Week 11: Final Cloud Security Audit

Name- Saish Dhiwar

PRN- 2124UCSM2011

Email- saish.dhiwar_24ucs@sanjivani.edu.in

Tasks- 1) Review all resources.

2) Identify misconfigurations.

3) Document final audit report.

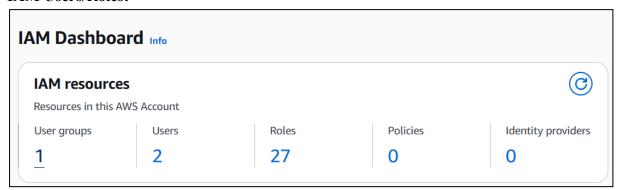## Task 1- Review All Resources.

EC2 Instances:

	Security group ID		Security group name		VPC ID		Description		Ov
	sg-0a2677257fd4d8378		security_group		vpc-04d890dcc91357448 ↗		first security group		24
	sg-0dcf267f966b37428		default		vpc-04d890dcc91357448 ↗		default VPC security group		24

Security Groups (2) Info — Actions ▼ — Export security groups to CSV ▼ — Create security group

S3 Buckets:

2124ucsm2011 Info

Objects | **Properties** | Permissions | Metrics | Management | Access Points

Bucket overview

AWS Region	Amazon Resource Name (ARN)	Creation date
Asia Pacific (Mumbai) ap-south-1	arn:aws:s3:::2124ucsm2011	July 17, 2025, 22:29:20 (UTC+05:30)

IAM Users/Roles:

IAM Dashboard Info

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	2	27	0	0

CloudTrail & Config:

CloudTrail-1 — Delete — Stop logging

General details — Edit

Trail logging	Trail log location	Log file validation	SNS notification delivery
⊘ Logging	aws-cloudtrail-logs-240110921708-0bc6a23d/AWSLogs/240110921708 ↗	Disabled	Disabled
Trail name		**Last file validation delivered**	**Last SNS notification**
CloudTrail-1	**Last log file delivered**	-	-
	August 18, 2025, 18:47:57 (UTC+05:30)		

Task 2- Identify Misconfigurations.

S3 Buckets:

do-not-delete-ssm-diagnosis-240110921708-ap-south-1-dfbay Info

| Objects | Properties | Permissions | Metrics | Management | Access Points |

Bucket overview

AWS Region	Amazon Resource Name (ARN)	Creation date
Asia Pacific (Mumbai) ap-south-1	arn:aws:s3:::do-not-delete-ssm-diagnosis-240110921 708-ap-south-1-dfbay	July 27, 2025, 17:54:21 (UTC+05:30)

IAM:

compromised-user Info   [Delete]

Summary

ARN	Console access	Access key 1
arn:aws:iam::240110921708:user/compromised-user	Disabled	**Create access key**
Created	**Last console sign-in**	
August 18, 2025, 13:09 (UTC+05:30)	-	

CloudTrail:

CloudTrail-1   [Delete] [Stop logging]

General details   [Edit]

Trail logging	Trail log location	Log file validation	SNS notification delivery
⊘ Logging	aws-cloudtrail-logs-240110921708-0bc6a23d/AWSLogs/240110921708 ↗	Disabled	Disabled
Trail name		**Last file validation delivered**	**Last SNS notification**
CloudTrail-1	**Last log file delivered**	-	-
	August 18, 2025, 20:03:42 (UTC+05:30)		
Multi-region trail			
Yes	**Log file SSE-KMS encryption**		
	Not enabled		
Apply trail to my organization			
Not enabled			