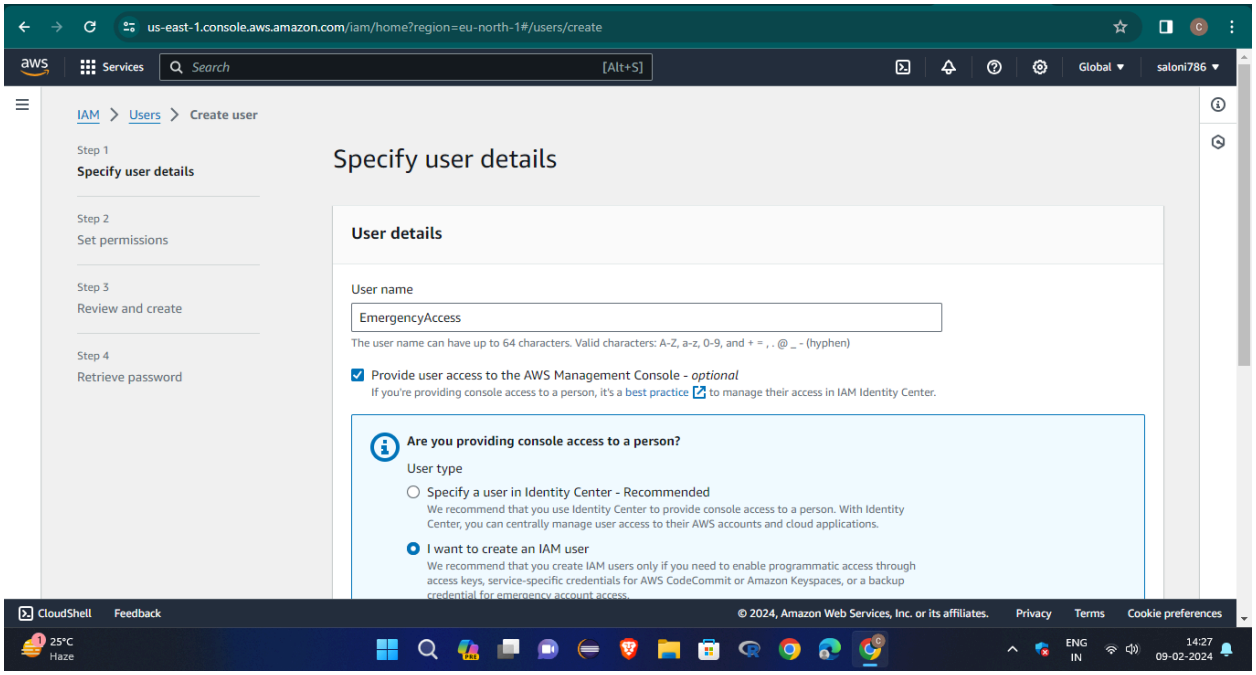
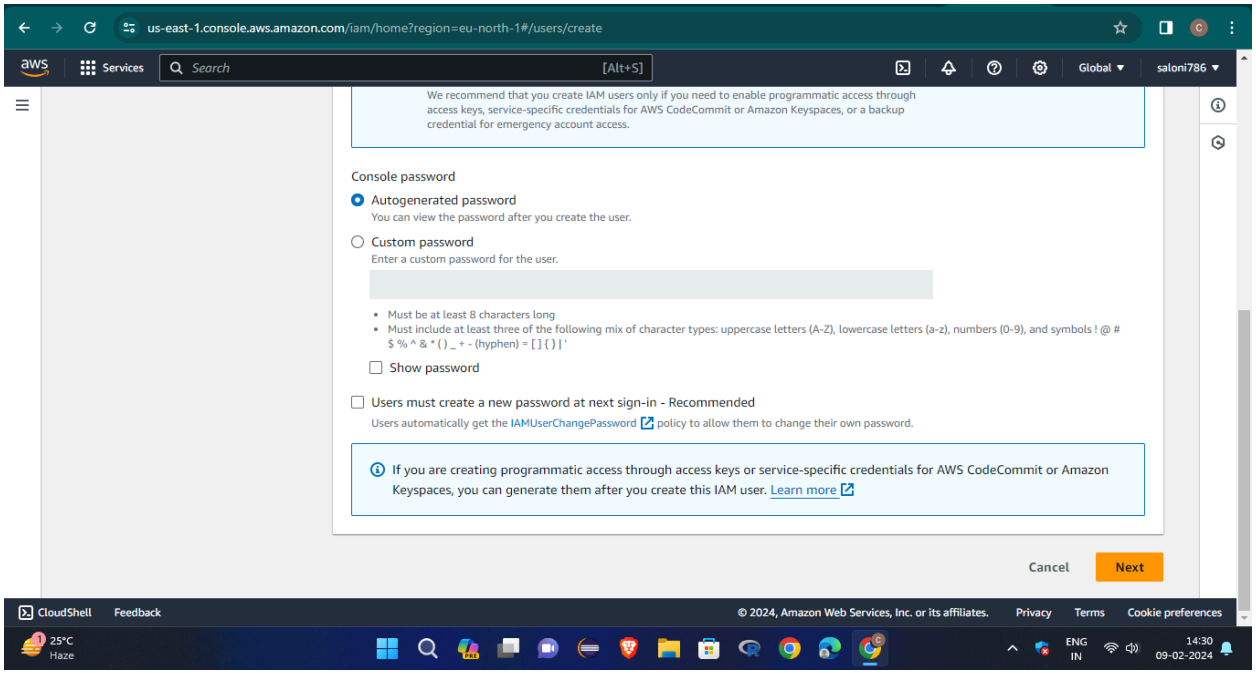
Practical no: 3

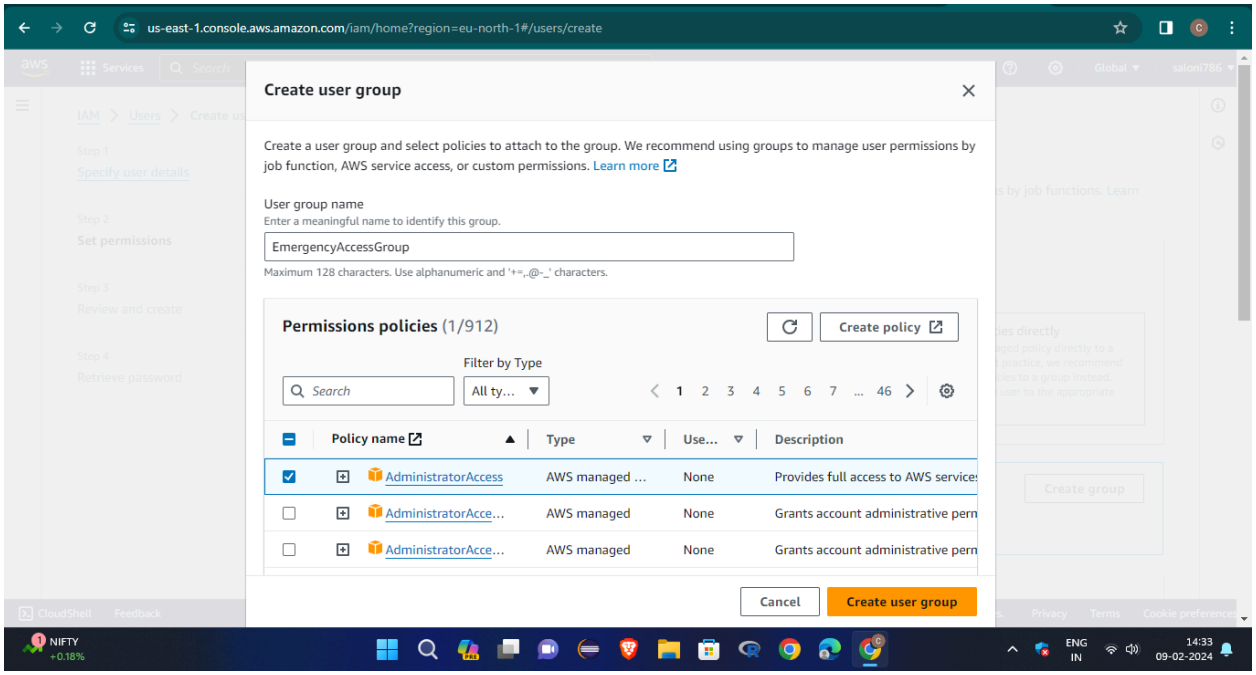
Name: Saloni Vishwakarma
Batch-Roll no: C1-13
Subject: Introduction to Cloud Security Lab
Date of Execution: 09/02/2024

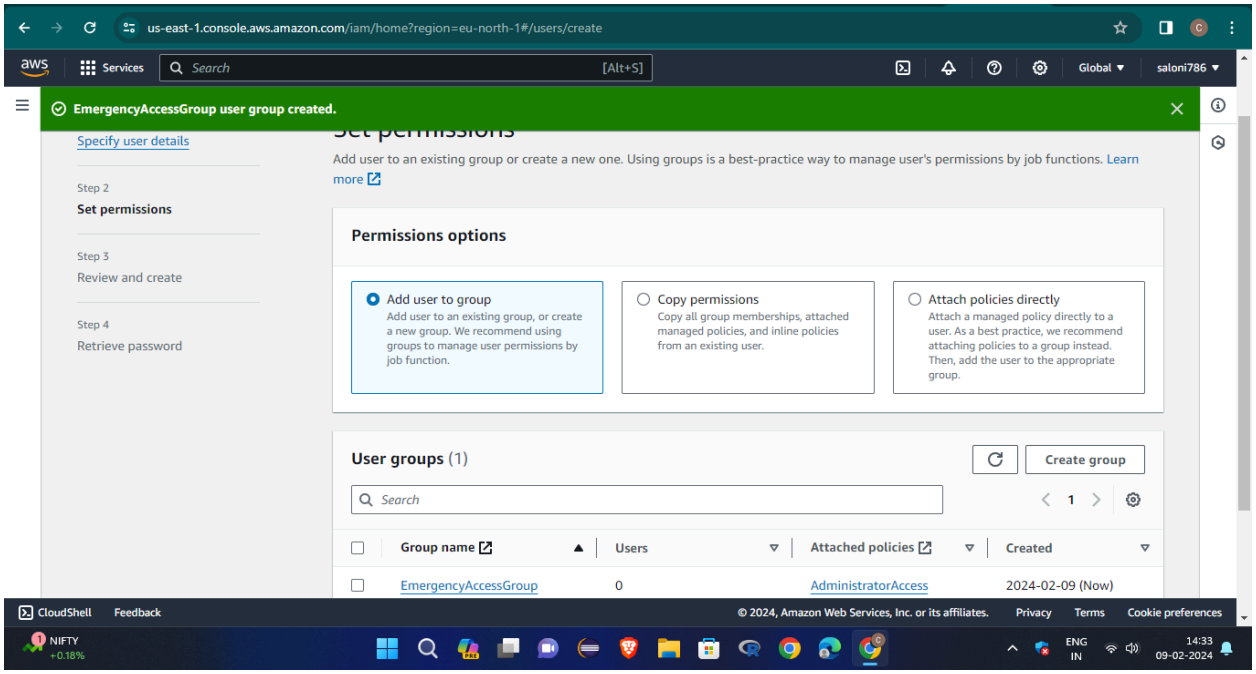
Aim: Configure AWS Identity and Access Management (IAM) Service.

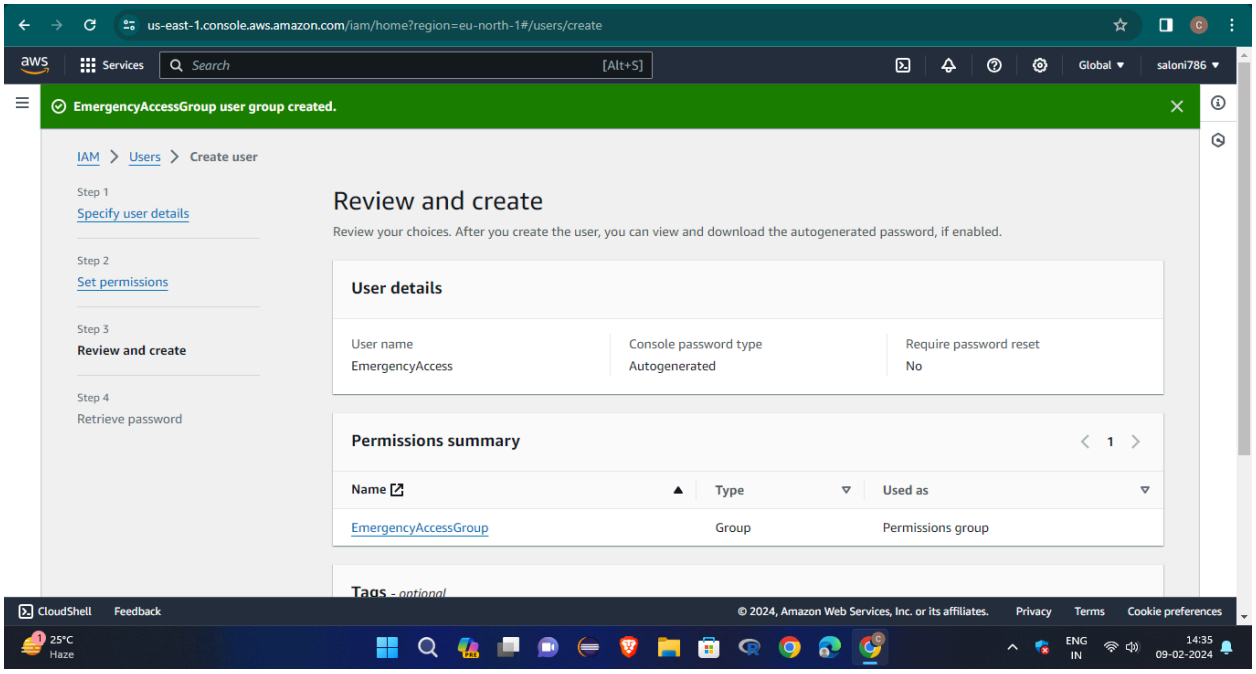
TASK 1:

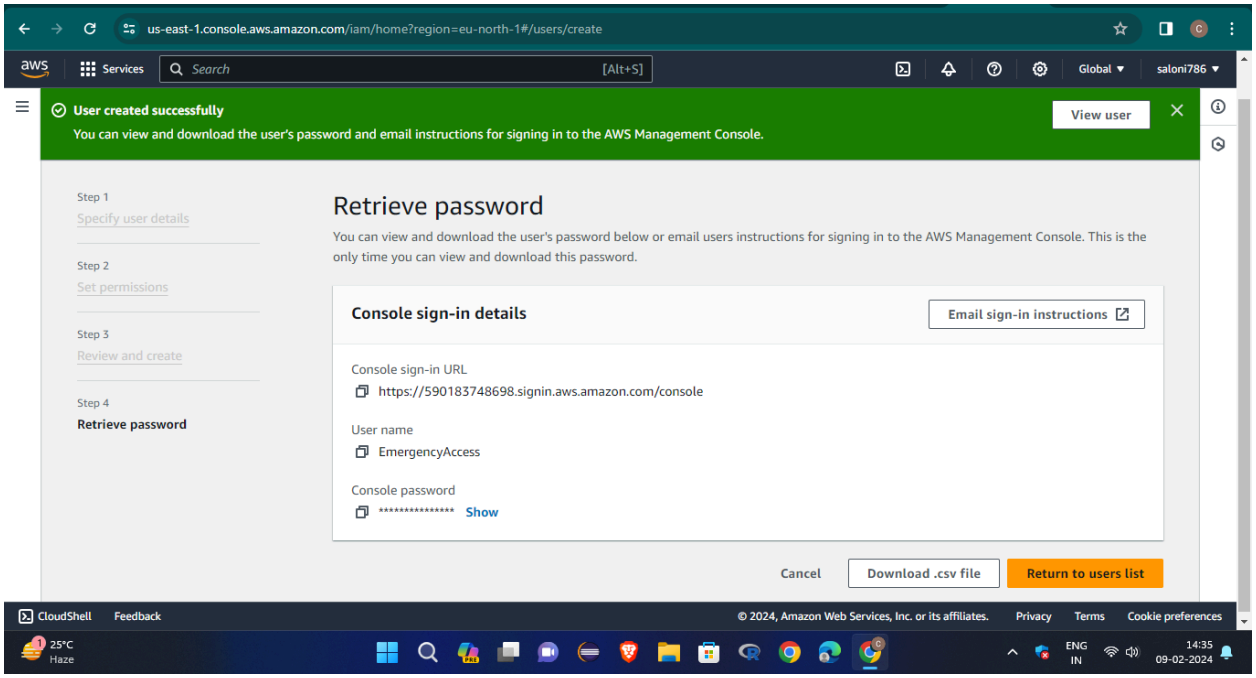


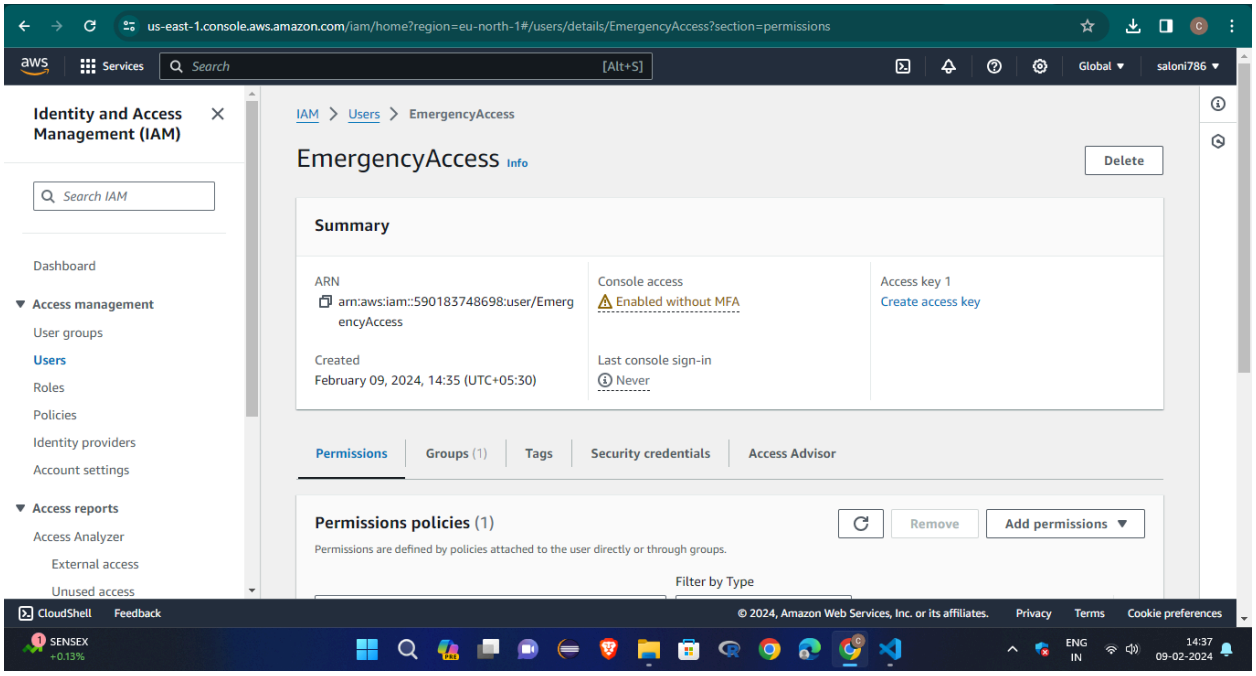

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Services
Search
[Alt+S]
Global
saloni786
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '
Show password
Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
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
25°C
Haze
ENG
IN
14:30
09-02-2024

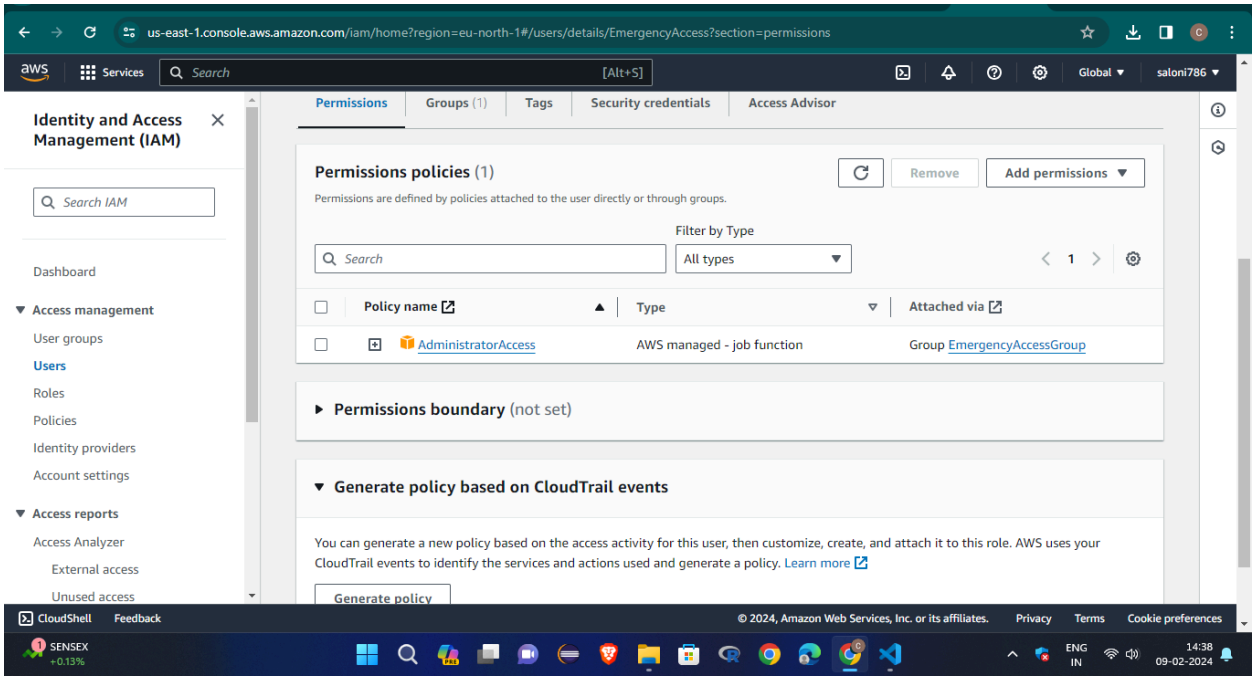

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Create user group
Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
User group name
Enter a meaningful name to identify this group.
EmergencyAccessGroup
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions policies (1/912)
Create policy
Filter by Type
Search
All ty...
1 2 3 4 5 6 7 ... 46
Policy name
Type
Use...
Description
AdministratorAccess
AWS managed ...
None
Provides full access to AWS service
AdministratorAcce...
AWS managed
None
Grants account administrative perm
AdministratorAcce...
AWS managed
None
Grants account administrative perm
Cancel
Create user group
NIFTY
+0.18%
ENG
IN
14:33
09-02-2024

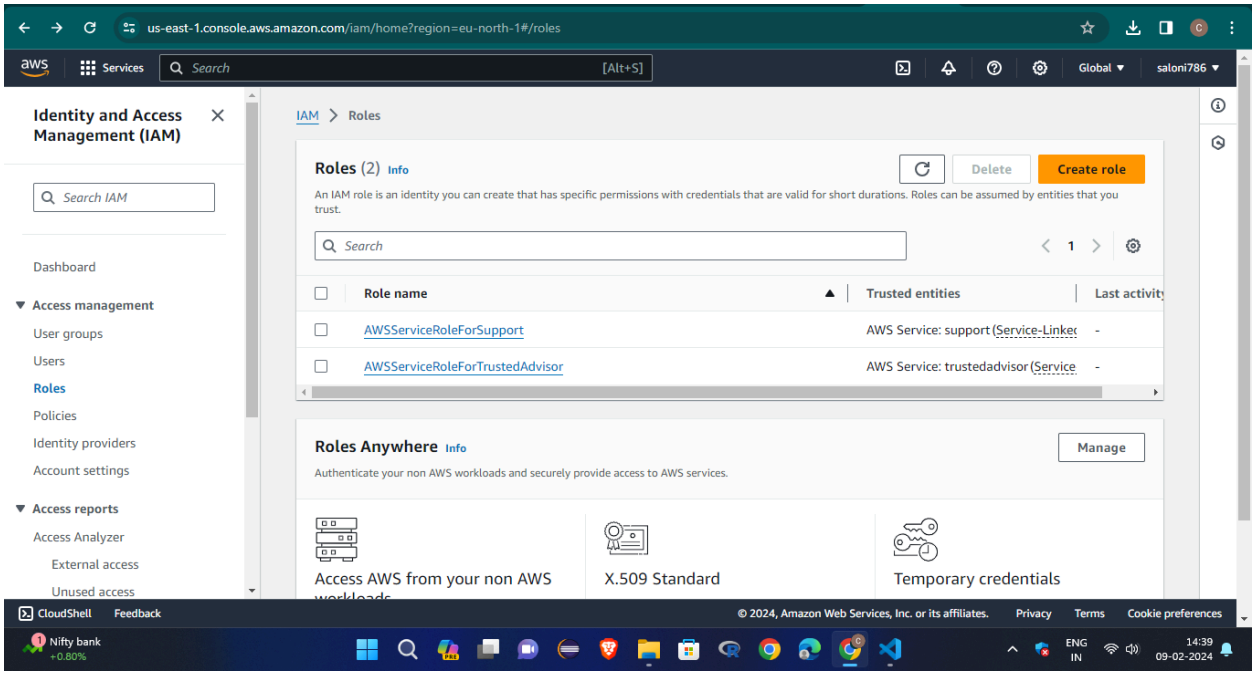

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Services
Search
[Alt+S]
Global
saloni786
EmergencyAccessGroup user group created.
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Add user to an existing group or create a new one. 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.
User groups (1)
Create group
Search
Group name
Users
Attached policies
Created
EmergencyAccessGroup
0
AdministratorAccess
2024-02-09 (Now)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
NIFTY
+0.18%
ENG
IN
14:33
09-02-2024

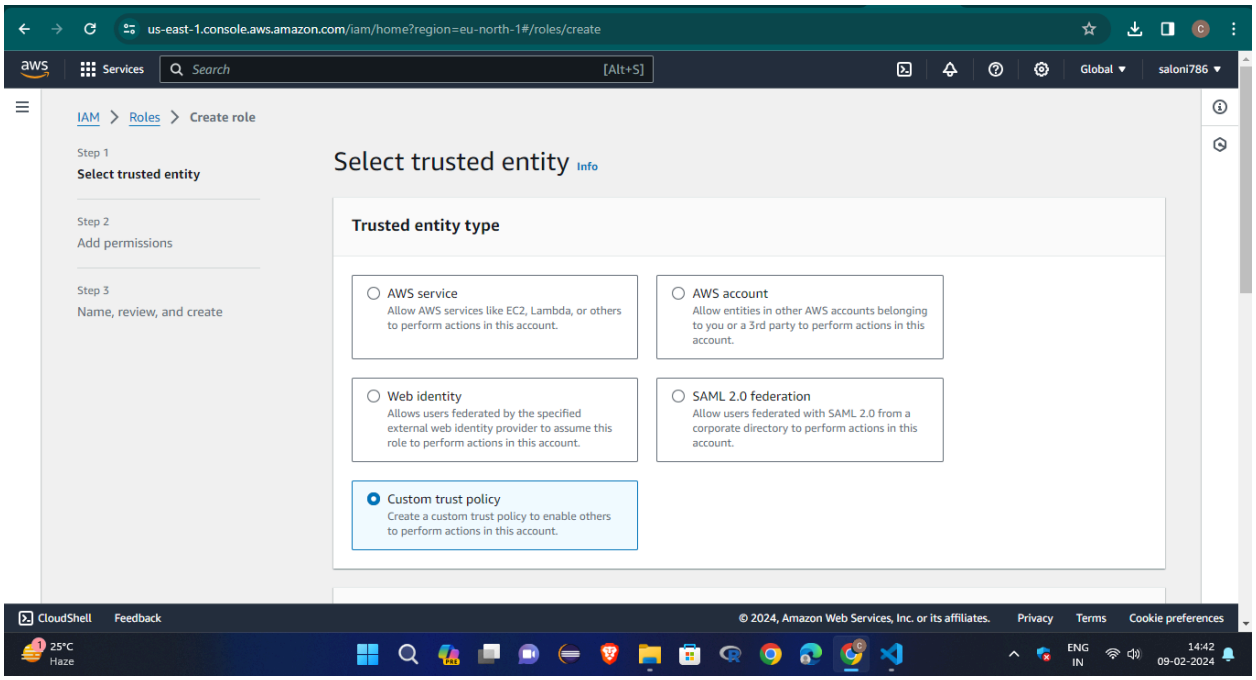

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Services
Search
[Alt+S]
Global
saloni786
EmergencyAccessGroup user group created.
IAM
Users
Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
EmergencyAccess
Console password type
Autogenerated
Require password reset
No
Permissions summary
Name
Type
Used as
EmergencyAccessGroup
Group
Permissions group
Tags - optional
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:35
09-02-2024

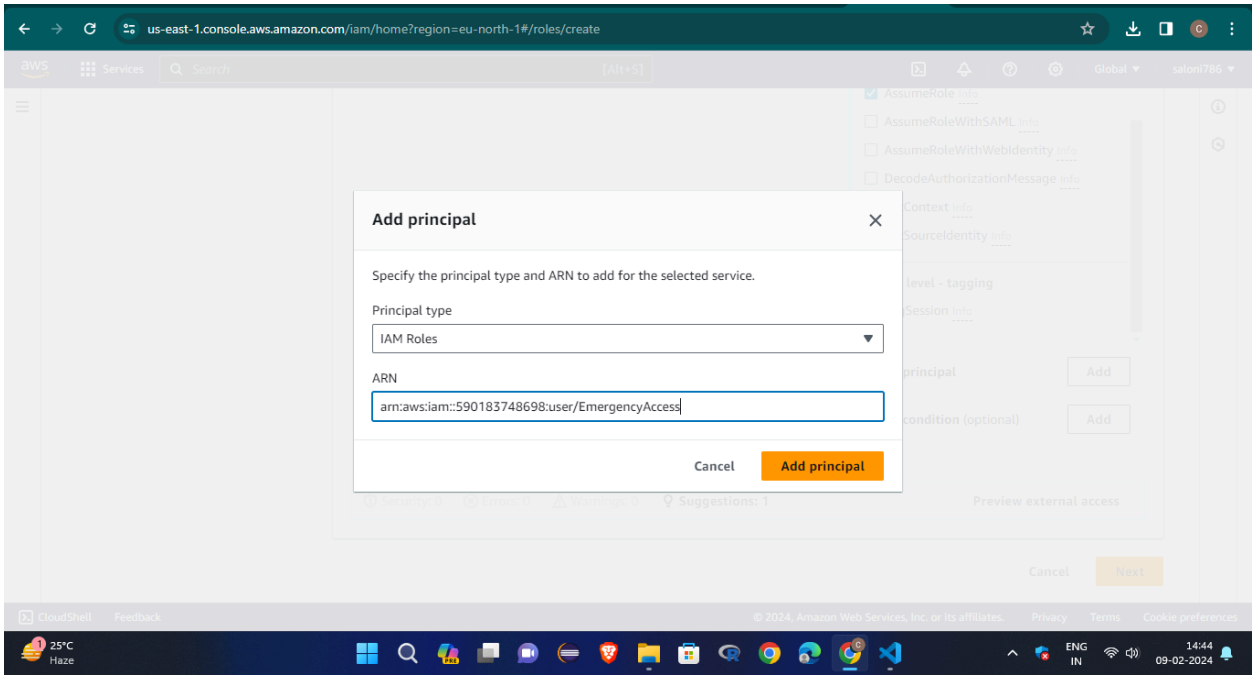

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Services
Search
[Alt+S]
Global
saloni786
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://590183748698.signin.aws.amazon.com/console
User name
EmergencyAccess
Console password
********** Show
Cancel
Download .csv file
Return to users list
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:35
09-02-2024

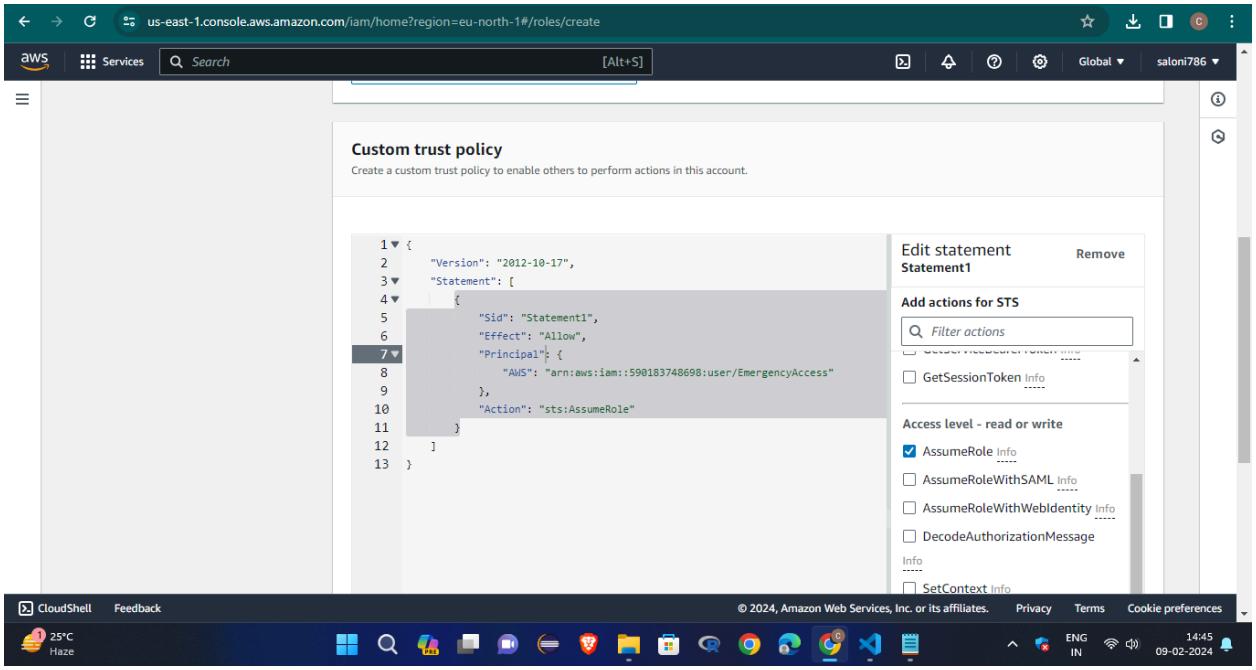

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/EmergencyAccess?section=permissions
Services
Search
[Alt+S]
Global
saloni786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
IAM > Users > EmergencyAccess
EmergencyAccess Info
Delete
Summary
ARN
arn:aws:iam::590183748698:user/EmergencyAccess
Console access
Enabled without MFA
Access key 1
Create access key
Created
February 09, 2024, 14:35 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
SENSEX
+0.13%
ENG
IN
14:37
09-02-2024

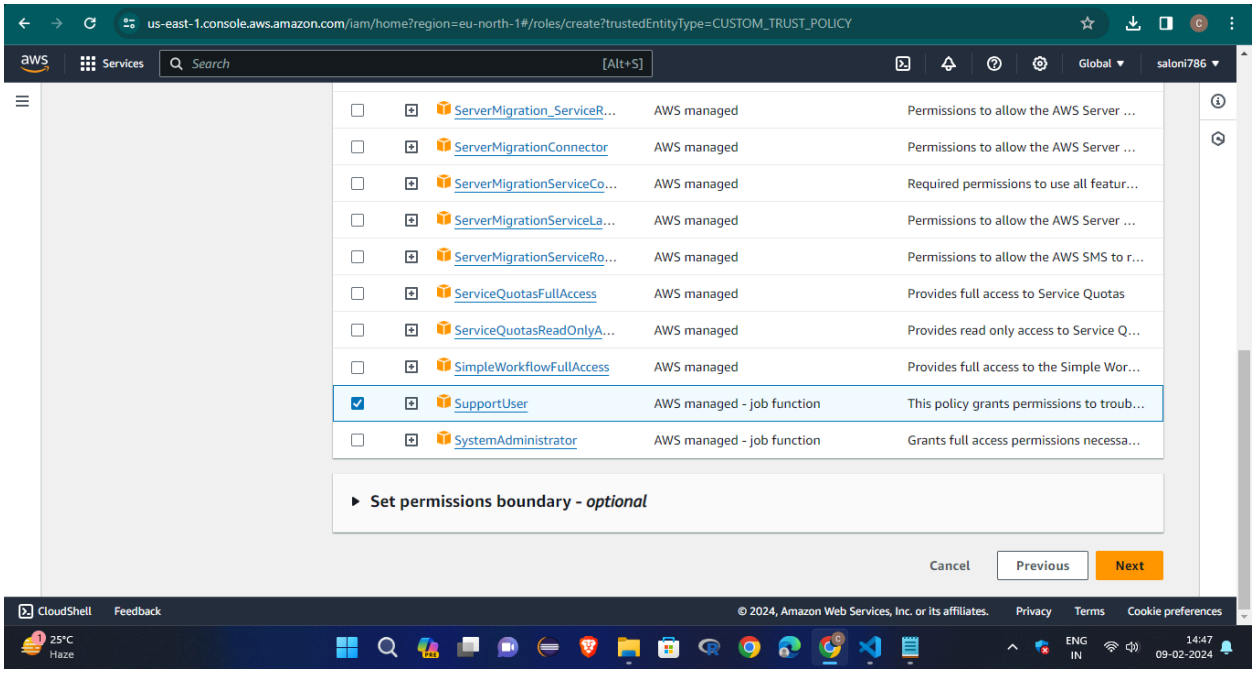

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/EmergencyAccess?section=permissions
Services
Search
[Alt+S]
Global
saloni786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Permissions policies (1)
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
AdministratorAccess
AWS managed - job function
Group EmergencyAccessGroup
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
Generate policy
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
SENSEX
+0.13%
ENG
IN
14:38
09-02-2024

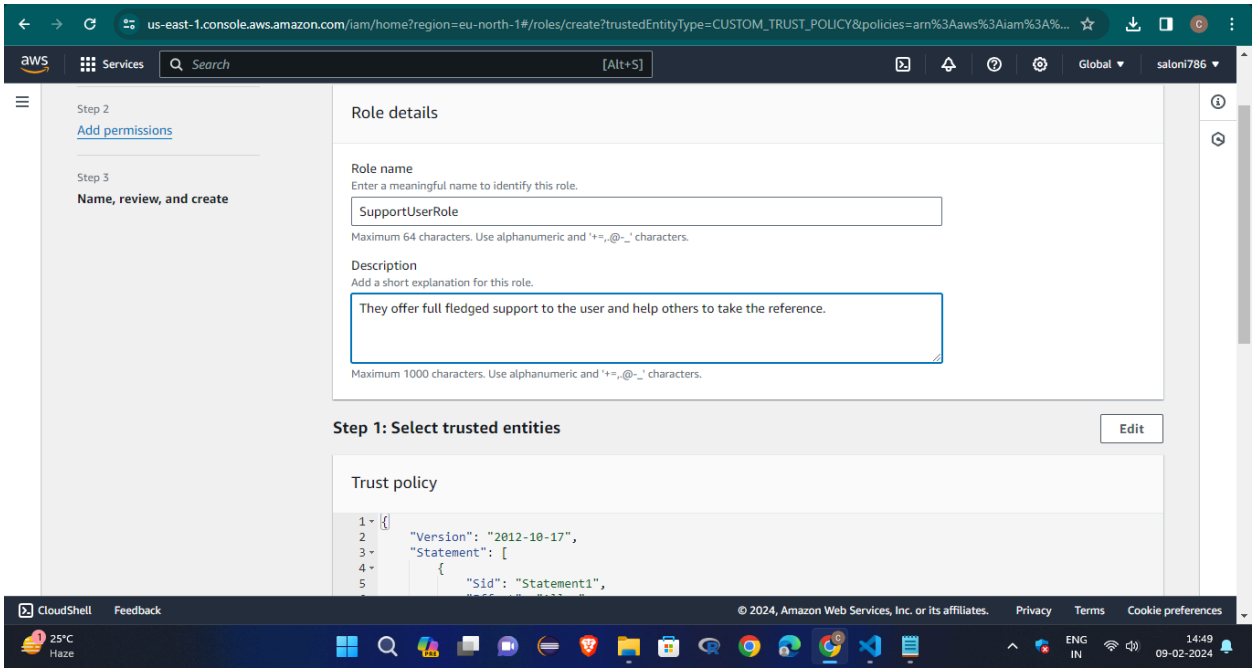

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles
Services
Search
[Alt+S]
Global
saloni786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
IAM
Roles
Roles (2) Info
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.
Delete
Create role
Search
Role name
Trusted entities
Last activity
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
Roles Anywhere Info
Authenticate your non AWS workloads and securely provide access to AWS services.
Manage
Access AWS from your non AWS workloads
X.509 Standard
Temporary credentials
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Nifty bank
+0.80%
ENG
IN
14:39
09-02-2024

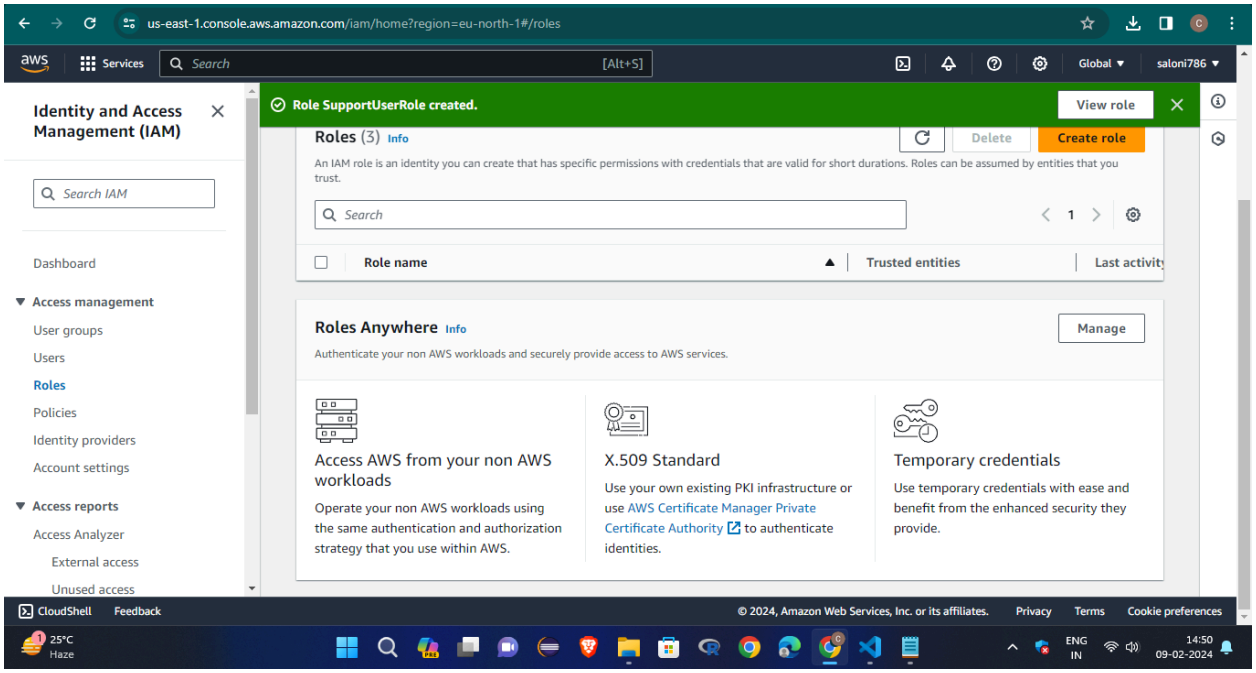

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create
Services
Search
[Alt+S]
Global
saloni786
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services 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.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:42
09-02-2024

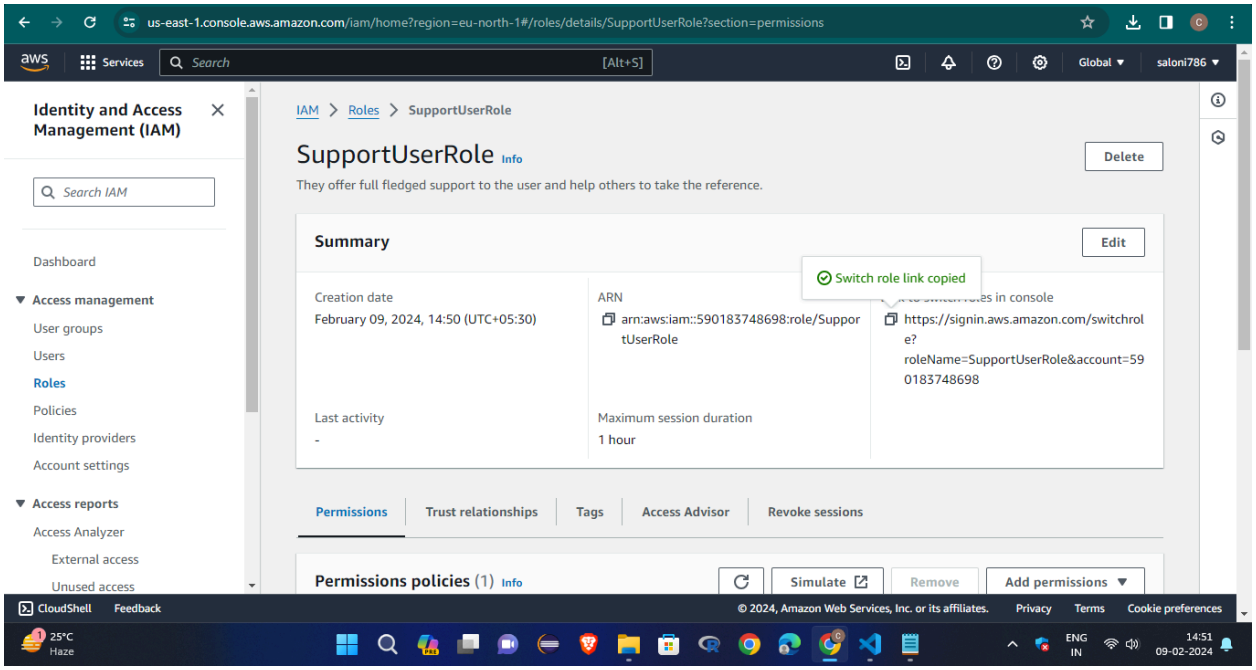

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create
Add principal
Specify the principal type and ARN to add for the selected service.
Principal type
IAM Roles
ARN
arn:aws:iam::590183748698:user/EmergencyAccess
Cancel
Add principal
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:44
09-02-2024

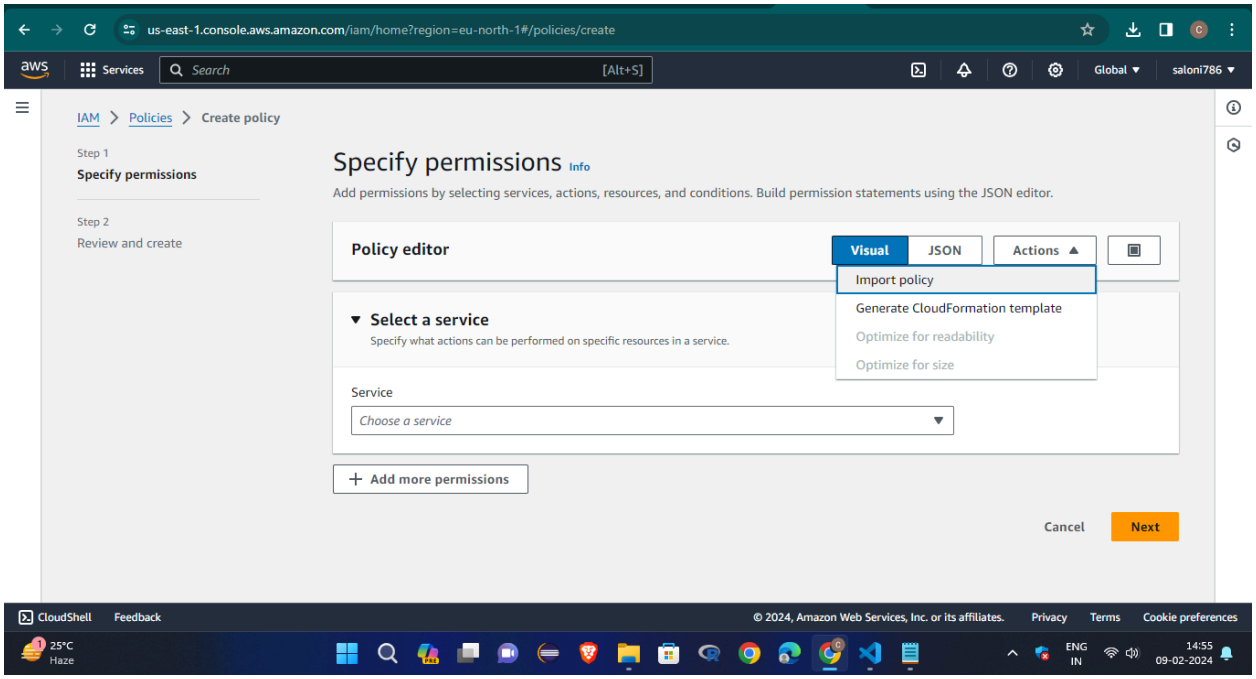

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create
Services
Search
[Alt+S]
Global
saloni786
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::590183748698:user/EmergencyAccess"
},
"Action": "sts:AssumeRole"
}
]
}
Edit statement
Statement1
Remove
Add actions for STS
Filter actions
GetSessionToken Info
Access level - read or write
AssumeRole Info
AssumeRoleWithSAML Info
AssumeRoleWithWebIdentity Info
DecodeAuthorizationMessage
Info
SetContext Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:45
09-02-2024

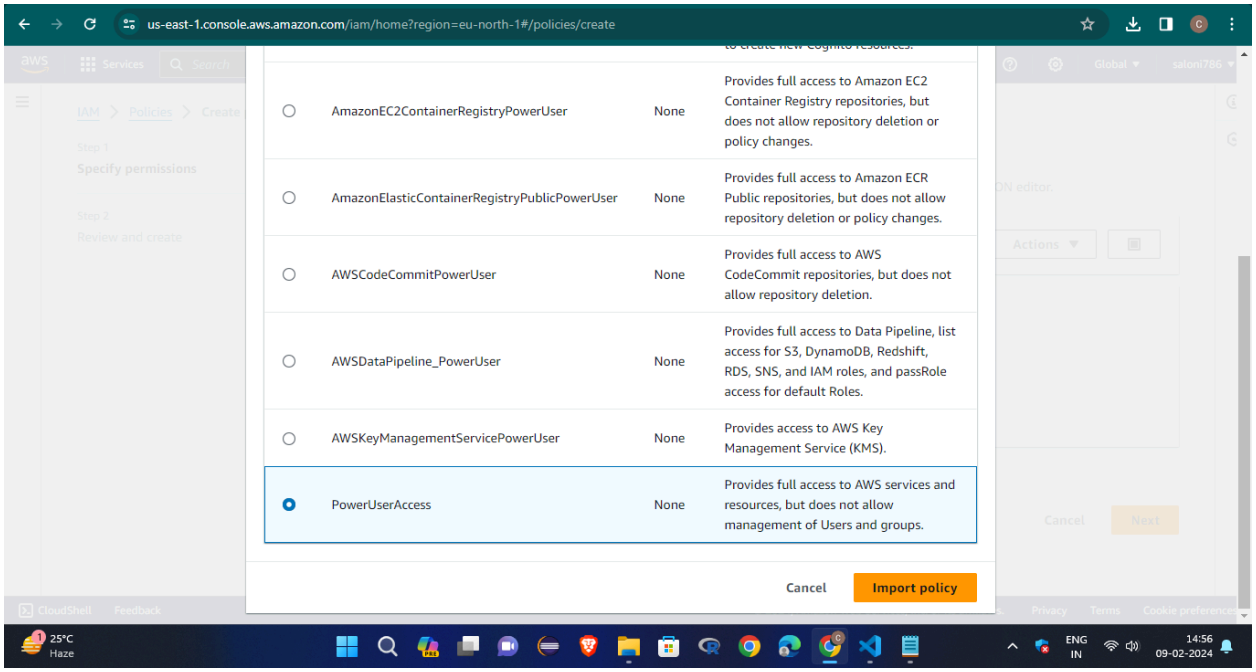

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create?trustedEntityType=CUSTOM_TRUST_POLICY
Services
Search
[Alt+S]
Global
saloni786
ServerMigration_ServiceR... AWS managed Permissions to allow the AWS Server ...
ServerMigrationConnector AWS managed Permissions to allow the AWS Server ...
ServerMigrationServiceCo... AWS managed Required permissions to use all featur...
ServerMigrationServiceLa... AWS managed Permissions to allow the AWS Server ...
ServerMigrationServiceRo... AWS managed Permissions to allow the AWS SMS to r...
ServiceQuotasFullAccess AWS managed Provides full access to Service Quotas
ServiceQuotasReadOnlyA... AWS managed Provides read only access to Service Q...
SimpleWorkflowFullAccess AWS managed Provides full access to the Simple Wor...
SupportUser AWS managed - job function This policy grants permissions to troub...
SystemAdministrator AWS managed - job function Grants full access permissions necessa...
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:47
09-02-2024

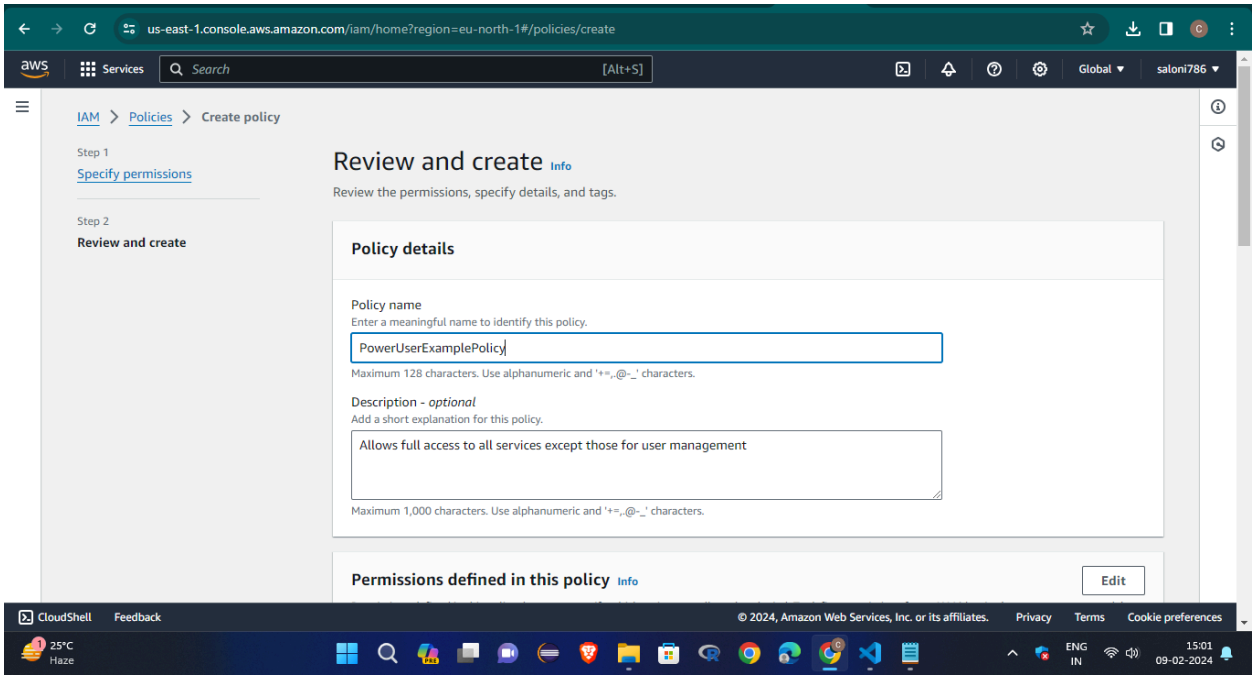

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create?trustedEntityType=CUSTOM_TRUST_POLICY&policies=arn%3Aaws%3Aiam%3A%...
Services
Search
[Alt+S]
Global
saloni786
Step 2
Add permissions
Step 3
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
SupportUserRole
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
They offer full fledged support to the user and help others to take the reference.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:49
09-02-2024

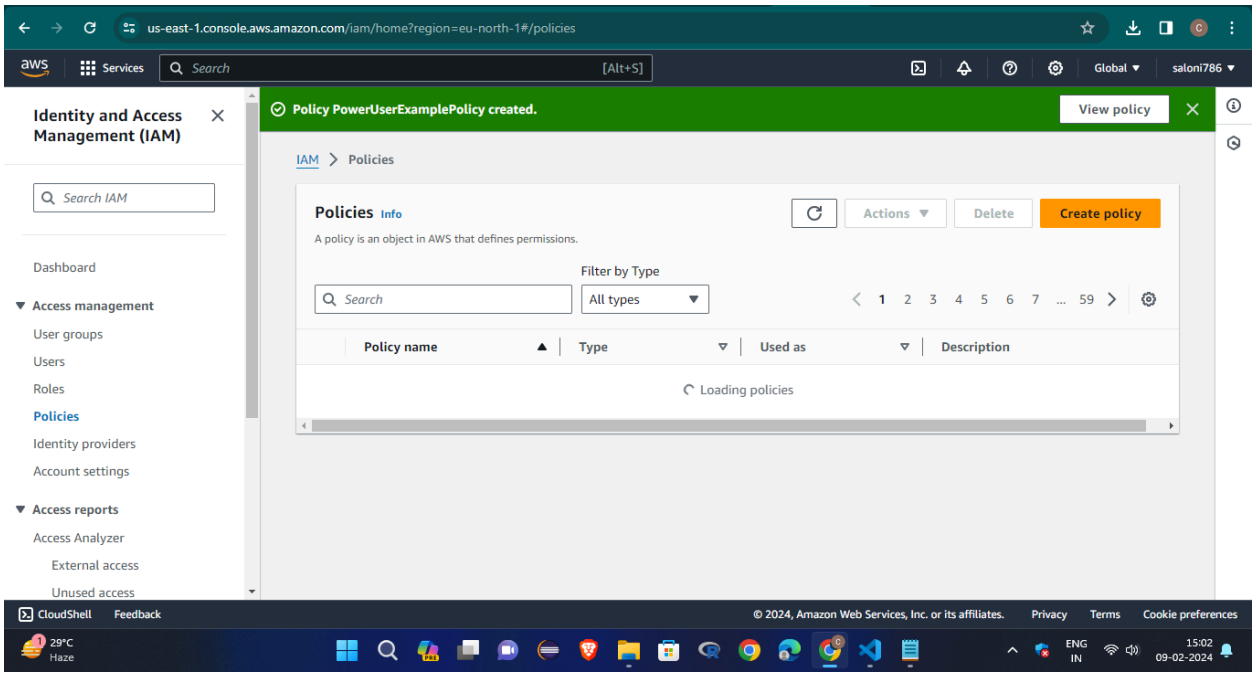

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles
Services
Search
[Alt+S]
Global
saloni786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Role SupportUserRole created.
View role
Roles (3) 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
Last activity
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.
X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.
Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:50
09-02-2024


us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/details/SupportUserRole?section=permissions
Services
Search
[Alt+S]
Global
saloni786
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
IAM > Roles > SupportUserRole
SupportUserRole Info
They offer full fledged support to the user and help others to take the reference.
Delete
Summary
Edit
Switch role link copied
Creation date
February 09, 2024, 14:50 (UTC+05:30)
ARN
arn:aws:iam::590183748698:role/SupportUserRole
https://signin.aws.amazon.com/switchrole?roleName=SupportUserRole&account=590183748698
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions
Permissions policies (1) Info
Simulate
Remove
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:51
09-02-2024


us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create
Services
Search
[Alt+S]
Global
saloni786
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
Import policy
Generate CloudFormation template
Optimize for readability
Optimize for size
Select a service
Specify what actions can be performed on specific resources in a service.
Service
Choose a service
Add more permissions
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
14:55
09-02-2024

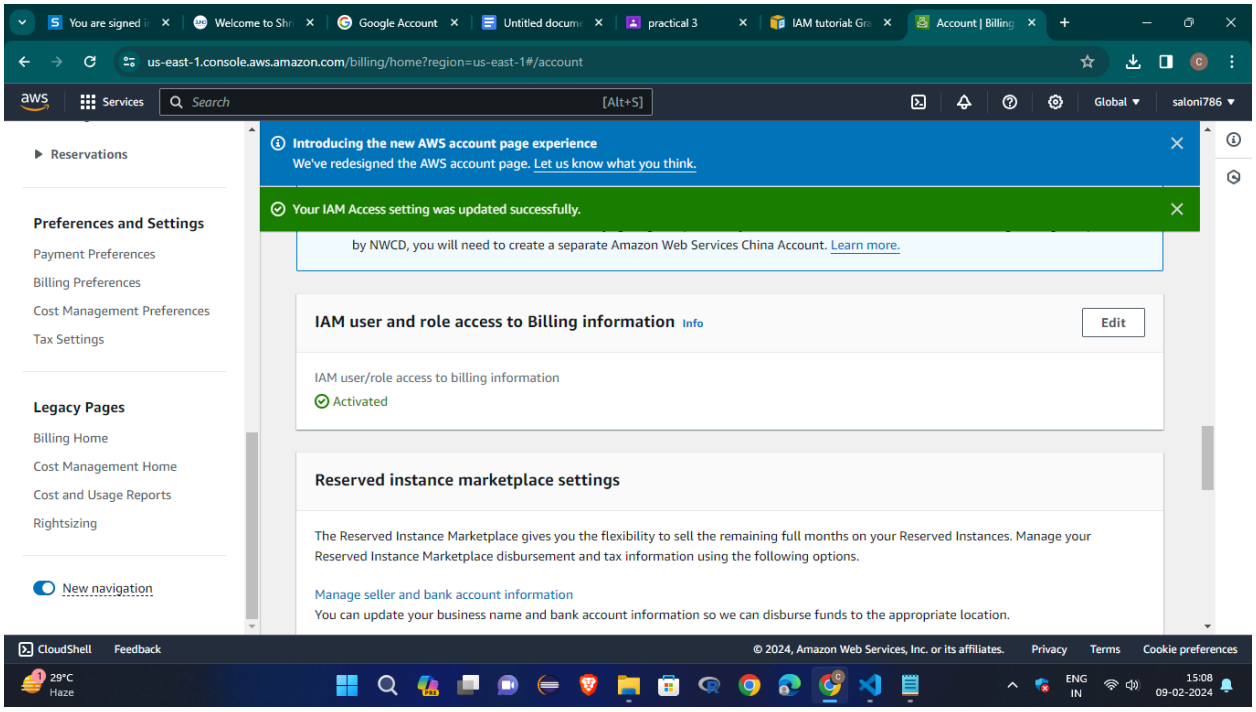

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create
AmazonEC2ContainerRegistryPowerUser
None
Provides full access to Amazon EC2 Container Registry repositories, but does not allow repository deletion or policy changes.
AmazonElasticContainerRegistryPublicPowerUser
None
Provides full access to Amazon ECR Public repositories, but does not allow repository deletion or policy changes.
AWSCodeCommitPowerUser
None
Provides full access to AWS CodeCommit repositories, but does not allow repository deletion.
AWSDataPipeline_PowerUser
None
Provides full access to Data Pipeline, list access for S3, DynamoDB, Redshift, RDS, SNS, and IAM roles, and passRole access for default Roles.
AWSKeyManagementServicePowerUser
None
Provides access to AWS Key Management Service (KMS).
PowerUserAccess
None
Provides full access to AWS services and resources, but does not allow management of Users and groups.
Cancel
Import policy

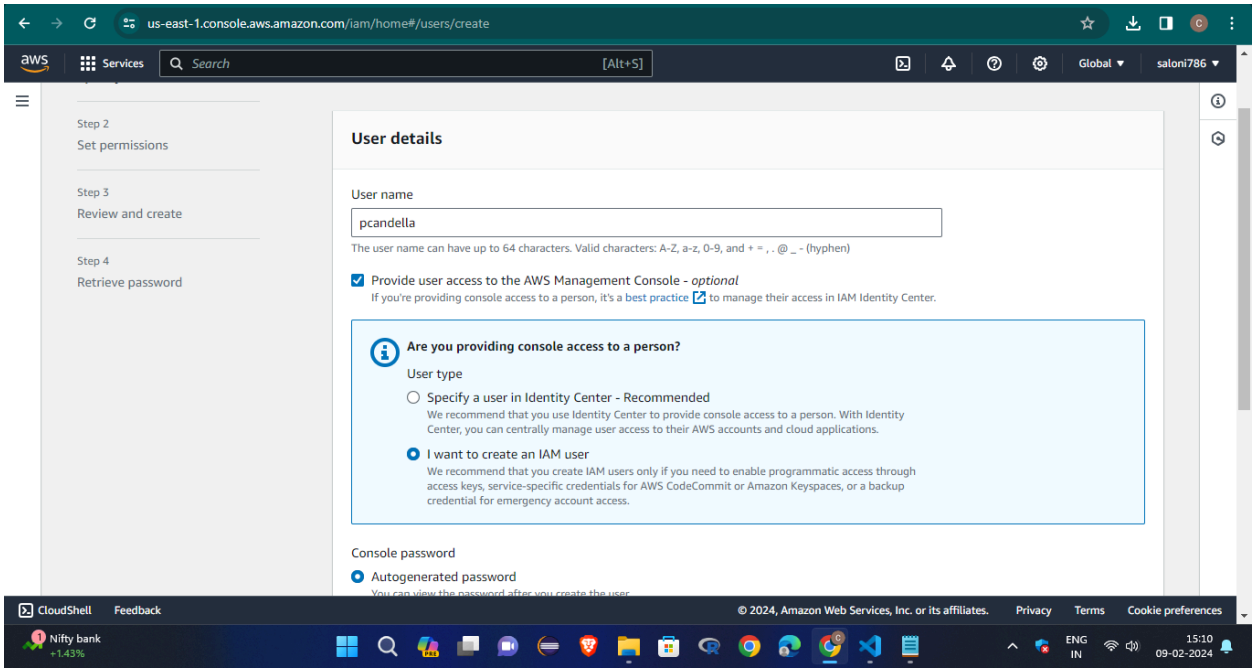

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create
Services
Search
[Alt+S]
Global
saloni786
IAM
Policies
Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
PowerUserExamplePolicy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Allows full access to all services except those for user management
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

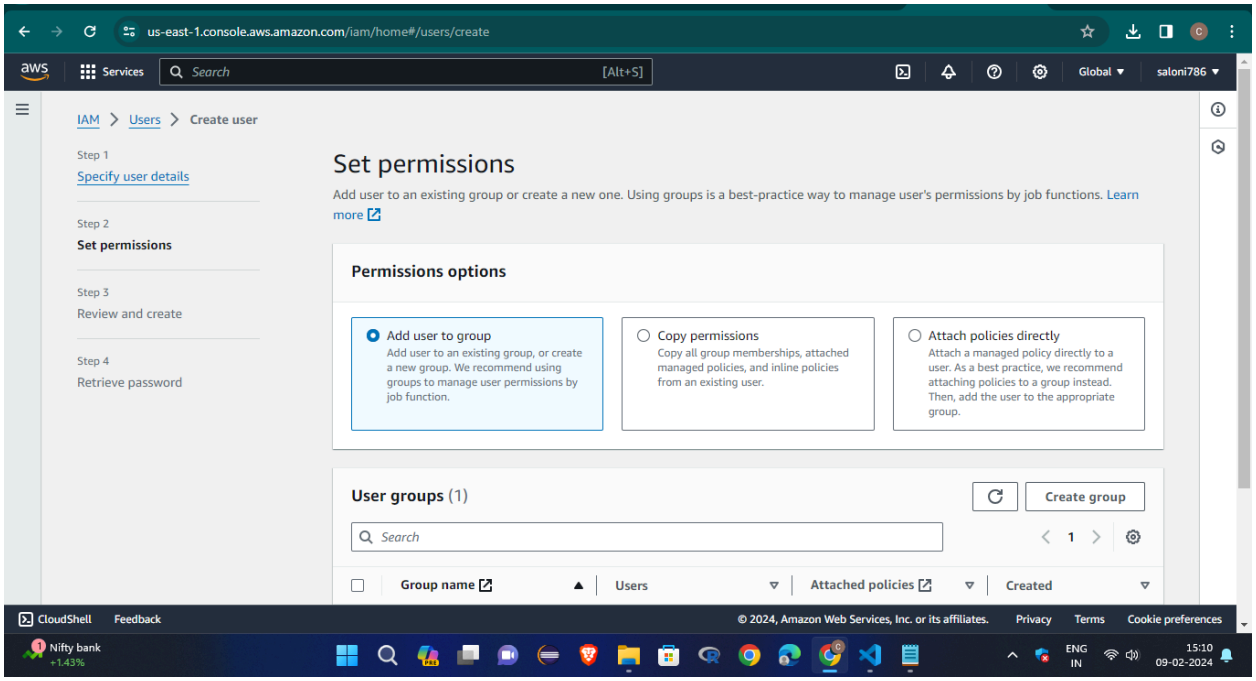


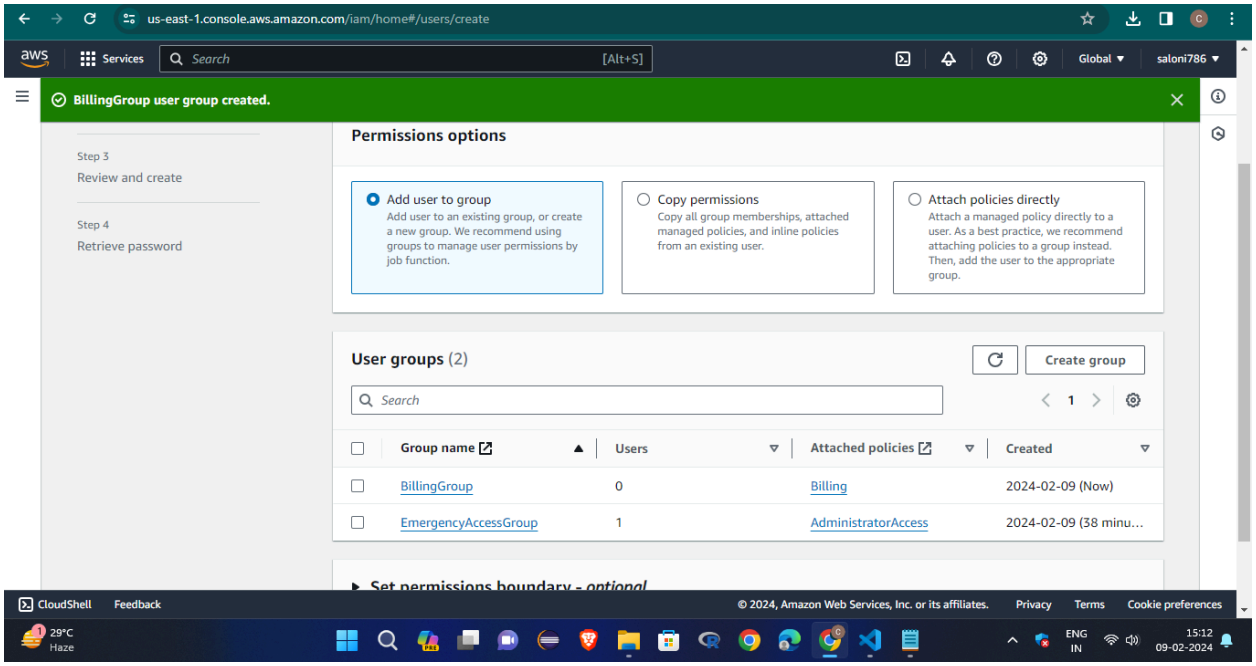
TASK 2:

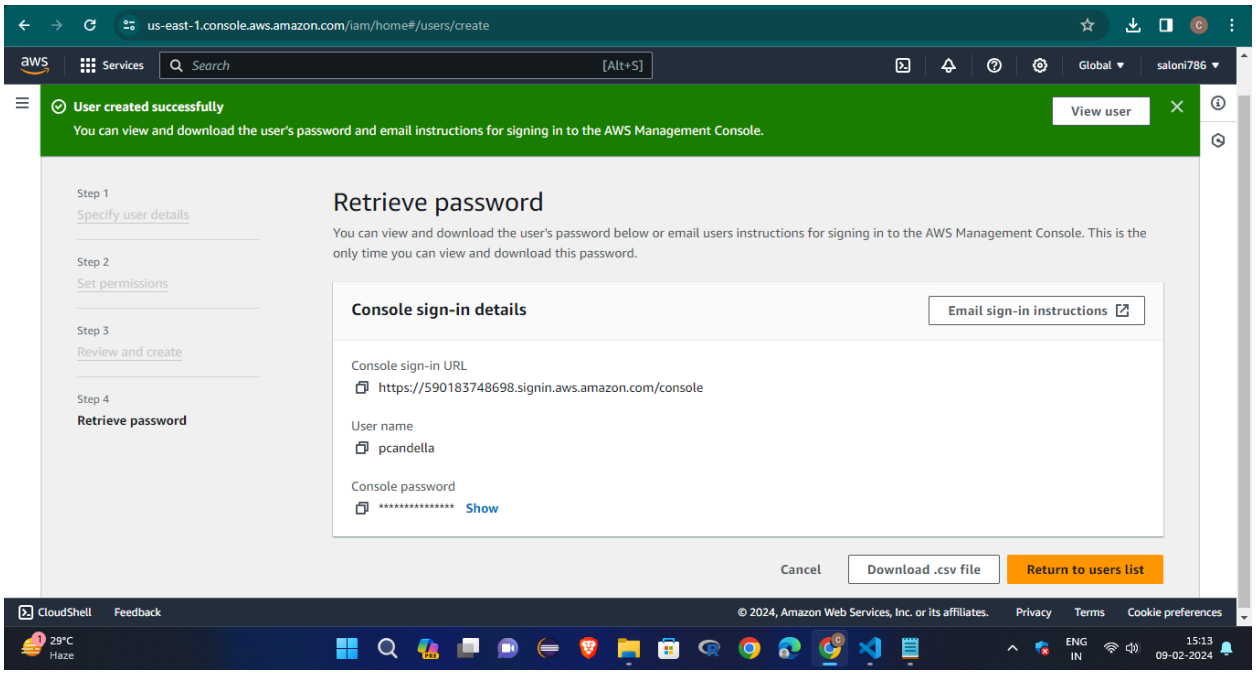
Grant access to the billing console

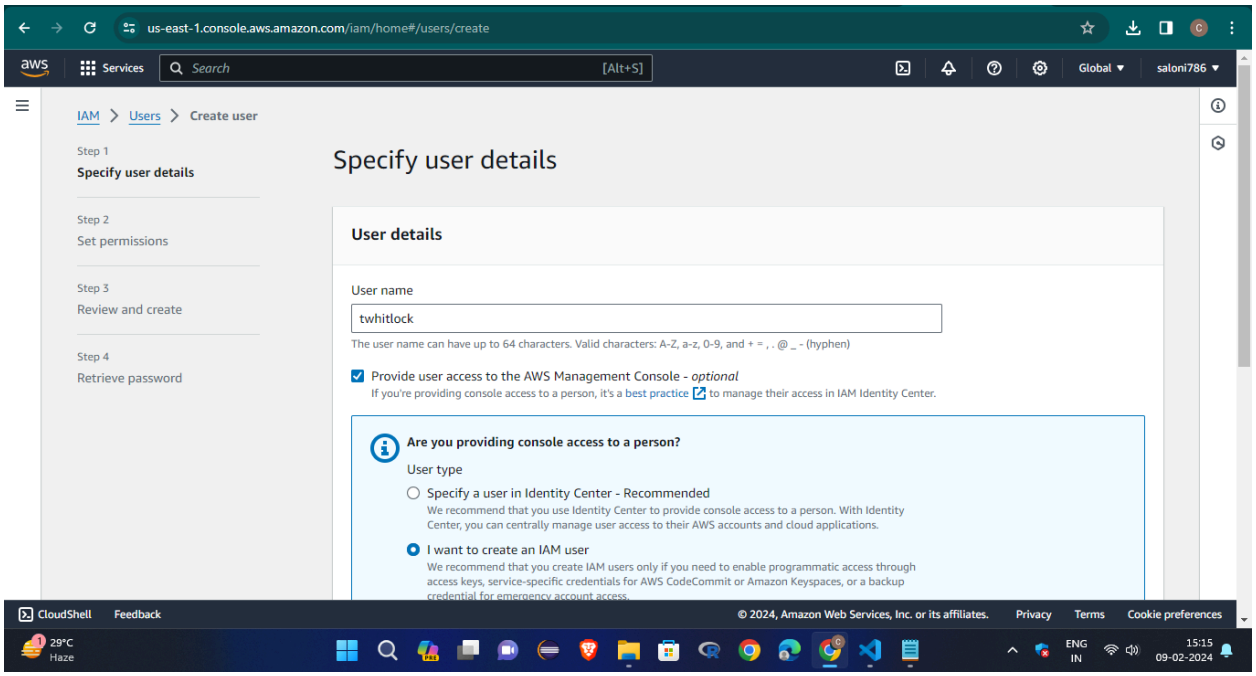


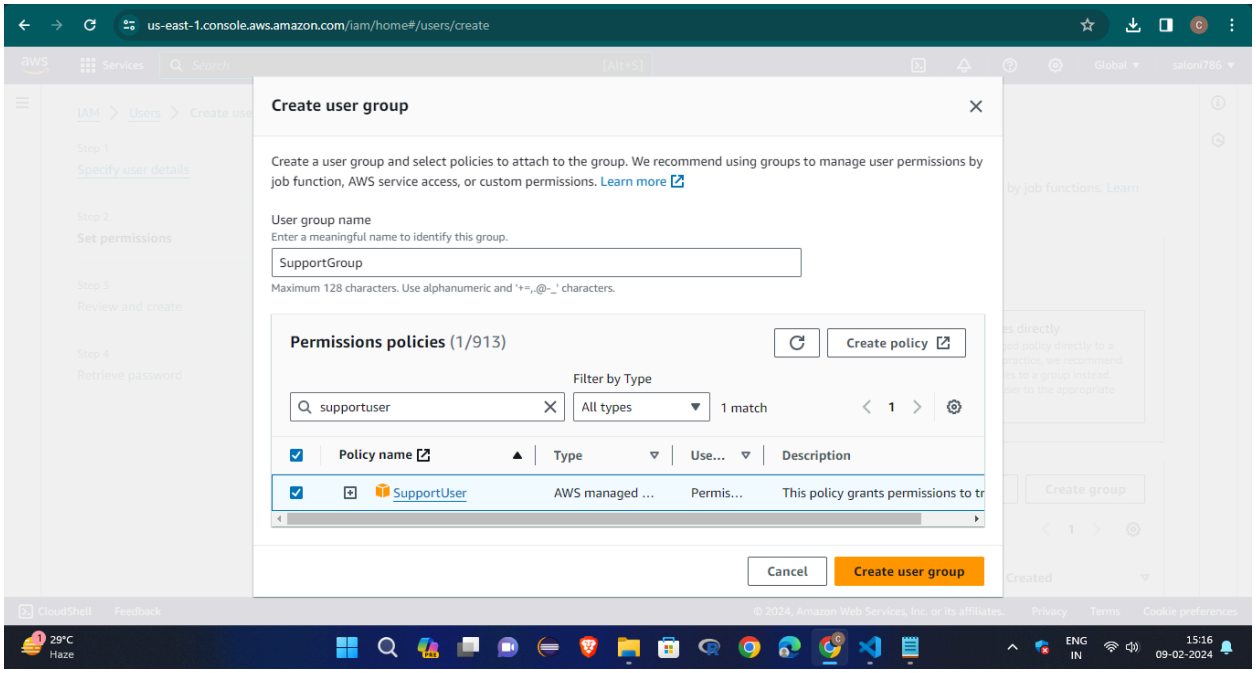

us-east-1.console.aws.amazon.com/iam/home#/users/create
Services
Search
[Alt+S]
Global
saloni786
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
User details
User name
pcandella
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
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.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Nifty bank
+1.43%
ENG
IN
15:10
09-02-2024

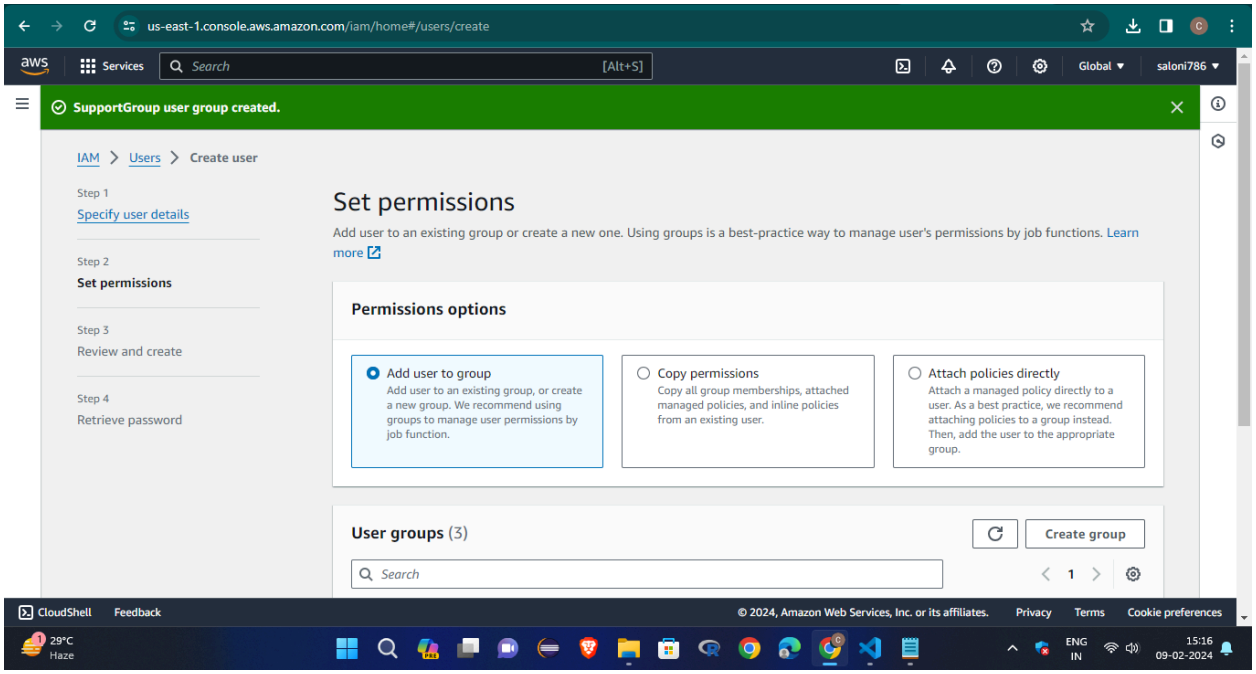

us-east-1.console.aws.amazon.com/iam/home#/users/create
Services
Search
[Alt+S]
Global
saloni786
IAM
Users
Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is 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.
User groups (1)
Create group
Search
1
Group name
Users
Attached policies
Created
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Nifty bank
+1.43%
ENG
IN
15:10
09-02-2024

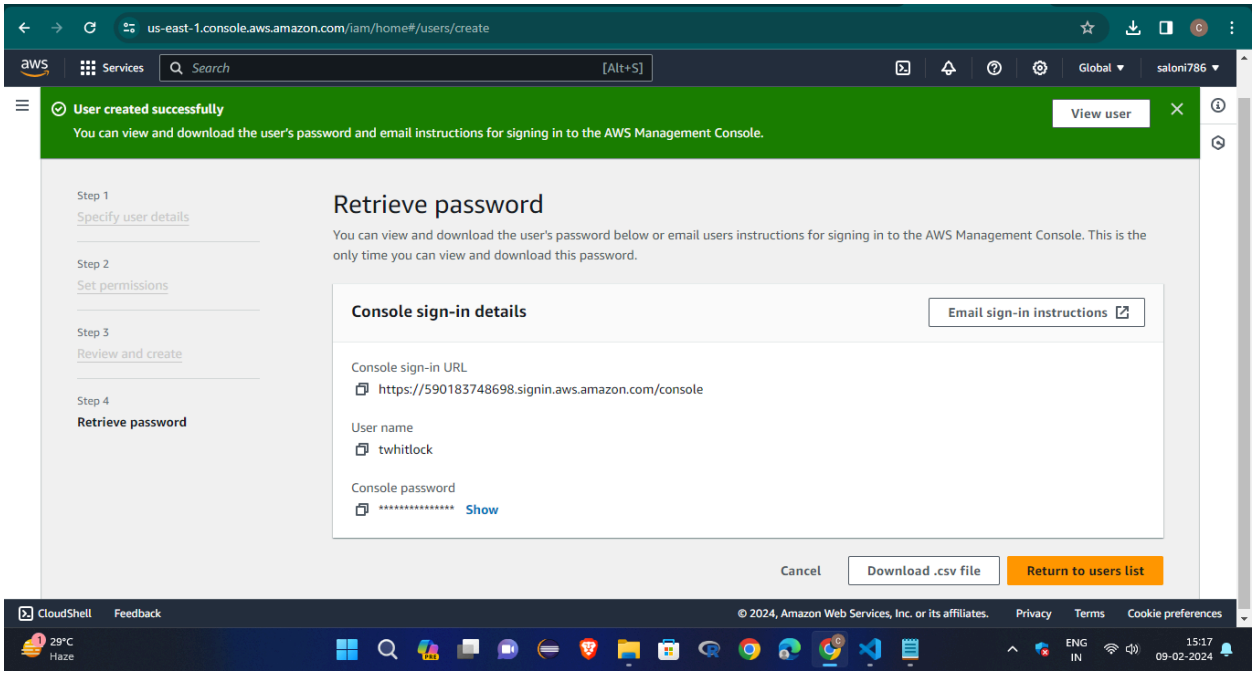

us-east-1.console.aws.amazon.com/iam/home#/users/create
Services
Search
[Alt+S]
Global
saloni786
BillingGroup user group created.
Step 3
Review and create
Step 4
Retrieve password
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to 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.
User groups (2)
Create group
Search
1
Group name
Users
Attached policies
Created
BillingGroup
0
Billing
2024-02-09 (Now)
EmergencyAccessGroup
1
AdministratorAccess
2024-02-09 (38 minu...
Set permissions boundary - optional
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Haze
ENG
IN
15:12
09-02-2024

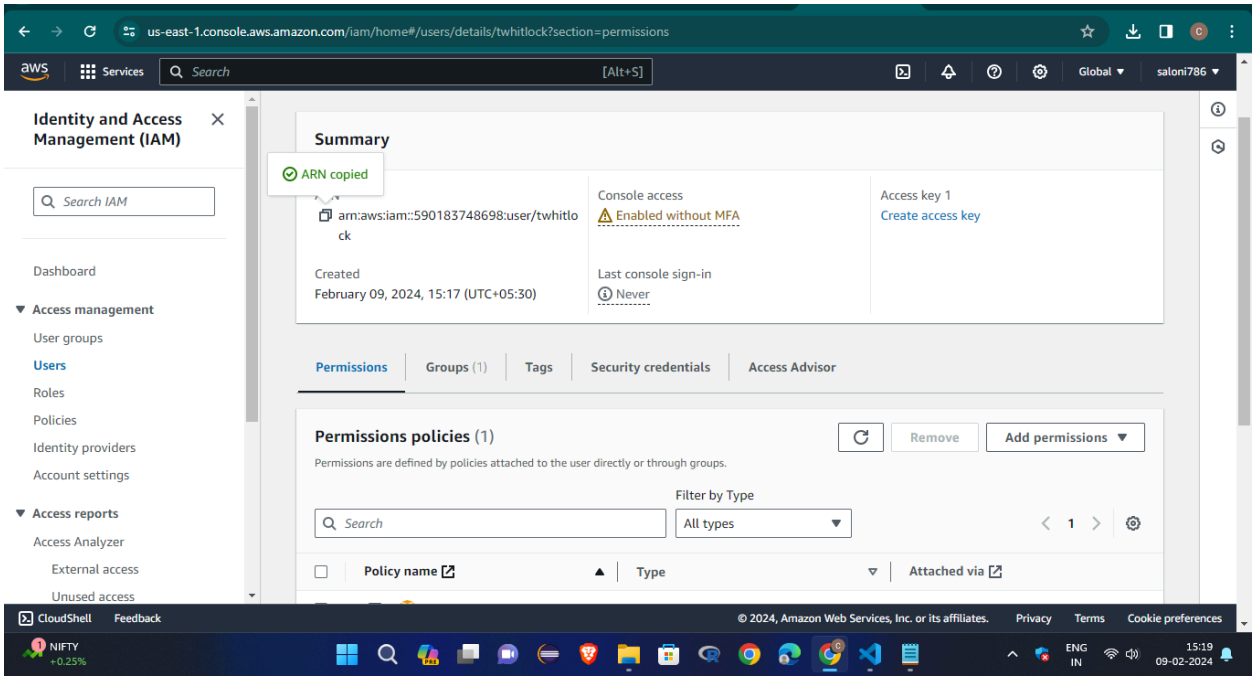

us-east-1.console.aws.amazon.com/iam/home#/users/create
Services
Search
[Alt+S]
Global
saloni786
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://590183748698.signin.aws.amazon.com/console
User name
pcandella
Console password
********** Show
Cancel
Download .csv file
Return to users list
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Haze
ENG
IN
15:13
09-02-2024

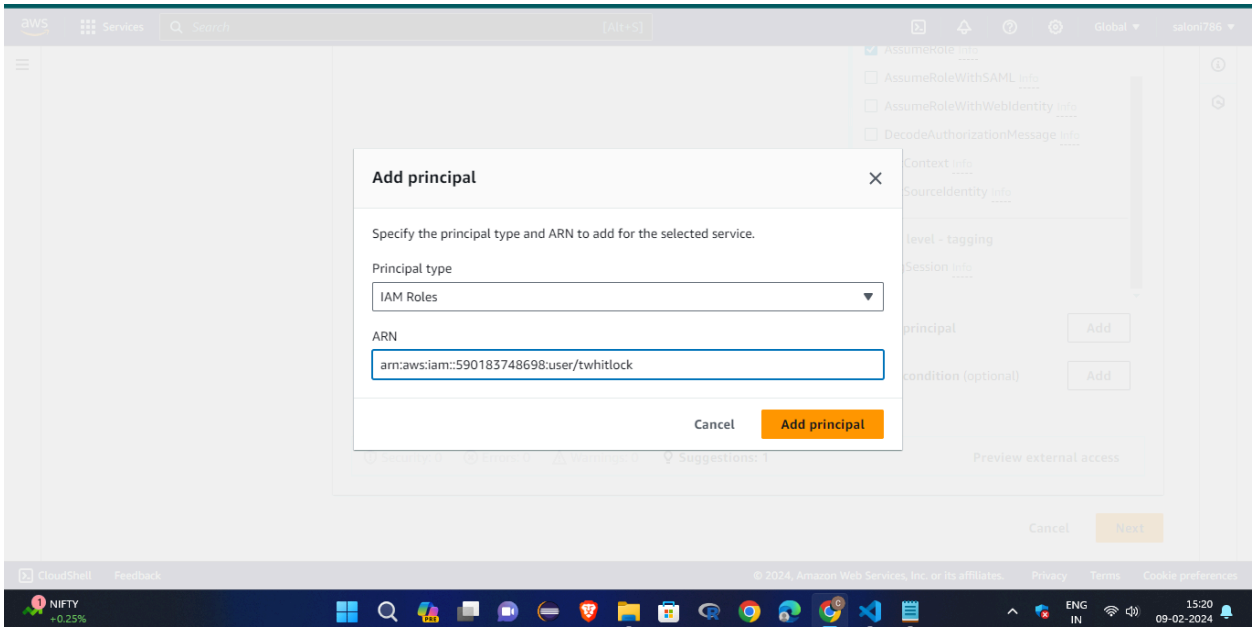

us-east-1.console.aws.amazon.com/iam/home#/users/create
Services
Search
[Alt+S]
Global
saloni786
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
twhitlock
The user name can have 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.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Haze
ENG
IN
15:15
09-02-2024

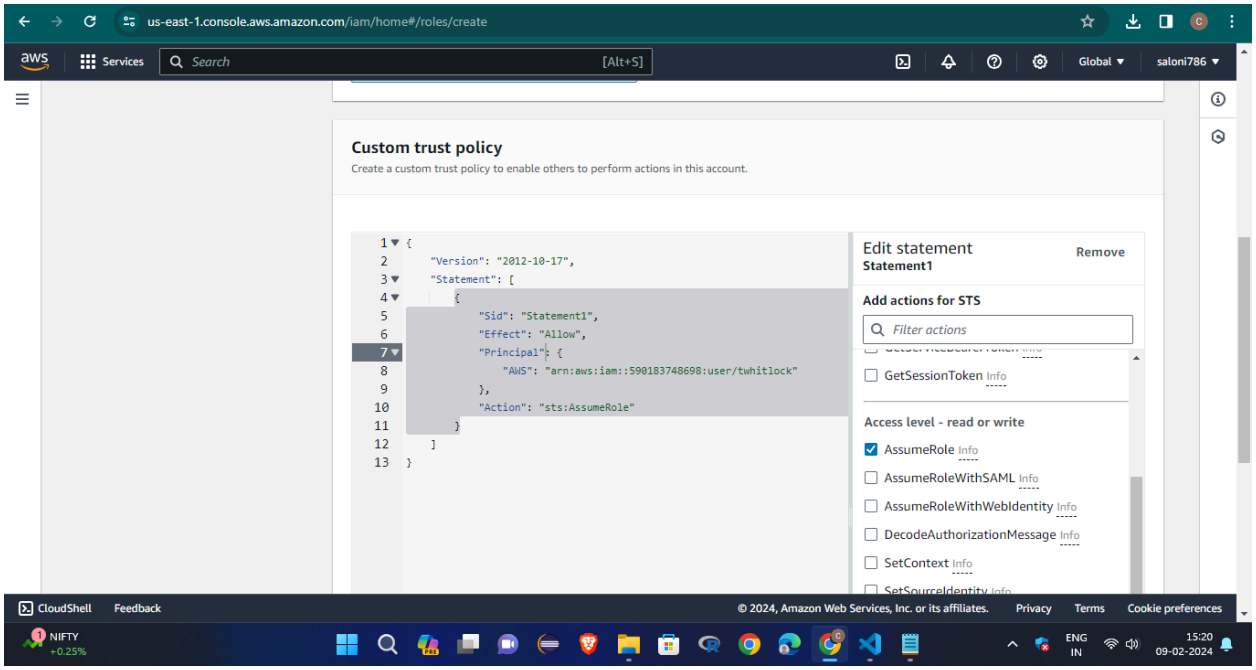

us-east-1.console.aws.amazon.com/iam/home#/users/create
Create user group
Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
User group name
Enter a meaningful name to identify this group.
SupportGroup
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions policies (1/913)
Create policy
Filter by Type
supportuser
All types
1 match
Policy name
Type
Use...
Description
SupportUser
AWS managed ...
Permis...
This policy grants permissions to tr
Cancel
Create user group
29°C
Haze
ENG
IN
15:16
09-02-2024

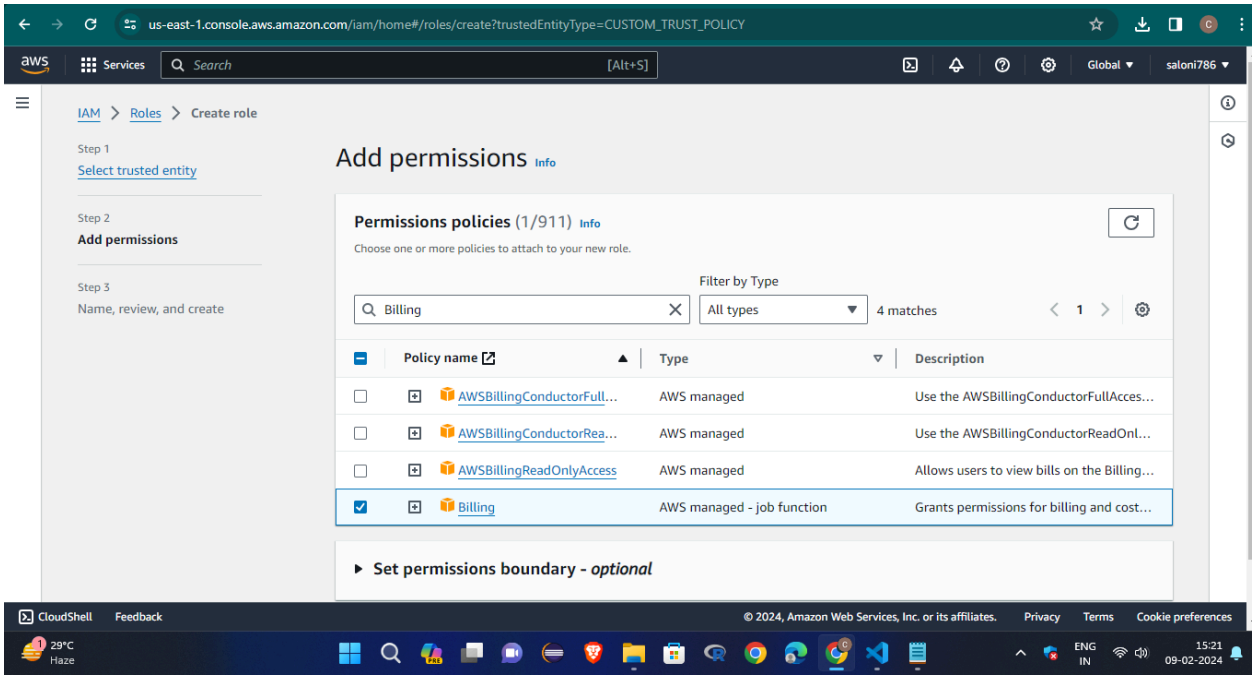

us-east-1.console.aws.amazon.com/iam/home#/users/create
Services
Search
[Alt+S]
Global
saloni786
SupportGroup user group created.
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group 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.
User groups (3)
Create group
Search
1
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Haze
ENG
IN
15:16
09-02-2024

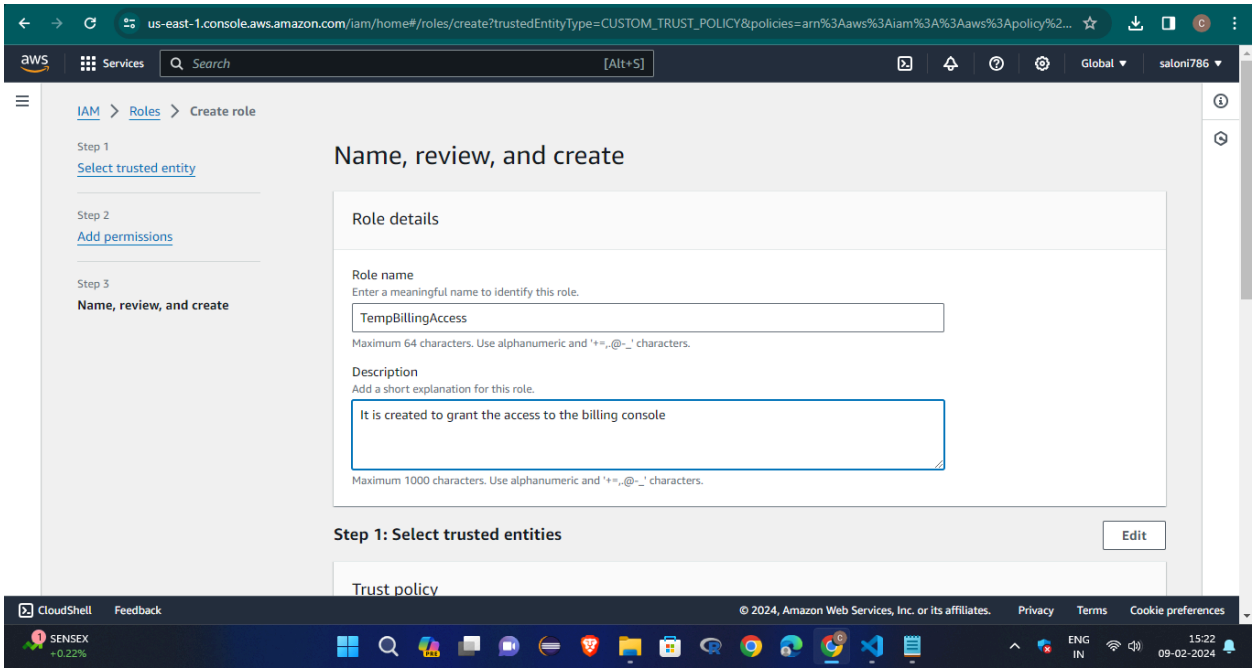

us-east-1.console.aws.amazon.com/iam/home#/users/create
Services
Search
[Alt+S]
Global
saloni786
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://590183748698.signin.aws.amazon.com/console
User name
twhitlock
Console password
********** Show
Cancel
Download .csv file
Return to users list
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Haze
ENG
IN
15:17
09-02-2024

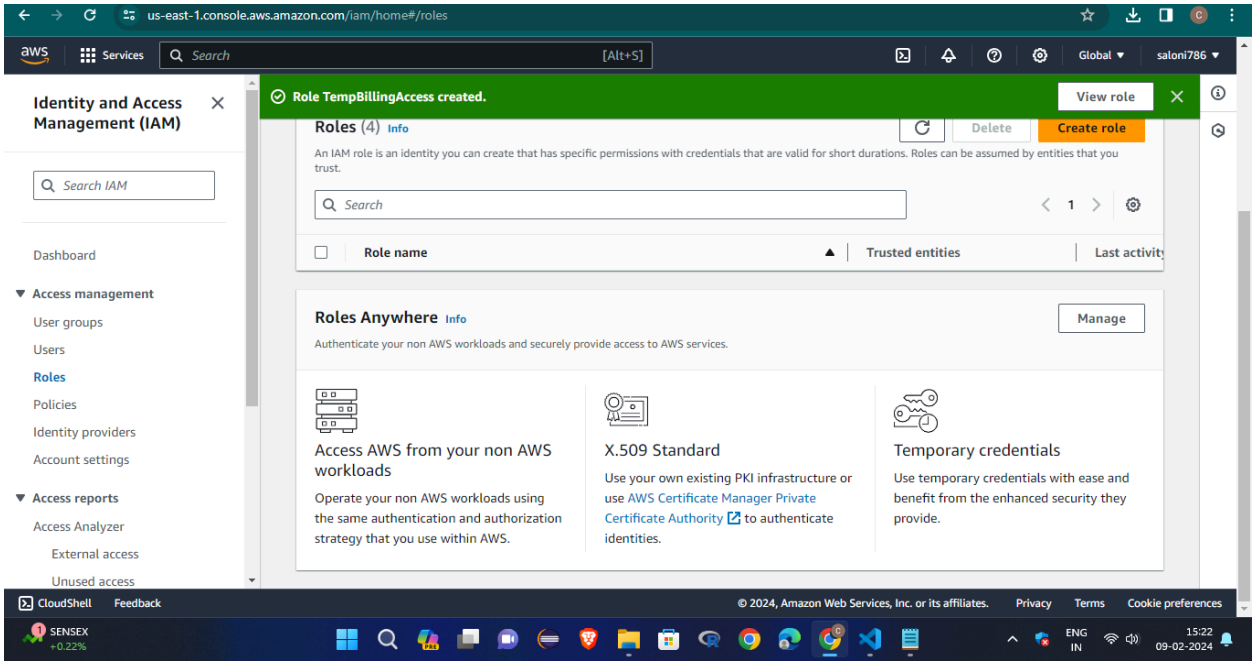

us-east-1.console.aws.amazon.com/iam/home#/users/details/twhitlock?section=permissions
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Summary
ARN copied
arn:aws:iam::590183748698:user/twhitlock
Console access
Enabled without MFA
Access key 1
Create access key
Created
February 09, 2024, 15:17 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Permissions policies (1)
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Add principal
Specify the principal type and ARN to add for the selected service.
Principal type
IAM Roles
ARN
arn:aws:iam::590183748698:user/twhitlock
Cancel
Add principal

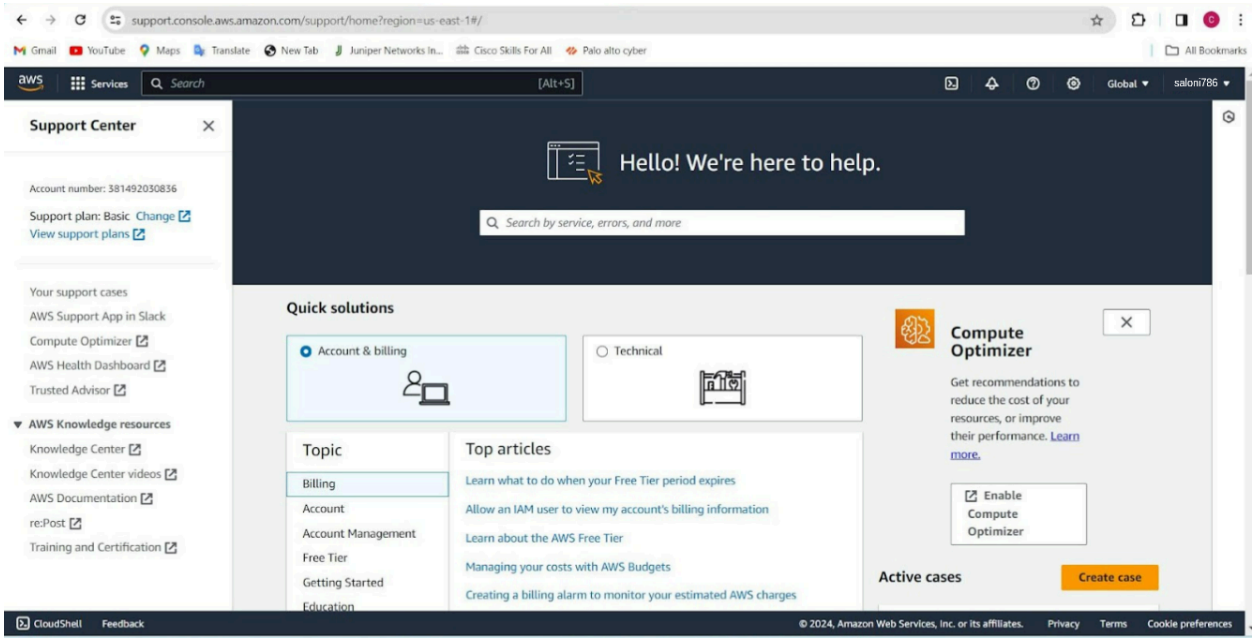

us-east-1.console.aws.amazon.com/iam/home#/roles/create
Services
Search
[Alt+S]
Global
saloni786
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::590183748698:user/twhitlock"
},
"Action": "sts:AssumeRole"
}
]
}
Edit statement
Statement1
Remove
Add actions for STS
Filter actions
GetSessionToken Info
Access level - read or write
AssumeRole Info
AssumeRoleWithSAML Info
AssumeRoleWithWebIdentity Info
DecodeAuthorizationMessage Info
SetContext Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
NIFTY
+0.25%
ENG
IN
15:20
09-02-2024

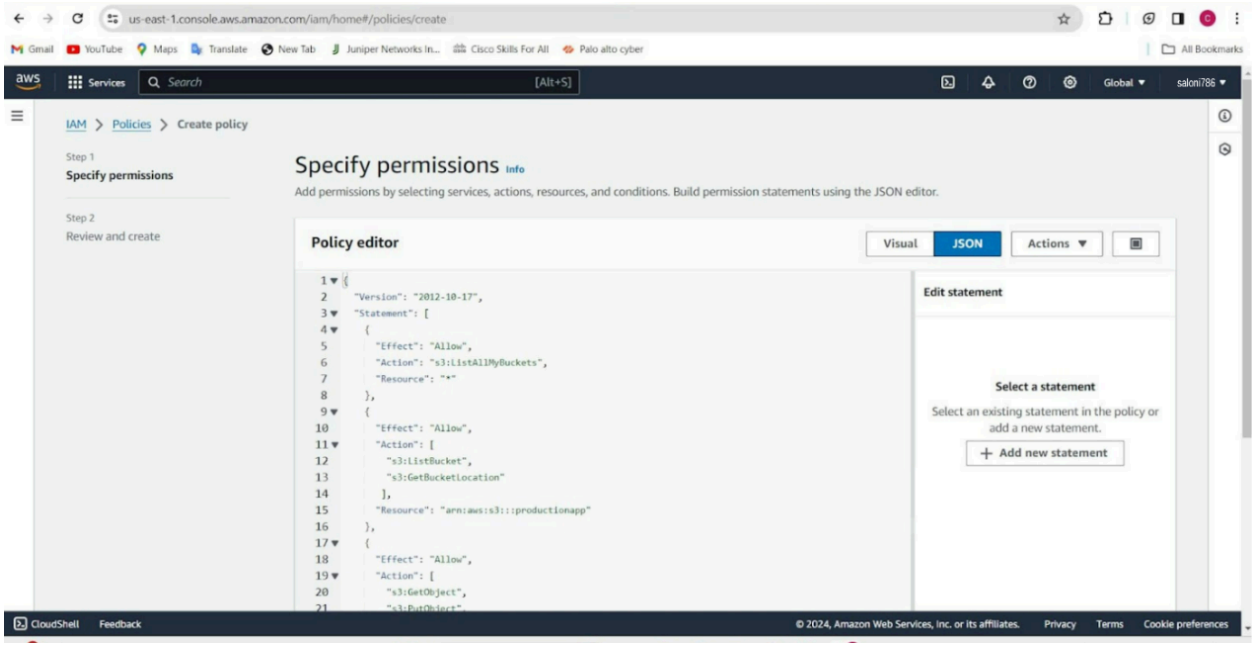

us-east-1.console.aws.amazon.com/iam/home#/roles/create?trustedEntityType=CUSTOM_TRUST_POLICY
Services
Search
[Alt+S]
Global
saloni786
IAM
Roles
Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/911) Info
Choose one or more policies to attach to your new role.
Filter by Type
Billing
All types
4 matches
1
Policy name
Type
Description
AWSBillingConductorFull...
AWS managed
Use the AWSBillingConductorFullAcces...
AWSBillingConductorRea...
AWS managed
Use the AWSBillingConductorReadOnl...
AWSBillingReadOnlyAccess
AWS managed
Allows users to view bills on the Billing...
Billing
AWS managed - job function
Grants permissions for billing and cost...
Set permissions boundary - optional
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Haze
ENG
IN
15:21
09-02-2024

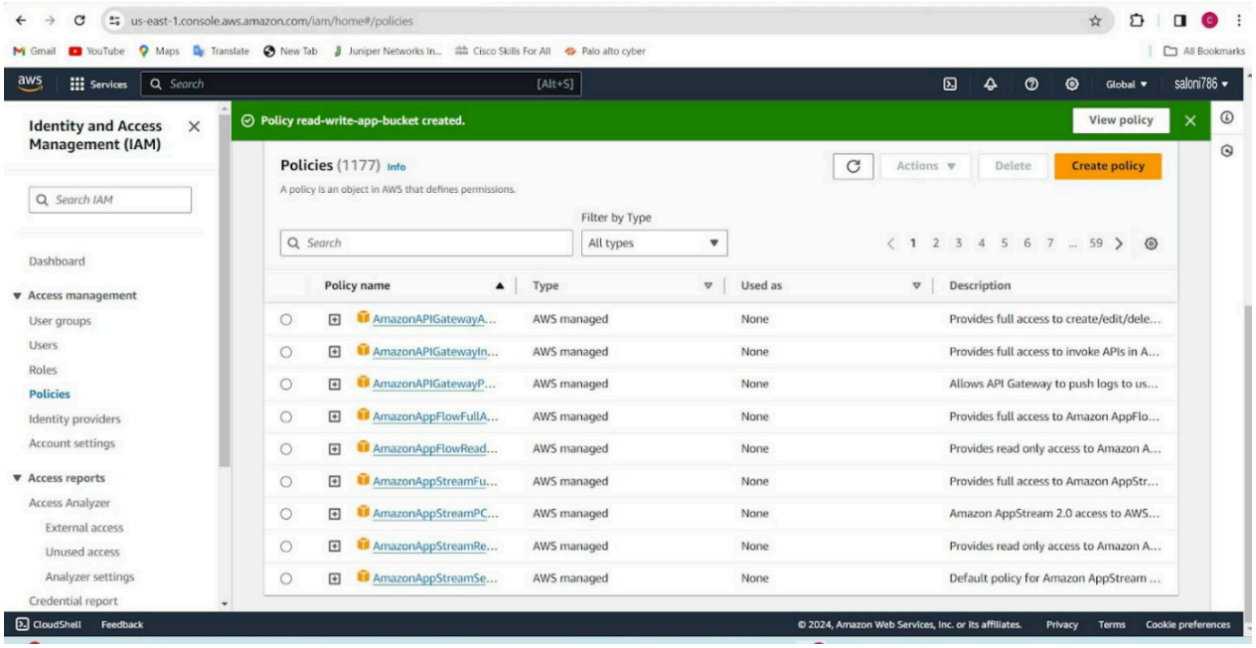

us-east-1.console.aws.amazon.com/iam/home#/roles/create?trustedEntityType=CUSTOM_TRUST_POLICY&policies=arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2...
Services
Search
[Alt+S]
Global
saloni786
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
TempBillingAccess
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
It is created to grant the access to the billing console
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
SENSEX
+0.22%
ENG
IN
15:22
09-02-2024

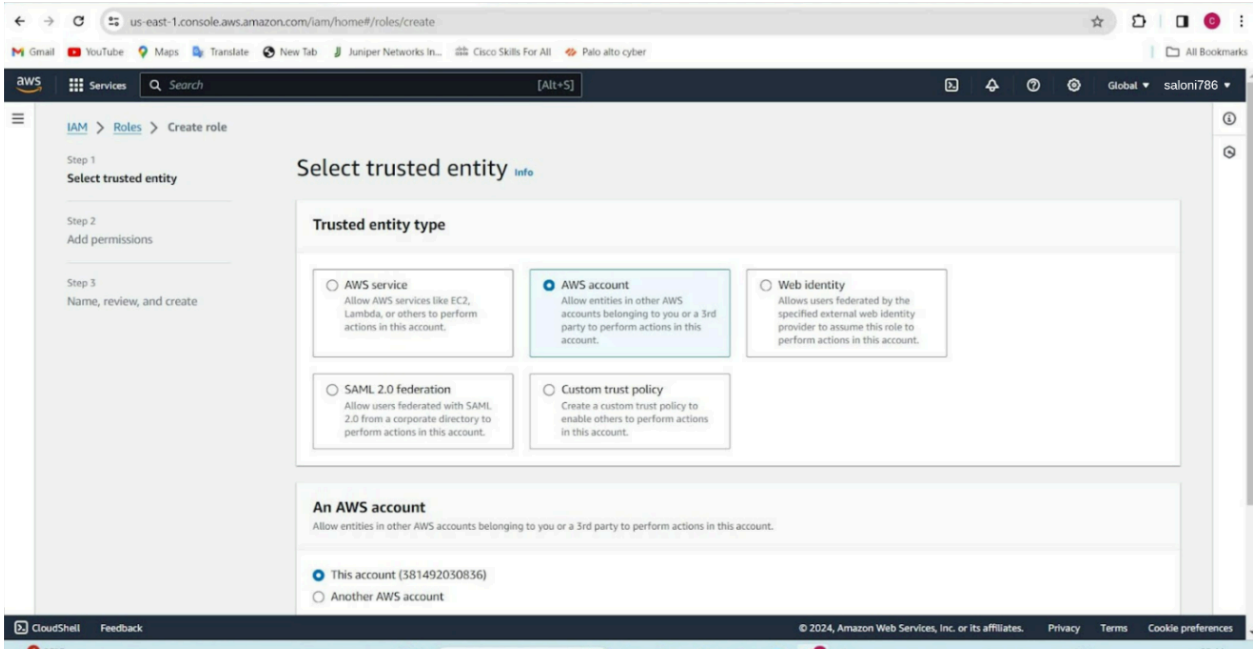

us-east-1.console.aws.amazon.com/iam/home#/roles
Services
Search
[Alt+S]
Global
saloni786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Role TempBillingAccess created.
View role
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
1
Role name
Trusted entities
Last activity
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.
X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.
Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
SENSEX
+0.22%
ENG
IN
15:22
09-02-2024

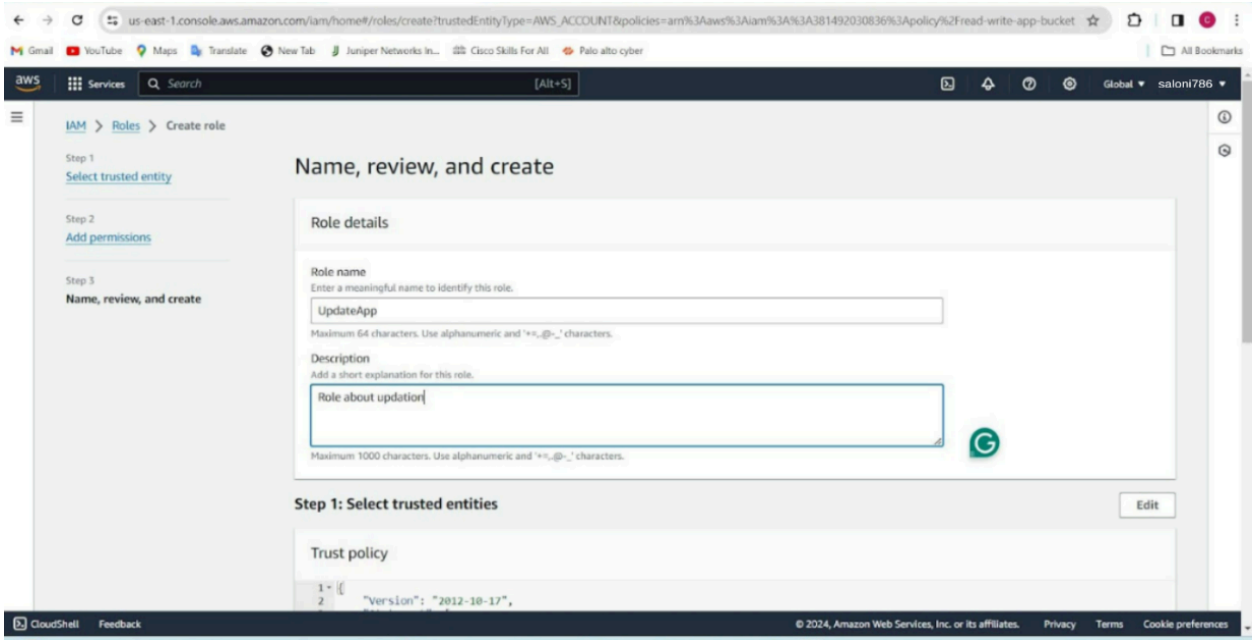
Delegate access across AWS accounts using roles

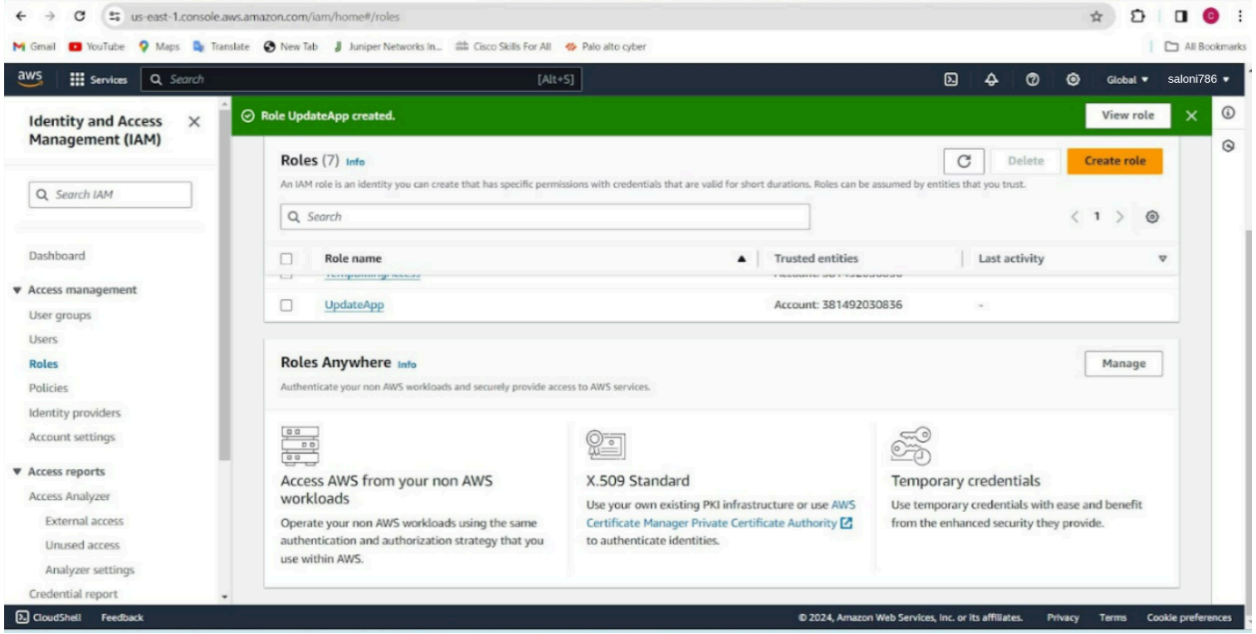


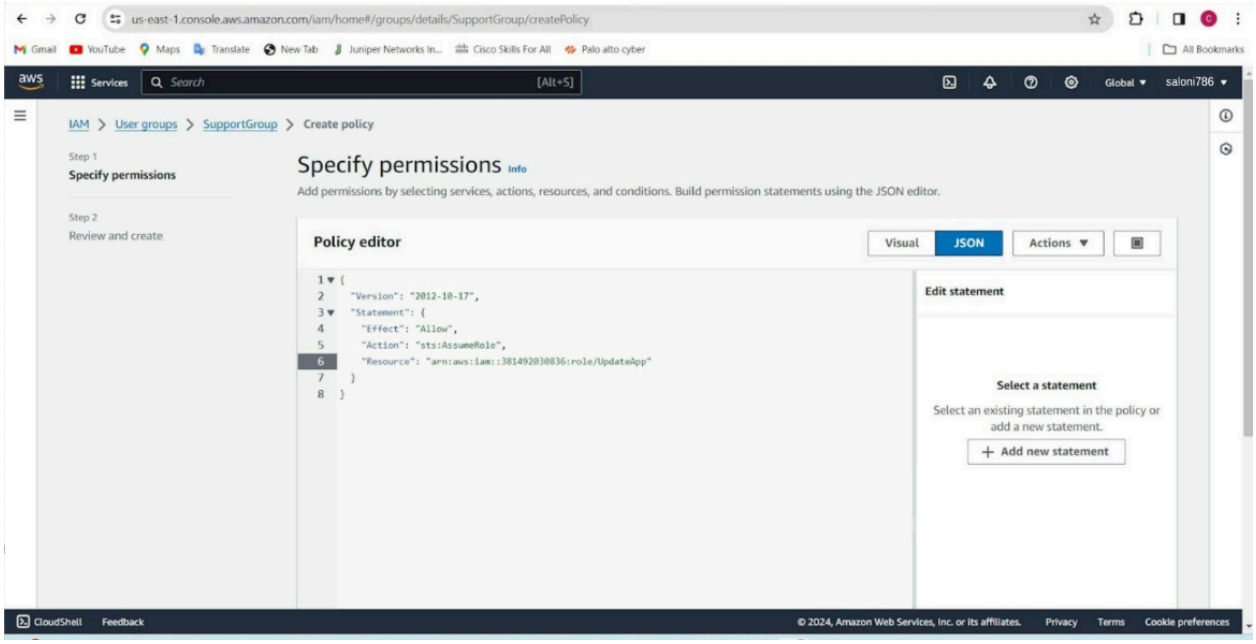


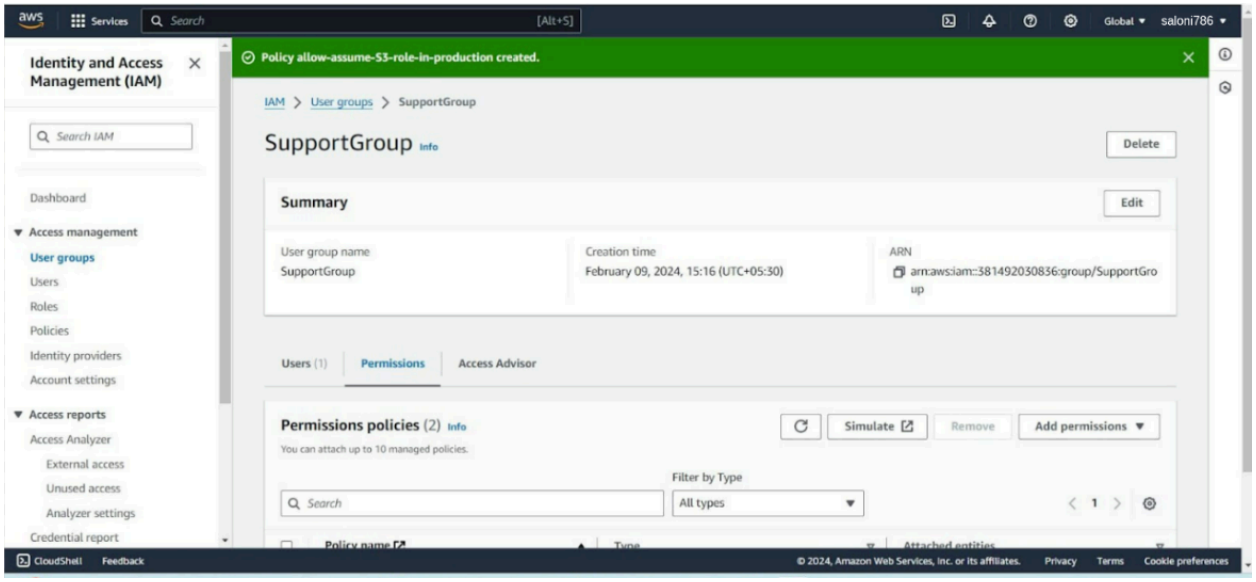

us-east-1.console.aws.amazon.com/iam/home#/policies
Identity and Access Management (IAM)
Policy read-write-app-bucket created.
View policy
Policies (1177) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Search IAM
Search
Filter by Type
All types
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Policy name
Type
Used as
Description
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...
AmazonAppStreamSe...
AWS managed
None
Default policy for Amazon AppStream ...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/iam/home#/roles/create
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.
An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
This account (381492030836)
Another AWS account
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

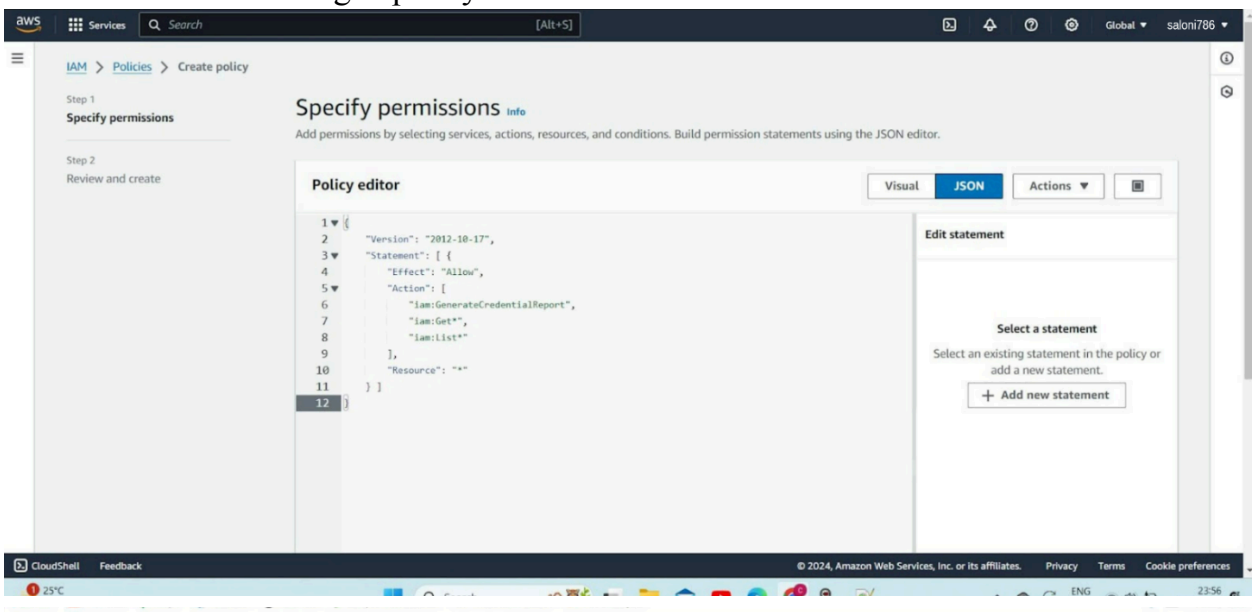

us-east-1.console.aws.amazon.com/iam/home#/roles/create?trustedEntityType=AWS_ACCOUNT&policies=arn%3Aaws%3Aiam%3A%3A381492030836%3Apolicy%2Fread-write-app-bucket
Gmail YouTube Maps Translate New Tab Juniper Networks In... Cisco Skills For All Palo alto cyber
All Bookmarks
aws Services Search [Alt+S] Global saloni786
IAM > Roles > Create role
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.
UpdateApp
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Role about updation
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
CloudShell Feedback
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

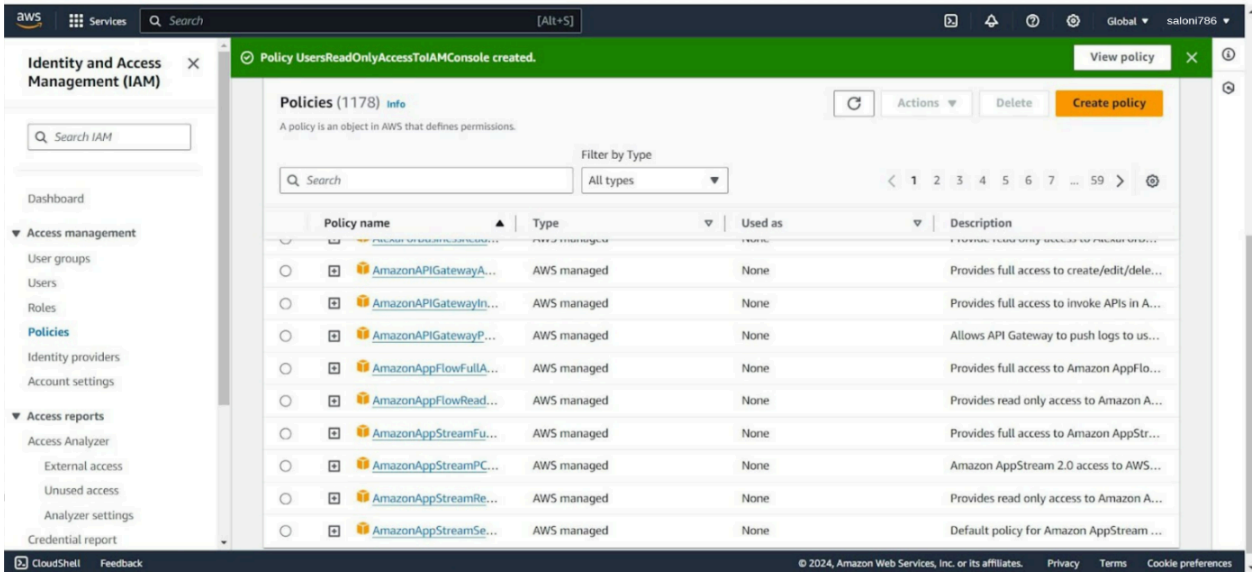

us-east-1.console.aws.amazon.com/iam/home#/roles
Gmail YouTube Maps Translate New Tab Juniper Networks In... Cisco Skills For All Palo alto cyber
All Bookmarks
aws Services Search [Alt+S] Global saloni786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Role UpdateApp created.
View role
Roles (7) Info
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.
Delete
Create role
Search
Role name
Trusted entities
Last activity
UpdateApp
Account: 381492030836
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.
X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.
Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.
CloudShell Feedback
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences


us-east-1.console.aws.amazon.com/iam/home#/groups/details/SupportGroup/createPolicy
Gmail
YouTube
Maps
Translate
New Tab
Juniper Networks In...
Cisco Skills For All
Palo alto cyber
All Bookmarks
aws
Services
Search
[Alt+S]
Global
saloni786
IAM > User groups > SupportGroup > 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
1 {
2 "Version": "2012-10-17",
3 "Statement": {
4 "Effect": "Allow",
5 "Action": "sts:AssumeRole",
6 "Resource": "arn:aws:iam::381492030836:role/UpdateApp"
7 }
8 }
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
saloni786
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
Policy allow-assume-S3-role-in-production created.
IAM > User groups > SupportGroup
SupportGroup Info
Delete
Summary
Edit
User group name
SupportGroup
Creation time
February 09, 2024, 15:16 (UTC+05:30)
ARN
arn:aws:iam::381492030836:group/SupportGroup
Users (1)
Permissions
Access Advisor
Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached entities
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create a customer managed policy





Conclusion : Through this practical, we learnt to configure AWS Identity and Management (IAM) Console.