AWS Module 2 | IAM

Introduction

This document provides evidence for proper completion of AWS module 2 on IAM. The two main features are:

- IAM User generation via a script to illustrate automation.
- Establishing an MFA policy

User Generation

The script, aws-iam-create-user.sh, reads rows from a csv file containing the user information to import into IAM. The columns in the csv file are user, group and password.

The script iterates over the rows in the csv file. The following aws iam commands generate the IAM users:

- aws iam create-user --user-name $user
- aws iam create-login-profile --password-reset-required --user-name $user --password $password
- aws iam add-user-to-group --group-name $group --user-name $user

CSV File

The csv file consists of 4 users.

```
[cloudshell-user@ip-10-2-50-56 ~]$ cat users2.csv
user,group,password
jane.doe,DBA,ChangeMe123456!
michael.scott,NetworkAdmin,ChangeMe123456!
barbara.brown,CloudAdmin,ChangeMe123456!
brian.garcia,LinuxAdmin,ChangeMe123456!
[cloudshell-user@ip-10-2-50-56 ~]$
```

Script Execution

The script takes the csv filename as a parameter.

```
[cloudshell-user@ip-10-6-114-148 ~]$ ls
aws-iam-create-user.sh  mission3_en  users2.csv
[cloudshell-user@ip-10-6-114-148 ~]$ ./aws-iam-create-user.sh users2.csv
```

The following is an excerpt of the output of the script execution.

```
        "CreateDate": "2023-04-26T07:24:44+00:00"
    }
}
{
    "LoginProfile": {
        "UserName": "barbara.brown",
        "CreateDate": "2023-04-26T07:24:46+00:00",
        "PasswordResetRequired": true
    }
}
{
    "User": {
        "Path": "/",
        "UserName": "brian.garcia",
        "UserId": "AIDARJLU734B7XLK76RUI",
        "Arn": "arn:aws:iam::088829058819:user/brian.garcia",
        "CreateDate": "2023-04-26T07:24:49+00:00"
    }
}
{
    "LoginProfile": {
        "UserName": "brian.garcia",
        "CreateDate": "2023-04-26T07:24:51+00:00",
        "PasswordResetRequired": true
    }
}
[cloudshell-user@ip-10-2-50-56 ~]$
```

Multiple Factor Authentication (MFA)

The Multiple Factor Authentication is established through a custom policy, entitled EnforceMFAPolicy. The custom policy is created using the json file, force_mfapolicy.json.

MFA uses Google Authenticator on my cell. MFA is configured for the root user and at least one IAM User.

IAM dashboard

Security recommendations

✅ **Root user has MFA**
Having multi-factor authentication (MFA) for the root user improves security for this account.

✅ **You have MFA**
Having multi-factor authentication (MFA) for the root user improves security for this account.

✅ **Your user, barbara.brown, does not have any active access keys that have been unused for more than a year.**
Deactivating or deleting unused access keys improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
5	5	2	1	0

IAM > Users

Users (5) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

	User name	Groups	Last activity	MFA	Password age	Active key age
☐	barbara.brown	CloudAdmin	✓ 5 minutes ago	Virtual	✓ 19 minutes ago	-
☐	brian.garcia	LinuxAdmin	Never	None	✓ 16 hours ago	-
☐	jane.doe	DBA	✓ 1 hour ago	None	✓ 15 hours ago	-
☐	michael.quick	None	Never	None	✓ 23 hours ago	-
☐	michael.scott	NetworkAdmin	Never	None	✓ 16 hours ago	-

Account Settings

A custom password policy is established.

Account settings Info

Password policy Info
Configure the password requirements for the IAM users.   Edit

This AWS account uses the following custom password policy:

Password minimum length
8 characters

Other requirements
- Never expire password

Password strength
- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)
- Require at least one number

Group Permission Policies

Each User Group has its own permission policies. Every User Group contains the EnforceMFAPolicy permission policy.

User group name
CloudAdmin

Creation time
April 25, 2023, 22:34

Users   **Permissions**   Access Advisor

Permissions policies (3) Info
You can attach up to 10 managed policies.

☐	Policy name ⬈	
☐	⊞ EnforceMFAPolicy	
☐	⊞ AdministratorAccess	
☐	⊞ IAMUserChangePassword	

User group name
LinuxAdmin

Creation time
April 25, 2023, 22:40

Users   **Permissions**   Access Advisor

Permissions policies (3) Info
You can attach up to 10 managed policies.

☐	Policy name ⬈	Type
☐	⊞ EnforceMFAPolicy	Customer managed
☐	⊞ AmazonEC2FullAccess	AWS managed
☐	⊞ IAMUserChangePassword	AWS managed

User group name	Creation time
NetworkAdmin	April 25, 2023, 22:50 (UTC-(

Users   **Permissions**   **Access Advisor**

Permissions policies (3) Info
You can attach up to 10 managed policies.

🔍 Filter policies by property or policy name and press enter.

☐	Policy name ⬀	▽	Type	▽
☐	⊞ EnforceMFAPolicy		Customer managed	
☐	⊞ 📦 IAMUserChangePassword		AWS managed	
☐	⊞ 📦 AmazonVPCFullAccess		AWS managed	

User group name	Creation time
DBA	April 25, 2023, 22:36 (

Users   **Permissions**   **Access Advisor**

Permissions policies (3) Info
You can attach up to 10 managed policies.

🔍 Filter policies by property or policy name and press enter.

☐	Policy name ⬀	▽	Type	⬂
☐	⊞ EnforceMFAPolicy		Customer managed	
☐	⊞ 📦 AmazonRDSFullAccess		AWS managed	
☐	⊞ 📦 IAMUserChangePassword		AWS managed	

User group name	Creation time
Trainee	April 25, 2023, 23:36 (UTC-07:00

Users   **Permissions**   **Access Advisor**

Permissions policies (3) Info
You can attach up to 10 managed policies.

🔍 Filter policies by property or policy name and press enter.

☐	Policy name ⬀	▽	Type	▽
☐	⊞ EnforceMFAPolicy		Customer managed	
☐	⊞ 📦 ReadOnlyAccess		AWS managed - job function	
☐	⊞ 📦 IAMUserChangePassword		AWS managed	