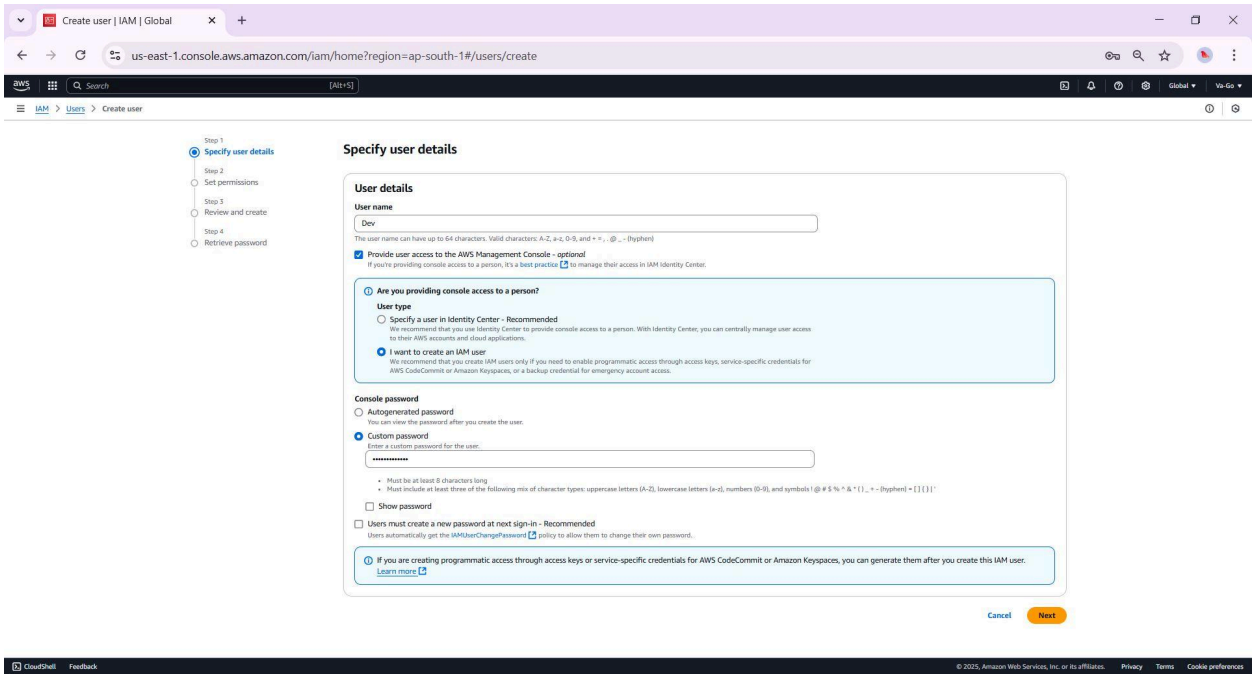
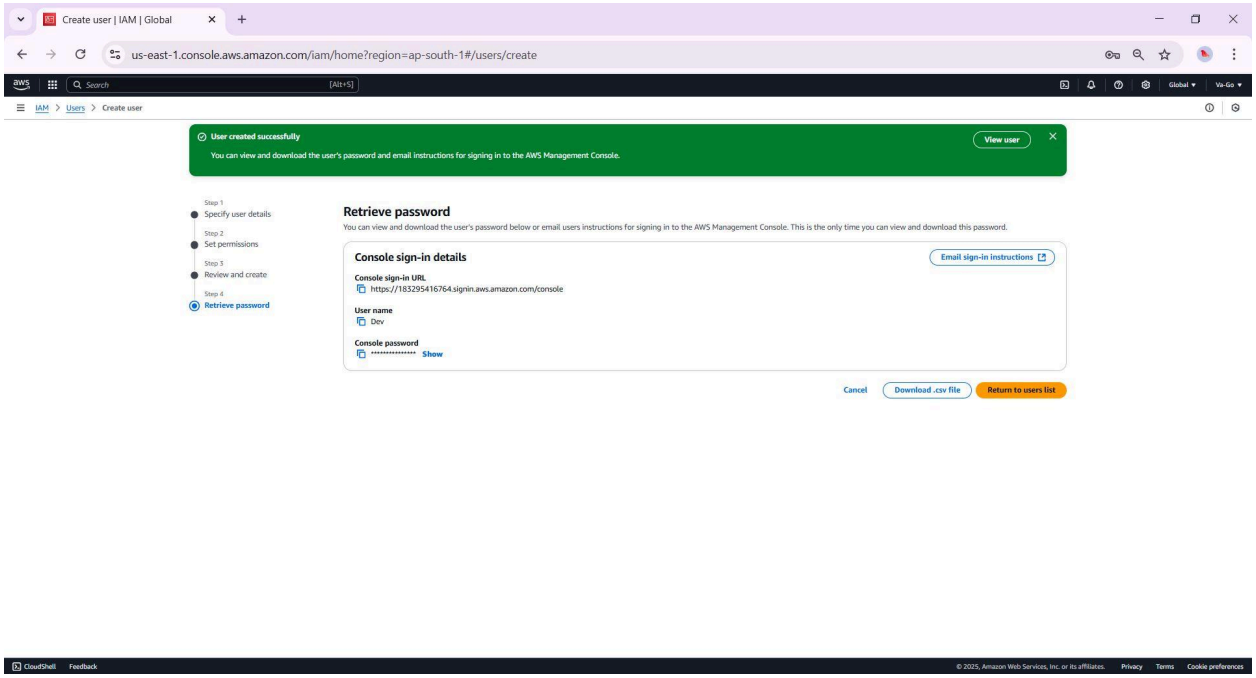
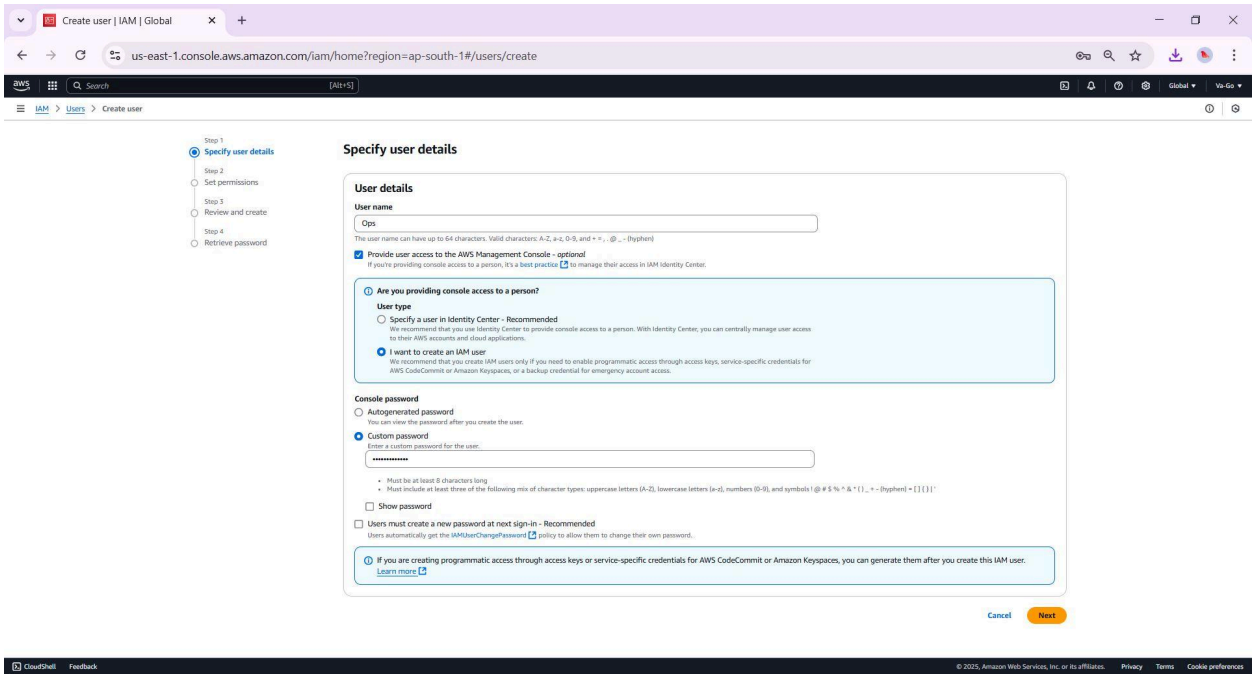
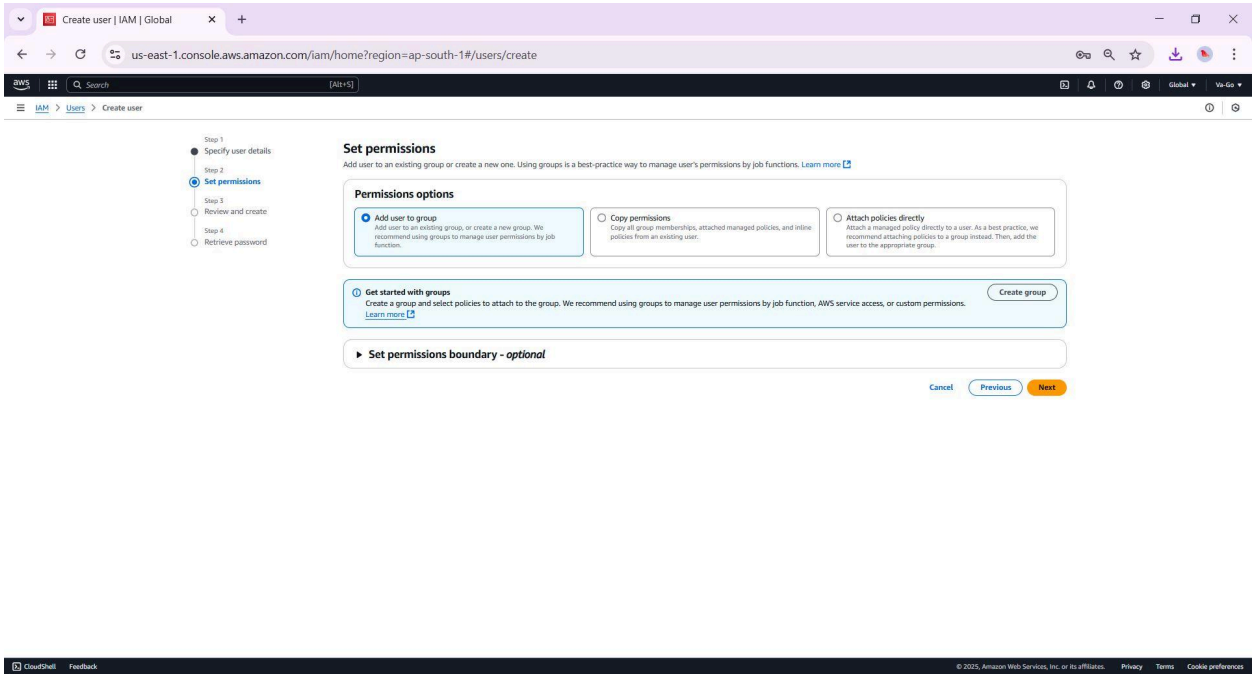
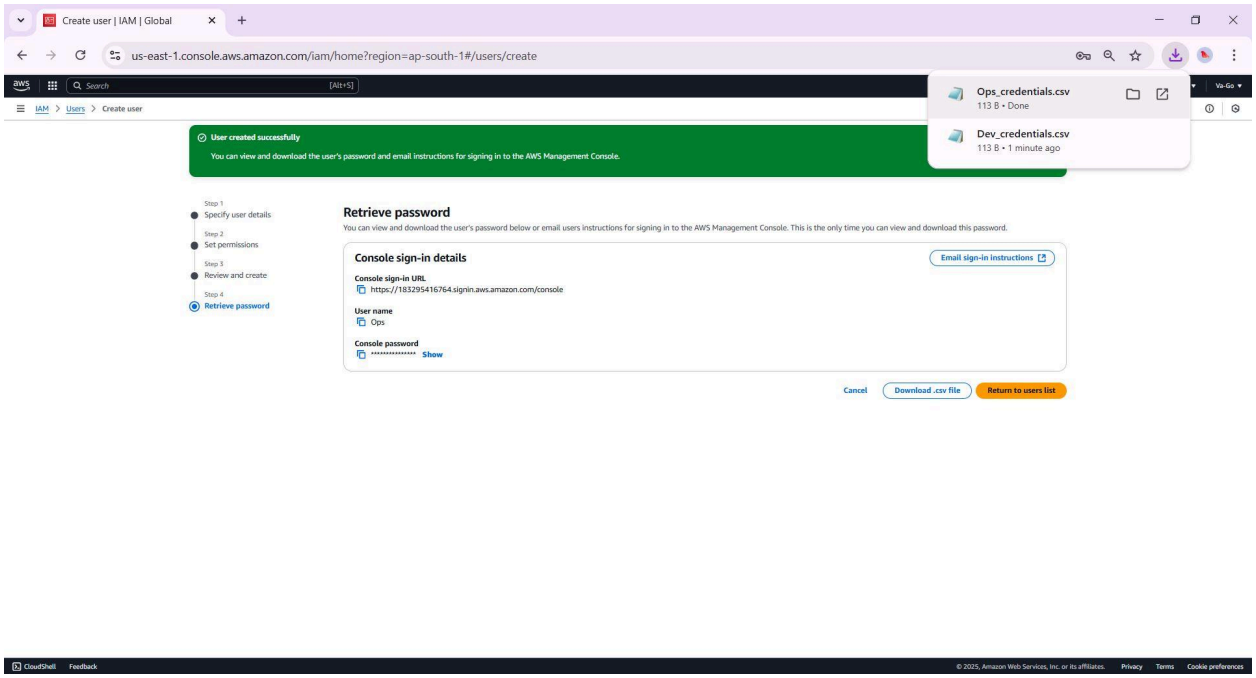
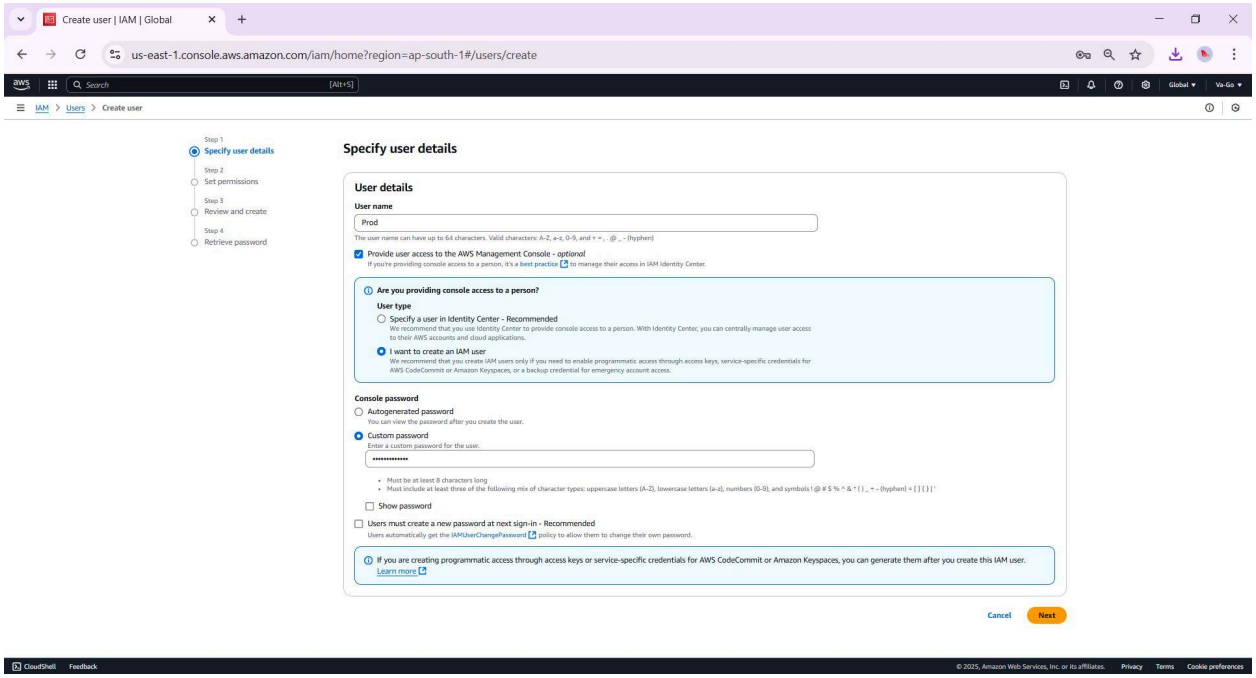

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
Dev
The user name can have up 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
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
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

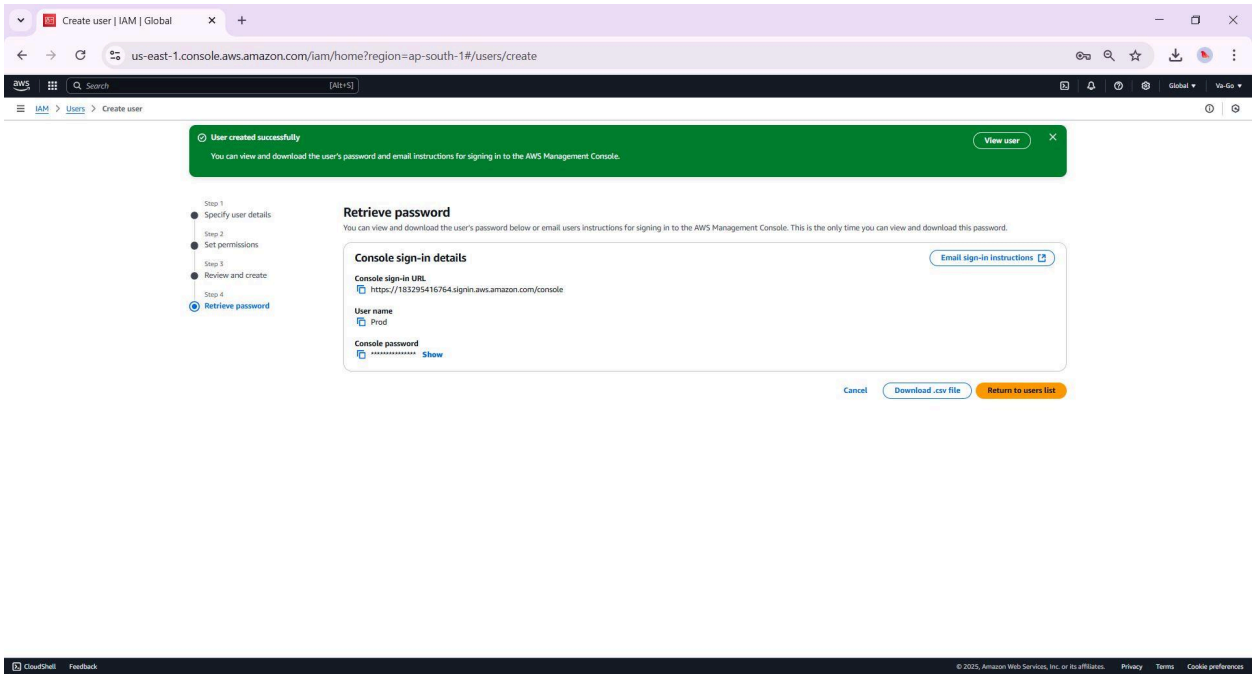

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
IAM > Users > Create user
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Step 1
Specify user details
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://183295416764.signin.aws.amazon.com/console
User name
Dev
Console password
Show
Cancel
Download .csv file
Return to users list
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

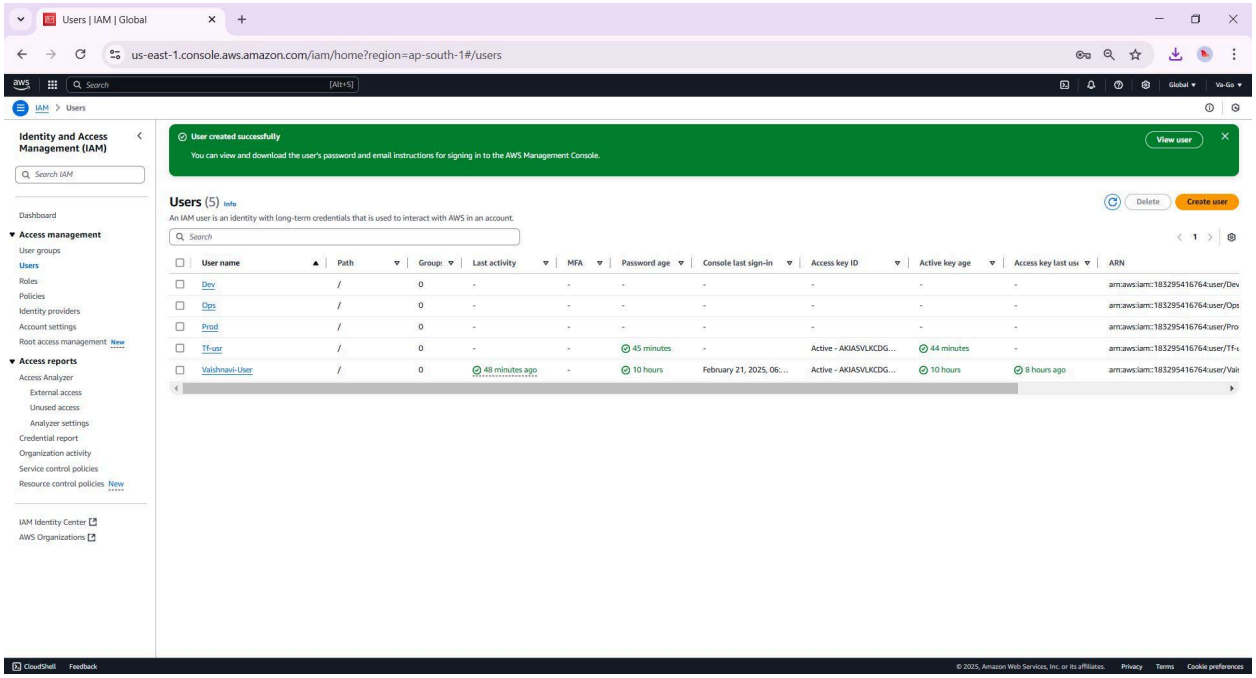

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
Ops
Provide user access to the AWS Management Console - optional
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
I want to create an IAM user
Console password
Autogenerated password
Custom password
Show password
Users must create a new password at next sign-in - Recommended
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

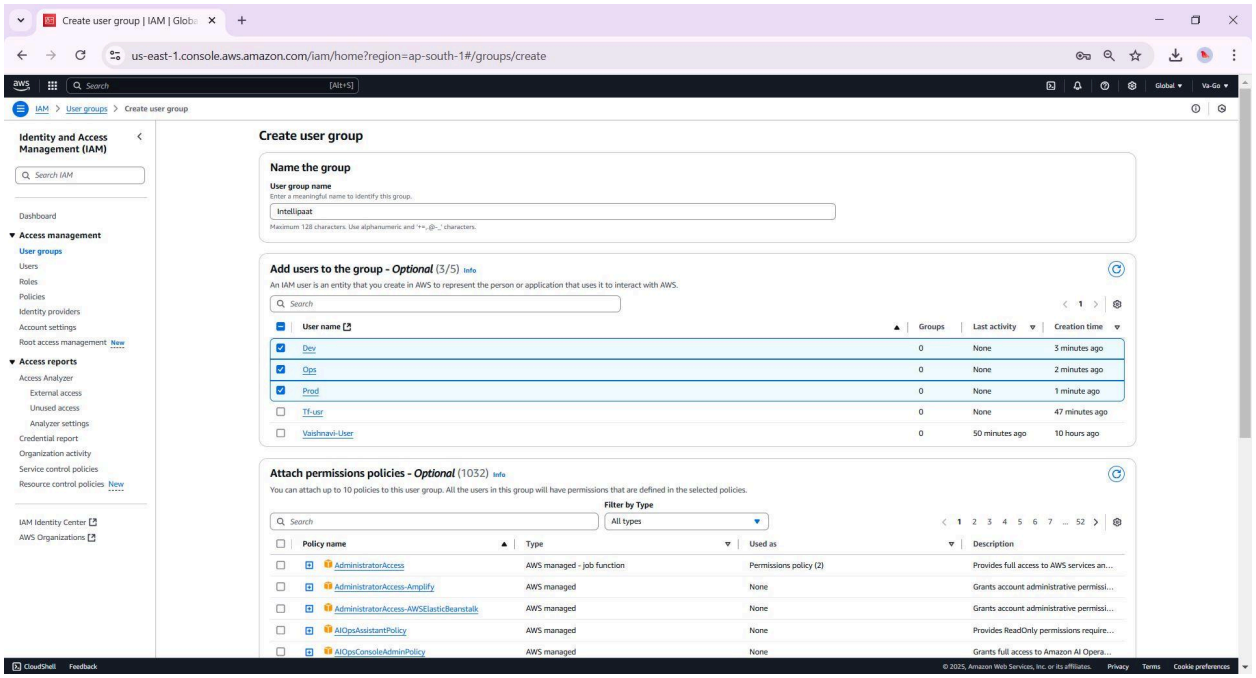

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Copy permissions
Attach policies directly
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions.
Learn more
Create group
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback

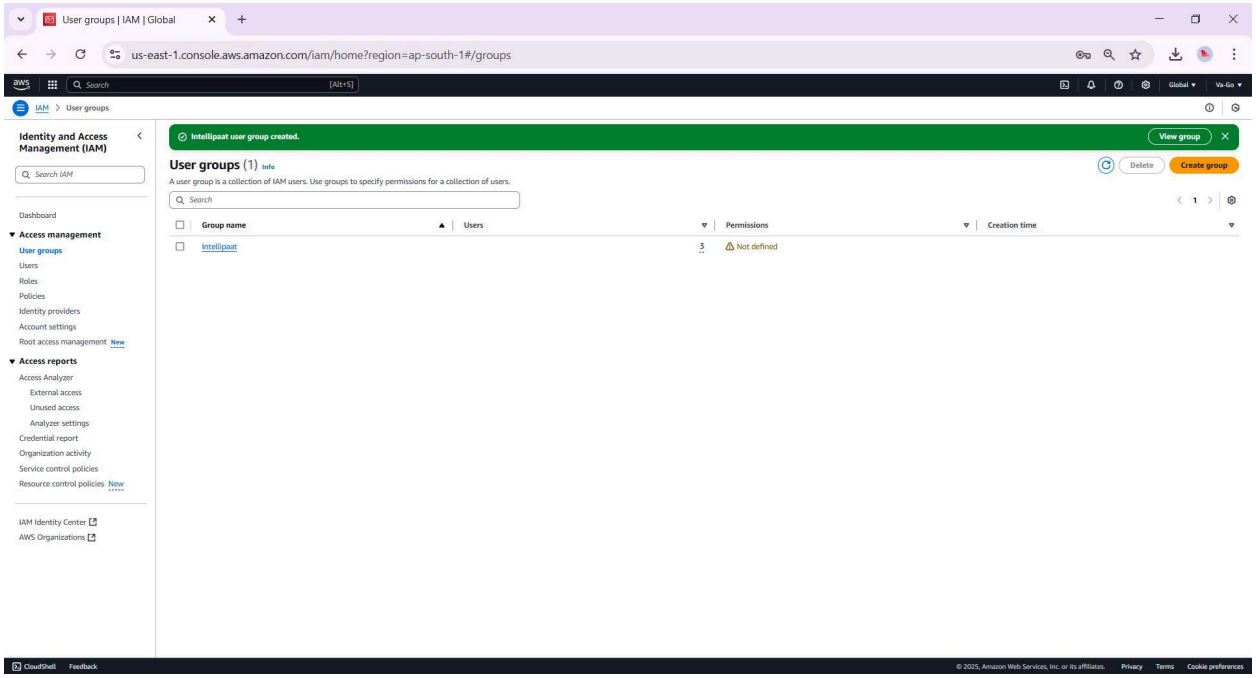

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Search [Alt+S]
IAM > Users > Create user
Ops_credentials.csv
113 B • Done
Dev_credentials.csv
113 B • 1 minute ago
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
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://183295416764.signin.aws.amazon.com/console
User name
Ops
Console password
Show
Cancel
Download .csv file
Return to users list
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

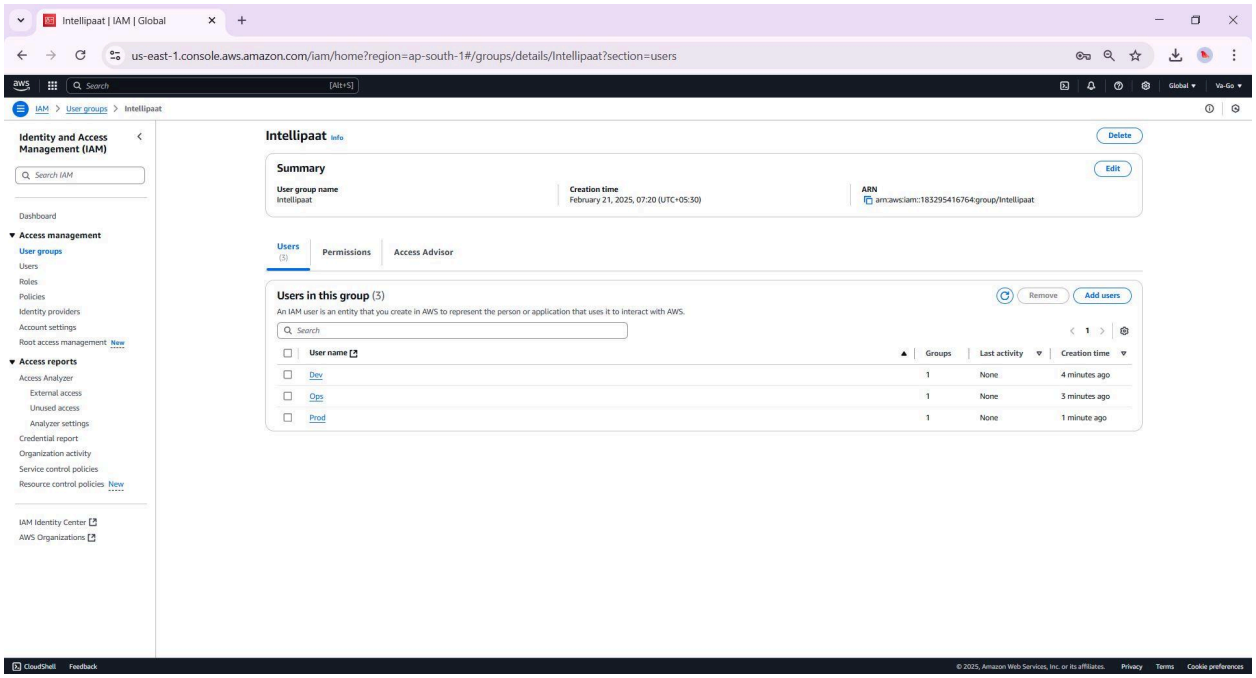

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Search [Alt+S]
IAM > Users > Create user
Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create
Step 4 Retrieve password
Specify user details
User details
User name
Prod
The user 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
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
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

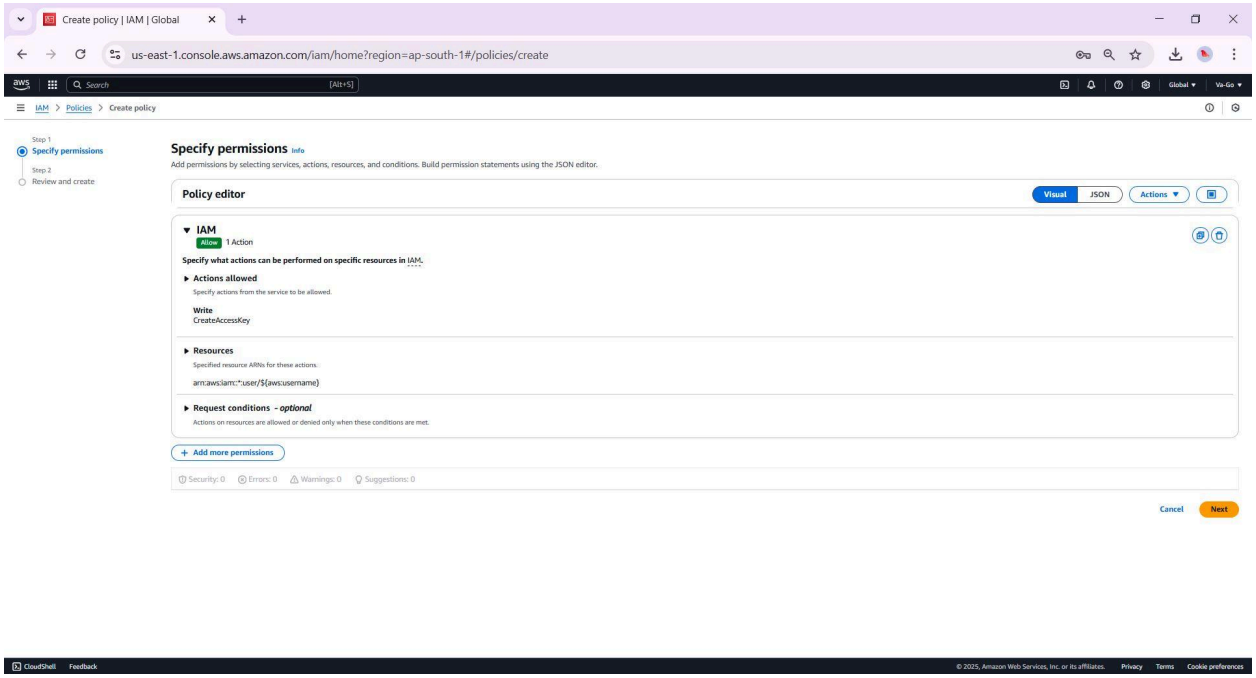

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
IAM > Users > Create user
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Step 1
Specify user details
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://183295416764.signin.aws.amazon.com/console
User name
Prod
Console password
Show
Cancel
Download .csv file
Return to users list
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

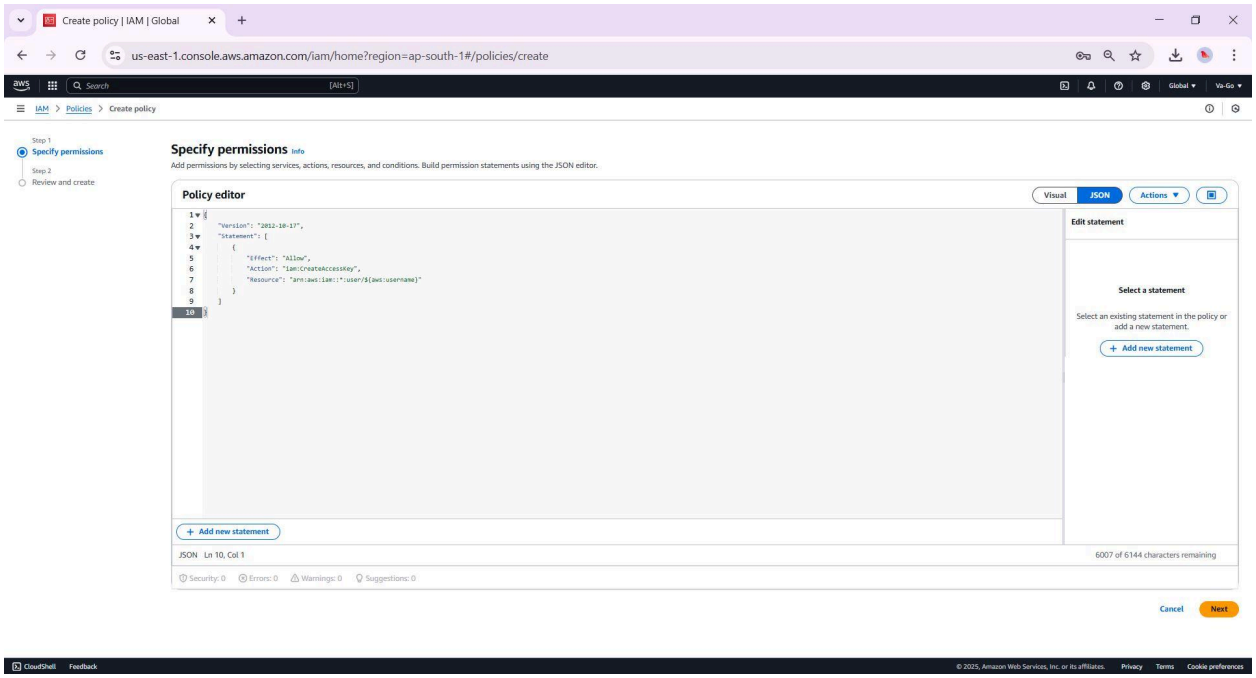

Users | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
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
Users (5) 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
Group:
Last activity
MFA
Password age
Console last sign-in
Access key ID
Active key age
Access key last us
ARN
Dev / 0 - - - - - - - arn:aws:iam::183295416764:user/Dev
Ops / 0 - - - - - - - arn:aws:iam::183295416764:user/Ops
Prod / 0 - - - - - - - arn:aws:iam::183295416764:user/Pro
Tf-usr / 0 - - 45 minutes - Active - AKIASVLKCDG... 44 minutes - arn:aws:iam::183295416764:user/TF-
Vaishnavi-User / 0 48 minutes ago - 10 hours February 21, 2025, 06:... Active - AKIASVLKCDG... 10 hours 8 hours ago arn:aws:iam::183295416764:user/Vai
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

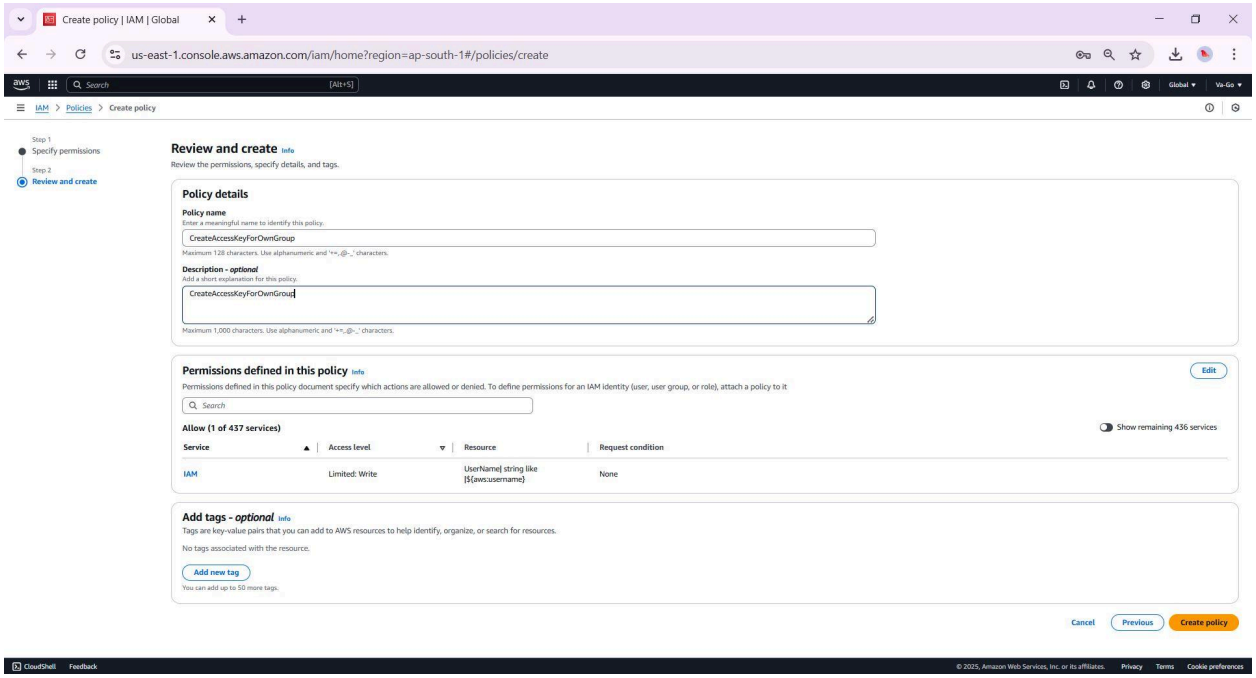

Create user group | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/create
IAM > User groups > Create user group
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
Intellipaat
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (3/5) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
User name
Groups
Last activity
Creation time
Dev 0 None 3 minutes ago
Ops 0 None 2 minutes ago
Prod 0 None 1 minute ago
Tf-usr 0 None 47 minutes ago
Vaishnavi-User 0 50 minutes ago 10 hours ago
Attach permissions policies - Optional (1032) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Filter by Type
All types
Policy name
Type
Used as
Description
AdministratorAccess AWS managed - job function Permissions policy (2) Provides full access to AWS services an...
AdministratorAccess-Amplify AWS managed None Grants account administrative permissi...
AdministratorAccess-AWSElasticBeanstalk AWS managed None Grants account administrative permissi...
AIOpsAssistantPolicy AWS managed None Provides ReadOnly permissions require...
AIOpsConsoleAdminPolicy AWS managed None Grants full access to Amazon AI Opera...
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

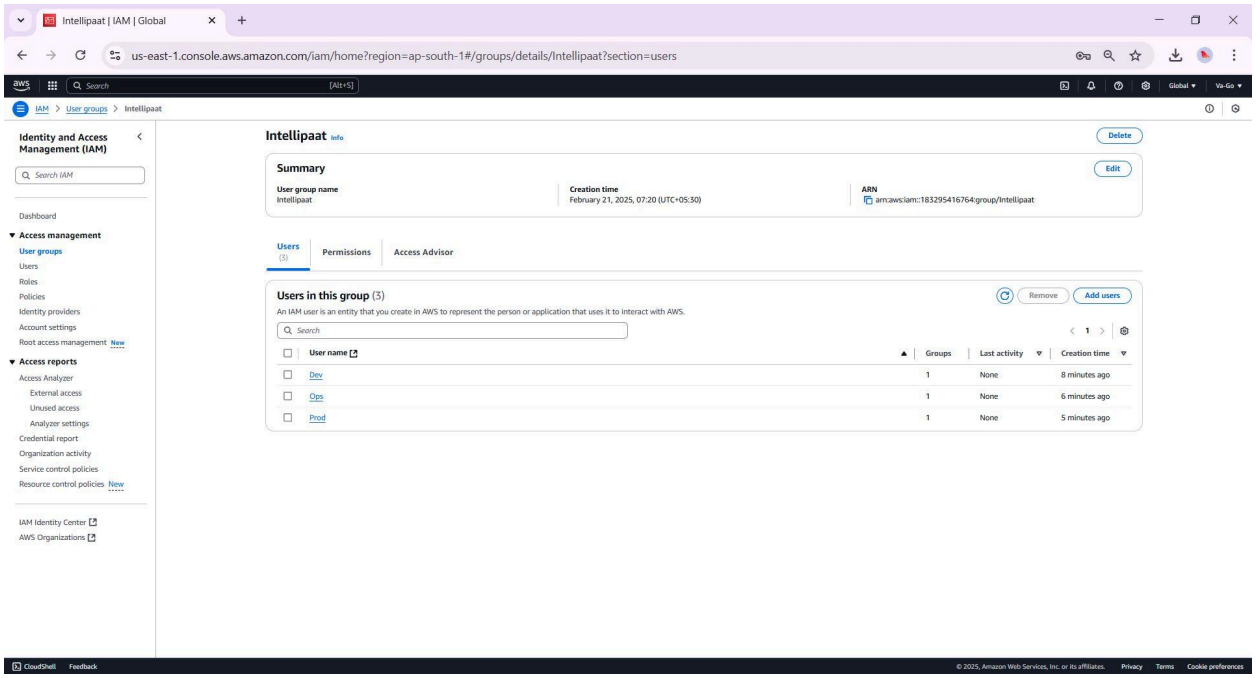

User groups | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups
IAM > User groups
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Intellipaat user group created.
View group
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
Intellipaat 3 Not defined
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

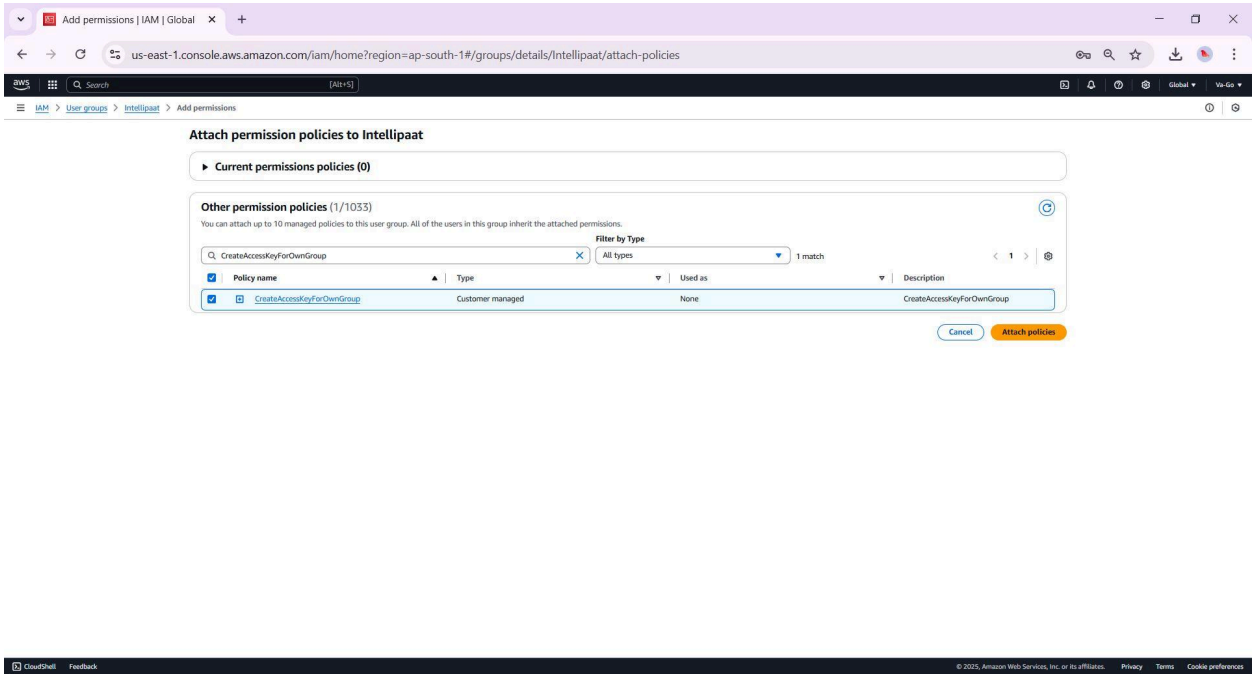

Intellipaat | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Intellipaat?section=users
IAM > User groups > Intellipaat
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Intellipaat Info
Delete
Summary
Edit
User group name
intellipaat
Creation time
February 21, 2025, 07:20 (UTC+05:30)
ARN
arn:aws:iam::183295416764:group/Intellipaat
Users (3)
Permissions
Access Advisor
Users in this group (3)
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
Dev
1
None
4 minutes ago
Ops
1
None
3 minutes ago
Prod
1
None
1 minute ago
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

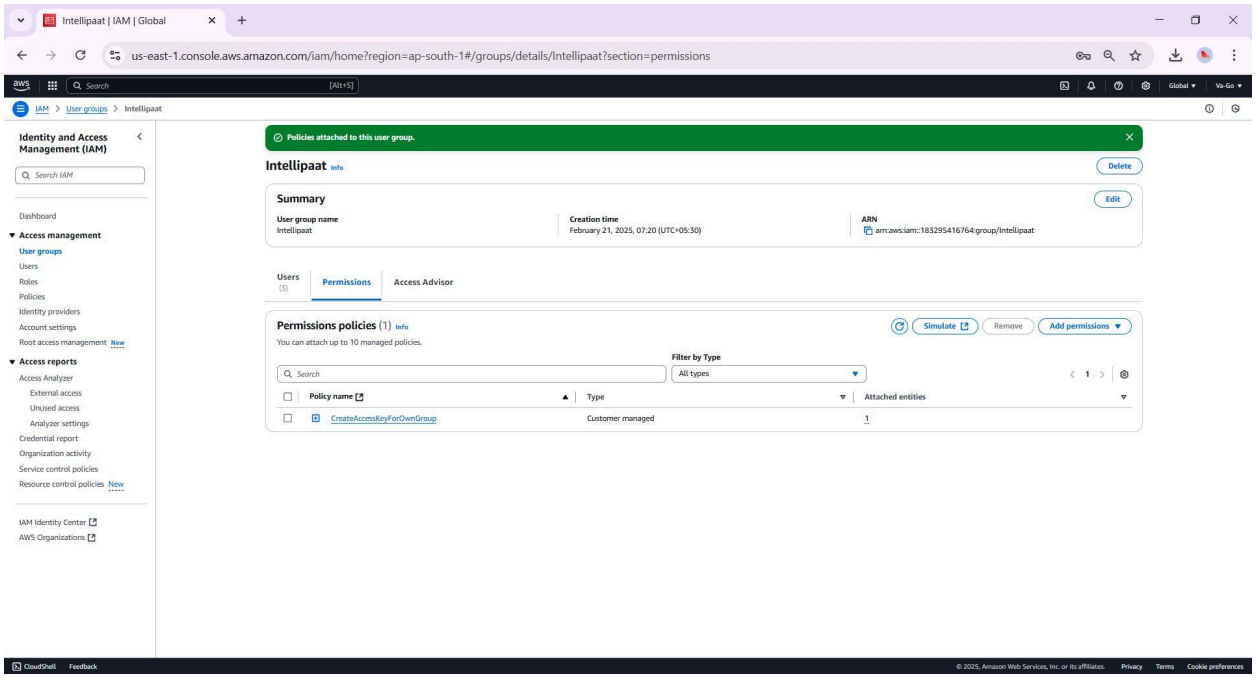

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
IAM
Allow
1 Action
Specify what actions can be performed on specific resources in IAM.
Actions allowed
Specify actions from the service to be allowed.
Write
CreateAccessKey
Resources
Specified resource ARNs for these actions.
arn:aws:iam::*:user/${aws:username}
Request conditions - optional
Actions on resources are allowed or denied only when these conditions are met.
Add more permissions
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

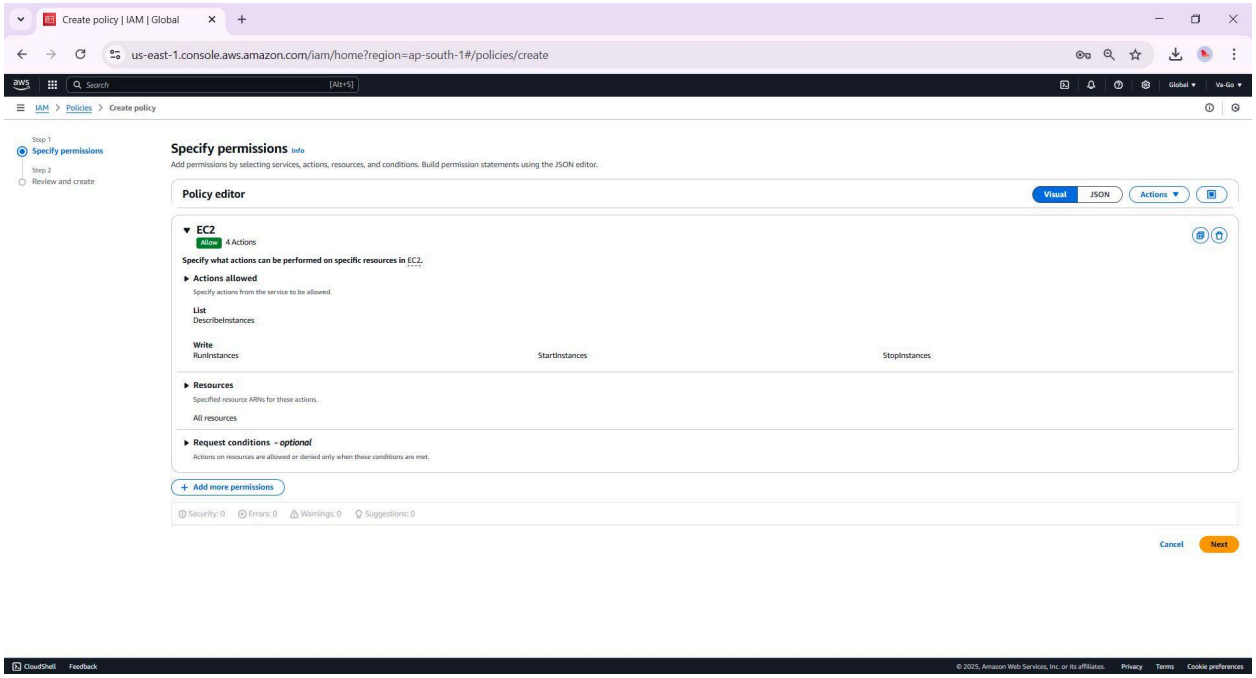

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "iam:CreateAccessKey",
"Resource": "arn:aws:iam::*:user/${aws:username}"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
+ Add new statement
JSON Ln 10, Col 1
6007 of 6144 characters remaining
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

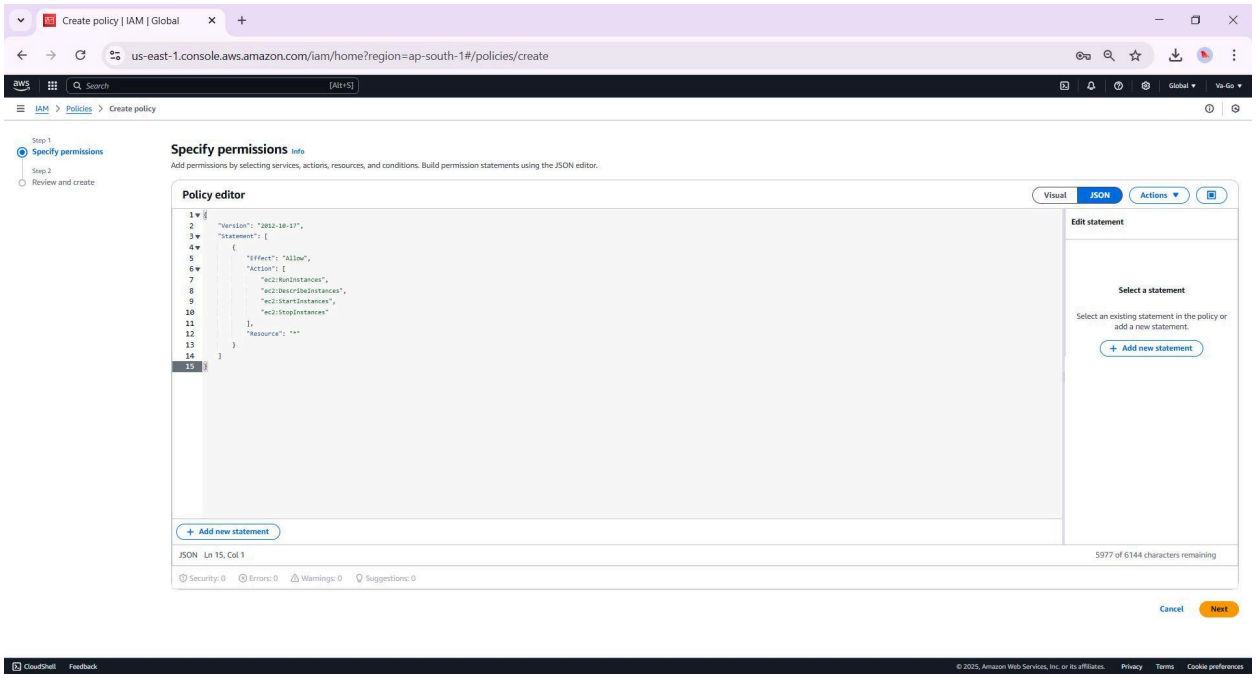

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
CreateAccessKeyForOwnGroup
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
CreateAccessKeyForOwnGroup
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 437 services)
Show remaining 436 services
Service
Access level
Resource
Request condition
IAM
Limited: Write
UserName| string like [${aws:username}
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
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

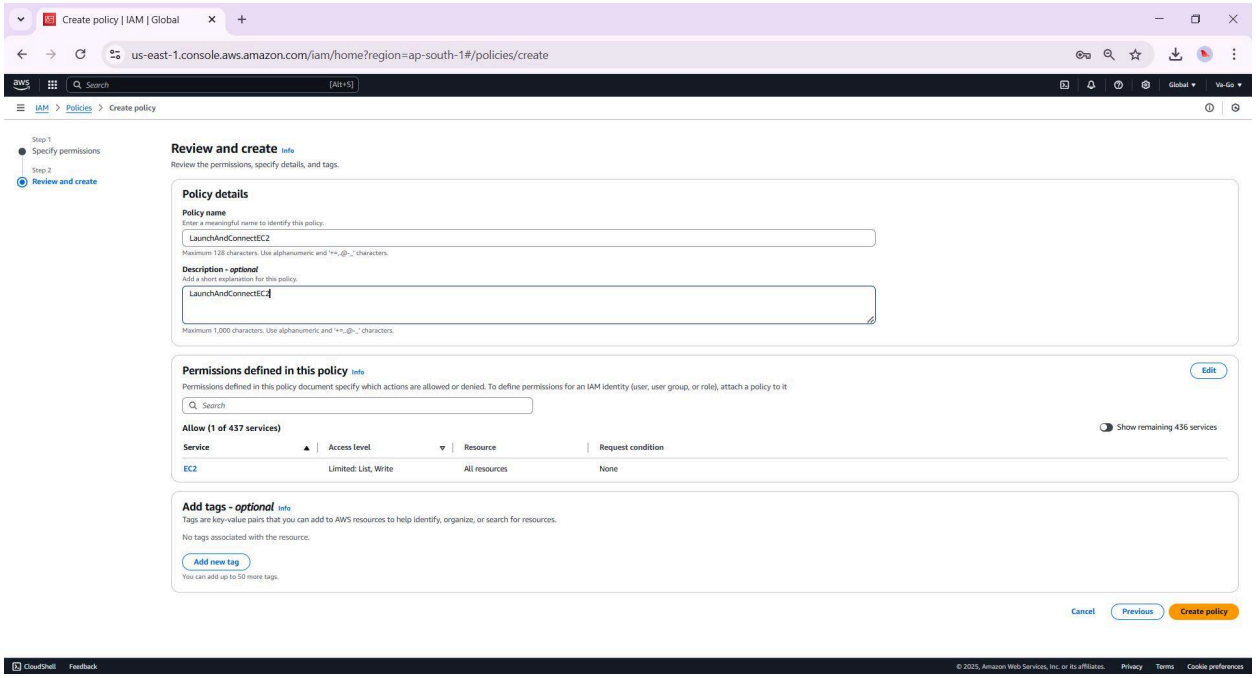

Intellipaat | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Intellipaat?section=users
IAM > User groups > Intellipaat
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Intellipaat Info
Delete
Summary
Edit
User group name
intellipaat
Creation time
February 21, 2025, 07:20 (UTC+05:30)
ARN
arn:aws:iam::183295416764:group/Intellipaat
Users (3)
Permissions
Access Advisor
Users in this group (3)
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
Dev
1
None
8 minutes ago
Ops
1
None
6 minutes ago
Prod
1
None
5 minutes ago
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

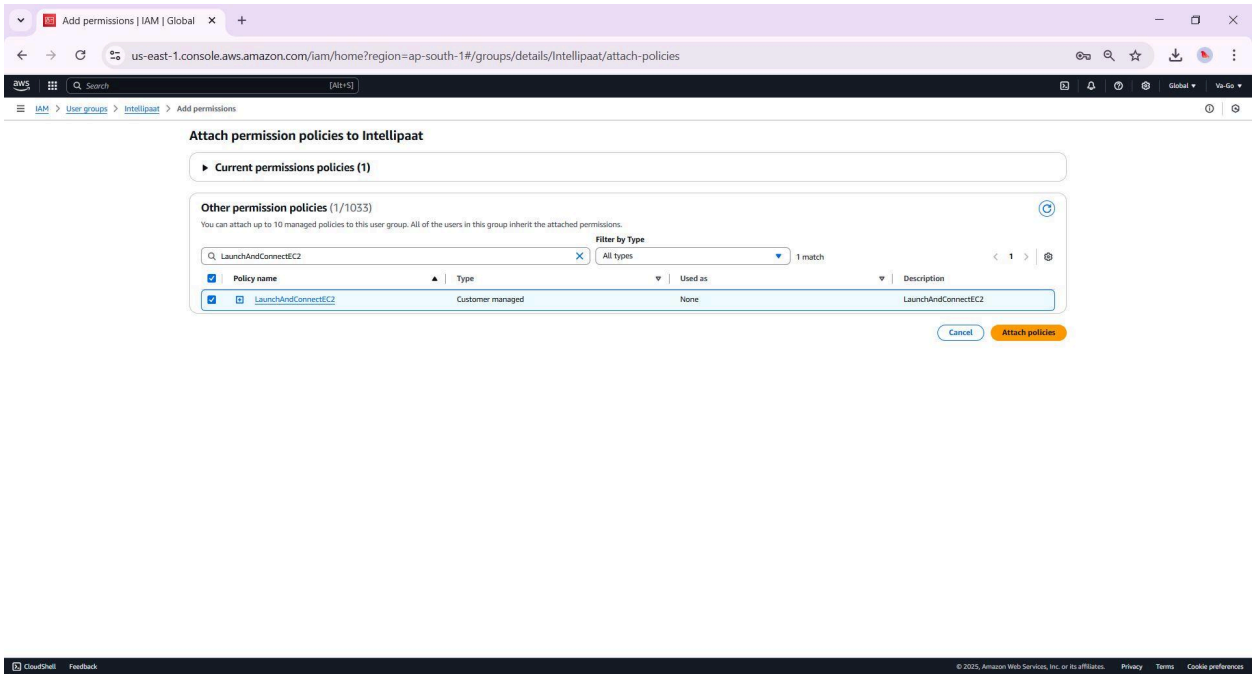

Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Intellipaat/attach-policies
IAM > User groups > Intellipaat > Add permissions
Attach permission policies to Intellipaat
Current permissions policies (0)
Other permission policies (1/1033)
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.
Filter by Type
CreateAccessKeyForOwnGroup
All types
1 match
Policy name
Type
Used as
Description
CreateAccessKeyForOwnGroup
Customer managed
None
CreateAccessKeyForOwnGroup
Cancel
Attach policies
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

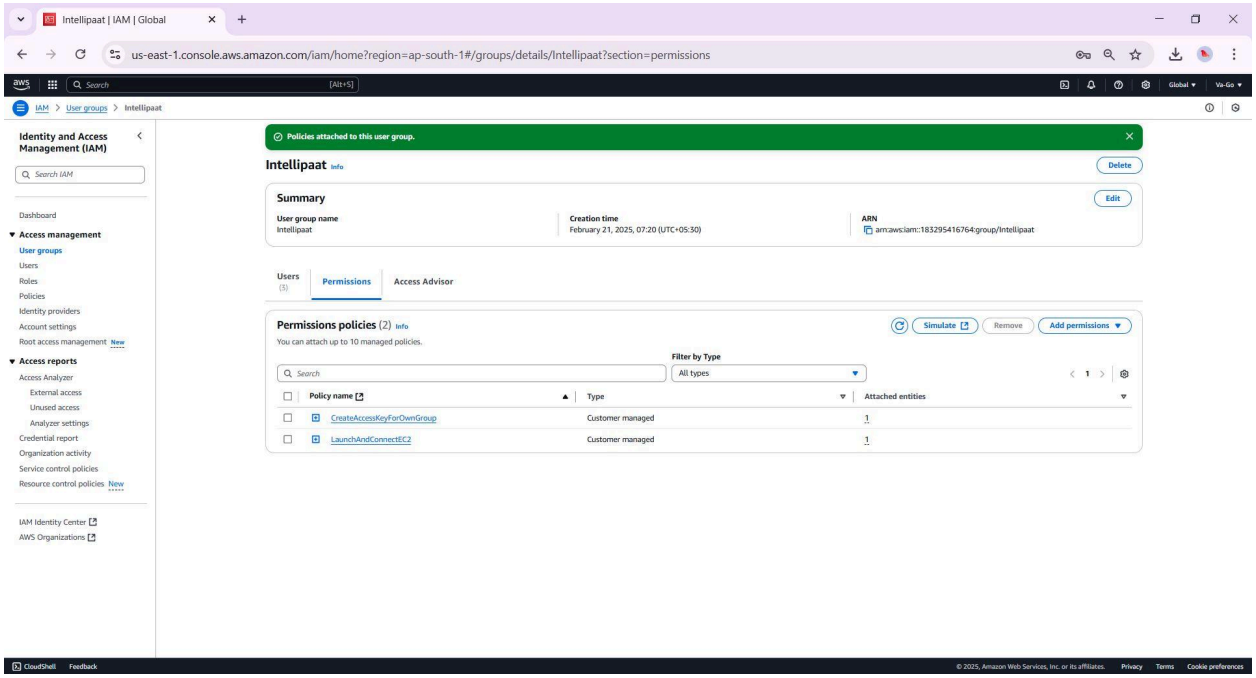

Intellipaat | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Intellipaat?section=permissions
IAM > User groups > Intellipaat
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Policies attached to this user group.
Intellipaat Info
Delete
Summary
Edit
User group name
Intellipaat
Creation time
February 21, 2025, 07:20 (UTC+05:30)
ARN
arn:aws:iam::183295416764:group/Intellipaat
Users (5)
Permissions
Access Advisor
Permissions policies (1) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached entities
CreateAccessKeyForOwnGroup
Customer managed
1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

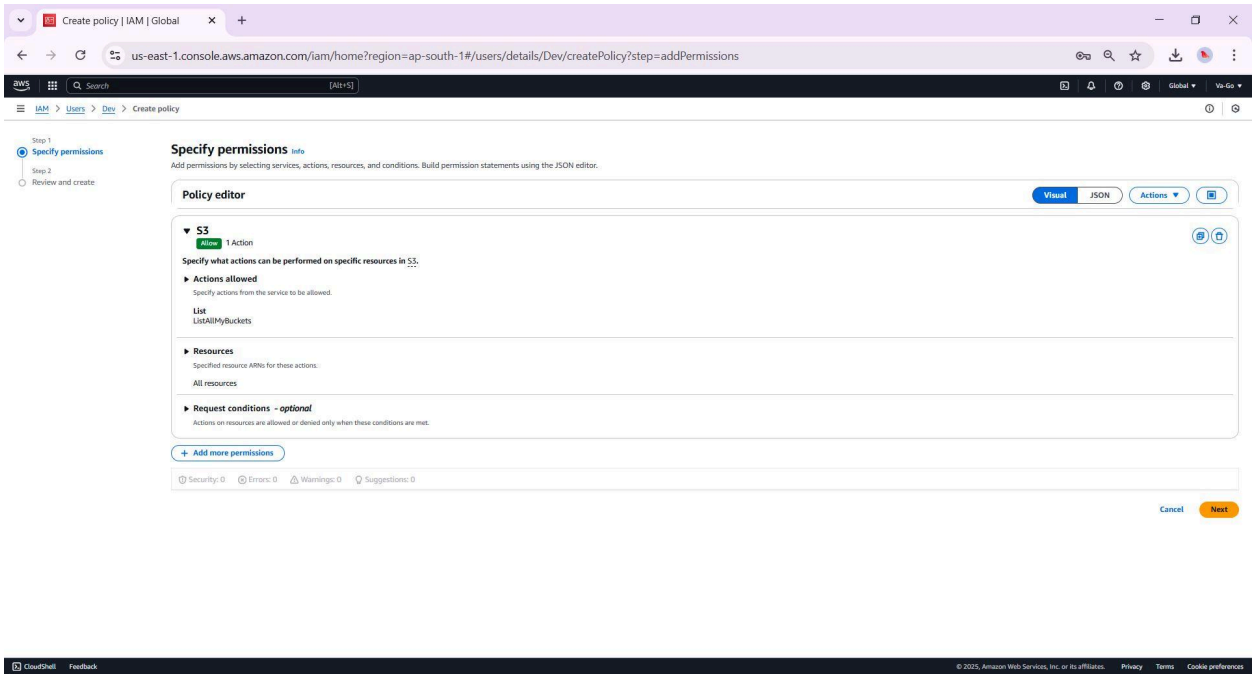

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
EC2
Allow
4 Actions
Specify what actions can be performed on specific resources in EC2.
Actions allowed
Specify actions from the service to be allowed.
List
DescribeInstances
Write
RunInstances
StartInstances
StopInstances
Resources
Specified resource ARNs for these actions.
All resources
Request conditions - optional
Actions on resources are allowed or denied only when these conditions are met.
Add more permissions
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

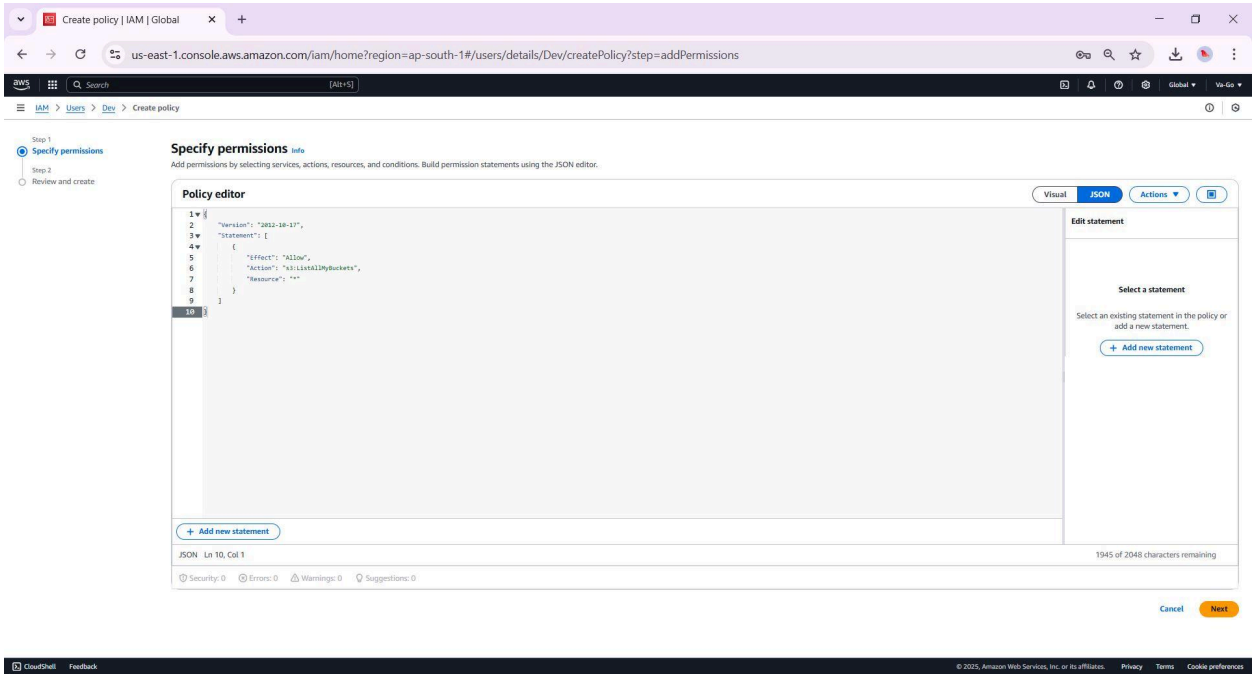

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:RunInstances",
"ec2:DescribeInstances",
"ec2:StartInstances",
"ec2:StopInstances"
],
"Resource": "*"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement
Add new statement
JSON Ln 15, Col 1
5977 of 6144 characters remaining
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

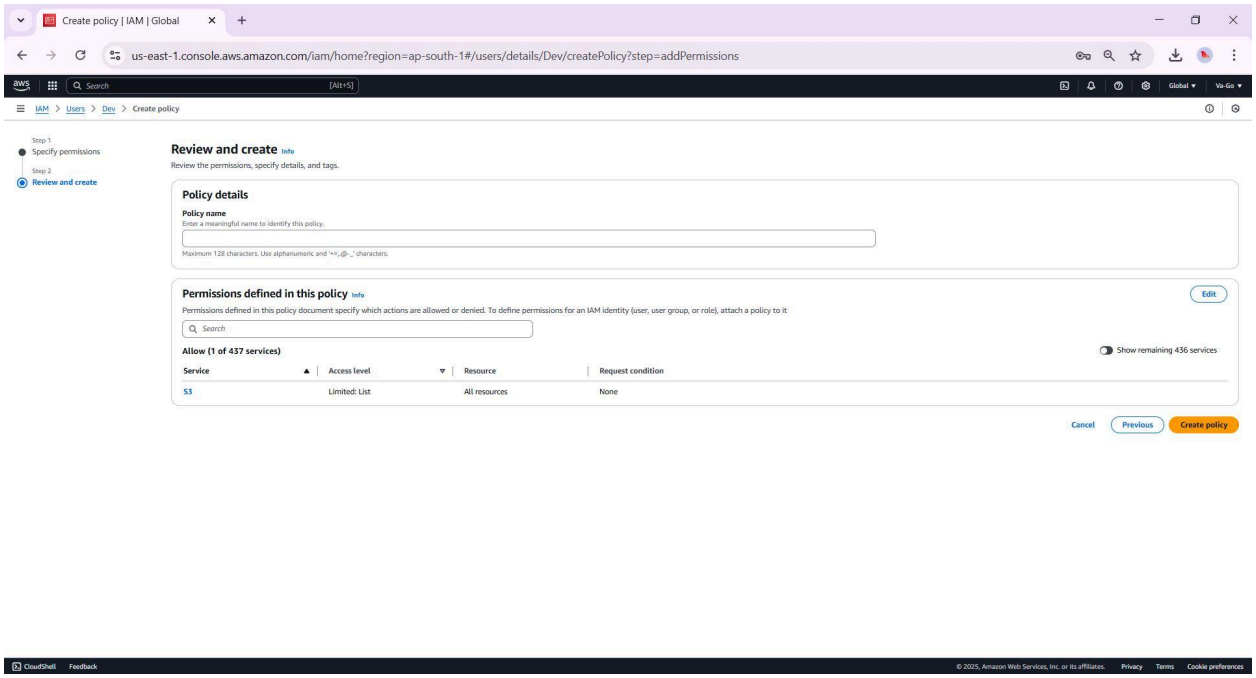

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
LaunchAndConnectEC2
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
LaunchAndConnectEC2
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 437 services)
Show remaining 436 services
Service
Access level
Resource
Request condition
EC2
Limited: List, Write
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
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

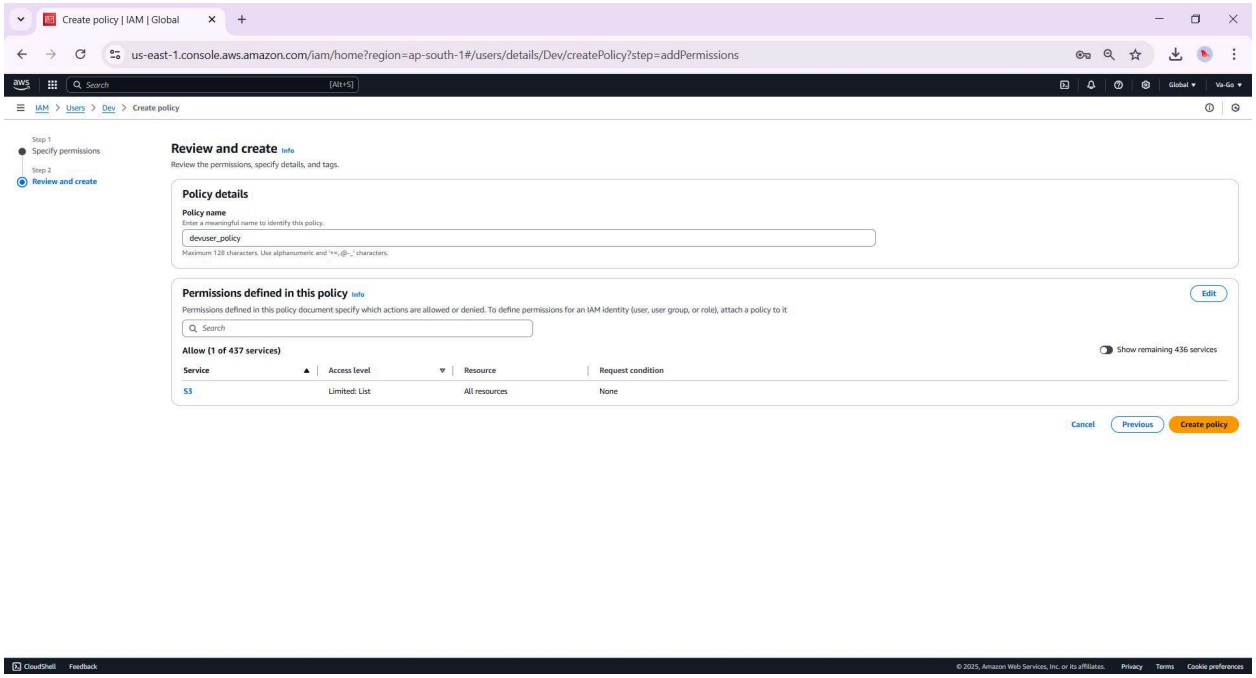

Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Intellipaat/attach-policies
IAM > User groups > Intellipaat > Add permissions
Attach permission policies to Intellipaat
Current permissions policies (1)
Other permission policies (1/1033)
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.
Filter by Type
LaunchAndConnectEC2
All types
1 match
Policy name
Type
Used as
Description
LaunchAndConnectEC2
Customer managed
None
LaunchAndConnectEC2
Cancel
Attach policies
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

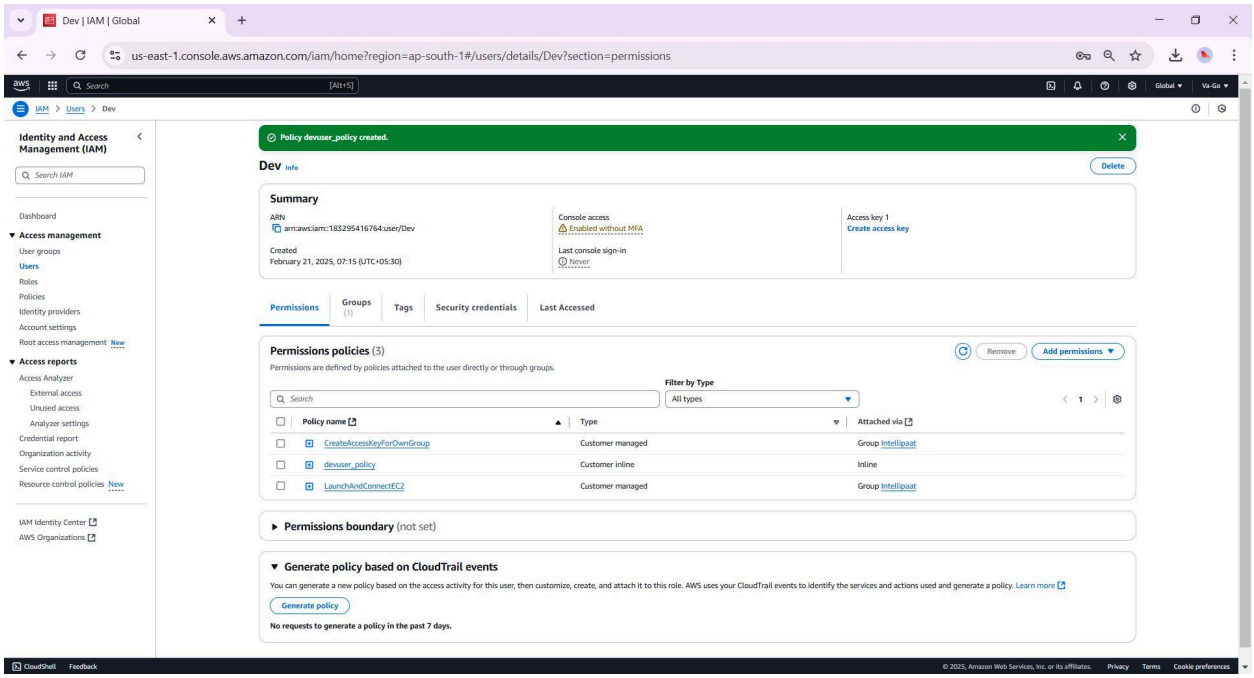

Intellipaat | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Intellipaat?section=permissions
IAM > User groups > Intellipaat
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Policies attached to this user group.
Intellipaat Info
Delete
Summary
Edit
User group name
Intellipaat
Creation time
February 21, 2025, 07:20 (UTC+05:30)
ARN
arn:aws:iam::183295416764:group/Intellipaat
Users (5)
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
CreateAccessKeyForOwnGroup
Customer managed
1
LaunchAndConnectEC2
Customer managed
1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

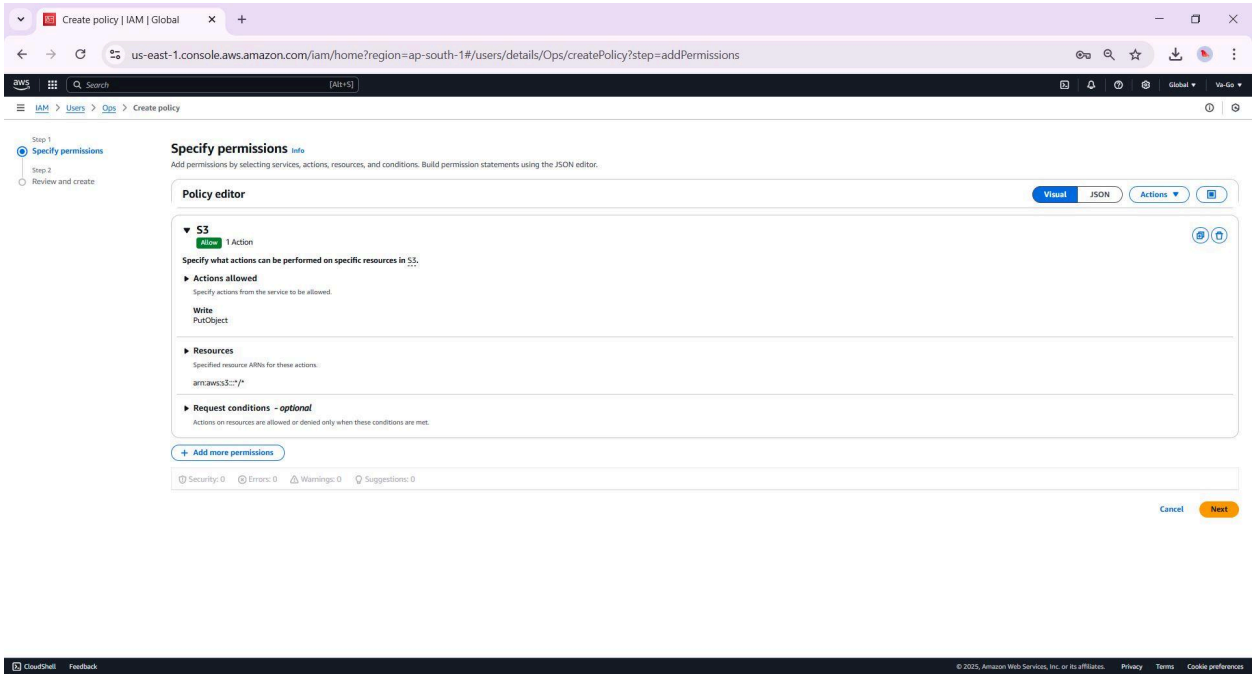

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Dev/createPolicy?step=addPermissions
IAM > Users > Dev > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
S3
Allow 1 Action
Specify what actions can be performed on specific resources in S3.
Actions allowed
Specify actions from the service to be allowed.
List
ListAllMyBuckets
Resources
Specified resource ARNs for these actions.
All resources
Request conditions - optional
Actions on resources are allowed or denied only when these conditions are met.
Add more permissions
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

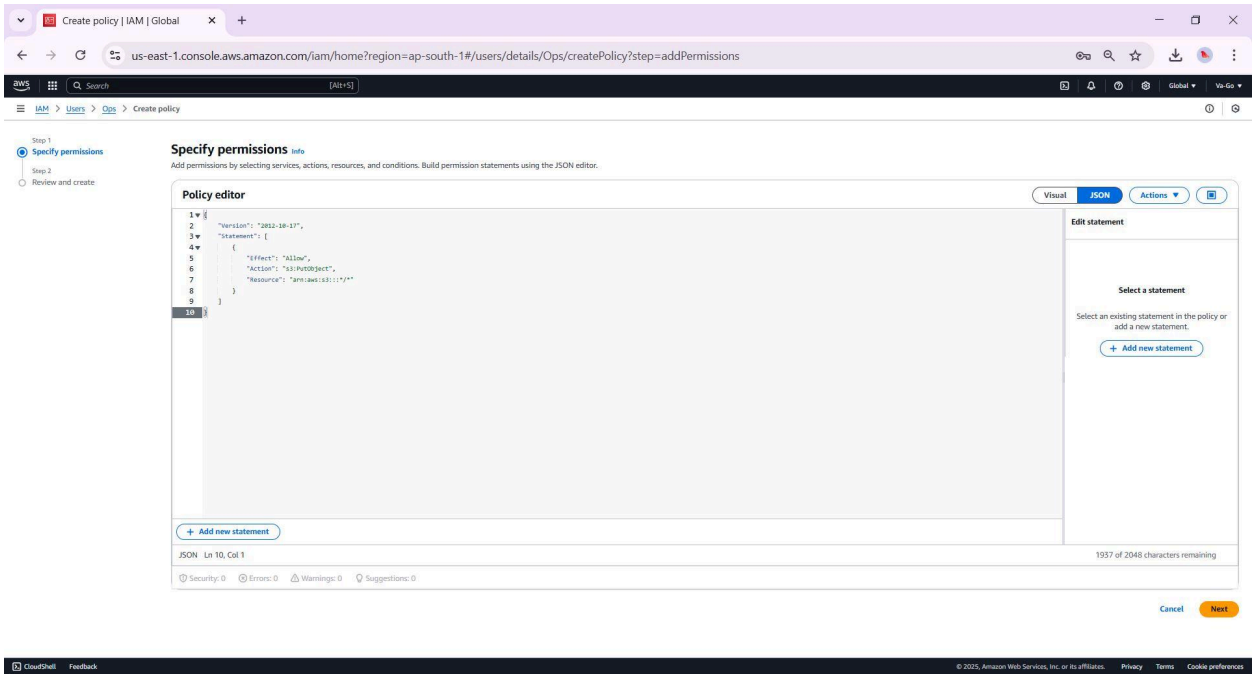

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Dev/createPolicy?step=addPermissions
IAM > Users > Dev > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "s3:ListAllMyBuckets",
"Resource": "*"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement
Add new statement
JSON Ln 10, Col 1
1945 of 2048 characters remaining
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

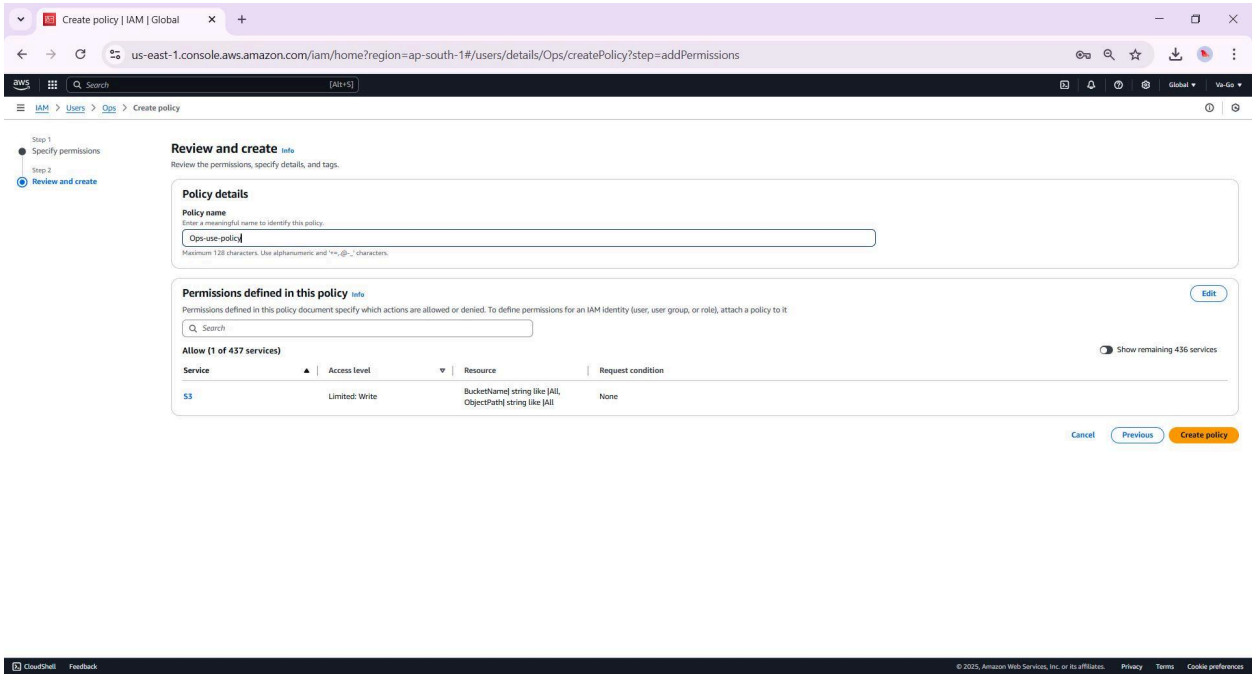

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Dev/createPolicy?step=addPermissions
IAM > Users > Dev > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 437 services)
Show remaining 436 services
Service
Access level
Resource
Request condition
S3
Limited: List
All resources
None
Cancel
Previous
Create policy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

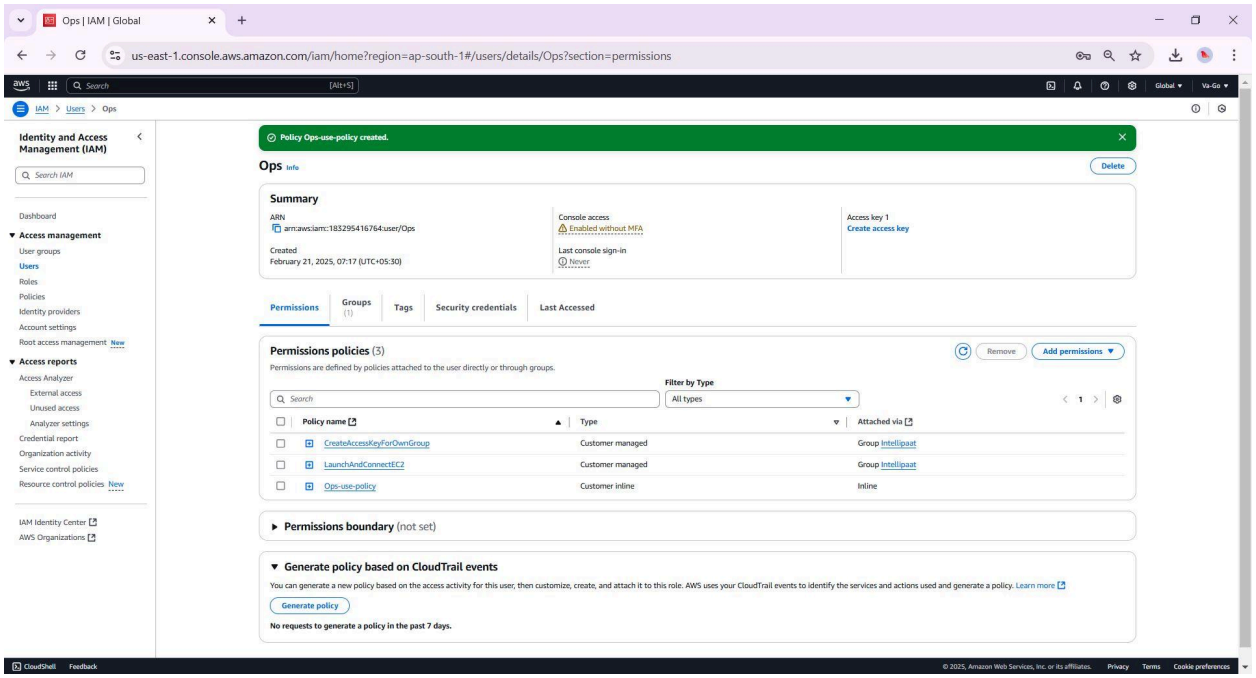

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Dev/createPolicy?step=addPermissions
IAM > Users > Dev > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
devuser_policy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 437 services)
Show remaining 436 services
Service
Access level
Resource
Request condition
S3
Limited: List
All resources
None
Cancel
Previous
Create policy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

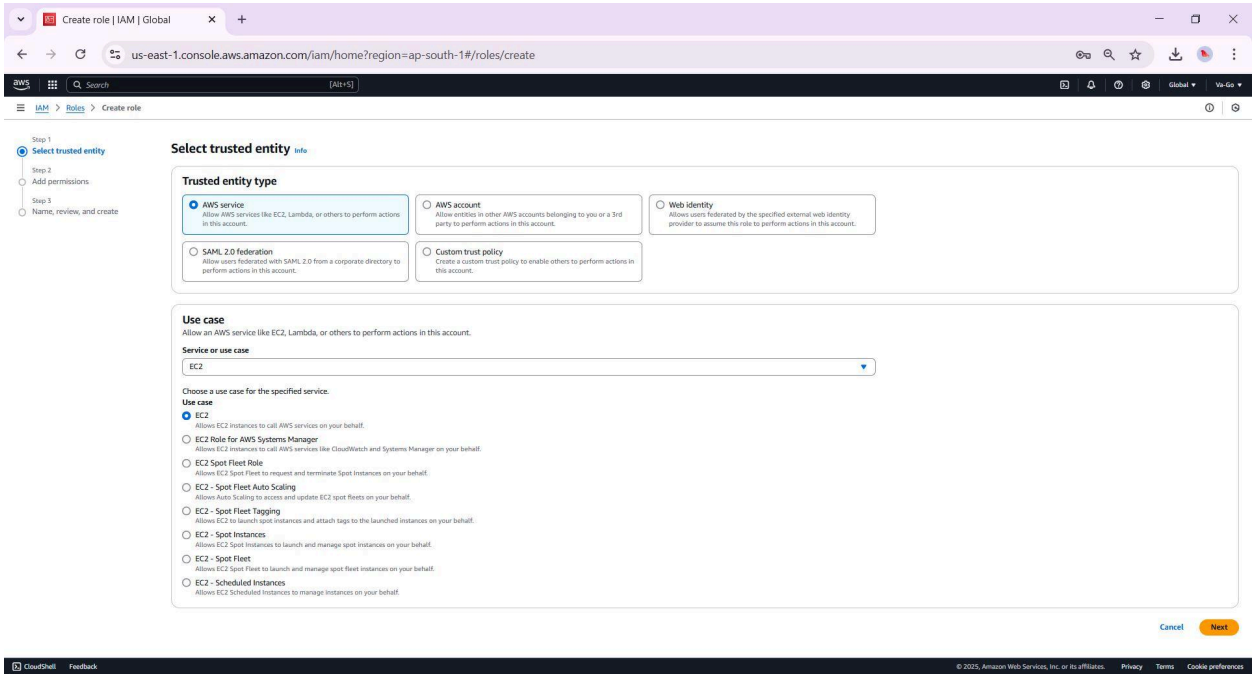

Dev | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Dev?section=permissions
IAM > Users > Dev
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Policy devuser_policy created.
Dev Info
Delete
Summary
ARN
arn:aws:iam::183295416764:user/Dev
Console access
Enabled without MFA
Access key 1
Create access key
Created
February 21, 2025, 07:15 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups (1)
Tags
Security credentials
Last Accessed
Permissions policies (3)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Search
Filter by Type
All types
Policy name
Type
Attached via
CreateAccessKeyForOwnGroup
Customer managed
Group Intellipaat
devuser_policy
Customer inline
Inline
LaunchAndConnectEC2
Customer managed
Group Intellipaat
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
No requests to generate a policy in the past 7 days.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

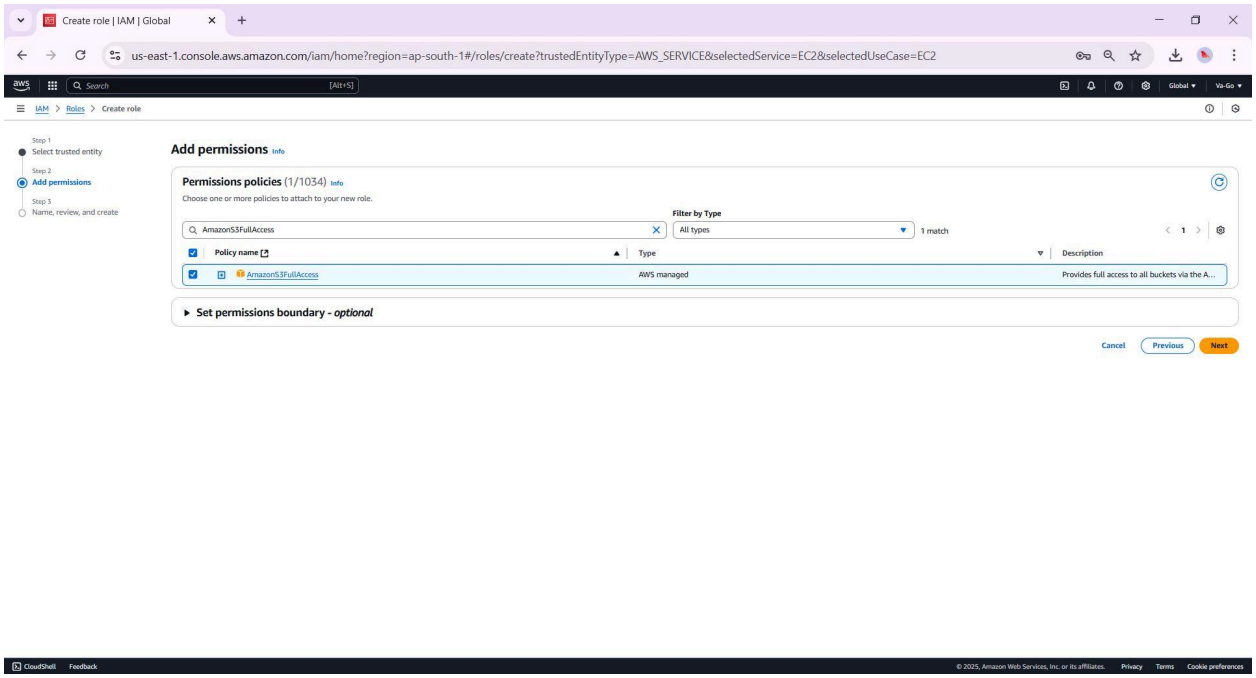

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Ops/createPolicy?step=addPermissions
IAM > Users > Ops > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
S3
Allow
1 Action
Specify what actions can be performed on specific resources in S3.
Actions allowed
Specify actions from the service to be allowed.
Write
PutObject
Resources
Specified resource ARNs for these actions.
arn:aws:s3:::*/*
Request conditions - optional
Actions on resources are allowed or denied only when these conditions are met.
Add more permissions
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

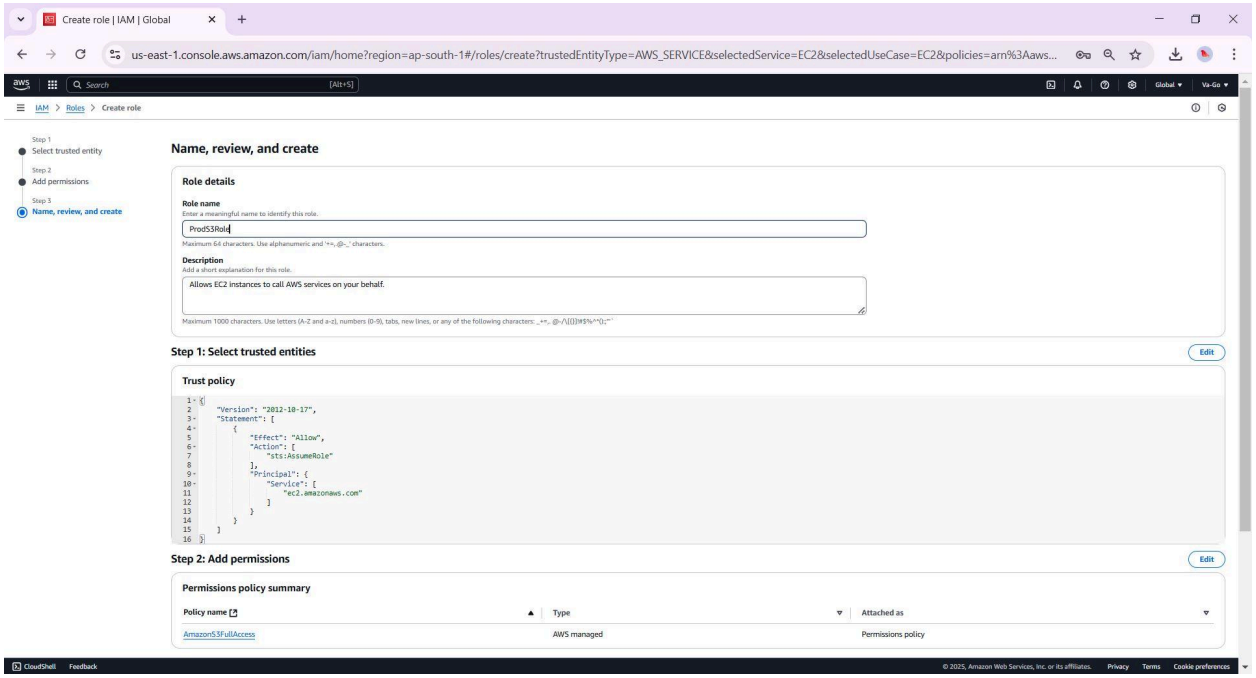

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Ops/createPolicy?step=addPermissions
IAM > Users > Ops > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "s3:PutObject",
"Resource": "arn:aws:s3:::*/*"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
+ Add new statement
JSON Ln 10, Col 1
1937 of 2048 characters remaining
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

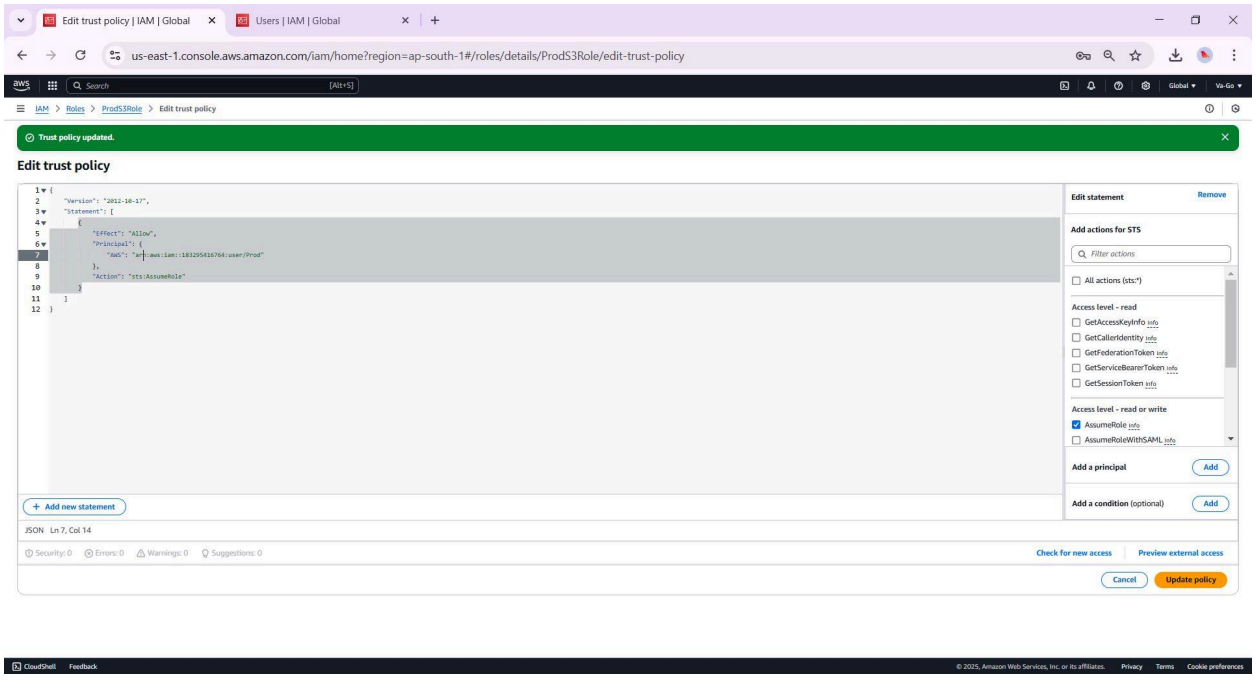

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Ops/createPolicy?step=addPermissions
IAM > Users > Ops > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Ops-use-policy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 437 services)
Show remaining 436 services
Service
Access level
Resource
Request condition
S3
Limited: Write
BucketName| string like |All, ObjectPath| string like |All
None
Cancel
Previous
Create policy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

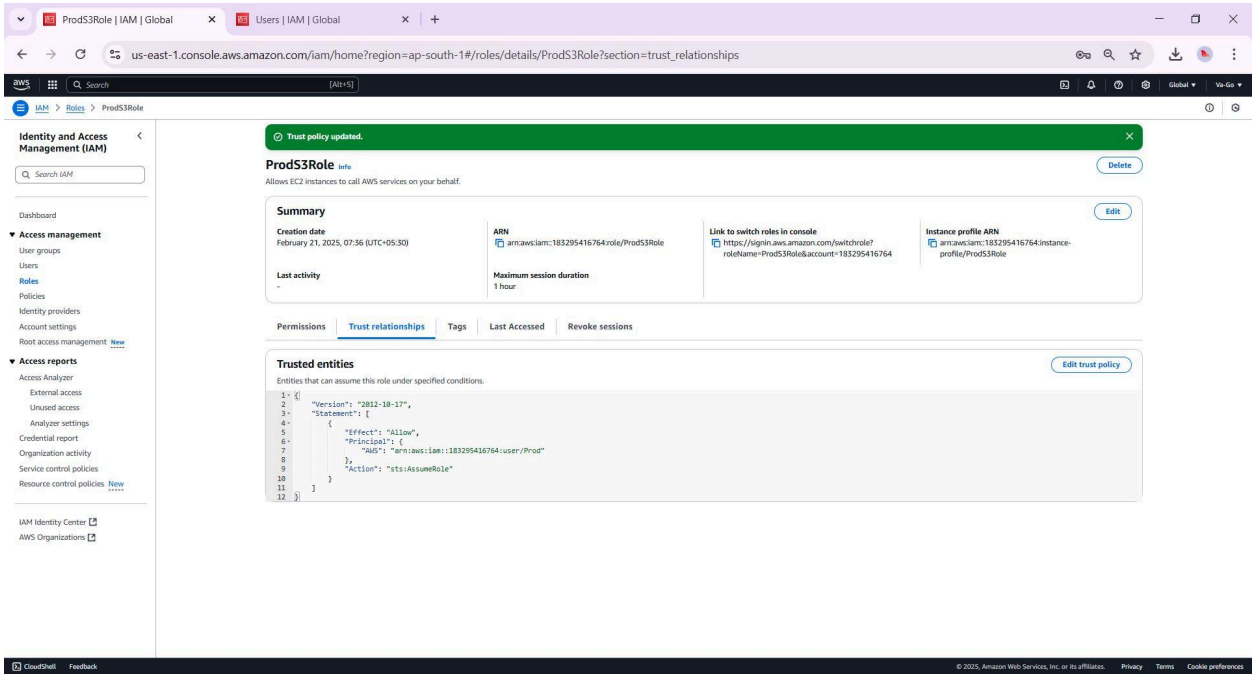

Ops | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Ops?section=permissions
IAM > Users > Ops
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Policy Ops-use-policy created.
Ops Info
Delete
Summary
ARN
arn:aws:iam::183295416764:user/Ops
Console access
Enabled without MFA
Access key 1
Create access key
Created
February 21, 2025, 07:17 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups (1)
Tags
Security credentials
Last Accessed
Permissions policies (3)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Search
Filter by Type
All types
Policy name
Type
Attached via
CreateAccessKeyForOwnGroup
Customer managed
Group Intellipaat
LaunchAndConnectEC2
Customer managed
Group Intellipaat
Ops-use-policy
Customer inline
Inline
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
No requests to generate a policy in the past 7 days.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

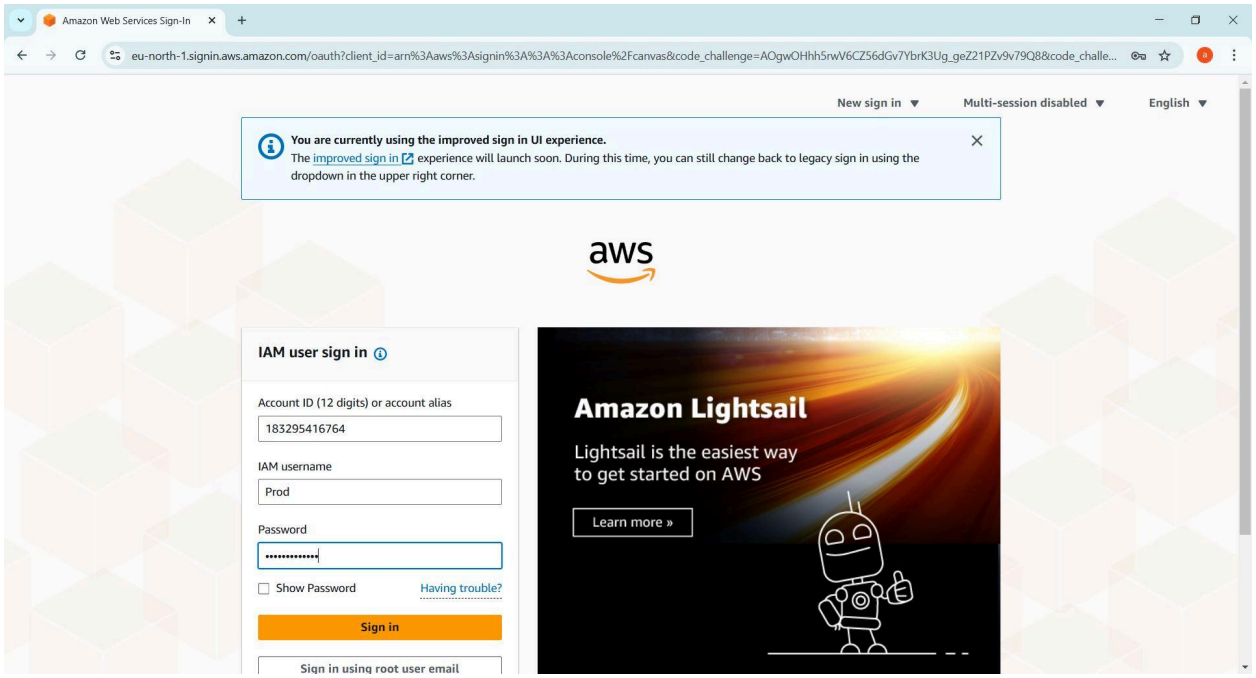

Create role | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, 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.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
EC2
Choose a use case for the specified service.
Use case
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

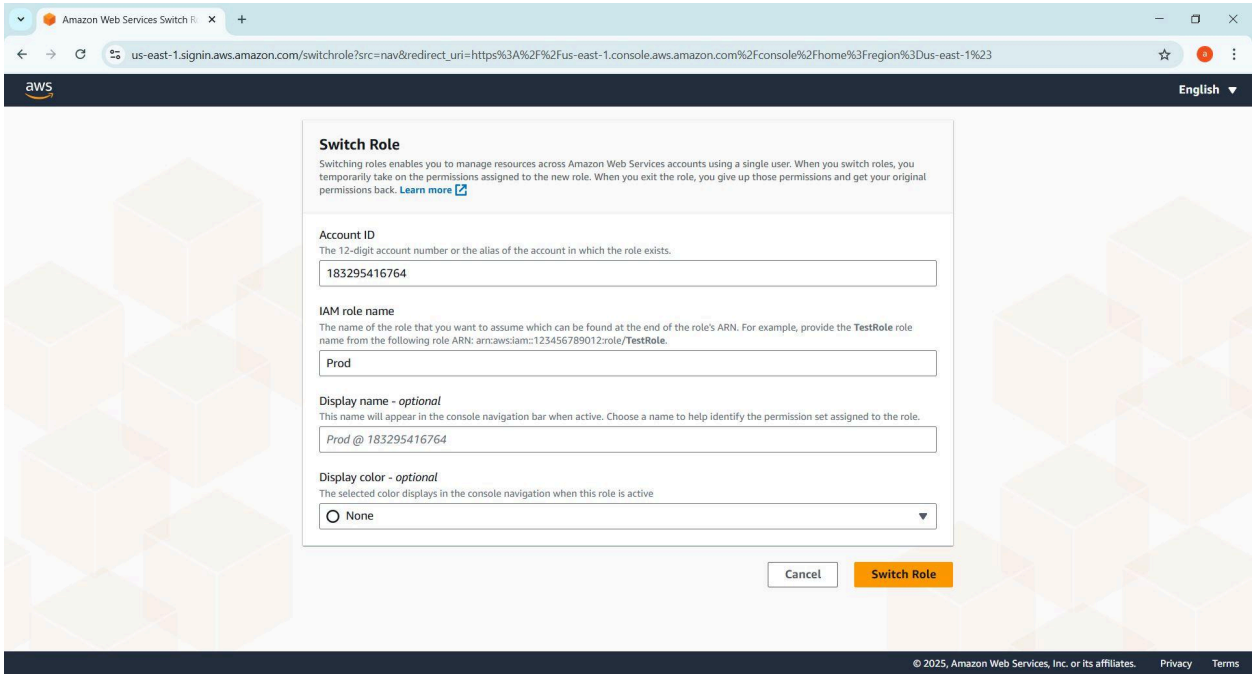

Create role | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&selectedUseCase=EC2
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/1034) Info
Choose one or more policies to attach to your new role.
Filter by Type
AmazonS3FullAccess
All types
1 match
Policy name
Type
Description
AmazonS3FullAccess
AWS managed
Provides full access to all buckets via the A...
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

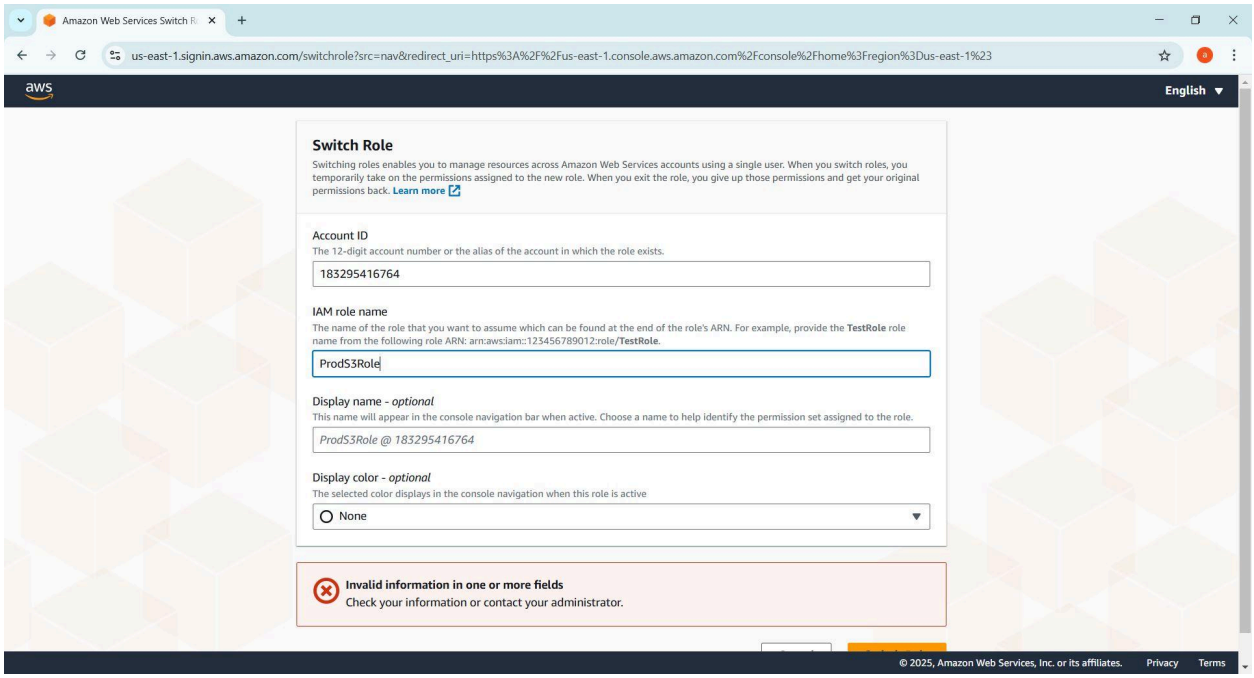

Create role | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&selectedUseCase=EC2&policies=arn%3Aaws...
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
ProdS3Role
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, .@-/\[{}]!#$%^*();:"'
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"ec2.amazonaws.com"
]
}
}
]
}
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AmazonS3FullAccess
AWS managed
Permissions policy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

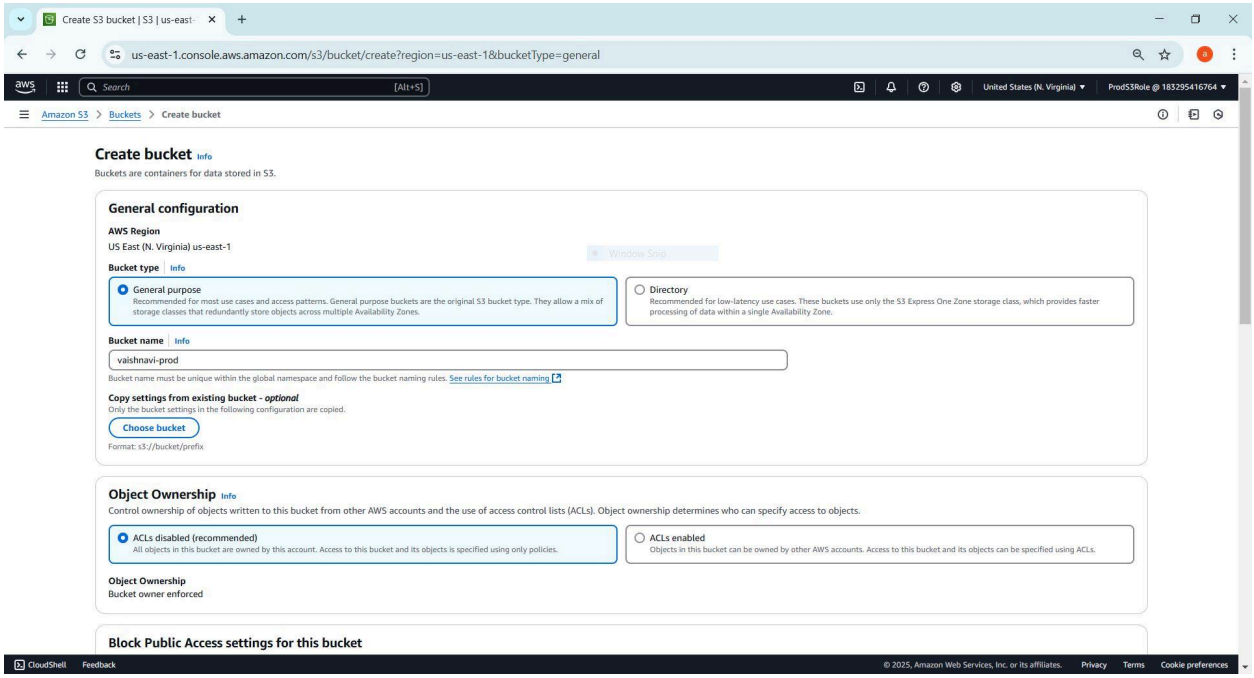

Edit trust policy | IAM | Global
Users | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/ProdS3Role/edit-trust-policy
IAM > Roles > ProdS3Role > Edit trust policy
Trust policy updated.
Edit trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::183295416764:user/Prod"
},
"Action": "sts:AssumeRole"
}
]
}
Edit statement
Remove
Add actions for STS
Filter actions
All actions (sts:*)
Access level - read
GetAccessKeyInfo
GetCallerIdentity
GetFederationToken
GetServiceBearerToken
GetSessionToken
Access level - read or write
AssumeRole
AssumeRoleWithSAML
Add a principal
Add
Add a condition (optional)
Add
Add new statement
JSON Ln 7, Col 14
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Check for new access
Preview external access
Cancel
Update policy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

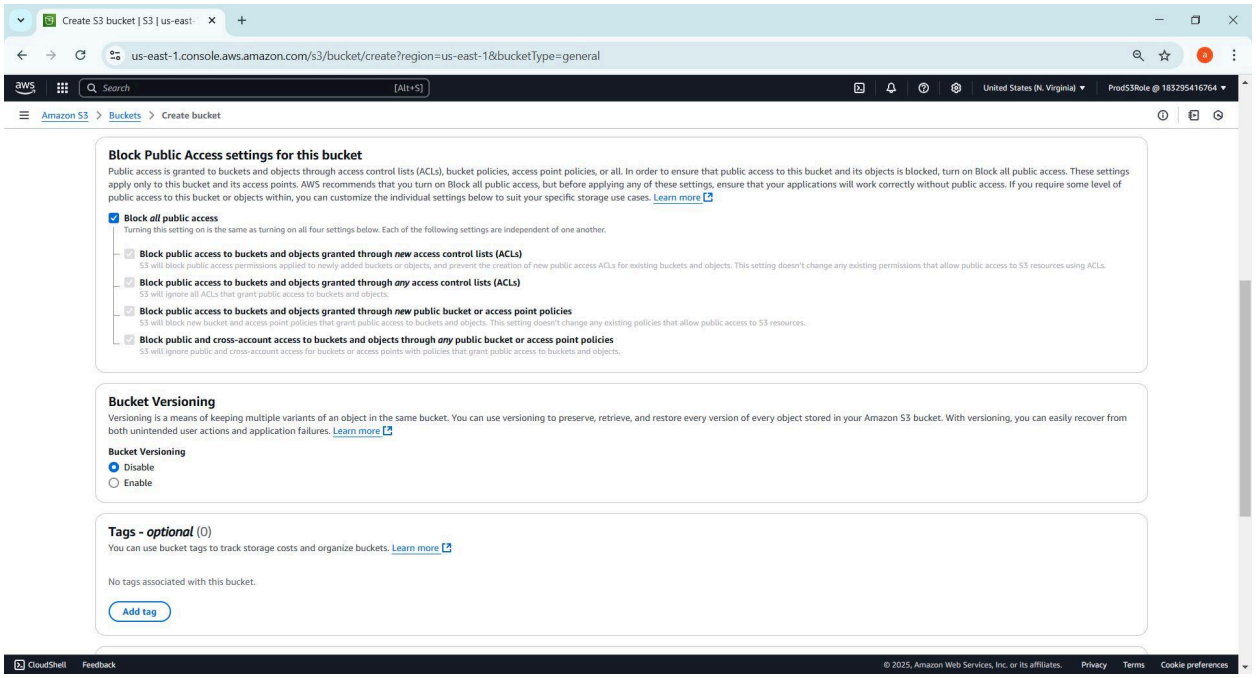

ProdS3Role | IAM | Global
Users | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/ProdS3Role?section=trust_relationships
IAM > Roles > ProdS3Role
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Trust policy updated.
ProdS3Role Info
Allows EC2 instances to call AWS services on your behalf.
Delete
Summary
Edit
Creation date
February 21, 2025, 07:36 (UTC+05:30)
ARN
arn:aws:iam::183295416764:role/ProdS3Role
Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=ProdS3Role&account=183295416764
Instance profile ARN
arn:aws:iam::183295416764:instance-profile/ProdS3Role
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags
Last Accessed
Revoke sessions
Trusted entities
Edit trust policy
Entities that can assume this role under specified conditions.
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::183295416764:user/Prod"
},
"Action": "sts:AssumeRole"
}
]
}
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

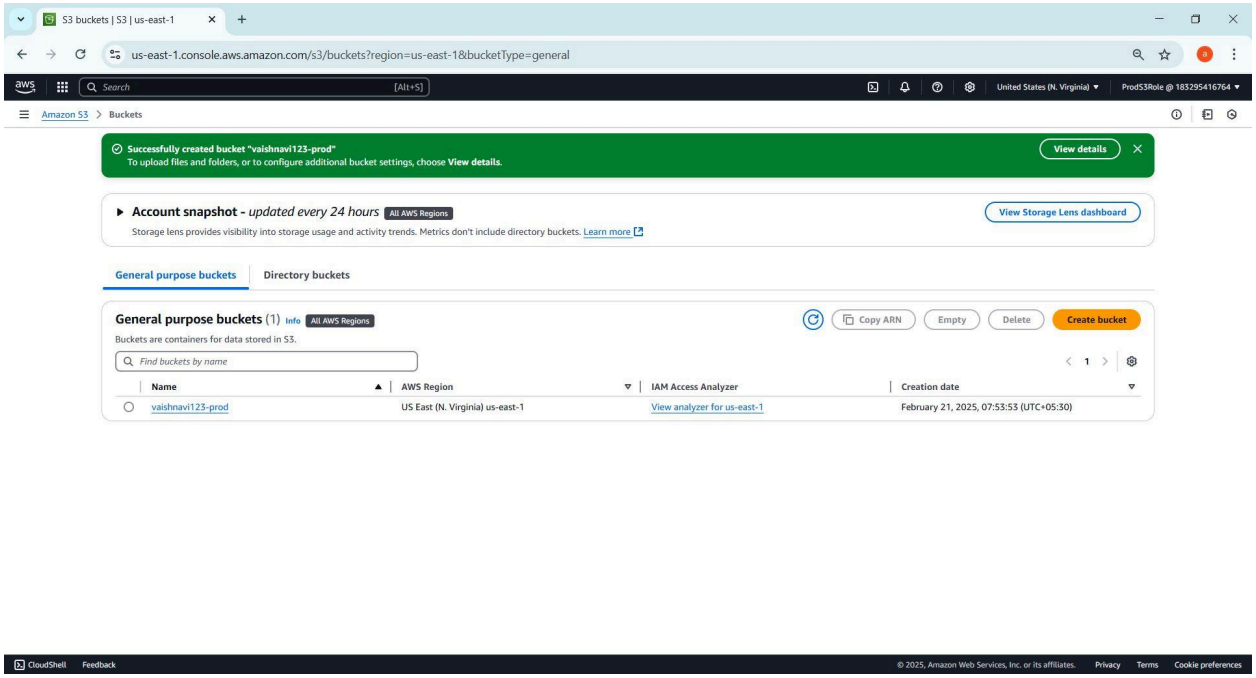

Amazon Web Services Sign-In
eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=AOgwOHhh5rwV6CZ56dGv7YbrK3Ug_geZ21PZv9v79Q8&code_challe...
New sign in
Multi-session disabled
English
You are currently using the improved sign in UI experience.
The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.
aws
IAM user sign in
Account ID (12 digits) or account alias
183295416764
IAM username
Prod
Password
Show Password
Having trouble?
Sign in
Sign in using root user email
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

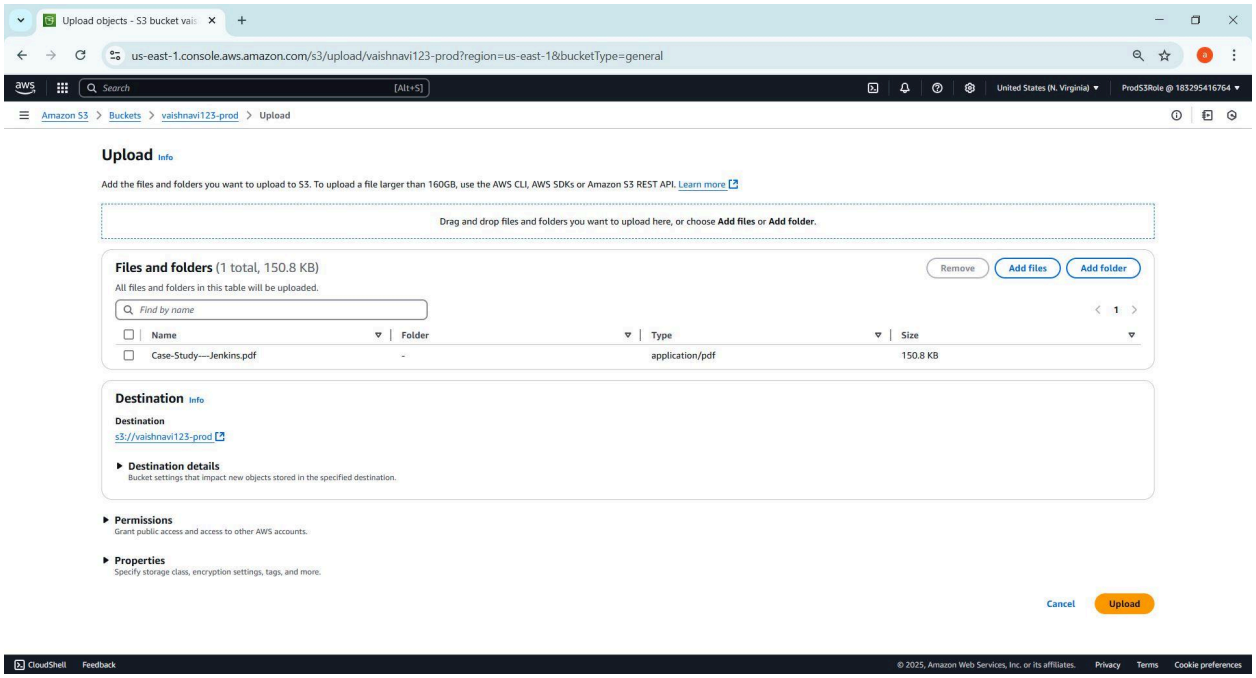

Amazon Web Services Switch R
us-east-1.signin.aws.amazon.com/switchrole?src=nav&redirect_uri=https%3A%2F%2Fus-east-1.console.aws.amazon.com%2Fconsole%2Fhome%3Fregion%3Dus-east-1%23
aws
English
Switch Role
Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. Learn more
Account ID
The 12-digit account number or the alias of the account in which the role exists.
183295416764
IAM role name
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the TestRole role name from the following role ARN: arn:aws:iam::123456789012:role/TestRole.
Prod
Display name - optional
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.
Prod @ 183295416764
Display color - optional
The selected color displays in the console navigation when this role is active
None
Cancel
Switch Role
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms

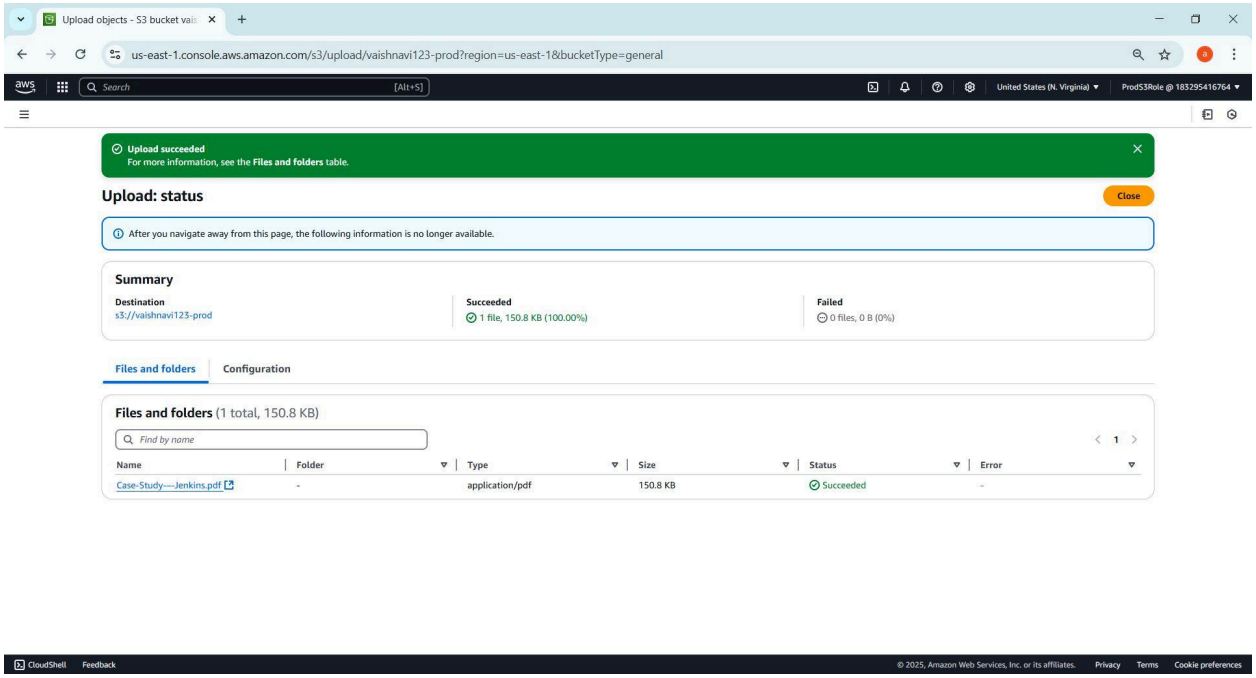

Amazon Web Services Switch R
us-east-1.signin.aws.amazon.com/switchrole?src=nav&redirect_uri=https%3A%2F%2Fus-east-1.console.aws.amazon.com%2Fconsole%2Fhome%3Fregion%3Dus-east-1%23
aws
English
Switch Role
Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. Learn more
Account ID
The 12-digit account number or the alias of the account in which the role exists.
183295416764
IAM role name
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the TestRole role name from the following role ARN: arn:aws:iam::123456789012:role/TestRole.
ProdS3Role
Display name - optional
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.
ProdS3Role @ 183295416764
Display color - optional
The selected color displays in the console navigation when this role is active
None
Invalid information in one or more fields
Check your information or contact your administrator.
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms

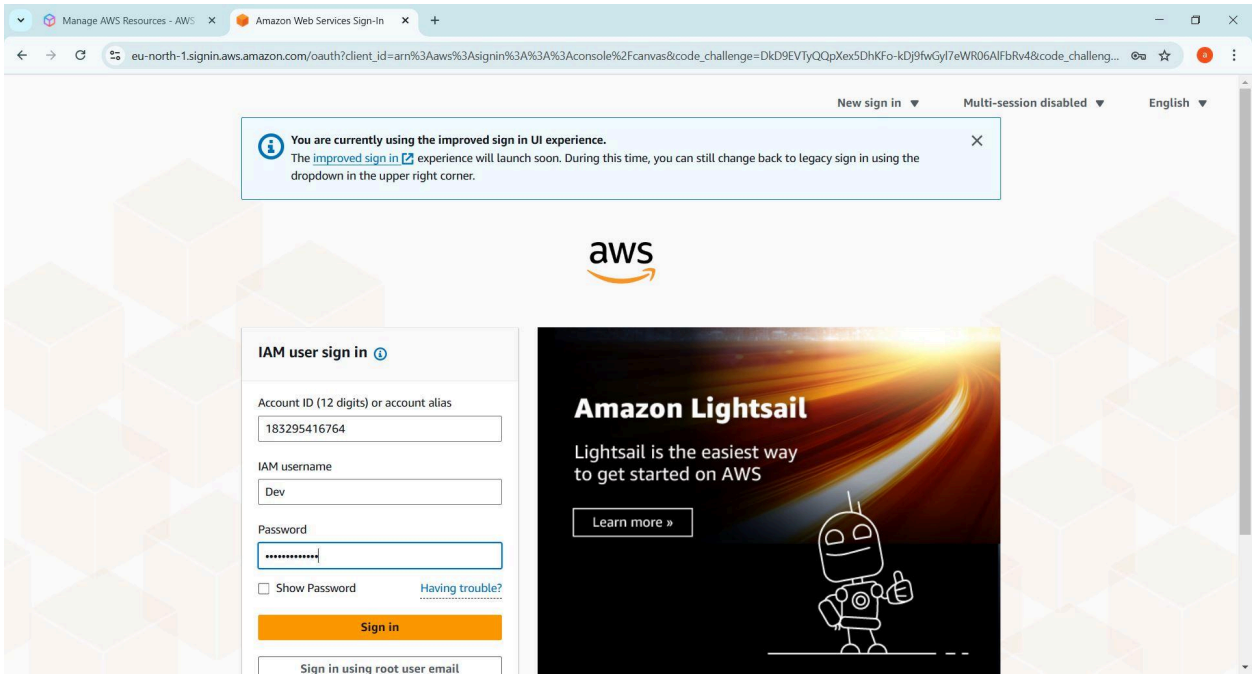

Create S3 bucket | S3 | us-east-
us-east-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Search
[Alt+S]
United States (N. Virginia)
ProdS3Role @ 183295416764
Amazon S3
Buckets
Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.
Bucket name Info
vaishnavi-prod
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced
Block Public Access settings for this bucket
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

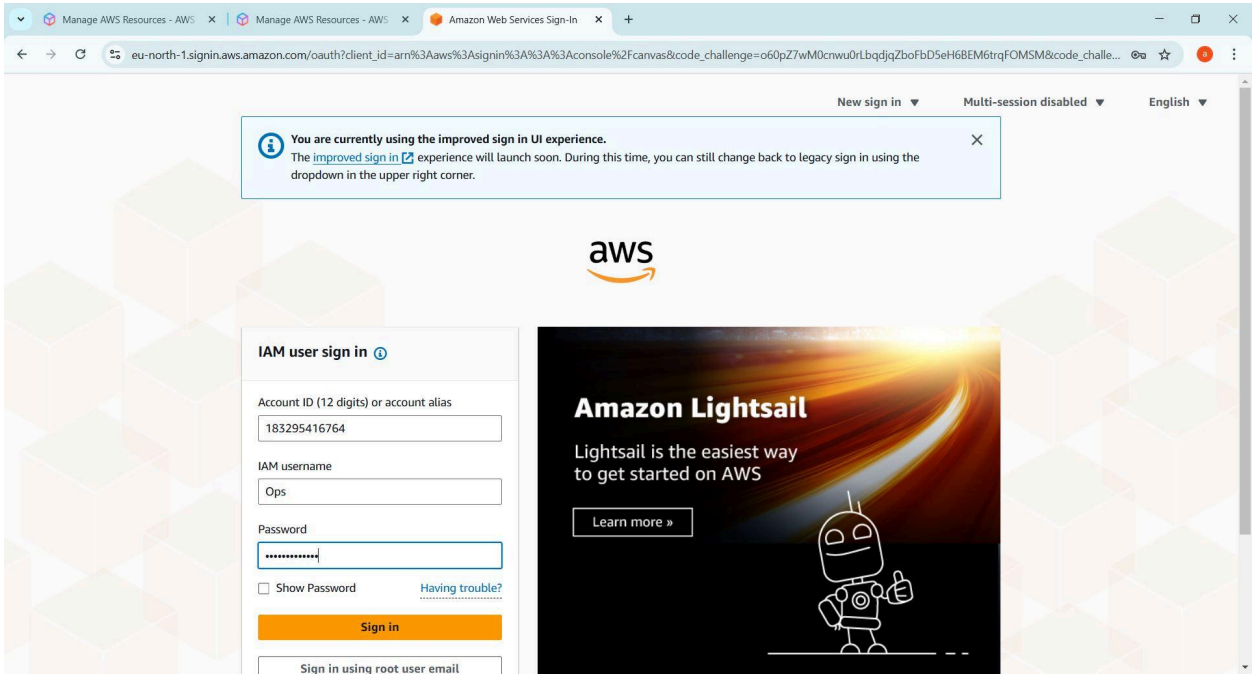

Create S3 bucket | S3 | us-east-
us-east-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Search [Alt+S]
United States (N. Virginia)
ProdS3Role @ 183295416764
Amazon S3 > Buckets > Create bucket
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

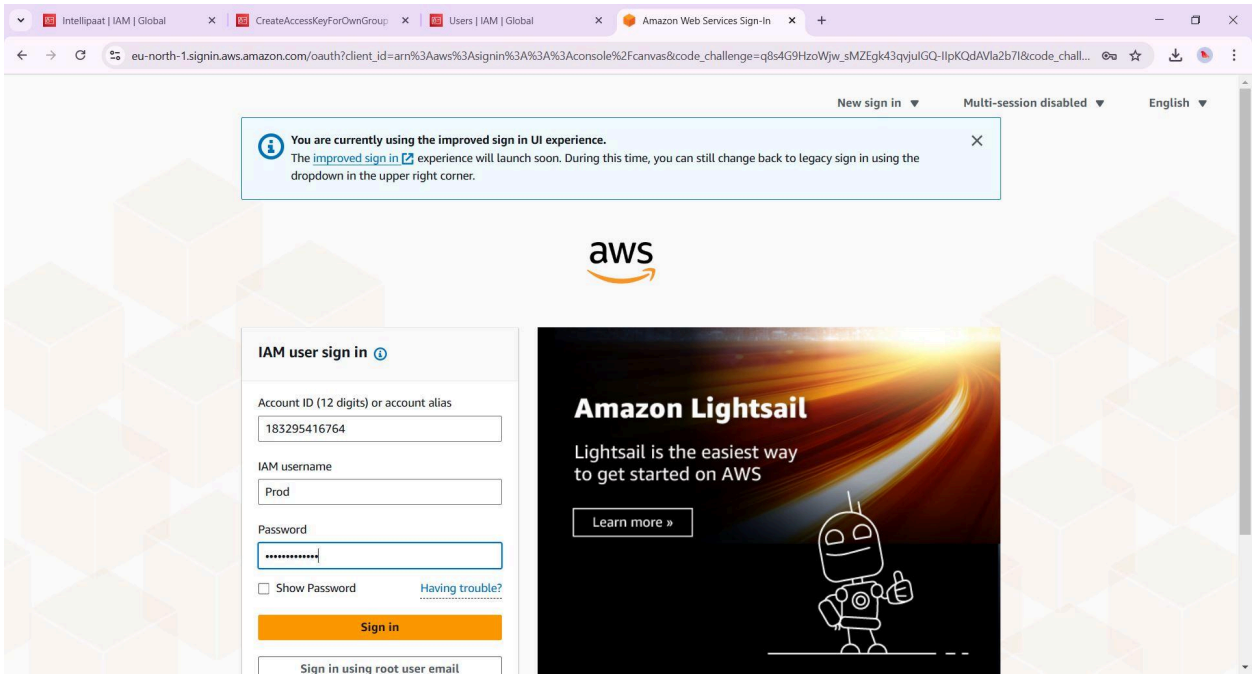

S3 buckets | S3 | us-east-1
us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general
Search [Alt+S]
United States (N. Virginia)
ProdS3Role @ 183295416764
Amazon S3 > Buckets
Successfully created bucket "vaishnavi123-prod"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. 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
vaishnavi123-prod
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 21, 2025, 07:53:53 (UTC+05:30)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

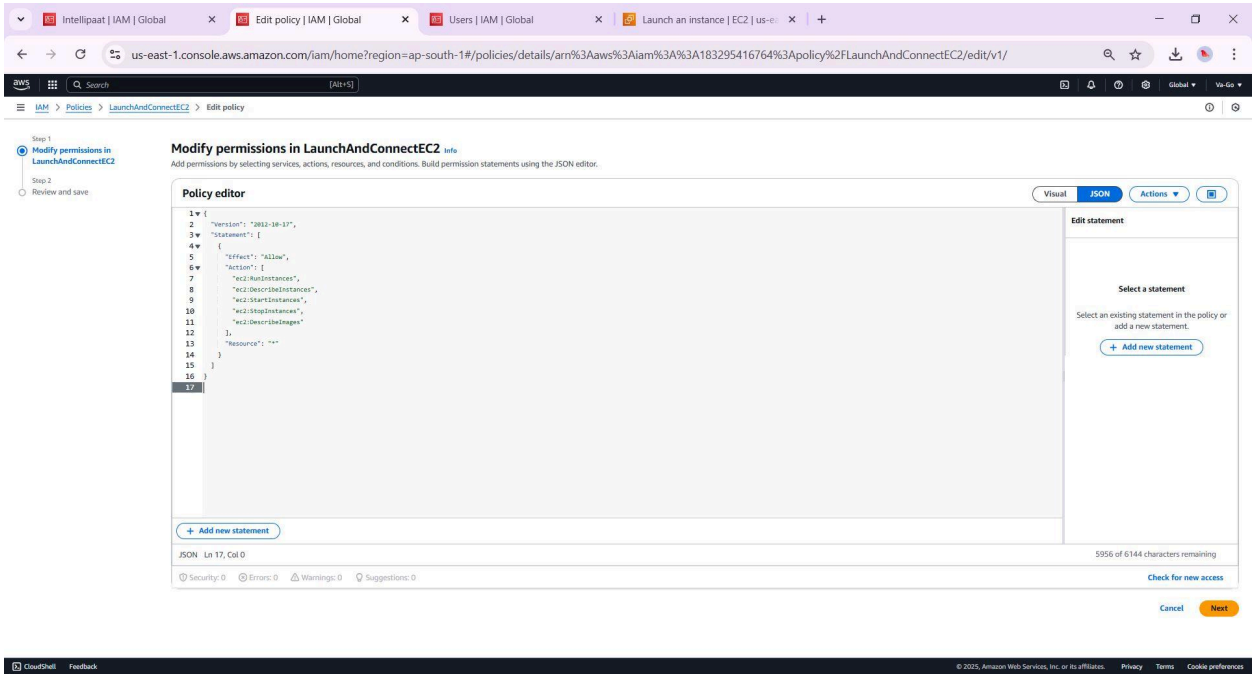

Upload objects - S3 bucket vai
us-east-1.console.aws.amazon.com/s3/upload/vaishnavi123-prod?region=us-east-1&bucketType=general
Search
[Alt+S]
United States (N. Virginia)
ProdS3Role @ 183295416764
Amazon S3 > Buckets > vaishnavi123-prod > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 total, 150.8 KB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
1
Name
Folder
Type
Size
Case-Study---Jenkins.pdf
-
application/pdf
150.8 KB
Destination Info
Destination
s3://vaishnavi123-prod
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
Cancel
Upload
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

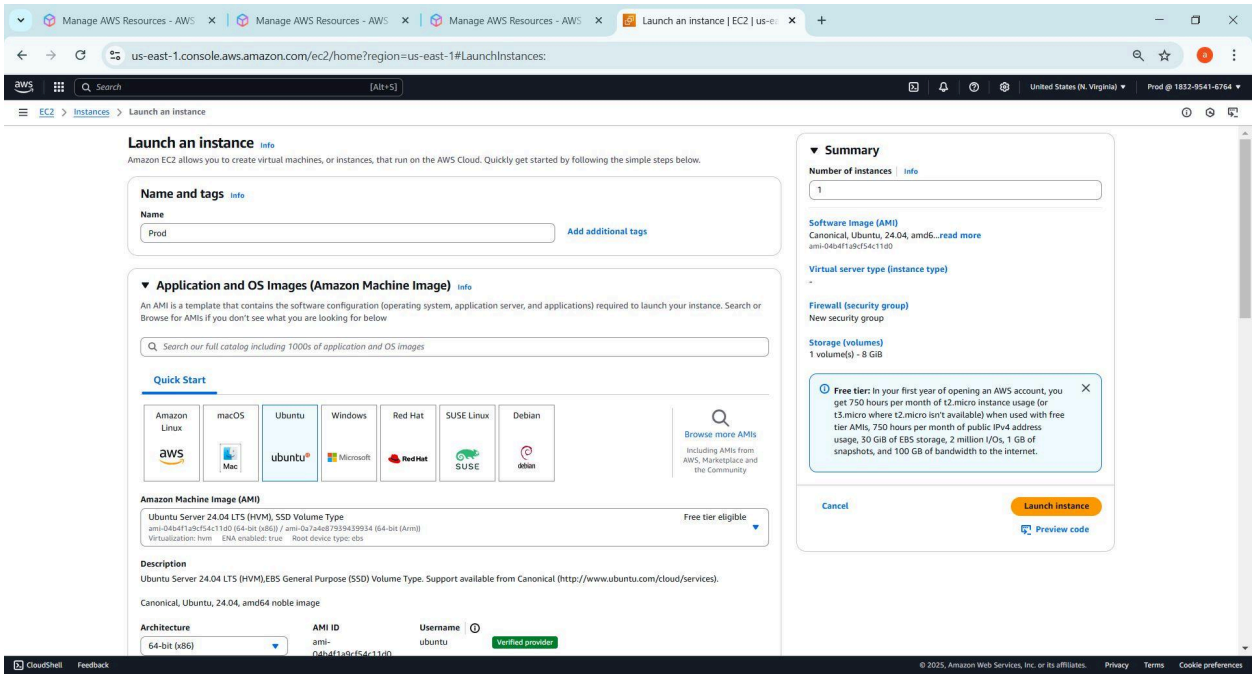

Upload objects - S3 bucket vai
us-east-1.console.aws.amazon.com/s3/upload/vaishnavi123-prod?region=us-east-1&bucketType=general
Search
[Alt+S]
United States (N. Virginia)
ProdS3Role @ 183295416764
Upload succeeded
For more information, see the Files and folders table.
Upload: status
Close
After you navigate away from this page, the following information is no longer available.
Summary
Destination
s3://vaishnavi123-prod
Succeeded
1 file, 150.8 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 150.8 KB)
Find by name
1
Name
Folder
Type
Size
Status
Error
Case-Study---Jenkins.pdf
-
application/pdf
150.8 KB
Succeeded
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

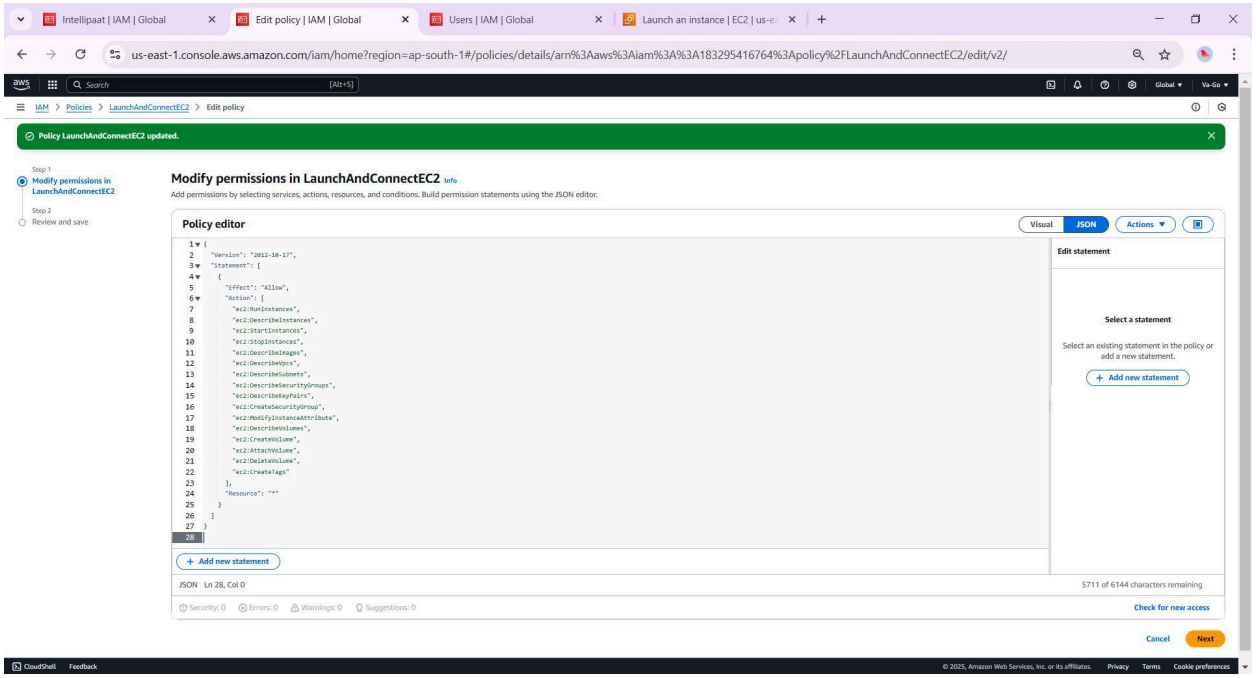

Manage AWS Resources - AWS
Amazon Web Services Sign-In
eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=DkD9EVTyQQpXex5DhKFo-kDj9fwGyI7eWR06AlFbRv4&code_challeng...
New sign in
Multi-session disabled
English
You are currently using the improved sign in UI experience.
The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.
aws
IAM user sign in
Account ID (12 digits) or account alias
183295416764
IAM username
Dev
Password
Show Password
Having trouble?
Sign in
Sign in using root user email
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »


Manage AWS Resources - AWS
Manage AWS Resources - AWS
Amazon Web Services Sign-In
eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=o60pZ7wM0cnwu0rLbqdjqZboFbD5eH6BEM6trqFOMSM&code_challe...
New sign in
Multi-session disabled
English
You are currently using the improved sign in UI experience.
The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.
aws
IAM user sign in
Account ID (12 digits) or account alias
183295416764
IAM username
Ops
Password
Show Password
Having trouble?
Sign in
Sign in using root user email
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »


Intellipaat | IAM | Global
CreateAccessKeyForOwnGroup
Users | IAM | Global
Amazon Web Services Sign-In
eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=q8s4G9HzoWjw_sMZEgk43qvjuIGQ-IIpKQdAVla2b7I&code_chall...
New sign in
Multi-session disabled
English
You are currently using the improved sign in UI experience.
The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.
aws
IAM user sign in
Account ID (12 digits) or account alias
183295416764
IAM username
Prod
Password
Show Password
Having trouble?
Sign in
Sign in using root user email
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »


Intellipaat | IAM | Global
Edit policy | IAM | Global
Users | IAM | Global
Launch an instance | EC2 | us-e
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A183295416764%3Apolicy%2FLaunchAndConnectEC2/edit/v1/
IAM > Policies > LaunchAndConnectEC2 > Edit policy
Step 1
Modify permissions in LaunchAndConnectEC2
Step 2
Review and save
Modify permissions in LaunchAndConnectEC2 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": [
{
"Effect": "Allow",
"Action": [
"ec2:RunInstances",
"ec2:DescribeInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:DescribeImages"
],
"Resource": "*"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
+ Add new statement
JSON Ln 17, Col 0
5956 of 6144 characters remaining
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Check for new access
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Manage AWS Resources - AWS
Launch an instance | EC2 | us-ea
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
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
Prod
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
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
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
Description
Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Canonical, Ubuntu, 24.04, amd64 noble image
Architecture
64-bit (x86)
AMI ID
Username
ubuntu
Verified provider
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
Virtual server type (instance type)
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Intellipaat | IAM | Global
Edit policy | IAM | Global
Users | IAM | Global
Launch an instance | EC2 | us-ea
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%183295416764%3Apolicy%2FLaunchAndConnectEC2/edit/v2/
IAM > Policies > LaunchAndConnectEC2 > Edit policy
Policy LaunchAndConnectEC2 updated.
Step 1
Modify permissions in LaunchAndConnectEC2
Step 2
Review and save
Modify permissions in LaunchAndConnectEC2 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": [
{
"Effect": "Allow",
"Action": [
"ec2:RunInstances",
"ec2:DescribeInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:DescribeImages",
"ec2:DescribeVpcs",
"ec2:DescribeSubnets",
"ec2:DescribeSecurityGroups",
"ec2:DescribeKeyPairs",
"ec2:CreateSecurityGroup",
"ec2:ModifyInstanceAttribute",
"ec2:DescribeVolumes",
"ec2:CreateVolume",
"ec2:AttachVolume",
"ec2:DeleteVolume",
"ec2:CreateTags"
],
"Resource": "*"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement
Add new statement
JSON Ln 28, Col 0
5711 of 6144 characters remaining
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Check for new access
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences