

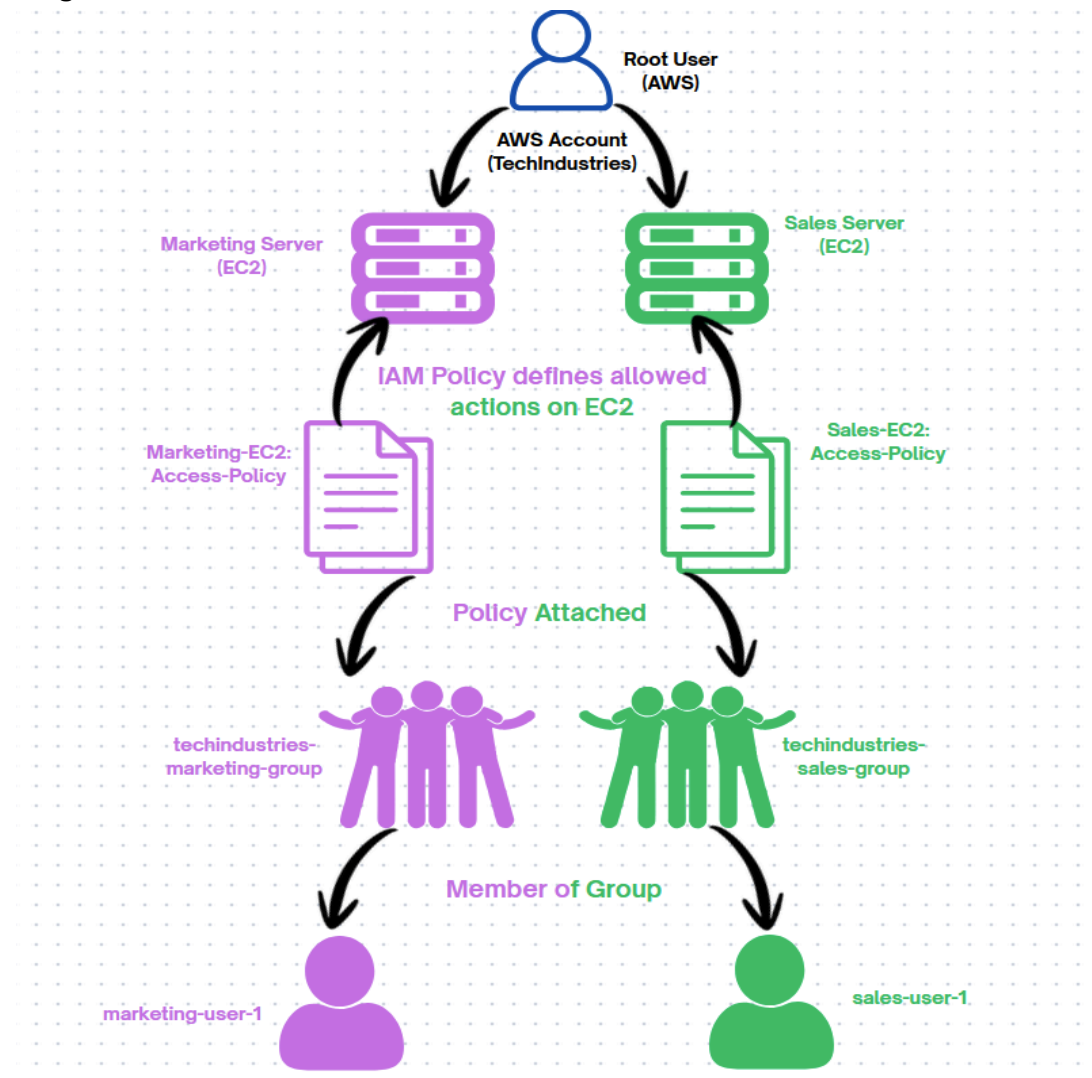
Cloud Security Project (AWS)

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:



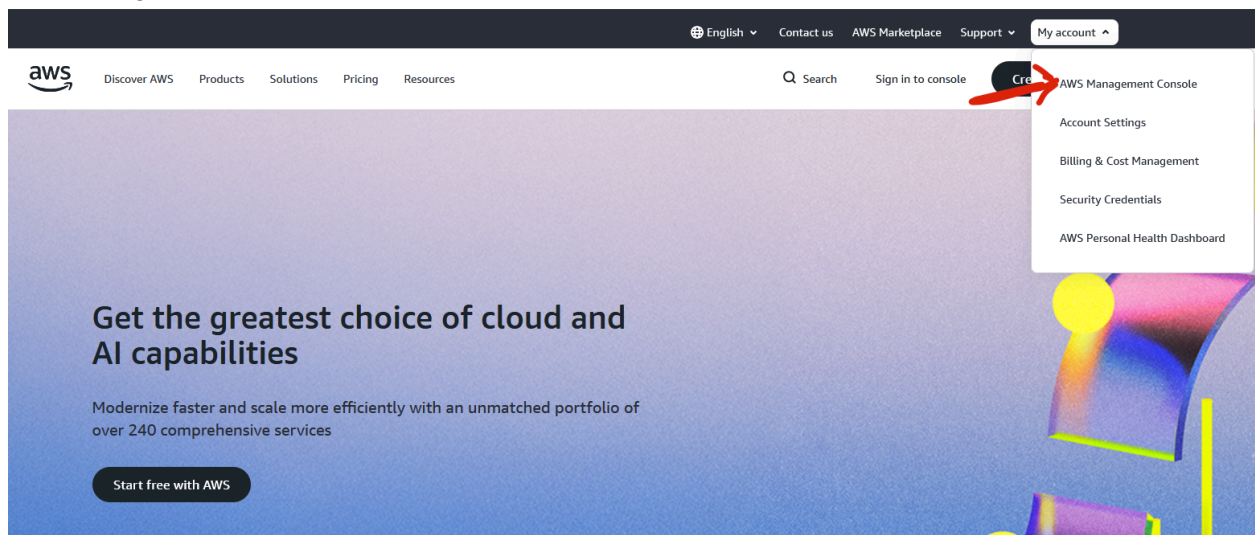
The root user is used only for account-level management, while IAM policies define permitted actions on EC2 resources. Department-specific groups are assigned policies granting scoped access to either the marketing or sales EC2 servers. Users inherit permissions through group membership, ensuring least-privilege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

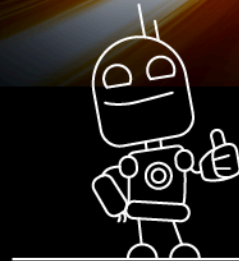
[Create a new AWS account](#)

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.

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
[redacted]

☐ Show password [Forgot password?](#)

Sign in

[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

The screenshot shows the AWS Management Console. At the top, there's a search bar with 'EC2' entered. Below it, the 'Services' section highlights 'EC2' as 'Virtual Servers in the Cloud'. The main content area shows the 'Instances' page, which is currently empty with a message: 'No instances. You do not have any instances in this region.' and a 'Launch instances' button. The left sidebar shows the navigation menu with 'EC2' selected.

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](#)

Q Name

X

Q techindustries-marketing-s

X

Select resource types

▼

Remove

Instances

X

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

Q Env

X

Q Marketing

X

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](#).

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

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

Q

[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	Info	
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

▼ 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

Q |

Proceed without a key pair (Not recommended) Default value

techindustries ✓
Type: rsa

[Create new key pair](#)

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](#)

Q Add CIDR, prefix list or security group

0.0.0.0/0 X

Description - *optional* [Info](#)

e.g. SSH for admin desktop


[Add security group rule](#)

(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](#)

Instances (2) [Info](#)

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

All states

< 1 >

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	techindustries-sales-server	i-01f1a3ca6b38a3de9	Running	t3.micro	Initializing	View alarms +	us-east-1f	ec2-35-171-146-127.co...	35.171.146.127	-
<input type="checkbox"/>	techindustries-marketing-server	i-06a4f2e57074b0fc1	Running	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

A policy is an object in AWS that defines permissions.

Actions

▼

Delete

Create policy


```

"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.

TechIndustriesMarketingEnvPolicy

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

Description - optional

Add a short explanation for this policy.

IAM policy for users in the marketing environment

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

✓ Policy TechIndustriesMarketingEnvPolicy created.

[View policy](#) ✕

TechIndustriesMarketingEnvPolicy [Info](#)

IAM policy for users in the marketing environment

[Edit](#)

[Delete](#)

TechIndustriesSalesEnvPolicy [Info](#)

IAM policy for users in the sales environment

[Edit](#)

[Delete](#)

Policy details

Type

Customer managed

Creation time

January 23, 2026, 13:32 (UTC)

Edited time

January 23, 2026, 13:32 (UTC)

ARN

[armaws:iam::533267199106:policy/TechIndustriesSalesEnvPolicy](#)

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. technudstriesusers
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>

techindustries-sales-group user group created. View group ×

techindustries-sales-group [Info](#) Delete

Summary Edit

User group name techindustries-sales-group	Creation time January 23, 2026, 13:52 (UTC)	ARN arn:aws:iam::533267199106:group/techindustries-sales-group
---	--	---

Users **Permissions** Access Advisor

Permissions policies (1) [Info](#) Simulate Remove Add permissions

You can attach up to 10 managed policies.

Search Filter by Type
All types

<input type="checkbox"/> Policy name i	<input type="checkbox"/> Type	<input type="checkbox"/> Attached entities
<input checked="" type="checkbox"/> TechIndustriesSalesEnvPolicy	Customer managed	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



Create group

< 1 > ⚙️

<input checked="" type="checkbox"/>	Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/>	techindustries-marketing-group	0	TechIndustriesMarketingEnvPolicy	2026-01-23 (6 minutes ago)

► 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

Console sign-in URL

<https://techindustriesusers.signin.aws.amazon.com/console>

User name

[marketing-user-1](#)

Console password

***** [Show](#)

[Email sign-in instructions](#)

Cancel

Download .csv file

Return to users list

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

1 User under the group that has been created

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

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 [Remove](#) [Add user to groups](#)

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.

<input type="checkbox"/>	Group name	Attached policies
<input type="checkbox"/>	techindustries-sales-group	TechIndustriesSalesEnvPolicy

Logging in as IAM User:

1. Navigate to users

- 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](#)

Created
January 23, 2026, 13:41 (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

Console sign-in Manage console access

Console sign-in link
<https://techindustriesusers.signin.aws.amazon.com/console>

Console password
Not enabled

Last console sign-in
[Never](#)



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.

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)



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 ⓘ

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

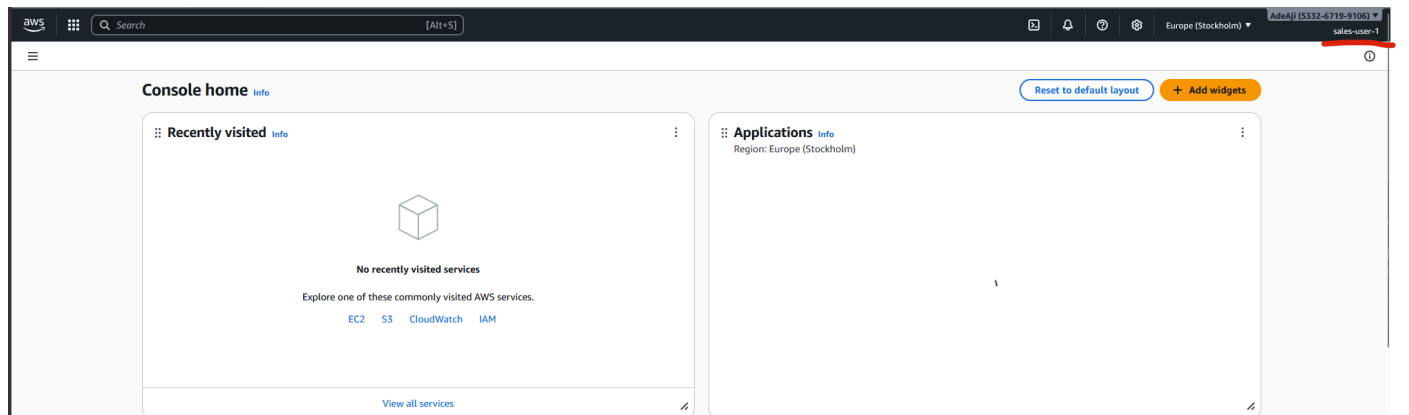
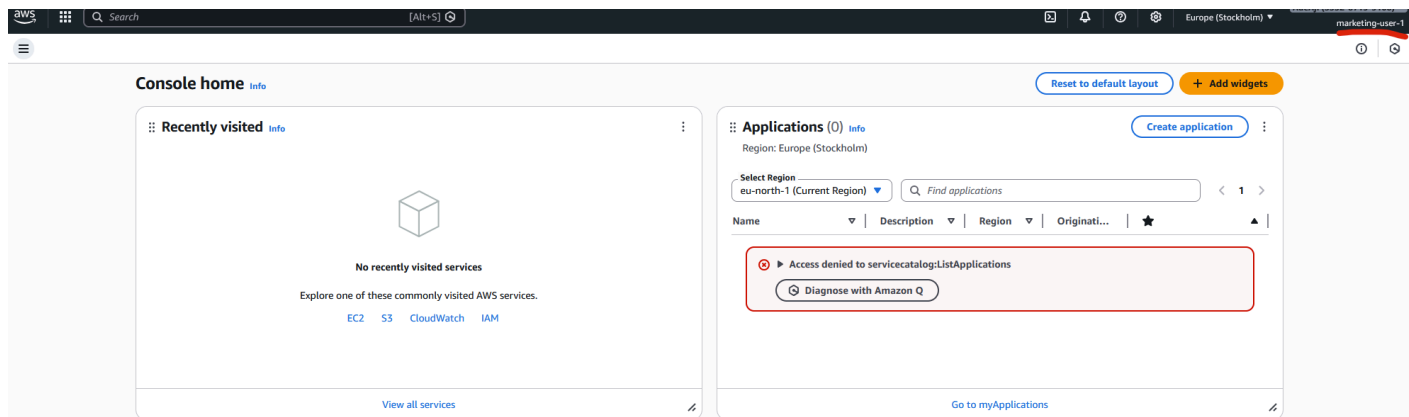
Confirm New Password

☒ Show Password

Matches

Confirm Password Change

[Sign in to a different account](#)



Test IAM User Access:

Proving security controls work.

Failed to terminate (delete) an instance: You are not authorized to perform this operation. User: arn:aws:iam::533267199106:user/marketing-user-1 is not authorized to perform: ec2:TerminateInstances on resource: i-05a8a284e4f46faa5 because no identity-based policy allows the ec2:TerminateInstances action. Encoded authorization failure message: iuHTS7Ffb2G8aQz-8YekMNI10QOizjVTX0cw-tkGxvaXtb9I0oP29KEgCX8vTdoMj5tOLGpB-3yAJnSdiedCT5TU1jGNuquHABJX22aLaY4TanxLZv5RYNgVo9k1uEz1aXULqIpsuHVNSYEHNSD4nkav54DAF_bYbwMOEc4dTP4LuulAswQK0gv2pUCmuDOXawIHZN1x-0Hhgl903s05InUK4KDQd8ahOycZA0_0BLg8zuFWPCPZLNjMTEEmeJ-KVNZ9L_HSP8CTGKHqyqfugRpz-CMCifaUf3iy75SMNIBvgBhN_jqM1YthPmaZT18TinY00xt7NyPunOFWldQGbePU8dDb585h0xyrHnypmgqEMQ8vQFRqJLx_k2mpBQgILhfj4lgCludanoGeqPypcjGkyrf57jtdEX2Q5mk1eNeGeHK9dr3IdMDBX6HO9qXZDK3FxQzU1-3eaBmUq9PgW3jCDrrsh4Qopi2IiWAsqP23EQebIBoD-JnxAJjagpOK02Ry7NhfKKh7qAmIvEBs6_SHumZx2YAQswfzaCgAljV766FhzD8ZNIJk31RebRZLXuVDXT-WvIB8KH3lvZEZ3_7TF7Qjq6qk_a1XraG2Z-O9QRmRwJZ5SRTi64LQ55Em-nNG3GRs7Dwp7rJJGv98QvAEdheJisxgsRMTWew2C-17y01YWnnohqNuuY2kFLGuCEFGZ5pE7aKvSaAKR4h-75eRiID-4QgKt7J101losPazFLoqYm3_Z153rEX_f8KGg77Z1J4ul5jQwVQh54zdgjG0CzqpT1DnaUqUgmJ4ZcrXV6zVpz4VaewGuLXSWJqEYXIZ8ZuJVGXL4aoEstrnGJv_KRjmc2R3TLO4H0YndLIEKv0Blwo8s2D8wPTa2-GmQNcVK0VycQ

Instances (1/3)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
techindustries...	i-0a2e6a1aafca58f	Running	t3.micro	3/3 checks passed	An unexpected	us-east-1f	ec2-44-222-193-176.com...	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	-	-

i-05a8a284e4f46faa5 (techindustries-sales-server)

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 displays the AWS IAM Dashboard with a blue header bar. A notification at the top states: "New access analyzers available. Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization." A "Create new analyzer" button is in the top right. The main content area is divided into three sections: "Security recommendations", "AWS Account", and "IAM resources".

Security recommendations

- 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: arn:aws:iam::533267199106:user/marketing-user-1
Action: iam:ListAccessKeys
Context: no identity-based policy allows the action

AWS Account

- 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

Quick Links

[My security credentials](#)
Manage your access keys, multi-factor authentication (MFA) and other credentials.

IAM resources
Resources in this AWS 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.