LAB: Create an S3 Bucket from a Fargate Cluster Task via IAM policies

You need:

- An AWS Account
- Configured AWS Cli locally

Duration of the Lab: 30 Minutes.

Difficulty: medium

Try to list S3 Buckets from your local machine.

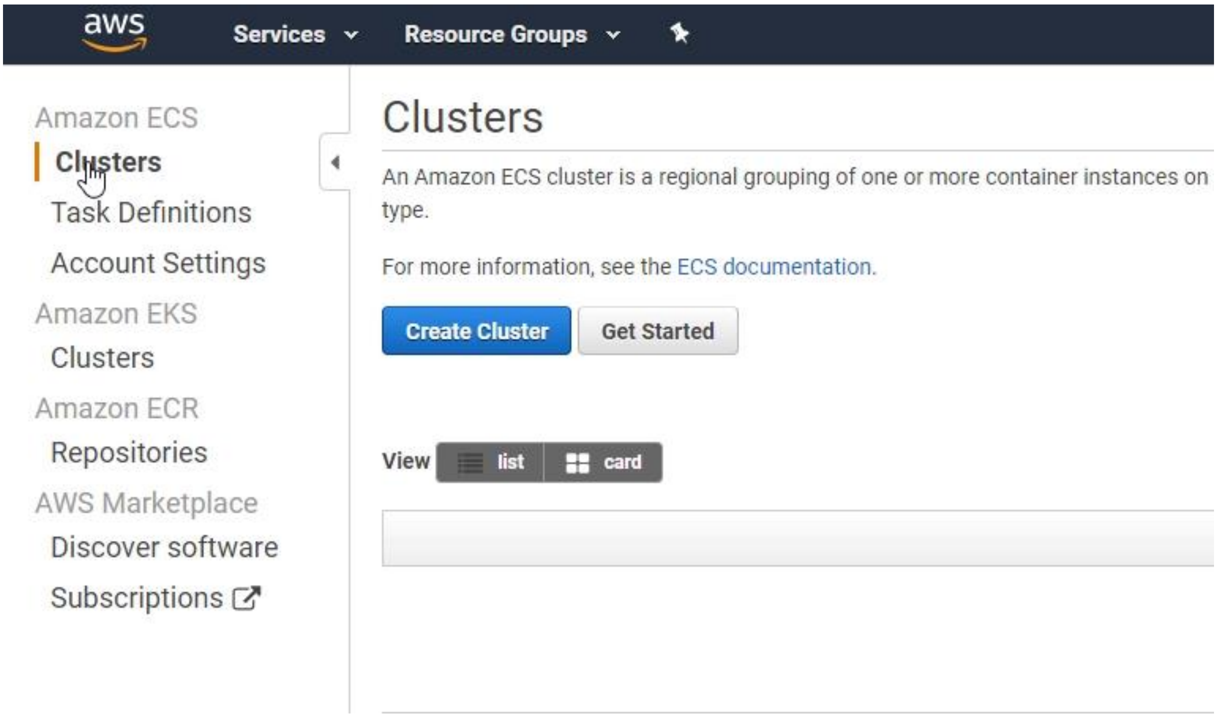
Open a new Terminal/PowerShell and see if you can run the image banst/awscli locally and mount your local aws credentials into the container:

```
docker run --rm -it -v ~/.aws:/root/.aws banst/awscli s3 ls
```

It should, ideally, output nothing (no error message), or S3 buckets, if you still have some. So we know the awscli works, let's use this in a container in the aws ecosystem!

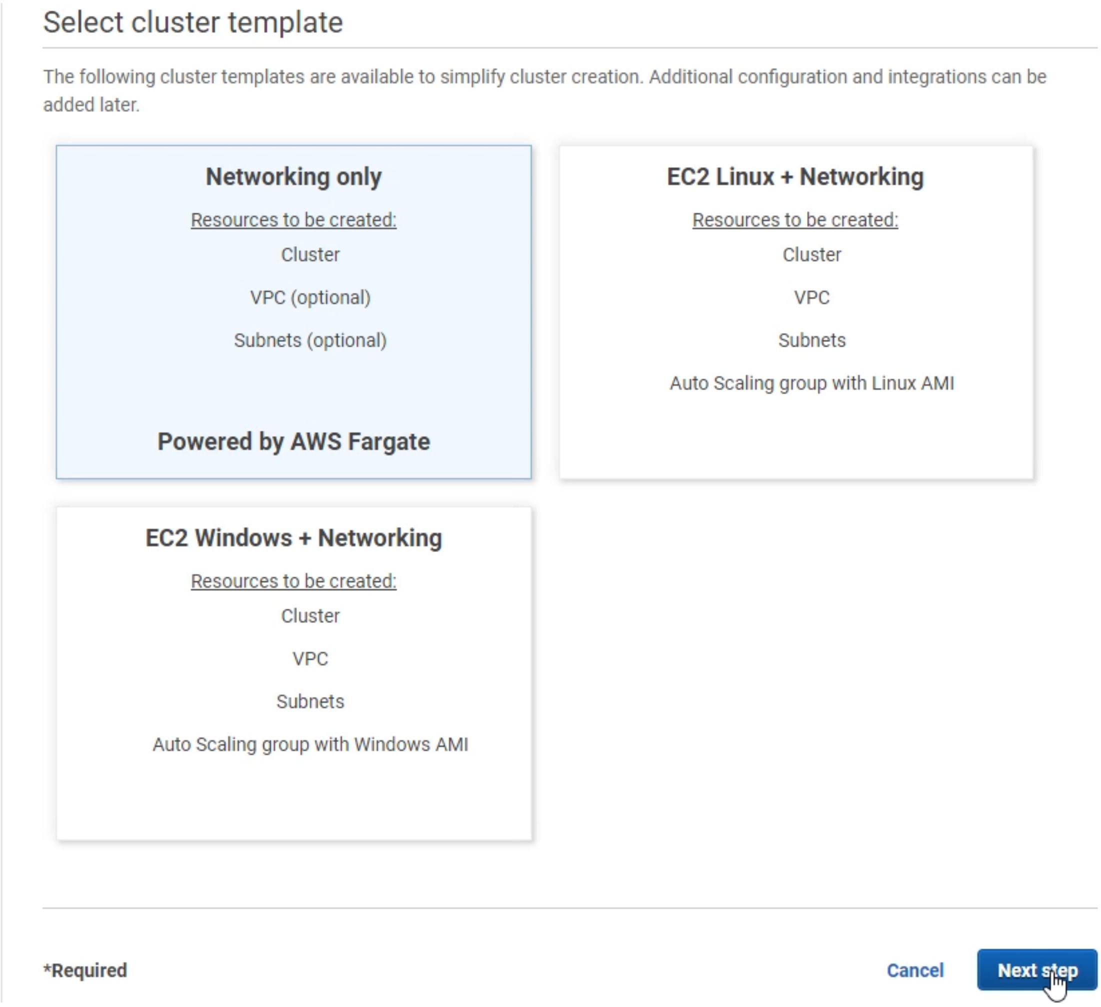
Create a new Fargate Cluster

If you deleted your cluster in the previous lab then create a new one:



An Amazon ECS cluster is a regional grouping of one or more container instances on type.

For more information, see the ECS documentation.



Select cluster template

The following cluster templates are available to simplify cluster creation. Additional configuration and integrations can be added later.

Networking only

Resources to be created:

Cluster

VPC (optional)

Subnets (optional)

Powered by AWS Fargate

EC2 Linux + Networking

Resources to be created:

Cluster

VPC

Subnets

Auto Scaling group with Linux AMI

EC2 Windows + Networking

Resources to be created:

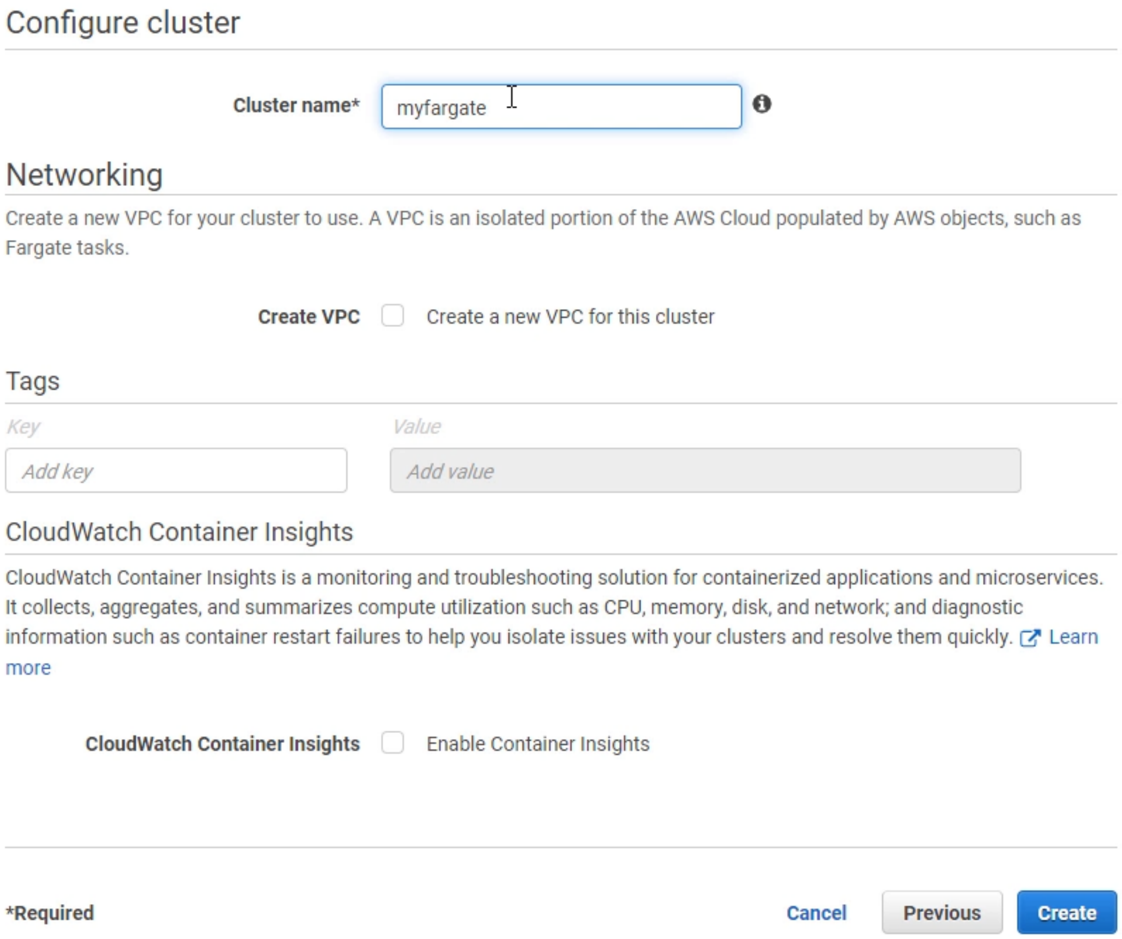
Cluster

VPC

Subnets

Auto Scaling group with Windows AMI

***Required**



Configure cluster

Cluster name* myfargate

Networking

Create a new VPC for your cluster to use. A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Fargate tasks.

Create VPC □ Create a new VPC for this cluster

Tags

Key	Value
Add key	Add value

CloudWatch Container Insights

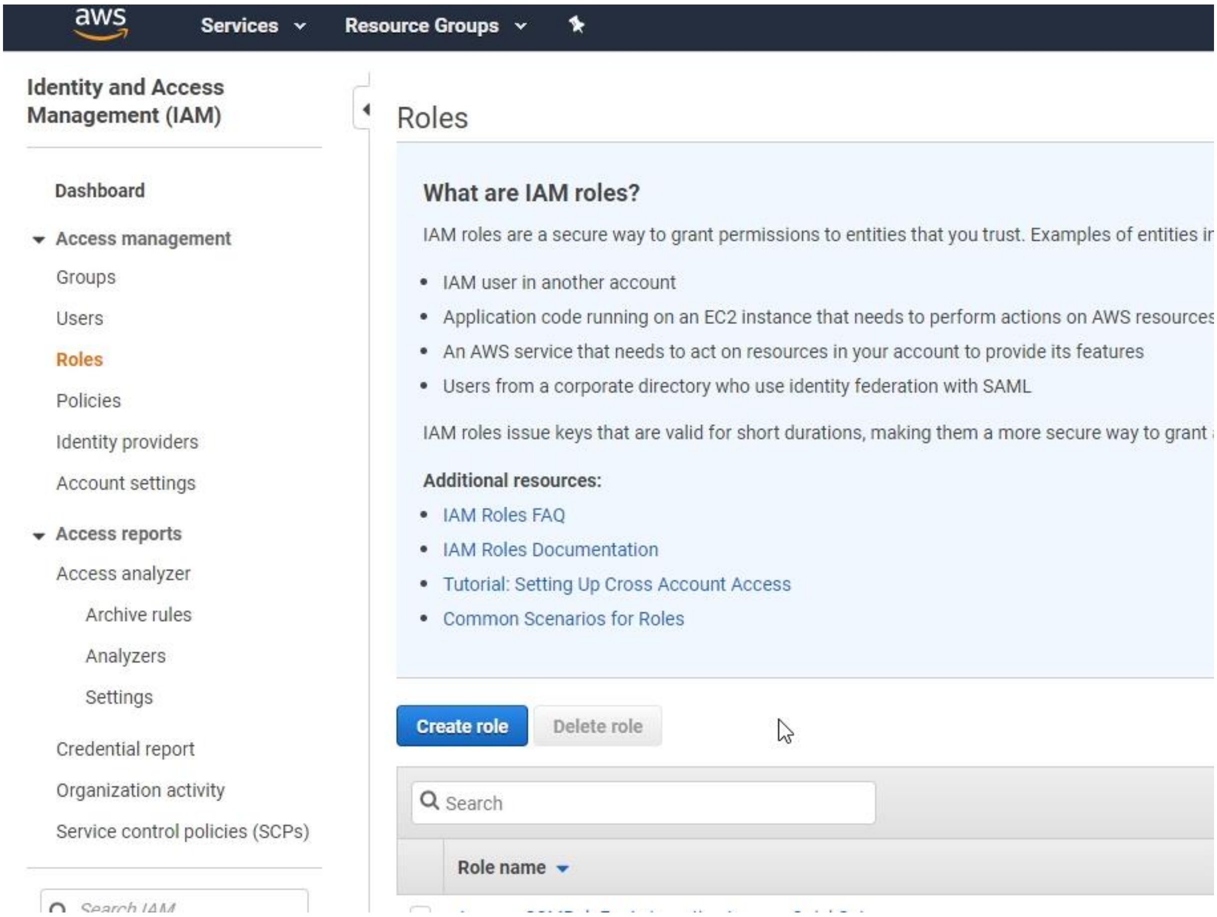
CloudWatch Container Insights is a monitoring and troubleshooting solution for containerized applications and microservices. It collects, aggregates, and summarizes compute utilization such as CPU, memory, disk, and network; and diagnostic information such as container restart failures to help you isolate issues with your clusters and resolve them quickly. Learn more

CloudWatch Container Insights □ Enable Container Insights

*Required

Create a new IAM Role for your Task

Open the IAM Dashboard -> Roles -> Create role



Identity and Access Management (IAM)

- Dashboard
- Access management
  - Groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
    - Archive rules
    - Analyzers
    - Settings
  - Credential report
  - Organization activity
  - Service control policies (SCPs)

Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities ir

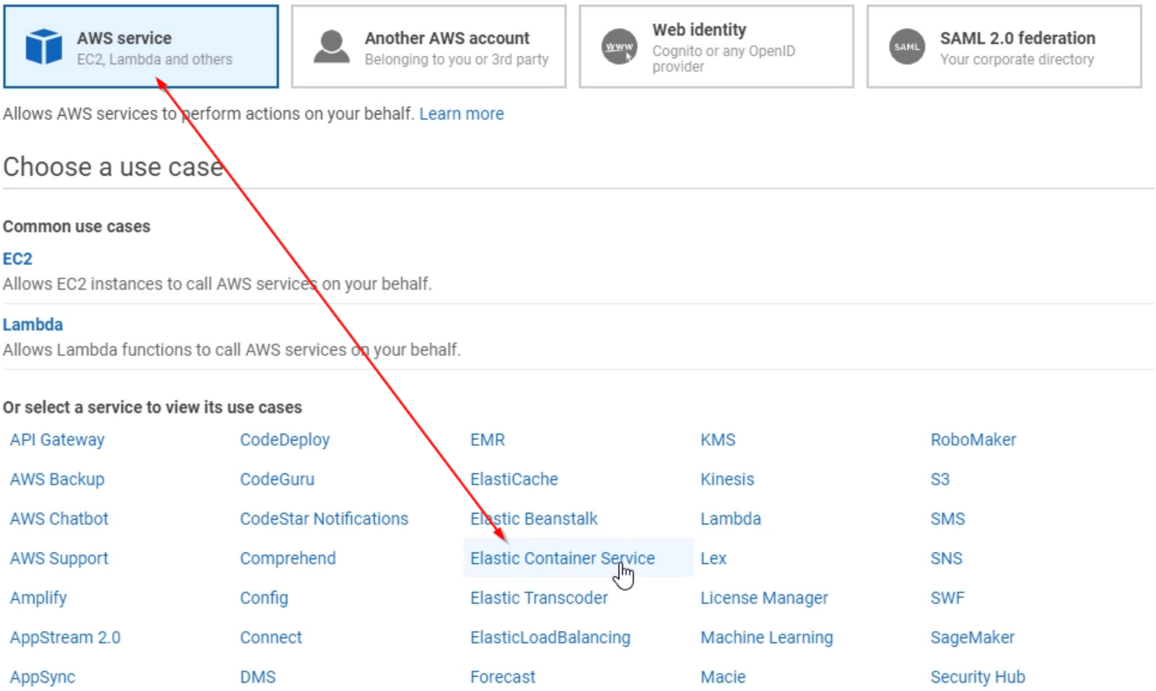
- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

This time select “Elastic Container Service” as AWS Service:



Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

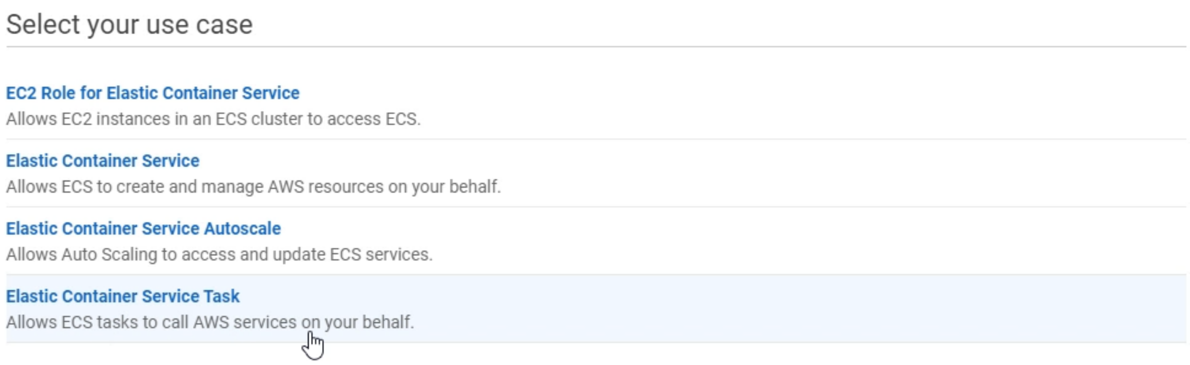
EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway
AWS Backup
AWS Chatbot
AWS Support
Amplify
AppStream 2.0
AppSync
CodeDeploy
CodeGuru
CodeStar Notifications
Comprehend
Config
Connect
DMS
EMR
ElastiCache
Elastic Beanstalk
Elastic Container Service
Elastic Transcoder
ElasticLoadBalancing
Forecast
KMS
Kinesis
Lambda
Lex
License Manager
Machine Learning
Macie
RoboMaker
S3
SMS
SNS
SWF
SageMaker
Security Hub

Select the Elastic Container Service Task, because our Task will talk to other AWS Services:



Select your use case

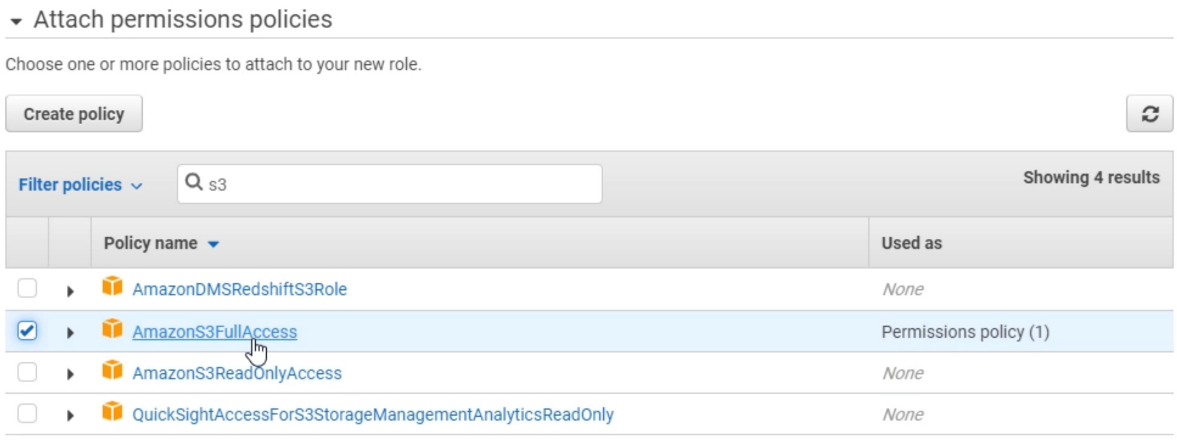
EC2 Role for Elastic Container Service
Allows EC2 instances in an ECS cluster to access ECS.

Elastic Container Service
Allows ECS to create and manage AWS resources on your behalf.

Elastic Container Service Autoscale
Allows Auto Scaling to access and update ECS services.

Elastic Container Service Task
Allows ECS tasks to call AWS services on your behalf.

Give S3 Full Access Permissions:



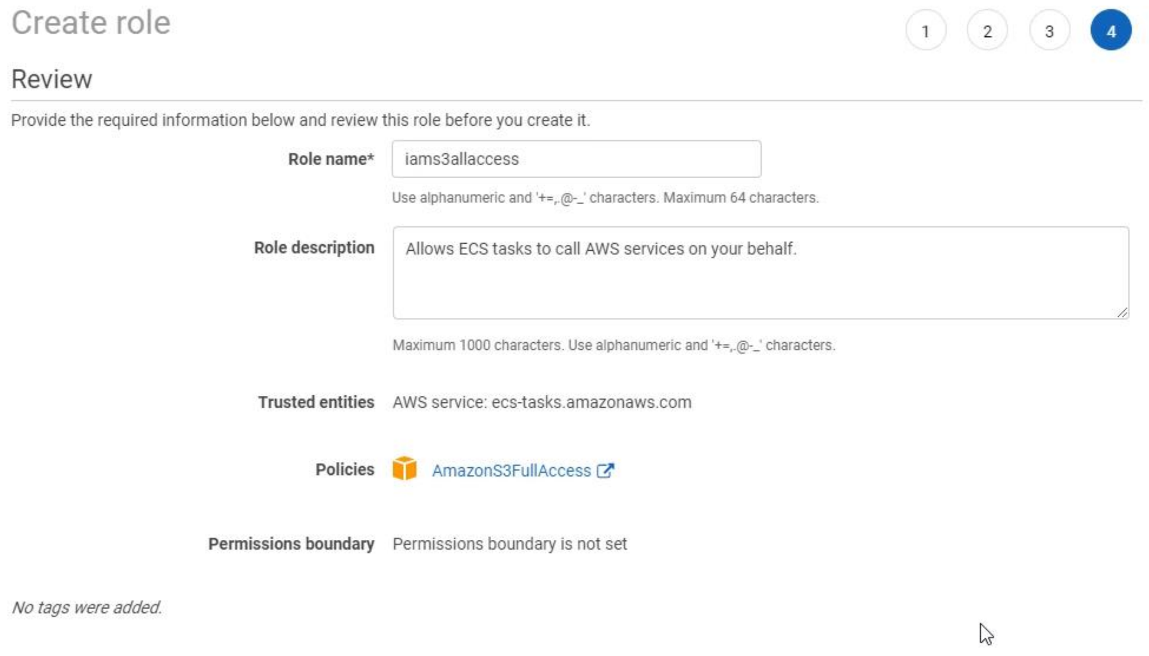
Attach permissions policies

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

s3

	Policy name	Used as
□	AmazonDMSRedshiftS3Role	*None*
☑	AmazonS3FullAccess	Permissions policy (1)
□	AmazonS3ReadOnlyAccess	*None*
□	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	*None*

Give the Role a name, for example “iams3allaccess”:



Create role

Review

Provide the required information below and review this role before you create it.

Role name* iams3allaccess

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

Role description Allows ECS tasks to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ecs-tasks.amazonaws.com

Policies AmazonS3FullAccess

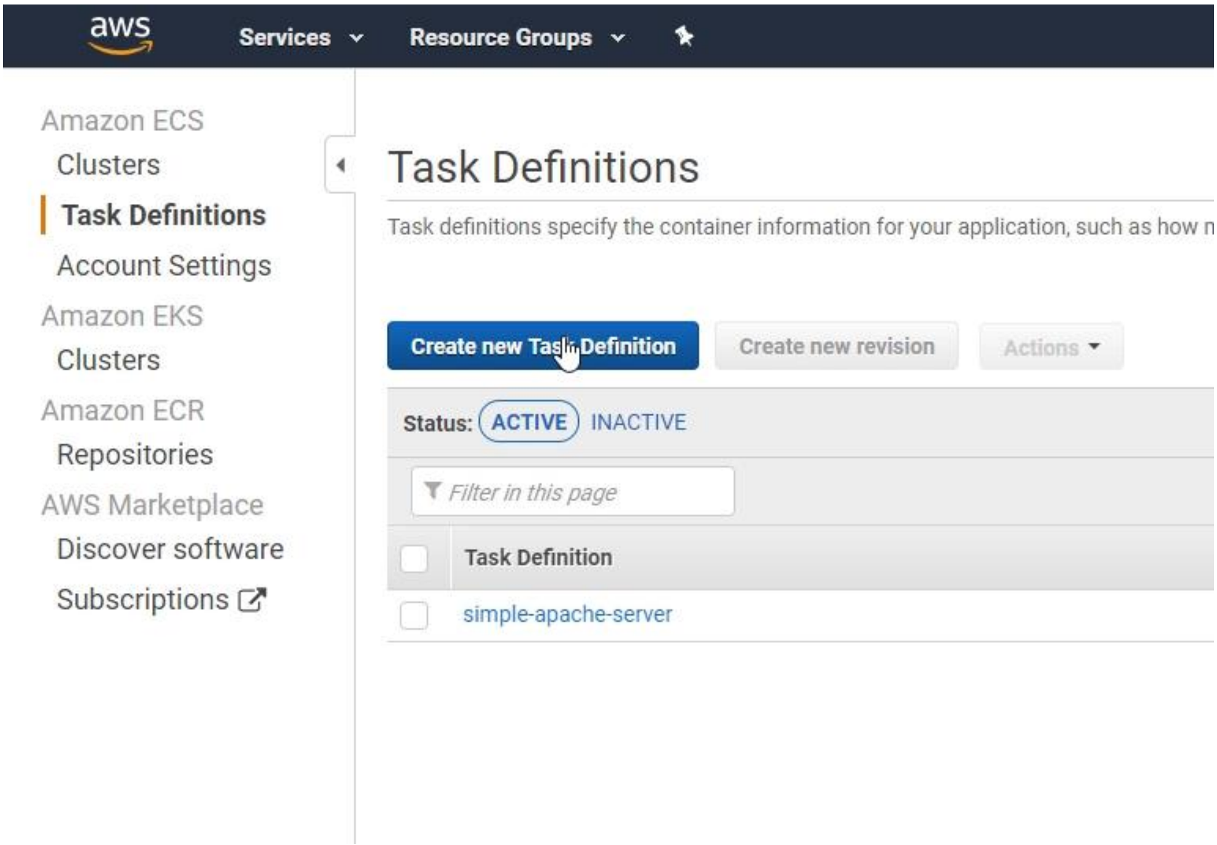
Permissions boundary Permissions boundary is not set

No tags were added.

Then Create the Role

Create a Task Definition

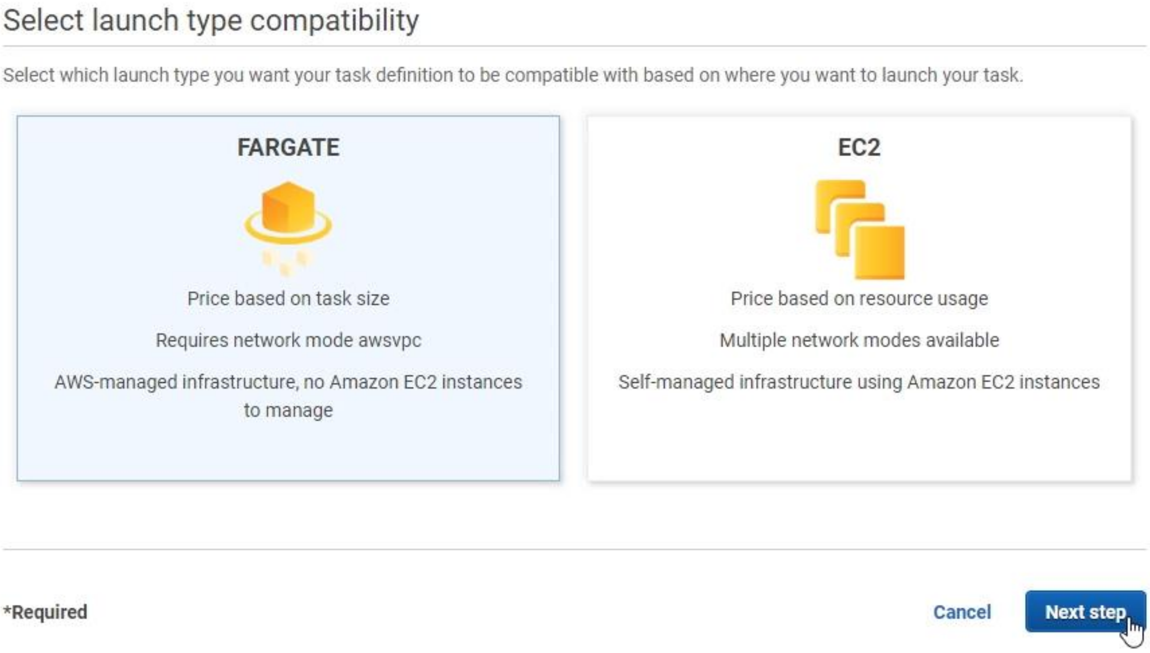
Now we need a Task definition for our task



Task Definitions

Task definitions specify the container information for your application, such as how n

□	Task Definition
□	simple-apache-server



Select launch type compatibility

Select which launch type you want your task definition to be compatible with based on where you want to launch your task.

FARGATE

Price based on task size

Requires network mode awsvpc

AWS-managed infrastructure, no Amazon EC2 instances to manage

EC2

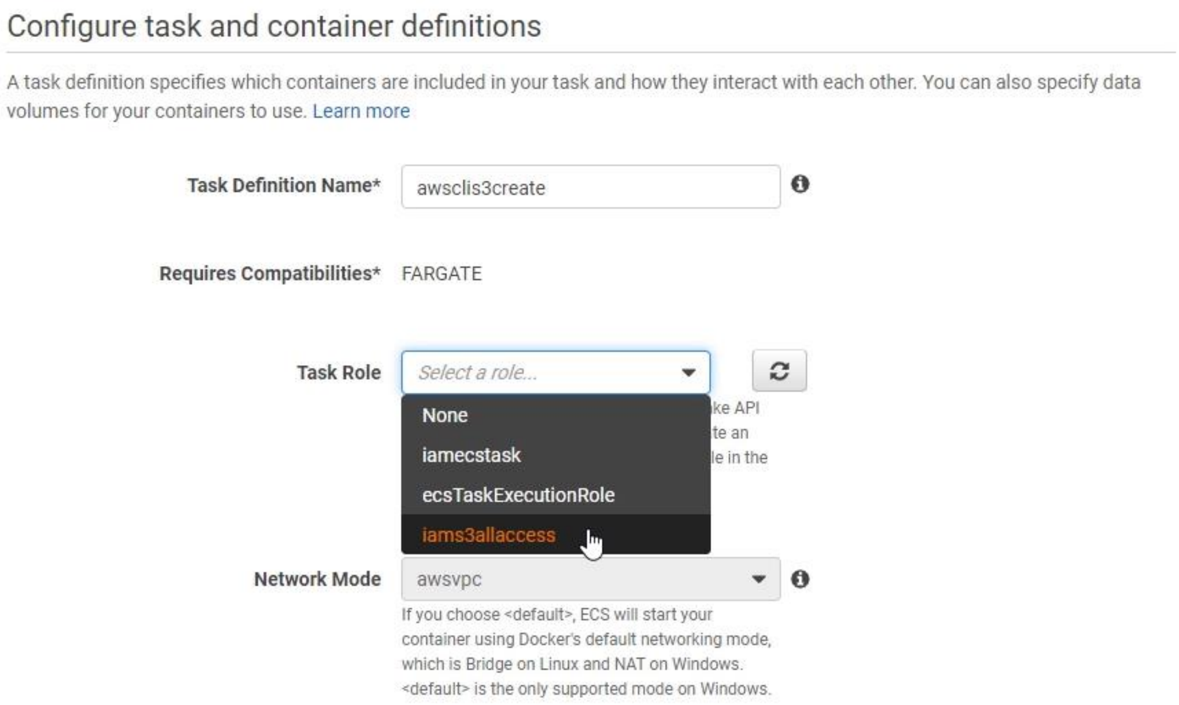
Price based on resource usage

Multiple network modes available

Self-managed infrastructure using Amazon EC2 instances

*Required

Select the Role you created in the previous IAM Step:



Configure task and container definitions

A task definition specifies which containers are included in your task and how they interact with each other. You can also specify data volumes for your containers to use. Learn more

Task Definition Name* awsclis3create

Requires Compatibilities* FARGATE

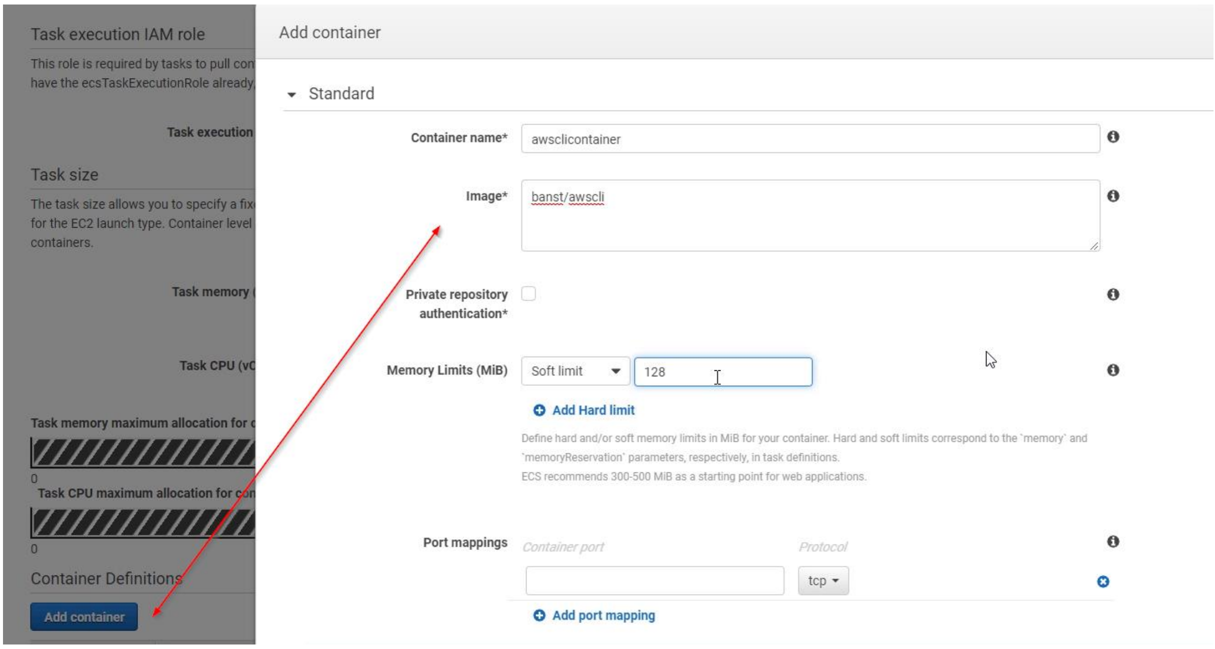
Task Role Select a role...

Network Mode awsvpc

If you choose <default>, ECS will start your container using Docker's default networking mode, which is Bridge on Linux and NAT on Windows. <default> is the only supported mode on Windows.

0.5GB of RAM and 0.25 vCPU is enough.

Add containers:



Add container

Standard

Container name* awsclicontainer

Image* banst/awscli

Private repository authentication* □

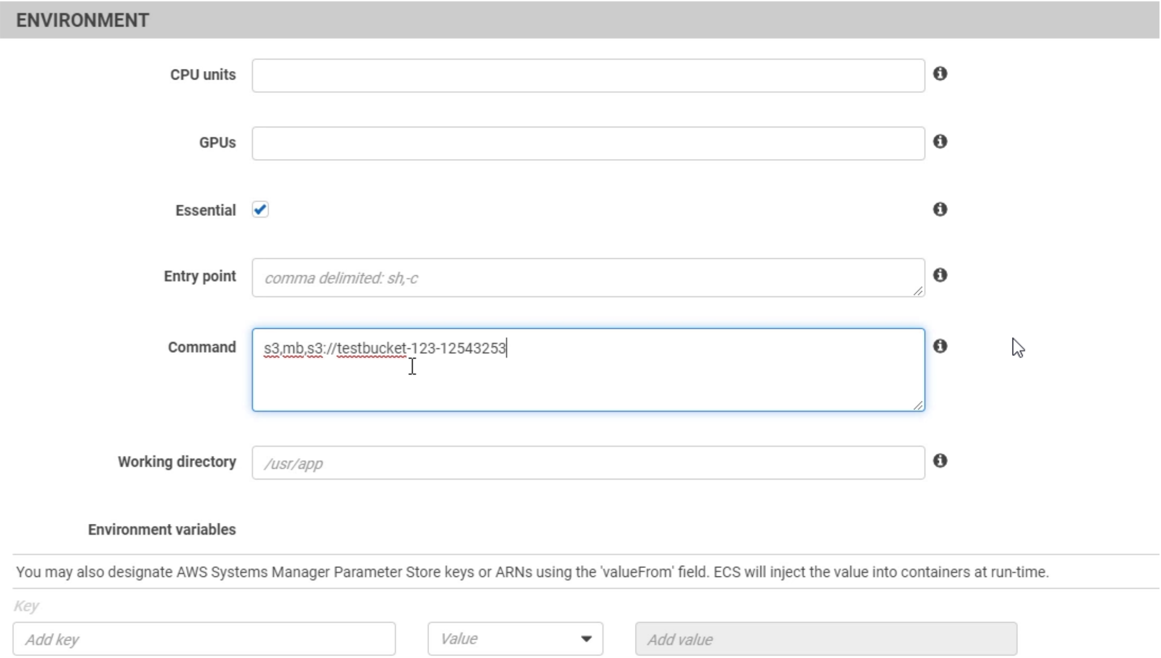
Memory Limits (MiB) Soft limit 128

Define hard and/or soft memory limits in MiB for your container. Hard and soft limits correspond to the 'memory' and 'memoryReservation' parameters, respectively, in task definitions.
ECS recommends 300-500 MiB as a starting point for web applications.

Port mappings Container port Protocol tcp

Image: banst/awscli

And as a command enter “s3,mb,s3://sometestbucket-123-123-234555”, so that bucket name should be pretty unique – hopefully. Otherwise change the bucket name to your own pattern/namespace or choose something random



ENVIRONMENT

CPU units:

GPUs:

Essential: ☑

Entry point: comma delimited: sh,-c

Command: s3,mb,s3://testbucket-123-12543253

Working directory: /usr/app

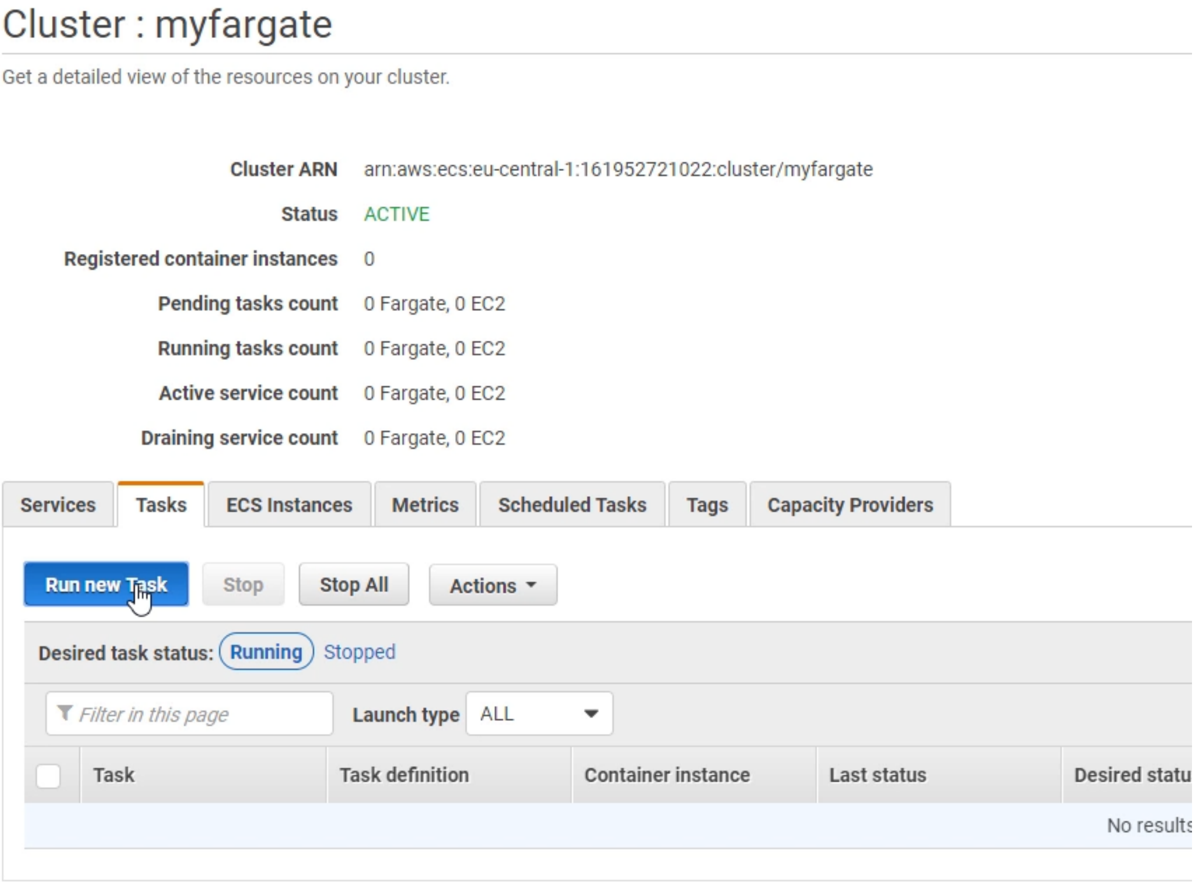
Environment variables

You may also designate AWS Systems Manager Parameter Store keys or ARNs using the 'valueFrom' field. ECS will inject the value into containers at run-time.

Then create the Task Definition.

Run the Task

Open your Cluster, but this time go to the Task Tab, not the Service tab. Hit “Run new Task”:



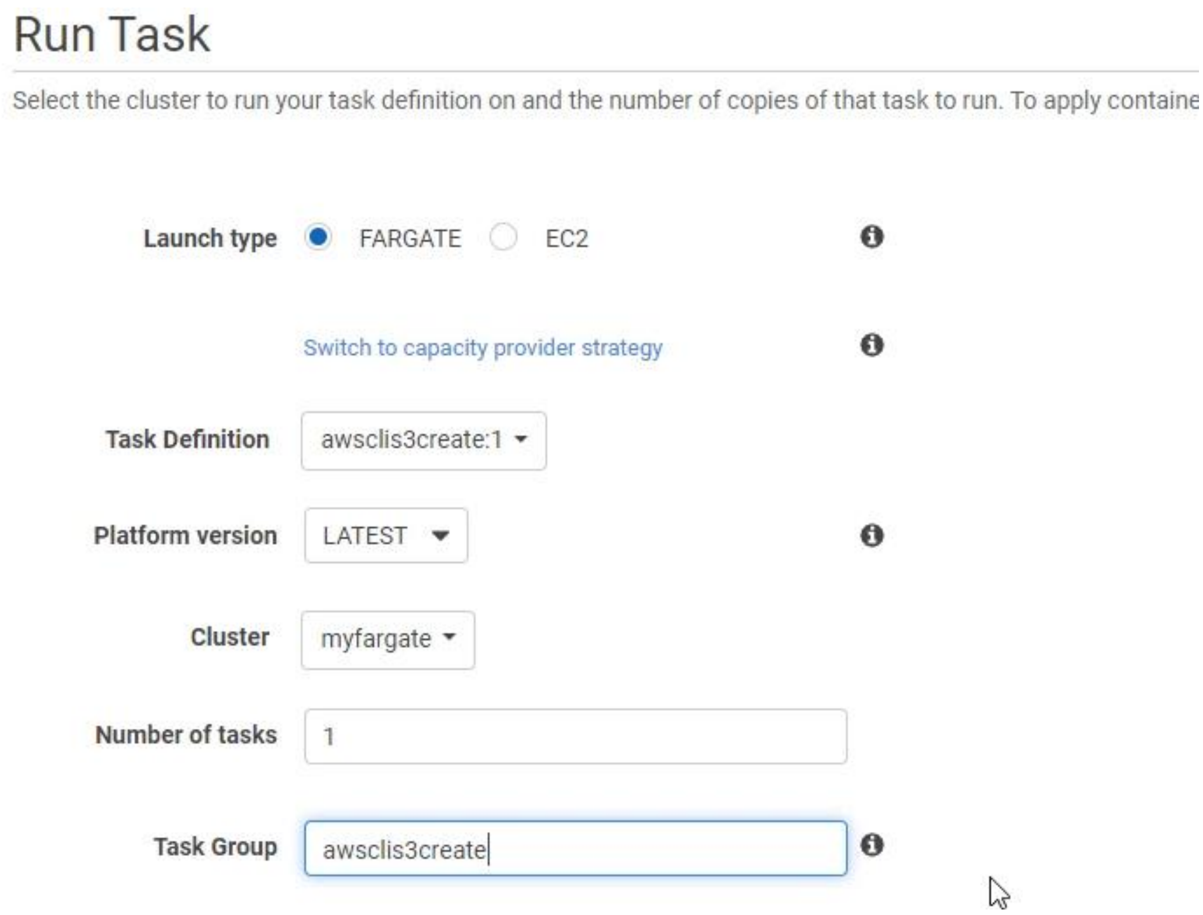
Cluster : myfargate

Get a detailed view of the resources on your cluster.

Cluster ARN	arn:aws:ecs:eu-central-1:161952721022:cluster/myfargate
Status	ACTIVE
Registered container instances	0
Pending tasks count	0 Fargate, 0 EC2
Running tasks count	0 Fargate, 0 EC2
Active service count	0 Fargate, 0 EC2
Draining service count	0 Fargate, 0 EC2

Task	Task definition	Container instance	Last status	Desired statu
				No results

Select your Task Definition, choose Fargate as Launch type, Choose your cluster and give the task group a name:



Run Task

Select the cluster to run your task definition on and the number of copies of that task to run. To apply containe

Launch type ● FARGATE ○ EC2

Task Definition awsclis3create:1

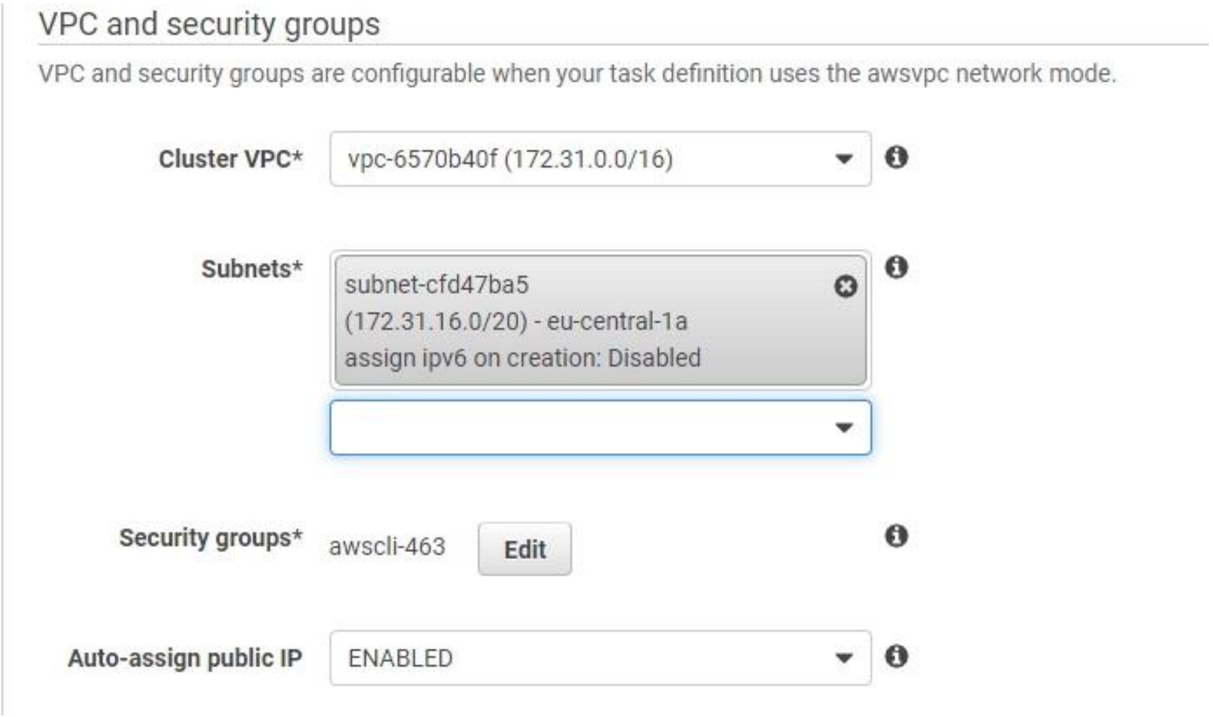
Platform version LATEST

Cluster myfargate

Number of tasks 1

Task Group awsclis3create

Choose your VPC and choose one Subnet where this task will be placed:



VPC and security groups

VPC and security groups are configurable when your task definition uses the awsvpc network mode.

Cluster VPC* vpc-6570b40f (172.31.0.0/16)

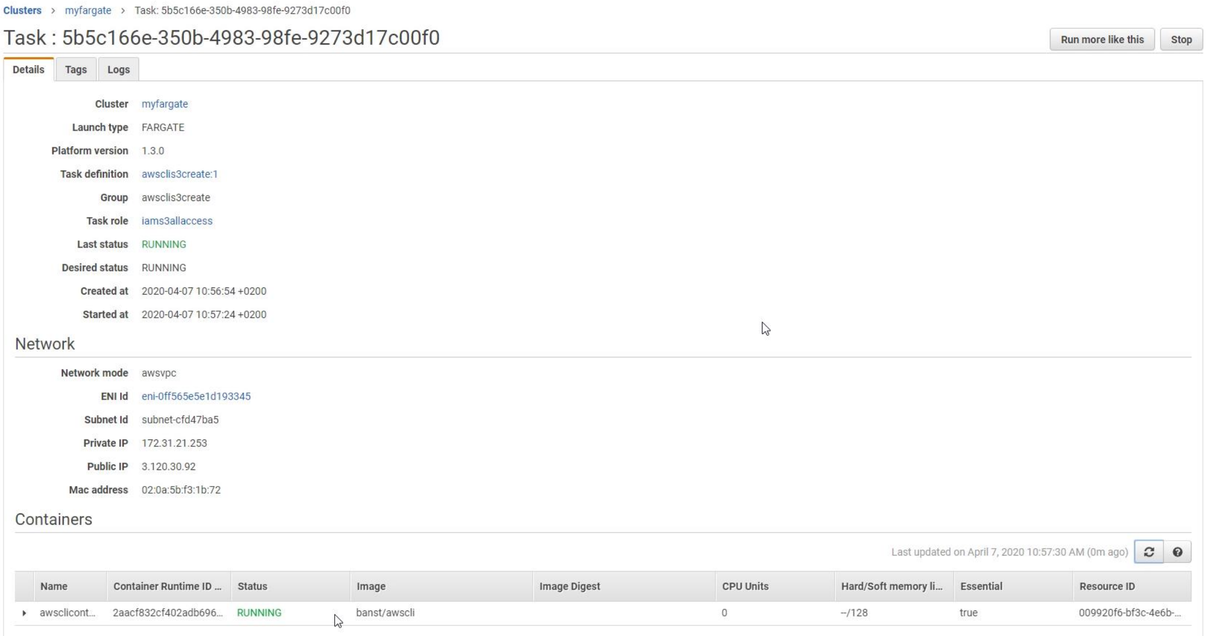
Subnets* subnet-cfd47ba5 (172.31.16.0/20) - eu-central-1a assign ipv6 on creation: Disabled

Security groups* awscli-463

Auto-assign public IP ENABLED

Then Run the Task.

Observe the Task going from Pending to Running to Stopped, because it’s not a long running task:


Clusters > myfargate > Task: 5b5c166e-350b-4983-98fe-9273d17c00f0
Run more like this
Stop
Details
Tags
Logs

Task : 5b5c166e-350b-4983-98fe-9273d17c00f0

Cluster	myfargate
Launch type	FARGATE
Platform version	1.3.0
Task definition	awsclis3create:1
Group	awsclis3create
Task role	iams3allaccess
Last status	RUNNING
Desired status	RUNNING
Created at	2020-04-07 10:56:54 +0200
Started at	2020-04-07 10:57:24 +0200

Network

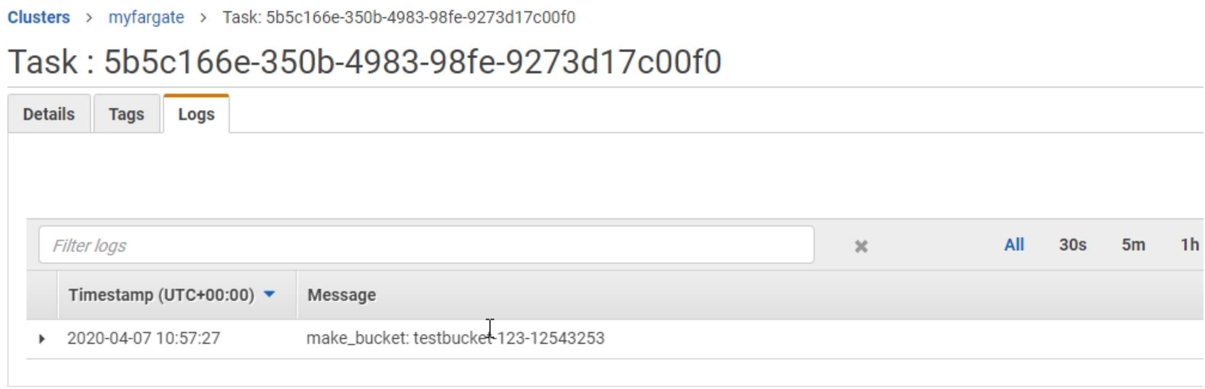
Network mode	awsvpc
ENI Id	eni-0ff565e5e1d193345
Subnet Id	subnet-cfd47ba5
Private IP	172.31.21.253
Public IP	3.120.30.92
Mac address	02:0a:5b:f3:1b:72

Containers

Last updated on April 7, 2020 10:57:30 AM (0m ago)

Name	Container Runtime ID ...	Status	Image	Image Digest	CPU Units	Hard/Soft memory li...	Essential	Resource ID
awsclicont...	2aacf832cf402adb696...	RUNNING	banst/awscli		0	--/128	true	009920f6-bf3c-4e6b-...

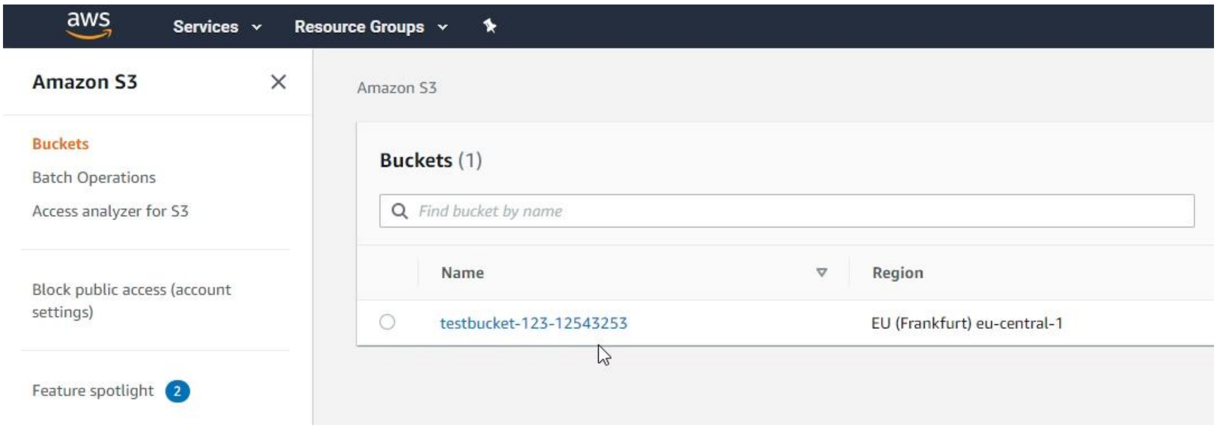
Head over to the “Logs” tab and observe it created the bucket:


Clusters > myfargate > Task: 5b5c166e-350b-4983-98fe-9273d17c00f0
Details
Tags
Logs
Filter logs
All
30s
5m
1h

Task : 5b5c166e-350b-4983-98fe-9273d17c00f0

Timestamp (UTC+00:00)	Message
2020-04-07 10:57:27	make_bucket: testbucket-123-12543253

If you check your S3 Dashboard, you’ll see your new Bucket:



Name	Region
○ testbucket-123-12543253	EU (Frankfurt) eu-central-1

Clean Up

- Delete the Bucket

Lab End