# Serverless Data Processing (CSCI 5410)

Dr. Saurabh Dey

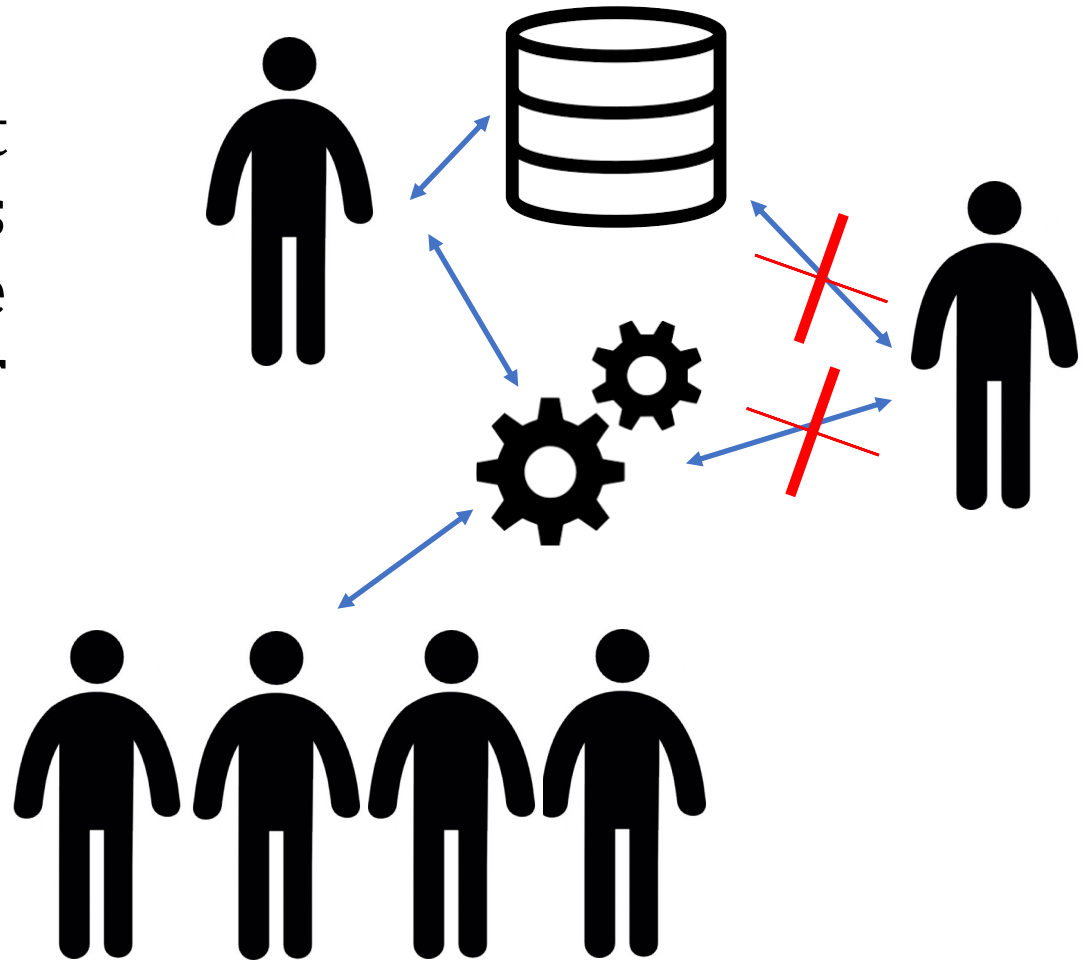
# Outline

1. Identity and Access Management

# Identity and Access Management

"Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reasons."

- Gartner



https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

# Cloud IAM


- Cloud IAM lets you grant granular access to specific Google Cloud resources and helps prevent access to other resources.

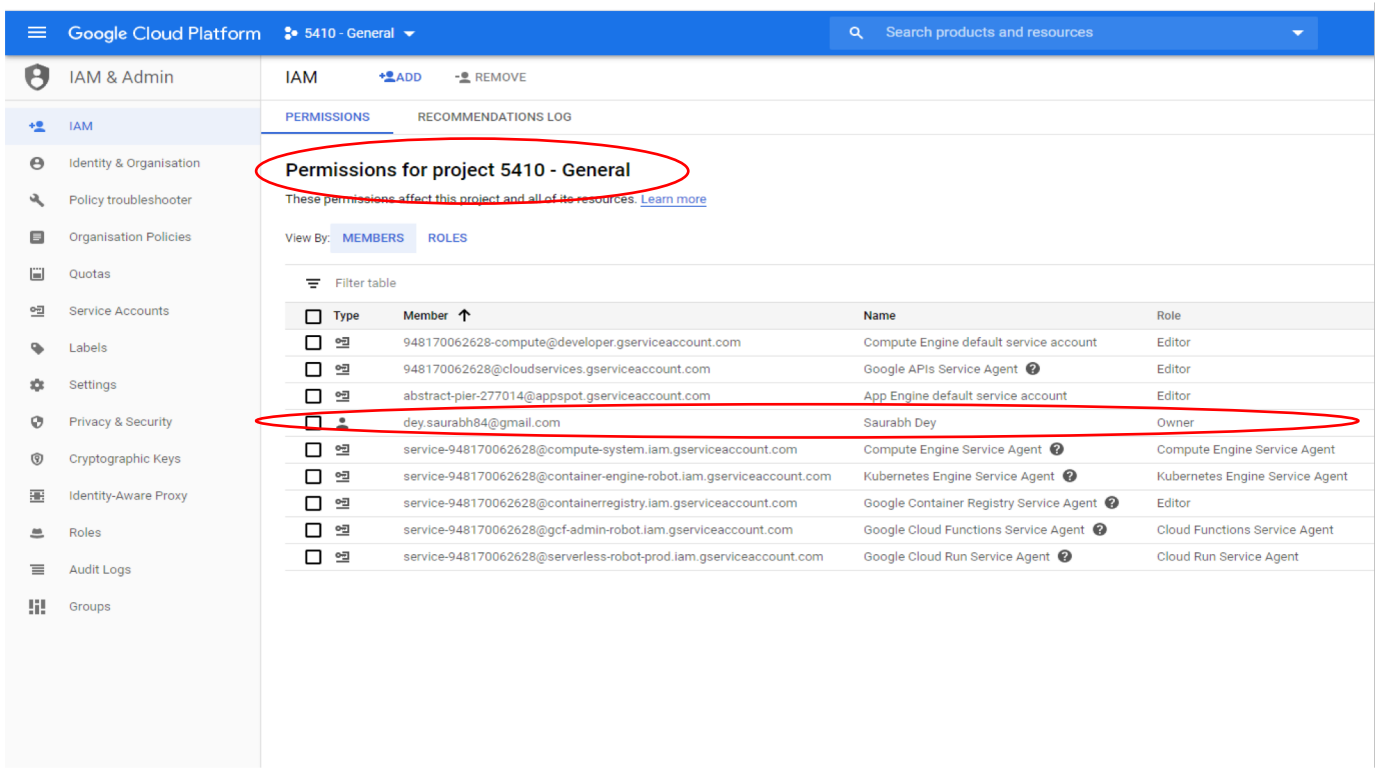
- With Cloud IAM, we manage access control by defining who (identity) has what access (role) for which resource.

- What is a resource?
  - Google Compute Engine virtual machine instances, Google Kubernetes Engine (GKE) clusters, and Cloud Storage buckets
  - Our project files, folders are also resources

# Cloud IAM Policy

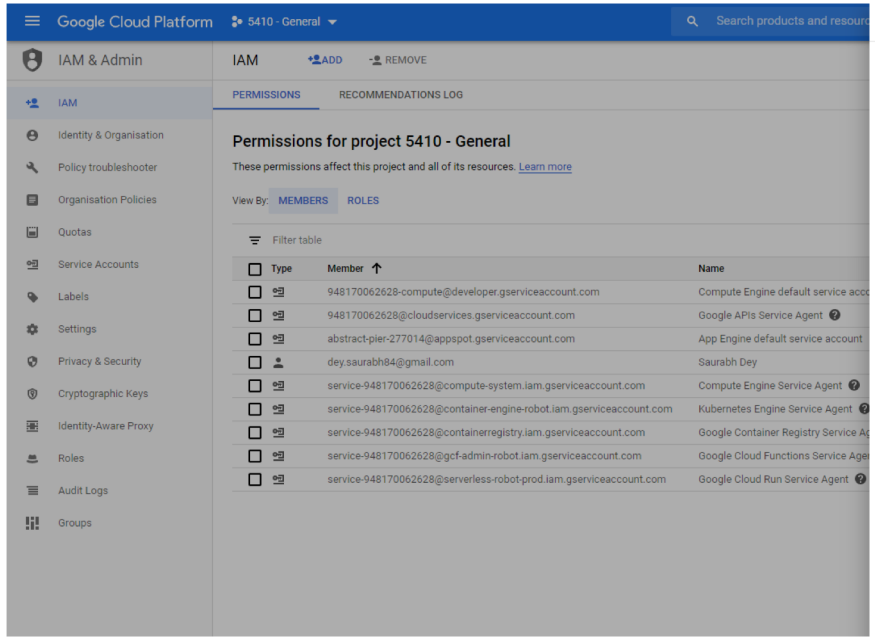

- A Cloud IAM policy defines and enforces what roles are granted to which members, and this policy is attached to a resource.

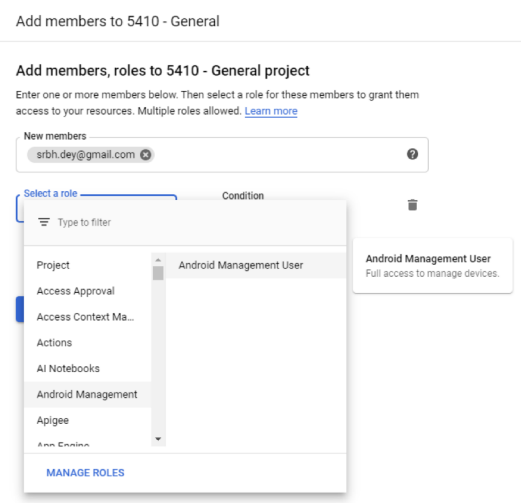
- When authenticated member attempts to access a resource, Cloud IAM checks the resource's policy to determine whether the action is permitted.

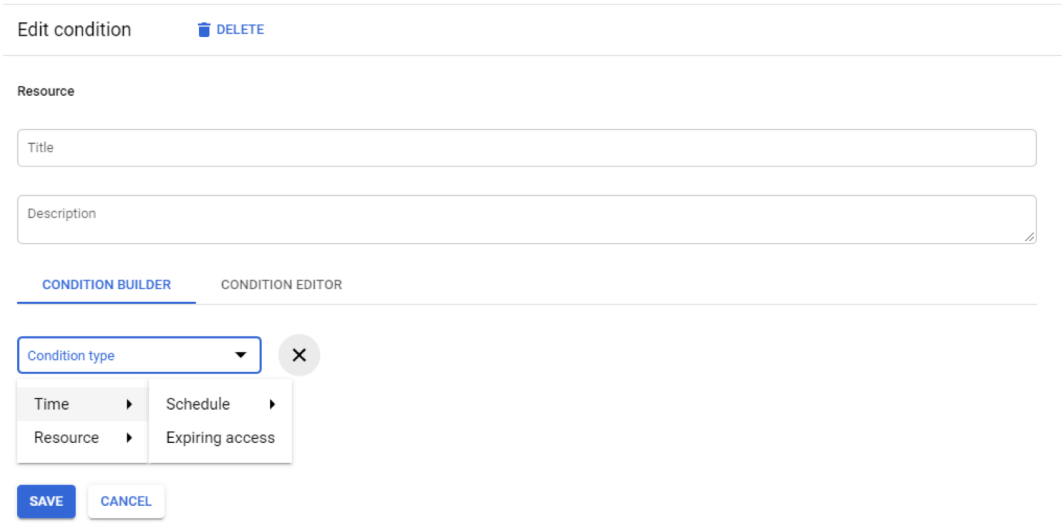


# Cloud IAM Policy

- A member can be added to a project, and roles can be granted with conditions, and it should be attached to a resource.




Google Cloud

# Cloud IAM Definitions

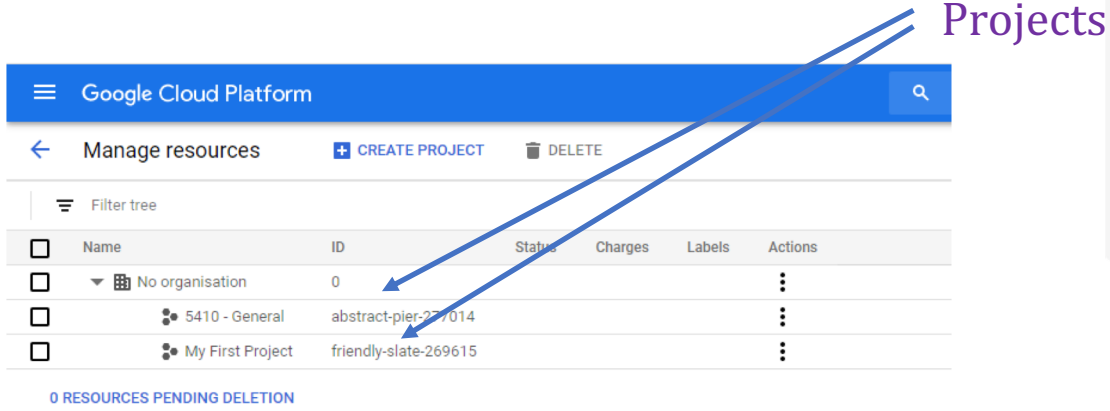

**Member:** A member can be a **Google Account,** a service account, a **Google group**, or a **G Suite** or **Cloud Identity domain** that can access a resource. The identity of a member is an **email address,** or a domain name associated with G Suite or Cloud Identity domains.

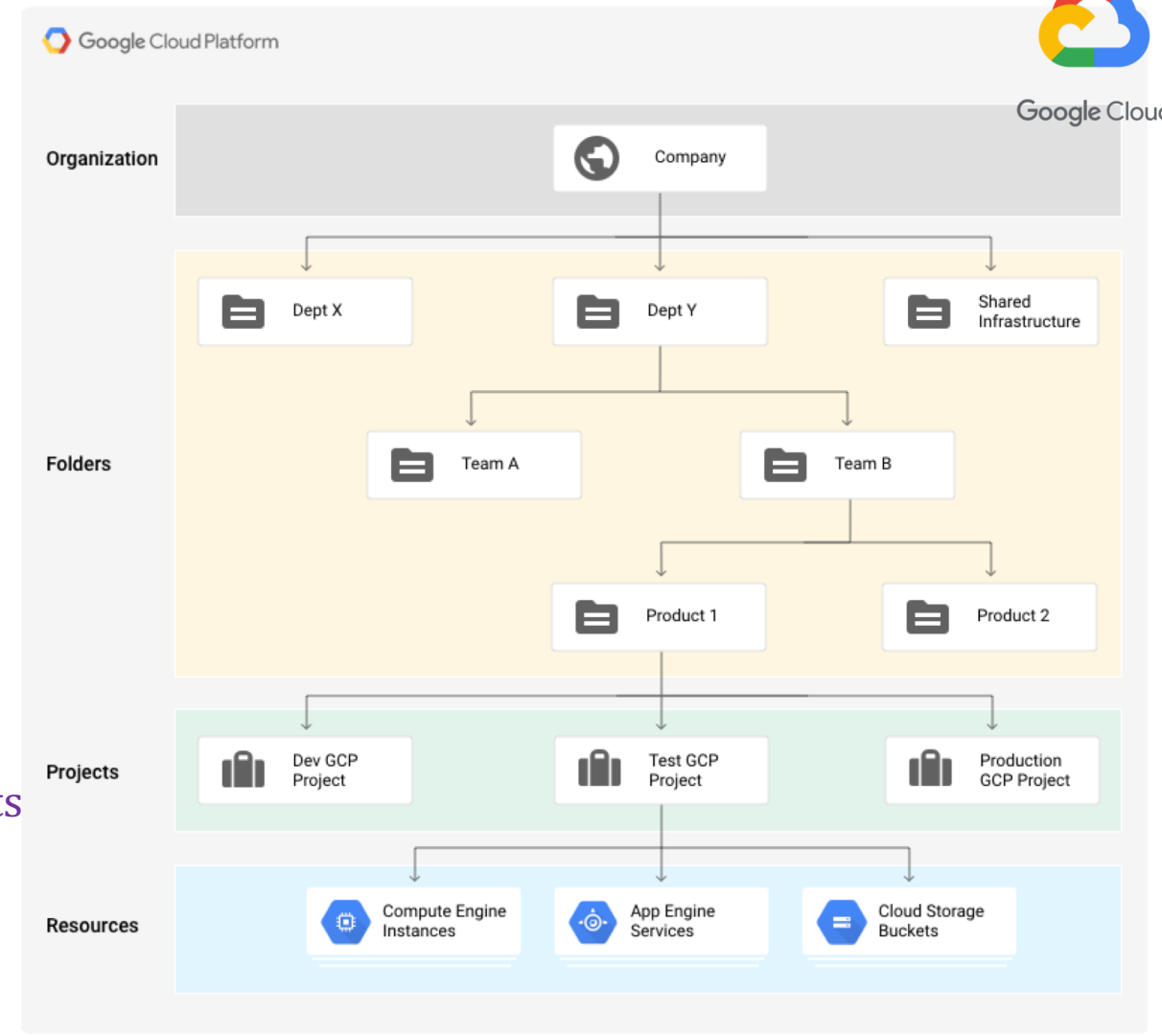
**Role:** A role is a collection of permissions. Permissions determine what operations are allowed on a resource. When you grant a role to a member, you grant all the permissions that the role contains.

**Policy:** The Cloud IAM policy binds one or more members to a role. When you want to define who (member) has what type of access (role) on a resource, you create a policy and attach it to the resource.

# Access Levels

The Organization resource is the root node of the Google Cloud resource hierarchy and all resources that belong to an organization are grouped under the organization node. This provides central visibility and control over every resource that belongs to an organization.



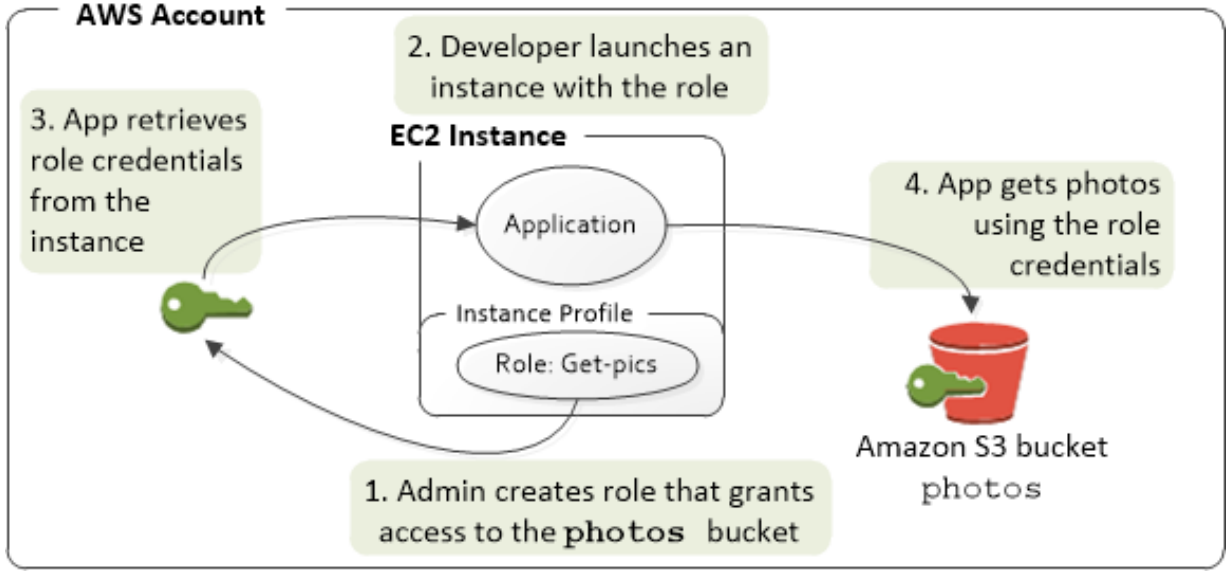
# AWS IAM


## Features

- Shared Access
- Granular Permission
- Secured Access to AWS resources for applications that run on EC2
- Multi Factor Authentication
- Identity Federation
- Free to Use

# AWS IAM

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.




https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

What is the role?
**Get_pics**

What is the permission policy?
**read_only**

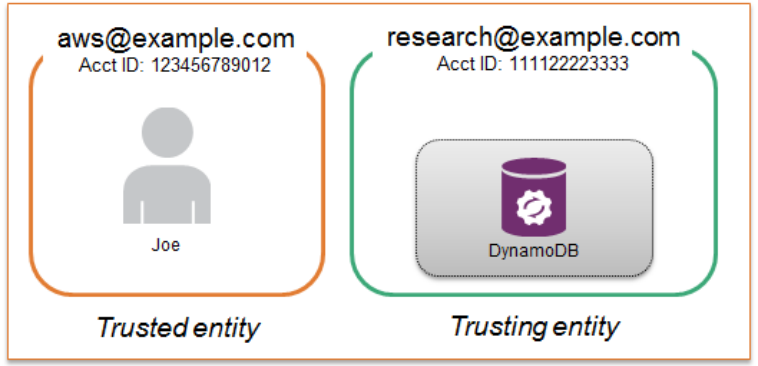
What is the role's trust policy?
**Only EC2 instances can assume the role**

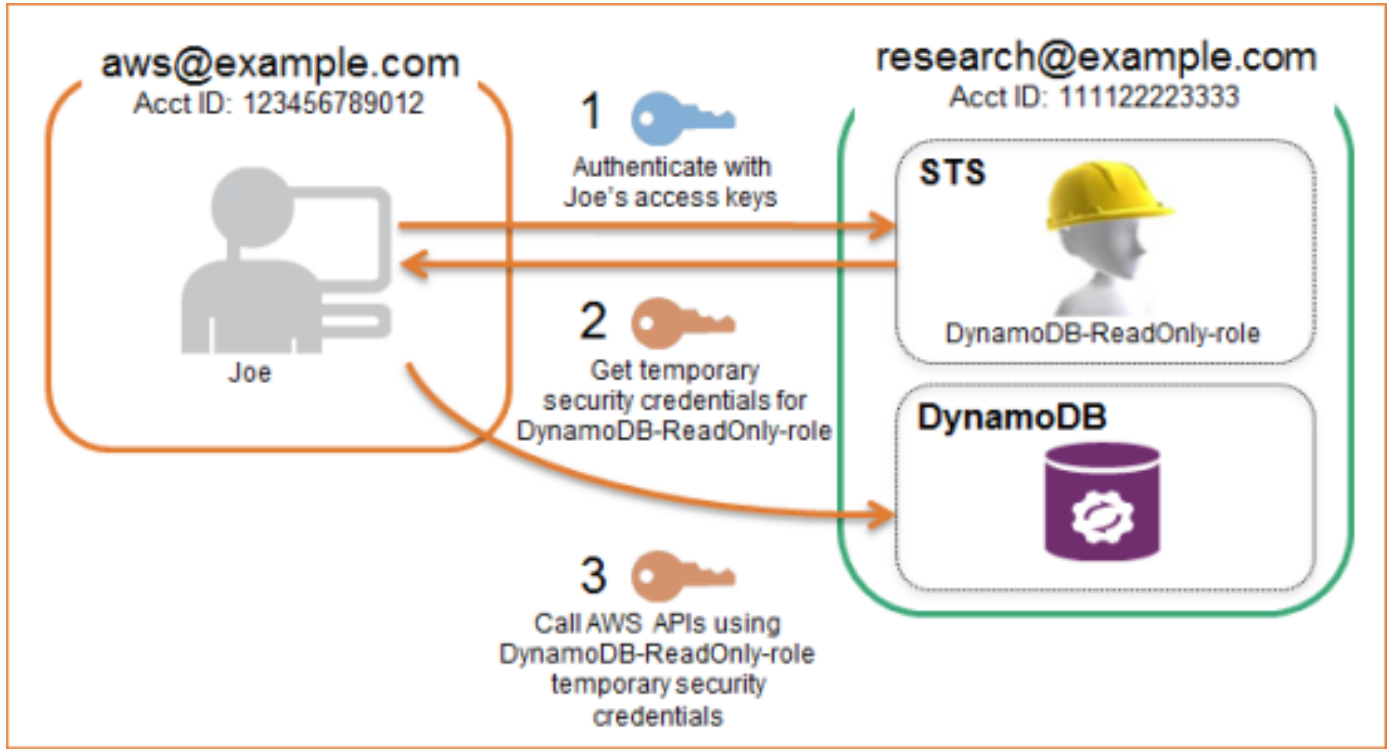
# Identities

| | |
|---|---|
| Root User | • Single sign-in identity that has complete access to all AWS services in the account |
| IAM User | • use for IAM users is to give people the ability to sign in to the AWS Management Console for interactive tasks and to make programmatic requests to AWS services using the API or CLI |
| IAM Groups | • Collection of IAM users that share the same access permission |
| IAM Roles | • An IAM user can assume a role to temporarily take on different permissions for a specific task. |

# AWS IAM – Use Case 1

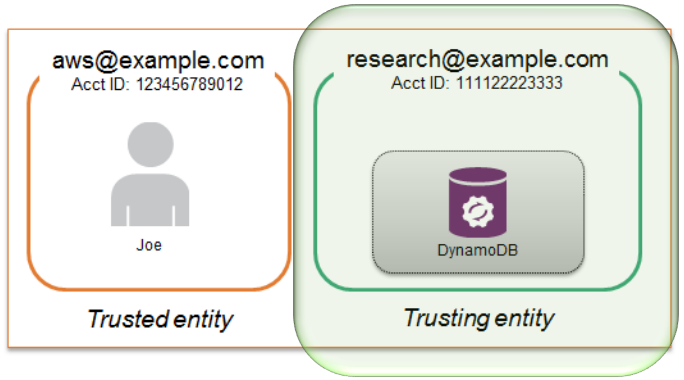
- research@example.com is where data from several research projects are stored
- aws@example.com is company's main account where most of the IAM users are created
- Joe needs read-only access to data stored in DynamoDB tables that are in research@example.com.
- Enabling cross-account API access requires establishing a trust relationship between the two accounts.

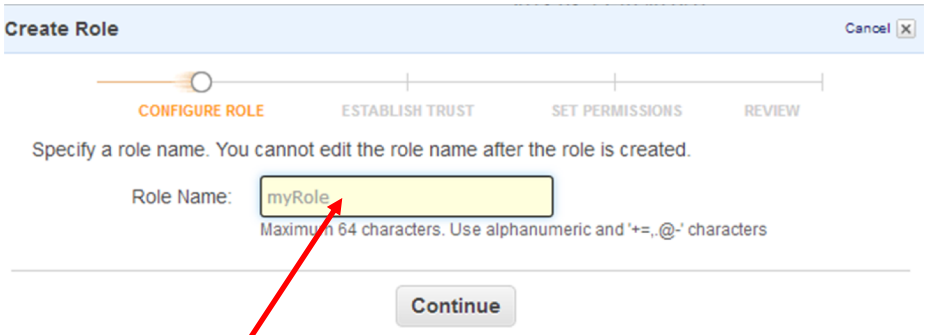



https://aws.amazon.com/blogs/security/delegating-api-access-to-aws-services-using-iam-roles/

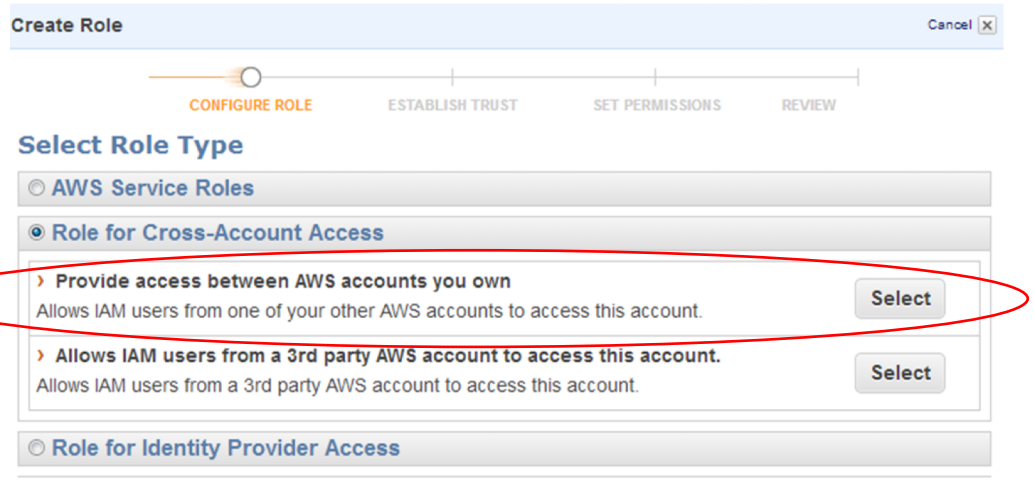
# Use Case 1 (Trusting Entity Configuration)



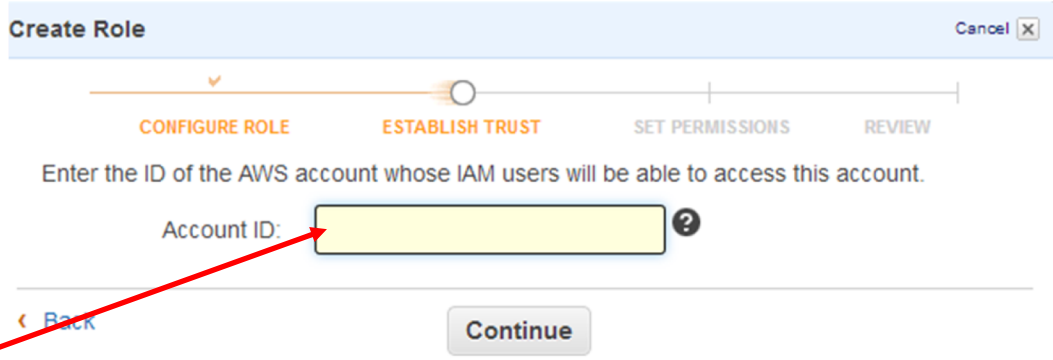




DynamoDB-ReadOnly-role

1




2

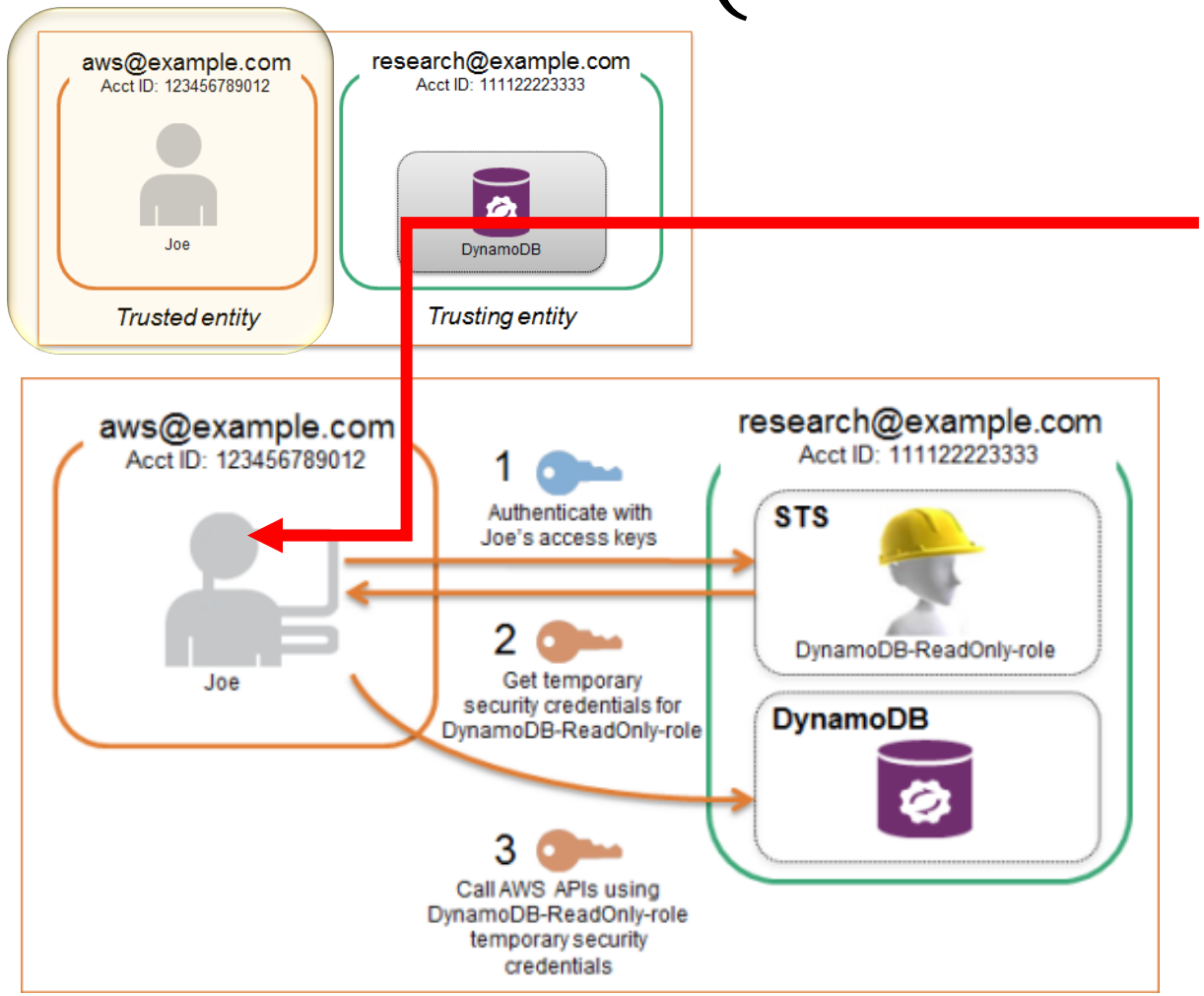



3

ID of aws@example.com

https://aws.amazon.com/blogs/security/delegating-api-access-to-aws-services-using-iam-roles/

# Use Case 1 (Trusted Entity Configuration)




```
{ "Statement": [
  {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::111122223333:role/DynamoDB-
ReadOnly-role"
  }
 ]
}
```

Policy assigned to Joe

https://aws.amazon.com/blogs/security/delegating-api-access-to-aws-services-using-iam-roles/

# When to Create AWS IAM Role?

- You are creating an application that runs on an Amazon Elastic Compute Cloud (Amazon EC2) instance and that application makes requests to AWS.

- You are creating an app that runs on a mobile phone and that makes requests to AWS.

- Users in your company are authenticated in your corporate network and want to be able to use AWS without having to sign in again—that is, you want to allow users to federate into AWS.

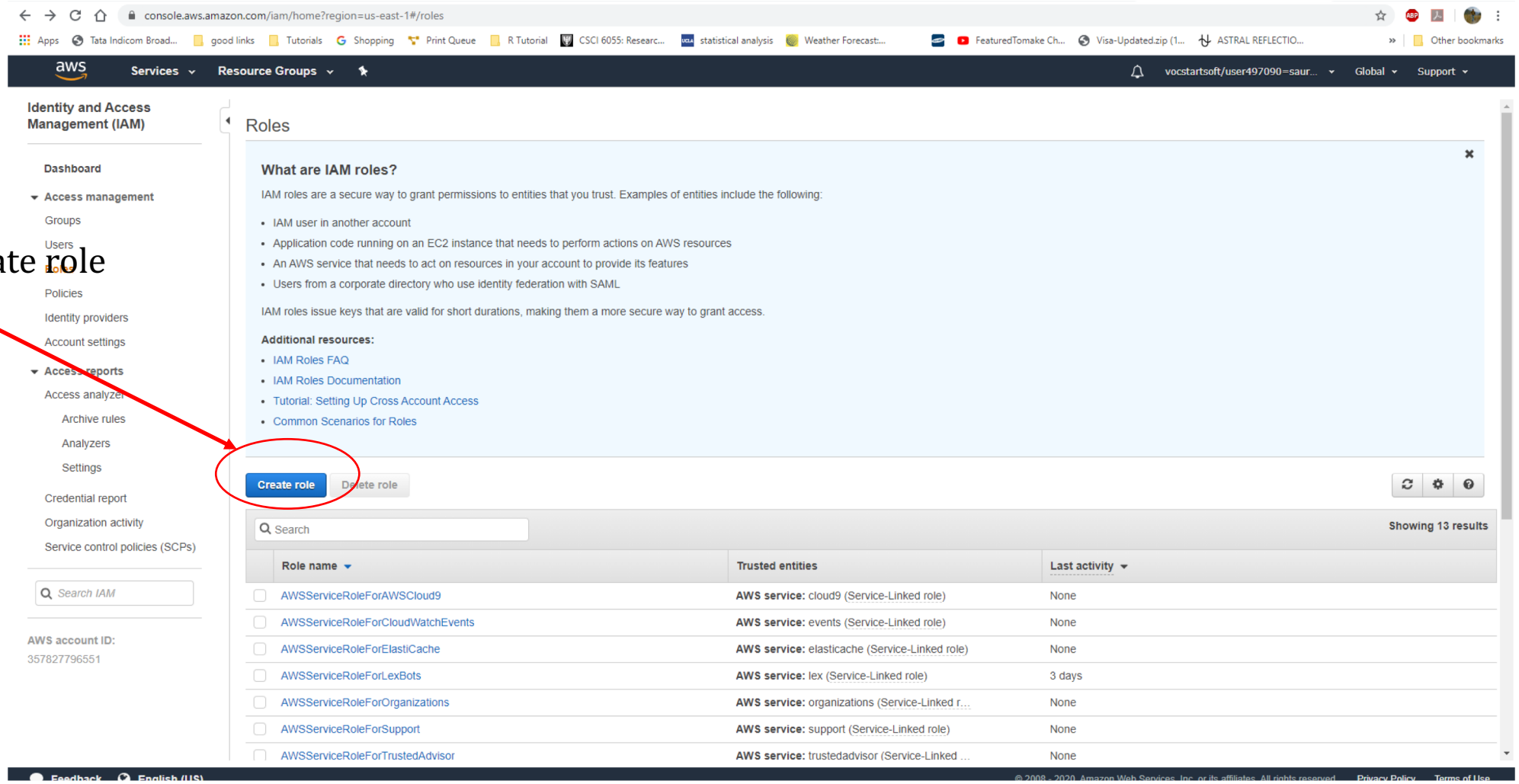
# When to Create IAM Users?

- You created an AWS account and you're the only person who works in your account.

- Other people in your group need to work in your AWS account, and your group is using no other identity mechanism.

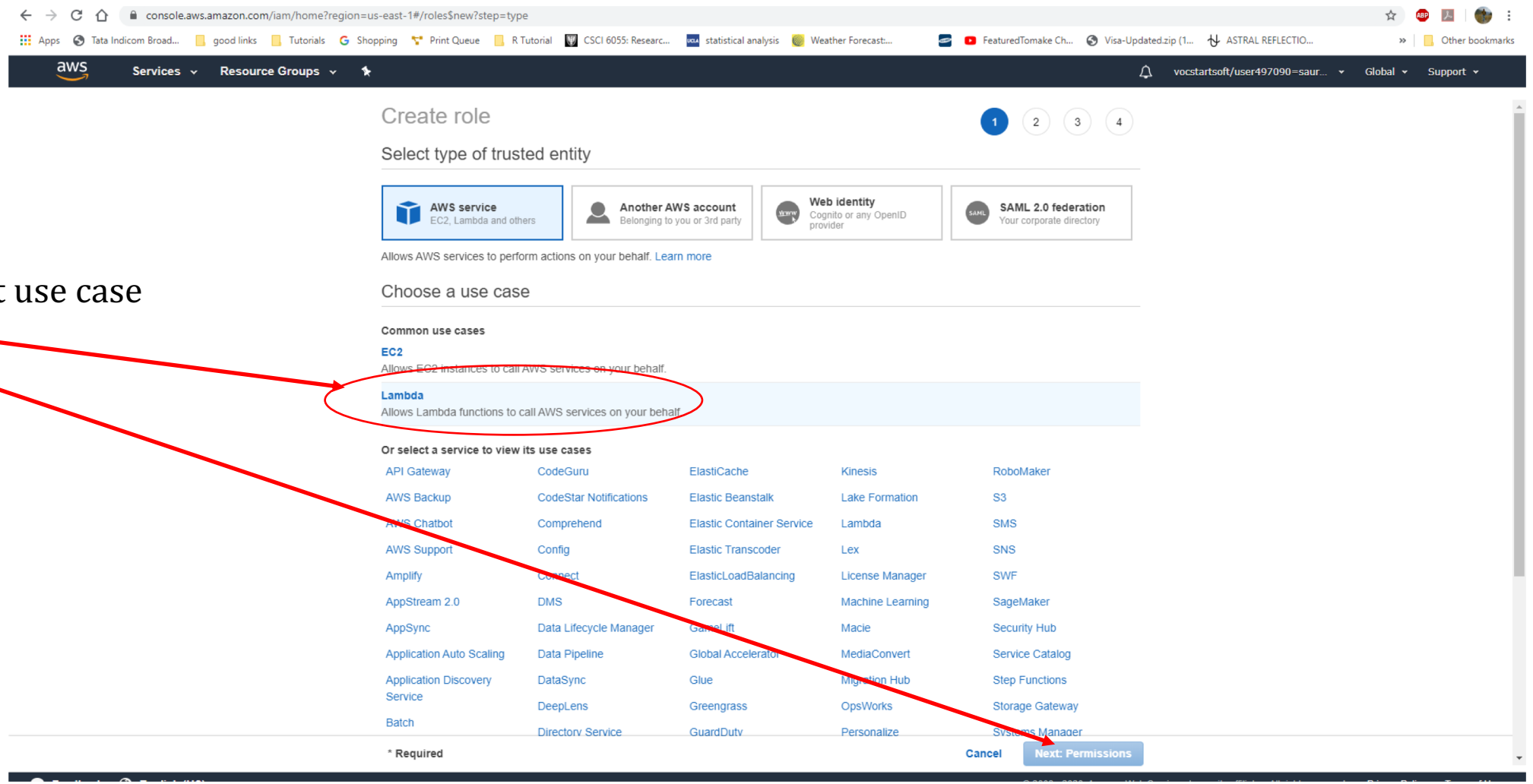
# Example – IAM Role creation (1 – 6)

Click to create role



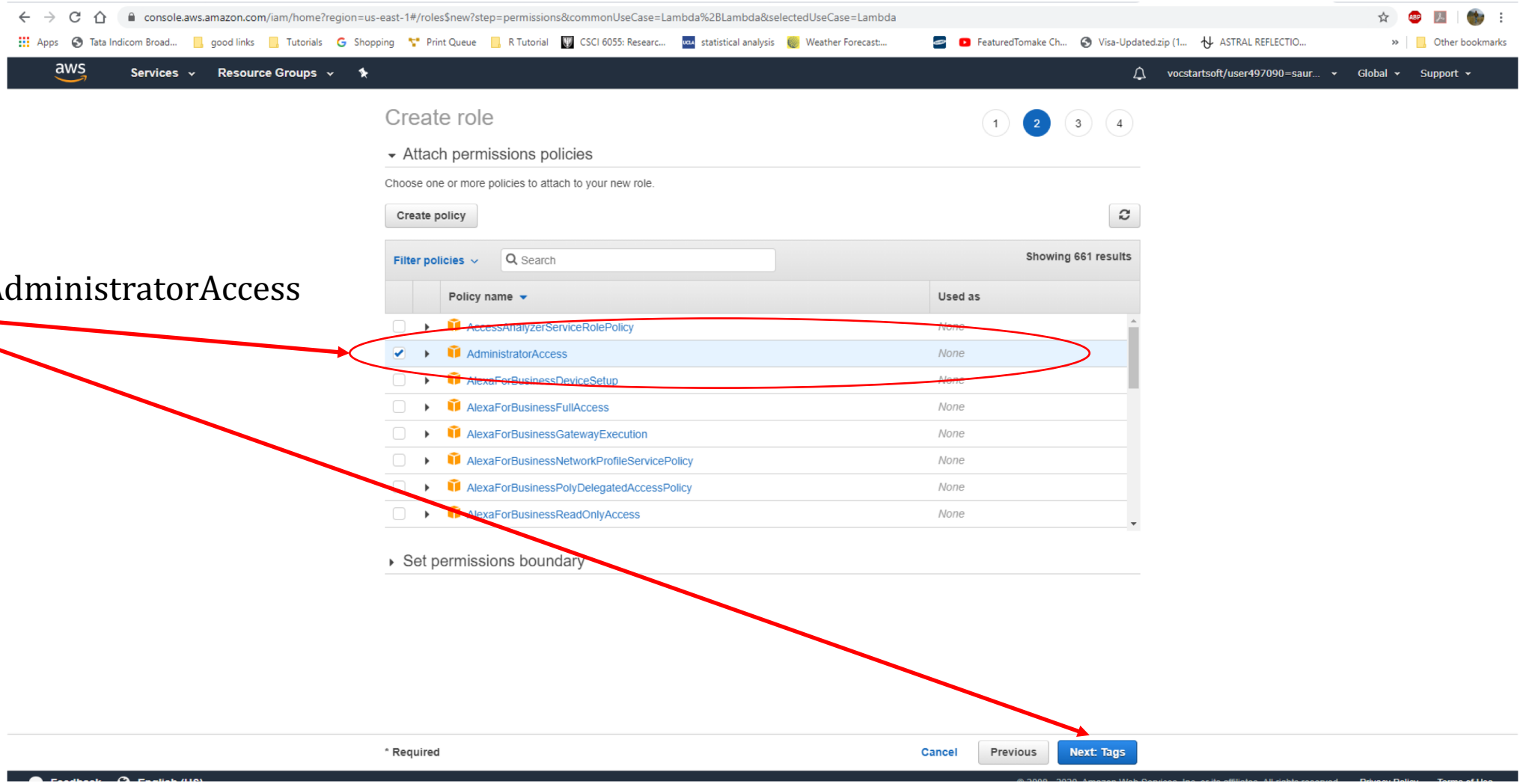
# Example – IAM Role creation (2 – 6)

Selecting a default use case



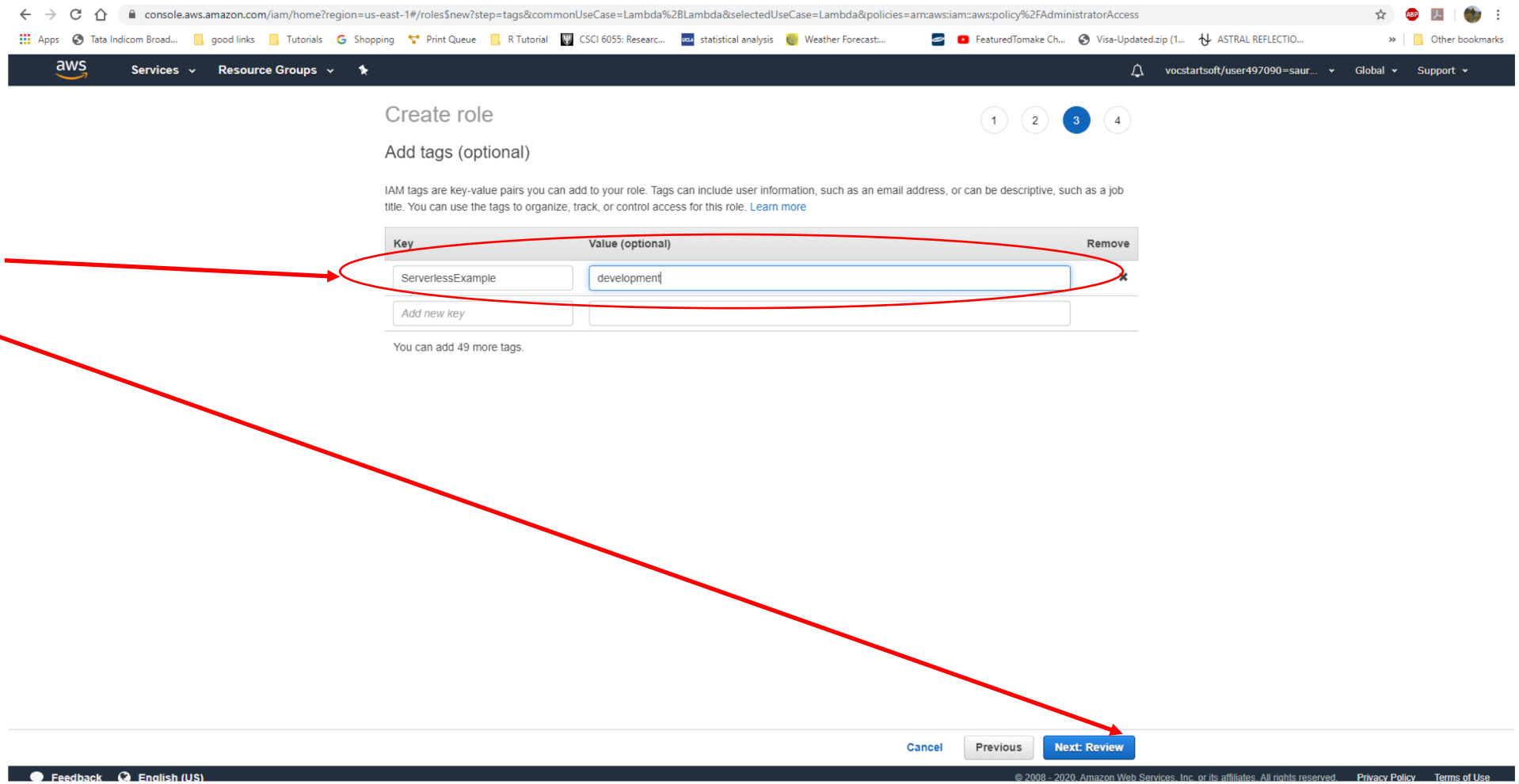
# Example – IAM Role creation (3 – 6)

Selecting AdministratorAccess

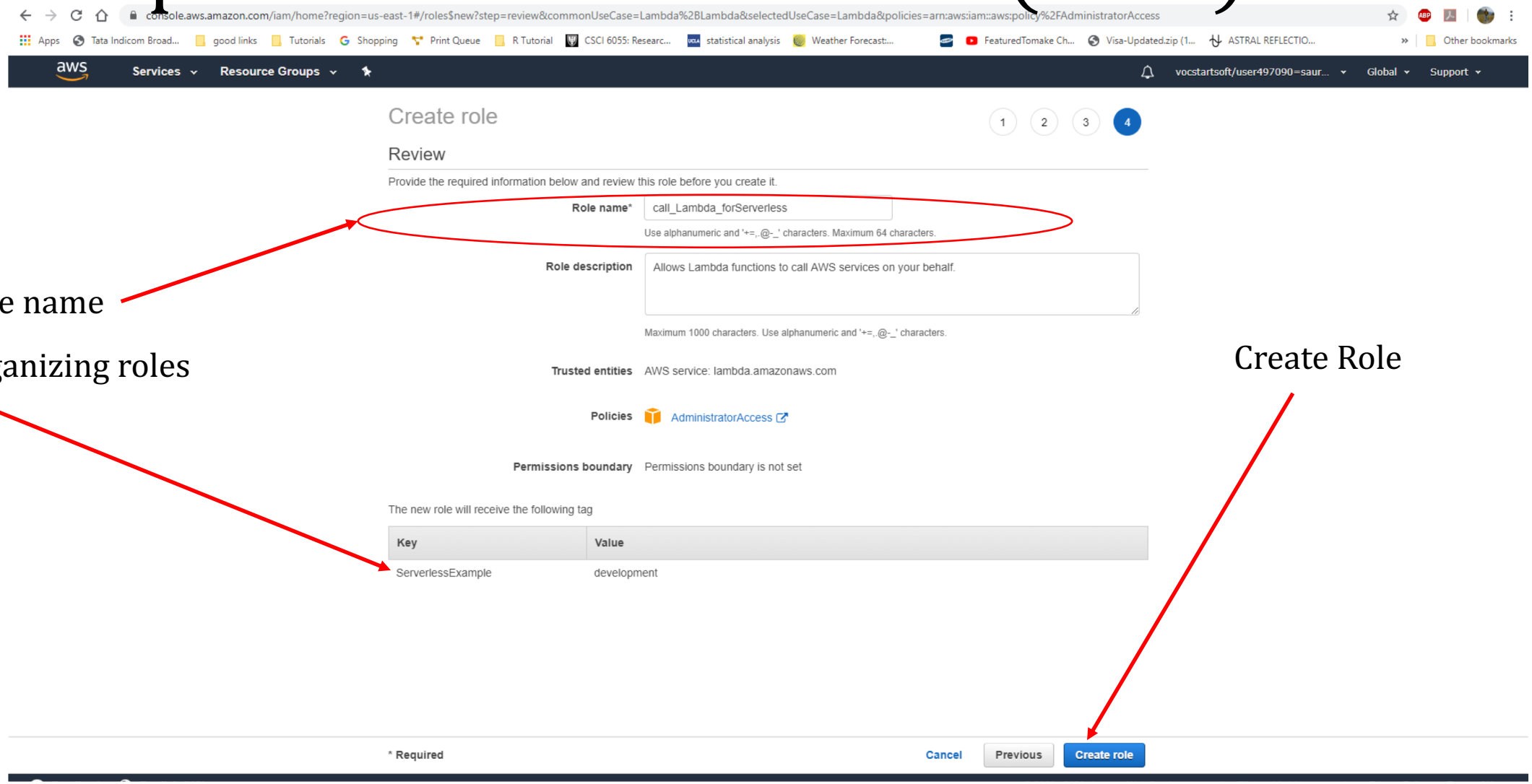


# Example – IAM Role creation (4 – 6)

Adding tags



# Example – IAM Role creation (5 – 6)



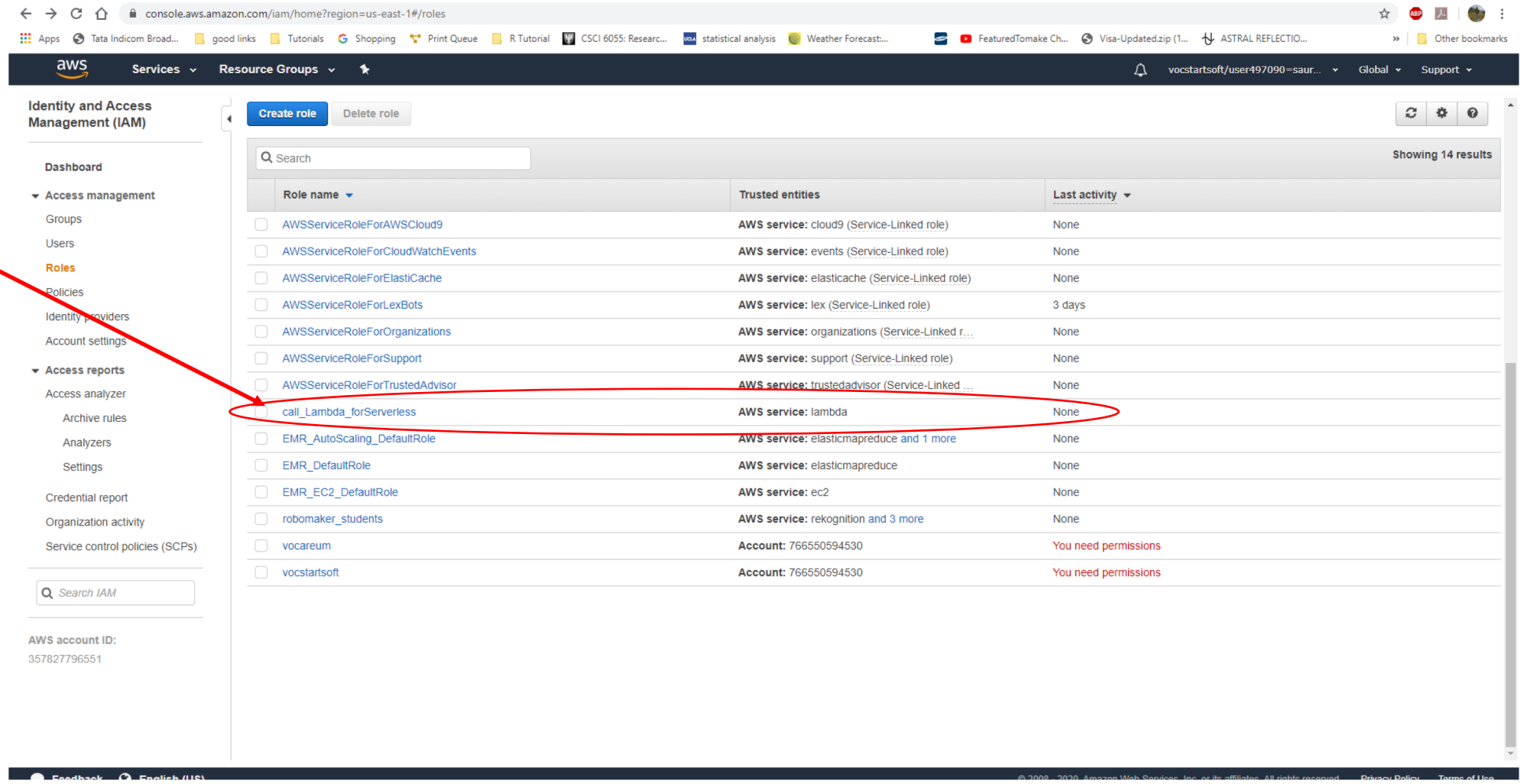

Adding role name

Helps in organizing roles

Create Role

# Example – IAM Role creation (6 – 6)

New role



# Questions to Consider

- Is IAM same for all cloud providers?
- Do we need to create or use roles for accessing any of the cloud services?