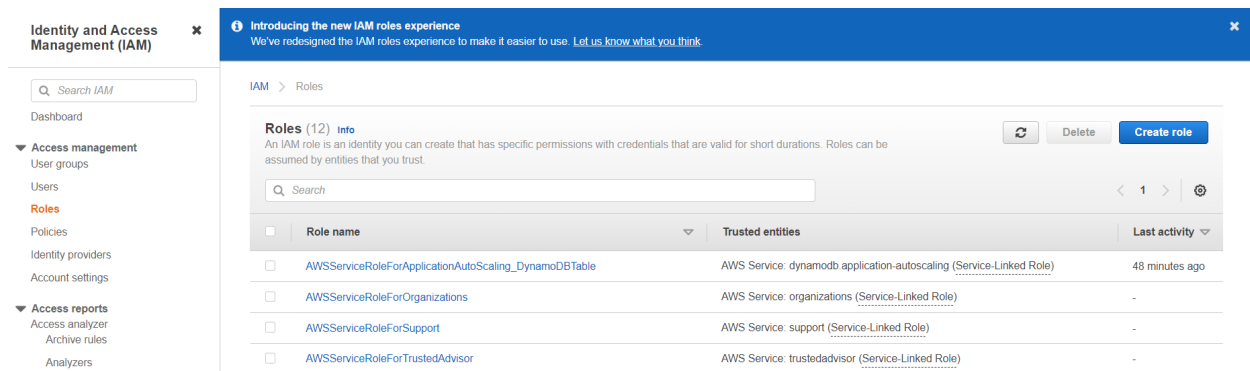
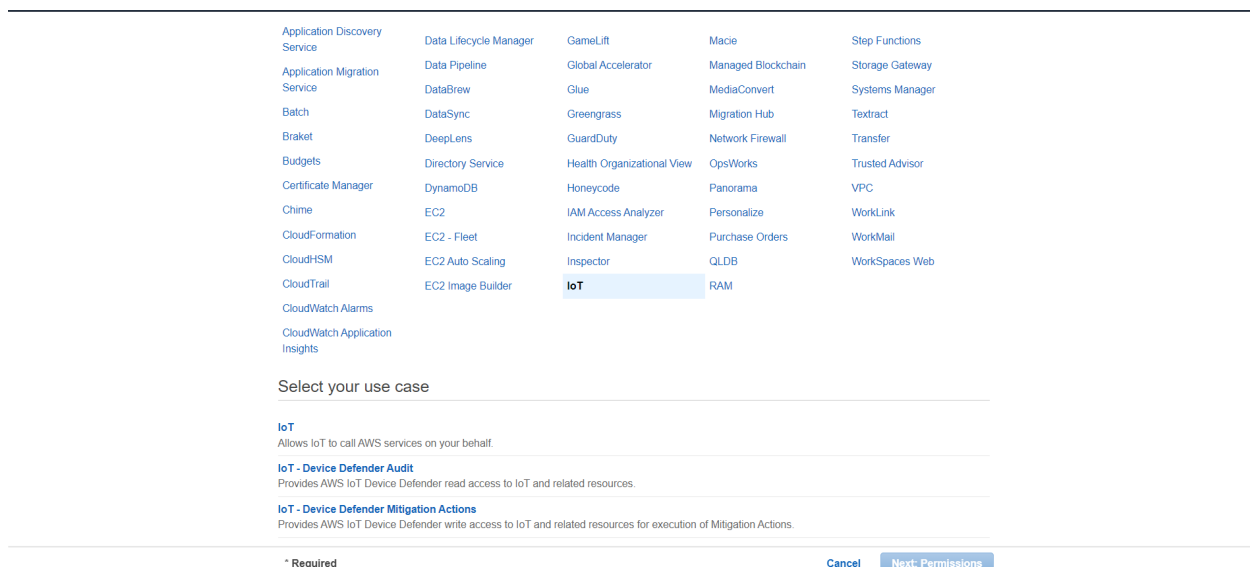


To understand the role creation associated with multiple resources and how to use it, please follow the below mentioned steps:

- 1. IoT Core related IAM role creation:** In this we are going to see how we can create the roles that are used in IoT core to create different rules for DynamoDB or Kinesis streams etc. Please follow the below mentioned steps
 - a. Goto IAM role as mentioned below:



- b. Click on Create role and it will take you to the next page. On this page look for IoT and allow all the services as mentioned in the following image:



- c. Click on Next and it will take you to the next page as mentioned below:

Create role

1 2 3 4

▼ Attached permissions policies

The type of role that you selected requires the following policy

Filter policies ▼

Q Search

Showing 3 results

Policy name ▼	Used as	Description
▶ AWSIoTLogging	Permissions policy (1)	Allows creation of Amazon CloudWatch Log gr...
▶ AWSIoTRuleActions	Permissions policy (3)	Allows access to all AWS services supported I...
▶ AWSIoTThingsRegistration	Permissions policy (1)	This policy allows users to register things at bu...

▶ Set permissions boundary

* Required

Cancel Previous Next: Tags

- Click on Next and assign the name for your role and click on Create to complete the role creation process.
- Once the role is created and you want to add additional permission for Kinesis and other resources, you can do that.
- Once the role is available go back to the rule creation page on IoT Core and choose the right resources for rule creation and this role will be available for you to choose.

AWS IoT

Monitor

Activity

▶ Connect

▶ Manage

▶ Fleet Hub

▶ Greengrass

▶ Wireless connectivity

▶ Secure

▶ Defend

▼ Act

Rules

Destinations

▶ Test

Software

Settings

Learn

Feature spotlight

Documentation

Configure action

Send a message to an Amazon Kinesis Stream

This will send the message to an Amazon Kinesis Stream.

*Stream name

Choose a resource

Create a new resource

*Partition key

deviceid

Choose or create a role to grant AWS IoT access to perform this action.

No role selected

Refresh

Close

Q Search for IAM roles

test2

Select

- Select the role and click on add actions to complete the rule creation process.


2. **Kinesis Delivery stream creation:** Please follow the below steps to create the delivery stream in the account.
 - a. Once you reach the delivery stream creation, make sure that you have created kinesis stream and S3 bucket.
 - b. Click on Advanced Setting as similar to below:

▼ **Advanced settings**

Server-side encryption disabled; error logging enabled; IAM role KinesisFirehoseServiceRole-KDS-S3-sVhSr-us-east-1-1643780312893; no tags.

Server-side encryption [Info](#)

You can use AWS Key Management Service (KMS) to create and manage Customer Master Keys (CMK) and to control the use of encryption across a wide range of AWS services in your applications.



Server-side encryption (SSE)

To enable SSE for the delivery stream, view the data stream selected above, and enable SSE on it. If you choose Direct PUT or other data sources for your delivery stream, you can enable SSE on the delivery stream directly.

Amazon CloudWatch error logging [Info](#)

Choose Enabled if you want Kinesis Data Firehose to log record delivery errors to CloudWatch Logs.

☐ Disabled

☒ Enabled

Permissions [Info](#)

Kinesis Data Firehose uses this IAM role for all the permissions that the delivery stream needs. To specify different roles for the different permissions, use the API or the CLI.

☒ Create or update IAM role **KinesisFirehoseServiceRole-KDS-S3-sVhSr-us-east-1-1643780312893**

Creates a new role or updates an existing one and adds the required policies to it, and enables Kinesis Data Firehose to assume it.

☐ Choose existing IAM role

The role that you choose must have policies that include the permissions that Kinesis Data Firehose needs.

Tags [Info](#)

You can add tags to organize your AWS resources, track costs, and control access.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel **Create delivery stream**

- c. Click on Create with default operation and this operation will not allow you to create the stream. However, as a next step, you can choose an existing IAM role and the role that was created will be available as mentioned below.

▼ Advanced settings

Server-side encryption disabled; error logging enabled; IAM role not selected; no tags.

Server-side encryption [Info](#)

You can use AWS Key Management Service (KMS) to create and manage Customer Master Keys (CMK) and to control the use of encryption across a wide range of AWS services in your applications.



Server-side encryption (SSE)

To enable SSE for the delivery stream, view the data stream selected above, and enable SSE on it. If you choose Direct PUT or other data sources for your delivery stream, you can enable SSE on the delivery stream directly.

Amazon CloudWatch error logging [Info](#)

Choose Enabled if you want Kinesis Data Firehose to log record delivery errors to CloudWatch Logs.

- ☐ Disabled
- ☒ Enabled


Permissions [Info](#)

Kinesis Data Firehose uses this IAM role for all the permissions that the delivery stream needs. To specify different roles for the different permissions, use the API or the CLI.

- ☐ Create or update IAM role **KinesisFirehoseServiceRole-KDS-S3-sVhSr-us-east-1-1643780312893**
Creates a new role or updates an existing one and adds the required policies to it, and enables Kinesis Data Firehose to assume it.
- ☒ Choose existing IAM role
The role that you choose must have policies that include the permissions that Kinesis Data Firehose needs.

Existing IAM roles

Only IAM roles with the required trust policy  are available for selection.



KinesisFirehoseServiceRole-KDS-S3-hjoYY-us-east-1-1643772435241
KinesisFirehoseServiceRole-KDS-S3-sVhSr-us-east-1-1643780312893

Add new tag

You can add up to 50 more tags.

- d. Go to the IAM page and search for the role that was created, and add the policies at least for S3 and Kinesis as shown below.

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles**
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analysers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Q Search IAM

AWS account ID: 430773705995

Summary

Role ARN: arn:aws:iam::430773705995:role/service-role/KinesisFirehoseServiceRole-KDS-S3-vHsr-us-east-1-1643780312893

Role description: Edit

Instance Profile ARNs:

Path: /service-role/

Creation time: 2022-02-02 11:15 UTC+0530

Last activity: Not accessed in the tracking period

Maximum session duration: 1 hour Edit

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Permissions policies (2 policies applied)

Attach policies Add inline policy

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy
AmazonKinesisFullAccess	AWS managed policy

Permissions boundary (not set)

- e. Go back and choose the role on kinesis delivery stream and click on the create delivery stream and the operation should succeed.

3. **Lambda related IAM role creation:** In this section we are going to create the roles for lambda functions. This is mostly useful at the places where you are using lambda functions. Please follow the below steps to create the roles

- a. Goto Lambda function page similar to below:

☒ Author from scratch
 Start with a simple Hello World example.

☐ Use a blueprint
 Build a Lambda application from sample code and configuration presets for common use cases.

☐ Container image
 Select a container image to deploy for your function.

☐ Browse serverless app repository
 Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

Function name
 Enter a name that describes the purpose of your function.

 Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
 Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Architecture Info
 Choose the instruction set architecture you want for your function code.
☒ x86_64
☐ arm64

Permissions Info
 By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.
[Change default execution role](#)

Advanced settings

Cancel Create function

- b. Enter the function name and runtime as python for this. Under the permissions; it will look as below:

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime [Info](#)
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Node.js 14.x

Architecture [Info](#)
Choose the instruction set architecture you want for your function code.

☒ x86_64
☐ arm64

Permissions [Info](#)
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ Change default execution role

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

☒ Create a new role with basic Lambda permissions
☐ Use an existing role
☐ Create a new role from AWS policy templates

ⓘ Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in this role.

Lambda will create an execution role named <myFunctionName>-role-27ucma0, with permission to upload logs to Amazon CloudWatch Logs.

► Advanced settings

Cancel **Create function**

- Below the execution role there is a link available to access IAM console and role creation. Click on this link and it will take you to the IAM page.
- Add the policies for different services that you want to access through your lambda function such as SNS, S3, DynamoDB, Kinesis etc.
- Once the role is created, go back to this page and click on Use and existing role option available.
- Newly created roles will be available for you to configure. Choose it and click on the create function. This should create the role for you without any issue.