

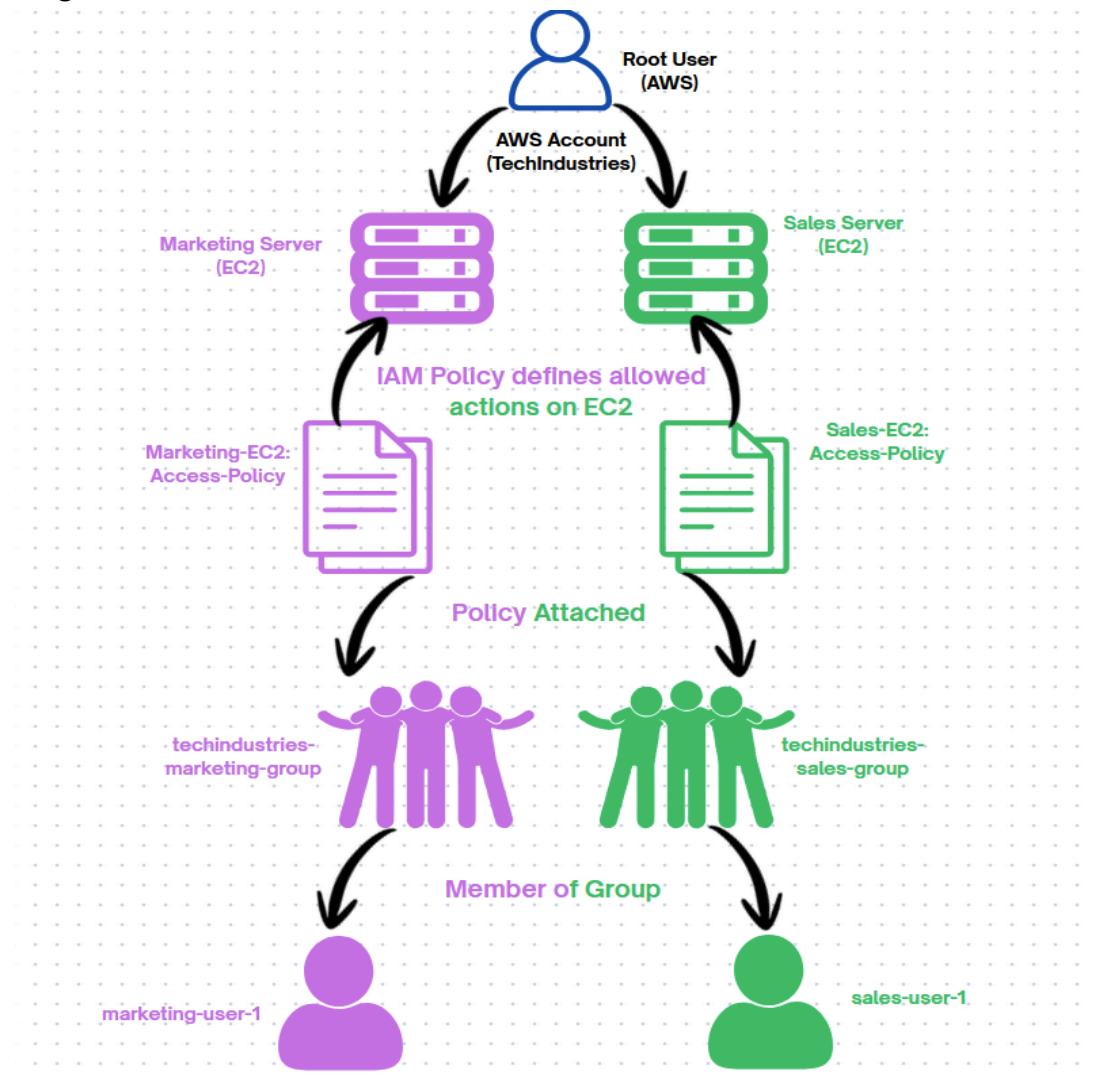
Cloud Security Project (AWS)

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:



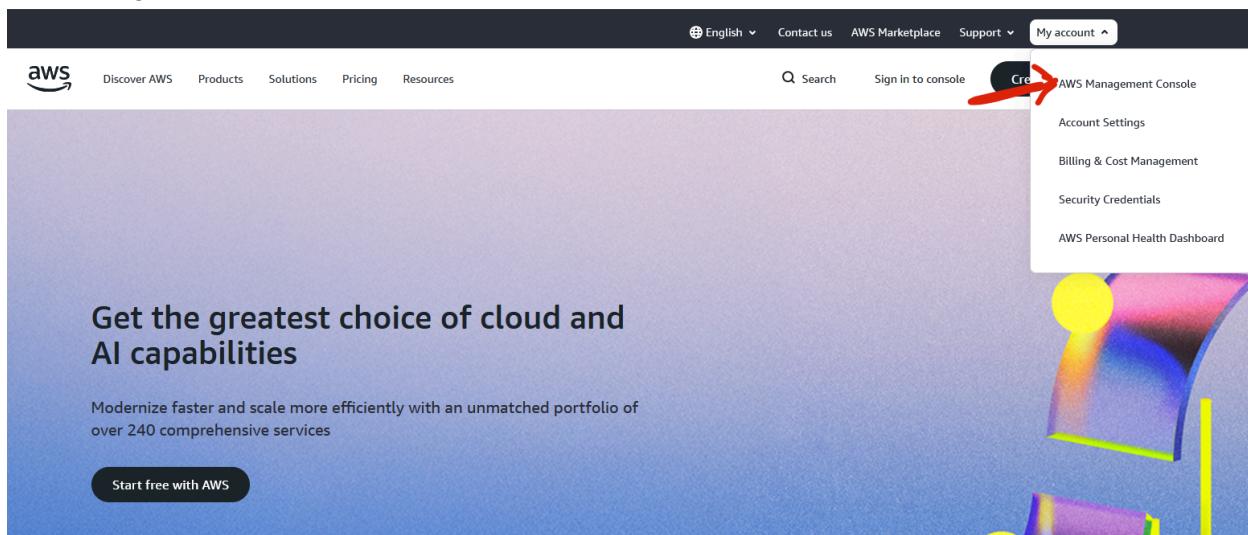
The root user is used only for account-level management, while IAM policies define permitted actions on EC2 resources. Department-specific groups are assigned policies granting scoped access to either the marketing or sales EC2 servers. Users inherit permissions through group membership, ensuring least-privilege 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 [\(i\)](#)

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.

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)



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

Next

OR

[New to AWS? Sign up](#)

Get AI-ready, cost-optimized storage

Store and query billions of vectors at up to 90% lower cost for search, RAG, and agent workflows.

[Discover S3 Vectors >](#)

Root user sign in

Enter the password for [REDACTED]@gmail.com (not you?)

Password

••••••••••••••••••

Show password [Forgot password?](#)

Sign in (highlighted by a red arrow)

[Sign in to a different account](#)

[Create a new AWS account](#)

Get AI-ready, cost-optimized storage

Store and query billions of vectors at up to 90% lower cost for search, RAG, and agent workflows.

[Discover S3 Vectors >](#)

Launching 2 EC2 Instances:

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

EC2

Ask Amazon Q

Services

Show more

Services Features Resources

EC2 Virtual Servers in the Cloud

Instances Info

Find Instance by attribute or tag (case-sensitive)

All states

Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 ... | Elastic IP | IPv6 IPs

No instances

You do not have any instances in this region

Launch instances (highlighted by a red arrow)

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 <input type="text" value="Name"/> X	Value Info <input type="text" value="techindustries-marketing-s"/> X	Resource types Info <input type="button" value="Select resource types"/> ▼ Remove Instances X
Key Info <input type="text" value="Env"/> X	Value Info <input type="text" value="Marketing"/> X	Resource types Info <input type="button" value="Select resource types"/> ▼ Remove Instances X

[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](#).

Recents	Quick Start					
						

[!\[\]\(4abb9e30c8f1a4cb50f04e228c782220_img.jpg\) Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI ami-07ff62358b87c7116 (64-bit (x86), uefi-preferred) / ami-059afa9e3a9c7af0c (64-bit (Arm), uefi) Virtualization: hvm ENA enabled: true Root device type: ebs	Free tier eligible ▼
---	--

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	(i)
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	

All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

techindustries

[Create new key pair](#)



Proceed without a key pair (Not recommended)

Default value

techindustries



Type: rsa

vpc-0c66e1571dd2921fa
172.31.0.0/16

(default) ▾



[Subnet](#) | [Info](#)

No preference



[Create new subnet](#) ↗

[Availability Zone](#) | [Info](#)

No preference



[Enable additional zones](#) ↗

[Auto-assign public IP](#) | [Info](#)

Enable



Additional charges apply when outside of [free tier allowance](#)

[Firewall \(security groups\)](#) | [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

[Create security group](#)

[Select existing security group](#)

Security group name - *required*

launch-wizard

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#@!+=;&|!\$*

Description - *required* | [Info](#)

launch-wizard created 2026-01-23T12:46:10.831Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

[Remove](#)

Type | [Info](#)

ssh

Protocol | [Info](#)

TCP

Port range | [Info](#)

22

Source type | [Info](#)

Anywhere

Source | [Info](#)

Add CIDR, prefix list or security group

Description - *optional* | [Info](#)

e.g. SSH for admin desktop

0.0.0.0/0

[Add security group rule](#)

(Create a default VPC)

▼ Configure storage Info

Advanced

1x GiB Root volume, 3000 IOPS, Not encrypted

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

[Add new volume](#)

i 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

i **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](#)

Instances (2) Info										
Last updated 🕒 Connect Instance state Actions Launch instances										
<input type="text"/> Find Instance by attribute or tag (case-sensitive) All states										
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	
techindustries-sales-server	i-01f1a3ca6b38a3de9	Running Q Q	t3.micro	Initializing	View alarms +	us-east-1f	ec2-35-171-146-127.co...	35.171.146.127	-	
techindustries-marketing-server	i-06a4f2e57074b0fc1	Running Q Q	t3.micro	Initializing	View alarms +	us-east-1f	ec2-13-223-233-5.com...	13.223.233.5	-	

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

Policies (1443) Info			
Actions Delete Create policy			
A policy is an object in AWS that defines permissions.			

```

"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:*",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ec2:ResourceTag/Env": "Marketing"
            }
        }
    },
]

```

Policy details

Policy name

Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+-=_,@-_` characters.

Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+-=_,@-_` characters.

Policy TechIndustriesMarketingEnvPolicy created.

[View policy](#)

X

TechIndustriesMarketingEnvPolicy [Info](#)

IAM policy for users in the marketing environment

[Edit](#)

[Delete](#)

TechIndustriesSalesEnvPolicy [Info](#)

IAM policy for users in the sales environment

[Edit](#)

[Delete](#)

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://533267199106signin.aws.amazon.com/console>

Create alias for AWS account 533267199106 X

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

The screenshot shows the AWS IAM User Groups creation interface. It consists of several stacked sections:

- User groups (0) Info**: A header with a refresh button, delete button, and a prominent orange "Create group" button.
- Name the group**: A section for entering the user group name. The input field contains "techindustries-marketing-group". Below it is a note: "Maximum 128 characters. Use alphanumeric and '+', '=', '@', '-' characters."
- Add users to the group - Optional (0) Info**: A section for adding users. It includes a search bar and a table with columns: User name, Group, Last activity, and Creation time. A message below says "No resources to display".
- Attach permissions policies - Optional (1/1114) Info**: A section for attaching policies. A search bar shows "marketing". The results table has columns: Policy name, Type, Used as, and Description. It lists two policies:
 - AWSPartnerCentralMarketingManagement (AWS managed, None, Provides necessary access for marketing..)
 - TechIndustriesMarketingEnvPolicy (Customer managed, None, IAM policy for users in the marketing e..)
- Success message**: A green banner at the bottom left says "⌚ techindustries-marketing-group user group created." with a circular icon.
- User groups (1) Info**: A final summary section showing one user group: "techindustries-marketing-group". It includes a "View group" button, a delete button, and another "Create group" button.

techindustries-sales-group [Info](#)

Summary

User group name: techindustries-sales-group

Creation time: January 23, 2026, 13:52 (UTC)

ARN: arn:aws:iam::533267199106:group/techindustries-sales-group

Permissions [Edit](#)

Users [Permissions](#) Access Advisor

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

Filter by Type	
<input type="text"/> Search	All types
<input type="checkbox"/> Policy name ?	Type
<input type="checkbox"/> TechIndustriesSalesEnvPolicy	Customer managed
Attached entities	
1	

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

Specify user details

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Provide user access to the AWS Management Console - *optional*

In addition to console access, users with SigninLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

Console password

Autogenerated password
You can view the password after you create the user.

Custom password
Enter a custom password for the user.

Show password

Users must create a new password at next sign-in - Recommended
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

[Cancel](#) [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

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more ↗](#)

Permissions options

Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

Search

Group name ↗

▲ | Users

▼ | Attached policies ↗

▼ | Created

techindustries-marketing-group

0

TechIndustriesMarketingEnvPolicy

2026-01-23 (6 minutes ago)



Create group

< 1 >



► Set permissions boundary - optional

Cancel

Previous

Next

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

[View user](#)

- Step 1 Specify user details
- Step 2 Set permissions
- Step 3 Review and create
- Step 4 Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

[Email sign-in instructions ↗](#)

Console sign-in URL

https://techindustriesuserssignin.aws.amazon.com/console

User name

marketing-user-1

Console password

***** [Show](#)

Cancel

[Download .csv file](#)

[Return to users list](#)

Group name	Users	Permissions
<input type="checkbox"/> techindustries-marketing-group	1	<input checked="" type="radio"/> Defined

1 User under the group that has been created

[sales-user-1](#) [Info](#)

Summary

ARN

arn:aws:iam::533267199106:user/sales-user-1

Created

January 23, 2026, 13:53 (UTC)

Console access

Enabled without MFA

Last console sign-in

Never

Access key 1

[Create access key](#)

Permissions

Groups (1)

Tags

Security credentials

Last Accessed

User groups membership

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

[Remove](#)

[Add user to groups](#)

Group name

Attached policies ↗

[techindustries-sales-group](#)

TechIndustriesSalesEnvPolicy

Logging in as IAM User:

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.

marketing-user-1 [Info](#) [Delete](#)

Summary					
ARN arn:aws:iam::533267199106:user/marketing-user-1	Console access ⚠ Enabled without MFA				
Created January 23, 2026, 13:41 (UTC)	Last console sign-in ⌚ Never				
Access key 1 Create access key					
Permissions Groups (1) Tags Security credentials Last Accessed					
Console sign-in <table border="1"> <tr> <td>Console sign-in link https://techindustriesusers.signin.aws.amazon.com/console</td> <td>Manage console access</td> </tr> <tr> <td>Console password Not enabled</td> <td>Last console sign-in ⌚ Never</td> </tr> </table>		Console sign-in link https://techindustriesusers.signin.aws.amazon.com/console	Manage console access	Console password Not enabled	Last console sign-in ⌚ Never
Console sign-in link https://techindustriesusers.signin.aws.amazon.com/console	Manage console access				
Console password Not enabled	Last console sign-in ⌚ Never				

IAM user sign in [i](#)

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.

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](#)

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.

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)





Password reset (i)

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

Show Password

New Password

Confirm New Password

Show Password

Matches

Confirm Password Change

[Sign in to a different account](#)

Test IAM User Access:

Proving security controls work.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs
techindustries...	i-0a2e6a1aafcae58f	Running	t3.micro	3/3 checks passed	An unexpected	us-east-1f	ec2-44-222-193-176.co...	44.222.193.176	-	-
techindustries...	i-0ba1cd8e0f07ea84e	Terminated	t3.micro	-	An unexpected	us-east-1f	-	-	-	-
techindustries...	i-05a8a284e4f46faa5	Running	t3.micro	3/3 checks passed	An unexpected	us-east-1f	ec2-98-93-175-68.com...	98.93.175.68	-	-

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

The screenshot shows the AWS IAM Dashboard. At the top, there's a blue header bar with a message about new access analyzers available and a 'Create new analyzer' button. Below the header, the main interface is divided into several sections:

- Security recommendations**: This section contains two items, both highlighted with red boxes:
 - Access denied to iam>ListMFADevices**: You don't have permission to `iam>ListMFADevices`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)
User: arn:aws:iam::533267199106:user/marketing-user-1
Action: iam>ListMFADevices
Context: no identity-based policy allows the action
 - Access denied to iam>ListAccessKeys**: You don't have permission to `iam>ListAccessKeys`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)
User: arnaws:iam::533267199106:user/marketing-user-1
Action: iam>ListAccessKeys
Context: no identity-based policy allows the action
- AWS Account**: This section also has a single item highlighted with a red box:
 - Access denied to iam>ListAccountAliases**: You don't have permission to `iam>ListAccountAliases`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)
User: arn:aws:iam::533267199106:user/marketing-user-1
Action: iam>ListAccountAliases
Context: no identity-based policy allows the action
- IAM resources**: A section showing resources in this AWS Account.
- Quick Links**: A section with a link to 'My security credentials'.

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.