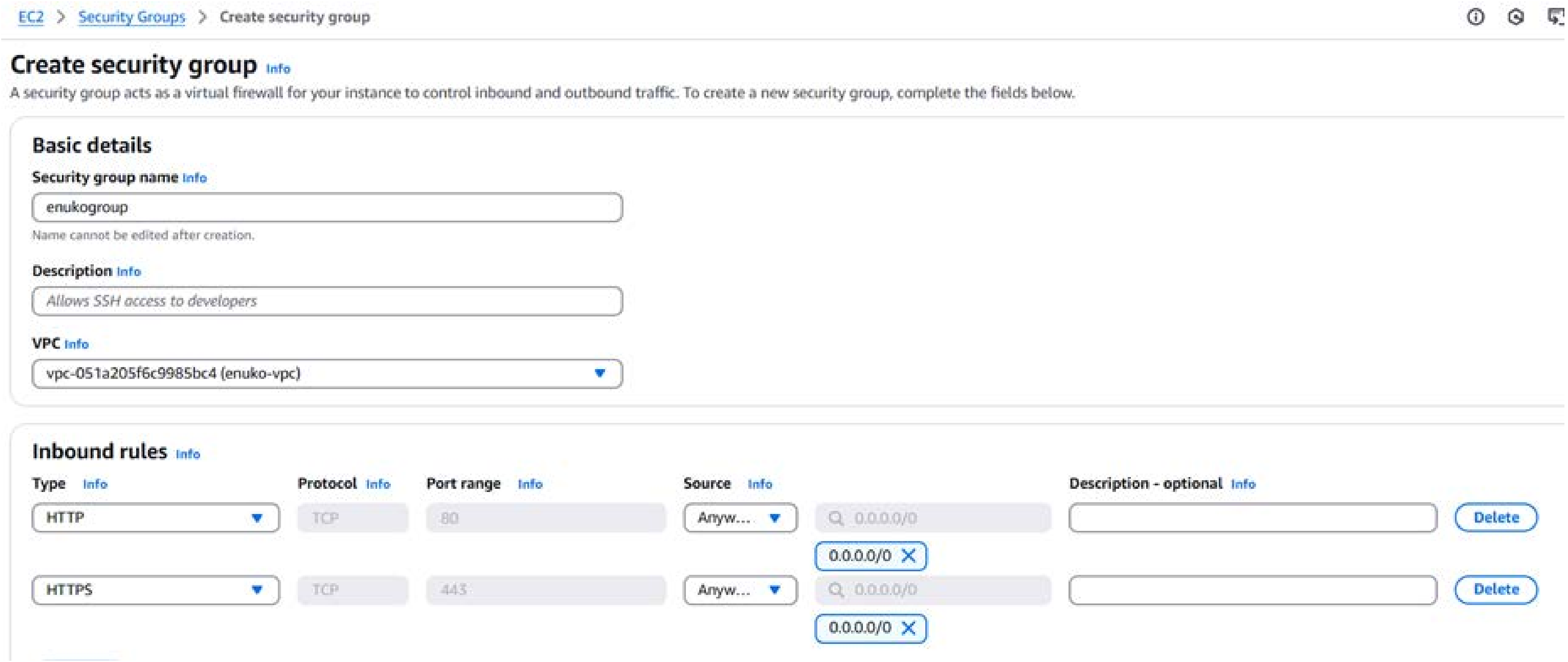
VPC Info

vpc-051a205f6c9985bc4 (enuko-vpc) ▼

Inbound rules Info

This security group has no inbound rules.

Outbound rules Info



EC2 > Security Groups > Create security group

Create security group Info

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

enukogroup

Name cannot be edited after creation.

Description Info

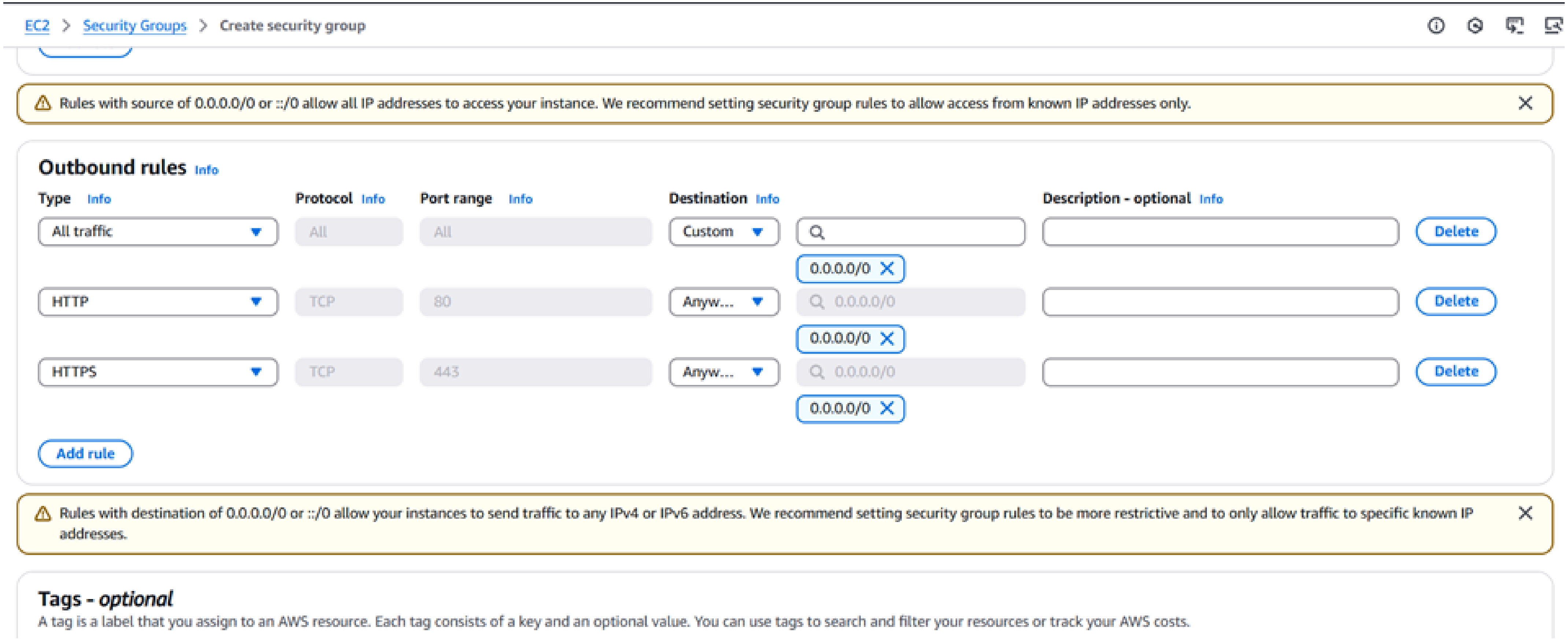
Allows SSH access to developers

VPC Info

vpc-051a205f6c9985bc4 (enuko-vpc) ▼

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
HTTP ▼	TCP	80	Anyw... ▼	0.0.0.0/0 0.0.0.0/0 ✕		Delete
HTTPS ▼	TCP	443	Anyw... ▼	0.0.0.0/0 0.0.0.0/0 ✕		Delete



EC2 > Security Groups > Create security group

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

Outbound rules Info

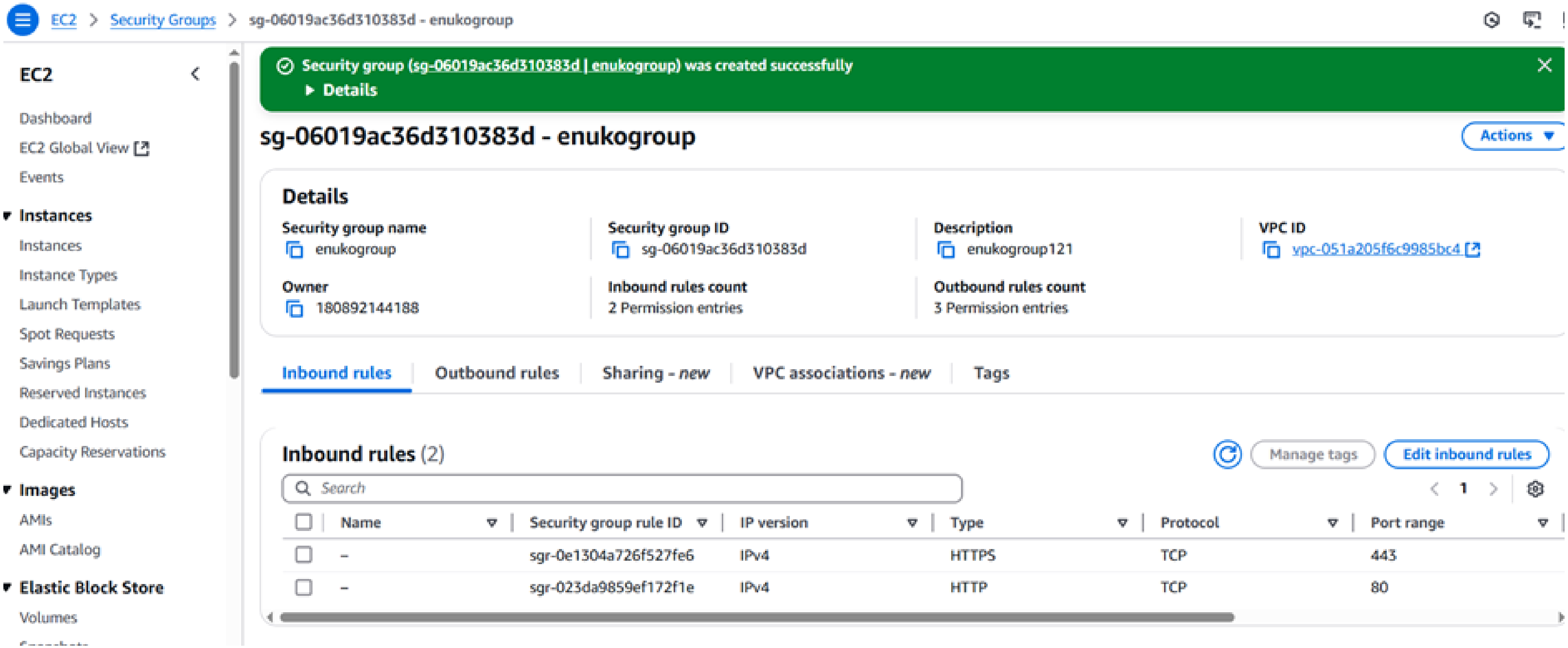
Type	Protocol	Port range	Destination		Description - optional	
All traffic	All	All	Custom	0.0.0.0/0		Delete
HTTP	TCP	80	Anyw...	0.0.0.0/0		Delete
HTTPS	TCP	443	Anyw...	0.0.0.0/0		Delete

Add rule

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

Tags - *optional*

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.



Security group (sg-06019ac36d310383d | enukogroup) was created successfully

▸ Details

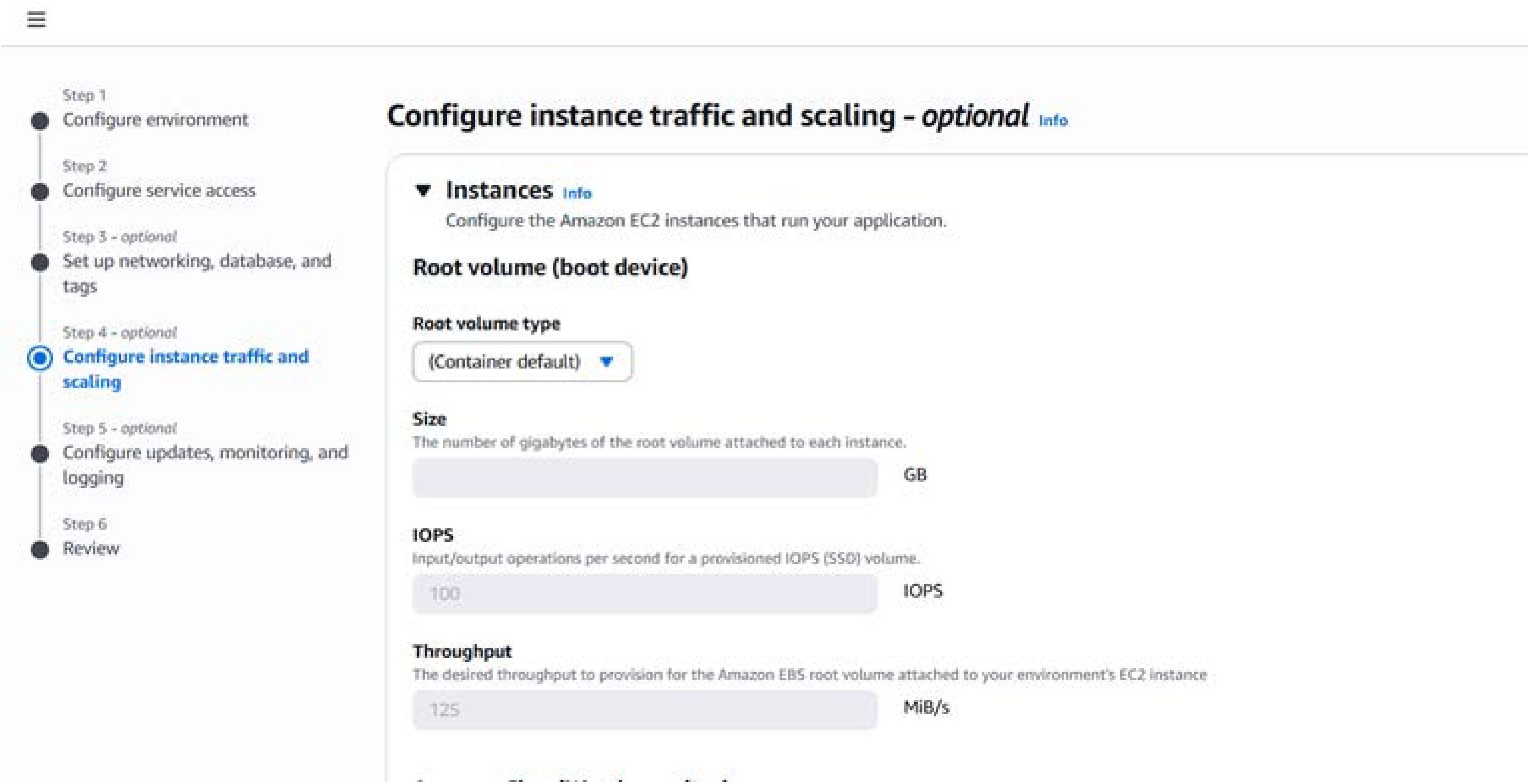
sg-06019ac36d310383d - enukogroup

Details

Security group name enukogroup	**Security group ID** sg-06019ac36d310383d	**Description** enukogroup121	**VPC ID** vpc-051a205f6c9985bc4
Owner 180892144188	**Inbound rules count** 2 Permission entries	**Outbound rules count** 3 Permission entries	

Inbound rules (2)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range
□	–	sgr-0e1304a726f527fe6	IPv4	HTTPS	TCP	443
□	–	sgr-023da9859ef172f1e	IPv4	HTTP	TCP	80



Step 1
● Configure environment

Step 2
● Configure service access

Step 3 - *optional*
● Set up networking, database, and tags

Step 4 - *optional*
◉ **Configure instance traffic and scaling**

Step 5 - *optional*
● Configure updates, monitoring, and logging

Step 6
● Review

Configure instance traffic and scaling - *optional*

▼ Instances

Configure the Amazon EC2 instances that run your application.

Root volume (boot device)

Root volume type

(Container default) ▼

Size

The number of gigabytes of the root volume attached to each instance.

[ ] GB

IOPS

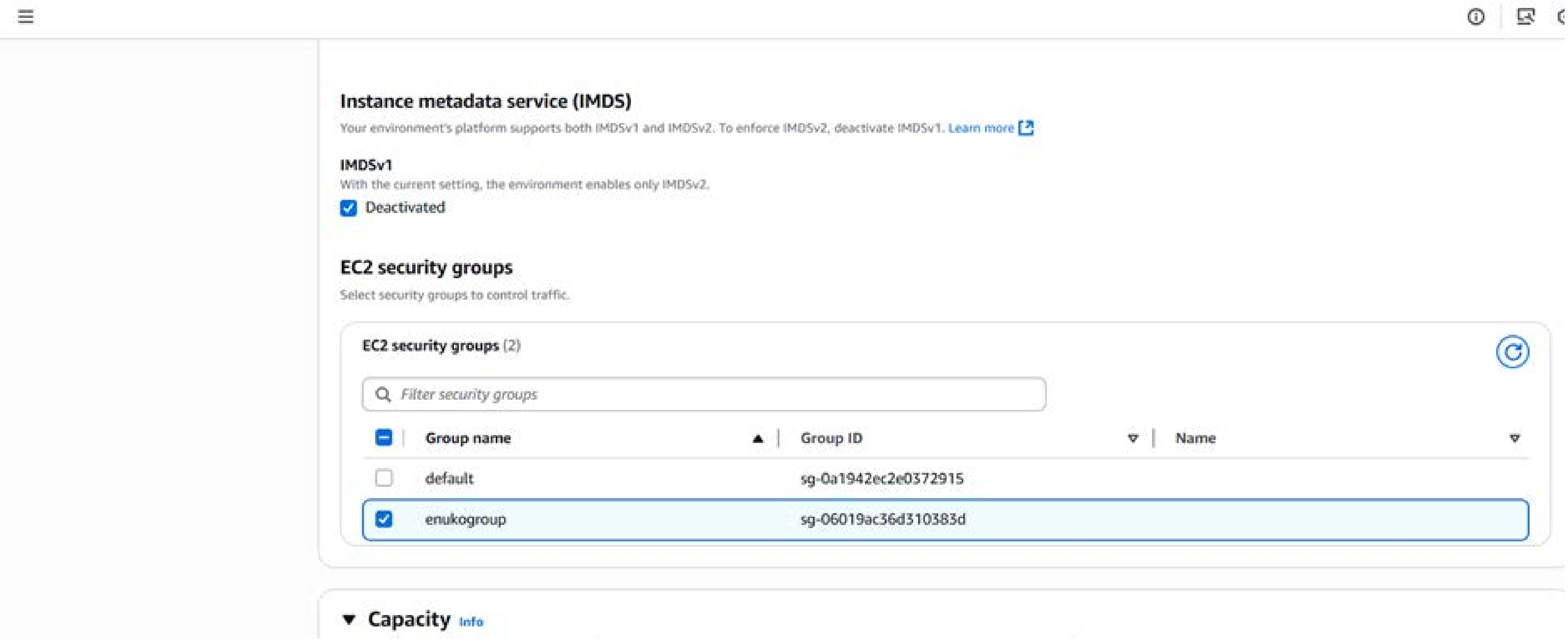
Input/output operations per second for a provisioned IOPS (SSD) volume.

100 IOPS

Throughput

The desired throughput to provision for the Amazon EBS root volume attached to your environment's EC2 instance

125 MiB/s



Instance metadata service (IMDS)

Your environment's platform supports both IMDSv1 and IMDSv2. To enforce IMDSv2, deactivate IMDSv1. Learn more

IMDSv1

With the current setting, the environment enables only IMDSv2.

☑ Deactivated

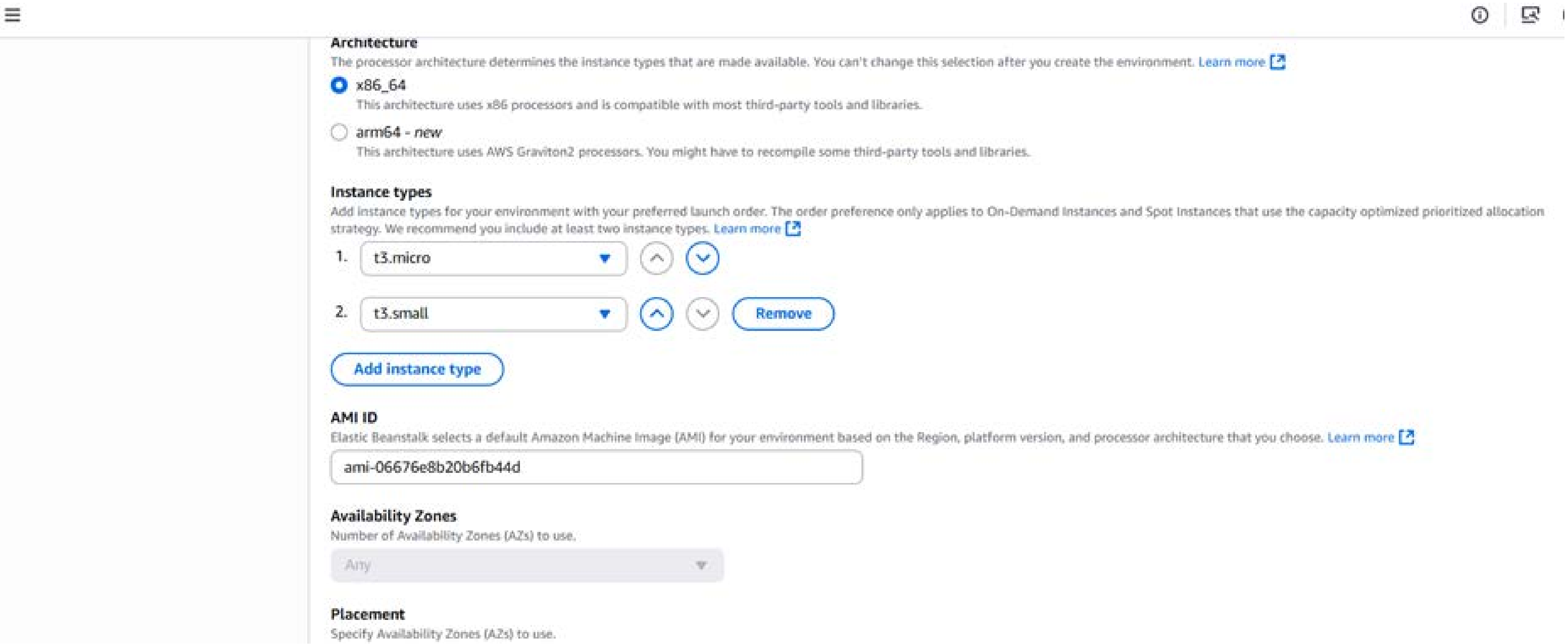
EC2 security groups

Select security groups to control traffic.

EC2 security groups (2)

☐	Group name	Group ID	Name
☐	default	sg-0a1942ec2e0372915	
☑	enukogroup	sg-06019ac36d310383d	

▼ Capacity Info



Architecture

The processor architecture determines the instance types that are made available. You can't change this selection after you create the environment. Learn more

● x86_64
This architecture uses x86 processors and is compatible with most third-party tools and libraries.

○ arm64 - *new*
This architecture uses AWS Graviton2 processors. You might have to recompile some third-party tools and libraries.

Instance types

Add instance types for your environment with your preferred launch order. The order preference only applies to On-Demand Instances and Spot Instances that use the capacity optimized prioritized allocation strategy. We recommend you include at least two instance types. Learn more

1. t3.micro
2. t3.small

AMI ID

Elastic Beanstalk selects a default Amazon Machine Image (AMI) for your environment based on the Region, platform version, and processor architecture that you choose. Learn more

ami-06676e8b20b6fb44d

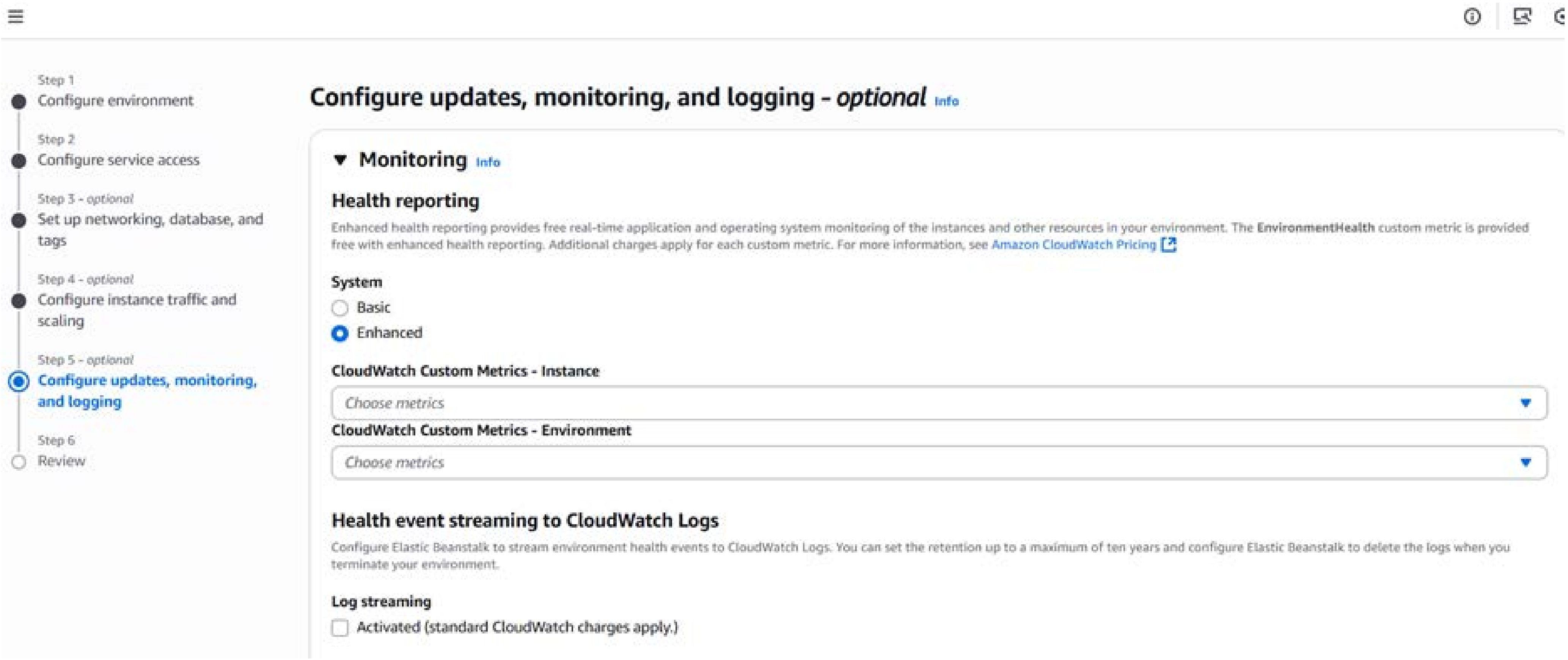
Availability Zones

Number of Availability Zones (AZs) to use.

Any

Placement

Specify Availability Zones (AZs) to use.



Step 1
● Configure environment

Step 2
● Configure service access

Step 3 - *optional*
● Set up networking, database, and tags

Step 4 - *optional*
● Configure instance traffic and scaling

Step 5 - *optional*
◉ **Configure updates, monitoring, and logging**

Step 6
○ Review

Configure updates, monitoring, and logging - *optional* Info

▼ Monitoring Info

Health reporting

Enhanced health reporting provides free real-time application and operating system monitoring of the instances and other resources in your environment. The **EnvironmentHealth** custom metric is provided free with enhanced health reporting. Additional charges apply for each custom metric. For more information, see Amazon CloudWatch Pricing

System

○ Basic

● Enhanced

CloudWatch Custom Metrics - Instance

Choose metrics ▼

CloudWatch Custom Metrics - Environment

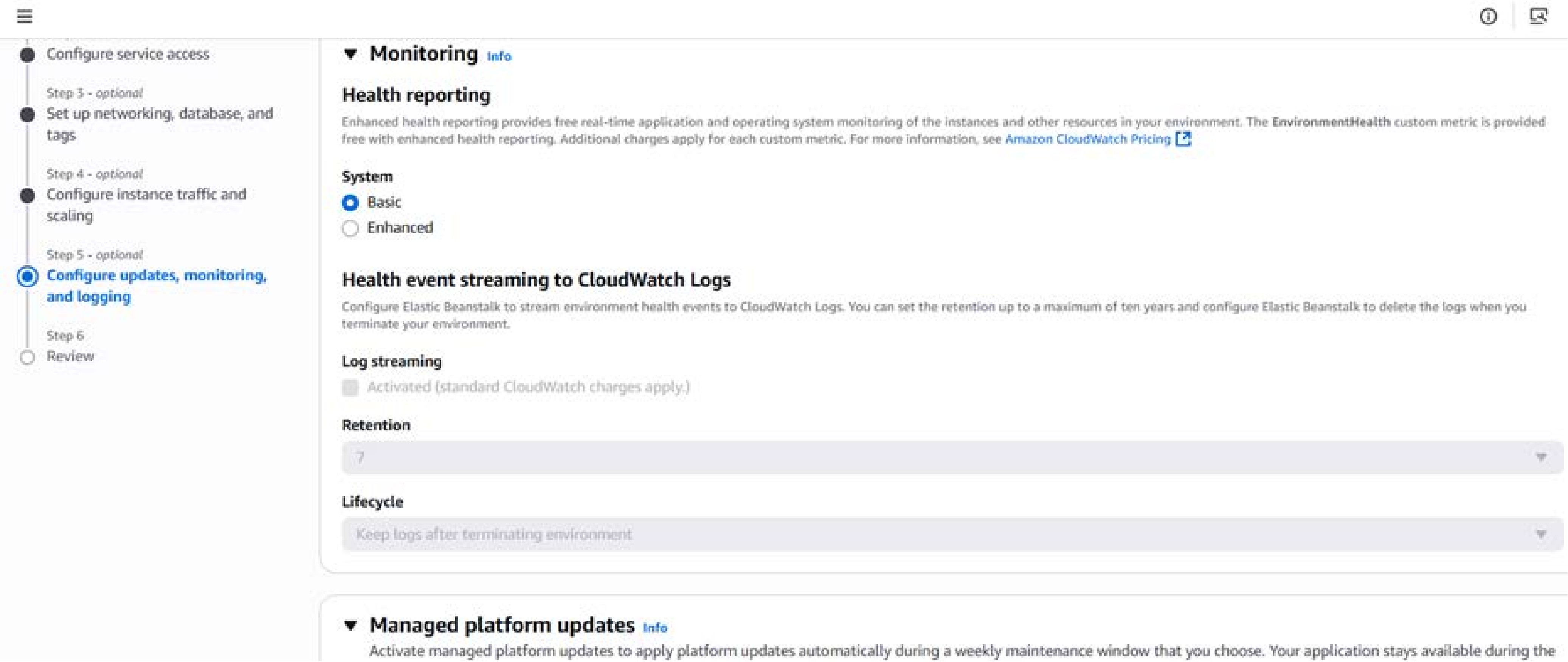
Choose metrics ▼

Health event streaming to CloudWatch Logs

Configure Elastic Beanstalk to stream environment health events to CloudWatch Logs. You can set the retention up to a maximum of ten years and configure Elastic Beanstalk to delete the logs when you terminate your environment.

Log streaming

□ Activated (standard CloudWatch charges apply.)



Configure service access
Step 3 - *optional*
Set up networking, database, and tags
Step 4 - *optional*
Configure instance traffic and scaling
Step 5 - *optional*
Configure updates, monitoring, and logging
Step 6
Review

▼ Monitoring Info

Health reporting

Enhanced health reporting provides free real-time application and operating system monitoring of the instances and other resources in your environment. The **EnvironmentHealth** custom metric is provided free with enhanced health reporting. Additional charges apply for each custom metric. For more information, see Amazon CloudWatch Pricing

System

● Basic

○ Enhanced

Health event streaming to CloudWatch Logs

Configure Elastic Beanstalk to stream environment health events to CloudWatch Logs. You can set the retention up to a maximum of ten years and configure Elastic Beanstalk to delete the logs when you terminate your environment.

Log streaming

□ Activated (standard CloudWatch charges apply.)

Retention

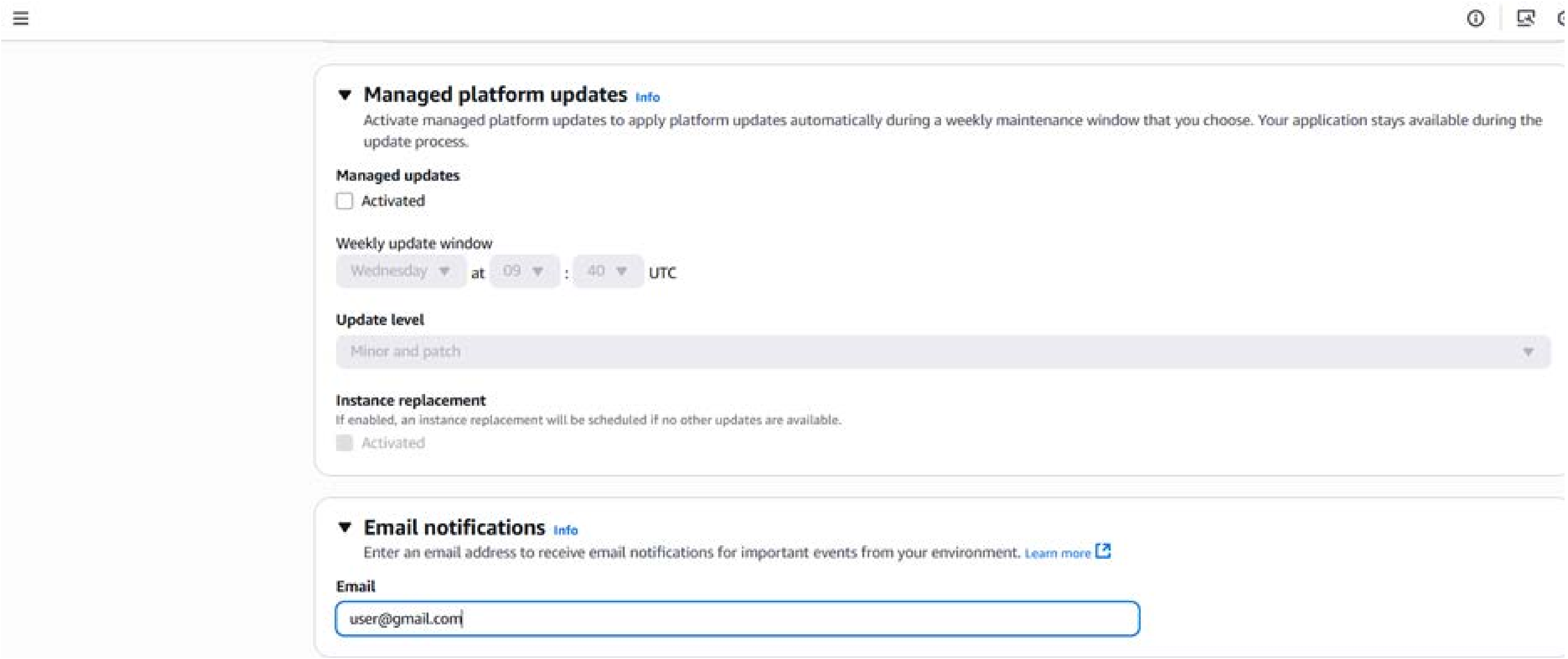
7

Lifecycle

Keep logs after terminating environment

▼ Managed platform updates Info

Activate managed platform updates to apply platform updates automatically during a weekly maintenance window that you choose. Your application stays available during the



Managed platform updates

Info

Activate managed platform updates to apply platform updates automatically during a weekly maintenance window that you choose. Your application stays available during the update process.

Managed updates

□ Activated

Weekly update window

Wednesday ▼ at 09 ▼ : 40 ▼ UTC

Update level

Minor and patch ▼

Instance replacement

If enabled, an instance replacement will be scheduled if no other updates are available.

□ Activated

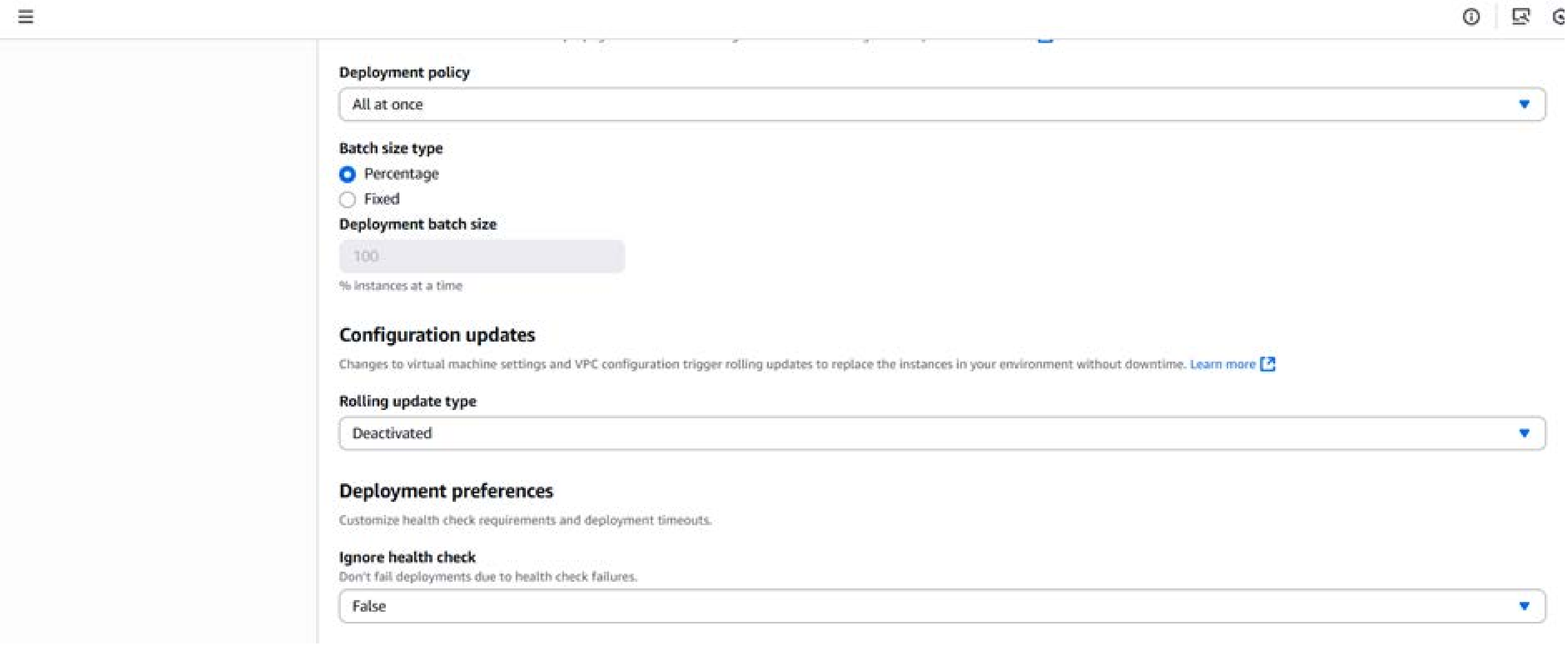
Email notifications

Info

Enter an email address to receive email notifications for important events from your environment. Learn more

Email

user@gmail.com



Deployment policy

All at once

Batch size type

● Percentage

○ Fixed

Deployment batch size

100

% instances at a time

Configuration updates

Changes to virtual machine settings and VPC configuration trigger rolling updates to replace the instances in your environment without downtime. Learn more

Rolling update type

Deactivated

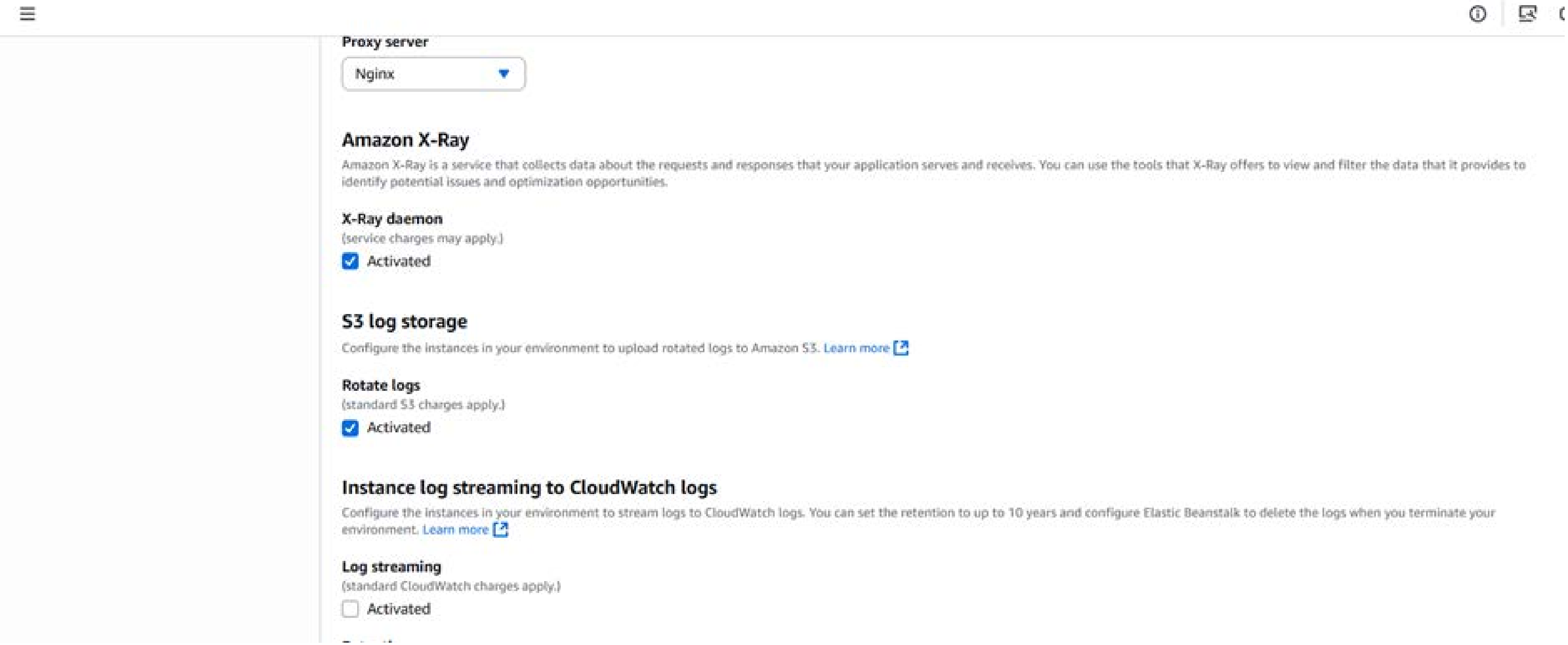
Deployment preferences

Customize health check requirements and deployment timeouts.

Ignore health check

Don't fail deployments due to health check failures.

False



Proxy server

Nginx ▼

Amazon X-Ray

Amazon X-Ray is a service that collects data about the requests and responses that your application serves and receives. You can use the tools that X-Ray offers to view and filter the data that it provides to identify potential issues and optimization opportunities.

X-Ray daemon
(service charges may apply.)

☑ Activated

S3 log storage

Configure the instances in your environment to upload rotated logs to Amazon S3. Learn more

Rotate logs
(standard S3 charges apply.)

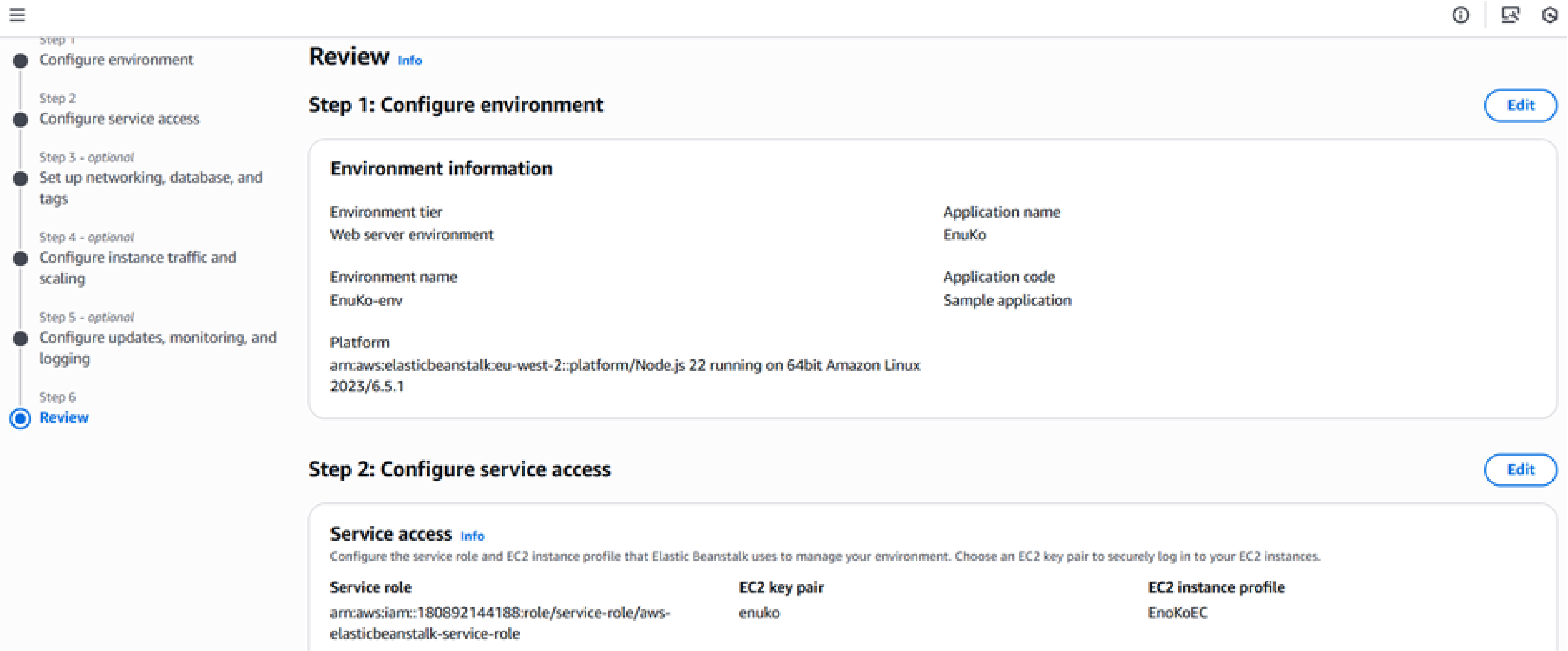
☑ Activated

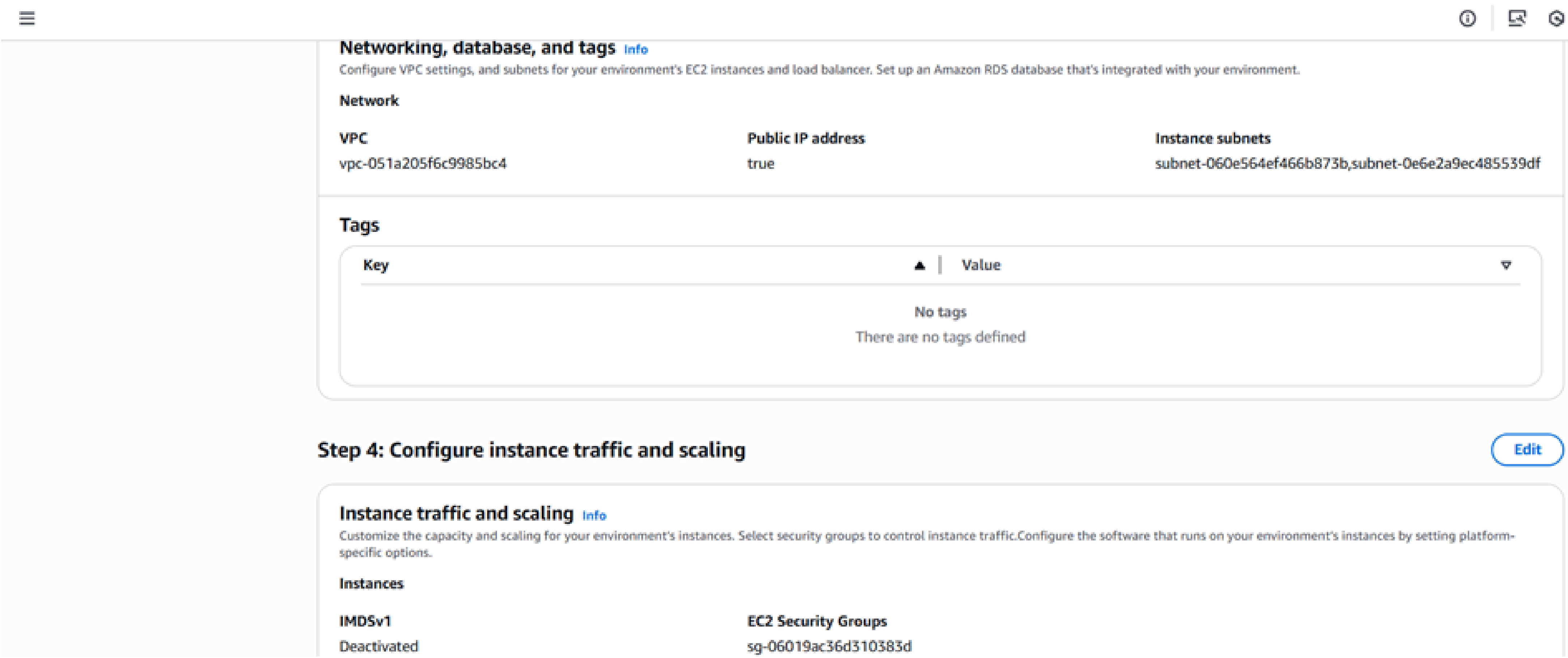
Instance log streaming to CloudWatch logs

Configure the instances in your environment to stream logs to CloudWatch logs. You can set the retention to up to 10 years and configure Elastic Beanstalk to delete the logs when you terminate your environment. Learn more

Log streaming
(standard CloudWatch charges apply.)

☐ Activated





Networking, database, and tags Info

Configure VPC settings, and subnets for your environment's EC2 instances and load balancer. Set up an Amazon RDS database that's integrated with your environment.

Network

VPC	Public IP address	Instance subnets
vpc-051a205f6c9985bc4	true	subnet-060e564ef466b873b,subnet-0e6e2a9ec485539df

Tags

Key	Value

No tags

There are no tags defined

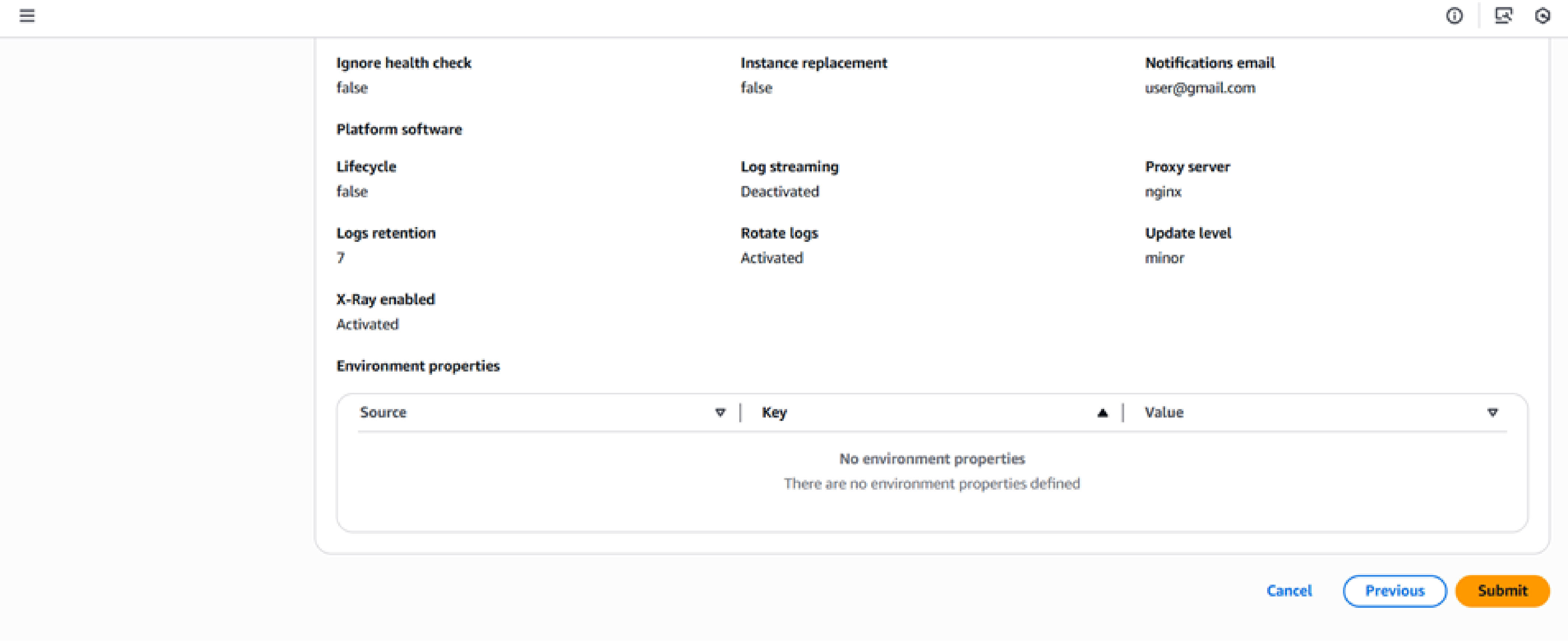
Step 4: Configure instance traffic and scaling

Instance traffic and scaling Info

Customize the capacity and scaling for your environment's instances. Select security groups to control instance traffic.Configure the software that runs on your environment's instances by setting platform-specific options.

Instances

IMDSv1	EC2 Security Groups
Deactivated	sg-06019ac36d310383d



Ignore health check
false

Instance replacement
false

Notifications email
user@gmail.com

Platform software

Lifecycle
false

Log streaming
Deactivated

Proxy server
nginx

Logs retention
7

Rotate logs
Activated

Update level
minor

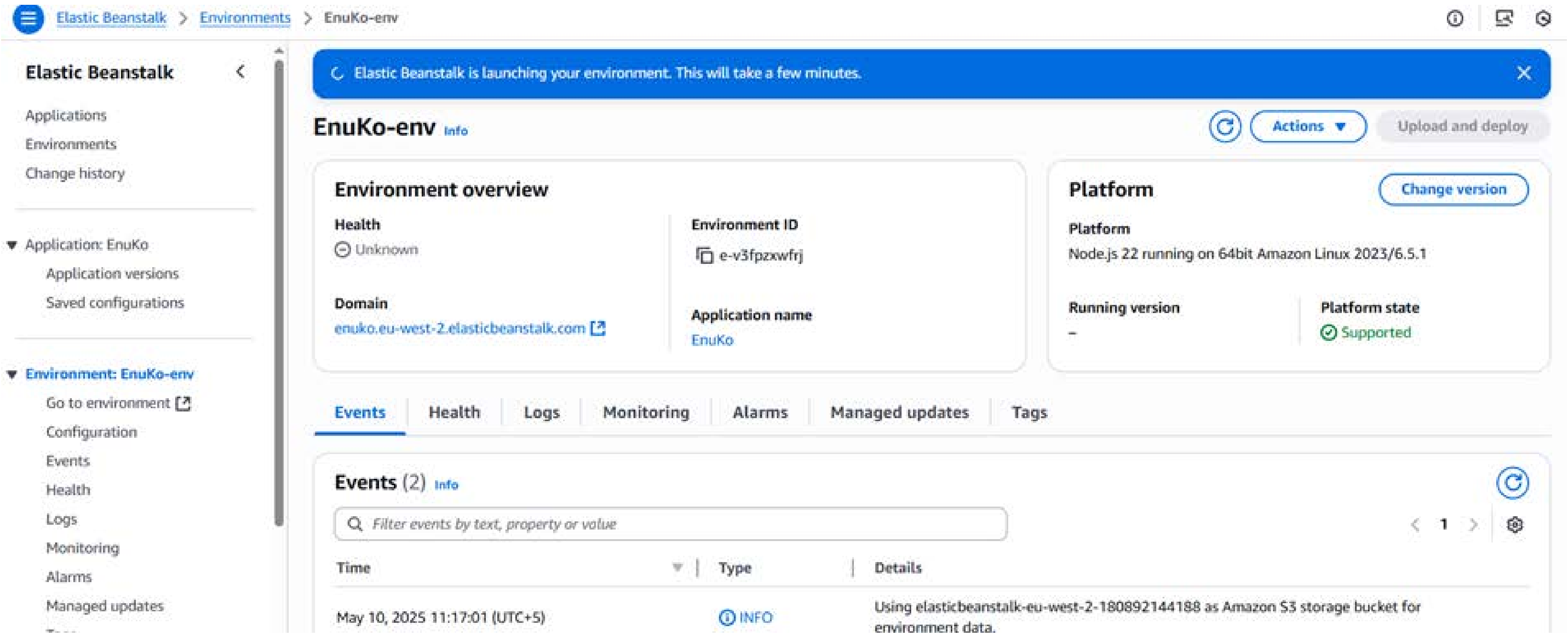
X-Ray enabled
Activated

Environment properties

Source	Key	Value

No environment properties

There are no environment properties defined



Elastic Beanstalk is launching your environment. This will take a few minutes.

EnuKo-env

Environment overview

Health: Unknown

Environment ID: e-v3fpzxwfrj

Domain: enuko.eu-west-2.elasticbeanstalk.com

Application name: EnuKo

Platform

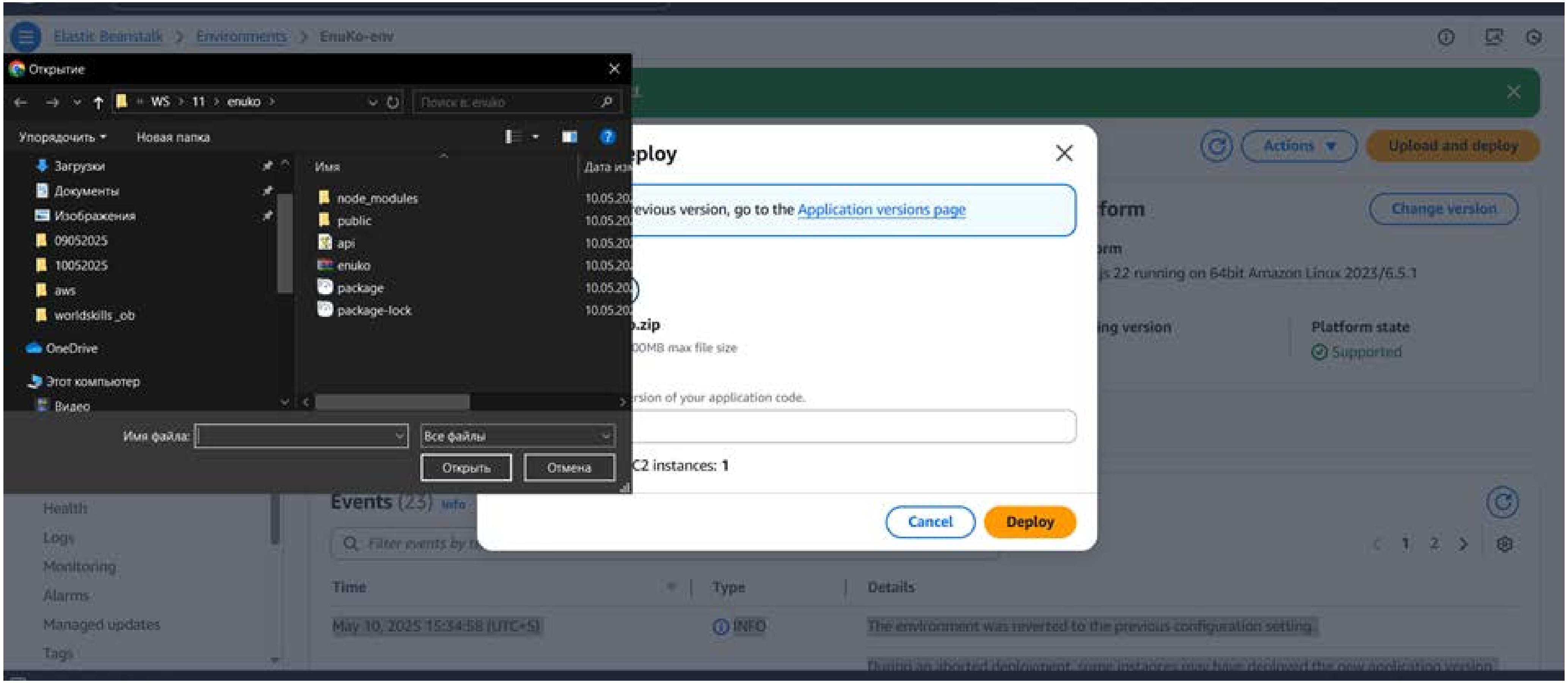
Platform: Node.js 22 running on 64bit Amazon Linux 2023/6.5.1

Running version: –

Platform state: Supported

Events (2)

Time	Type	Details
May 10, 2025 11:17:01 (UTC+5)	INFO	Using elasticbeanstalk-eu-west-2-180892144188 as Amazon S3 storage bucket for environment data.



eploy

revious version, go to the Application versions page

.zip

00MB max file size

rsion of your application code.

C2 instances: 1

form

rm

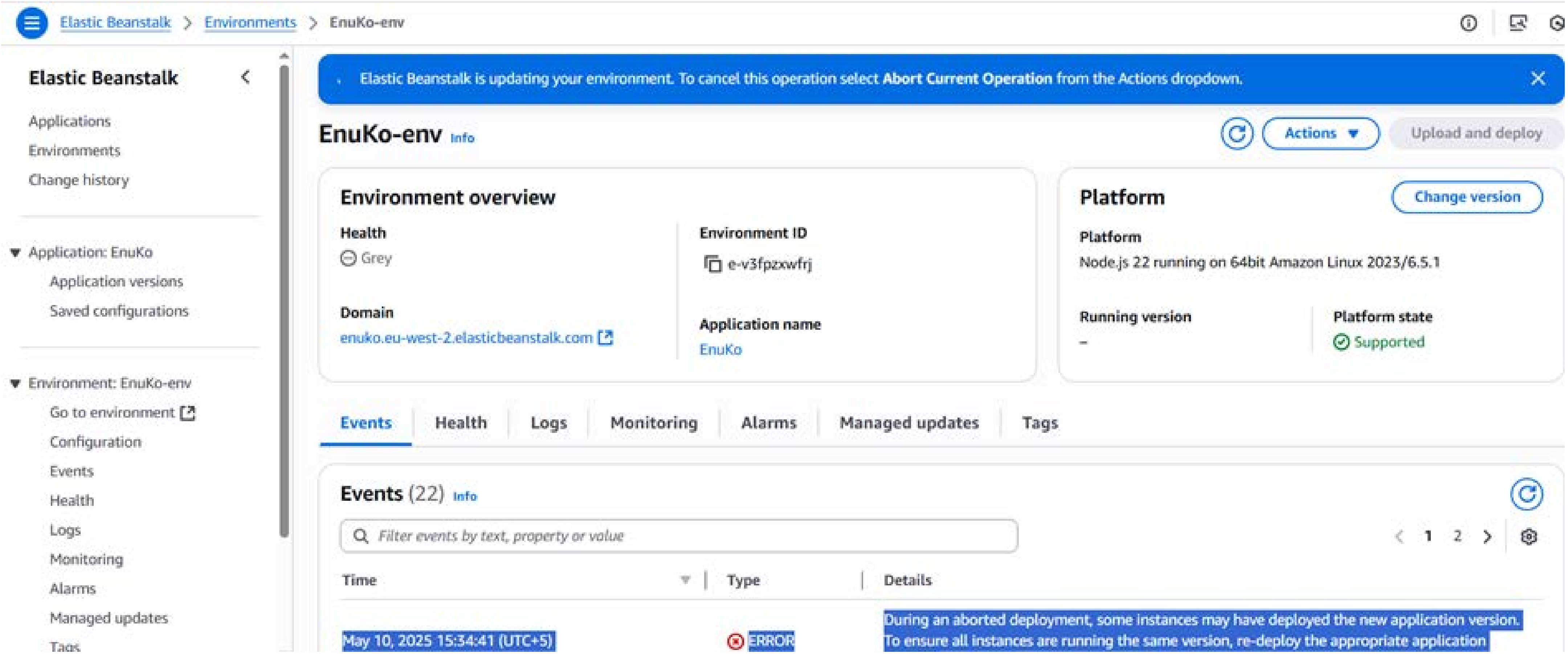
js 22 running on 64bit Amazon Linux 2023/6.5.1

ing version

Platform state

Supported

Time	Type	Details
May 10, 2025 15:34:58 (UTC+5)	INFO	The environment was reverted to the previous configuration setting.
		During an aborted deployment, some instances may have deployed the new application version.



Elastic Beanstalk is updating your environment. To cancel this operation select **Abort Current Operation** from the Actions dropdown.

EnuKo-env

Environment overview

Health
Grey

Environment ID
e-v3fpzxwfrj

Domain
enuko.eu-west-2.elasticbeanstalk.com

Application name
EnuKo

Platform

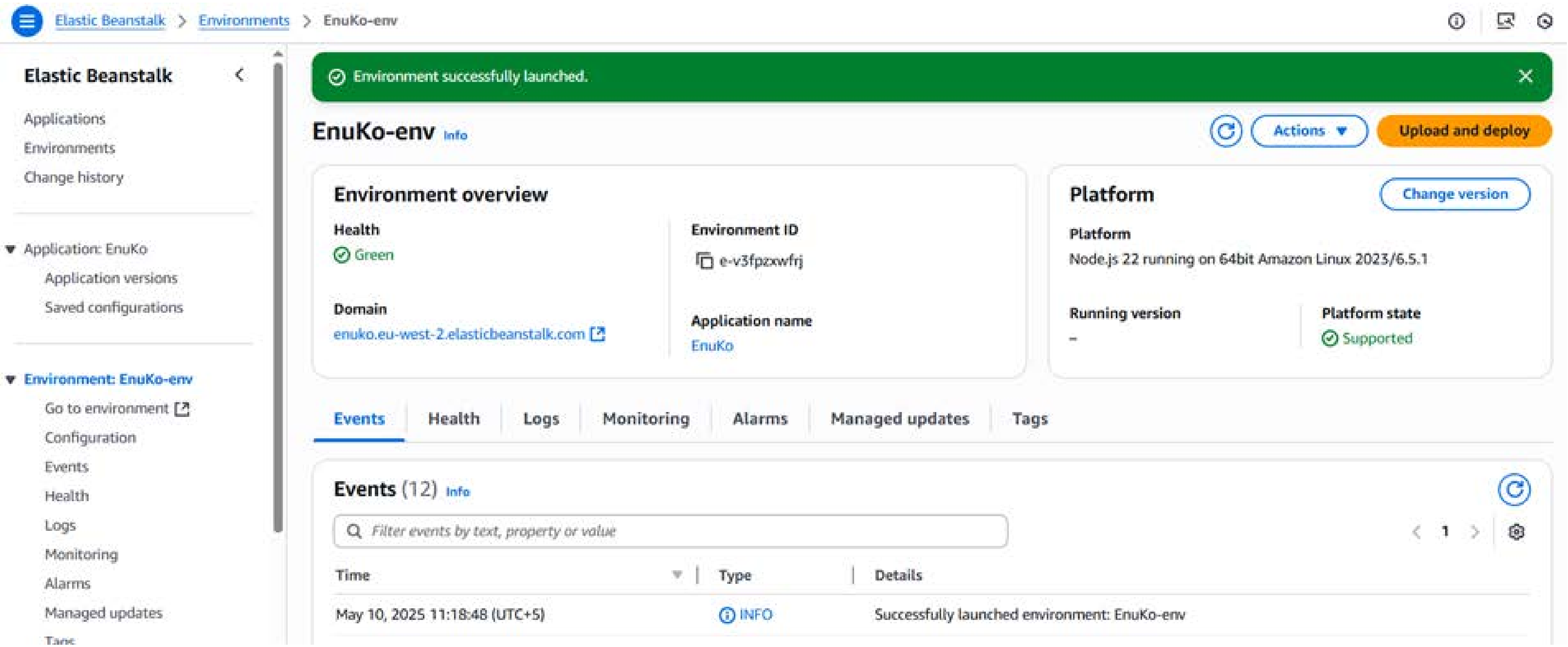
Platform
Node.js 22 running on 64bit Amazon Linux 2023/6.5.1

Running version
–

Platform state
✓ Supported

Events (22)

Time	Type	Details
May 10, 2025 15:34:41 (UTC+5)	⊗ ERROR	During an aborted deployment, some instances may have deployed the new application version. To ensure all instances are running the same version, re-deploy the appropriate application



Environment successfully launched.

EnuKo-env

Environment overview

Health: Green

Environment ID: e-v3fpzxwfrj

Domain: enuko.eu-west-2.elasticbeanstalk.com

Application name: EnuKo

Platform

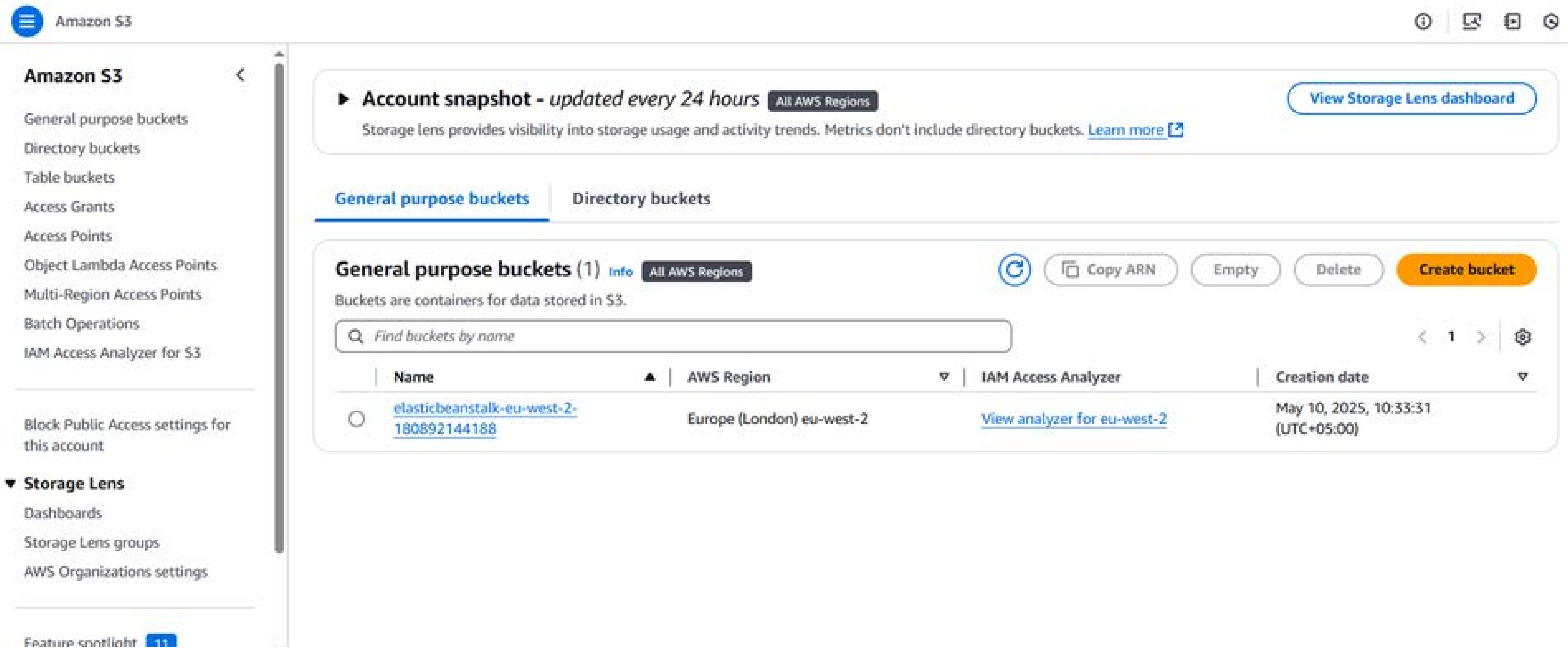
Platform: Node.js 22 running on 64bit Amazon Linux 2023/6.5.1

Running version: –

Platform state: Supported

Events (12)

Time	Type	Details
May 10, 2025 11:18:48 (UTC+5)	INFO	Successfully launched environment: EnuKo-env



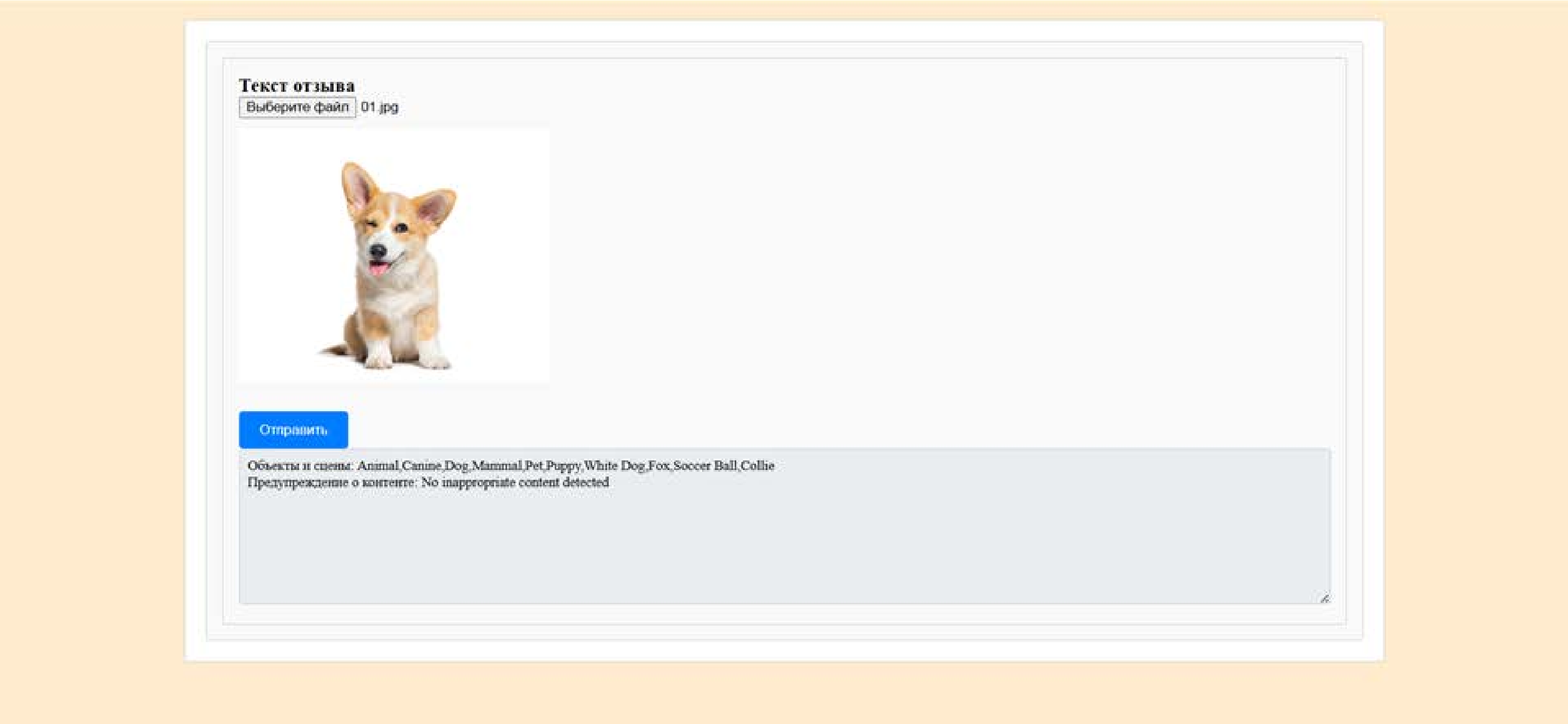
Account snapshot - *updated every 24 hours* All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more

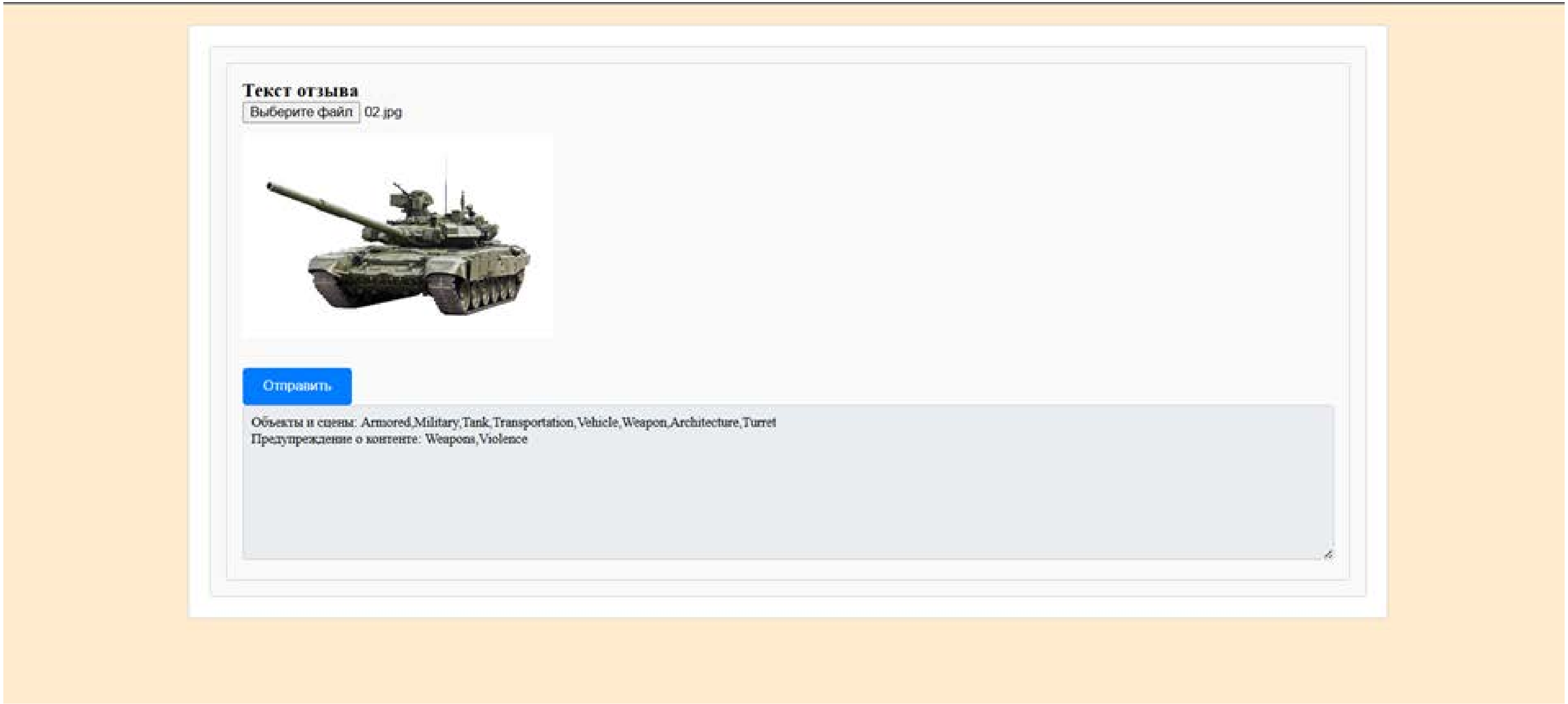
General purpose buckets (1)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	elasticbeanstalk-eu-west-2-180892144188	Europe (London) eu-west-2	View analyzer for eu-west-2	May 10, 2025, 10:33:31 (UTC+05:00)



```
Объекты и сцены: Animal,Canine,Dog,Mammal,Pet,Puppy,White Dog,Fox,Soccer Ball,Collie
Предупреждение о контенте: No inappropriate content detected
```



Объекты и сцены: Armored,Military,Tank,Transportation,Vehicle,Weapon,Architecture,Turret
Предупреждение о контенте: Weapons,Violence