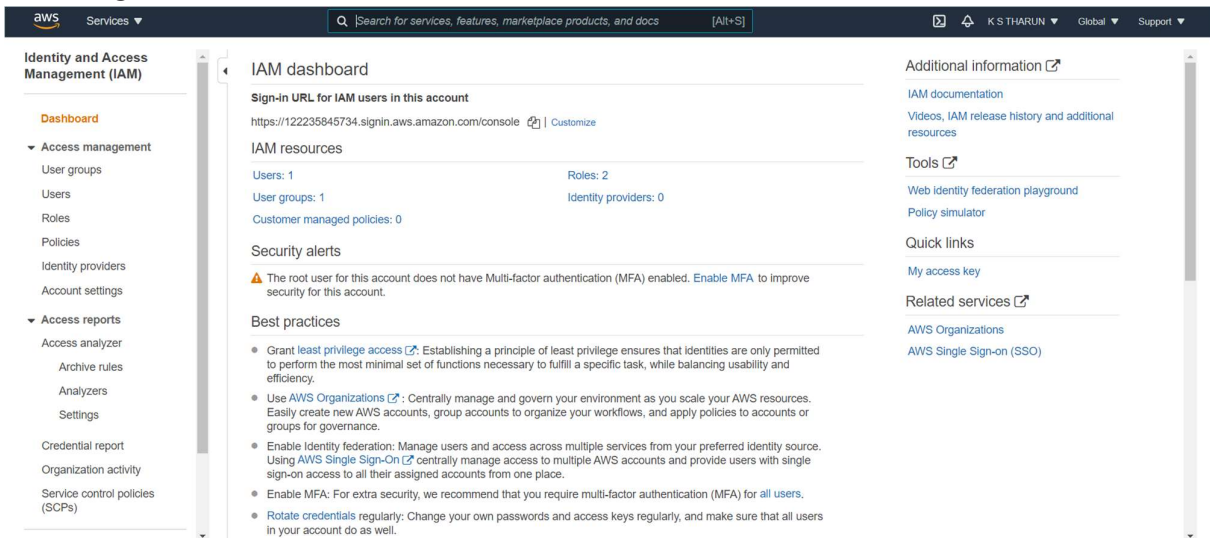


AWS Cloud Computing Zero to Hero

Assignment – 1

➤ Working with IAM

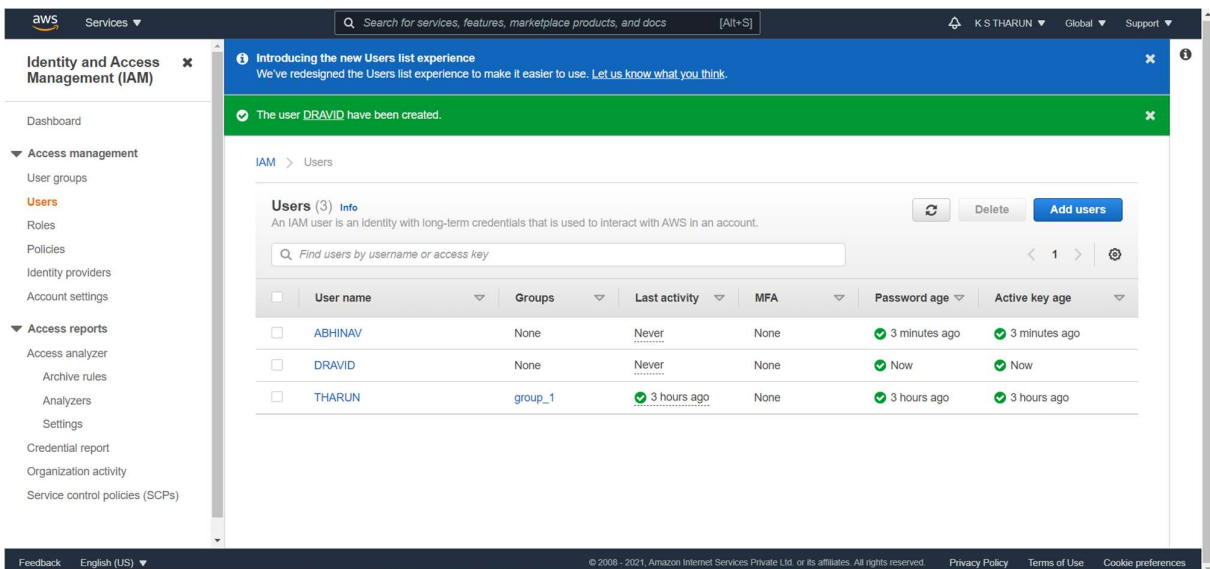


The screenshot shows the AWS IAM dashboard. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area displays the 'IAM dashboard' with a sign-in URL, IAM resources (Users: 1, Roles: 2, User groups: 1, Identity providers: 0, Customer managed policies: 0), Security alerts (warning about MFA), and Best practices (Grant least privilege access, Use AWS Organizations, Enable Identity federation, Use AWS Single Sign-On, Enable MFA, Rotate credentials).

➤ Create 3 Users

○ USERS

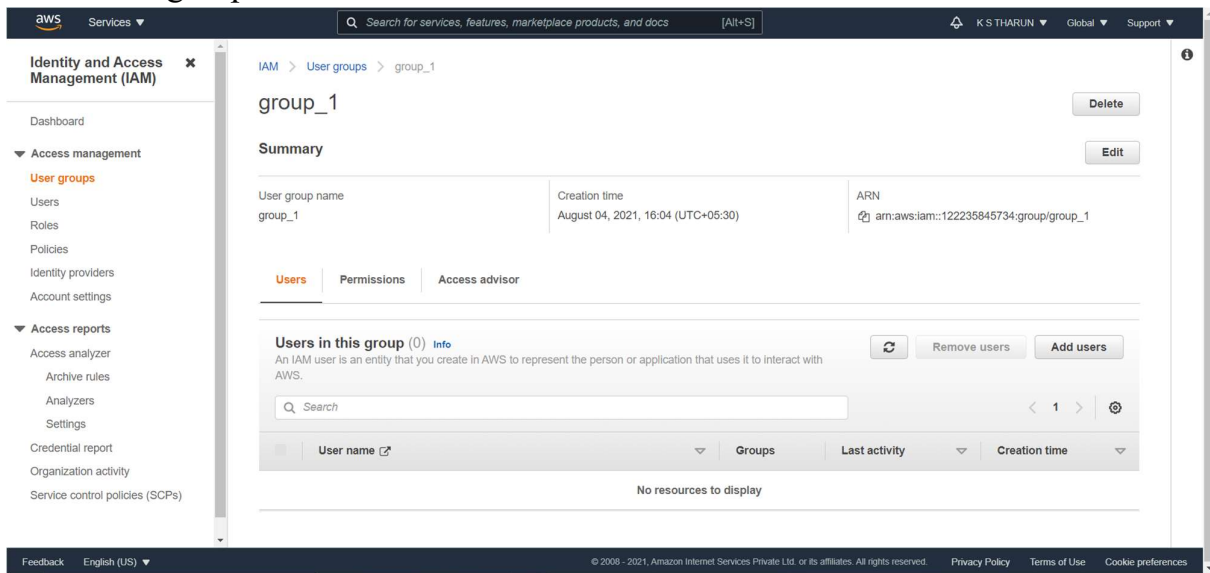
- THARUN
- ABHINAV
- DRAVID



The screenshot shows the AWS IAM 'Users' list page. A green notification banner at the top states 'The user DRAVID have been created.' Below the banner, the 'Users (3)' section shows a table of users. The table has columns for User name, Groups, Last activity, MFA, Password age, and Active key age. The users listed are ABHINAV, DRAVID, and THARUN.

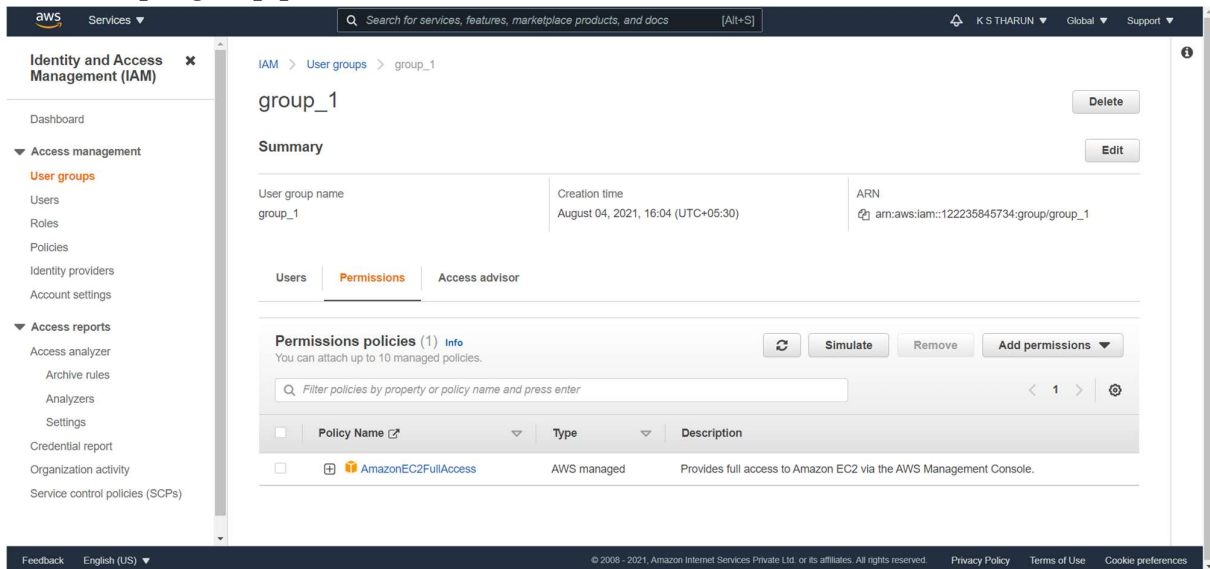
	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	ABHINAV	None	Never	None	3 minutes ago	3 minutes ago
<input type="checkbox"/>	DRAVID	None	Never	None	Now	Now
<input type="checkbox"/>	THARUN	group_1	3 hours ago	None	3 hours ago	3 hours ago

➤ Create one group



The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area displays the 'group_1' user group page. The 'Summary' section shows the user group name 'group_1', creation time 'August 04, 2021, 16:04 (UTC+05:30)', and ARN 'arn:aws:iam::122235845734:group/group_1'. The 'Users' tab is selected, showing 'Users in this group (0)'. Below this, there is a search bar and a table with columns: User name, Groups, Last activity, and Creation time. The table is empty, displaying 'No resources to display'.

➤ Set a unique group permission



The screenshot shows the AWS IAM console interface, similar to the previous one, but with the 'Permissions' tab selected. The 'Summary' section remains the same. The 'Permissions' tab shows 'Permissions policies (1)'. Below this, there is a search bar and a table with columns: Policy Name, Type, and Description. The table contains one entry: 'AmazonEC2FullAccess' (AWS managed) with the description 'Provides full access to Amazon EC2 via the AWS Management Console.'.

➤ Set user permissions

○ THARUN

The screenshot shows the AWS IAM console for user THARUN. The left sidebar lists navigation options under 'Identity and Access Management (IAM)', including Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'Summary' and displays user details: User ARN (arn:aws:iam::122235845734:user:THARUN), Path (/), and Creation time (2021-08-04 20:09 UTC+0530). Below this, the 'Permissions' tab is active, showing 'Permissions policies (2 policies applied)'. A table lists the attached policies: 'AmazonEC2FullAccess' and 'IAMUserChangePassword', both identified as 'AWS managed policy'. There are buttons for 'Add permissions' and 'Add inline policy'. A section for 'Permissions boundary (not set)' and a 'Generate policy based on CloudTrail events' option are also visible. The footer includes a feedback link, language selection (English (US)), and copyright information.

Summary

User ARN: arn:aws:iam::122235845734:user:THARUN
Path: /
Creation time: 2021-08-04 20:09 UTC+0530

Permissions

Permissions policies (2 policies applied)

Add permissions Add inline policy

Policy name	Policy type
Attached directly	
AmazonEC2FullAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

○ ABHINAV

The screenshot shows the AWS IAM console for user ABHINAV. The interface is identical to the THARUN user page, displaying the same navigation sidebar and 'Summary' section with user details (arn:aws:iam::122235845734:user:ABHINAV, creation time 2021-08-04 20:00 UTC+0530). The 'Permissions' tab shows the same two attached policies: 'AmazonEC2FullAccess' and 'IAMUserChangePassword', both as 'AWS managed policy'. The 'Permissions boundary (not set)' and 'Generate policy based on CloudTrail events' sections are also present.

Summary

User ARN: arn:aws:iam::122235845734:user:ABHINAV
Path: /
Creation time: 2021-08-04 20:00 UTC+0530

Permissions

Permissions policies (2 policies applied)

Add permissions Add inline policy

Policy name	Policy type
Attached directly	
AmazonEC2FullAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy

Permissions boundary (not set)

Generate policy based on CloudTrail events

○ DRAVID

The screenshot shows the AWS IAM console for user DRAVID. The interface is identical to the previous two user pages, displaying the same navigation sidebar and 'Summary' section with user details (arn:aws:iam::122235845734:user:DRAVID, creation time 2021-08-04 20:03 UTC+0530). The 'Permissions' tab shows the same two attached policies: 'AmazonEC2FullAccess' and 'IAMUserChangePassword', both as 'AWS managed policy'. The 'Permissions boundary (not set)' and 'Generate policy based on CloudTrail events' sections are also present.

Summary

User ARN: arn:aws:iam::122235845734:user:DRAVID
Path: /
Creation time: 2021-08-04 20:03 UTC+0530

Permissions

Permissions policies (2 policies applied)

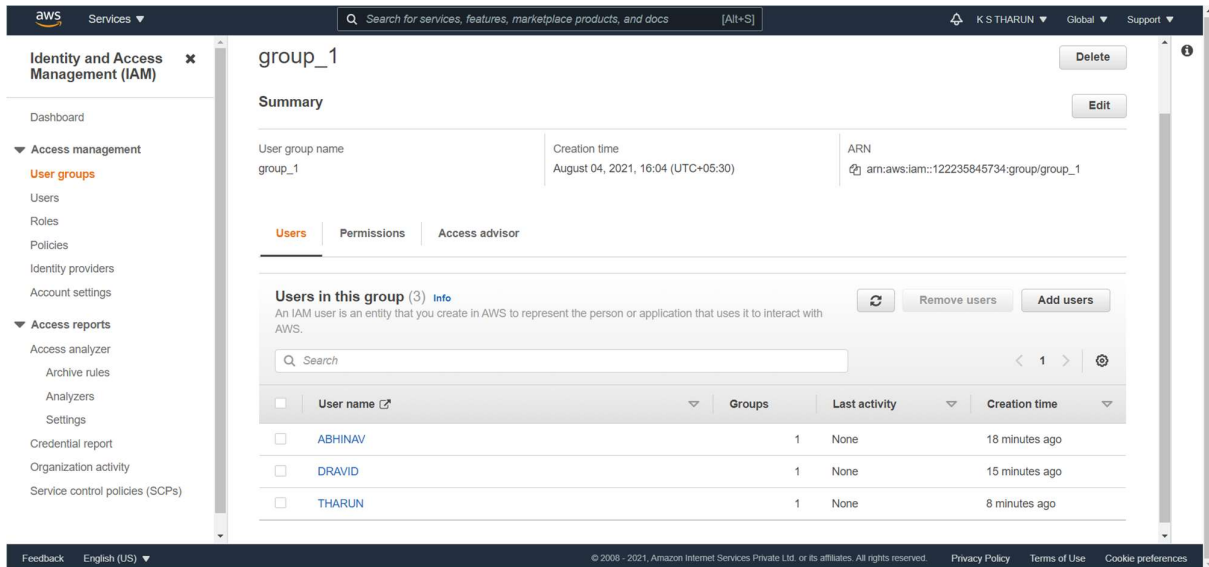
Add permissions Add inline policy

Policy name	Policy type
Attached directly	
AmazonEC2FullAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy

Permissions boundary (not set)

Generate policy based on CloudTrail events

➤ Add users to group

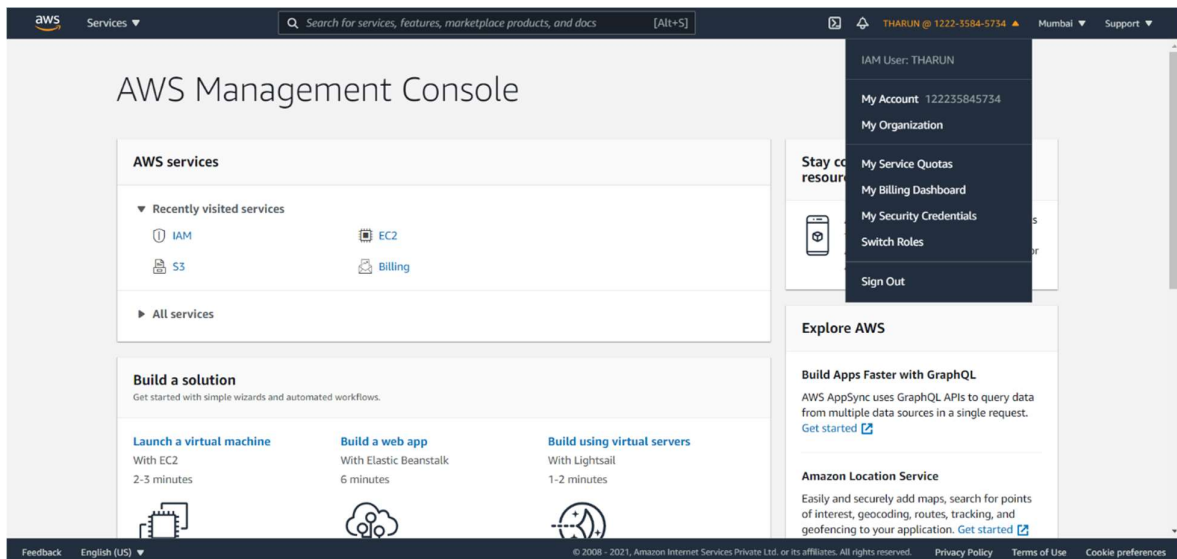


The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with options like Dashboard, Access management, and Access reports. The main content area displays the 'group_1' user group. The 'Summary' section shows the group name, creation time (August 04, 2021, 16:04 UTC+05:30), and ARN. Below this, the 'Users' tab is active, showing a list of three users: ABHINAV, DRAVID, and THARUN. The 'Add users' button is visible in the top right of the users list.

User name	Groups	Last activity	Creation time
ABHINAV	1	None	18 minutes ago
DRAVID	1	None	15 minutes ago
THARUN	1	None	8 minutes ago

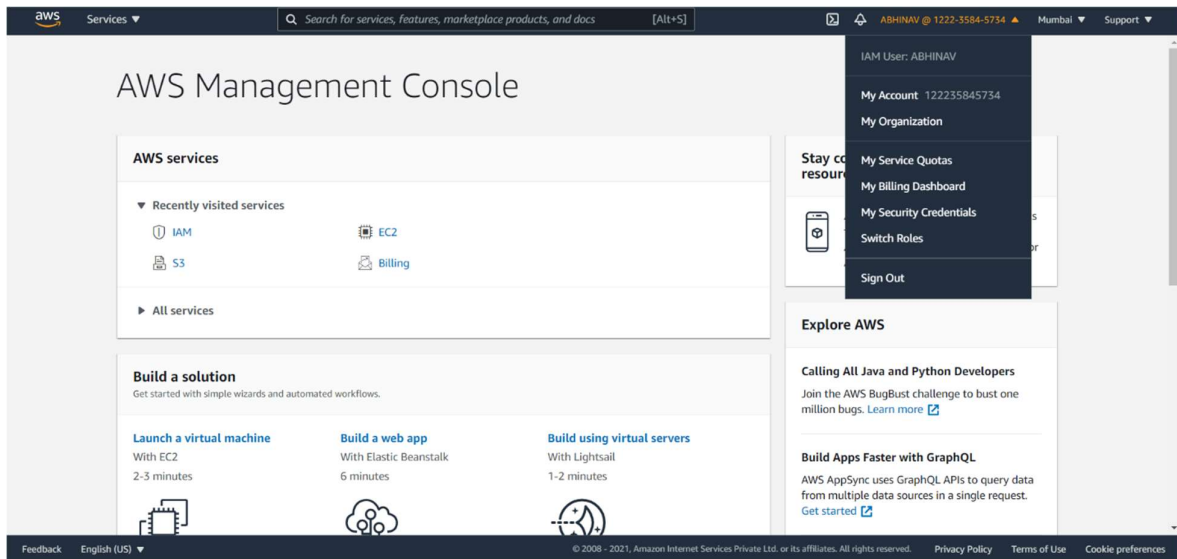
➤ Login as the IAM user.

- THARUN

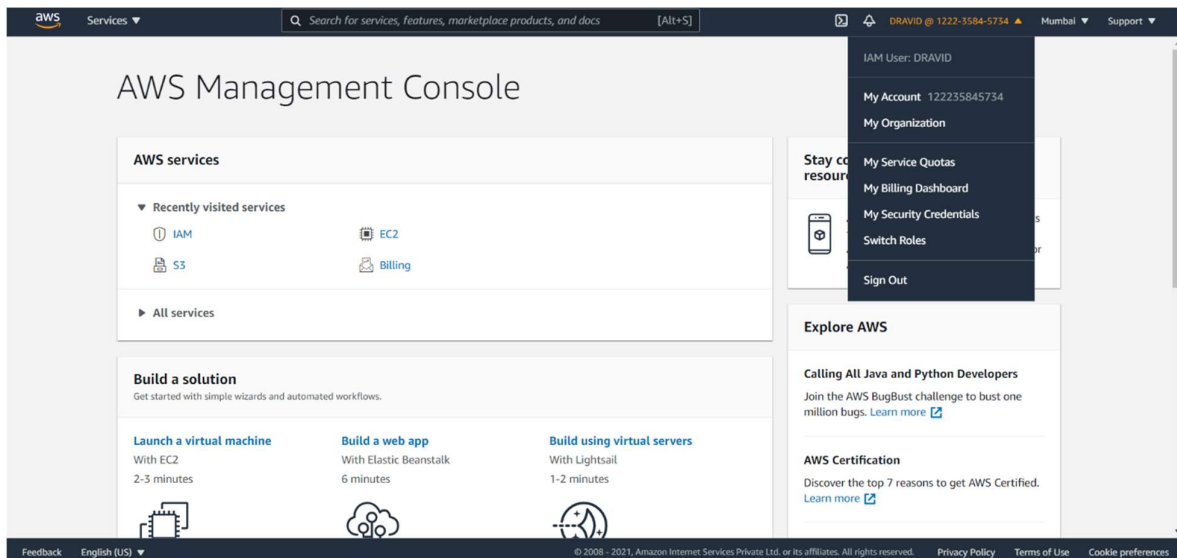


The screenshot shows the AWS Management Console interface. The top navigation bar displays the user profile 'THARUN @ 1222-5584-5734' with a dropdown menu. The dropdown menu includes options like 'My Account', 'My Organization', 'My Service Quotas', 'My Billing Dashboard', 'My Security Credentials', 'Switch Roles', and 'Sign Out'. The main content area shows the 'AWS services' section with 'Recently visited services' (IAM, EC2, S3, Billing) and 'All services'. Below this, the 'Build a solution' section offers quickstart guides for launching a virtual machine, building a web app, and building using virtual servers.

○ ABHINAV



○ DRAVID



- Show that the user permission and the group permissions are applied.
- User permission for THARUN

The screenshot shows the AWS Management Console for the Mumbai region. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main content area is divided into several sections: Resources (listing EC2 resources), Launch instance (with a 'Launch instance' button), Service health (showing 'This service is operating'), Account attributes (showing VPC details), and Explore AWS (showing a 'Build a Containerized Web Application' card).

- Group permission for THARUN

The screenshot shows the AWS Management Console for the Amazon S3 service. The left sidebar contains navigation links for Buckets, Access Points, Object Lambda Access Points, Batch Operations, Access analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main content area is divided into several sections: Account snapshot (showing 'Storage lens provides visibility into storage usage and activity trends'), Buckets (showing 'No buckets' and 'You don't have any buckets'), and Storage Lens (showing 'Dashboards' and 'AWS Organizations settings').

○ User permission for ABHINAV

The screenshot shows the AWS Management Console for user ABHINAV. The left sidebar displays the navigation menu with categories like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main content area is titled 'Resources' and shows a table of Amazon EC2 resources in the Asia Pacific (Mumbai) Region. The table includes columns for resource type and count. A 'Launch instance' button is visible at the bottom. The right sidebar shows 'Account attributes' and 'Explore AWS' sections.

Resources	
Instances (running)	0
Elastic IPs	0
Key pairs	0
Placement groups	0
Snapshots	0
Dedicated Hosts	0
Instances	0
Load balancers	0
Security groups	1
Volumes	0

○ Group permission for THARUN

The screenshot shows the AWS Management Console for user THARUN, specifically the Amazon S3 console. The left sidebar displays the navigation menu with categories like Buckets, Access Points, and Storage Lens. The main content area is titled 'Buckets (0)' and shows a table of S3 buckets. The table includes columns for Name, AWS Region, Access, and Creation date. A 'Create bucket' button is visible at the bottom. The right sidebar shows 'Account snapshot' and 'View Storage Lens dashboard' sections.

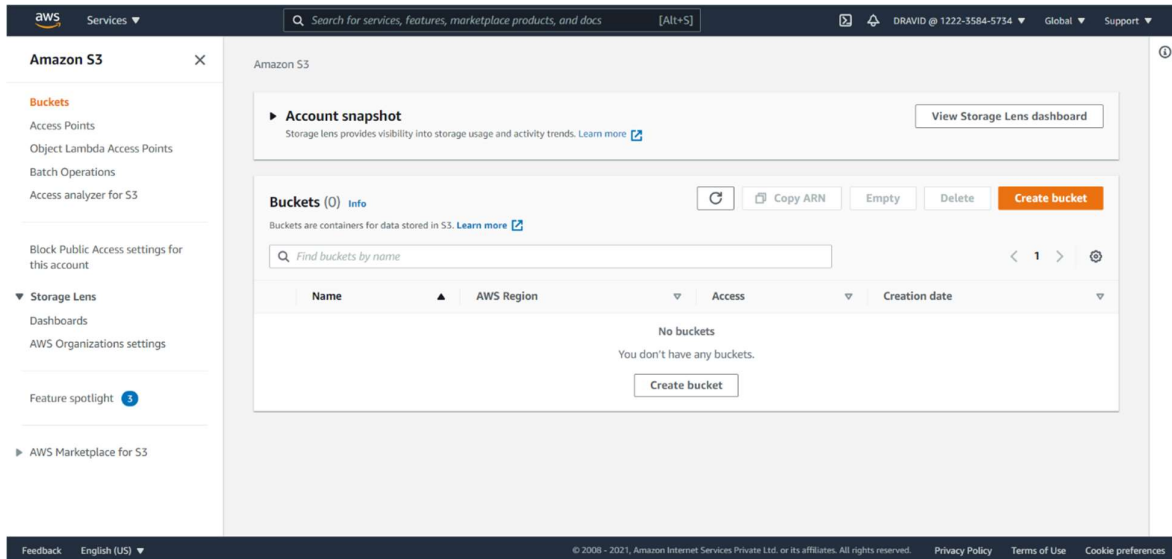
Name	AWS Region	Access	Creation date
No buckets			

○ User permission for DRAVID

The screenshot shows the AWS Management Console for user DRAVID. The left sidebar displays the navigation menu with categories like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main content area is titled 'Resources' and shows a table of Amazon EC2 resources in the Asia Pacific (Mumbai) Region. The table includes columns for resource type and count. A 'Launch instance' button is visible at the bottom. The right sidebar shows 'Account attributes' and 'Explore AWS' sections.

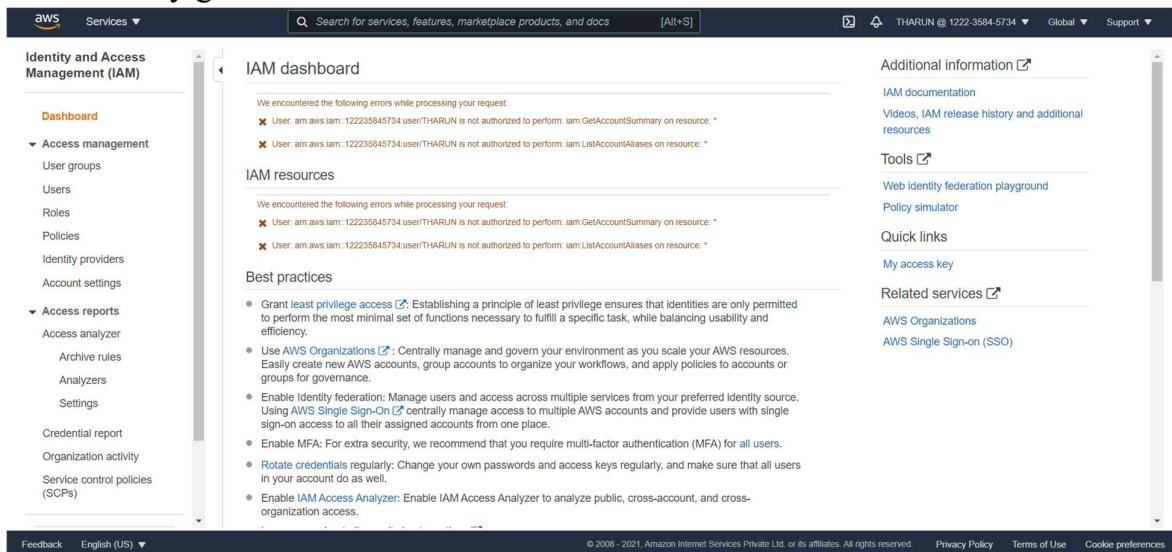
Resources	
Instances (running)	0
Elastic IPs	0
Key pairs	0
Placement groups	0
Snapshots	0
Dedicated Hosts	0
Instances	0
Load balancers	0
Security groups	1
Volumes	0

○ Group permission for THARUN

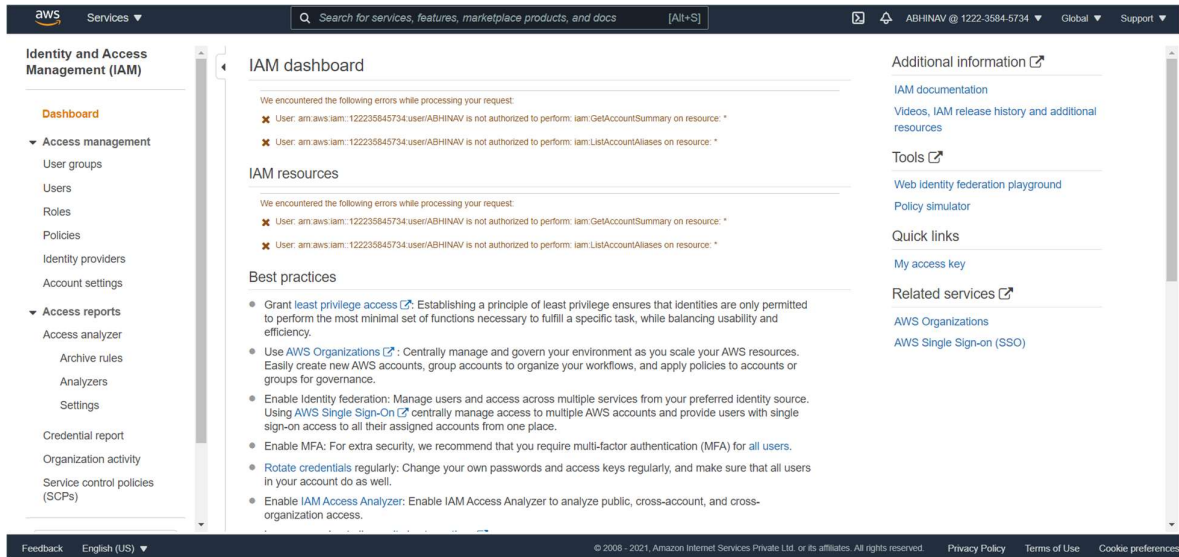


➤ Check which policy gives access to IAM.

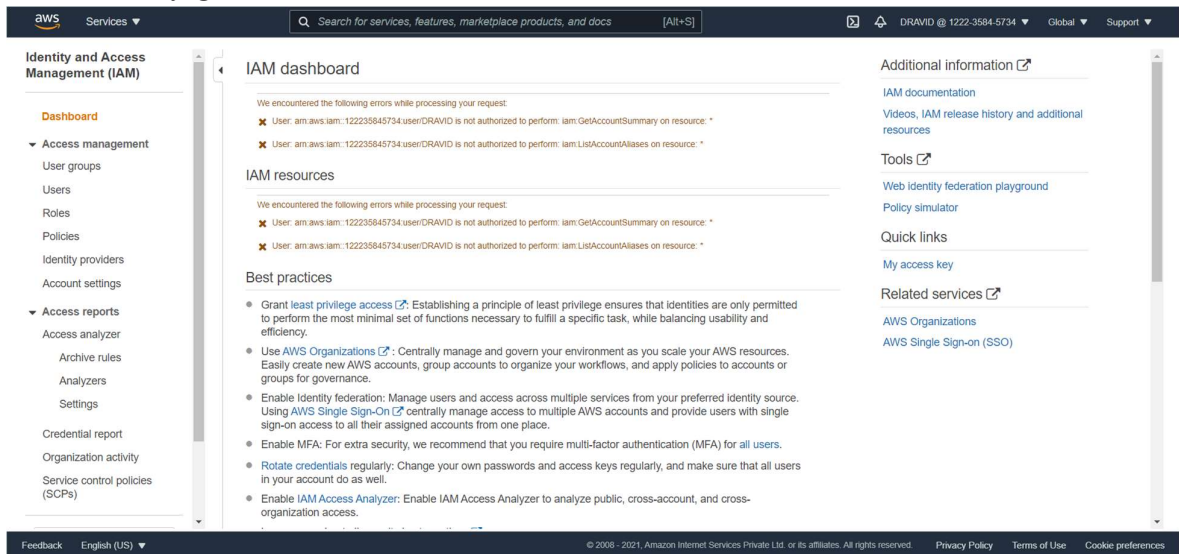
○ Policy given access to IAM for user THARUN



○ Policy given access to IAM for user ABHINAV



○ Policy given access to IAM for user DRAVID



To allow console users to simulate policies for users

Include the following actions in your policy:

- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAttachedUserPolicies
- iam:ListGroupsForUser
- iam:ListGroupPolicies

- iam:ListUserPolicies
- iam:ListUsers

To allow console users to simulate policies for user groups

Include the following actions in your policy:

- iam:GetGroup
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:ListAttachedGroupPolicies
- iam:ListGroupPolicies
- iam:ListGroups