ATTACK DEFENSE

by PentesterAcademy

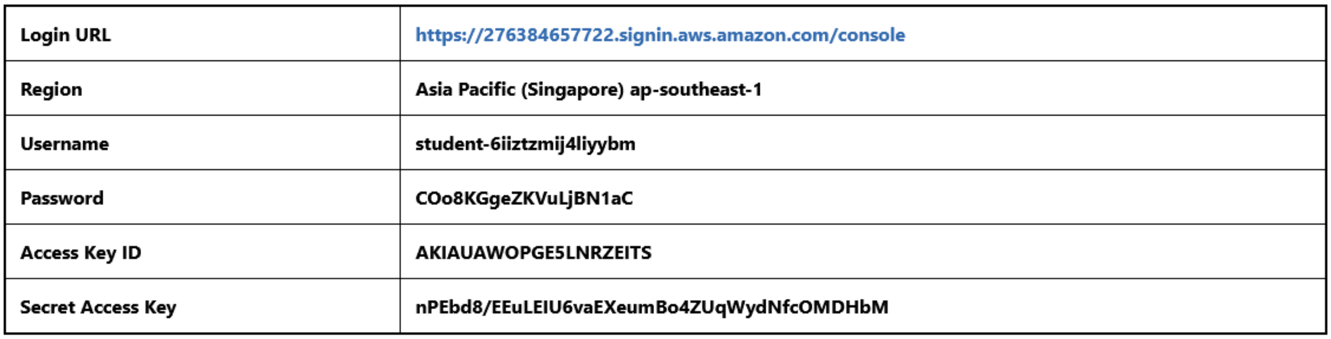
Name	ECR Enumeration
URL	https://attackdefense.com/challengedetails?cid=2428
Type	AWS Cloud Security : ECS and ECR

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

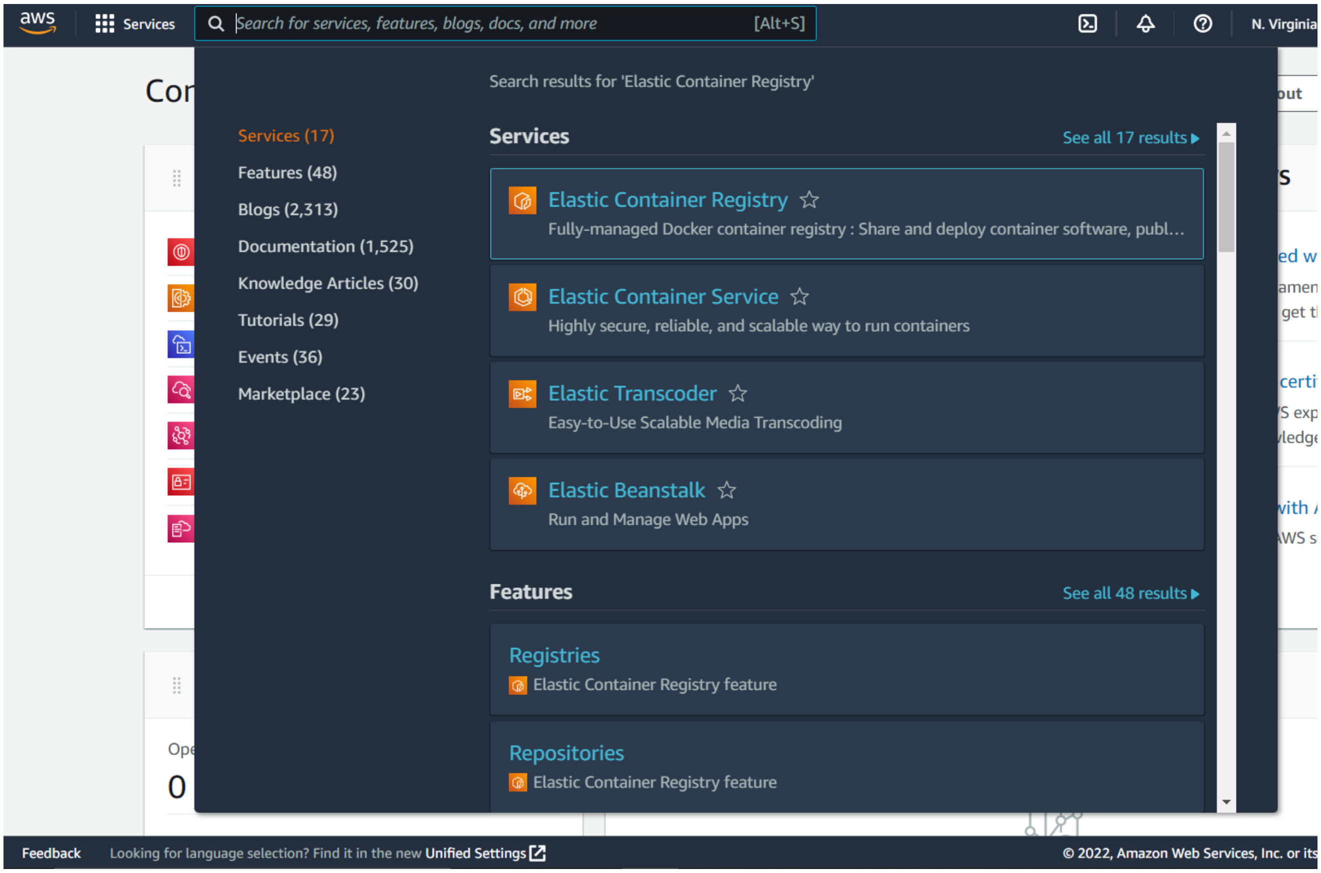
We will enumerate the ECR service provided by amazon. ECR stands for Elastic Container Registry it is an AWS managed container image registry service that is secure, scalable, and reliable.

Step 1: Click on the lab link button to get access to AWS lab credentials.



Login URL	https://276384657722.signin.aws.amazon.com/console
Region	Asia Pacific (Singapore) ap-southeast-1
Username	student-6iiztzmij4liyybm
Password	COo8KGgeZKVuLjBN1aC
Access Key ID	AKIAUAWOPGE5LNRZEITS
Secret Access Key	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

Step 2: Log in to the AWS account through the console search for Elastic Container Registry and click on it.



Search results for 'Elastic Container Registry'

Elastic Container Registry ☆
Fully-managed Docker container registry : Share and deploy container software, publ…

Elastic Container Service ☆
Highly secure, reliable, and scalable way to run containers

Elastic Transcoder ☆
Easy-to-Use Scalable Media Transcoding

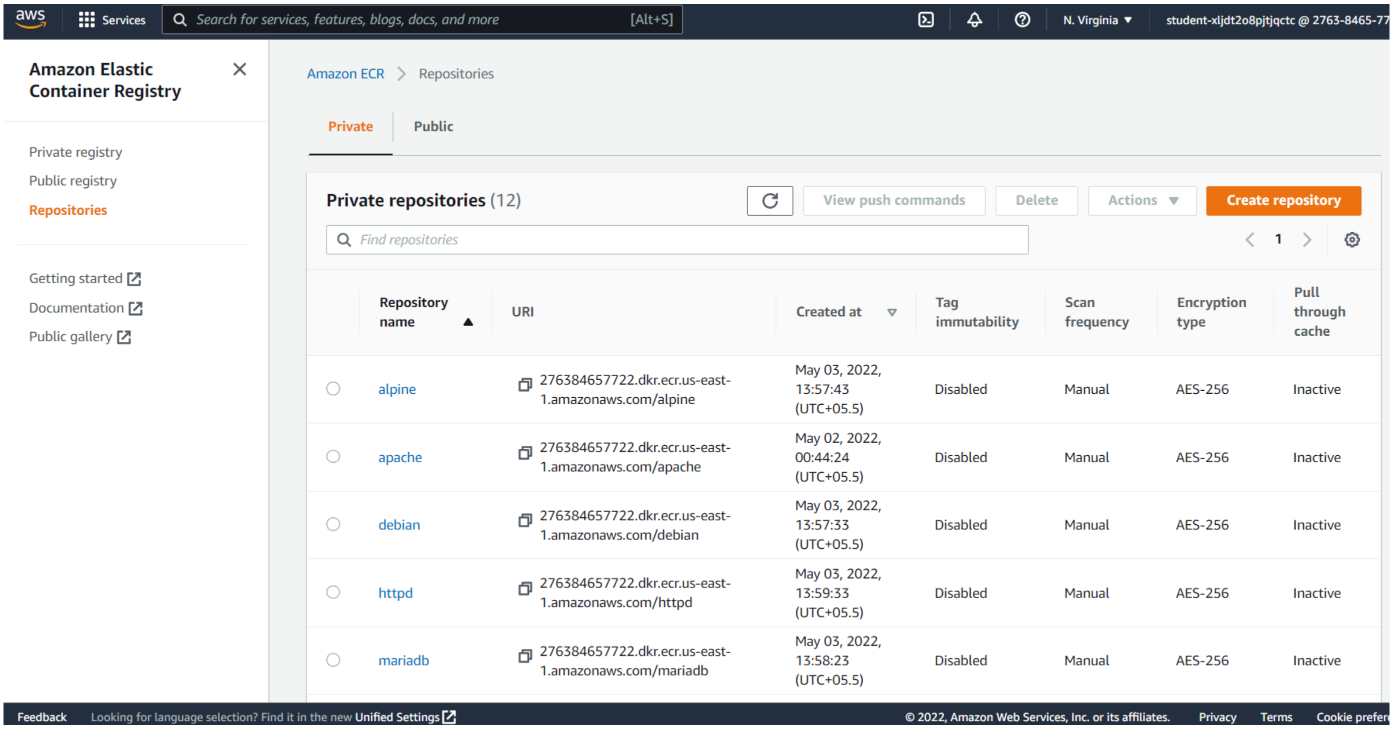
Elastic Beanstalk ☆
Run and Manage Web Apps

Registries
Elastic Container Registry feature

Repositories
Elastic Container Registry feature

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its

Step 3: The Private registry hosts our docker repositories and is a secure scalable service to use for deploying ECS clusters.


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia ▼
student-xljdt2o8pjtjqctc @ 2763-8465-77
Amazon Elastic Container Registry
Private registry
Public registry
Repositories
Getting started
Documentation
Public gallery
Amazon ECR > Repositories
Private
Public
View push commands
Delete
Actions ▼
Create repository
Find repositories
1
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie prefer

Private repositories (12)

	Repository name ▲	URI	Created at ▽	Tag immutability	Scan frequency	Encryption type	Pull through cache
○	alpine	276384657722.dkr.ecr.us-east-1.amazonaws.com/alpine	May 03, 2022, 13:57:43 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	apache	276384657722.dkr.ecr.us-east-1.amazonaws.com/apache	May 02, 2022, 00:44:24 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	debian	276384657722.dkr.ecr.us-east-1.amazonaws.com/debian	May 03, 2022, 13:57:33 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	httpd	276384657722.dkr.ecr.us-east-1.amazonaws.com/httpd	May 03, 2022, 13:59:33 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	mariadb	276384657722.dkr.ecr.us-east-1.amazonaws.com/mariadb	May 03, 2022, 13:58:23 (UTC+05.5)	Disabled	Manual	AES-256	Inactive

This page contains the image details such as the URI, creation time, encryption type, and more details along with the repository name.

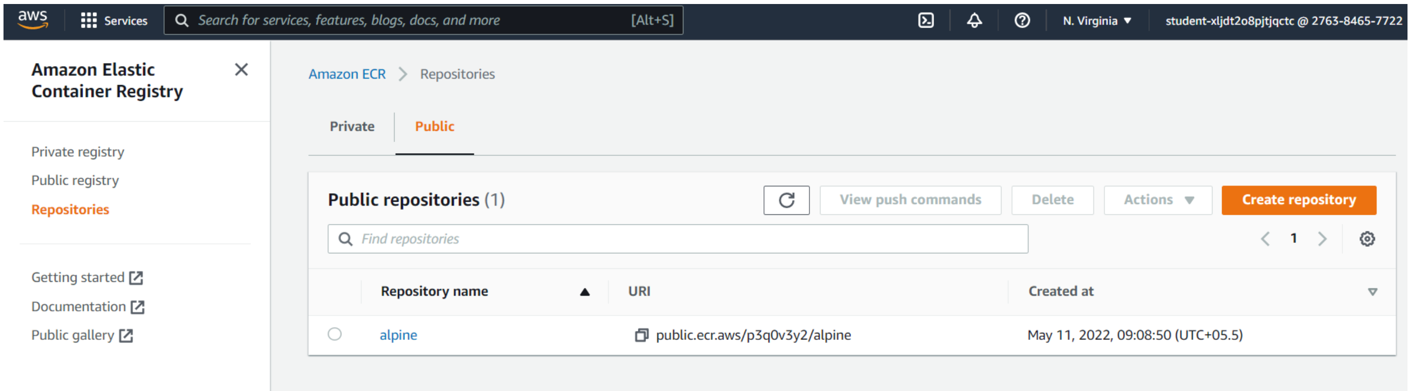
The **URI** is what is used to reference the repository images while creating containers on ECS clusters.
The **URI** is of the format **<account-id>.dkr.ecr.<region>.amazonaws.com/<repo-name>**

The **Tag immutability** column lists its status, if tag immutability is enabled it will prevent image pushes with pre-existing tags from overwriting the images.

The **Encryption type** column lists the encryption properties of the repository, it shows the default encryption types such as AES-256, or has KMS enabled encryptions.

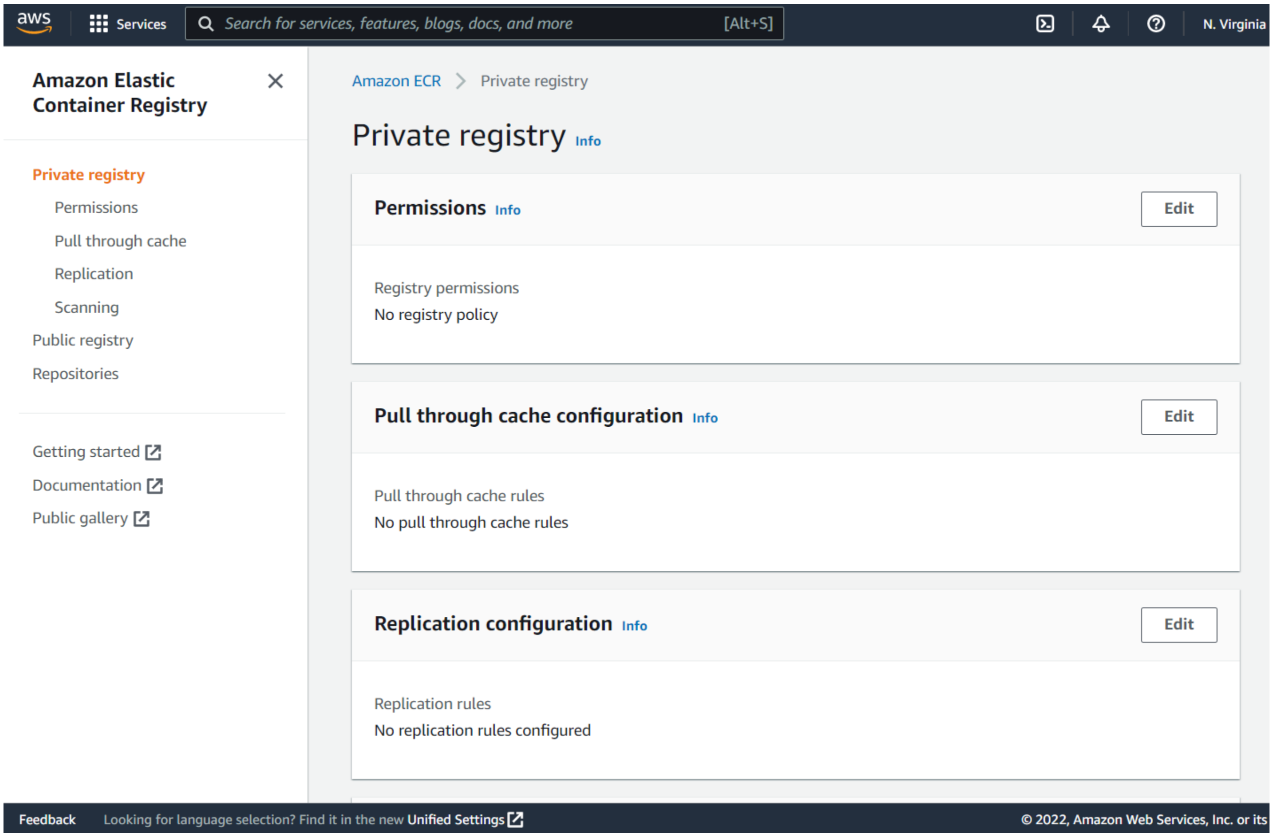
The **Pull through cache** column lists its status, if Pull through cache status is Active it will cache repositories in an external public repository into your private repository.

The Public tab lists the repositories which are publically accessible from this account. A unique default alias is added to the repository name at creation, it is used for identification of this repository from the multitude of public repositories on AWS.



Repository name	URI	Created at
alpine	public.ecr.aws/p3q0v3y2/alpine	May 11, 2022, 09:08:50 (UTC+05.5)

Step 4: Clicking on the Private registry option from the side menu, takes us to the private registry settings.



aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia

Amazon Elastic Container Registry

Private registry
Permissions
Pull through cache
Replication
Scanning
Public registry
Repositories
Getting started
Documentation
Public gallery

Amazon ECR > Private registry

Private registry Info

Permissions Info

Registry permissions
No registry policy

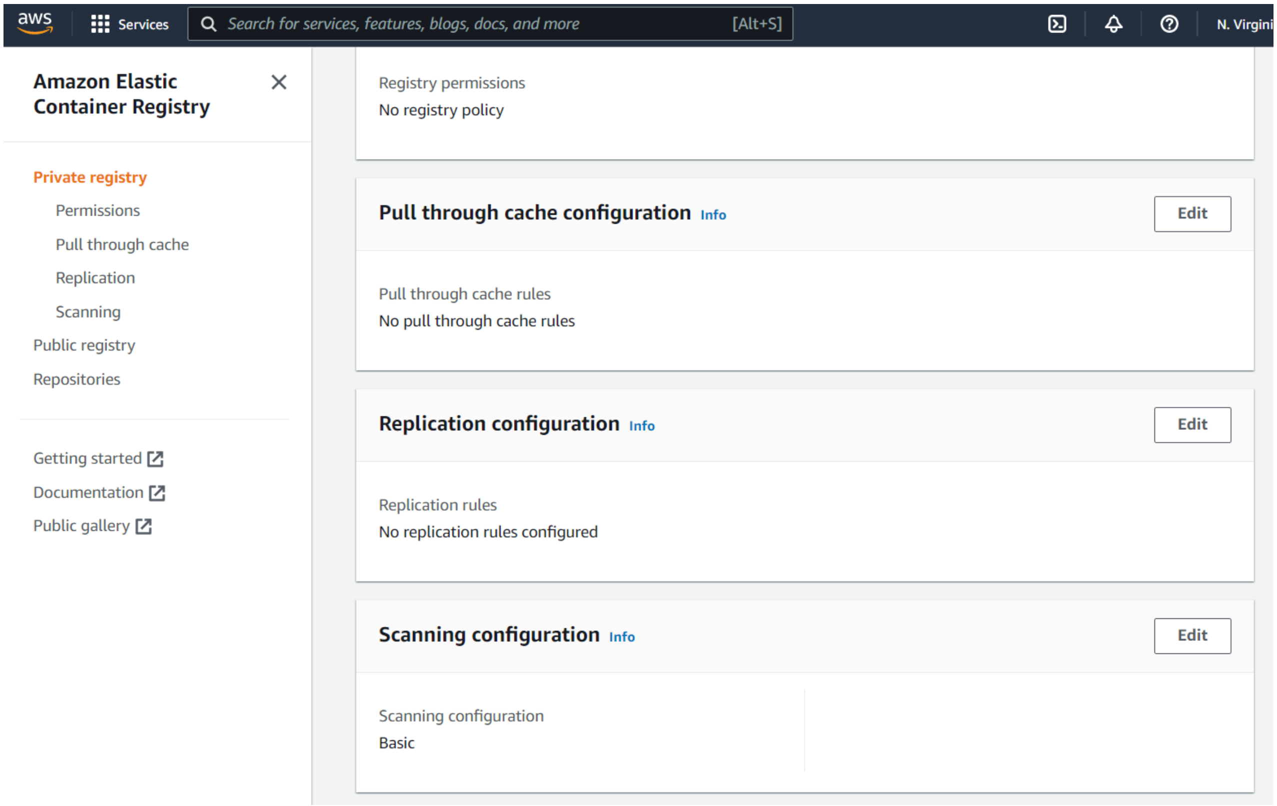
Pull through cache configuration Info

Pull through cache rules
No pull through cache rules

Replication configuration Info

Replication rules
No replication rules configured

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its



Registry permissions
No registry policy

Pull through cache configuration

Pull through cache rules
No pull through cache rules

Replication configuration

Replication rules
No replication rules configured

Scanning configuration

Scanning configuration
Basic

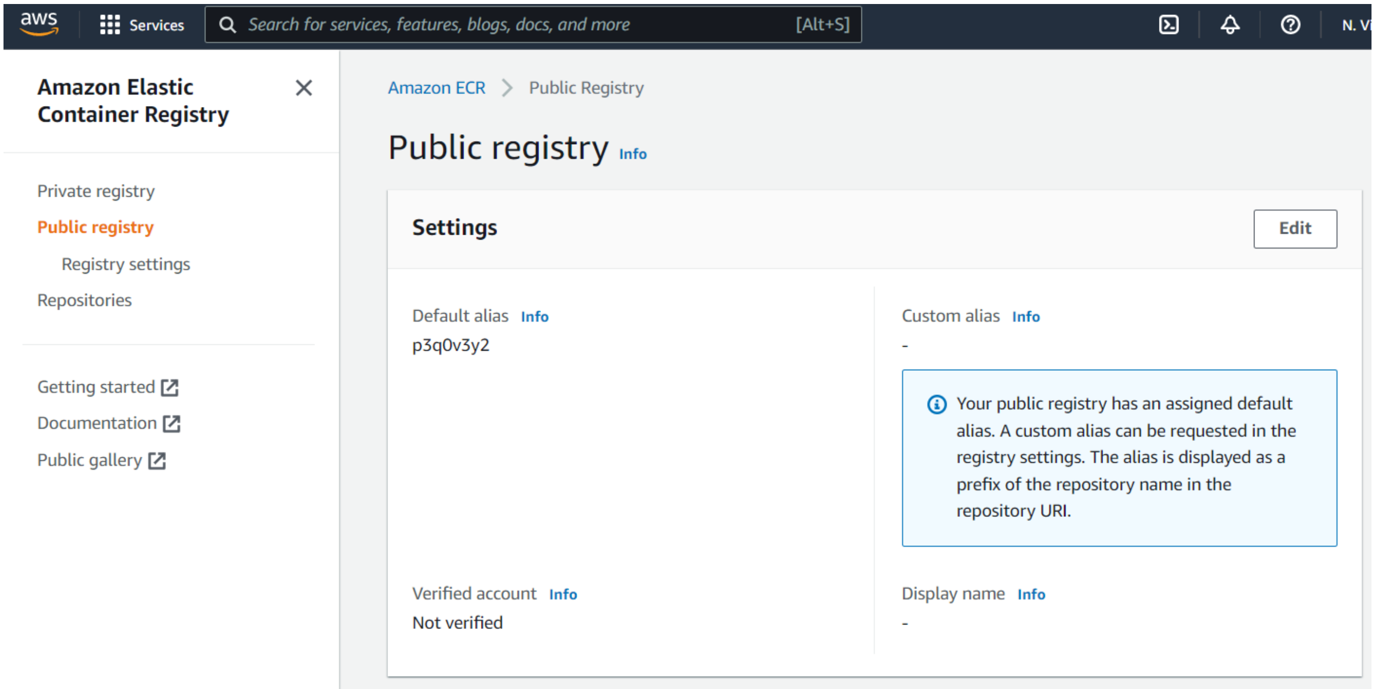
The **Permissions** section allows us to apply a **registry policy** to grant permissions to an AWS principal at the private registry level. These allow us to scope access to the Replication and pull through cache configuration features of our private registry.

The **Pull through cache configuration** lets us set pull through cache rules for the repository.

The **Replication configuration** lets us set rules to manage cross region and cross account repository replication.

The **Scanning configuration** has two options: basic and enhanced scanning. Basic scanning is a free service that allows manual scans and scans on push of images in the registry. Enhanced scanning provides automated continuous scanning that identifies vulnerabilities in both operating systems and enhanced scanning.

Step 5: Clicking on the Public registry option from the side menu, takes us to the public registry settings.



Amazon Elastic Container Registry

- Private registry
- Public registry
  - Registry settings
- Repositories

- Getting started
- Documentation
- Public gallery

Amazon ECR > Public Registry

Public registry Info

Settings Edit

Default alias Info
p3q0v3y2

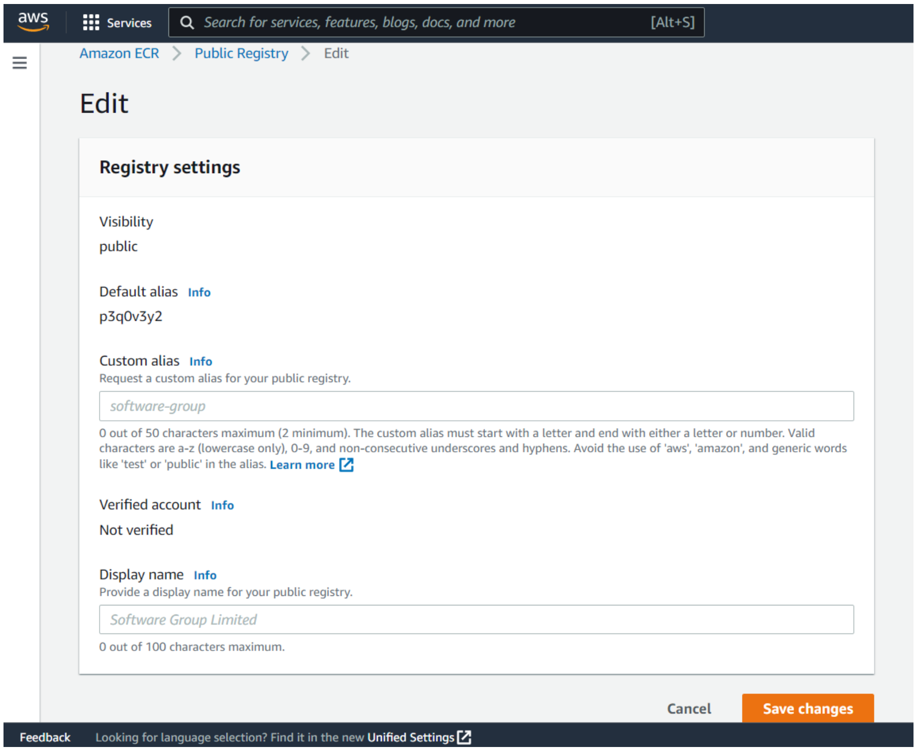
Custom alias Info
-

Your public registry has an assigned default alias. A custom alias can be requested in the registry settings. The alias is displayed as a prefix of the repository name in the repository URI.

Verified account Info
Not verified

Display name Info
-

This page displays the default alias of the public registry and also has options to set up a custom alias and display name for the same.



Amazon ECR > Public Registry > Edit

Edit

Registry settings

Visibility
public

Default alias Info
p3q0v3y2

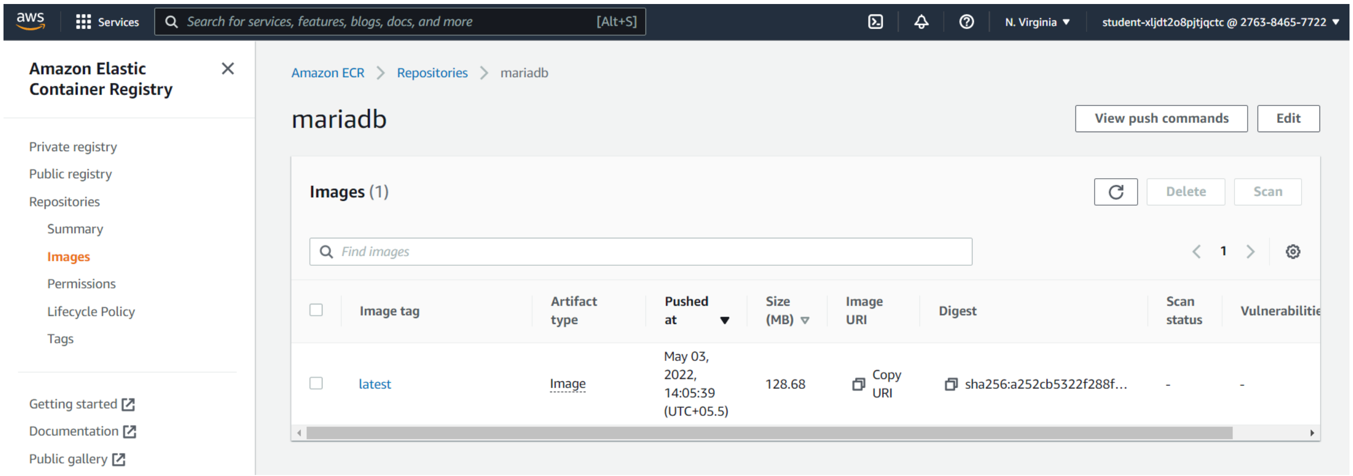
Custom alias Info
Request a custom alias for your public registry.
software-group
0 out of 50 characters maximum (2 minimum). The custom alias must start with a letter and end with either a letter or number. Valid characters are a-z (lowercase only), 0-9, and non-consecutive underscores and hyphens. Avoid the use of 'aws', 'amazon', and generic words like 'test' or 'public' in the alias. Learn more

Verified account Info
Not verified

Display name Info
Provide a display name for your public registry.
Software Group Limited
0 out of 100 characters maximum.

Cancel
Save changes
Feedback
Looking for language selection? Find it in the new Unified Settings

Step 6: Click on the mariadb repository from the private tab.

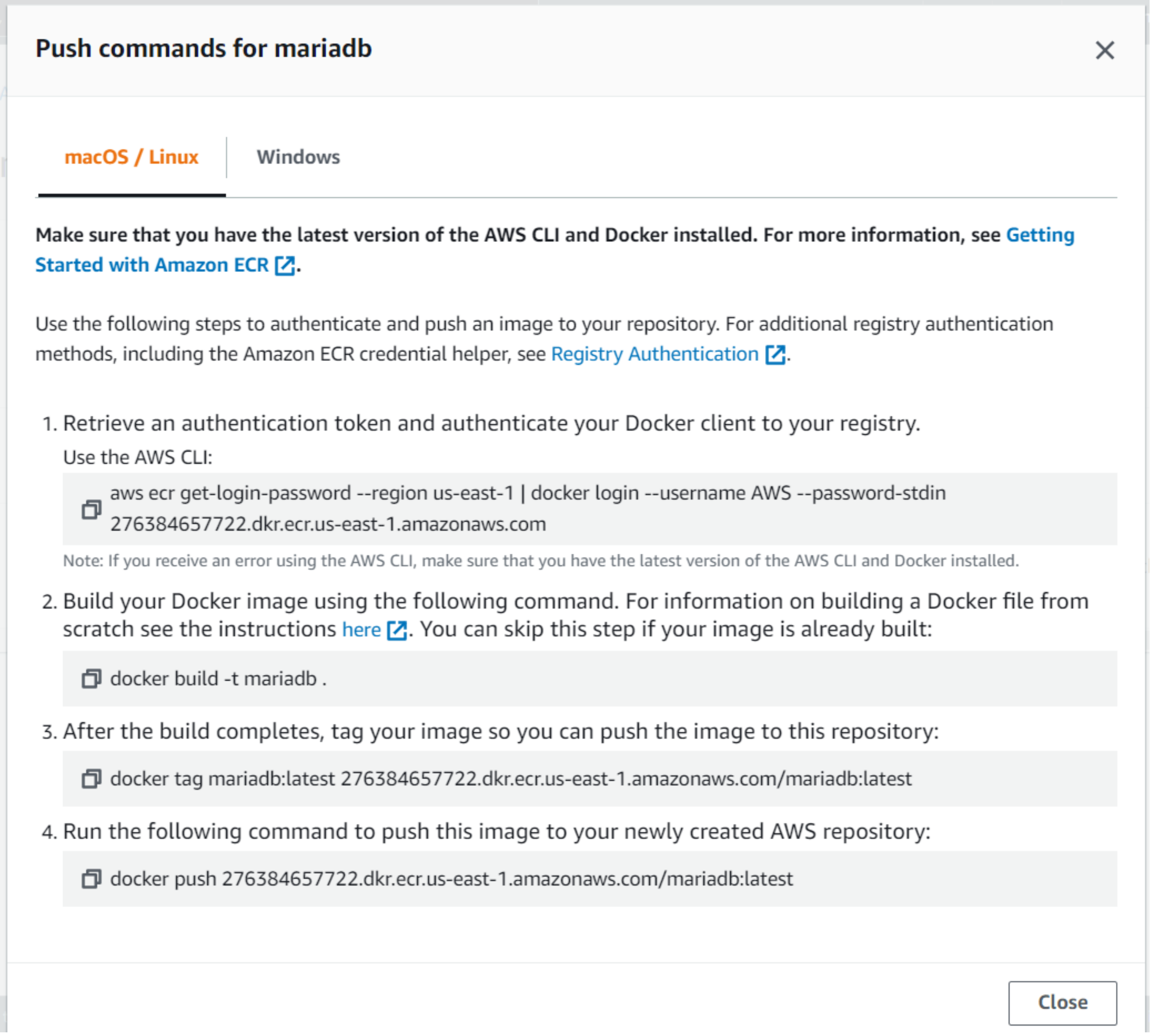


mariadb

Images (1)

	Image tag	Artifact type	Pushed at	Size (MB)	Image URI	Digest	Scan status	Vulnerabilitie
□	latest	Image	May 03, 2022, 14:05:39 (UTC+05.5)	128.68	Copy URI	sha256:a252cb5322f288f...	-	-

This page lists the images in this repository, it also has additional image information like the size, digest, pushed date, etc. Clicking on the **View push commands** button will open a pop up. These are the commands which will let a user push any local image to the private ECR repository.



Make sure that you have the latest version of the AWS CLI and Docker installed. For more information, see Getting Started with Amazon ECR.

Use the following steps to authenticate and push an image to your repository. For additional registry authentication methods, including the Amazon ECR credential helper, see Registry Authentication.

1. Retrieve an authentication token and authenticate your Docker client to your registry.
   Use the AWS CLI:

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 276384657722.dkr.ecr.us-east-1.amazonaws.com
```

   Note: If you receive an error using the AWS CLI, make sure that you have the latest version of the AWS CLI and Docker installed.

2. Build your Docker image using the following command. For information on building a Docker file from scratch see the instructions here. You can skip this step if your image is already built:

```
docker build -t mariadb .
```

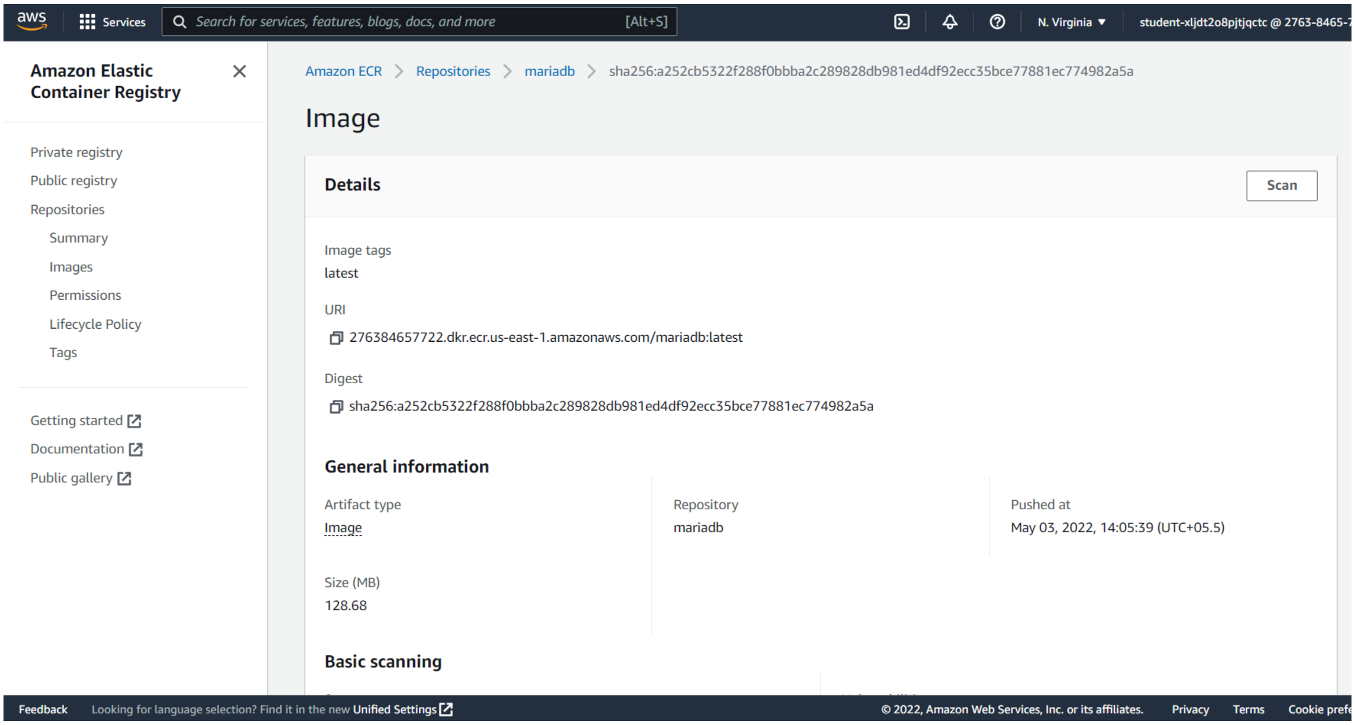
3. After the build completes, tag your image so you can push the image to this repository:

```
docker tag mariadb:latest 276384657722.dkr.ecr.us-east-1.amazonaws.com/mariadb:latest
```

4. Run the following command to push this image to your newly created AWS repository:

```
docker push 276384657722.dkr.ecr.us-east-1.amazonaws.com/mariadb:latest
```

Step 7: On clicking on the Image tag **latest** link, additional information about the image is displayed.


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia ▼
student-xljdt2o8pjtjqctc @ 2763-8465-7
Amazon Elastic Container Registry
Private registry
Public registry
Repositories
Summary
Images
Permissions
Lifecycle Policy
Tags
Getting started
Documentation
Public gallery
Scan
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie prefe

Amazon ECR > Repositories > mariadb > sha256:a252cb5322f288f0bbba2c289828db981ed4df92ecc35bce77881ec774982a5a

Image

Details

Image tags
latest

URI
276384657722.dkr.ecr.us-east-1.amazonaws.com/mariadb:latest

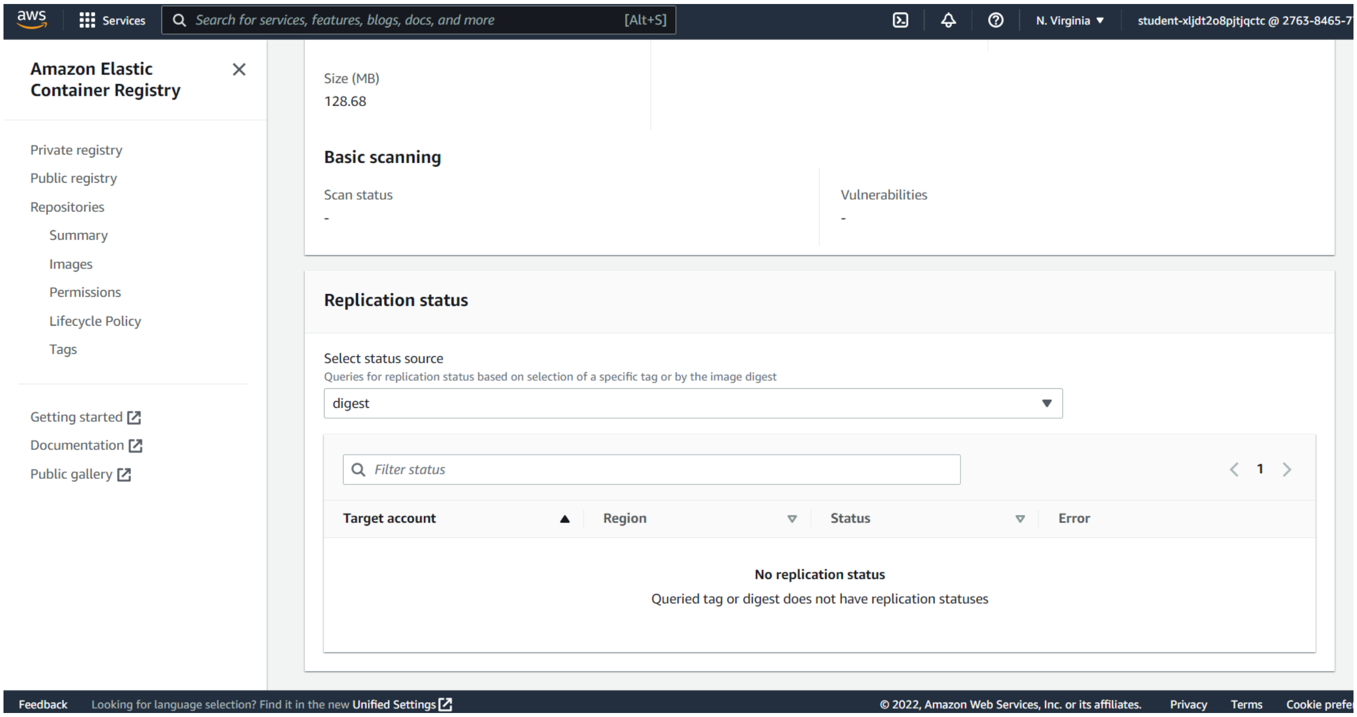
Digest
sha256:a252cb5322f288f0bbba2c289828db981ed4df92ecc35bce77881ec774982a5a

General information

Artifact type	Repository	Pushed at
Image	mariadb	May 03, 2022, 14:05:39 (UTC+05.5)

Size (MB)
128.68

Basic scanning


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia ▼
student-xljdt2o8pjtjqctc @ 2763-8465-7
Amazon Elastic Container Registry
Private registry
Public registry
Repositories
Summary
Images
Permissions
Lifecycle Policy
Tags
Getting started
Documentation
Public gallery
Filter status
1
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie prefe

Size (MB)
128.68

Basic scanning

Scan status	Vulnerabilities
-	-

Replication status

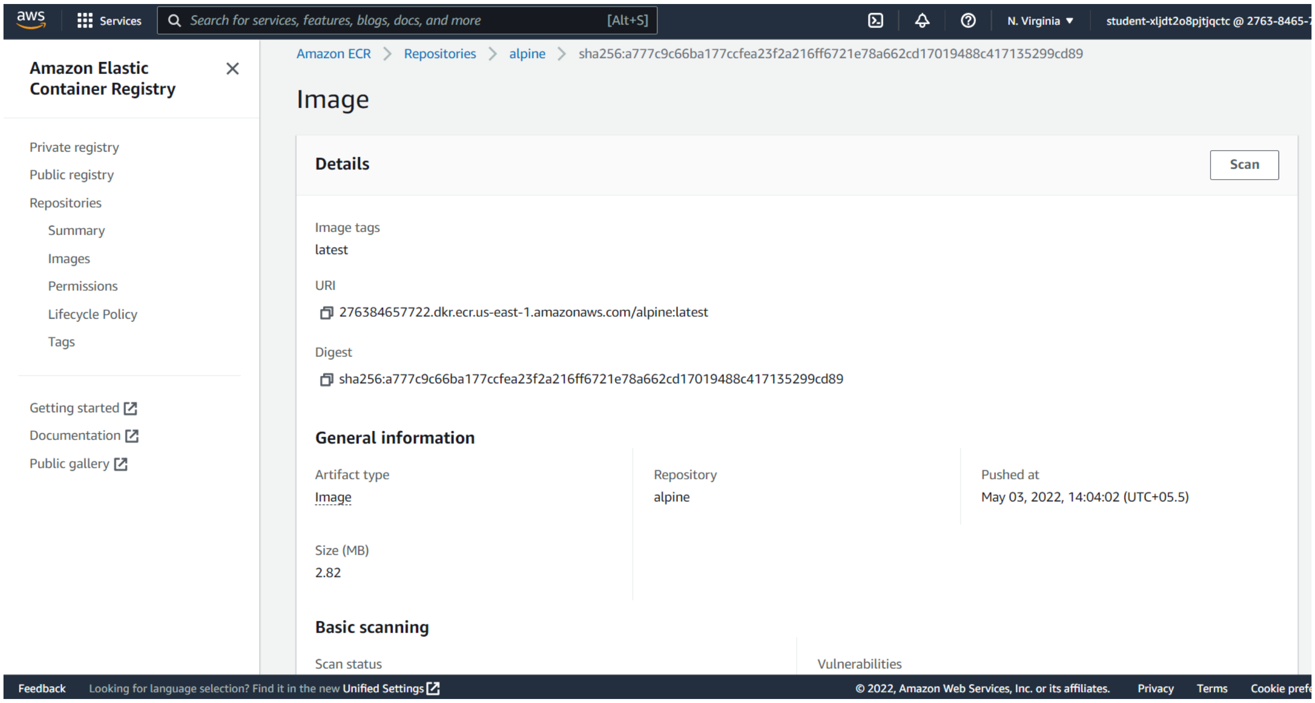
Select status source
Queries for replication status based on selection of a specific tag or by the image digest
digest

Target account	Region	Status	Error

No replication status
Queried tag or digest does not have replication statuses

This page also displays the Image replication status for this image, when replicated this would list the accounts and the regions where the image has been replicated.

Similarly clicking on the tag on the public repository will bring us to another image details page. This page doesn't have the scanning and Image replication information as it is already publicly available.


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
student-xljdt2o8pjtjqctc @ 2763-8465-
Amazon Elastic Container Registry
Private registry
Public registry
Repositories
Summary
Images
Permissions
Lifecycle Policy
Tags
Getting started
Documentation
Public gallery
Amazon ECR > Repositories > alpine > sha256:a777c9c66ba177ccfea23f2a216ff6721e78a662cd17019488c417135299cd89
Scan
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie prefe

Image

Details

Image tags
latest

URI
276384657722.dkr.ecr.us-east-1.amazonaws.com/alpine:latest

Digest
sha256:a777c9c66ba177ccfea23f2a216ff6721e78a662cd17019488c417135299cd89

General information

Artifact type
Image

Repository
alpine

Pushed at
May 03, 2022, 14:04:02 (UTC+05.5)

Size (MB)
2.82

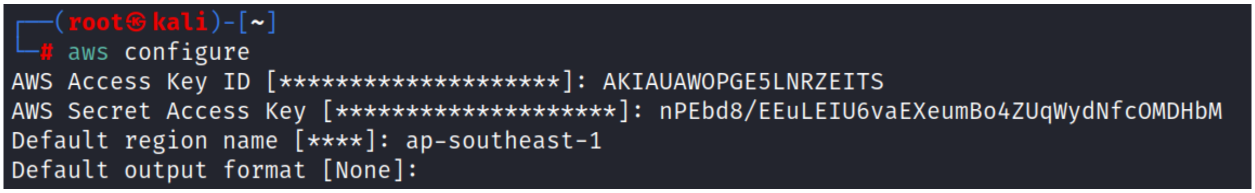
Basic scanning

Scan status

Vulnerabilities

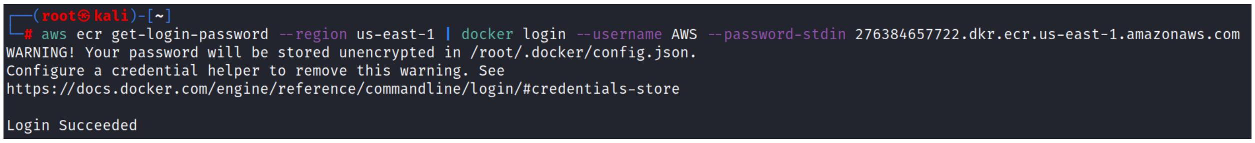
Step 8: To pull an image from the private registry first configure aws cli with lab credentials. Then authenticate docker to interact with the ecr service.

Command: aws configure



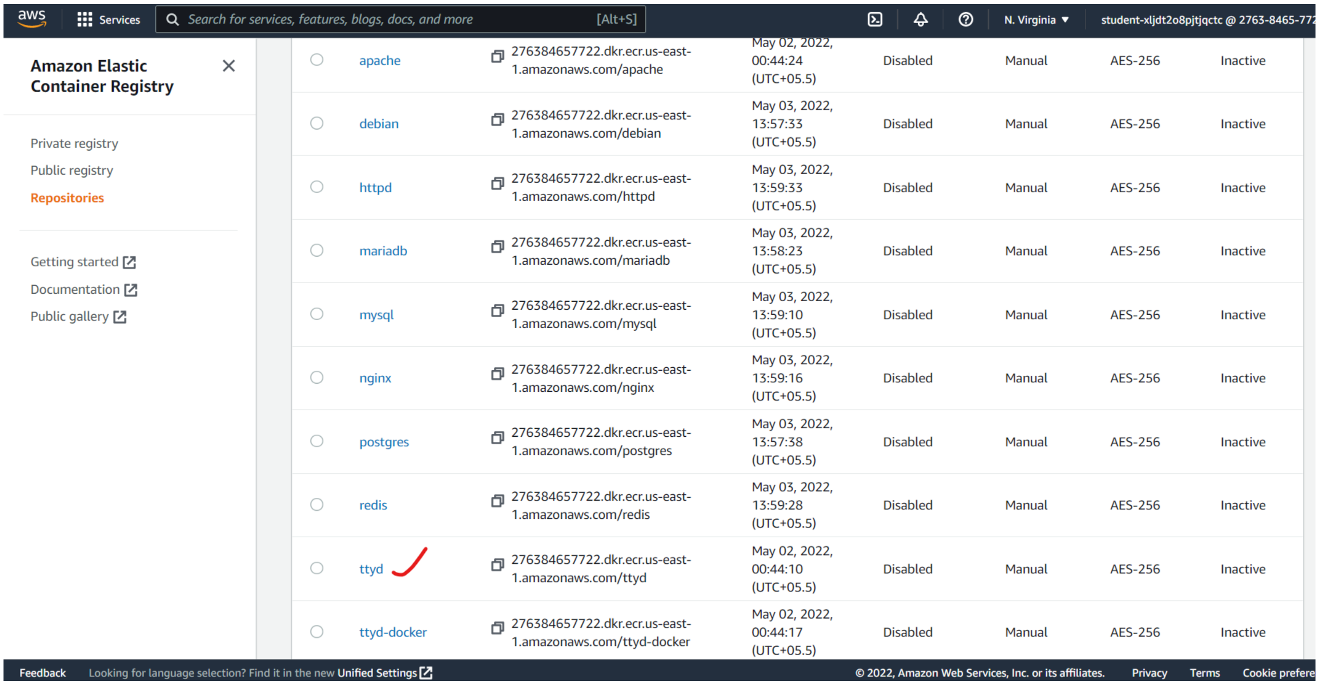
```
┌──(root㉿kali)-[~]
└─# aws configure
AWS Access Key ID [*******************]: AKIAUAWOPGE5LNRZEITS
AWS Secret Access Key [*******************]: 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
Default region name [****]: ap-southeast-1
Default output format [None]:
```

Command: aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 276384657722.dkr.ecr.us-east-1.amazonaws.com



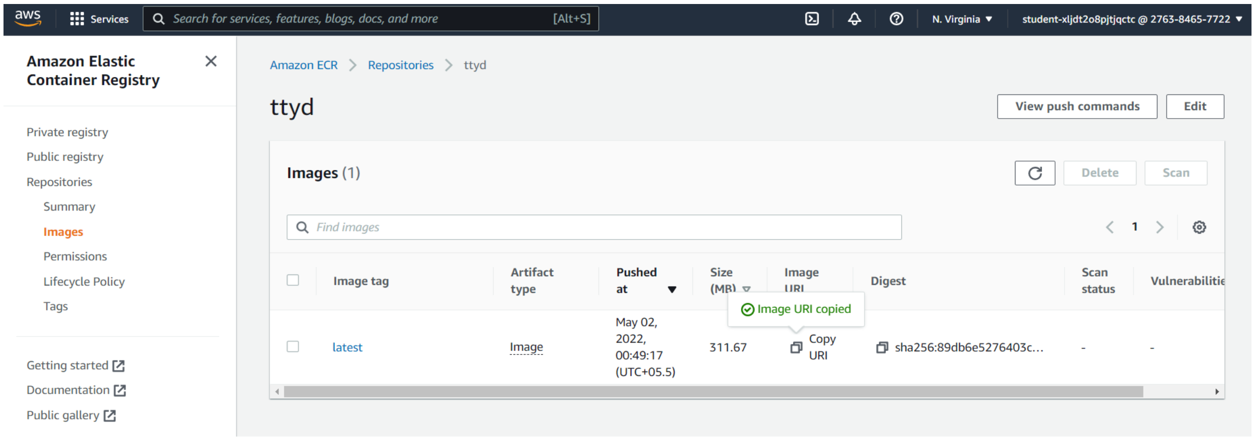
```
┌──(root㉿kali)-[~]
└─# aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 276384657722.dkr.ecr.us-east-1.amazonaws.com
WARNING! Your password will be stored unencrypted in /root/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
```

From the Private repositories page click on the ttyd repository.


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia ▼
student-xljdt2o8pjtjqctc @ 2763-8465-772
Amazon Elastic Container Registry
✕
Private registry
Public registry
Repositories
Getting started
Documentation
Public gallery
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie prefere

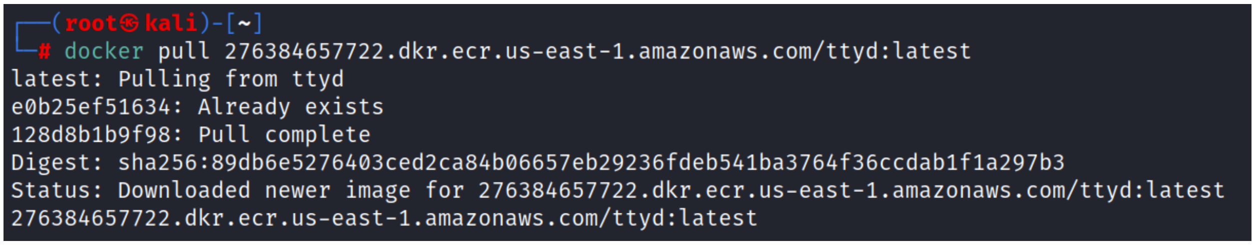
○	apache	276384657722.dkr.ecr.us-east-1.amazonaws.com/apache	May 02, 2022, 00:44:24 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	debian	276384657722.dkr.ecr.us-east-1.amazonaws.com/debian	May 03, 2022, 13:57:33 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	httpd	276384657722.dkr.ecr.us-east-1.amazonaws.com/httpd	May 03, 2022, 13:59:33 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	mariadb	276384657722.dkr.ecr.us-east-1.amazonaws.com/mariadb	May 03, 2022, 13:58:23 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	mysql	276384657722.dkr.ecr.us-east-1.amazonaws.com/mysql	May 03, 2022, 13:59:10 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	nginx	276384657722.dkr.ecr.us-east-1.amazonaws.com/nginx	May 03, 2022, 13:59:16 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	postgres	276384657722.dkr.ecr.us-east-1.amazonaws.com/postgres	May 03, 2022, 13:57:38 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	redis	276384657722.dkr.ecr.us-east-1.amazonaws.com/redis	May 03, 2022, 13:59:28 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	ttyd ✓	276384657722.dkr.ecr.us-east-1.amazonaws.com/ttyd	May 02, 2022, 00:44:10 (UTC+05.5)	Disabled	Manual	AES-256	Inactive
○	ttyd-docker	276384657722.dkr.ecr.us-east-1.amazonaws.com/ttyd-docker	May 02, 2022, 00:44:17 (UTC+05.5)	Disabled	Manual	AES-256	Inactive

On the ttyd images page click on the copy URI button this is the URI for this image.



□	Image tag	Artifact type	Pushed at ▼	Size (MB)	Image URI	Digest	Scan status	Vulnerabilitie
□	latest	Image	May 02, 2022, 00:49:17 (UTC+05.5)	311.67	Copy URI	sha256:89db6e5276403c...	-	-

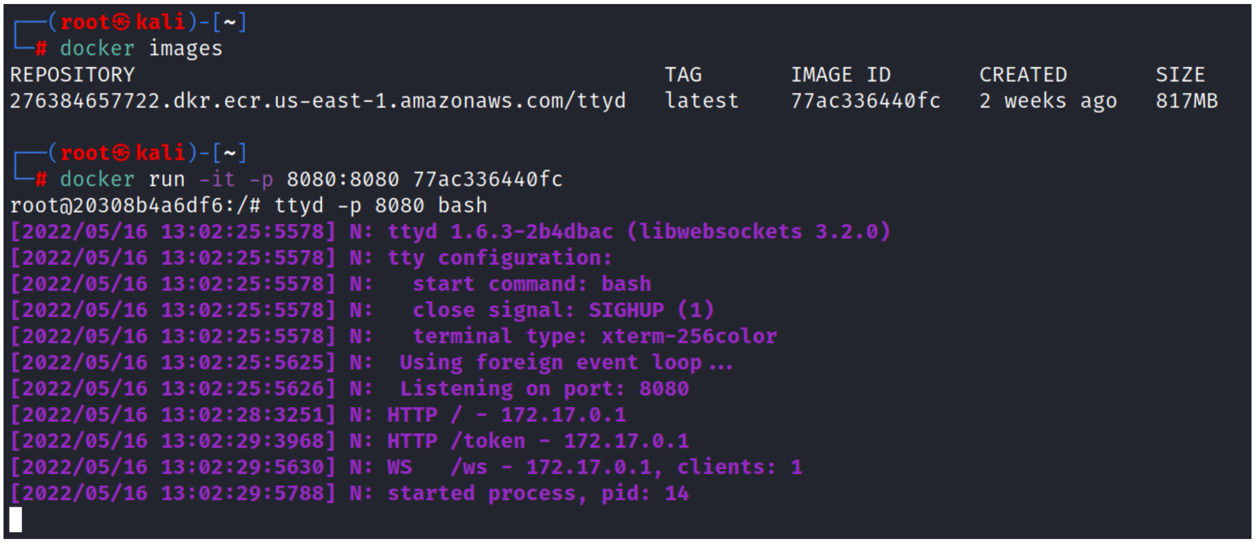
Next do a simple docker pull with the Image URI.
Command: docker pull 276384657722.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest



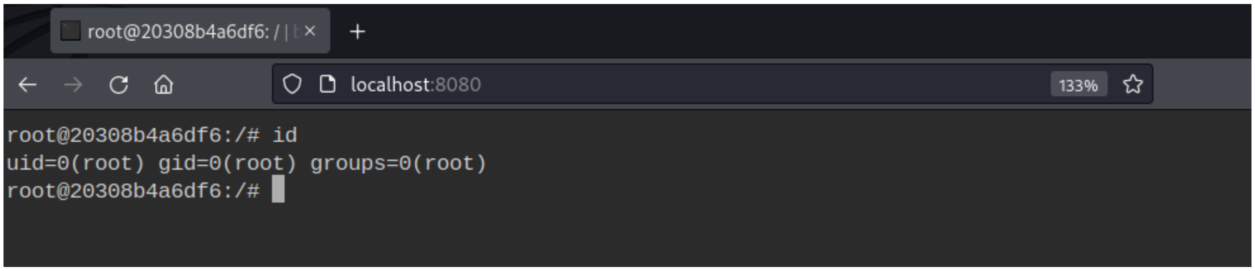
```
┌──(root㉿kali)-[~]
└─# docker pull 276384657722.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest
latest: Pulling from ttyd
e0b25ef51634: Already exists
128d8b1b9f98: Pull complete
Digest: sha256:89db6e5276403ced2ca84b06657eb29236fdeb541ba3764f36ccdab1f1a297b3
Status: Downloaded newer image for 276384657722.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest
276384657722.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest
```

Step 9: Let’s run this pulled image. After pulling the image from ecr all regular docker operations can be performed on this local image.

Commands:
docker images
docker run –it –p 8080:8080 <Image ID>
ttyd –p 8080 bash



```
┌──(root㉿kali)-[~]
└─# docker images
REPOSITORY                                          TAG       IMAGE ID       CREATED        SIZE
276384657722.dkr.ecr.us-east-1.amazonaws.com/ttyd   latest    77ac336440fc   2 weeks ago    817MB

┌──(root㉿kali)-[~]
└─# docker run -it -p 8080:8080 77ac336440fc
root@20308b4a6df6:/# ttyd -p 8080 bash
[2022/05/16 13:02:25:5578] N: ttyd 1.6.3-2b4dbac (libwebsockets 3.2.0)
[2022/05/16 13:02:25:5578] N: tty configuration:
[2022/05/16 13:02:25:5578] N:   start command: bash
[2022/05/16 13:02:25:5578] N:   close signal: SIGHUP (1)
[2022/05/16 13:02:25:5578] N:   terminal type: xterm-256color
[2022/05/16 13:02:25:5625] N:  Using foreign event loop...
[2022/05/16 13:02:25:5626] N:  Listening on port: 8080
[2022/05/16 13:02:28:3251] N: HTTP / - 172.17.0.1
[2022/05/16 13:02:29:3968] N: HTTP /token - 172.17.0.1
[2022/05/16 13:02:29:5630] N: WS   /ws - 172.17.0.1, clients: 1
[2022/05/16 13:02:29:5788] N: started process, pid: 14
```



```
root@20308b4a6df6:/# id
uid=0(root) gid=0(root) groups=0(root)
root@20308b4a6df6:/#
```

References:

1. AWS ECR Documentation (https://docs.aws.amazon.com/ecr/index.html)