ADC-D3

Multi-tenant data isolation using AWS databases

Venkatesh Periyathambi

Principal Solutions Architect, Database
AWS

Agenda

- SaaS Fundamentals
- Multi-tenant deployment models
- Design Challenges
- Decision Matrix
- Design Considerations
- Takeaways
- Call to action

AWS Databases Landscape


Amazon Aurora


Amazon DocumentDB
(with MongoDB compatibility)


Amazon DynamoDB


Amazon MemoryDB
for Redis


Amazon Keyspaces
(for Apache Cassandra)


AWS Database Migration
Service (AWS DMS)


Amazon Neptune


Amazon Quantum Ledger
Database (Amazon QLDB)


Amazon Relational Database
Service (Amazon RDS)


Amazon RDS on
VMware


Amazon Timestream


Amazon ElastiCache

SaaS Fundamentals

What is SaaS

Software-as-a-Service (SaaS) is a business and software delivery model that enables organizations to offer their solution in a low-friction, service-centric approach.

Core SaaS architecture concepts

Data partitioning

How is data organized and stored in a multi-tenant environment?

Tenant isolation

How does your architecture ensure that one tenant can't access the resources of another tenant?

SaaS Identity

How is a user identity associated with a tenant identity and how is that context shared across your architecture?

Onboarding

How are new tenants added to your system in a frictionless manner?

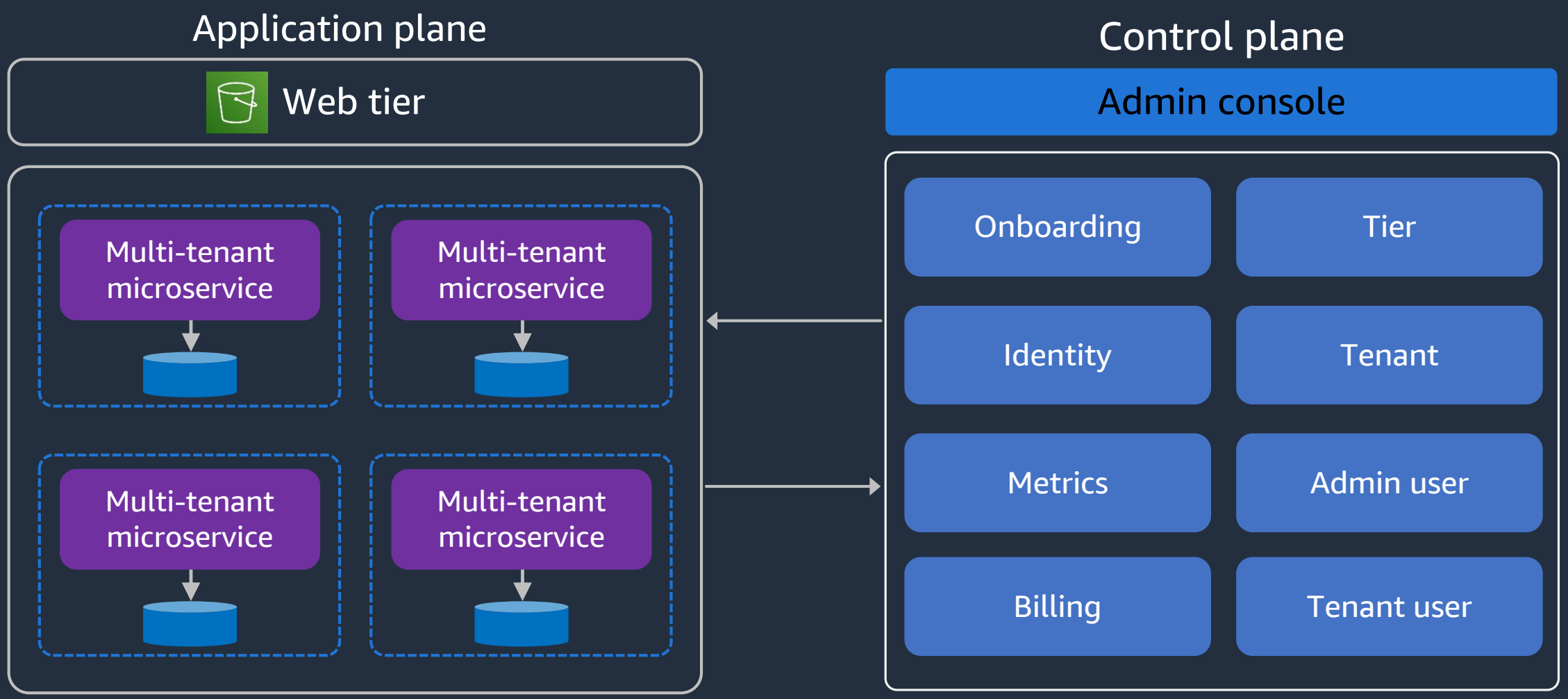
Tiering

How do we offer different experiences to tenants at different price points?

Metering and billing

How do you instrument your application to meter tenant activity and generate a bill?

Two halves of SaaS

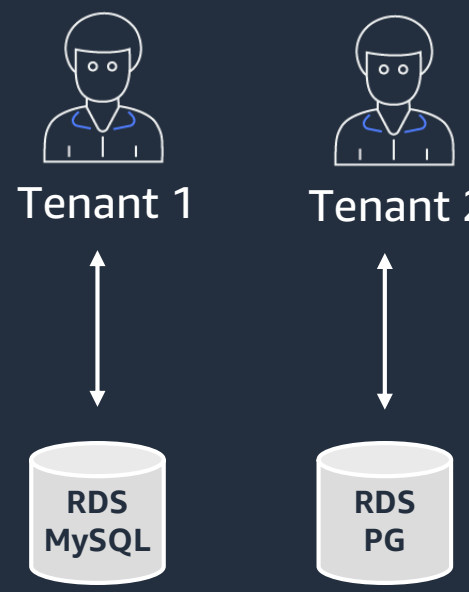


Multi-Tenant Deployment Models

ADC-D3

Multi-tenant Deployment Models

Silo model



Bridge model

Name	SKU	Cost
Glove	939301	12.39
Shirt	194193	7.83
Hat	539294	15.41
Scarf	793891	130.84
Pants	490023	17.45

tenant1_articles

Name	SKU	Cost
Glove	939301	12.39
Shirt	194193	7.83
Hat	539294	15.41
Scarf	793891	130.84
Pants	490023	17.45

tenant2_articles

Pool model

TenantID	Name	SKU	Cost
Tenant1	Glove	939301	12.39
Tenant2	Shirt	194193	7.83
Tenant1	Hat	539294	15.41
Tenant2	Scarf	793891	130.84
Tenant3	Pants	490023	17.45

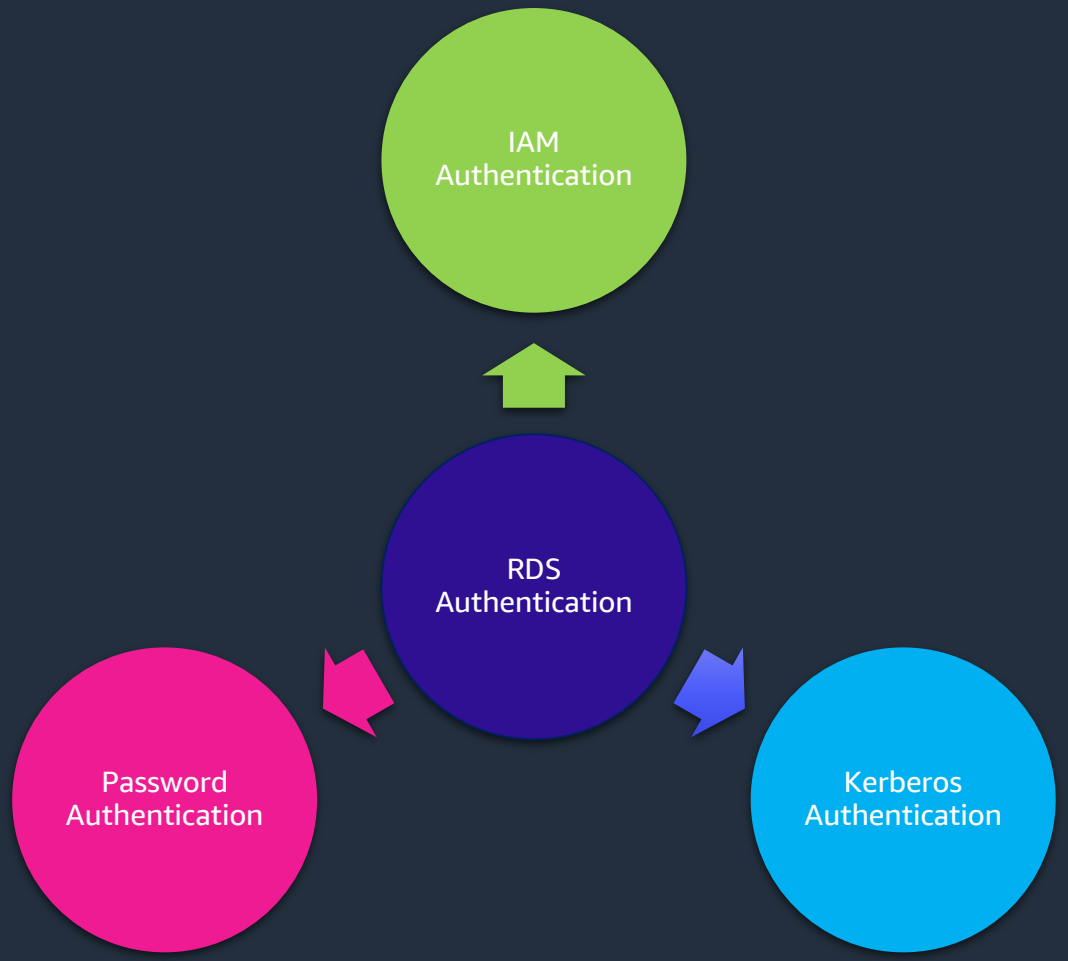
articles

Max. isolation

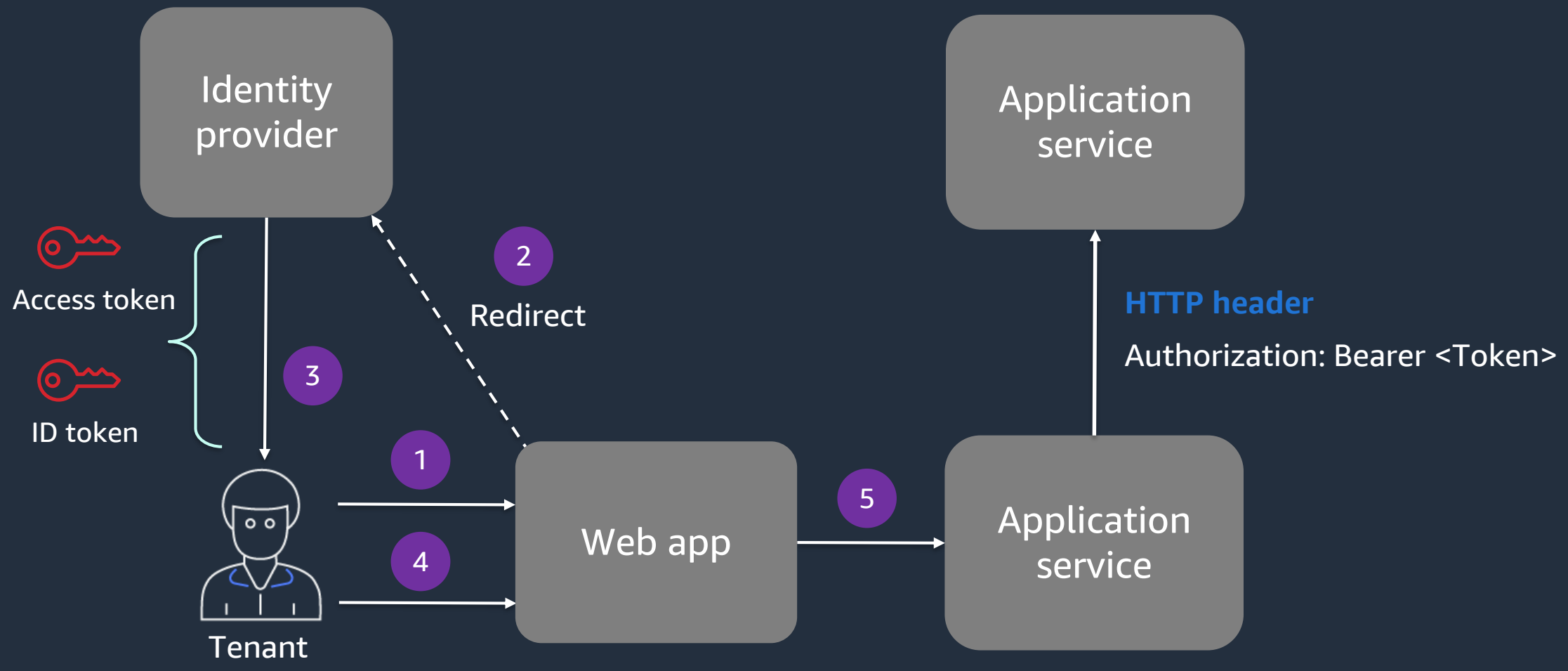
Max. Resource Sharing

Multi-tenancy Authentication

Amazon RDS Authentication Methods

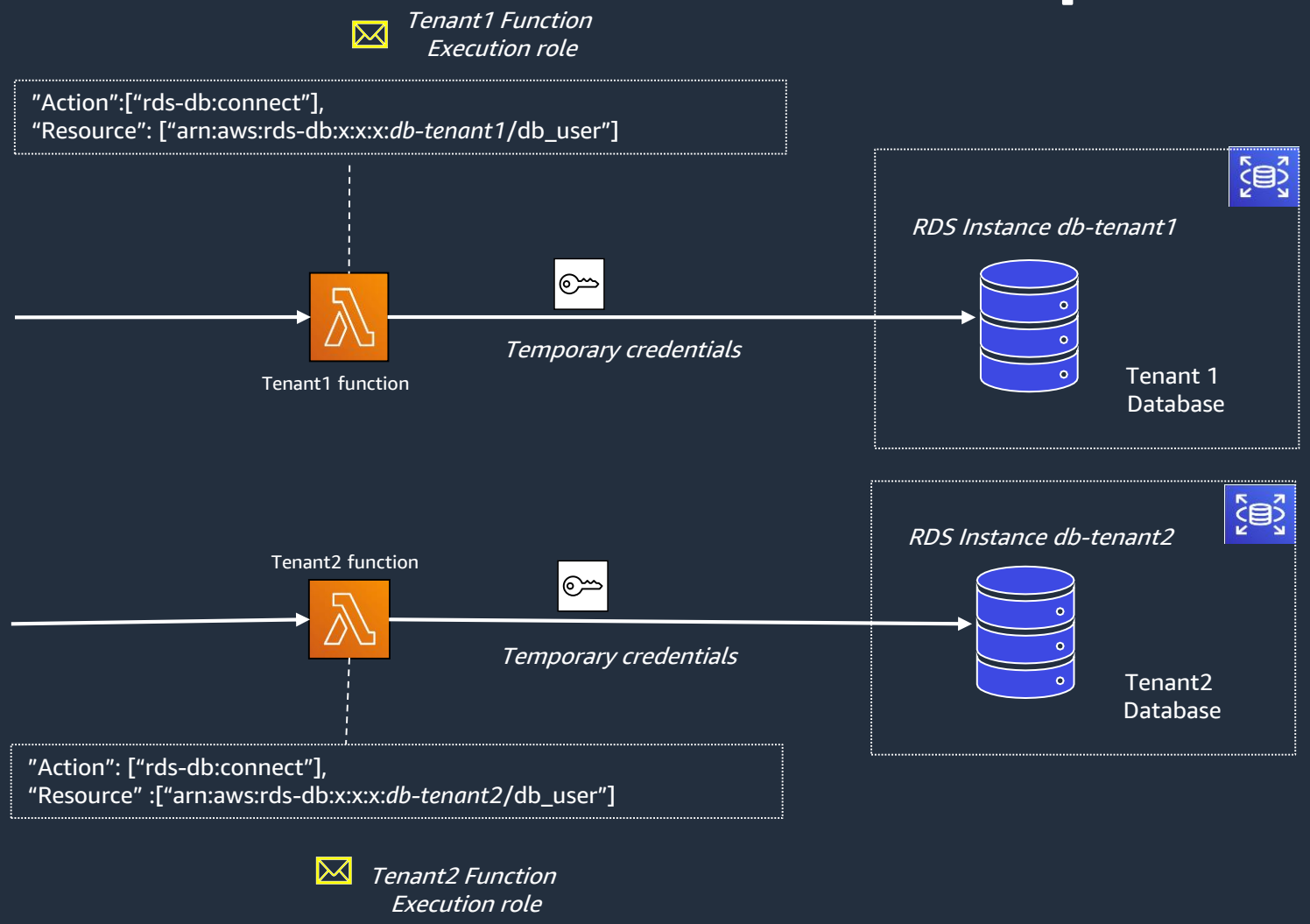


Tenant-aware identity

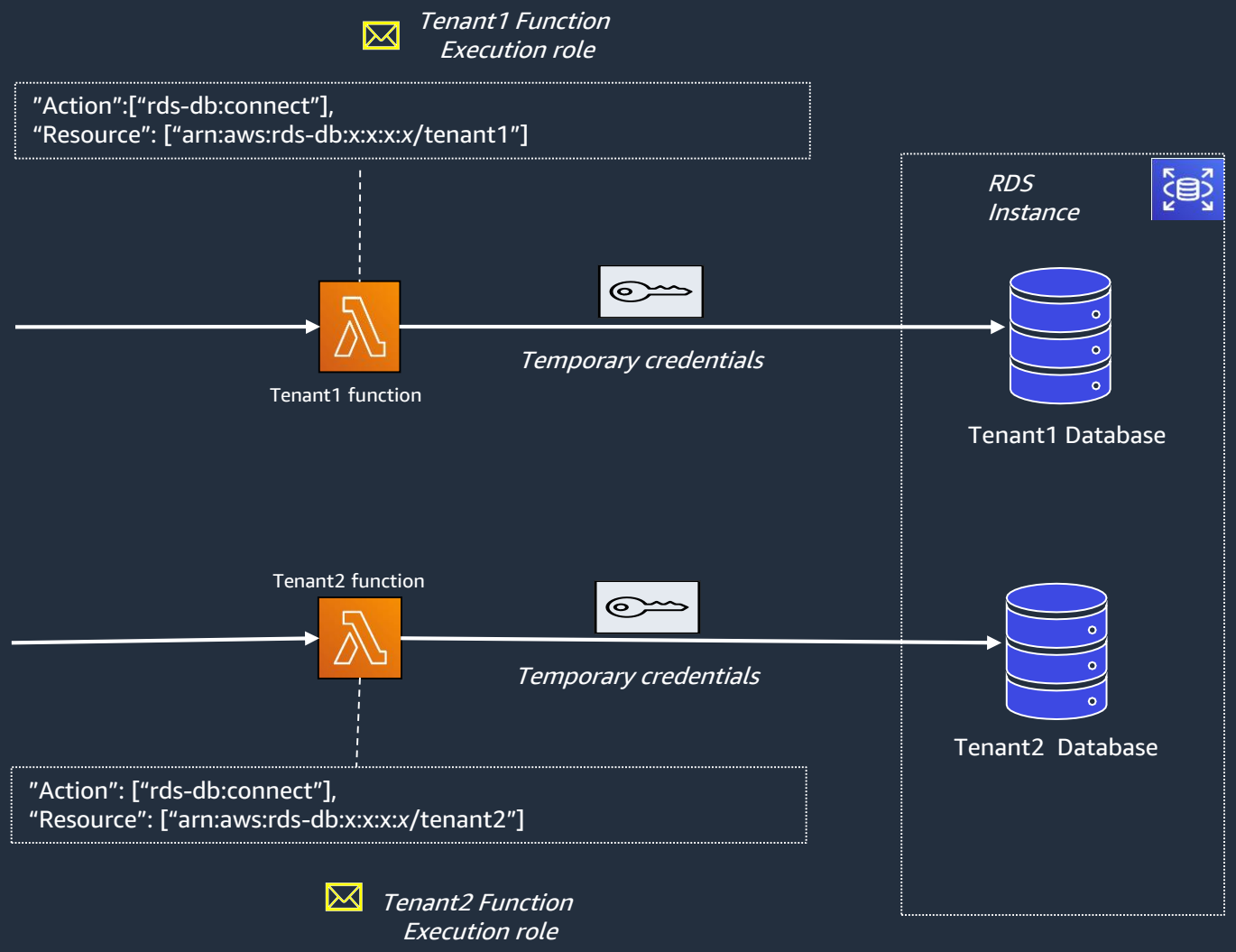


Design Challenges #1
Data Access Patterns

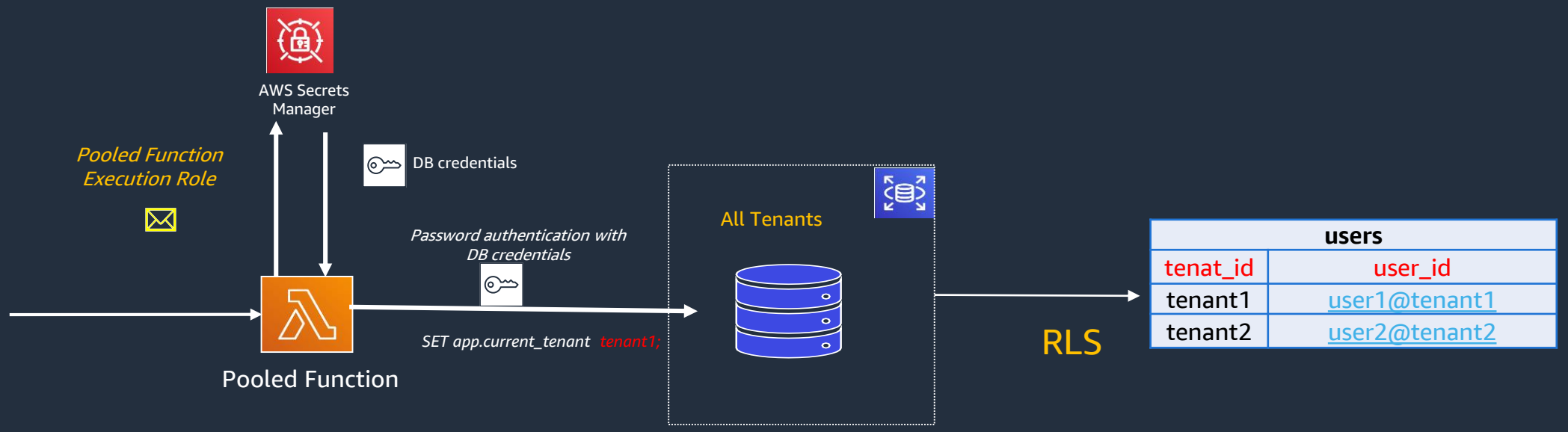
Silo database isolation with siloed compute



Bridge database isolation with siloed compute



Pool database Isolation with pooled compute



Pool with RLS and Amazon Aurora PostgreSQL

Initialize RLS

```
-- Turn on RLS
ALTER TABLE tenant ENABLE ROW LEVEL SECURITY;

-- Scope read/write by tenant
CREATE POLICY tenant_isolation_policy ON tenant
USING (tenant_id::TEXT = current_user);
```

Query with RLS

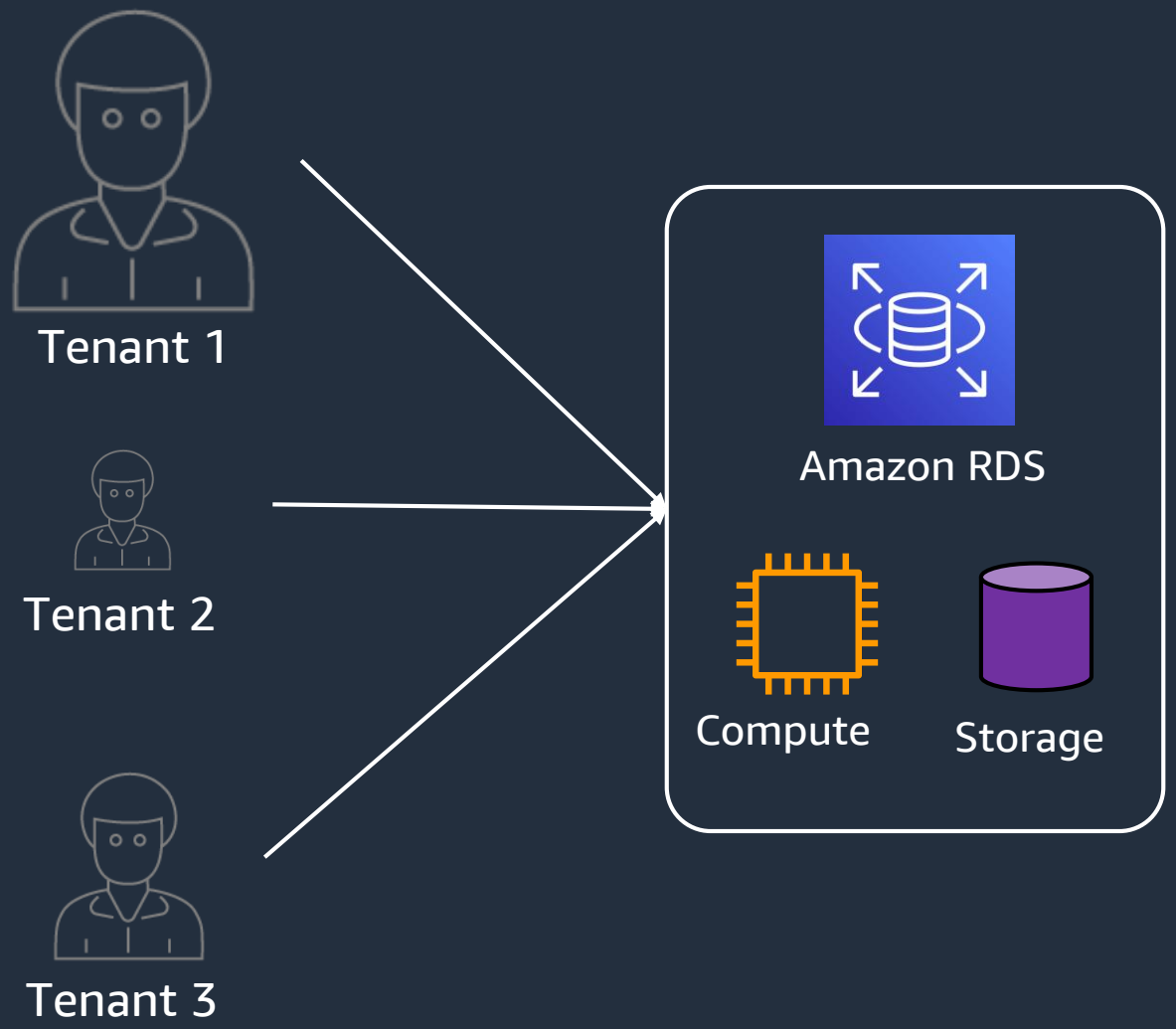
```
-- No tenant context required
rls_multi_tenant=> SELECT * FROM tenant;

-- Attempt to force tenant id
rls_multi_tenant=> SELECT * FROM tenant WHERE tenant_id
= 'tenant1'
```

FK	SKU	Name
Tenant1	93529-94	Black T-shirt
Tenant2	24411-01	Blue hoodie
Tenant1	76235-92	Wool socks
Tenant3	95419-37	Green polo
Tenant2	88314-99	White hat
Tenant1	24598-72	Tennis shoes

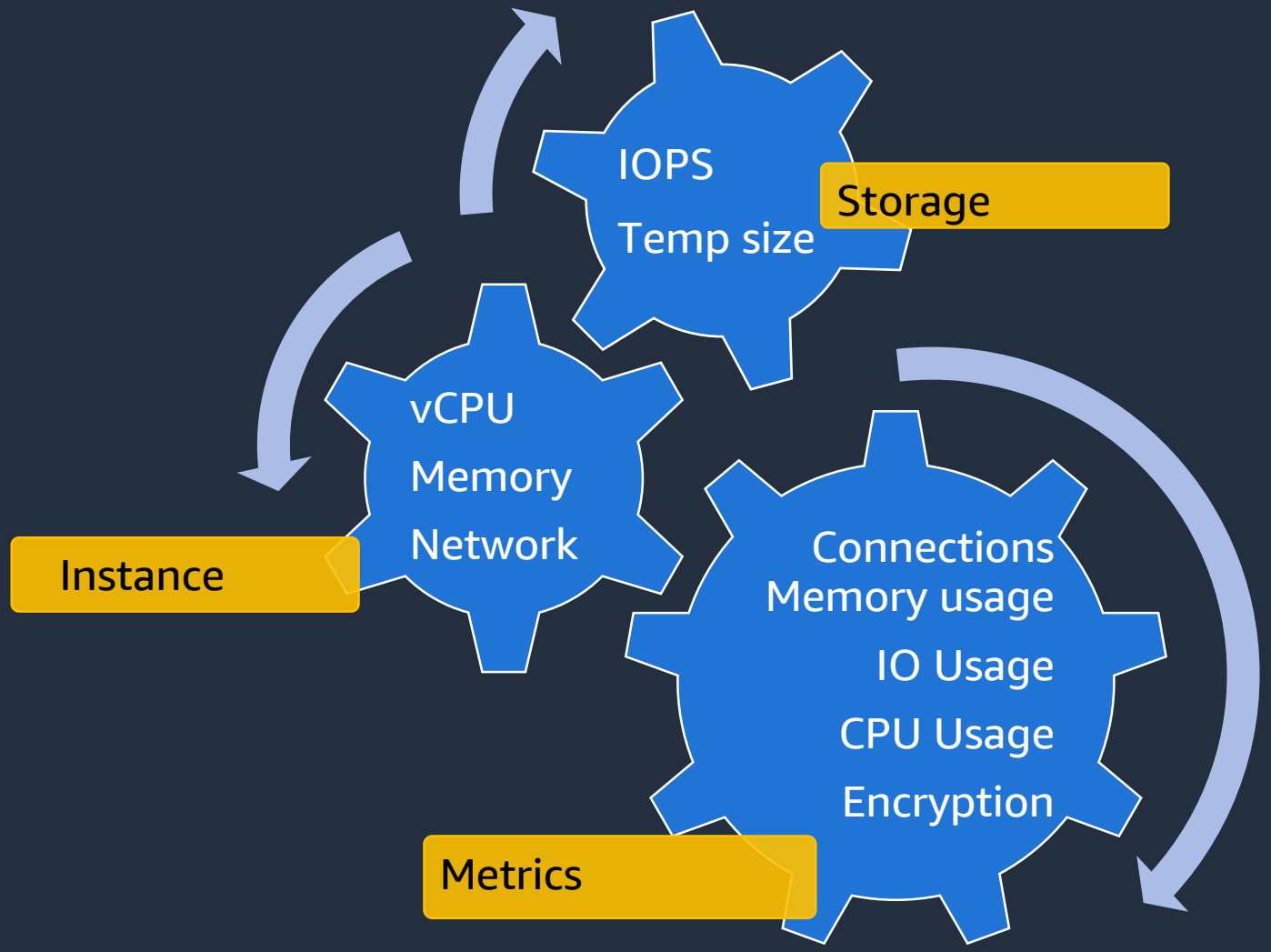
Design Challenges #2
Sizing considerations

The sizing challenge



- How do you accommodate different size tenants (noisy neighbor)?
- How do you prevent over-provisioning?
- How do you optimize based on actual consumption?
- How will you support tiering and SLAs?

Tenant bin packing



Design Challenges #3
Database engine

IAM granularity can be a factor

Course-grained IAM control

Amazon RDS

Amazon Elasticsearch Service

Fine-grained IAM control

Amazon DynamoDB

Amazon Simple Storage Service (S3)

```
Effect: "Allow",
Action: rds-db:connect
Resources:
-  arn:aws:rds-db:db-instance-id/db-user
```

```
Effect: "Allow",
Action: dynamodb:GetItem
Resources:
-  arn:aws:dynamodb:table/table
```

Data isolation with Amazon DynamoDB

Table per tenant (silo)

Tenant 1

Name	SKU	Cost
Glove	939301	12.39
Shirt	194193	7.83
Hat	539294	15.41
Pants	490023	17.45

order-table-tenant1

Tenant 2

Name	SKU	Cost
Shoes	840842	15.49
Hat	491309	44.89
Scarf	112514	96.01
Socks	309194	83.35

order-table-tenant2

Shared tenant table (pool)

Tenant 1

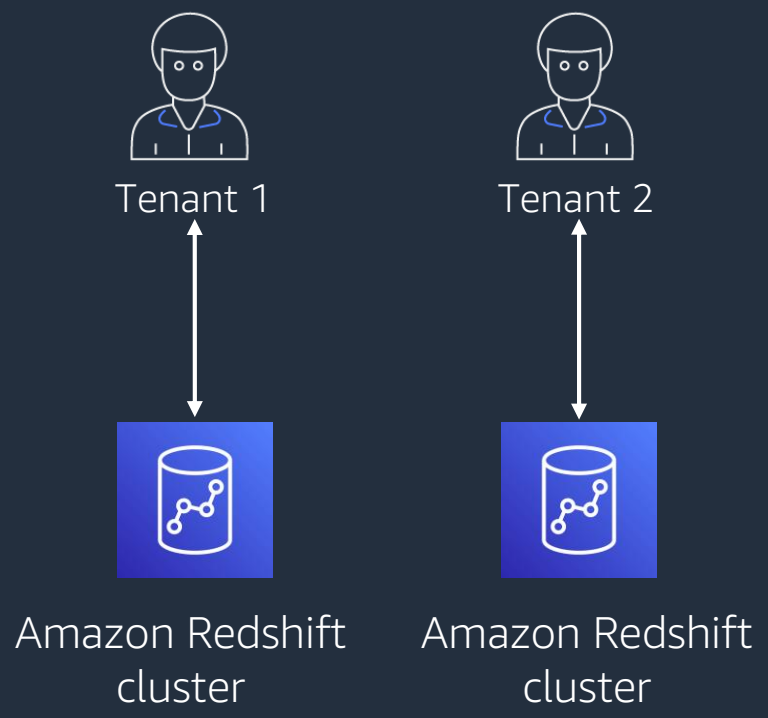
Tenant 2

TenantID	Name	SKU	Cost
Tenant1	Hat	230914	7.35
Tenant2	Socks	581641	15.98
Tenant1	Gloves	402198	89.43
Tenant2	Shirt	620985	17.64

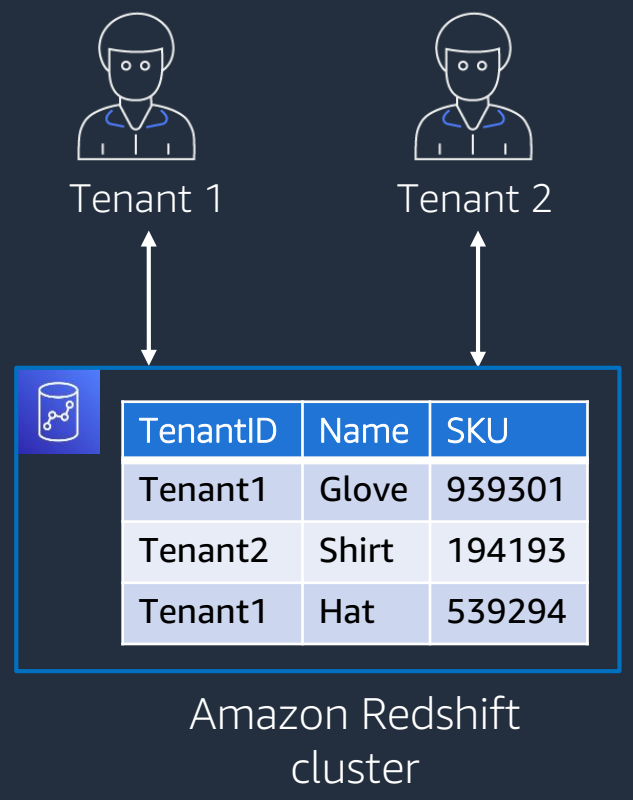
order-table

Data partitioning with Redshift

Cluster per tenant (silo)



Shared cluster for all tenants (pool)



TenantID	Name	SKU
Tenant1	Glove	939301
Tenant2	Shirt	194193
Tenant1	Hat	539294

A different strategy for each service

Amazon RDS

Amazon DynamoDB

Amazon Elasticsearch Service

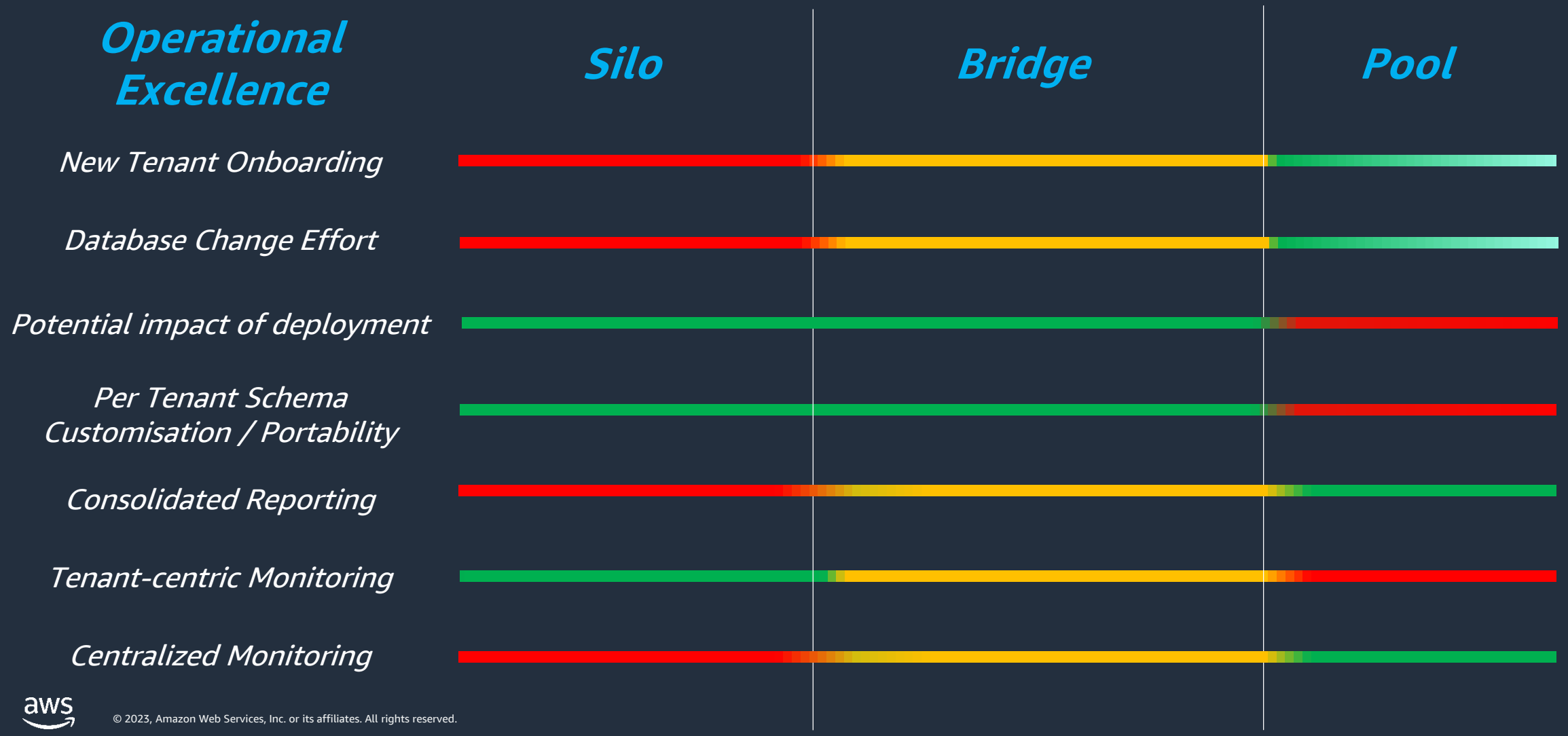
Amazon Simple Storage Service (S3)

Amazon Timestream

Amazon Redshift

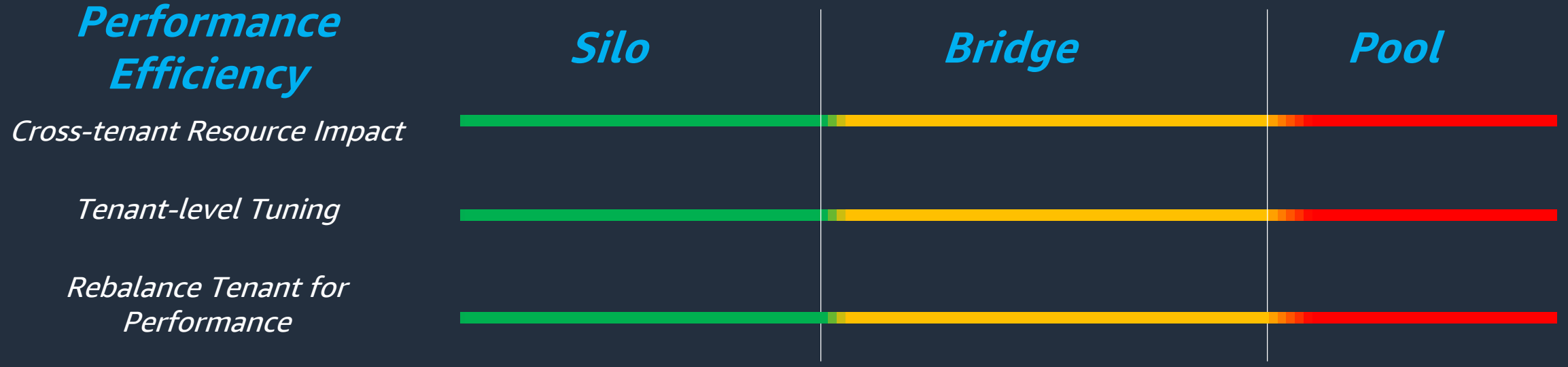
Decision Matrix

Decision Matrix – Operational Excellence



Decision Matrix – Reliability

Decision Matrix – Performance Efficiency



Decision Matrix – Cost Optimization

Silo Model – Single vs Multi-tenant

Why people choose this model

- Compliance alignment
- Partitioned environments
- No cross-tenant impacts
- Tenant-specific tuning
- Tenant level availability

Challenges

- Cost
- Agility compromised
- Management complexity
- Deployment challenges
- Analytics/metering aggregation

Bridge/Pool Model- – Single vs Multi-tenant

Why people choose this model

- Agility
- Cost optimization
- Centralized management
- Simplified deployment
- Analytics/metering aggregation

Challenges

- Agility
- Tenant Data Distribution.
- Resistance due to “shared” nature of Pool.
- Cross-tenant impacts
- Compliance challenges

Design recommendations

Performance Considerations

Evaluate Workload

- Connection Pooling
- Partitions
- Optimize for Reads and Writes
- Avoid SubTransactions
- Avoid long running Transactions
- Isolate Noisy Tenants

HA/DR consideration

- Configure HA for Critical Workloads
- Backup Strategy
- Business Continuity Plan
- Proactive Monitoring
- Plan downtime for upgradesHA/DR consideration

Takeaways

- Design with isolation in mind
- Authentication and Authorization ≠ Isolation
- Factor scale and account limits into your isolation strategy
- Use decision matrix for isolation strategy on RDS & Aurora
- Use sizing considerations for tenant bin packing
- Validate that your isolation model is working
- Isolation is fundamental to success in a multi-tenant environment

Workshop outline

1: Setup at an AWS Event

2: Splitting the monolith

3: Multi-tenant data isolation

4: Database Operations with Infrastructure as Code

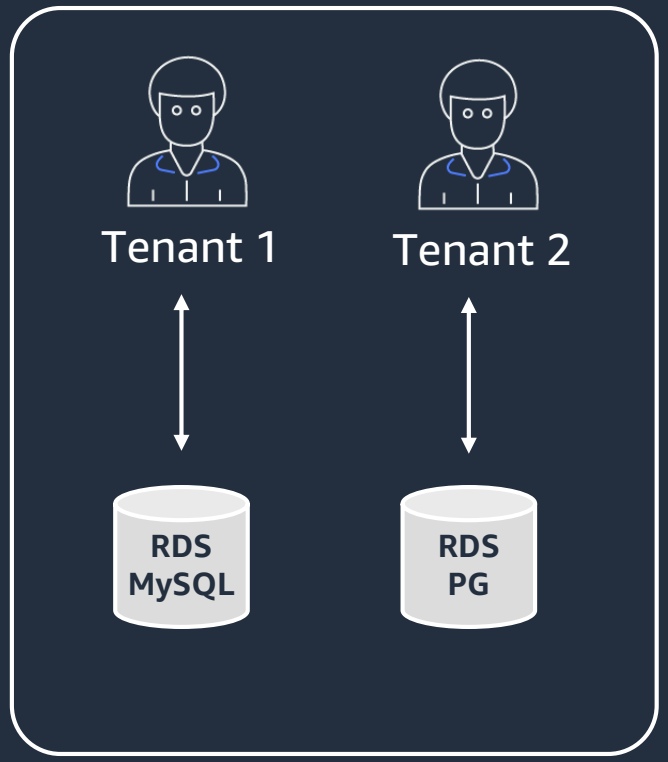
5: Data Migration & Portability

6: Cleanup

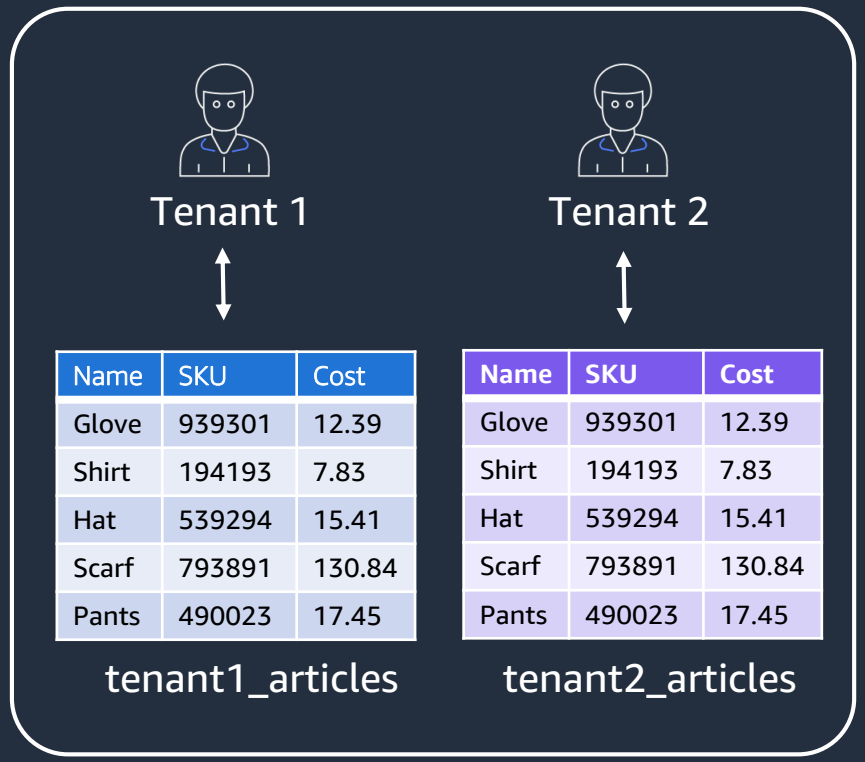
ADC-D3

Multi-tenant data isolation Overview

Silo model



Bridge model



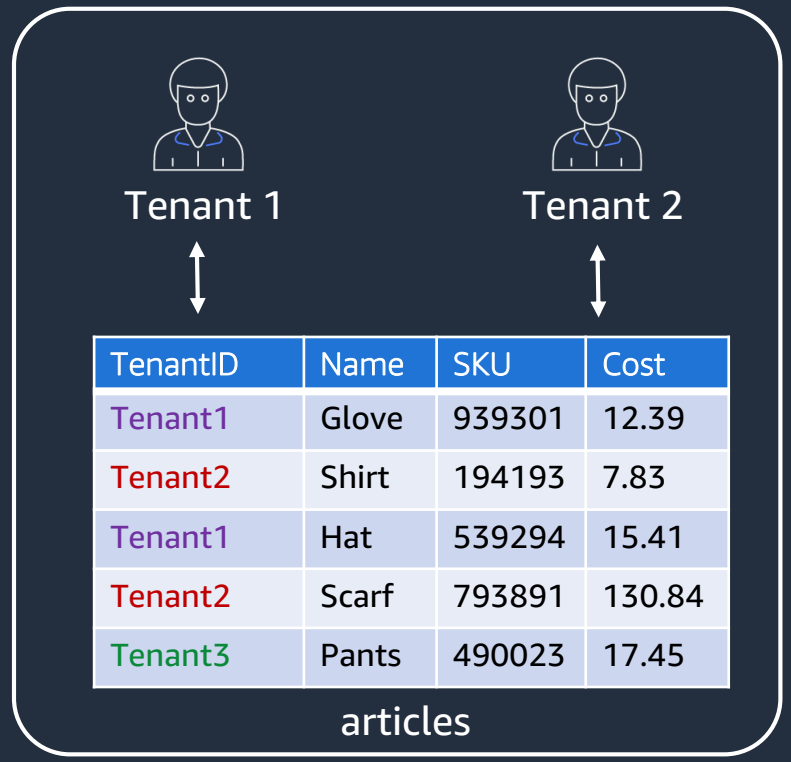
Name	SKU	Cost
Glove	939301	12.39
Shirt	194193	7.83
Hat	539294	15.41
Scarf	793891	130.84
Pants	490023	17.45

tenant1_articles

Name	SKU	Cost
Glove	939301	12.39
Shirt	194193	7.83
Hat	539294	15.41
Scarf	793891	130.84
Pants	490023	17.45

tenant2_articles

Pool model



TenantID	Name	SKU	Cost
Tenant1	Glove	939301	12.39
Tenant2	Shirt	194193	7.83
Tenant1	Hat	539294	15.41
Tenant2	Scarf	793891	130.84
Tenant3	Pants	490023	17.45

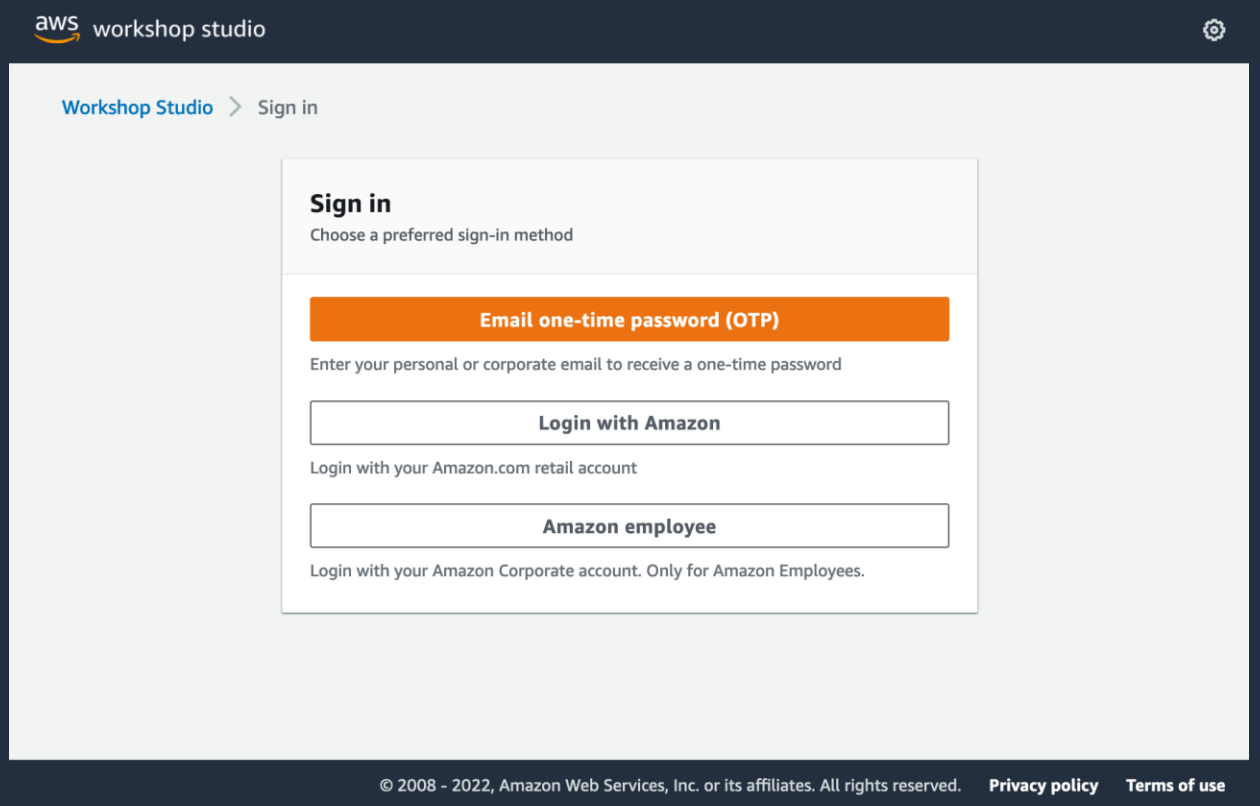
articles

Max. isolation

Max. Resource Sharing

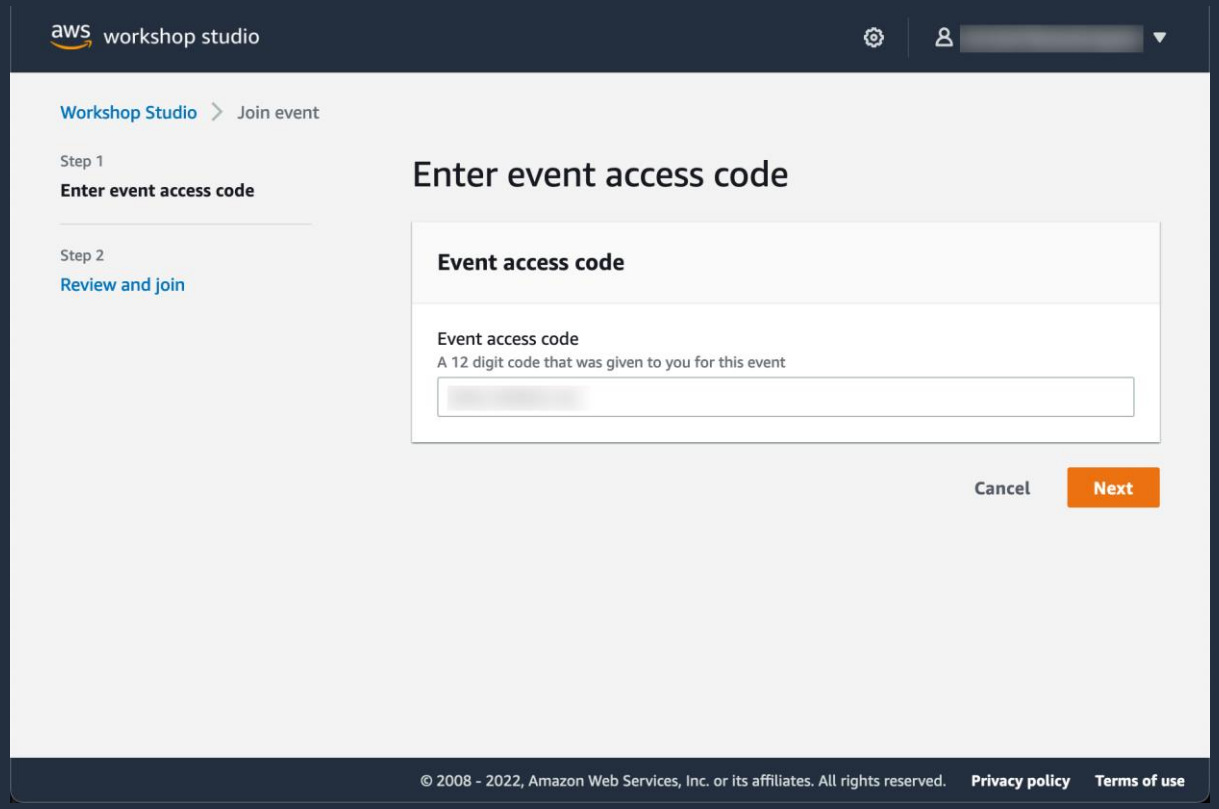
Step 1: Sign in via your preferred method

https://catalog.workshops.aws/join



Step 2: Enter event access code

Enter 12-digit event access code: cfe8-07f6b4-48



Step 3: Review terms and join event

aws workshop studio

Workshop Studio > Join event

Step 1
Enter event access code

Step 2
Review and join

Review and join

Event details

Name	Start time	Duration	Level
AWS General Immersion Day	9/23/2022 01:13 AM	12 hours	-

Description
AWS General Immersion Day

Terms and Conditions

Read and accept before joining the event

1. By using AWS Workshop Studio for the relevant event, you agree to the AWS Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.
2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivate works of materials provided by AWS, including but not limited to, data sets.
3. AWS is under no obligation to enable the transmission of your materials through Event Engine and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.
4. Your use of AWS Workshop Studio will comply with these terms and all applicable laws, and your access to AWS Workshop Studio will immediately and automatically terminate if you do not comply with any of these terms or conditions.

☑ I agree with the Terms and Conditions

Cancel | Previous | Join event

Step 4: Access AWS account

Access the AWS Management Console, or generate AWS CLI credentials as needed

aws workshop studio

AWS Database for SaaS workshop

- Workshop Setup
  - Setup at an AWS Event
- 1. Splitting the monolith
- 2. Multi-tenant data isolation
  - Silo Isolation
  - Bridged Isolation
  - Pooled Isolation
  - Conclusions and Improvements
- 3. Database Operations with Infrastructure as Code
- 4. Data Migration & Portability
- Cleanup

AWS Database for SaaS workshop > Workshop Setup > Setup at an AWS Event

Setup at an AWS Event

Only complete this section if you participate at an AWS hosted event.

If you are attending an AWS Event, then you will be provided with an AWS account which you can use to deploy and build the workshop. This AWS account will come with a Cloud9 environment already provisioned for you with all the pre-requisites installed. We will use this Cloud9 environment for this workshop.

Login to the AWS Workshop Portal

1. You will need the Event access code to login. This will be provided during the event. Connect to the portal by browsing to https://catalog.workshops.aws/join
2. Enter the provided hash in the text box and click Next. If you were given a one-click join link, you can skip this step.
3. Review terms and join event.
4. Now, access the AWS Console by following the link

Open Cloud 9 Instance

Navigate to the Cloud 9 Console and select the IDE that was created by the CloudFormation template. Once you open your IDE, you will see a welcome screen. Below, you should see a terminal prompt where you will be able to execute all the commands.

Update your Cloud9 IAM settings

Once you opened the Cloud9 IDE, you will need to update the IAM settings, to ensure that the Cloud9 IDE utilises the correct AWS credentials.

aws | Services | Search for services, features, blogs, docs, and more [Option+S] | N. Virginia

Console Home Info

Reset to default layout | + Add widgets

Introducing the new widget Recent AWS blog posts.

Welcome to AWS

- Getting started with AWS — Learn the fundamentals and find valuable information to get the most out of AWS.
- Training and certification — Learn from AWS experts and advance your skills and knowledge.
- What's new with AWS? — Discover new AWS services, features, and Regions.

AWS Health Info

No health data

This could be because you don't have permissions to access AWS Health. Please contact your account administrator.

Go to AWS Health

Cost and usage Info

Feedback | Looking for language selection? Find it in the new Unified Settings | © 2022, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences