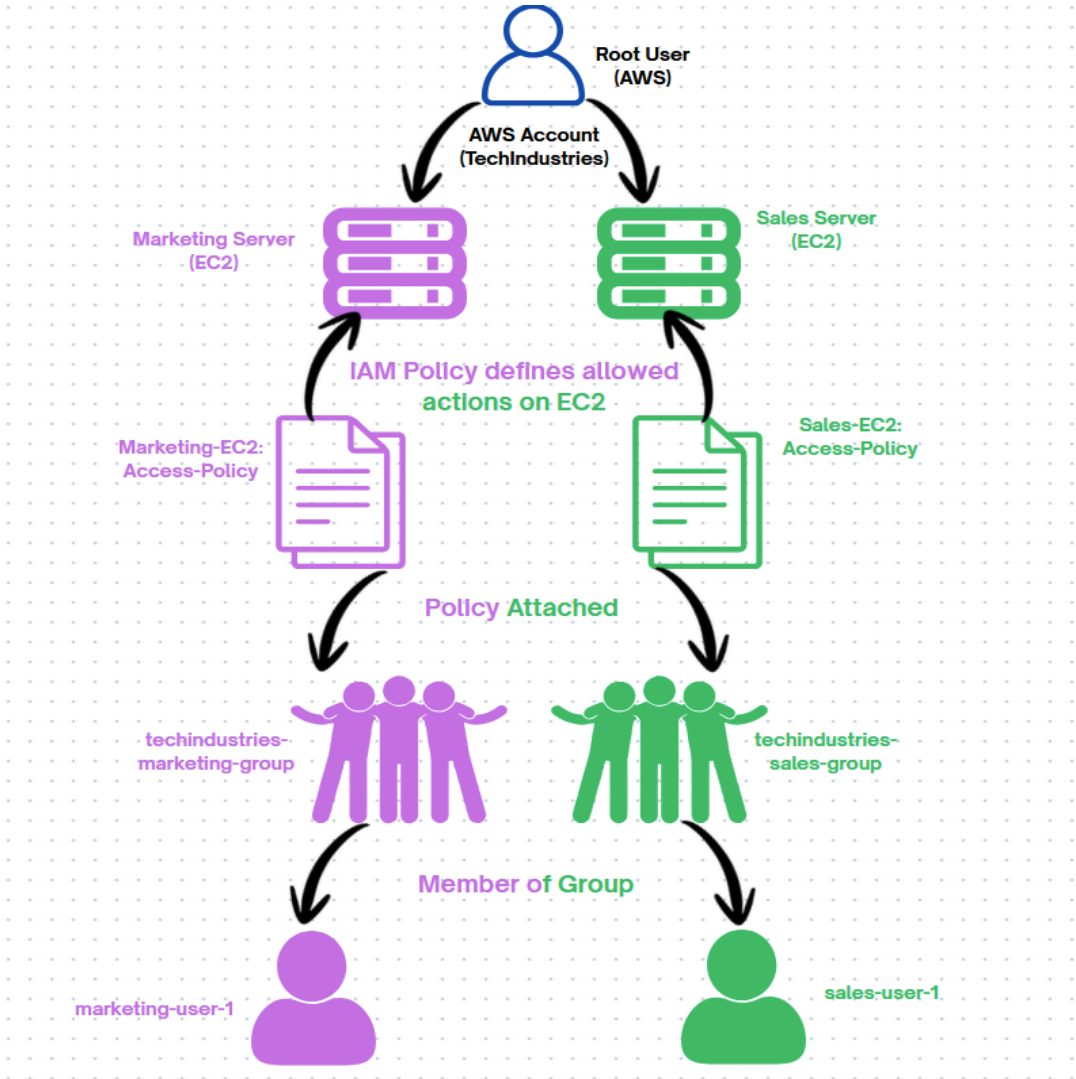
Cloud Security Project (AWS)

This project demonstrates the use of AWS Identity and Access Management (IAM) to secure cloud infrastructure by enforcing least-privilege access. Two EC2 instances were deployed to simulate organisational servers, and a custom IAM policy was created to allow read-only access. Access testing confirmed that the IAM user could view resources but was restricted from making changes, showcasing effective cloud security implementation.

Cloud security steps (IAM)

1. Setup an AWS Management console
2. Launch 2 EC2 instances
3. Create an IAM policy
4. Create an AW alias
5. Create IAM group and user
6. Test the IAM user access

Diagram of IAM-based access control within the TechIndustries AWS account:



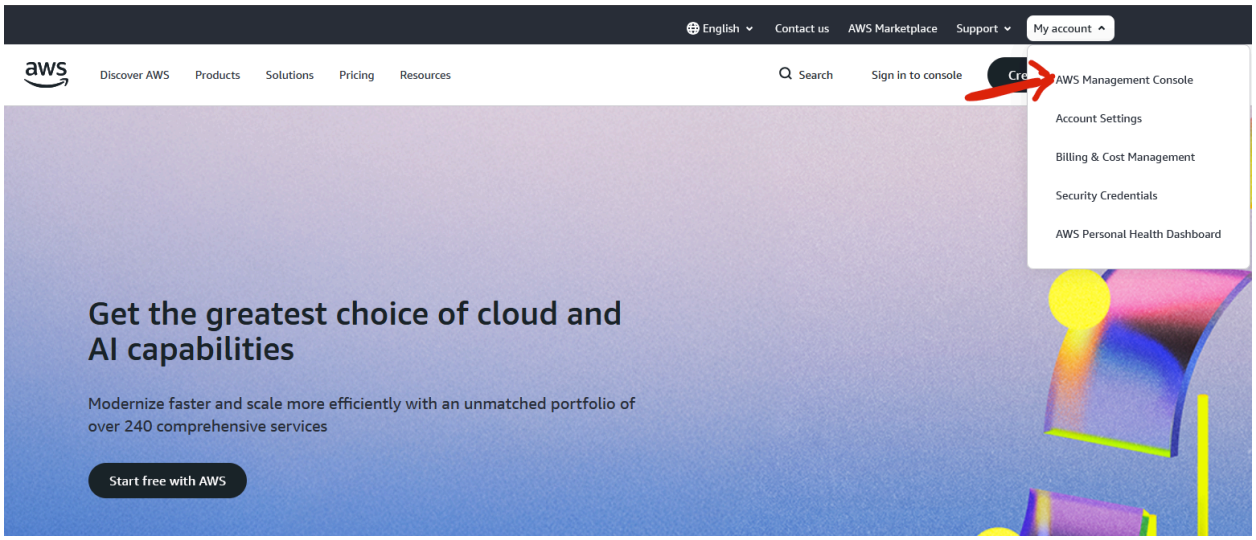
The root user is used only for account-level management, while IAM policies define permitted actions on EC2 resources. Department-specific groups are assigned policies granting scoped access to either the marketing or sales EC2 servers. Users inherit permissions through group membership, ensuring least-privilege access and strong separation of duties.

What You'll Need:

1. AWS account - Free Tier
2. Good Internet Connection
3. Google Authenticator App - (IAM users)

Setting up AWS management console:

1. Navigate to AWS
2. Sign in or create an AWS Account - Free tier
3. Log in as the root user (email + password)



IAM user sign in

Account ID or alias (Don't have?)

Remember this account

IAM username

Password

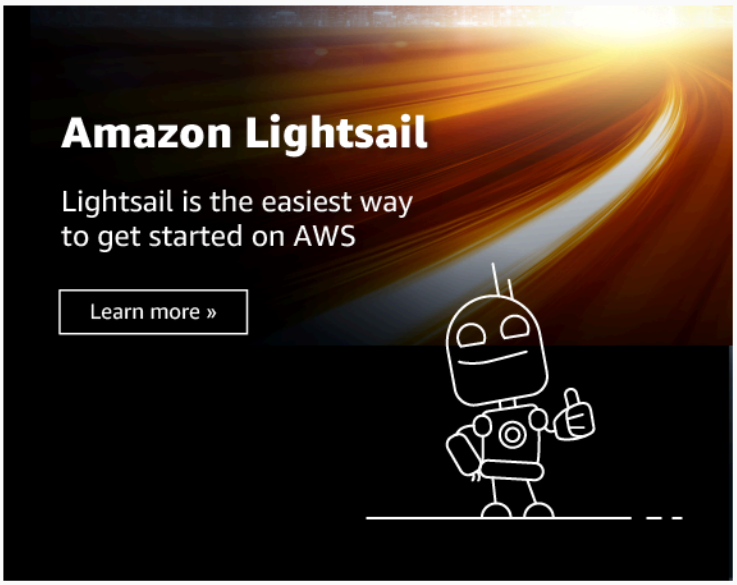
Show Password Having trouble?

Sign in

Sign in using root user email

Create a new AWS account

By continuing, you agree to AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.



Sign In

Access your AWS account by user type.

User type (not sure?)

Root user
Account owner that performs tasks requiring unrestricted access.

IAM user
User within an account that performs daily tasks.

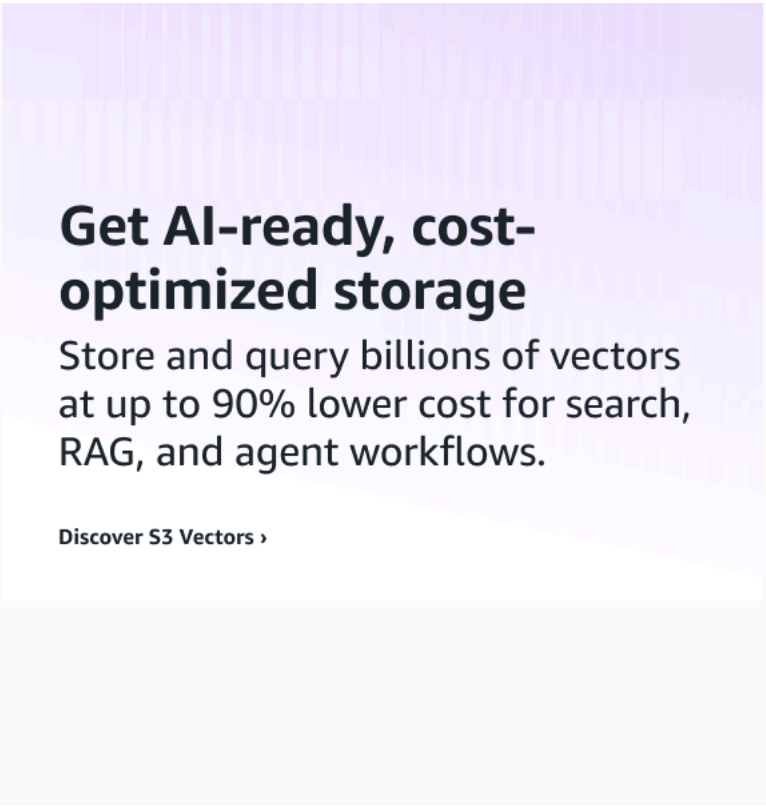
Email address

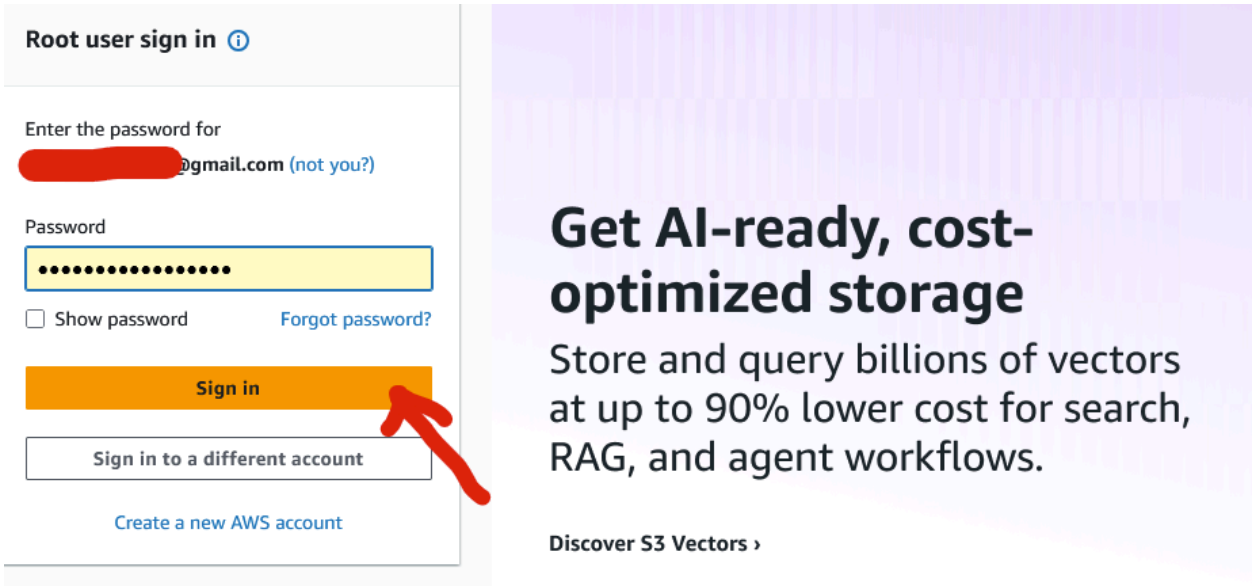
[redacted]@gmail.com

Next

OR

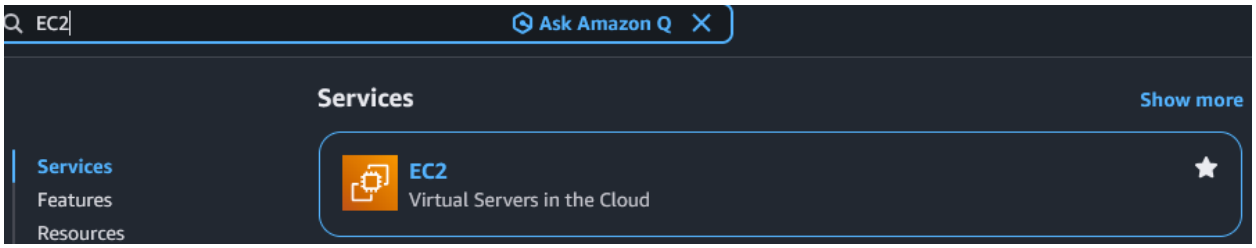
New to AWS? Sign up

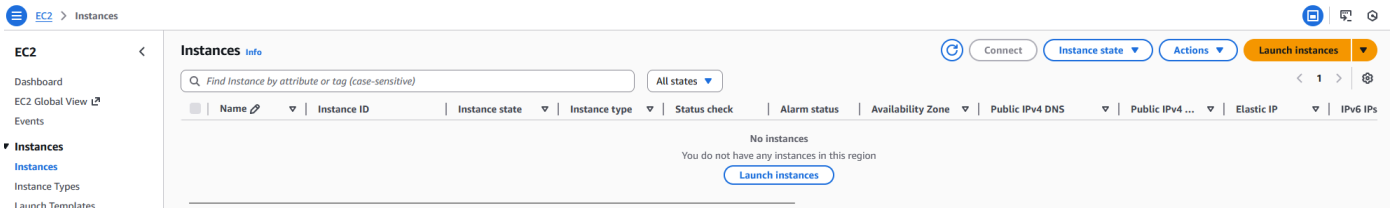




Launching 2 EC2 Instances:

1. Navigate to EC2 using search bar
2. Open EC2 dashboard
3. Click Launch Instance





Next:

1. Name the ec2 instance
    a. Add additional tags (Env and Marketing)
2. Select Amazon Linux 2 (Free Tier eligible
3. Instance type: t3.micro
4. Configure a key pair
    a. Create a new key pair (download and keep safe)
5. Network:
    a. Default VPC
    b. Enable ssh (port 22)
6. Launch the instance
7. Repeat steps for the 2nd ec2 instance.

Name and tags Info

Key Info	Value Info	Resource types Info	
Name	techindustries-marketing-s	Select resource types → Instances	Remove
Env	Marketing	Select resource types → Instances	Remove

Add new tag

You can add up to 48 more tags.

Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose **Browse more AMIs**.

Search our full catalog including 1000s of application and OS images

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI — Free tier eligible

ami-07ff62358b87c7116 (64-bit (x86), uefi-preferred) / ami-059afa9e3a9c7af0c (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.10.20260105.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username	
64-bit (x86)	uefi-preferred	ami-07ff62358b87c7116	2026-01-02	ec2-user	Verified provider

Instance type Info | Get advice

Instance type

t3.micro — Free tier eligible

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour On-Demand SUSE base pricing: 0.0104 USD per Hour

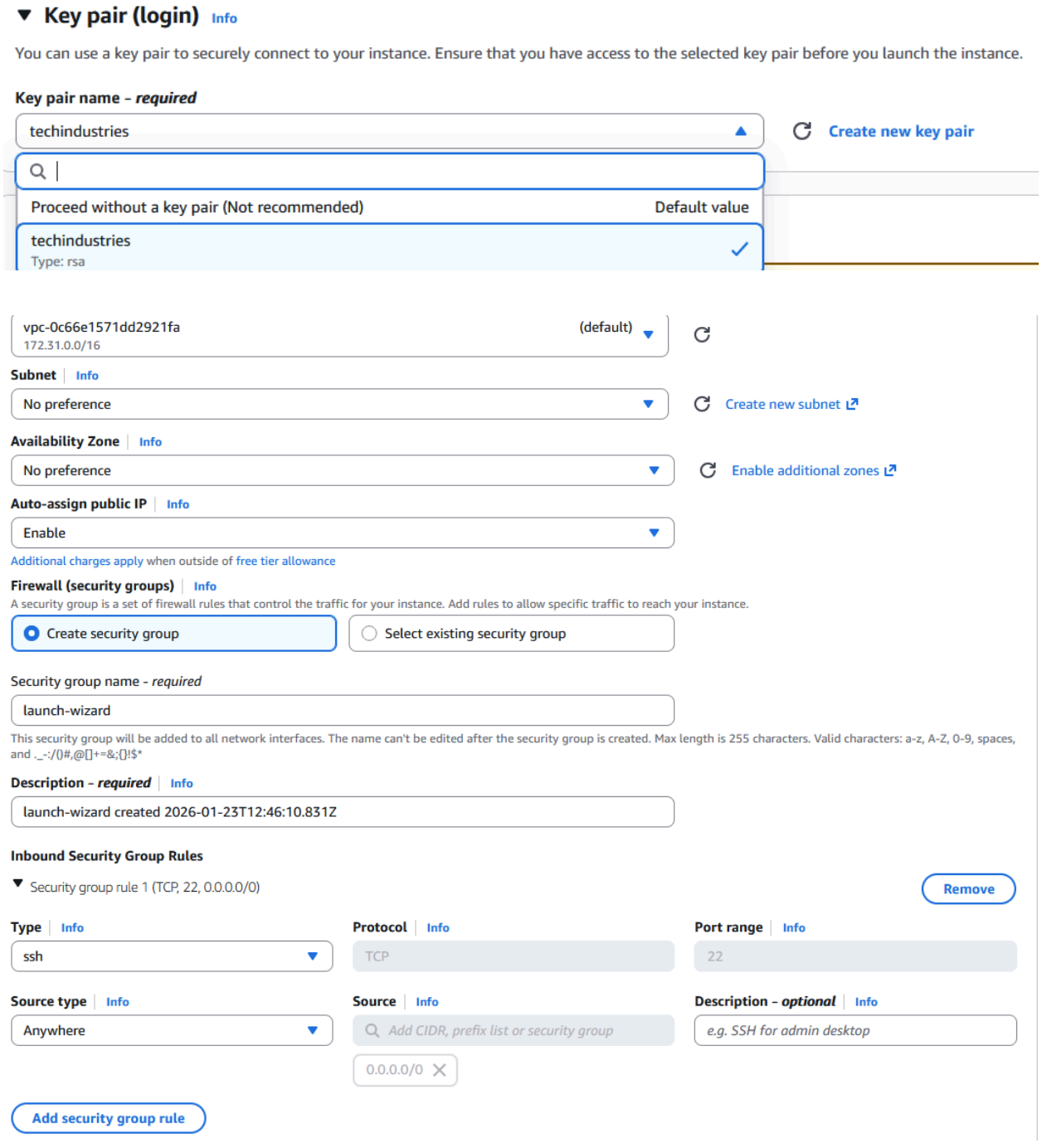
On-Demand Linux base pricing: 0.0104 USD per Hour On-Demand RHEL base pricing: 0.0392 USD per Hour

On-Demand Windows base pricing: 0.0196 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software



(Create a default VPC)

Configure storage Info

Advanced

1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.10....read more

ami-07ff62358b87c7116

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

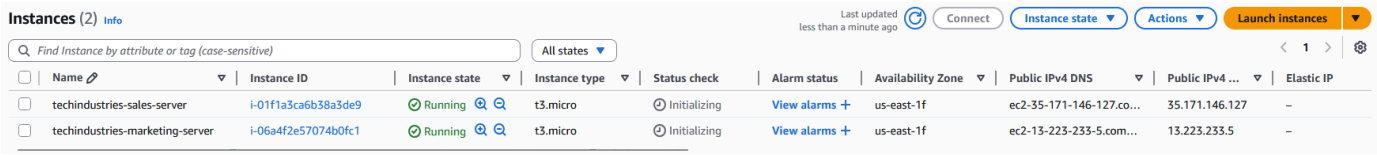
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

Cancel

Launch instance

Preview code



EC2 instances have successfully been created.

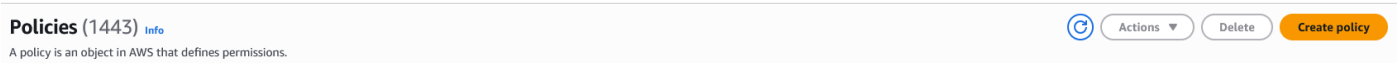
Create an IAM (Identity Access Management) policy:

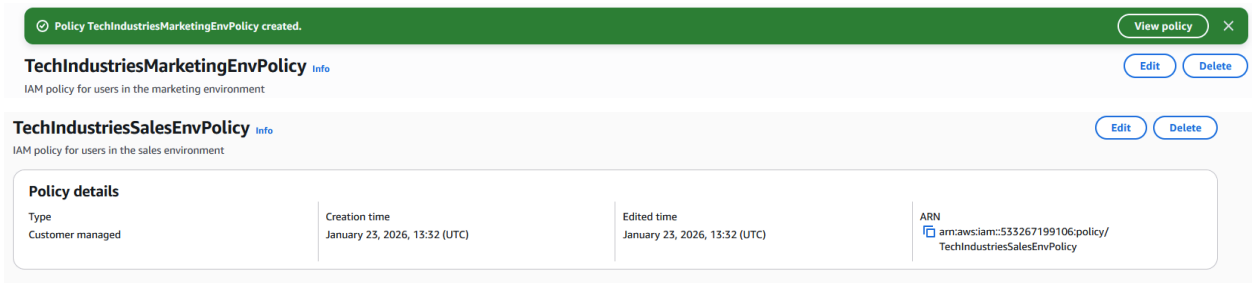
Purpose of this policy is to define the exact permissions users are allowed.
Example: “Allow read-only EC2 access.”

A descriptive tag is applied to each EC2 instance:

Instance	Tag Key	Tag Value
Marketing	Env	Marketing
Sales	Env	Sales

1. Navigate to the IAM dashboard (same process as finding EC2)
2. Navigate to policy
    a. Click create a new policy
3. Click on JSON
    a. Imported the JSON script
4. Edit the JSON script
    a. Environment tag: “Marketing”
5. Click on Next
6. Edit the policy
    a. Name: “TechIndustriesMarketingEnvPolicy”
    b. Description: IAM policy for users in the marketing environment
7. Click on create policy
8. Repeat the same steps but create a sales environment policy





Create an AWS account alias:

The purpose is to make login more secure and user-friendly.

1. Navigate to the IAM dashboard
2. Under AWS account click “Create alias”
3. Choose a name
    a. techinudstriesusers
4. Alias has been created

AWS Account

Account ID
533267199106

Account Alias
Create

Sign-in URL for IAM users in this account
https://533267199106.signin.aws.amazon.com/console

Create alias for AWS account 533267199106

Preferred alias

techindustriesusers

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL
https://techindustriesusers.signin.aws.amazon.com/console

IAM users will still be able to use the default URL containing the AWS account ID.

Cancel | Create alias

AWS Account

Account ID
533267199106

Account Alias
techindustriesusers Edit | Delete

Sign-in URL for IAM users in this account
https://techindustriesusers.signin.aws.amazon.com/console

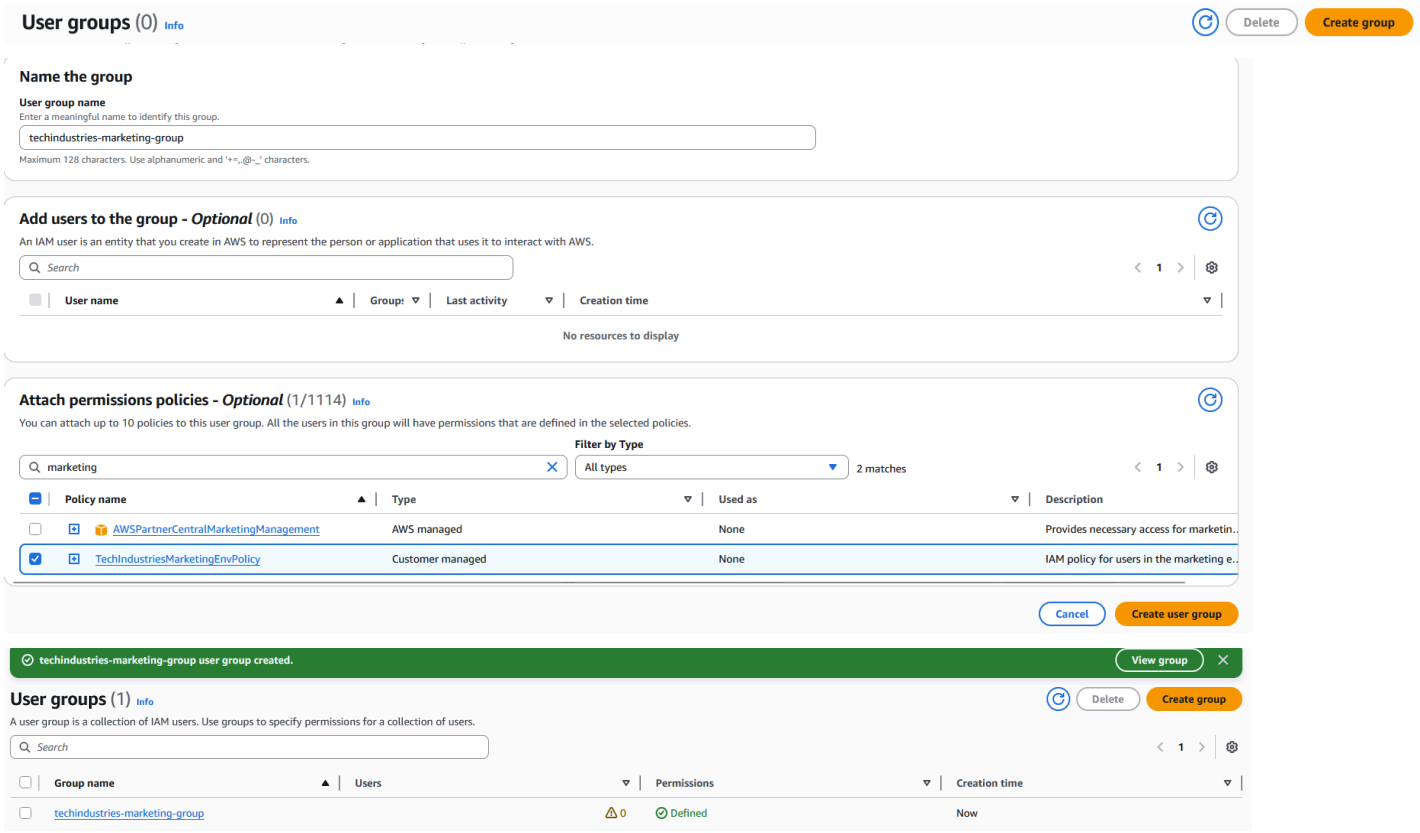
IAM users will log in via this url: https://techindustriesusers.signin.aws.amazon.com/console

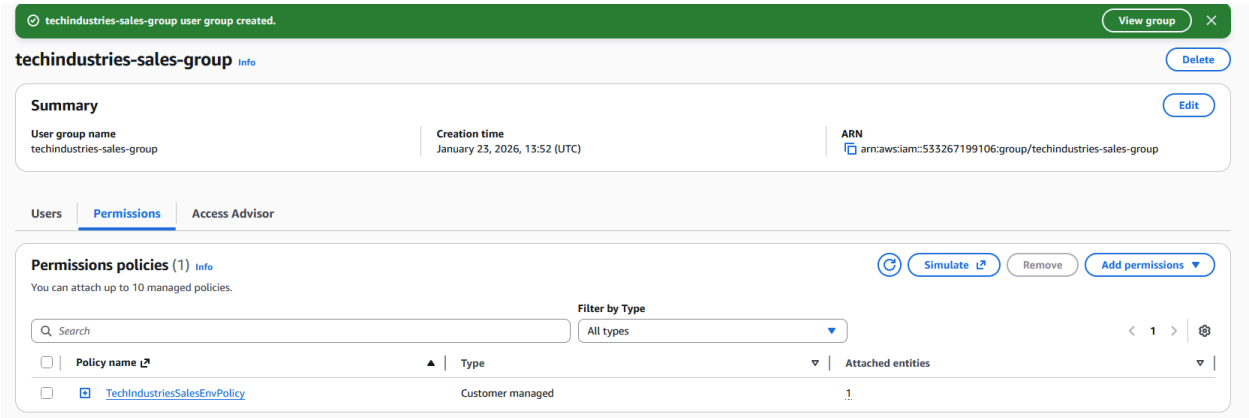
Creating an IAM group and user

The purpose is to manage permissions effectively using groups

IAM Group:

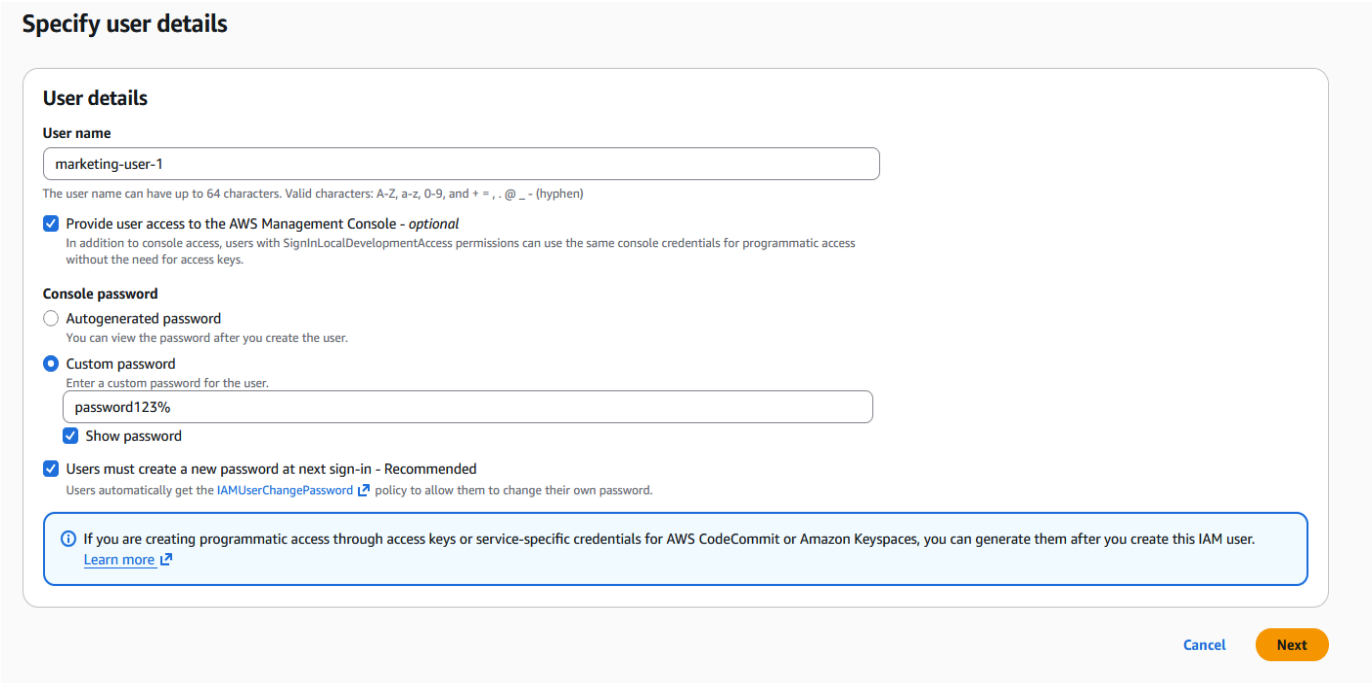
1. Navigate to IAM Dashboard
    a. Click on “User Groups”
2. Click “Create Group”
3. Name the Group - “techindustries-marketing-group”
4. Attach responding policy - “TechIndustriesMarketingEnvPolicy”
5. Click on Create user group
6. Repeat Process for Sales





IAM User:

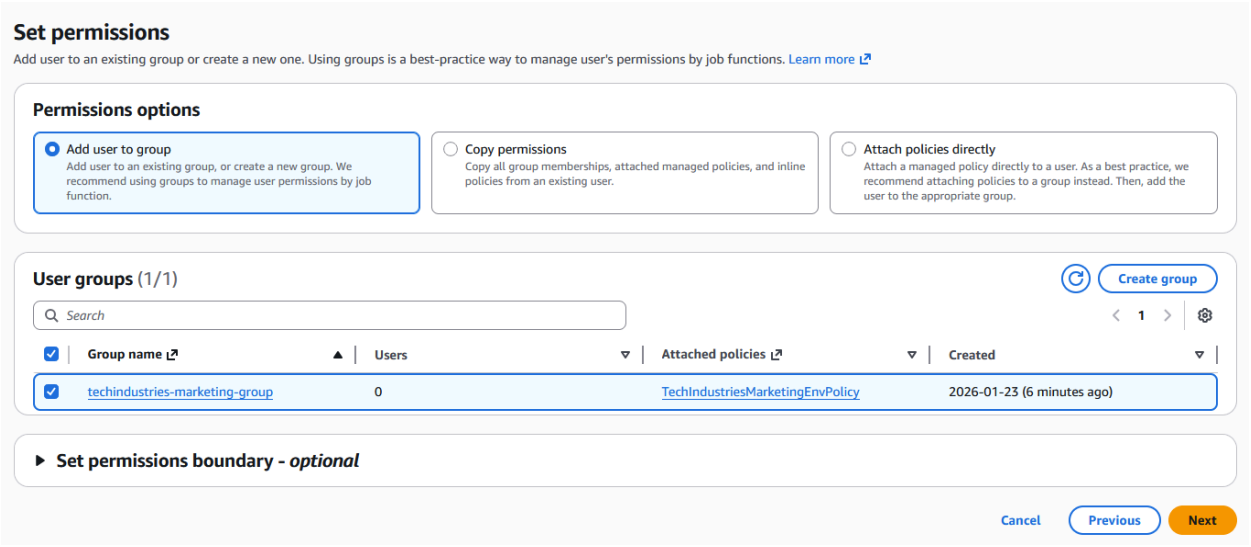
1. Navigate to Users
2. Click on “Create User”
3. Name the user - “marketing-user-1”
4. Click on “Provide User Access to the AWS management console”
5. Create a custom password - “password123%”
6. Check the box “User must create a new password at next sign-in”
7. Click Next

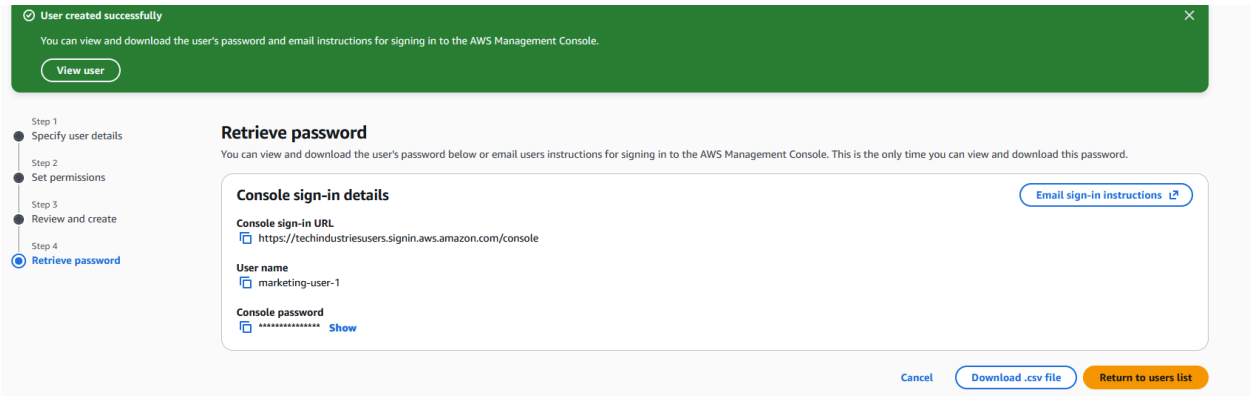


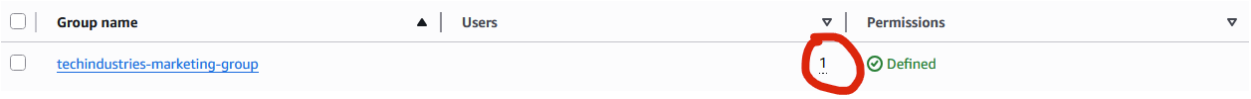
IAM user and group:

1. Click on the responding group to attach user to - “techindustries-marketing-group”
2. Click Next
3. Click Create User
4. Download csv file (optional)

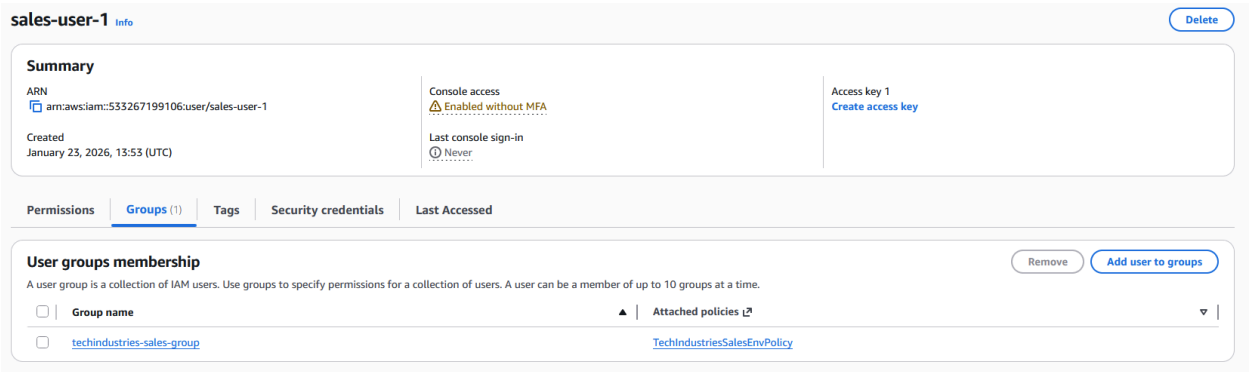
5. Repeat Process for Sales







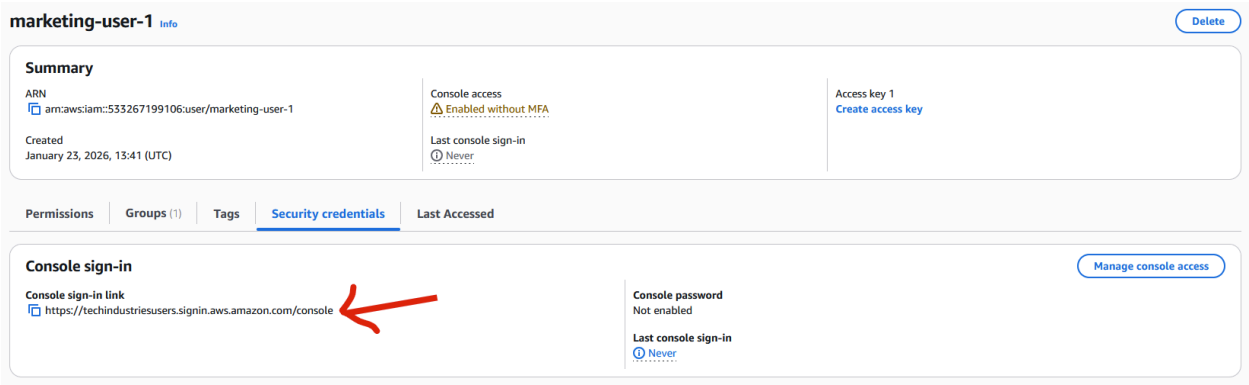
1 User under the group that has been created

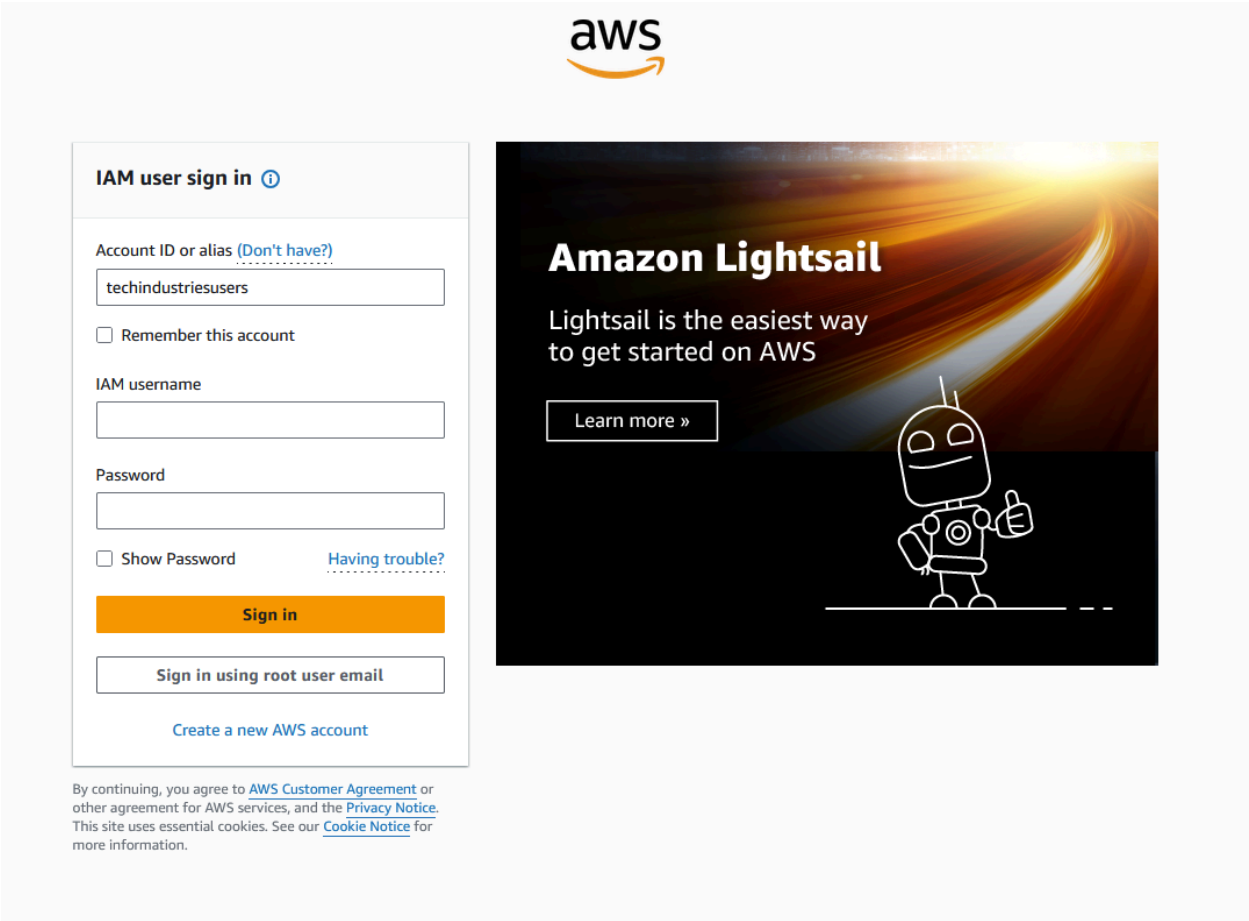


<u>Logging in as IAM User:</u>

1. Navigate to users
    a. Click on the user you created and click on the link

2. Input the credentials of the user's username and password.
    a. Prompted with a reset password (reset it to whatever you like)
3. Confirm the password change and log in.





IAM user sign in

Account ID or alias (Don't have?)

techindustriesusers

Remember this account

IAM username

marketing-user-1

Password

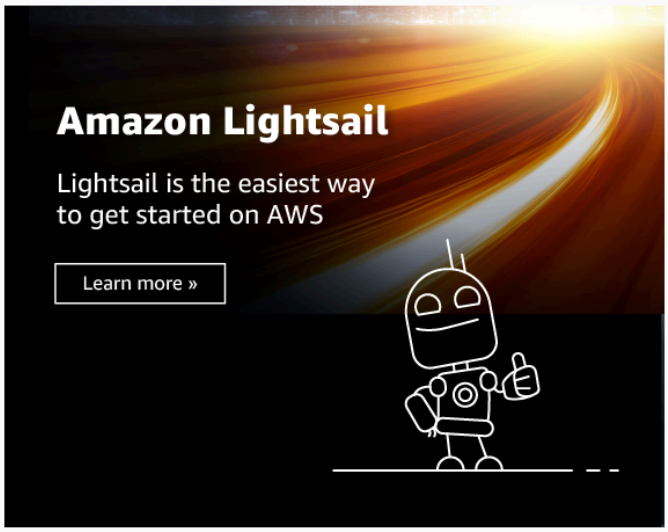
password123%

Show Password Having trouble?

Sign in

Sign in using root user email

Create a new AWS account



Password reset

Your account **(533267199106)** password has expired or requires a reset.

To continue, please verify your old and set a new password for **marketing-user-1** (not you?).

Old Password

password123%

Show Password

New Password

TechIndustriesRules123$

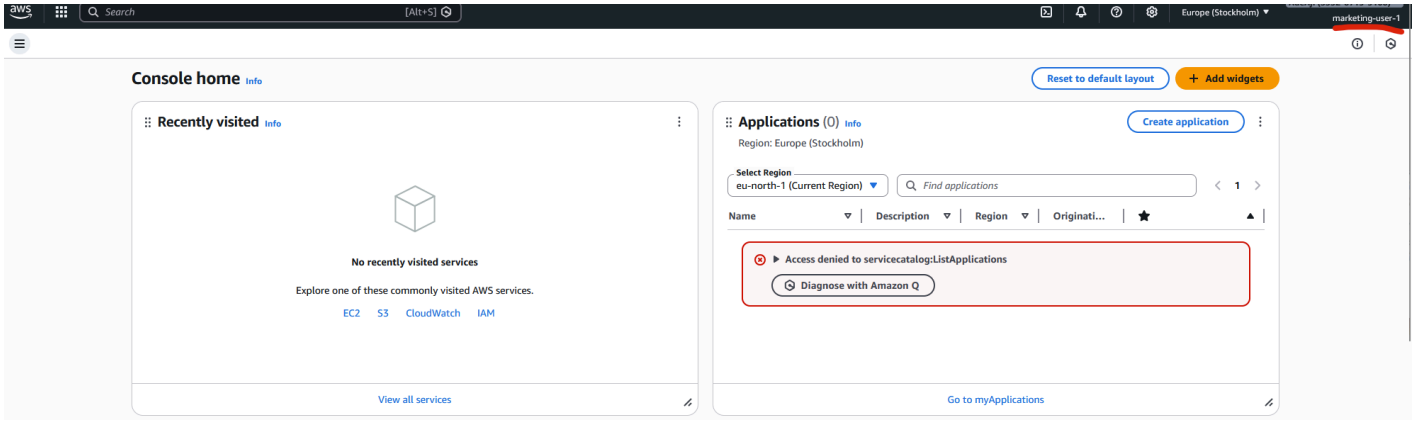
Confirm New Password

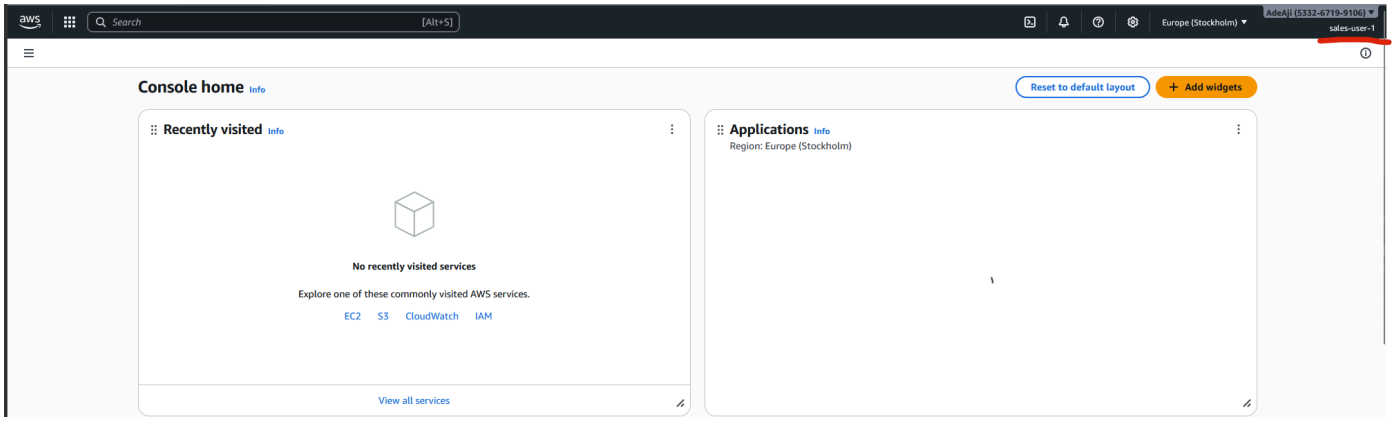
TechIndustriesRules123$

Show Password Matches

Confirm Password Change

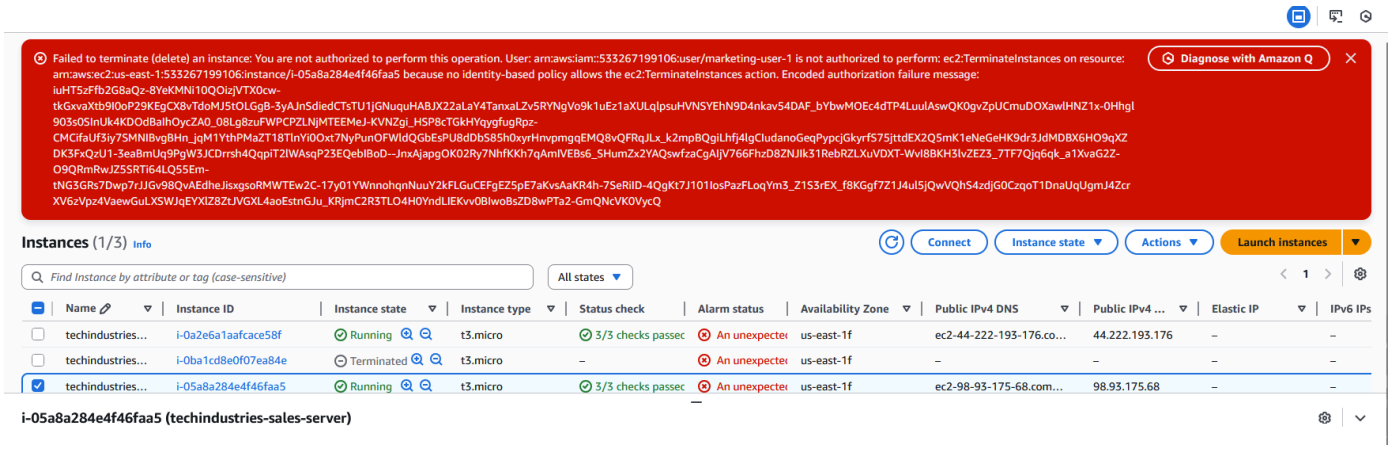
Sign in to a different account



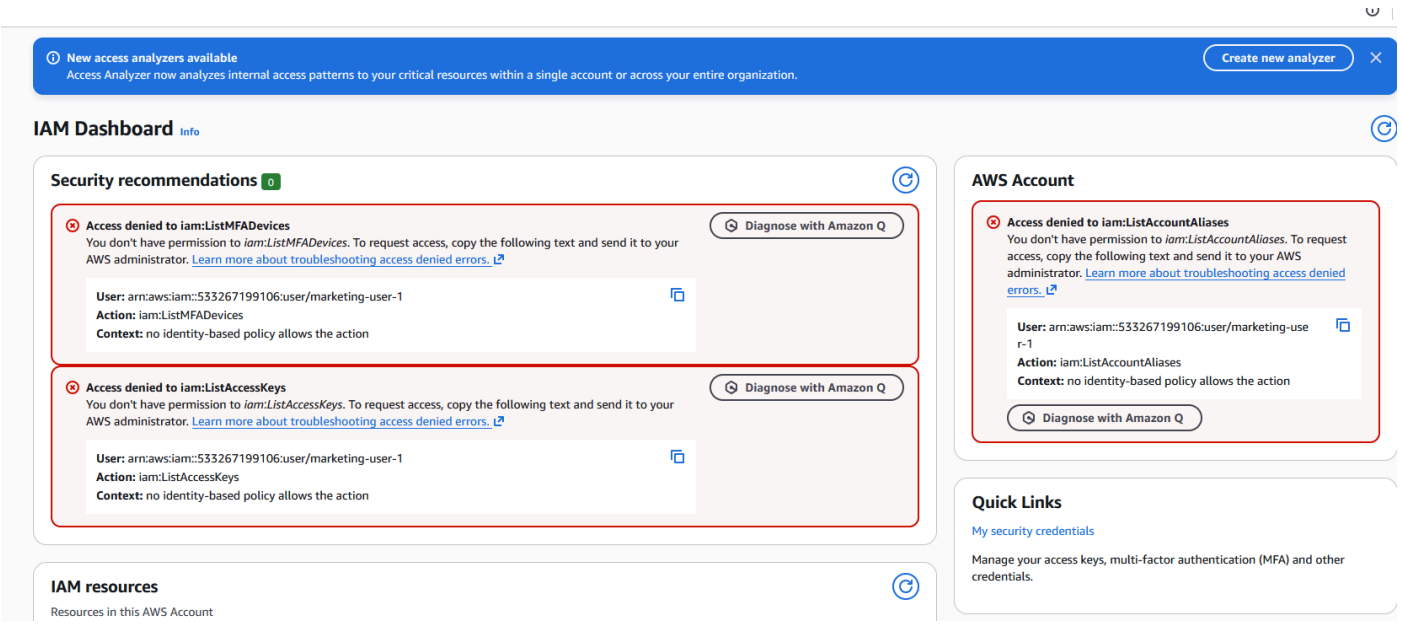


Test IAM User Access:

Proving security controls work.



When trying to terminate the sales ec2 instance, it denied access to do that as I am not in a sales IAM account.



Access denied to the IAM dashboard ^

Conclusion

The successful implementation of this lab highlights IAM as the foundational layer of cloud security. Key achievements included:

- Granular Security: Used resource tags (Marketing vs. Sales) to ensure users could only interact with their department's specific servers.
- Scalable Management: Implemented Group-based permissions, showcasing how to manage departmental access efficiently as an organization grows.
- Verified Boundaries: "Access Denied" results during testing proved that the security controls effectively prevented unauthorized modifications and lateral movement within the account.
- Best Practices: Established a secure environment by moving administrative tasks away from the Root account and requiring forced password resets for new IAM users.