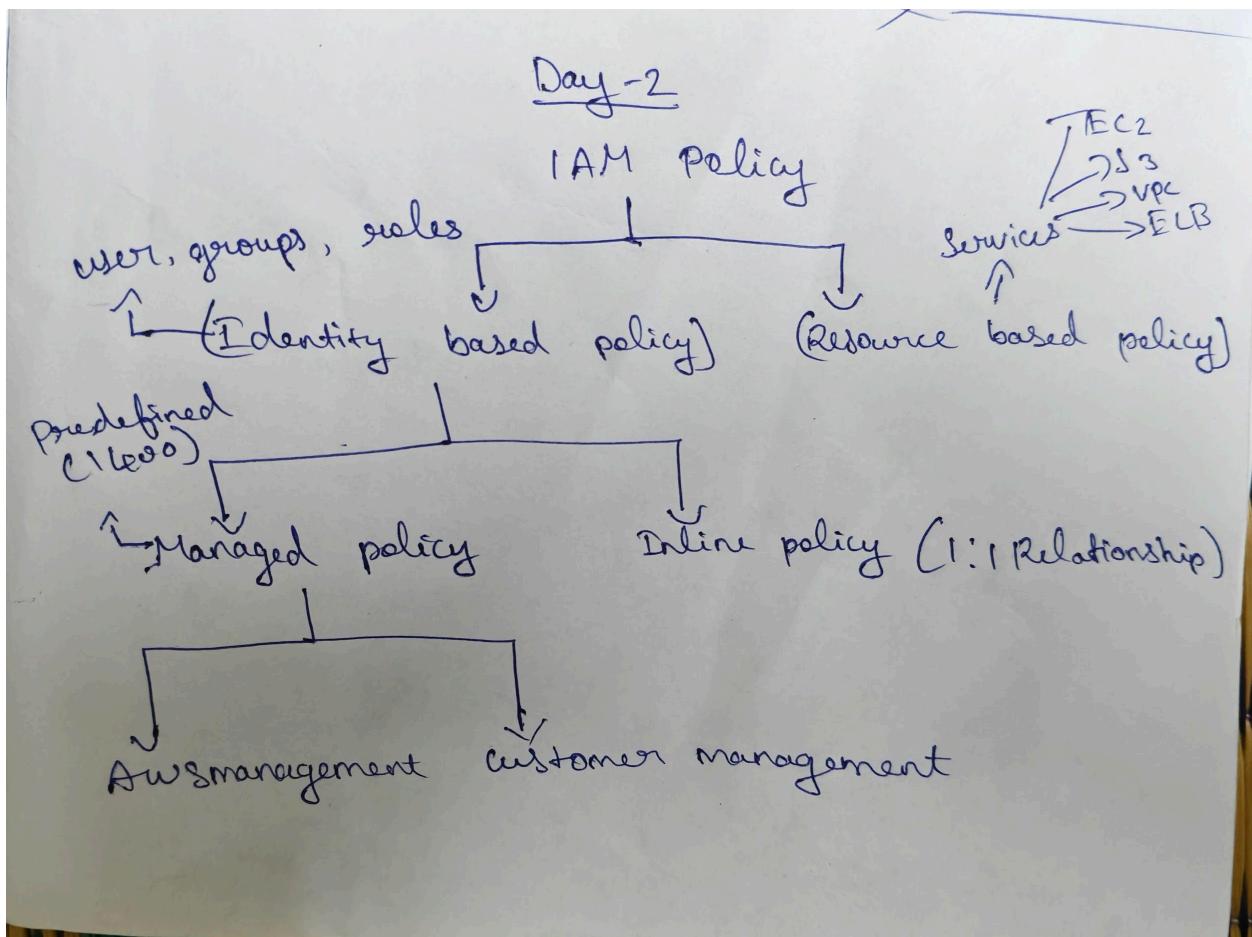
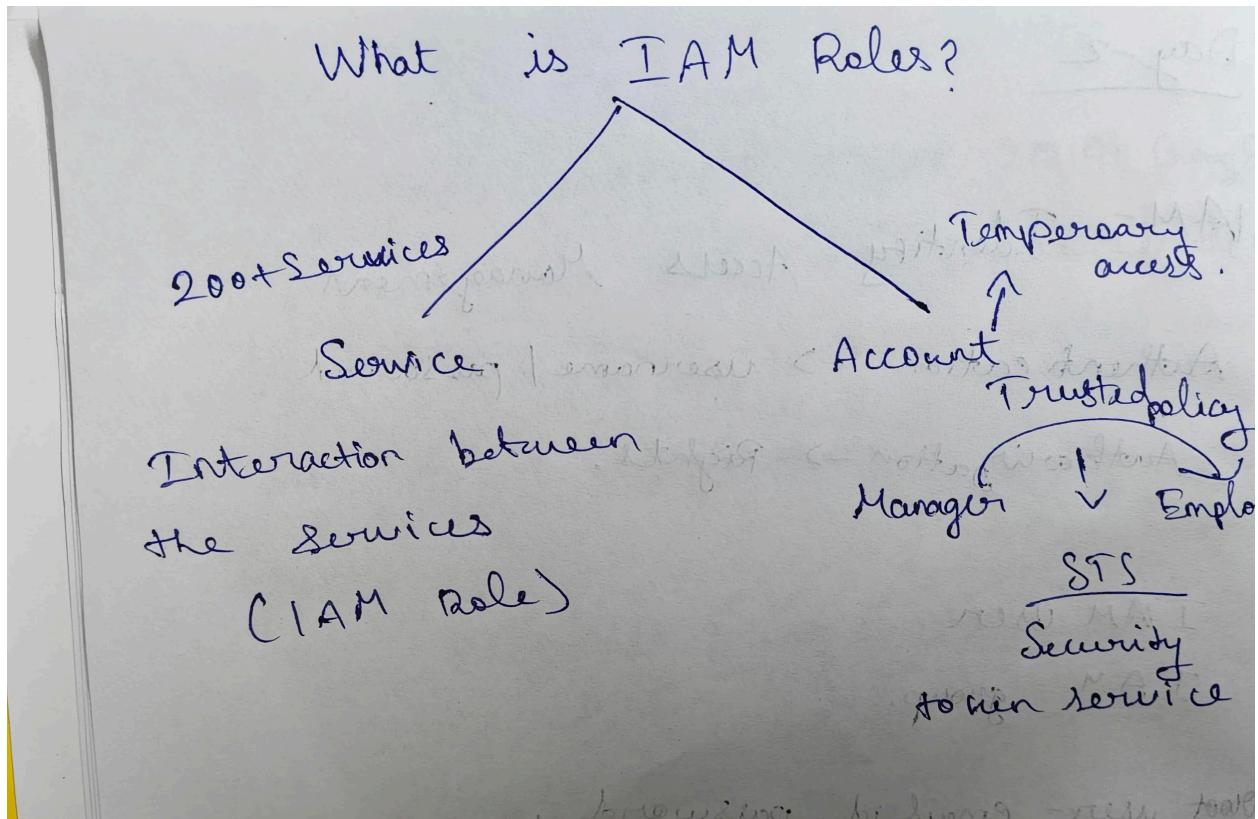


IAM ROLES AND POLICIES





Users | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#users

Search [Alt+S]

Hari pragadeesh (6076-0766-2137) Hari%0pragadeesh

IAM > Users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access Management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings
- Root access management
- Temporary delegation requests
- New

Access reports

- Access Analyzer
- Resource analysis New
- Unused access

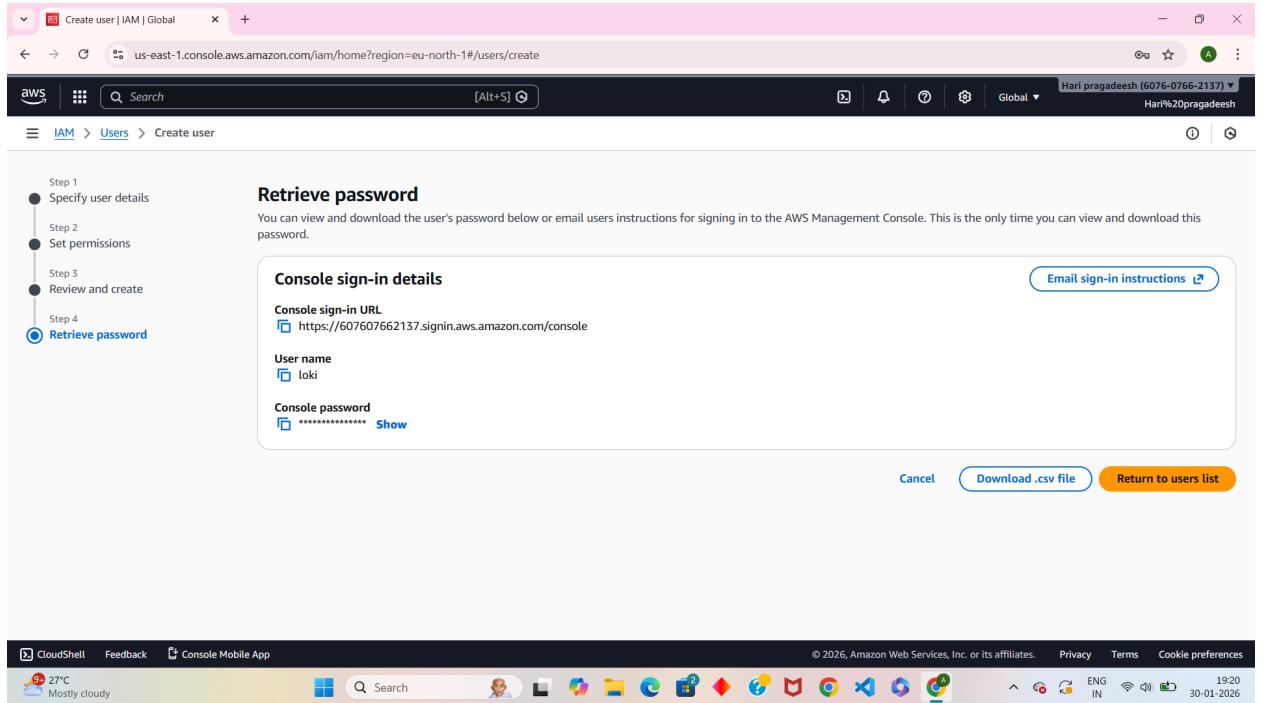
CloudShell Feedback Console Mobile App

27°C Mostly cloudy

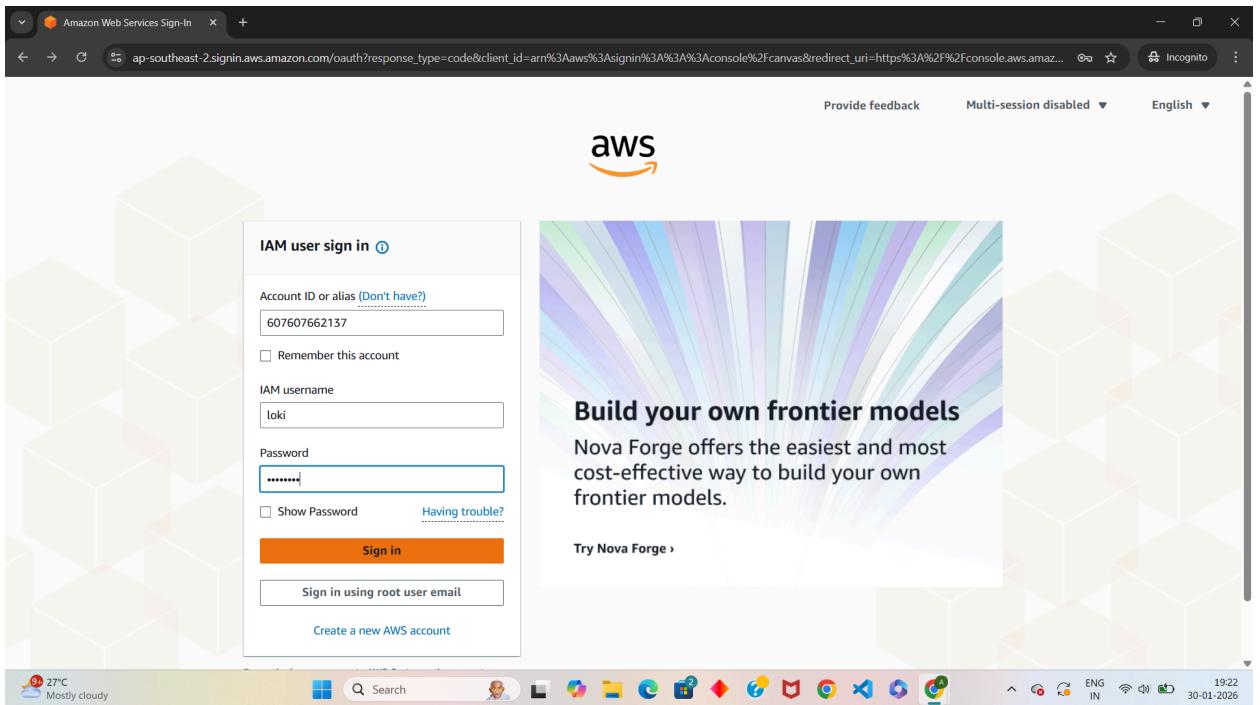
© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 19:20 30-01-2026

- IAM Users section is opened

- **No IAM users** are currently listed (Users = 0)
- Option available to **Create a new IAM user**
- This page is used to **manage users and their access**



- A new **IAM user "loki"** has been created
- **Console sign-in URL** is generated
- **Temporary password** is shown (only visible once)
- Option to download credentials as **CSV**
- Used to share login details with the user

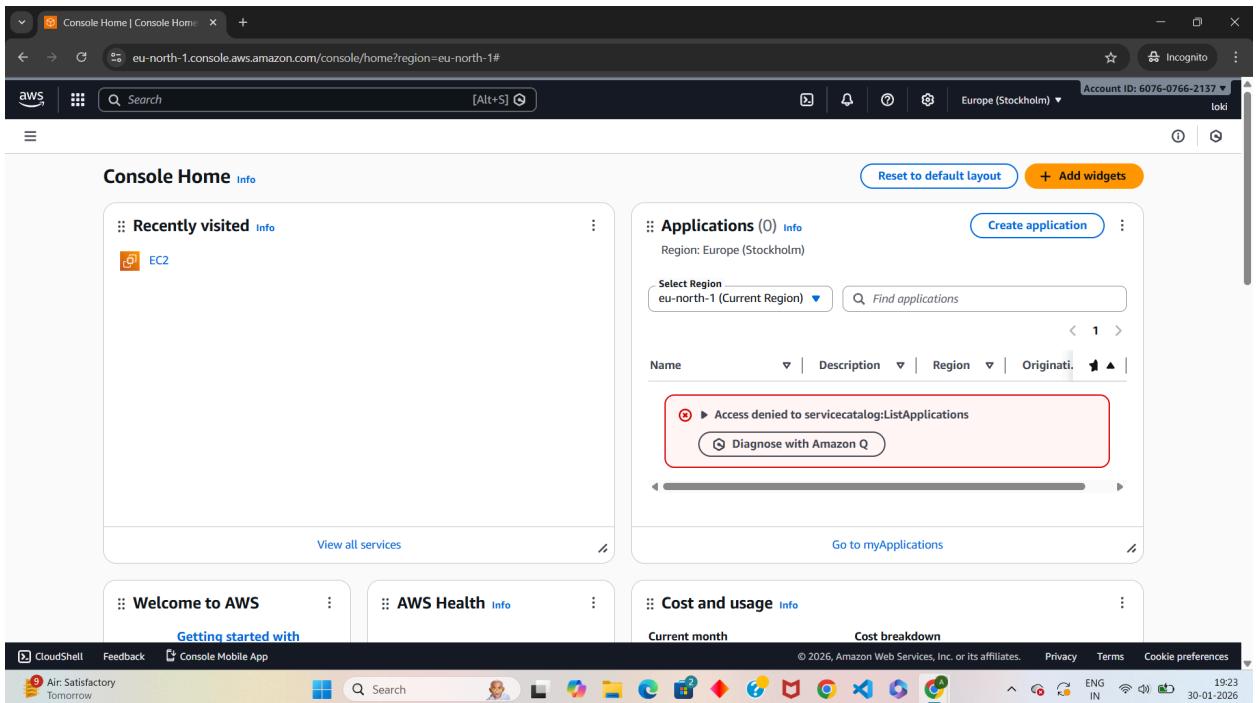


IAM user login screen

Account ID, username, and password are entered

User is signing in as an IAM user (not root)

Used to access AWS Console with limited permissions



IAM user successfully logged in

Region selected: Europe (Stockholm)

EC2 shown under recently visited services

Access denied error appears (insufficient permissions)

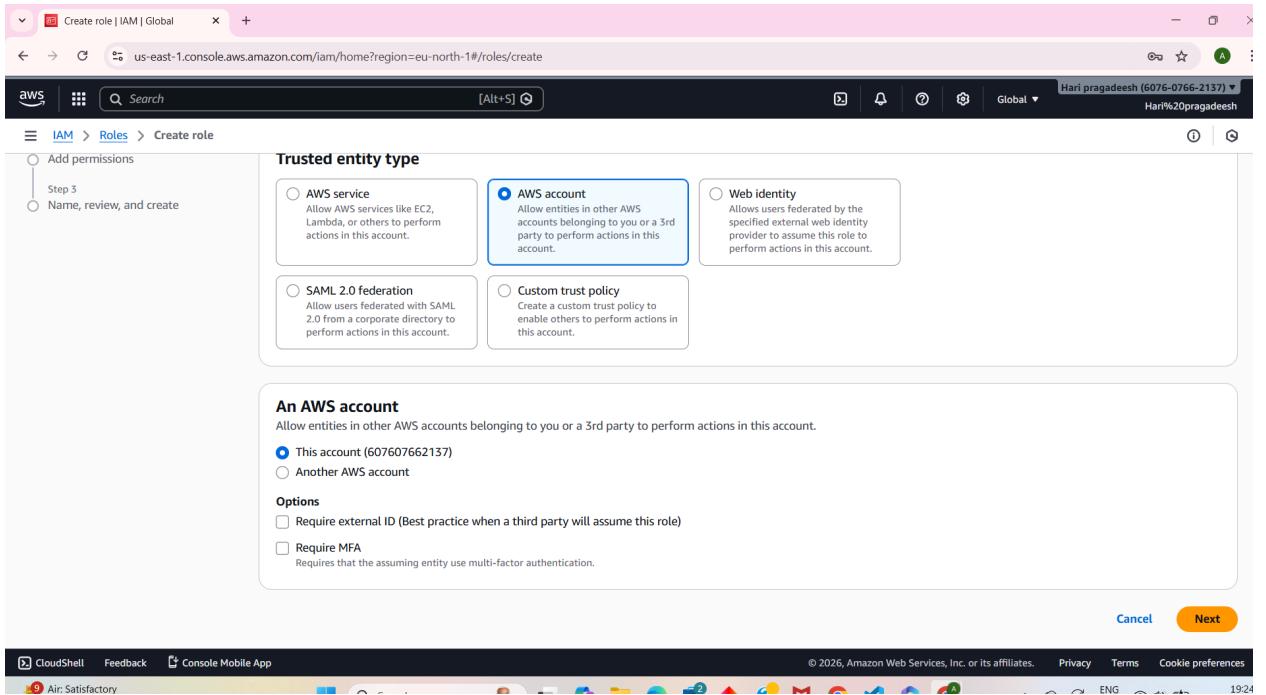
Indicates IAM user does not have required policies

The screenshot shows the AWS IAM Roles page. The left sidebar is collapsed, and the main content area displays the 'Roles' section. The table lists three roles:

| Role name | Trusted entities | Last activity |
|-----------------------------------|--|---------------|
| AWSServiceRoleForResourceExplorer | AWS Service: resource-explorer-2 (Service) | 2 hours ago |
| AWSServiceRoleForSupport | AWS Service: support (Service-Linked) | - |
| AWSServiceRoleForTrustedAdvisor | AWS Service: trustedadvisor (Service) | - |

Below the table, there are two sections: 'Roles Anywhere' and 'Access AWS from your non AWS workloads'. The 'X.509 Standard' section is expanded, showing instructions to use existing PKI infrastructure or AWS Certificate Manager Private Certificate Authority to authenticate identities.

- **IAM Roles section is opened**
- **3 existing roles are listed**
- **Roles are AWS service-linked roles**
- **Option available to Create a new role**



- **Creating a new IAM role**
- **AWS account selected as trusted entity**
- **This allows entities in the same account to assume the role**
- **Option to require MFA / External ID (not selected)**

The screenshot shows the AWS IAM 'Create role' wizard at Step 3. The left sidebar shows 'Name, review, and create'. The main area lists policies to attach to the new role. The 'AdministratorAccess' policy is selected (checked) and highlighted with a blue border. Other policies listed include 'AccountManagementFromVercel', 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBeanstalk', 'AIOpsAssistantIncidentReportPolicy', 'AIOpsAssistantPolicy', 'AIOpsConsoleAdminPolicy', 'AIOpsOperatorAccess', 'AIOpsReadOnlyAccess', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', and 'AlexaForBusinessGatewayExecution'. The 'AdministratorAccess' policy is described as providing full access to AWS services.

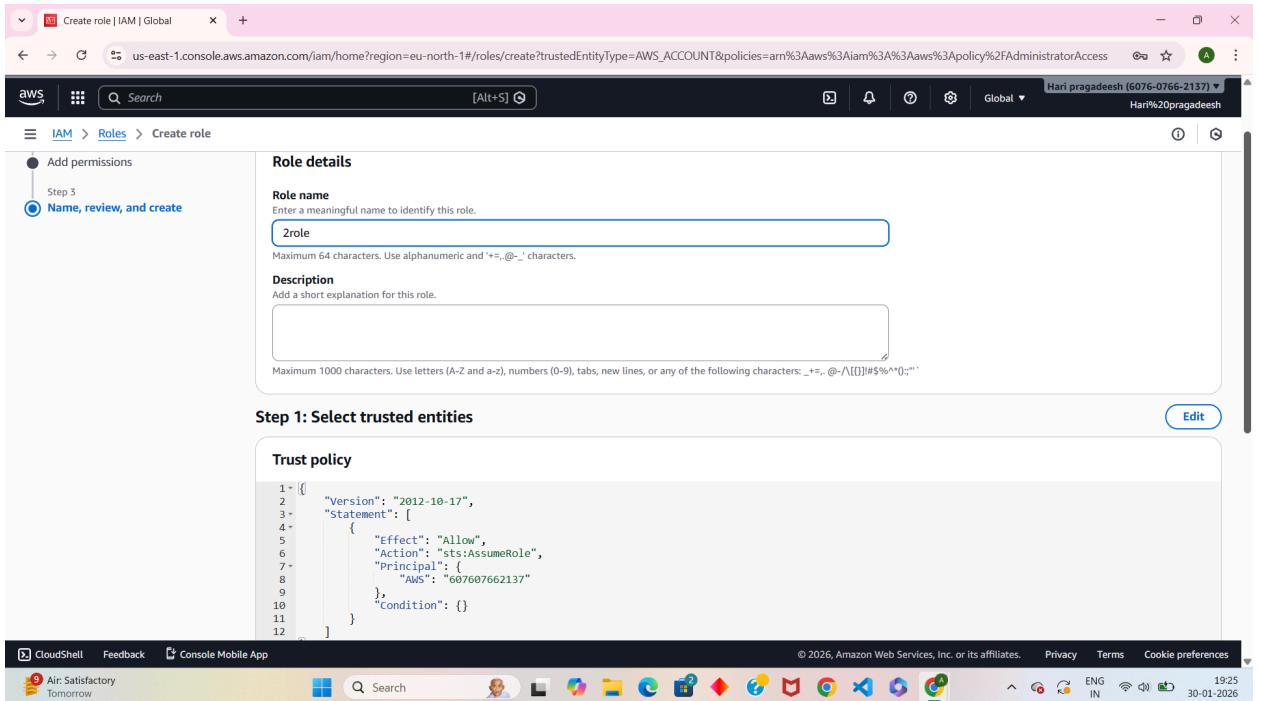
| Policy name | Type | Description |
|---|----------------------------|--|
| AdministratorAccess | AWS managed - job function | Provides full access to AWS services and administrative permissions. |
| AccountManagementFromVercel | AWS managed | For use with accounts created through Vercel. |
| AdministratorAccess-Amplify | AWS managed | Grants account administrative permissions. |
| AdministratorAccess-AWSElasticBeanstalk | AWS managed | Grants account administrative permissions. |
| AIOpsAssistantIncidentReportPolicy | AWS managed | Provides permissions required by the AI Ops Assistant. |
| AIOpsAssistantPolicy | AWS managed | Provides ReadOnly permissions required by the AI Ops Assistant. |
| AIOpsConsoleAdminPolicy | AWS managed | Grants full access to Amazon AI Operations. |
| AIOpsOperatorAccess | AWS managed | Grants access to the Amazon AI Operator. |
| AIOpsReadOnlyAccess | AWS managed | Grants ReadOnly permissions to the AI Ops Assistant. |
| AlexaForBusinessDeviceSetup | AWS managed | Provide device setup access to AlexaForBusiness. |
| AlexaForBusinessFullAccess | AWS managed | Grants full access to AlexaForBusiness. |
| AlexaForBusinessGatewayExecution | AWS managed | Provide gateway execution access to AlexaForBusiness. |

AdministratorAccess policy selected

This policy gives full access to AWS services

Policy type: AWS managed

Used to grant admin-level permissions to the role



Role name entered: 2role

Trust policy shows this AWS account can assume the role

Role is being reviewed before creation

Shows STS AssumeRole permission in trust policy

The screenshot shows the AWS IAM Roles page. A green banner at the top indicates that a role named "2role" has been created successfully. Below this, a table lists four IAM roles:

| Role name | Trusted entities | Last activity |
|---|--|---------------|
| 2role | Account: 607607662137 | - |
| AWSServiceRoleForResourceExplorer | AWS Service: resource-explorer-2 (Service) | 2 hours ago |
| AWSServiceRoleForSupport | AWS Service: support (Service-Linker) | - |
| AWSServiceRoleForTrustedAdvisor | AWS Service: trustedadvisor (Service) | - |

Below the table, there are sections for "Roles Anywhere" and "Temporary credentials". The "Temporary credentials" section includes a "Manage" button.

- **Role “2role” created successfully**
- **Total roles increased from 3 to 4**
- **Trusted entity: AWS Account**
- **Role is now ready to be assumed**

The screenshot shows the AWS IAM User Details page for a user named 'loki'. The top navigation bar includes the AWS logo, a search bar, and a global dropdown for 'Hari pragadeesh (6076-0766-2137)'. The main content area displays the 'Summary' tab for the 'loki' user. Key details shown include:

- ARN:** arn:aws:iam::607607662137:user/loki
- Console access:** Enabled without MFA
- Created:** January 30, 2026, 19:20 (UTC+05:30)
- Last console sign-in:** Today
- Access key 1:** Create access key

The 'Permissions' tab is selected, showing one attached policy:

- Policy name:** IAMUserChangePassword
- Type:** AWS managed
- Attached via:** Directly

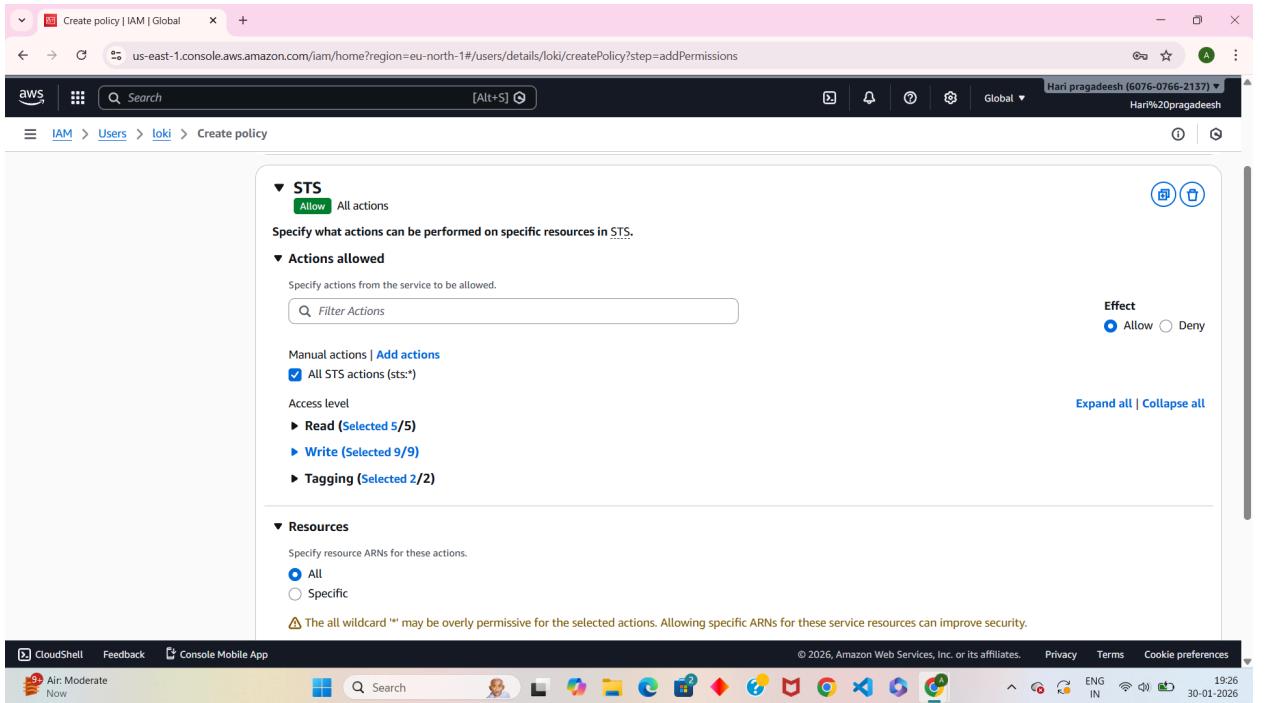
Below the permissions section, there is a note: "Permissions are defined by policies attached to the user directly or through groups." A 'Permissions boundary' section is also present but noted as not set.

IAM user loki details displayed

Console access enabled without MFA

User currently has limited permissions

Only basic policy attached initially

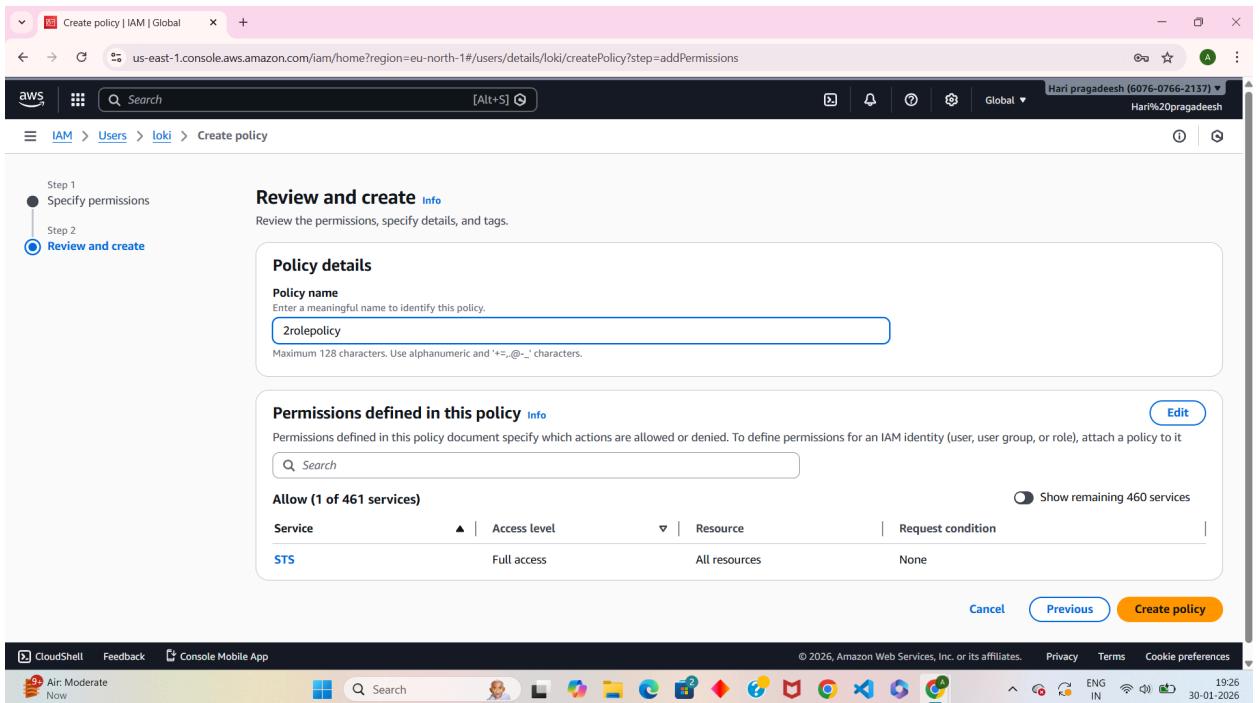


Creating a custom inline policy for user

STS service selected

All STS actions (sts:*) allowed

Resources set to All



- **Policy name entered: 2rolepolicy**
- **Policy allows full STS access**
- **This enables role assumption**
- **Ready to create the policy**

The screenshot shows the AWS IAM User details page for a user named 'loki'. A green success message at the top states 'Policy 2rolepolicy created.' Below it, the 'Summary' section provides details about the user: ARN (arn:aws:iam::607607662137:user/loki), Created (January 30, 2026, 19:20 (UTC+05:30)), Console access (Enabled without MFA), Last console sign-in (Today), and Access key 1 (Create access key). The 'Permissions' tab is selected, showing two attached policies: '2rolepolicy' (Customer inline) and 'sts' (Customer inline). The browser interface includes a search bar, a navigation bar with 'aws' and 'Search' buttons, and a top right corner showing the user's name 'Hari pragadeesh (6076-0766-2137)' and profile picture.

Policy 2rolepolicy created and attached

Policy type: Customer inline

User now has STS permissions

Used for Switch Role / Assume Role

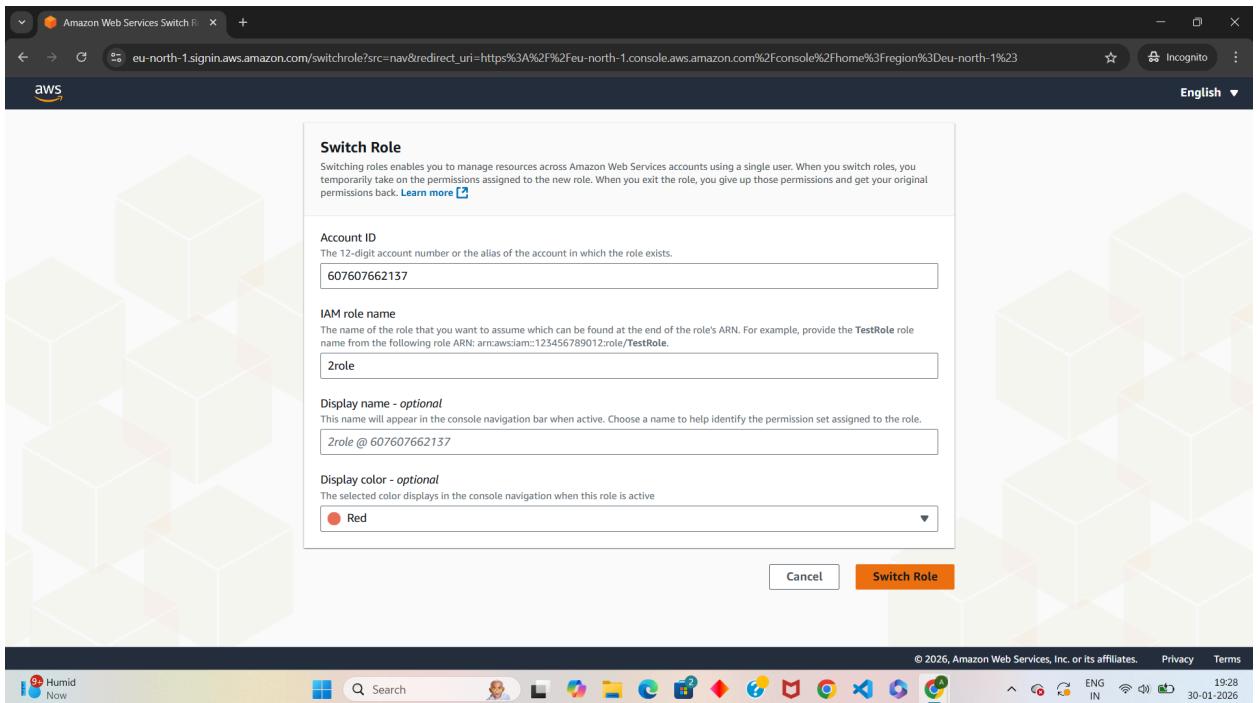
The screenshot shows the AWS Console Home page. On the left, there's a sidebar with 'Recently visited' services (EC2) and a 'View all services' link. In the center, the 'Applications' section shows a message: 'Access denied to servicecatalog>ListApplications'. On the right, a sidebar lists account details (Account ID: 6076-0766-2137, IAM user: loki) and navigation links (Account, Organization, Service Quotas, etc.). At the bottom, there are links for 'Turn on multi-session support', 'Switch role', and 'Sign out'.

User loki logged in successfully

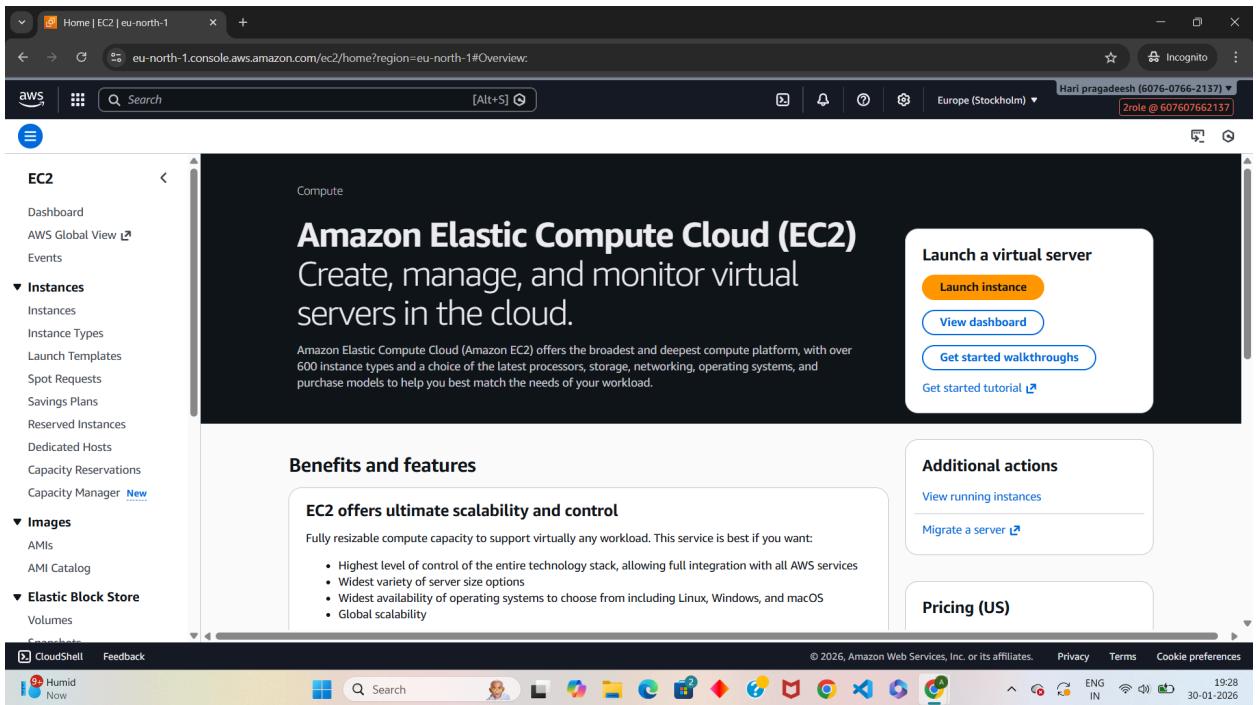
Region: Europe (Stockholm)

Still shows Access Denied for some services

Indicates user must switch to role to get admin access



- **Switch Role option is opened**
- **Account ID of the same AWS account is entered**
- **IAM role name `2role` is provided**
- **Display name and color selected for identification**
- **Used to assume the role temporarily**



Role 2role is successfully assumed

EC2 service opens without access denied

AdministratorAccess permissions are active

User can now launch and manage EC2 instances

The screenshot shows the AWS IAM console interface. The left sidebar has 'Access Management' expanded, with 'Users' selected. The main area displays a table titled 'Users (1/1)'. A green banner at the top states 'User "loki" deleted.' The table row for 'loki' shows the following details:

| User name | Path | Groups | Last activity | MFA | Password age | Console last sign-in | Access key last used |
|-----------|------|--------|---------------|-----|--------------|----------------------|----------------------|
| loki | / | 0 | 8 minutes ago | - | 6 minutes | 8 minutes ago | - |

At the bottom right of the table are three buttons: 'Edit' (blue), 'Delete' (orange), and 'Create user' (yellow).

IAM user `loki` deleted successfully

Confirmation message displayed

Shows last activity and login time

User is no longer available for access

The screenshot shows the AWS IAM Roles page. A prominent message at the top left says "Role deleted 2role." Below this, the "Roles (3)" section is displayed with three entries:

| Role name | Trusted entities | Last activity |
|---|--|---------------|
| AWSServiceRoleForResourceExplorer | AWS Service: resource-explorer-2 (Service) | 2 hours ago |
| AWSServiceRoleForSupport | AWS Service: support (Service-Linker) | - |
| AWSServiceRoleForTrustedAdvisor | AWS Service: trustedadvisor (Service) | - |

Below the table, there are two sections: "Roles Anywhere" and "Access AWS from your non AWS workloads". The "Access AWS from your non AWS workloads" section includes links to "X.509 Standard" and "Temporary credentials". The status bar at the bottom right shows the date as 30-01-2026.

IAM role 2role deleted

Roles count reduced back to 3

Only AWS service-linked roles remain

Cleanup of temporary role completed