

Automating user creation with AWS Identity and Access Management (IAM) resources

Introduction

In this article, I will demonstrate a simple automated user group and user account creation process to help you avoid the repetitive manual tasks in provisioning AWS accounts.

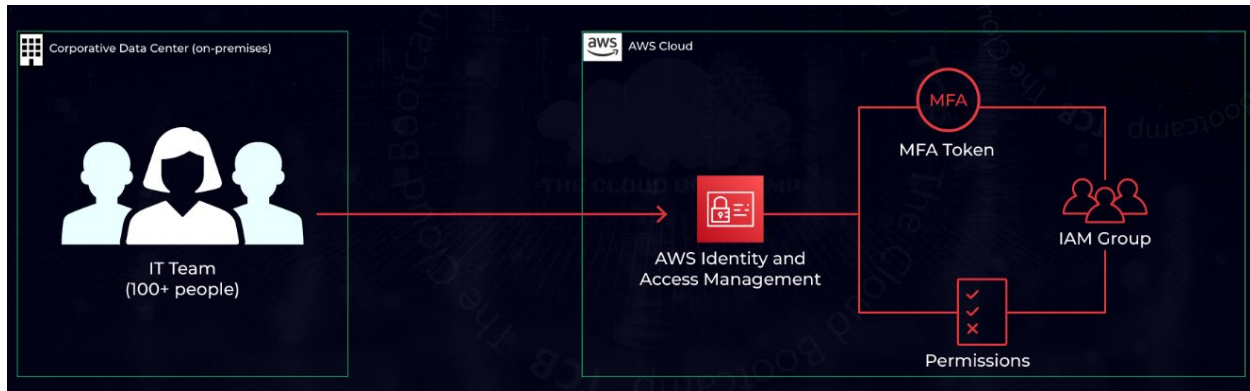


Note: AWS-specific account information will be redacted in all images and sample outputs. If you follow the steps in this article and change any object or file names, ensure you update the commands given herein with the names you used.

Use Case

Let's assume you need to migrate 100+ users; each user must have Multi-factor Authentication (MFA) enabled, and their profile must be set to require the password to be reset on the first login. Each user must be assigned a specific user group to maintain the best practice of minimal privileged user access required for their role. Since we are not federating user accounts, we must also provide the ability for the users to change their passwords.

Solution Architecture



MFA Policy

Our MFA policy must allow the logged-in user to:

- Allow the user to see their user profile.
- Allow the user to view MFA devices.
- Manage their own MFA device.
- Deny access to all other services if MFA has not been set up.

Download the policy JSON file [here](#).

Important note: By defining the resource in the policy, the user can only create an MFA device named as their username. Example: "Resource": "arn:aws:iam::*:mfa/\${aws:username}"

To implement the MFA policy in your AWS environment:

1. Log in to your AWS console
2. Open the CloudShell
3. Upload the MFA policy JSON file
4. Execute the following command

```
aws iam create-policy --policy-document file://enforce_mfapolicy.json --policy-name EnforceMFAPolicy
```

The output from the command will look something like this:

```
{
  "Policy": {
    "PolicyName": "EnforceMFAPolicy",
    "PolicyId": "A1B2C3D4E5F6G7H8I9J0",
    "Arn": "arn:aws:iam::123456789012:policy/EnforceMFAPolicy",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 0,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "CreateDate": "2023-04-26T03:29:09+00:00",
    "UpdateDate": "2023-04-26T03:29:09+00:00"
  }
}
```

```
}  
}
```

Prerequisites

The following package is required to run the scripts to create user groups and accounts.

1. Log in to your AWS console
2. Open the CloudShell
3. Execute the following command

```
sudo yum install dos2unix -y
```

Automating User Group Creation

The script to create the predefined user groups automatically will take the group name and default policy from an input CSV file. The script will also apply the standard AWS IAM User Change Password and the MFA enforcement policies we created to the user group.

The input file is a simple CSV file with group and policy attributes. Example:

```
group,policy  
CloudAdmin,AdministratorAccess  
DBA,AmazonRDSFullAccess  
LinuxAdmin,AmazonEC2FullAccess  
NetworkAdmin,AmazonVPCFullAccess  
Trainees,ReadOnlyAccess
```

Download the script file [here](#).

Edit the aws-iam-create-group.sh file and replace the <policy arn> for the MFA Policy, for example:

```
aws iam attach-group-policy --group-name $group --policy-arn  
arn:aws:iam::[REDACTED]:policy/EnforceMFAPolicy
```

Note: If you don't like the AWS CloudShell vim editor, you can use the instructions [here](#) to install the nano editor.

Steps to create the groups:

1. Log in to your AWS console
2. Open the CloudShell
3. Upload the aws-iam-create-group.sh script and your groups.csv file
4. Execute the following command to set up permission to execute the script

```
chmod +x aws-iam-create-group.sh
```











5. Execute the following command to create the groups

```
./aws-iam-create-group.sh groups.csv
```

Sample output for the CloudAdmin group given in the sample input file data:

```
{
  "Group": {
    "Path": "/",
    "GroupName": "CloudAdmin",
    "GroupId": "[REDACTED]",
    "Arn": "arn:aws:iam::[REDACTED]:group/CloudAdmin",
    "CreateDate": "2023-04-26T01:19:13+00:00"
  }
}
```

IAM > User groups

User groups (5) Info			
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.			
<input type="text" value="Filter User groups by property or group name and press enter"/>			
<input type="checkbox"/>	Group name	Users	Permissions
<input type="checkbox"/>	CloudAdmin	 0	 Defined
<input type="checkbox"/>	DBA	 0	 Defined
<input type="checkbox"/>	LinuxAdmin	 0	 Defined
<input type="checkbox"/>	NetworkAdmin	 0	 Defined
<input type="checkbox"/>	Trainees	 0	 Defined

AWS UI User Group Listing

IAM > User groups > CloudAdmin

CloudAdmin

Delete

Summary

Edit

User group name	Creation time	ARN
CloudAdmin	April 25, 2023, 20:19 (UTC-05:00)	arn:aws:iam: :group/CloudAdmin

Users Permissions Access Advisor

Permissions policies (3) Info

You can attach up to 10 managed policies.



Simulate

Remove

Add permissions

Filter policies by property or policy name and press enter.

< 1 >

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	EnforceMFAPolicy	Customer managed	
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to AWS
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	Provides the ability for an IAM

Permissions listing of an AWS User Group

Automatically Create Users and Assign them to Designated Groups

The script to create the predefined list of users automatically will take the username, group name, and password from an input CSV file. The script will also implement the requirement to reset the user's password on the first login.

The input file is a simple CSV file with user, group, and password attributes. Example:

```
user,group,password
jane.doe,DBA,ChangeMe123456!
john.doe,NetworkAdmin,ChangeMe123456!
billy.joe,CloudAdmin,ChangeMe123456!
jim.bob,LinuxAdmin,ChangeMe123456!
mary.sunshine,Trainees,ChangeMe123456!
```

Download the script file [here](#).

Steps to create the user accounts:

1. Log in to your AWS console
2. Open the CloudShell
3. Upload the aws-iam-create-user.sh script and your users.csv file
4. Execute the following command to set up permission to execute the script

```
chmod +x aws-iam-create-user.sh
```

5. Execute the following command to create the user accounts.

```
./aws-iam-create-user.sh users.csv
```

Sample output for the jane.doe user given in the sample input file data:

```
{
  "User": {
    "Path": "/",
    "UserName": "jane.doe",
    "UserId": "[REDACTED]",
    "Arn": "arn:aws:iam::[REDACTED]:user/jane.doe",
    "CreateDate": "2023-04-26T02:54:20+00:00"
  }
}
{
  "LoginProfile": {
    "UserName": "jane.doe",
    "CreateDate": "2023-04-26T02:54:22+00:00",
    "PasswordResetRequired": true
  }
}
```

IAM > User groups

User groups (5) Info			
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.			
<input type="text" value="Filter User groups by property or group name and press enter"/>			
<input type="checkbox"/>	Group name	Users	Permissions
<input type="checkbox"/>	CloudAdmin	1	Defined
<input type="checkbox"/>	DBA	1	Defined
<input type="checkbox"/>	LinuxAdmin	1	Defined
<input type="checkbox"/>	NetworkAdmin	1	Defined
<input type="checkbox"/>	Trainees	1	Defined

AWS User Group Listing

Shows that each group now has user assigned.

CloudAdmin

Delete

Summary

Edit

User group name	Creation time	ARN
CloudAdmin	April 25, 2023, 20:19 (UTC-05:00)	arn:aws:iam: [REDACTED] :group/CloudAdmin

Users

Permissions

Access Advisor

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.



Remove users

Add users

Search

< 1 > ⚙

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	billy.joe	1	None	52 minutes ago

AWS CloudAdmin Users Listing

Shows that the expected user has been created and assigned to the CloudAdmin group.

Finally, after the users have logged in, changed their passwords, and added an MFA device, we can see the results:

Users (5) [Info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.



Delete

Add users

Find users by username or access key

< 1 > ⚙

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password a...	Active key age
<input type="checkbox"/>	billy.joe	CloudAdmin	✓ 12 minutes ago	Virtual	✓ 12 minutes ago	-
<input type="checkbox"/>	jane.doe	DBA	Never	None	✓ 22 hours ago	-
<input type="checkbox"/>	jim.bob	LinuxAdmin	✓ 2 hours ago	None	✓ 2 hours ago	-
<input type="checkbox"/>	john.doe	NetworkAdmin	Never	None	✓ 22 hours ago	-
<input type="checkbox"/>	mary.sunshine	Trainees	✓ 3 hours ago	Virtual	✓ 3 hours ago	-

AWS Users Listing

Summary

We walked through creating an MFA policy in the AWS CloudShell and then executed the automated assignment of that policy and others during the User Group creation process. Then we walked through an automated user account creation process, including assigning the appropriate user groups.

If you face any issues while implementing these scripts, please get in touch with me on [LinkedIn](#). If you enjoyed reading this article or found it helpful, don't forget to click the like button or follow me.