Name: **Đỗ Minh Trí**

Staff Code: **SD5976**

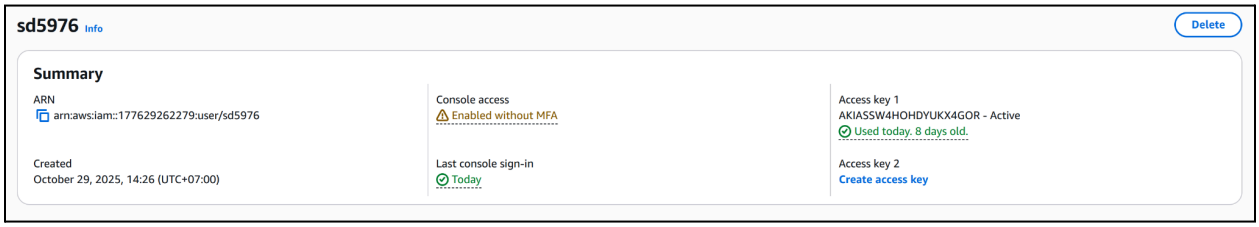
AWS Infrastructure

I. Setting Up AWS Infrastructure with Terraform

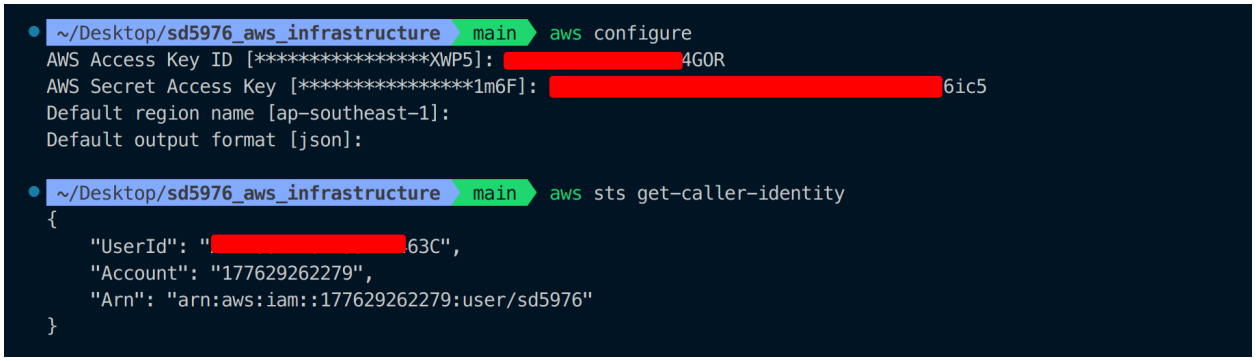
We will deploy AWS infrastructure using Terraform through this repository:

https://github.com/tri-dominh/sd5976_aws_infrastructure

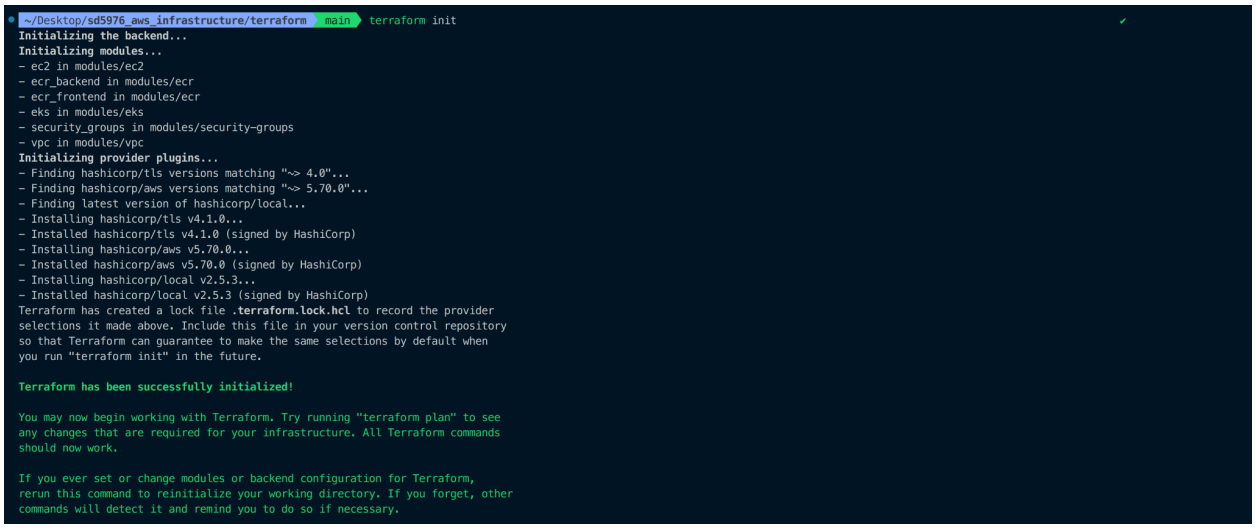
First, I created an IAM user for practical DevOps training: **sd5976**.



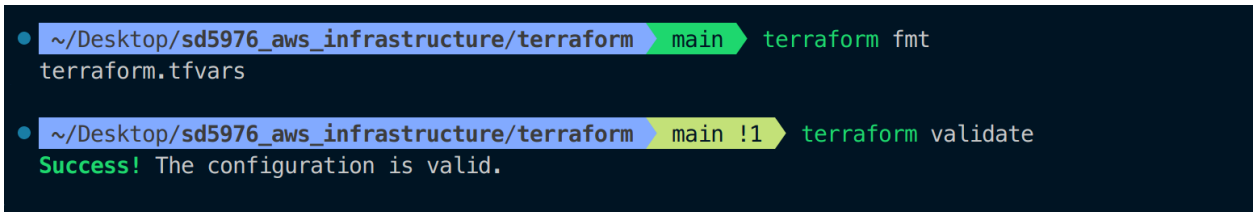
Configure this IAM user on local via **AWS CLI** with Access Key and Secret Access Key.



Go to **sd5976_aws_infrastructure/terraform**, run **terraform init** to initialize the infrastructure.



Use **terraform fmt** and **terraform validate** to format and check your code.



Run **terraform plan** to preview resources that will be created.

Execute **terraform apply** to deploy the resources.

Type **yes** to confirm.

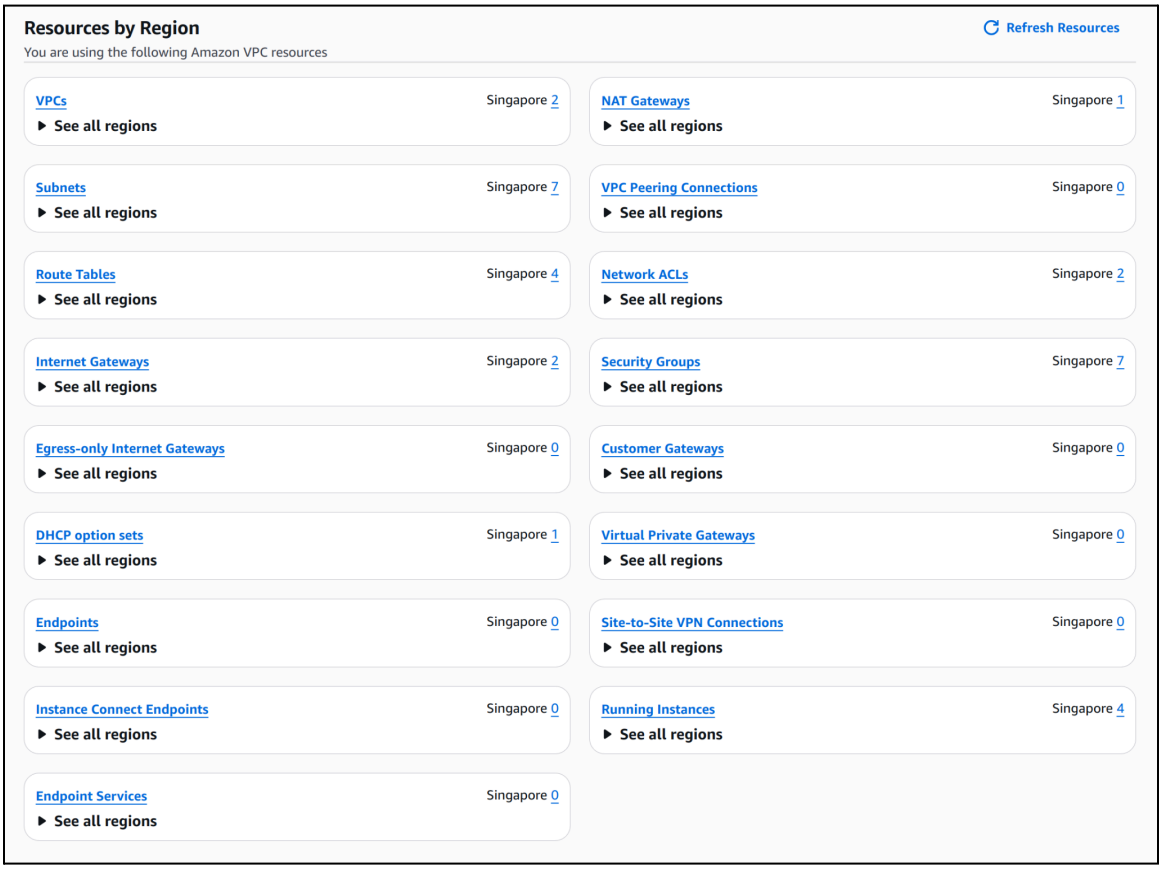
```
Plan: 38 to add, 0 to change, 0 to destroy.

Changes to Outputs:
  + configure_kubectl               = "aws eks update-kubeconfig --region ap-southeast-1 --name cicd-pipeline-cluster"
  + docker_ip                       = (known after apply)
  + ecr_backend_repository_name     = "sd5976-backend"
  + ecr_backend_repository_url      = (known after apply)
  + ecr_frontend_repository_name    = "sd5976-frontend"
  + ecr_frontend_repository_url     = (known after apply)
  + eks_cluster_endpoint            = (known after apply)
  + eks_cluster_name                = "cicd-pipeline-cluster"
  + jenkins_initial_password_command = (known after apply)
  + jenkins_ip                      = (known after apply)
  + jenkins_url                     = (known after apply)
  + ssh_connection_docker           = (known after apply)
  + ssh_connection_jenkins          = (known after apply)
  + vpc_id                          = (known after apply)

Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.

  Enter a value: yes
```

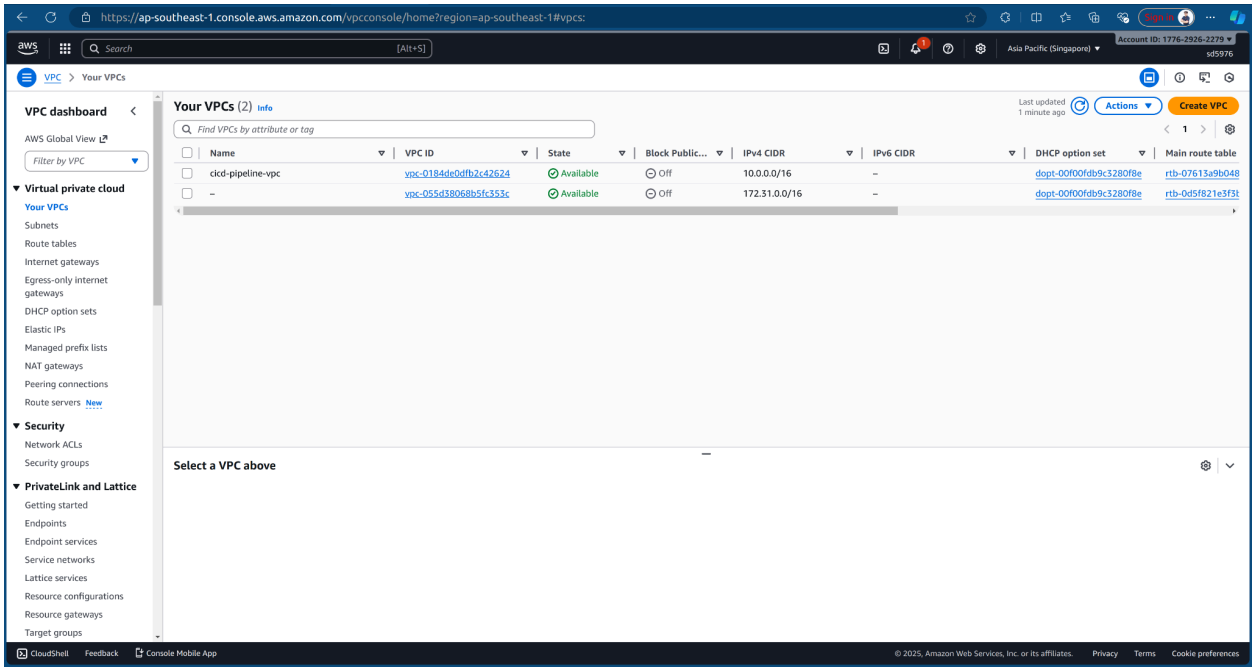
Resource creation may take around 20 minutes or more.

```
Apply complete! Resources: 38 added, 0 changed, 0 destroyed.

Outputs:

configure_kubectl = "aws eks update-kubeconfig --region ap-southeast-1 --name cicd-pipeline-cluster"
docker_ip = "47.128.237.198"
ecr_backend_repository_name = "sd5976-backend"
ecr_backend_repository_url = "177629262279.dkr.ecr.ap-southeast-1.amazonaws.com/sd5976-backend"
ecr_frontend_repository_name = "sd5976-frontend"
ecr_frontend_repository_url = "177629262279.dkr.ecr.ap-southeast-1.amazonaws.com/sd5976-frontend"
eks_cluster_endpoint = "https://9A770A8B363B32838F392C1018289B7E.gr7.ap-southeast-1.eks.amazonaws.com"
eks_cluster_name = "cicd-pipeline-cluster"
jenkins_initial_password_command = "ssh -i cicd-pipeline-key.pem ubuntu@13.228.28.131 'sudo cat /var/lib/jenkins/secrets/initialAdminPassword'"
jenkins_ip = "13.228.28.131"
jenkins_url = "http://13.228.28.131:8080"
ssh_connection_docker = "ssh -i cicd-pipeline-key.pem ubuntu@47.128.237.198"
ssh_connection_jenkins = "ssh -i cicd-pipeline-key.pem ubuntu@13.228.28.131"
vpc_id = "vpc-0184de0dfb2c42624"

○ ~/Desktop/sd5976_aws_infrastructure/terraform main
```

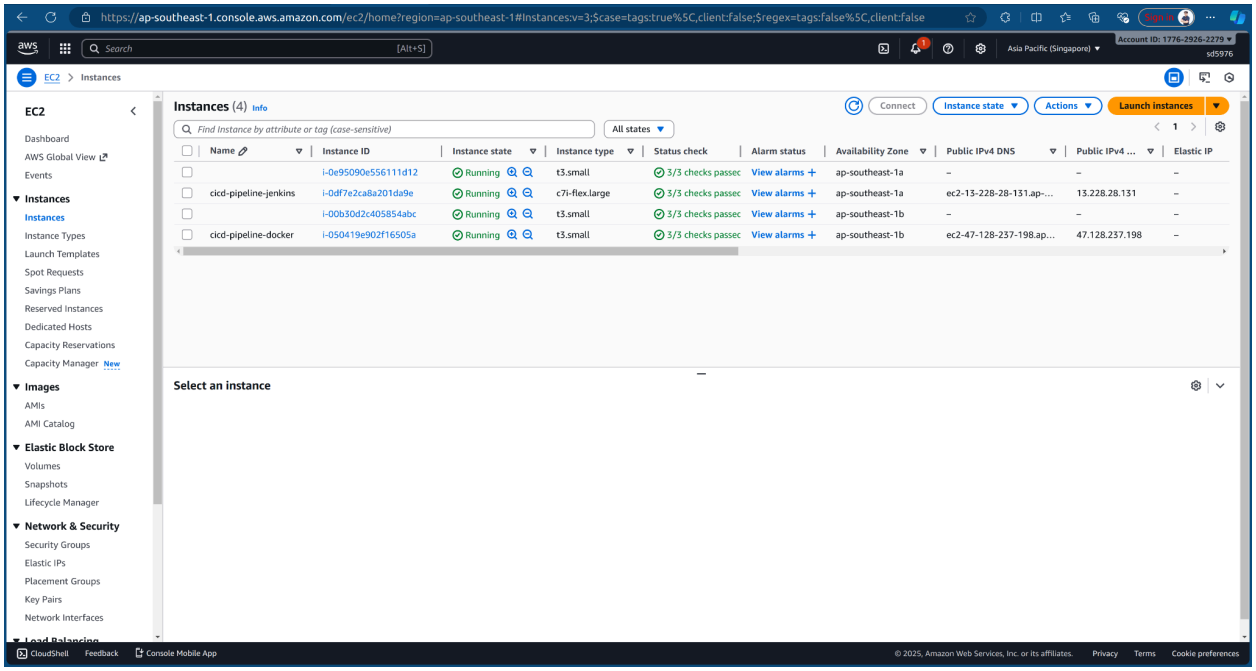
After applying, you can see the following resources on AWS:

VPC

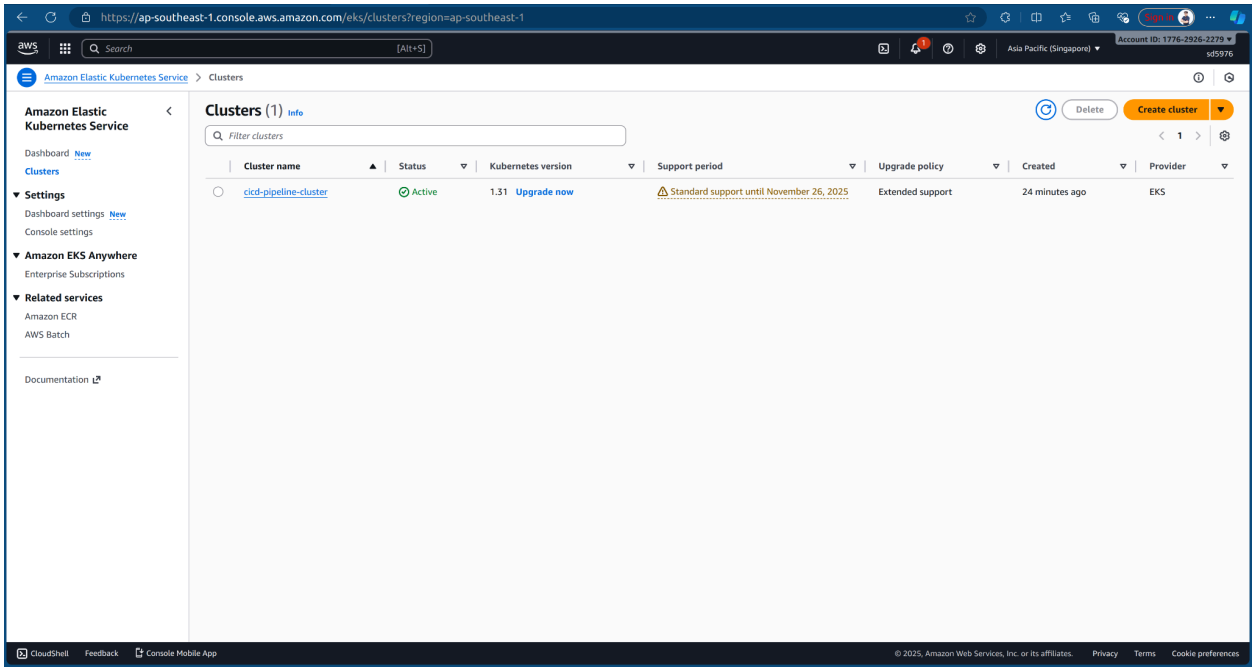


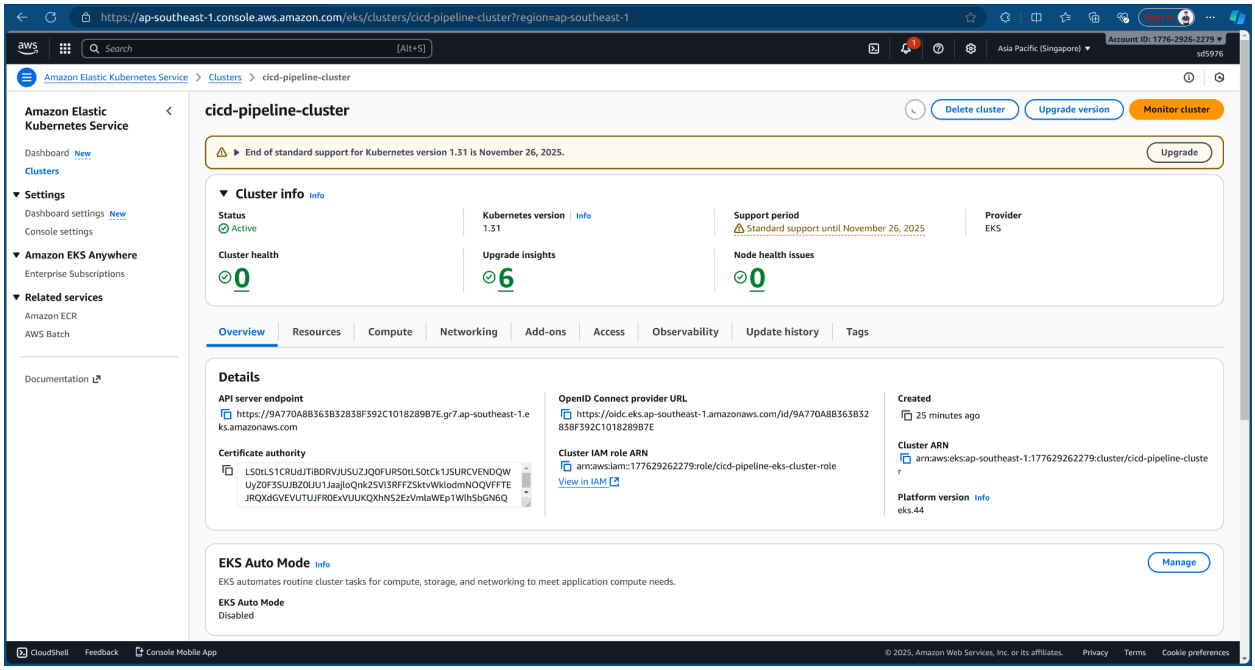


EC2


https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-southeast-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
Search
[Alt+S]
Asia Pacific (Singapore)
Account ID: 1776-2926-2279
sd5976
EC2 > Instances
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Instances (4) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
i-0e95090e556111d12 Running t3.small 3/3 checks passed View alarms ap-southeast-1a – – –
cicd-pipeline-jenkins i-0df7e2ca8a201da9e Running c7i-flex.large 3/3 checks passed View alarms ap-southeast-1a ec2-13-228-28-131.ap-... 13.228.28.131 –
i-00b30d2c405854abc Running t3.small 3/3 checks passed View alarms ap-southeast-1b – – –
cicd-pipeline-docker i-050419e902f16505a Running t3.small 3/3 checks passed View alarms ap-southeast-1b ec2-47-128-237-198.ap... 47.128.237.198 –
Select an instance
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

EKS

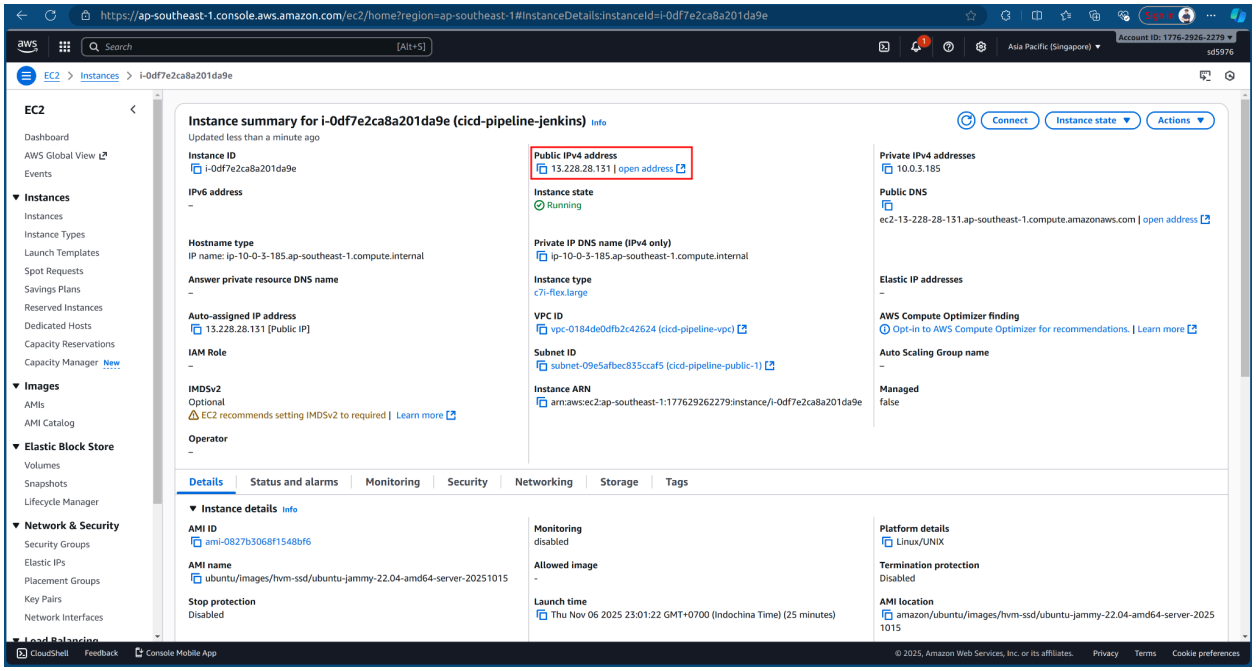

https://ap-southeast-1.console.aws.amazon.com/eks/clusters?region=ap-southeast-1
Search
[Alt+S]
Asia Pacific (Singapore)
Account ID: 1776-2926-2279
sd5976
Amazon Elastic Kubernetes Service > Clusters
Amazon Elastic Kubernetes Service
Dashboard New
Clusters
Settings
Dashboard settings New
Console settings
Amazon EKS Anywhere
Enterprise Subscriptions
Related services
Amazon ECR
AWS Batch
Documentation
Clusters (1) Info
Delete
Create cluster
Filter clusters
Cluster name
Status
Kubernetes version
Support period
Upgrade policy
Created
Provider
cicd-pipeline-cluster Active 1.31 Upgrade now Standard support until November 26, 2025 Extended support 24 minutes ago EKS
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

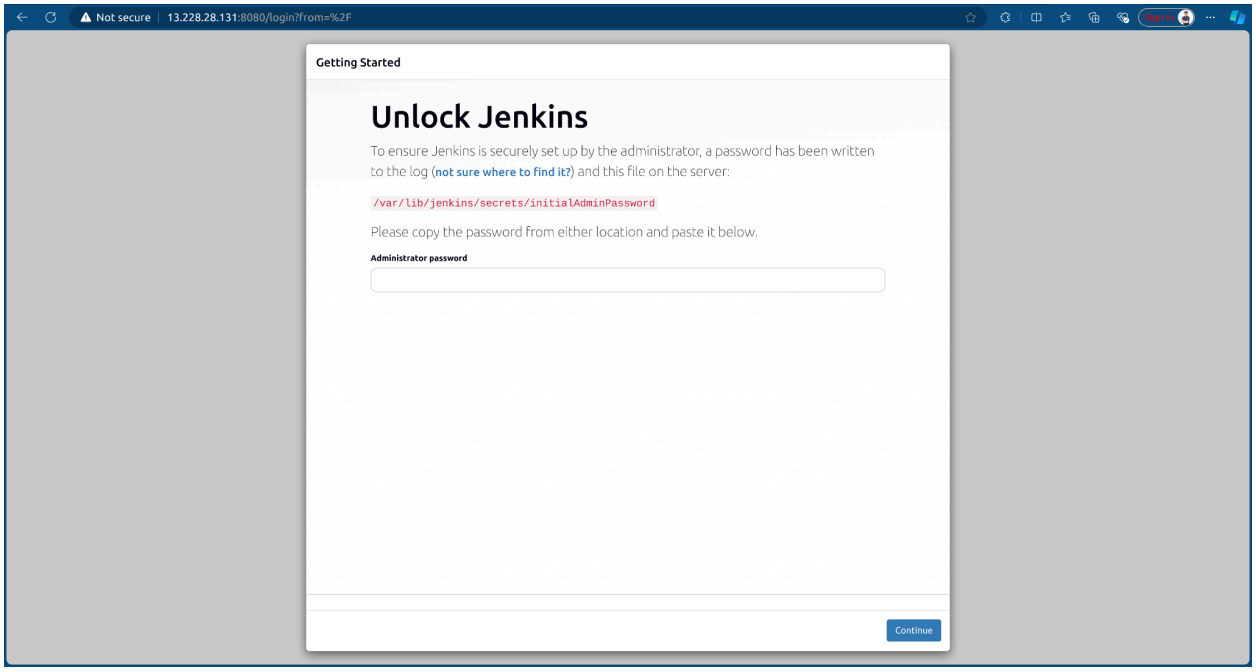

https://ap-southeast-1.console.aws.amazon.com/eks/clusters/cicd-pipeline-cluster?region=ap-southeast-1
Search
[Alt+S]
Asia Pacific (Singapore)
Account ID: 1776-2926-2279
sd5976
Amazon Elastic Kubernetes Service
Clusters
cicd-pipeline-cluster
Amazon Elastic Kubernetes Service
Dashboard New
Clusters
Settings
Dashboard settings New
Console settings
Amazon EKS Anywhere
Enterprise Subscriptions
Related services
Amazon ECR
AWS Batch
Documentation
cicd-pipeline-cluster
Delete cluster
Upgrade version
Monitor cluster
End of standard support for Kubernetes version 1.31 is November 26, 2025.
Upgrade
Cluster info Info
Status
Active
Kubernetes version Info
1.31
Support period
Standard support until November 26, 2025
Provider
EKS
Cluster health
0
Upgrade insights
6
Node health issues
0
Overview
Resources
Compute
Networking
Add-ons
Access
Observability
Update history
Tags
Details
API server endpoint
https://9A770A8B363B32838F392C1018289B7E.gr7.ap-southeast-1.eks.amazonaws.com
Certificate authority
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURCVENDQWUyZ0F3SUJBZ0lJU1JaajloQnk2SVl3RFFZSktvWklodmNOQVFFTEJRQXdGVEVUTUJFR0ExVUUKQXhNS2EzVmlaWEp1WlhSbGN6Q
OpenID Connect provider URL
https://oidc.eks.ap-southeast-1.amazonaws.com/id/9A770A8B363B32838F392C1018289B7E
Cluster IAM role ARN
arn:aws:iam::177629262279:role/cicd-pipeline-eks-cluster-role
View in IAM
Created
25 minutes ago
Cluster ARN
arn:aws:eks:ap-southeast-1:177629262279:cluster/cicd-pipeline-cluster
Platform version Info
eks.44
EKS Auto Mode Info
Manage
EKS automates routine cluster tasks for compute, storage, and networking to meet application compute needs.
EKS Auto Mode
Disabled
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

II. Access Jenkins

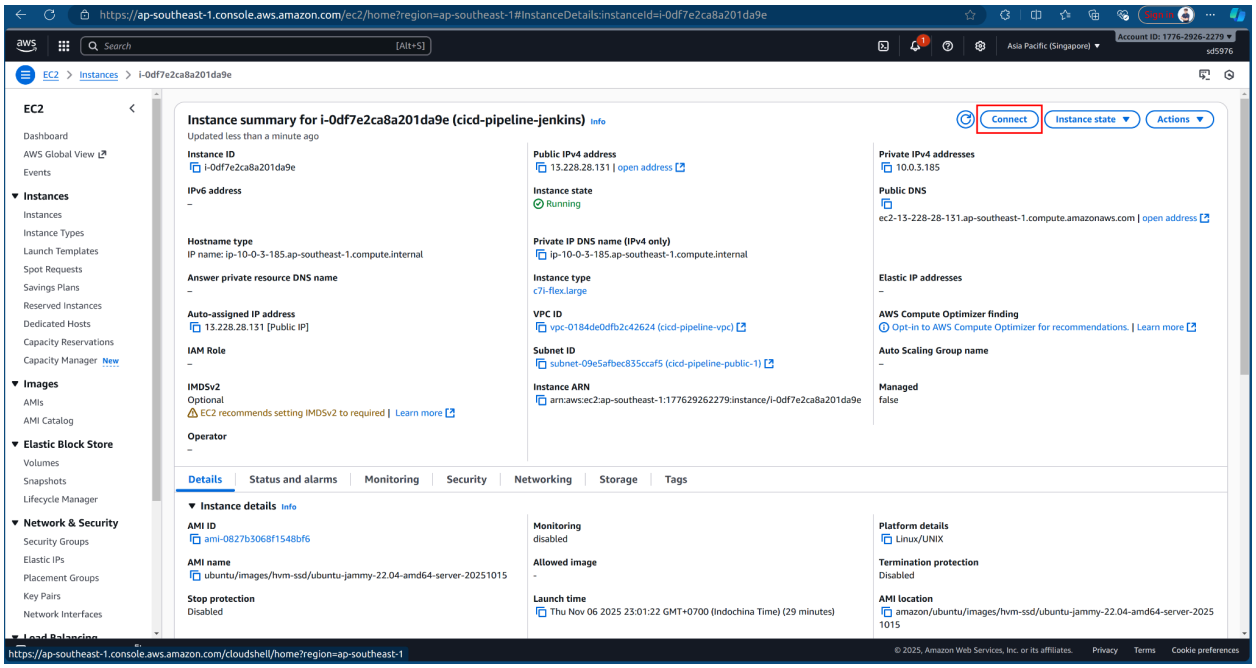
Terraform has already created an EC2 instance with Jenkins installed. Access Jenkins at:

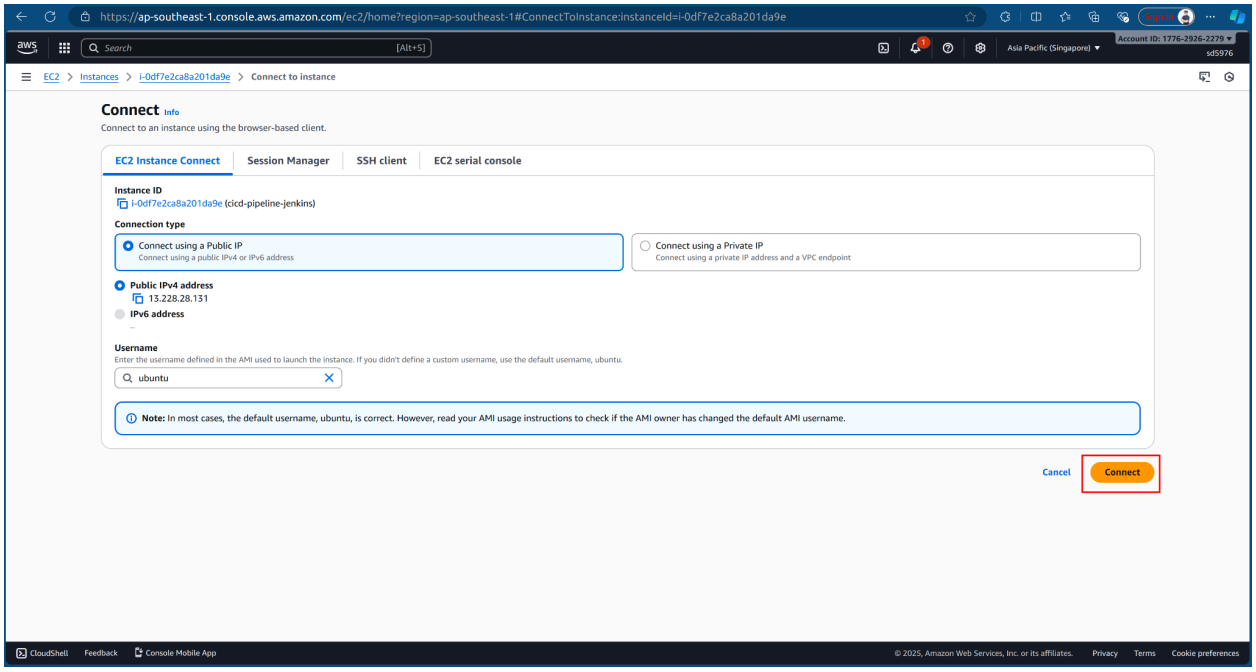
http://13.228.28.131:8080/





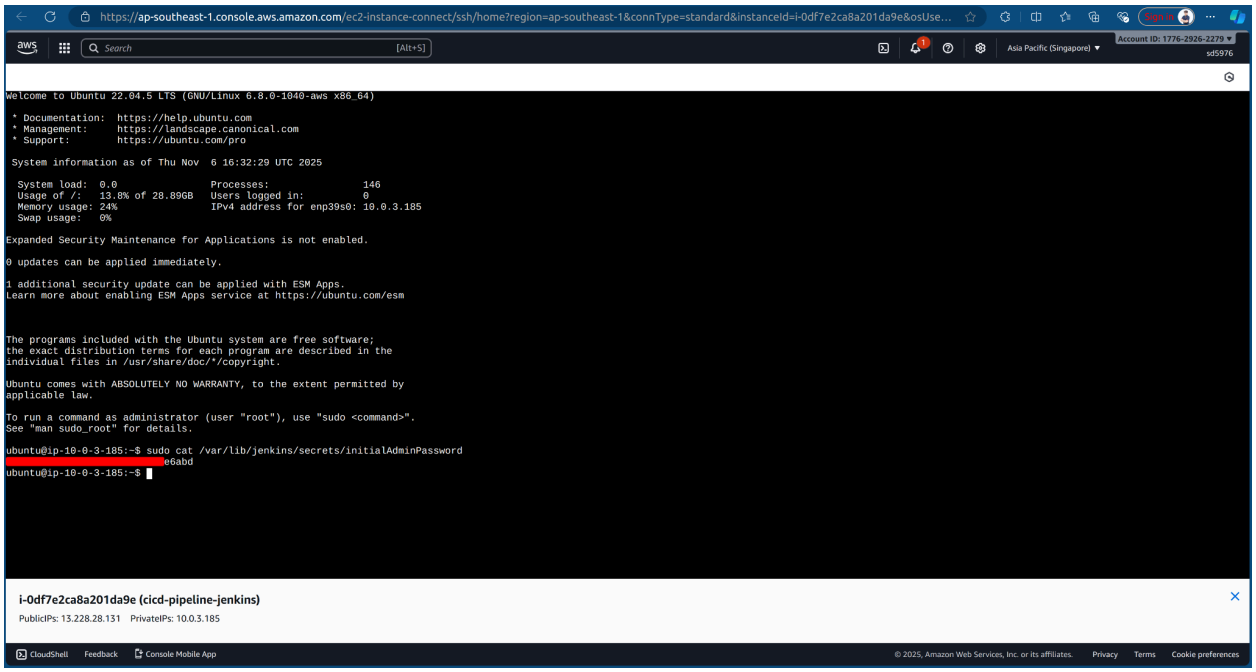
To get the initialAdminPassword, we need to connect to the EC2 instance **cicd-pipeline-jenkins**.



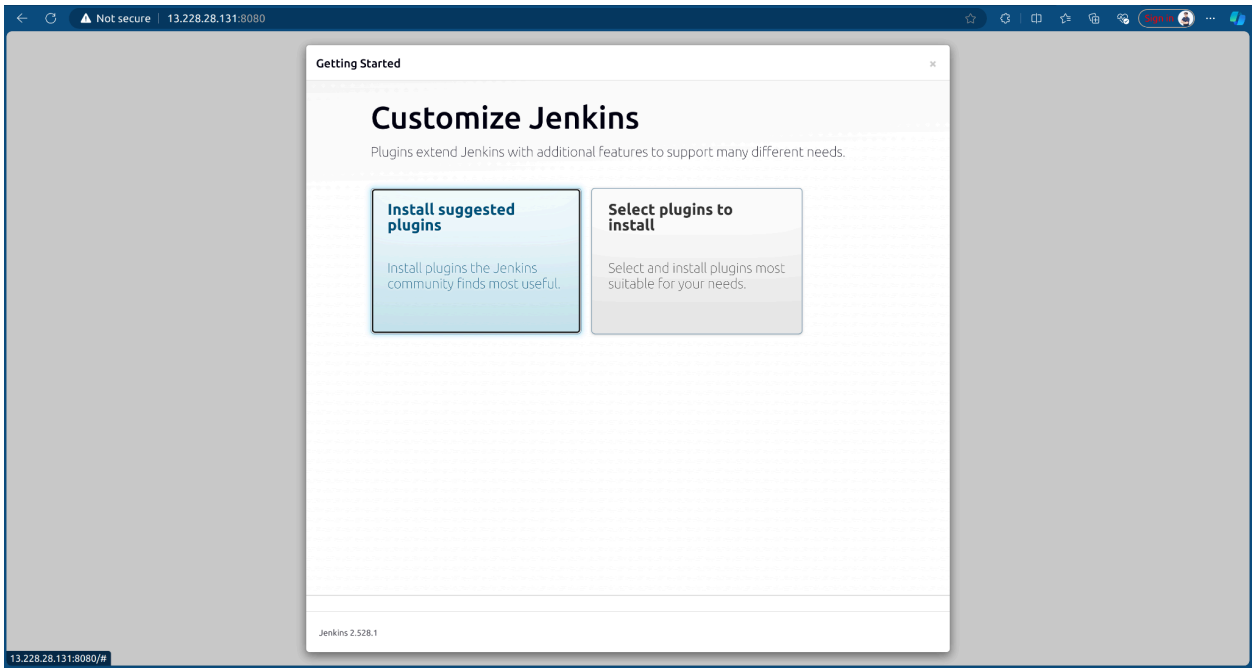


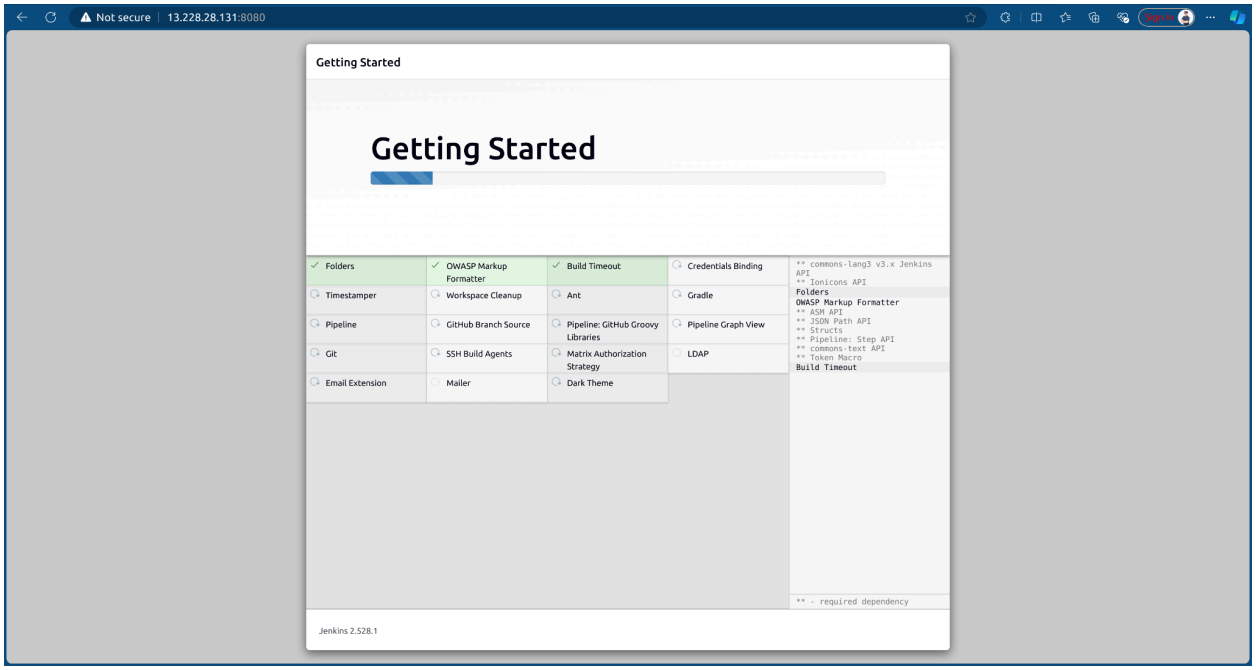
Retrieve the initial admin password:

sudo cat /var/lib/jenkins/secrets/initialAdminPassword

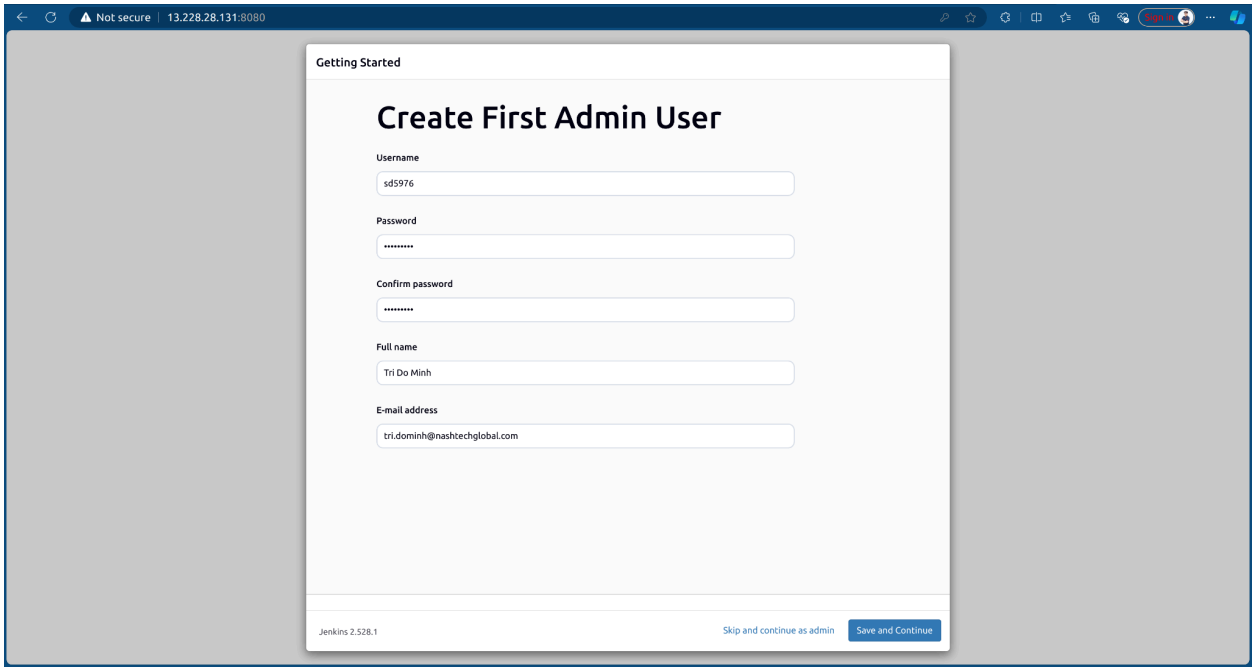


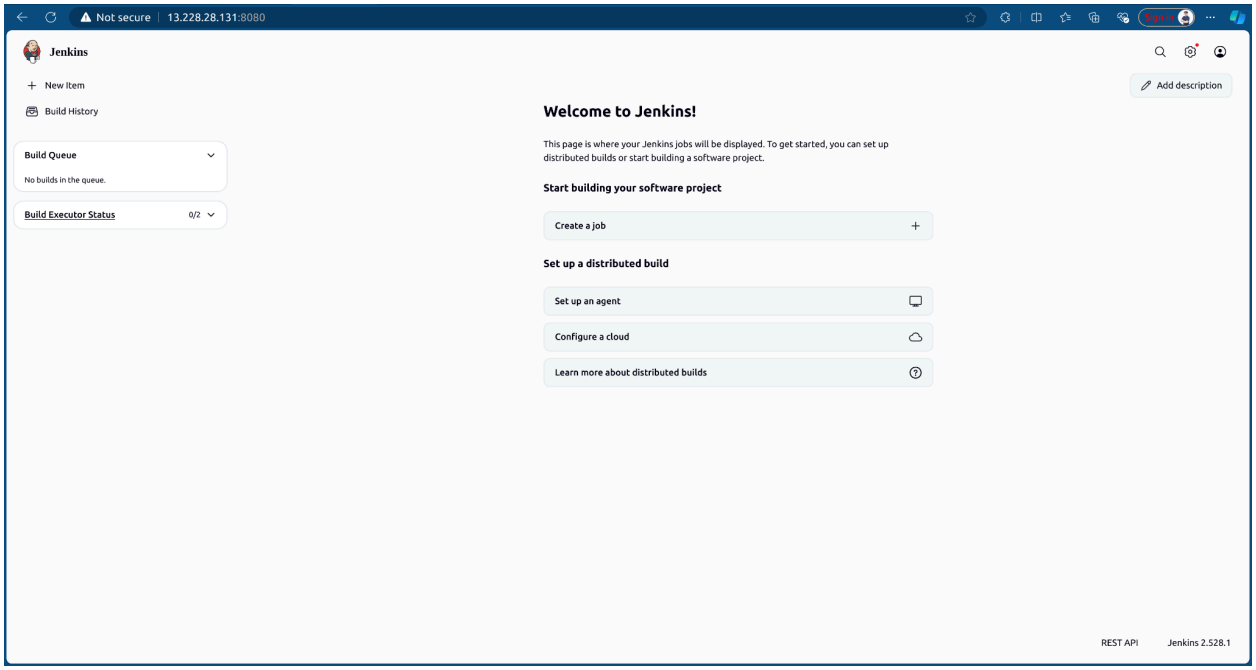
Copy the password and paste it into Jenkins UI, then select **Install suggested plugins**.





After installation, create an Admin User to log in to the dashboard.

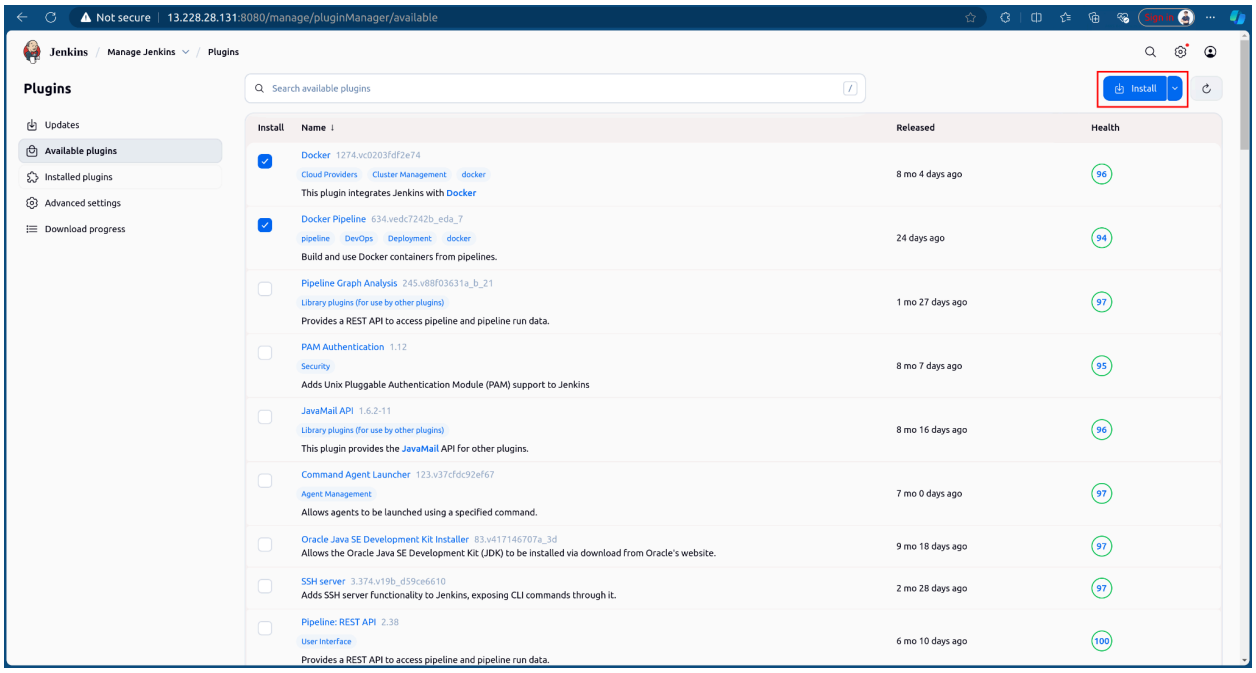




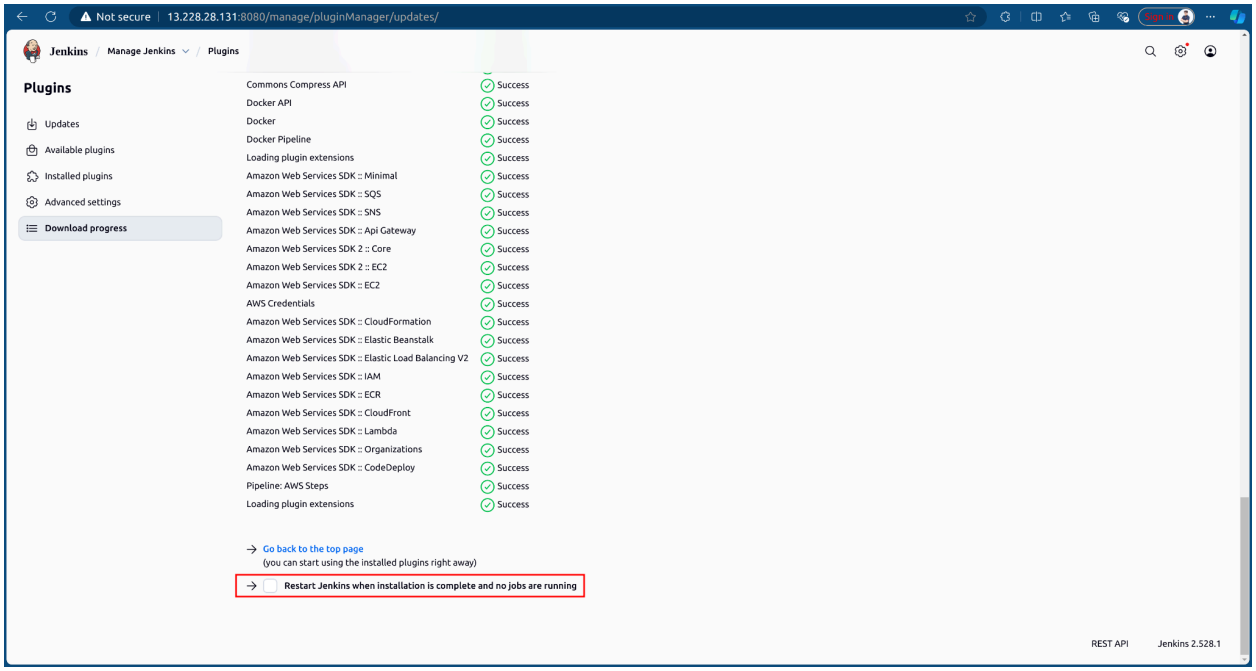
To run CI/CD, we need to install some plugins:

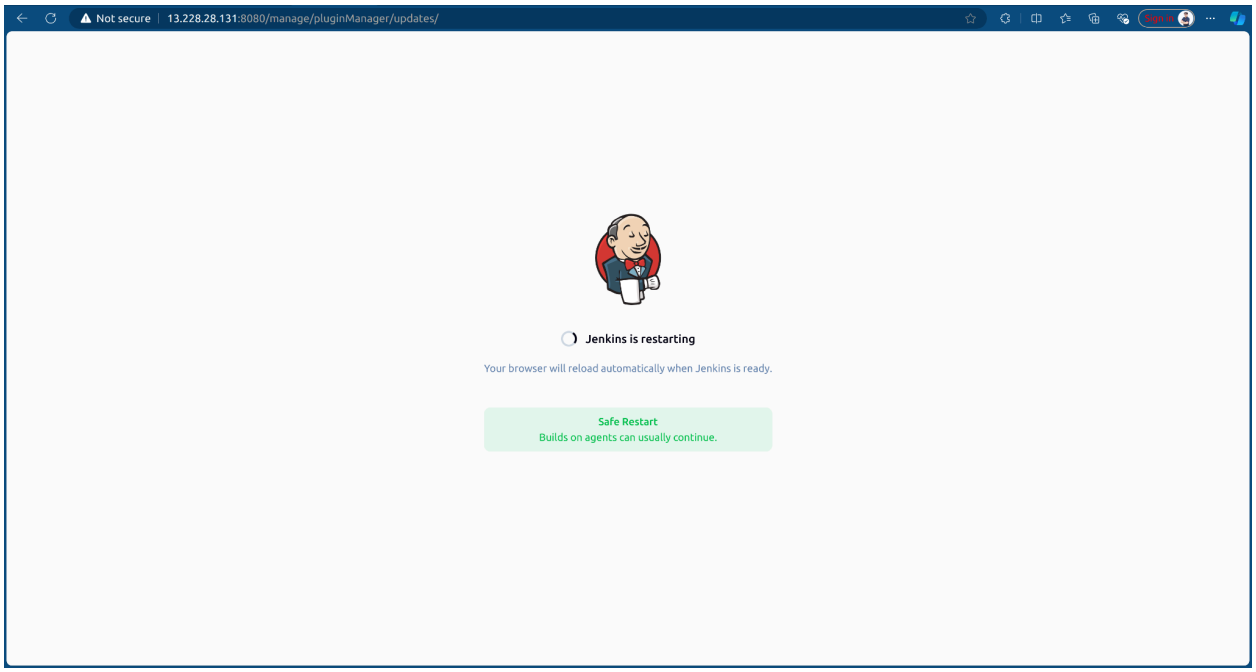
- Docker
- Docker Pipeline
- Pipeline: AWS Steps

Go to **Manage Jenkins → Plugins → Available plugins** tab.



Restart Jenkins after plugin installation.

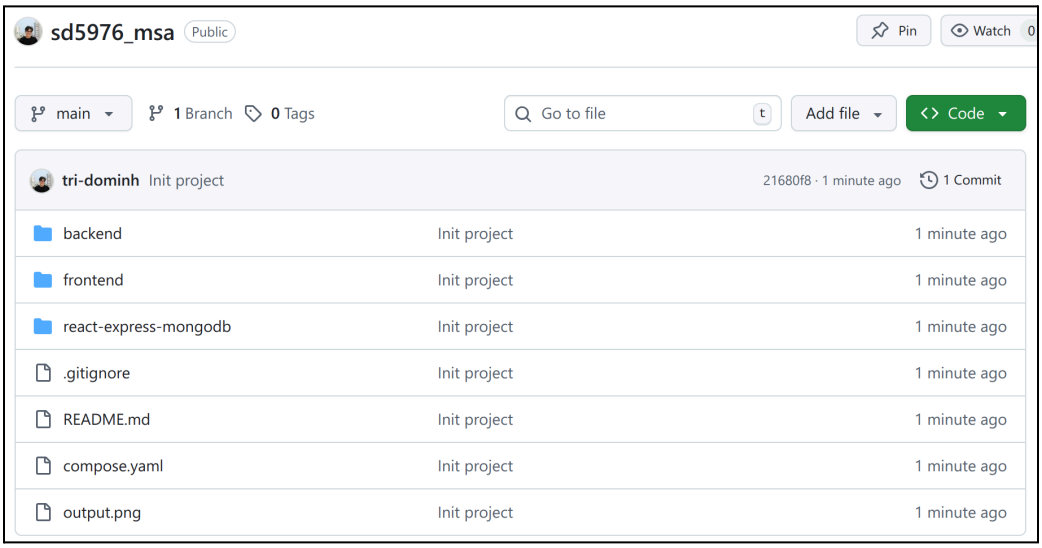




III. Deploying the MSA Application to EKS with Jenkins CI/CD

Prepare the MSA repository containing *frontend* and *backend*:

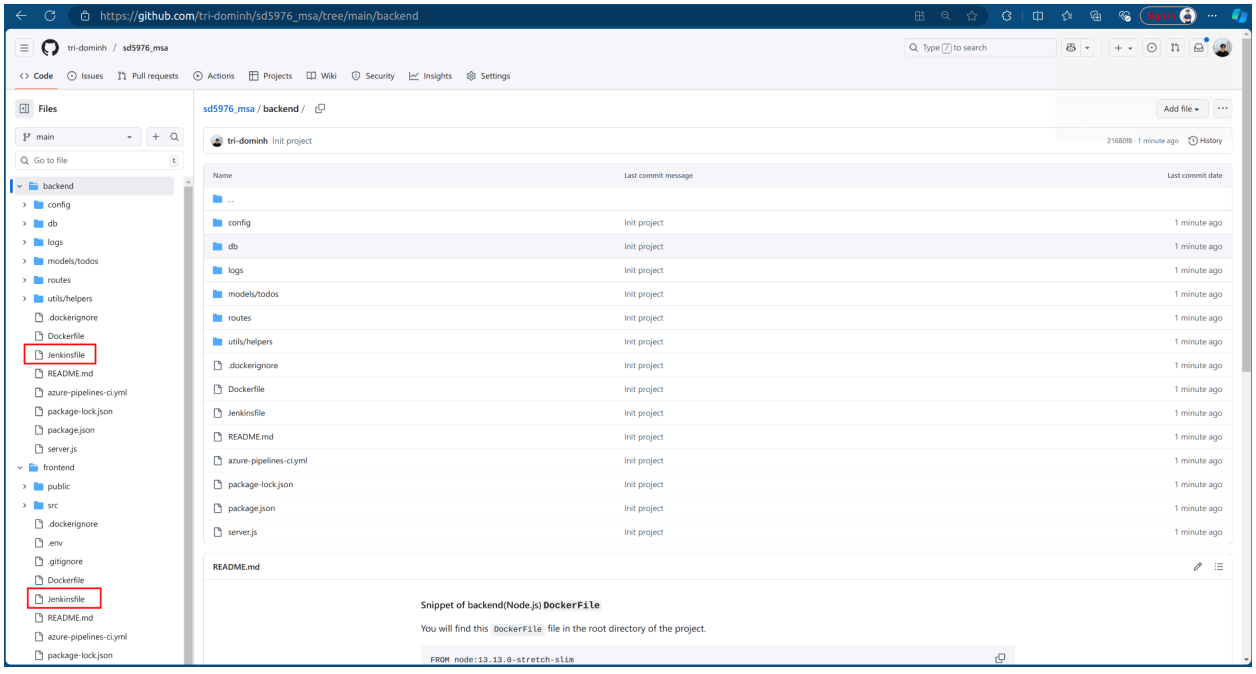
https://github.com/tri-dominh/sd5976_msa



Each source (*frontend*/*backend*) should have a **Jenkinsfile** defining agent and stages: install, build, validate, test, and push to ECR.

https://github.com/tri-dominh/sd5976_msa/blob/main/backend/Jenkinsfile

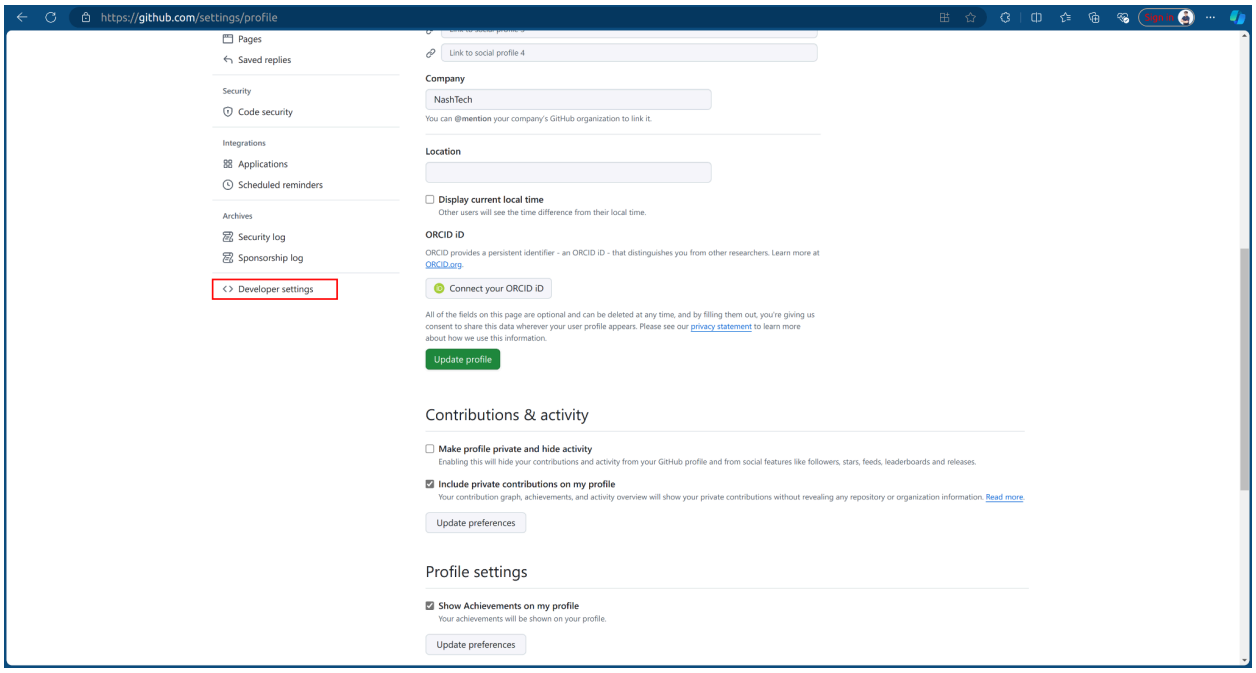
https://github.com/tri-dominh/sd5976_msa/blob/main/frontend/Jenkinsfile

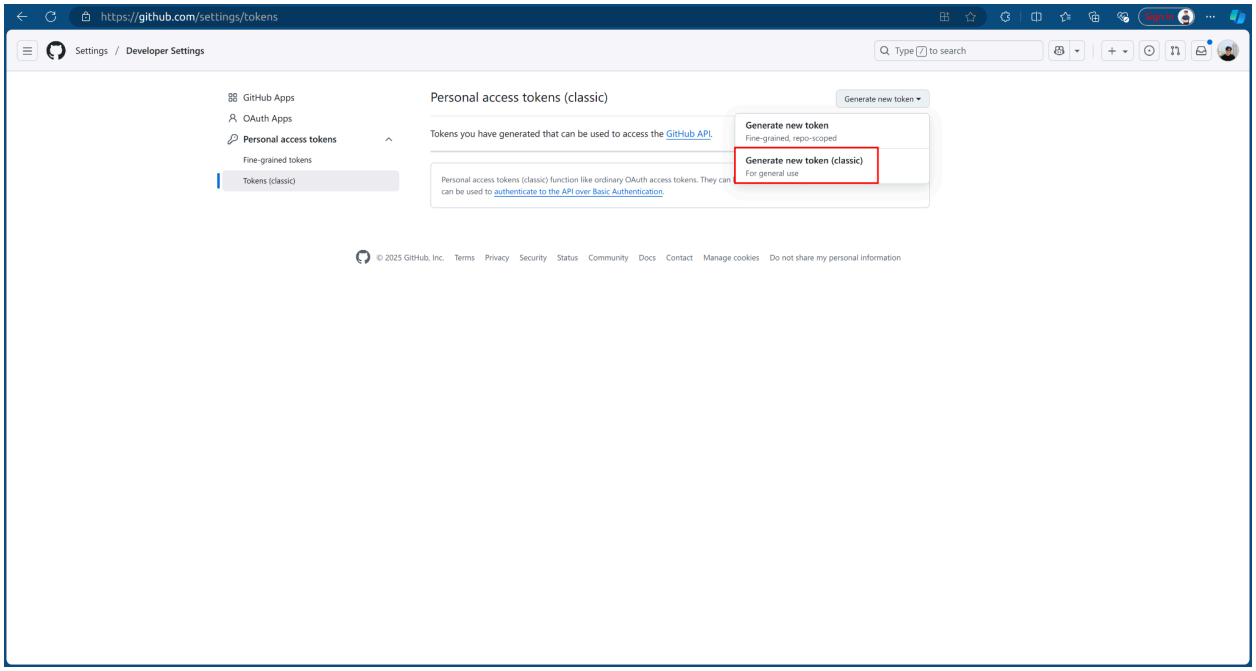


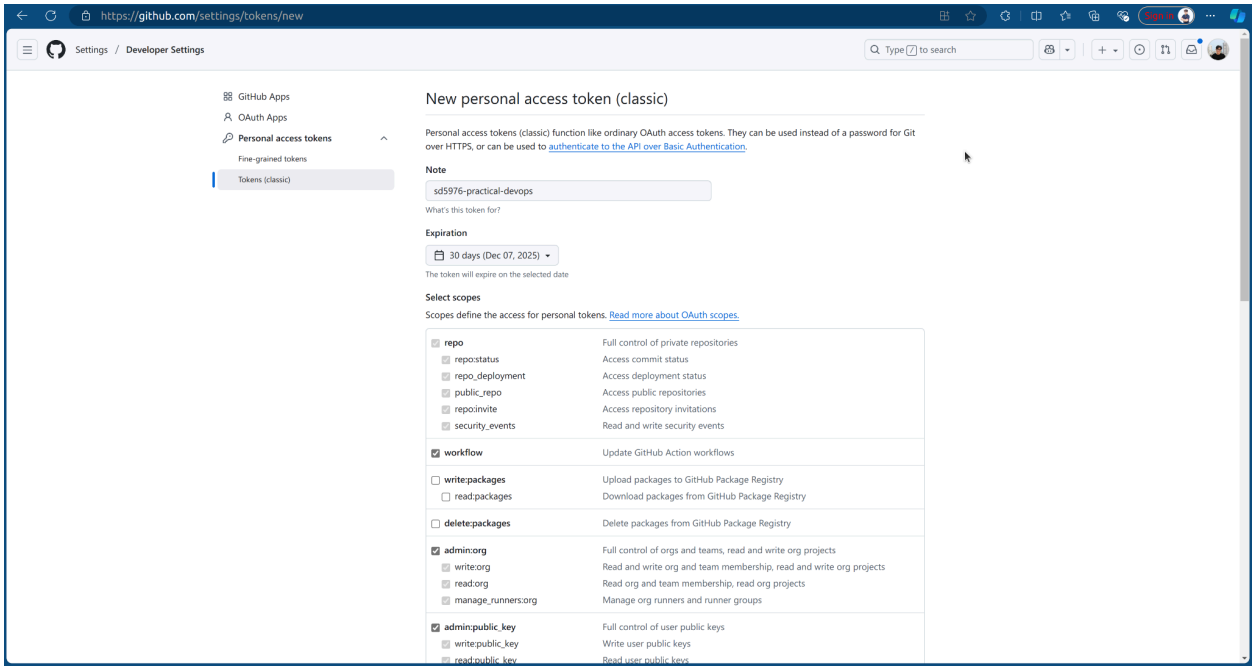
Next, we need to configure Jenkins to access GitHub and AWS resources.

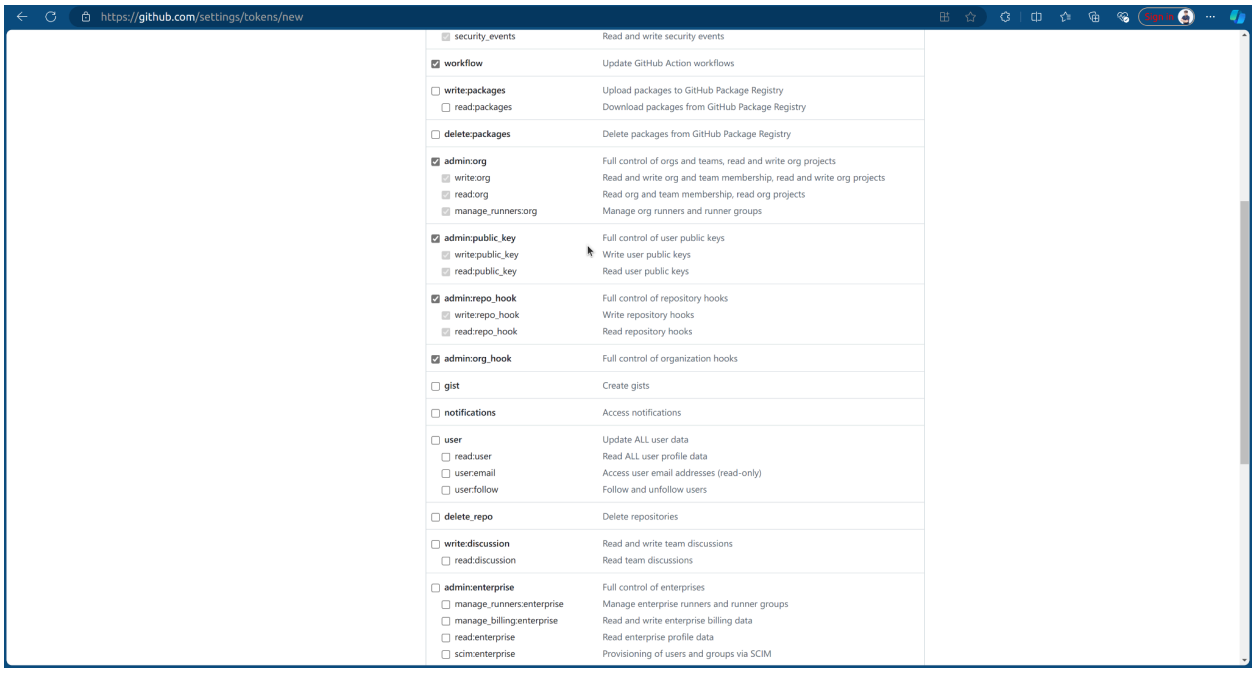
Create a GitHub Access Token for Jenkins to access the MSA repository.

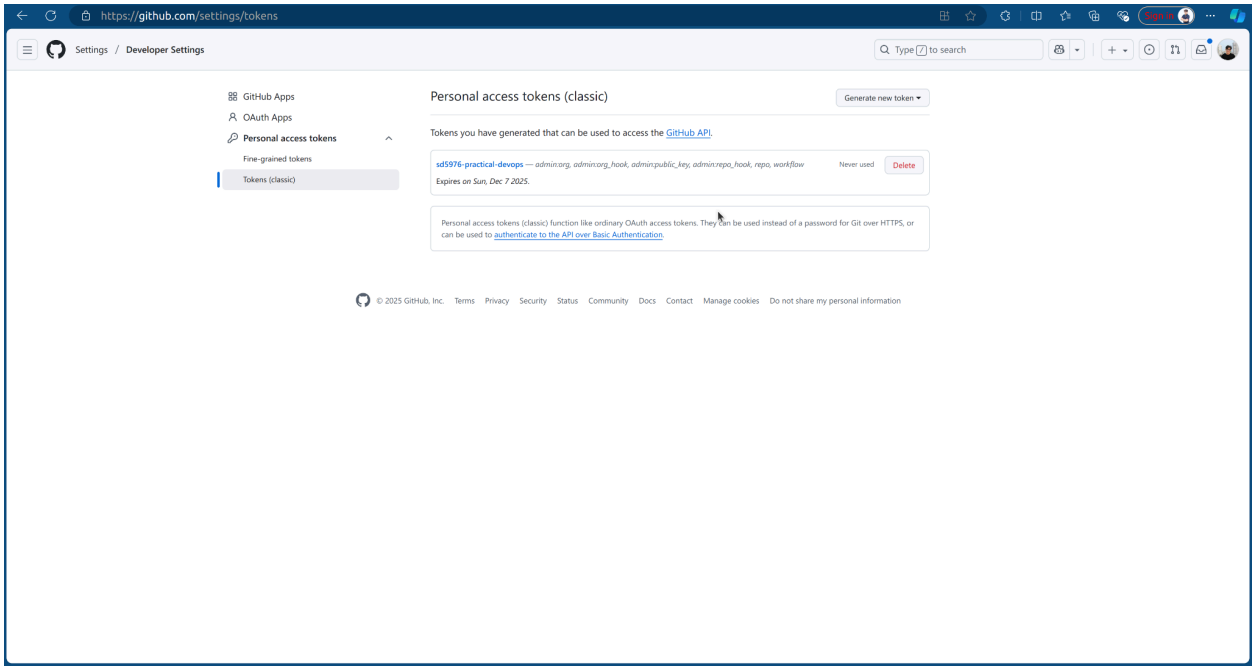
Go to **Settings → Developer settings → Personal access tokens → Tokens (classic) → Generate new token (classic)** → Enter token name and select scopes to allow Jenkins access to GitHub → Create.

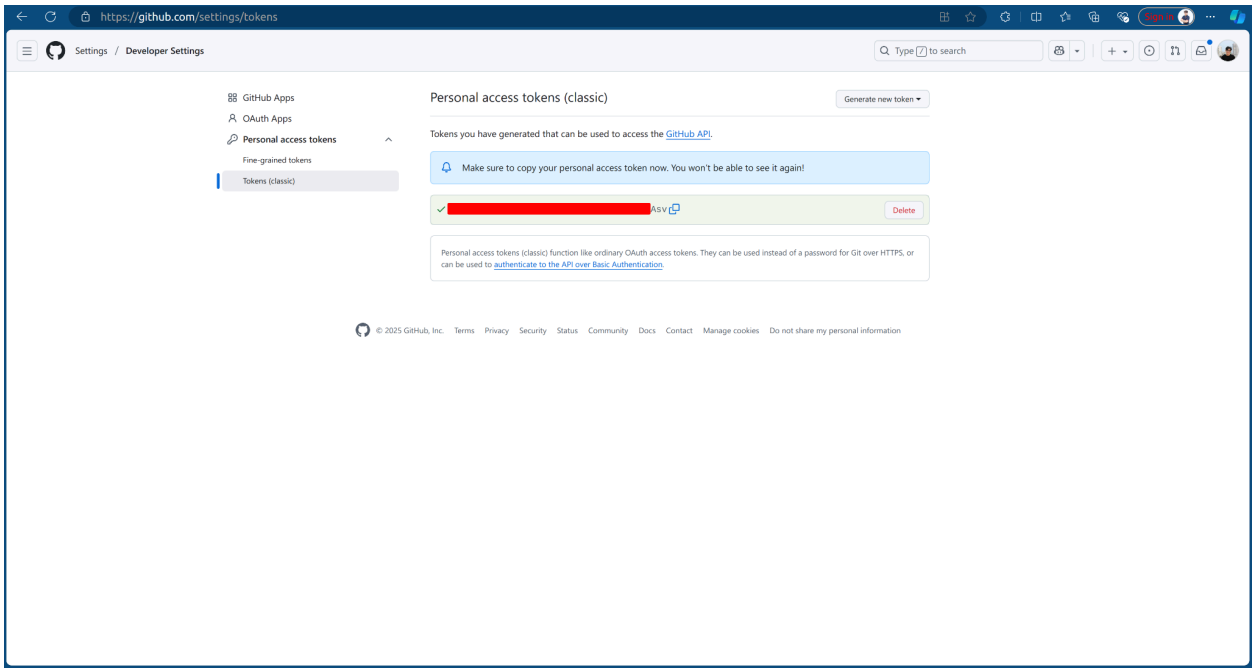




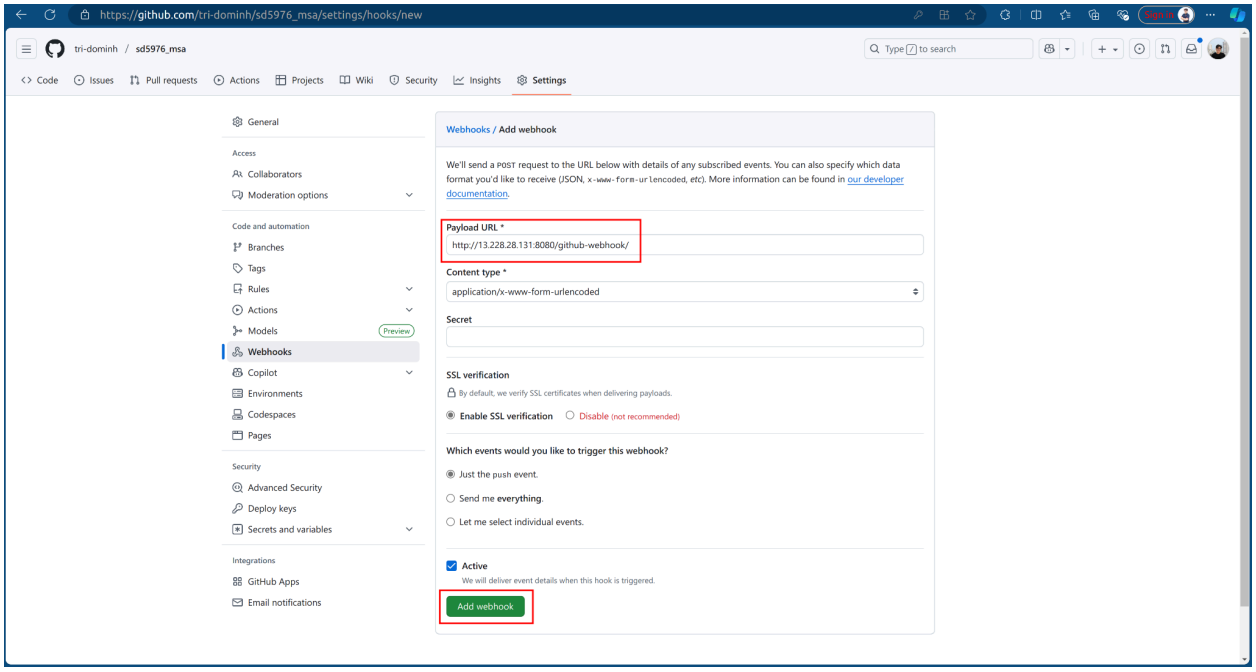

https://github.com/settings/tokens/new
Settings / Developer Settings
Type / to search
GitHub Apps
OAuth Apps
Personal access tokens
Fine-grained tokens
Tokens (classic)
New personal access token (classic)
Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.
Note
sd5976-practical-devops
What's this token for?
Expiration
30 days (Dec 07, 2025)
The token will expire on the selected date
Select scopes
Scopes define the access for personal tokens. Read more about OAuth scopes.
repo Full control of private repositories
repo:status Access commit status
repo_deployment Access deployment status
public_repo Access public repositories
repo:invite Access repository invitations
security_events Read and write security events
workflow Update GitHub Action workflows
write:packages Upload packages to GitHub Package Registry
read:packages Download packages from GitHub Package Registry
delete:packages Delete packages from GitHub Package Registry
admin:org Full control of orgs and teams, read and write org projects
write:org Read and write org and team membership, read and write org projects
read:org Read org and team membership, read org projects
manage_runners:org Manage org runners and runner groups
admin:public_key Full control of user public keys
write:public_key Write user public keys
read:public_key Read user public keys


https://github.com/settings/tokens/new
security_events Read and write security events
workflow Update GitHub Action workflows
write:packages Upload packages to GitHub Package Registry
read:packages Download packages from GitHub Package Registry
delete:packages Delete packages from GitHub Package Registry
admin:org Full control of orgs and teams, read and write org projects
write:org Read and write org and team membership, read and write org projects
read:org Read org and team membership, read org projects
manage_runners:org Manage org runners and runner groups
admin:public_key Full control of user public keys
write:public_key Write user public keys
read:public_key Read user public keys
admin:repo_hook Full control of repository hooks
write:repo_hook Write repository hooks
read:repo_hook Read repository hooks
admin:org_hook Full control of organization hooks
gist Create gists
notifications Access notifications
user Update ALL user data
read:user Read ALL user profile data
user:email Access user email addresses (read-only)
user:follow Follow and unfollow users
delete_repo Delete repositories
write:discussion Read and write team discussions
read:discussion Read team discussions
admin:enterprise Full control of enterprises
manage_runners:enterprise Manage enterprise runners and runner groups
manage_billing:enterprise Read and write enterprise billing data
read:enterprise Read enterprise profile data
scim:enterprise Provisioning of users and groups via SCIM


https://github.com/settings/tokens
Settings / Developer Settings
Type / to search
GitHub Apps
OAuth Apps
Personal access tokens
Fine-grained tokens
Tokens (classic)
Personal access tokens (classic)
Generate new token
Tokens you have generated that can be used to access the GitHub API.
sd5976-practical-devops — admin:org, admin:org_hook, admin:public_key, admin:repo_hook, repo, workflow
Never used
Delete
Expires on Sun, Dec 7 2025.
Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.
© 2025 GitHub, Inc. Terms Privacy Security Status Community Docs Contact Manage cookies Do not share my personal information

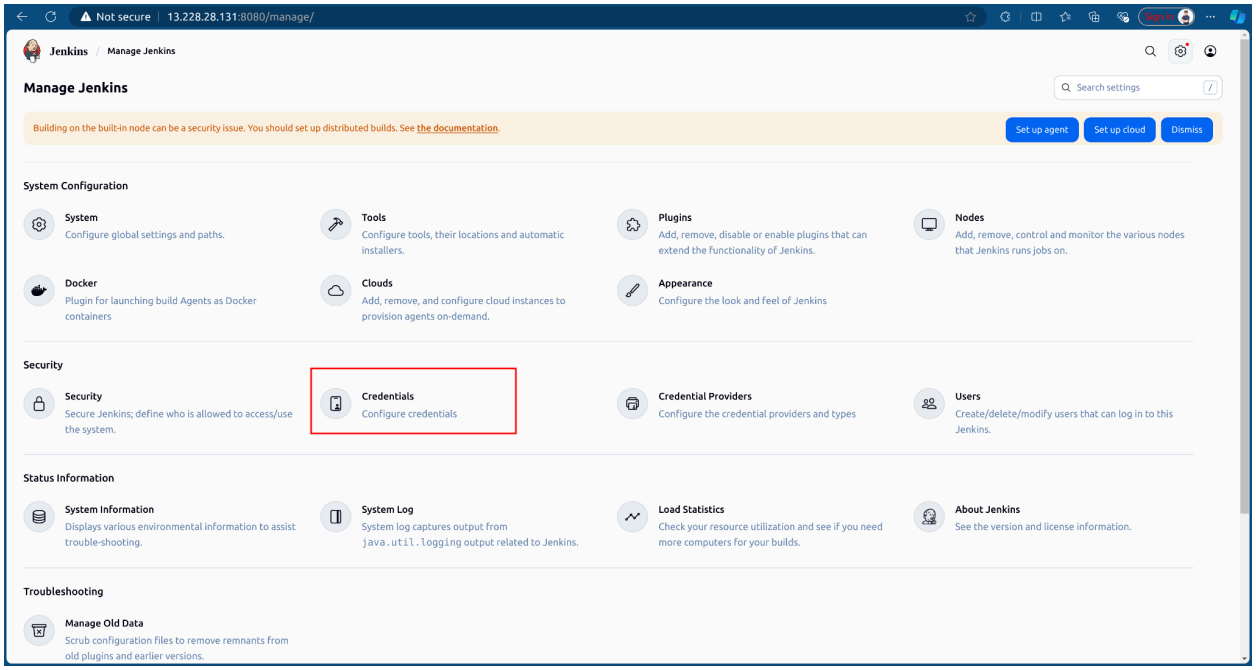

https://github.com/settings/tokens
Settings / Developer Settings
Type / to search
GitHub Apps
OAuth Apps
Personal access tokens
Fine-grained tokens
Tokens (classic)
Personal access tokens (classic)
Generate new token
Tokens you have generated that can be used to access the GitHub API.
Make sure to copy your personal access token now. You won't be able to see it again!
[redacted]Asv
Delete
Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.
© 2025 GitHub, Inc. Terms Privacy Security Status Community Docs Contact Manage cookies Do not share my personal information

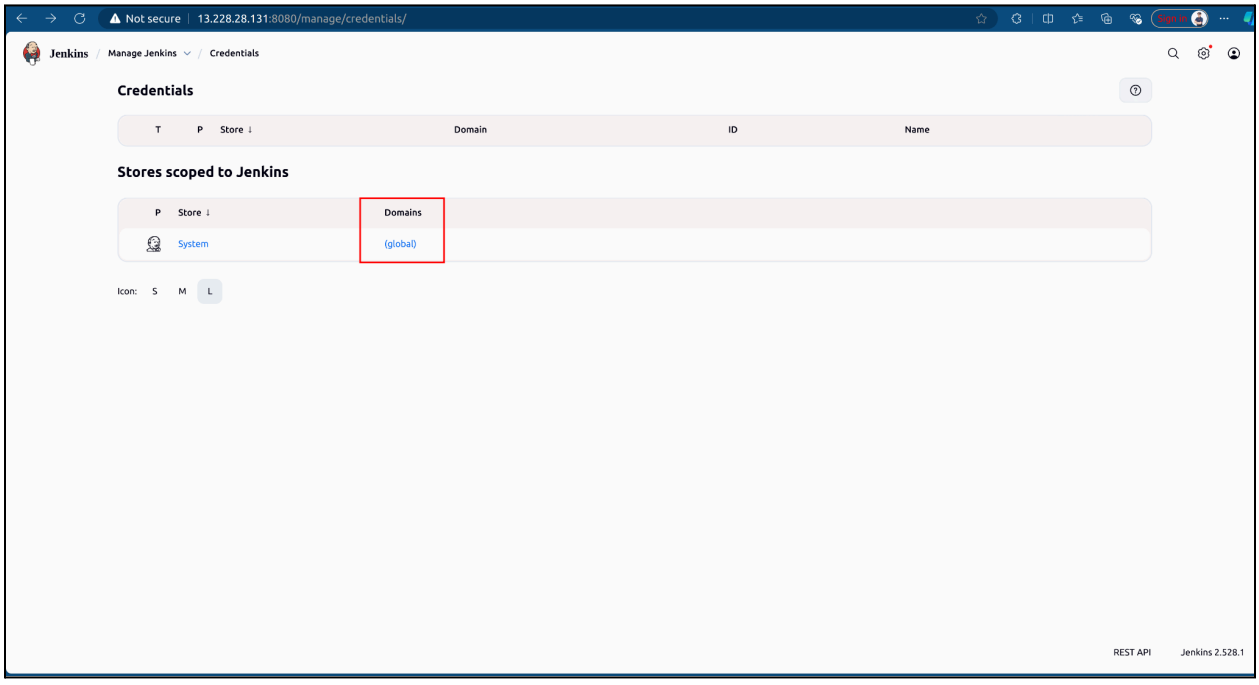
Then, we create a Github webhook to trigger Jenkins whenever we push new code. In the **sd5976-msa** repo, go to **Settings → Webhooks → Add webhook**, enter the Jenkins URL with */github-webhook/*

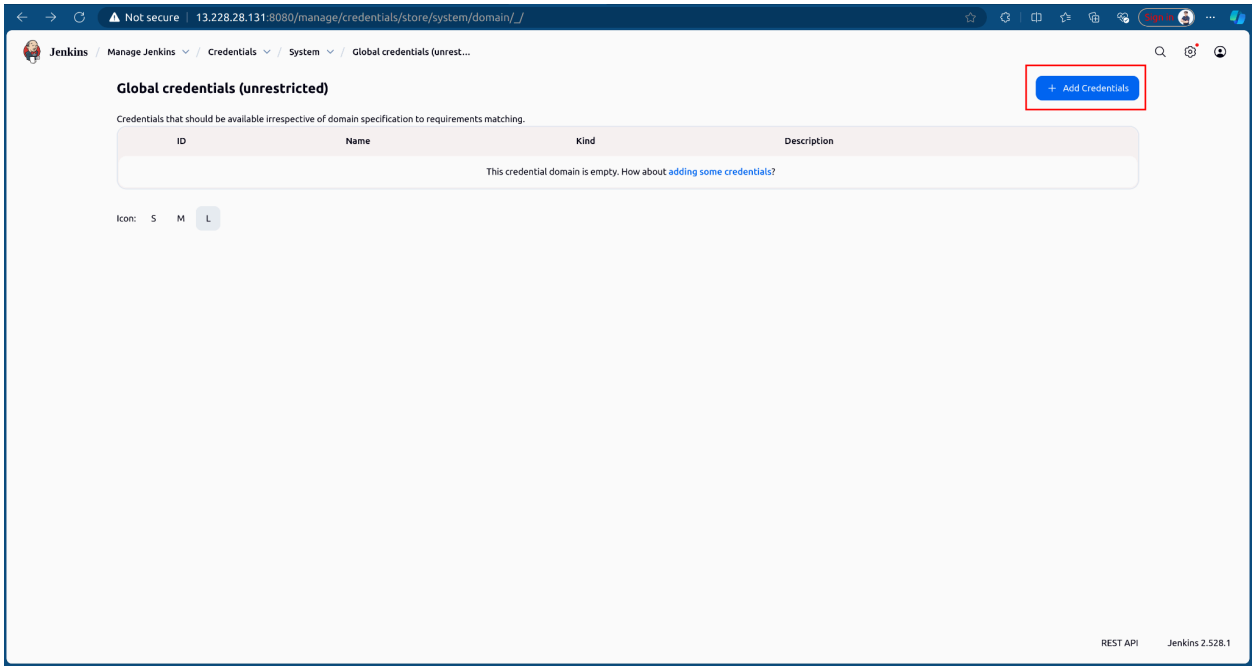


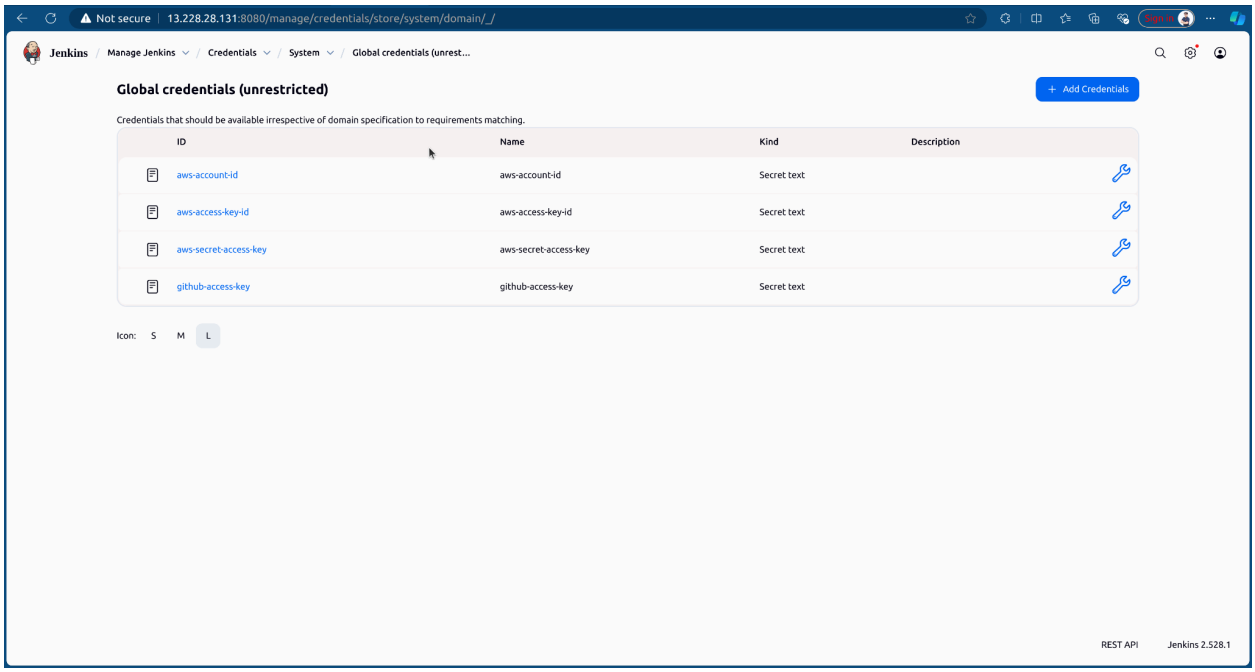
After that, we create the credentials in Jenkins which allow Jenkins access to Resources. Go to **Jenkins Credentials** → Click on **(global)** → **Add Credentials** (*Secret text* kind).

- AWS Account ID, AWS Access Key ID, AWS Secret Access Key.
- GitHub Token.

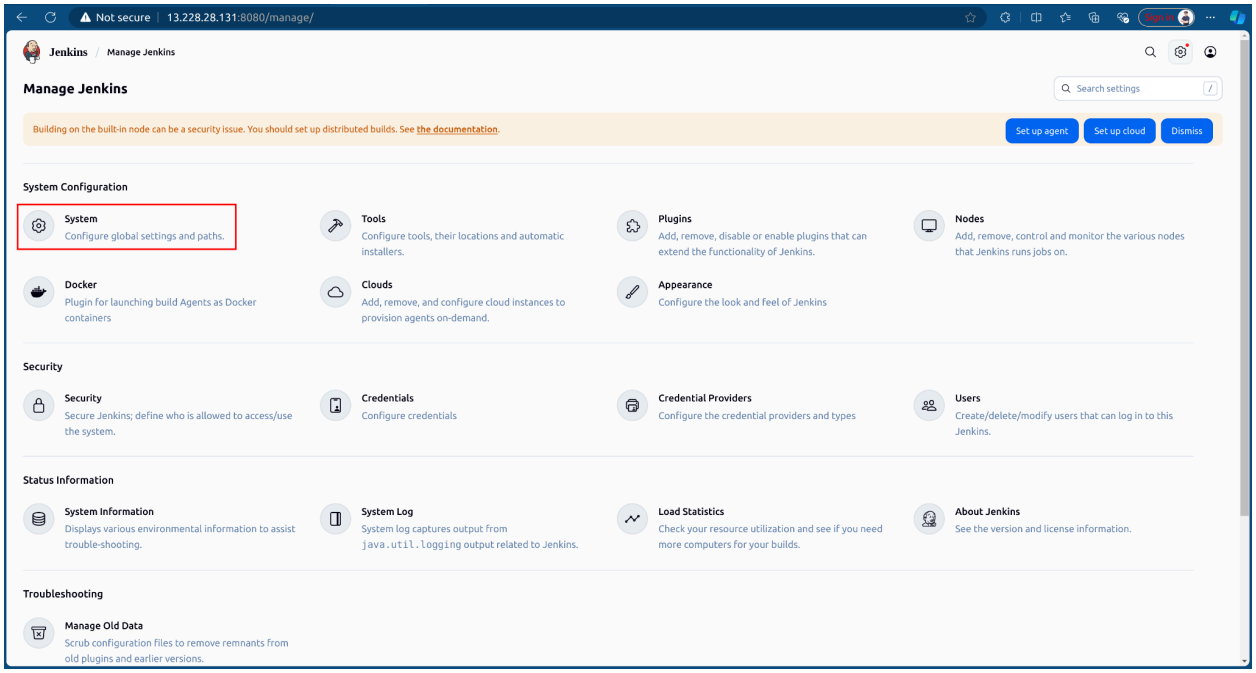

Not secure | 13.228.28.131:8080/manage/
Jenkins / Manage Jenkins
Manage Jenkins
Search settings
Building on the built-in node can be a security issue. You should set up distributed builds. See the documentation.
Set up agent
Set up cloud
Dismiss
System Configuration
System
Configure global settings and paths.
Tools
Configure tools, their locations and automatic installers.
Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins.
Nodes
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.
Docker
Plugin for launching build Agents as Docker containers
Clouds
Add, remove, and configure cloud instances to provision agents on-demand.
Appearance
Configure the look and feel of Jenkins
Security
Security
Secure Jenkins; define who is allowed to access/use the system.
Credentials
Configure credentials
Credential Providers
Configure the credential providers and types
Users
Create/delete/modify users that can log in to this Jenkins.
Status Information
System Information
Displays various environmental information to assist trouble-shooting.
System Log
System log captures output from java.util.logging output related to Jenkins.
Load Statistics
Check your resource utilization and see if you need more computers for your builds.
About Jenkins
See the version and license information.
Troubleshooting
Manage Old Data
Scrub configuration files to remove remnants from old plugins and earlier versions.

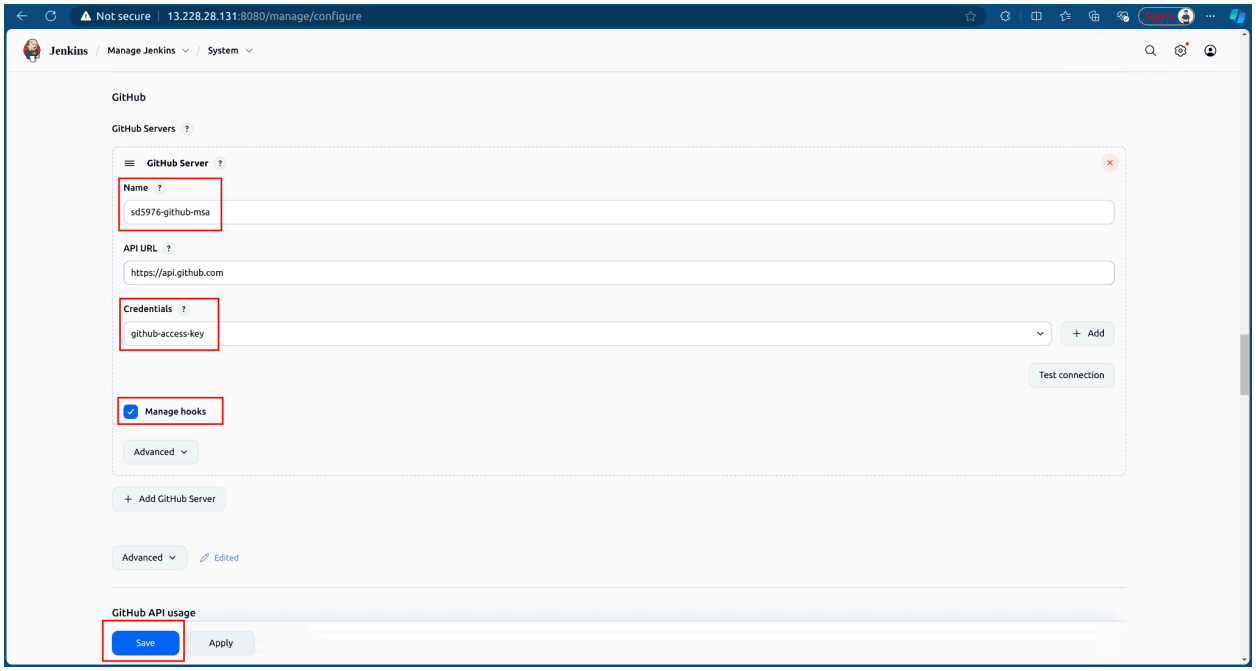

Not secure | 13.228.28.131:8080/manage/credentials/
Jenkins / Manage Jenkins / Credentials
Credentials
T
P
Store ↓
Domain
ID
Name
Stores scoped to Jenkins
P
Store ↓
Domains
System
(global)
Icon: S M L
REST API
Jenkins 2.528.1


Not secure | 13.228.28.131:8080/manage/credentials/store/system/domain/_/
Jenkins / Manage Jenkins / Credentials / System / Global credentials (unrest...
Global credentials (unrestricted)
+ Add Credentials
Credentials that should be available irrespective of domain specification to requirements matching.
ID
Name
Kind
Description
This credential domain is empty. How about adding some credentials?
Icon: S M L
REST API
Jenkins 2.528.1


Not secure | 13.228.28.131:8080/manage/credentials/store/system/domain/_/
Jenkins / Manage Jenkins / Credentials / System / Global credentials (unrest...
Global credentials (unrestricted)
+ Add Credentials
Credentials that should be available irrespective of domain specification to requirements matching.
ID
Name
Kind
Description
aws-account-id
aws-account-id
Secret text
aws-access-key-id
aws-access-key-id
Secret text
aws-secret-access-key
aws-secret-access-key
Secret text
github-access-key
github-access-key
Secret text
Icon: S M L
REST API
Jenkins 2.528.1

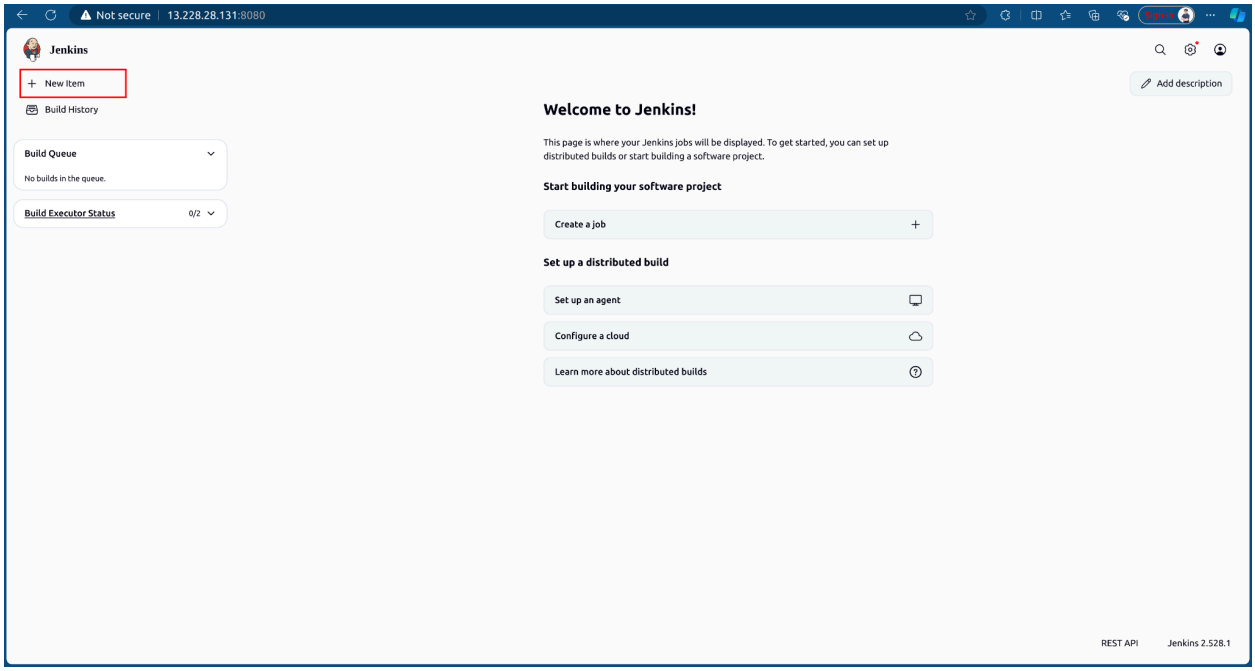
Add GitHub Server for Jenkins, go to **Settings** → **System** → In **GitHub** section → **Add GitHub Server** → Enter name, select credentials **github-access-key** and tick **Manage hooks** → Save.

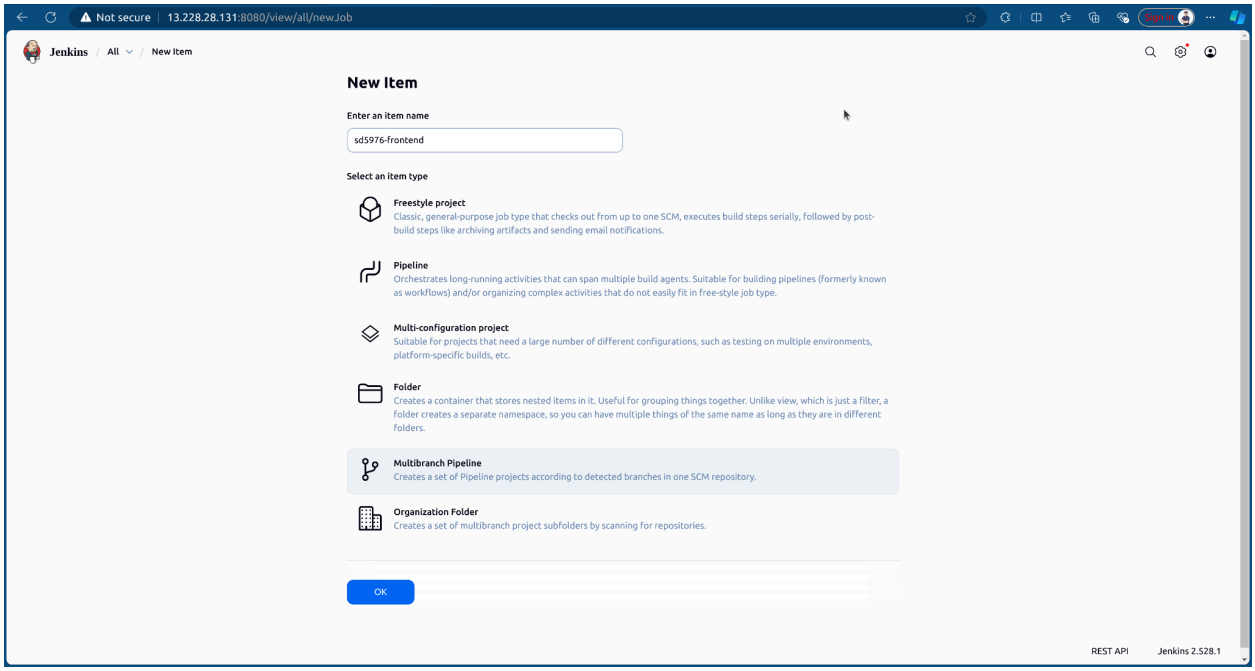




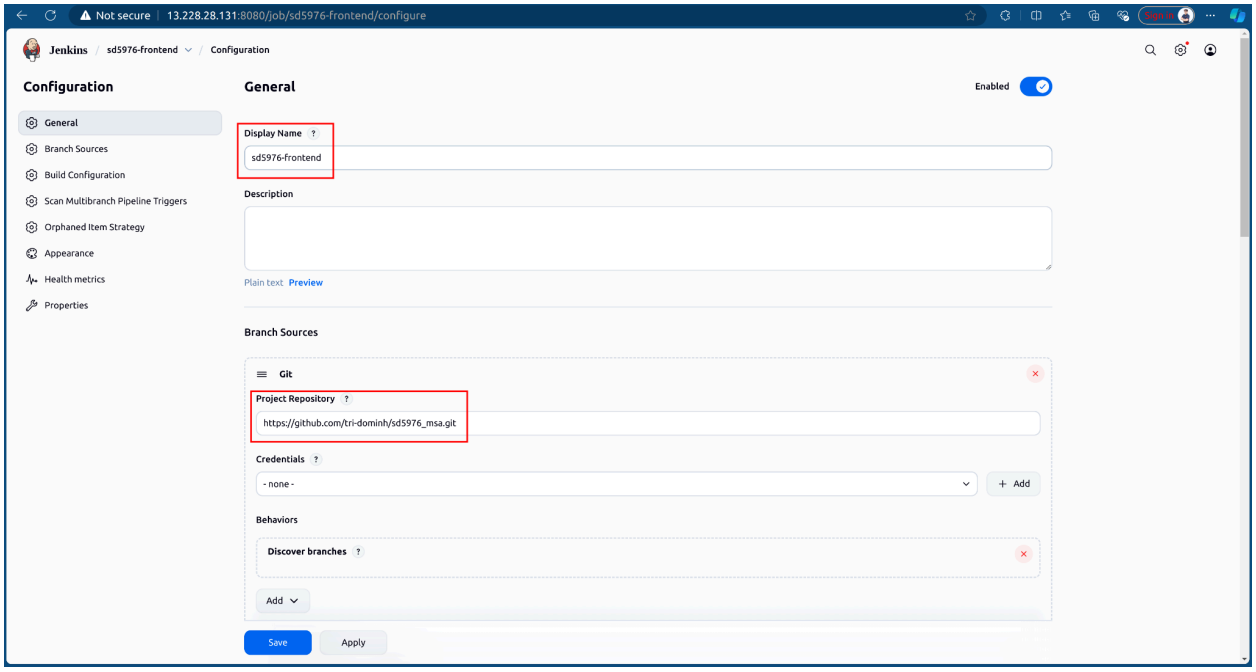
IV. Creating CI jobs for MSA Application

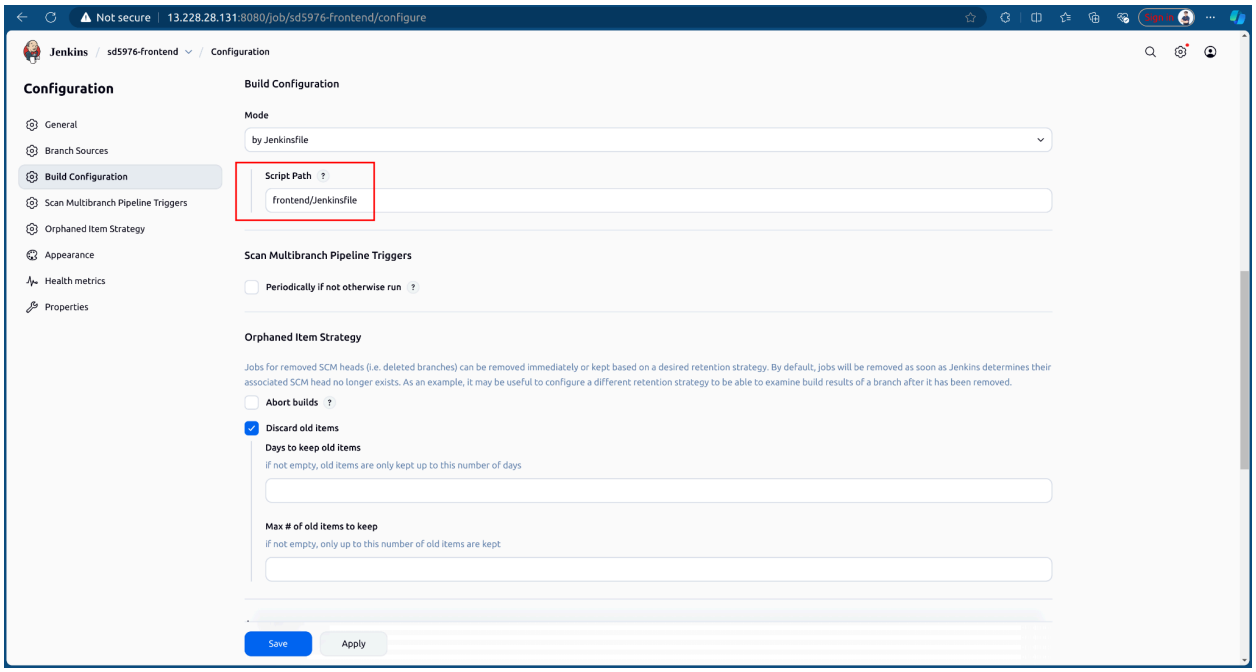
First, we build a job for the *Frontend*, click **New item** → Enter name and select **Multibranch pipeline** job.



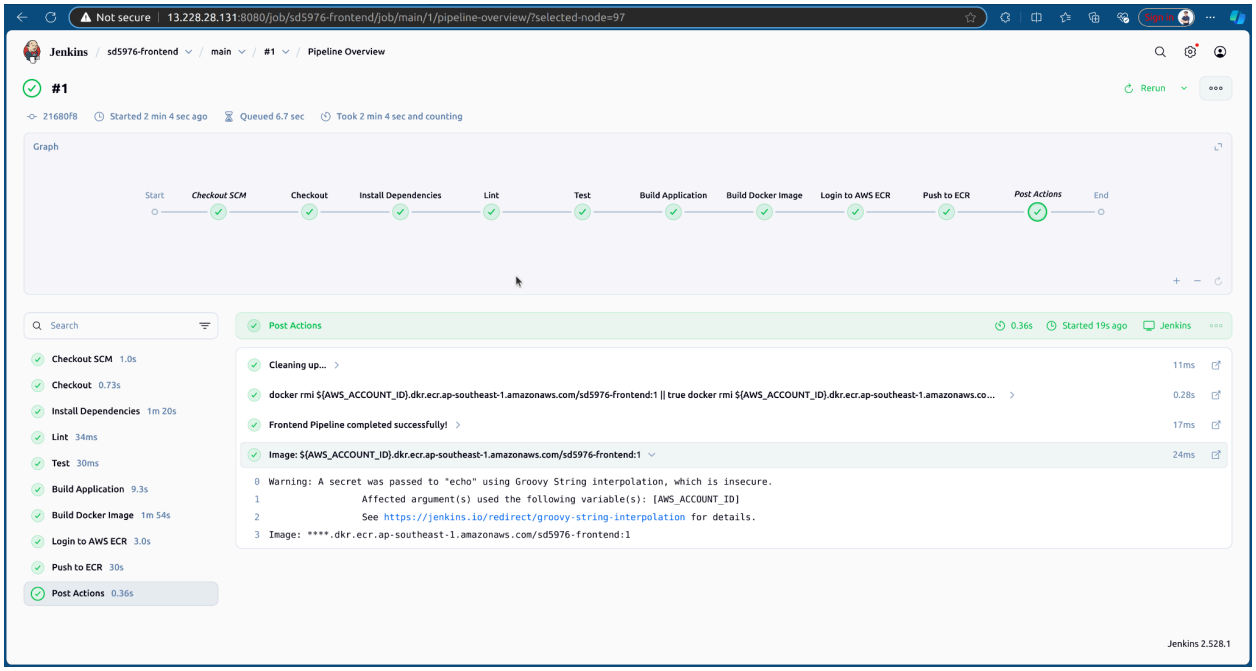


Configure Jenkins job to point to the *Frontend* branch and Jenkinsfile of *Frontend*.

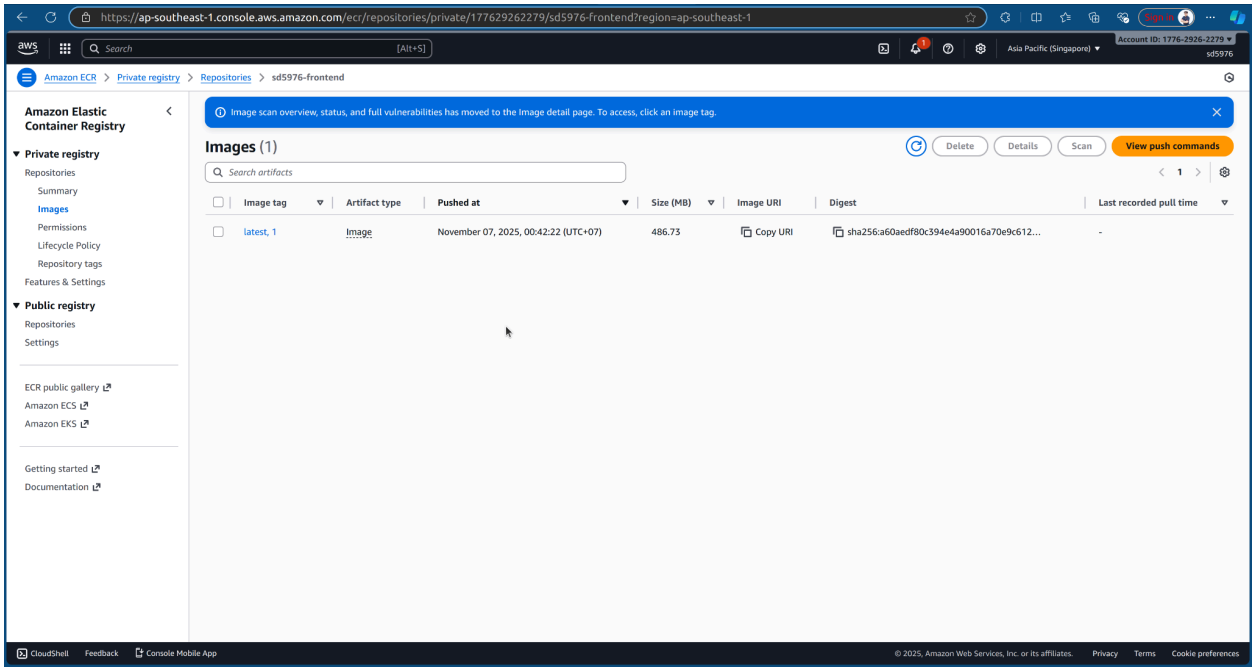




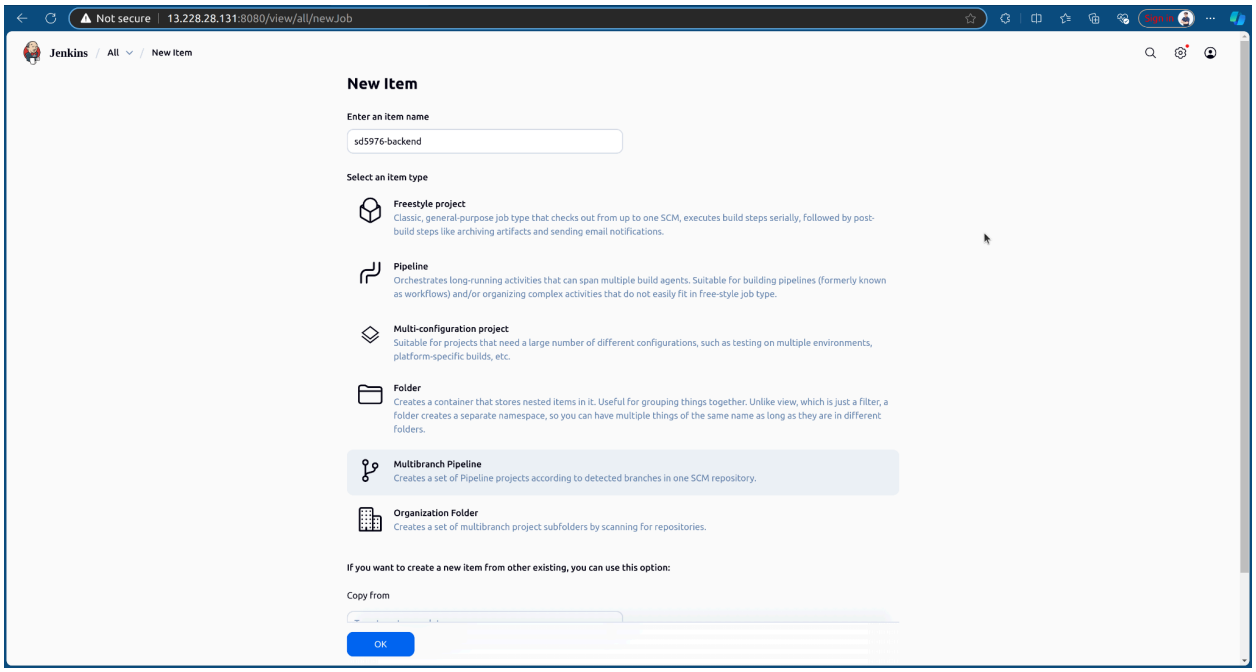
After creating, the job will run Jenkins based on the Jenkinsfile and source.



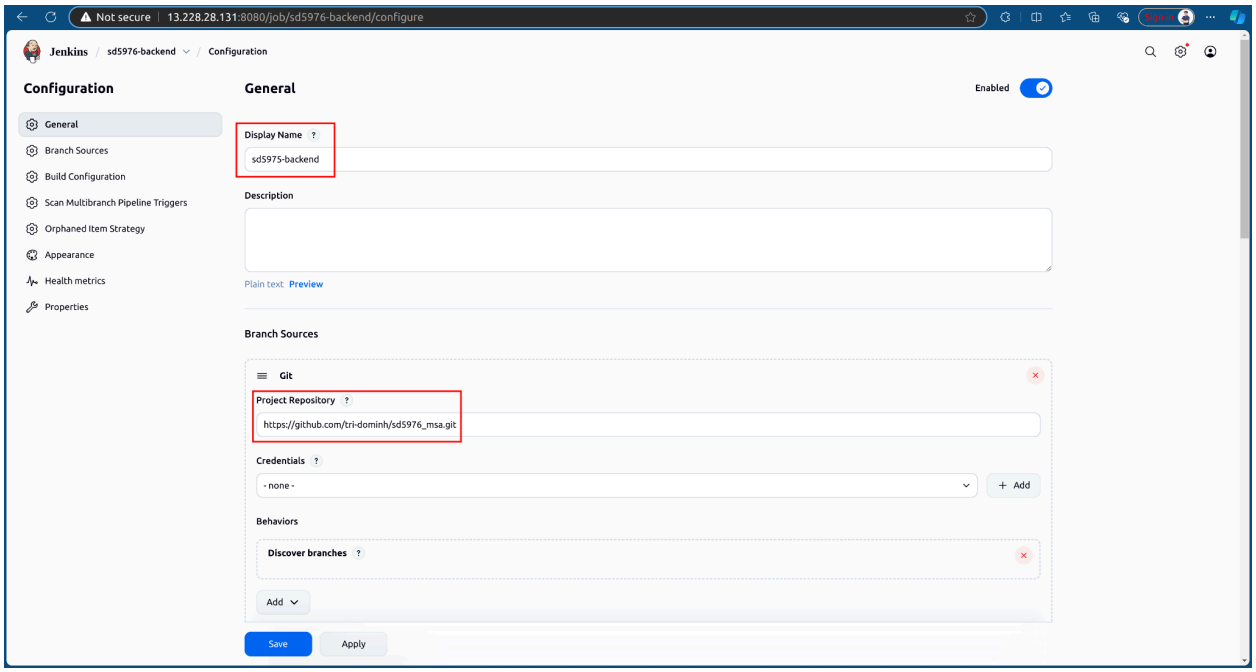
CI will run and push the *Frontend* image to ECR.

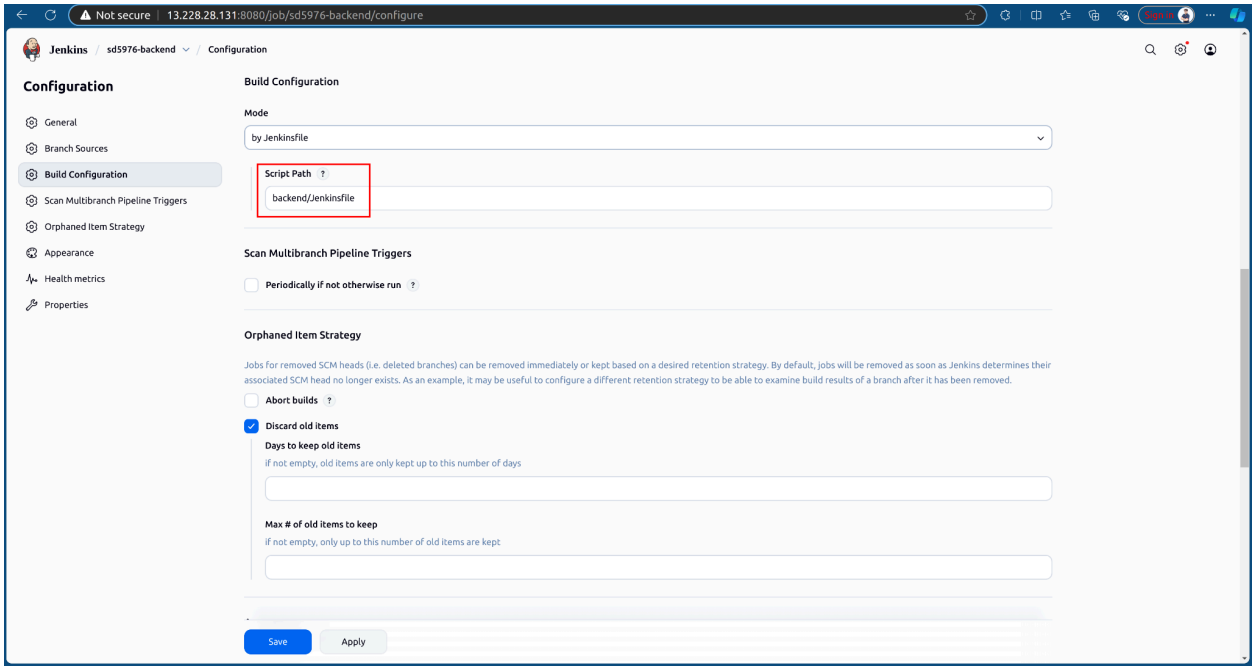


Next, we will create a similar job for the *Backend*, click **New item** → Enter name and select **Multibranch pipeline** job.

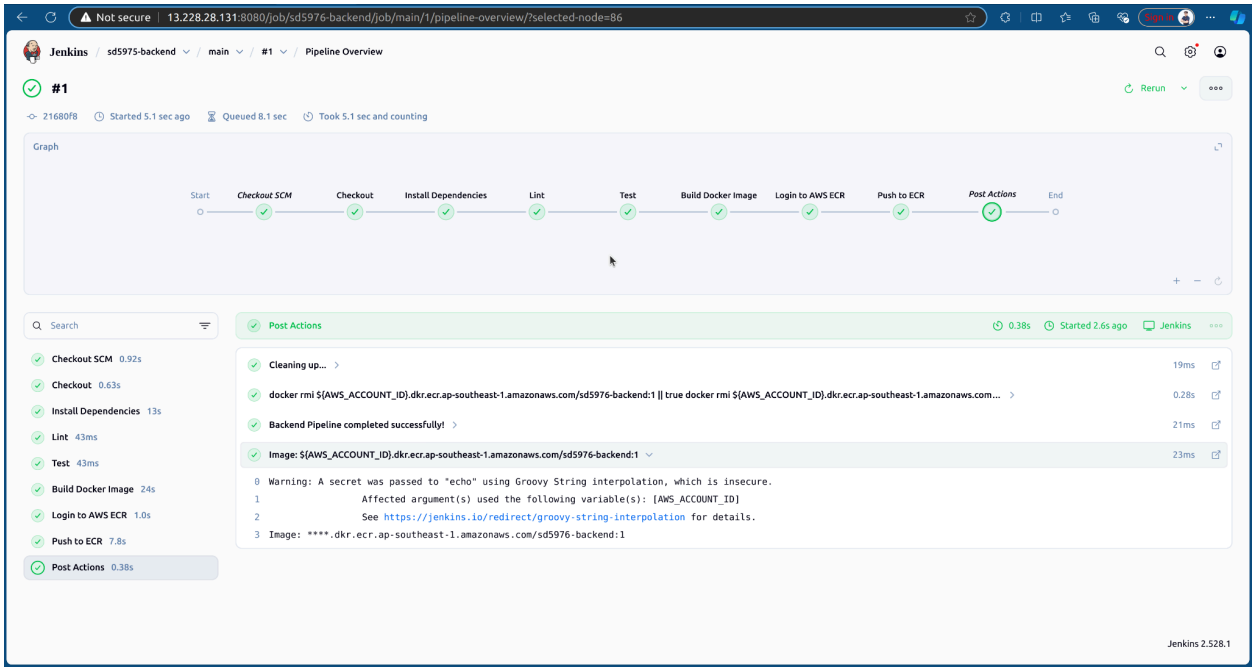


Configure Jenkins job to point to *Backend* branch and Jenkinsfile of *Backend*.

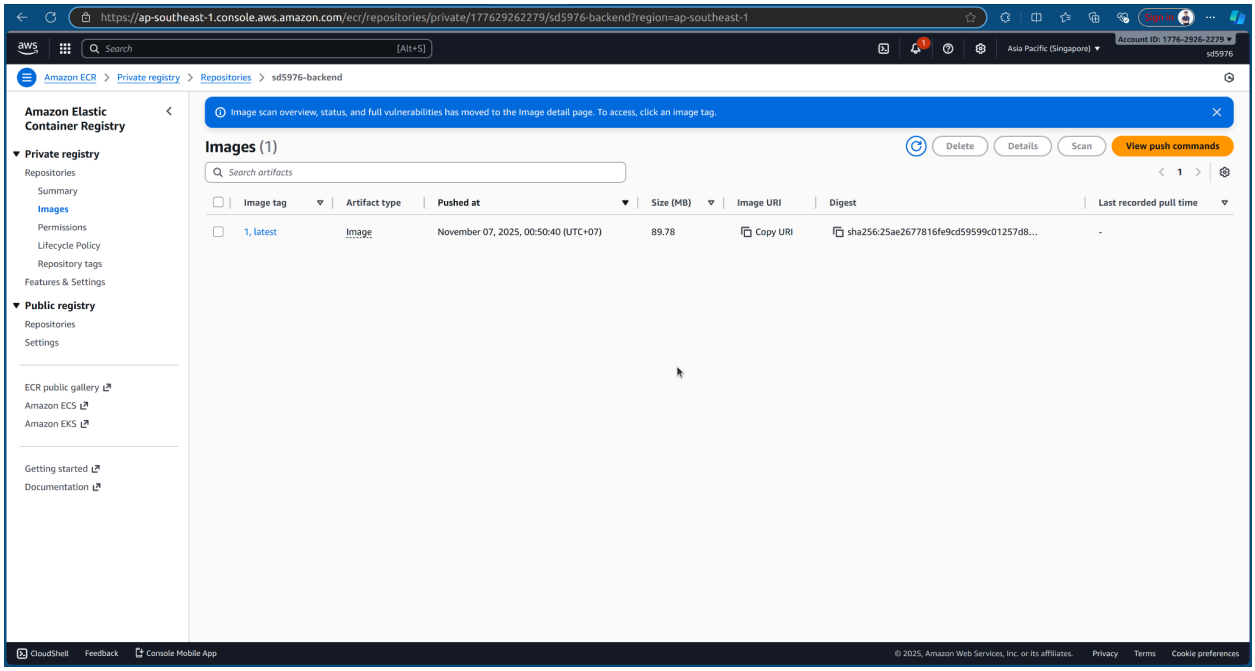




After creating, the job will run Jenkins based on the Jenkinsfile and source.

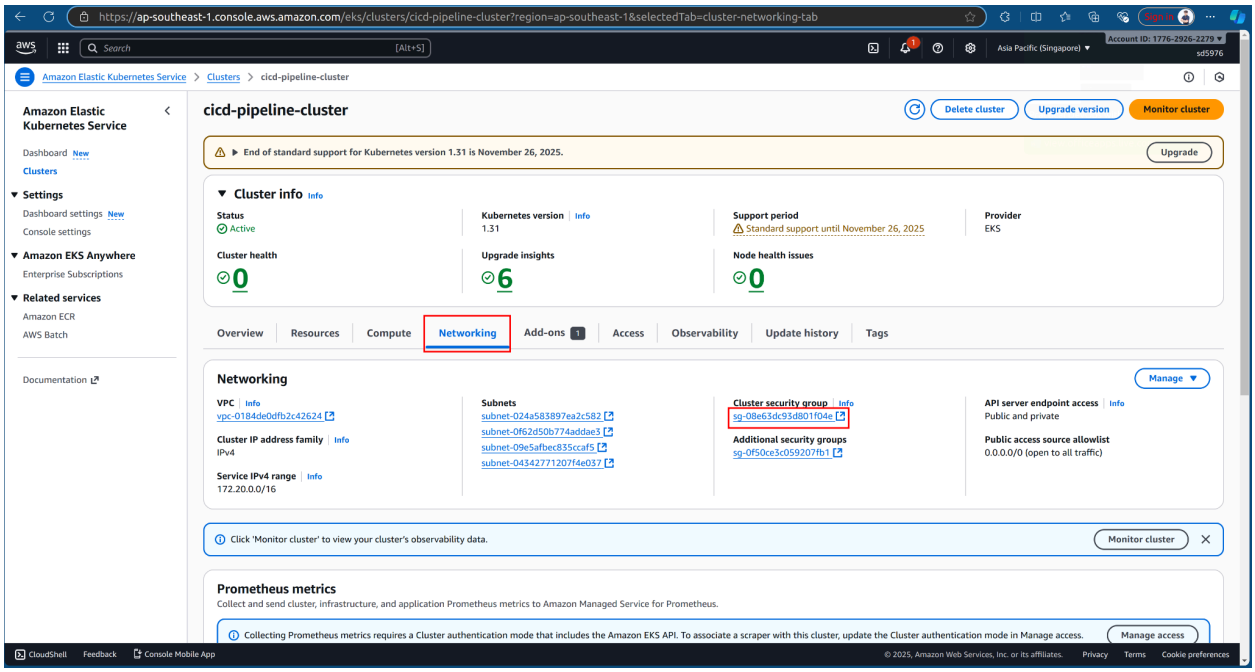


CI will run and push the *Backend* image to ECR.

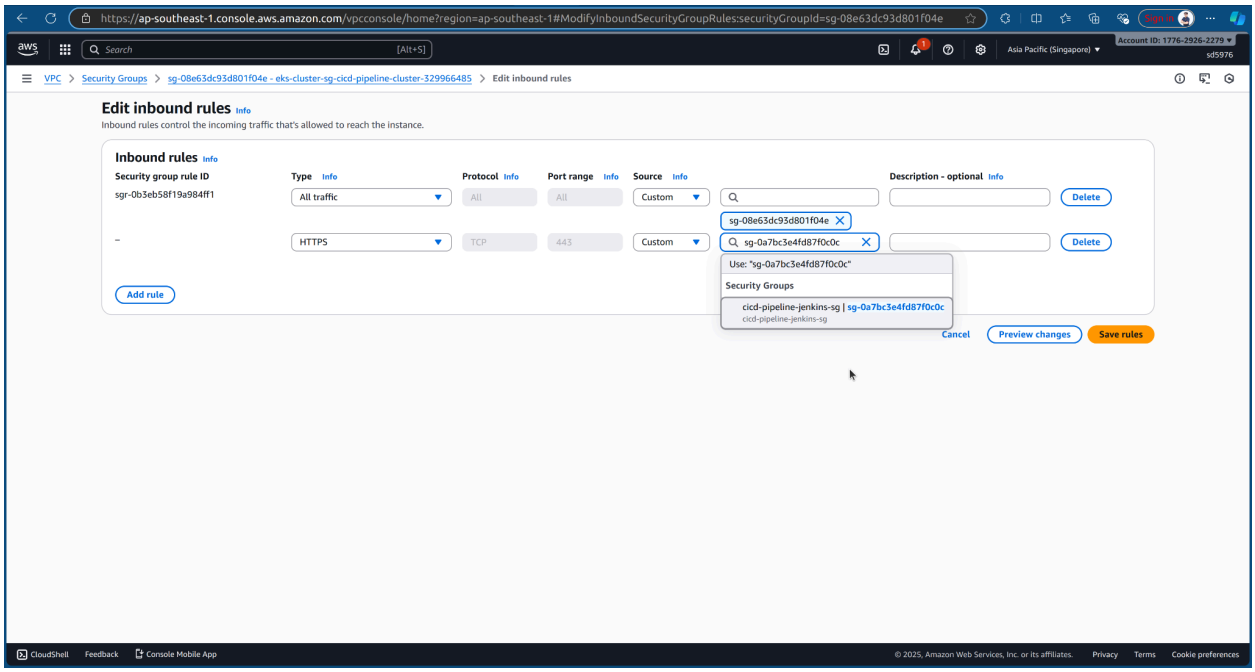


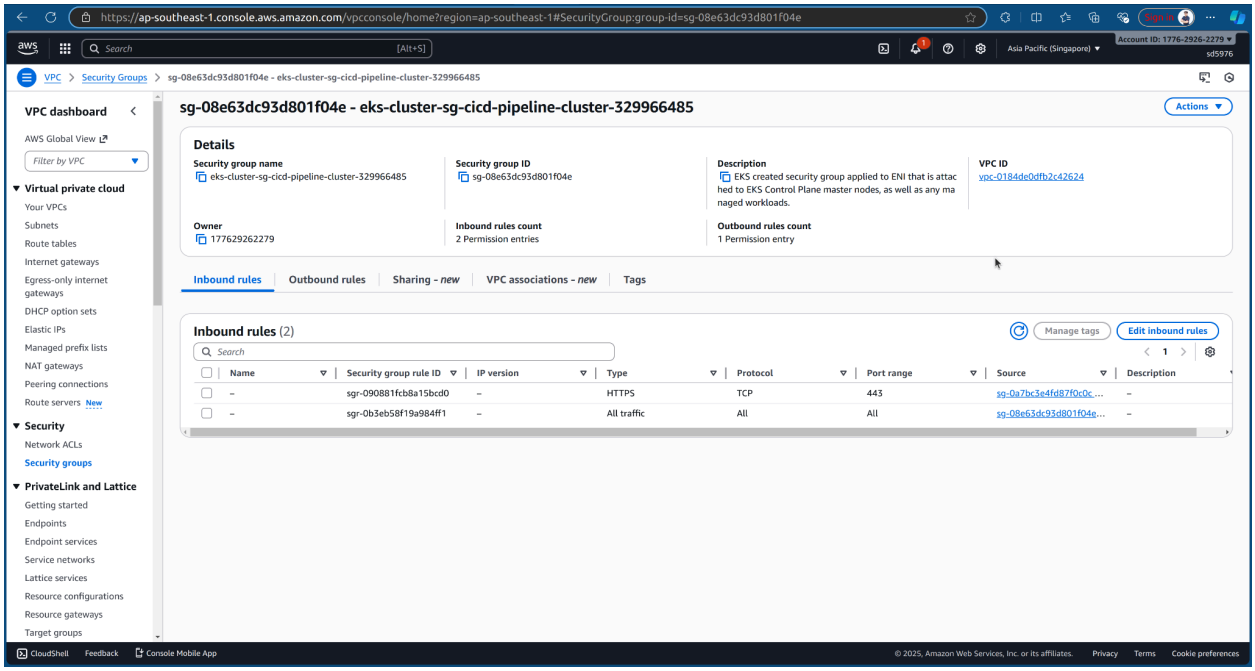
V. Deployment

First, we need to add inbound rules to allow the Jenkins EC2 instance's security group to access the EKS cluster. Go to **cicd-pipeline-cluster** → **Networking** → Click on the security group → **Edit Inbound rules**.



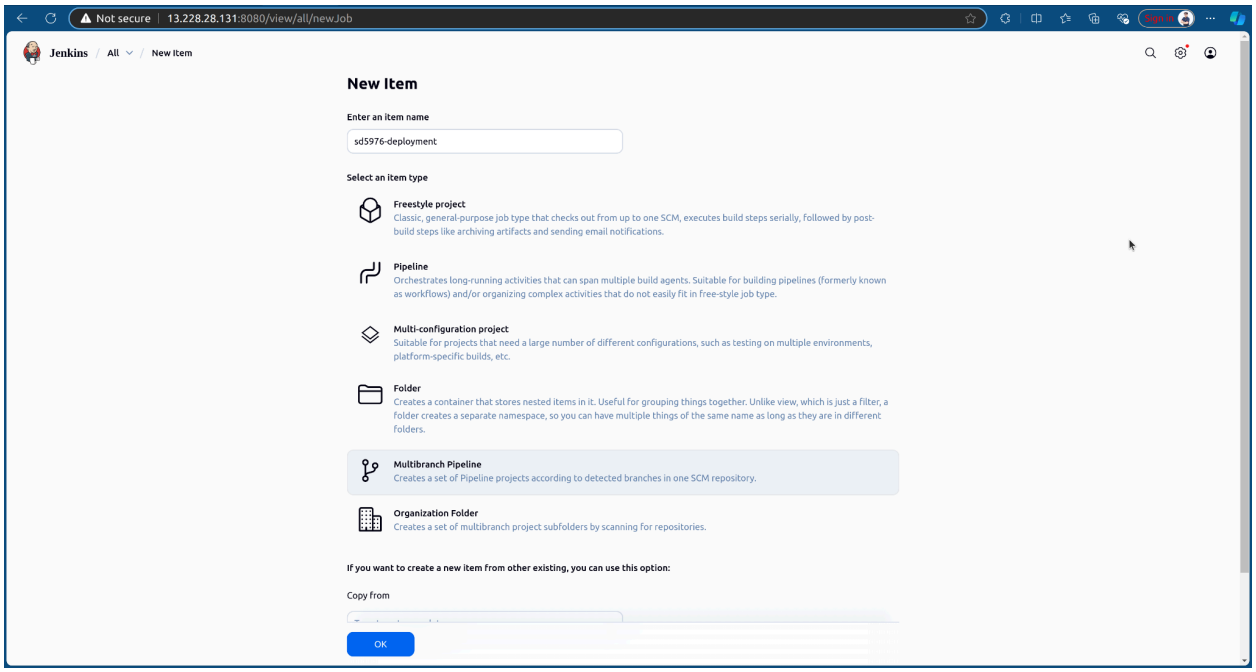
Add HTTPS inbound rule from Jenkins EC2 instance's security group **cicd-pipeline-jenkins-sg** and save rules.



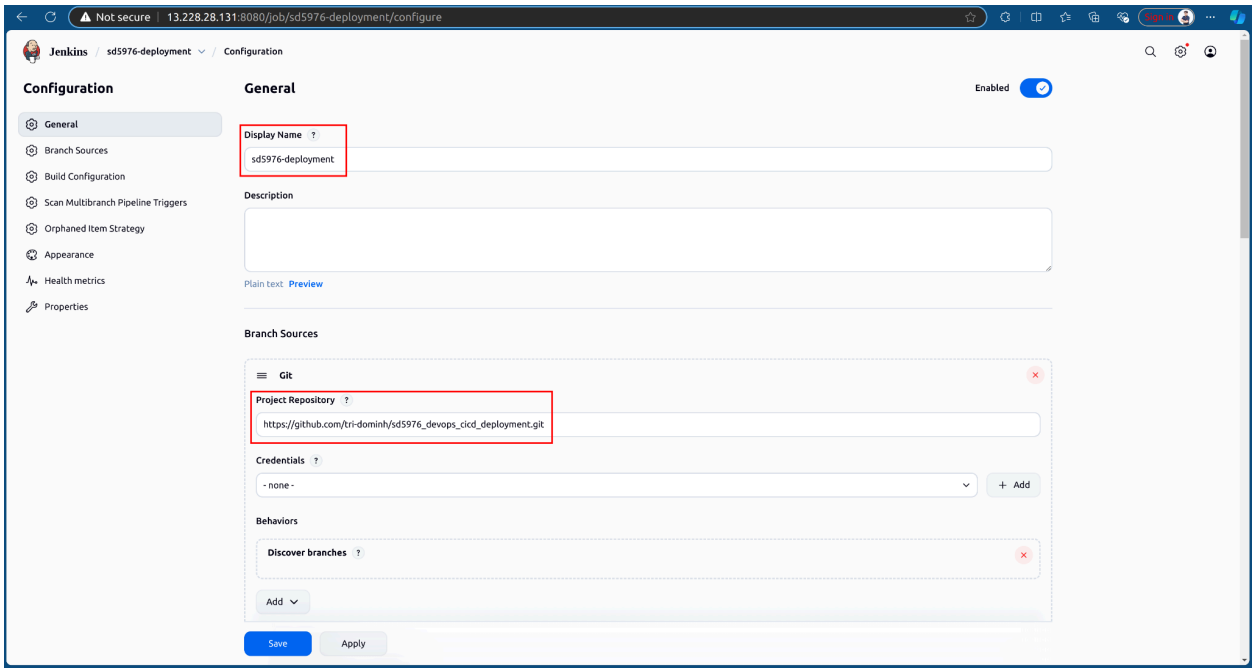


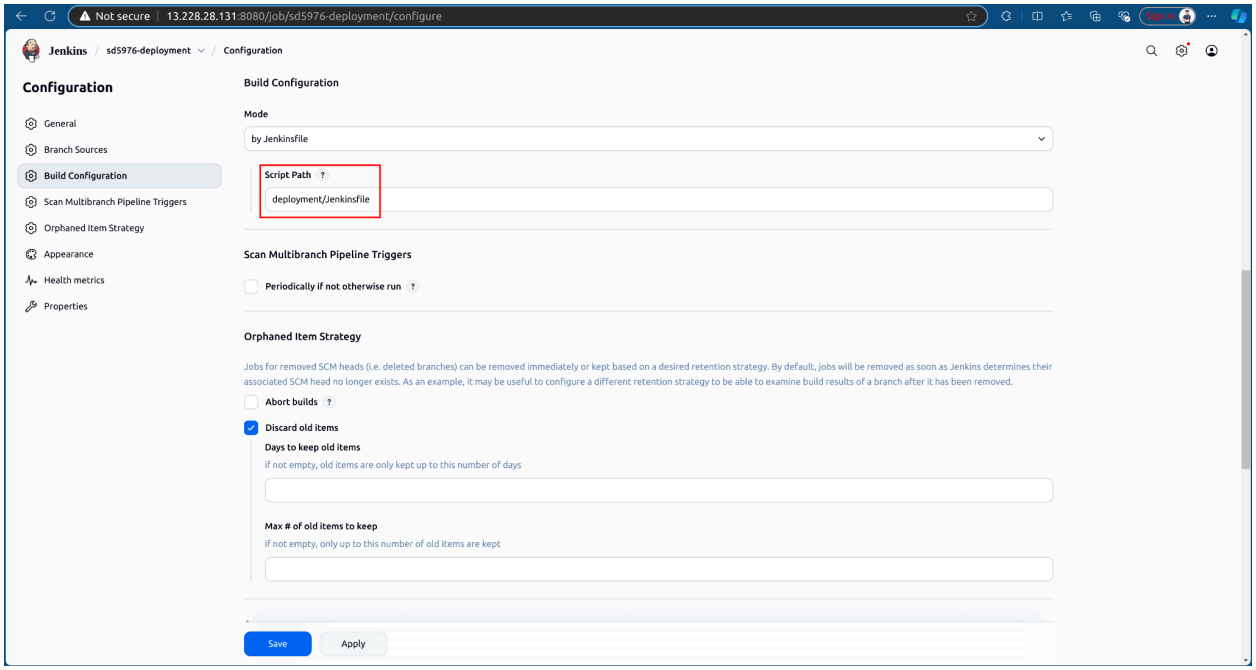
Second, we create a new Multibranch Pipeline job. Refer to:

https://github.com/tri-dominh/sd5976_devops_cicd_deployment/tree/main/deployment

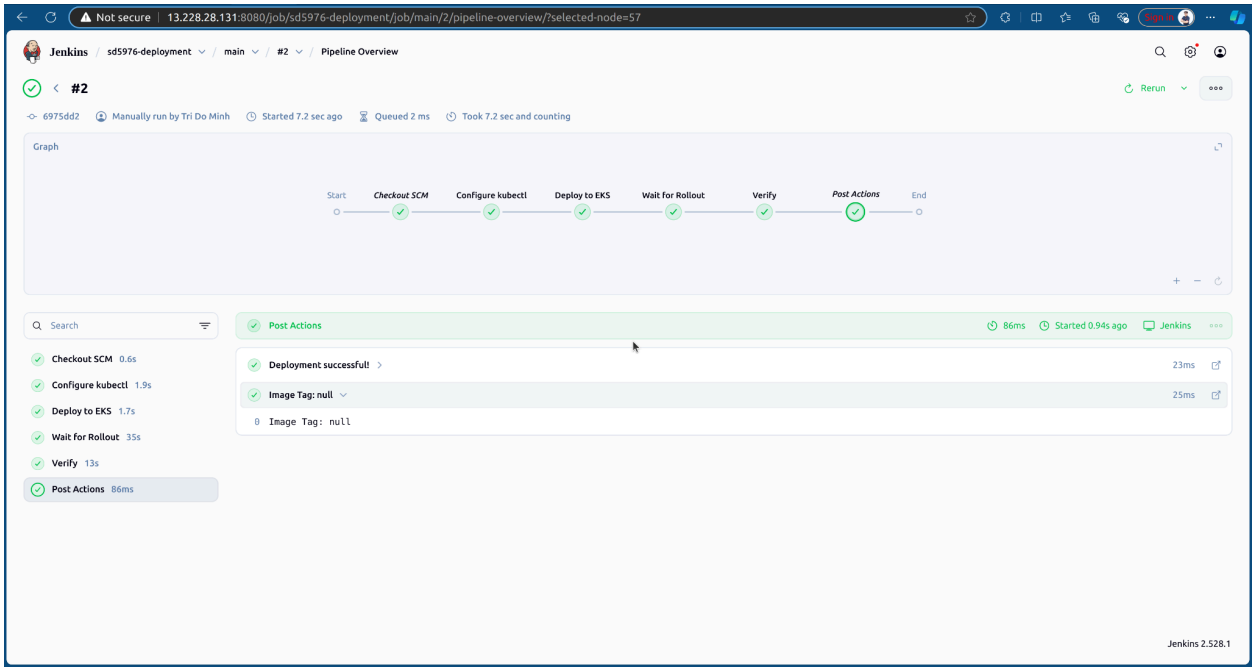


Configure Jenkins to point to Deployment resource and Jenkinsfile.





After creating, the job will run Jenkins based on the Jenkinsfile and source.



Jenkins will deploy *Frontend* & *Backend* from ECR to EKS in **sd5976-msa** namespace.

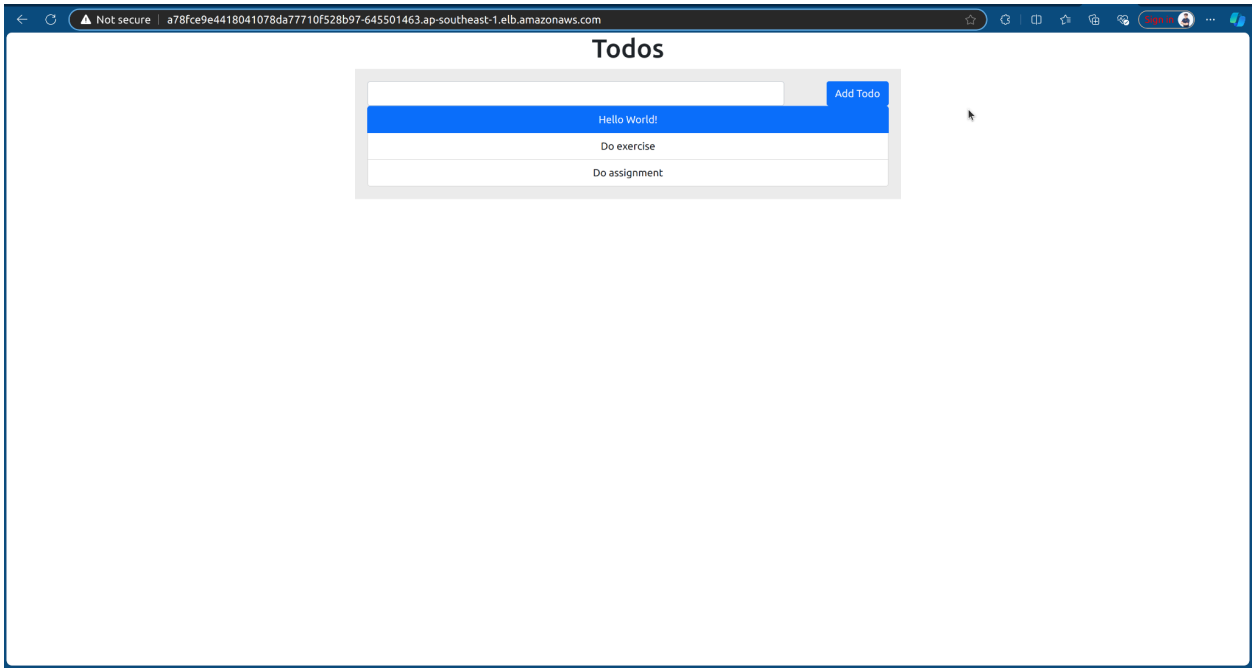
Use **kubectl get pods -n sd5976-msa** to get all pods inside the namespace.

```
~/Desktop/sd5976_msa | main  kubectl get pods -n sd5976-msa

NAME                        READY   STATUS    RESTARTS   AGE
backend-cc7cd898b-2vj9q     1/1     Running   0          11m
backend-cc7cd898b-9sxcr     1/1     Running   0          11m
frontend-5c776bf9c5-rthpd   1/1     Running   0          11m
frontend-5c776bf9c5-tf6qk   1/1     Running   0          11m
mongodb-78547887ff-h686t    1/1     Running   0          11m

~/Desktop/sd5976_msa | main
```

Use **kubectl get svc frontend -n sd5976-msa** to get the Frontend URL from EKS.

```
~/Desktop/sd5976_msa | main  kubectl get svc frontend -n sd5976-msa                                                    ✔ | base Py | cicd-pipeline-cluster ○
NAME       TYPE           CLUSTER-IP      EXTERNAL-IP                                                                  PORT(S)        AGE
frontend   LoadBalancer   172.20.241.30   a78fce9e4418041078da77710f528b97-645501463.ap-southeast-1.elb.amazonaws.com   80:31416/TCP   12m

~/Desktop/sd5976_msa | main                                                                                                                ✔ | base Py
```

We can access the application using the frontend URL from EKS.



VI. Monitoring with Prometheus and Grafana

Define .yaml file to deploy Prometheus and Grafana in sd5976_aws_infrastructure:

https://github.com/tri-dominh/sd5976_aws_infrastructure/tree/main/monitoring

Deploy metrics-server to collect cluster metrics.

kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/releases/latest/download/components.yaml

```
~/Desktop/sd5976_aws_infrastructure | main  kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/releases/latest/download/components.yaml
serviceaccount/metrics-server created
clusterrole.rbac.authorization.k8s.io/system:aggregated-metrics-reader created
clusterrole.rbac.authorization.k8s.io/system:metrics-server created
rolebinding.rbac.authorization.k8s.io/metrics-server-auth-reader created
clusterrolebinding.rbac.authorization.k8s.io/metrics-server:system:auth-delegator created
clusterrolebinding.rbac.authorization.k8s.io/system:metrics-server created
service/metrics-server created
deployment.apps/metrics-server created
apiservice.apiregistration.k8s.io/v1beta1.metrics.k8s.io created

~/Desktop/sd5976_aws_infrastructure | main                                    ✔ | 5s | base Py
```

Deploy Prometheus and Grafana

kubectl apply -f monitoring/prometheus.yaml

kubectl apply -f monitoring/grafana.yaml

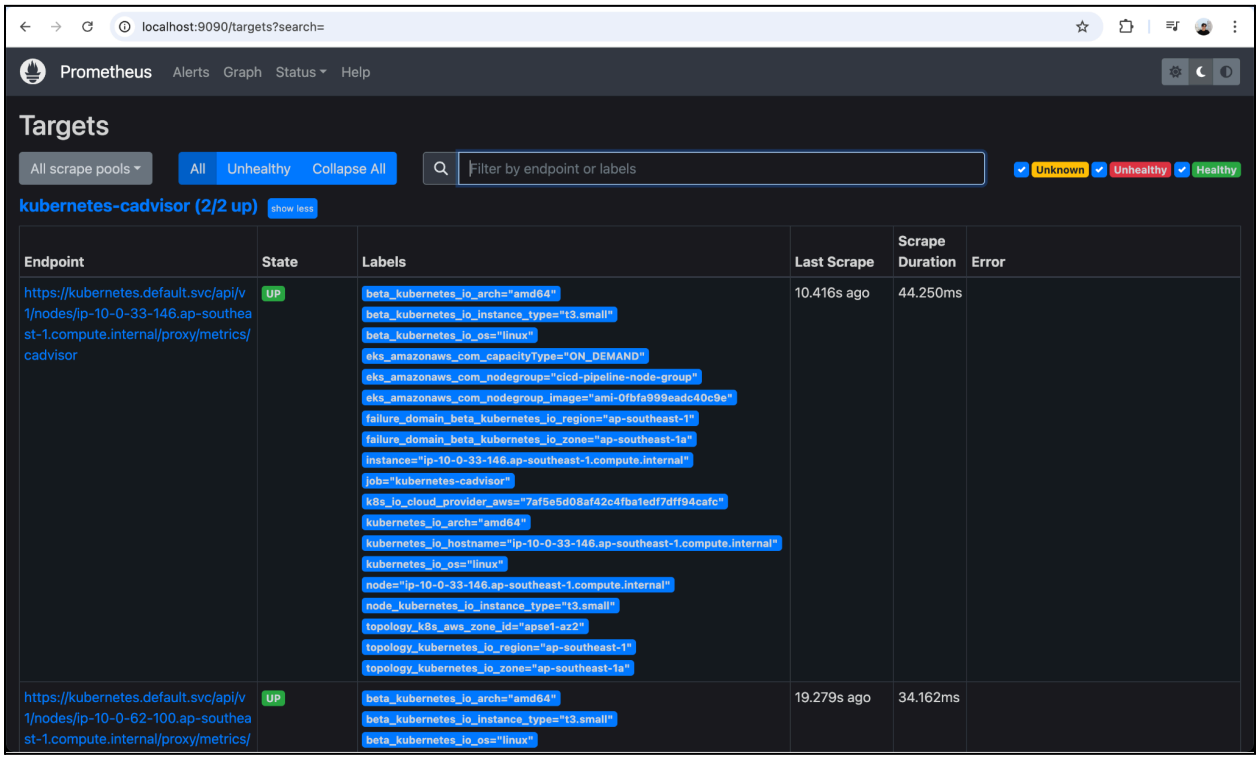
```
~/De/sd5976_aws_infrastructure | main kubectl apply -f monitoring/prometheus.yaml
peline-cluster ○
namespace/monitoring created
serviceaccount/prometheus created
clusterrole.rbac.authorization.k8s.io/prometheus created
clusterrolebinding.rbac.authorization.k8s.io/prometheus created
configmap/prometheus-config created
deployment.apps/prometheus created
service/prometheus created

~/De/sd5976_aws_infrastructure | main kubectl apply -f monitoring/grafana.yaml
peline-cluster ○
configmap/grafana-datasources created
deployment.apps/grafana created
service/grafana created
```

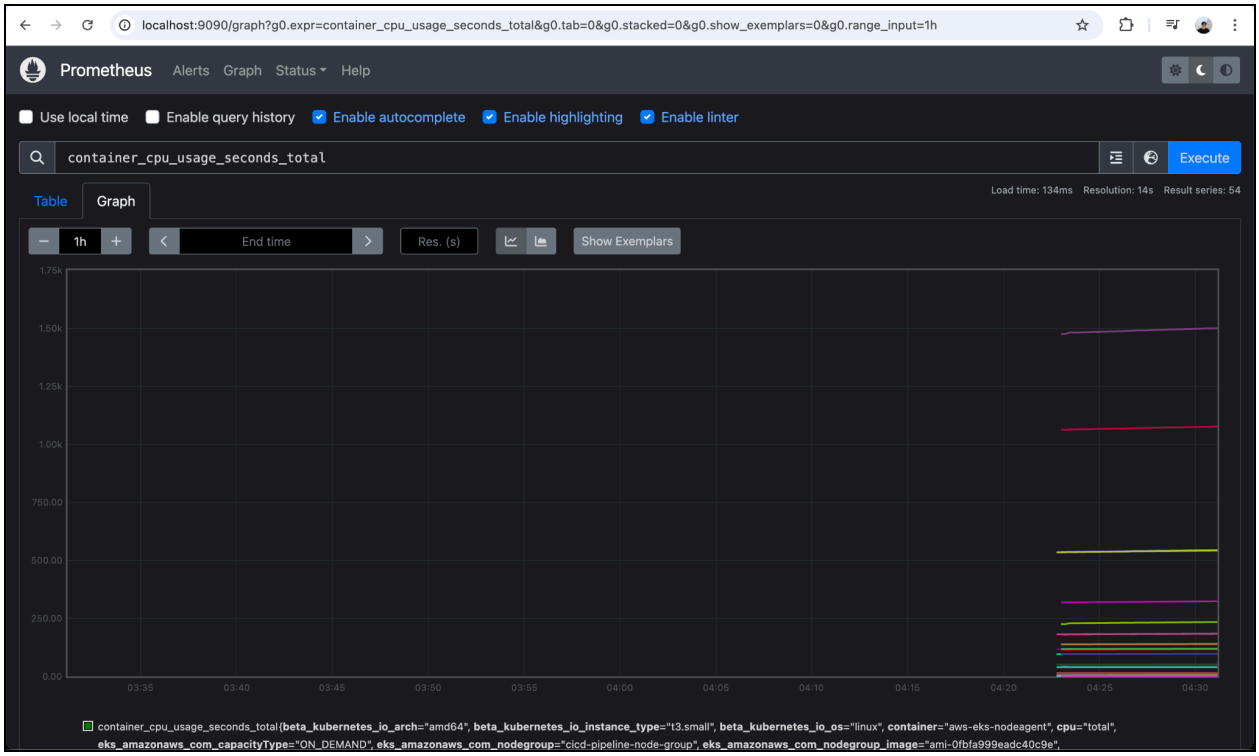
Forward Prometheus port from EKS to local.

kubectl port-forward -n monitoring svc/prometheus 9090:9090

```
~/De/sd5976_aws_infrastructure | main kubectl port-forward -n monitoring svc/prometheus 9090:9090
Forwarding from 127.0.0.1:9090 -> 9090
Forwarding from [::1]:9090 -> 9090
```

We can monitor Prometheus via http://localhost:9090





Forward Grafana port from EKS to local.

kubectl port-forward -n monitoring svc/grafana 3000:3000

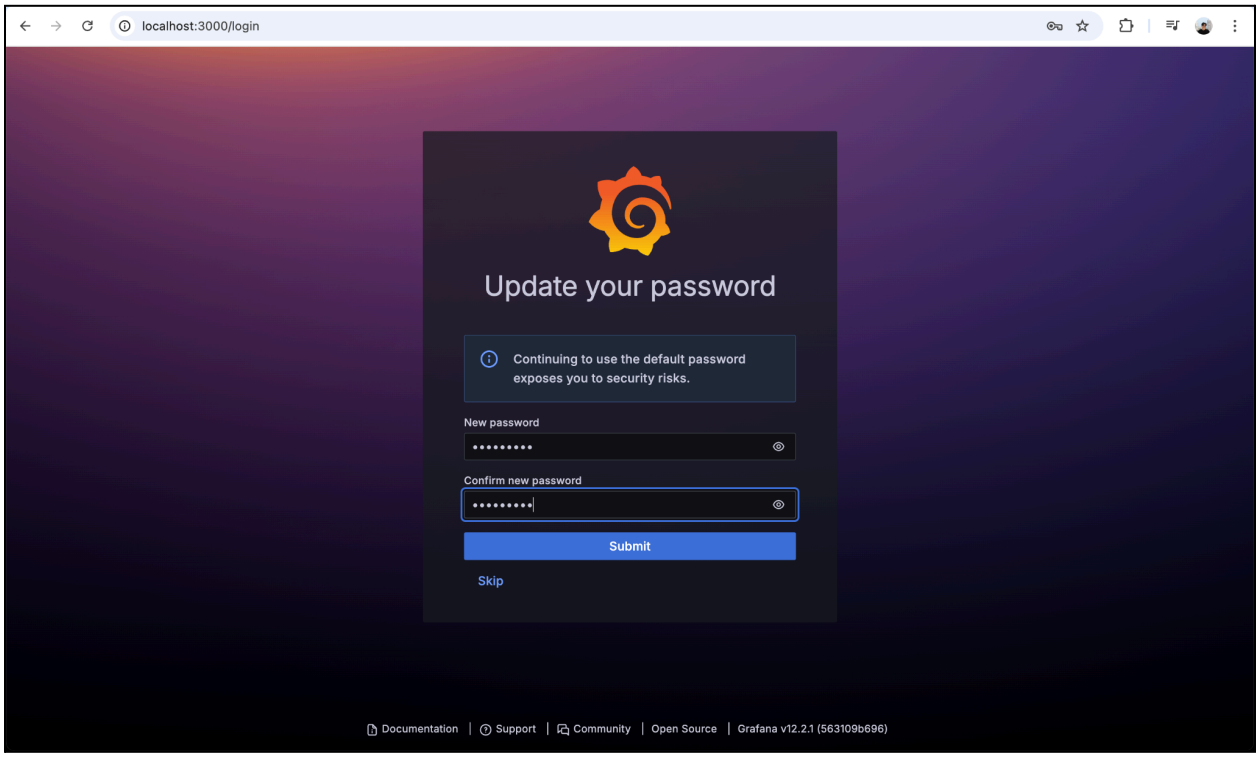
```
~/Desktop/sd5976_aws_infrastructure | main  kubectl port-forward -n monitoring svc/grafana 3000:3000
Forwarding from 127.0.0.1:3000 -> 3000
Forwarding from [::1]:3000 -> 3000
```

We can access Grafana via http://localhost:3000/login

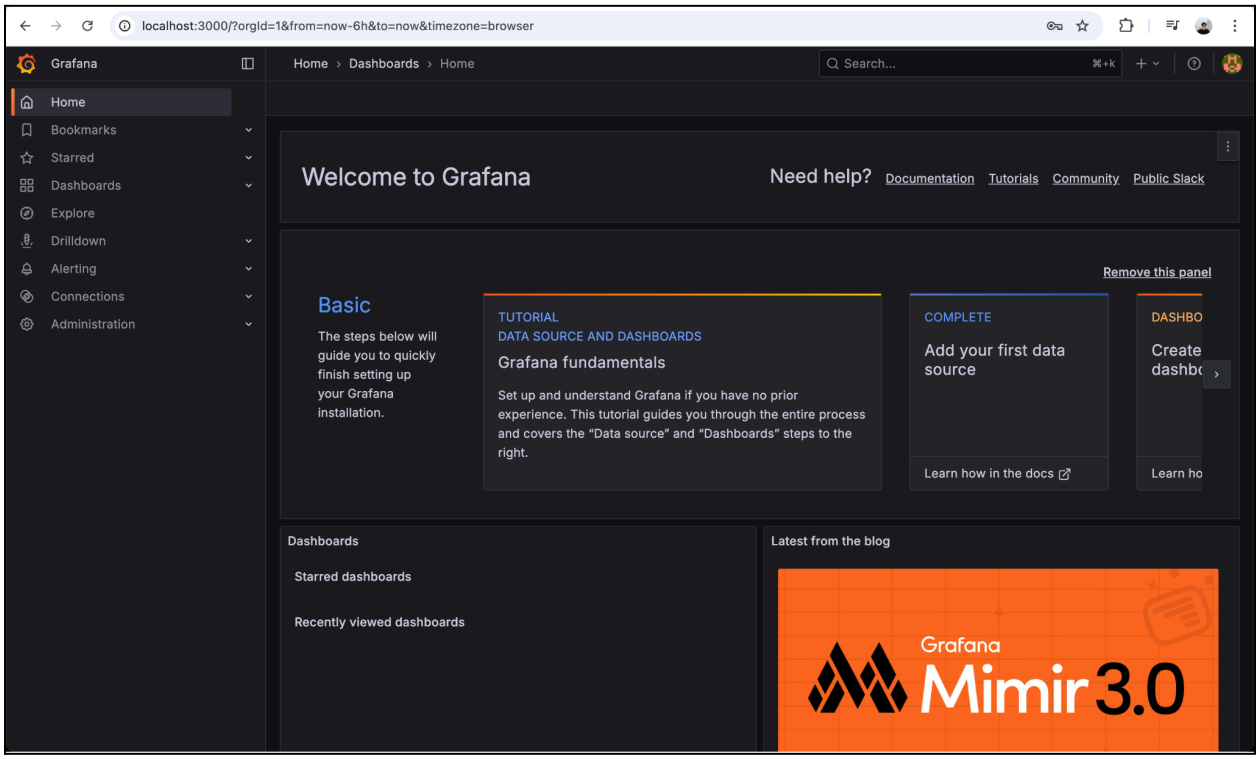
Default username: **admin**

Default password: **admin**

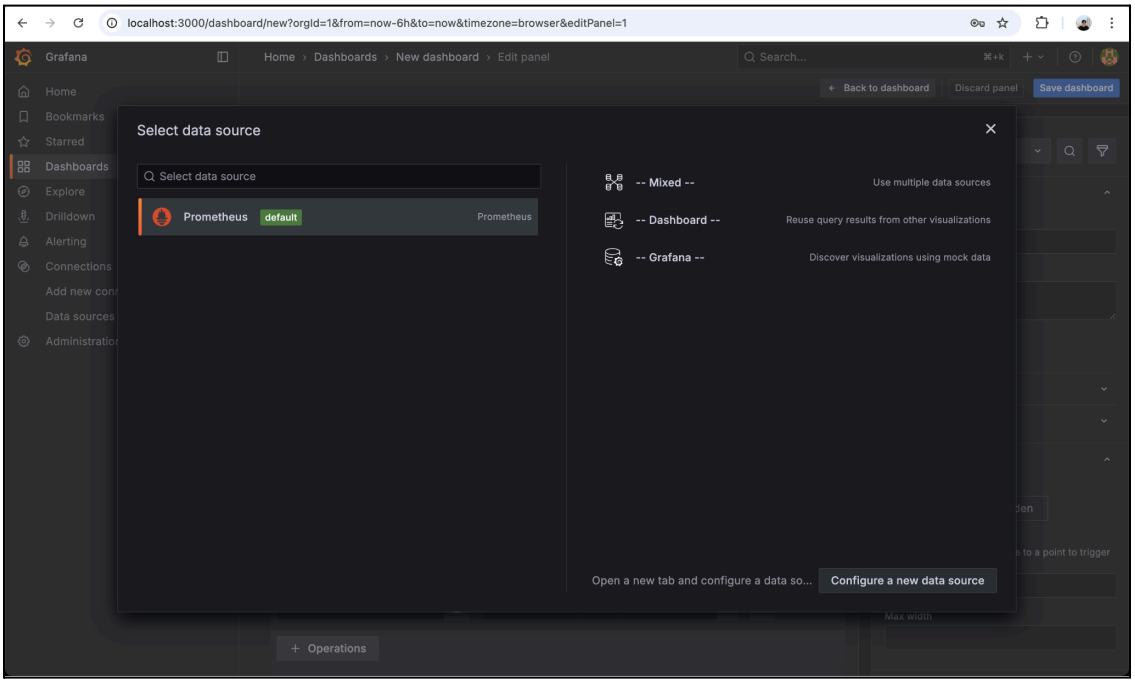
We need to update the password.



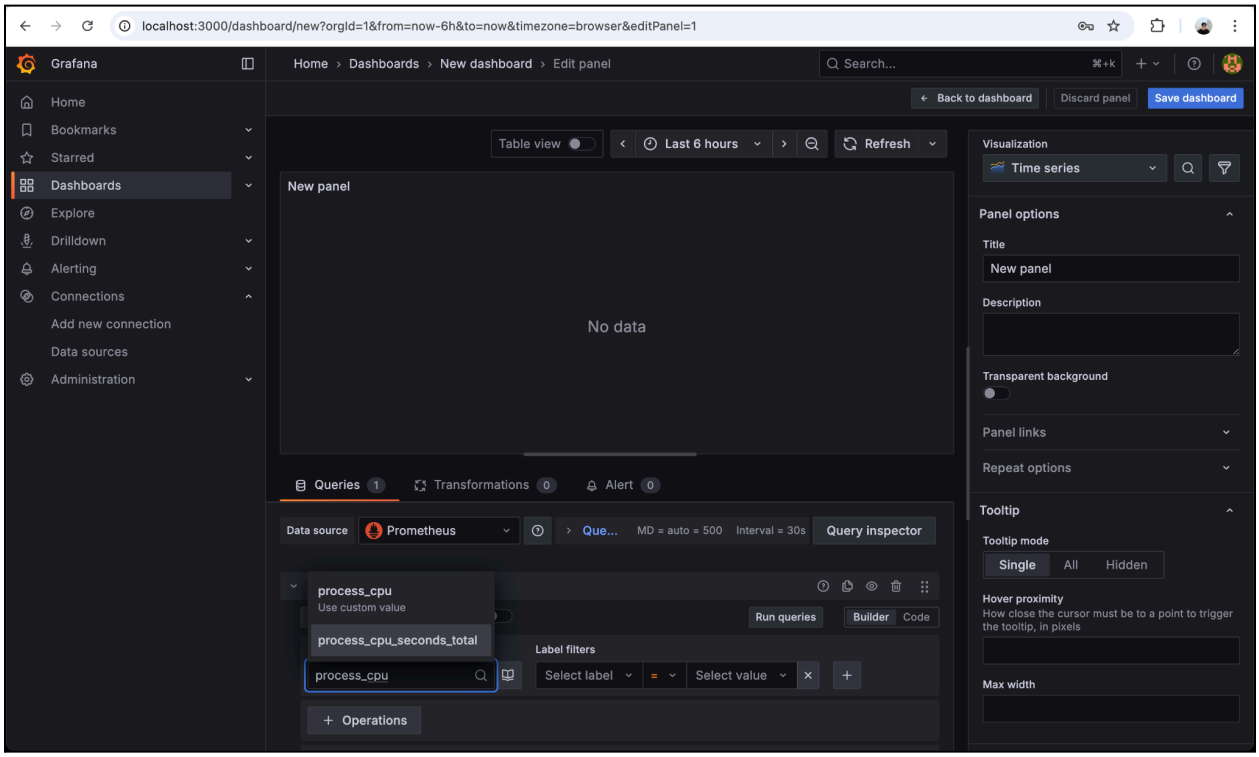
Logged in the Grafana successfully.



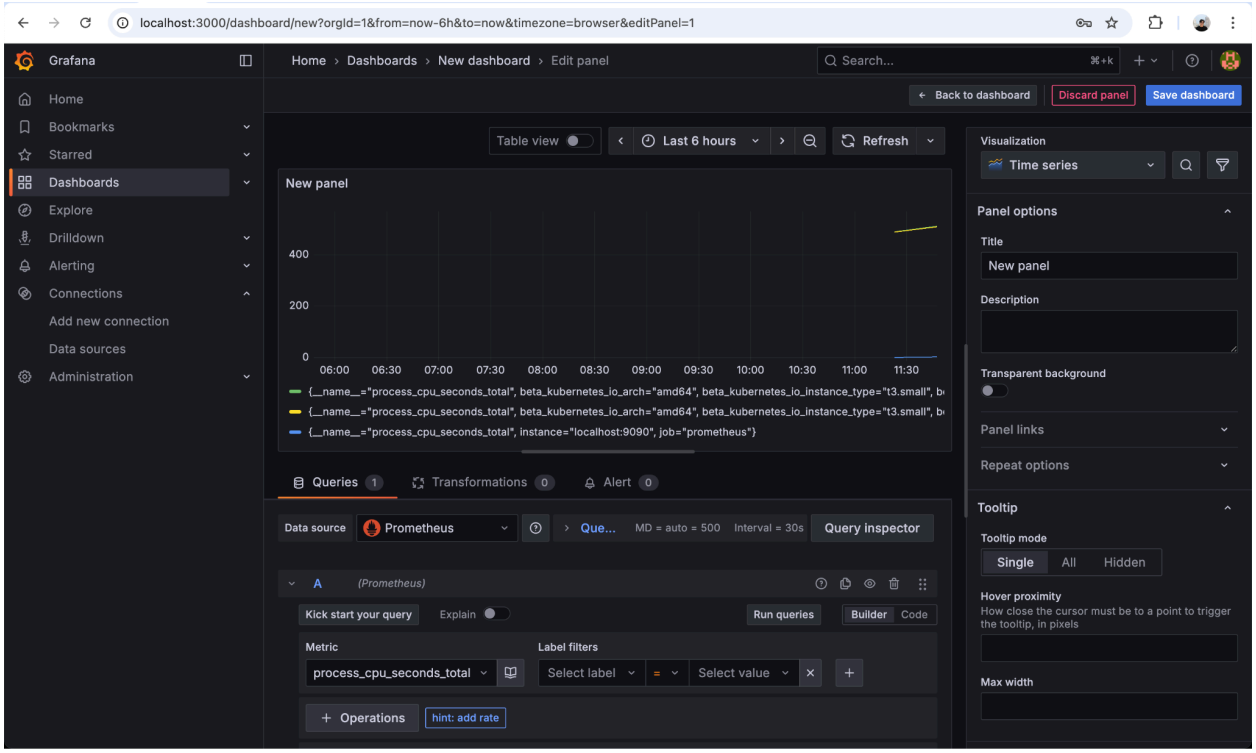
Go to **Dashboard → Create dashboard → Add visualization →** Select **Prometheus (default)**.



In metrics, search and select **process_cpu_seconds_total** and run the queries.



After showing on the panel, click **Save dashboard**.



Now we can monitor with Grafana.