1.2. Student Handout

AWS Account Creation and Introduction to IAM: Student Handout

---

Introduction to AWS

Amazon Web Services (AWS) is a cloud computing platform offering a variety of services such as computing power, storage, and databases. AWS allows you to rent these services on-demand, paying only for what you use.

AWS Global Infrastructure

AWS operates in multiple **Regions** and **Availability Zones (AZs)** worldwide. Regions are distinct geographic areas, and each region contains multiple AZs, which are isolated to ensure high availability and fault tolerance.

Setting Up an AWS Account

Steps to Create an AWS Free-Tier Account

1. **Visit AWS Website**: Go to aws.amazon.com and click "Create an AWS Account."
2. **Enter Email and Password**: Provide a valid email and create a strong password.
3. **Provide Contact Information**: Enter your name, address, and phone number.
4. **Choose the Free Tier**: Opt for the Free Tier to explore AWS services for free for 12 months.
5. **Enter Payment Information**: Provide a credit or debit card for verification.
6. **Identity Verification**: Verify your identity via a code sent to your phone.
7. **Select a Support Plan**: Choose the Basic Support Plan, which is free.
8. **Complete the Setup**: Finish the setup to start using AWS services.

Examples

- **Example 1**: Creating an account to host a personal website using AWS services.
- **Example 2**: Setting up an account for a startup to manage cloud resources.
- **Example 3**: Using the Free Tier to experiment with AWS machine learning services.

Billing Management and Cost Control

AWS provides tools to manage billing and control costs, such as setting up budgets and alerts to notify you when usage exceeds a certain threshold.

Introduction to Identity and Access Management (IAM)

IAM is a service that manages who can access AWS resources and what they can do with them. It enforces the principle of least privilege, ensuring users only have the permissions necessary for their tasks.

Key IAM Components

1. **Users**: Individual accounts representing people or applications.
2. **Groups**: Collections of users with shared permissions.
3. **Roles**: Assigned to applications or services for accessing AWS resources.
4. **Policies**: Documents defining permissions for users, groups, or roles.

Examples

- **Example 1**: Creating a user account for a developer with access to specific AWS services.
- **Example 2**: Setting up a group for the finance team with permissions to access billing information.
- **Example 3**: Assigning a role to an EC2 instance to access an S3 bucket.

Creating and Managing IAM Users

1. **Log in to AWS Management Console**: Use your root account.
2. **Navigate to IAM**: Search for "IAM" and click on it.
3. **Create a New User**: Click "Add user," enter a username, and select access type.
4. **Assign Permissions**: Attach policies directly or add the user to a group.

5. **Review and Create**: Review details and create the user.

Examples

- **Example 1**: Creating a user with programmatic access for API interactions.
- **Example 2**: Adding a user to a group with read-only access to AWS resources.
- **Example 3**: Assigning console access to a user for managing AWS services via the web interface.

Using IAM Policies to Control Access

IAM policies define what actions a user, group, or role can perform on AWS resources. Policies are written in JSON and specify permissions like "Allow" or "Deny."

Examples

- **Example 1**: A policy allowing a user to read objects from an S3 bucket.
- **Example 2**: A policy denying access to delete resources in a specific region.
- **Example 3**: A policy granting full access to manage EC2 instances.

Best Practices for Securing Your AWS Account

1. **Enable Multi-Factor Authentication (MFA)**: Adds an extra layer of security.
2. **Implement Least Privilege**: Only give necessary permissions.
3. **Audit Access**: Regularly review access and permissions.

Hands-On: Setting Up IAM Users and Policies

1. **Log in to AWS**: Use your root account.
2. **Go to IAM**: Search for "IAM" and click on it.
3. **Create a User**: Click "Add user," enter a username, and select access type.
4. **Assign Permissions**: Attach the "AdministratorAccess" policy.
5. **Review and Create**: Review details and create the user.
6. **Enable MFA**: Add MFA for enhanced security.

Conclusion

This guide covered AWS account creation and IAM basics, including setting up an account, managing billing, and controlling access with IAM. By following best practices, you can ensure your AWS account is secure and well-managed.

Diagram: AWS Account and IAM Structure

```
+-------------+
| AWS Account |
+-------------+
                |
                +------------+
                |            |
+------+----+ +------+-----+
| IAM Users | | IAM Groups |
+-----------+ +------------+
                |            |
+------+----+ +------+-------+
| IAM Roles | | IAM Policies |
+-----------+ +--------------+
```

Next Steps

In the next session, we’ll explore specific AWS services and how to use IAM roles for applications.