

Practical 3

classmate

Date _____

Page _____

IAM user groups

- An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users which can make it easier to manage those users. For ex, if you have a user group called 'Admins' & give that user group typical administrator permissions. Any users in that user group automatically have 'Admins' group permission. If a new user joins your organization & needs administrator privileges you can assign the appropriate permissions by adding the user to the 'Admins' user group. If a person changes jobs in your organization, instead of editing that user's permissions you can remove them.
- You can attach identity-based policy to a user group so that all of the users in the user group receive the policy's permission. You cannot add identity a user group as a principal in a policy (such as resource based policy) because groups relate to permissions, not authentication.
- Some important characteristics of user group are
 - A user group can contain many users and a user belong to multiple user groups.

- 3) User groups can be nested, they can contain only users not other user groups.
- 4) There is no default user groups that automatically include all users in the AWS account. If you want to have a user group like that, you must create it & assign each new user to it.
- i) The number & size of IAM resources in an AWS account, such as the no. of groups & the no. of groups that a user can be a member of is limited.
- * USERS
- i) Root user:

The account owner with complete access to all AWS services & resources. You are the root user if you created the AWS account & you sign in using your root user email & password.

- ii) IAM identity center user:

A user whose AWS account is a part of AWS Organizations who signs in through the AWS access portal with a unique URL. These users can either be created directly in IAM identity center.

Q1] IAM user -

An identity within your AWS account that's granted specific custom permissions. You're an IAM user if you didn't create the AWS account & your administrator or help desk employee provided you your sign-in credentials that include an AWS account.

Q2] IAM

AWS identity & access management (IAM) is a web-service that helps you securely control access to AWS resources. With IAM, you can manage permission that control which AWS services users can access. You use IAM to control who is authenticated (signed in) & unauthorized (has permissions) to use resources.

Identities.

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services & resources in the account. This identity is called the AWS account root user & is accessed by signing in with an email ID & password.

Access Management.

After a user is setup in IAM, they will sign up credentials to authenticate with AWS authentication provided by matching the origin credentials to a principal (an IAM user, federated user, IAM role) trusted by the AWS account.

Next, a request is made to grant the principal access to resources.

For eg. when you first sign in to the console & on the console homepage,

you aren't accessing a specific service.

When you select a service, the request for authorization is sent to that service

& it looks to see if your identity is on the list of authorized users, what policies are being enforced to control the level of access.

Q3 IAM Roles.

An IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user in that it is an AWS identity with permission policies that determine what the identity can & cannot do in AWS.

However, instead of being uniquely associated with one person, a role has credentials such as a password or access key associated with it.

You can use roles to delegate access to more apps, or services that don't normally have access to your AWS resources. For eg- you might want to grant users in your AWS account access to resources they don't usually have or grant user in one AWS account access to resources in another account. Or you sometimes- you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or you access to your account to 3rd party so they can perform an audit on your resources.

Practical-3

IAM

Steps

1. Go to IAM

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar menu includes options like Dashboard, Access management, and Access reports. The main area displays security recommendations (Add MFA for root user, Root user has no active access keys), IAM resources (User groups: 0, Users: 1, Roles: 2, Policies: 1, Identity providers: 0), and a 'What's new' section. To the right, there's an 'AWS Account' summary with fields for Account ID (891377383675), Account Alias (Create), and Sign-in URL (https://891377383675.siginin.aws.amazon.com/console). A 'Quick Links' section and a 'Tools' section are also present.

2. Go to users and add a user

Specify user details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, ., @, _ (hyphen)

Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

3. Either auto generate the password or create custom password

Identity and Access Management (IAM)

teishaaaa

Summary

ARN arn:aws:iam::123456789012:root

Created August 03, 2023

Permissions

Console sign-in https://80

Enable console access

Autogenerated password

User must create new password at next sign-in

Cancel Enable console access

Multi-factor authentication (MFA) (0)

Remove Resync Assign MFA device

4. Use the gen URL and password

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/teishaaaa)section=security_credentials

Identity and Access Management (IAM)

Console access enabled.

teishaaaa

Summary

ARN arn:aws:iam::891377383675:user/teishaaaa

Created August 03, 2023

Console password

You have successfully enabled the user's new password. This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL https://891377383675.signin.aws.amazon.com/console

User name teishaaaa

Console password ***** Show

Download .csv file Close

Access key 1 Create access key

Manage console access

14:38 GMT+5:30

Multi-factor authentication (MFA) (0)

Remove Resync Assign MFA device

5.open a new window and use the generated credentials

ap-southeast-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=XoJ_gVMVsX... ☆ Incognito New Chrome available

Try the new sign in UI See our new improved Amazon Web Services sign in experience before we officially launch. Enable new sign in

aws

Sign in as IAM user

Account ID (12 digits) or account alias 891377383675

IAM user name teishaaaa

Password

Remember this account

Sign in

Sign in using root user email

Forgot password?

AWS re:Invent

Browse the 2024 session catalog to explore all the learning opportunities this year.

Browse catalog

DECEMBER 2-6, 2024 | LAS VEGAS, NEVADA

English

6. As of now, permissions are denied even though console is visible.

Console Home

Recently visited

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 RDS Lambda

View all services

Applications (0)

Create application

Region: Asia Pacific (Sydney)

ap-southeast-2 (Current Region) Find applications

Name Description Region Originating account

Access denied

Welcome to AWS

Getting started with AWS

Learn the fundamentals and find valuable information to

AWS Health

Cost and usage

Current month costs Cost breakdown

Access denied Access denied

Forecasted month end costs

Go to myApplications

Identity and Access Management (IAM)

Policies (1221)

A policy is an object in AWS that defines permissions.

Filter by Type

Policy name	Type	Used as	Description
AccessAnalyzerServ...	AWS managed	None	
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAcces...	AWS managed	None	Grants account administrative permis...
AdministratorAcces...	AWS managed	None	Grants account administrative permis...
AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFu...	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLif...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessPo...	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessRe...	AWS managed	None	Provide read only access to AlexaForB...

7. ^ go to policy and create policy, change SID to your created user

The screenshot shows the AWS IAM Policy Editor interface. On the left, there's a sidebar with 'Step 1 Specify permissions' and 'Step 2 Review and create'. The main area is titled 'Specify permissions' with a 'Info' link. Below it, a note says 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' A large text area contains the following JSON code:

```
1  {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "VisualEditor0",
6             "Effect": "Allow",
7             "Action": "s3:*",
8             "Resource": "*"
9         }
10    ]
11 }
```

To the right of the code, there are several panels: 'Edit statement' (with a 'Remove' button), 'Add actions' (with a 'Choose a service' dropdown and a 'Filter services' search bar), 'Included' (listing S3), 'Available' (listing AMP, API Gateway, API Gateway V2, ASC, Access Analyzer, Account), and an 'Add a resource' section with an 'Add' button.

8. Name the policy and add description

The screenshot shows the 'Review and create' step of the policy creation process. It has 'Step 1 Specify permissions' and 'Step 2 Review and create' in the sidebar. The main area is titled 'Review and create' with an 'Info' link. It says 'Review the permissions, specify details, and tags.' Below that is a 'Policy details' section with fields for 'Policy name' (containing 'policy_for_teisha') and 'Description - optional' (containing 'granted s3 services').

At the bottom, there's a 'Permissions defined in this policy' section with an 'Edit' button. It says 'Permissions defined in this policy' with an 'Info' link. It notes 'Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.' A search bar is available. Below is a table titled 'Allow (1 of 420 services)' with a 'Show remaining 419 services' link. The table columns are Service, Access level, Resource, and Request condition. One row is shown for 'S3' with 'Full access' as the access level and 'All resources' as the resource.

9. Attach the created policy

Add permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1224)

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	0
AdministratorAccess	AWS managed - job function	0
AdministratorAccess-Amplify	AWS managed	0
AdministratorAccess-AWSElastic...	AWS managed	0

10. Attach the policy the user

Add permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1224)

Policy name	Type	Attached entities
policy_for_teisha	Customer managed	0

Cancel **Next**

S3 permission has been granted!

Identity and Access Management (IAM)

policy_for_teisha Info

granted s3 services

Policy details

Type Customer managed	Creation time August 03, 2024, 14:46 (UTC+05:30)	Edited time August 03, 2024, 14:46 (UTC+05:30)	ARN arn:aws:iam::891377383675:policy/policy_for_teisha
--------------------------	---	---	---

Permissions Entities attached Tags Policy versions (1) Access Advisor

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Service	Access level	Resource	Request condition
S3	Full access	All resources	None

11. Open the account using user credentials again and we can see s3 permissions have been granted as a bucket is now created for user “teishaaa”

Amazon S3 > Buckets

Account snapshot - updated every 24 hours All AWS Regions

To upload files and folders, or to configure additional bucket settings, choose View details.

General purpose buckets Directory buckets

General purpose buckets (3) Info All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
bucketnumberoneog	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	July 27, 2024, 15:57:13 (UTC+05:30)
bucky1111	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	August 3, 2024, 13:41:08 (UTC+05:30)
teishabucket	Asia Pacific (Sydney) ap-southeast-2	View analyzer for ap-southeast-2	August 3, 2024, 14:57:42 (UTC+05:30)

Create buckets and folders as required.