



SUMMIT  
ONLINE

IMM02

# Building secure multitenant .NET core apps on AWS

Sriwantha Attanayake

Senior Specialised Solutions Architect,  
Amazon Web Services





# Multitenant SaaS

Billing

Performance

Analytics

Business model

Scalability

Security



- Authentication
- Authorisation
- Tenant onboarding
- Data partitioning & tenant isolation



# Authentication

Password security & encryption

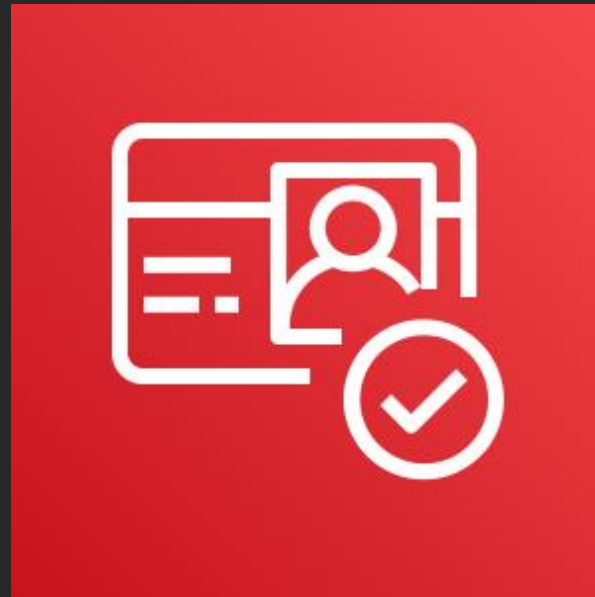
Device tracking

Emails & SMS

Federation

Users & groups  
management

Multiple  
applications



Amazon Cognito

Custom claims & claims augmentation



# AWS Management Console






## AWS services

### Find Services

You can enter names, keywords or acronyms.

🔍 *Example: Relational Database Service, database, RDS*

### ▼ Recently visited services

-  [Cognito](#)
-  [IAM](#)
-  [EC2](#)
-  [DynamoDB](#)
-  [AWS Organizations](#)

▶ [All services](#)

## Build a solution

Get started with simple wizards and automated workflows.

## Access resources on the go



Access the Management Console using the AWS Console Mobile App. [Learn more](#) 🔗

## Explore AWS

### AWS IQ

Connect with AWS Certified third-party experts for on-demand consultations and project help. [Get started](#) 🔗

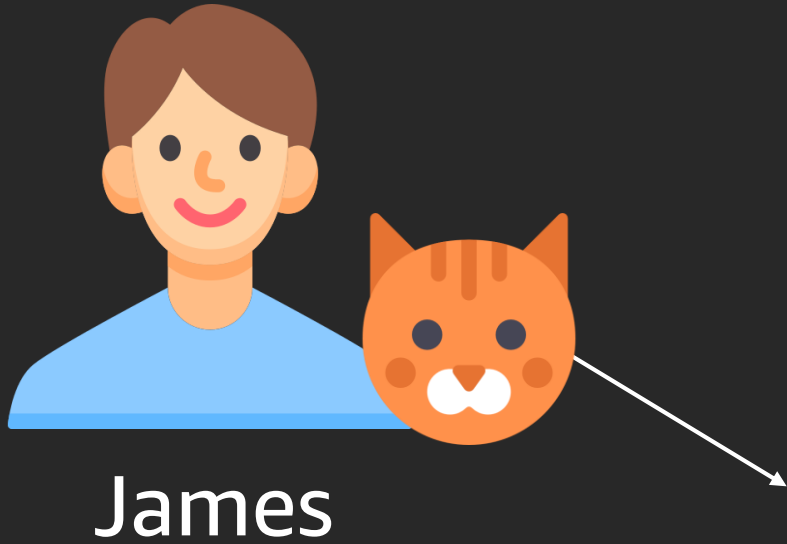
### Amazon SageMaker Studio

The first visual integrated development environment for machine learning. [Learn more](#) 🔗

### AWS Security Hub

# Authorisation

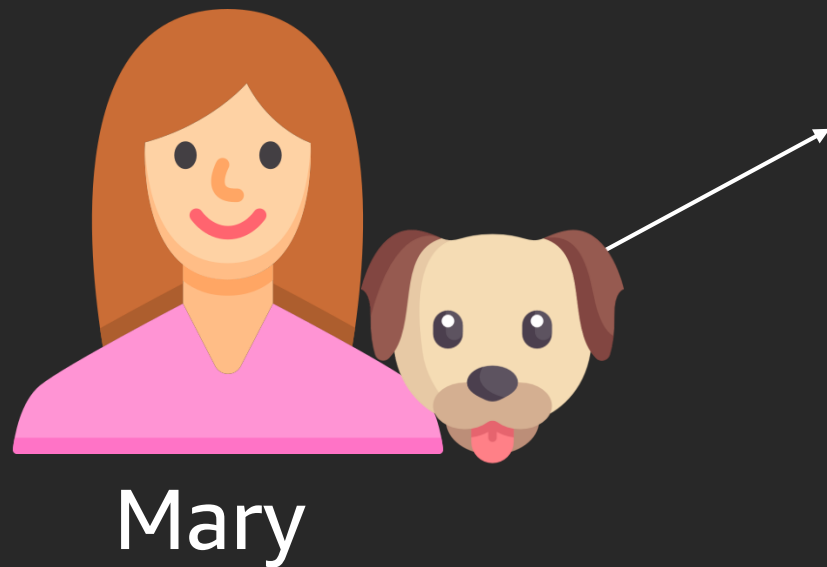




```
public class FoodController : Controller
{
    0 references
    public IActionResult Index()
    {
        return View();
    }

    [Authorize(Roles = "CatOwners")]
    0 references
    public IActionResult CatFood()
    {
        return View();
    }

    [Authorize(Roles = "DogOwners")]
    0 references
    public IActionResult DogFood()
    {
        return View();
    }
}
```





James

Feedback

English (US)

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

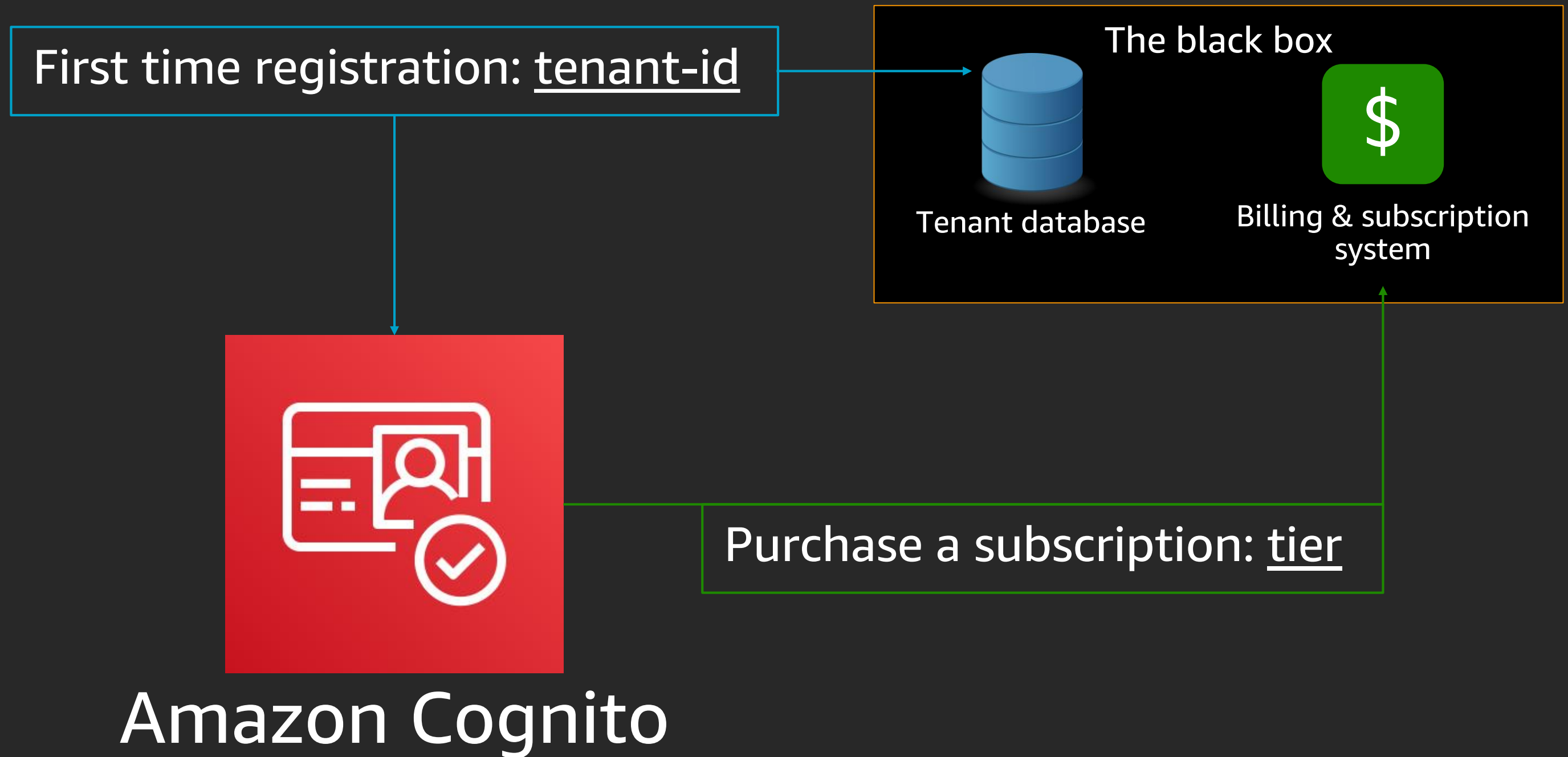
Privacy Policy

Terms of Use



# Tenant onboarding

# Custom attributes





☒ Also allow sign in with preferred username (a username that your users can change)

- ☐ **Email address or phone number** - Users can use an email address or phone number as their "username" to sign up and sign in.
- ☐ Allow email addresses
- ☐ Allow phone numbers
- ☐ Allow both email addresses and phone numbers (users can choose one)

### Which standard attributes are required?

These attributes were selected when the pool was created and cannot be changed.

Required	Attribute
<input type="checkbox"/>	address
<input type="checkbox"/>	birthdate
<input checked="" type="checkbox"/>	email
<input type="checkbox"/>	family name
<input type="checkbox"/>	gender
<input type="checkbox"/>	given name
<input type="checkbox"/>	locale
<input type="checkbox"/>	middle name
<input type="checkbox"/>	name

Required	Attribute
<input type="checkbox"/>	nickname
<input checked="" type="checkbox"/>	phone number
<input type="checkbox"/>	picture
<input type="checkbox"/>	preferred username
<input type="checkbox"/>	profile
<input type="checkbox"/>	zoneinfo
<input type="checkbox"/>	updated at
<input type="checkbox"/>	website

### Do you want to add custom attributes?

Enter the name and select the type and settings for custom attributes.

[Add custom attribute](#)

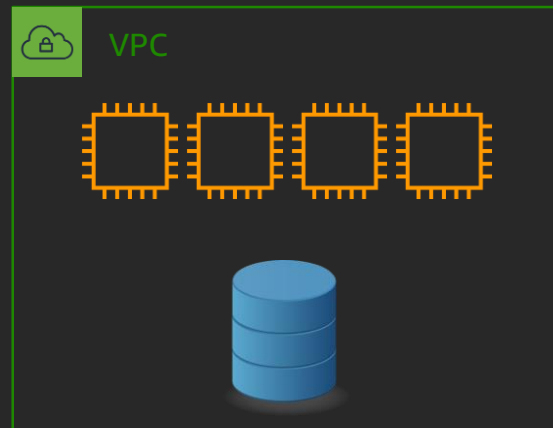
# Tenant isolation and data partitioning



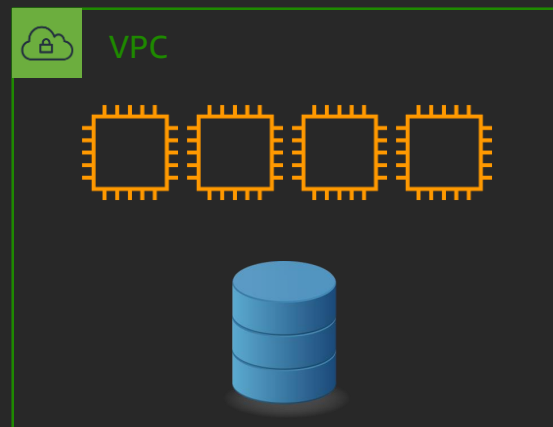
# Approach to multitenancy

## Share nothing

Tenant 1 infrastructure



Tenant 2 infrastructure



## Share some



## Share all





Use code logic

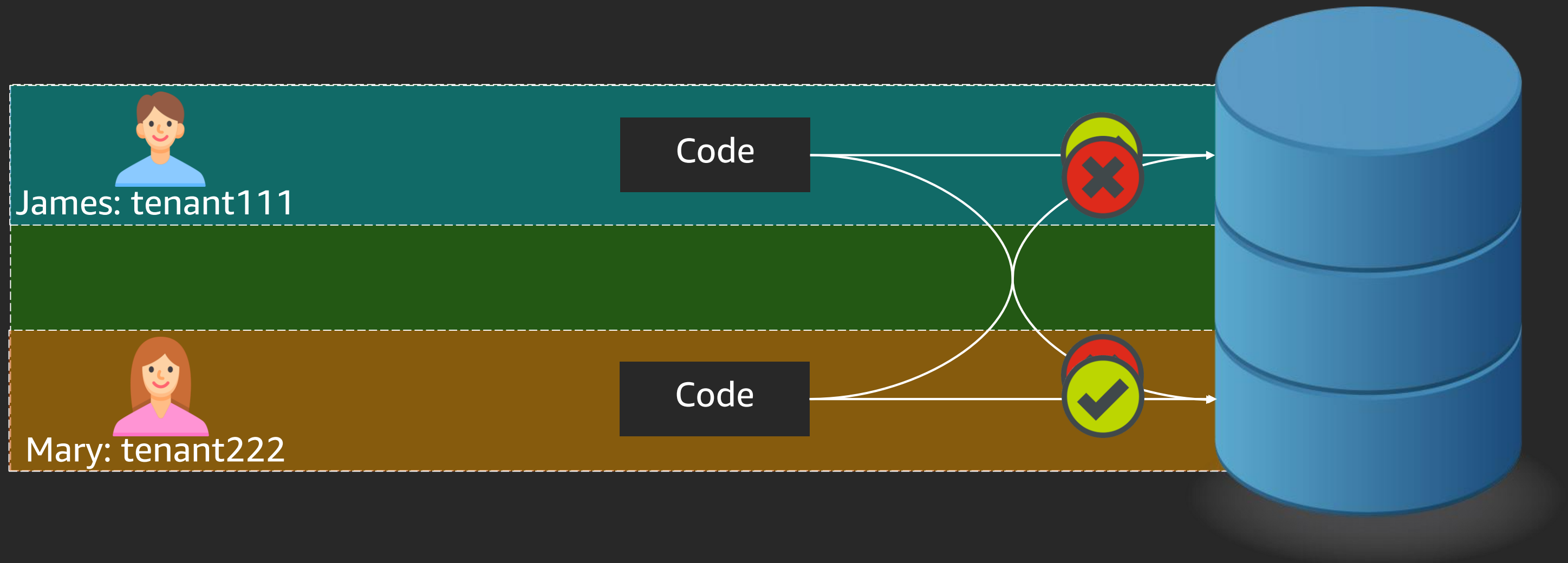
Use infrastructure level  
data partitioning





# Share all permission mechanism

Security module



# GoldTierPolicyTemplate.json

```
{
  "Sid": "AllowSpecificTenantAndTier",
  "Effect": "Allow",
  "Action": [
    "dynamodb:DescribeTable",
    "dynamodb:GetItem",
    "dynamodb:BatchGetItem",
    "dynamodb:Query",
    "dynamodb:PutItem",
    "dynamodb:UpdateItem",
    "dynamodb>DeleteItem",
    "dynamodb:BatchWriteItem"
  ],
  "Resource": [
    "###table-arn###"
  ],
  "Condition": {
    "ForAllValues:StringLike": {
      "dynamodb:LeadingKeys": [
        "###tenant-id###*"
      ]
    },
    "ForAllValues:StringEquals": {
      "dynamodb:Attributes": [
        "AnimalId",
        "Age",
        "Breed",
        "Image",
        "Name"
      ]
    },
    "StringEqualsIfExists": {
      "dynamodb:Select": "SPECIFIC_ATTRIBUTES"
    }
  }
}
```

Service sts, ClaimsPrincipal claims)

Animals [Close](#)

Overview **Items** Metrics Alarms Capacity Indexes Global Tables Backups Contributor Insights

Create item Actions ▾

Scan: [Table] Animals: AnimalId ^

Scan ▾ [Table] Animals: AnimalId ▾ ^

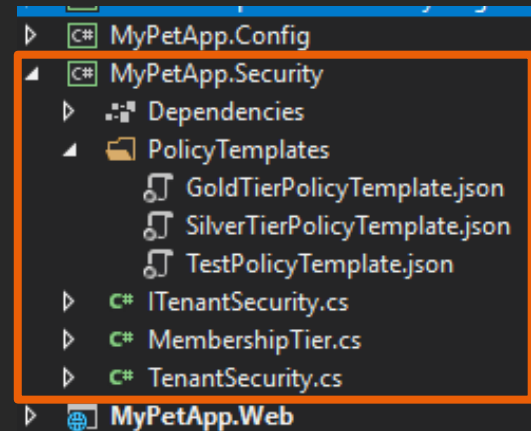
+ Add filter

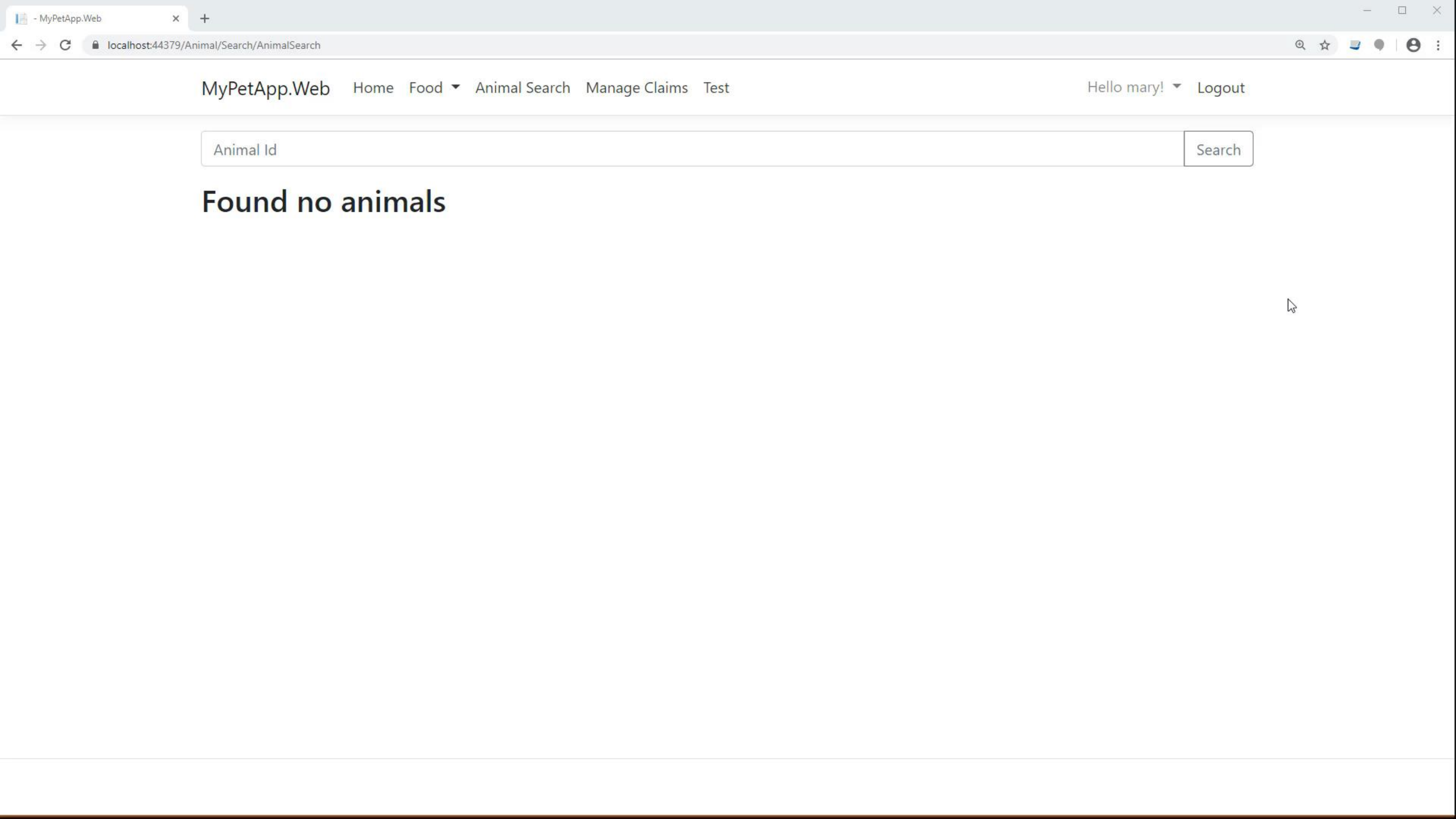
Start search

	AnimalId ⓘ	Age	Breed	Image	Name
<input type="checkbox"/>	tenant111-cat1	3	Birman	tenant222/dog1-111.jpg	Shanthi
<input type="checkbox"/>	tenant111-cat2	6	Persian	tenant111/cat2-222.jpg	Smokey
<input type="checkbox"/>	tenant111-cat3	4	British Shorthair	tenant111/cat3-333.jpg	Patch
<input type="checkbox"/>	tenant111-cat4	7	Himalayan	tenant444/cat4-444.jpg	Lilly
<input type="checkbox"/>	tenant111-cat5	12	Russian Blue	tenant111/cat5-555.jpg	Oscar
<input type="checkbox"/>	tenant111-cat6	1	Bengal	tenant111/cat6-666.jpg	Missy
<input type="checkbox"/>	tenant222-dog1	2	French Bulldog	tenant222/dog1-111.jpg	Barbes
<input type="checkbox"/>	tenant222-dog2	5	German Shepherd	tenant222/dog2-222.jpg	Charlie
<input type="checkbox"/>	tenant222-dog3	7	Dachshund	tenant222/dog3-333.jpg	Milo
<input type="checkbox"/>	tenant222-dog4	2	Labrador	tenant222/dog4-444.jpg	Toby
<input type="checkbox"/>	tenant555-dog5	8	Yorkshire Terrier	tenant222/dog5-555.jpg	Molly

ession-{tenantId}";

result.Credentials;





MyPetApp.Web

[Home](#)

[Food](#) ▼

[Animal Search](#)

[Manage Claims](#)

[Test](#)

Hello mary! ▼

[Logout](#)

Search

Found no animals



# Column level security

Animals Close

Overview

Items

Metrics

Alarms

Capacity

Indexes

Global Tables

Backups

Contributor Insights

Create item

Actions ▾

Scan: [Table] Animals: AnimalId ^

Scan ▾

[Table] Animals: AnimalId ▾

^

+ Add filter

Start search

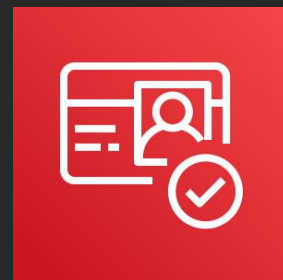
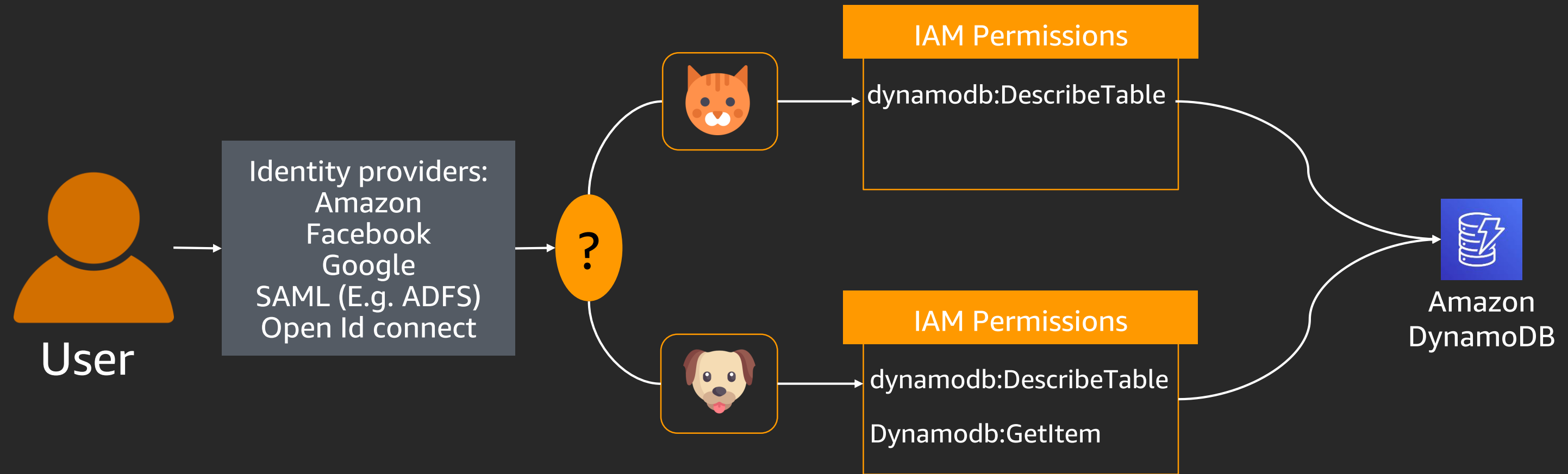
<input type="checkbox"/>	AnimalId ⓘ ▲	Age ▾	Breed ▾	Image ▾	Name ▾
<input type="checkbox"/>	tenant111-cat1	3	Birman	tenant222/dog1-111.jpg	Shanthi
<input type="checkbox"/>	tenant111-cat2	6	Persian	tenant111/cat2-222.jpg	Smokey
<input type="checkbox"/>	tenant111-cat3	4	British Shorthair	tenant111/cat3-333.jpg	Patch
<input type="checkbox"/>	tenant111-cat4	7	Himalayan	tenant444/cat4-444.jpg	Lilly
<input type="checkbox"/>	tenant111-cat5	12	Russian Blue	tenant111/cat5-555.jpg	Oscar
<input type="checkbox"/>	tenant111-cat6	1	Bengal	tenant111/cat6-666.jpg	Missy
<input type="checkbox"/>	tenant222-dog1	2	French Bulldog	tenant222/dog1-111.jpg	Barbes
<input type="checkbox"/>	tenant222-dog2	5	German Shepherd	tenant222/dog2-222.jpg	Charlie
<input type="checkbox"/>	tenant222-dog3	7	Dachshund	tenant222/dog3-333.jpg	Milo
<input type="checkbox"/>	tenant222-dog4	2	Labrador	tenant222/dog4-444.jpg	Toby
<input type="checkbox"/>	tenant555-dog5	8	Yorkshire Terrier	tenant222/dog5-555.jpg	Molly

## Gold tier policy

```
"ForAllValues:StringEquals": {
  "dynamodb:Attributes": [
    "AnimalId",
    "Age",
    "Breed",
    "Image",
    "Name"
  ]
},
"StringEqualsIfExists": {
  "dynamodb:Select": "SPECIFIC_ATTRIBUTES"
}
```

## Silver tier policy

```
"ForAllValues:StringEquals": {
  "dynamodb:Attributes": [
    "AnimalId",
    "Age",
    "Image",
    "Name"
  ]
},
"StringEqualsIfExists": {
  "dynamodb:Select": "SPECIFIC_ATTRIBUTES"
}
```



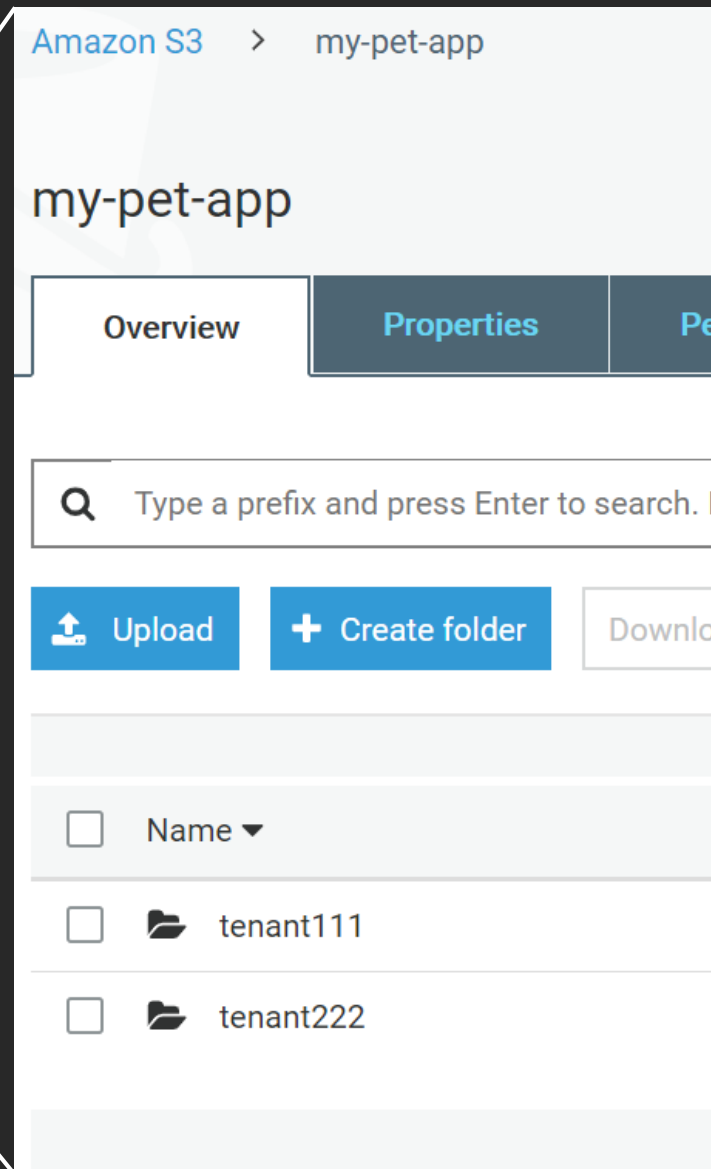
# Amazon Cognito

# Data partitioning using presigned URLs





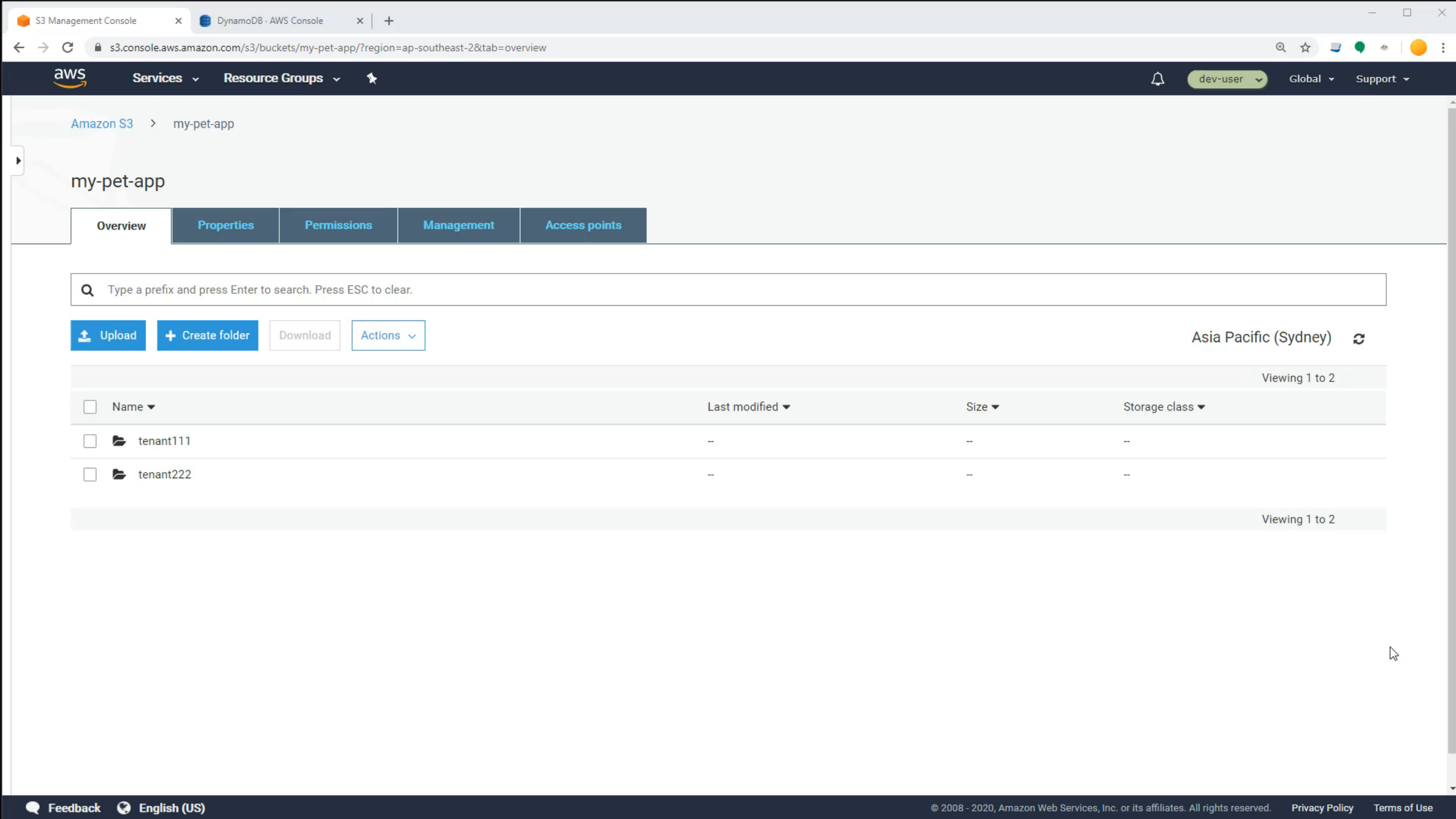
Amazon S3 Bucket  
my-pet-app



Code  
Create a presigned  
URL



```
IAmazonS3 s3 = new AmazonS3Client(stsCredentails, Amazon.RegionEndpoint.APSoutheast2);  
string imageUrl=s3.GeneratePreSignedURL("my-pet-app", imagePath, DateTime.Now.AddMinutes(5), null);
```



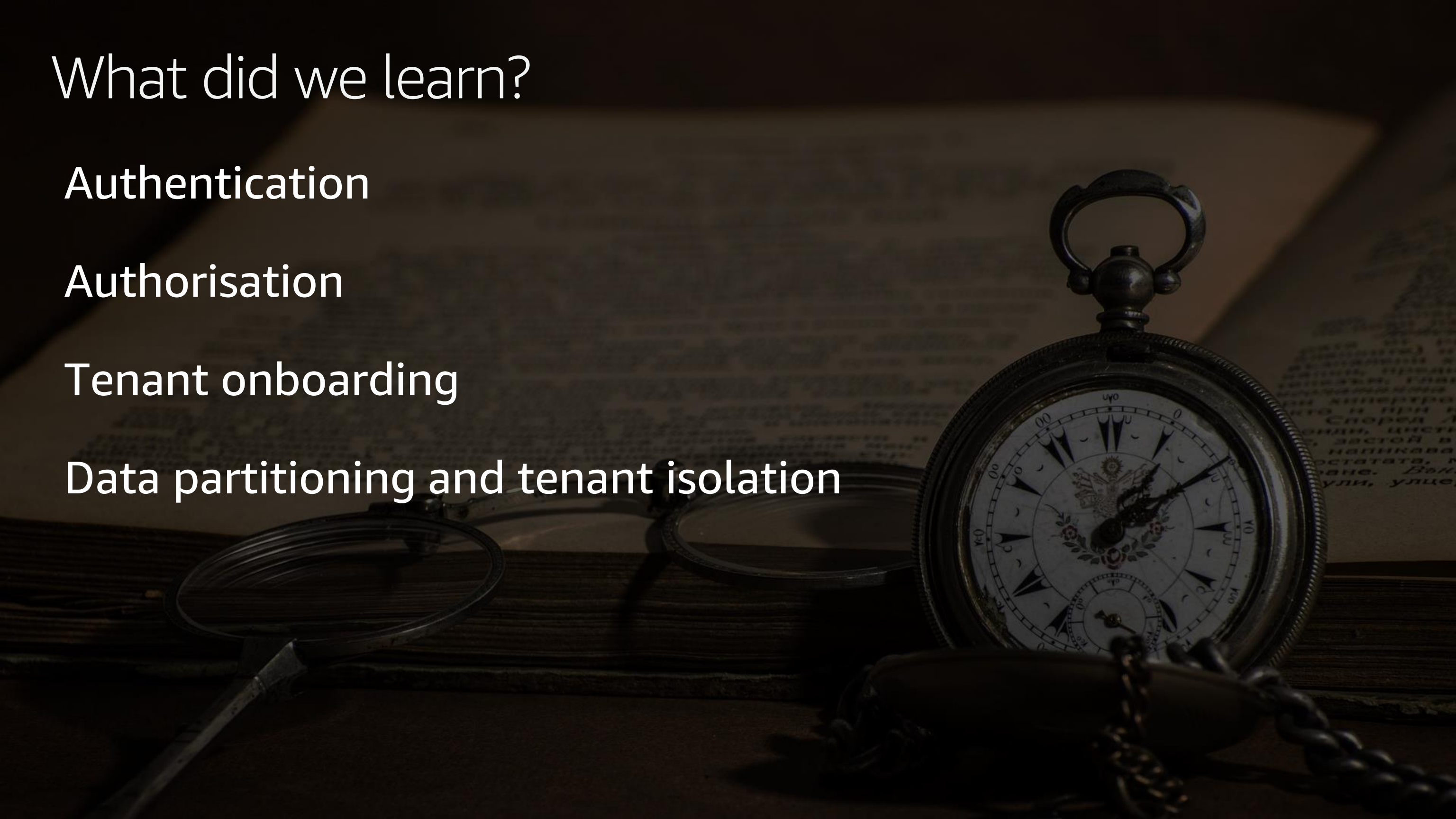
# What did we learn?

Authentication

Authorisation

Tenant onboarding

Data partitioning and tenant isolation







aws SUMMIT  
SYDNEY



# Thank you!

Sriwantha Attanayake

[sriwanth@amazon.com](mailto:sriwanth@amazon.com)

[www.linkedin.com/in/sriwantha](https://www.linkedin.com/in/sriwantha)