Project Report

On

AWS INFRASTRUCTURE COMPLIANCE SECURITY

Submitted in fulfillment for the award of

Post Graduate Diploma in IT Infrastructure System & Security

(PG-DITISS) from CDAC ACTS (Pune)

Guided By:

Mr. Sandeep Walvekar

Presented By:

Siddhi	PRN: 230340123046
Priyanka Kumari	PRN: 230340123032
Kusalkar Isha Maruti	PRN: 230340123007

DECLARATION

We declare that this written submission represents our ideas in our own words and where others ideas or words have been included; we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed**.**

Place: Pune

Date: 22/02/2024

Siddhi	Priyanka Kumari	Kusalkar Isha Maruti
(230944223042**)**	**(**230944223028**)**	**(**230944223018**)**

CERTIFICATE

This is to certify that the project report entitled **"AWS INFRASTRUCTURE COMPLIANCE SECURITY"**, submitted by **Siddhi** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Mr. Sandeep Walvekar
Guide

Mr. Vishal Salunkhe
Course Coordinator

CERTIFICATE

This is to certify that the project report entitled **"AWS INFRASTRUCTURE COMPLIANCE SECURITY"**, submitted by **Priyanka Kumari** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Mr. Sandeep Walvekar
Guide

Mr. Vishal Salunkhe
Course Coordinator

CERTIFICATE

This is to certify that the project report entitled **"AWS INFRASTRUCTURE COMPLIANCE SECURITY"**, submitted by **Kusalkar Isha Maruti** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date: 22/02/2024

Mr. Sandeep Walvekar
Guide

Mr. Vishal Salunkhe
Course Coordinator

APPROVAL CERTIFICATE

This Project II report entitled **"AWS INFRASTRUCTURE COMPLIANCE SECURITY"**by **Siddhi (230944223042)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner: _____

(Signature)

_____

(Name)

APPROVAL CERTIFICATE

This Project II report entitled **"AWS INFRASTRUCTURE COMPLIANCE SECURITY"** by **Priyanka Kumari (230944223028)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner: _____

(Signature)

_____

(Name)

APPROVAL CERTIFICATE

This Project II report entitled **"AWS INFRASTRUCTURE COMPLIANCE SECURITY"** by **Kusalkar Isha Maruti (230944223018)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner: _____

(Signature)

_____

(Name)

ACKNOWLEDGEMENT

This project "AWS Infrastructure Compliance Security" was a great learning experience for us and we are submitting this work to Advanced Computing Training School (CDAC ACTS).

We all are very glad to mention the name of *Mr. Sandeep Walvekar* for her valuable guidanceto work on this project. Her guidance and support helped us to overcomevarious obstacles and intricacies during the course of projectwork.

Our most heartfelt thanks go to *Mr. Vishal Salunke* (Course Coordinator, PG-*DITISS*) who gave all the required support and kind coordination to provide all the necessities like required hardware, internet facility and extra Lab hours to complete the project and throughout the course up to the last dayhere in C- DAC ACTS, Pune.

Sincerely,
1) Siddhi
2) Priyanka Kumari
3) Kusalkar Isha Maruti

TABLE OF CONTENTS

ABSTRACT

This report concludes work on a research project to explore the feasibility of Compliance AWS Infrastructure , This project runs security check on AWS Infrastructure with the help of AWS securityhub and performs checks on AWS Foundational Security Best Practices and various compliance frameworks. These frameworks include the Center for Internet Security (CIS), and the Payment Card Industry Data Security Standard (PCI DSS). AWS Security hub is integrated with third-party tool Defect dojo to generate Audit ready report and triage vulnerabilities .Further we can also add remediation by applying rules in AWS lambda for our findings.

This project addresses the problem of how to develop a secure Infrastructure which is industry ready and can pass all the Compliance Standards.

Compliances help with Server and network security, which are the basis for secure data transfer in the cloud, as they are crucial for the prevention of unauthorized access. In order to improve the security of customer data,the credit card companies have come to get her to create a security standard, called Payment Card Industry Data Security Standard (PCI DSS), which involve mandatory requirements for merchants that accept credit card transactions. The Security Standards ("PCI DSS" and “PA DSS”) have emerged from private ordering, although threats so of liability have also influenced their development and implementation.

INTRODUCTION

Aimsand Objective

Automating security compliances Infrastructureon AWS.

Objectives:

- Automate server deployment
- Automation of security and compliances

OVERALL DESCRIPTION

Introduction

What is AWS: Amazon Web Services, Inc. (AWS) is a subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis. These cloud computing web services provide distributed computing processing capacity and software tools via AWS server farms. One ofthese services is Amazon Elastic Compute Cloud (EC2), which allows sers to have at their disposal a virtual cluster of computers, available all the time, through the Internet. AWS's virtual computers emulate most ofthe attributes of a real computer, including hardware central processing units (CPUs) and graphics processing units (GPUs) for processing; local/RAM memory; hard-disk/SSD storage; a choice of operatingsystems; networking; and pre-loaded application software such as web servers, databases, and customer relationship management (CRM). AWS services are delivered to customers via a network of AWS server farms located throughout the world. Fees are based on a combination of usage (known as a "Pay-as-you-go" model), hardware, operating system, software, or networking features chosen by the subscriber required availability, redundancy, security, and service options. Subscriberscanpay for single virtual AWS computer, a dedicated physical computer, or clusters of either. Amazon provides select portions of security for subscribers (e.g. physical security of the data centers) while other aspectsof security are the responsibility of the subscriber (e.g. account management, vulnerability scanning, patching). AWS operates from many global geographical regions including 6 in North America. Amazon markets AWS to subscribers as a way of obtaining large-scale computing capacity more quickly and cheaply than building an actual physical server farm. All services are billed based on usage, but each service measures usage in varying ways. As of 2021 Q4, AWS has 33% market share for cloud infrastructure while the next two competitors Microsoft Azure and Google Cloud have 21%, and 10% respectively, according to Synergy Group.

What is EC2:

Amazon Elastic Compute Cloud (Amazon EC2) offers the broadestanddeepestcomputeplatform,withover500instancesand choi e of the latest processor, storage, networking, operating system, and purchase model to help you best match the needs of your workload. We are the first major cloud provider that supports Intel, AMD, and Arm Processors,the only cloud with on-demand EC2 Mac instances,and the only cloud with 400Gbps Ethernet networking.We offer the best price performance for machine learning training, as well as the lowest cost perinference instances in the cloud. More SAP, high performance computing (HPC), ML, and Windows workloads run on AWS than any other cloud.

What is Defect dojo:

Defect Dojo is a security orchestration and vulnerability management platform. Defect Dojo allows you to manage your application security program, maintain product and application information, triage vulnerabilities and push findings to systems like JIRA and Slack. Defect dojo enriches and refines vulnerability data using a number of heuristic algorithms that improve with the more you use the platform.

What are the components used for this project:

1. **GitHub:-**
   GitHub, Inc. is a platform and cloud-based service for software development and version control using Git, allowing developers to store and manage their code .

2. **Docker:-**
   Docker is a software platform that allows you to build, test, and deploy applications quickly. Docker packages software into standardized units called containers that have everything the software needs to run including libraries, system tools, code, and runtime. Using Docker, you can quickly deploy and scale applications into any environment and know your code will run.

3. **Docker Compose:-**
   Docker Compose is a tool that helps you define and share multi-container applications. With Compose, you can create a YAML file to define the services and with a single command, you can spin everything up or tear it all down.

4. **Python3:-**
   Python 3 is the latest version of the language, and it's great for new and seasoned developers alike. In fact, it's one of the most popular programming languages in the world.

5. **Pip3**:-
   pip3 is the official package installer for Python 3. It can be used to install packages from the Python Package Index. Python is a powerful andflexible general-purpose language with many applications.

6. **EC2:-**
   Amazon Elastic Compute Cloud is a part of Amazon.com cloud-computing platform, Amazon Web Services, that allows users to rent virtual computers on which to run their own computer applications.

7. **Security hub:-**
   AWS Security Hub is a cloud security posture management (CSPM) service that performs security best practice checks, aggregates alerts, and enables automated remediation.

8. **AWS Config:-**
   AWS Config continually assesses, audits, and evaluates the config rations and relationships of your resources on AWS, on premises, and on other clouds.

9. **S3 bucket:-**
   Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can store and protectany amount of data for virtually any use case, such as data lakes, cloud- native applications, and mobile apps. With cost-effective storage classes and easy-to-use management features, you can optimize costs, organize data, and configure fine-tuned access controls to meet specific business, organizational, and compliance requirements.

10. **AWS CLI:-**

The AWS Command Line Interface (AWS CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

The AWS CLI v2 offers several new features including improved installers, new configuration options such as AWS IAM Identity Center (successor to AWS SSO), and various interactive features

11. **IAM:-**

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

12. **Jenkins:-**

Jenkins offers a simple way to set up a continuous integration or continuous delivery (CI/CD) environment for almost any combination of languages and source code repositories using pipelines, as well as automating other routine development tasks. While Jenkins doesn't eliminate the need to create scripts for individual steps, it does give you a faster and more robust way to integrate your entire chain of build, test, and deployment tools than you can easily build yourself.

13. **DefectDojo:-**

Defect Dojo is a security orchestration and vulnerability management platform. Defect Dojo allows you to manage your application security program, maintain product and application information, triage vulnerabilities and push findings to systems like JIRA and Slack. DefectDojo enriches and refines vulnerability data using a number of heuristic algorithms that improve with the more you use the platform.

What is Compliance: Compliance is all about meeting a set of rules or standards. Information security is concerned with protecting the confidentiality, integrity, and availability of information and technology assets within an organization. So, information security compliance means meeting rules or standards about the protection of data and information. There will be a number of government, industry, and other regulations for any organization that determine the specific security requirements for data and information. Ensuring information security compliance, including IT security compliance, is a vital component of any information security system. Infosec compliance is partly driven by the need to meet the needs of any external regulatory organizations for information security,including any national information security applicable laws andregulations. But information security compliance within an organization must also be driven by the desire to avoid being disrupted by data and security breaches.

What is PCI DSS: The PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources forsafe payments worldwide. The PCI SSC mission is to enhance global payment account data security by developing standards and supporting

services that drive education, awareness, and effective implementation by stakeholders. To achieve this with a strategic framework to guide the decision-making process and ensure that every initiative is aligned with the mission and supports the needs of the global payments industry. The four pillars PCI DSS strategic frame work include:

- Increase industry participation and knowledge in the PCI Standards development process and stakeholder support for standard simple mentation. This ensures that standards and resources reflect and address industry needs and challenges.

- Evolve security standards and validation programs to support a range of environments, technologies and methodologies for achieving security.This ensures standards and resources that support and enable safe commerce and the flexibility to use different approaches to meet those standards.

- Secure emerging payment channels via development of PCI Standards and resources to support broader payment acceptance. This enables safe commerce in new and emerging card and card-based payment channels such as mobile and internet-of-things.

- Increase standards alignment and consistency of PCI Stand rds to minimize redundancy and support effective implementation.

What is PA DSS: Payment Application Data Security Standard (PA-DSS) is a set of requirements intended to help software vendors develop secure payment applications for credit card transactions. This ensures that companies do not store prohibited data, such as the securityPIN, magnetic strip or CVV2. PA-DSS applies to third-party applications that store, process or transmit payment cardholder data as part of an authorization or settlement. PCI DSS compliance is required by all credit card brands, such as American Express, Mastercard, JCB International and Visa Inc. However, the same is not mandated by law.

Architecture

We will be deploying an EC2 instance which will act as server for abank payment gateway and would be loaded up with all the compliances required for its security.

Which Operating System to Use?

The first step is choosing the correct operating system. During our research we found that Ubuntu would be the perfect operating system to be used as it is arock-solid, well-supported operating system.It's u ed by multiple departments to address multiple problems, from security to database to logging. It's very easy to maintain, and it's also very secure. Red Hat Enterprise Linux has built-in security features such as Security-Enhanced Linux (SELinux) and mandatory access controls (MAC) tohelp you combat intrusions and meet regulatory compliance. Using a supported, enterprise open source OS, like Red Hat Enterprise Linux, means that thousands of developers are monitoring millions of lines of code in the Linux kernel—finding flaws and developing fixes before vulnerabilities become problems. And with Linux kernel live patching, security patch scan be applied without down time. Red Hat has dedicated teams of experts verifying those bug fixes and deploying patches without interrupting your applications.

What Compliances and Guidelines to follow?

We will be following the PCI DSS compliances, CIS AWS Foundations Benchmark, AWS Foundational Security Best Practices. Below we have mentioned each compliance we are following:

PCI-DSS Guidelines

CIS AWS Foundations Benchmark

AWS Foundational Security Best Practices

How are we following these Compliances and Guidelines?

We will be listing all the compliances one by and explaining how are we going to follow them:

PCI-DSS Guidelines

1. Install and maintain a firewall configuration to protect card holder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored card holder data.
4. Encrypt transmission of card holder data across open, public networks.
5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to card holder data by business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to card holder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

CIS-Benchmark

1. Identity and Access Management
2. Logging
3. Monitoring
4. Networking

SYSTEM REQUIREMENTS

Requirements

- EC2Instance

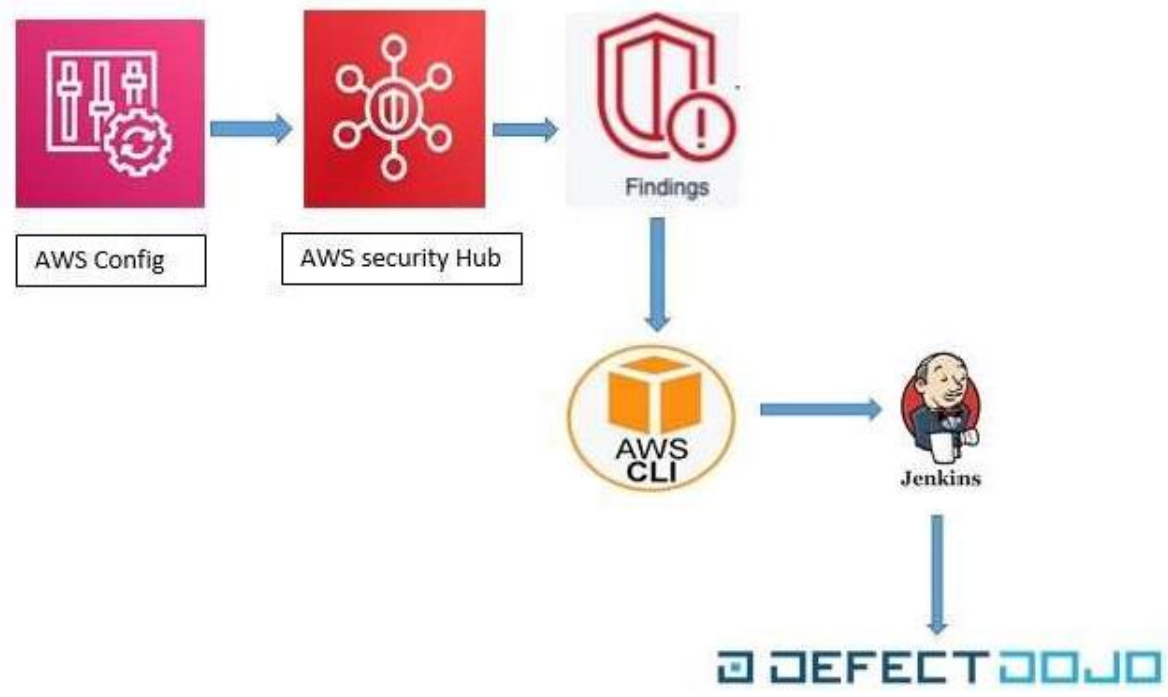
OperatingSystem

- Ubuntu

HardwareRequirements

- RAM upto 4GB
- Typet2.medium
- Hard disk 30GB
- Processor8vCPUs
- ArchitectureX86_64

Working Flow of Project



WORKING OF PROJECT

AWS SECURITY HUB

AWS Security Hub is a comprehensive security management service provided byAmazon WebServices(AWS) to help users centrally manage and prioritize security findings across their AWS environment. It acts as a hub for aggregating, organizing, and prioritizing security alerts and findings from various AWS services and third-party integrations.

AWS CONFIG

AWS Config and AWS Security Hub are two AWS services that can work together to provide a comprehensive solution for ensuring compliance and security within your AWS environment.

AWS Findings

AWS Security Hub continuously evaluates the configuration settings of your AWS resources against a set of predefined security standard sand compliance benchmarks.Security Hub aggregates findings from multiple AWS services that perform compliance checks.

AWS Command Line Interface(CLI)

The AWS Command Line Interface (CLI) is a unified tool provided by Amazon Web Services(AWS)that allows you to manage various AWS services and resources from the command line of your terminal or command prompt.
Through AWS CLI, we loggedin in our terminal with the credential of AWS IAM Administrator who has given a programmatic access.
With the help of AWS CLI we gathered all the findings generated in the security hub after running compliance check on different frameworks. These findings are stored in a **JSON** format.

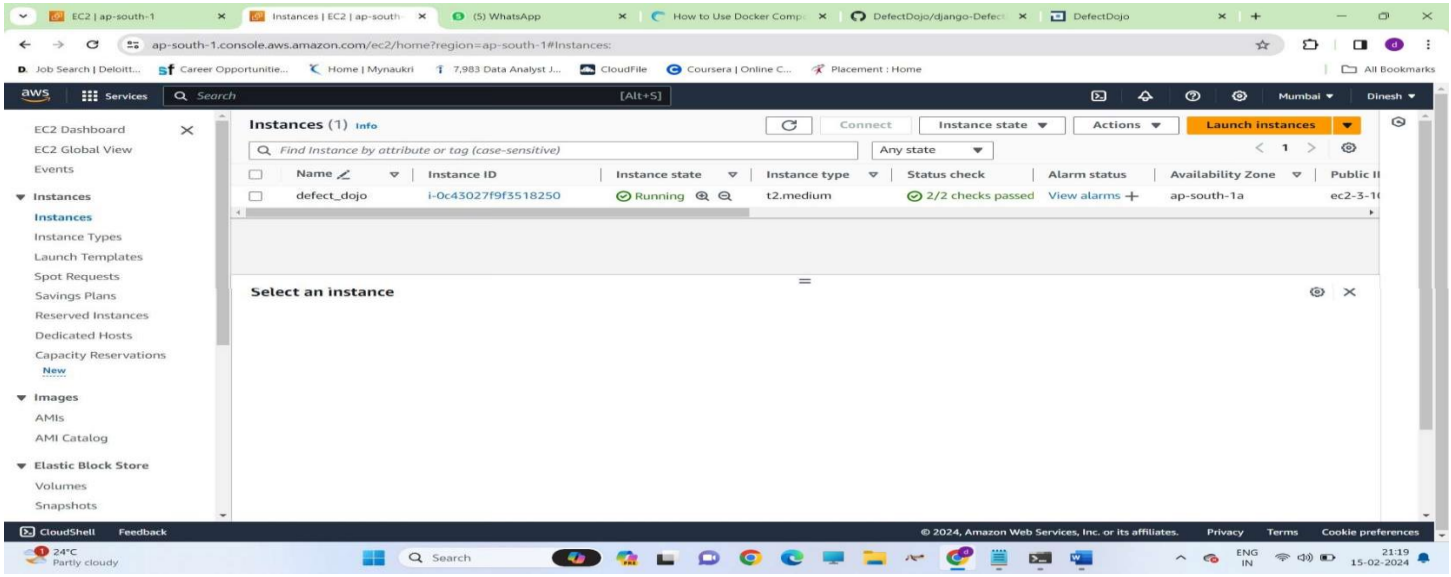
Defectdojo

The next step is integration of Defectdojo with the AWS Security Hub, for this Defectdojo provides add product optionwhere we can add different tools to integrate with Defectdojo.We added Securityhub and then engagement is created to parse to all the findings generated through AWS Security Hub.
In order to parse the findings from securityhub in Defectdojo we have used HTTP Post method. After gathering all the findings from AWS CLI in JSON format,through HTTP Postmethod this Json file is parsed to Defectdojo.
We have created a Linux shell Script to automate this process of gathering all the findings in Json file and then parsing this findings to Defectdojo through HTTP Post mehod.

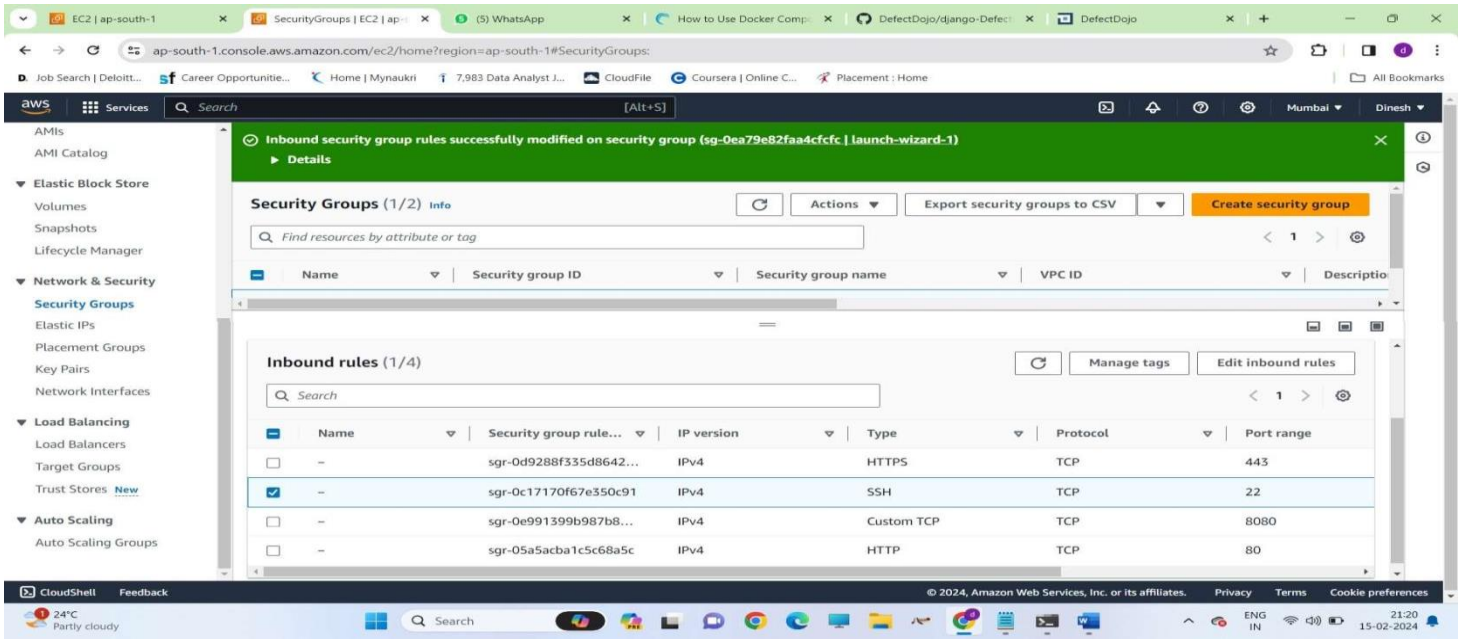
Jenkins

This whole process is automated with Jenkins. In order to integrate jenkin server with AWS Security Hub we have created a role and gave full access of AWS Security Hub to Jenkins server. We have use AWS Credential plugin in Jenkins. When ever new findings or failed security check occur at AWS Security hub according to compliance framework Jenkins will automatically use build trigger and automatically creates a json file and parse this findings to defectdojo so that we Can Continuously monitor AWS Infrastructure Security Checks.

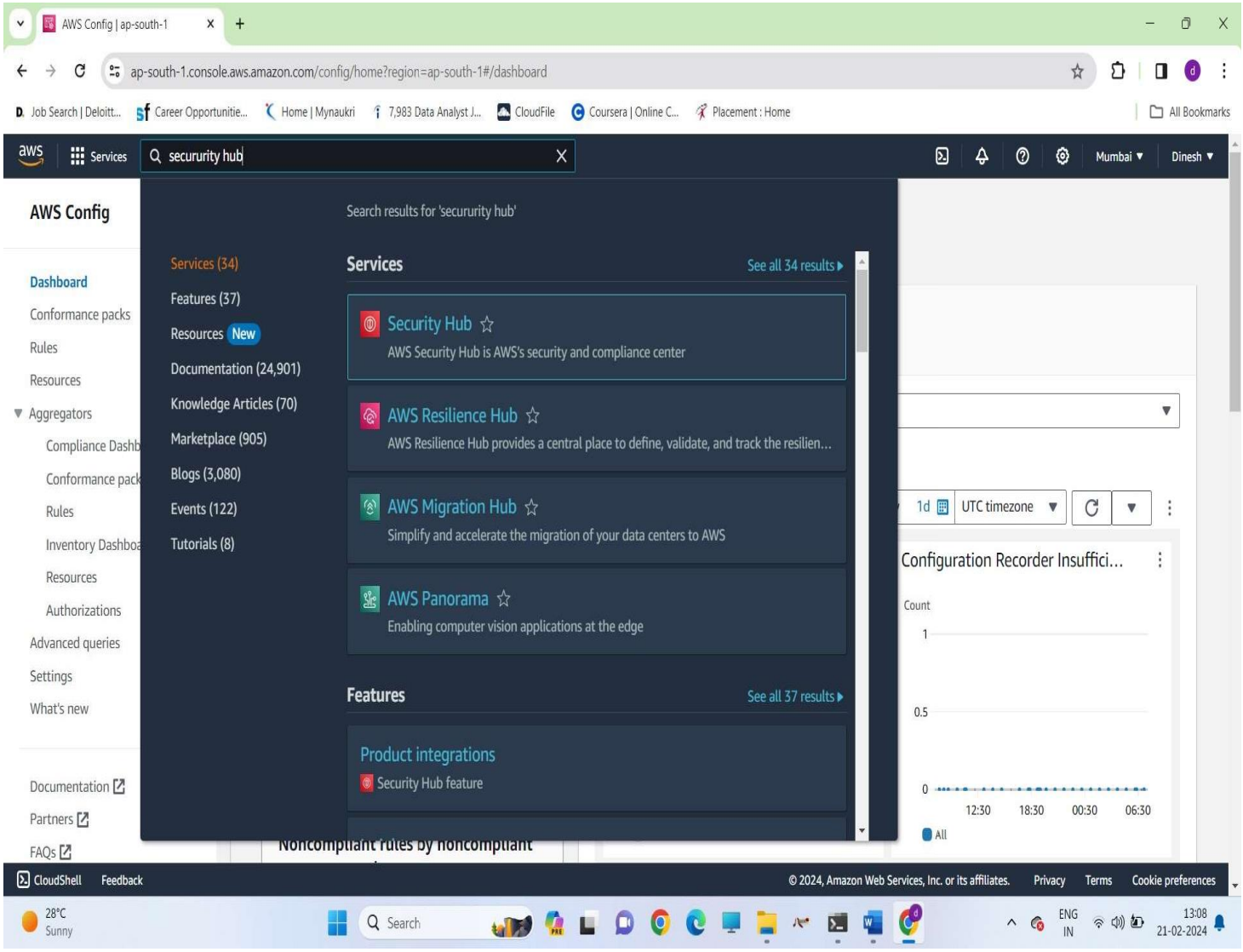
SCREENSHOTS



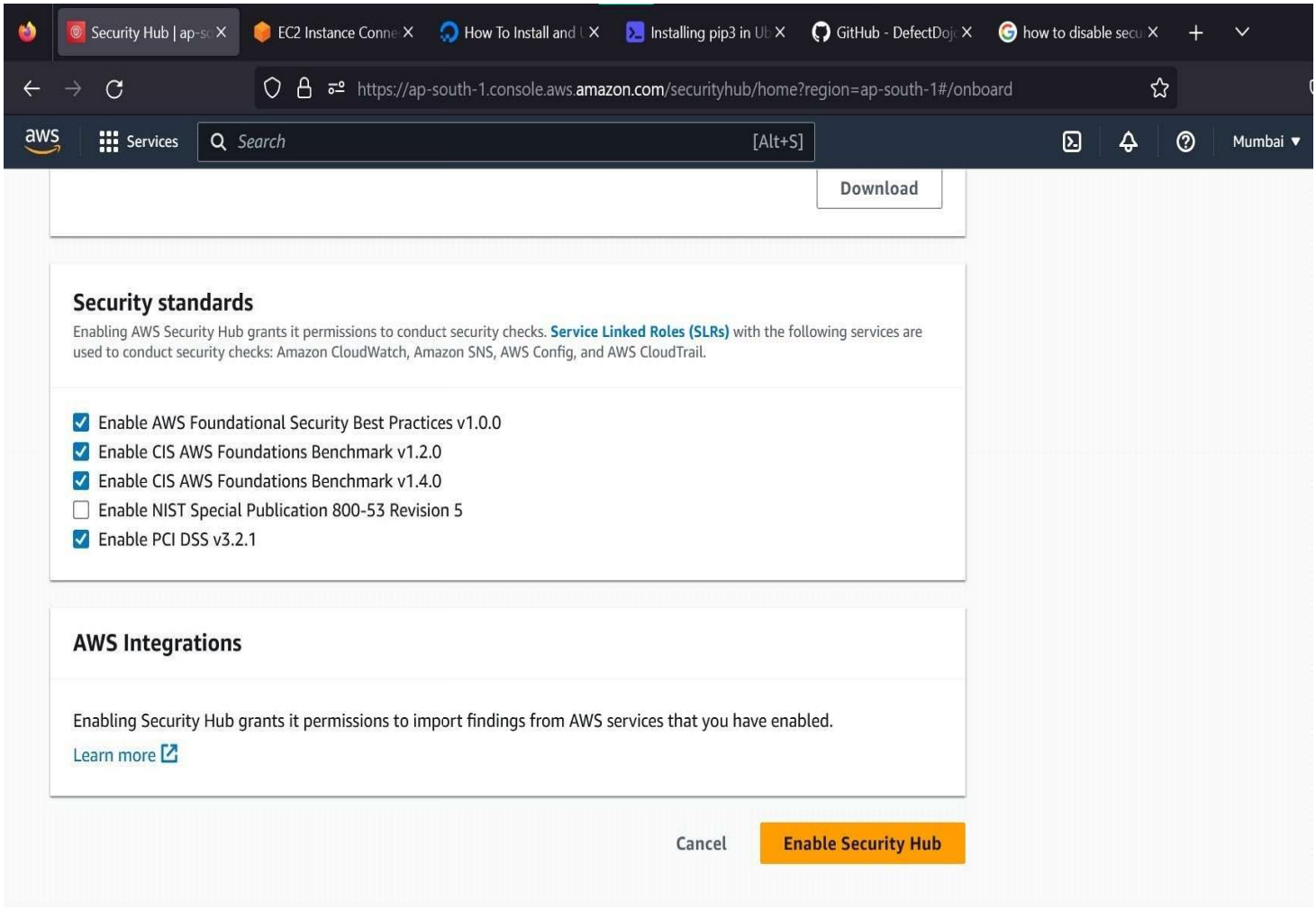
EC2 instances



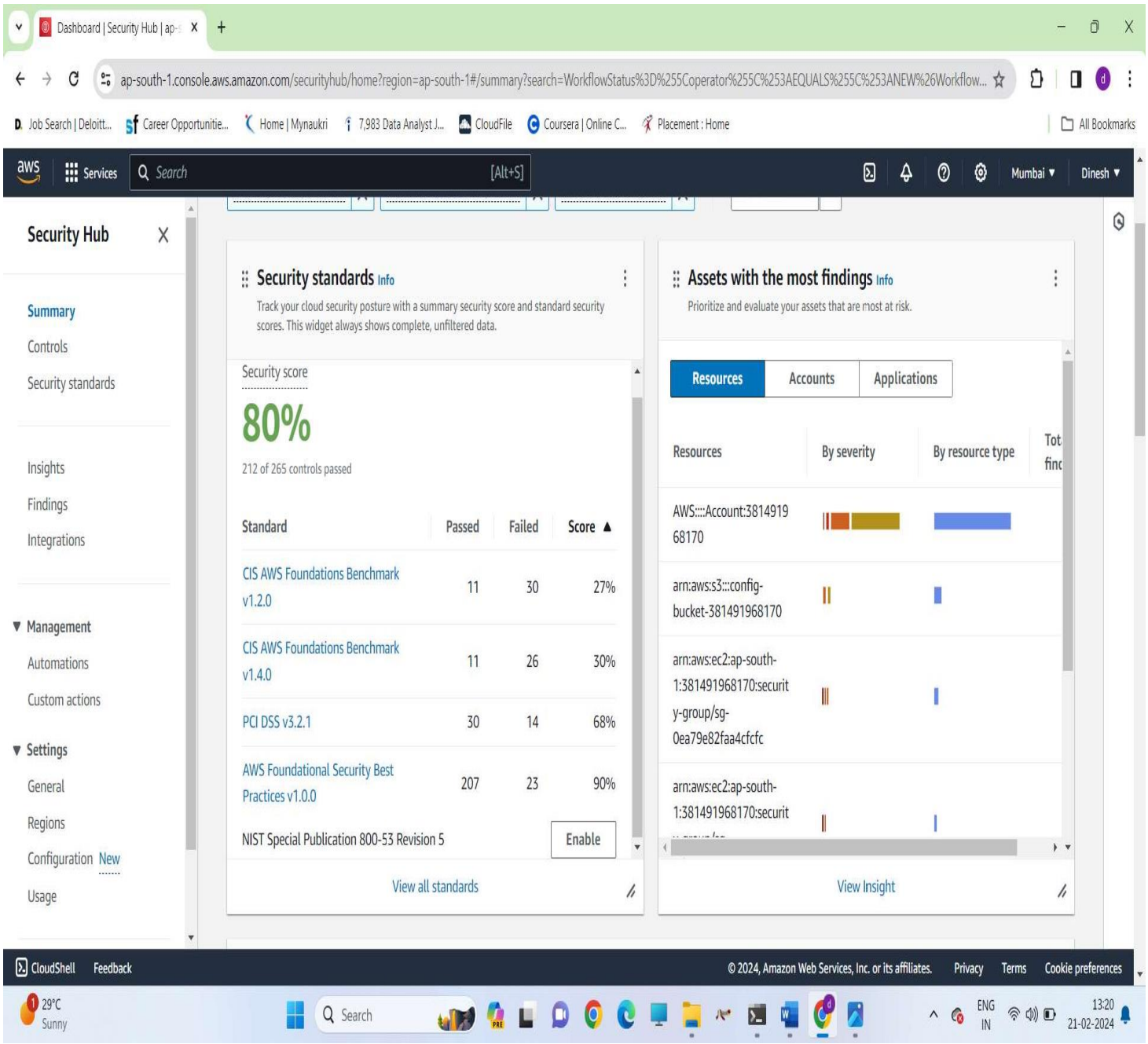
Adding TCP rule to Inbounds rules



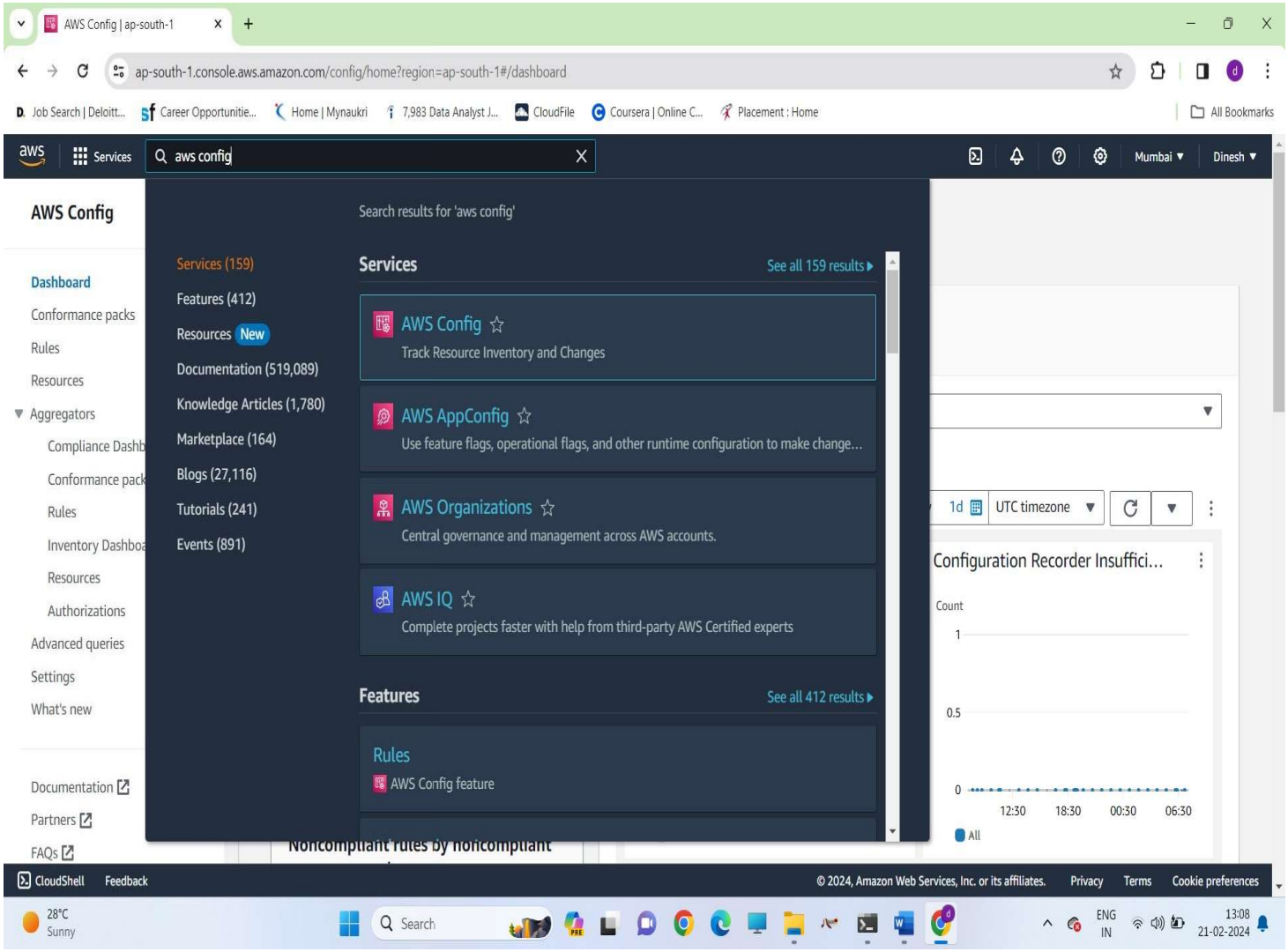
Setup the Security Hub



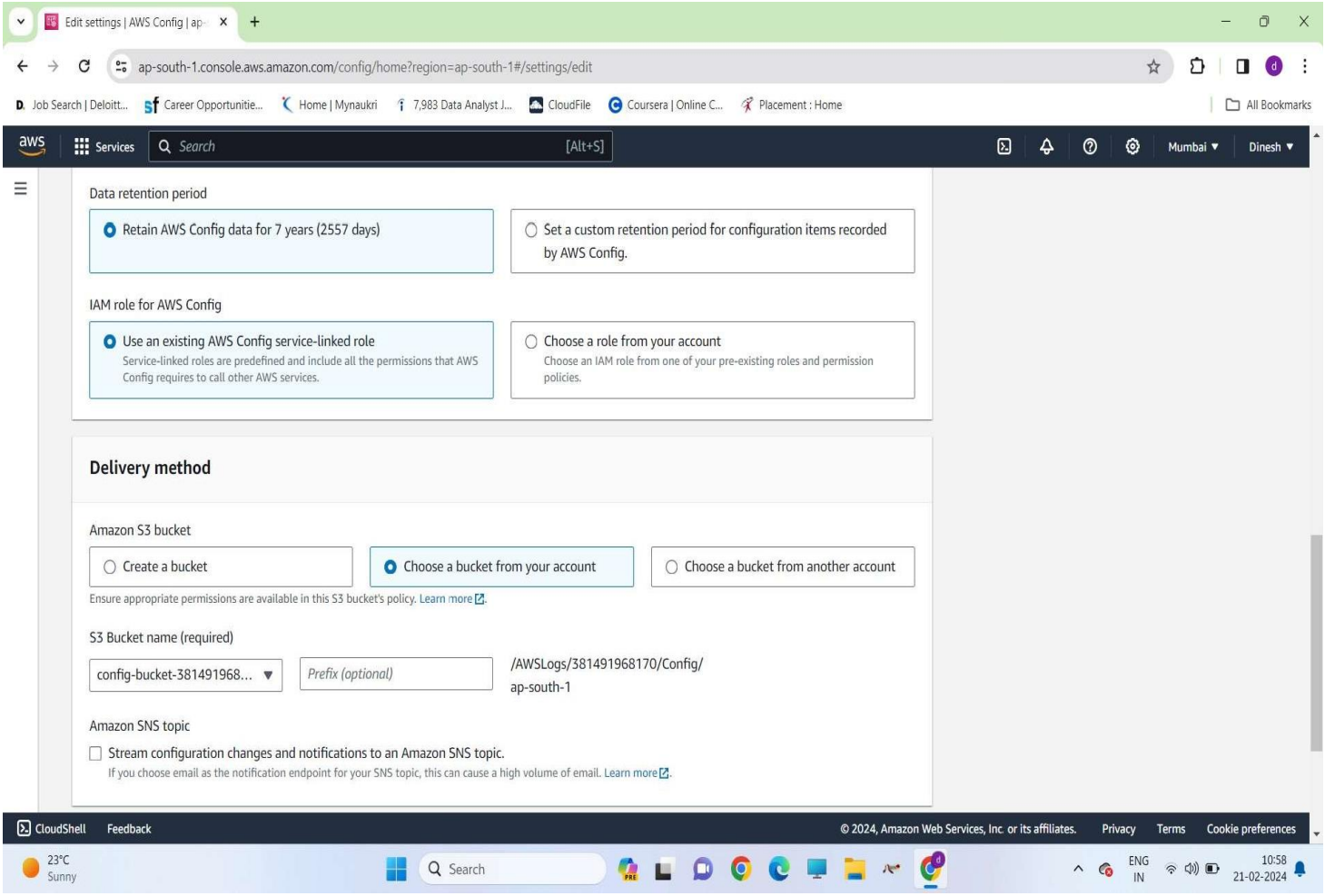
Enable the Standard



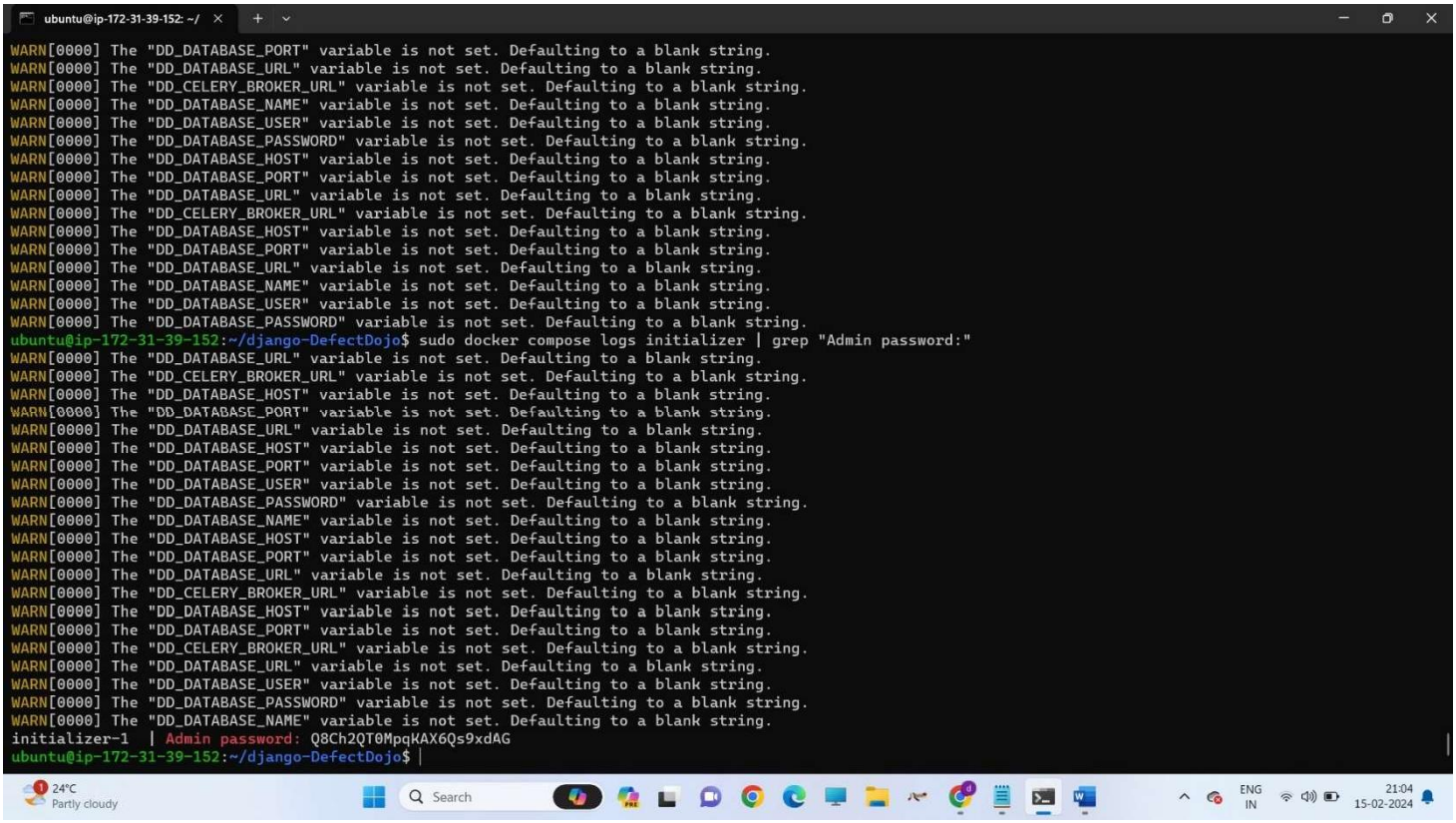
Security score

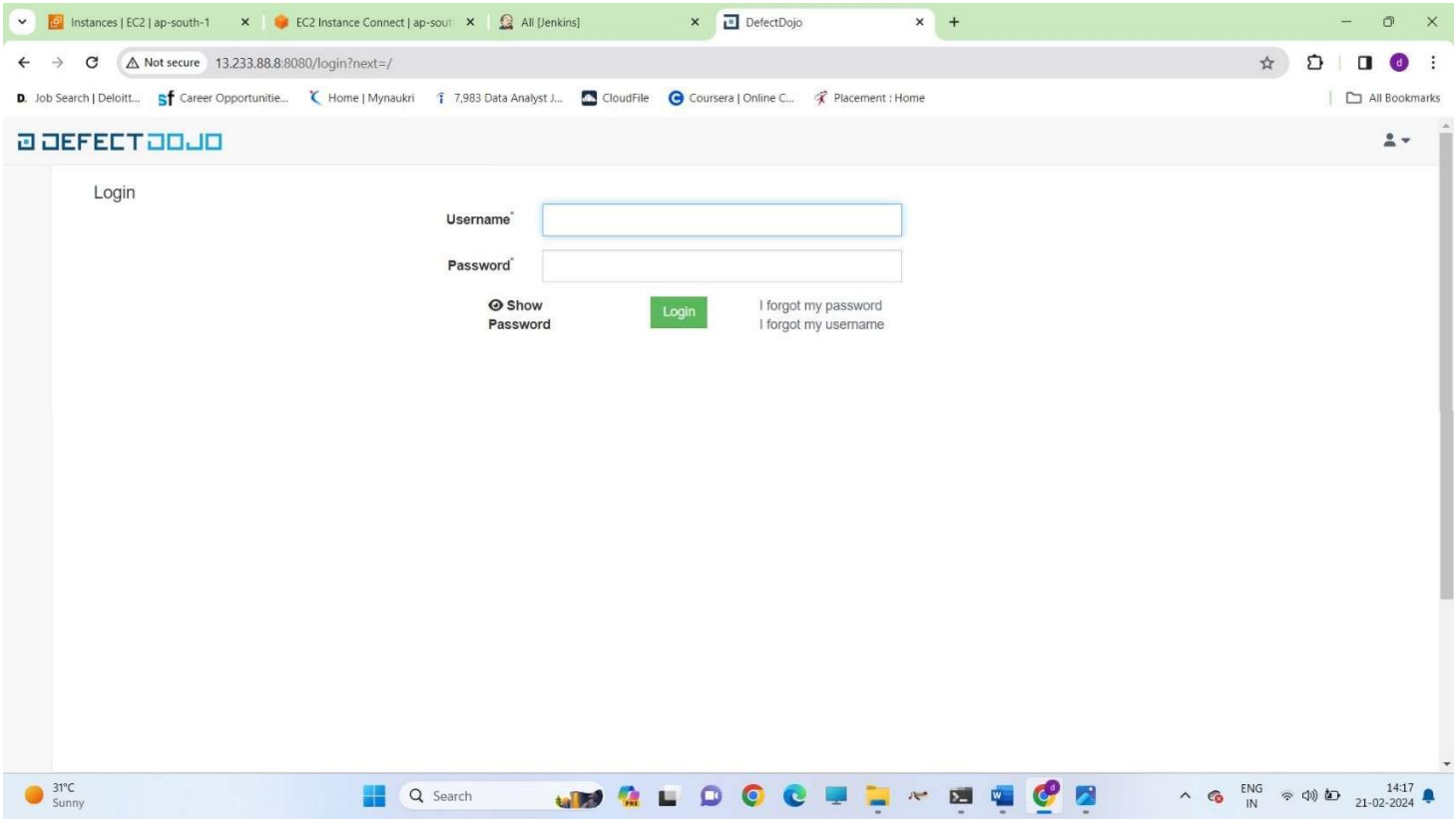


Enable AWS Config for active

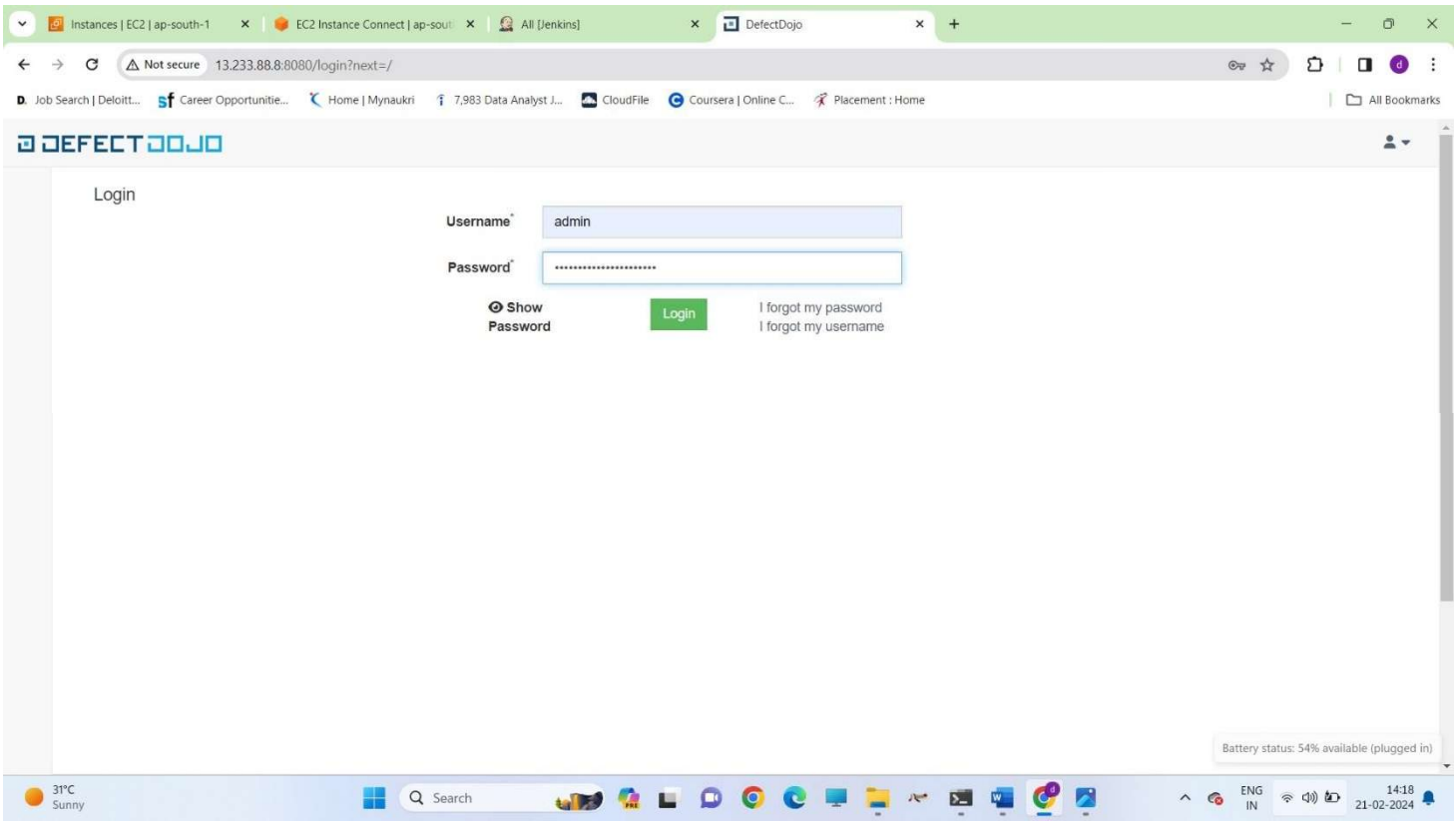

Edit settings | AWS Config | ap-
ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/settings/edit
Job Search | Deloitt...
Career Opportunitie...
Home | Mynaukri
7,983 Data Analyst J...
CloudFile
Coursera | Online C...
Placement : Home
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
Dinesh
Data retention period
Retain AWS Config data for 7 years (2557 days)
Set a custom retention period for configuration items recorded by AWS Config.
IAM role for AWS Config
Use an existing AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.
Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.
Delivery method
Amazon S3 bucket
Create a bucket
Choose a bucket from your account
Choose a bucket from another account
Ensure appropriate permissions are available in this S3 bucket's policy. Learn more
S3 Bucket name (required)
config-bucket-381491968...
Prefix (optional)
/AWSLogs/381491968170/Config/
ap-south-1
Amazon SNS topic
Stream configuration changes and notifications to an Amazon SNS topic.
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. Learn more
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
23°C
Sunny
Search
ENG
IN
10:58
21-02-2024

After implementation of defectdojo , create a username and password of defect dojo

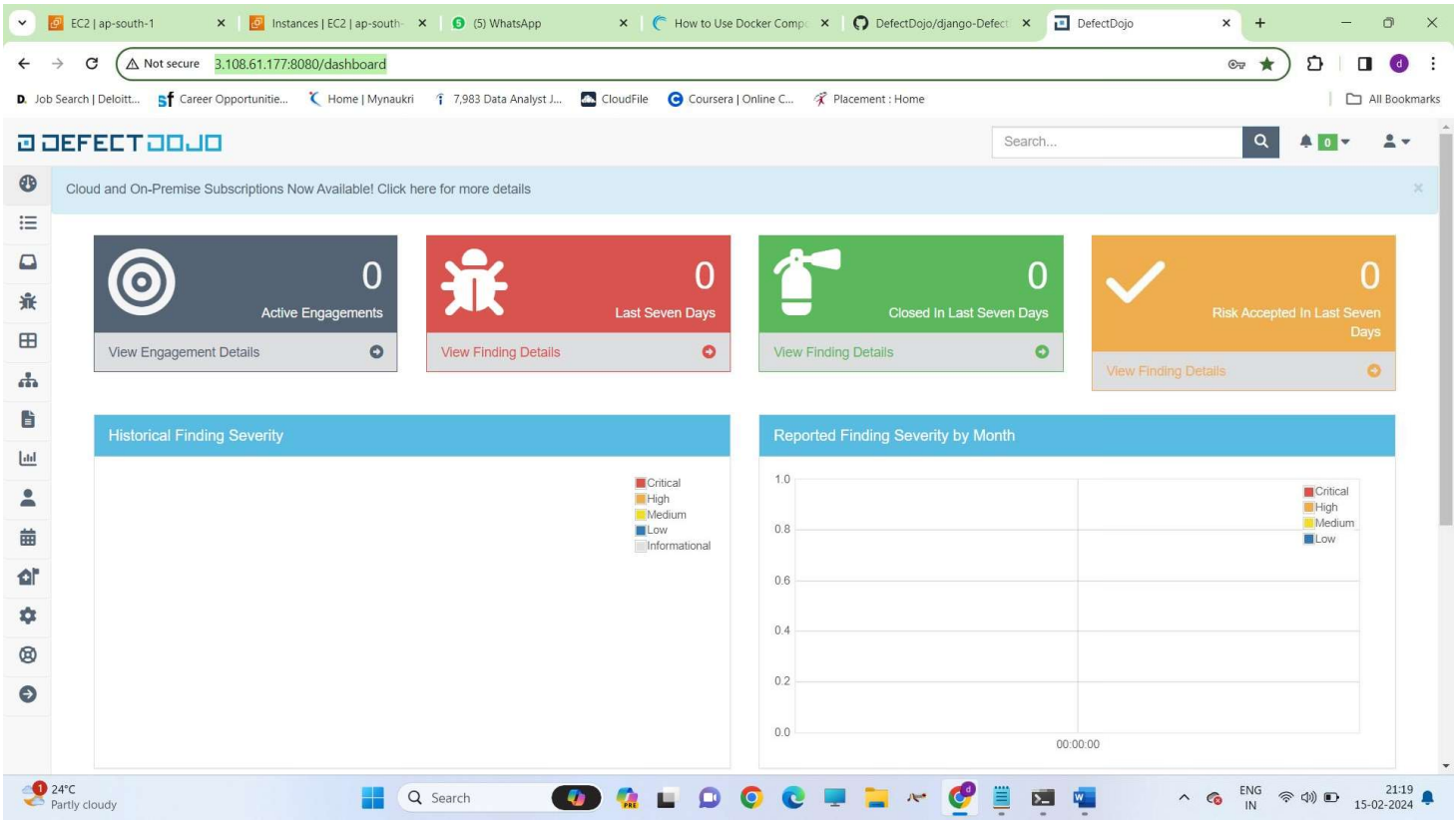




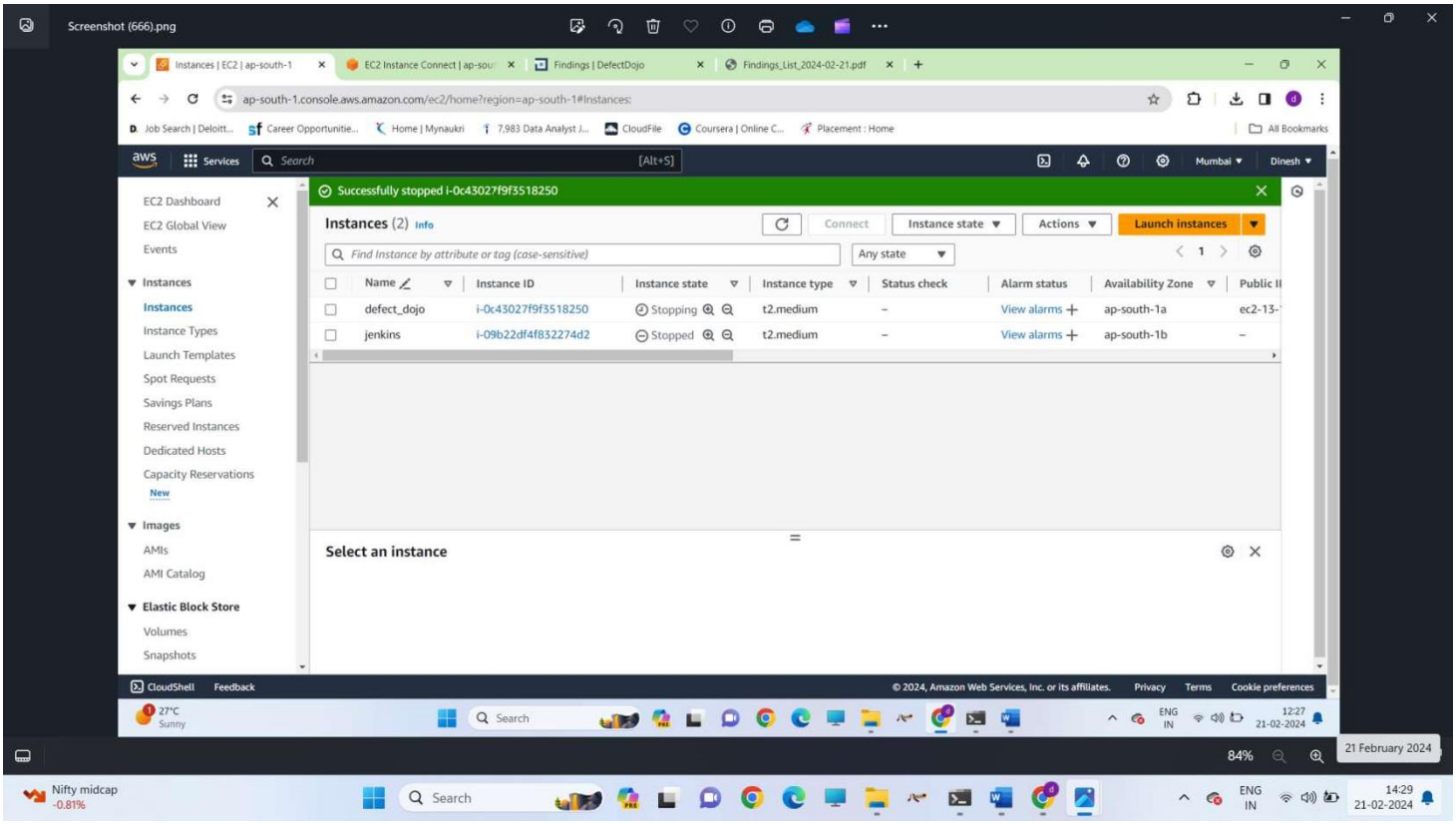
Navigate to http://public_ip:8080



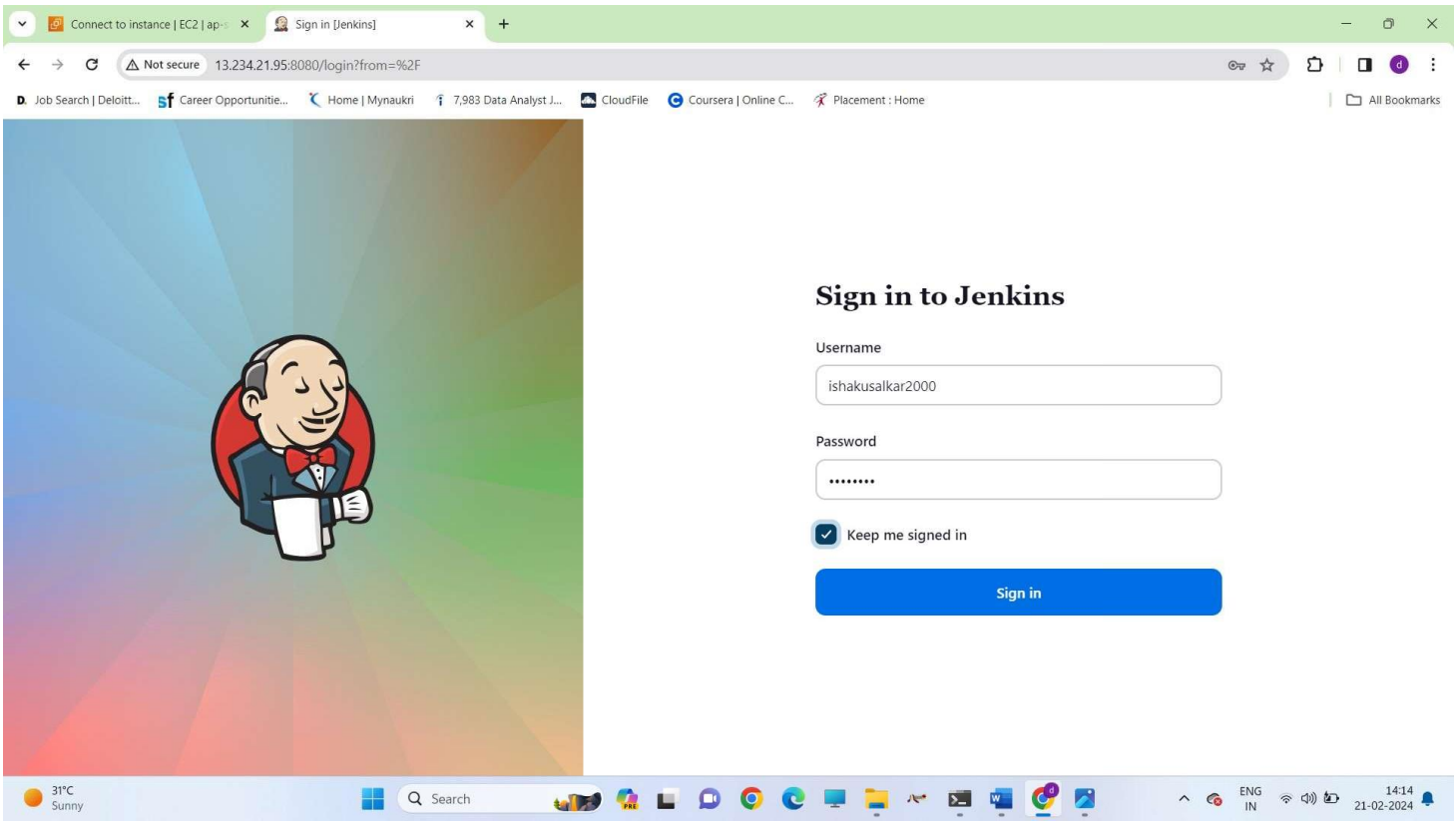
Grep the admin password from docker-compose logs initializer



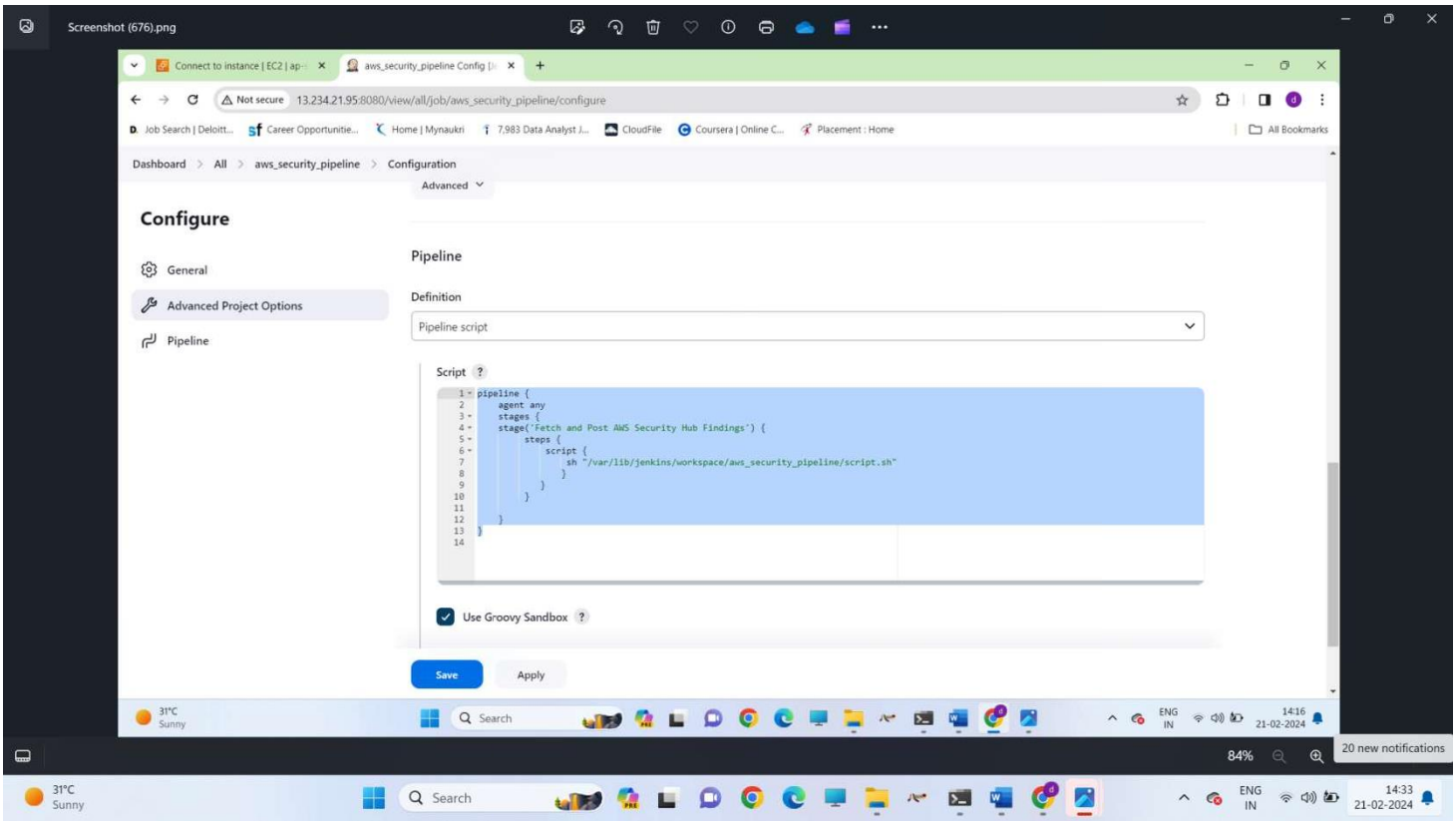
Defect dojo Dashboard



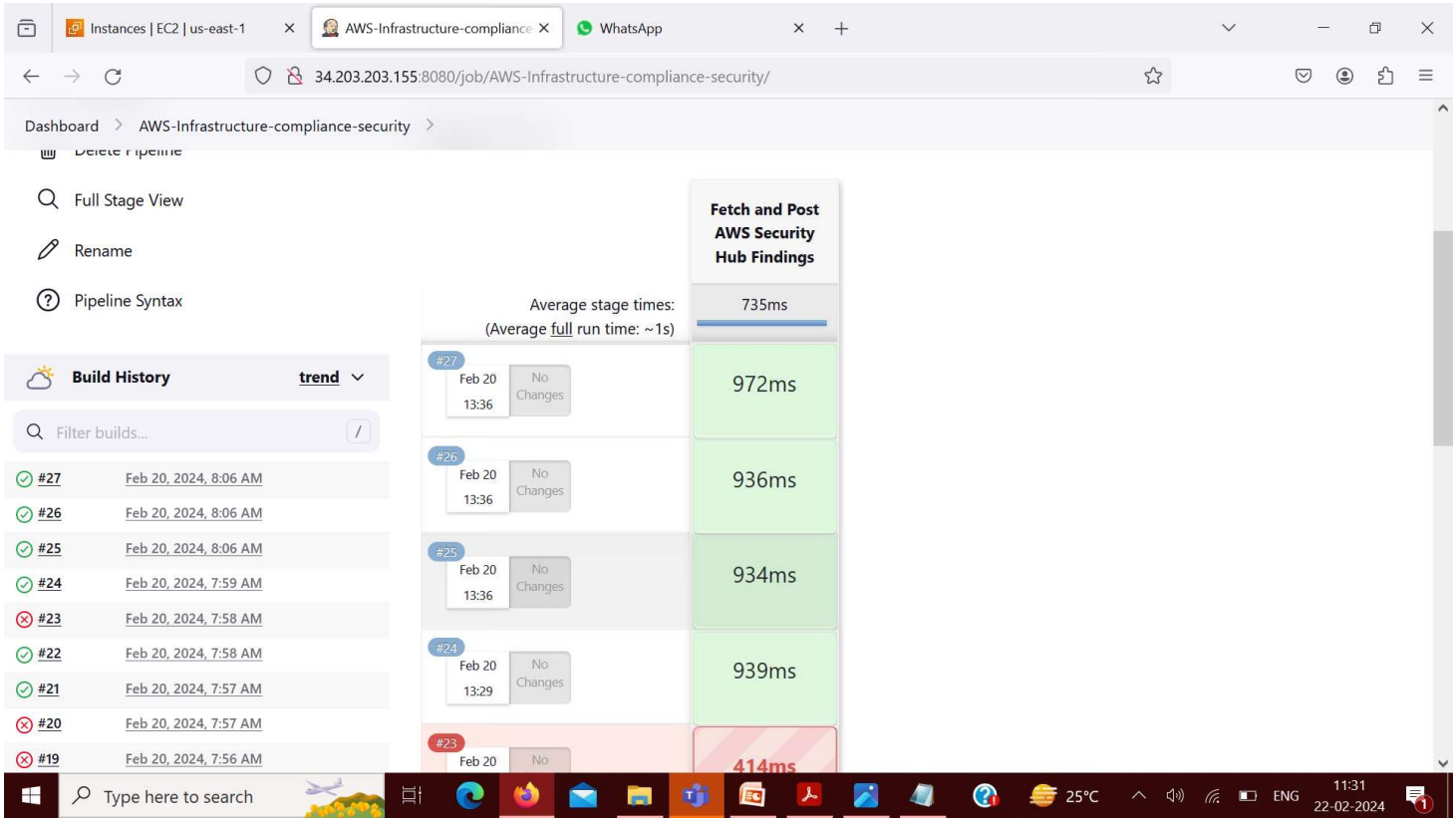
Create another EC2 instance for install jenkin



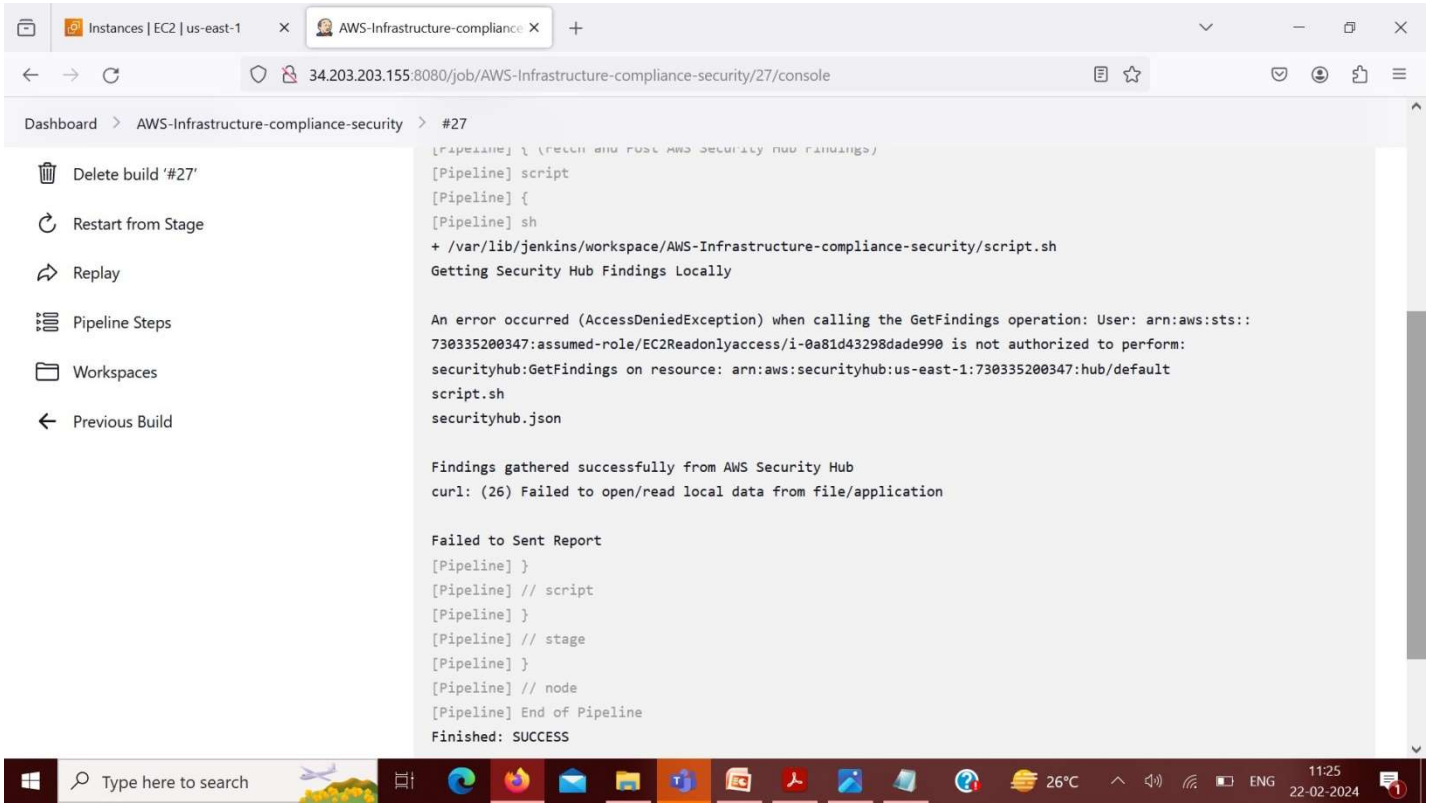
Sign in to Jenkin



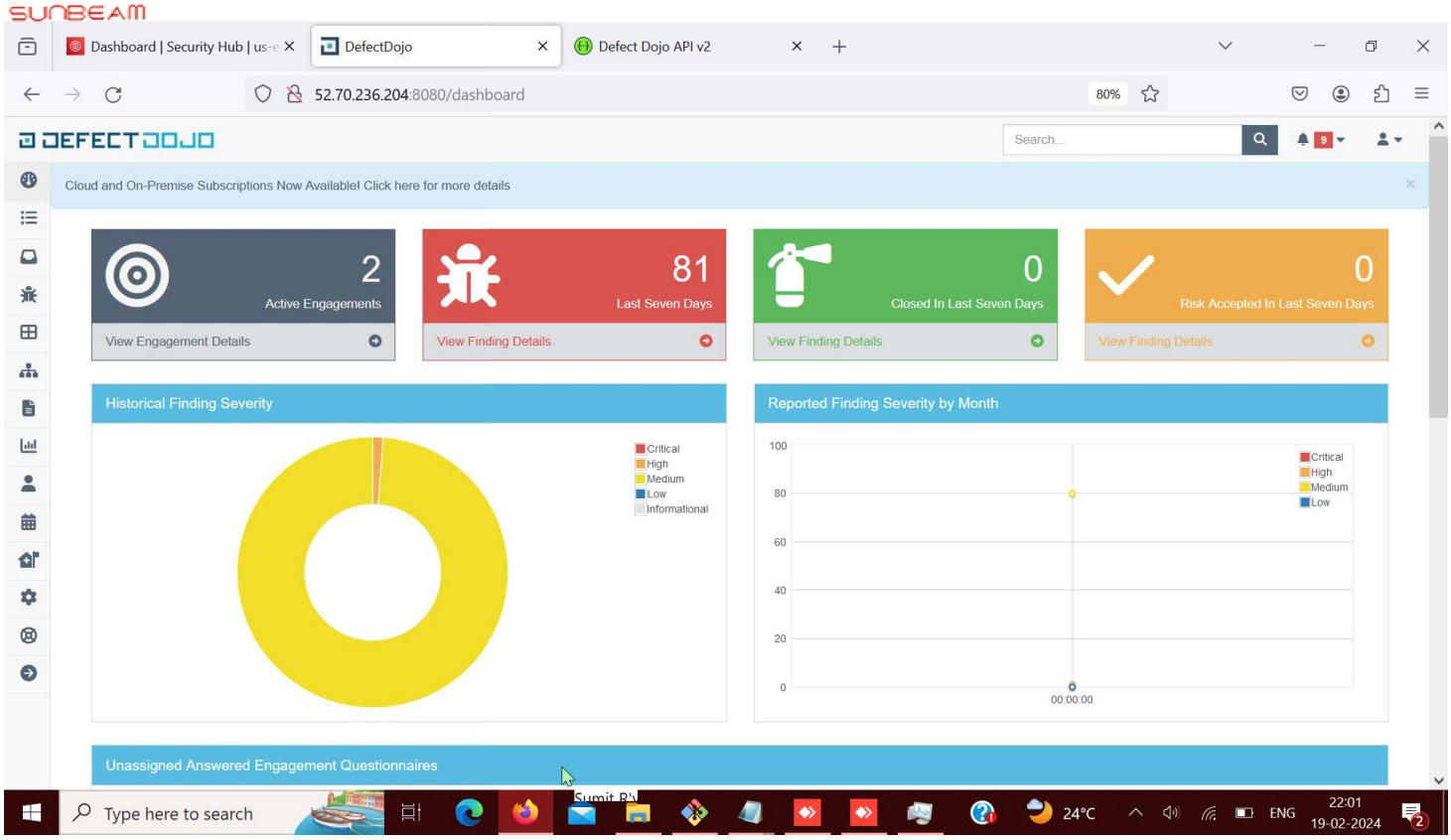
Write script for pipeline



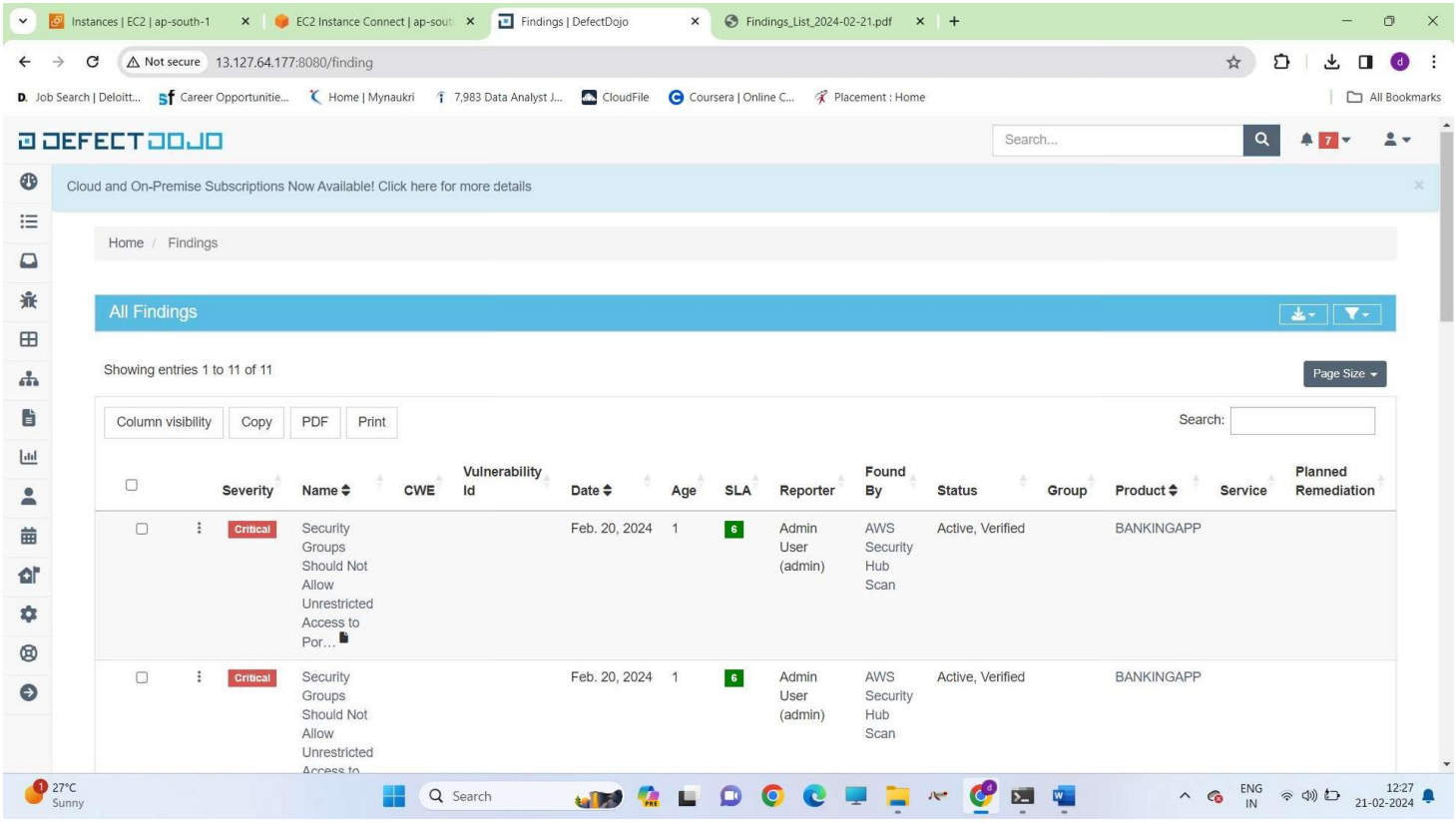
Build pipeline



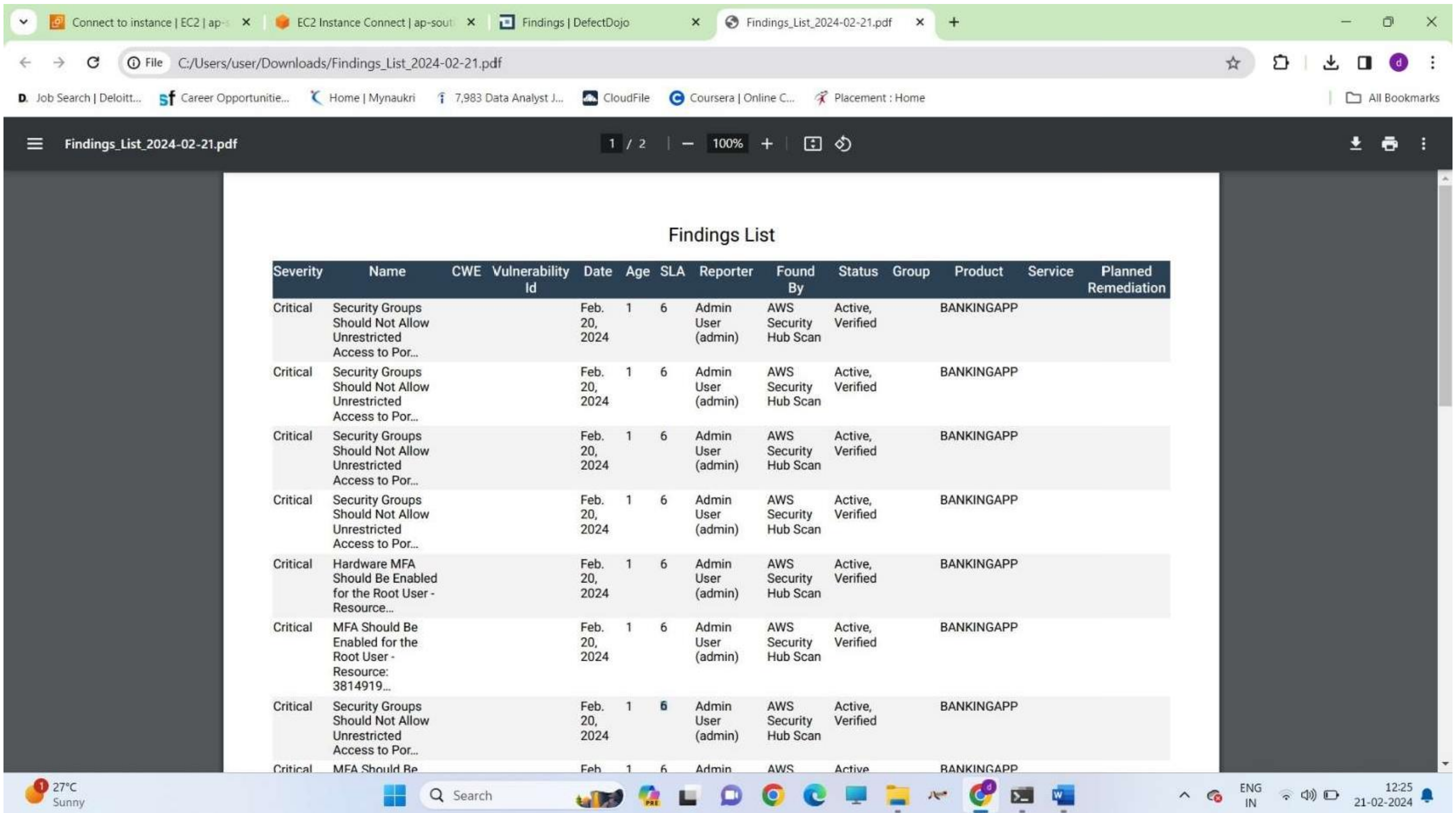
Console output



Defect-Dojo Dashboard



Details information of Finding



Findings List

Severity	Name	CWE	Vulnerability Id	Date	Age	SLA	Reporter	Found By	Status	Group	Product	Service	Planned Remediation
Critical	Security Groups Should Not Allow Unrestricted Access to Por...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	Security Groups Should Not Allow Unrestricted Access to Por...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	Security Groups Should Not Allow Unrestricted Access to Por...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	Security Groups Should Not Allow Unrestricted Access to Por...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	Hardware MFA Should Be Enabled for the Root User - Resource...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	MFA Should Be Enabled for the Root User - Resource: 3814919...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	Security Groups Should Not Allow Unrestricted Access to Por...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	MFA Should Be			Feb.	1	6	Admin	AWS	Active		BANKINGAPP		

REPORT GENERATES

CONCLUSION & FUTURE SCOPE

Conclusion:

A secure AWS Infrastructure is assured with the compliance checks and udit ready report generated in order to remediate findings and triage vulnerabilities.

Future Scope:

We can add automated and custom remediation by applying rules in AWS lambda for our findings.

REFERENCES

1. https://aws.amazon.com/
2. https://www.digitalocean.com/
3. http://www.docker.net/
4. https://www.defectdojo.com/
5. https://www.github.org/
6. https://www.jenkins.com/