

Security in Cloud Computing and IoT

Lab 1

1. AIM:

The aim of this experiment is to implement a cloud security policy and to analyze and mitigate security risks in IaaS, PaaS, and SaaS cloud service models using AWS Security Hub.

2. REQUIREMENTS:

Software Requirements:

- AWS Account
- AWS Config
- AWS Security Hub
- Amazon EC2
- Amazon RDS
- AWS IAM

3. INTRODUCTION

Cloud computing provides services over the internet, but security is a major concern. If cloud resources are not configured properly, they can be exposed to attackers. AWS provides Security Hub, which continuously checks the security posture of cloud resources and reports security issues called findings.

In this experiment:

- EC2 is used for IaaS
- Amazon RDS is used for PaaS
- IAM is used for SaaS

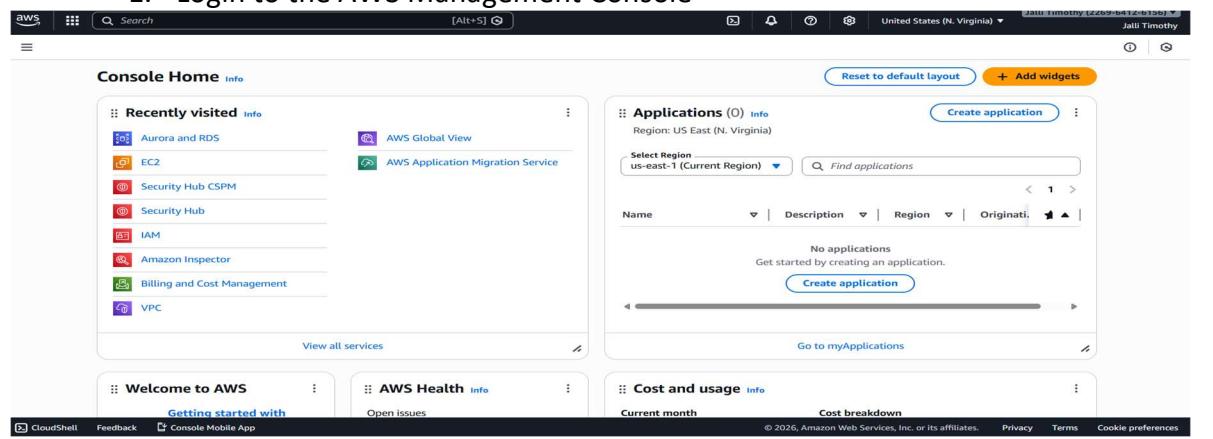
4. PROCEDURE

4.1. STEP1: ENABLE AWS CONFIG

AWS Config is used to record and track configuration changes of AWS resources. AWS Security Hub depends on AWS Config to evaluate security controls. Without enabling AWS Config, Security Hub findings may be inaccurate.

• Steps

1. Login to the AWS Management Console



Security in Cloud Computing and IoT Lab 1

2. Search for AWS Config
3. Click Get started

The screenshot shows the AWS Config 'Set up AWS Config' wizard. The 'Settings' tab is selected. Under 'Recording method', the 'All resource types with customizable overrides' option is selected. Under 'Default settings', 'Continuous recording' is chosen. At the bottom, there are 'Override settings' and a 'Next Step' button.

4. Enable Resource recording

The screenshot shows the 'AWS WAFv2 IP Set' configuration page. It lists various resources and their recording status: AWS WAFv2 ManagedRuleSet (Continuous), AWS WAFv2 RegexPatternSet (Continuous), AWS WAFv2 RuleGroup (Continuous), AWS WAFv2 WebACL (Continuous), AWS WorkSpaces ConnectionAlias (Continuous), AWS WorkSpaces Workspace (Continuous), and AWS XRay EncryptionConfig (Continuous). Below this, under 'Delivery method', it shows an S3 bucket name: config-bucket-226964126156. Under 'AWS Config rules (0)', it says 'No rules selected'. At the bottom are 'Cancel', 'Previous', and 'Confirm' buttons.

5. Select Record all resources
6. Choose Service-linked role
7. Click Confirm

The screenshot shows the AWS Config 'Dashboard' page. On the left, a sidebar includes 'Conformance packs', 'Rules', 'Resources', 'Aggregators' (with 'Compliance Dashboard' and 'Inventory Dashboard'), 'Advanced queries', 'Settings', 'What's new', 'Documentation', 'Partners', and 'FAQs'. The main dashboard area has sections for 'Conformance Packs by Compliance Score' (which shows 'No conformance packs deployed. Try deploying a new conformance pack.'), 'Compliance status' (showing 0 Noncompliant rules and 0 Compliant rule(s)), and 'Noncompliant rules by noncompliant'. To the right, there is a 'AWS Config usage metrics' section with a chart titled 'Configuration Items Recorded' and another titled 'Configuration Recorder Insufficient Permission Count'. Both charts show 'No data available.'

Security in Cloud Computing and IoT

Lab 1

4.2. STEP 2: ENABLE AWS SECURITY HUB

AWS Security Hub is a centralized security service that collects findings from AWS services and checks resources against security standards like CIS and AWS Foundational Security Best Practices.

• Steps

1. Open AWS Console

The screenshot shows the AWS Console Home page. On the left, there's a sidebar with 'Recently visited' links including Aurora and RDS, EC2, Security Hub CSPM, Security Hub, IAM, Amazon Inspector, Billing and Cost Management, and VPC. Below this is a 'Welcome to AWS' section with 'Getting started with' and 'AWS Health' with 'Open issues'. On the right, there's an 'Applications' section with a message 'No applications. Get started by creating an application.' and a 'Create application' button. At the bottom, there are links for 'CloudShell', 'Feedback', and 'Console Mobile App'.

2. Search for AWS Security Hub

3. Click Enable Security Hub

The screenshot shows the AWS Security Hub Summary page. On the left, there's a sidebar with 'Dashboard' (Summary, Threats, Exposure, Vulnerabilities, Posture management, Sensitive data), 'Inventory' (All findings, Resources), 'Management' (Automations, Integrations), and 'Settings' (General, Account coverage). The main area has a 'Getting started' section with three cards: 'Configure cross-Region aggregation' (Aggregate findings from multiple Regions into one place), 'Turn on security capabilities' (View your security coverage and enable security capabilities), and 'Enable Security Hub for your organization - optional' (Define how Security Hub is enabled for your organization with policies). At the bottom, there are tabs for 'Executive' and 'Triage', and filter options.

4. Enable security standards:

- AWS Foundational Security Best Practices
- CIS AWS Foundations Benchmark

The screenshot shows the AWS Security Hub CSPM Security standards page. On the left, there's a sidebar with 'Summary', 'Controls', 'Security standards', 'Insights', 'Findings', 'Integrations', 'Management' (Automations, Custom actions), 'Settings' (General, Regions, Configuration, Usage), and 'What's new'. The main area shows four security standards: 'AWS Foundational Security Best Practices v1.0.0' (Successfully enabled), 'AWS Resource Tagging Standard v1.0.0' (not yet enabled), 'CIS AWS Foundations Benchmark v1.2.0' (not yet requested), and 'CIS AWS Foundations Benchmark v1.4.0' (not yet requested). Each standard card includes a 'View results' and 'Disable standard' button.

Security in Cloud Computing and IoT

Lab 1

5. Enable integrations like GuardDuty

The screenshot shows the AWS Security Hub CSPM Summary page. On the left, there's a navigation sidebar with sections like Security Hub CSPM (Summary, Controls, Security standards), Insights, Findings, Integrations, Management (Automations, Custom actions), Settings (General, Regions, Configuration New, Usage), and What's new. The main content area has two main sections: 'Security standards' (warning: security score cannot be calculated until AWS Config is enabled) and 'Assets with the most findings'. The 'Assets with the most findings' section lists resources by severity and resource type, with AWS::Account:226964126156 at the top.

4.3. STEP 3: IaaS RISK ANALYSIS – AMAZON EC2

Amazon EC2 is an Infrastructure as a Service (IaaS). If security groups are misconfigured, EC2 instances can be accessed by anyone on the internet.

- **Steps**

1. Open Amazon EC2

The screenshot shows the AWS EC2 Dashboard. The left sidebar includes sections for Dashboard, Instances (Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager New), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes). The main content area has sections for Resources (listing Instances (running), Auto Scaling Groups, Capacity Reservations, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, Volumes), Launch instance (with 'Launch instance' and 'Migrate a server' buttons), Service health (AWS Health Dashboard), and Account attributes (Default VPC, Settings, Explore AWS).

2. Click Launch Instance

The screenshot shows the 'Launch an instance' wizard. It starts with the 'Name and tags' step, where 'My Web Server' is entered. Next is the 'Application and OS Images (Amazon Machine Image)' step, showing a search bar and recent AMIs (Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian). The final step is 'Summary', which shows 1 instance, the selected Software Image (Amazon Linux 2023 AMI), Virtual server type (t2.micro), Firewall (New security group), Storage (1 volume(s) - 8 GiB), and a note about free tier usage. Buttons for 'Cancel', 'Launch instance', and 'Preview code' are at the bottom.

Security in Cloud Computing and IoT

Lab 1

3. Choose Amazon Linux
4. Select t2.micro / t3.micro (Free Tier)
5. In Security Group, allow:
 - o SSH from 0.0.0.0/0 (*intentional risk*)

The screenshot shows the AWS EC2 Instances details page for instance i-09a2f3c7ecaaf84f5. The instance is running and has a public IPv4 address of 100.31.159.172 and a private IP DNS name of ip-172-31-21-55.ec2.internal. It is an t2.micro instance with a VPC ID of vpc-02ee7fa0f10decad0. The instance is associated with a subnet subnet-0e72b81a7d808a7e2 and an instance ARN of arn:aws:ec2:us-east-1:226964126156:instance/i-09a2f3c7ecaaf84f5. The instance is managed by a user.

6. Launch the instance

The screenshot shows the AWS EC2 Instances launch confirmation page. A green success message indicates that the instance was successfully initiated. Below the message, there is a 'Launch log' section and a 'Next Steps' section with several options: 'Create billing and free tier usage alerts', 'Connect to your instance', 'Connect an RDS database', 'Create EBS snapshot policy', 'Manage detailed monitoring', 'Create Load Balancer', 'Create AWS Budget', and 'Manage CloudWatch alarms'. Each option has a corresponding button.

- **Finding (IaaS)**

AWS Security Hub reported findings related to EC2 and IAM usage, indicating an infrastructure-level security risk due to permissive access.

The screenshot shows the AWS EC2 Instances search results page. A single instance named 'IaaS' is listed, showing it is running, has an instance type of t2.micro, and is in the us-east-1d availability zone. The instance has a public IPv4 address of 100.31.159.172. There are buttons for 'Connect', 'Actions', and 'Launch instances'.

Security in Cloud Computing and IoT

Lab 1

• Mitigation (IaaS)

Security group rules were reviewed and restricted to improve infrastructure security.

The screenshot shows the AWS Security Hub CSPM Findings page. A prominent warning message states: "Findings might be inaccurate. If you receive a failed finding for Config.1, you might not have AWS Config recording correctly configured. This can result in inaccurate control findings." Below this, there is a search bar and filter options: "Workflow status is NEW", "Workflow status is NOTIFIED", "Record state is ACTIVE", and "Clear filters". The main table lists four findings:

Severity	Workflow status	Region	Account ID	Product	Resource	Compliance Status
INFORMATIONAL	NEW	us-east-1	226964126156	Security Hub	IAM User timothy	⚠ WARNING
MEDIUM	NEW	us-east-1	226964126156	Security Hub	S3 Bucket config-bucket-226964126156	🔴 FAILED
MEDIUM	NEW	us-east-1	226964126156	Security Hub	AwsEc2Subnet subnet-0e72b81a7d80a7e2	🔴 FAILED
MEDIUM	NEW	us-east-1	226964126156	Security Hub	AwsEc2Subnet subnet-0428b48919e3f0fe3	🔴 FAILED

4.4. STEP 4: PaaS RISK ANALYSIS – AMAZON RDS

Amazon RDS is a Platform as a Service (PaaS).

A database should never be exposed to the public internet.

Public access to a database can lead to data breaches.

• Steps

1. Open Amazon RDS

The screenshot shows the Aurora and RDS Dashboard. On the left, a sidebar lists various RDS-related services like Databases, Query editor, and Performance insights. The main area displays "Resources" and "Explore Aurora & RDS". The "Resources" section shows DB Instances (0/40), DB Clusters (0/40), and other metrics. The "Explore Aurora & RDS" section includes a "Start tutorial" button and a "Recommended services" section with a note: "No recommendations yet. Recommended services will display based on your AWS console usage."

2. Click Create database

The screenshot shows the "Create database" page. It starts with a "Choose a database creation method" section where "Full configuration" is selected. Below this are "Engine options" and "Engine version" sections. Under "Engine options", there are eight engine choices: Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible) (selected), MySQL, PostgreSQL, MariaDB, Oracle (Oracle logo), Microsoft SQL Server (Microsoft SQL Server logo), IBM Db2, and IBM Db2 (IBM Db2 logo). There is also an "Engine version" link.

Security in Cloud Computing and IoT

Lab 1

3. Select MySQL

4. Choose Free Tier

The screenshot shows the 'Create database' wizard in the AWS RDS console. Under 'Engine version', 'MySQL 8.4.7' is selected. Under 'Templates', 'Free tier' is selected. Under 'Availability and durability', 'Single-AZ DB instance deployment (1 instance)' is selected. The status bar at the bottom indicates '© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

5. Set DB identifier as paas-lab-db

The screenshot shows the 'Settings' tab in the 'Create database' wizard. The 'DB instance identifier' field is filled with 'paas-lab-db'. Under 'Credentials Settings', 'Master username' is set to 'admin'. Under 'Credentials management', 'Self managed' is selected. The status bar at the bottom indicates '© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

6. Enable Public access = Yes (intentional risk)

The screenshot shows the 'Databases' page in the AWS RDS console. A blue banner at the top says 'Creating database paas-lab-db'. The database 'paas-lab-db' is listed in the table, showing it is 'Creating' and has an 'Instance' status. The status bar at the bottom indicates '© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

7. Create database

Security in Cloud Computing and IoT

Lab 1

The screenshot shows the AWS Aurora and RDS console under the 'Databases' section. A green success message at the top states: 'Successfully created database paas-lab-db'. Below it, a table lists the database 'paas-lab-db' with details: Config..., Instance, MySQL Co..., SECOND, us-east-1a, db.t4g.micro. The left sidebar includes links for Dashboard, Databases, Query editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Zero-ETL integrations, Events, and Event subscriptions.

• Finding (PaaS)

The RDS database was found to be publicly accessible, which represents a PaaS security misconfiguration.

The screenshot shows the AWS Security Hub CSPM 'Findings' page. It displays five findings related to the RDS instance 'paas-lab-db': 1. 'RDS instances should have automatic backups enabled' (Medium, New). 2. 'RDS instances should not use a database engine default port' (Low, New). 3. 'RDS DB Instances should prohibit public access, as determined by the PubliclyAccessible configuration' (Critical, New). 4. 'Ensure a log metric filter and alarm exist for AWS Config configuration changes' (Low, New). The left sidebar includes links for Summary, Controls, Security standards, Insights, Findings (selected), Integrations, Management, Automations, Custom actions, Settings, General, Regions, Configuration (New), and Usage.

• Mitigation (PaaS)

1. Go to RDS → Databases
2. Select the database
3. Click Modify
4. Change Public access → Not publicly accessible
5. Apply changes immediately

The screenshot shows the AWS Aurora and RDS console under the 'Databases' section. A green success message at the top states: 'Successfully modified paas-lab-db.' Below it, the database 'paas-lab-db' is listed with its status as 'Modify...'. The left sidebar includes links for Dashboard, Databases, Query editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Zero-ETL integrations, Events, and Event subscriptions.

Security in Cloud Computing and IoT

Lab 1

4.5. STEP 5: SaaS RISK ANALYSIS – IAM / ROOT ACCOUNT

IAM is a Software as a Service (SaaS).

Using the root account without MFA is risky because the root user has full permissions.

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access Management', 'Access reports', and 'AWS CloudTrail'. The main area has a blue banner at the top stating 'New access analyzers available' with a link to 'Create new analyzer'. Below it is the 'IAM Dashboard' section with 'Security recommendations' (two items: 'Root user has MFA' and 'Root user has no active access keys'), 'IAM resources' (User groups: 0, Users: 1, Roles: 11, Policies: 0, Identity providers: 0), and a 'Quick Links' section with 'My security credentials' and a 'Sign-in URL for IAM users in this account' (https://226964126156.signin.aws.amazon.com/console). A 'What's new' section is also present.

- **Finding (SaaS)**

AWS Security Hub detected usage of root credentials, indicating a SaaS-level security issue.

The screenshot shows the AWS Security Hub CSPM 'Findings' page. The left sidebar includes 'Summary', 'Controls', 'Security standards', 'Insights', 'Findings' (selected), 'Integrations', 'Management', 'Automations', 'Custom actions', and 'Settings' (General, Regions, Configuration, Usage). The main area lists several findings under 'Management Console authentication failures':

- Ensure a log metric filter and alarm exist for CloudTrail configuration changes (Low, NEW, us-east-1, 226964126156, Security Hub, Account 226964126156)
- Ensure a log metric filter and alarm exist for IAM policy changes (Low, NEW, us-east-1, 226964126156, Security Hub, Account 226964126156)
- A log metric filter and alarm should exist for usage of the "root" user (Low, NEW, us-east-1, 226964126156, Security Hub, Account 226964126156)
- Ensure a log metric filter and alarm exist for Management Console sign-in without MFA (Low, NEW, us-east-1, 226964126156, Security Hub, Account 226964126156)
- Ensure a log metric filter and alarm exist for VPC changes (Low, NEW, us-east-1, 226964126156, Security Hub, Account 226964126156)
- Ensure a log metric filter and alarm exist for route table changes (Low, NEW, us-east-1, 226964126156, Security Hub, Account 226964126156)
- Ensure a log metric filter and alarm exist for changes to network gateways (Low, NEW, us-east-1, 226964126156, Security Hub, Account 226964126156)

- **Mitigation (SaaS)**

1. Open IAM
2. Go to IAM Dashboard
3. Click Activate MFA on root account
4. Configure Virtual MFA
5. Complete MFA setup

Security in Cloud Computing and IoT

Lab 1

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists navigation options like Dashboard, Access Management, and Access reports. The main area displays security recommendations (Root user has MFA, Root user has no active access keys), IAM resources (User groups: 0, Users: 1, Roles: 11, Policies: 0, Identity providers: 0), and AWS Account details (Account ID: 226964126156, Account Alias: Create, Sign-in URL: https://226964126156.signin.aws.amazon.com/console). A blue banner at the top right indicates "New access analyzers available" and provides a "Create new analyzer" button.

5. RESULT:

All identified security risks in IaaS, PaaS, and SaaS were successfully mitigated using AWS Security Hub and AWS security best practices.

6. CONCLUSION:

This experiment helped in understanding how cloud security risks occur due to misconfiguration.
Using AWS Security Hub, security risks were identified and mitigated, thereby improving the overall cloud security posture.