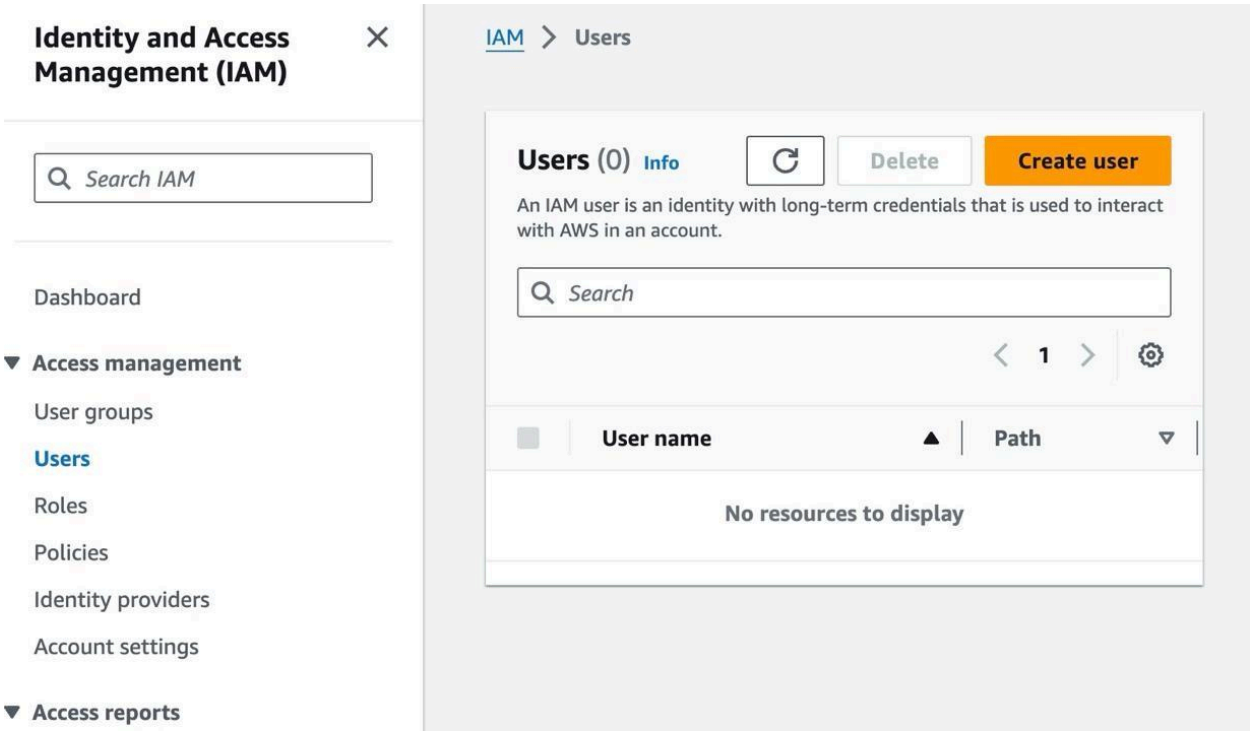
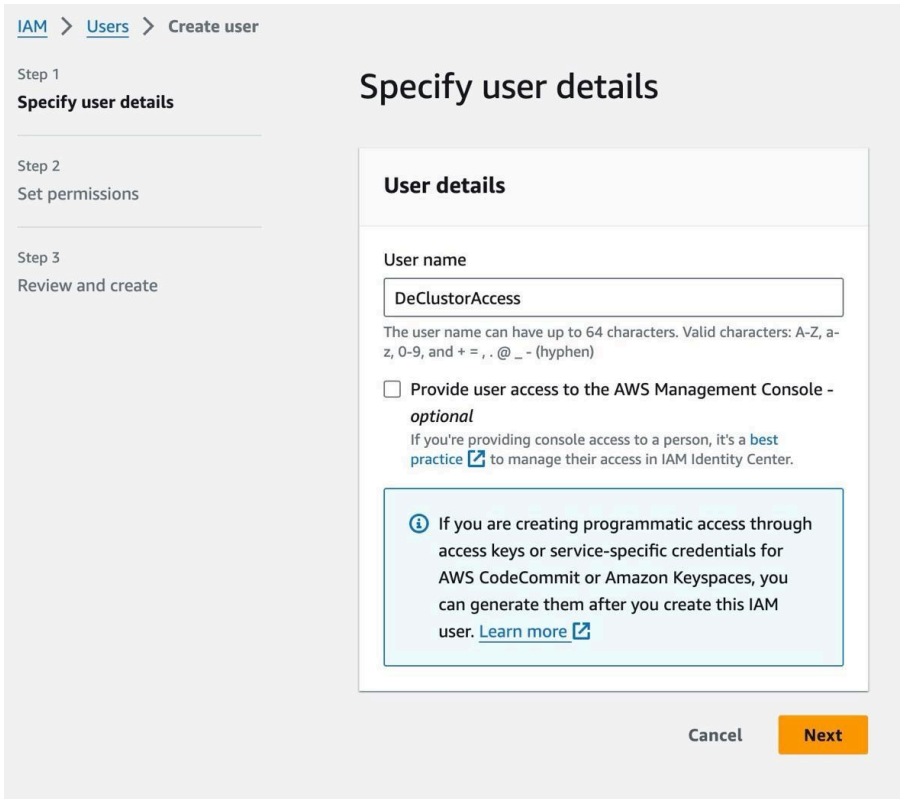
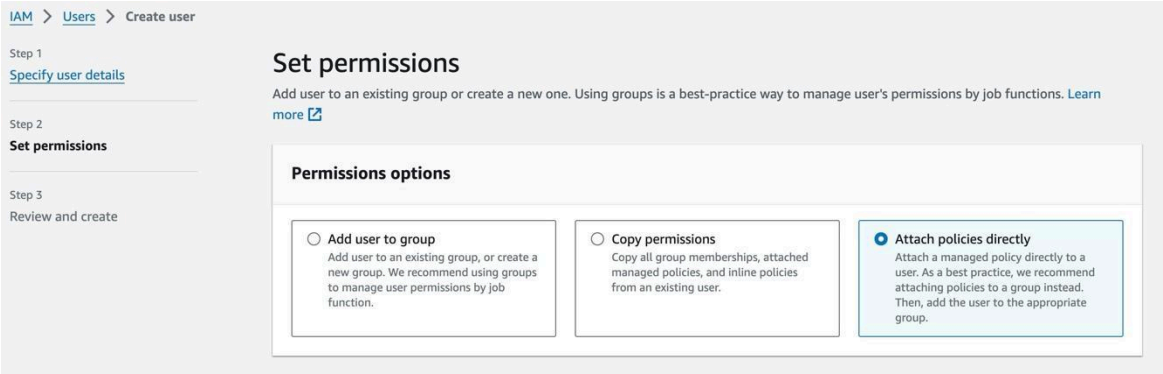
1. **Log in to AWS Management Console, navigate to Identify and Access Management(IAM), and create a user**



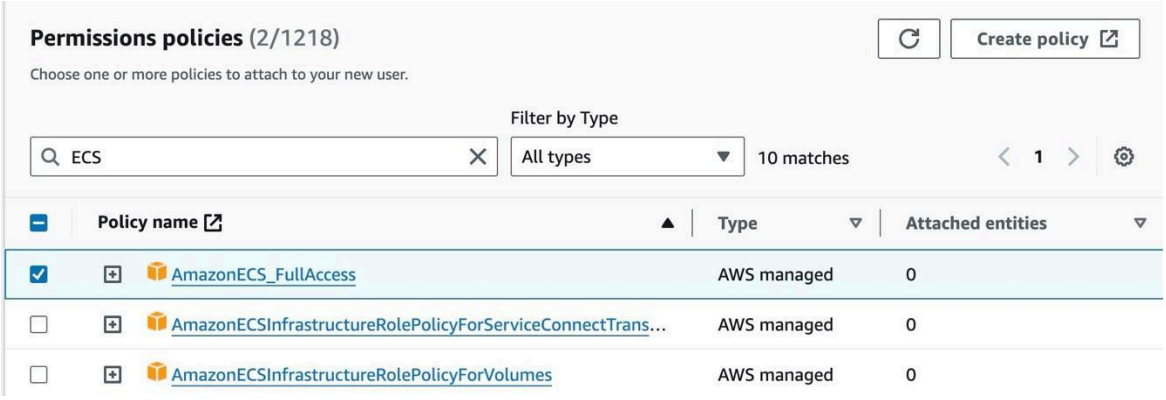
2. **Configure User Details**

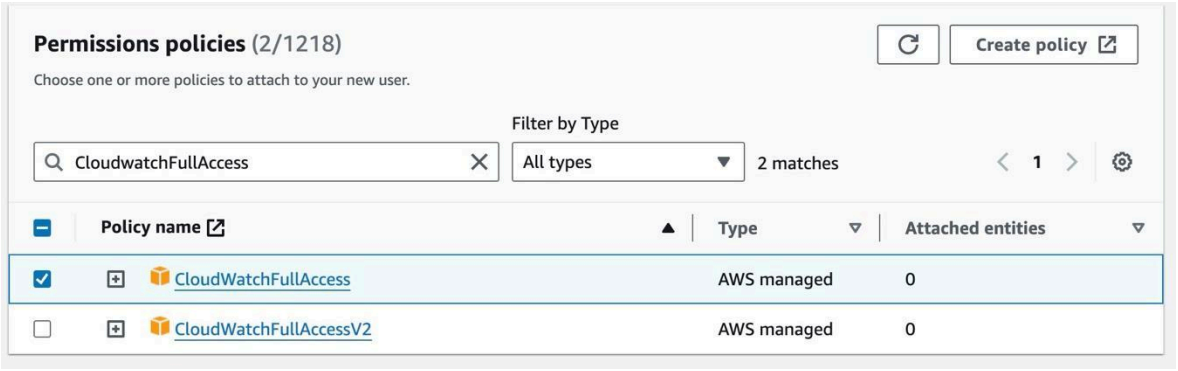


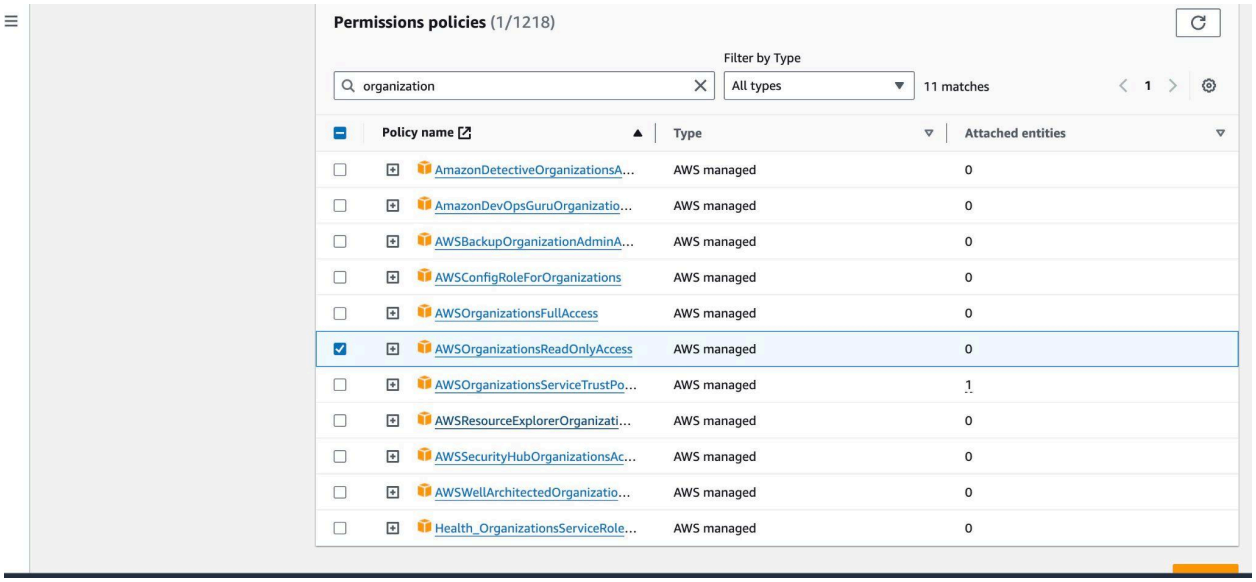
3. Set Permissions



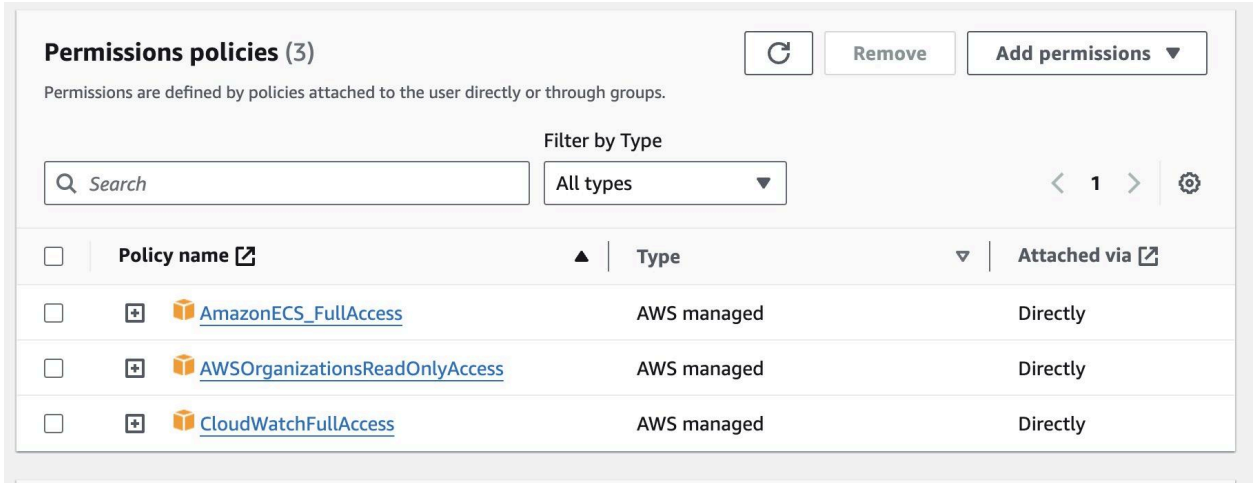
4. Add AmazonECS_FullAccess policy and CloudwatchFullAccess policy



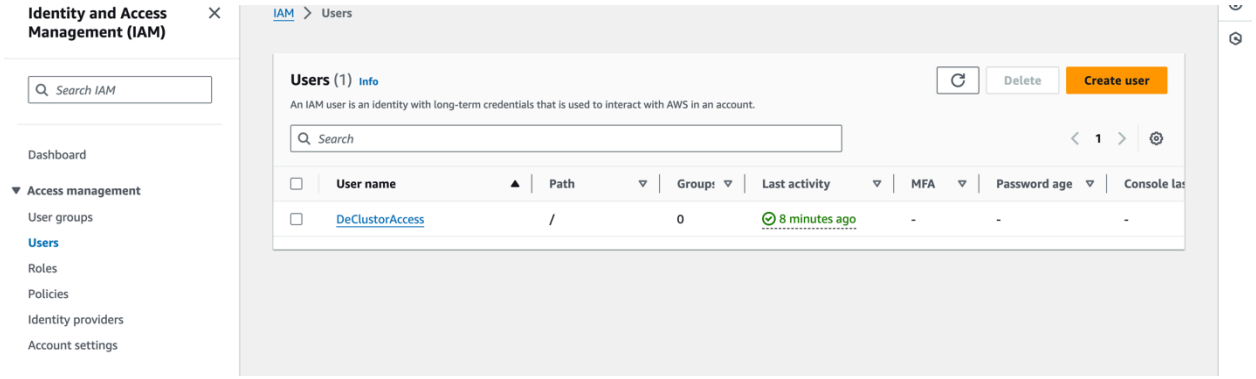




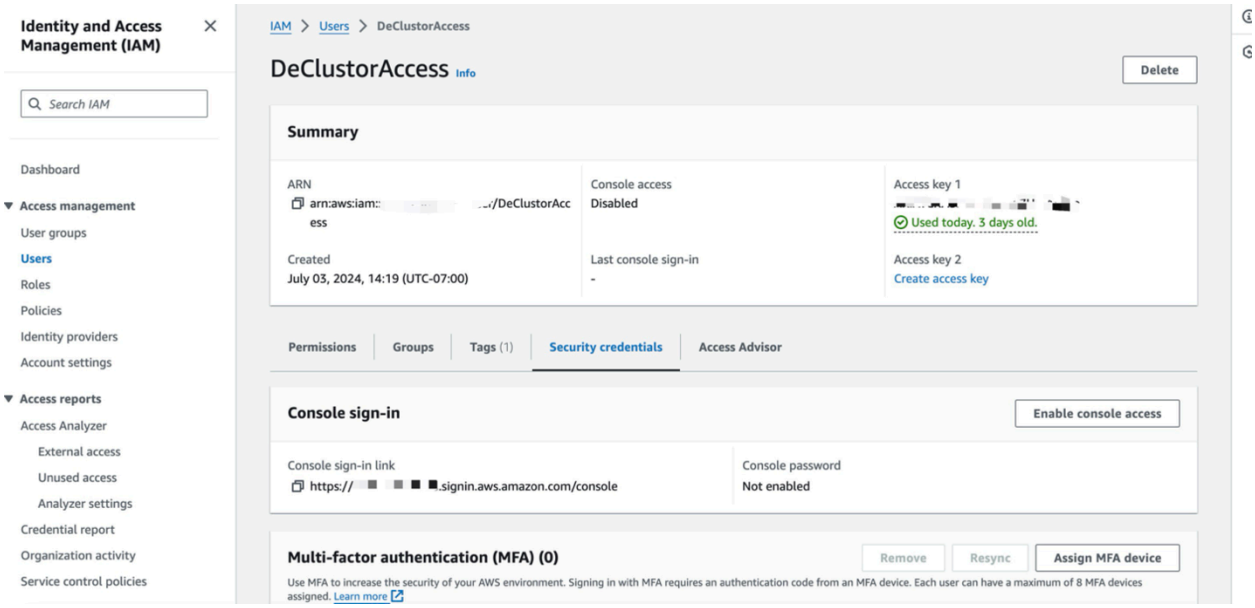
We need these three policies to manage your AWS accounts and get metric data from Cloudwatch

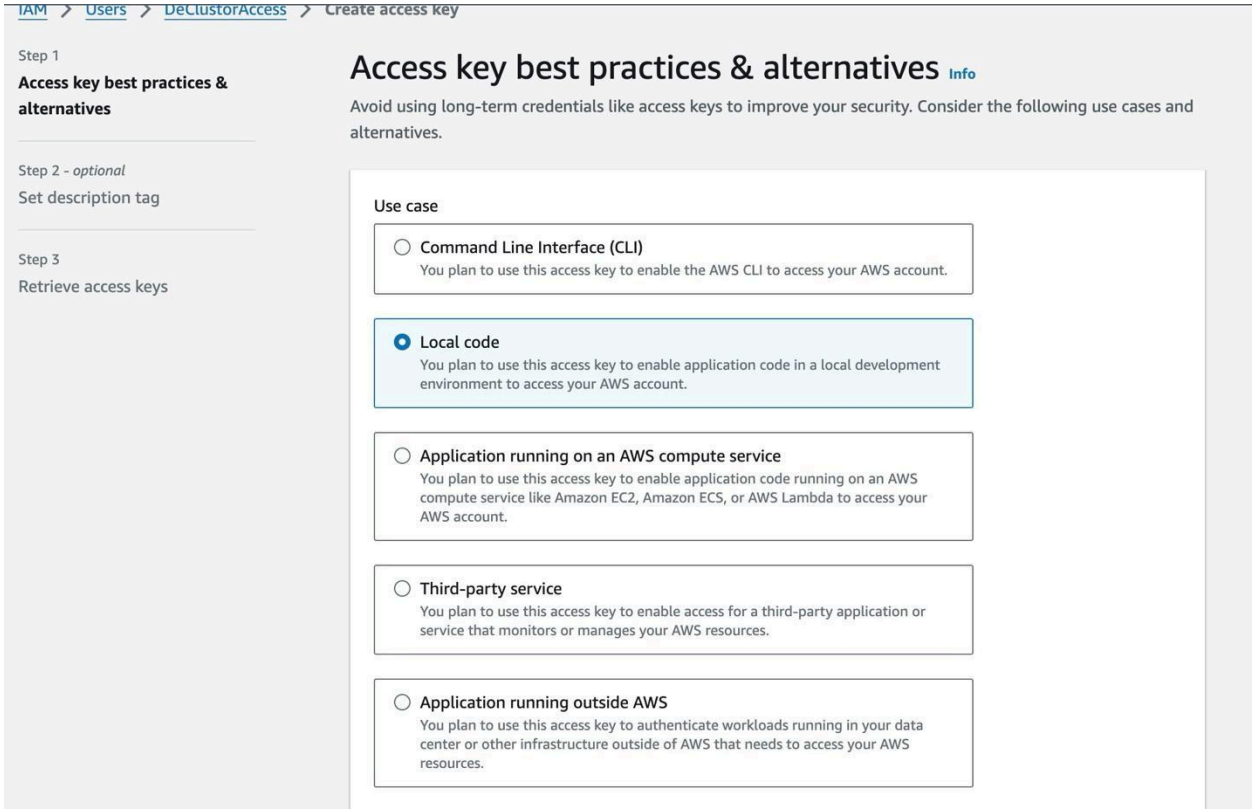


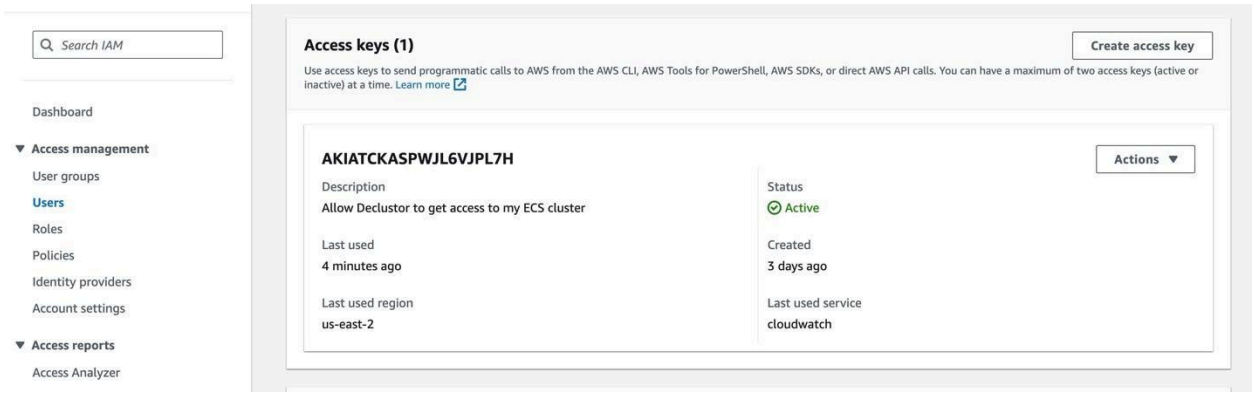
5. **Click on the user you just create**



6. **Create Access key for DeClustorAccess user**


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
IAM > Users > DeClustorAccess
DeClustorAccess Info
Delete
Summary
ARN
arn:aws:iam:: .../DeClustorAccess
Console access
Disabled
Access key 1
Used today. 3 days old.
Created
July 03, 2024, 14:19 (UTC-07:00)
Last console sign-in
-
Access key 2
Create access key
Permissions
Groups
Tags (1)
Security credentials
Access Advisor
Console sign-in
Enable console access
Console sign-in link
https:// .signin.aws.amazon.com/console
Console password
Not enabled
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more


IAM > Users > DeClustorAccess > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Access key best practices & alternatives Info
Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.
Use case
Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.
Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.
Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.


Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
Access keys (1)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
AKIATCKASPWJL6VJPL7H
Actions
Description
Allow Declustor to get access to my ECS cluster
Status
Active
Last used
4 minutes ago
Created
3 days ago
Last used region
us-east-2
Last used service
cloudwatch