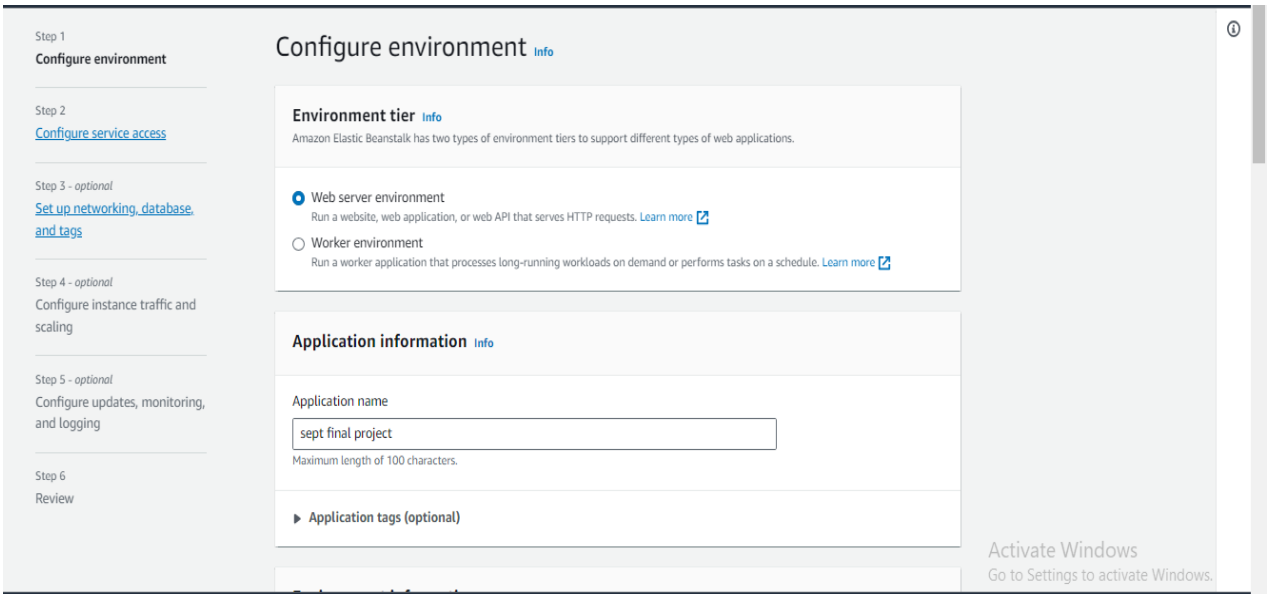
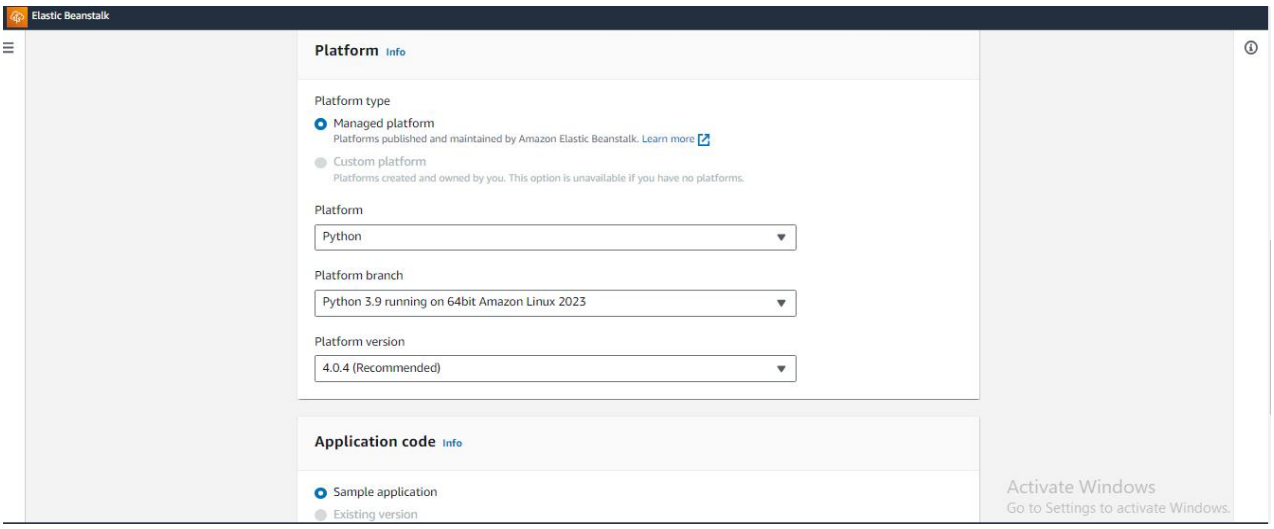
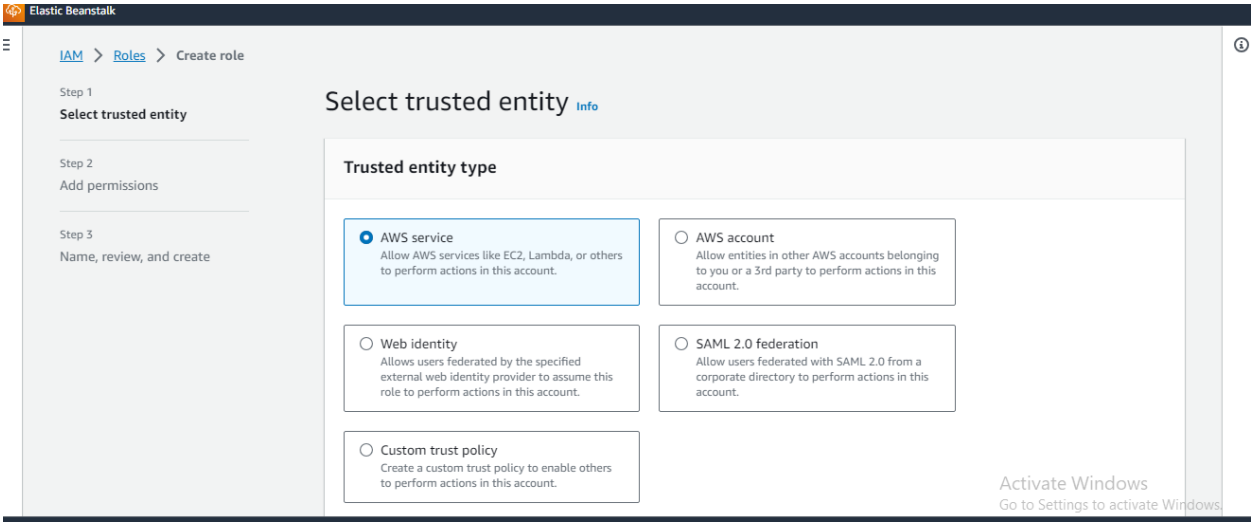
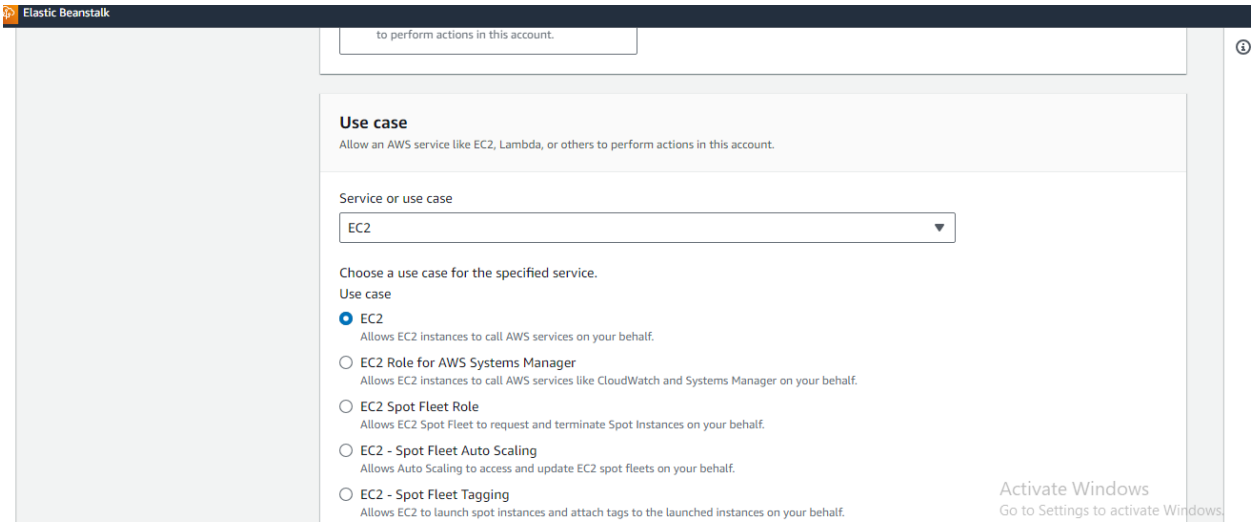
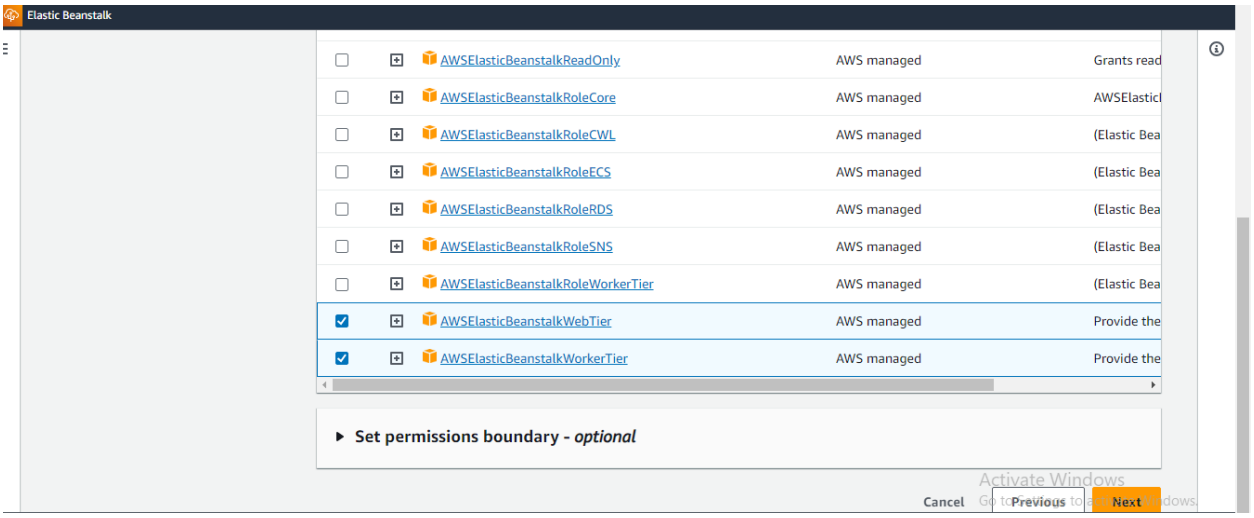
Project Name: Scalable Web Application using AWS Elastic Beanstalk.

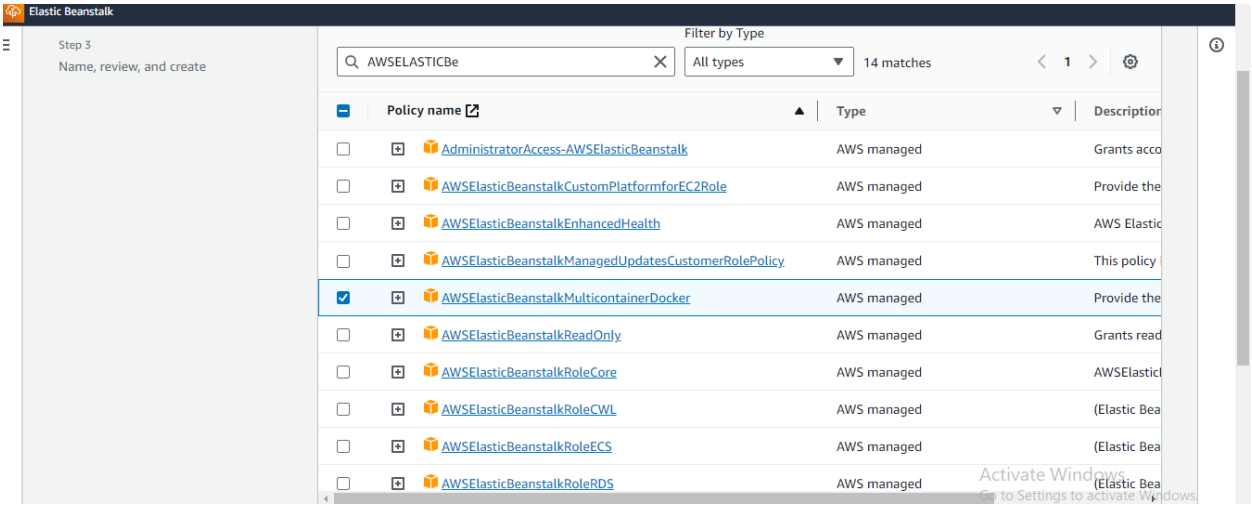


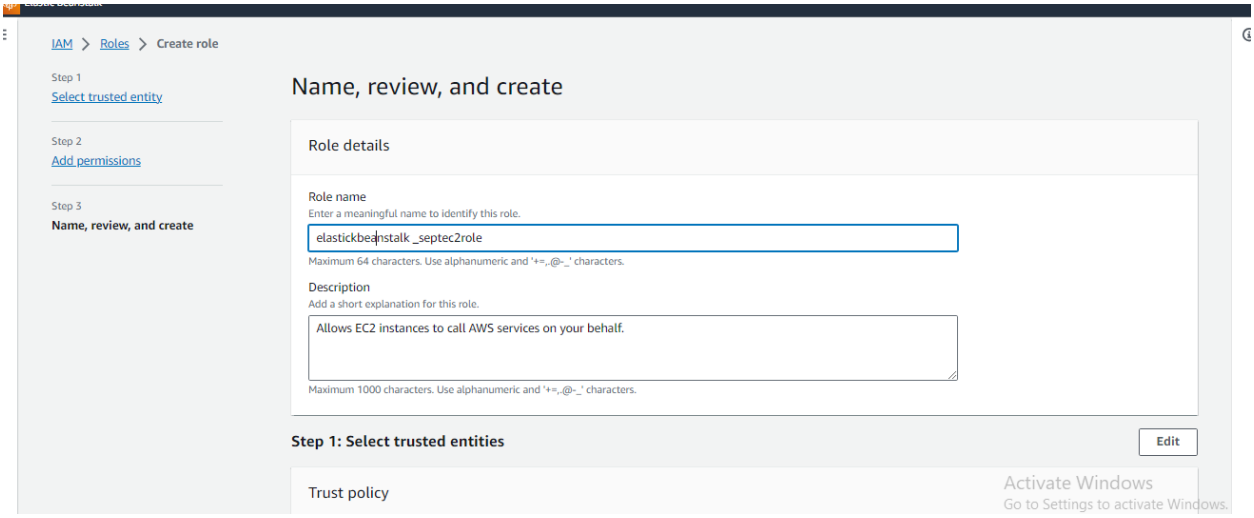


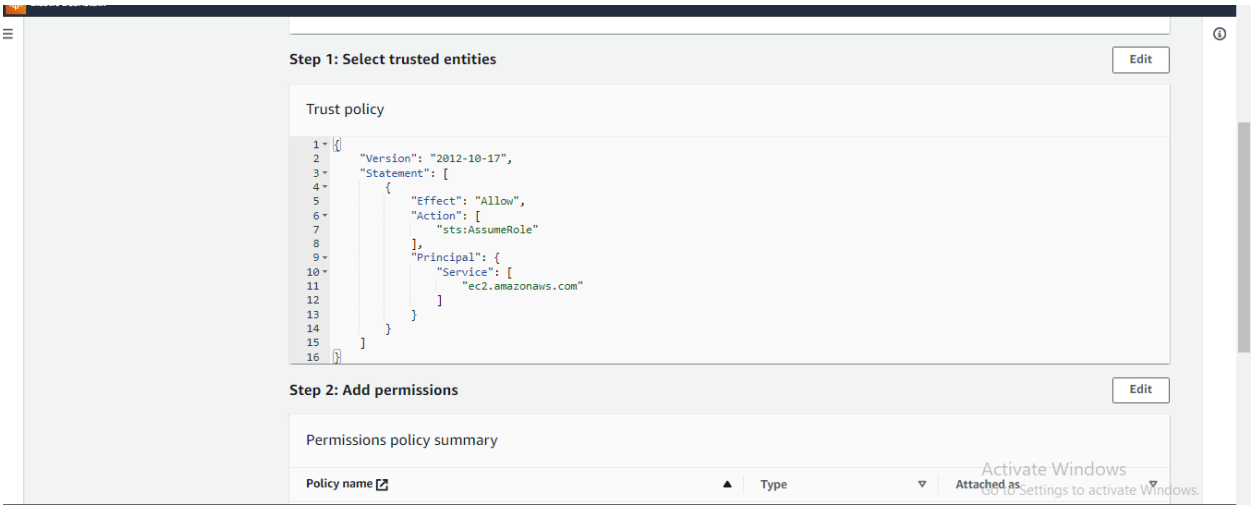

Elastic Beanstalk
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other 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.
Activate Windows
Go to Settings to activate Windows.

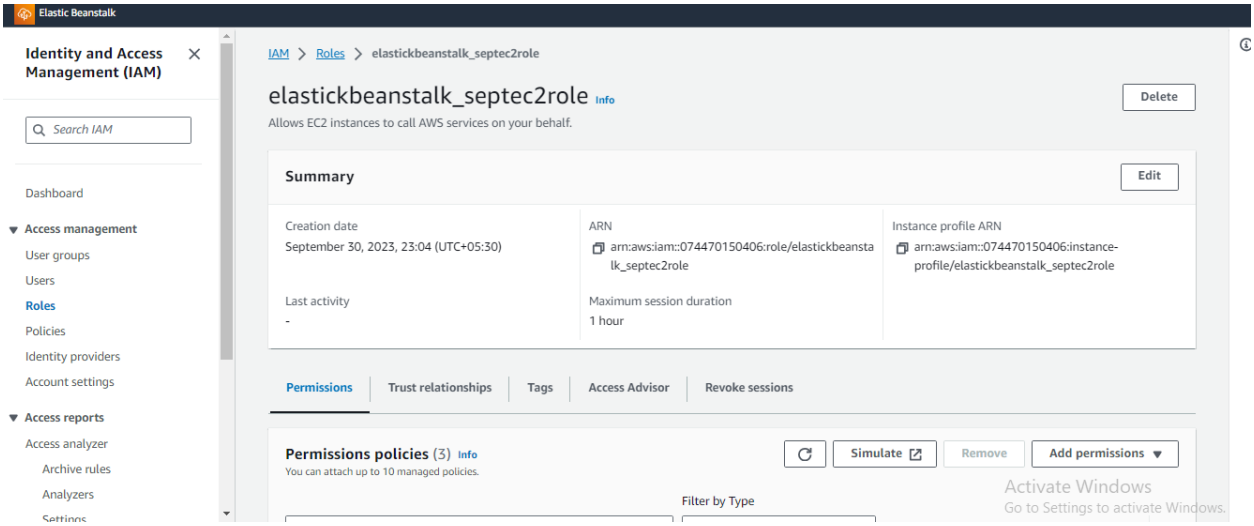

Elastic Beanstalk
to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
EC2
Choose a use case for the specified service.
Use case
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
Activate Windows
Go to Settings to activate Windows.

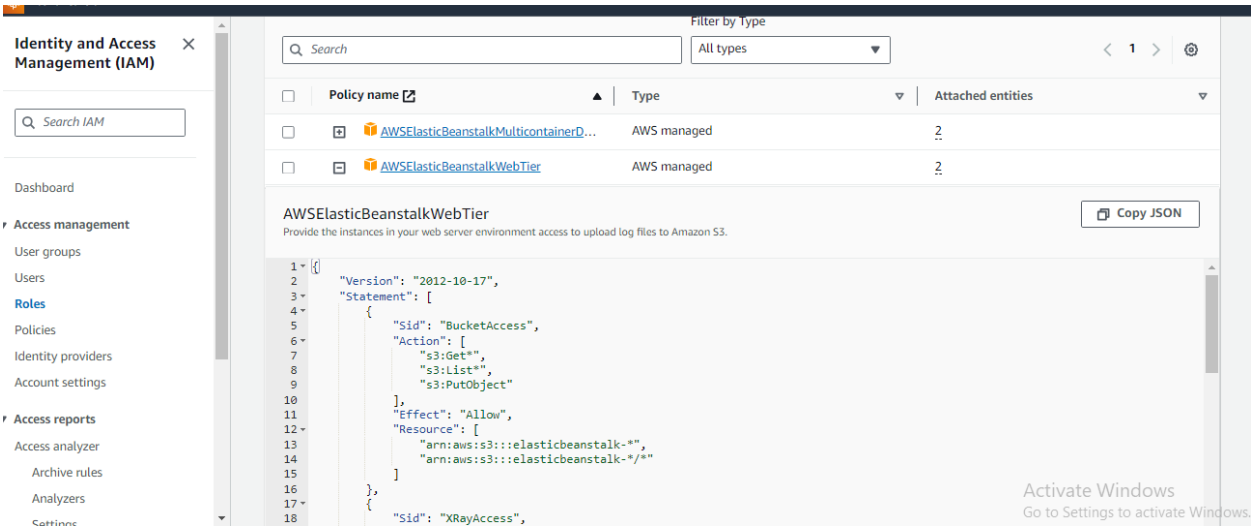

Elastic Beanstalk
AWSElasticBeanstalkReadOnly AWS managed Grants read
AWSElasticBeanstalkRoleCore AWS managed AWSElastic
AWSElasticBeanstalkRoleCWL AWS managed (Elastic Bea
AWSElasticBeanstalkRoleECS AWS managed (Elastic Bea
AWSElasticBeanstalkRoleRDS AWS managed (Elastic Bea
AWSElasticBeanstalkRoleSNS AWS managed (Elastic Bea
AWSElasticBeanstalkRoleWorkerTier AWS managed (Elastic Bea
AWSElasticBeanstalkWebTier AWS managed Provide the
AWSElasticBeanstalkWorkerTier AWS managed Provide the
Set permissions boundary - optional
Activate Windows
Cancel
Previous
Next

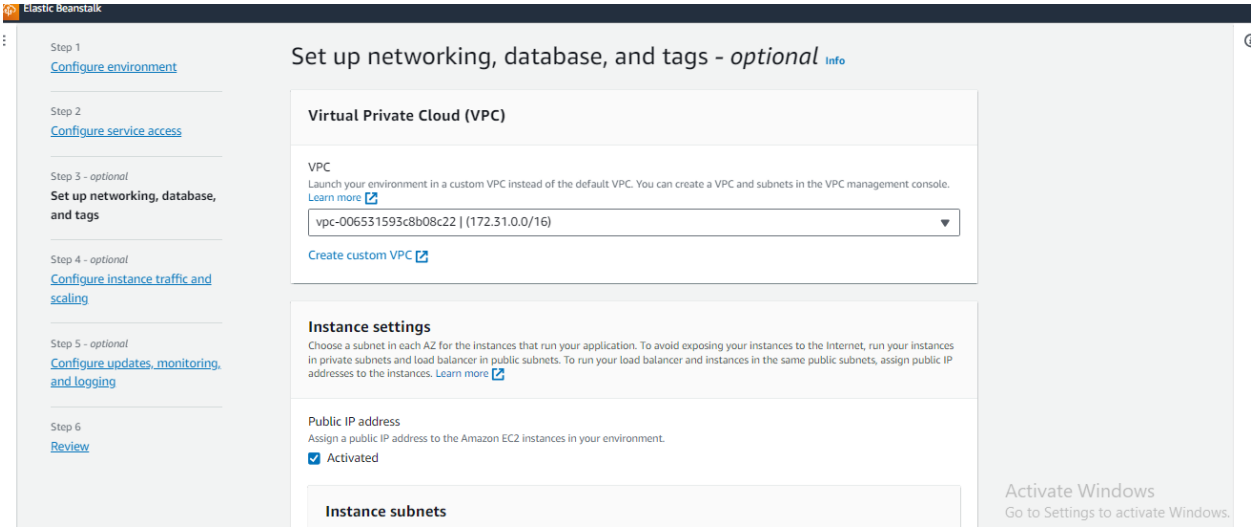

Elastic Beanstalk
Step 3
Name, review, and create
Filter by Type
AWSELASTICBe
All types
14 matches
1
Policy name
Type
Description
AdministratorAccess-AWSElasticBeanstalk
AWS managed
Grants acco
AWSElasticBeanstalkCustomPlatformforEC2Role
AWS managed
Provide the
AWSElasticBeanstalkEnhancedHealth
AWS managed
AWS Elastic
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
AWS managed
This policy
AWSElasticBeanstalkMulticontainerDocker
AWS managed
Provide the
AWSElasticBeanstalkReadOnly
AWS managed
Grants read
AWSElasticBeanstalkRoleCore
AWS managed
AWSElastic
AWSElasticBeanstalkRoleCWL
AWS managed
(Elastic Bea
AWSElasticBeanstalkRoleECS
AWS managed
(Elastic Bea
AWSElasticBeanstalkRoleRDS
AWS managed
(Elastic Bea
Activate Windows
Go to Settings to activate Windows.

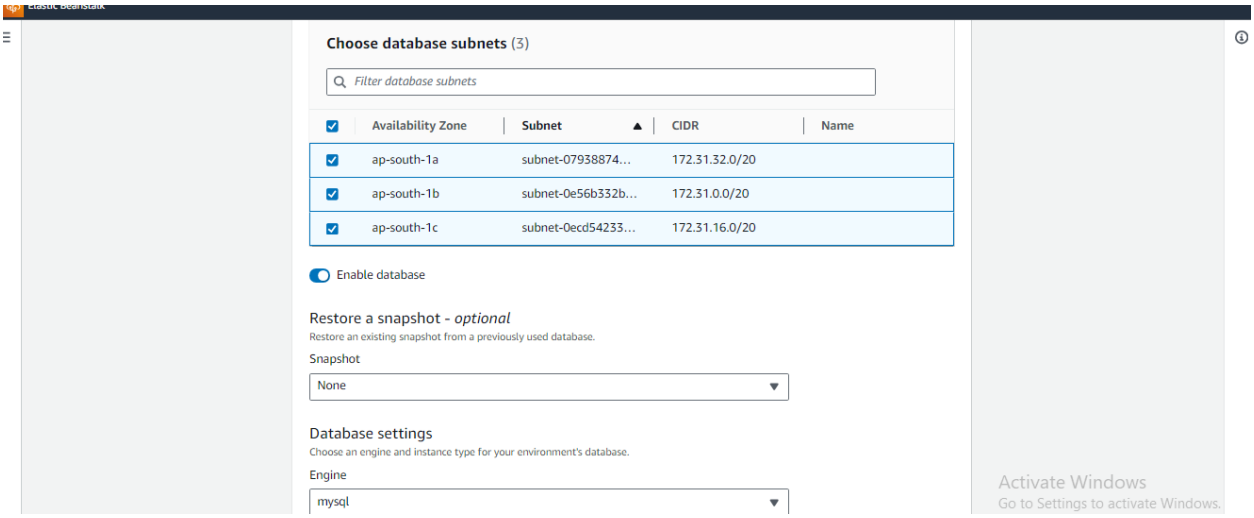

IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
elastickbeanstalk _septec2role
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
Activate Windows
Go to Settings to activate Windows.

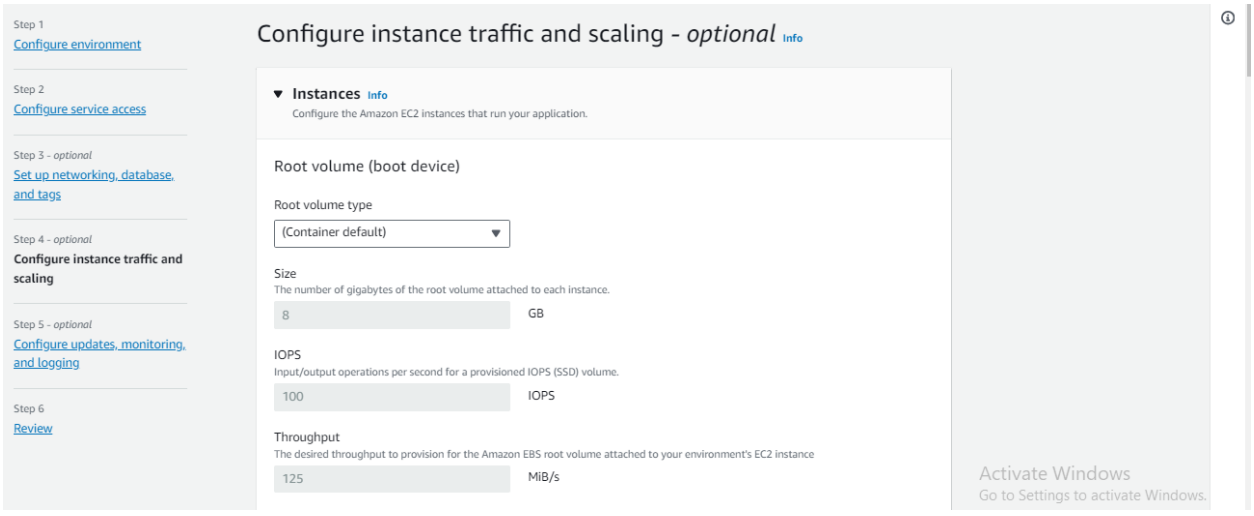

Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"ec2.amazonaws.com"
]
}
}
]
}
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
Activate Windows
Go to Settings to activate Windows.

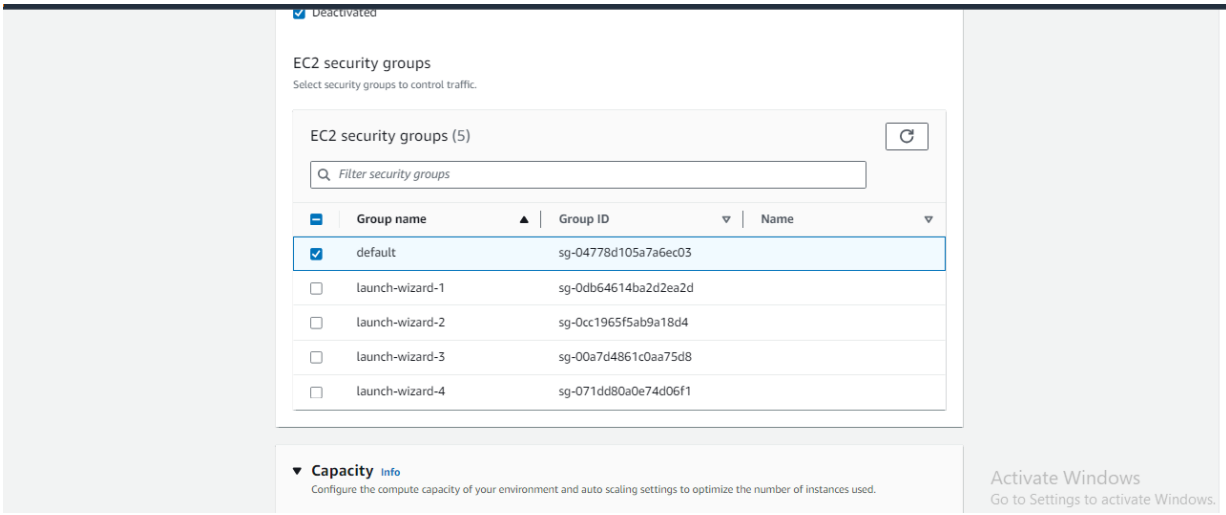

Elastic Beanstalk
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
IAM > Roles > elastickbeanstalk_septec2role
elastickbeanstalk_septec2role Info
Allows EC2 instances to call AWS services on your behalf.
Delete
Summary
Edit
Creation date
September 30, 2023, 23:04 (UTC+05:30)
ARN
arn:aws:iam::074470150406:role/elastickbeanstalk_septec2role
Instance profile ARN
arn:aws:iam::074470150406:instance-profile/elastickbeanstalk_septec2role
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions
Permissions policies (3) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
Activate Windows
Go to Settings to activate Windows.

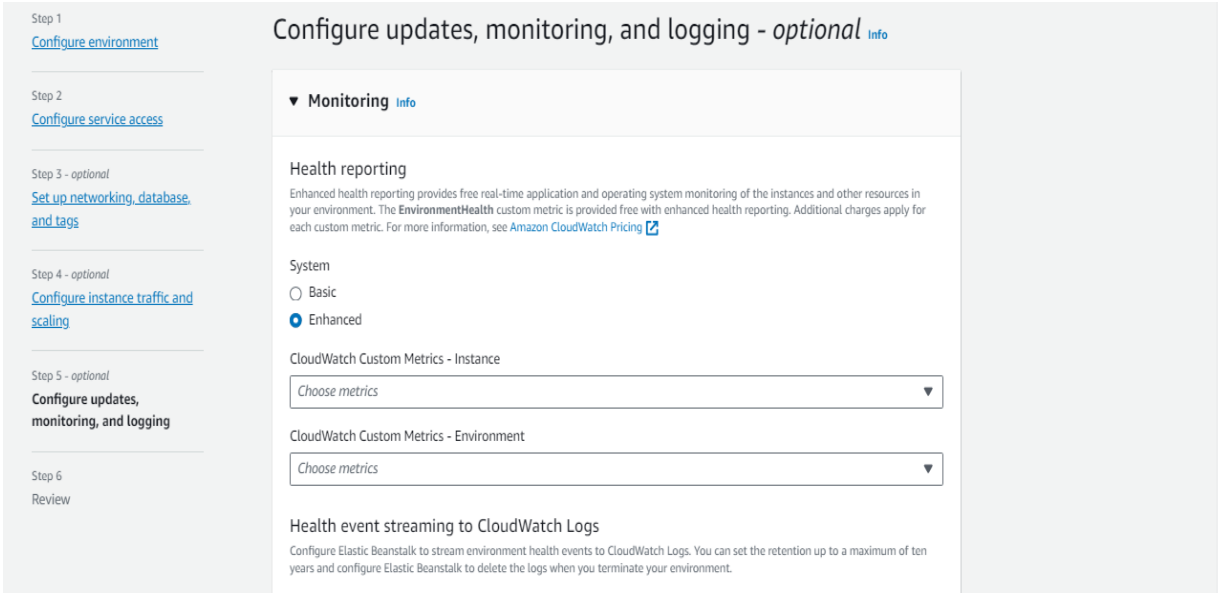

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Filter by Type
Search
All types
1
Policy name
Type
Attached entities
AWSElasticBeanstalkMulticontainerD...
AWS managed
2
AWSElasticBeanstalkWebTier
AWS managed
2
AWSElasticBeanstalkWebTier
Provide the instances in your web server environment access to upload log files to Amazon S3.
Copy JSON
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "BucketAccess",
"Action": [
"s3:Get*",
"s3:List*",
"s3:PutObject"
],
"Effect": "Allow",
"Resource": [
"arn:aws:s3:::elasticbeanstalk-*",
"arn:aws:s3:::elasticbeanstalk-*/*"
]
},
{
"Sid": "XRayAccess",
Activate Windows
Go to Settings to activate Windows.

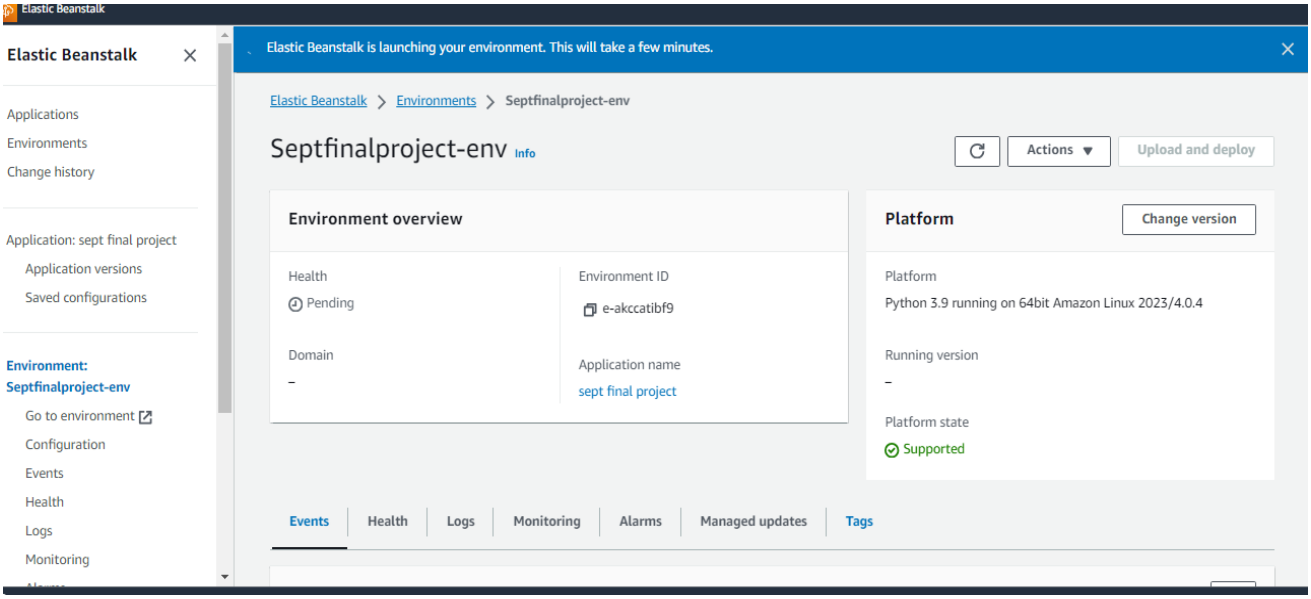

Elastic Beanstalk
Step 1
Configure environment
Step 2
Configure service access
Step 3 - optional
Set up networking, database, and tags
Step 4 - optional
Configure instance traffic and scaling
Step 5 - optional
Configure updates, monitoring, and logging
Step 6
Review
Set up networking, database, and tags - optional Info
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-006531593c8b08c22 | (172.31.0.0/16)
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
Activate Windows
Go to Settings to activate Windows.

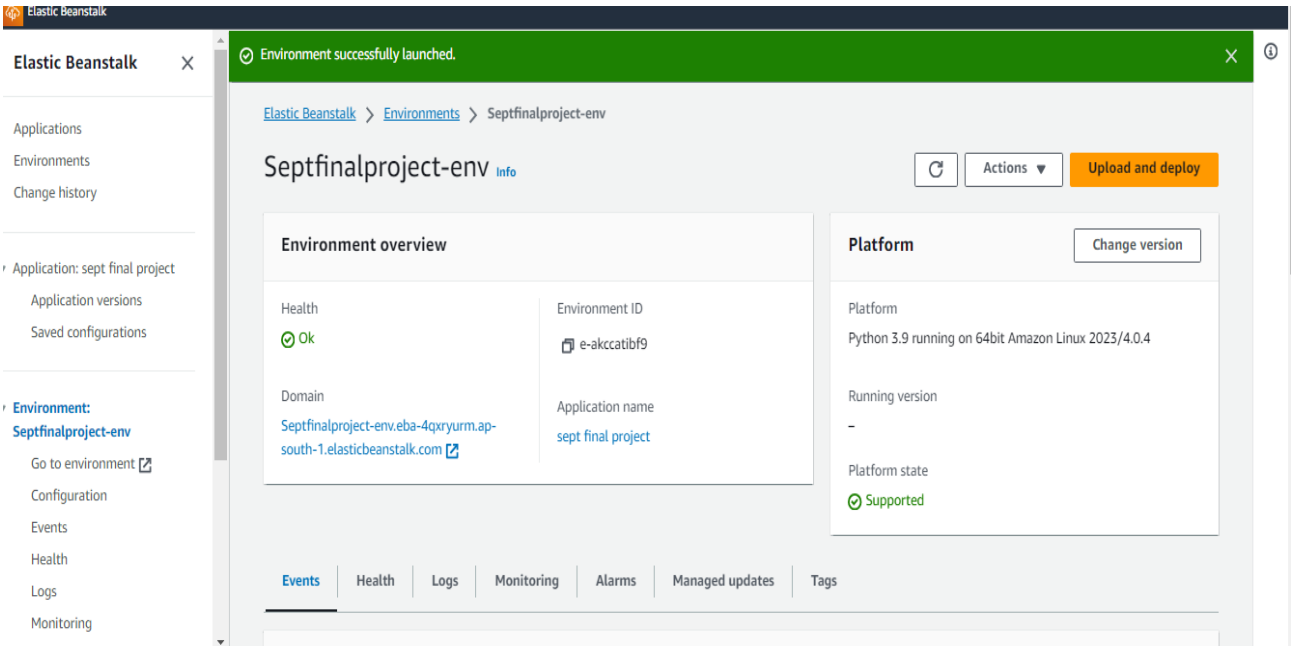

Choose database subnets (3)
Filter database subnets
Availability Zone
Subnet
CIDR
Name
ap-south-1a
subnet-07938874...
172.31.32.0/20
ap-south-1b
subnet-0e56b332b...
172.31.0.0/20
ap-south-1c
subnet-0ecd54233...
172.31.16.0/20
Enable database
Restore a snapshot - optional
Restore an existing snapshot from a previously used database.
Snapshot
None
Database settings
Choose an engine and instance type for your environment's database.
Engine
mysql
Activate Windows
Go to Settings to activate Windows.

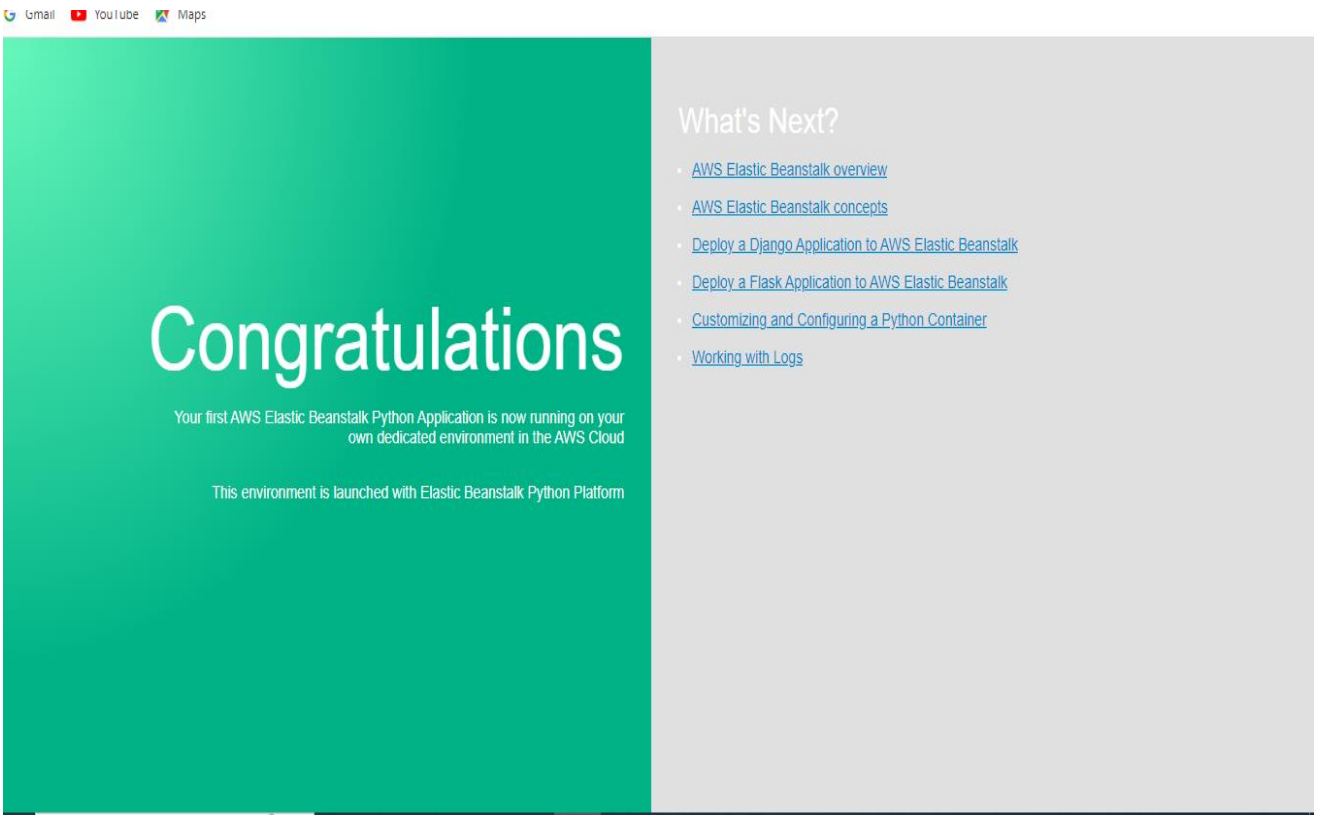

Step 1
Configure environment
Step 2
Configure service access
Step 3 - optional
Set up networking, database, and tags
Step 4 - optional
Configure instance traffic and scaling
Step 5 - optional
Configure updates, monitoring, and logging
Step 6
Review
Configure instance traffic and scaling - optional Info
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.
8
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
Activate Windows
Go to Settings to activate Windows.


Deactivated
EC2 security groups
Select security groups to control traffic.
EC2 security groups (5)
Filter security groups
Group name
Group ID
Name
default
sg-04778d105a7a6ec03
launch-wizard-1
sg-0db64614ba2d2ea2d
launch-wizard-2
sg-0cc1965f5ab9a18d4
launch-wizard-3
sg-00a7d4861c0aa75d8
launch-wizard-4
sg-071dd80a0e74d06f1
Capacity Info
Configure the compute capacity of your environment and auto scaling settings to optimize the number of instances used.
Activate Windows
Go to Settings to activate Windows.


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.


Elastic Beanstalk
Elastic Beanstalk is launching your environment. This will take a few minutes.
Elastic Beanstalk > Environments > Septfinalproject-env
Septfinalproject-env Info
Actions
Upload and deploy
Environment overview
Health
Pending
Environment ID
e-akccatibf9
Domain
-
Application name
sept final project
Platform
Change version
Platform
Python 3.9 running on 64bit Amazon Linux 2023/4.0.4
Running version
-
Platform state
Supported
Events
Health
Logs
Monitoring
Alarms
Managed updates
Tags
Applications
Environments
Change history
Application: sept final project
Application versions
Saved configurations
Environment: Septfinalproject-env
Go to environment
Configuration
Events
Health
Logs
Monitoring


Elastic Beanstalk
Environment successfully launched.
Elastic Beanstalk > Environments > Septfinalproject-env
Septfinalproject-env Info
Actions
Upload and deploy
Environment overview
Health
Ok
Environment ID
e-akccatibf9
Domain
Septfinalproject-env.eba-4qxryurm.ap-south-1.elasticbeanstalk.com
Application name
sept final project
Platform
Change version
Platform
Python 3.9 running on 64bit Amazon Linux 2023/4.0.4
Running version
-
Platform state
Supported
Events
Health
Logs
Monitoring
Alarms
Managed updates
Tags
Applications
Environments
Change history
Application: sept final project
Application versions
Saved configurations
Environment: Septfinalproject-env
Go to environment
Configuration
Events
Health
Logs
Monitoring


Gmail
YouTube
Maps
Congratulations
Your first AWS Elastic Beanstalk Python Application is now running on your own dedicated environment in the AWS Cloud
This environment is launched with Elastic Beanstalk Python Platform
What's Next?
AWS Elastic Beanstalk overview
AWS Elastic Beanstalk concepts
Deploy a Django Application to AWS Elastic Beanstalk
Deploy a Flask Application to AWS Elastic Beanstalk
Customizing and Configuring a Python Container
Working with Logs