

Identity and Access Management (IAM)

- Dashboard
- Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Access reports
- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report

New feature to generate a policy based on CloudTrail events.

AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this role.

Roles > capstoneloTRole

Summary

Delete role

Role ARN	arn:aws:iam::221389831253:role/capstoneloTRole
Role description	This role is created for capstone project. Edit
Instance Profile ARNs	
Path	/
Creation time	2021-09-29 10:02 UTC+0530
Last activity	2021-10-02 11:46 UTC+0530 (Today)
Maximum session duration	1 hour Edit

PermissionsTrust relationshipsTagsAccess AdvisorRevoke sessions

Permissions policies (4 policies applied)

Attach policiesAdd inline policy

Policy name	Policy type	
<div></div> AWSIoTThingsRegistration	AWS managed policy	
<div></div> AWSIoTLogging	AWS managed policy	
<div></div> AmazonDynamoDBFullAccess	AWS managed policy	
<div></div> AWSIoTRuleActions	AWS managed policy	

Permissions boundary (not set)

You need permissions

You do not have the permission required to perform this operation. Ask your administrator to add permissions.

- User: arn:aws:sts::221389831253:assumed-role/vocstartsoft/user1335070=amar141989@gmail.com is not authorized to perform: access-analyzer:ListPolicyGenerations on resource: arn:aws:access-analyzer:us-east-1:221389831253:* with an explicit deny