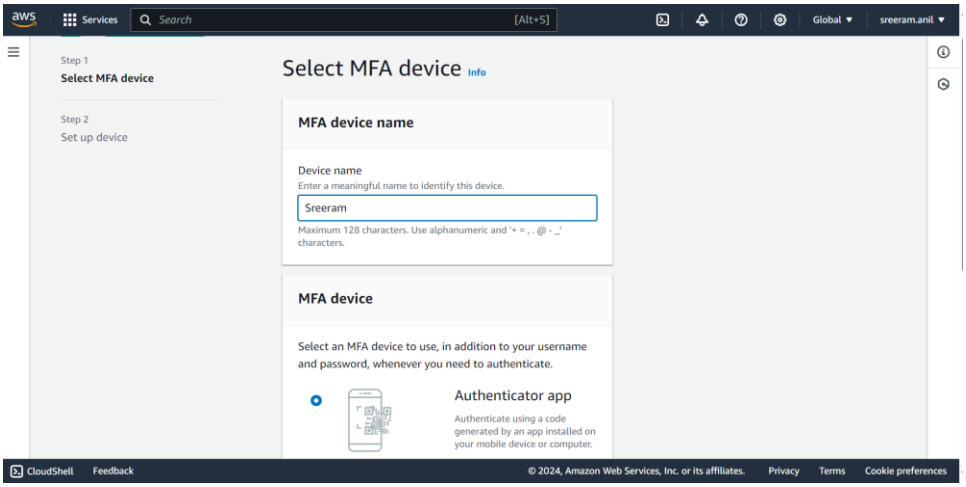
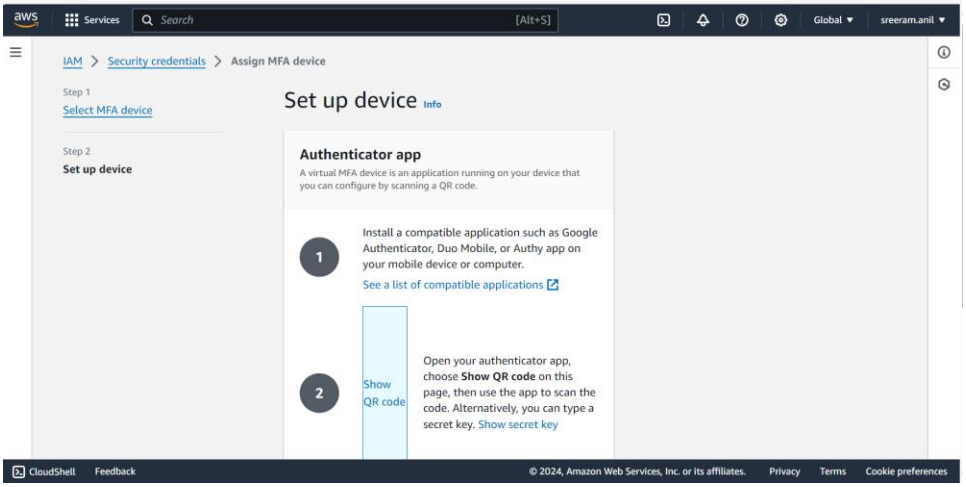
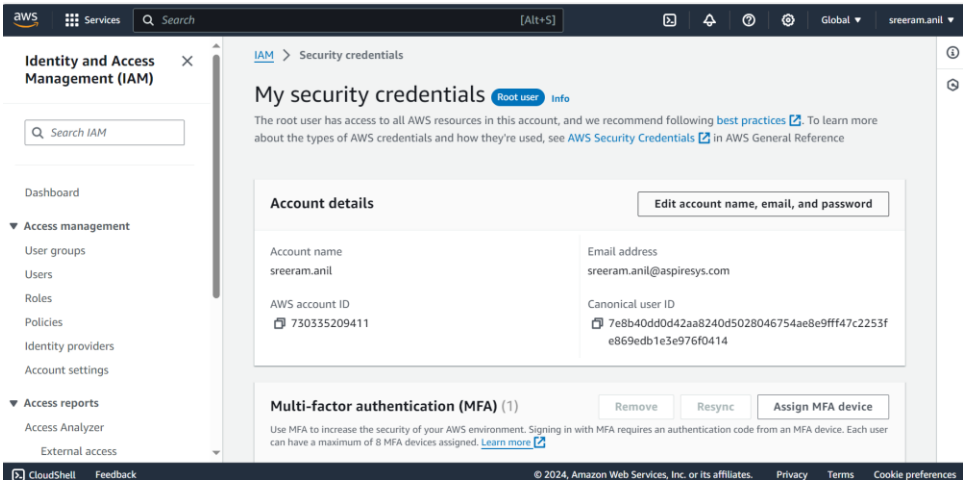
AWS IAM

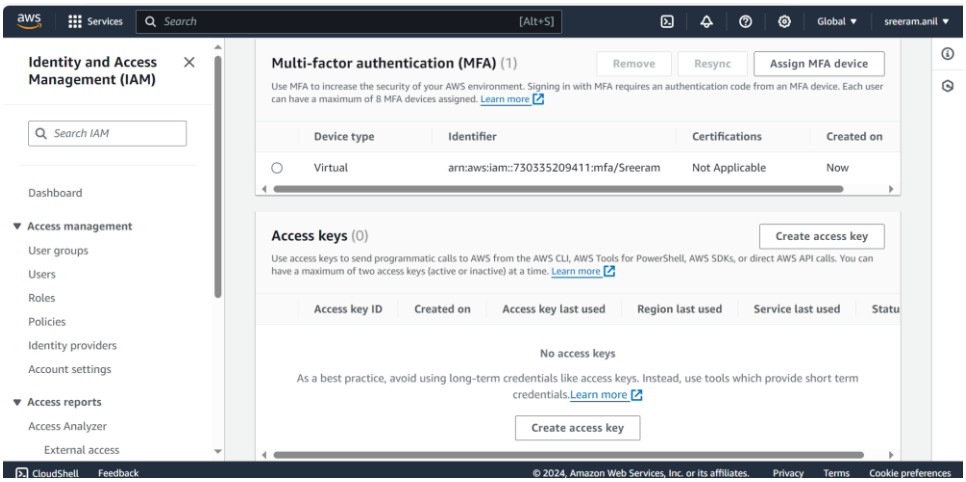
Sreeram Anil

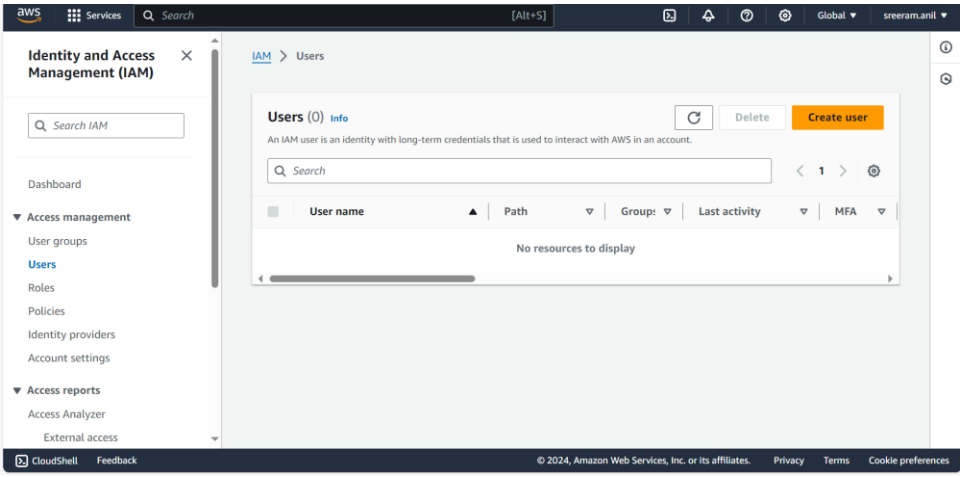
ACE:11631

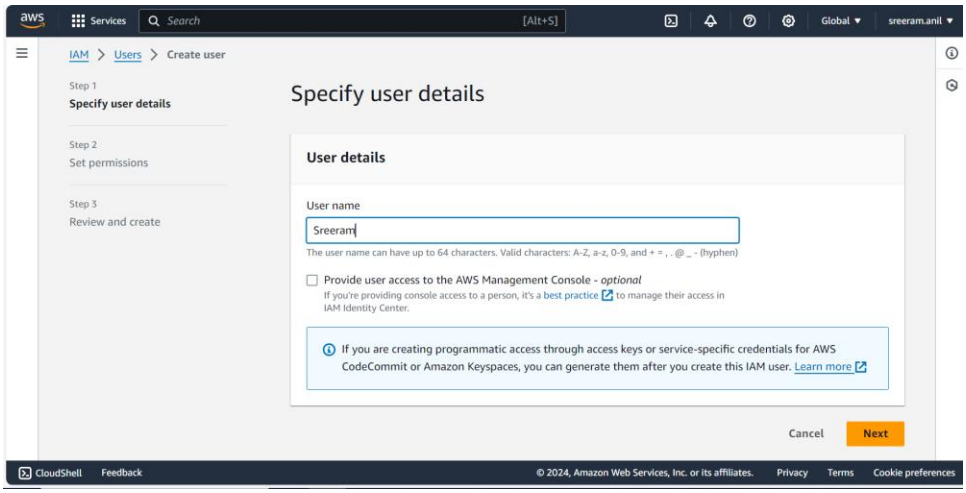


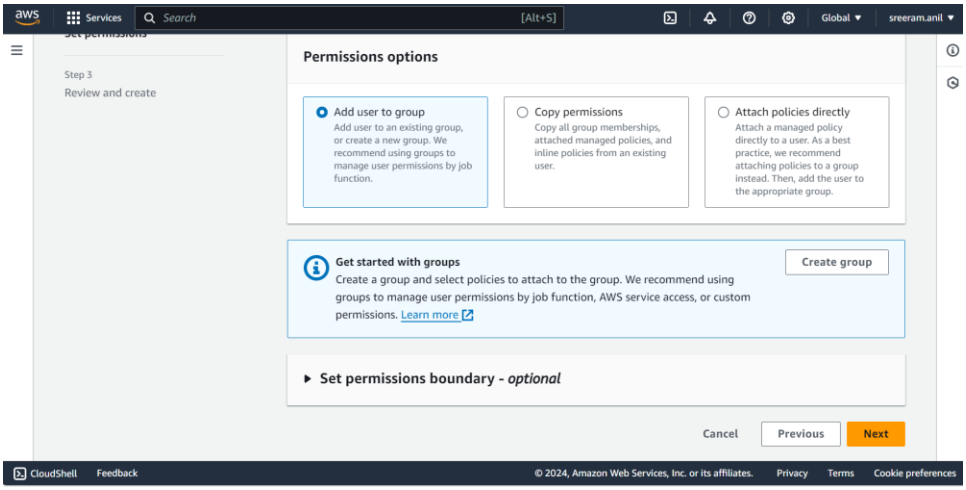


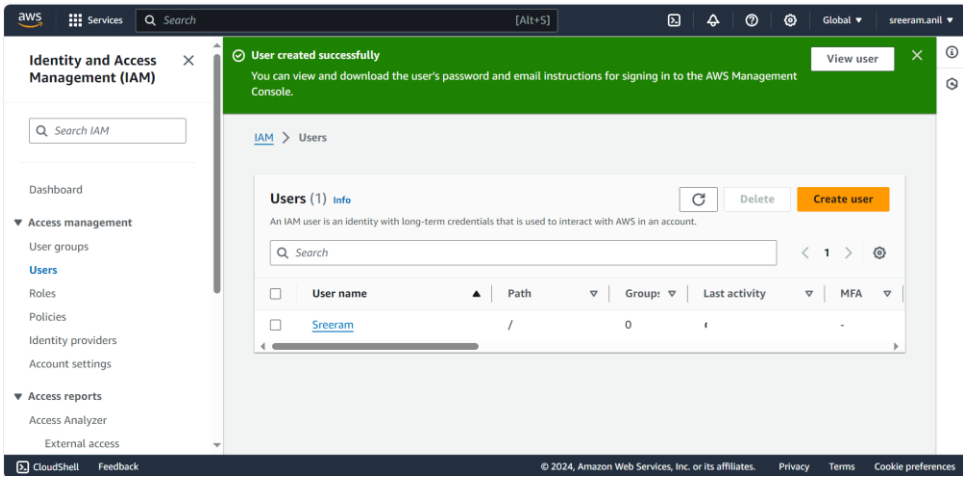

Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
IAM > Security credentials
My security credentials
Root user
Info
The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference
Account details
Edit account name, email, and password
Account name
sreeram.anil
Email address
sreeram.anil@aspiresys.com
AWS account ID
730335209411
Canonical user ID
7e8b40dd0d42aa8240d5028046754ae8e9fff47c2253fe869edb1e3e976f0414
Multi-factor authentication (MFA) (1)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

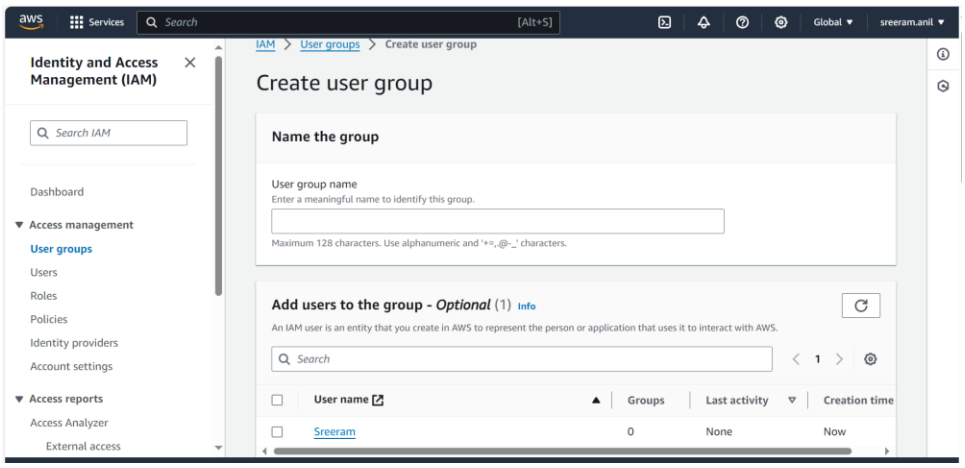

Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Multi-factor authentication (MFA) (1)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Device type
Identifier
Certifications
Created on
Virtual
arn:aws:iam::730335209411:mfa/Sreeram
Not Applicable
Now
Access keys (0)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
Access key ID
Created on
Access key last used
Region last used
Service last used
No access keys
As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more
Create access key
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

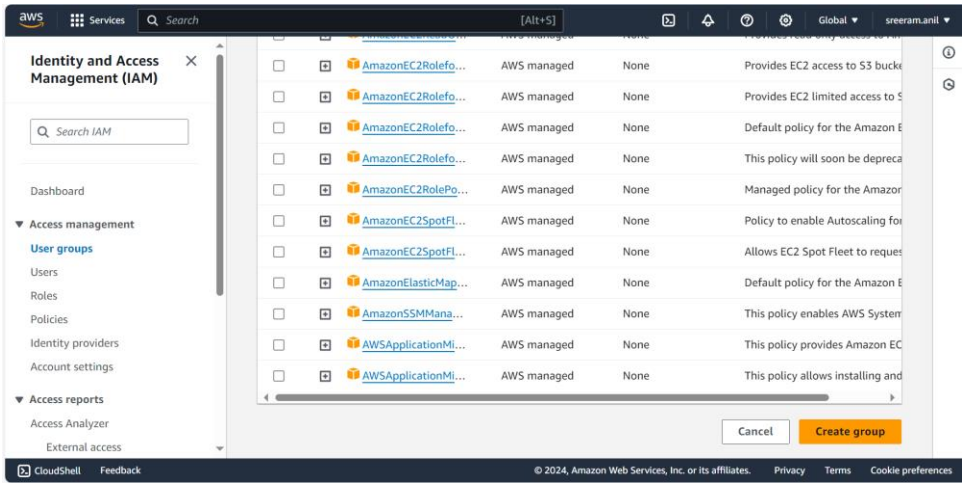

Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
IAM > Users
Users (0)
Info
Delete
Create user
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
User name
Path
Groups
Last activity
MFA
No resources to display
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

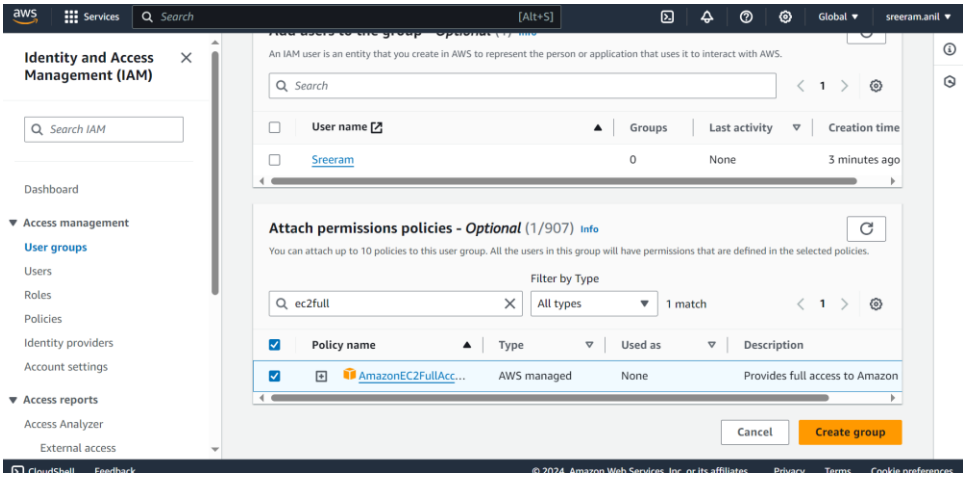

aws
Services
Search
[Alt+S]
Global
sreeram.anil
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
Sreeram
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

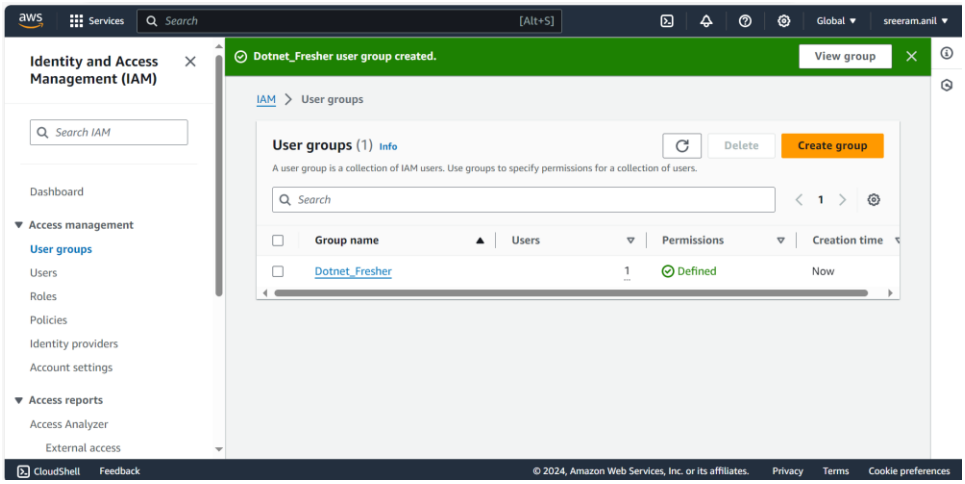

aws
Services
Search
[Alt+S]
Global
sreeram.anil
Step 3
Review and create
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

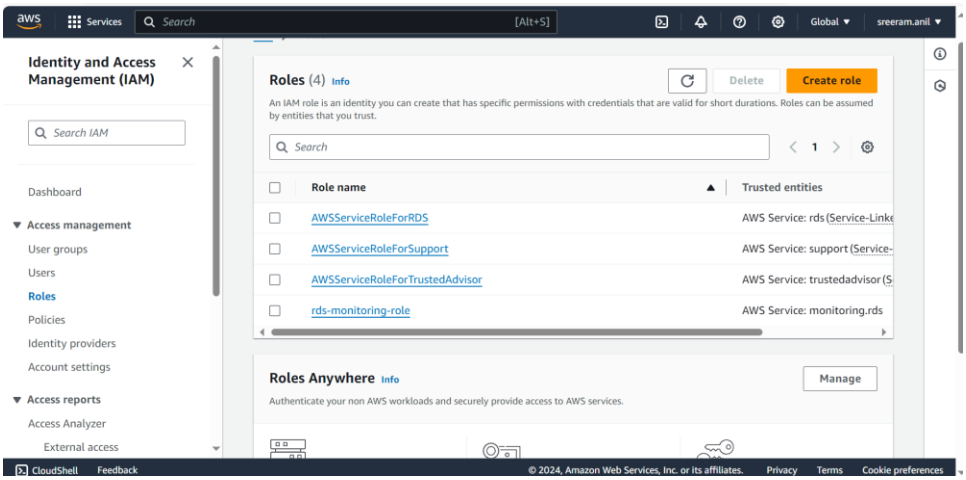

aws
Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
IAM > Users
Users (1) 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
1
User name
Path
Groups
Last activity
MFA
Sreeram
/
0
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

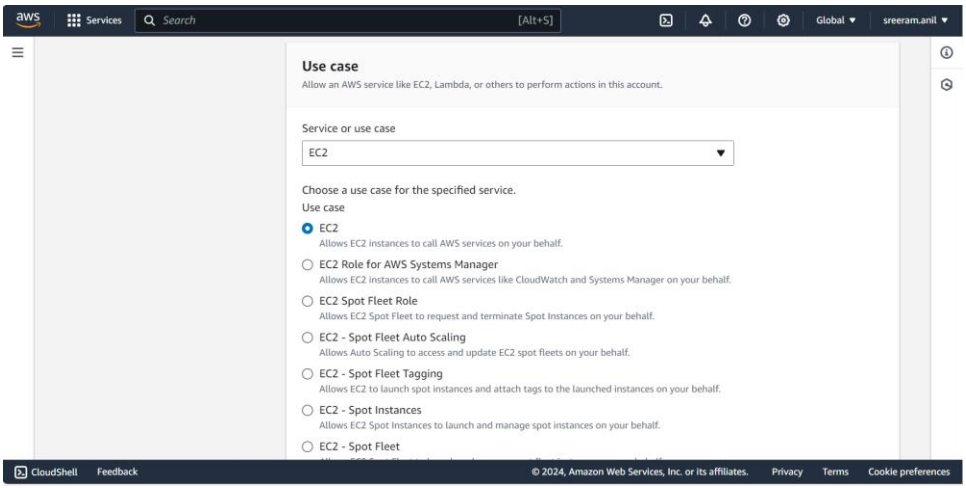

Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (1) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
User name
Groups
Last activity
Creation time
Sreeram
0
None
Now

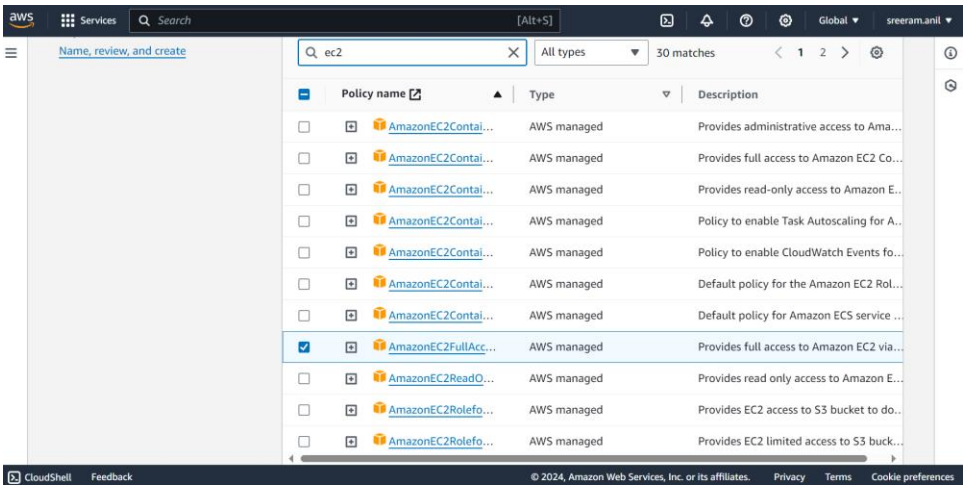

Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
AmazonEC2Rolefo...
AWS managed
None
Provides EC2 access to S3 bucke
Provides EC2 limited access to S
Default policy for the Amazon E
This policy will soon be depreca
AmazonEC2RolePo...
Managed policy for the Amazor
AmazonEC2SpotFl...
Policy to enable Autoscaling for
Allows EC2 Spot Fleet to reques
AmazonElasticMap...
Default policy for the Amazon E
AmazonSSMMana...
This policy enables AWS System
AWSApplicationMi...
This policy provides Amazon EC
This policy allows installing and
Cancel
Create group
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

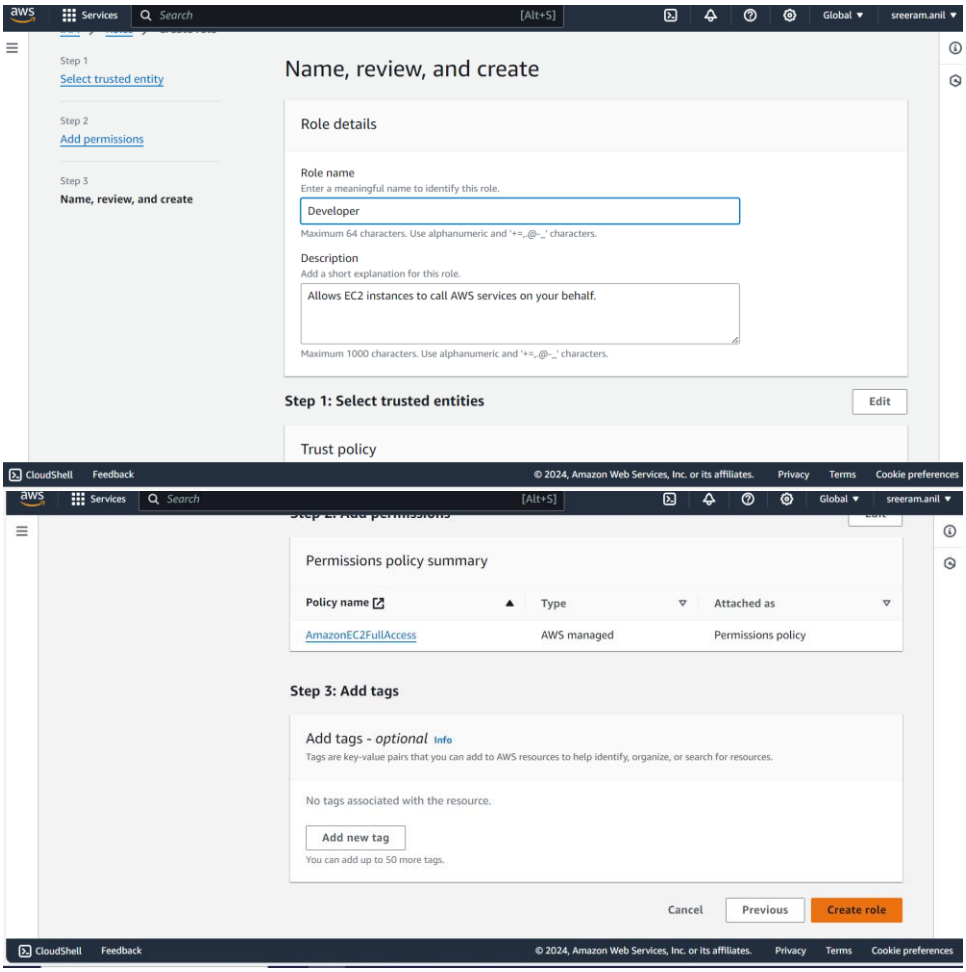

Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
User name
Groups
Last activity
Creation time
Sreeram
0
None
3 minutes ago
Attach permissions policies - Optional (1/907) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Filter by Type
ec2full
All types
1 match
Policy name
Type
Used as
Description
AmazonEC2FullAcc...
AWS managed
None
Provides full access to Amazon
Cancel
Create group

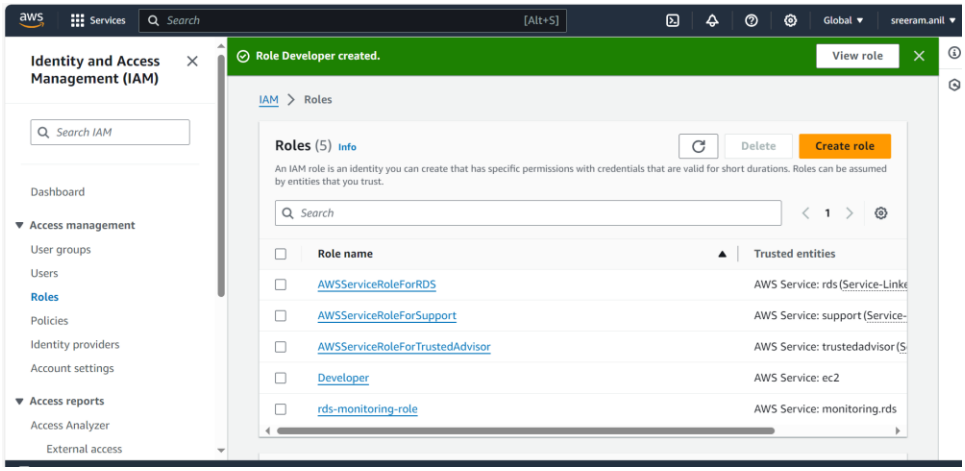

Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Dotnet_Fresher user group created.
View group
IAM > User groups
User groups (1) Info
Delete
Create group
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Search
Group name
Users
Permissions
Creation time
Dotnet_Fresher
1
Defined
Now
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

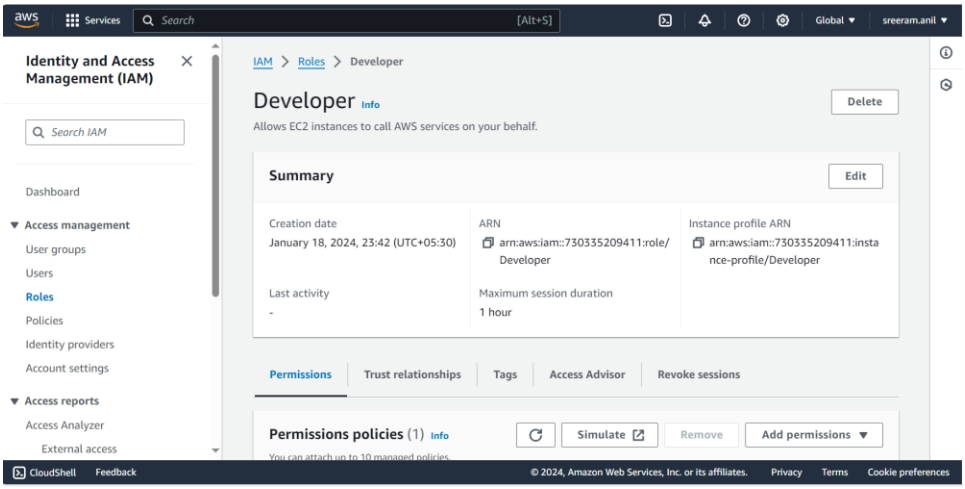

Services
Search
[Alt+S]
Global
sreeram.anil
Identity and Access Management (IAM)
Roles (4) Info
Delete
Create role
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Search
Role name
Trusted entities
AWSServiceRoleForRDS
AWS Service: rds (Service-Linke
AWSServiceRoleForSupport
AWS Service: support (Service-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (S
rds-monitoring-role
AWS Service: monitoring.rds
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
Global
sreeram.anil
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
EC2
Choose a use case for the specified service.
Use case
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
EC2 - Spot Fleet
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
sreeram.anil
Name, review, and create
ec2
All types
30 matches
1
2
Policy name
Type
Description
AmazonEC2Contai...
AWS managed
Provides administrative access to Ama...
AmazonEC2Contai...
AWS managed
Provides full access to Amazon EC2 Co...
AmazonEC2Contai...
AWS managed
Provides read-only access to Amazon E...
AmazonEC2Contai...
AWS managed
Policy to enable Task Autoscaling for A...
AmazonEC2Contai...
AWS managed
Policy to enable CloudWatch Events fo...
AmazonEC2Contai...
AWS managed
Default policy for the Amazon EC2 Rol...
AmazonEC2Contai...
AWS managed
Default policy for Amazon ECS service ...
AmazonEC2FullAcc...
AWS managed
Provides full access to Amazon EC2 via...
AmazonEC2ReadO...
AWS managed
Provides read only access to Amazon E...
AmazonEC2Rolefo...
AWS managed
Provides EC2 access to S3 bucket to do...
AmazonEC2Rolefo...
AWS managed
Provides EC2 limited access to S3 buck...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
sreeram.anil
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
Developer
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Permissions policy summary
Policy name
Type
Attached as
AmazonEC2FullAccess
AWS managed
Permissions policy
Step 3: Add tags
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 role
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
sreeram.anil
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
Role Developer created.
View role
IAM > Roles
Roles (5) Info
Delete
Create role
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Search
1
Role name
Trusted entities
AWSServiceRoleForRDS
AWS Service: rds (Service-Linke
AWSServiceRoleForSupport
AWS Service: support (Service-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (S
Developer
AWS Service: ec2
rds-monitoring-role
AWS Service: monitoring.rds


aws
Services
Search
[Alt+S]
Global
sreeram.anil
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
IAM > Roles > Developer
Developer Info
Delete
Allows EC2 instances to call AWS services on your behalf.
Summary
Edit
Creation date
January 18, 2024, 23:42 (UTC+05:30)
ARN
arn:aws:iam::730335209411:role/Developer
Instance profile ARN
arn:aws:iam::730335209411:instance-profile/Developer
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions
Permissions policies (1) Info
Simulate
Remove
Add permissions
You can attach up to 10 managed policies
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences