Practical 3

IAM user groups.

— An IAM user group is a collection of IAM user. User groups let you specify permissions for multiple users which can make it easier to make & manage the permissions for those users. For ex, you have a user group called 'Admins' & give that user group typical administrator permissions. Any users in that user group automatically has 'Admins' group permission. If a new user joins your organization & needs administrator privileges you can assign the appropriate permissions by addition of the user to the 'admins' user groups. If a person changes jobs in your organization, instead of editing that user's permissions you can remove them.

— You can attach an identity-based policy to a user group so that all of the users in the user group receive the policy's permission. You cannot identify 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.

2] Users groups can be nested, they can contain only users not other user groups

3] 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 ~~the~~ create it & assign each new user to it.

4] 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 no. of are limited.

* USERS :

1] 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 organization who signs in through the AWS access portal with a unique URL. These users can either be created directly in IAM identity center.

11] 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 resources users can access. You use IAM to control who is authenticated (signed in) & authorized (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 email ID & password.

Access Management.

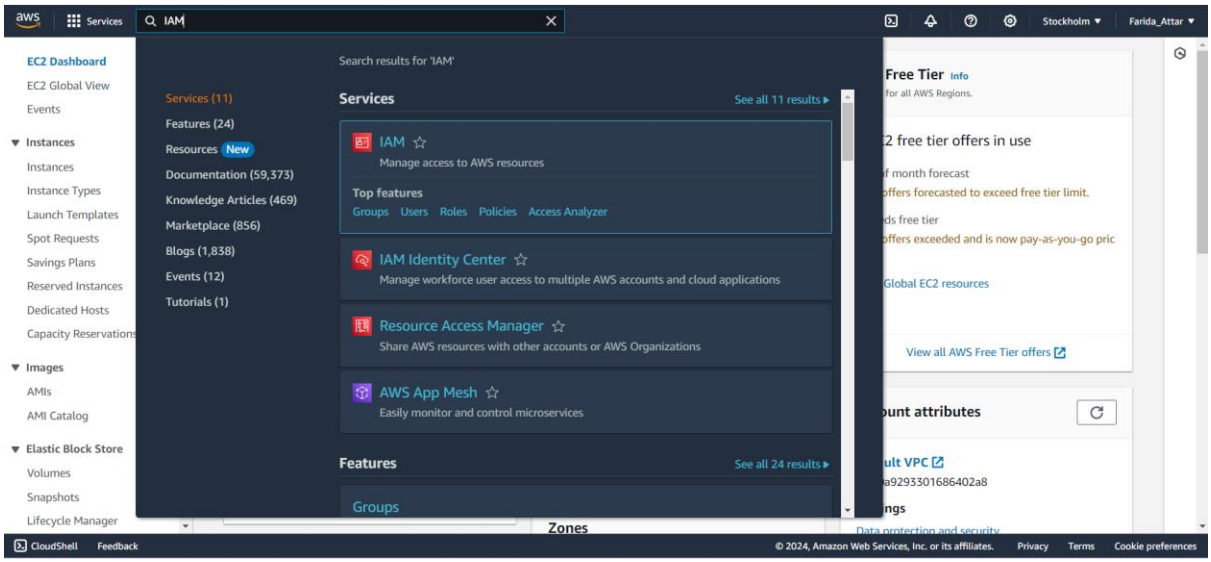
After a user is setup in IAM, they use their sign up credentials to authenticate & with AWS. Authentication provided by matching the sign in credentials to a principal (an IAM user, federated user, IAM role) trusted by the AWS account. Next, a request is made to grant the principal access to resources.
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.

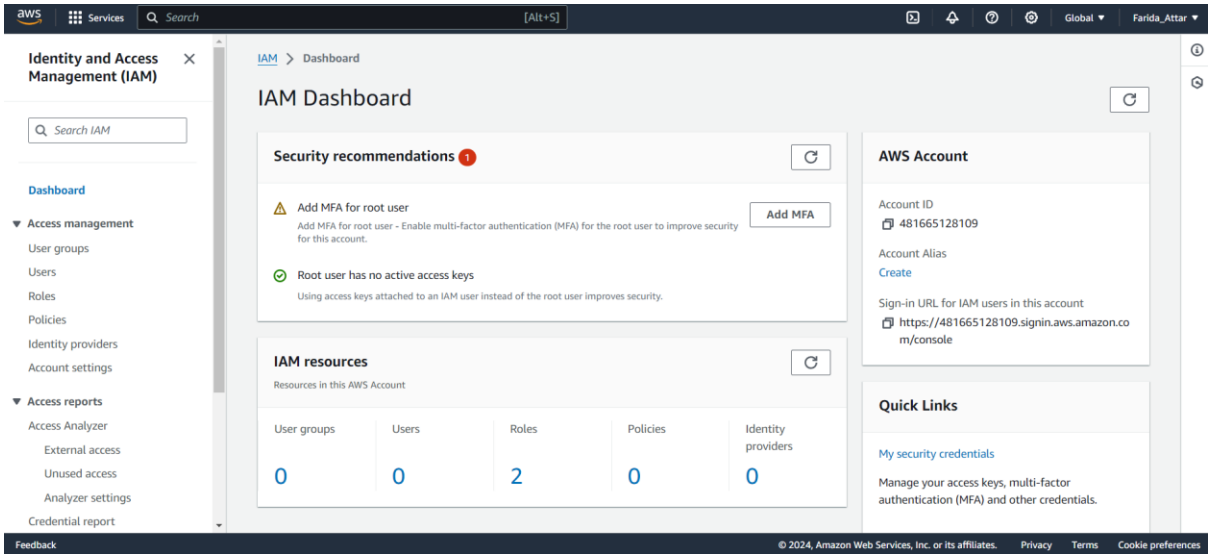
Q3 IAM Roles.

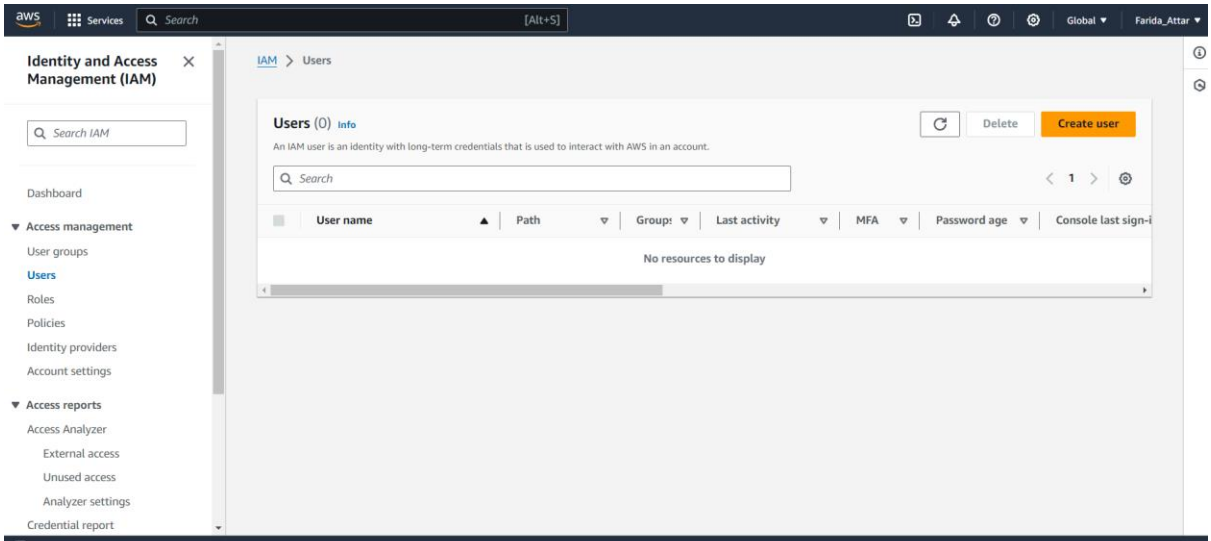
An IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can & cannot do in AWS. However, instead of being uniquely associated with one person, a role credentials such as a password or access key associated with it.

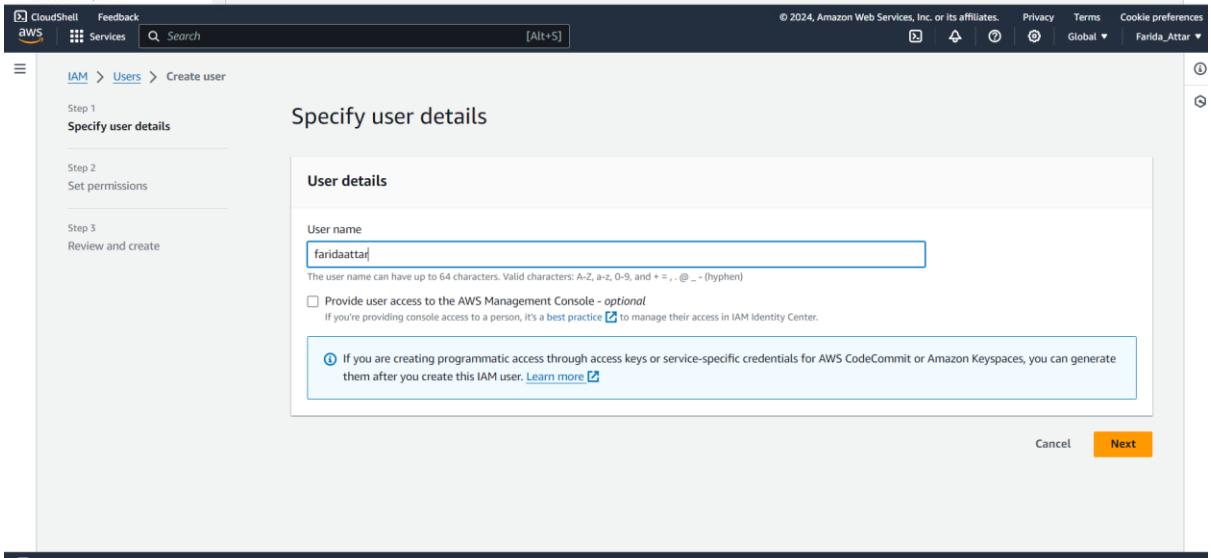
You can use roles to delegate access to users apps, or services that don't normally have access to your AWS resources. For eg. you might want to grant users in your AWS account access to resources they don't usually have or grant users in one AWS account access to resources in another account. Or you 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.

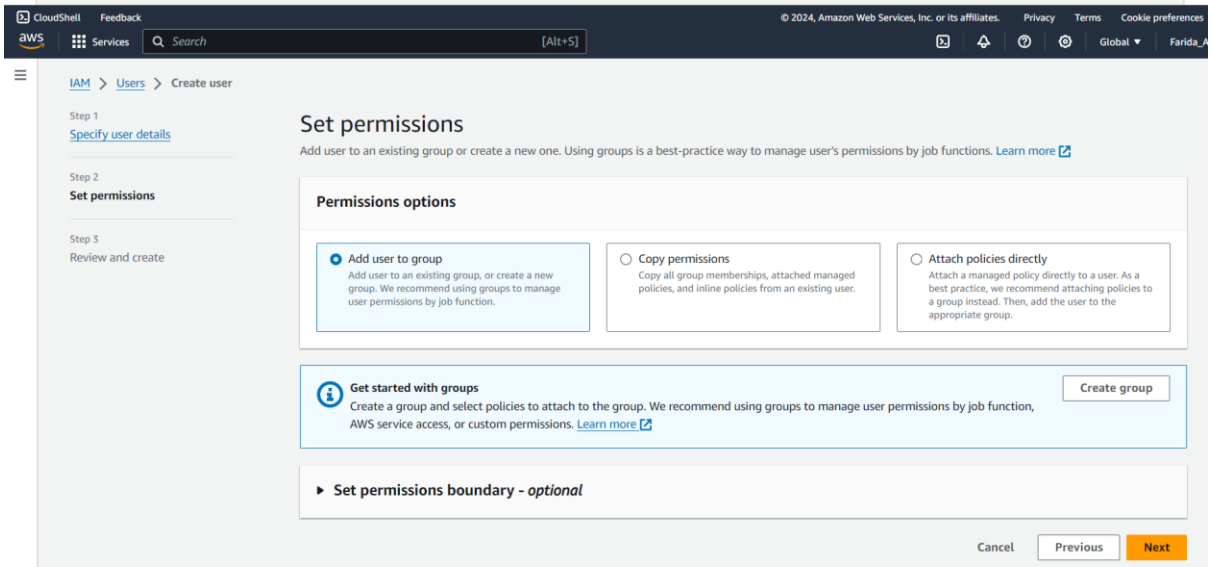
CC_prac3

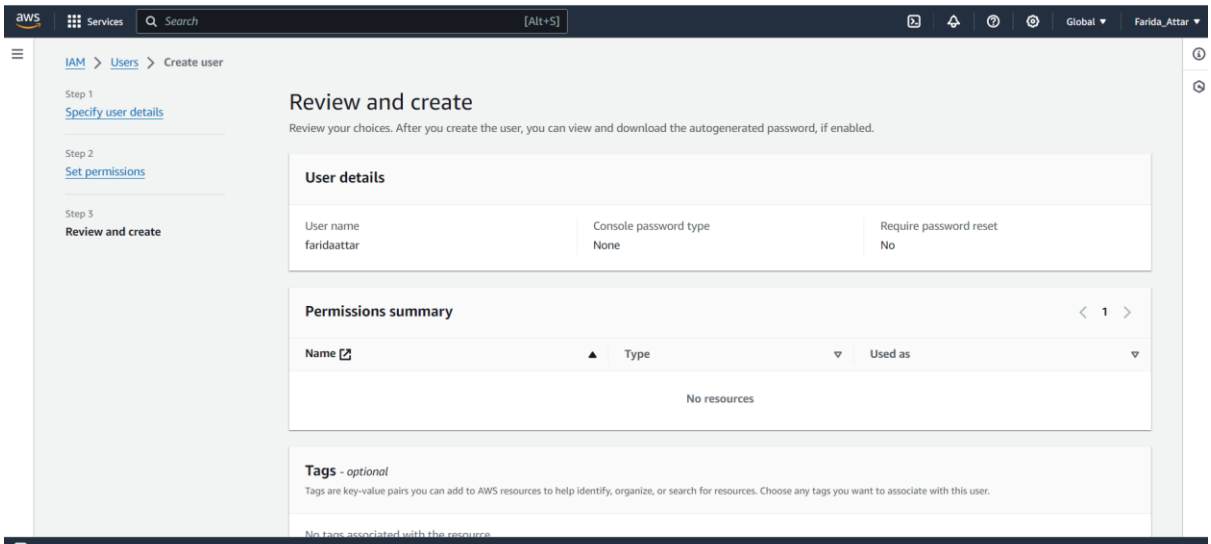

aws
Services
IAM
Stockholm
Farida_Attar
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Search results for 'IAM'
Services (11)
Features (24)
Resources New
Documentation (59,373)
Knowledge Articles (469)
Marketplace (856)
Blogs (1,838)
Events (12)
Tutorials (1)
Services
See all 11 results
IAM
Manage access to AWS resources
Top features
Groups Users Roles Policies Access Analyzer
IAM Identity Center
Manage workforce user access to multiple AWS accounts and cloud applications
Resource Access Manager
Share AWS resources with other accounts or AWS Organizations
AWS App Mesh
Easily monitor and control microservices
Features
See all 24 results
Groups
Zones
Free Tier Info
for all AWS Regions.
2 free tier offers in use
f month forecast
offers forecasted to exceed free tier limit.
ds free tier
offers exceeded and is now pay-as-you-go pric
Global EC2 resources
View all AWS Free Tier offers
ount attributes
ult VPC
a9293301686402a8
ngs
Data protection and security
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

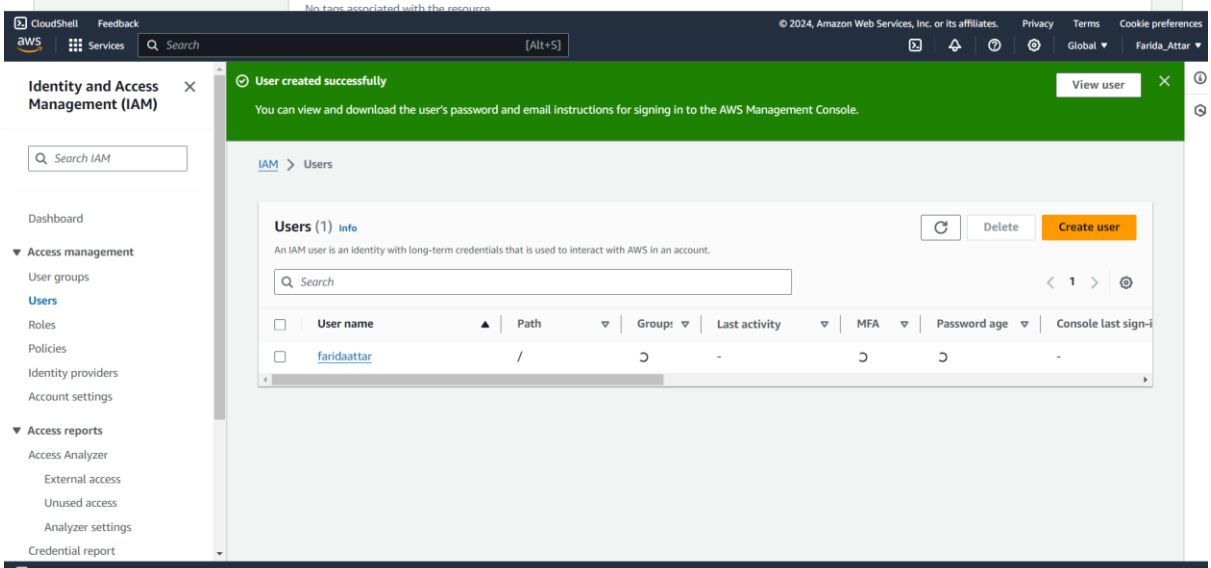

aws
Services
Search
[Alt+S]
Global
Farida_Attar
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
IAM > Dashboard
IAM Dashboard
Security recommendations 1
Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.
Add MFA
Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.
IAM resources
Resources in this AWS Account
User groups
0
Users
0
Roles
2
Policies
0
Identity providers
0
AWS Account
Account ID
481665128109
Account Alias
Create
Sign-in URL for IAM users in this account
https://481665128109.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

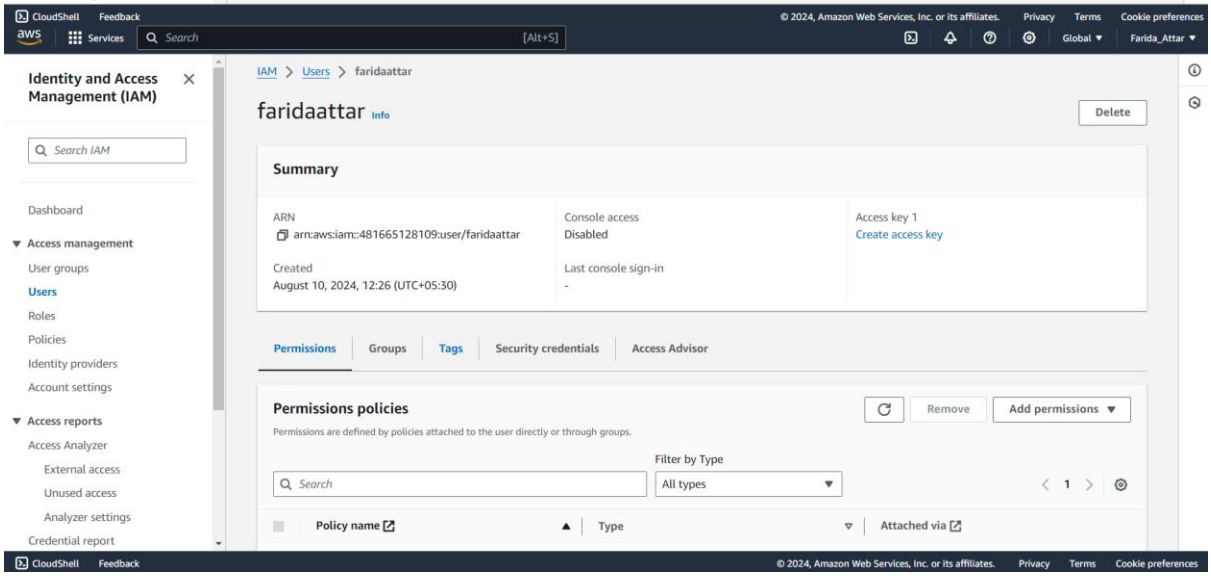

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
IAM > Users
Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
No resources to display

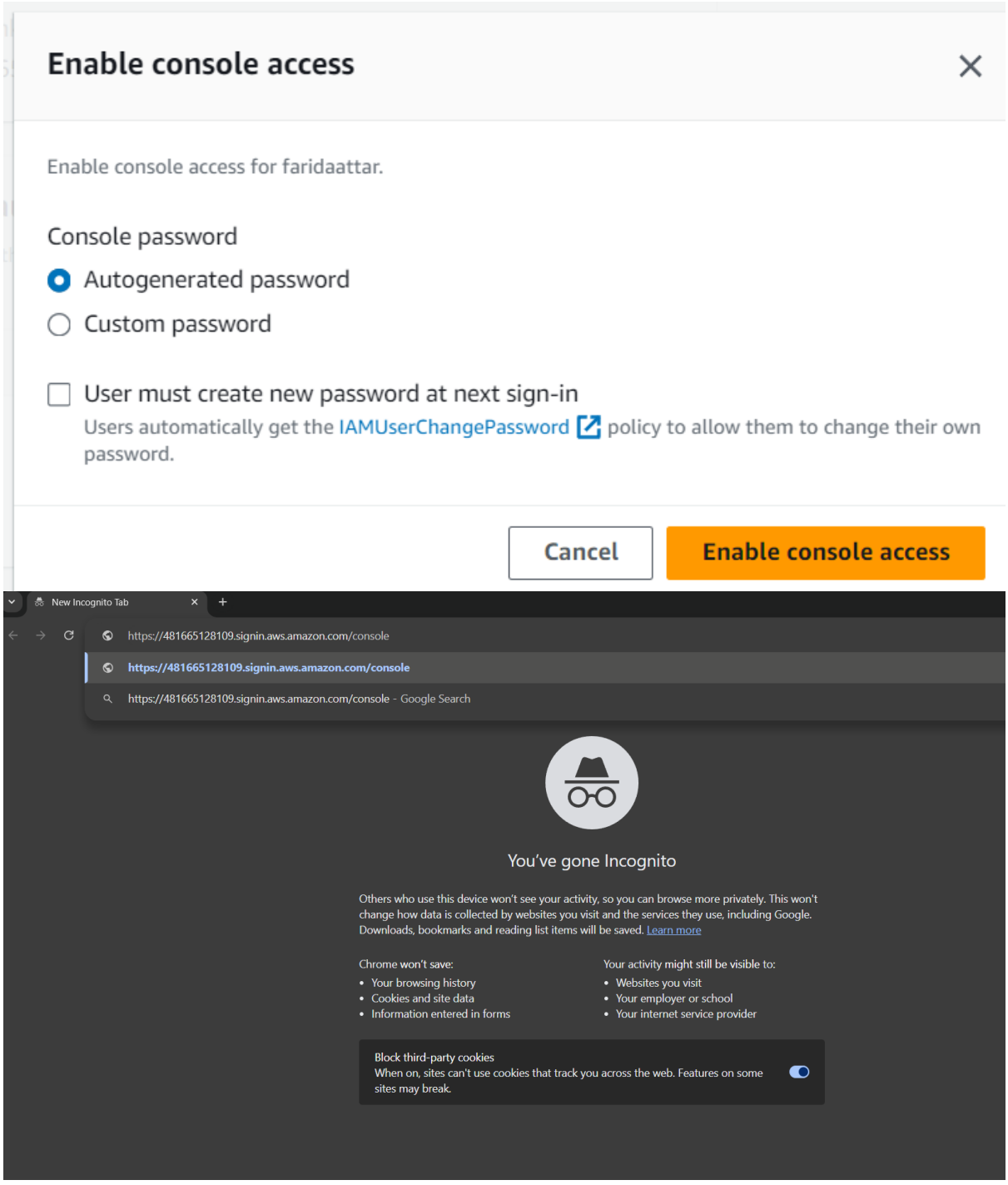

IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
faridaattar
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management 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


IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Set 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, and inline policies 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.
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
Create group
Set permissions boundary - optional
Cancel
Previous
Next


Services
Search
[Alt+S]
Global
Farida_Attar
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
faridaattar
Console password type
None
Require password reset
No
Permissions summary
Name
Type
Used as
No resources
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.


CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Identity and Access Management (IAM)
User created successfully
View user
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
IAM > Users
Users (1) Info
Delete
Create user
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
faridaattar
/
-
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report


CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Identity and Access Management (IAM)
IAM > Users > faridaattar
faridaattar Info
Delete
Summary
ARN
arn:aws:iam::481665128109:user/faridaattar
Console access
Disabled
Access key 1
Create access key
Created
August 10, 2024, 12:26 (UTC+05:30)
Last console sign-in
-
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached via
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report


Enable console access
Enable console access for faridaattar.
Console password
Autogenerated password
Custom password
User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
Cancel
Enable console access
New Incognito Tab
https://481665128109.signin.aws.amazon.com/console
https://481665128109.signin.aws.amazon.com/console
https://481665128109.signin.aws.amazon.com/console - Google Search
You've gone Incognito
Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks and reading list items will be saved. Learn more
Chrome won't save:
Your browsing history
Cookies and site data
Information entered in forms
Your activity might still be visible to:
Websites you visit
Your employer or school
Your internet service provider
Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

Sign in as IAM user

Account ID (12 digits) or account alias

481665128109

IAM user name

Farida Attar

Password

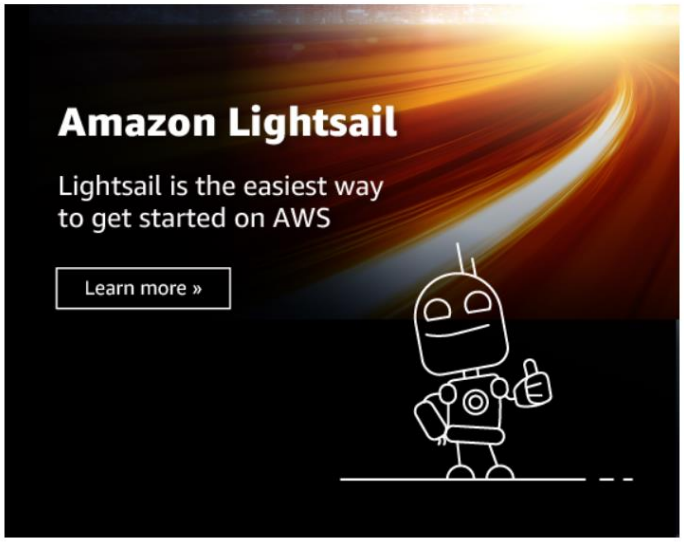
••••••••••

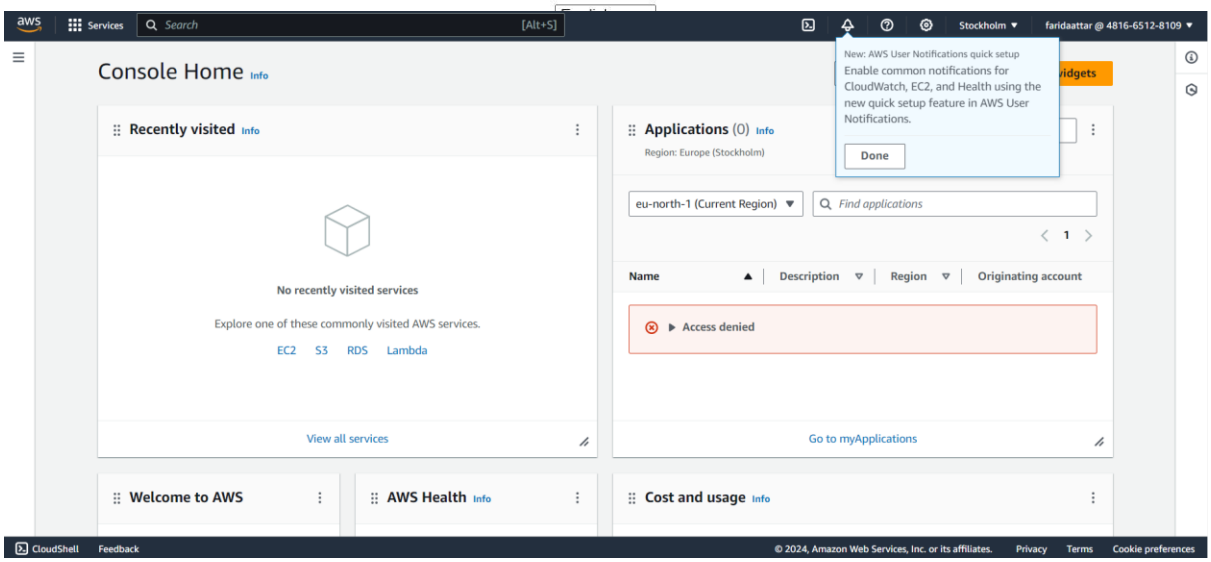
Remember this account

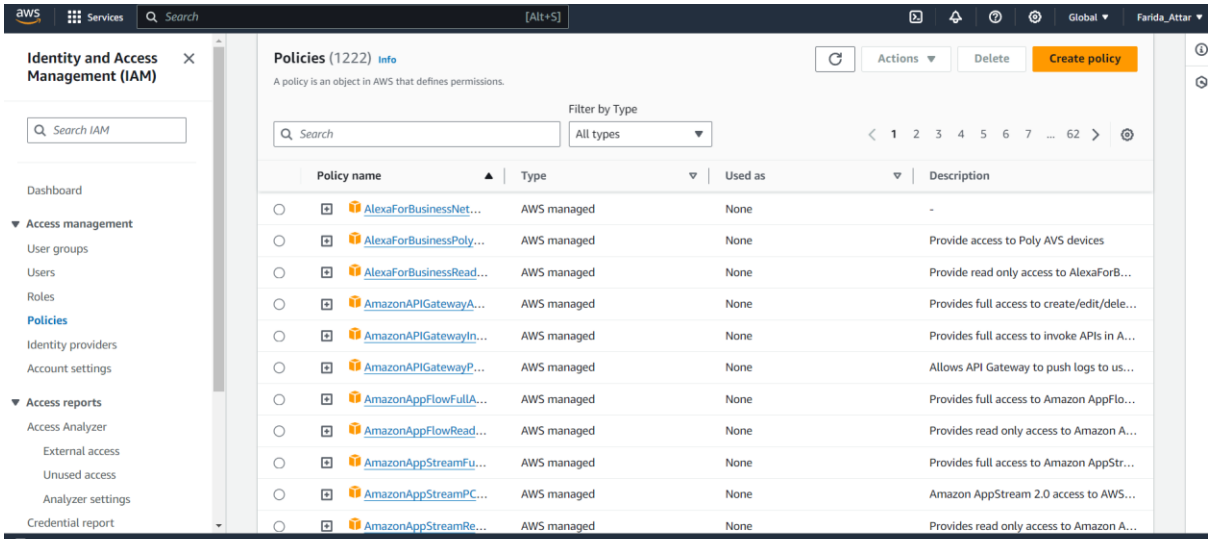
Sign in

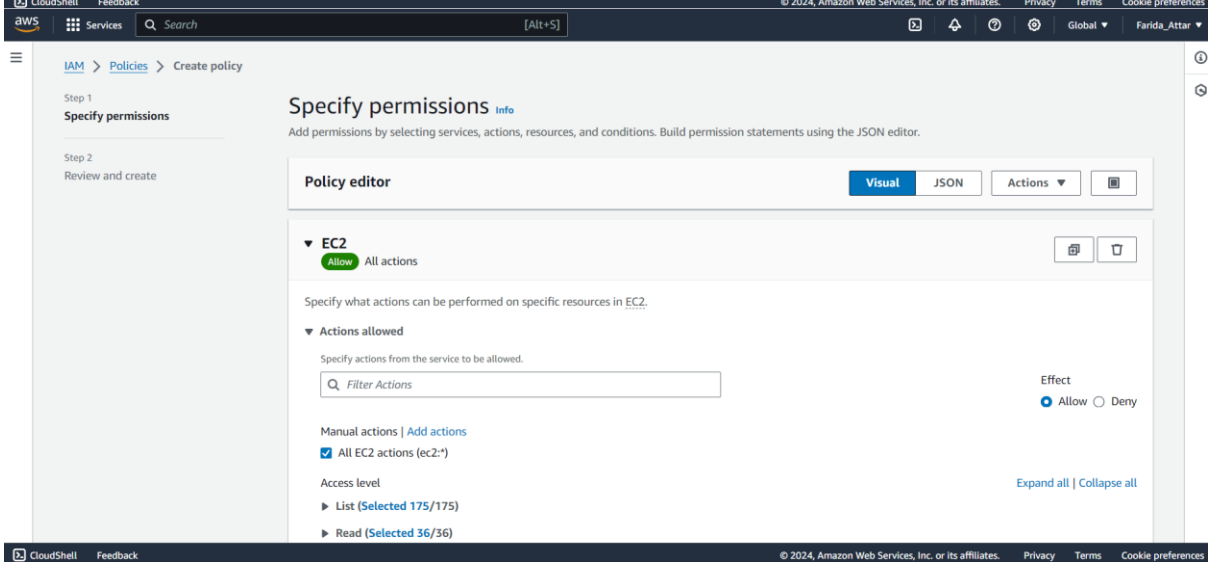
Sign in using root user email

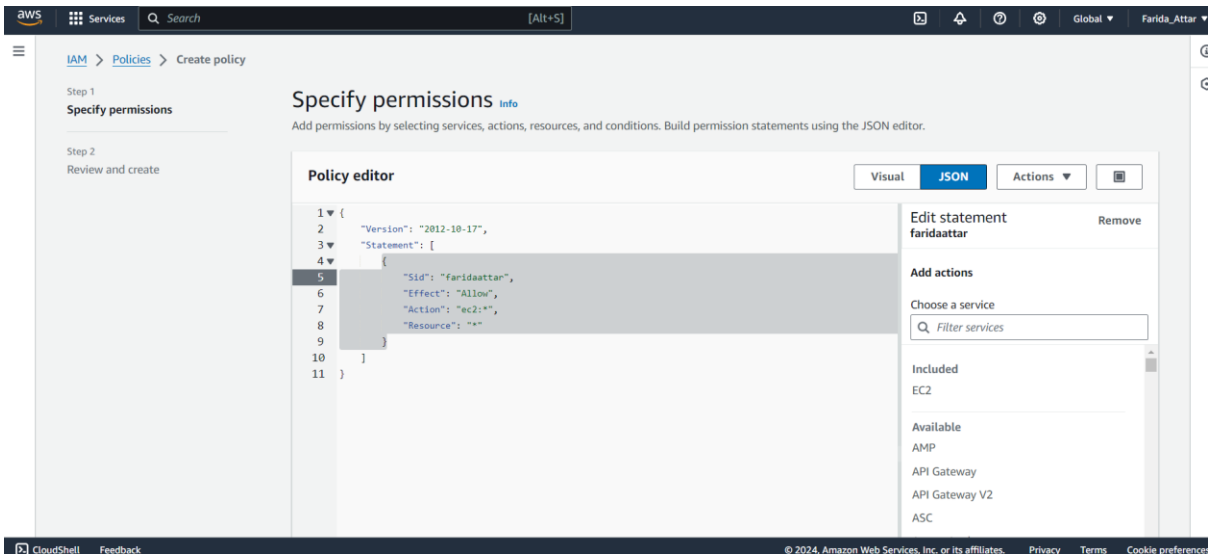
Forgot password?

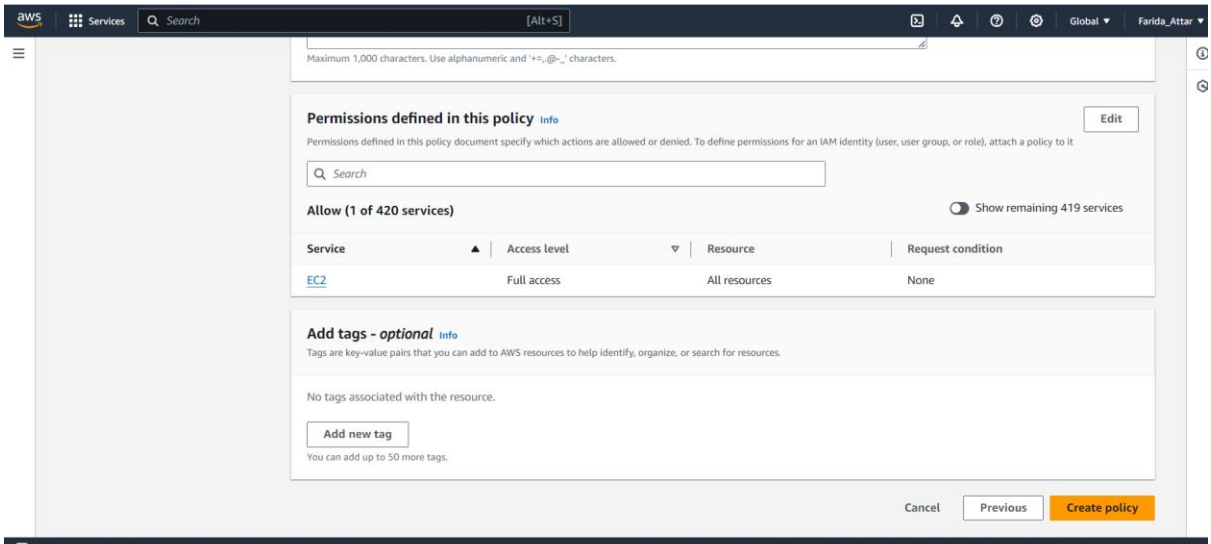


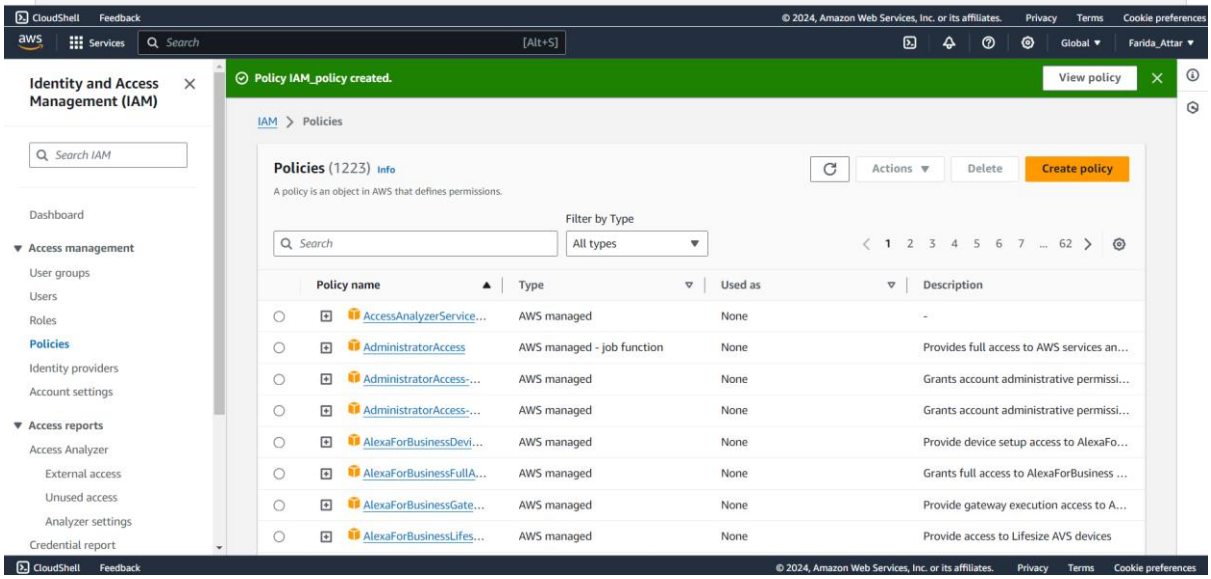


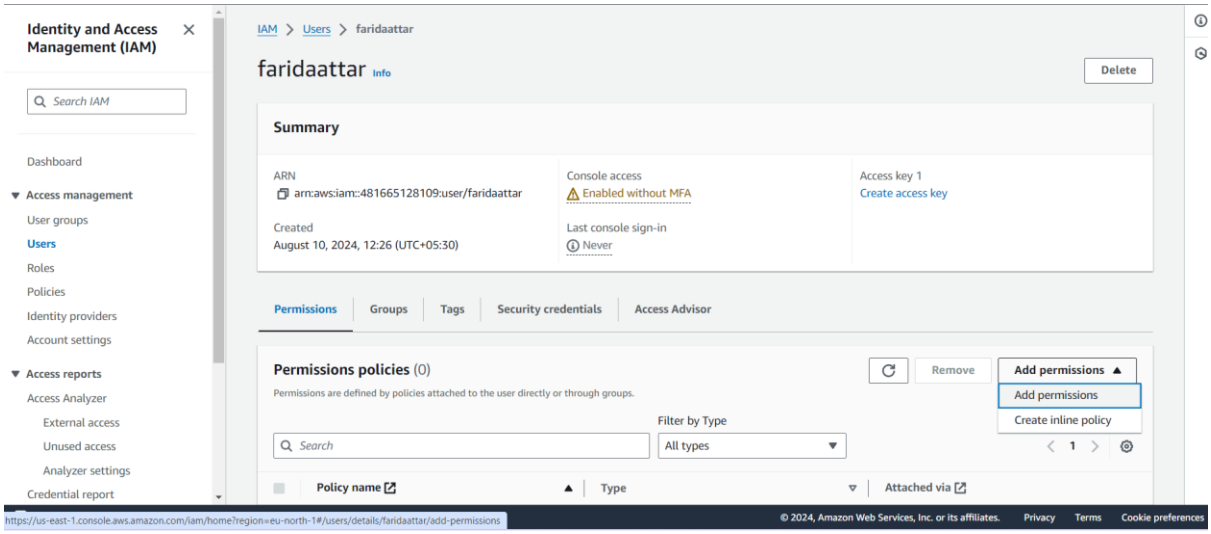

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Policies (1222) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Search
Filter by Type
All types
Policy name
Type
Used as
Description
AlexaForBusinessNet...
AWS managed
None
-
AlexaForBusinessPoly...
AWS managed
None
Provide access to Poly AVS devices
AlexaForBusinessRead...
AWS managed
None
Provide read only access to AlexaForB...
AmazonAPIGatewayA...
AWS managed
None
Provides full access to create/edit/dele...
AmazonAPIGatewayIn...
AWS managed
None
Provides full access to invoke APIs in A...
AmazonAPIGatewayP...
AWS managed
None
Allows API Gateway to push logs to us...
AmazonAppFlowFullA...
AWS managed
None
Provides full access to Amazon AppFlo...
AmazonAppFlowRead...
AWS managed
None
Provides read only access to Amazon A...
AmazonAppStreamFu...
AWS managed
None
Provides full access to Amazon AppStr...
AmazonAppStreamPC...
AWS managed
None
Amazon AppStream 2.0 access to AWS...
AmazonAppStreamRe...
AWS managed
None
Provides read only access to Amazon A...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

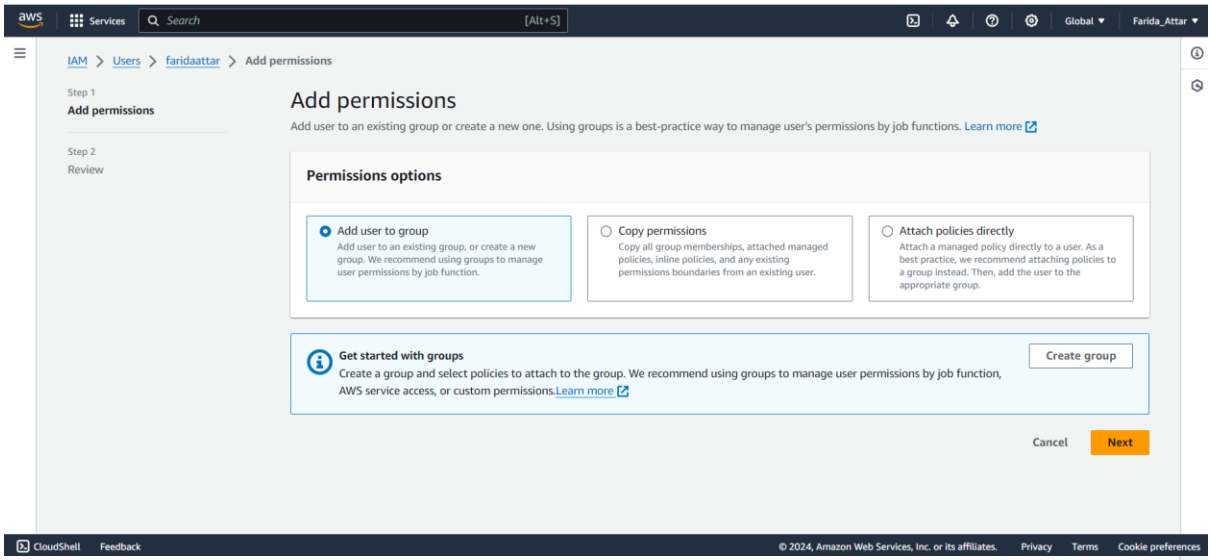

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
EC2
Allow
All actions
Specify what actions can be performed on specific resources in EC2.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All EC2 actions (ec2:*)
Access level
Expand all | Collapse all
List (Selected 175/175)
Read (Selected 36/36)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

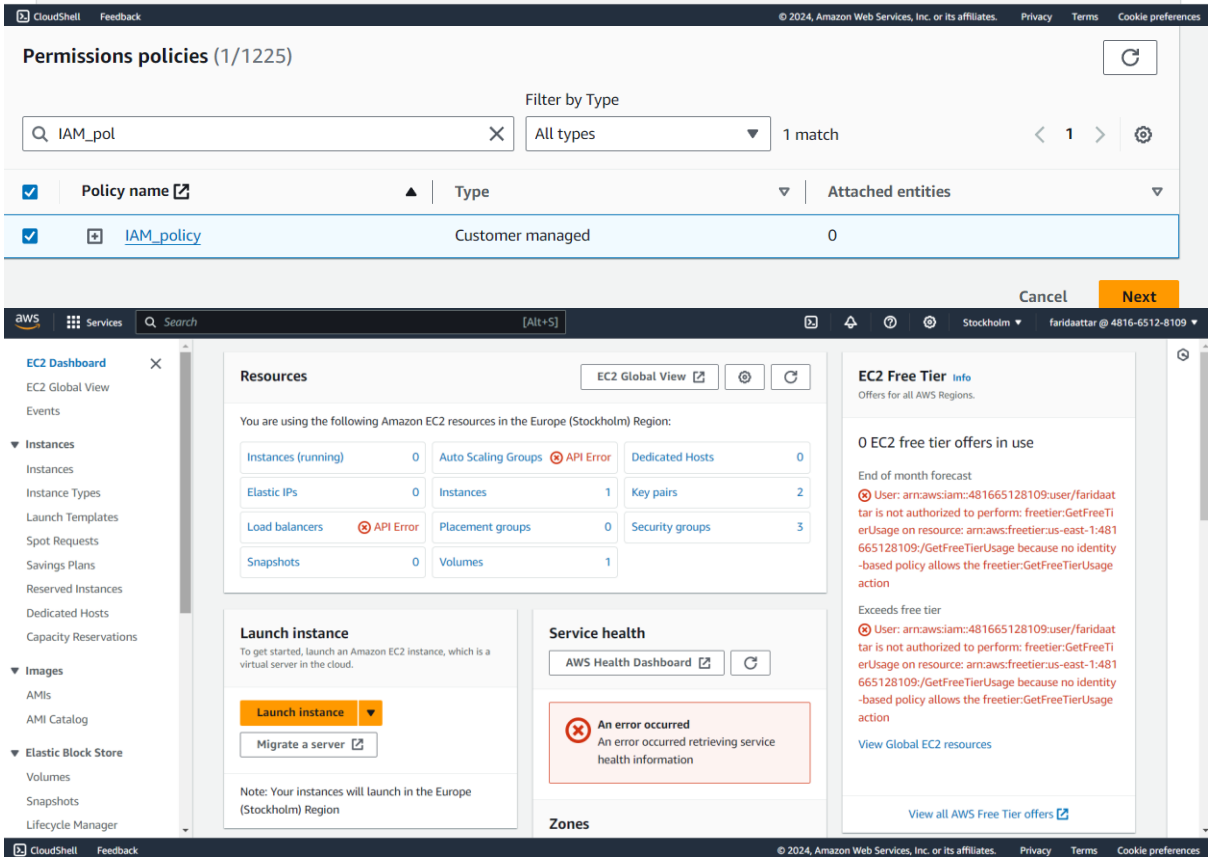

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "faridaattar",
"Effect": "Allow",
"Action": "ec2:*",
"Resource": "*"
}
]
}
Edit statement
faridaattar
Remove
Add actions
Choose a service
Filter services
Included
EC2
Available
AMP
API Gateway
API Gateway V2
ASC
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
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
Search
Allow (1 of 420 services)
Show remaining 419 services
Service
Access level
Resource
Request condition
EC2
Full access
All resources
None
Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create policy


Policy IAM_policy created.
View policy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
IAM > Policies
Policies (1223) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
All types
Policy name
Type
Used as
Description
AccessAnalyzerService...
AWS managed
None
AdministratorAccess
AWS managed - job function
None
Provides full access to AWS services an...
AdministratorAccess-...
AWS managed
None
Grants account administrative permissi...
AlexaForBusinessDevi...
Provide device setup access to AlexaFo...
AlexaForBusinessFullA...
Grants full access to AlexaForBusiness ...
AlexaForBusinessGate...
Provide gateway execution access to A...
AlexaForBusinessLifes...
Provide access to Lifesize AVS devices


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
IAM > Users > faridaattar
faridaattar Info
Delete
Summary
ARN
arn:aws:iam::481665128109:user/faridaattar
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 10, 2024, 12:26 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (0)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Add permissions
Create inline policy
Filter by Type
All types
Policy name
Type
Attached via


Services
Search
[Alt+S]
Global
Farida_Attar
IAM > Users > faridaattar > Add permissions
Step 1
Add permissions
Step 2
Review
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.
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions.Learn more
Create group
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Permissions policies (1/1225)
Filter by Type
IAM_pol
All types
1 match
1
Policy name
Type
Attached entities
IAM_policy
Customer managed
0
Cancel
Next
Services
Search
[Alt+S]
Stockholm
faridaattar @ 4816-6512-8109
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Resources
EC2 Global View
You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:
Instances (running) 0
Auto Scaling Groups API Error
Dedicated Hosts 0
Elastic IPs 0
Instances 1
Key pairs 2
Load balancers API Error
Placement groups 0
Security groups 3
Snapshots 0
Volumes 1
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Note: Your instances will launch in the Europe (Stockholm) Region
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Zones
EC2 Free Tier Info
Offers for all AWS Regions.
0 EC2 free tier offers in use
End of month forecast
User: arn:aws:iam::481665128109:user/faridaattar is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:481665128109:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
Exceeds free tier
User: arn:aws:iam::481665128109:user/faridaattar is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:481665128109:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
View Global EC2 resources
View all AWS Free Tier offers
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

key12

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

- (●) **RSA** — RSA encrypted private and public key pair
- ( ) **ED25519** — ED25519 encrypted private and public key pair

Private key file format

- (●) **.pem** — For use with OpenSSH
- ( ) **.ppk** — For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Cancel | **Create key pair**