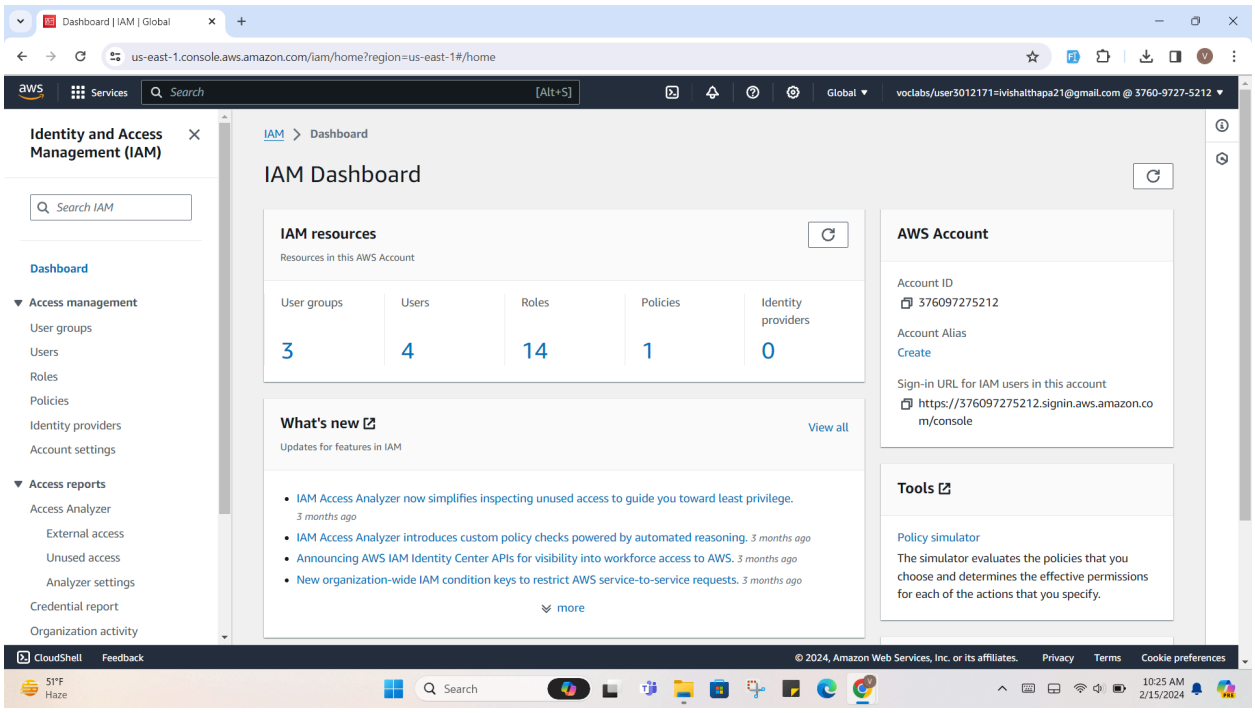
4. IAM Users and Roles Lab:

Objective:
The objective of this lab is to gain the understanding of AWS IAM by creating and managing users, groups, and roles.

Steps involved:

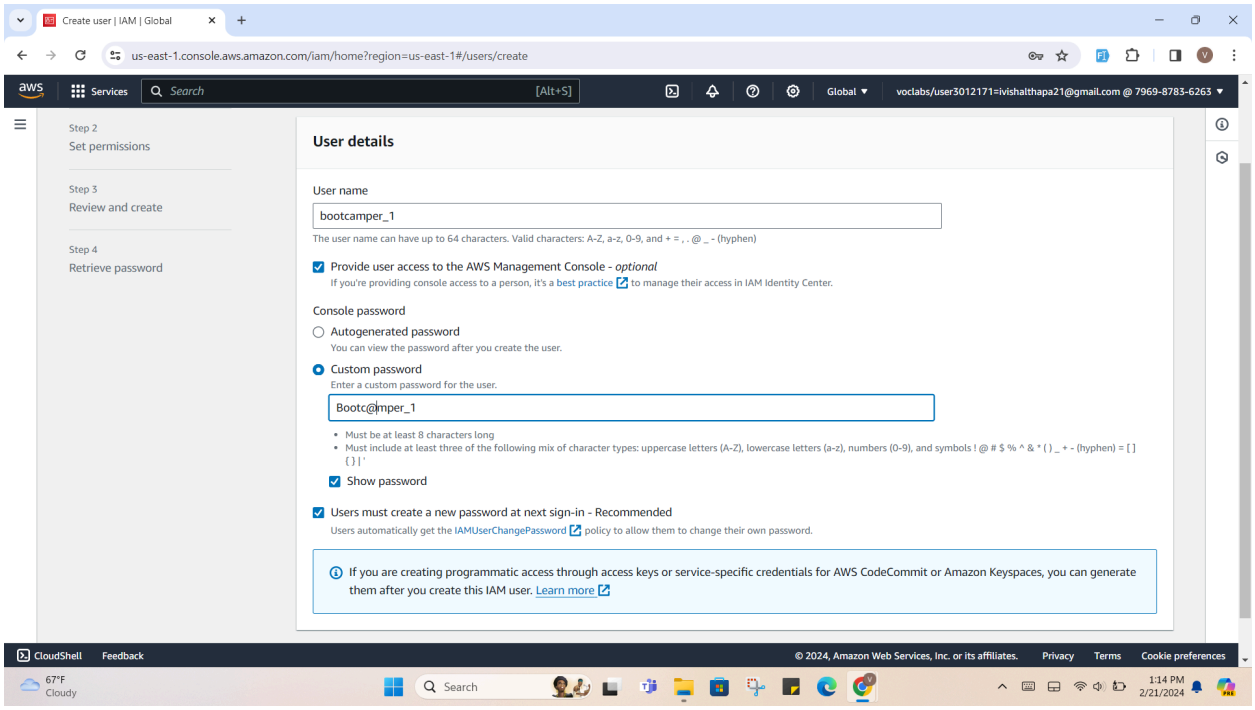
I. Access the IAM Dashboard:

a. Once signed in, locate and select the “IAM” service from the list of available services which will send us to the IAM dashboard.



II. Create IAM Users:

a. In the IAM dashboard, select “Users” from the left-hand menu.
b. Click on “Add user” button
c. Enter a username for the new IAM user
d. Choose the access type
e. Set the user’s permissions: we can either add the user to an existing group with predefined permissions or attach policies directly to the user.
f. Click “Next” to review our choices and then “Create user” to create the IAM user



III. Create IAM Groups:

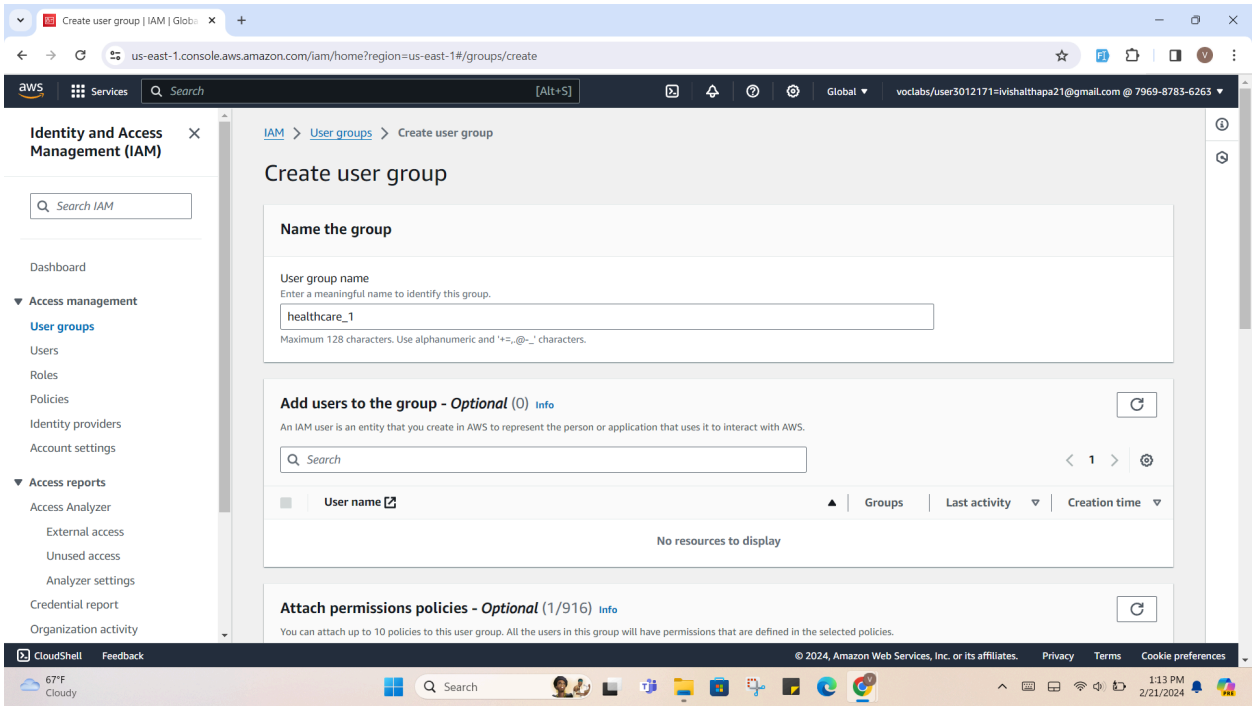
a. In the IAM dashboard, select “Groups” from the left-hand menu

b. Click on “Create Group” button

c. Enter a name for the group and add a description (Optional)

d. Attach policies to the group to define its permissions

e. Click “Create group” to create the IAM group

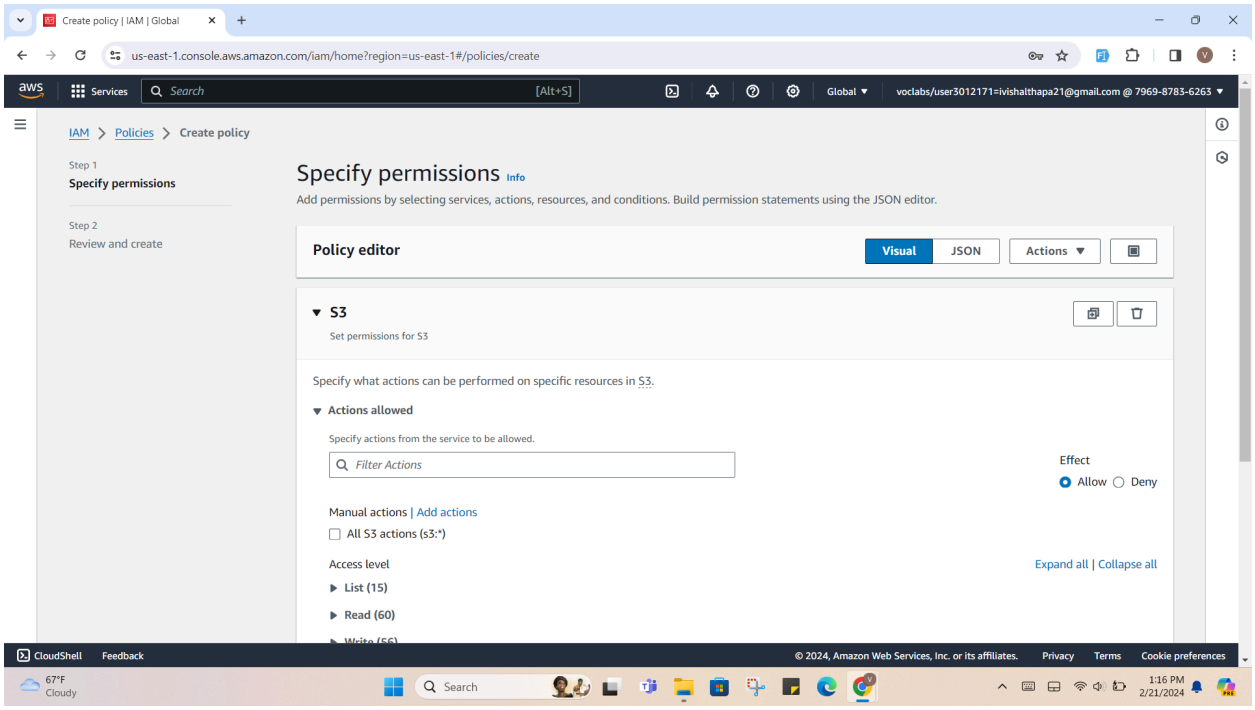


IV. Assign IAM Users to Groups:

a. In the IAM dashboard, select “Users” from the navbar
b. Select the IAM user we want to add to a group
c. Click on “Add user to group” button
d. Select the group/groups we want to add to user
e. Click “Add to groups” to assign the user to the selected group/groups.

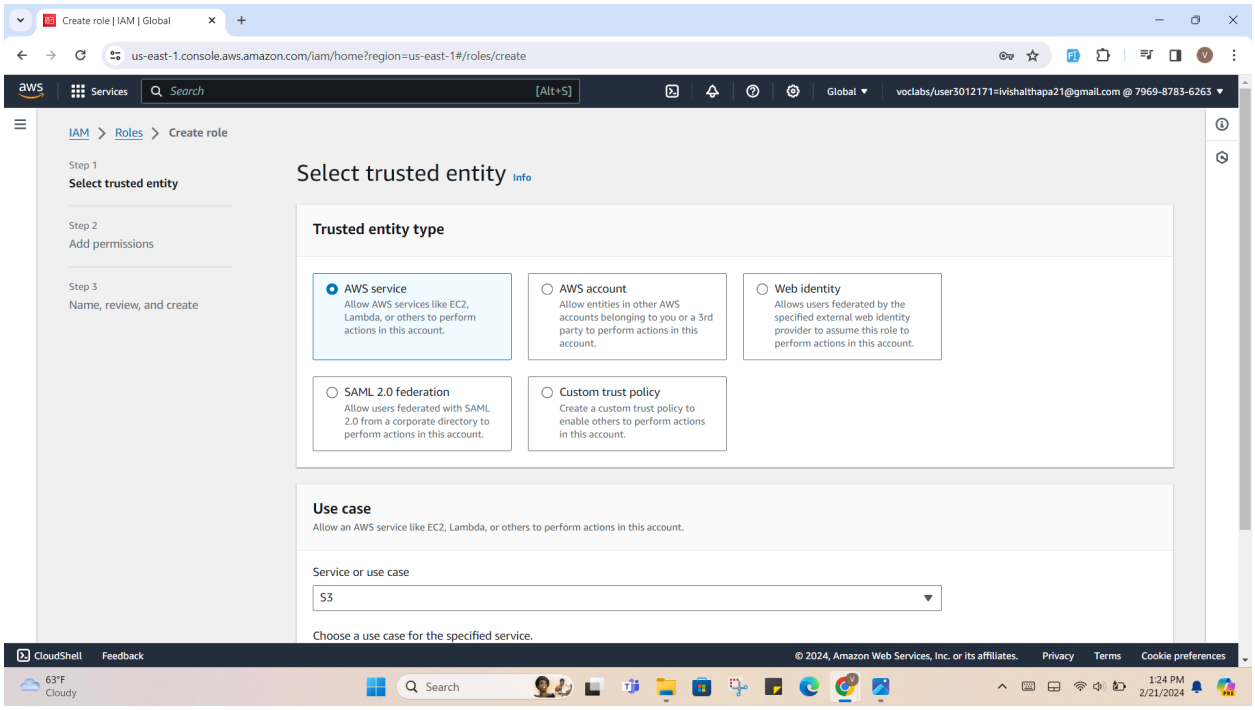
V. Apply IAM policies to Users and Groups:

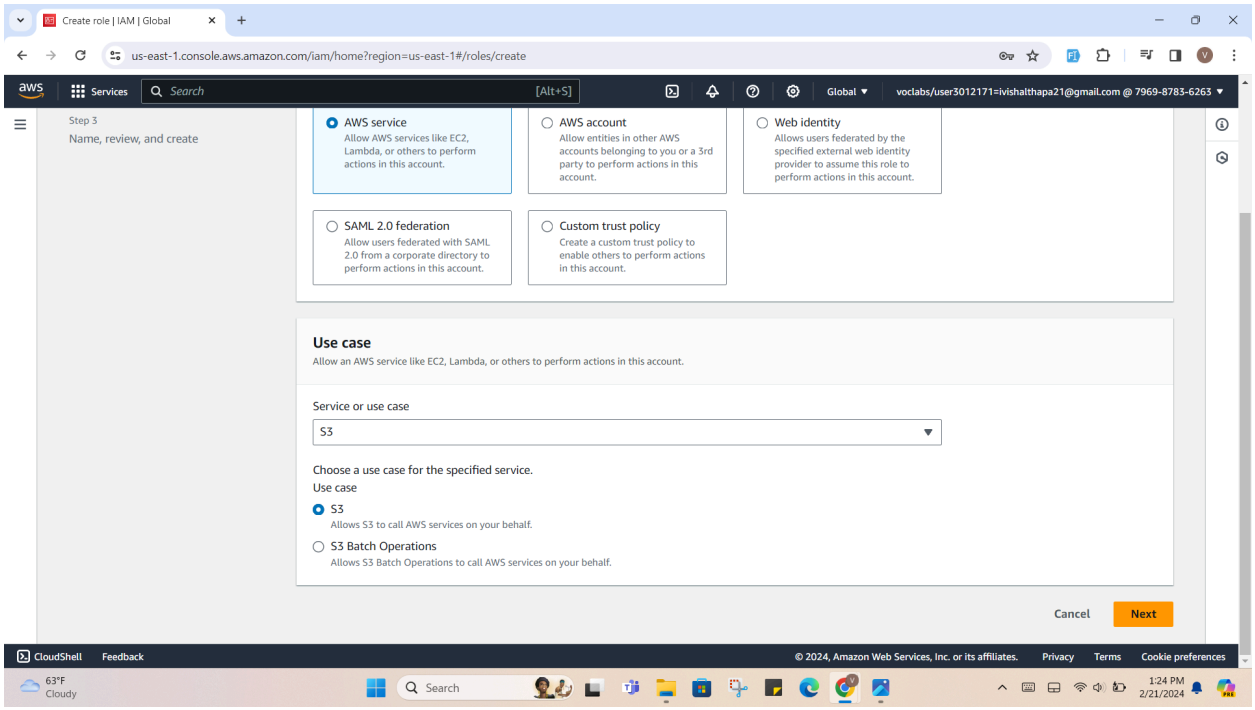
a. In the IAM dashboard, navigate to the “Policies” section
b. Choose whether to create a custom policy or use existing one
c. Attach the policy to IAM users or groups by selecting them and clicking on “Attach Policy”



VI. Create IAM Roles:

a. In the IAM dashboard, select “Roles” from the navbar
b. Click on “Create role” button
c. Choose the trusted entity type (i.e. AWS Service)
d. Select the service that will use this role
e. Attach a policies to define the permissions for the role
f. Click “Create role” to create the IAM role.


Create role | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
Services
Search
[Alt+S]
Global
voclabs/user3012171=ivishalthapa21@gmail.com @ 7969-8783-6263
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
S3
Choose a use case for the specified service.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
63°F
Cloudy
Search
1:24 PM
2/21/2024


Create role | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
Services
Search
[Alt+S]
Global
voclabs/user3012171=ivishalthapa21@gmail.com @ 7969-8783-6263
Step 3
Name, review, and create
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
S3
Choose a use case for the specified service.
Use case
S3
Allows S3 to call AWS services on your behalf.
S3 Batch Operations
Allows S3 Batch Operations to call AWS services on your behalf.
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
63°F
Cloudy
Search
1:24 PM
2/21/2024