

Using Role Based Access Control (RBAC) with AWS IAM

The purpose of this assignment is to use [AWS IAM](#) to create users and assign the appropriate policies / permissions for them to be able to complete their job responsibilities. There is no charge for creating a user and adding permissions. However, to test some of the permissions you may need to create some AWS resources. ***If you are working on this assignment over an extended period, be sure to power-off / shutdown AWS resources (i.e., VMs) that have actual charges to ensure you reduce the cloud charges.***

The following individuals have been hired by Skynet. You must provide the user accounts with appropriate access to perform their job responsibilities.

Employee Name	Username	Job Title	Job Responsibilities
Tom Brady	tbrady	Cloud Administrator	Responsible for IAM and overall management of the cloud platform. Requires all AWS permissions. Sometimes referred to as Root or God Mode.
Geno Smith	gsmith	Virtual Machine Administrator	Requires the ability to create, manage, and destroy virtual machines
Kenny Pickett	kpickett	Cloud FinOps Analyst	Responsible for cloud billing setup, cost management, and cost projections.
Russell Wilson	rwilson	Backup Operator	Responsible for backup and restores of AWS resources
Steve Young	syoung	Internal Auditor	Requires the ability to audit / view all AWS resources, such as IAM, VMs, DBs, etc.

Before you start creating user accounts, you will create AWS groups. The group names will reflect the job titles, and the policies / permissions for each group will align to the job responsibilities.

1. (10 points) Within AWS IAM, create the following groups shown in the table below and assign the appropriate policies / permissions based on job responsibilities. Populate the table below with the policies you assigned to each group and **provide screenshots to support your work.**

Using Role Based Access Control (RBAC) with AWS IAM

This screenshot shows the AWS IAM console interface for the 'Admin' user group. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Organization activity. The main content area displays the 'Admin' user group details, including a summary with the user group name 'Admin', creation time, and ARN. Below this, the 'Permissions' tab is active, showing a table of permissions policies. The table lists one policy named 'AdministratorAccess' of type 'AWS managed - job function', which is attached to 1 entity. The interface includes buttons for 'Delete', 'Edit', 'Simulate', 'Remove', and 'Add permissions'.

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

▼ Access reports

Access Analyzer

Resource analysis [New](#)

Unused access

Analyzer settings

Credential report

Organization activity

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This screenshot shows the AWS IAM console interface for the 'VMAdmins' user group. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Organization activity. The main content area displays the 'VMAdmins' user group details, including a summary with the user group name 'VMAdmins', creation time, and ARN. Below this, the 'Permissions' tab is active, showing a table of permissions policies. The table lists one policy named 'AmazonEC2FullAccess' of type 'AWS managed', which is attached to 2 entities. The interface includes buttons for 'Delete', 'Edit', 'Simulate', 'Remove', and 'Add permissions'.

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

▼ Access reports

Access Analyzer

Resource analysis [New](#)

Unused access

Analyzer settings

Credential report

Organization activity

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Using Role Based Access Control (RBAC) with AWS IAM

The screenshot shows the AWS IAM console interface for the 'FinOps' user group. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Organization activity. The main content area displays the 'Permissions' tab for the 'FinOps' user group. The 'Summary' section shows the user group name 'FinOps', creation time, and ARN. Below this, the 'Permissions policies' section lists three attached policies: 'AWSBillingReadOnlyAccess', 'AWSBudgetsReadOnlyAccess', and 'Billing'. Each policy is associated with 'AWS managed' or 'AWS managed - job function' type and has one attached entity.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

Access reports

Access Analyzer

Resource analysis [New](#)

Unused access

Analyzer settings

Credential report

Organization activity

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

FinOps Info

Summary

User group name: FinOps

Creation time: [Redacted]

ARN: [Redacted]

Permissions

Users (1)

Permissions policies (3) Info

You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
AWSBillingReadOnlyAccess	AWS managed	1
AWSBudgetsReadOnlyAccess	AWS managed	1
Billing	AWS managed - job function	1

The screenshot shows the AWS IAM console interface for the 'BackupOps' user group. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Organization activity. The main content area displays the 'Permissions' tab for the 'BackupOps' user group. The 'Summary' section shows the user group name 'BackupOps', creation time, and ARN. Below this, the 'Permissions policies' section lists three attached policies: 'AmazonEC2ReadOnlyAccess', 'AmazonS3FullAccess', and 'AWSBackupFullAccess'. Each policy is associated with 'AWS managed' type and has one attached entity.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

Access reports

Access Analyzer

Resource analysis [New](#)

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies [New](#)

IAM Identity Center

AWS Organizations

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

BackupOps Info

Summary

User group name: BackupOps

Creation time: [Redacted]

ARN: [Redacted]

Permissions

Users (1)

Permissions policies (3) Info

You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
AmazonEC2ReadOnlyAccess	AWS managed	1
AmazonS3FullAccess	AWS managed	1
AWSBackupFullAccess	AWS managed	1

The screenshot shows the AWS IAM console interface for the 'Auditor' user group. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Organization activity. The main content area displays the 'Permissions' tab for the 'Auditor' user group. The 'Summary' section shows the user group name 'Auditor', creation time, and ARN. Below this, the 'Permissions policies' section lists three attached policies: 'IAMReadOnlyAccess', 'ReadOnlyAccess', and 'SecurityAudit'. Each policy is associated with 'AWS managed' or 'AWS managed - job function' type and has one attached entity.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

Access reports

Access Analyzer

Resource analysis [New](#)

Unused access

Analyzer settings

Credential report

Organization activity

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Auditor Info

Summary

User group name: Auditor

Creation time: [Redacted]

ARN: [Redacted]

Permissions

Users (1)

Permissions policies (3) Info

You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
IAMReadOnlyAccess	AWS managed	1
ReadOnlyAccess	AWS managed - job function	1
SecurityAudit	AWS managed - job function	1

Using Role Based Access Control (RBAC) with AWS IAM

Group Name	Policies / Permissions
Admins	AdministratorAccess
VMAdmins	AmazonEC2FullAccess
FinOps	Billing, AWSBudgetsReadOnlyAccess, and AWSBillingReadOnlyAccess
BackupOps	AWSBackupFullAccess, AmazonS3FullAccess, and AmazonEC2ReadOnlyAccess
Auditor	SecurityAudit, ReadOnlyAccess, and IAMReadOnlyAccess

Your group creation should look like the screenshot below:

The screenshot shows the AWS IAM console 'User groups' page. The main content area lists five user groups, each with 1 user and 'Defined' permissions. The left sidebar shows the navigation menu with 'Access management' expanded, highlighting 'User groups'.

Group name	Users	Permissions
Admins	1	Defined
Auditor	1	Defined
BackupOps	1	Defined
FinOps	1	Defined
VMAdmins	1	Defined

Note: Be sure you are creating the groups & users using IAM and not Identity Center

- (5 points) Next, you will create the users shown in the table on the previous page. Provide screenshots for provisioning the user and attaching the appropriate group. Be sure to grant each user console access and to document the console sign-in URL (shown in the screenshots below).

Using Role Based Access Control (RBAC) with AWS IAM

User details

User name

gsmith

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

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can manage console access for a person in a central location.

☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys.

IAM > Users > Create 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.

Console sign-in details

Console sign-in URI

User name

Console password

IAM > Users > tbrady

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

tbrady Info

Summary

ARN

Created

Console access

Enabled without MFA

Last console sign-in

Today

Access key 1

Create access key

Permissions

Groups (1)

Tags (1)

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.

Group name

Admin

Attached policies

AdministratorAccess

IAM > Users > gsmith

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

gsmith Info

Summary

ARN

Created

Console access

Enabled without MFA

Last console sign-in

Today

Access key 1

Create access key

Permissions

Groups (1)

Tags (1)

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.

Group name

VMAdmins

Attached policies

AmazonEC2FullAccess

Using Role Based Access Control (RBAC) with AWS IAM

This screenshot shows the AWS IAM console interface for user **kpickett**. The left sidebar contains navigation links for Identity and Access Management (IAM), including Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report), and Organization activity. The main content area displays the user's summary, including ARN, Created date, Console access status (Enabled without MFA), and Last console sign-in (Today). Below the summary, there are tabs for Permissions, Groups (1), Tags (1), Security credentials, and Last Accessed. The 'User groups membership' section shows a list of groups the user belongs to, with a 'Remove' button and an 'Add user to groups' button. The footer includes a CloudShell icon, a Feedback link, and copyright information for Amazon Web Services.

Identity and Access Management (IAM)

kpickett Info

Summary

ARN [REDACTED]

Created [REDACTED]

Console access **Enabled without MFA**

Last console sign-in **Today**

Access key 1 [Create access key](#)

Permissions Groups (1) Tags (1) 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

FinOps Billing, ViewOnlyAccess and 2 more

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This screenshot shows the AWS IAM console interface for user **rwilson**. The layout is identical to the first screenshot, showing the user's summary, tabs for Permissions, Groups (1), Tags (1), Security credentials, and Last Accessed. The 'User groups membership' section shows that the user is a member of **BackupOps**, **AmazonEC2FullAccess**, **AmazonS3FullAccess**, and 1 more group. The footer includes a CloudShell icon, a Feedback link, and copyright information for Amazon Web Services.

Identity and Access Management (IAM)

rwilson Info

Summary

ARN [REDACTED]

Created [REDACTED]

Console access **Enabled without MFA**

Last console sign-in **Today**

Access key 1 [Create access key](#)

Permissions Groups (1) Tags (1) 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

BackupOps AmazonEC2FullAccess, AmazonS3FullAccess and 1 more

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This screenshot shows the AWS IAM console interface for user **syoung**. The layout is identical to the previous screenshots, showing the user's summary, tabs for Permissions, Groups (1), Tags (1), Security credentials, and Last Accessed. The 'User groups membership' section shows that the user is a member of **ReadOnlyAccess**, **IAMReadOnlyAccess**, and 1 more group. The footer includes a CloudShell icon, a Feedback link, and copyright information for Amazon Web Services.

Identity and Access Management (IAM)

syoung Info

Summary

ARN [REDACTED]

Created [REDACTED]

Console access **Enabled without MFA**

Last console sign-in **Today**

Access key 1 [Create access key](#)

Permissions Groups (1) Tags (1) 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

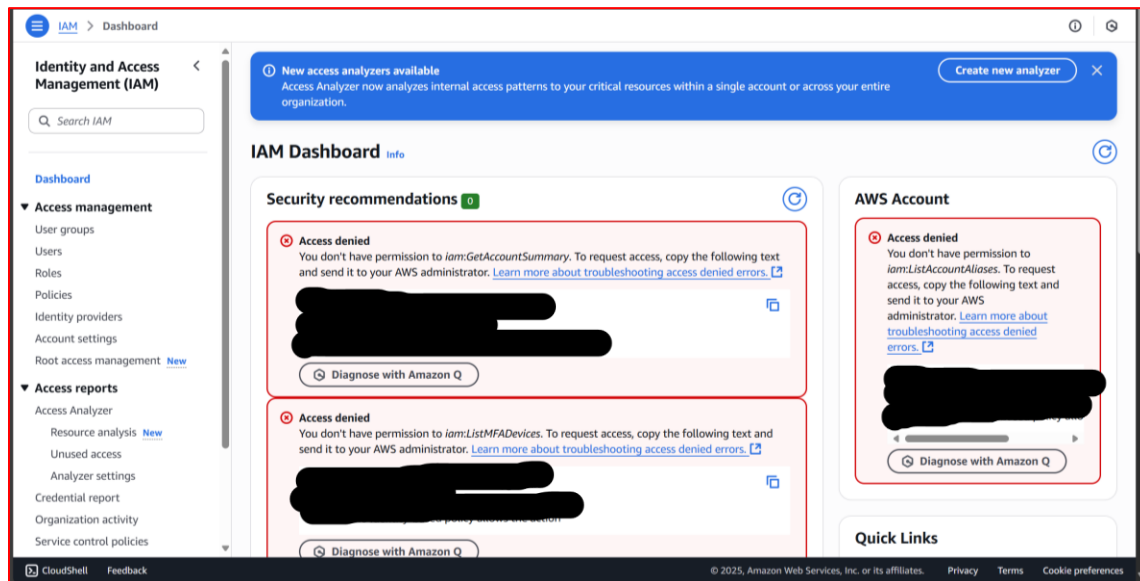
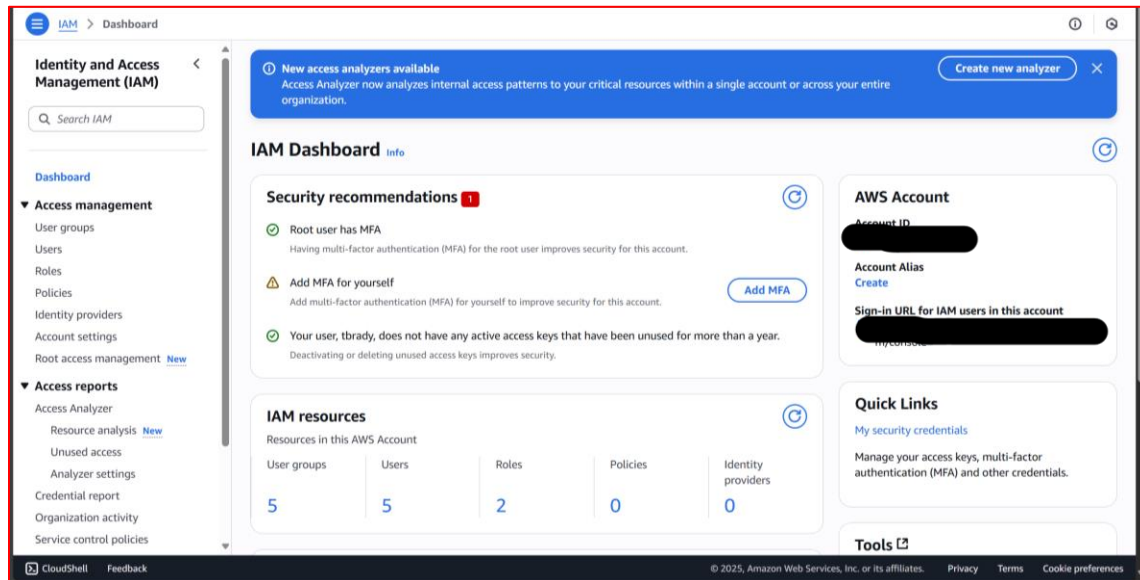
Auditor ReadOnlyAccess, IAMReadOnlyAccess and 1 more

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Using Role Based Access Control (RBAC) with AWS IAM

3. (40 points) Using console sign-in URL login and each user account verifies RBAC has been setup appropriately for each employee. **Tip: Use different browsers and/or incognito mode so that you can still have access to the AWS console with your root account to potentially adjust settings.**



Using Role Based Access Control (RBAC) with AWS IAM

This screenshot shows the AWS IAM Dashboard with a focus on security recommendations. The left sidebar contains navigation links for Identity and Access Management (IAM), including Dashboard, Access management, and Access reports. The main content area features a blue banner for 'New access analyzers available'. Below this, the 'IAM Dashboard' section displays 'Security recommendations' with two 'Access denied' alerts. The first alert states: 'You don't have permission to iam:GetAccountSummary. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.' The second alert states: '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.' Both alerts include a 'Diagnose with Amazon Q' button. To the right, the 'AWS Account' section shows another 'Access denied' alert for 'iam:ListAccountAliases' with a similar 'Diagnose with Amazon Q' button. A 'Quick Links' section is visible at the bottom right.

This screenshot is identical to the one above, showing the AWS IAM Dashboard with security recommendations and access denied errors. The layout and content are the same, highlighting the 'Access denied' alerts for 'iam:GetAccountSummary', 'iam:ListMFADevices', and 'iam:ListAccountAliases'.

This screenshot shows the AWS IAM Dashboard with a focus on security recommendations and IAM resources. The left sidebar is the same. The main content area features a blue banner for 'New access analyzers available'. Below this, the 'IAM Dashboard' section displays 'Security recommendations' with three items: 'Root user has MFA', 'Add MFA for yourself', and 'Your user, syoung, does not have any active access keys that have been unused for more than a year.' Each item has a corresponding button ('Add MFA' for the second item). Below the recommendations, the 'IAM resources' section shows a table of resources in the AWS Account:

User groups	Users	Roles	Policies	Identity providers
5	5	2	0	0

To the right, the 'AWS Account' section shows 'Account ID', 'Account Alias', and a 'Sign in UI for IAM users in this account' link. A 'Quick Links' section is visible at the bottom right.


Using Role Based Access Control (RBAC) with AWS IAM

Populate the table below with either **(YES/NO)** with “YES” meaning the user has access to the service / perform the function or “NO” meaning the user does not have access. **Below, the table provides screenshots to support your answers.**


User	Create EC2 (YES/NO)	View EC2	Create IAM User	View IAM Users	Create S3 Bucket	View S3 Buckets	View Billing	Modify Payment Preference
tbrady	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
gsmith	Yes	Yes	No	No	No	No	No	No
kpickett	No	No	No	No	No	No	Yes	Yes
rwilson	No	Yes	No	No	Yes	Yes	No	No
syoung	No	Yes	No	Yes	No	Yes	Yes	No

Example screenshots showing denied access:

AWS Billing Dashboard

 **You Need Permissions**

You don't have permission to access billing information for this account. Contact your AWS administrator if you need help. If you are an AWS administrator, you can provide permissions for your users or groups by making sure that (1) [this account allows IAM and federated users to access billing information](#) and (2) [you have the required IAM permissions](#).

 **Access denied**

You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)


User: [REDACTED]

Service: iam

Action: GetAccountSummary

On resource(s): *

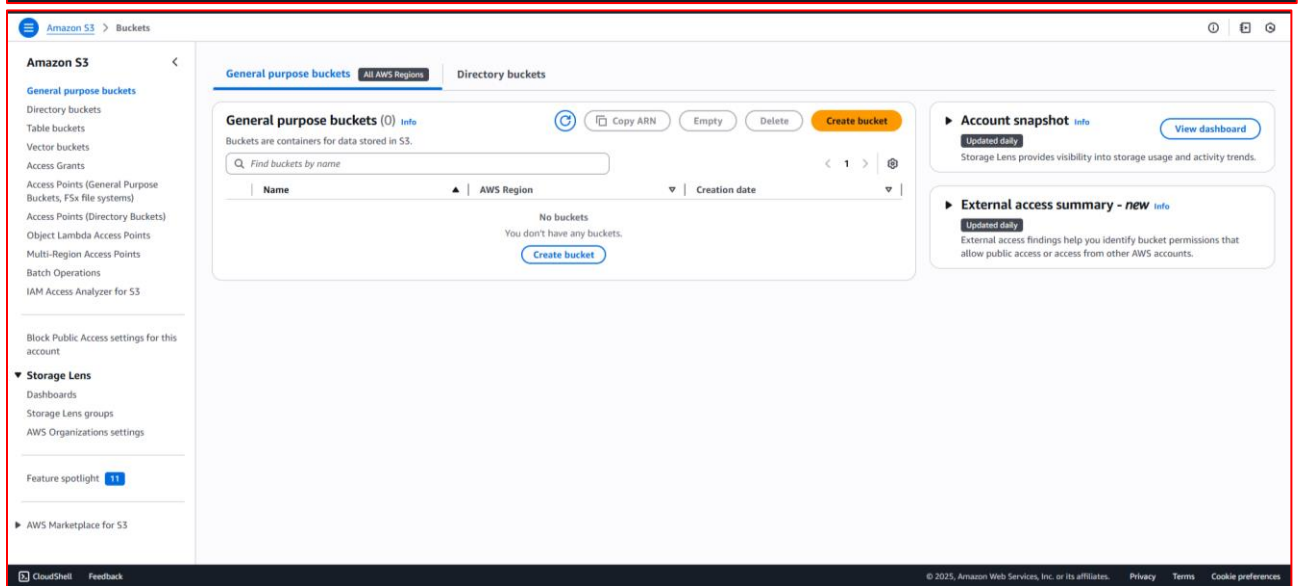
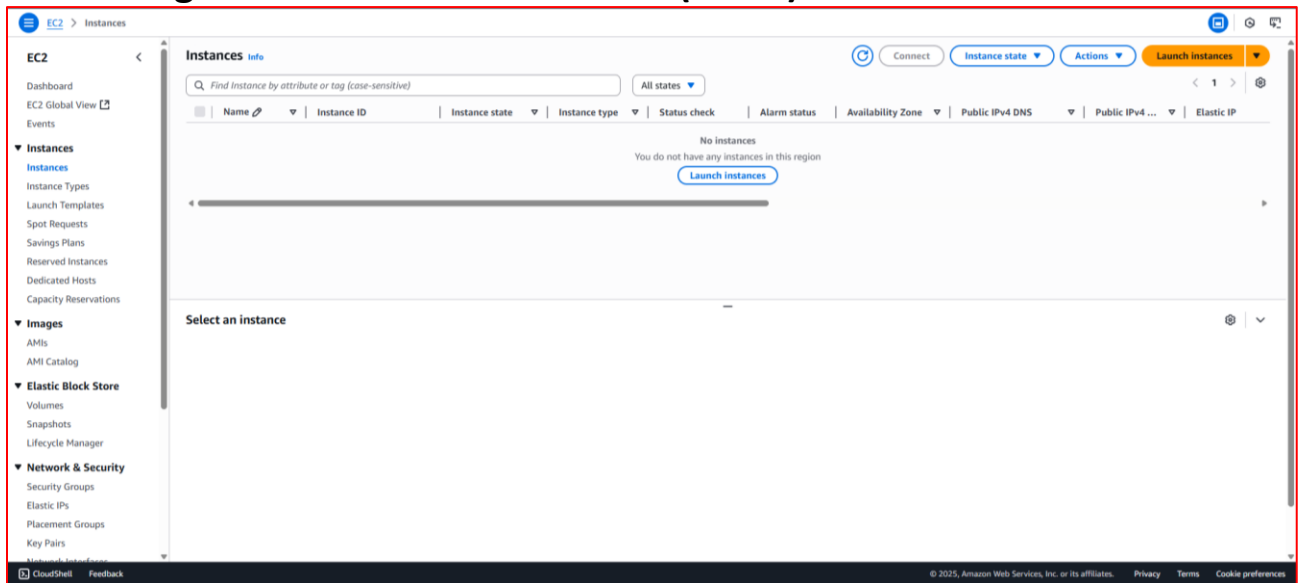
Context: no identity-based policy allows the iam:GetAccountSummary action

 Copy

4. (5 points) When completed with this assignment, delete all billable resources. Note: AWS IAM resources are not billable!

Provide screenshots showing that this is completed.

Using Role Based Access Control (RBAC) with AWS IAM



Using Role Based Access Control (RBAC) with AWS IAM

The screenshot shows the AWS Billing and Cost Management console. The left sidebar contains navigation links for Billing and Cost Management, Cost and Usage Analysis, and Cost Organization. The main content area displays the 'Bills' page for 'Amazon Web Services, Inc. charges by service'. It includes a table with columns for Description, Usage Quantity, and Amount in USD. The table lists charges for Data Transfer, Elastic Compute Cloud, and Virtual Private Cloud, all with a total amount of USD 0.00. A 'Total tax' row also shows USD 0.00. A footer note states that usage and recurring charges for this statement period will be charged on the next billing date.

Billing and Cost Management > Bills

Credits cover your free plan costs. Your free access to AWS services will end when your free plan period expires or when you have depleted all credits.

Starting November 1st the 'Download all to CSV' button will no longer be available on the Bills page. If you have already set up the delivery of the eCSV report, you can get this report from the S3 bucket configured during set up. To set up additional reports, please visit the [Data Exports](#) page.

Charges by service | Charges by account | Invoices | Savings | Taxes by service

Amazon Web Services, Inc. charges by service [Info](#) [Expand all](#)

Total active services: **3** Total pre-tax service charges in USD: **USD 0.00**

Filter by service name or region name

Description	Usage Quantity	Amount in USD
Data Transfer		USD 0.00
Elastic Compute Cloud		USD 0.00
Virtual Private Cloud		USD 0.00
Total tax		USD 0.00

Usage and recurring charges for this statement period will be charged on your next billing date. Estimated charges shown on this page, or shown on any notifications that we send to you, may differ from your actual charges for this statement period. This is because estimated charges presented on this page do not include usage charges accrued during this statement period after the date you view this page. Similarly, information about estimated charges sent to you in a notification do not include usage charges accrued during this statement period after the date we send you the notification. One-time fees and subscription charges are assessed separately from usage and recurring charges, on the date that they occur. The charges on this page exclude taxes, unless it is listed as a separate line item. To access your tax information, contact your AWS Organization's management owner.

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

The screenshot shows the AWS IAM Dashboard. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and IAM Identity Center. The main content area displays the 'IAM Dashboard' with sections for Security recommendations, IAM resources, and What's new. The Security recommendations section lists two items: 'Root user has MFA' and 'Root user has no active access keys'. The IAM resources section shows a table with columns for User groups, Users, Roles, Policies, and Identity providers. The What's new section lists updates for features in IAM.

IAM Dashboard [Info](#)

Security recommendations [Info](#)

- Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.
- Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources [Info](#)

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
5	5	3	0	0

What's new [View all](#)

Updates for features in IAM

- Amazon Bedrock introduces API keys for streamlined development. 3 months ago
- AWS Service Reference Information now supports annotations for service actions. 3 months ago
- AWS expands resource control policies (RCPs) support to two additional services. 3 months ago
- AWS IAM now enforces MFA for root users across all account types. 4 months ago

[more](#)

AWS Account

[Sign in URL for IAM users in this account](#)

Quick Links

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

Tools

- [Policy simulator](#)
- The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Additional information

- [Security best practices in IAM](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)