

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

The screenshot shows the AWS IAM console for the 'Admin' user group. The 'Permissions' tab is selected. One policy, 'AdministratorAccess', is listed under 'Attached entities'. This policy is an AWS managed job function.

Attached entities	Type
AdministratorAccess	AWS managed - job function

The screenshot shows the AWS IAM console for the 'VMAdmins' user group. The 'Permissions' tab is selected. One policy, 'AmazonEC2FullAccess', is listed under 'Attached entities'. This policy is an AWS managed policy.

Attached entities	Type
AmazonEC2FullAccess	AWS managed

Using Role Based Access Control (RBAC) with AWS IAM

The image displays three separate screenshots of the AWS IAM User Groups interface, each showing a different user group configuration. Each screenshot includes a sidebar with navigation links for IAM, User groups, and various reports.

Screenshot 1: FinOps

Summary: User group name: FinOps, Creation time: [REDACTED], ARN: [REDACTED].

Permissions: Permissions tab selected. Permissions policies attached:

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

Screenshot 2: BackupOps

Summary: User group name: BackupOps, ARN: [REDACTED].

Permissions: Permissions tab selected. Permissions policies attached:

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

Screenshot 3: Auditor

Summary: User group name: Auditor, Creation time: [REDACTED], ARN: [REDACTED].

Permissions: Permissions tab selected. Permissions policies attached:

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
VMAadmins	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 User Groups page. At the top, there is a search bar labeled "Search". Below it is a table with columns: "Group name", "Users", and "Permissions". The table contains five rows, each representing a user group:

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

At the bottom right of the table, there are buttons for "Delete" and "Create group". On the left side of the page, there is a sidebar with navigation links for Identity and Access Management (IAM), Access management, Access reports, and IAM Identity Center.

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

2. (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

The screenshot shows the "Create user" wizard in the AWS IAM console. Step 1: "Specify user details" shows a user name "gsmith" and a checked checkbox for "Provide user access to the AWS Management Console - optional". Step 2: "Set permissions" is shown. Step 3: "Review and create". Step 4: "Retrieve password". A "Console sign-in details" section on the right shows a redacted ARN, a user name "gsmith", and a console password.

The screenshot shows the "tbrady" user profile page. The "Summary" section shows the ARN, which is redacted, and the user was created today. Under "Permissions", there is one group ("Groups (1)") assigned, which is "Admin". Under "Attached policies", it lists "AdministratorAccess". An "Access key 1" section shows a redacted access key and a "Create access key" button. The "User groups membership" section shows the user is a member of the "Admin" group.

The screenshot shows the "gsmith" user profile page. The "Summary" section shows the ARN, which is redacted, and the user was created today. Under "Permissions", there is one group ("Groups (1)") assigned, which is "VMAdmins". Under "Attached policies", it lists "AmazonEC2FullAccess". An "Access key 1" section shows a redacted access key and a "Create access key" button. The "User groups membership" section shows the user is a member of the "VMAdmins" group.

Using Role Based Access Control (RBAC) with AWS IAM

The image displays three separate screenshots of the AWS IAM User Details page, each showing the configuration for a different user: kpickett, rwilson, and syoung. Each screenshot includes a sidebar with navigation links for IAM, Users, and various management and reporting tools.

kpickett (User ID: kpickett)

- 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:** Attached policies: Billing, ViewOnlyAccess and 2 more.

rwilson (User ID: rwilson)

- 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:** Attached policies: AmazonEC2FullAccess, AmazonS3FullAccess and 1 more.

syoung (User ID: syoung)

- 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:** Attached policies: ReadOnlyAccess, IAMReadOnlyAccess and 1 more.

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.**

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists 'Identity and Access Management (IAM)' with options like 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management'. Below this is 'Access reports' with 'Access Analyzer', 'Resource analysis', 'Unused access', 'Analyzer settings', 'Credential report', 'Organization activity', and 'Service control policies'. At the bottom of the sidebar are 'CloudShell' and 'Feedback' buttons. The main area is titled 'IAM Dashboard' and contains a 'Security recommendations' section with three items: 'Root user has MFA' (green), 'Add MFA for yourself' (yellow), and 'Your user, tbrady, does not have any active access keys that have been unused for more than a year.' (green). It also features an 'AWS Account' summary with 'Account ID' (redacted), 'Account Alias' (Create), and 'Sign-In URL for IAM users in this account' (redacted). A 'Quick Links' section for 'My security credentials' is shown, along with a 'Tools' section. The bottom right corner includes copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

This screenshot is identical to the one above, but it highlights two specific error messages in the 'Security recommendations' section. Both messages are red circles with a 'D' icon and the text 'Access denied'. The first message 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 message 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 messages include a 'Diagnose with Amazon Q' button at the bottom. The rest of the interface is the same as the first screenshot.

Using Role Based Access Control (RBAC) with AWS IAM

The screenshot shows the IAM Dashboard with a sidebar containing 'Identity and Access Management (IAM)' and 'AWS Account'. The main area displays 'Security recommendations' and 'AWS Account' sections. Both sections show 'Access denied' errors related to 'iam:ListAccountAliases' and 'iam>ListMFADevices'. Buttons for 'Diagnose with Amazon Q' are present.

This screenshot is identical to the one above, showing the same 'Access denied' errors for 'iam:ListAccountAliases' and 'iam>ListMFADevices'.

The screenshot shows the IAM Dashboard with a sidebar containing 'Identity and Access Management (IAM)' and 'AWS Account'. The main area displays 'Security recommendations' and 'AWS Account' sections. The 'Security recommendations' section includes items like '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'. The 'AWS Account' section shows 'Account ID' (redacted), 'Account Alias Create', and 'Sign-in URL for IAM users in this account' (redacted). A 'Quick Links' section for 'My security credentials' is also visible.

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:

The image contains two screenshots of the AWS Billing Dashboard. The top screenshot shows a general permission denial message: "You Need Permissions" with a red circle and an exclamation mark icon. It states: "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 [?].". The bottom screenshot shows a more detailed access denied message: "Access denied" with a red circle and an exclamation mark icon. It 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.](#) [?]" Below this, there is a scrollable text area showing the following details:
User: [REDACTED]
Service: iam
Action: GetAccountSummary
On resource(s): *
Context: no identity-based policy allows the iam:GetAccountSummary action
A "Copy" button is visible next to the scrollable text area.

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

The screenshot displays two separate AWS service dashboards, both highlighted with a red border, illustrating the use of Role Based Access Control (RBAC) with AWS IAM.

AWS EC2 Instances Dashboard:

- Left Sidebar:** Shows navigation links for EC2, Dashboard, EC2 Global View, Events, Instances (with sub-links for Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interface), CloudShell, and Feedback.
- Top Bar:** Includes search, filter (All states), and actions (Connect, Instance state, Actions, Launch Instances).
- Content Area:** Displays a message "No instances" and "You do not have any instances in this region". A prominent blue "Launch instances" button is at the bottom.

Amazon S3 Buckets Dashboard:

- Left Sidebar:** Shows navigation links for Amazon S3, General purpose buckets (with sub-links for Directory buckets, Table buckets, Vector buckets, Access Grants, Access Points (General Purpose Buckets, FSx file systems), Access Points (Directory Buckets), Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, and Block Public Access settings for this account), Storage Lens (Dashboards, Storage Lens groups, AWS Organizations settings), Feature spotlight (11 items), and AWS Marketplace for S3.
- Top Bar:** Includes search, filter (All AWS Regions), and actions (Copy ARN, Empty, Delete, Create bucket).
- Content Area:** Displays a message "No buckets" and "You don't have any buckets." A blue "Create bucket" button is at the bottom. To the right, there are sections for Account snapshot (Updated daily, Storage Lens provides visibility into storage usage and activity trends) and External access summary - new (Updated daily, External access findings help you identify bucket permissions that allow public access or access from other AWS accounts).

Using Role Based Access Control (RBAC) with AWS IAM

The screenshot shows the AWS Billing and Cost Management Bills page. The left sidebar includes links for Home, Getting Started, Dashboards, Billing and Payments, Cost and Usage Analysis, Cost Organization, and CloudShell. The main content area displays a table of charges by service, with a total of 3 active services. The table includes columns for Description, Usage Quantity, and Amount in USD. The total pre-tax service charges are listed as USD 0.00.

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 Organizations management owner.

The screenshot shows the AWS IAM Dashboard. The left sidebar includes links for Identity and Access Management (IAM), Dashboard, Access management, Access reports, and IAM Identity Center. The main content area displays security recommendations, IAM resources, and a What's new section. The IAM resources section shows 5 user groups, 5 users, 3 roles, 0 policies, and 0 identity providers. The What's new section lists recent changes such as the introduction of API keys for streamlined development and expanded resource control policies.

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

What's new

- 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