This lab demonstrates the steps from *Demo: Navigating the IAM Dashboard.*
My full AWS Architect Associate course can be found here:
https://www.udemy.com/course/ultimateaws/?referralCode=7ED214B795C444141361

Lab Guide: Exploring the IAM Dashboard and Managing the Root Account in AWS

Objective:

- Understand the basic elements of the AWS Identity and Access Management (IAM) dashboard.
- Learn about root account security configurations and key IAM concepts.

---

1. Accessing the AWS Console and Region Settings

Steps:

1. **Log in to the AWS Management Console.**
   - Upon logging in, you will see the AWS home screen.
   - The top right corner displays the current region (e.g., *Ohio*).
   - AWS regions represent different geographic locations where AWS data centers operate.
2. **Understand Regional vs. Global Services:**
   - Certain AWS services, such as **VPCs** (Virtual Private Clouds) and **EC2 instances**, are regional. Resources created in one region are not automatically available in another.
   - IAM, however, is a **global service**. Changes made in IAM apply across all AWS regions.

Key Concept:

- **Global Services**: Services that operate across all AWS regions (e.g., IAM, Route 53).
- **Regional Services**: Services limited to a specific region (e.g., EC2, S3).

---

2. Navigating to the IAM Dashboard

Steps:

1. **Search for IAM:**
    - Use the **search bar** at the top of the AWS console and type "IAM."
    - Select the **IAM dashboard** from the dropdown menu.
2. **Observe the Dashboard Layout:**
    - The IAM dashboard provides an overview of security recommendations and configuration status.
    - Key recommendations include:
        - Enabling **multi-factor authentication (MFA)** for the root account.
        - Deleting **root account access keys** (if any exist).

---

3. Securing the Root Account

Steps:

1. **Access Root Account Security Credentials:**
    - Click on your **account name** in the top right corner.
    - Select **"Security Credentials"** from the dropdown menu.
2. **Review Root Account Configurations:**
    - **Password Management**: You can update the root account password here.
    - **Multi-Factor Authentication (MFA)**:
        - MFA adds an extra layer of security by requiring a second authentication factor (e.g., a smartphone).
        - If MFA is not enabled, click **"Manage"** to set up an MFA device.
3. **Enabling MFA for the Root Account:**
    - Select **"Add MFA Device."**
    - Follow the prompts to scan a QR code with your MFA app (e.g., Google Authenticator).
    - Test and confirm the MFA setup.
4. **Access Key Management:**
    - Verify that there are **no access keys** for the root account. Access keys are credentials used for programmatic access to AWS services.
    - If access keys exist, delete them to enhance security.

Key Concept:

- **Root Account**: The master account with full administrative privileges. It should only be used for critical tasks and secured with strong security measures.
- **MFA**: Enhances account security by requiring both a password and a time-based one-time code.

---

4. IAM Sign-In URL and Account Alias

Steps:

1. **Locate the IAM User Sign-In URL:**
    - On the IAM dashboard, locate the **Sign-In URL** in the right-hand panel.
    - This URL is specific to your AWS account and can be used by IAM users to log in.
2. **Test the Sign-In URL:**

    - Copy the URL and open it in an **incognito/private browsing window**.
    - Paste the URL into the address bar.
    - Notice that it directs you to a sign-in page specific to your AWS account.
3. **Sign-In Options:**
    - You can log in as an **IAM user** with a username and password.
    - Alternatively, log in as the **root user** using the email address associated with the account.
4. **Customize the Account Alias:**
    - In the IAM dashboard, locate the **Account Alias** setting.
    - The alias customizes the sign-in URL to make it more user-friendly (e.g., `your-company.signin.aws.amazon.com`).
    - To edit the alias:
        - Click **"Edit"** next to the current alias.
        - Enter a new alias (e.g., `YourOrg-Security`).
        - Save the changes.
5. **Verify the Updated URL:**
    - After updating the alias, notice that the sign-in URL now reflects the new alias.

Key Concepts:

- **IAM Sign-In URL**: A unique URL for IAM user login, tied to your AWS account.
- **Account Alias**: A customizable identifier that makes the sign-in URL easier to remember.

---

5. Best Practices for the IAM Dashboard

- **Enable MFA** on all accounts, especially the root account.
- **Delete root access keys** to minimize security risks.
- Use **IAM users** and **groups** with appropriate permissions instead of logging in as the root user.
- Regularly review and update IAM policies and permissions.

Conclusion:

In this lab, you explored the IAM dashboard, secured the root account, and learned how IAM configurations apply globally across AWS regions. You also customized the IAM sign-in URL to enhance user access. These foundational steps are critical for maintaining security and efficient account management in AWS.