AWS Identity Services Setup Guide

This guide provides a comprehensive walkthrough for setting up AWS Identity and Access Management (IAM) services, including creating groups, users, policies, and roles.

Prerequisites

- AWS Account with administrative access
- Access to AWS Management Console

Table of Contents

Accessing IAM Dashboard

1. Open the AWS Management Console
2. Search for "IAM" in the services search bar
3. Click on "IAM" to open the Identity and Access Management dashboard

Creating User Groups

Creating Admin Group

1. Navigate to **User groups** in the IAM dashboard
2. Click **Create group**
3. Enter group name: `admin`
4. Click **Create group**

Creating Development Group

1. Navigate to **User groups** in the IAM dashboard
2. Click **Create group**

3. Enter group name: `dev`
4. Click **Create group**

Creating IAM Users

Step-by-Step User Creation

1. Navigate to **Users** in the IAM dashboard
2. Click **Create user**
3. Configure user settings:
   - Check "Provide user access to the AWS Management Console"
   - Select "I want to create an IAM user"
4. Click **Next**
5. In the permissions section, select user groups:
   - Check `admin` group
6. Click **Create user**

User Credentials Example

After user creation, you'll receive:

- **Console sign-in URL**: `https://266833220666.signin.aws.amazon.com/console`
- **Username**: `raviv-admin`
- **Temporary password**: `rEF3#7[[`

Important: Users must change their password on first login.

Managing Group Permissions

Adding IAM Read-Only Access to Admin Group

1. Navigate to **User groups**
2. Select the `admin` group
3. Click **Add permissions → Attach policies**
4. Search for and select `IAMReadOnlyAccess`
5. Click **Attach policies**

This allows IAM users in the admin group to access the IAM menu and view IAM resources.

Adding S3 Full Access to Dev Group

1. Navigate to **User groups**
2. Select the `dev` group
3. Click **Add permissions → Attach policies**
4. Search for and select `AmazonS3FullAccess`
5. Click **Attach policies**

Adding Users to Multiple Groups

To add an existing user to additional groups:

1. Navigate to **Users**
2. Select the user (e.g., `raviv-admin`)
3. Go to the **Groups** tab
4. Click **Add user to groups**
5. Select the `dev` group
6. Click **Add to groups**

Now the user has both admin and S3 full access permissions.

Creating Custom Policies

Creating a Custom IAM Policy

1. Navigate to **Policies** in the IAM dashboard
2. Click **Create policy**
3. Configure policy settings:
   - **Service**: Select IAM
   - **Actions**:
     - All Read actions
     - All List actions
   - **Resources**: All resources
4. Click **Next**
5. Enter policy name: `pol01`
6. Click **Create policy**

Attaching Custom Policy to Group

1. Navigate to **User groups**
2. Select the `admin` group
3. Click **Add permissions** → **Attach policies**
4. Search for `pol01`
5. Select the policy and click **Attach policies**

Attaching Roles to EC2 Instances

Creating an IAM Role for EC2

1. Navigate to **Roles** in the IAM dashboard
2. Click **Create role**
3. Select **AWS service** as the trusted entity type
4. Select **EC2** as the use case
5. Click **Next**
6. Search for and attach `IAMReadOnlyAccess` policy
7. Click **Next**
8. Enter role name: `iam-readonly-role`
9. Click **Create role**

Attaching Role to EC2 Instance

1. Navigate to the **EC2 Dashboard**
2. Create or select an existing EC2 instance
3. Right-click the instance → **Security** → **Modify IAM role**
4. Select the `iam-readonly-role` from the dropdown
5. Click **Update IAM role**

Testing Permissions

Testing from EC2 Instance CLI

Once the IAM role is attached to the EC2 instance, you can test the permissions:

1. Connect to your EC2 instance via SSH
2. Run the following AWS CLI command:

```bash
aws iam list-users
```

This command should successfully return a list of IAM users, confirming that the role and permissions are working correctly.

Security Best Practices

- **Principle of Least Privilege**: Only grant the minimum permissions necessary for users to perform their tasks
- **Regular Audits**: Periodically review user permissions and remove unnecessary access
- **Strong Passwords**: Enforce strong password policies for IAM users
- **MFA**: Enable Multi-Factor Authentication for enhanced security
- **Role-Based Access**: Use IAM roles for applications and services instead of embedding access keys

Troubleshooting Common Issues

- **Access Denied Errors**: Verify that the correct policies are attached to users/groups/roles
- **Console Access Issues**: Ensure users have the necessary console access permissions
- **CLI Authentication**: Verify that IAM roles are properly attached to EC2 instances for CLI access

Conclusion

This guide covers the fundamental aspects of AWS Identity Services setup, including user management, group creation, policy attachment, and role-based access control. Following these steps will establish a solid foundation for managing access to your AWS resources securely and efficiently.