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.***

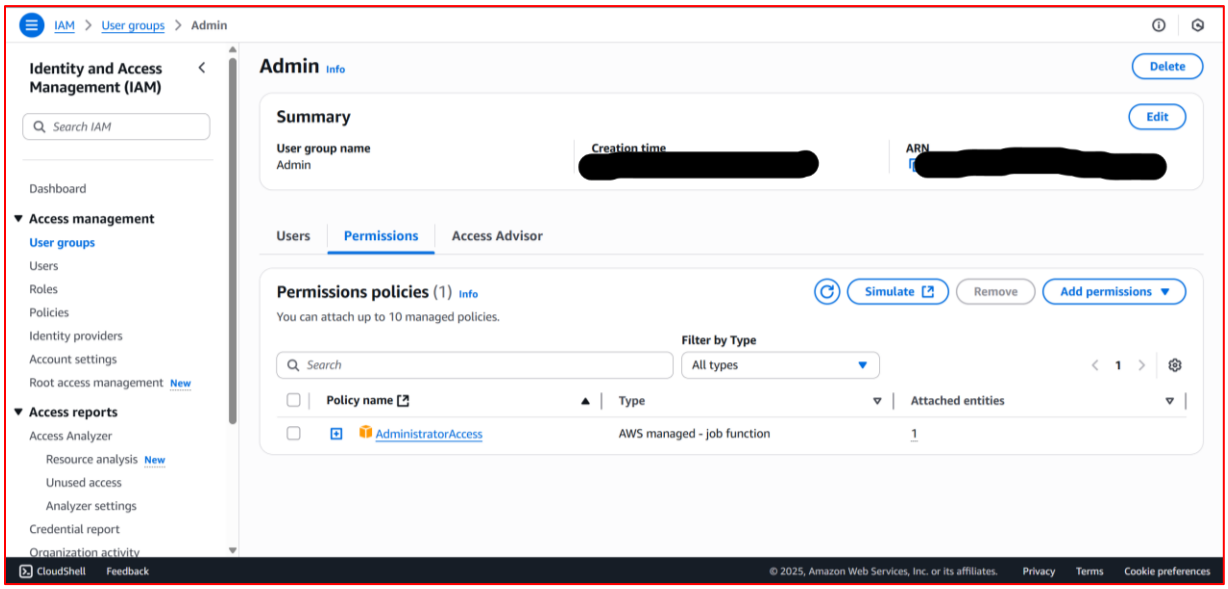
The following individuals have been hired by Skynet. You must provide the user accounts with appropriate access to perform their job responsibilities.

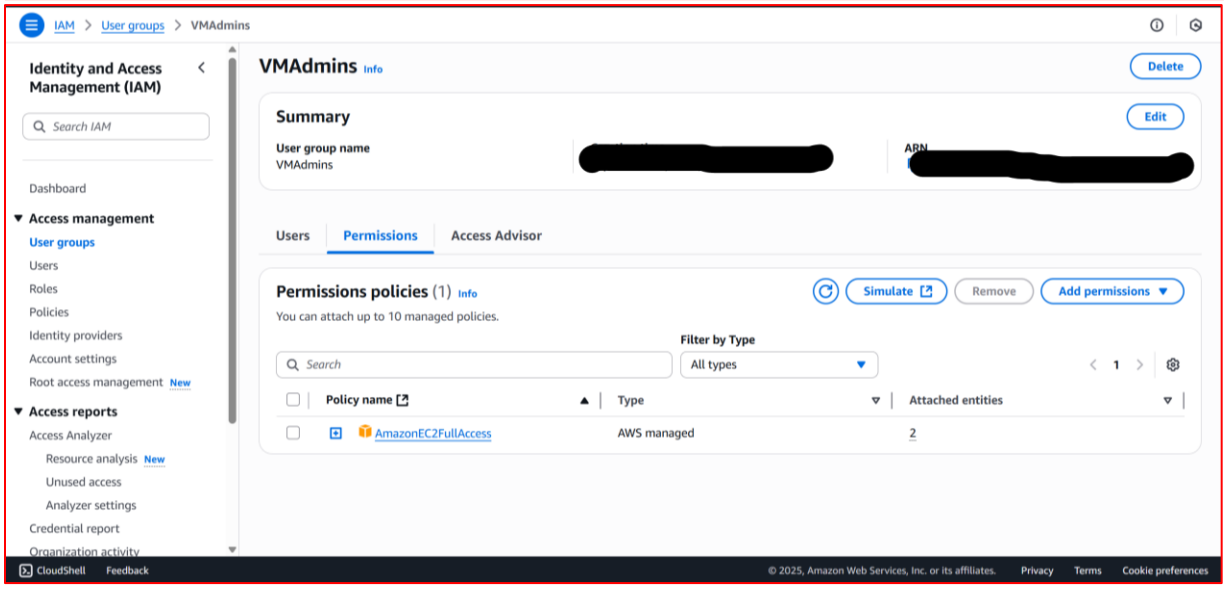
Employee Name	Username	Job Title	Job Responsibilities
Tom Brady	tbrady	Cloud Administrator	Responsible for IAM and overall management of the cloud platform. Requires all AWS permissions. Sometimes referred to as Root or God Mode.
Geno Smith	gsmith	Virtual Machine Administrator	Requires the ability to 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.

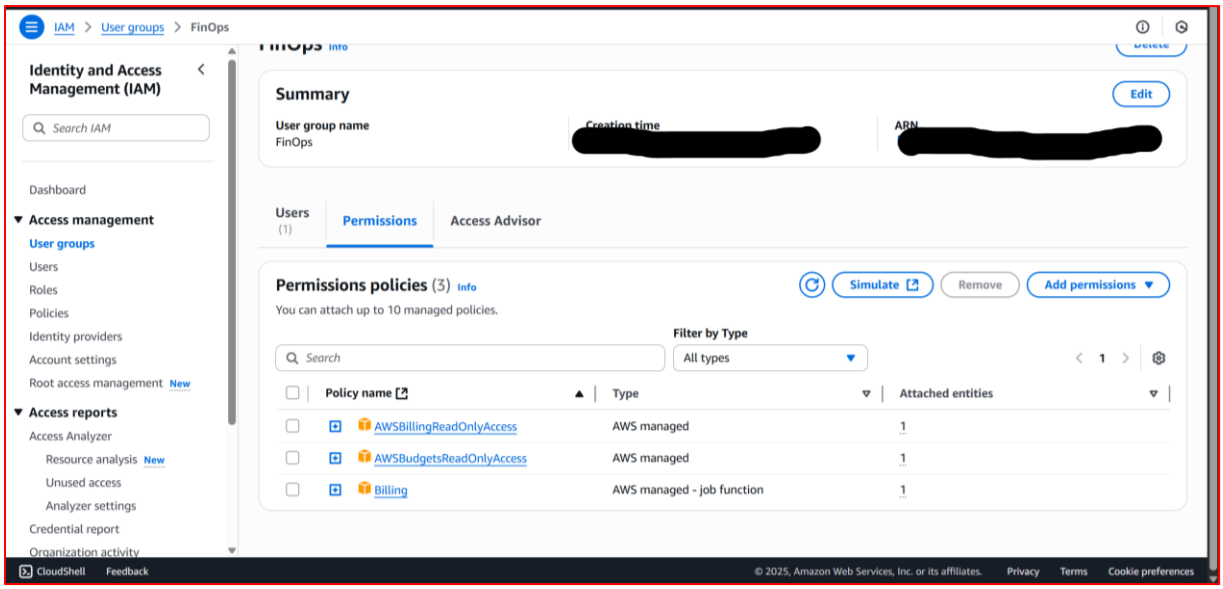
1. (10 points) Within AWS IAM, create the following groups shown in the table below and assign the appropriate policies / permissions based on job responsibilities. Populate the table below with the policies you assigned to each group and **provide screenshots to support your work**.

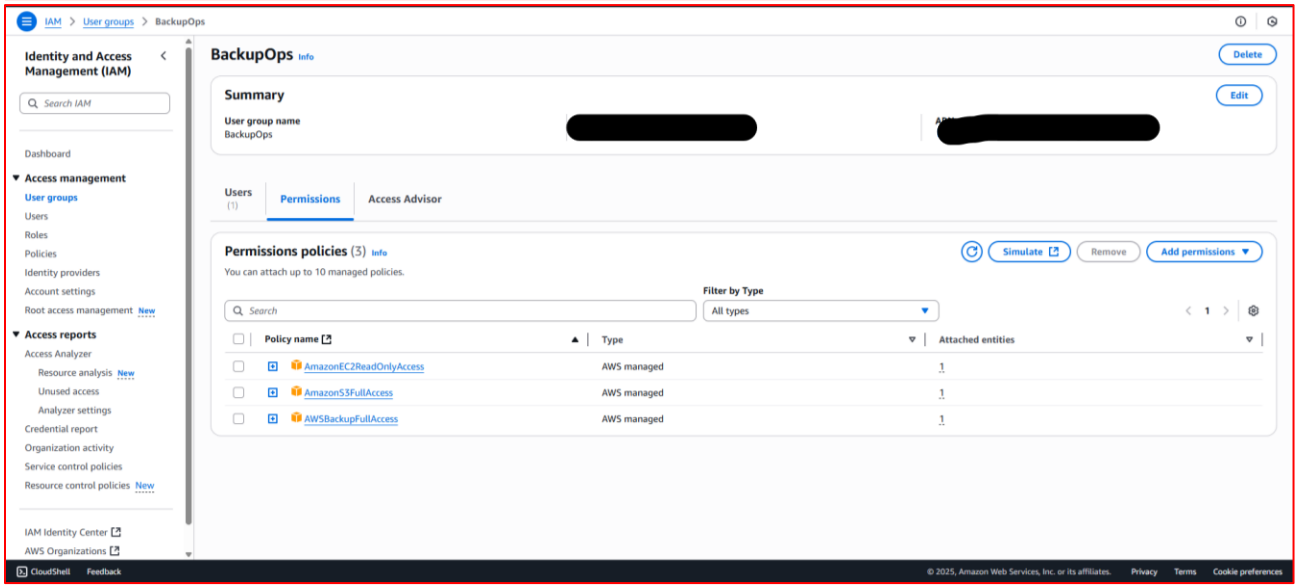
Using Role Based Access Control (RBAC) with AWS IAM

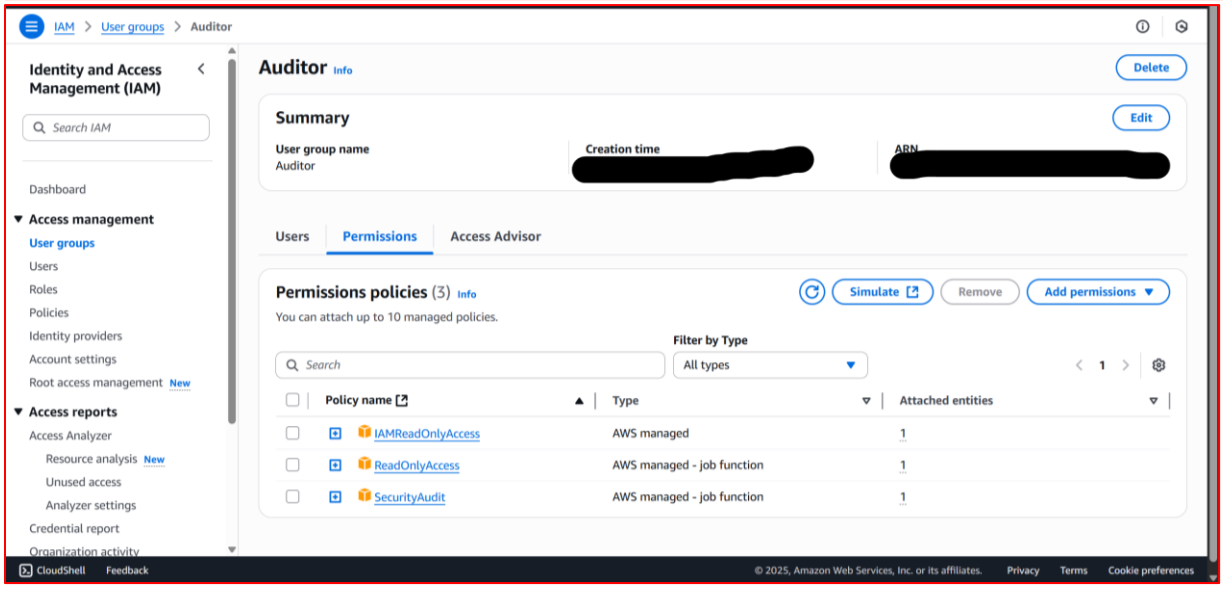




Using Role Based Access Control (RBAC) with AWS IAM



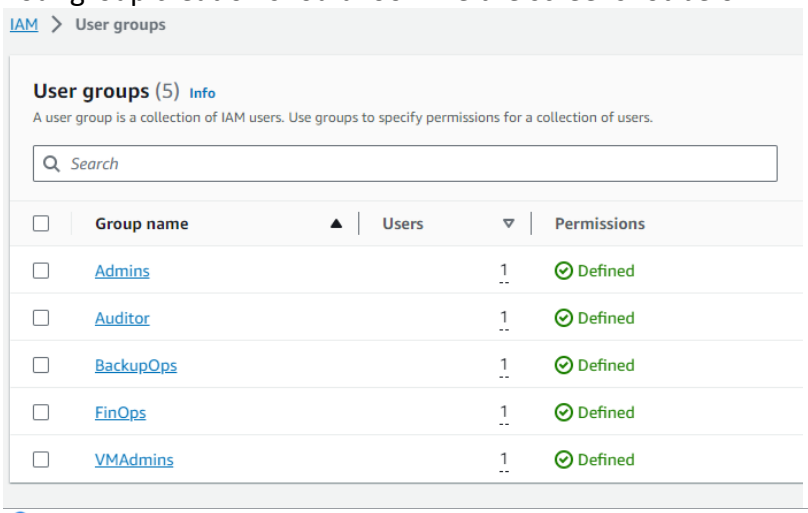


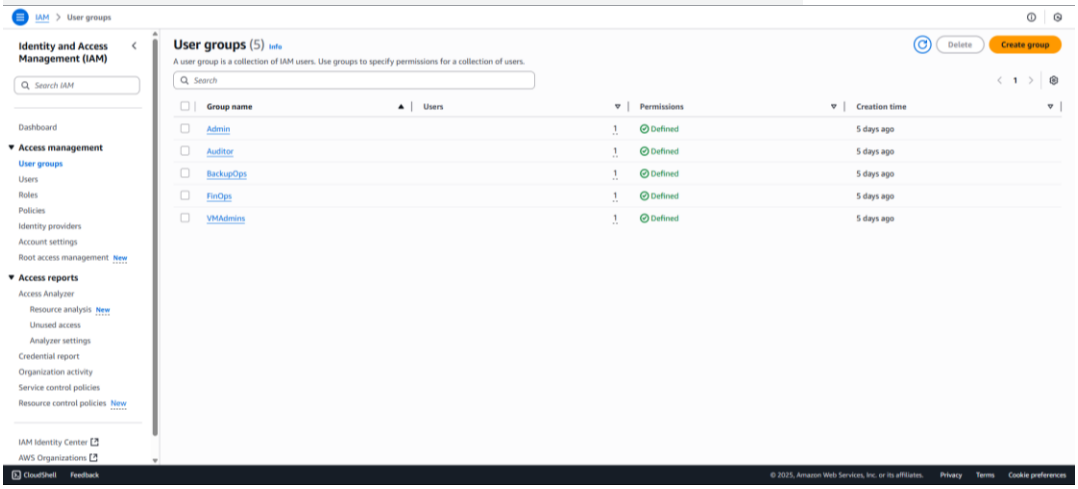


Using Role Based Access Control (RBAC) with AWS IAM

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:

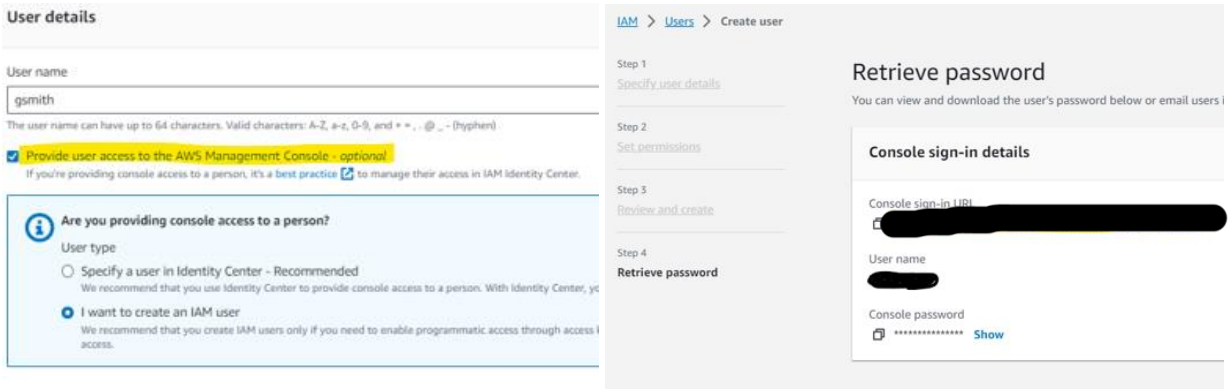


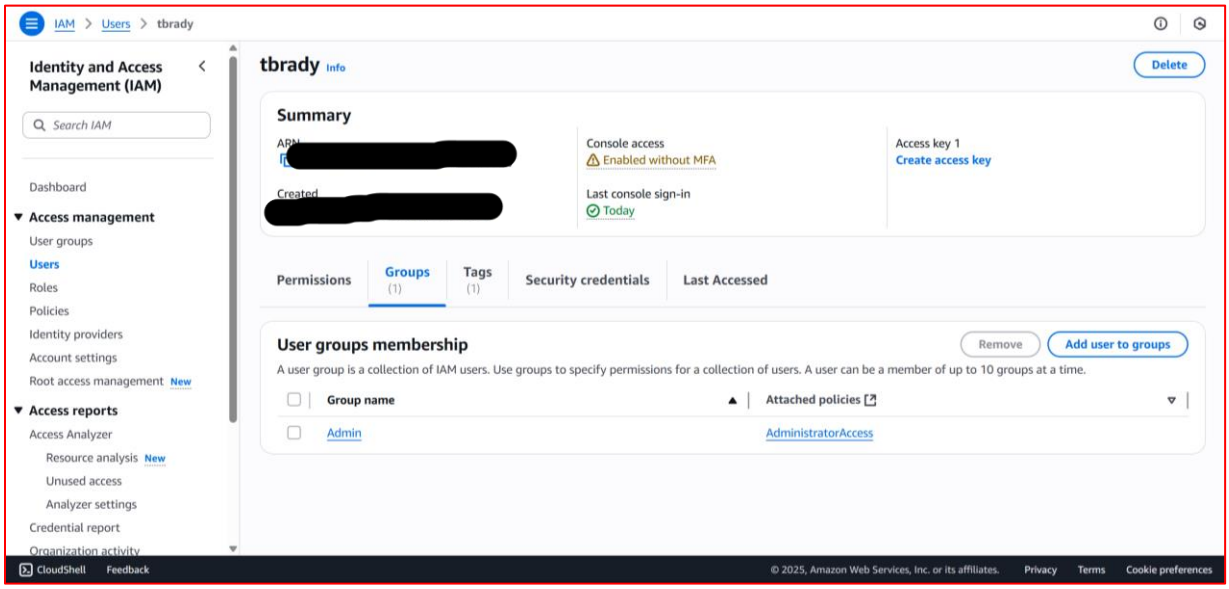


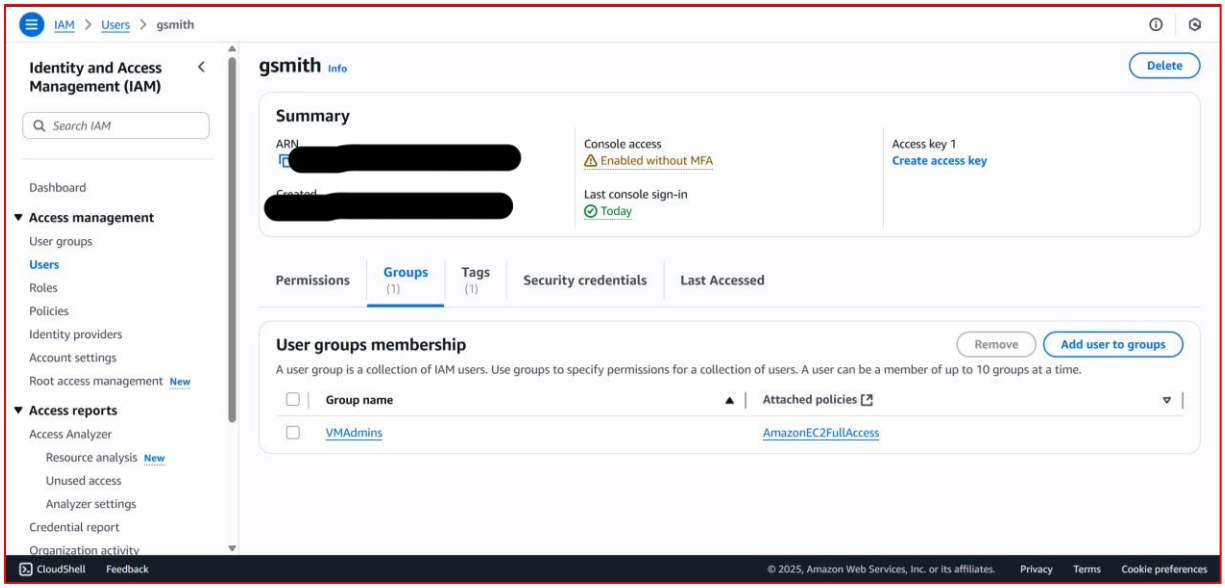
Note: Be sure you are creating the groups & users using IAM and not Identity Center

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).

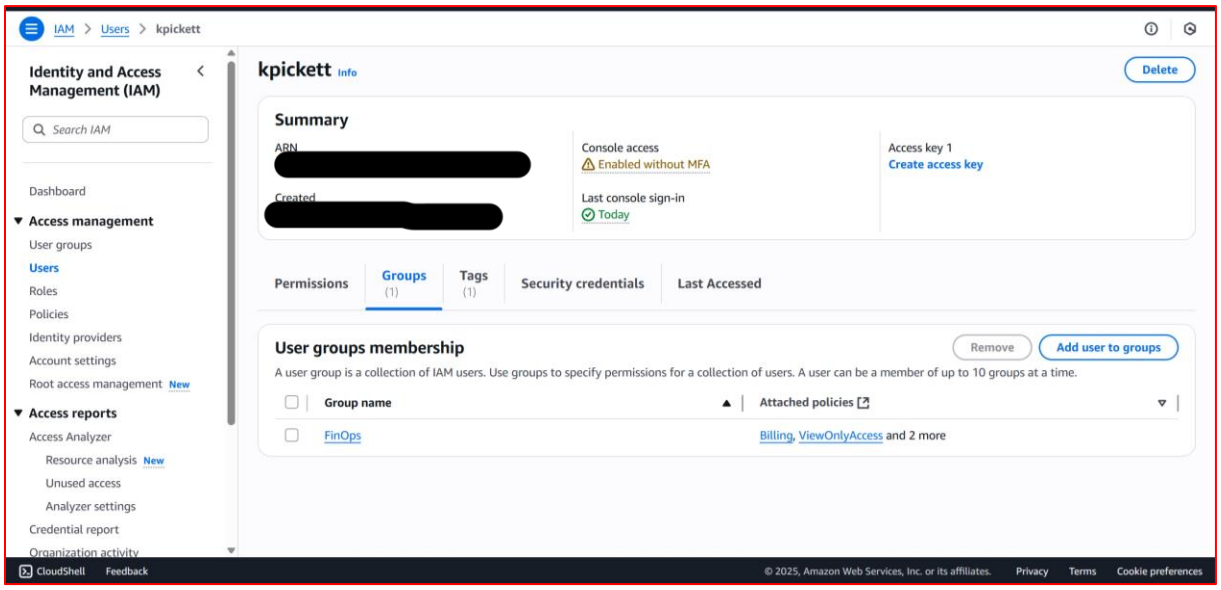
Using Role Based Access Control (RBAC) with AWS IAM

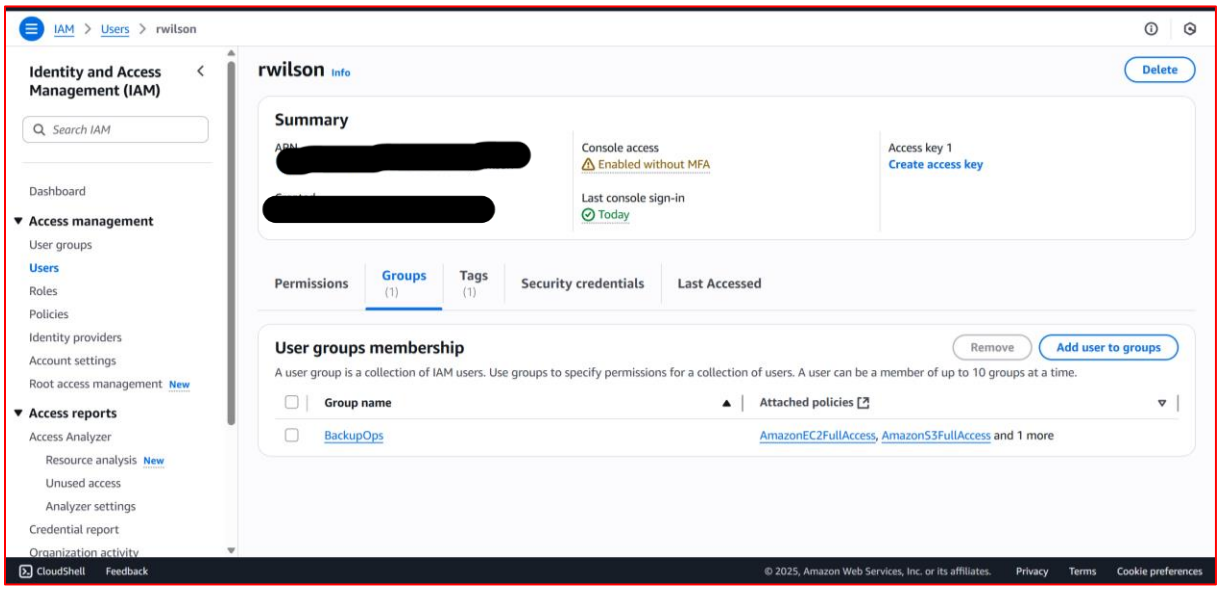


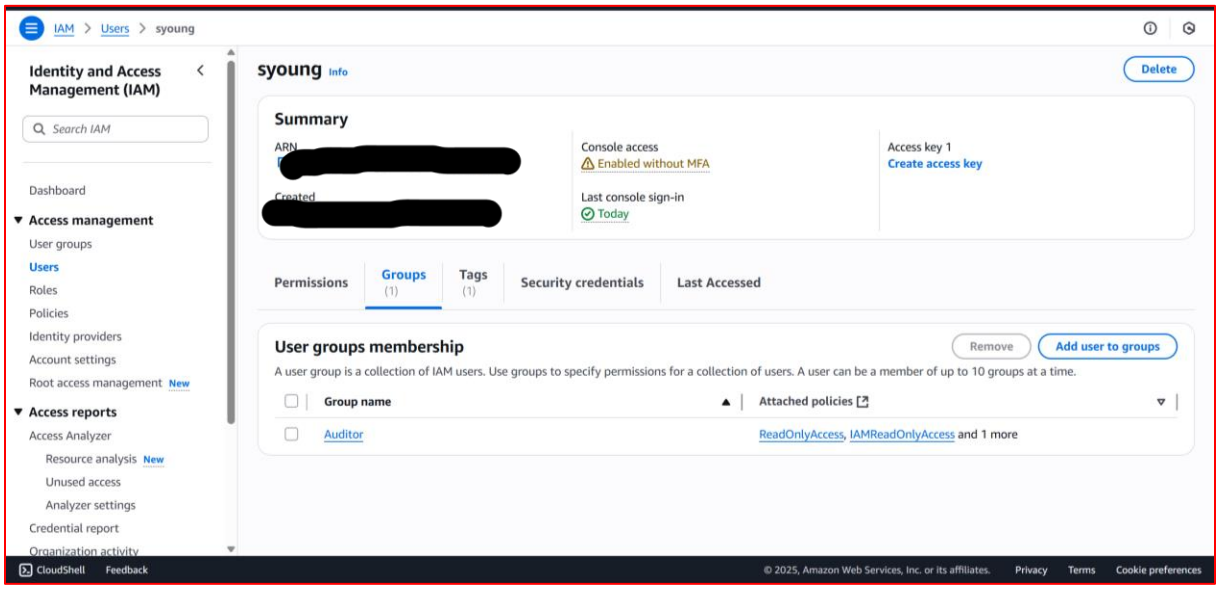




Using Role Based Access Control (RBAC) with AWS IAM

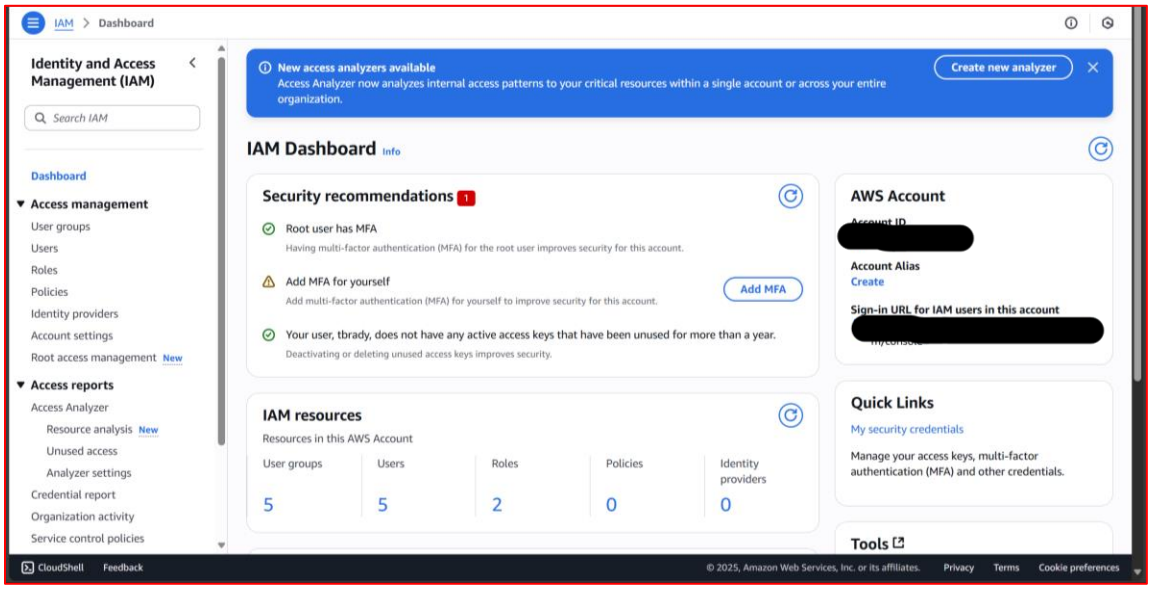


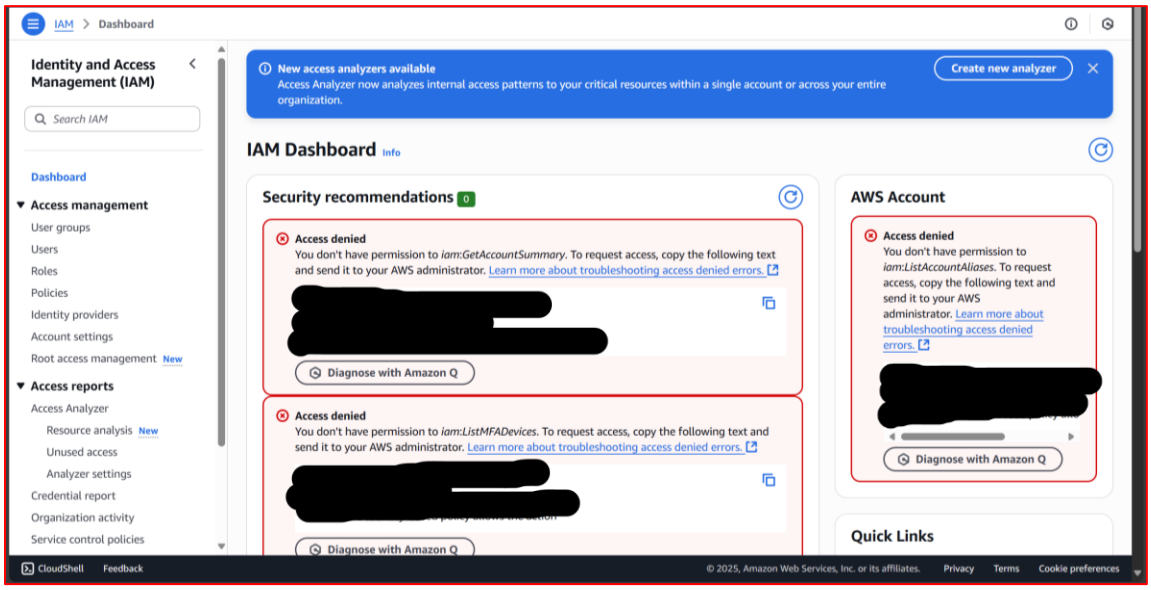




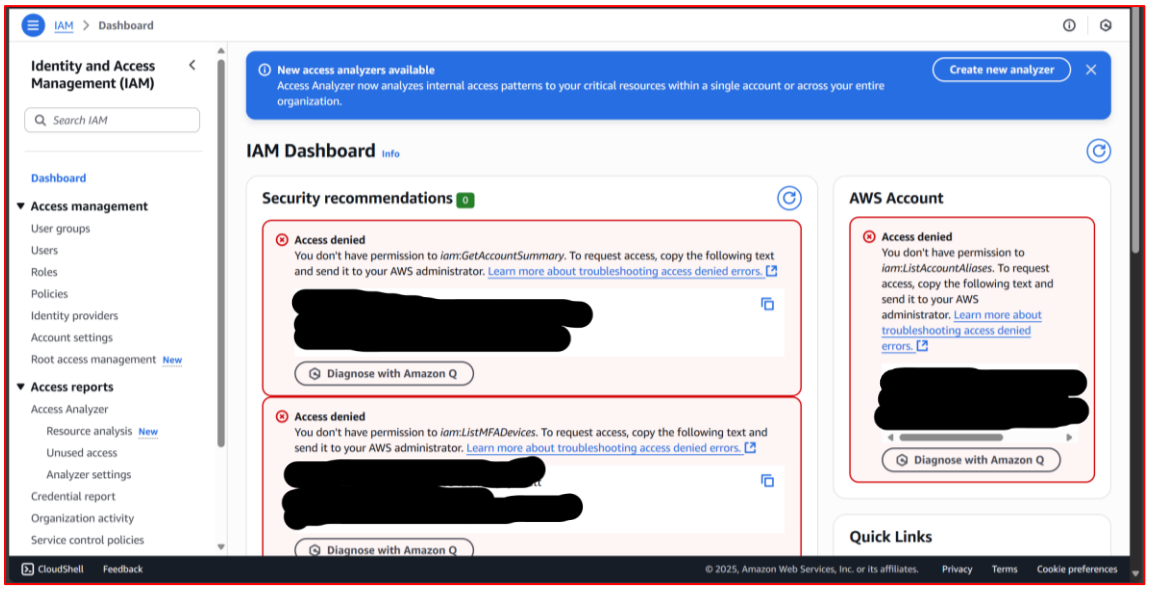
Using Role Based Access Control (RBAC) with AWS IAM

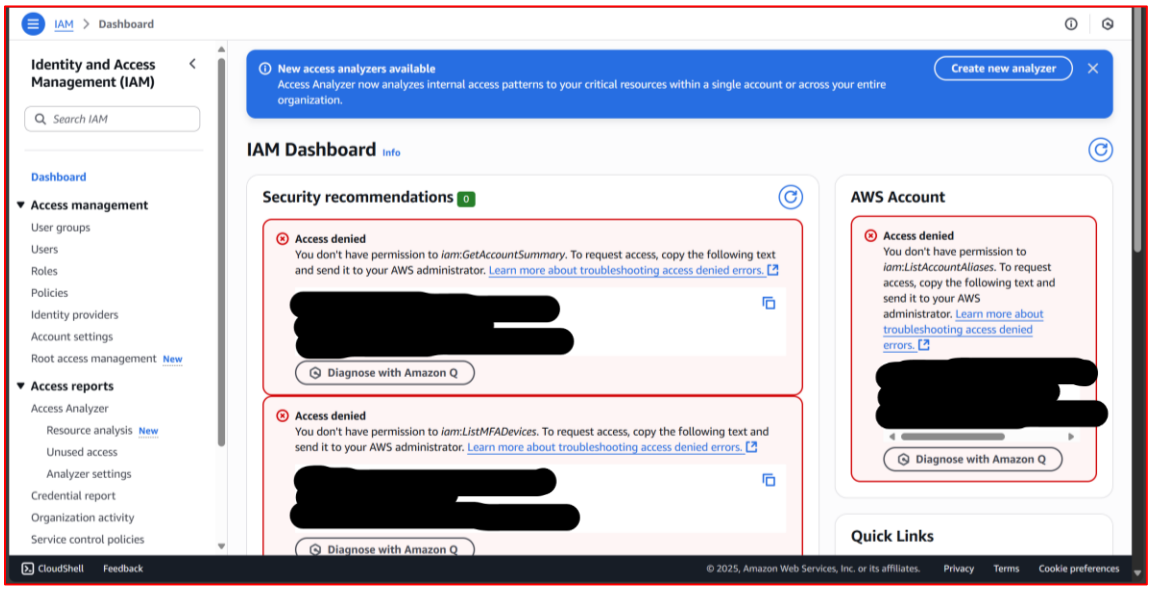
3. (40 points) Using console sign-in URL login and each user account verifies RBAC has been setup appropriately for each employee. **Tip: Use different browsers and/or incognito mode so that you can still have access to the AWS console with your root account to potentially adjust settings.**

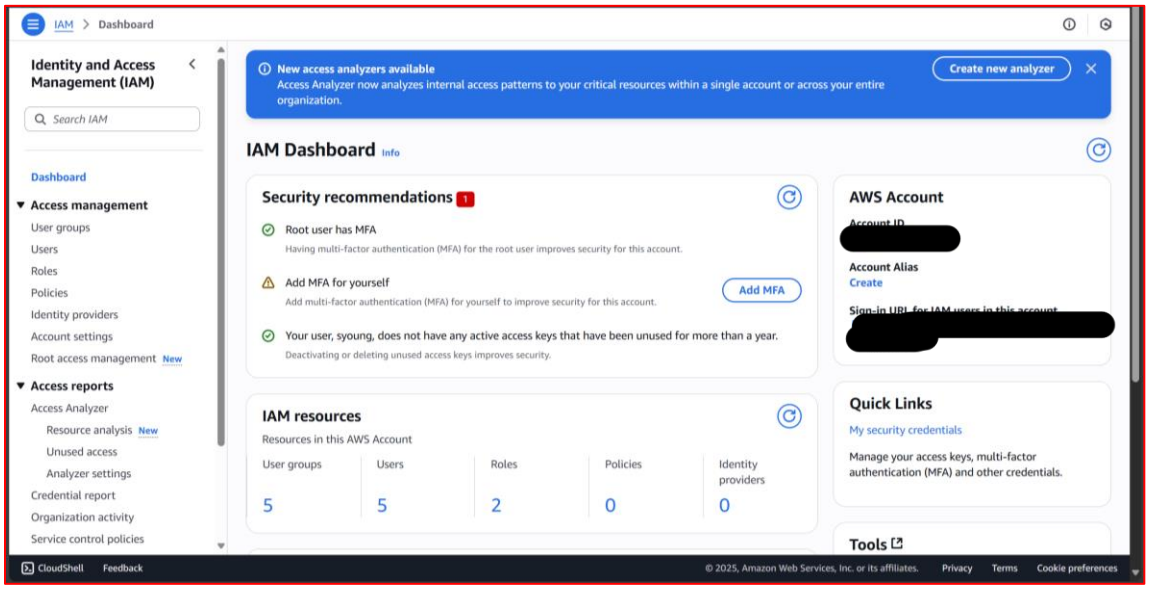




Using Role Based Access Control (RBAC) with AWS IAM





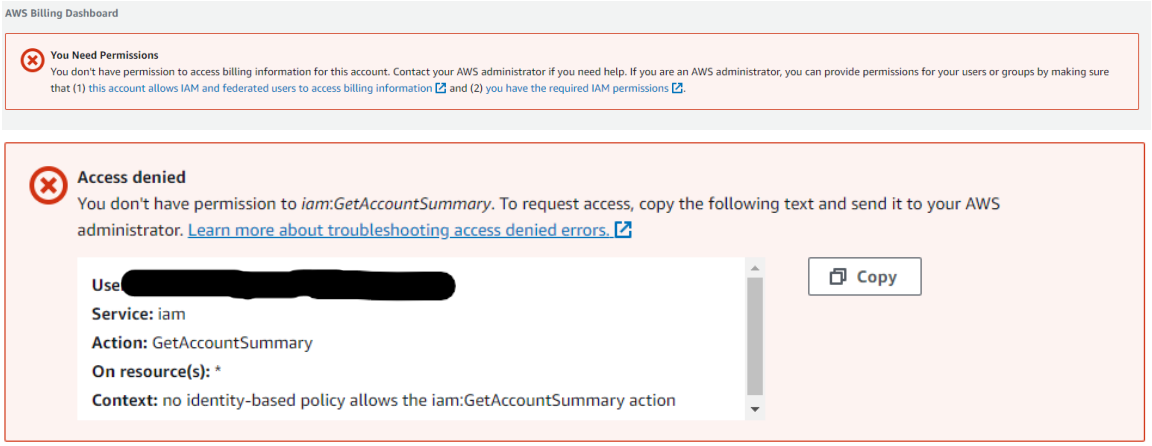


Using Role Based Access Control (RBAC) with AWS IAM

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

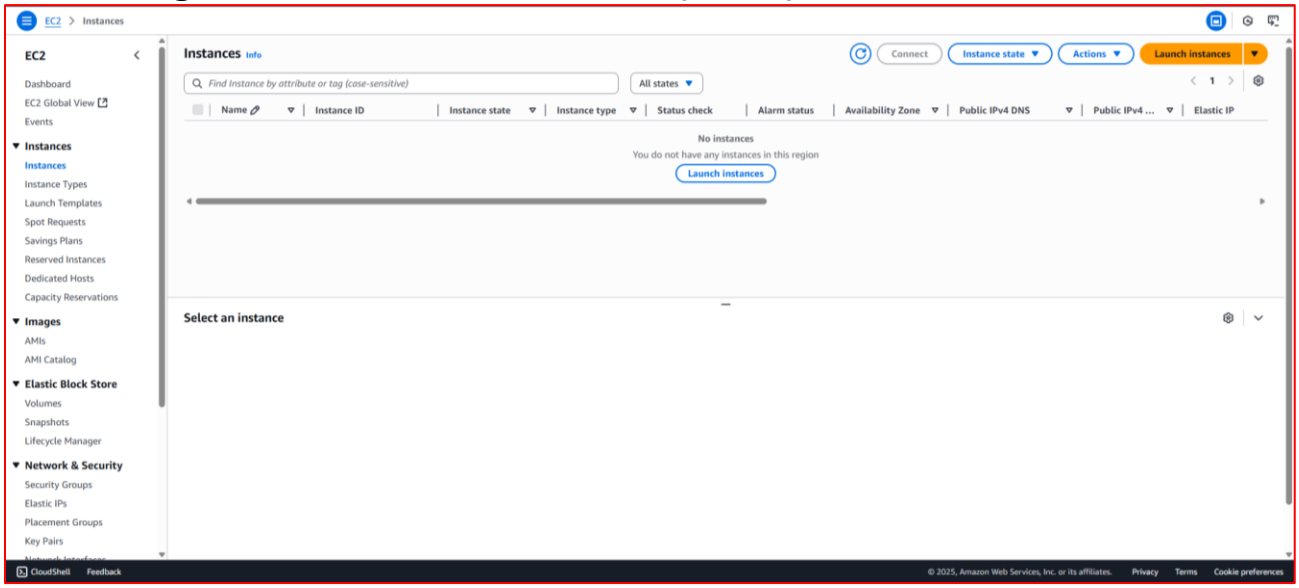
Example screenshots showing denied access:

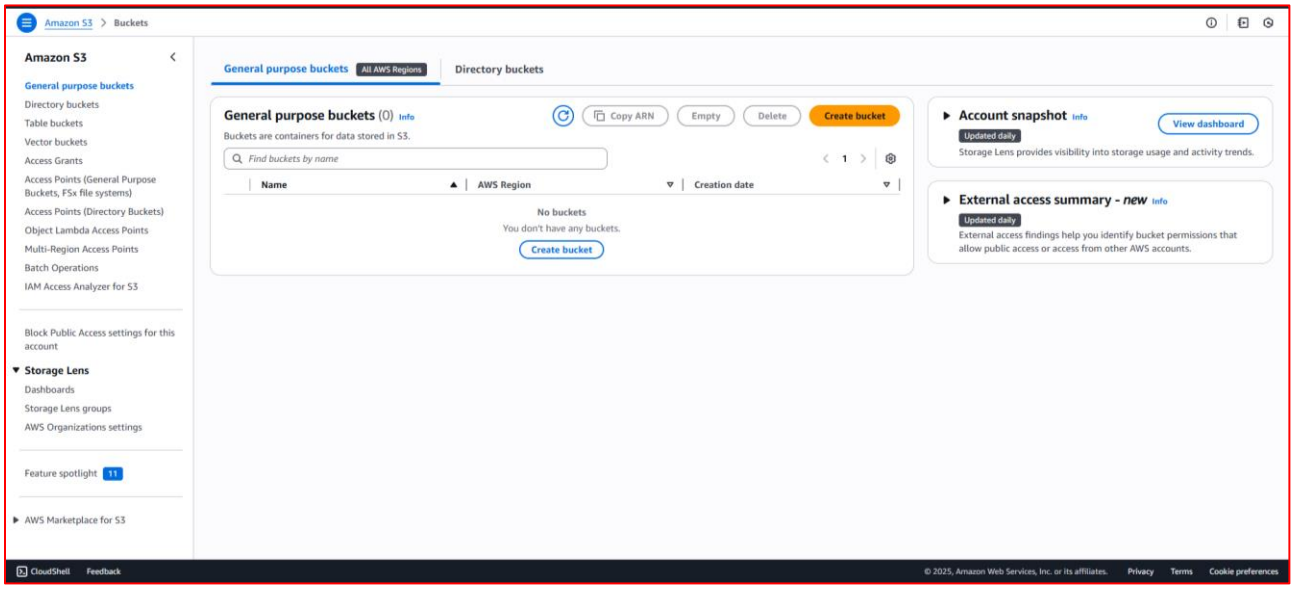


4. (5 points) When completed with this assignment, delete all billable resources. Note: AWS IAM resources are not billable!

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