



SUNBEAM
Exploring New Ideas Reaching New Heights

सौरी डैक
CDAC अॅक्टर्स
acts
Authorized Training Centre

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



SUNBEAM
Exploring New Ideas Reaching New Heights

सौर डैक
CDAC अॅक्टर्स
acts
Authorized Training Centre

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
(230944223042)

Priyanka Kumari
(230944223028)

Kusalkar Isha Maruti
(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 guidance to work on this project. Her guidance and support helped us to overcome various obstacles and intricacies during the course of project work.

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 day here in C-DAC ACTS, Pune.

Sincerely,

- 1) Siddhi
- 2) Priyanka Kumari
- 3) Kusalkar Isha Maruti



TABLE OF CONTENTS

1. Declaration

2. Certificate

3. Approval Certificate

4. Acknowledgement

5. Abstract

6. Introduction and Overview of Project

 1) Aims and Objective

7. Overall Description

 1) Introduction

 2) Architecture

8. System Requirements

9. Working and Screenshots

 1) Working Flow Diagram

 2) Working Description

 3) Screenshots

10. Conclusion & Future Scope

11. References



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 together 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 to liability have also influenced their development and implementation.

INTRODUCTION

Aims and Objective

Automating security compliances Infrastructure on 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 of these services is Amazon Elastic Compute Cloud (EC2), which allows users to have at their disposal a virtual cluster of computers, available all the time, through the Internet. AWS's virtual computers emulate most of the 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 operating systems; 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. Subscribers can pay 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 aspects of 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 broadest and deepest compute platform, with over 500 instances and choice 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 400 Gbps Ethernet networking. We offer the best price performance for machine learning training, as well as the lowest cost per inference 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 and flexible 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 ratios 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 protect any 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 and regulations. 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 for safe 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 Standards 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 security PIN, 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 a bank 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 a rock-solid, well-supported operating system. It's used 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) to help 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 patches can 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 one 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

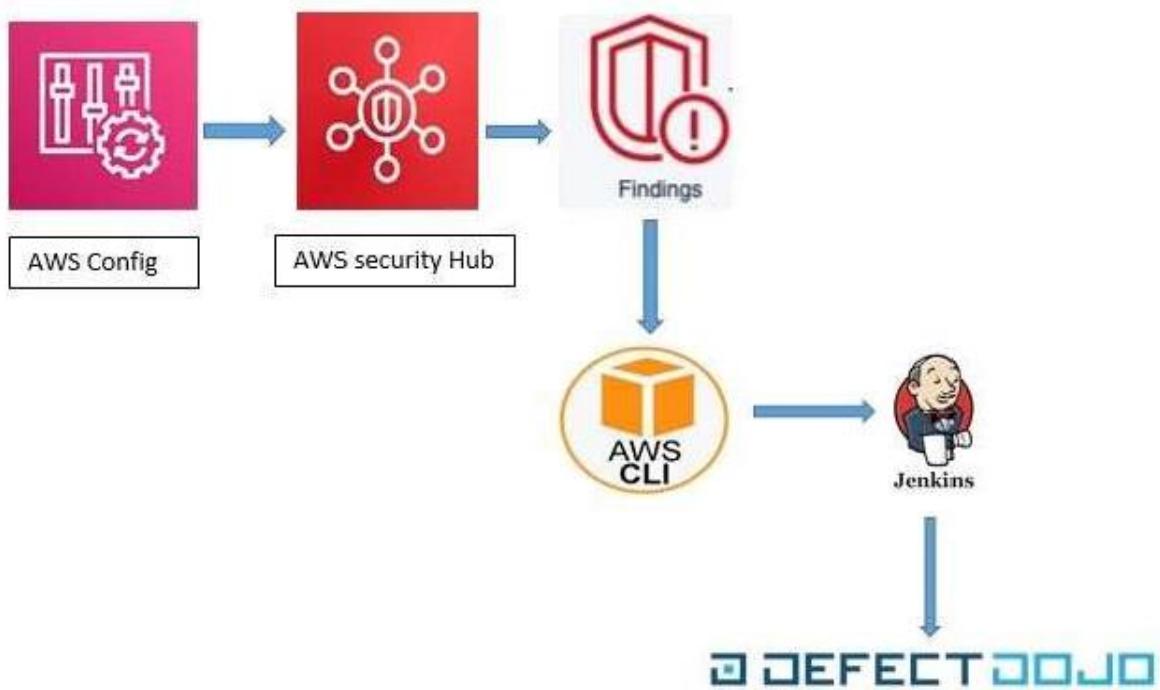
OperatingSystem

- Ubuntu

Hardware Requirements

- 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 by Amazon Web Services(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 option where 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 Post method 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 method.

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

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, and Elastic Block Store. The main content area displays a table titled 'Instances (1) info' with one row for the instance 'defect_dojo'. The instance details are: Name: defect_dojo, Instance ID: i-0c43027f9f3518250, Instance state: Running, Instance type: t2.medium, Status check: 2/2 checks passed, Alarm status: View alarms, Availability Zone: ap-south-1a, and Public IP: ec2-3-10. Below the table, a message says 'Select an instance'.

EC2 instances

The screenshot shows the AWS Security Groups page. The sidebar includes links for AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security (selected), Security Groups (selected), Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, Load Balancing, Load Balancers, Target Groups, Trust Stores, Auto Scaling, Auto Scaling Groups, CloudShell, and Feedback. A green success message at the top states 'Inbound security group rules successfully modified on security group (sg-0ea79e82faa4cfcc | launch-wizard-1)'. The main area shows a table for 'Security Groups (1/2) info' with one row. Below it, another table titled 'Inbound rules (1/4)' lists four rules:

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-0d9288f335d8642...	IPv4	HTTPS	TCP	443
<input checked="" type="checkbox"/>	sgr-0c17170f67e350c91	IPv4	SSH	TCP	22
-	sgr-0e991399b987b8...	IPv4	Custom TCP	TCP	8080
-	sgr-05a5acba1c5c68a5c	IPv4	HTTP	TCP	80

Adding TCP rule to Inbounds rules

AWS Config | ap-south-1

ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/dashboard

Job Search | Deloitte... Career Opportunitie... Home | Mynaukri 7,983 Data Analyst J... CloudFile Coursera | Online C... Placement : Home All Bookmarks

aws Services Q security hub X Mumbai Dinesh

AWS Config

Services (34)

- Dashboard
- Conformance packs
- Rules
- Resources
- Aggregators
 - Compliance Dashb...
 - Conformance pack...
 - Rules
 - Inventory Dashbo...
 - Resources
 - Authorizations
 - Advanced queries
 - Settings
 - What's new
- Documentation (24,901)
- Knowledge Articles (70)
- Marketplace (905)
- Blogs (3,080)
- Events (122)
- Tutorials (8)

Search results for 'security hub'

Services See all 34 results ▾

- Security Hub** ☆
AWS Security Hub is AWS's security and compliance center
- AWS Resilience Hub** ☆
AWS Resilience Hub provides a central place to define, validate, and track the resilien...
- AWS Migration Hub** ☆
Simplify and accelerate the migration of your data centers to AWS
- AWS Panorama** ☆
Enabling computer vision applications at the edge

Features See all 37 results ▾

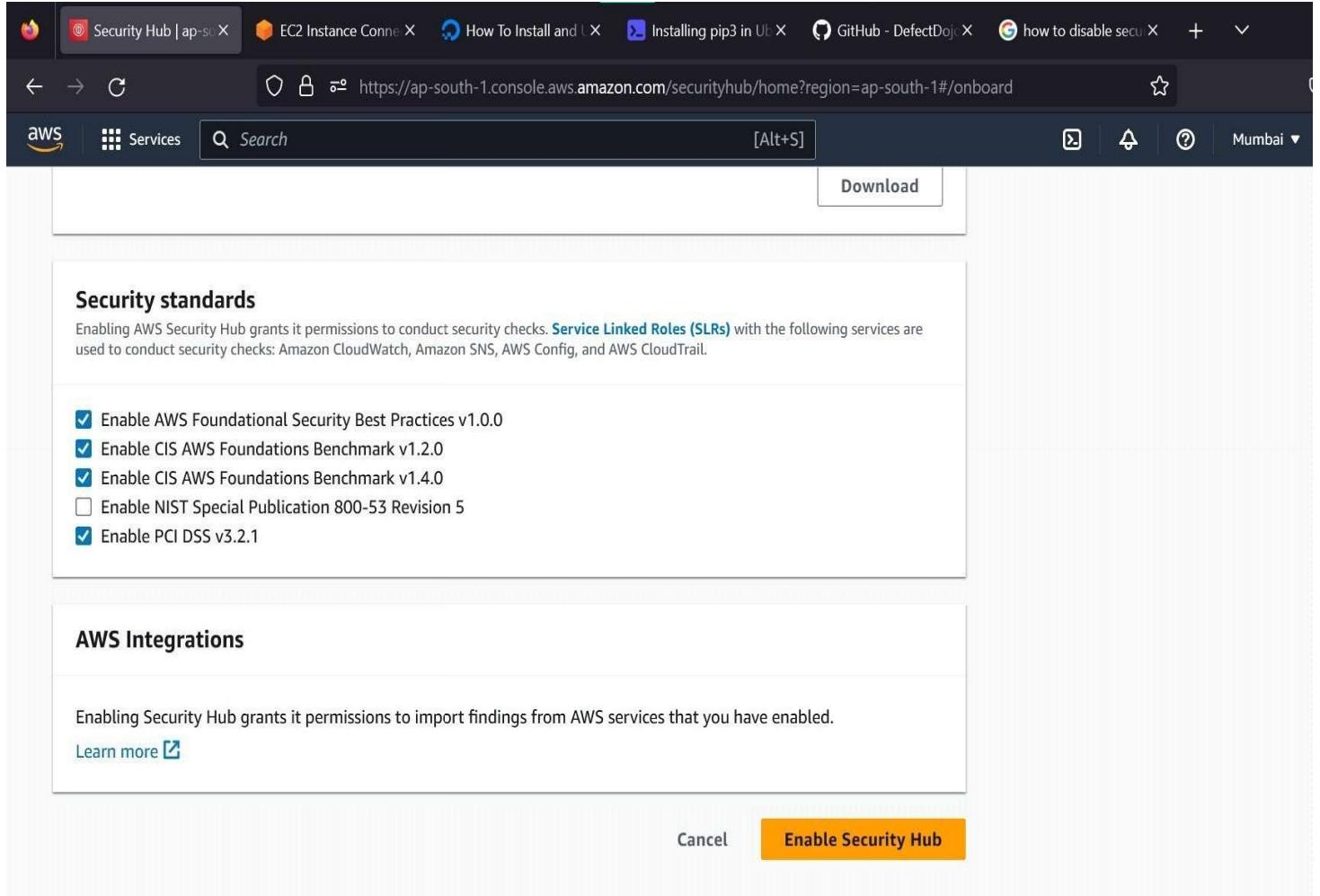
- Product integrations**
 - Security Hub feature

Noncompliant rules by noncompliant

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Sunny Search ENG IN 13:08 21-02-2024

Setup the Security Hub



The screenshot shows the AWS Security Hub Onboarding interface. At the top, there's a navigation bar with tabs like 'Security Hub | ap-south-1', 'EC2 Instance Connect', 'How To Install and...', 'Installing pip3 in U...', 'GitHub - DefectDojo...', 'how to disable se...', and others. Below the navigation bar is a header with the AWS logo, a 'Services' dropdown, a search bar, and a 'Download' button.

Security standards

Enabling AWS Security Hub grants it permissions to conduct security checks. **Service Linked Roles (SLRs)** with the following services are used to conduct security checks: Amazon CloudWatch, Amazon SNS, AWS Config, and AWS CloudTrail.

Enable AWS Foundational Security Best Practices v1.0.0
 Enable CIS AWS Foundations Benchmark v1.2.0
 Enable CIS AWS Foundations Benchmark v1.4.0
 Enable NIST Special Publication 800-53 Revision 5
 Enable PCI DSS v3.2.1

AWS Integrations

Enabling Security Hub grants it permissions to import findings from AWS services that you have enabled.

[Learn more](#)

Cancel **Enable Security Hub**

Enable the Standard

Dashboard | Security Hub | ap-south-1 | +

ap-south-1.console.aws.amazon.com/securityhub/home?region=ap-south-1#/summary?search=WorkflowStatus%3D%255Coperator%253AEQUALS%255C%253AWorkflow... ☆

Job Search | Deloitte... Career Opportunitie... Home | Mynaukri 7,983 Data Analyst J... CloudFile Coursera | Online C... Placement : Home All Bookmarks

aws Services Search [Alt+S] Mumbai Dinesh

Security Hub

- Summary
- Controls
- Security standards
- Insights
- Findings
- Integrations
- Management
 - Automations
 - Custom actions
- Settings
 - General
 - Regions
 - Configuration New
 - Usage

Security standards Info

Track your cloud security posture with a summary security score and standard security scores. This widget always shows complete, unfiltered data.

Security score

80%

212 of 265 controls passed

Standard	Passed	Failed	Score ▲
CIS AWS Foundations Benchmark v1.2.0	11	30	27%
CIS AWS Foundations Benchmark v1.4.0	11	26	30%
PCI DSS v3.2.1	30	14	68%
AWS Foundational Security Best Practices v1.0.0	207	23	90%
NIST Special Publication 800-53 Revision 5	Enable		

[View all standards](#)

Assets with the most findings Info

Prioritize and evaluate your assets that are most at risk.

Resources	By severity	By resource type	Total
AWS::Account:381491968170			100%
arn:aws:s3::config-bucket-381491968170			100%
arn:aws:ec2:ap-south-1:381491968170:security-group/sg-0ea79e82faa4cfefc			100%
arn:aws:ec2:ap-south-1:381491968170:security-group/sg-0ea79e82faa4cfefc			100%

[View Insight](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

29°C Sunny ENG IN 13:20 21-02-2024

AWS Config | ap-south-1

ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/dashboard

Job Search | Deloitte... Career Opportunitie... Home | Mynaukri 7,983 Data Analyst J... CloudFile Coursera | Online C... Placement : Home

All Bookmarks

AWS Services Q aws config X Mumbai Dinesh

AWS Config

Dashboard Conformance packs Rules Resources Aggregators Compliance Dashb Conformance pack Rules Inventory Dashboard Resources Authorizations Advanced queries Settings What's new Documentation Partners FAQs

Services (159) Features (412) Resources (New) Documentation (519,089) Knowledge Articles (1,780) Marketplace (164) Blogs (27,116) Tutorials (241) Events (891)

Search results for 'aws config'

Services See all 159 results ▶

- AWS Config** ☆ Track Resource Inventory and Changes
- AWS AppConfig** ☆ Use feature flags, operational flags, and other runtime configuration to make change...
- AWS Organizations** ☆ Central governance and management across AWS accounts.
- AWS IQ** ☆ Complete projects faster with help from third-party AWS Certified experts

Features See all 412 results ▶

- Rules**
- AWS Config feature**

Noncompliant rules by noncompliant

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Sunny ENG IN 13:08 21-02-2024

Enable AWS Config for active

Edit settings | AWS Config | ap-south-1

ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/settings/edit

D Job Search | Deloitte... Sf 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-381491968170... ▾

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

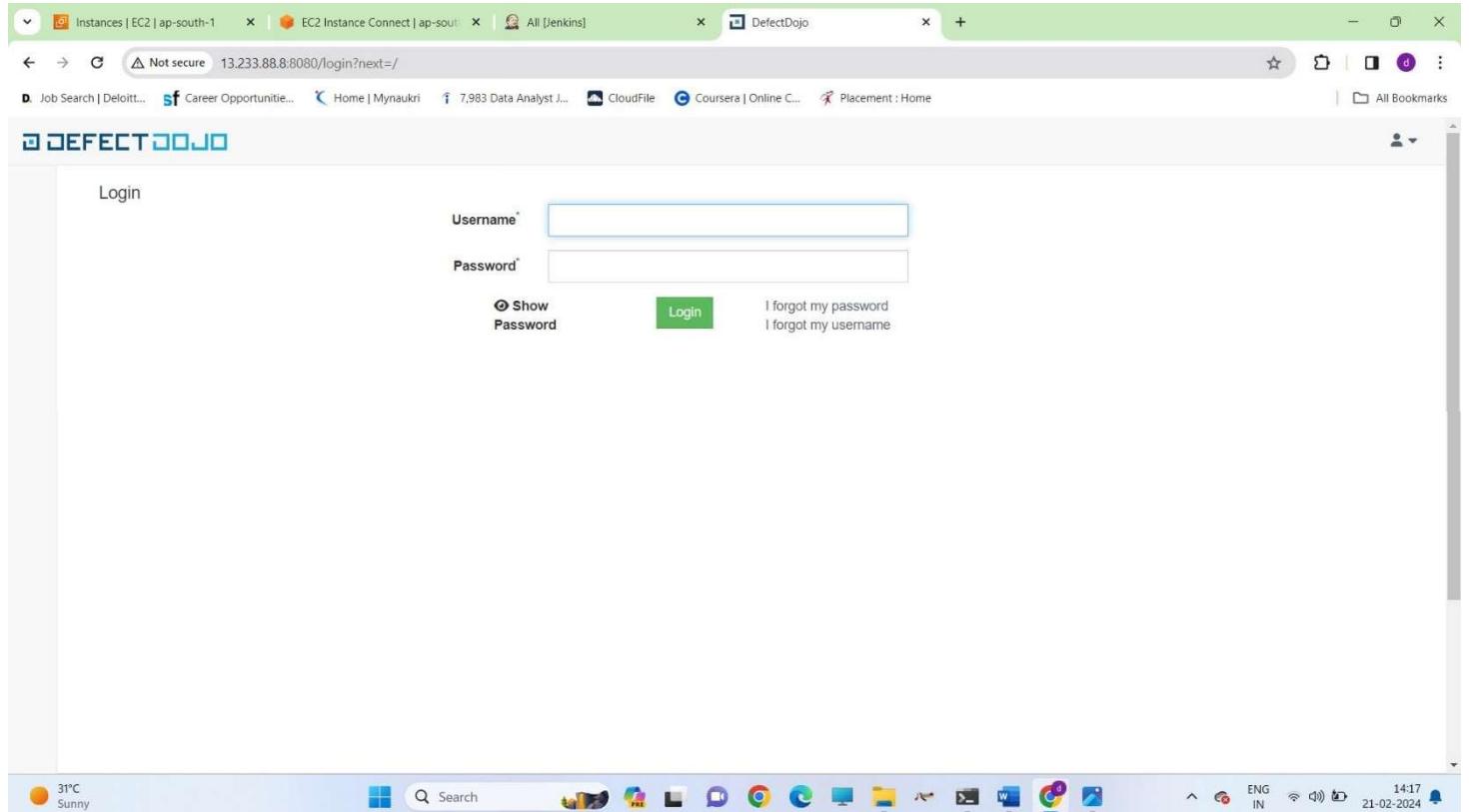
After implementation of defectdojo , create a username and password of defect dojo

```
ubuntu@ip-172-31-39-152:~/django-DefectDojo$ sudo docker compose logs initializer | grep "Admin password:"
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_NAME" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_USER" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PASSWORD" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_NAME" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_USER" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PASSWORD" variable is not set. Defaulting to a blank string.
ubuntu@ip-172-31-39-152:~/django-DefectDojo$ sudo docker compose logs initializer | grep "Admin password:"
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_CELERY_BROKER_URL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_HOST" variable is not set. Defaulting to a blank string.
WARN[0000] The "DD_DATABASE_PORT" variable is not set. Defaulting to a blank string.
initializer-1 | Admin password: Q8Ch2QT0MpgKAX6Qs9xdAG
ubuntu@ip-172-31-39-152:~/django-DefectDojo$ |
```

24°C
Partly cloudy



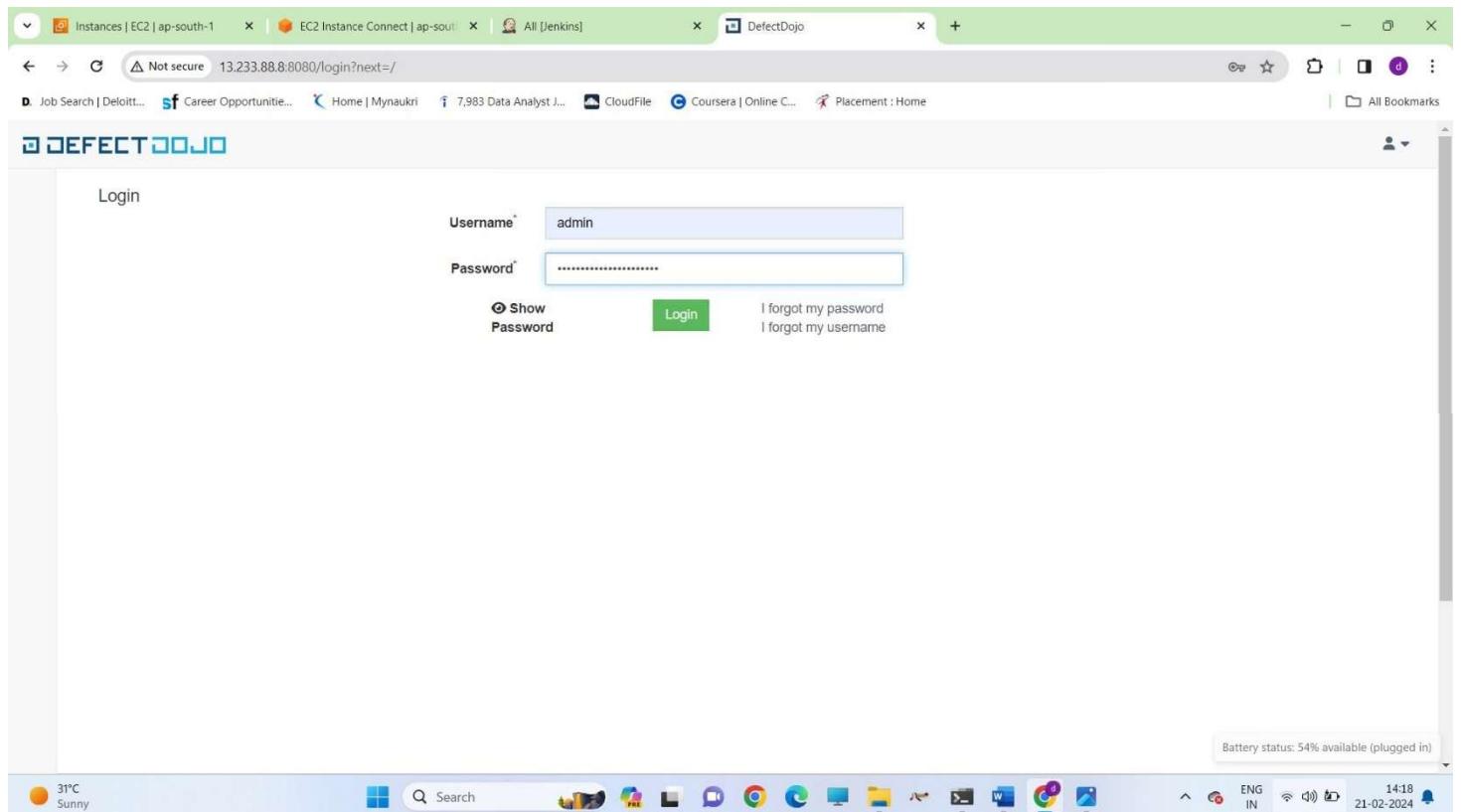
ENG IN 21:04 15-02-2024



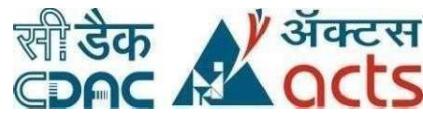
The screenshot shows a web browser window with the following details:

- Address Bar:** 13.233.88.8:8080/login?next=/
- Page Title:** DEFECTDOJO
- Login Form:**
 - Username:
 - Password:
 - Show Password link
 - Login button
 - I forgot my password link
 - I forgot my username link
- Toolbar:** Includes links for Job Search, Career Opportunities, Home, Data Analyst Jobs, CloudFile, Coursera, Placement, Weather (31°C, Sunny), and various system icons.
- Status Bar:** Shows the date (21-02-2024) and time (14:17).

Navigate to http://public_ip:8080

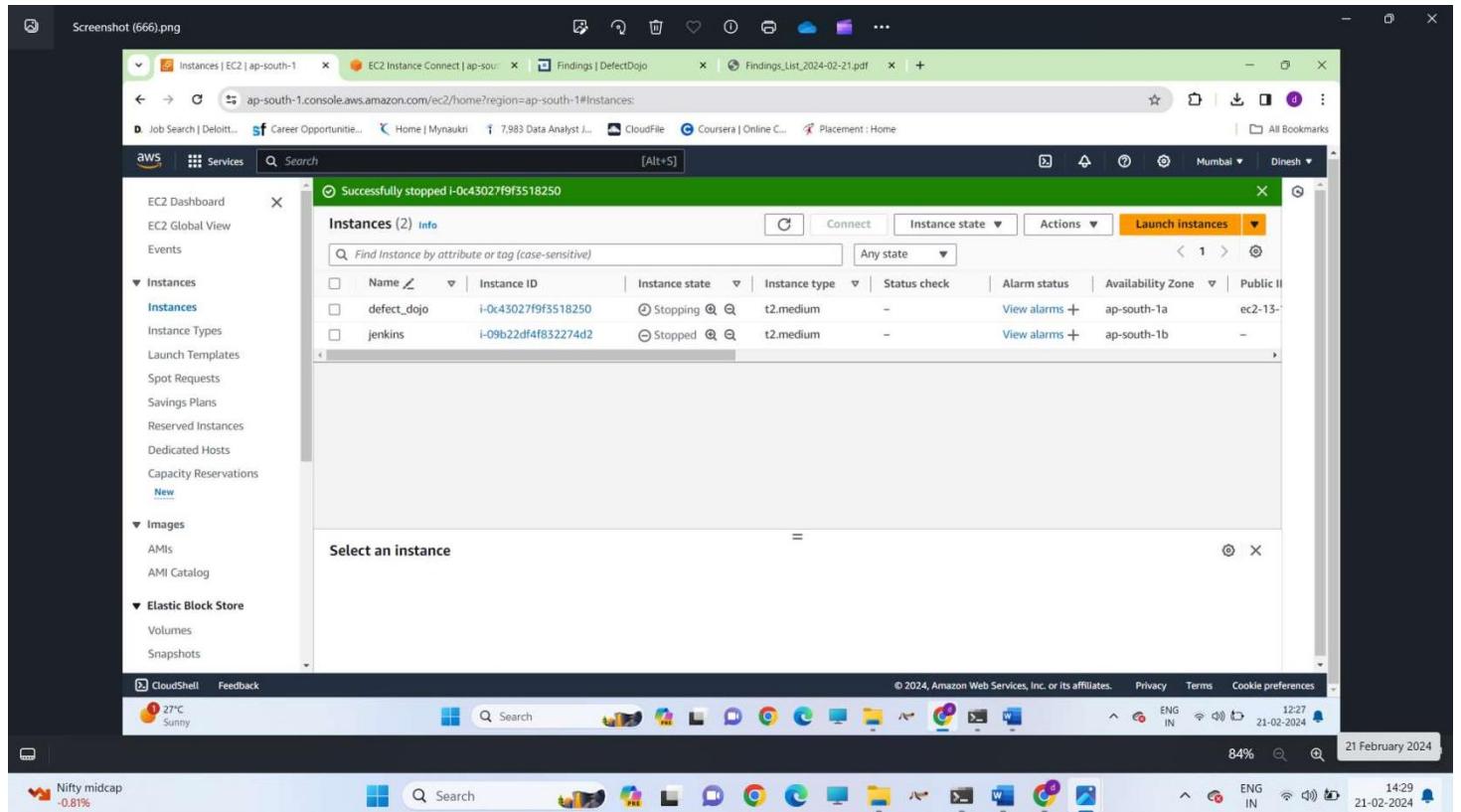


Grep the admin password from docker-compose logs initializer

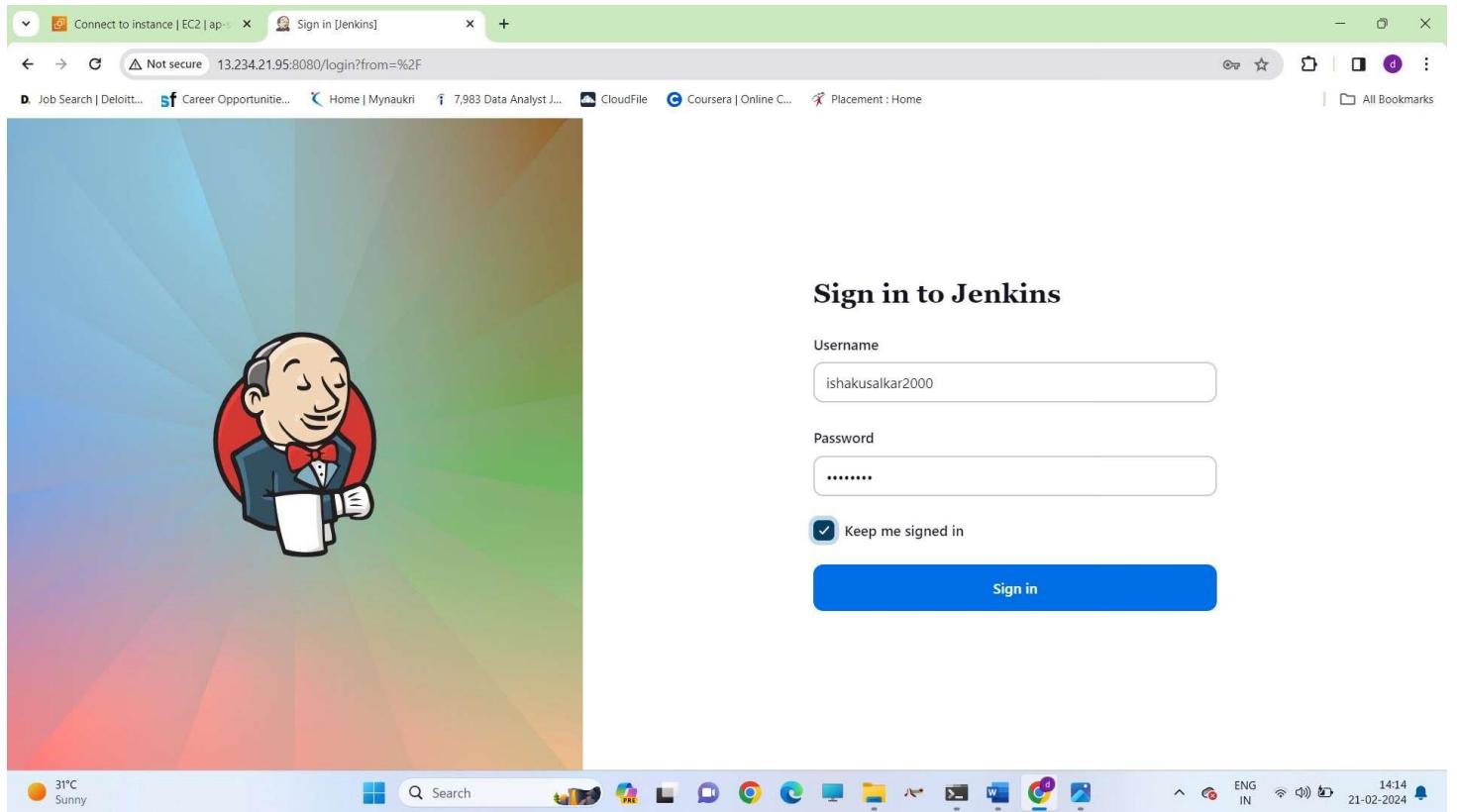


The screenshot shows the DefectDojo application interface. At the top, there's a navigation bar with links like 'Job Search | Deloitte...', 'Career Opportunitie...', 'Home | Mynaukri', '7,983 Data Analyst J...', 'CloudFile', 'Coursera | Online C...', and 'Placement : Home'. Below the navigation is the DefectDojo logo and a search bar. The main dashboard features four large cards: 'Active Engagements' (0), 'Last Seven Days' (0), 'Closed In Last Seven Days' (0), and 'Risk Accepted In Last Seven Days' (0). Each card has a 'View Engagement Details', 'View Finding Details', or 'View Finding Details' button. Below these are two charts: 'Historical Finding Severity' (a donut chart showing 0% for all severity levels) and 'Reported Finding Severity by Month' (a line chart showing 0.0 for all months). The bottom of the screen includes a weather widget (24°C, Partly cloudy), a taskbar with various icons, and system status indicators.

Defect dojo Dashboard

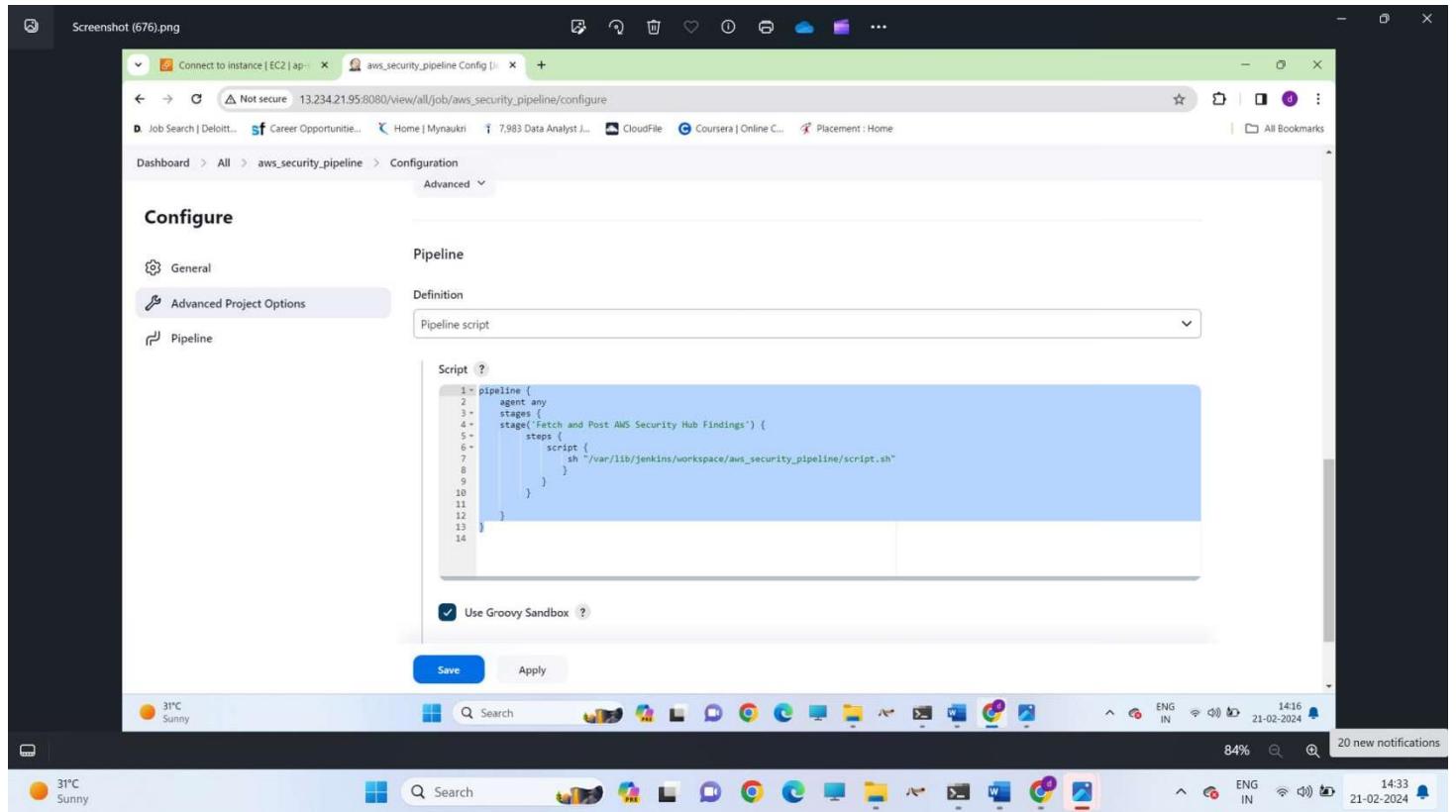


Create another EC2 instance for install jenkin

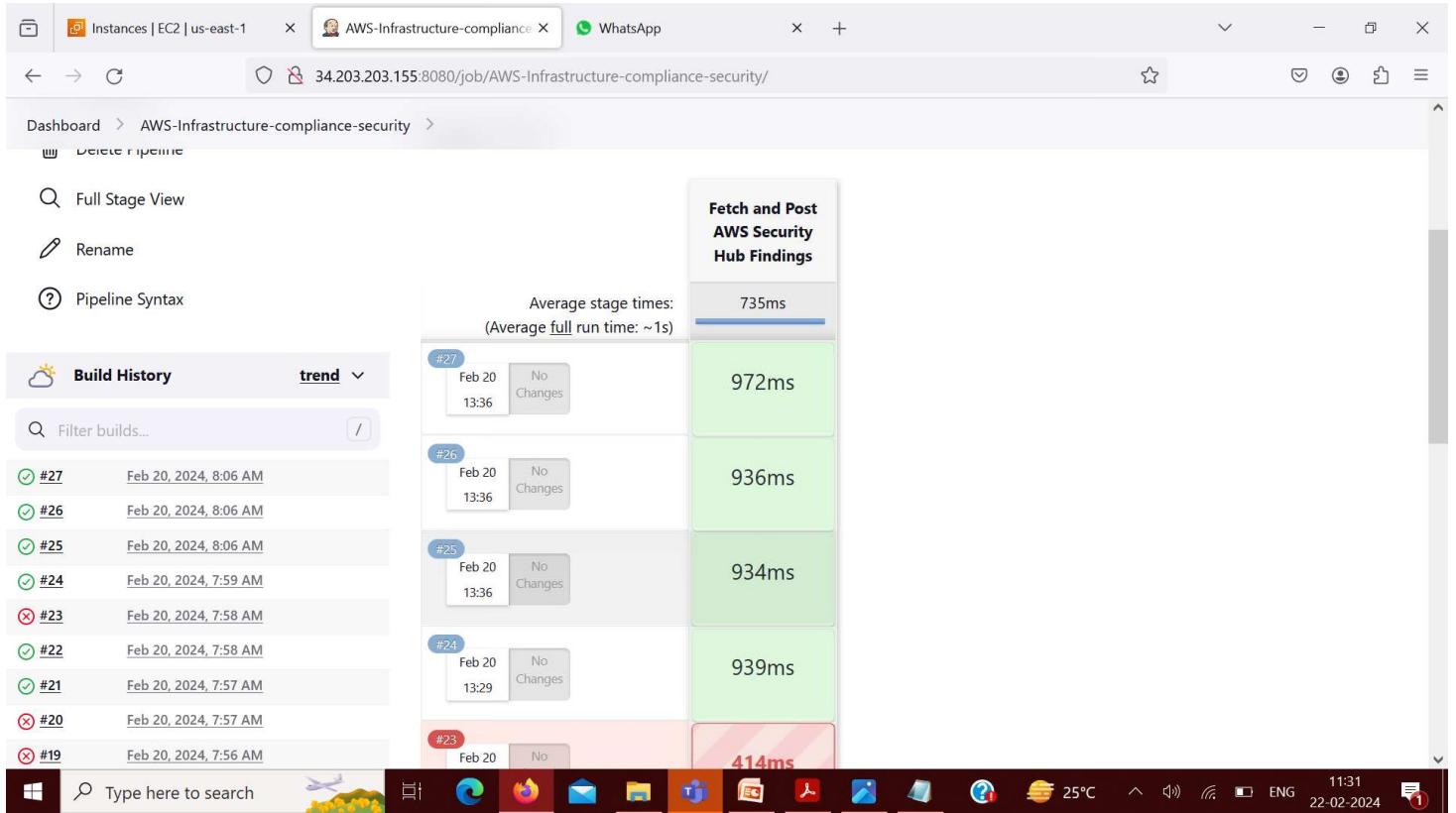


A screenshot of a web browser window. The address bar shows "Not secure 13.234.21.95:8080/login?from=%2F". The main content area displays the Jenkins sign-in page. On the left, there is a colorful background with a cartoon character of a man in a suit holding a coffee cup. The right side has the heading "Sign in to Jenkins" and fields for "Username" (containing "ishakusalkar2000") and "Password" (containing "*****"). There is a checked "Keep me signed in" checkbox and a blue "Sign in" button. The browser's toolbar at the top includes icons for refresh, search, and various bookmarks. The taskbar at the bottom shows weather (31°C Sunny), system icons, and the date/time (21-02-2024, 14:14).

Sign in to Jenkin



Write script for pipeline



Average stage times:
(Average full run time: ~1s)

Stage	Run ID	Run Date	Duration
Fetch and Post AWS Security Hub Findings	#27	Feb 20 13:36	735ms
	#26	Feb 20 13:36	972ms
	#25	Feb 20 13:36	936ms
	#24	Feb 20 13:29	934ms
	#23	Feb 20 No	939ms
	#22	Feb 20 13:29	414ms

Build History

- #27 Feb 20, 2024, 8:06 AM
- #26 Feb 20, 2024, 8:06 AM
- #25 Feb 20, 2024, 8:06 AM
- #24 Feb 20, 2024, 7:59 AM
- #23 Feb 20, 2024, 7:58 AM
- #22 Feb 20, 2024, 7:58 AM
- #21 Feb 20, 2024, 7:57 AM
- #20 Feb 20, 2024, 7:57 AM
- #19 Feb 20, 2024, 7:56 AM

Type here to search

Build pipeline

Instances | EC2 | us-east-1 AWS-Infrastructure-compliance X +

34.203.203.155:8080/job/AWS-Infrastructure-compliance-security/27/console

Dashboard > AWS-Infrastructure-compliance-security > #27

Delete build '#27'
Restart from Stage
Replay
Pipeline Steps
Workspaces
Previous Build

```
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ /var/lib/jenkins/workspace/AWS-Infrastructure-compliance-security/script.sh
Getting Security Hub Findings Locally

An error occurred (AccessDeniedException) when calling the GetFindings operation: User: arn:aws:sts::730335200347:assumed-role/EC2ReadOnlyAccess/i-0a81d43298dade990 is not authorized to perform: securityhub:GetFindings on resource: arn:aws:securityhub:us-east-1:730335200347:hub/default
script.sh
securityhub.json

Findings gathered successfully from AWS Security Hub
curl: (26) Failed to open/read local data from file/application

Failed to Sent Report
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

Type here to search 26°C 11:25 22-02-2024

Console output

The screenshot shows the DefectDojo dashboard with the following key metrics:

- Active Engagements:** 2 (View Engagement Details)
- Last Seven Days:** 81 (View Finding Details)
- Closed In Last Seven Days:** 0 (View Finding Details)
- Risk Accepted In Last Seven Days:** 0 (View Finding Details)

Historical Finding Severity: A donut chart showing the distribution of findings across severity levels. The legend indicates:

- Critical (Red)
- High (Orange)
- Medium (Yellow)
- Low (Blue)
- Informational (Grey)

The chart is almost entirely yellow, representing Medium severity.

Reported Finding Severity by Month: A scatter plot showing the number of findings per month. The Y-axis represents the count of findings (0 to 100), and the X-axis represents the date (00:00:00). Two data points are visible: one at approximately (Month 1, Count 5) and another at approximately (Month 2, Count 80).

Defect-Dojo Dashboard

Instances | EC2 | ap-south-1 | EC2 Instance Connect | ap-south-1 | Findings | DefectDojo | Findings_List_2024-02-21.pdf | +

Not secure 13.127.64.177:8080/finding

Job Search | Deloitte... Career Opportunitie... Home | Mynaukri 7,983 Data Analyst J... CloudFile Coursera | Online C... Placement : Home All Bookmarks

DEFECTDOJO

Cloud and On-Premise Subscriptions Now Available! Click here for more details

Home / Findings

All Findings

Showing entries 1 to 11 of 11

Page Size ▾

	Severity	Name	CWE	Vulnerability Id	Date	Age	SLA	Reporter	Found By	Status	Group	Product	Service	Planned Remediation
<input type="checkbox"/>	Critical	Security Groups Should Not Allow Unrestricted Access to Port...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
<input type="checkbox"/>	Critical	Security Groups Should Not Allow Unrestricted Access to Port...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		

27°C Sunny

Search

12:27 21-02-2024 ENG IN

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 Port...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	Security Groups Should Not Allow Unrestricted Access to Port...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	Security Groups Should Not Allow Unrestricted Access to Port...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		BANKINGAPP		
Critical	Security Groups Should Not Allow Unrestricted Access to Port...			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 Port...			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...			Feb. 20, 2024	1	6	Admin User (admin)	AWS Security Hub Scan	Active, Verified		RANKINGAPP		

REPORT GENERATES

CONCLUSION & FUTURE SCOPE

Conclusion:

A secure AWS Infrastructure is assured with the compliance checks and audit 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/>