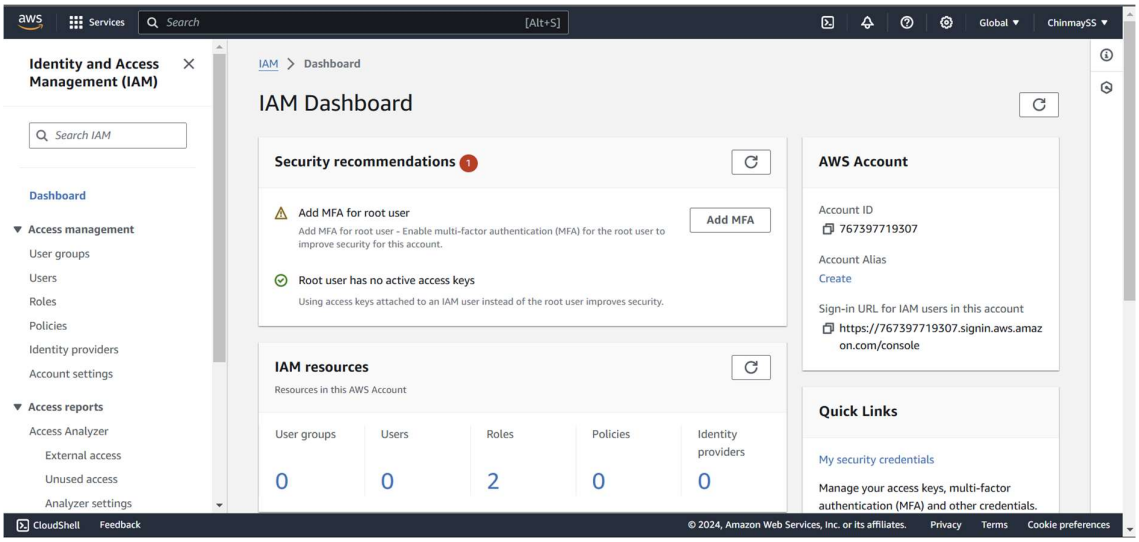
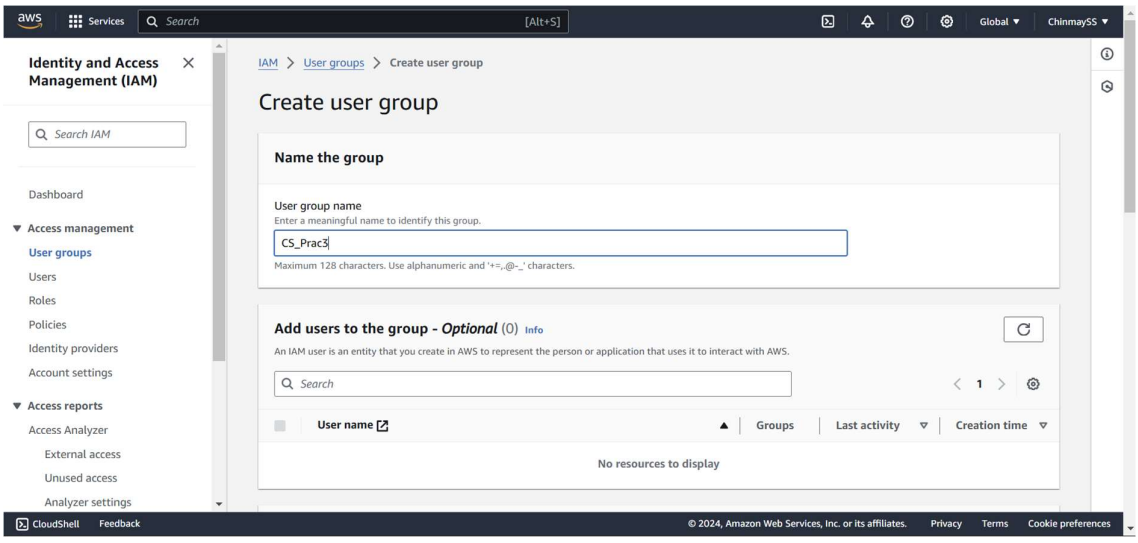
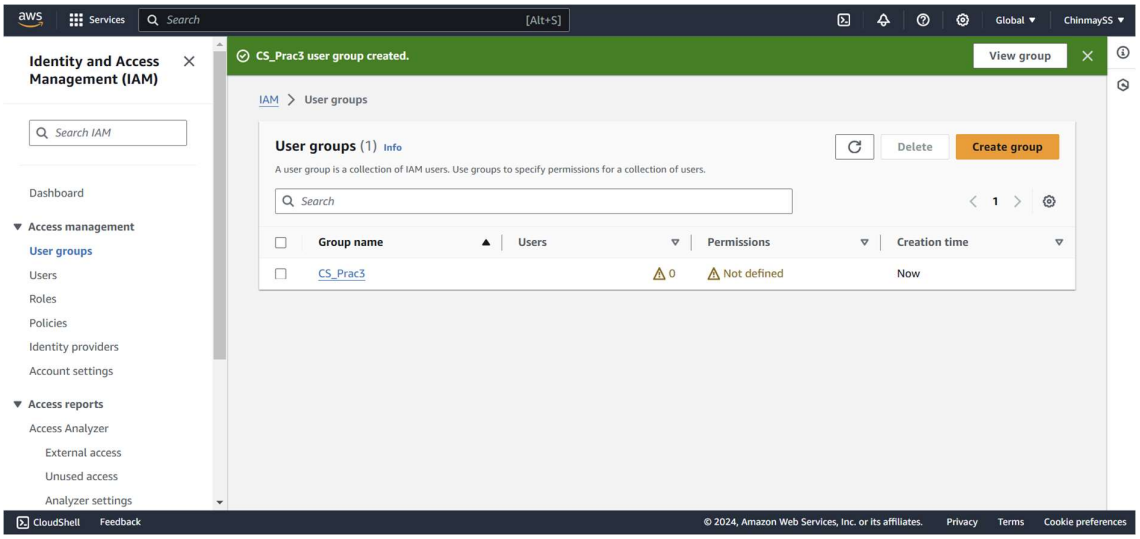
SVKM'S NMIMS Nilkamal School of Mathematics, Applied Statistics & Analytics
Master of Science (Statistics & Data Science)
Practical-3: Identity Access Management

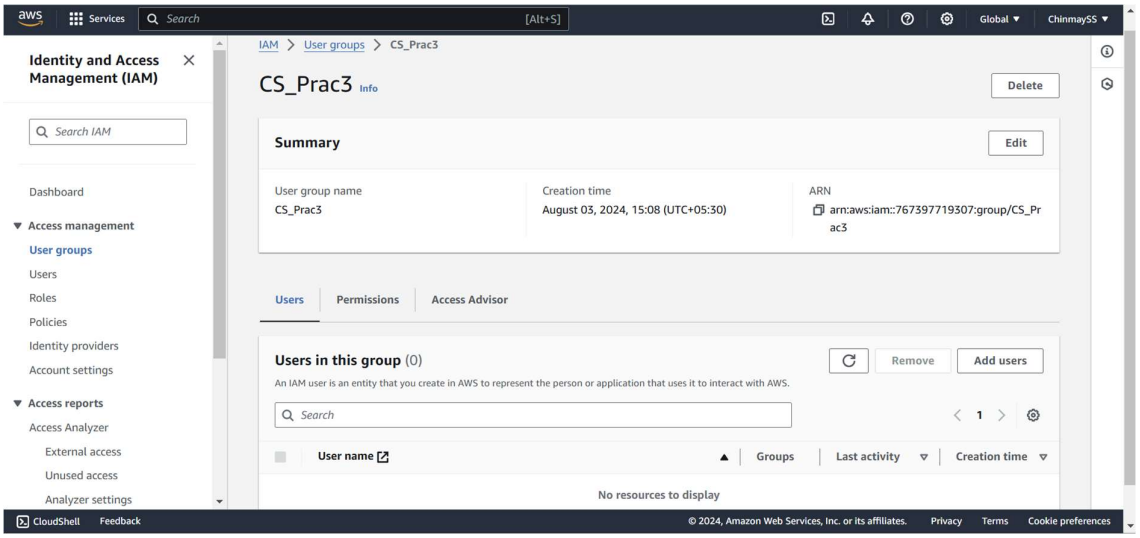
Name: Chinmay Shinde Roll No.: A066 SAP ID: 86062300031

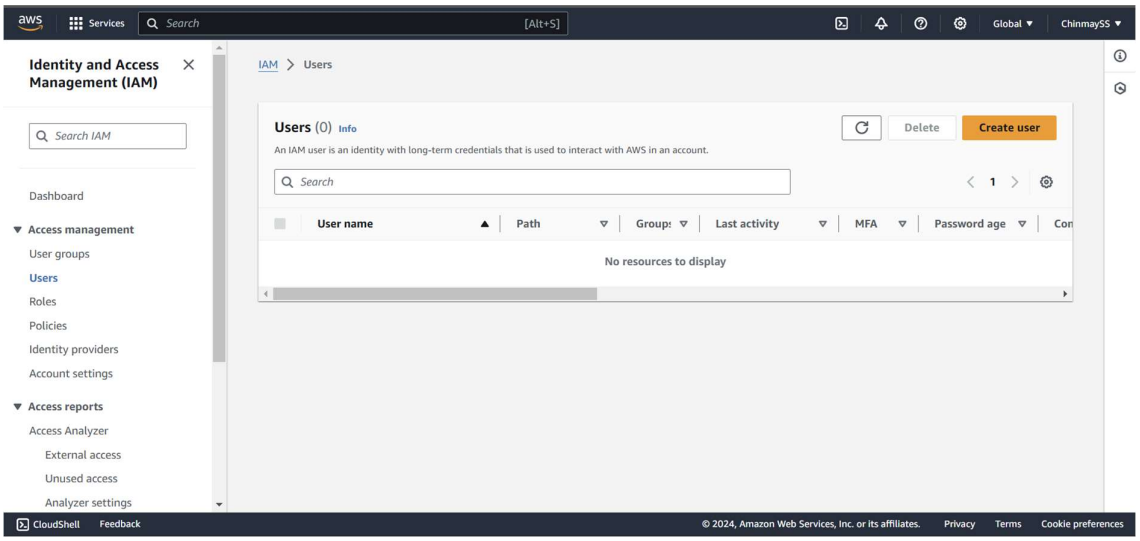
Create and Implement policies IAM user for accessing any 2 services from the AWS user and group. (S3 and EC2)

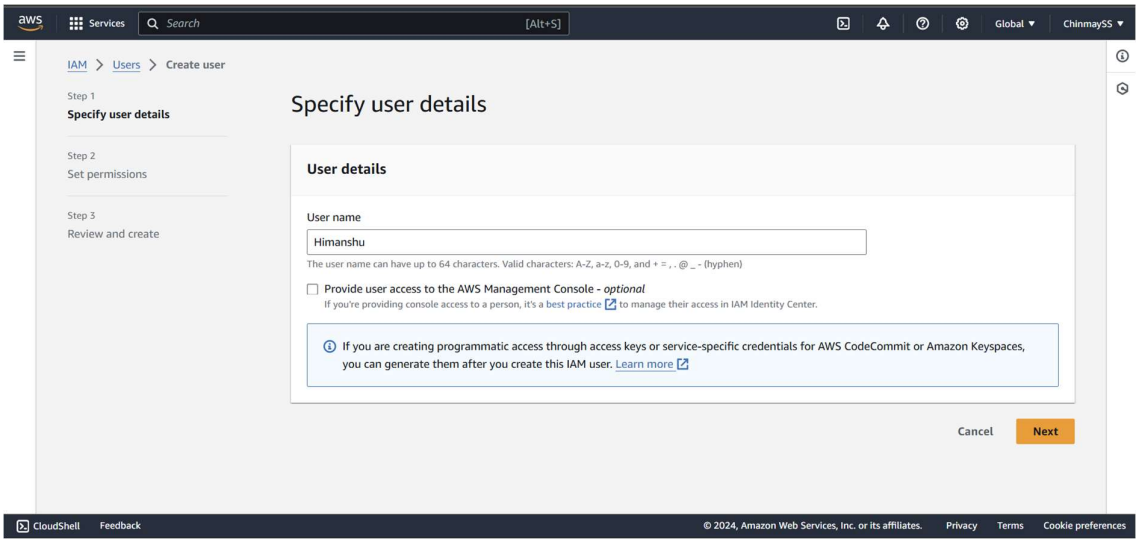


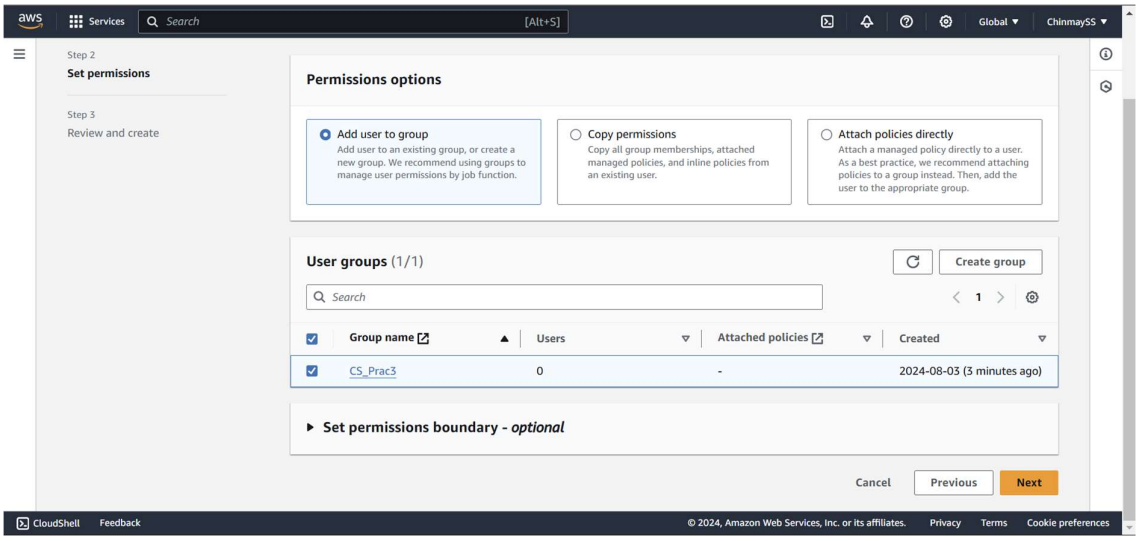


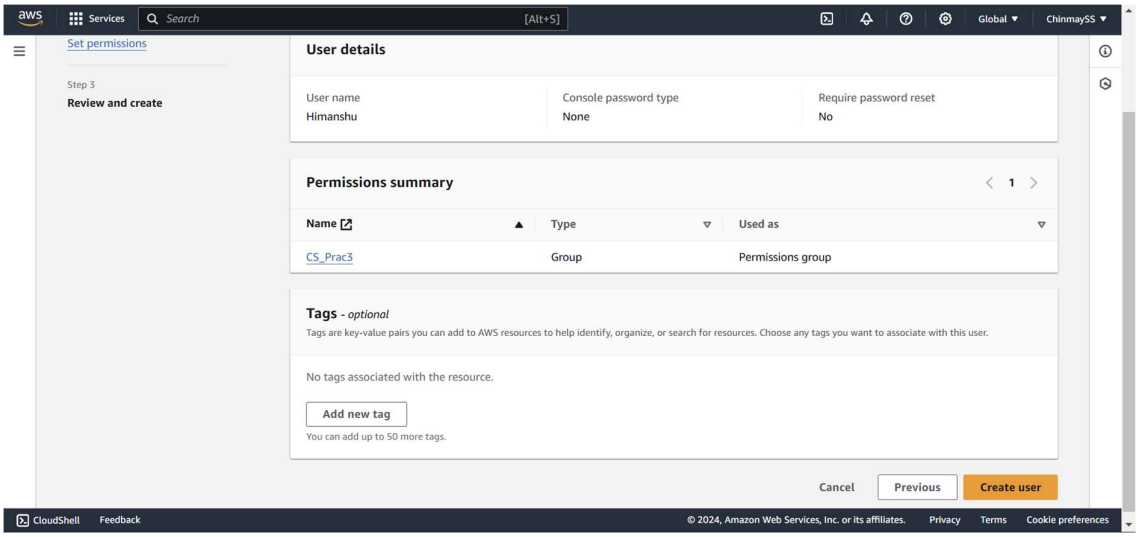

aws
Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
CS_Prac3 user group created.
View group
IAM > User groups
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
Creation time
CS_Prac3
0
Not defined
Now
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

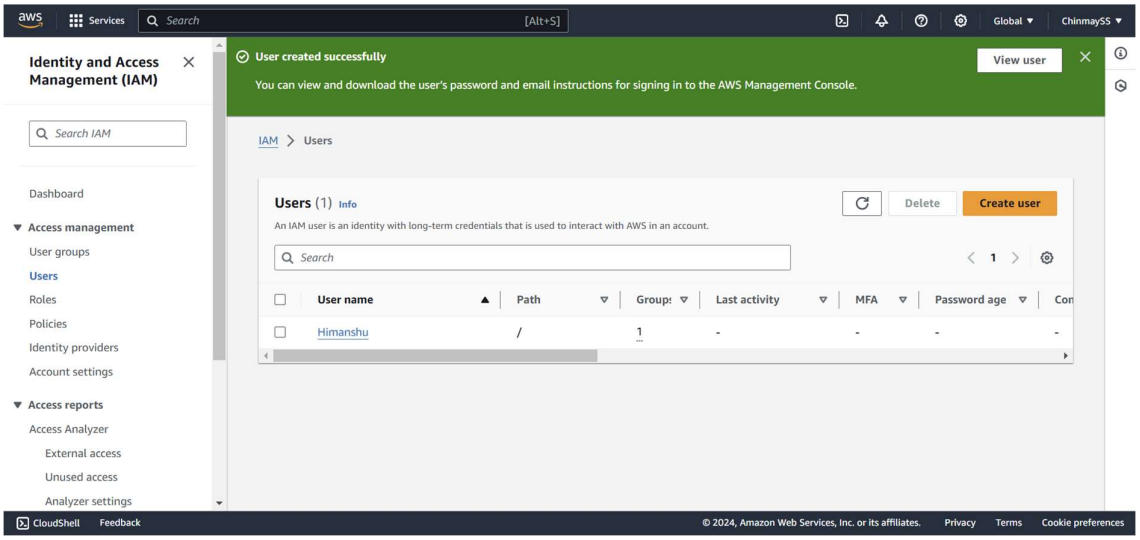

aws
Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
IAM > User groups > CS_Prac3
CS_Prac3 Info
Delete
Summary
Edit
User group name
CS_Prac3
Creation time
August 03, 2024, 15:08 (UTC+05:30)
ARN
arn:aws:iam::767397719307:group/CS_Prac3
Users
Permissions
Access Advisor
Users in this group (0)
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Remove
Add users
Search
User name
Groups
Last activity
Creation time
No resources to display
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

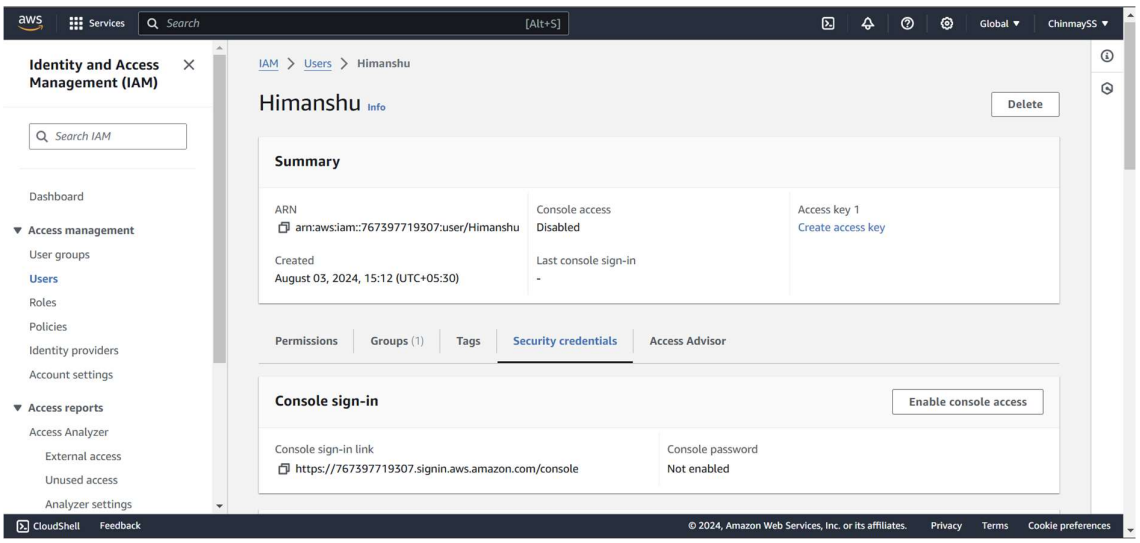

aws
Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
IAM > Users
Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Groups
Last activity
MFA
Password age
No resources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

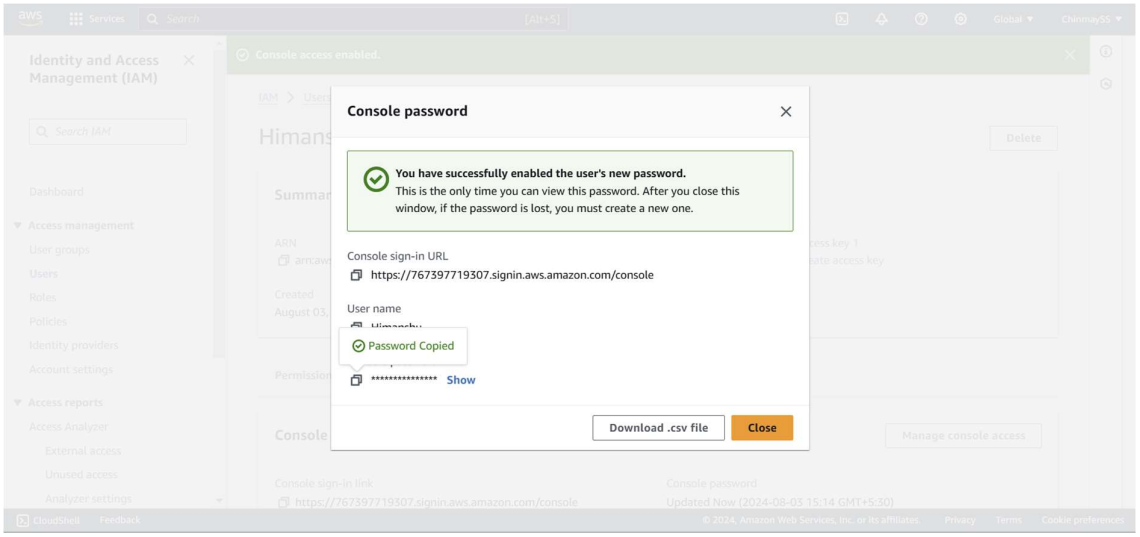

aws
Services
Search
[Alt+S]
Global
ChinmaySS
IAM
Users
Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
Himanshu
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide 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

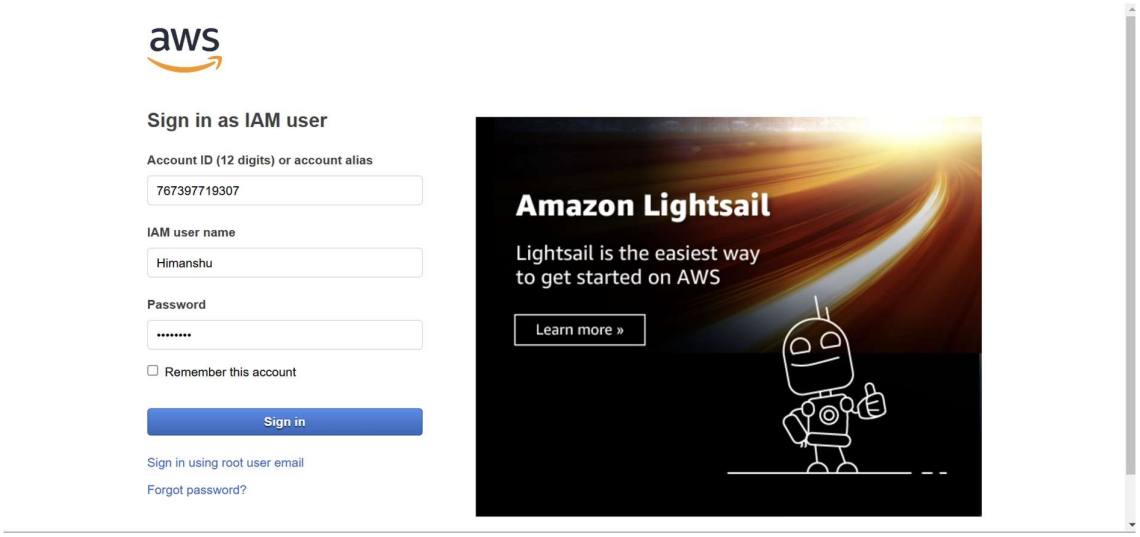

aws
Services
Search
[Alt+S]
Global
ChinmaySS
Step 2
Set permissions
Step 3
Review and create
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached 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.
User groups (1/1)
Create group
Search
1
Group name
Users
Attached policies
Created
CS_Prac3
0
-
2024-08-03 (3 minutes ago)
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

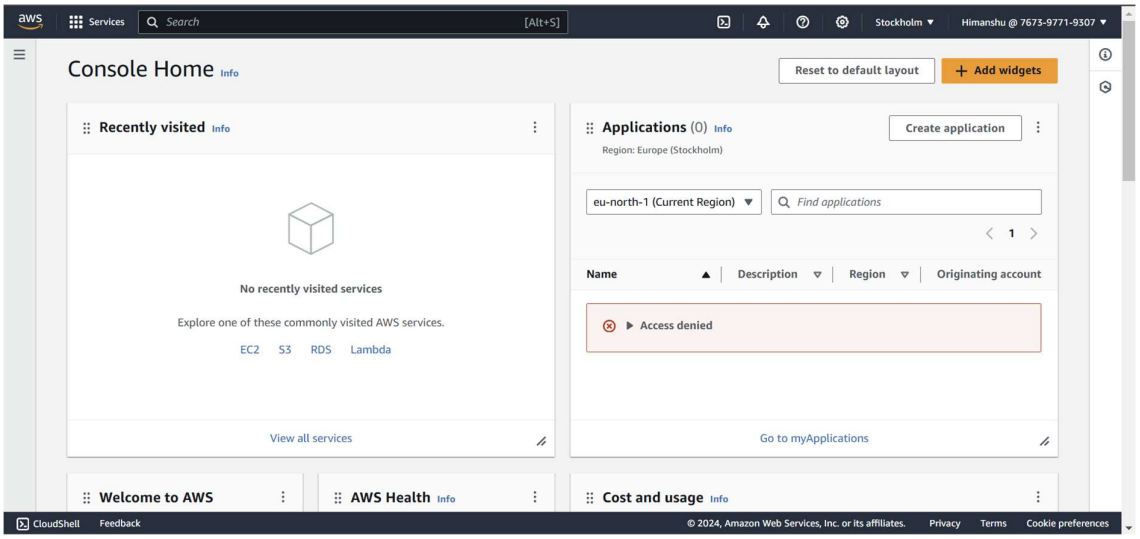

Services
Search
[Alt+S]
Global
ChinmaySS
Set permissions
Step 3
Review and create
User details
User name
Himanshu
Console password type
None
Require password reset
No
Permissions summary
Name
Type
Used as
CS_Prac3
Group
Permissions group
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

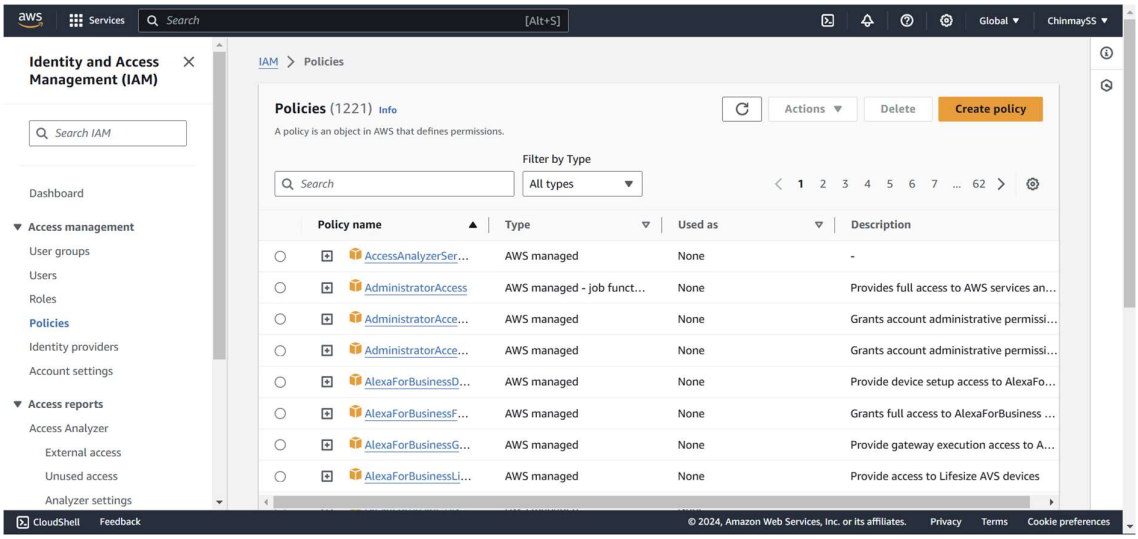

Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
User created successfully
You can view 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
User name
Path
Groups
Last activity
MFA
Password age
Himanshu
/
1
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

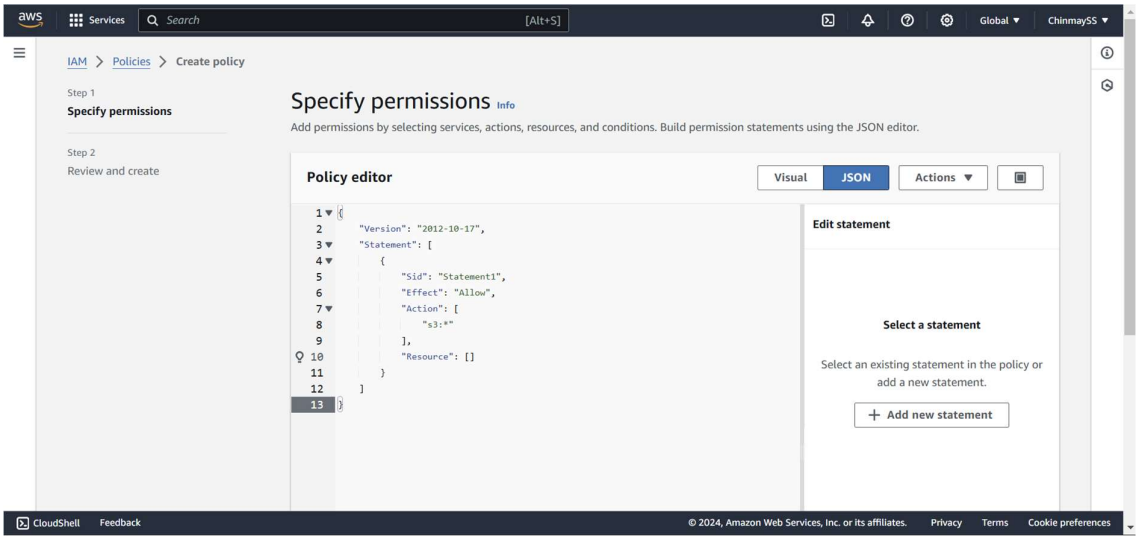

Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
IAM
Users
Himanshu
Himanshu Info
Delete
Summary
ARN
arn:aws:iam::767397719307:user/Himanshu
Console access
Disabled
Access key 1
Create access key
Created
August 03, 2024, 15:12 (UTC+05:30)
Last console sign-in
-
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Console sign-in
Enable console access
Console sign-in link
https://767397719307.signin.aws.amazon.com/console
Console password
Not enabled
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

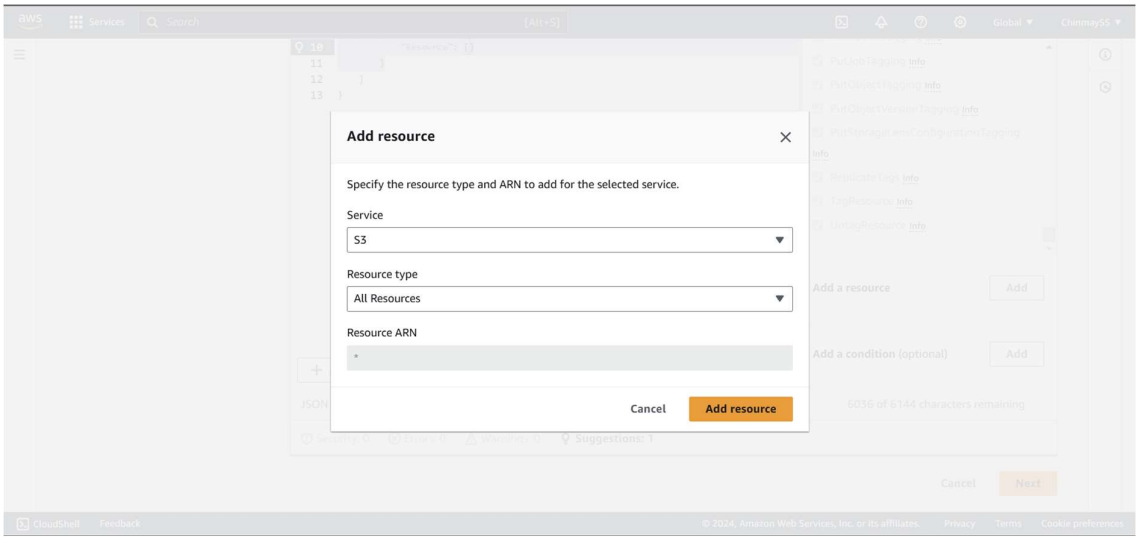

Console password
You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.
Console sign-in URL
https://767397719307.signin.aws.amazon.com/console
User name
Password Copied
Show
Download .csv file
Close

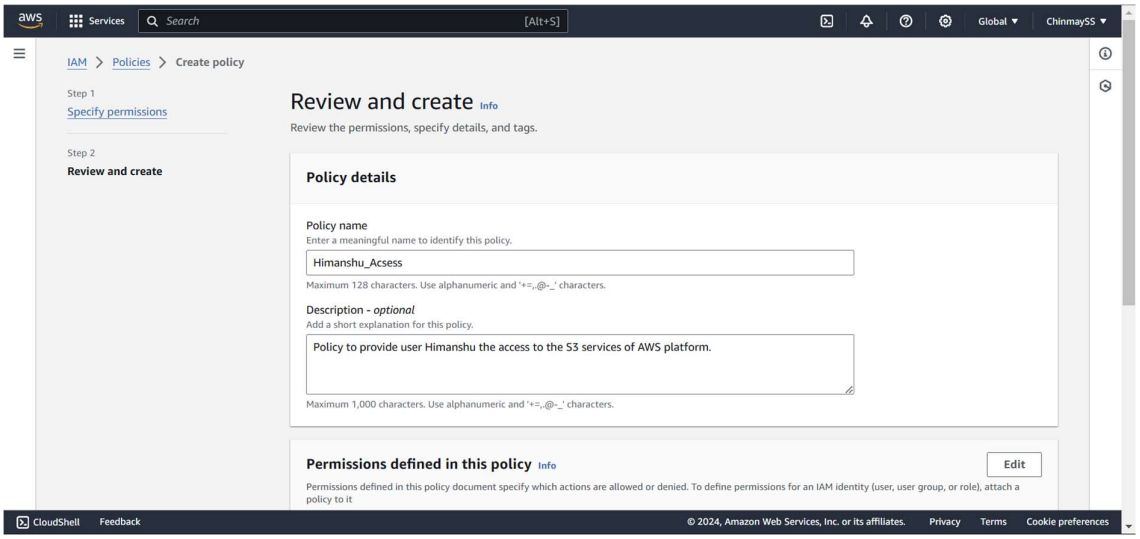

Sign in as IAM user
Account ID (12 digits) or account alias
767397719307
IAM user name
Himanshu
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

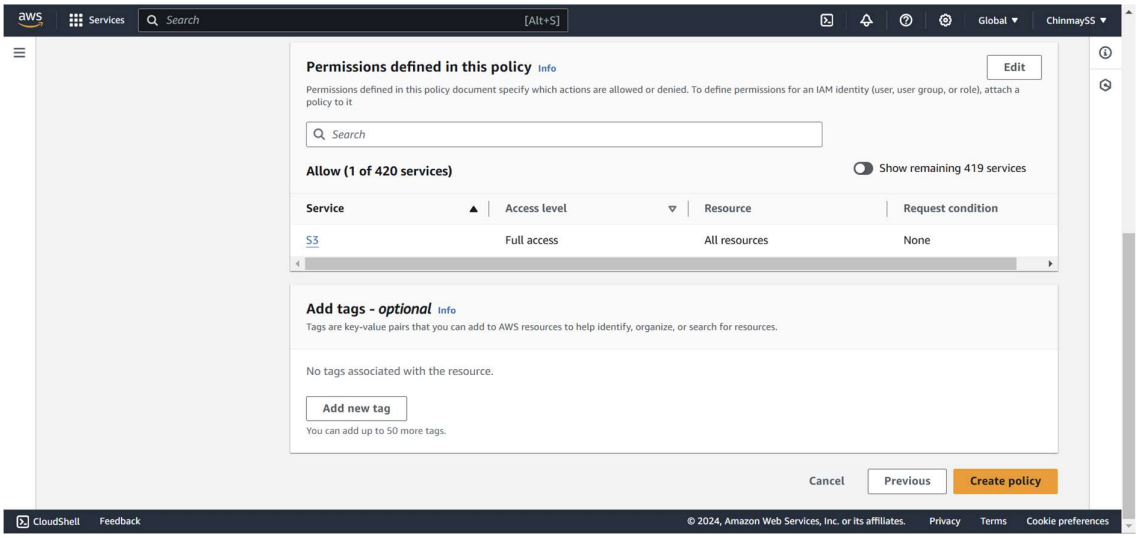

Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
No recently visited services
Explore one of these commonly visited AWS services.
EC2 S3 RDS Lambda
View all services
Applications (0) Info
Region: Europe (Stockholm)
Create application
eu-north-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
Go to myApplications
Welcome to AWS
AWS Health Info
Cost and usage Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

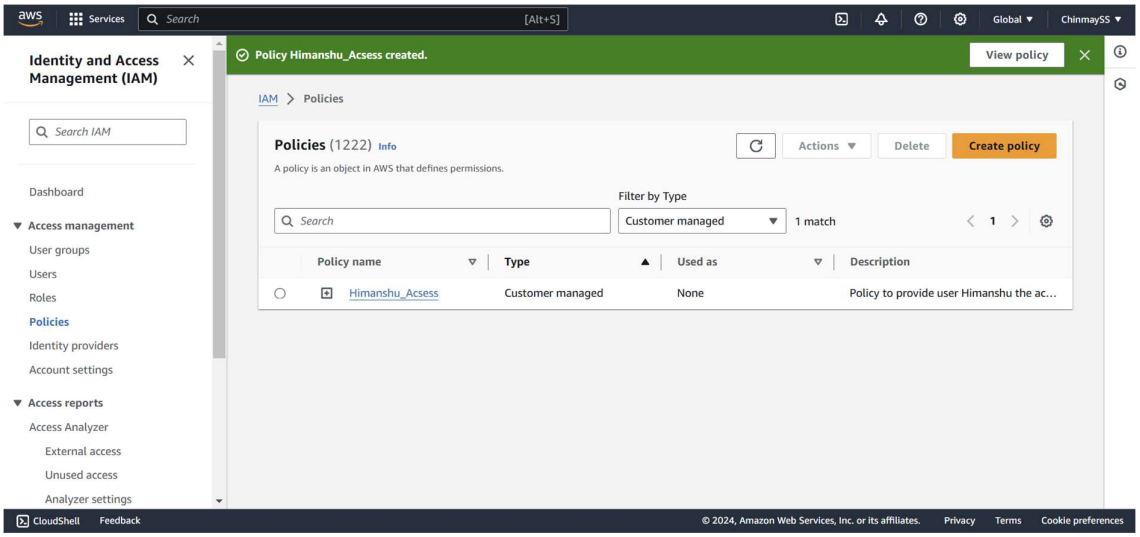

aws
Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
IAM > Policies
Policies (1221) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 62
Policy name
Type
Used as
Description
AccessAnalyzerSer... AWS managed None -
AdministratorAccess AWS managed - job funct... None Provides full access to AWS services an...
AdministratorAcce... AWS managed None Grants account administrative permissi...
AdministratorAcce... AWS managed None Grants account administrative permissi...
AlexaForBusinessD... AWS managed None Provide device setup access to AlexaFo...
AlexaForBusinessF... AWS managed None Grants full access to AlexaForBusiness ...
AlexaForBusinessG... AWS managed None Provide gateway execution access to A...
AlexaForBusinessLi... AWS managed None Provide access to Lifesize AVS devices
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

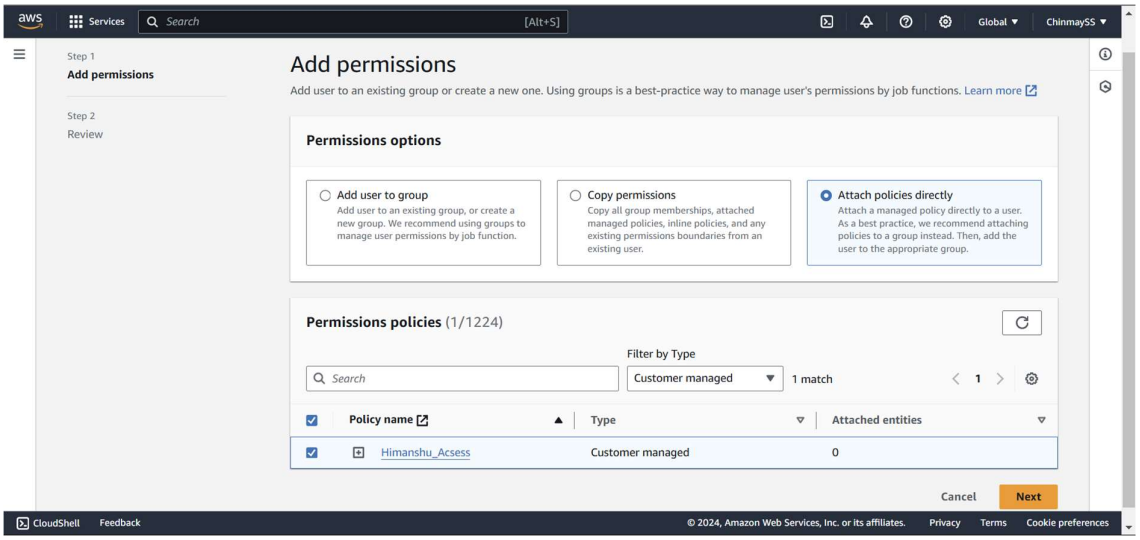

aws
Services
Search
[Alt+S]
Global
ChinmaySS
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Action": [
"s3:*"
],
"Resource": []
}
]
}
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

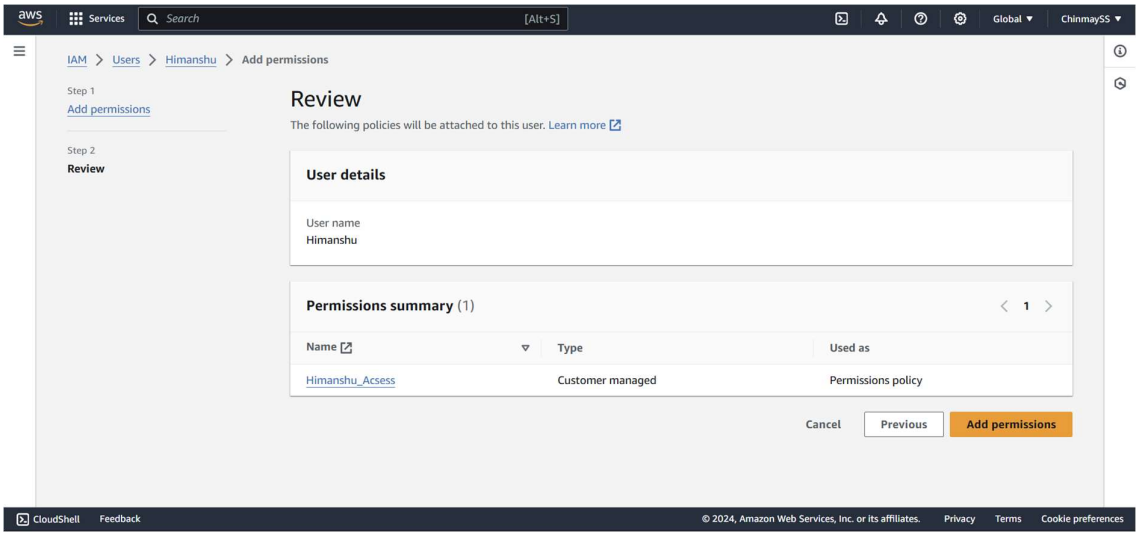

Add resource
Specify the resource type and ARN to add for the selected service.
Service
S3
Resource type
All Resources
Resource ARN
*
Cancel
Add resource

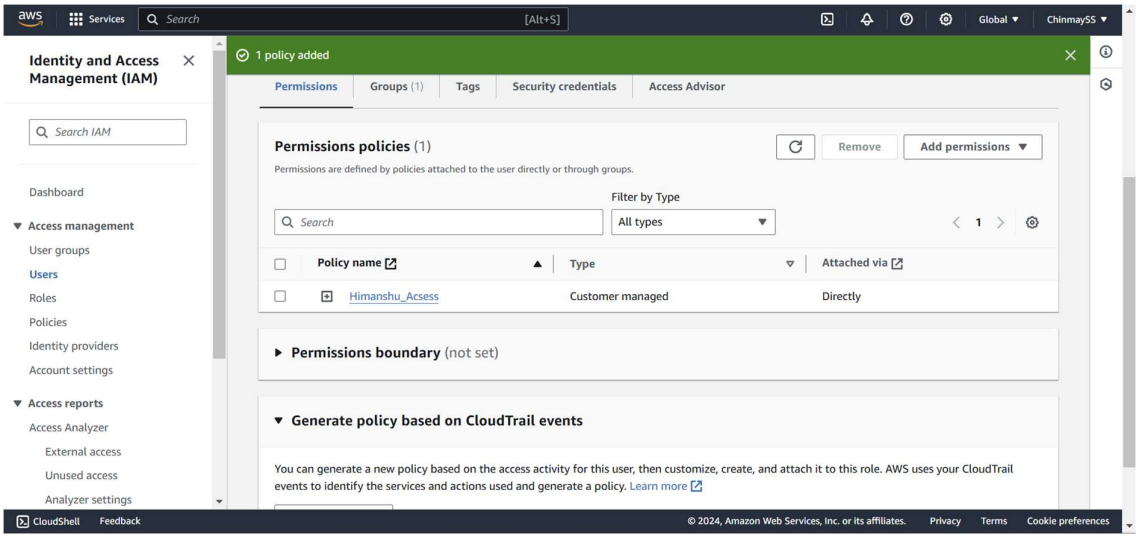

aws
Services
Search
[Alt+S]
Global
ChinmaySS
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Himanshu_Acsess
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Policy to provide user Himanshu the access to the S3 services of AWS platform.
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

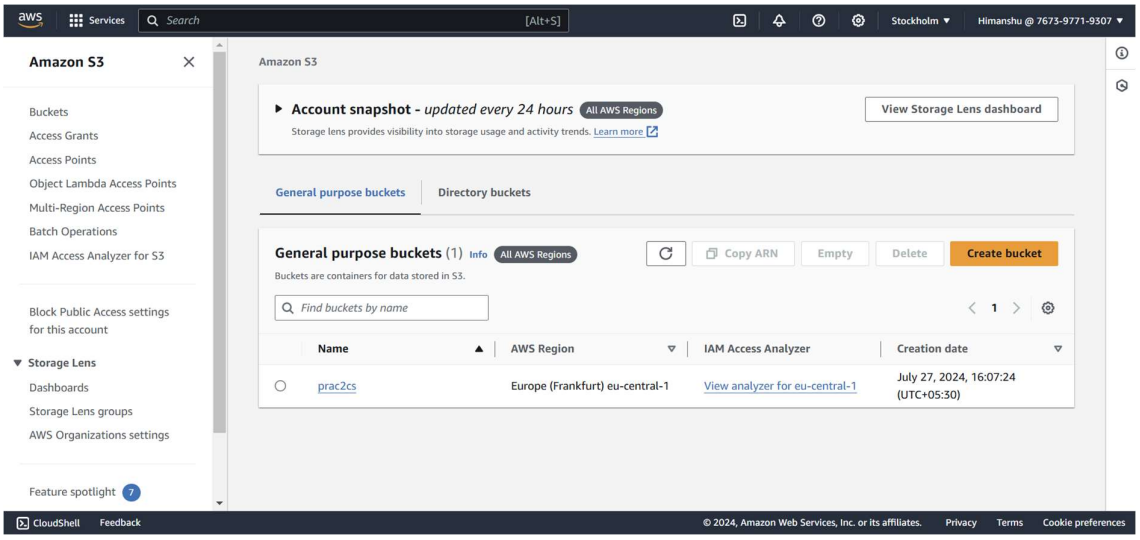

aws
Services
Search
[Alt+S]
Global
ChinmaySS
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 420 services)
Show remaining 419 services
Service
Access level
Resource
Request condition
S3
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
ChinmaySS
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
Policy Himanshu_Acsess created.
View policy
IAM > Policies
Policies (1222) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
Customer managed
1 match
1
Policy name
Type
Used as
Description
Himanshu_Acsess
Customer managed
None
Policy to provide user Himanshu the ac...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

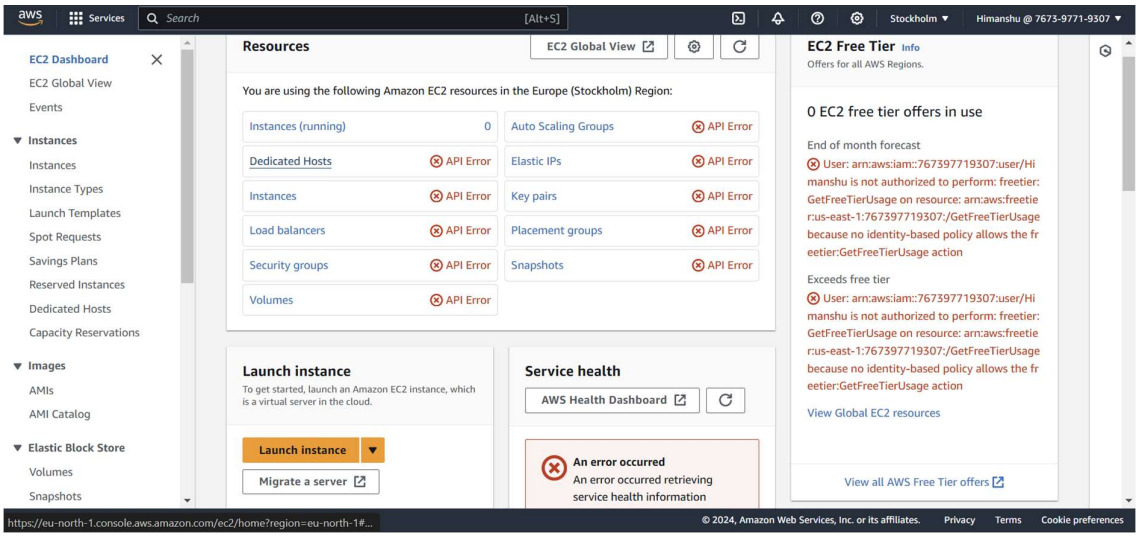

aws
Services
Search
[Alt+S]
Global
ChinmaySS
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing 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.
Permissions policies (1/1224)
Filter by Type
Search
Customer managed
1 match
1
Policy name
Type
Attached entities
Himanshu_Acsess
Customer managed
0
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

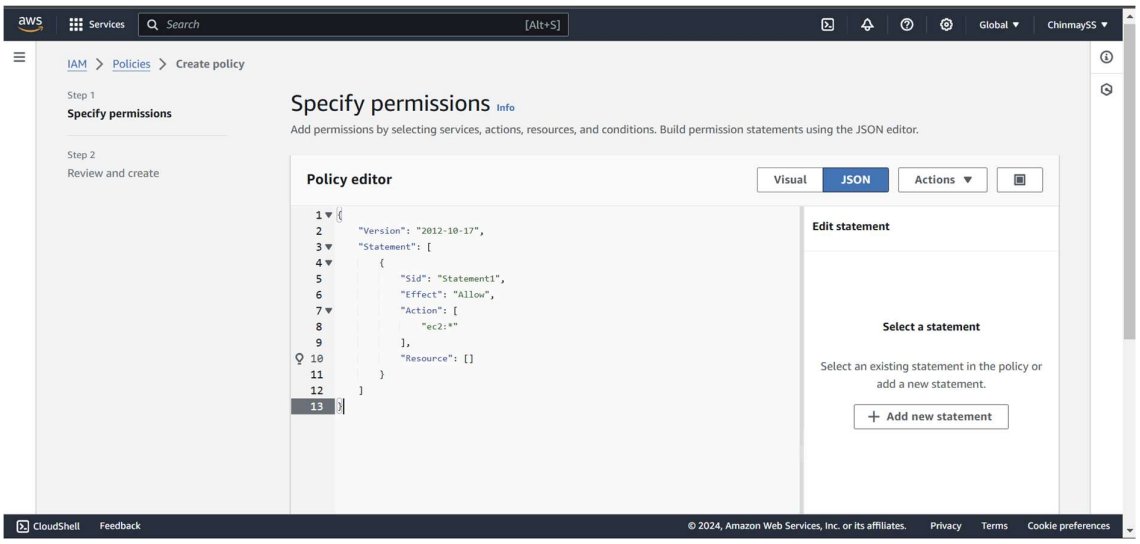

aws
Services
Search
[Alt+S]
Global
ChinmaySS
IAM
Users
Himanshu
Add permissions
Step 1
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
Himanshu
Permissions summary (1)
1
Name
Type
Used as
Himanshu_Acsess
Customer managed
Permissions policy
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

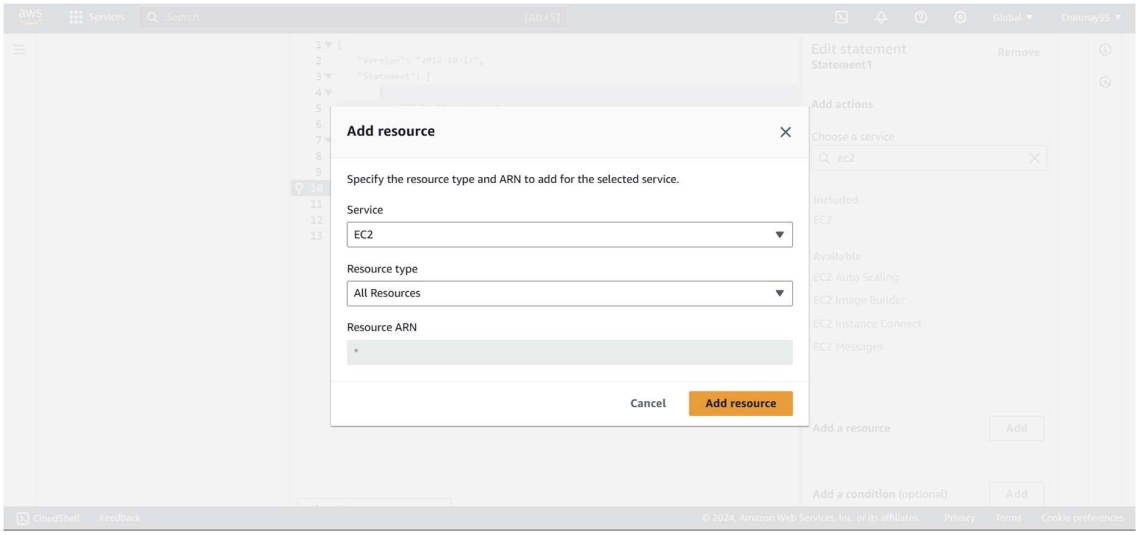

aws
Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
1 policy added
Permissions
Groups (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
1
Policy name
Type
Attached via
Himanshu_Acsess
Customer managed
Directly
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

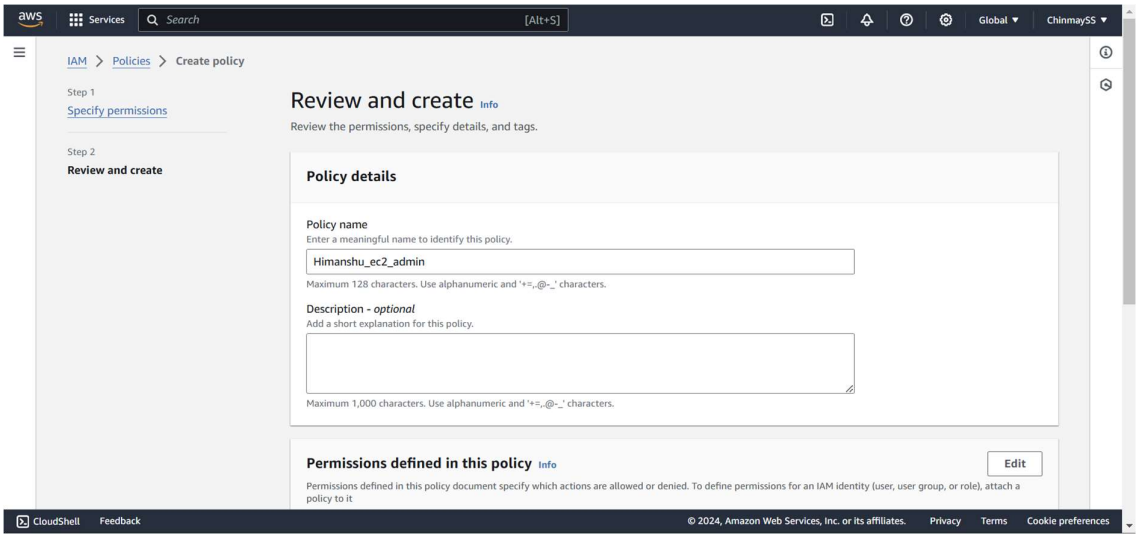

Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
prac2cs
Europe (Frankfurt) eu-central-1
View analyzer for eu-central-1
July 27, 2024, 16:07:24 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

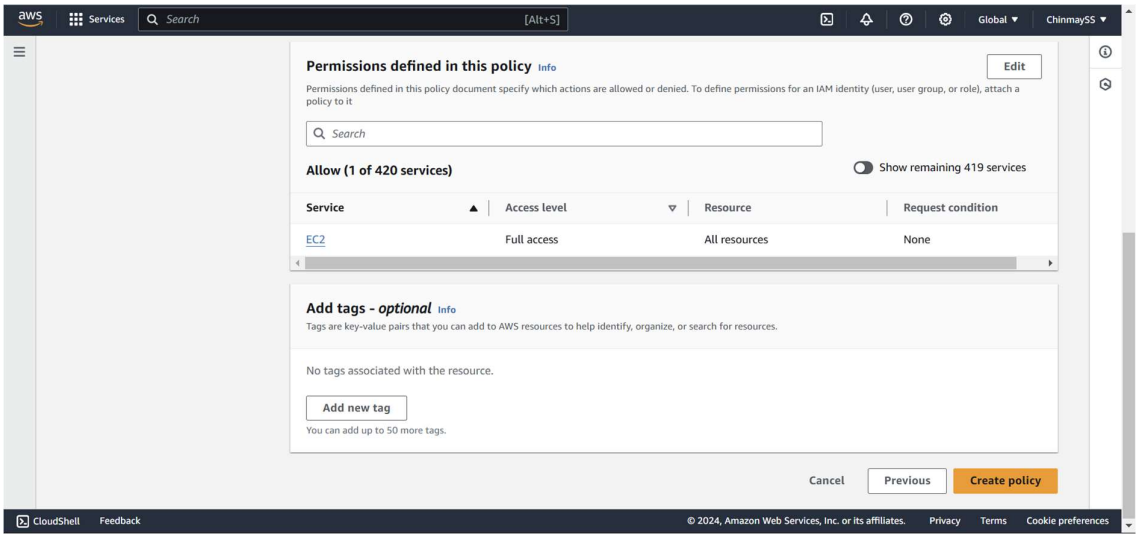
- **EC2**

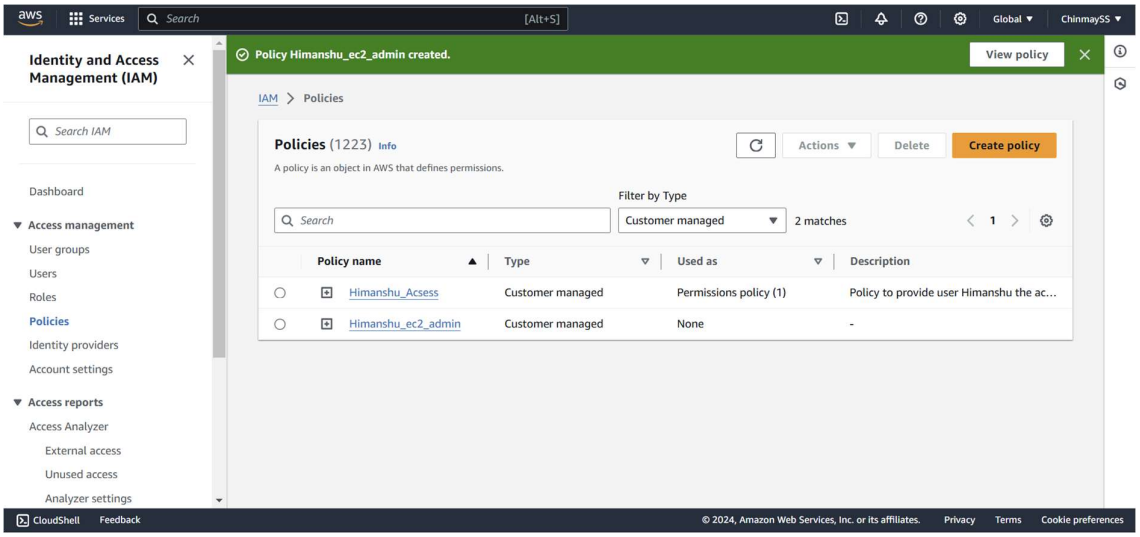

EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Resources
EC2 Global View
You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:
Instances (running) 0
Auto Scaling Groups API Error
Dedicated Hosts API Error
Elastic IPs API Error
Instances API Error
Key pairs API Error
Load balancers API Error
Placement groups API Error
Security groups API Error
Snapshots API Error
Volumes API Error
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
EC2 Free Tier Info
Offers for all AWS Regions.
0 EC2 free tier offers in use
End of month forecast
User: arn:aws:iam::767397719307:user/Himanshu is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:767397719307:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
Exceeds free tier
User: arn:aws:iam::767397719307:user/Himanshu is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:767397719307:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
View Global EC2 resources
View all AWS Free Tier offers
https://eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#...
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

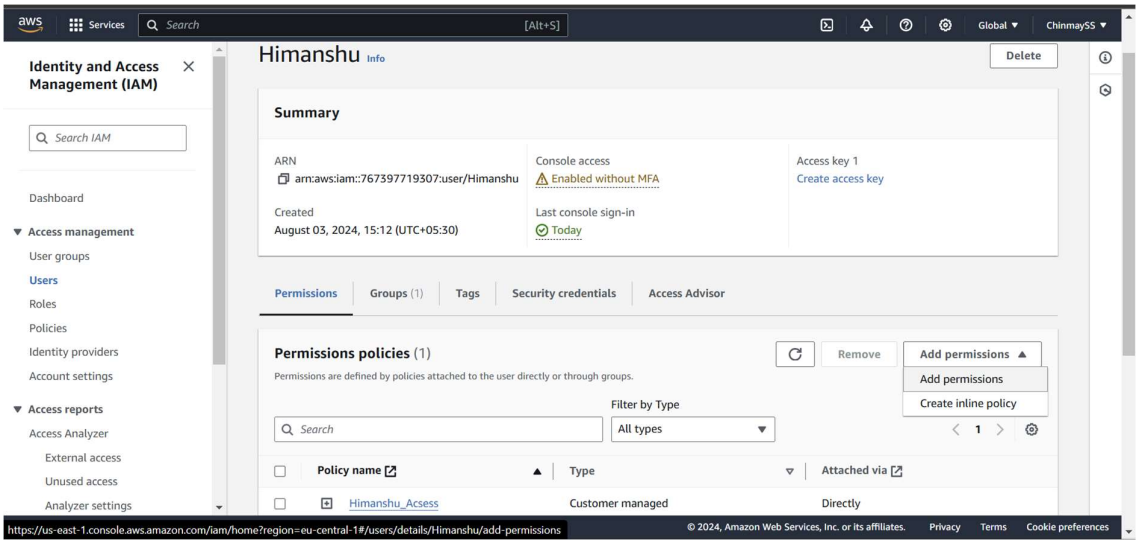

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Action": [
"ec2:*"
],
"Resource": []
}
]
}
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

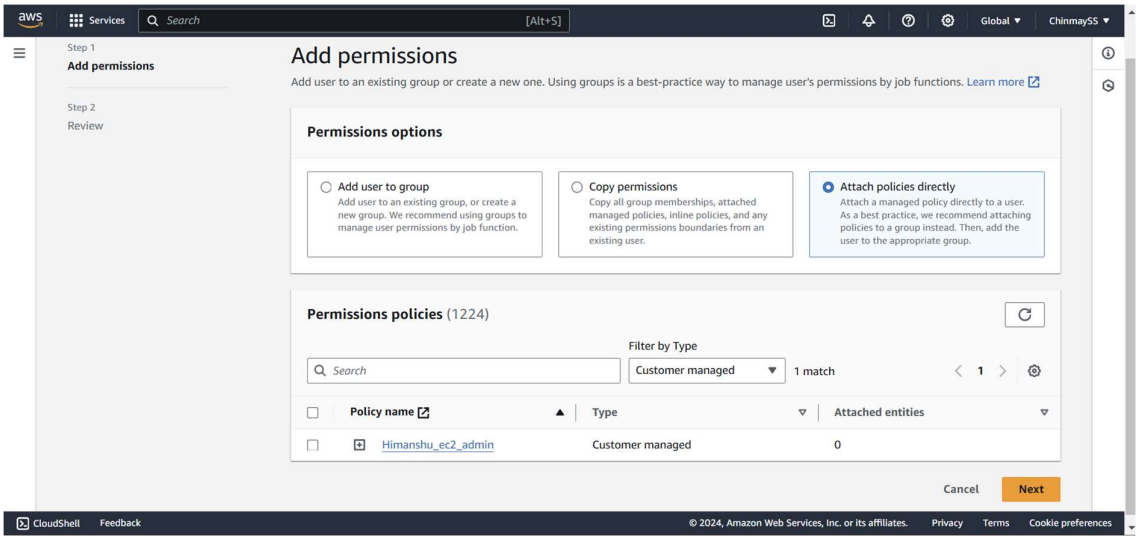

Add resource
Specify the resource type and ARN to add for the selected service.
Service
EC2
Resource type
All Resources
Resource ARN
*
Cancel
Add resource

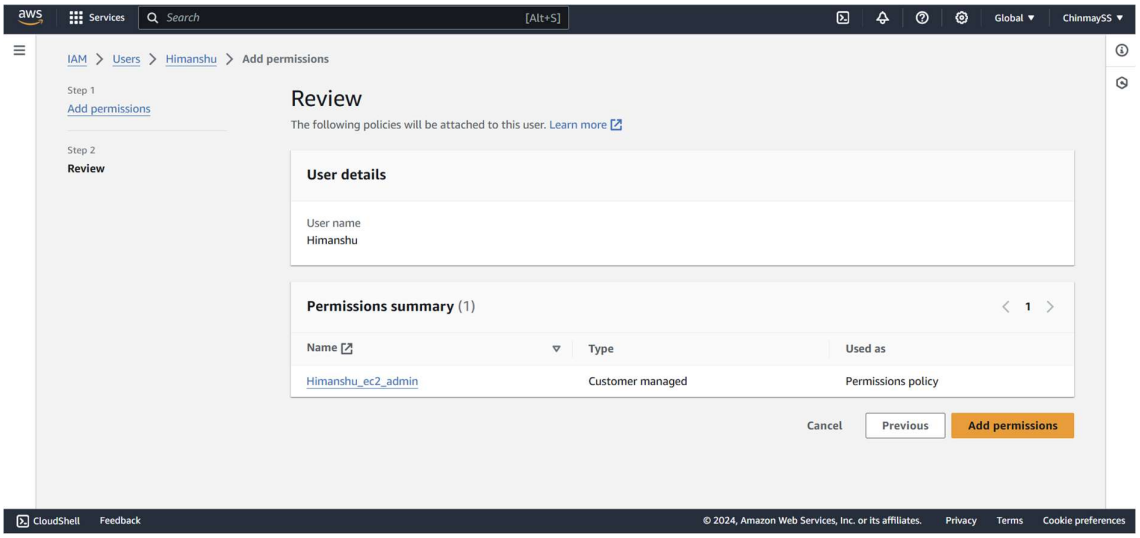

Services
Search
[Alt+S]
Global
ChinmaySS
IAM
Policies
Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Himanshu_ec2_admin
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

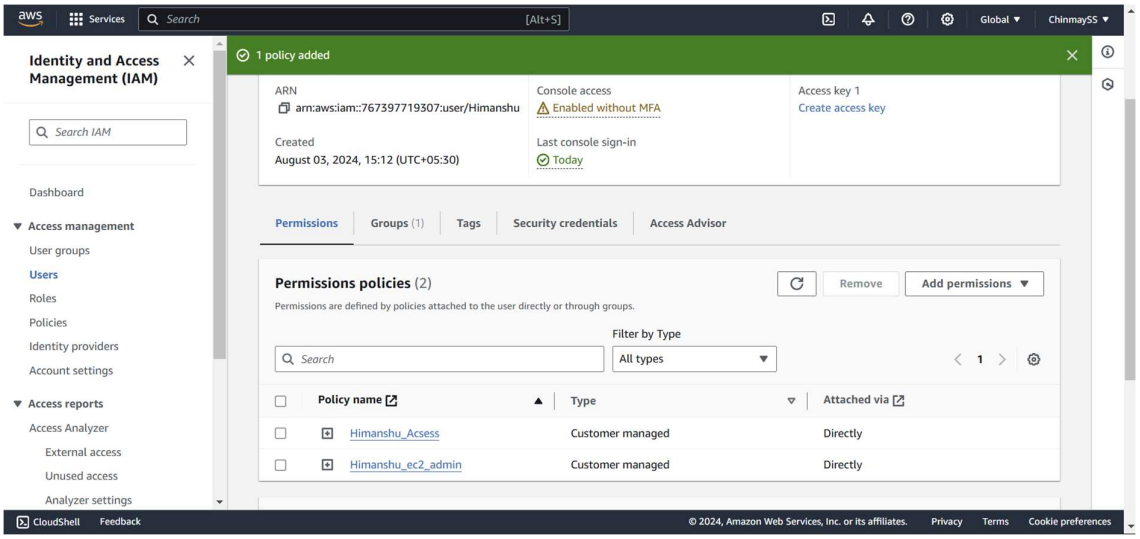

Services
Search
[Alt+S]
Global
ChinmaySS
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 420 services)
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

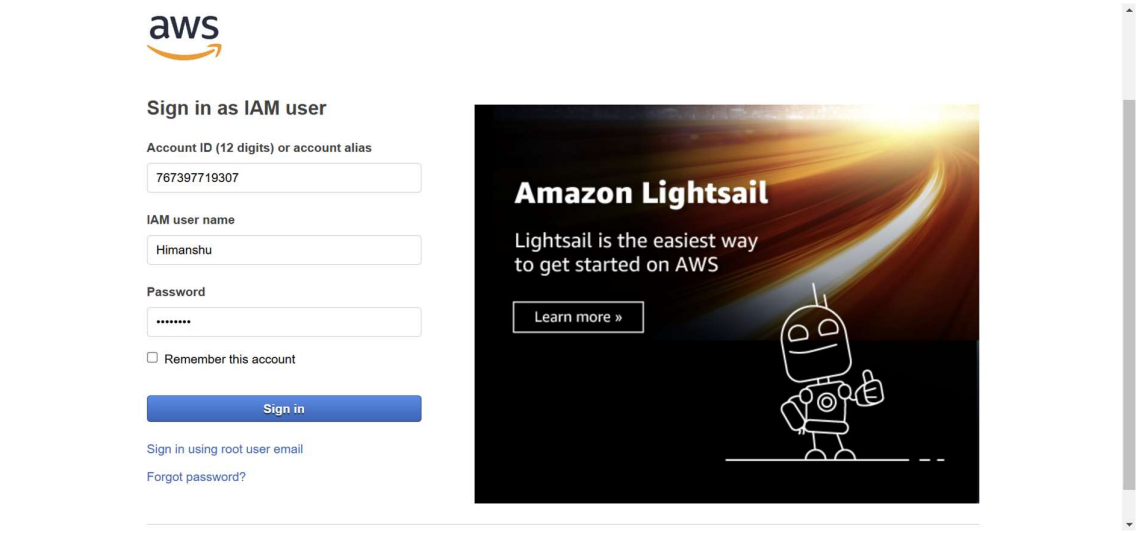

Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
Policy Himanshu_ec2_admin created.
View policy
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
IAM > Policies
Policies (1223) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
Customer managed
2 matches
Policy name
Type
Used as
Description
Himanshu_Acsess
Customer managed
Permissions policy (1)
Policy to provide user Himanshu the ac...
Himanshu_ec2_admin
Customer managed
None
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

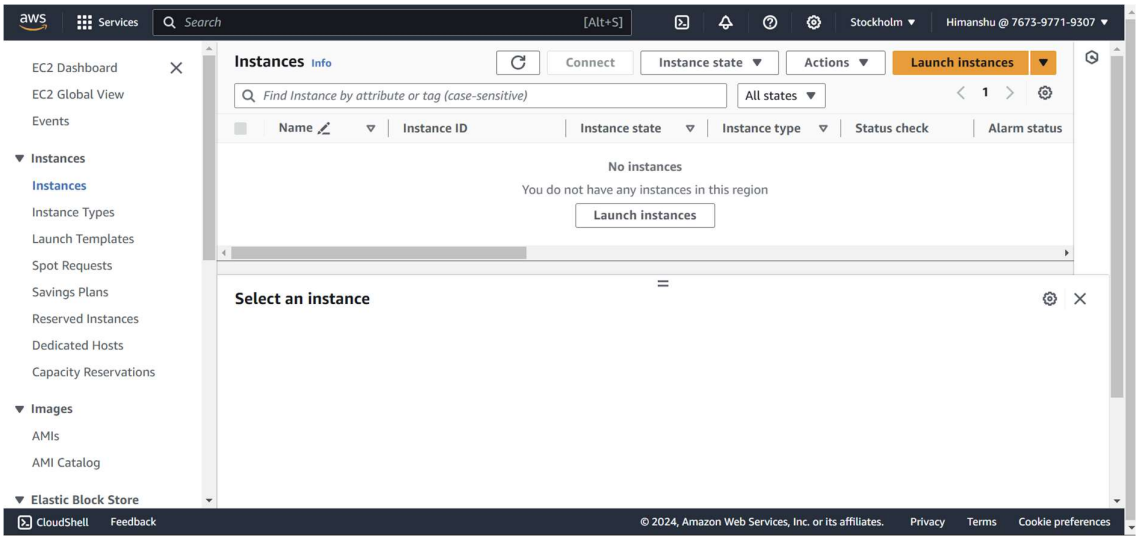

Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
Himanshu Info
Delete
Search IAM
Summary
ARN
arn:aws:iam::767397719307:user/Himanshu
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 15:12 (UTC+05:30)
Last console sign-in
Today
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
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
Add permissions
Create inline policy
Filter by Type
Search
All types
Policy name
Type
Attached via
Himanshu_Acsess
Customer managed
Directly
https://us-east-1.console.aws.amazon.com/iam/home?region=eu-central-1#/users/details/Himanshu/add-permissions
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

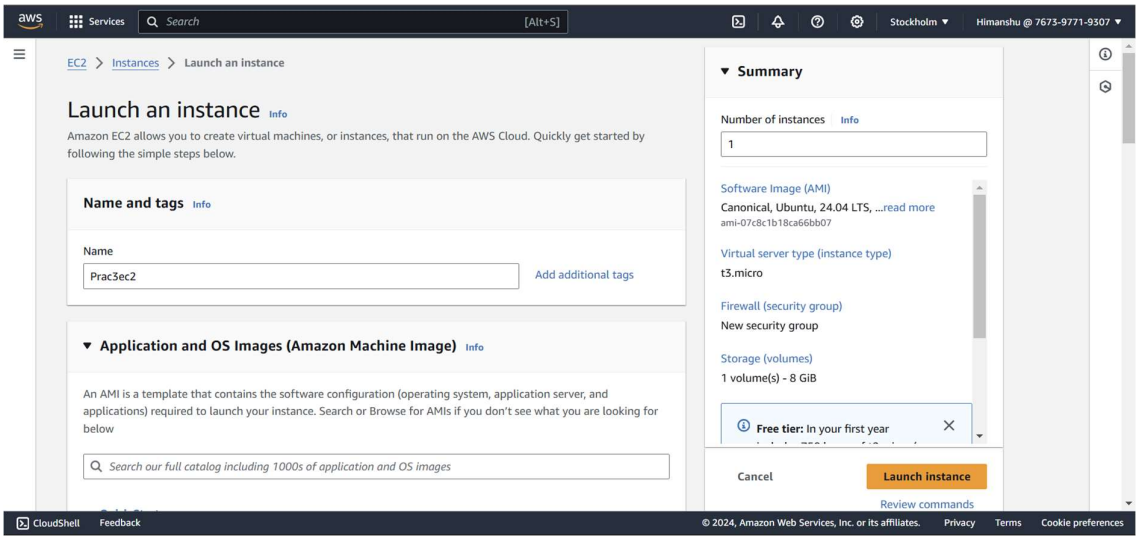

Services
Search
[Alt+S]
Global
ChinmaySS
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing 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.
Permissions policies (1224)
Filter by Type
Search
Customer managed
1 match
Policy name
Type
Attached entities
Himanshu_ec2_admin
Customer managed
0
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

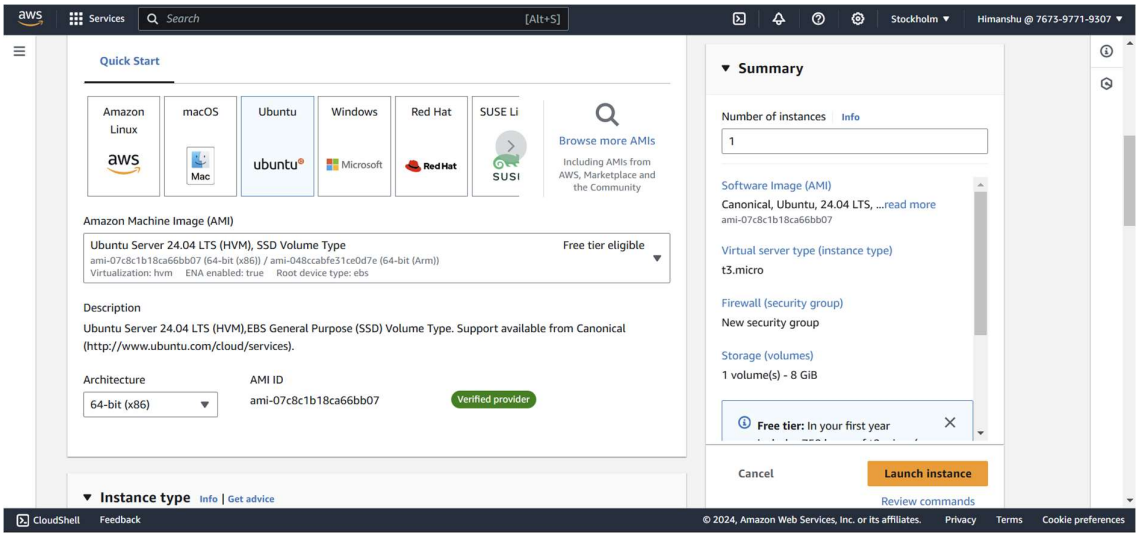

Services
Search
[Alt+S]
Global
ChinmaySS
IAM
Users
Himanshu
Add permissions
Step 1
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
Himanshu
Permissions summary (1)
Name
Type
Used as
Himanshu_ec2_admin
Customer managed
Permissions policy
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

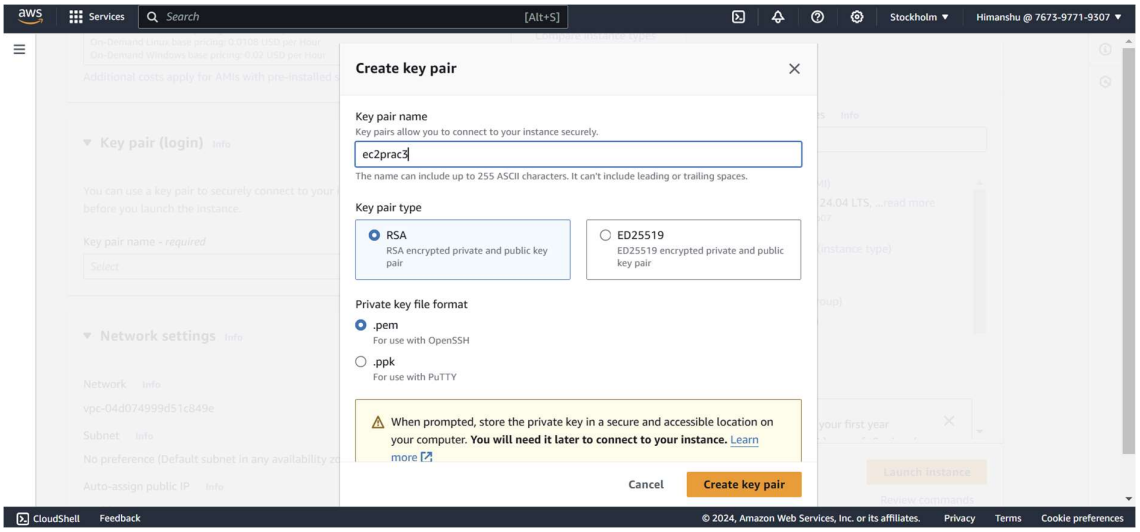

Services
Search
[Alt+S]
Global
ChinmaySS
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
1 policy added
ARN
arn:aws:iam::767397719307:user/Himanshu
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 15:12 (UTC+05:30)
Last console sign-in
Today
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Permissions policies (2)
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
Himanshu_Acsess
Customer managed
Directly
Himanshu_ec2_admin
Customer managed
Directly
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

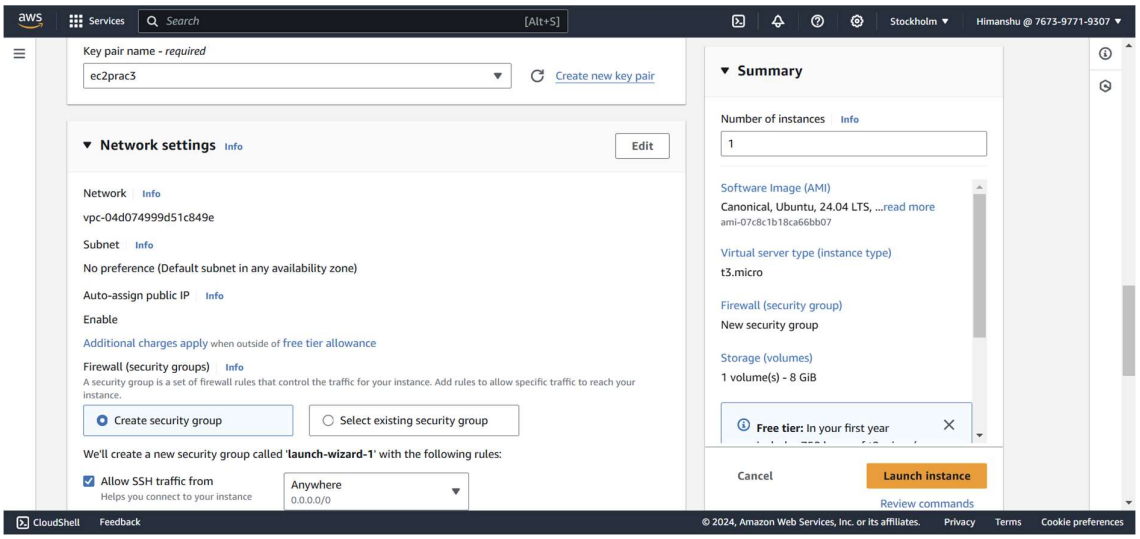

aws
Sign in as IAM user
Account ID (12 digits) or account alias
767397719307
IAM user name
Himanshu
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

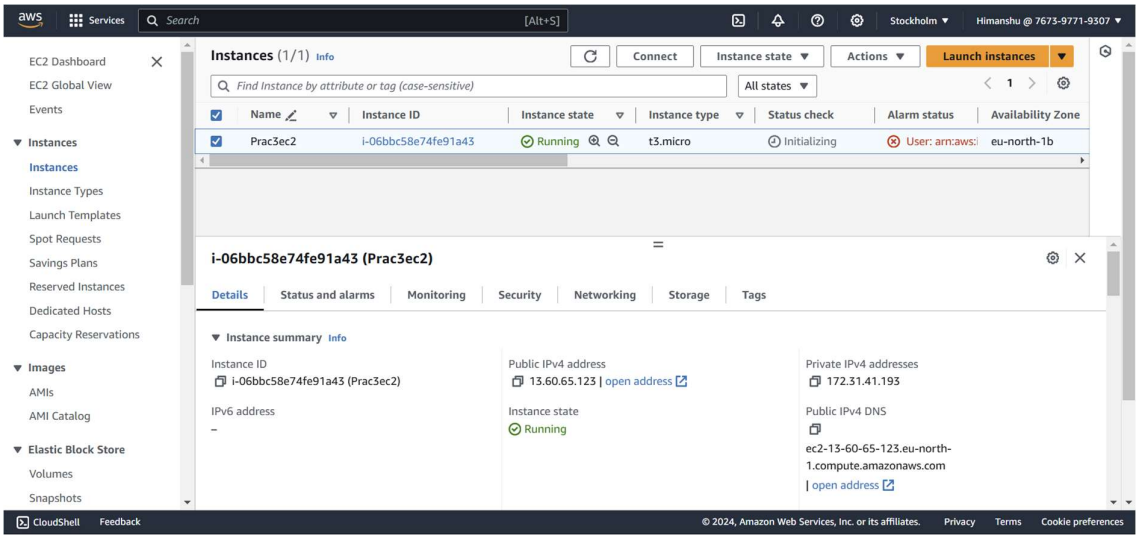

aws
Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Instances Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
No instances
You do not have any instances in this region
Launch instances
Select an instance
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

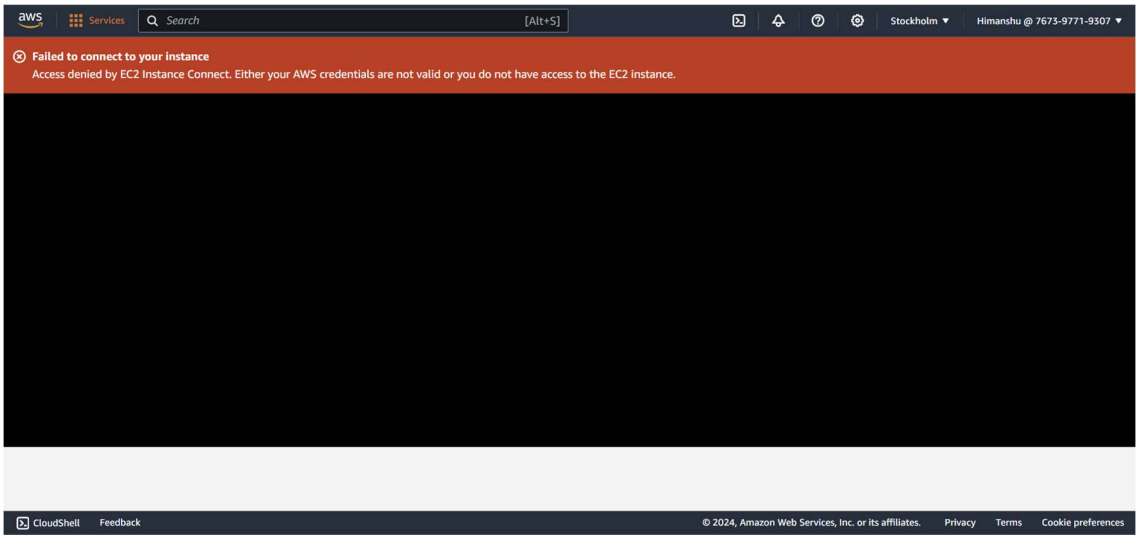

aws
Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
Prac3ec2
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-07c8c1b18ca66bb07
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

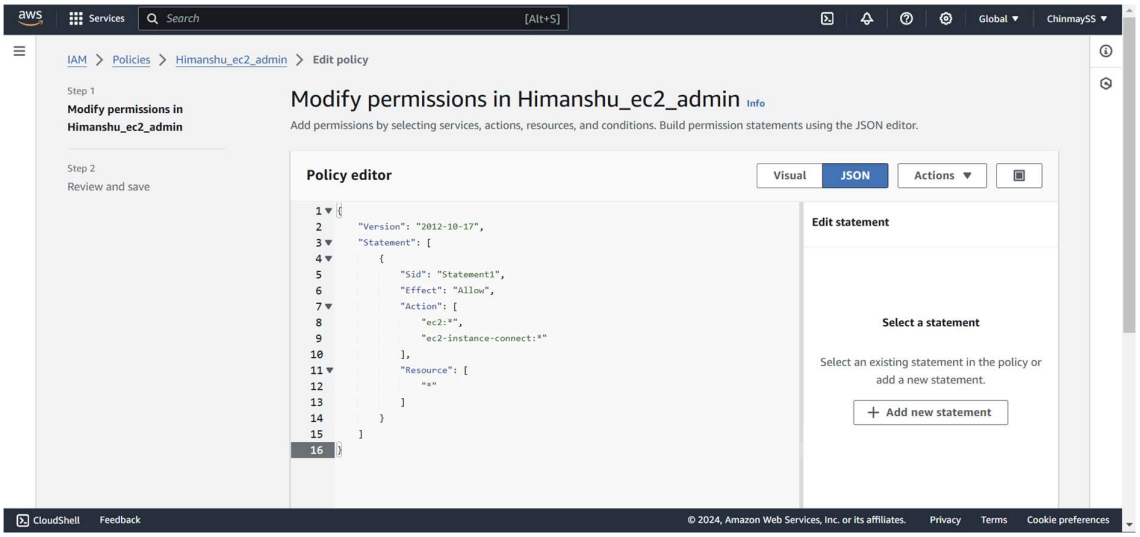

Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Li
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
Free tier eligible
ami-07c8c1b18ca66bb07 (64-bit (x86)) / ami-048ccabfe31ce0d7e (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs
Description
Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Architecture
64-bit (x86)
AMI ID
ami-07c8c1b18ca66bb07
Verified provider
Instance type Info | Get advice
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-07c8c1b18ca66bb07
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

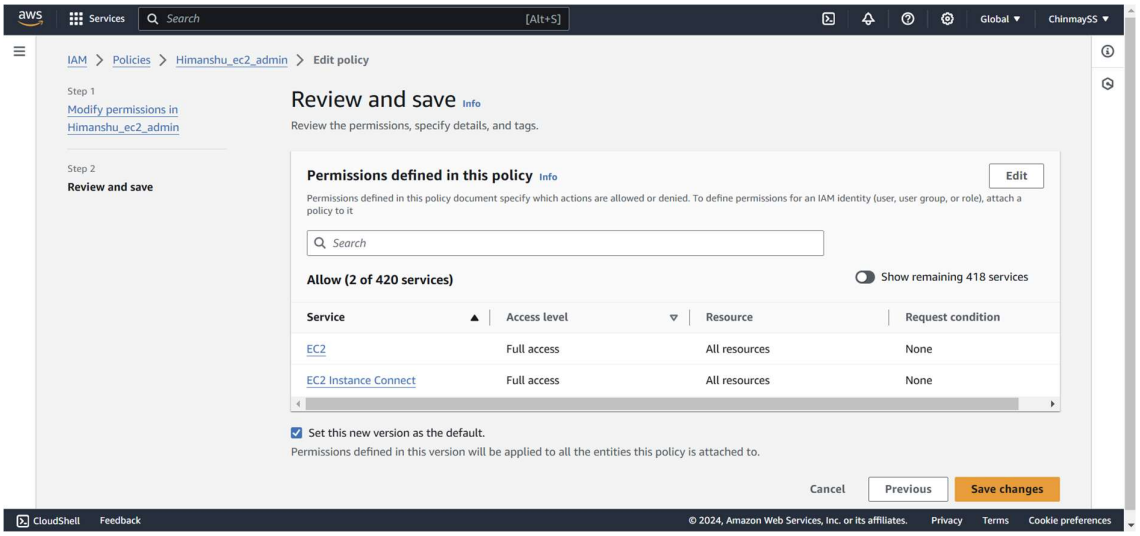

Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
ec2prac3
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

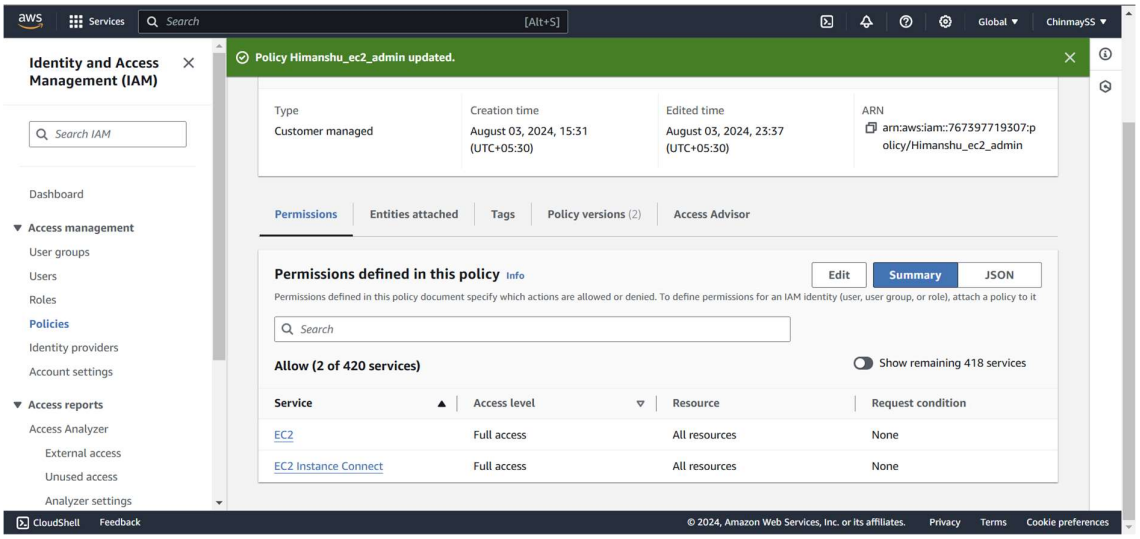

Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
Key pair name - required
ec2prac3
Create new key pair
Network settings Info
Edit
Network Info
vpc-04d074999d51c849e
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-1' with the following rules:
Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-07c8c1b18ca66bb07
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

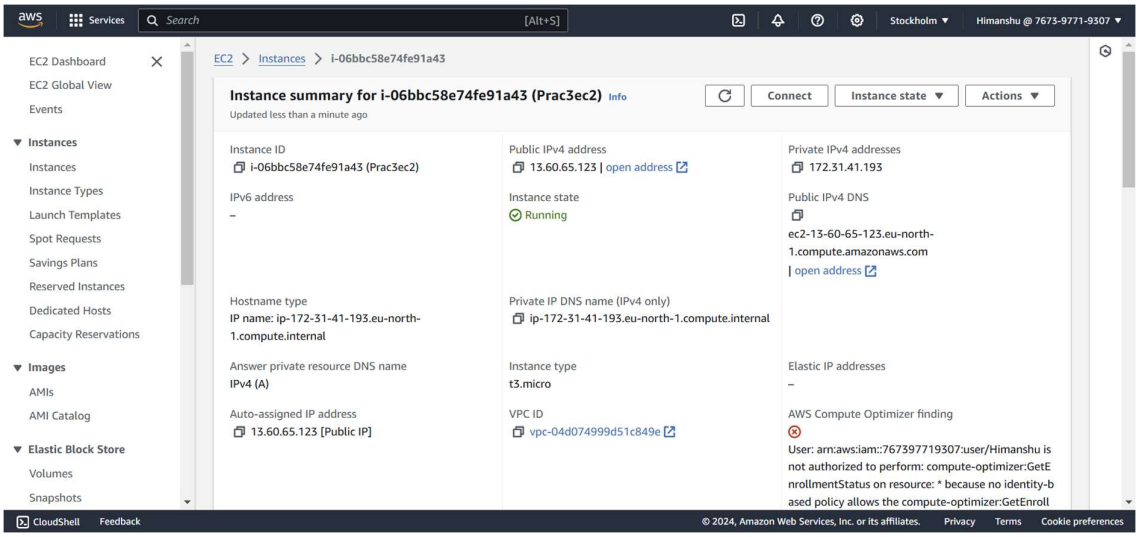

Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Prac3ec2
i-06bbc58e74fe91a43
Running
t3.micro
Initializing
User: arn:aws:
eu-north-1b
i-06bbc58e74fe91a43 (Prac3ec2)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-06bbc58e74fe91a43 (Prac3ec2)
Public IPv4 address
13.60.65.123 | open address
Private IPv4 addresses
172.31.41.193
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-13-60-65-123.eu-north-1.compute.amazonaws.com | open address
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

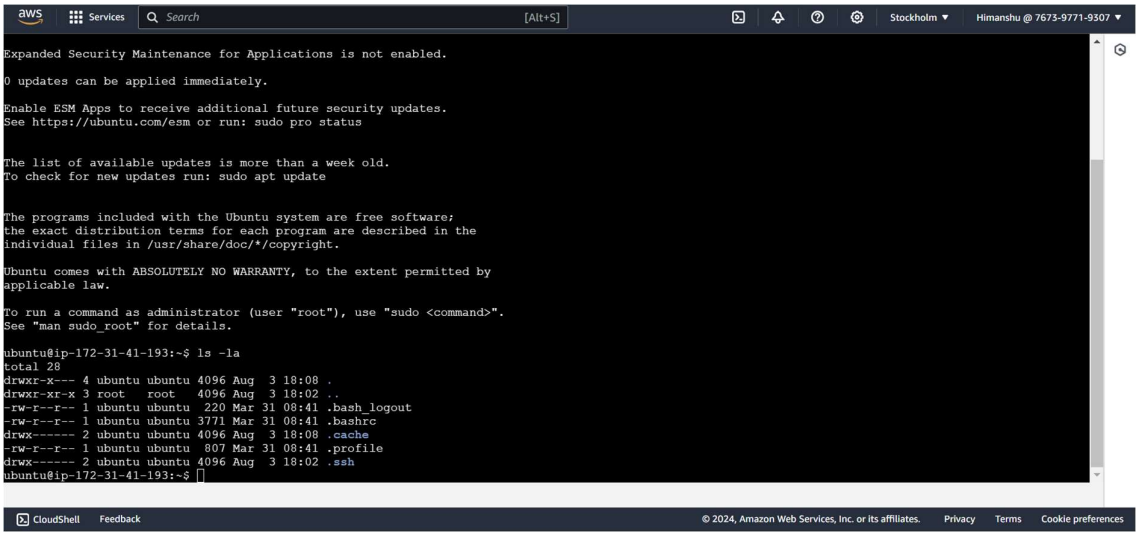

Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
Failed to connect to your instance
Access denied by EC2 Instance Connect. Either your AWS credentials are not valid or you do not have access to the EC2 instance.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
Global
ChinmaySS
IAM
Policies
Himanshu_ec2_admin
Edit policy
Step 1
Modify permissions in Himanshu_ec2_admin
Step 2
Review and save
Modify permissions in Himanshu_ec2_admin 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": "Statement1",
"Effect": "Allow",
"Action": [
"ec2:*",
"ec2-instance-connect:*"
],
"Resource": [
"*"
]
}
]
}
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
ChinmaySS
IAM > Policies > Himanshu_ec2_admin > Edit policy
Step 1
Modify permissions in Himanshu_ec2_admin
Step 2
Review and save
Review and save Info
Review the permissions, specify details, and tags.
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 (2 of 420 services)
Show remaining 418 services
Service
Access level
Resource
Request condition
EC2
Full access
All resources
None
EC2 Instance Connect
Full access
All resources
None
Set this new version as the default.
Permissions defined in this version will be applied to all the entities this policy is attached to.
Cancel
Previous
Save changes
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
ChinmaySS
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
Policy Himanshu_ec2_admin updated.
Type
Customer managed
Creation time
August 03, 2024, 15:31 (UTC+05:30)
Edited time
August 03, 2024, 23:37 (UTC+05:30)
ARN
arn:aws:iam::767397719307:policy/Himanshu_ec2_admin
Permissions
Entities attached
Tags
Policy versions (2)
Access Advisor
Permissions defined in this policy Info
Edit
Summary
JSON
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 (2 of 420 services)
Show remaining 418 services
Service
Access level
Resource
Request condition
EC2
Full access
All resources
None
EC2 Instance Connect
Full access
All resources
None
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
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
EC2 > Instances > i-06bbc58e74fe91a43
Instance summary for i-06bbc58e74fe91a43 (Prac3ec2) Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-06bbc58e74fe91a43 (Prac3ec2)
Public IPv4 address
13.60.65.123 | open address
Private IPv4 addresses
172.31.41.193
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-13-60-65-123.eu-north-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-172-31-41-193.eu-north-1.compute.internal
Private IP DNS name (IPv4 only)
ip-172-31-41-193.eu-north-1.compute.internal
Answer private resource DNS name
IPv4 (A)
Instance type
t3.micro
Elastic IP addresses
–
Auto-assigned IP address
13.60.65.123 [Public IP]
VPC ID
vpc-04d074999d51c849e
AWS Compute Optimizer finding
User: arn:aws:iam::767397719307:user/Himanshu is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnroll
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Stockholm
Himanshu @ 7673-9771-9307
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-41-193:~$ ls -la
total 28
drwxr-x--- 4 ubuntu ubuntu 4096 Aug 3 18:08 .
drwxr-xr-x 3 root root 4096 Aug 3 18:02 ..
-rw-r--r-- 1 ubuntu ubuntu 220 Mar 31 08:41 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Mar 31 08:41 .bashrc
drwx------ 2 ubuntu ubuntu 4096 Aug 3 18:08 .cache
-rw-r--r-- 1 ubuntu ubuntu 807 Mar 31 08:41 .profile
drwx------ 2 ubuntu ubuntu 4096 Aug 3 18:02 .ssh
ubuntu@ip-172-31-41-193:~$
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences