

Serverless Data Processing (CSCI 5410)

Dr. Saurabh Dey

Outline

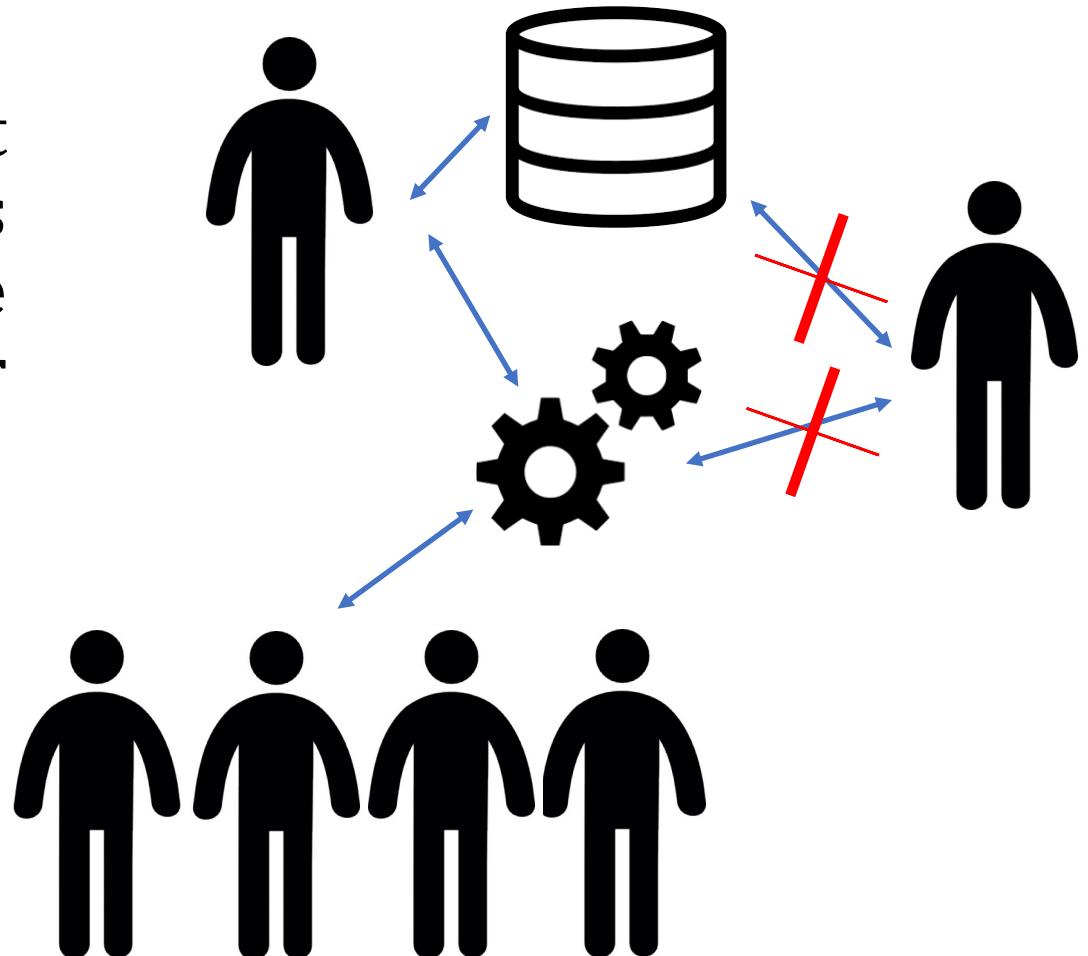
1. Identity and Access Management



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





Google Cloud

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



Google Cloud

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.

| Type | Member | Name | Role |
|------|---|---|---------------------------------|
| | 948170062628-compute@developer.gserviceaccount.com | Compute Engine default service account | Editor |
| | 948170062628@cloudservices.gserviceaccount.com | Google APIs Service Agent | Editor |
| | abstract-pier-277014@appspot.gserviceaccount.com | App Engine default service account | Editor |
| | dey.saurabh84@gmail.com | Saurabh Dey | Owner |
| | service-948170062628@compute-system.iam.gserviceaccount.com | Compute Engine Service Agent | Compute Engine Service Agent |
| | service-948170062628@container-engine-robot.iam.gserviceaccount.com | Kubernetes Engine Service Agent | Kubernetes Engine Service Agent |
| | service-948170062628@containerregistry.iam.gserviceaccount.com | Google Container Registry Service Agent | Editor |
| | service-948170062628@gcf-admin-bot.iam.gserviceaccount.com | Google Cloud Functions Service Agent | Cloud Functions Service Agent |
| | service-948170062628@serverless-robot-prod.iam.gserviceaccount.com | Google Cloud Run Service Agent | Cloud Run Service Agent |

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.

The screenshot shows the Google Cloud Platform IAM & Admin interface. On the left, there's a sidebar with various options like IAM, Identity & Organisation, Policy troubleshooter, Organisation Policies, Quotas, Service Accounts, Labels, Settings, Privacy & Security, Cryptographic Keys, Identity-Aware Proxy, Roles, Audit Logs, and Groups. The main area is titled "Permissions for project 5410 - General" and lists members with their names and corresponding service accounts. At the top right, there are "ADD" and "REMOVE" buttons. Below the table, there are tabs for "MEMBERS" and "ROLES".

| Type | Member | Name |
|---|---|---|
| Compute Engine default service account | 948170062628-compute@developer.gserviceaccount.com | Compute Engine default service account |
| Google APIs Service Agent | 948170062628@cloudservices.gserviceaccount.com | Google APIs Service Agent |
| App Engine default service account | abstract-pier-277014.appspot.gserviceaccount.com | App Engine default service account |
| Saurabh Dey | dey.saurabh84@gmail.com | Saurabh Dey |
| Compute Engine Service Agent | service-948170062628@compute-system.iam.gserviceaccount.com | Compute Engine Service Agent |
| Kubernetes Engine Service Agent | service-948170062628@container-engine-robot.iam.gserviceaccount.com | Kubernetes Engine Service Agent |
| Google Container Registry Service Agent | service-948170062628@containerregistry.iam.gserviceaccount.com | Google Container Registry Service Agent |
| Google Cloud Functions Service Agent | service-948170062628@gcf-admin-robot.iam.gserviceaccount.com | Google Cloud Functions Service Agent |
| Google Cloud Run Service Agent | service-948170062628@serverless-robot-prod.iam.gserviceaccount.com | Google Cloud Run Service Agent |

This screenshot shows the "Add members to 5410 - General" dialog. It has a search bar at the top and a section for "New members" where "srbh.dey@gmail.com" is listed. Below that is a "Select a role" dropdown menu. The "Project" dropdown is set to "Android Management User". Other visible roles include "Access Approval", "Access Context Ma...", "Actions", "AI Notebooks", "Android Management", "Apigee", and "Announcements". A tooltip for "Android Management User" says "Full access to manage devices".

This screenshot shows the "Edit condition" dialog. It includes fields for "Title" and "Description". Below these are tabs for "CONDITION BUILDER" and "CONDITION EDITOR", with "CONDITION BUILDER" currently selected. Under "CONDITION BUILDER", there's a "Condition type" dropdown with "Time" and "Resource" options, each followed by arrows and "Schedule" and "Expiring access" options. At the bottom are "SAVE" and "CANCEL" buttons.



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.

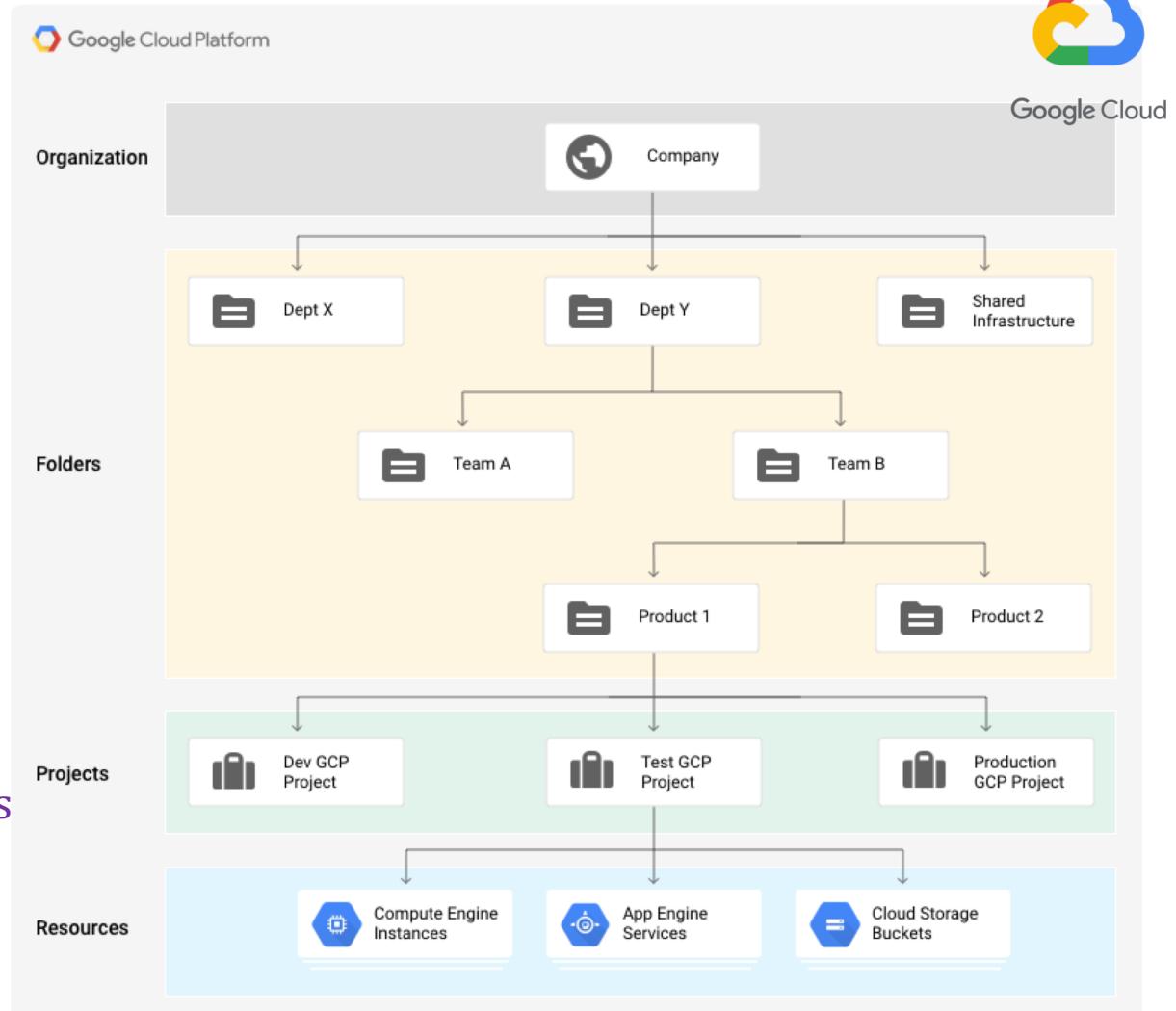
Access Levels

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.

The screenshot shows the Google Cloud Platform's 'Manage resources' interface. At the top, there is a blue header bar with the 'Google Cloud Platform' logo, a search bar, and navigation links for 'Manage resources', '+ CREATE PROJECT', and 'DELETE'. Below the header is a 'Filter tree' button. The main area is a table titled 'Projects' with columns: Name, ID, Status, Charges, Labels, and Actions. The table contains three rows:

| Name | ID | Status | Charges | Labels | Actions |
|------------------|-----------------------|--------|---------|--------|---------|
| No organisation | 0 | | | | ⋮ |
| 5410 - General | abstract-pier-277014 | | | | ⋮ |
| My First Project | friendly-slate-269615 | | | | ⋮ |

At the bottom of the table, it says '0 RESOURCES PENDING DELETION'.





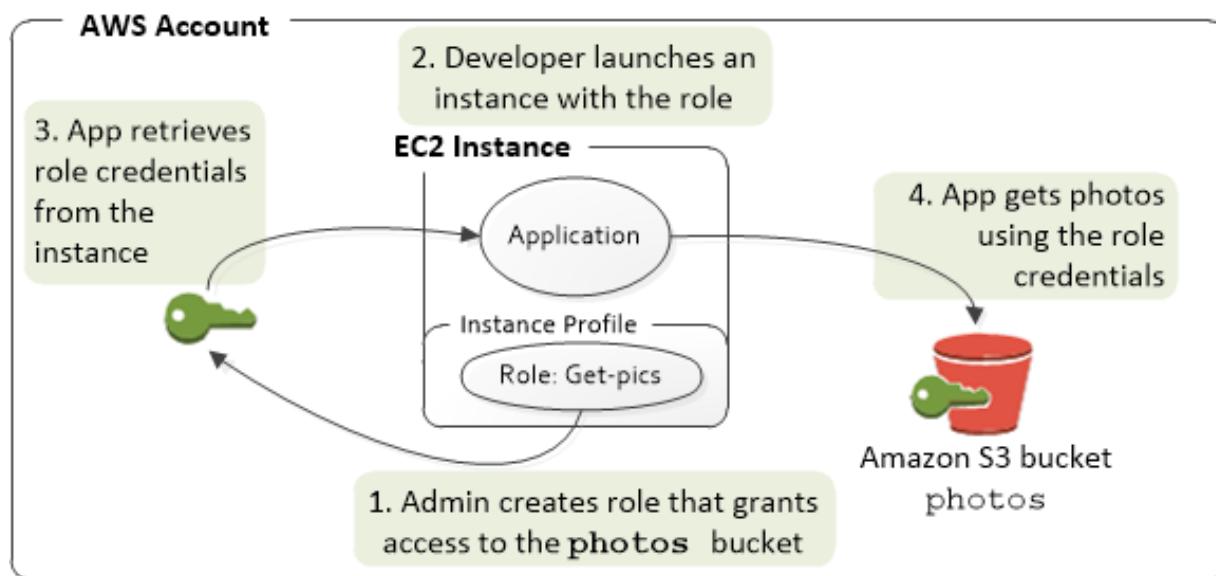
AWS IAM

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.



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

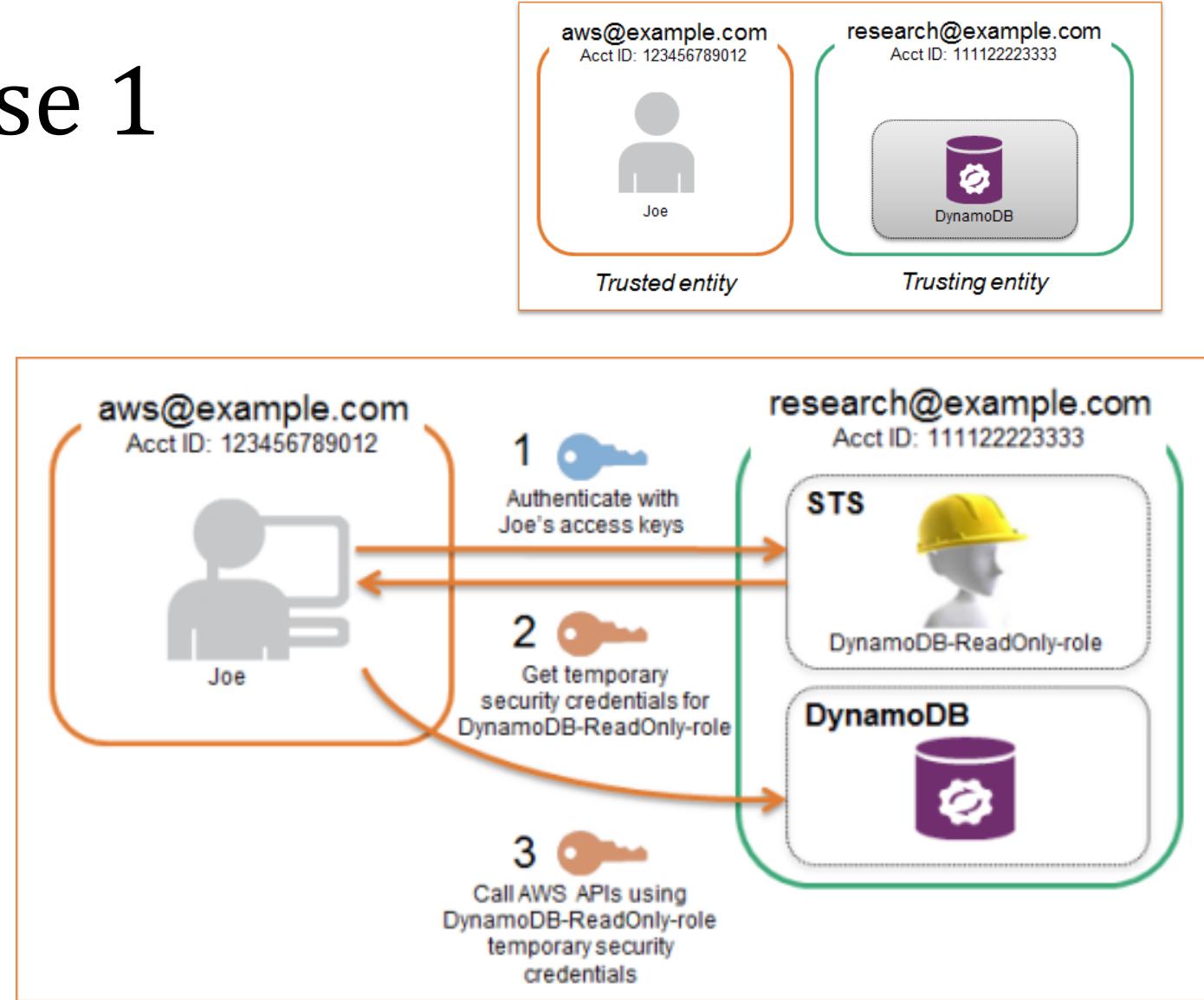
- Collection of IAM users that share the same access permission

IAM Roles

- An IAM user can assume a role to temporarily take on different permissions for a specific task.

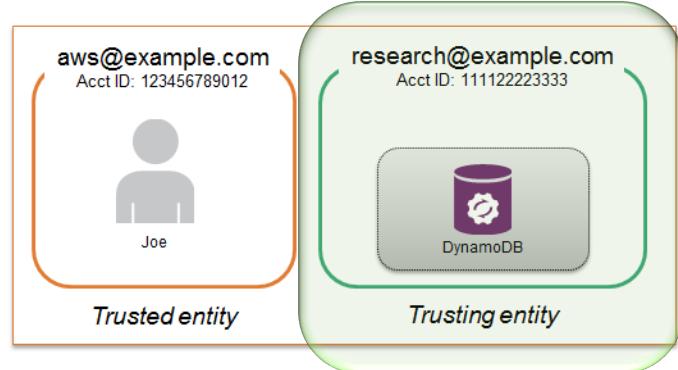
AWS IAM – Use Case 1

- 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)



The screenshot shows the first step of the IAM role creation wizard:

- Step: CONFIGURE ROLE
- Role Name: myRole (highlighted with a red arrow from the diagram)
- Maximum 64 characters. Use alphanumeric and '+,.,@-' characters
- Continue button

DynamoDB-ReadOnly-role

1

The screenshot shows the second step of the IAM role creation wizard:

- Step: SELECT ROLE TYPE
- Role Type: Role for Cross-Account Access (selected, highlighted with a red circle)
- Provide access between AWS accounts you own (Select button)
- Allows IAM users from one of your other AWS accounts to access this account.
- Allows IAM users from a 3rd party AWS account to access this account. (Select button)
- Role for Identity Provider Access

2

The screenshot shows the third step of the IAM role creation wizard:

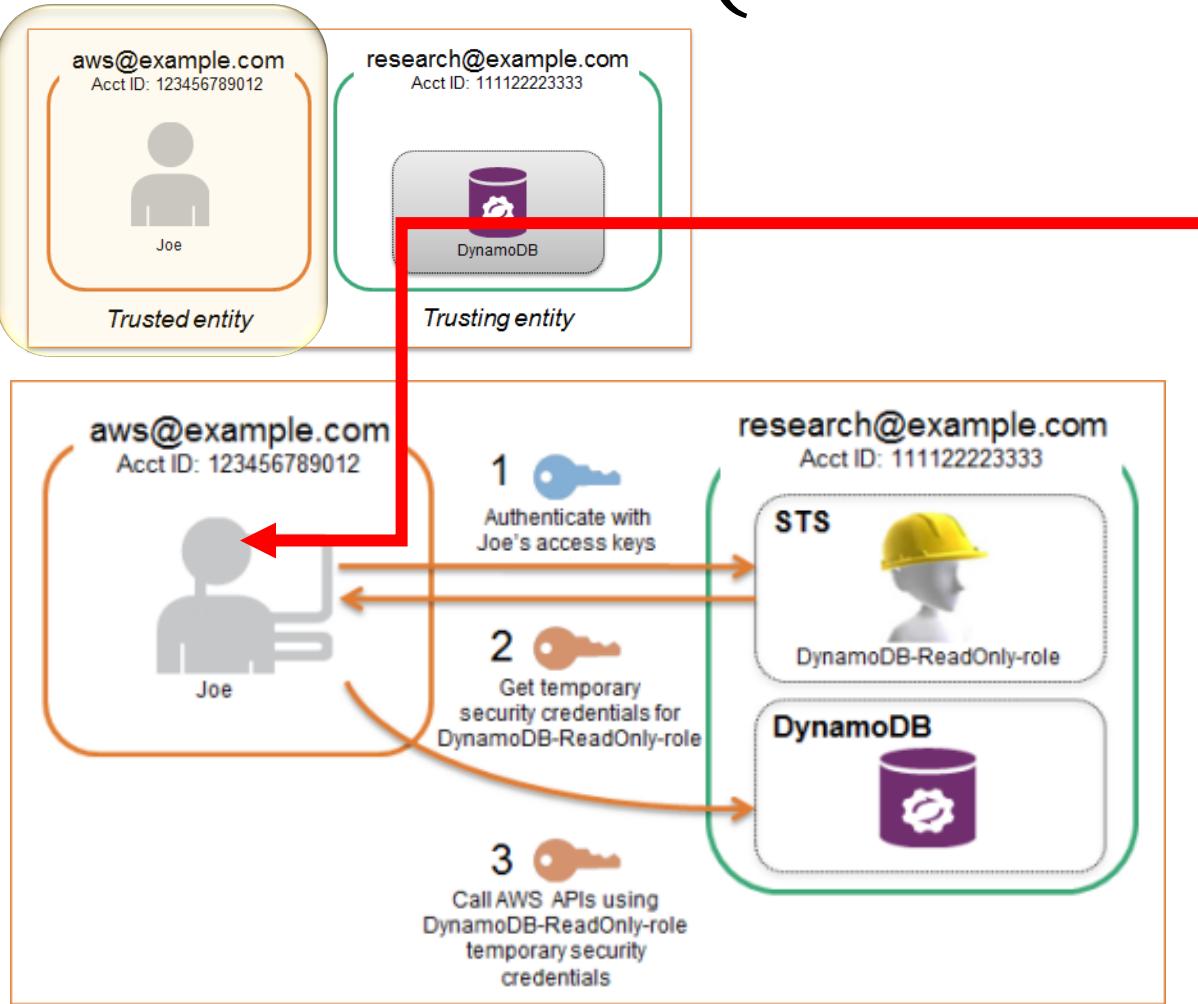
- Step: ESTABLISH TRUST
- Enter the ID of the AWS account whose IAM users will be able to access this account.
- Account ID: (highlighted with a red arrow from the diagram)
- Back button
- Continue button

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

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

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation sidebar with various options like Dashboard, Groups, Users, Policies, Identity providers, Account settings, and more. A large red arrow points from the text "Click to create role" towards the "Create role" button in the center of the page. The main content area is titled "Roles" and contains sections about what IAM roles are, additional resources, and a table listing existing roles. The "Create role" button is highlighted with a red oval.

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

| Role name | Trusted entities | Last activity |
|-----------------------------------|--|---------------|
| AWSServiceRoleForAWSCloud9 | AWS service: cloud9 (Service-Linked role) | None |
| AWSServiceRoleForCloudWatchEvents | AWS service: events (Service-Linked role) | None |
| AWSServiceRoleForElastiCache | AWS service: elasticache (Service-Linked role) | None |
| AWSServiceRoleForLexBots | AWS service: lex (Service-Linked role) | 3 days |
| AWSServiceRoleForOrganizations | AWS service: organizations (Service-Linked r...) | None |
| AWSServiceRoleForSupport | AWS service: support (Service-Linked role) | None |
| AWSServiceRoleForTrustedAdvisor | AWS service: trustedadvisor (Service-Linked ...) | None |

Example – IAM Role creation (2 – 6)

Selecting a default use case

console.aws.amazon.com/iam/home#region=us-east-1#/roles\$new?step=type

AWS Services Resource Groups

Create role

Select type of trusted entity

1 2 3 4

AWS service EC2, Lambda and others

Another AWS account Belonging to you or 3rd party

Web identity Cognito or any OpenID provider

SAML 2.0 federation Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf

Or select a service to view its use cases

| | | | | |
|-------------------------------|------------------------|---------------------------|------------------|-----------------|
| API Gateway | CodeGuru | ElasticCache | Kinesis | RoboMaker |
| AWS Backup | CodeStar Notifications | Elastic Beanstalk | Lake Formation | S3 |
| AWS Chatbot | Comprehend | Elastic Container Service | Lambda | SMS |
| AWS Support | Config | Elastic Transcoder | Lex | SNS |
| Amplify | Connect | Elastic Load Balancing | License Manager | SWF |
| AppStream 2.0 | DMS | Forecast | Machine Learning | SageMaker |
| AppSync | Data Lifecycle Manager | Global Accelerator | Macie | Security Hub |
| Application Auto Scaling | Data Pipeline | Glue | MediaConvert | Service Catalog |
| Application Discovery Service | DataSync | Greengrass | Migration Hub | Step Functions |
| Batch | DeepLens | GuardDuty | OpsWorks | Storage Gateway |
| | Directory Service | GuardDuty | Personalize | Systems Manager |

* Required Cancel Next: Permissions

The screenshot shows the 'Create role' wizard step 1: 'Select type of trusted entity'. It lists four options: 'AWS service' (selected), 'Another AWS account', 'Web identity', and 'SAML 2.0 federation'. Below this, it says 'Allows AWS services to perform actions on your behalf.' A red arrow points from the text 'Selecting a default use case' to the 'Lambda' use case option under 'Common use cases'. The 'Lambda' option is highlighted with a red oval. At the bottom, there are buttons for 'Cancel' and 'Next: Permissions'.

Example – IAM Role creation (3 – 6)

Selecting AdministratorAccess

console.aws.amazon.com/iam/home?region=us-east-1#/roles/new?step=permissions&commonUseCase=Lambda%2BLambda&selectedUseCase=Lambda

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies ▾ Search Showing 661 results

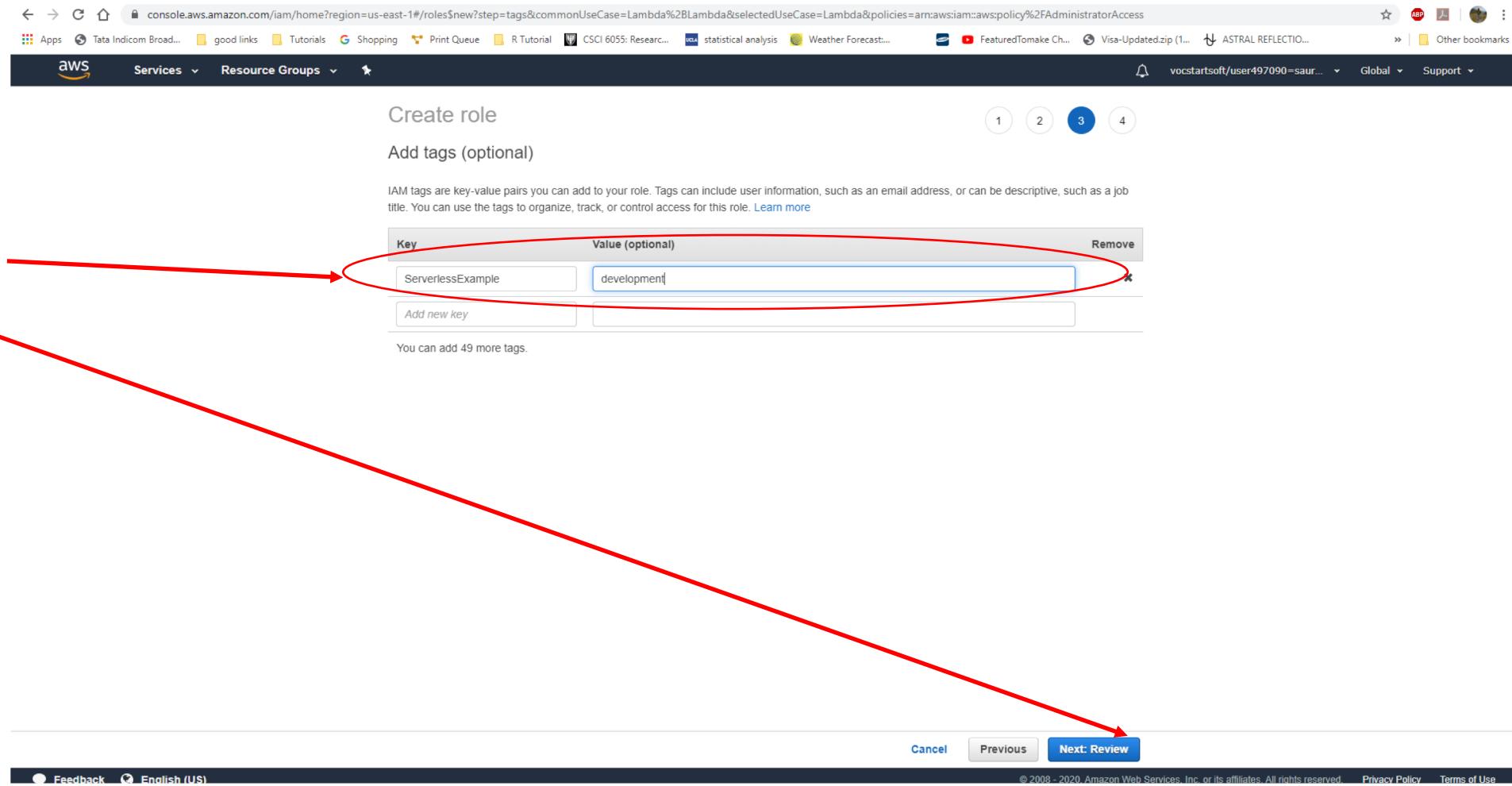
| Policy name ▾ | Used as |
|--|---------|
| <input type="checkbox"/> AccessAnalyzerServiceRolePolicy | None |
| <input checked="" type="checkbox"/> AdministratorAccess | None |
| <input type="checkbox"/> AlexaForBusinessDeviceSetup | None |
| <input type="checkbox"/> AlexaForBusinessFullAccess | None |
| <input type="checkbox"/> AlexaForBusinessGatewayExecution | None |
| <input type="checkbox"/> AlexaForBusinessNetworkProfileServicePolicy | None |
| <input type="checkbox"/> AlexaForBusinessPolyDelegatedAccessPolicy | None |
| <input type="checkbox"/> AlexaForBusinessReadOnlyAccess | None |

Set permissions boundary

* Required Cancel Previous Next: Tags

Feedback English (US) © 2006–2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Example – IAM Role creation (4 – 6)



console.aws.amazon.com/iam/home?region=us-east-1#/roles\$new?step=tags&commonUseCase=Lambda%2BLambda&selectedUseCase=Lambda&policies=arn:aws:iam::aws:policy%2FAdministratorAccess

Services Resource Groups

Create role

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

| Key | Value (optional) | Remove |
|-------------------|------------------|--------|
| ServerlessExample | development | X |

Add new key

You can add 49 more tags.

Cancel Previous Next: Review

Feedback English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Example – IAM Role creation (5 – 6)

Adding role name

Helps in organizing roles

Create Role

Create role

Review

Provide the required information below and review this role before you create it.

Role name* call_Lambda_forServerless

Use alphanumeric and '+-=,@-_` characters. Maximum 64 characters

Role description Allows Lambda functions to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+-=,@-_` characters.

Trusted entities AWS service: lambda.amazonaws.com

Policies AdministratorAccess

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

| Key | Value |
|-------------------|-------------|
| ServerlessExample | development |

* Required

Cancel Previous Create role

Example – IAM Role creation (6 – 6)

New role

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, a sidebar menu is open under the 'Identity and Access Management (IAM)' section, with 'Roles' selected. A red arrow points from the text 'New role' to the 'call_lambda_forServerless' role listed in the main content area. The main content area displays a table of existing roles, showing columns for 'Role name', 'Trusted entities', and 'Last activity'. The 'call_lambda_forServerless' role is highlighted with a red oval.

| Role name | Trusted entities | Last activity |
|-----------------------------------|--|----------------------|
| AWSServiceRoleForAWSCloud9 | AWS service: cloud9 (Service-Linked role) | None |
| AWSServiceRoleForCloudWatchEvents | AWS service: events (Service-Linked role) | None |
| AWSServiceRoleForElastiCache | AWS service: elasticcache (Service-Linked role) | None |
| AWSServiceRoleForLexBots | AWS service: lex (Service-Linked role) | 3 days |
| AWSServiceRoleForOrganizations | AWS service: organizations (Service-Linked r...) | None |
| AWSServiceRoleForSupport | AWS service: support (Service-Linked role) | None |
| AWSServiceRoleForTrustedAdvisor | AWS service: trustedadvisor (Service-Linked ...) | None |
| call_lambda_forServerless | AWS service: lambda | None |
| EMR_AutoScaling_DefaultRole | AWS service: elasticmapreduce and 1 more | None |
| EMR_DefaultRole | AWS service: elasticmapreduce | None |
| EMR_EC2_DefaultRole | AWS service: ec2 | None |
| robomaker_students | AWS service: rekognition and 3 more | None |
| vocareum | Account: 766550594530 | You need permissions |
| vocstartsoft | Account: 766550594530 | You need permissions |

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?

