Week 12: Homework 2: Project: Chapter 7: Building Predictive Analytics For AWS IoT

https://hc.labnet.sfbu.edu/~henry/npu/classes//iot/learning_aws_iot/slide/exercise_learning_aws_iot.html

Q7 ==> Project: Chapter 7: Building Predictive Analytics For AWS IoT

7. Project: Chapter 7: Building Predictive Analytics For AWS IoT
   ○ Step 1: Prepare Raspberry Pi emulator + VirtualBox + Sense HAT Emulator
      ○ References
         ▪ DHT22 for Raspberry Pi
            ○ Adafruit_Python_DHT
         ▪ Raspberry Pi Tutorial: How to Use the DHT-22
   ○ Step 2: Continue the proces of Building Predictive Analytics For AWS IoT
   ○ Step 3: Update your portfolio about this project
   ○ Step 4: Submit a PDF file document showing the procedure as part of the homework answers.
   ○ Step 5: Submit the URL of your GitHub webpage as part of the homework answers.
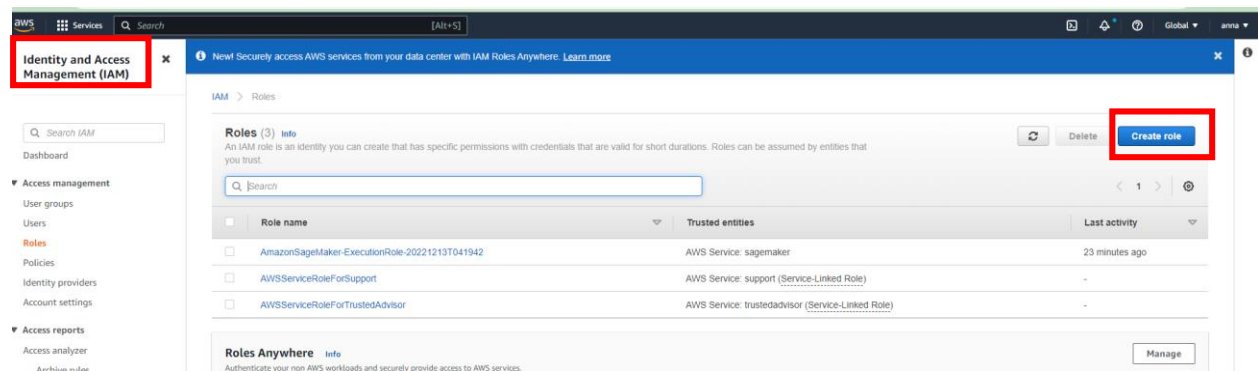   ▪ GitHub directory structure

```
IoT
    AWS IoT + Raspberry Pi Emulator + Sensor HAT Emulator + Predictive Analysis
```

Building Predictive Analysis in AWS

Machine learning is unavailable anymore, we will use SageMaker canvas to build model.

1. Create an AWS IAM role

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

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.

Use cases for other AWS services:

Choose a service to view use case ▼

Cancel   Next

Select trusted entity Info

Trusted entity type

AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

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.

Use cases for other AWS services:

SageMaker ▼

● SageMaker - Execution
Allows SageMaker notebook instances, training jobs, and models to access S3, ECR, and CloudWatch on your behalf.

Cancel   Next

Add permissions policies for the role:

Add permissions Info

Permissions policies (1) Info
The type of role that you selected requires the following policy.

Policy name ⬀	▼	Type ▼	Attached entities		▼
⊞ 📦 AmazonSageMaker…		AWS m…	1		

▼ **Set permissions boundary - *optional*** Info
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

🔘 Create role without a permissions boundary
⚪ Use a permissions boundary to control the maximum role permissions

Cancel   Previous   Next

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

ml-test

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

Description
Add a short explanation for this role.

Allows SageMaker notebook instances, training jobs, and models to access S3, ECR, and CloudWatch on your behalf.

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

Step 1: Select trusted entities   Edit

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "",
6              "Effect": "Allow",
7              "Principal": {
8                  "Service": "sagemaker.amazonaws.com"
9              },
10             "Action": "sts:AssumeRole"
11         }
12     ]
13 }
```

Step 2: Add permissions   Edit

Step 2: Add permissions

Edit

Permissions policy summary

Policy name ⧉	Type	Attached as
AmazonSageMakerFullAccess	AWS managed	Permissions policy

Tags

Add tags - *optional*   Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Cancel   Previous   **Create role**

IAM > Roles > ml-test

ml-test

Delete

Allows SageMaker notebook instances, training jobs, and models to access S3, ECR, and CloudWatch on your behalf.

Summary

Edit

Creation date
December 14, 2022, 17:13 (UTC-08:00)

Last activity
None

ARN
⧉ arn:aws:iam::124263914630:role/ml-test

Maximum session duration
1 hour

Permissions	Trust relationships	Tags	Access Advisor	Revoke sessions

Permissions policies (1)   Info

You can attach up to 10 managed policies.

⟳   Simulate   Remove   **Add permissions** ▼

🔍 Filter policies by property or policy name and press enter.

< 1 >   ⚙

	Policy name ⧉	Type	Description
⊞	AmazonSageMakerFullAccess	AWS managed	Provides full access to Amazon SageMaker via the AWS Management Console and SDK. Also provides select access to related services (e.g., S3, ECR, Clo...

Permissions boundary - (not set)   Info

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting but can be used to delegate permission management to others.

Set permissions boundary

Copy the role ARN information for later when creating SageMaker Domain to launch Canvas.
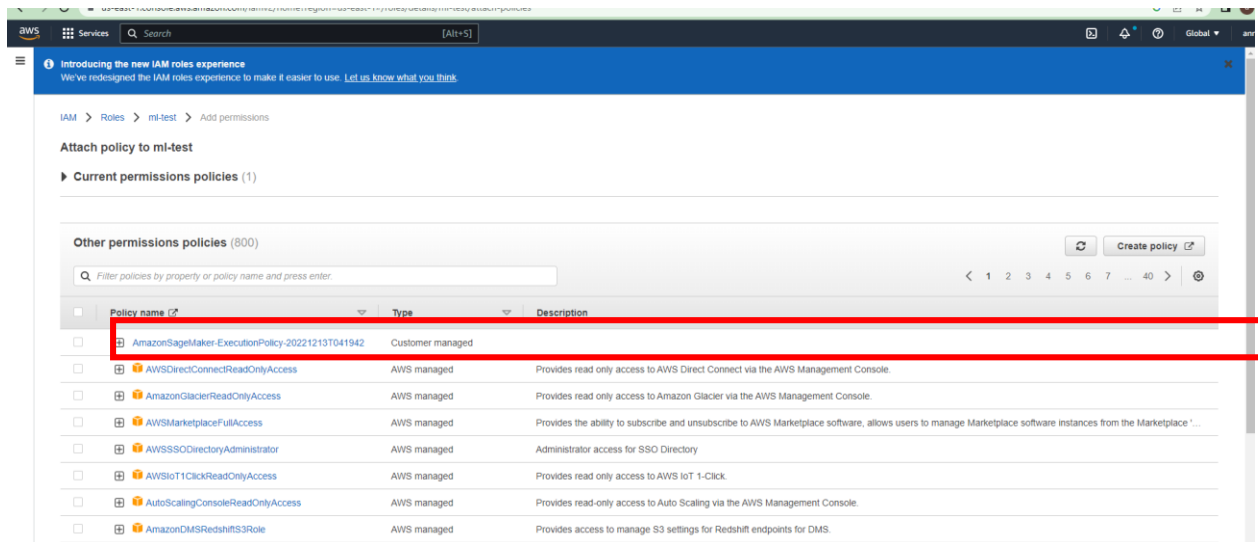
2. Create an AWS S3 bucket
   The bucket is used for store the training data for SageMaker Canvas.

Buckets are containers for data stored in S3. Learn more [↗]

General configuration

Bucket name

mydata5

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming [↗]

AWS Region

US East (N. Virginia) us-east-1   ▼

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Choose bucket

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more [↗]

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more 🔗

☐ **Block** *all* **public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

　☐ **Block public access to buckets and objects granted through** *new* **access control lists (ACLs)**
　　S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

　☐ **Block public access to buckets and objects granted through** *any* **access control lists (ACLs)**
　　S3 will ignore all ACLs that grant public access to buckets and objects.

　☐ **Block public access to buckets and objects granted through** *new* **public bucket or access point policies**
　　S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

　☐ **Block public and cross-account access to buckets and objects through** *any* **public bucket or access point policies**
　　S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠️ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more 🔗

Bucket Versioning
○ Disable
● Enable

Tags (0) - *optional*

You can use bucket tags to track storage costs and organize buckets. Learn more 🔗

No tags associated with this bucket.

Add tag

Default encryption

Automatically encrypt new objects stored in this bucket. Learn more 🔗

Server-side encryption
● Disable
○ Enable

3. Go to Amazon SageMaker, set up Canvas.
   a. Create a domain

aws Services Q Search [Alt+S]

Amazon SageMaker ✕

Getting started
    Studio
    Studio Lab ↗
    Canvas
    RStudio

Domains

SageMaker dashboard
    Images
    Lifecycle configurations
    Search
▼ JumpStart
    Foundation models NEW
▶ Governance
▶ Ground Truth
▶ Notebook
▶ Processing
▶ Training
▶ Inference
▶ Edge Manager

Amazon SageMaker

SageMaker Canvas
Generate accurate machine learning predictions — no code required

Get Started

Create an Amazon SageMaker domain to use Studio and Studio Notebooks.

Create a SageMaker domain

How it works

Amazon SageMaker Canvas - Generate accurate ML Pre... 🗐 Copy link

▶

Amazon SageMaker

Watch on ▶ YouTube

Pricing (US)

AWS Free Tier

If you are new to SageMaker you are eligible for the AWS Free Tier which includes up to 10 models with up to 1M cells of data free for the first 2 months.

Learn More ↗

Documentation

Getting Started ↗

Amazon SageMaker > Setup SageMaker Domain

Setup SageMaker Domain

Use SageMaker Domain as the central store to manage the configuration of SageMaker for your organization.

Quick setup (1 min)

Let Amazon SageMaker configure your account, and set up permissions for your SageMaker Domain.

- ⊘ Public internet access, and standard encryption
- ⊘ SageMaker Studio Integration
- ⊘ Sharable SageMaker Studio Notebooks
- ⊘ SageMaker Canvas
- ⊘ IAM Authentication

Perfect for single user domains and first time users looking to get started with SageMaker.

Domain name

Name
Domain name should be unique across the AWS account.

```
ml-test
```

User profile

Name

```
default-1671069123626
```

The name can have up to 63 characters. Valid characters: A-Z, a-z, 0-9, and - (hyphen)

Execution role
The default execution role for both users and spaces in the domain. The execution role must have the **AmazonSageMakerFullAccess** policy attached.

```
Enter a custom IAM role ARN                                          ▼
```

Custom IAM role ARN

Domain name

Name
Domain name should be unique across the AWS account.

ml-test

User profile

Name

default-1671069123626

The name can have up to 63 characters. Valid characters: A-Z, a-z, 0-9, and - (hyphen)

Execution role
The default execution role for both users and spaces in the domain. The execution role must have the **AmazonSageMakerFullAccess** policy attached.

Enter a custom IAM role ARN ▼

Custom IAM role ARN

arn:aws:iam::124263914630:role/ml-test

Create role using the role creation wizard 🔗

🔵 Enable SageMaker Canvas permissions   **Info**

Enable SageMaker Canvas permissions to attach the **AmazonSageMakerCanvasFullAccess** 🔗 policy to the default execution role. This also enables time series forecasting in Canvas and creates the AmazonSagemakerCanvasForecastRole and attaches the **AmazonSagemakerCanvasForecastRolePolicy** 🔗 policy to the role.

Cancel   **Submit**

ⓘ Jupyter Lab 3 will be the officially supported version in SageMaker Studio, while Jupyter Lab 1 will only receive security fixes from August 31, 2022.   Learn more   ✕

Amazon SageMaker > Domains > Domain: ml-test

ml-test

Domain details
Configure and manage the domain.

User profiles   Space management   Environment   Domain settings

User profiles   ⟳   Add user

A user profile represents a single user within a domain. It is the main way to reference a user for the purposes of sharing, reporting, and other user-oriented features.

🔍 Search users   < 1 >   ⚙

Name ▽	Modified on ▽	Created on ▽	
default-1671069123626	Dec 15, 2022 02:05 UTC	Dec 15, 2022 02:05 UTC	Launch ▼

b. Launch Canvas
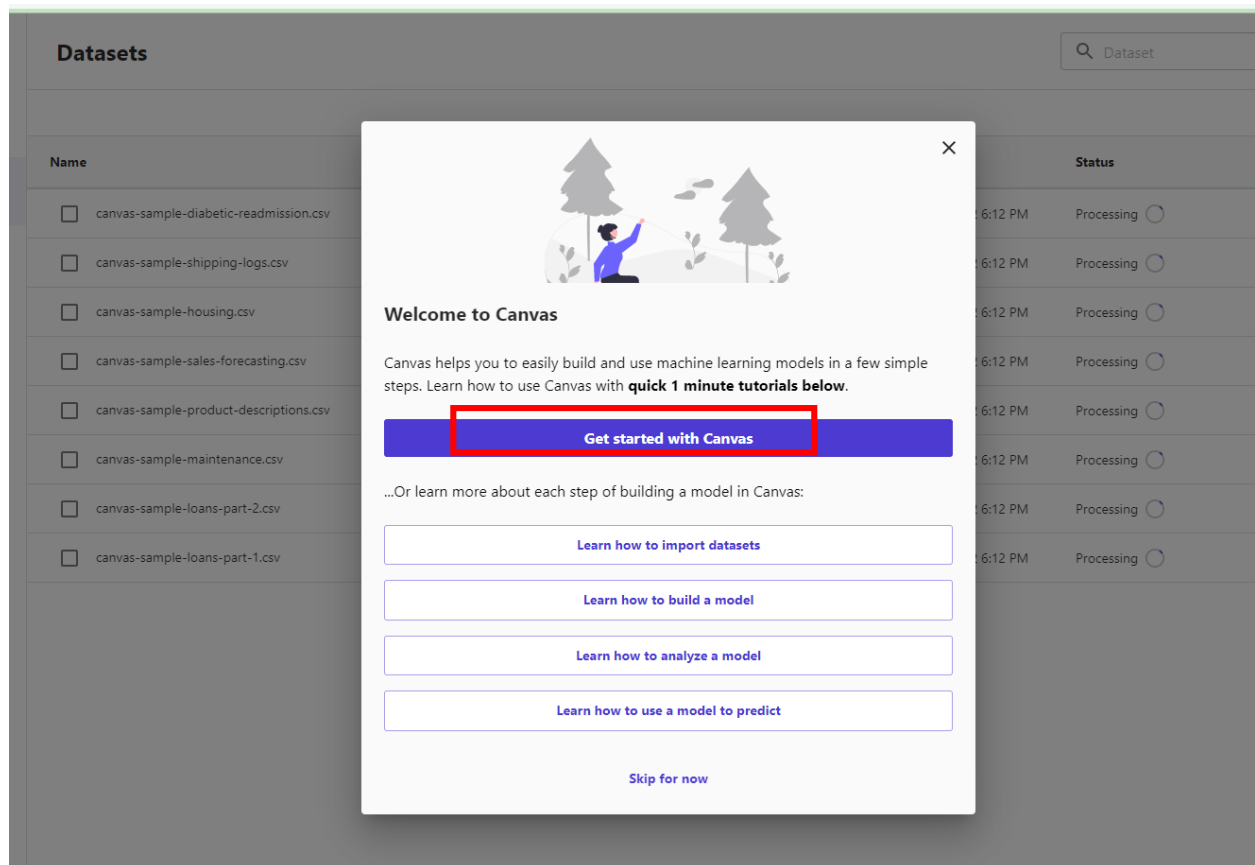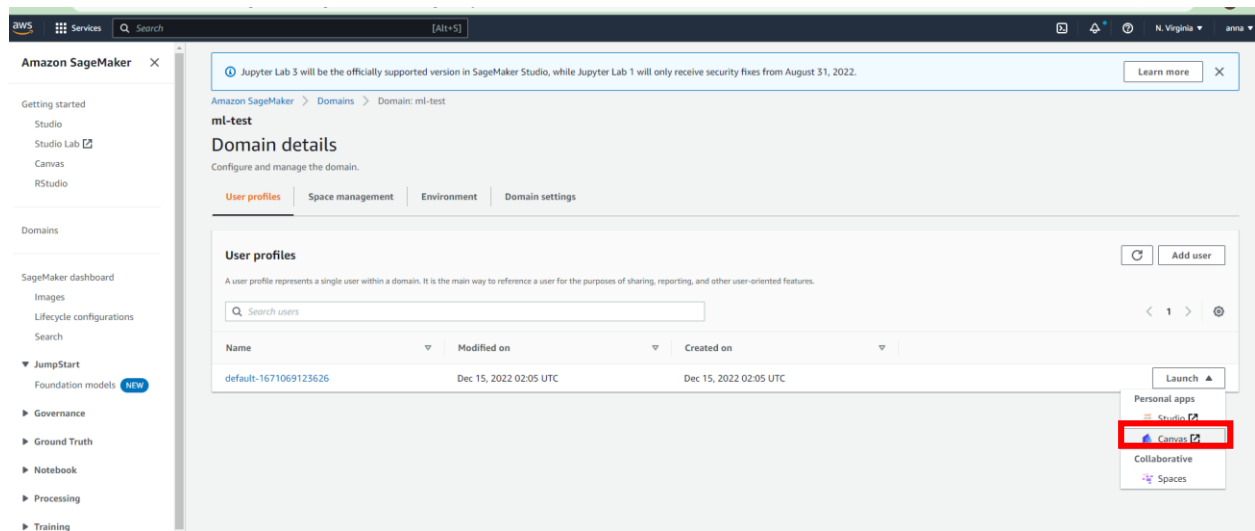
c. Select one data sample -> Create a model

Datasets

Name	Source	Columns	Rows	Cells	Created	Status
☑ canvas-sample-diabetic-readmission.csv	S3	16	1,000	16,000	12/14/2022 6:12 PM	Ready
☐ canvas-sample-shipping-logs.csv	S3	12	1,000	12,000	12/14/2022 6:12 PM	Ready
☐ canvas-sample-housing.csv	S3	10	1,000	10,000	12/14/2022 6:12 PM	Ready
☐ canvas-sample-sales-forecasting.csv	S3	5	1,000	5,000	12/14/2022 6:12 PM	Ready
☐ canvas-sample-product-descriptions.csv	S3	5	120	600	12/14/2022 6:12 PM	Ready
☐ canvas-sample-maintenance.csv	S3	9	1,000	9,000	12/14/2022 6:12 PM	Ready
☐ canvas-sample-loans-part-2.csv	S3	5	1,000	5,000	12/14/2022 6:12 PM	Ready
☐ canvas-sample-loans-part-1.csv	S3	19	1,000	19,000	12/14/2022 6:12 PM	Ready

1 selected   Create a model   Delete

Create new model   ✕

Model name

sensor-data-ml-model

Use only letters, numbers, and underscores up to 32 characters.

Cancel   **Create**

Enter target column, select one index, such as age:

d. Quick build a training model

e. Predict -> single predict

Change the values you want to test, and click update, you will see the prediction result.

Done !