

# Group 4 Case Study

## Group Members

---

W A Shadman

Sumeet Kaur Saund

Noorpreet Gill

Arshjot Ghuman

Vi Le

Austin Chapdelaine



# Abstract

- Our employer is adopting the principle that employees can work seamlessly no matter where they are, while centralized management ensures they only access the specific resources they need for their jobs.
- As the security consultant to the organization, it is our role to work with the operation and cloud team to set up Identity and Access Management (IAM).
- The proposed solution will allow new users to be added with appropriate permissions that reflect the principle of least privilege.

# Objectives

1

Enumerate all the users (use only your team members) and add them to the IAM identity management module of IAM in Amazon Web Services (AWS).

2

Assign them IAM roles based on the principle of least privilege.

3

Develop a detailed policy for identity and access management.

# Demo (User Groups)

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, a search bar, and a user profile. The left sidebar is titled 'Identity and Access Management (IAM)' and contains a search bar and a list of navigation items: Dashboard, Access management (expanded), Access reports, and Account settings. The main content area is titled 'IAM > User groups' and shows a list of three user groups. Each group has a checkbox, a name, a user count, a permissions status, and a creation time. The groups are 'Admin' (1 user, Defined, 4 hours ago), 'Developer' (3 users, Defined, 1 hour ago), and 'Employee' (2 users, Defined, 1 hour ago). The bottom of the page features a footer with 'Feedback', 'Language', and copyright information.

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Admin	1	✓ Defined	4 hours ago
<input type="checkbox"/>	Developer	3	✓ Defined	1 hour ago
<input type="checkbox"/>	Employee	2	✓ Defined	1 hour ago



# Demo (Users)

aws

Services

Search

[Alt+S]

Global

Vi @ 2605-2835-7873

EC2

Identity and Access Management (IAM)

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity

IAM > Users

Users (6) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

Refresh Delete Add users

< 1 > Settings

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	Arshjot	Developer	Never	None	7 minutes ago	-
<input type="checkbox"/>	Austin	Employee	20 minutes ago	Virtual	19 minutes ago	-
<input type="checkbox"/>	Gill	Employee	17 minutes ago	None	17 minutes ago	-
<input type="checkbox"/>	Shadman	Developer	10 minutes ago	None	9 minutes ago	-
<input type="checkbox"/>	Sumeet	Developer	8 minutes ago	None	8 minutes ago	-
<input type="checkbox"/>	Vi	Admin	23 minutes ago	Virtual	4 days ago	4 days ago

Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Demo (Admin Permission)

aws

Services

Search [Alt+S]

Global

Vi @ 2605-2835-7873

EC2

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity

Summary

Edit

User group name: Admin

Creation time: March 28, 2023, 12:00 (UTC-05:00)

ARN: arn:aws:iam::260528357873:group/Admin

UsersPermissionsAccess Advisor

Permissions policies (5) Info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

	Policy name	Type	Description
<input type="checkbox"/>	<a href="#">Admin</a>	Customer managed	For Admin
<input type="checkbox"/>	<a href="#">Developer</a>	Customer managed	For developer
<input type="checkbox"/>	<a href="#">Employee</a>	Customer managed	For employee, read only
<input type="checkbox"/>	<a href="#">AmazonRDSFullAccess</a>	AWS managed	Provides full access to Amazon RDS via the AWS Management Console.
<input type="checkbox"/>	<a href="#">IAMFullAccess</a>	AWS managed	Provides full access to IAM via the AWS Management Console.

https://us-east-1.console.aws.amazon.com/iamv2/home#

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Demo (Developer Permission)

The screenshot displays the AWS IAM console interface. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and a user profile 'Vi @ 2605-2835-7873'. The left sidebar shows the 'Identity and Access Management (IAM)' section with a search bar and a list of navigation items: Dashboard, Access management (expanded), User groups (selected), Users, Roles, Policies, Identity providers, Account settings, Access reports (expanded), Access analyzer, Archive rules, Analyzers, Settings, Credential report, and Organization activity.

The main content area is titled 'Developer' and includes a 'Delete' button. Below the title is a 'Summary' section with a table of key information:

User group name Developer	Creation time March 28, 2023, 15:24 (UTC-05:00)	ARN <a href="#">arn:aws:iam::260528357873:group/Developer</a>
------------------------------	--	--

Below the summary is a tabbed interface with 'Users', 'Permissions' (selected), and 'Access Advisor' tabs. The 'Permissions' tab shows 'Permissions policies (1)' with an 'Info' link. A note states: 'You can attach up to 10 managed policies.' Action buttons include 'Simulate', 'Remove', and 'Add permissions'. A search bar allows filtering policies by property or name.

A table lists the attached policy:

<input type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Description
<input type="checkbox"/>	<a href="#">+ Developer</a>	Customer managed	For developer

The footer of the console shows the URL 'https://us-east-1.console.aws.amazon.com/iamv2/home#', copyright information '© 2023, Amazon Web Services, Inc. or its affiliates.', and links for 'Privacy', 'Terms', and 'Cookie preferences'.

# Demo (Employee Permission)

The screenshot displays the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services' link, a search bar, and the user's account information 'Vi @ 2605-2835-7873'. The left sidebar shows the 'Identity and Access Management (IAM)' section with a search bar and a list of navigation items: Dashboard, Access management (expanded), User groups (selected), Users, Roles, Policies, Identity providers, Account settings, Access reports (expanded), Access analyzer, Archive rules, Analyzers, Settings, Credential report, and Organization activity.

The main content area is titled 'Employee' and includes a 'Delete' button. Below the title is a 'Summary' section with three columns: 'User group name' (Employee), 'Creation time' (March 28, 2023, 15:00 (UTC-05:00)), and 'ARN' (arn:aws:iam::260528357873:group/Employee). Below the summary are three tabs: 'Users', 'Permissions' (active), and 'Access Advisor'.

The 'Permissions' tab shows 'Permissions policies (1)' with an 'Info' link. Below this is a search bar with the placeholder text 'Filter policies by property or policy name and press enter.' and a table with the following columns: 'Policy name', 'Type', and 'Description'. The table contains one entry: 'Employee' (with a plus icon), 'Customer managed', and 'For employee, read only'. Above the table are buttons for 'Simulate', 'Remove', and 'Add permissions'.

The bottom of the console shows the URL 'https://us-east-1.console.aws.amazon.com/iamv2/home#' and the footer text '© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.



# Demo (Permission Example- Developer)

aws

Services

Search

[Option+S]

🔍 🔔 ⓘ Global Shadman @ 2605-2835-7873

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3


Amazon S3 > Storage Lens

Storage Lens

Info


Storage Lens provides visibility into storage usage and activity trends at the organization or account level, with drill-downs by Region, storage class, bucket, and prefix. [Learn more](#)

▼ Getting started with Storage Lens




Create dashboard

Configure the scope of your dashboard, choose a metrics tier, and optionally configure a metrics export.



Daily aggregation

Each day your storage metrics are pre-aggregated by account, Region, storage class, and bucket - and optionally by AWS organization and prefix.



Analyze your storage

Use the interactive dashboard to explore usage and activity trends and insights, and contextual recommendations for best practices to optimize your storage.

ⓘ

⛔ Insufficient permissions to get Storage Lens

After you or your AWS administrator have updated your IAM permissions to allow the `s3:ListStorageLensConfigurations`, refresh the page. Learn more about [Identity and access management in Amazon S3](#)

▶ API response

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Demo (Admin Policy)

aws

Services

Search

[Alt+S]

EC2

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Policies > Admin

Summary

Delete policy

Policy ARNarn:aws:iam::260528357873:policy/Admin

DescriptionFor Admin

PermissionsPolicy usageTagsPolicy versionsAccess Advisor

Policy summaryJSONEdit policy

Filter

Service	Access level	Resource	Request condition
Allow (1 of 371 services) Show remaining 370			
EC2	Full: Read, Permissions management, Tagging Limited: Write	All resources	aws:MultiFactorAuthPresent   Bool   true (If Exists)

FeedbackLanguage

© 2023, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

aws

Services

Search

[Alt+S]

EC2

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Policies > Admin

Summary

Delete policy

Policy ARNarn:aws:iam::260528357873:policy/Admin

DescriptionFor Admin

PermissionsPolicy usageTagsPolicy versionsAccess Advisor

Policy summaryJSONEdit policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:GetIpamResourceCidrs",
9         "ec2:GetInstanceUefidData",
10        "ec2:GetIpamPoolCidrs",
11        "ec2:MonitorInstances",
12        "ec2:GetEbsEncryptionByDefault",
13        "ec2:CreateKeyPair",
14        "ec2:ExportClientVpnClientConfiguration",
15        "ec2:GetHostReservationPurchasePreview",
16        "ec2:CreateImage",
17        "ec2:CopyImage",
18        "ec2:GetConsoleScreenshot",
19        "ec2:GetLaunchTemplateData"
```

https://us-east-1.console.aws.amazon.com/iam/home#

© 2023, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

# Demo (Developer Policy)

aws

Services

Search

[Alt+S]

EC2

Identity and Access Management (IAM)

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Search IAM

Feedback

Language

Policies > Developer

Summary

Delete policy

Policy ARN: am:aws:iam::260528357873:policy/Developer

Description: For developer

Permissions | Policy usage | Tags | Policy versions | Access Advisor

Policy summary | {} JSON | Edit policy

Filter

Service	Access level	Resource	Request condition
Allow (2 of 371 services) Show remaining 369			
EC2	Full: Read, Tagging Limited: List, Write	All resources	aws:MultiFactorAuthPresent   Bool   true (If Exists)
STS	Limited: Write	All resources	aws:MultiFactorAuthPresent   Bool   true (If Exists)

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Services

Search

[Alt+S]

EC2

Identity and Access Management (IAM)

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Search IAM

Feedback

Language

Policies > Developer

Summary

Delete policy

Policy ARN: am:aws:iam::260528357873:policy/Developer

Description: For developer

Permissions | Policy usage | Tags | Policy versions | Access Advisor

Policy summary | {} JSON | Edit policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:ExportImage",
9         "ec2:GetResourcePolicy",
10        "ec2:GetDefaultCreditSpecification",
11        "ec2:GetIpamResourceCidrs",
12        "ec2:GetIpamPoolCidrs",
13        "ec2:GetInstanceUefiData",
14        "ec2:DeleteTags",
15        "ec2:CreateKeyPair",
16        "ec2:GetEbsEncryptionByDefault",
17        "ec2:ExportClientVpnClientConfiguration",
18        "ec2:GetCapacityReservationUsage",
19        "ec2:DescribeCapacityReservations"
20      ]
21     }
22   ]
23 }
```

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Demo (Employee Policy)

aws

Services

Search

[Alt+S]

EC2

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Policies > Employee

Summary

Delete policy

Policy ARN: am:aws:iam::260528357873:policy/Employee

Description: For employee, read only

Permissions

Policy usage

Tags

Policy versions

Access Advisor

Policy summary

{ } JSON

Edit policy

Filter

Service	Access level	Resource	Request condition
EC2	Limited: Read	Multiple	aws:MultiFactorAuthPresent   Bool   true (If Exists)

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Services

Search

[Alt+S]

EC2

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Policies > Employee

Summary

Delete policy

Policy ARN: am:aws:iam::260528357873:policy/Employee

Description: For employee, read only

Permissions

Policy usage

Tags

Policy versions

Access Advisor

Policy summary

{ } JSON

Edit policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:GetPasswordData",
9         "ec2:GetLaunchTemplateData",
10        "ec2:GetInstanceUefiData",
11        "ec2:GetConsoleScreenshot",
12        "ec2:GetAssociatedEnclaveCertificateIamRoles",
13        "ec2:GetConsoleOutput"
14      ],
15      "Resource": [
16        "arn:aws:ec2:*:260528357873:instance/*",
17        "arn:aws:acm:*:260528357873:certificate/*"
18      ]
19    }
20  ]
21 }
```

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Demo (Roles)

aws

Services

Search

[Alt+S]

Global

Vi @ 2605-2835-7873

EC2

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity

IAM > Roles

Roles (9) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Refresh Delete Create role

Search

	Role name	Trusted entities	Last activity
<input type="checkbox"/>	<a href="#">AWSServiceRoleForElasticLoadBalancing</a>	AWS Service: elasticloadbalancing (Service-Linked Role)	19 days ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForOrganizations</a>	AWS Service: organizations (Service-Linked Role)	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForRDS</a>	AWS Service: rds (Service-Linked Role)	19 days ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForSSO</a>	AWS Service: sso (Service-Linked Role)	2 hours ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linked Role)	13 days ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service-Linked Role)	-
<input type="checkbox"/>	<a href="#">Developer</a>	Account: 260528357873	55 minutes ago
<input type="checkbox"/>	<a href="#">Employee</a>	Account: 260528357873	53 minutes ago
<input type="checkbox"/>	<a href="#">rds-monitoring-role</a>	AWS Service: monitoring.rds	20 days ago

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences



# Demo (Switch Roles- Developer)

← → ↻ sign-in.aws.amazon.com/switchrole?src=nav&redirect\_uri=https%3A%2F%2Fus-east-1.console.aws.amazon.com%2Fiam%2Fhome%23%2Fpolicies%2Farn%3Aaws%3Aiam%3A%3A260... ⌵ ☆ 🌐 ⓘ Update ⓘ

**aws**

### Switch Role

Allows management of resources across Amazon Web Services accounts using a single user ID and password. You can switch roles after an Amazon Web Services administrator has configured a role and given you the account and role details. [Learn more.](#)

Account\*  ⓘ

Role\*  ⓘ

Display Name  ⓘ

Color 🟡 🟠 🟢 🟣 🟤 ⬛

\*Required Cancel Switch Role

**aws** Services 🔍 Search [Alt+S] Global Vi @ 2605-2835-7873

**EC2**

## Identity and Access Management (IAM)

Search IAM

- Dashboard
- Access management
  - User groups
  - Users
  - Roles**
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analizers
  - Settings
  - Credential report
  - Organization activity

### Developer

For Dev

Delete

#### Summary

Edit

Creation date March 28, 2023, 15:53 (UTC-05:00)	ARN <a href="#">arn:aws:iam::260528357873:role/Developer</a>	Link to switch roles in console <a href="#">https://signin.aws.amazon.com/switchrole?roleName=Developer&amp;account=260528357873</a>
Last activity <span>🟢 56 minutes ago</span>	Maximum session duration 1 hour	

**Permissions** Trust relationships Tags Access Advisor Revoke sessions

#### Permissions policies (2) Info

You can attach up to 10 managed policies.

🔍 Filter policies by property or policy name and press enter.

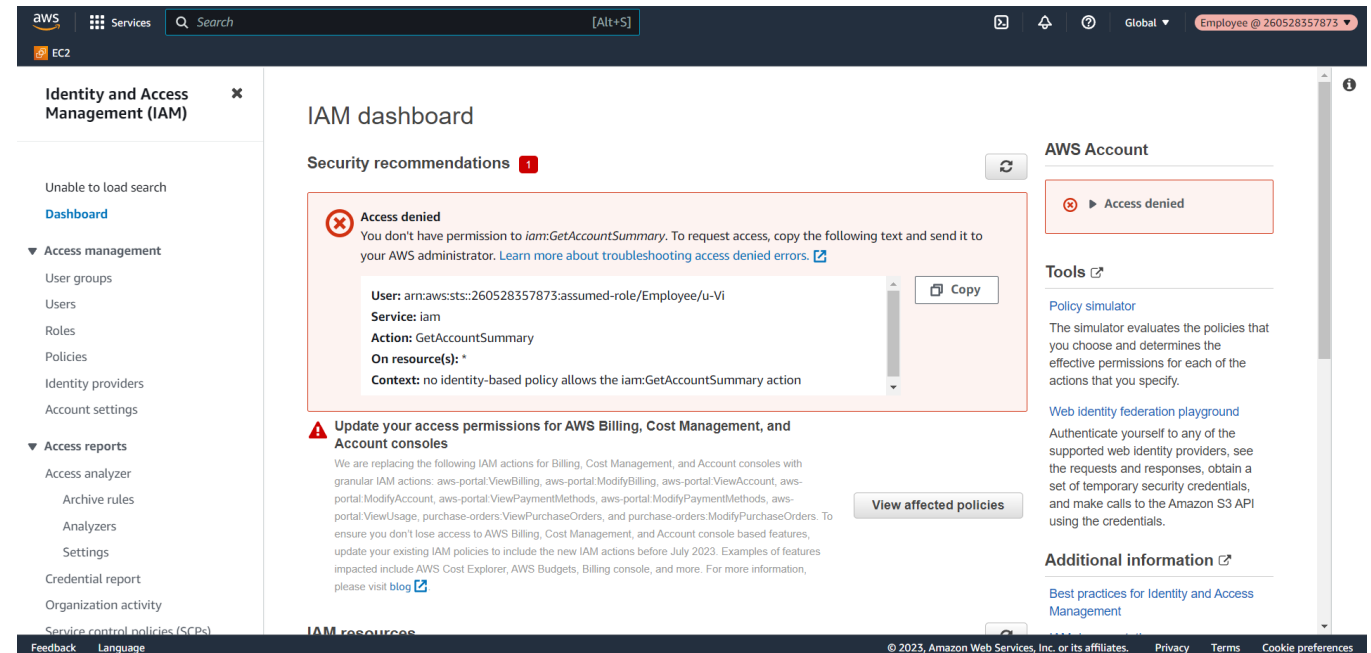
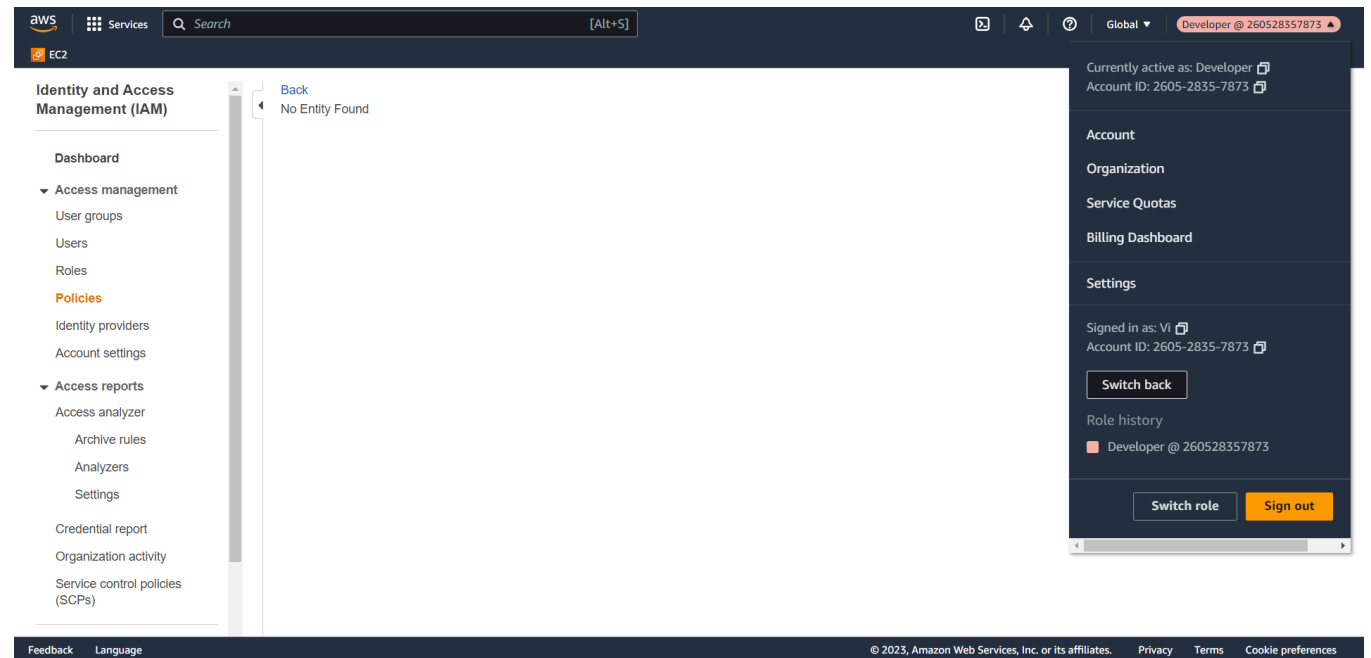
<input type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Description
<input type="checkbox"/>	<a href="#">Developer</a>	Customer managed	For developer
<input type="checkbox"/>	<a href="#">Employee</a>	Customer managed	For employee, read only

🔄 Simulate Remove Add permissions ▼

1

[https://us-east-1.console.aws.amazon.com/iamv2/home#](#) © 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

# Demo (Switch Roles- Employee)



# AWS Identity and Access Management Best Practices

- Use temporary credentials
- Require multi-factor authentication (MFA)
- Rotate access keys regularly for use cases that require long-term credentials
- Safeguard your root user credentials and don't use them for everyday tasks
- Grant least privilege
- Use IAM Access Analyzer
- Set permissions guardrails across multiple accounts
- Delegate permissions management within an account by using permissions boundaries

# Bibliography

- *AWS Identity and Access Management (IAM) Best Practices - Amazon Web Services*. (n.d.). Amazon Web Services, Inc. Retrieved March 29, 2023, from <https://aws.amazon.com/iam/resources/best-practices/>

**Thank you.  
Questions?**

