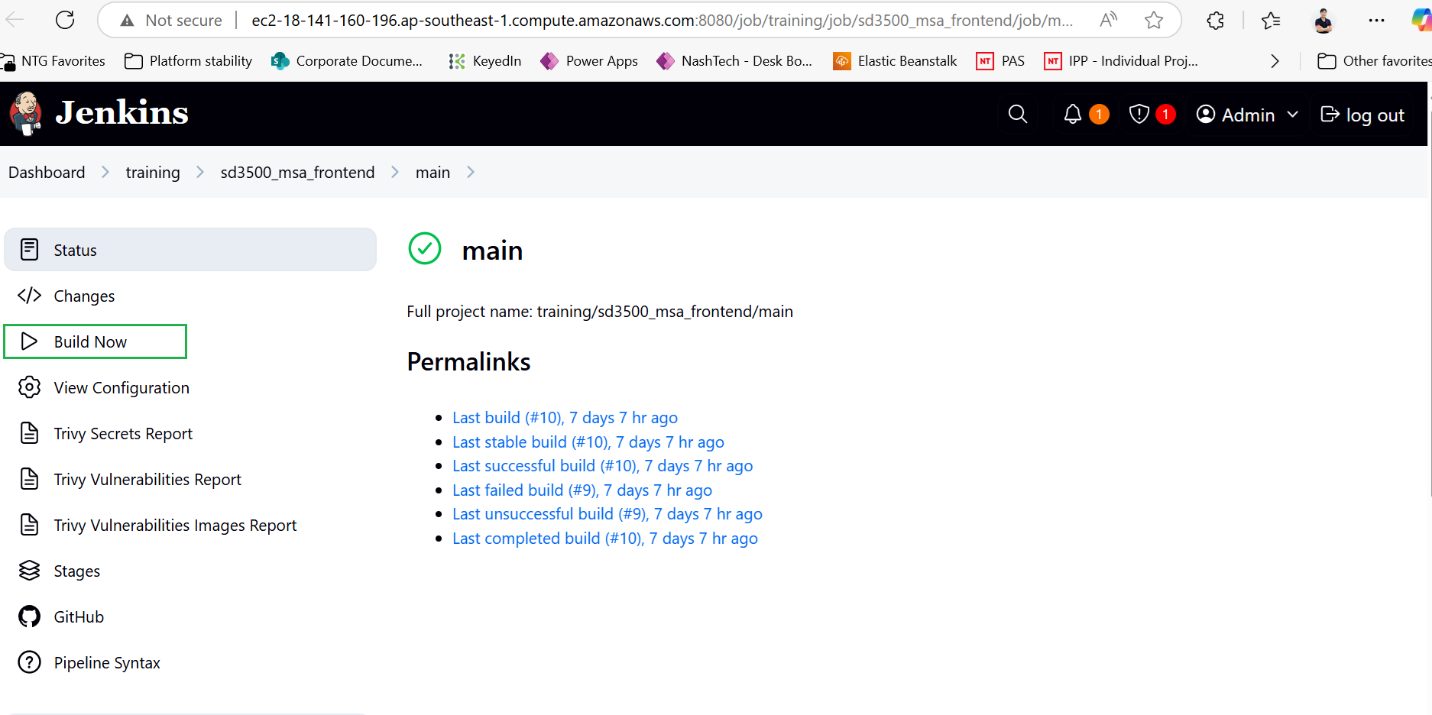
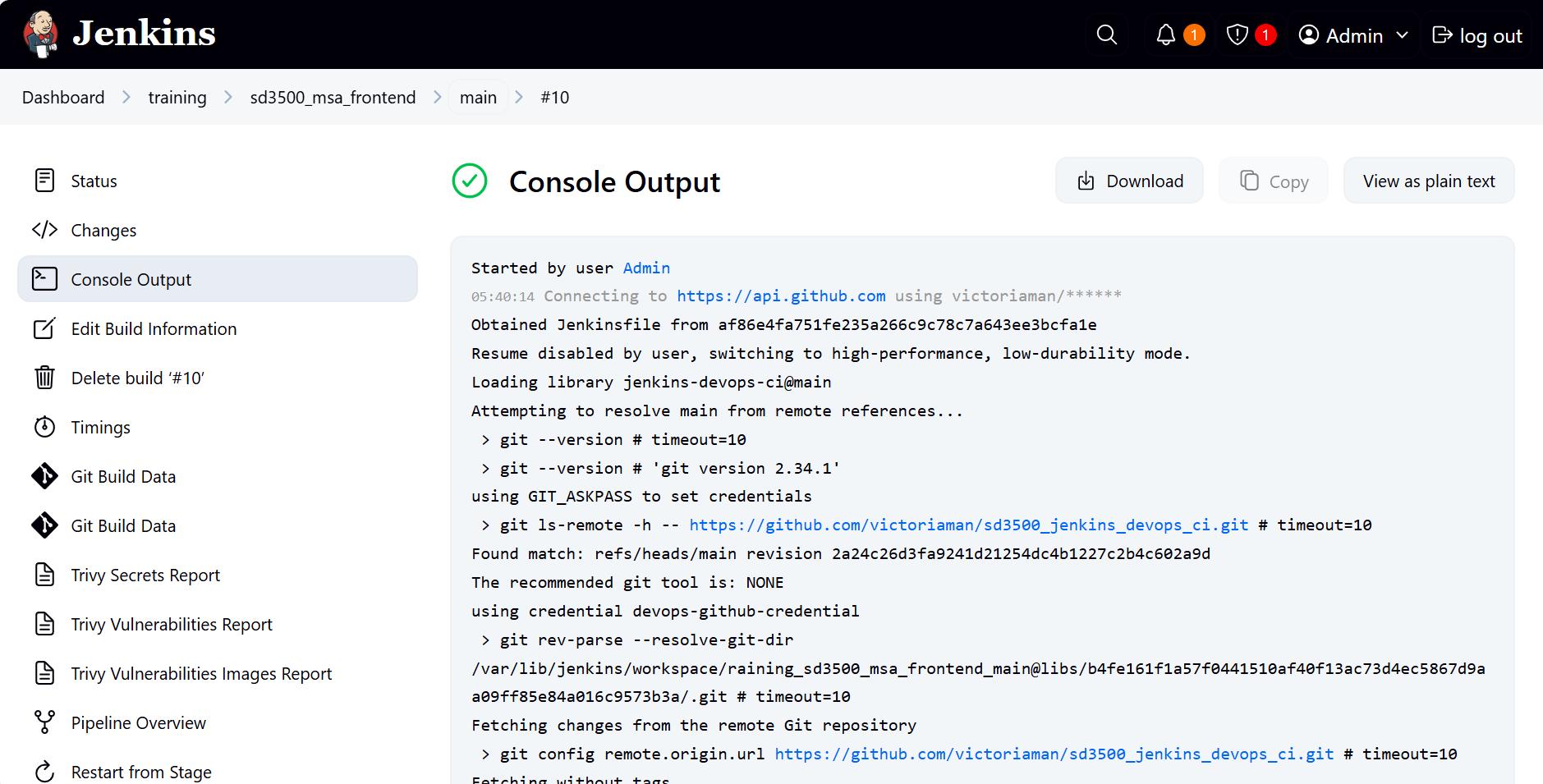
## Verify CI flow

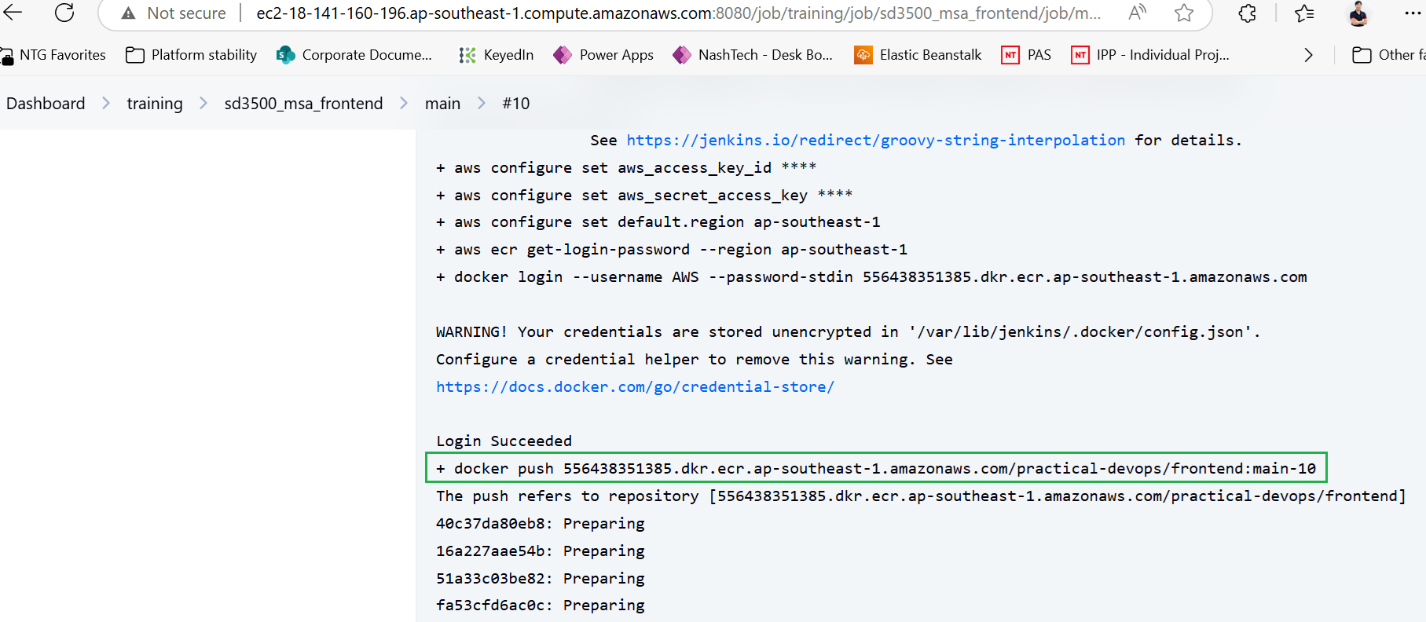
# Navigate to pipeline sd3500\_msa\_frontend/main => Build Now



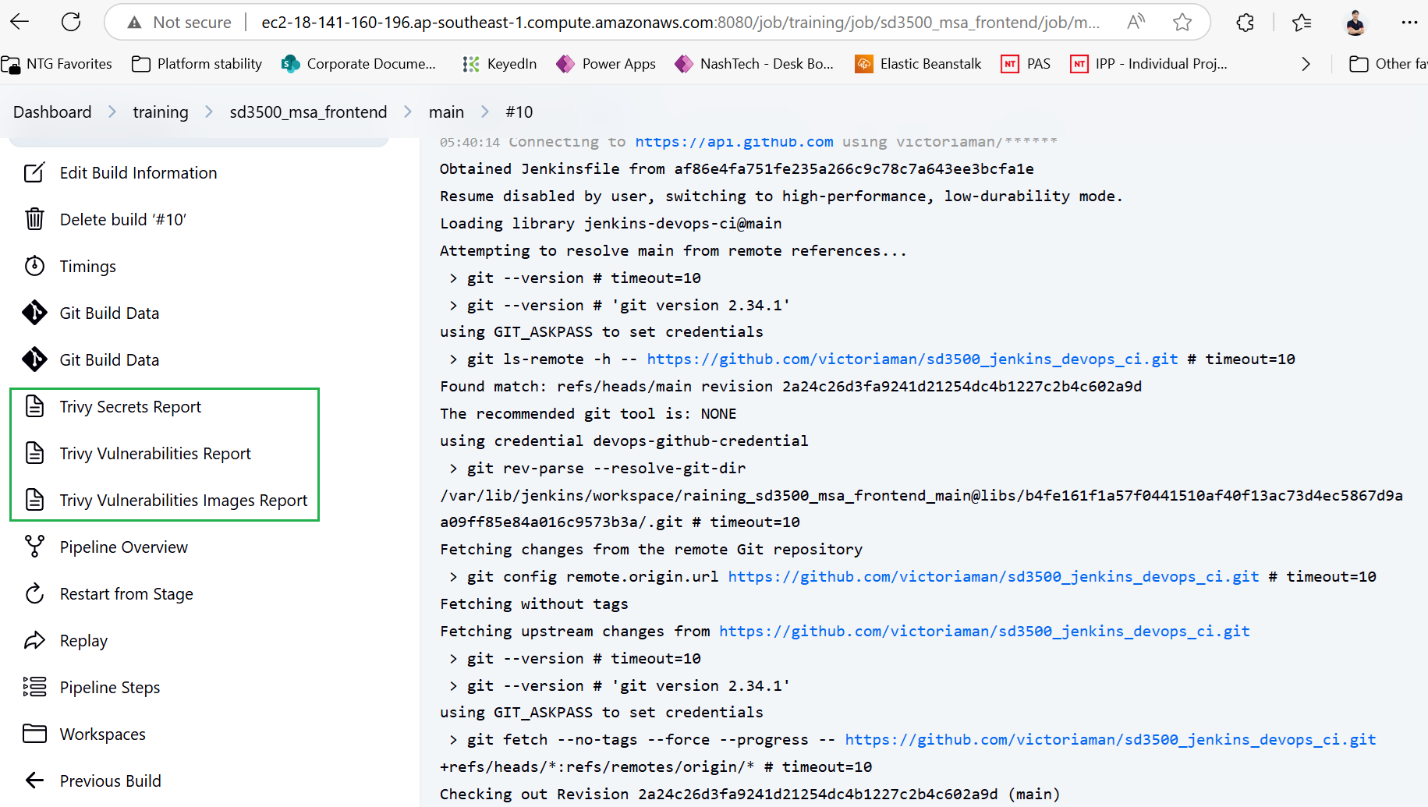
After pipeline run completed



# Tag of Docker image is printed in console log

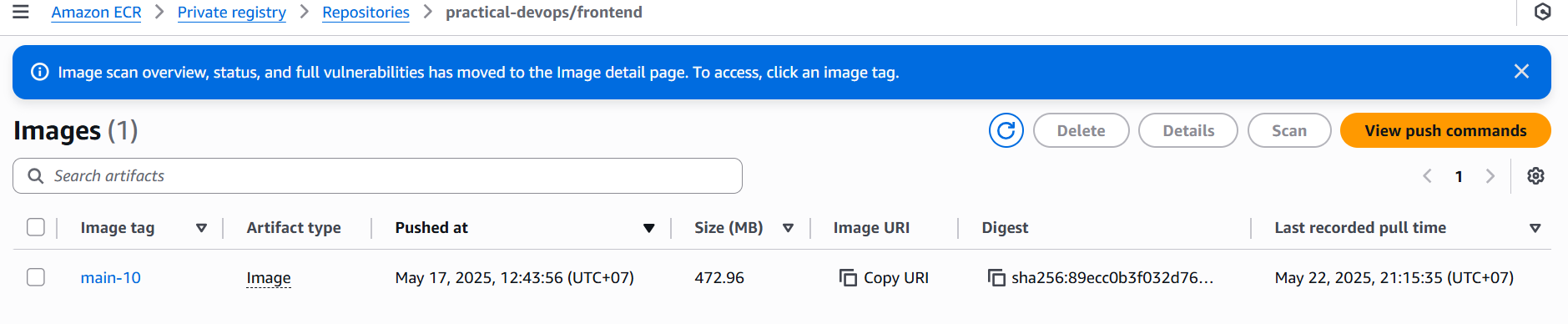


# Click Trivy Vulnerabilities Report to view detail report



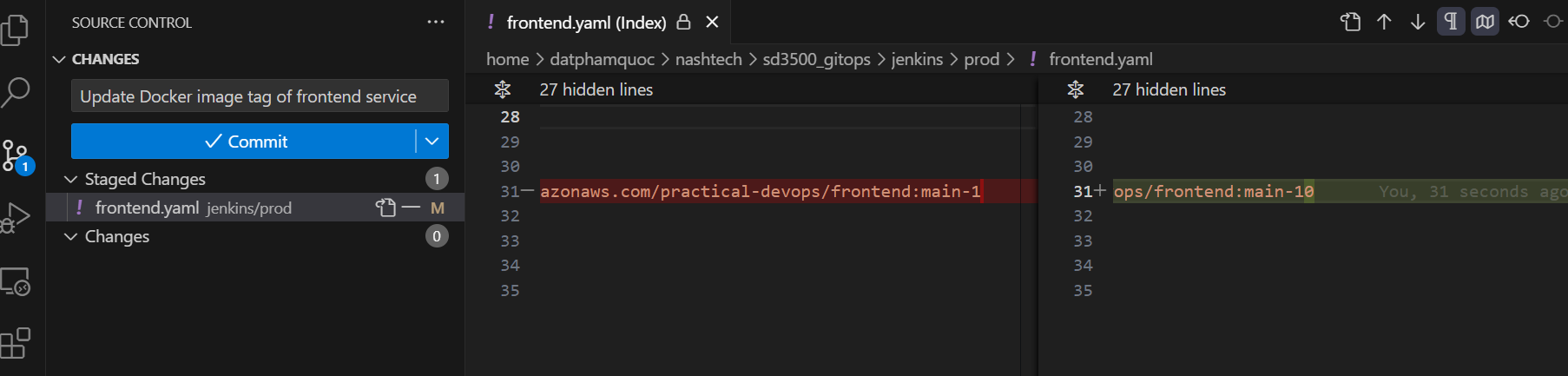


# Check new image is published to AWS ECR

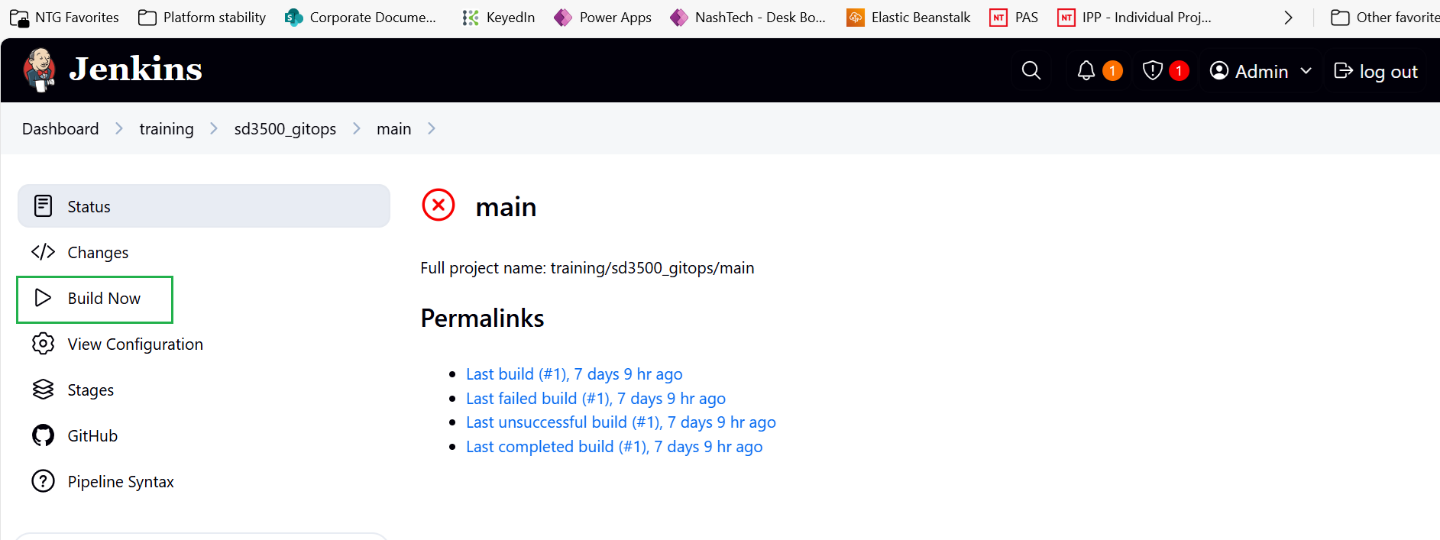


## Verify CD flow

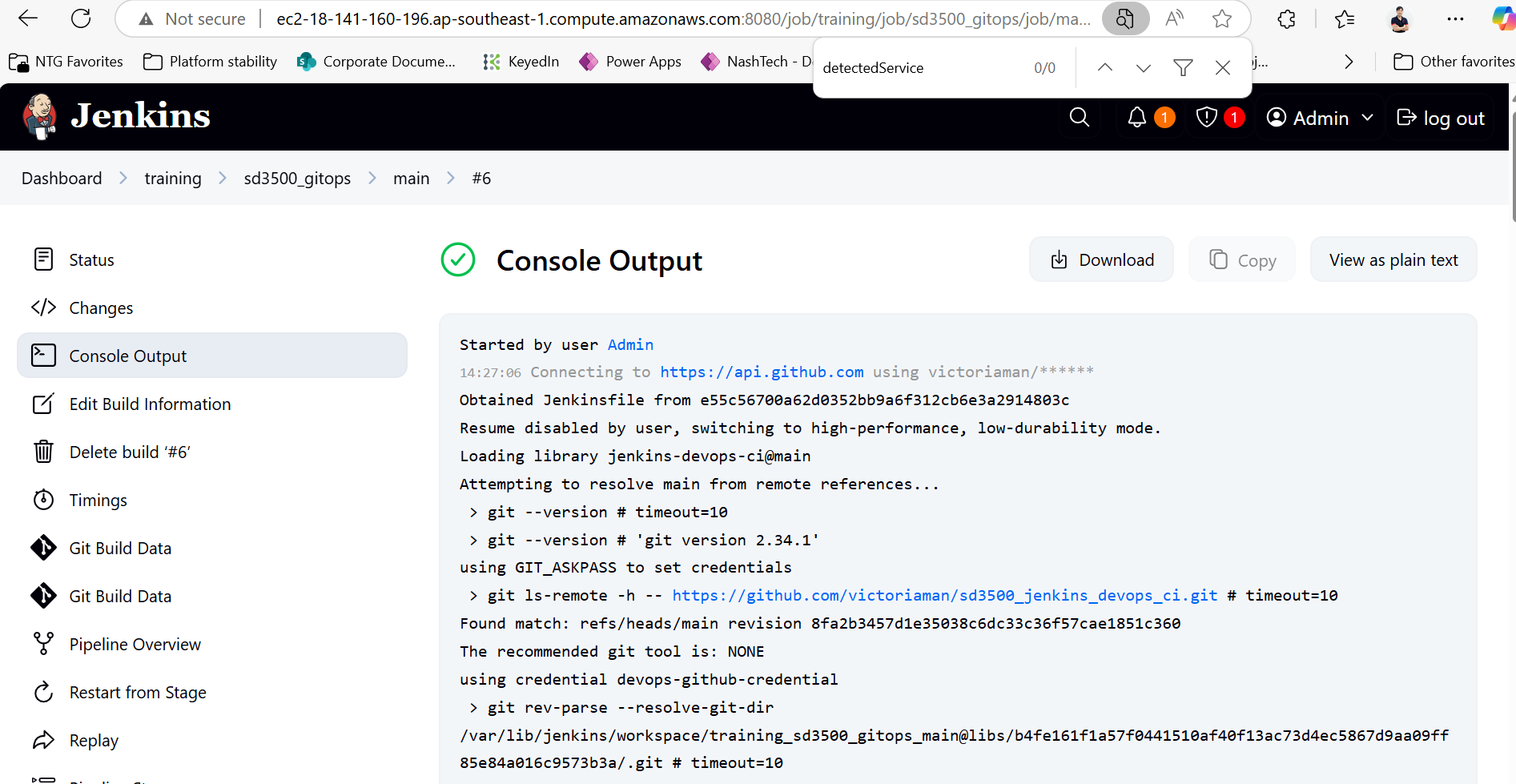
# Update image tag in [sd3500\_gitops/jenkins/prod/frontend.yaml at main · victoriaman/sd3500\_gitops](https://github.com/victoriaman/sd3500_gitops/blob/main/jenkins/prod/frontend.yaml) with the tag from latest image in AWS ECR

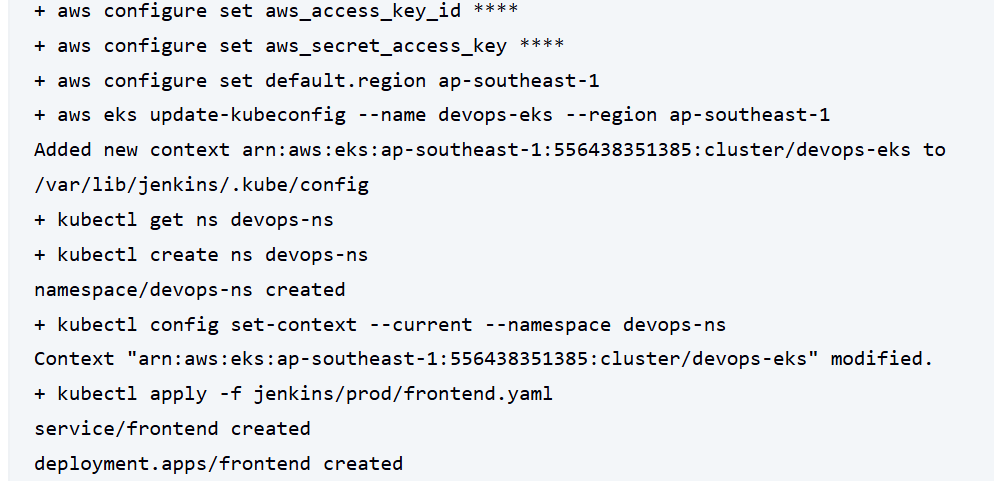


# Navigate to pipeline => Build Now



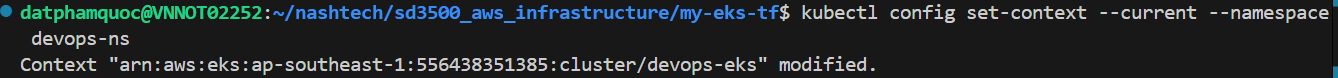
After pipeline run completed



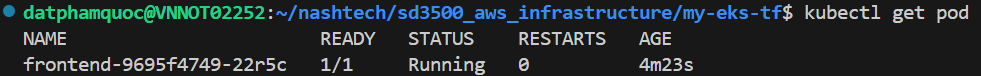


**Open terminal to check frontend service in EKS**

# Switch namespace to devops-ns  
kubectl config set-context --current --namespace devops-ns

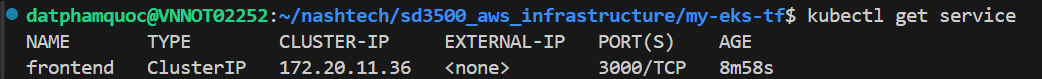


# Verify pod  
kubectl get pod



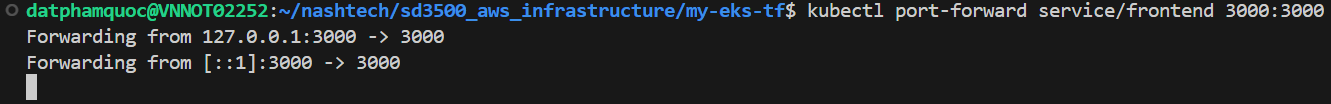
# verify frontend service

kubectl get service



# Application verification by exposing frontend service, expose frontend service to access application

kubectl port-forward service/frontend 3000:3000



# Access to <http://localhost:3000> to verify the frontend application, which is hosted in AWS EKS

