DevOps- AWS Training

AWS IAM – 4 Oct. 2024

Set 1

Scenario 1:

At a company where multiple teams need access to different AWS services. You are asked to create a new IAM user for a developer, who only needs access to read and write to an S3 bucket and should not have access to any other AWS resources. You also want to make sure access is secured with MFA (Multi-Factor Authentication).

Questions:

1. Follow the least privilege principle.
2. What are the steps to enforce MFA on this user?
3. How can the user access the S3 bucket using the credentials you provide?

Scenario 2:

You are a cloud architect for a medium-sized company that has just started migrating its on-premises infrastructure to AWS. The company has various departments, including **Finance**, **Development**, and **Marketing**. Each department has a distinct set of users with different access needs. For example:

- **Finance** users need access to sensitive financial data stored in **Amazon S3** and the ability to run reports using **Amazon Athena**.
- **Development** users need access to launch and manage **EC2** instances, **RDS** databases, and access source code stored in **S3**.
- **Marketing** users need access to certain **S3** buckets that store customer-facing content and analytics data from **Amazon QuickSight**.

Security is a top priority, and the company has strict requirements:

1. Access to AWS resources must follow the principle of **least privilege**.
2. All IAM policies should be **managed centrally** to avoid duplication and ease policy updates.
3. Developers should be allowed only to access EC2 instance with **specific tags.**

Questions:

1. How would you organize the AWS IAM setup to ensure that users from each department only have access to the resources they need?
2. How would you implement **centralized IAM policy management** so that it’s easy to update permissions across departments?

Scenario 3:

You are the cloud architect for a large university that uses AWS for various academic and research projects. The university has multiple departments (Computer Science, Biology, Physics, etc.), and each department runs its projects on AWS. Technical staffs, Non-technical staffs and students in each department already have accounts in the university's **Central Database** system, which is managed by the IT department.

The university wants to integrate the existing Central Database with AWS so that users from different departments can access the AWS Management Console and other services. However, there are some strict guidelines:

Tasks (Describe how will you implement the scenario):

1. How would you integrate the university's Central Database with AWS so that users can log in with their login credentials?
2. How would you assign different permissions to faculty and students, ensuring they only access resources relevant to their department?
3. How would you enforce MFA for users before they can access AWS?
4. How would you configure the system so that users can only access the AWS account assigned to their department, even though all accounts are part of a single AWS Organization?

Scenario 4:

FinBank, a financial services company, has an AWS account for **Data Storage** in which financial data are stored . They make use of a 3rd party analytics team for data analysis. They need access to data stored in S3 buckets in the storage account to run reports and analysis. To ensure security and compliance with financial regulations, the CTO requires that this access be managed through **IAM Roles** with strict permissions and cross-account access controls with temporary credentials, ensuring no unnecessary access is granted.

Tasks (Describe how will you implement the scenario):

1. How would you provide solution for the above scenario?
2. Provide the steps involved in implementing the solution.