AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

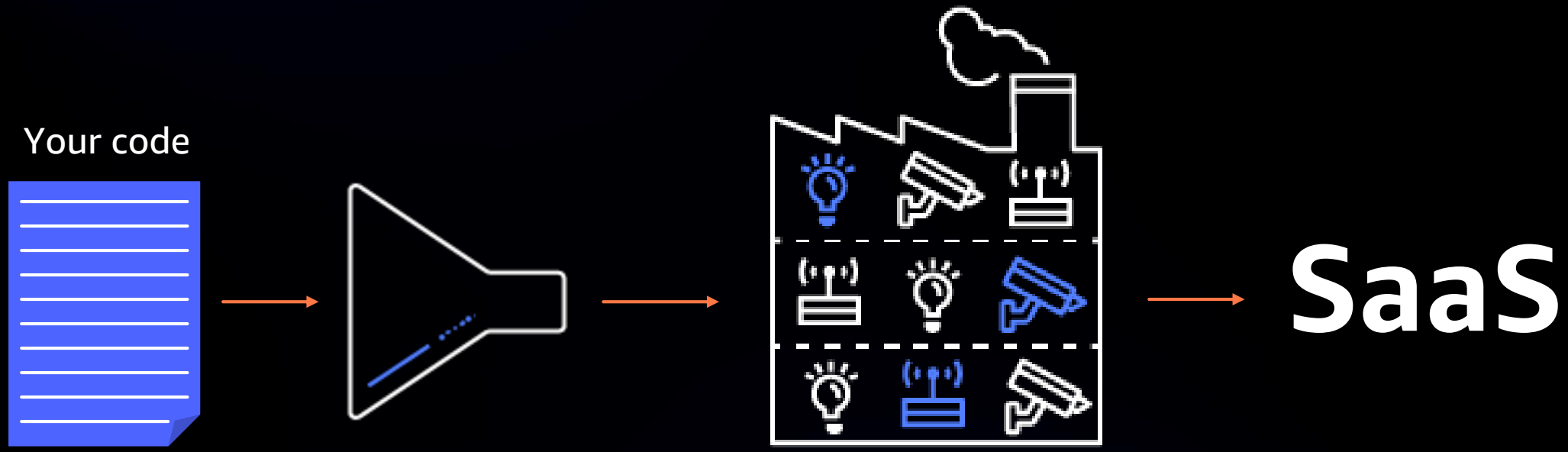
ARC306

SaaS architecture patterns: From concept to implementation

Tod Golding
Principal Partner Solutions Architect, SaaS Factory
AWS

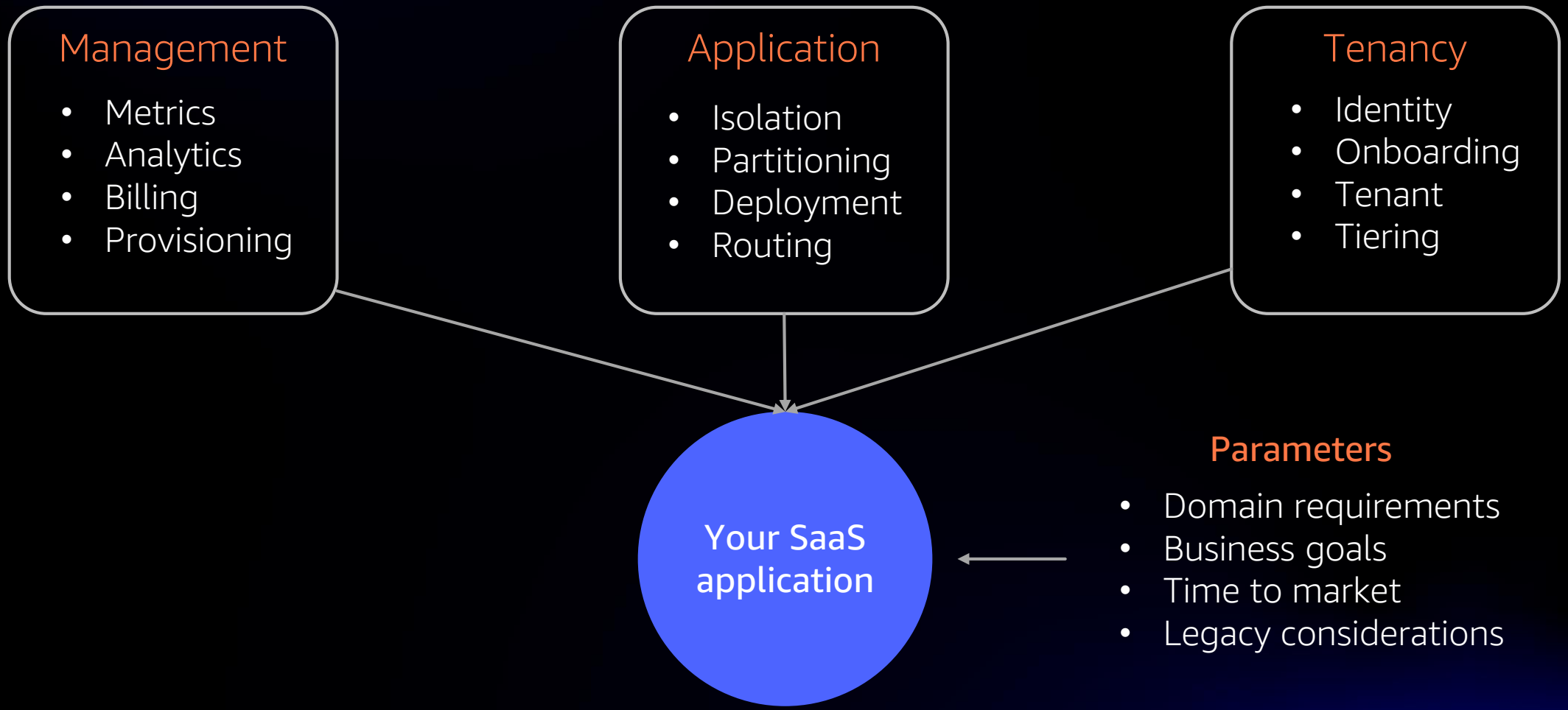
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

There’s no blueprint for SaaS



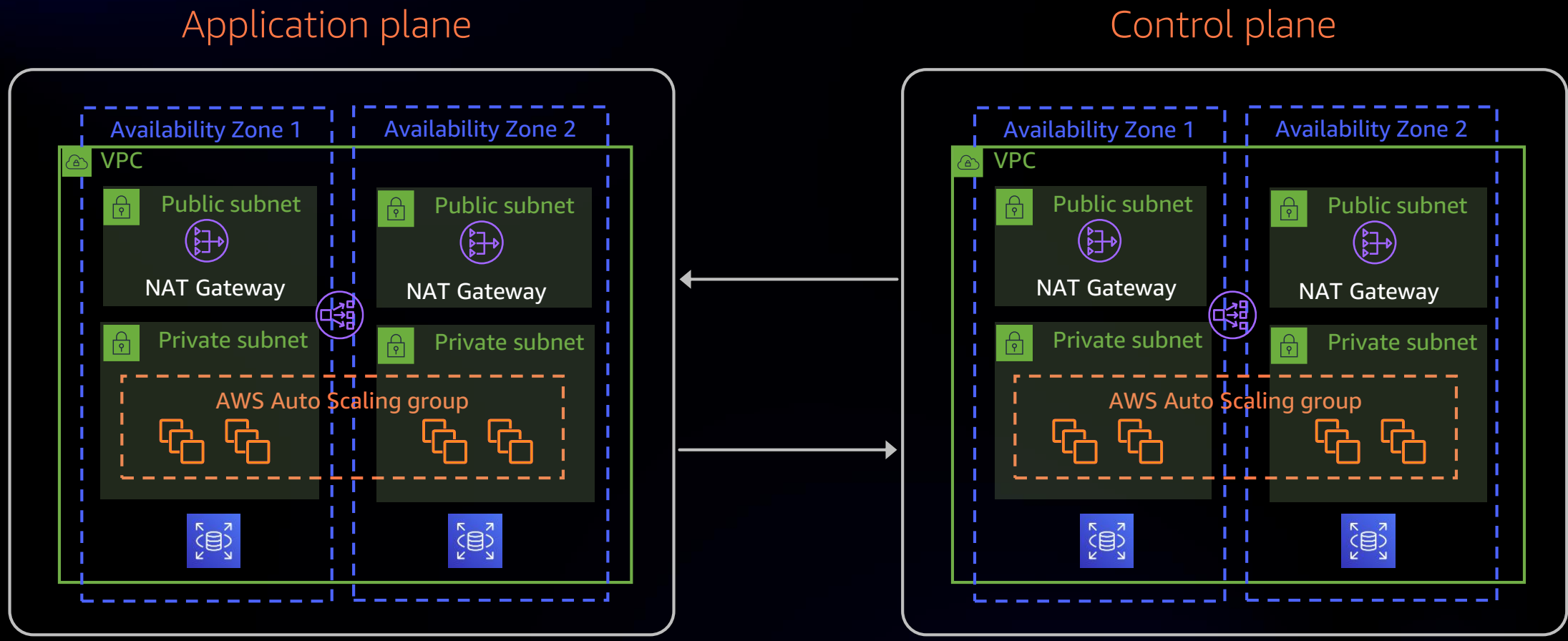
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Composing SaaS from patterns



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The two halves of SaaS

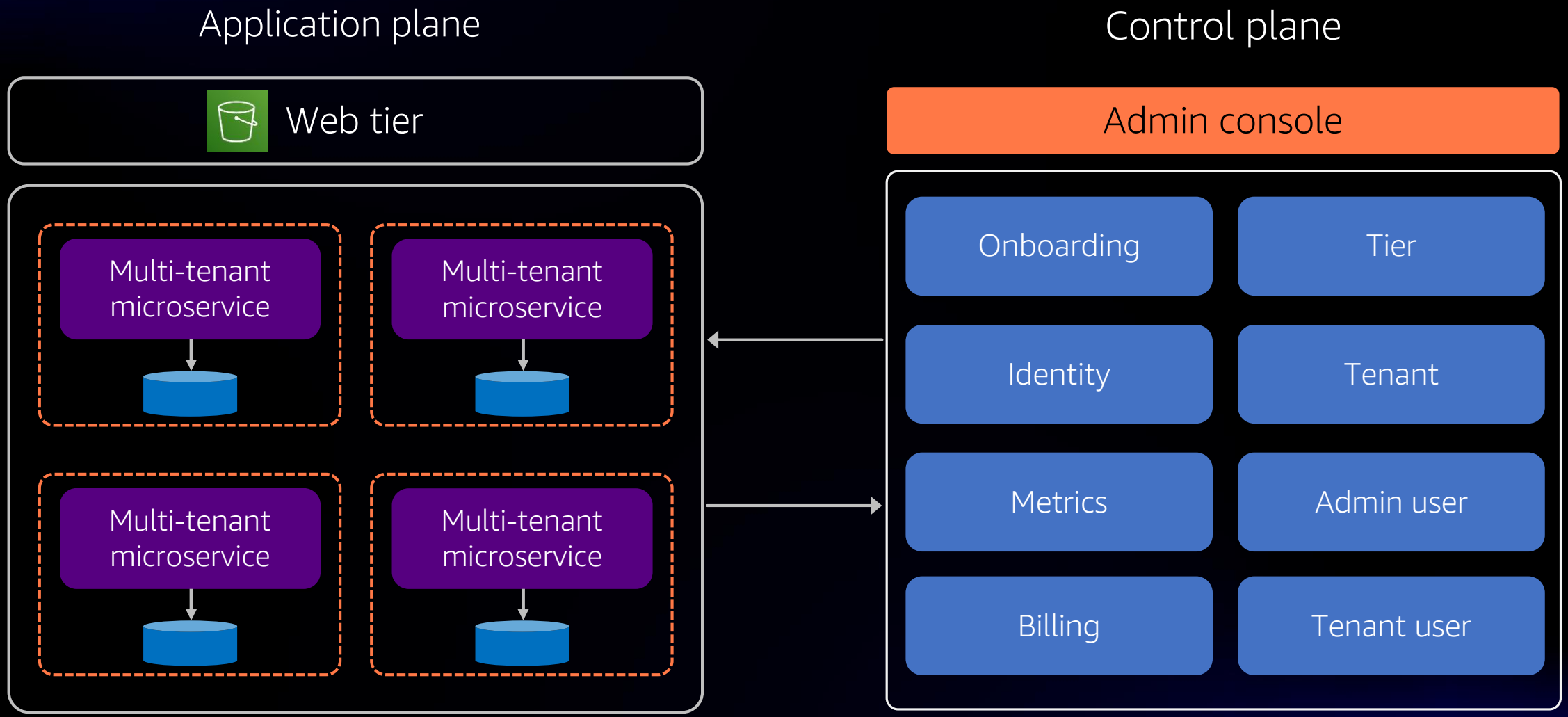


- Multi-tenant environment
- Home for all tenant functionality

- Operates and manages all tenants
- Home to all shared services

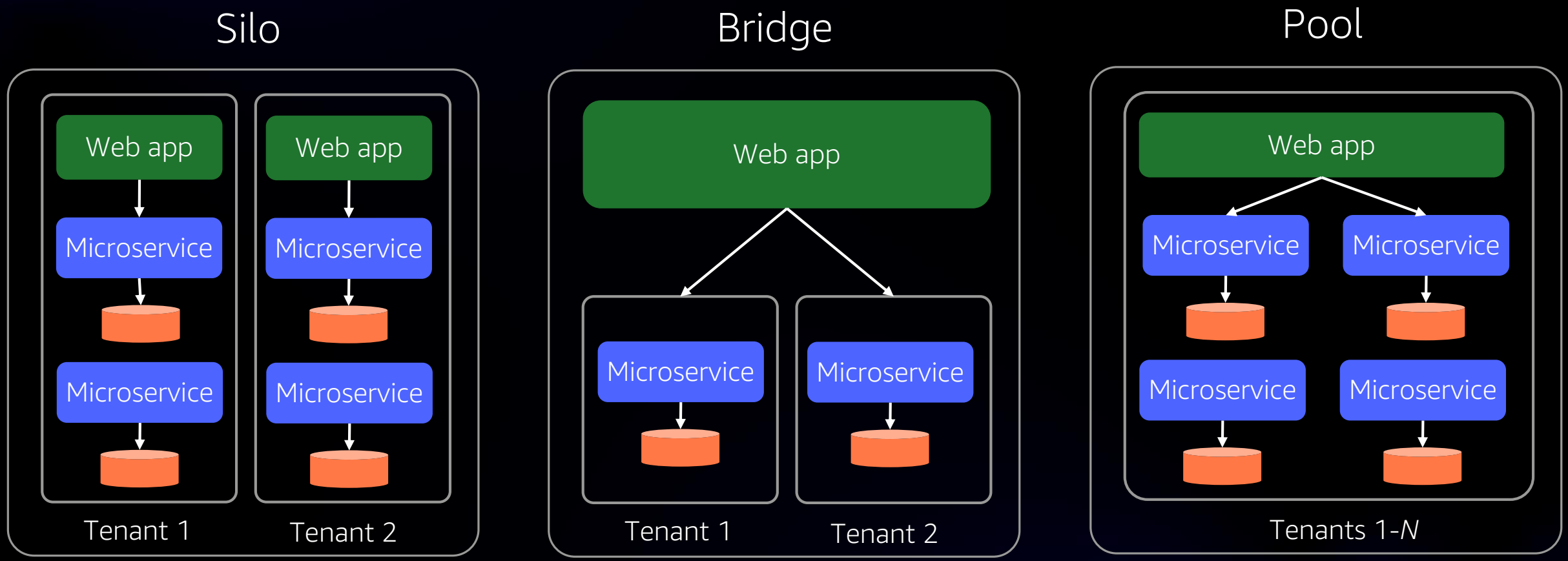
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A multi-tenant application vs. a SaaS service



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Describing SaaS environments

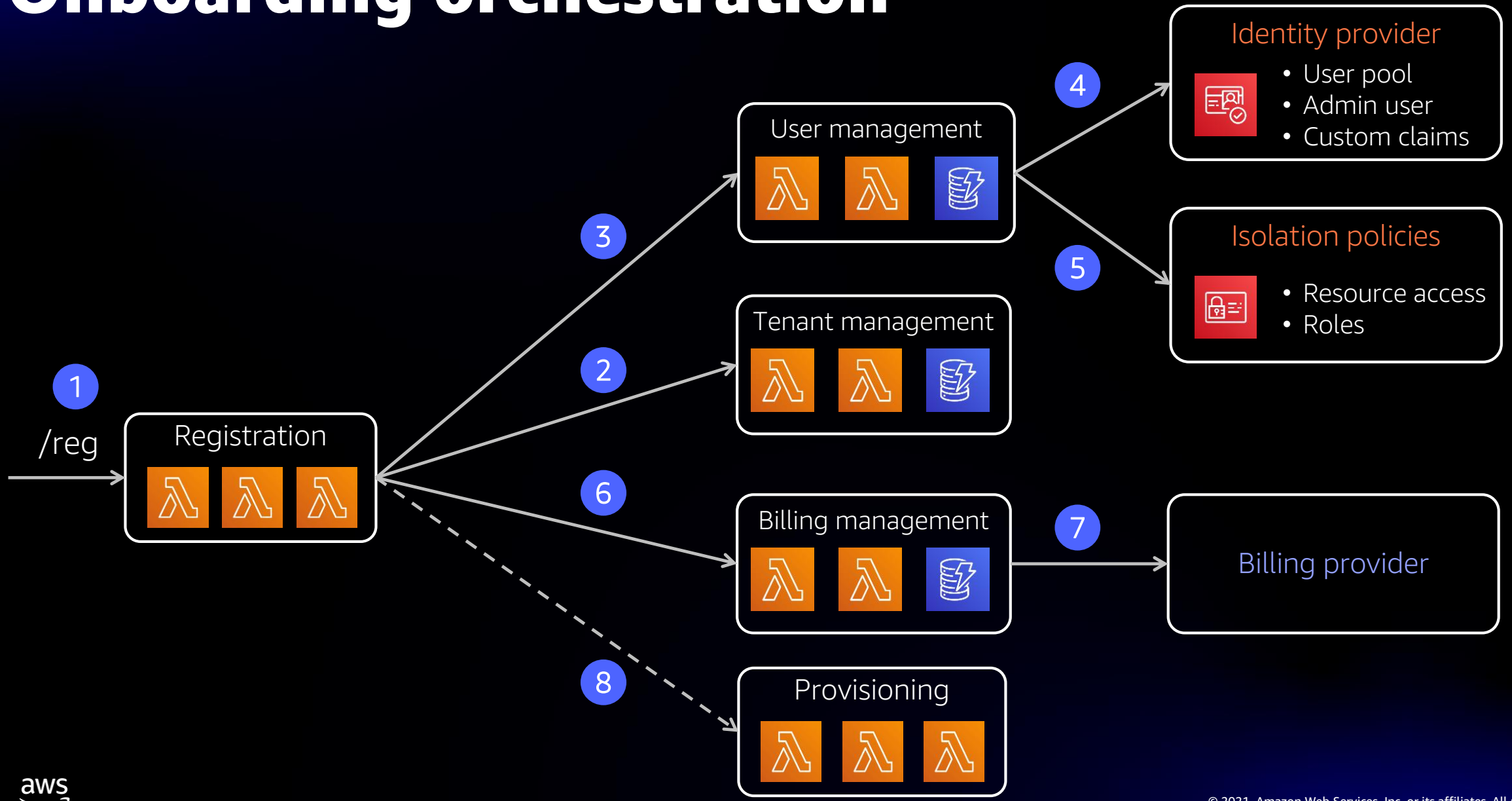


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Control plane patterns

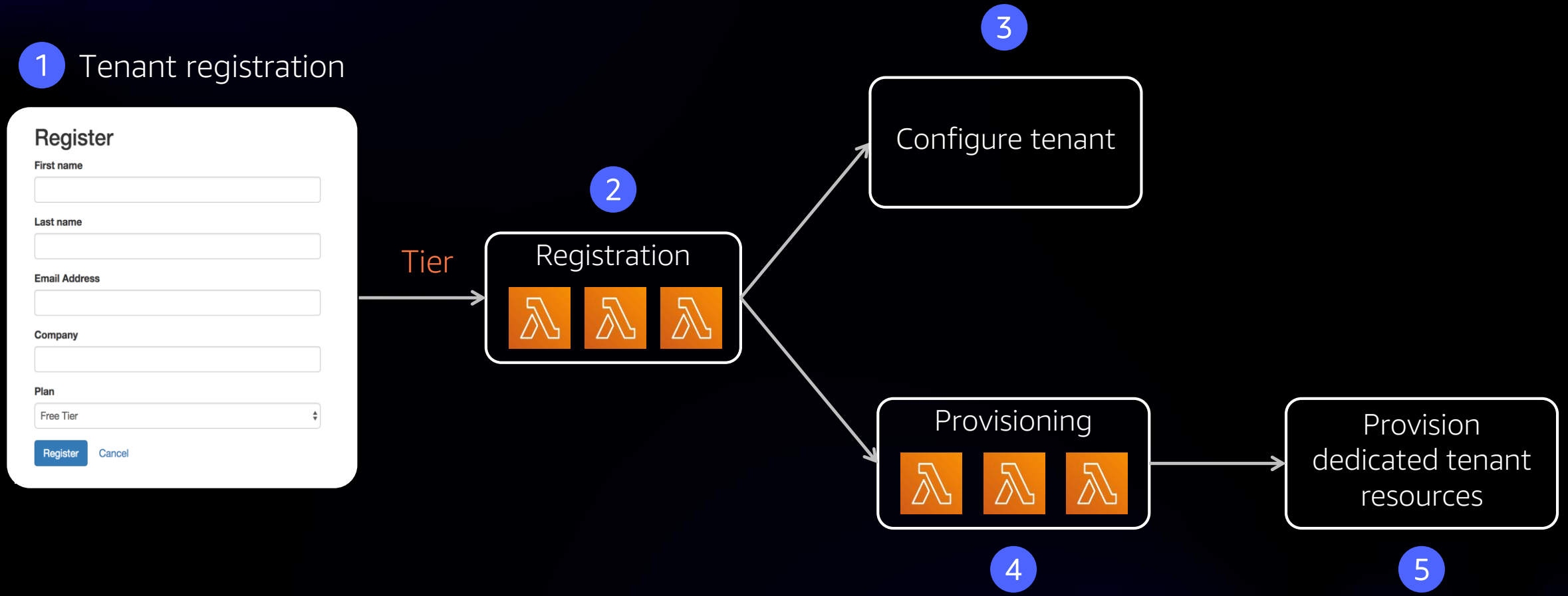
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Onboarding orchestration



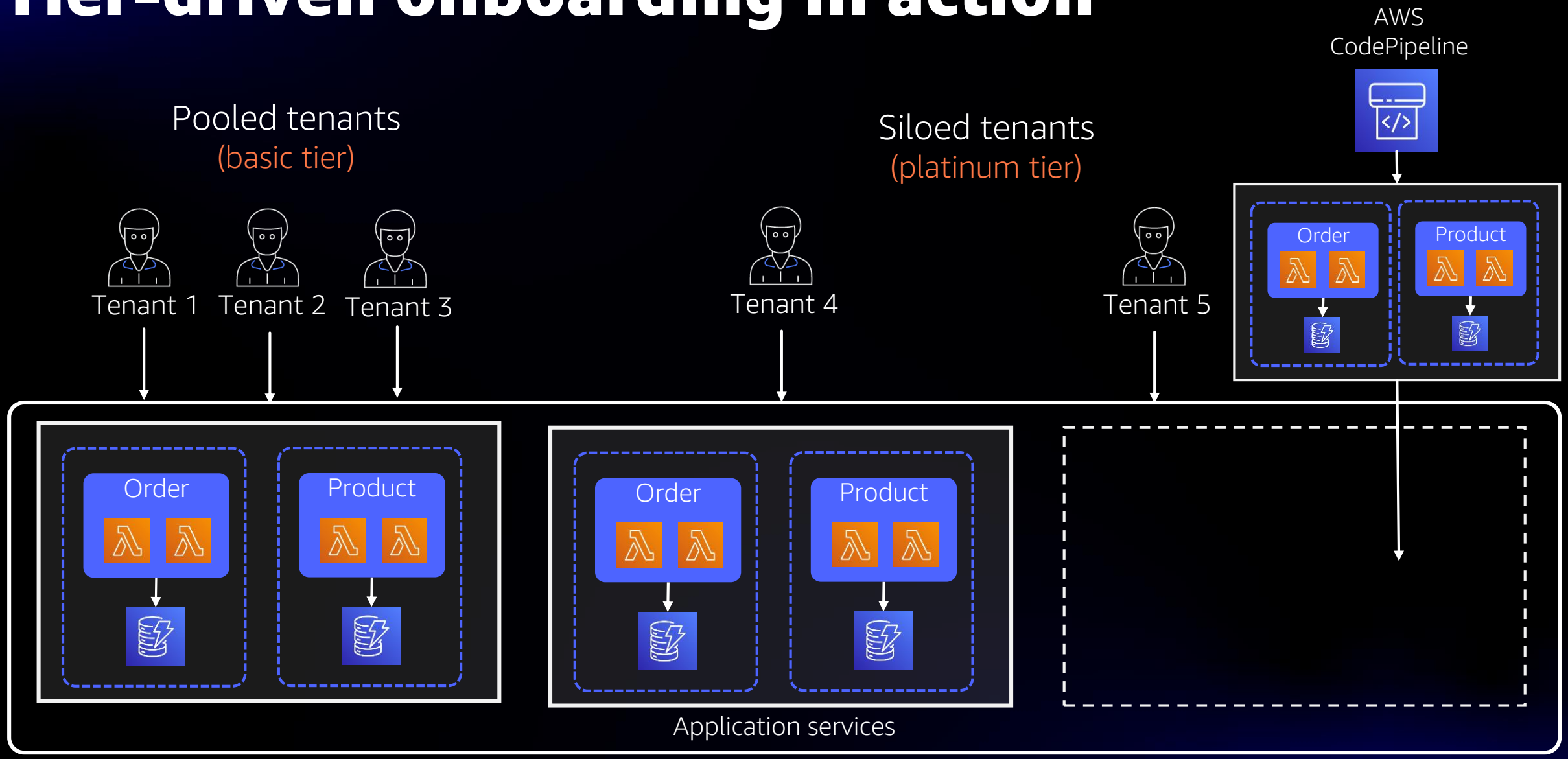
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tier-driven onboarding



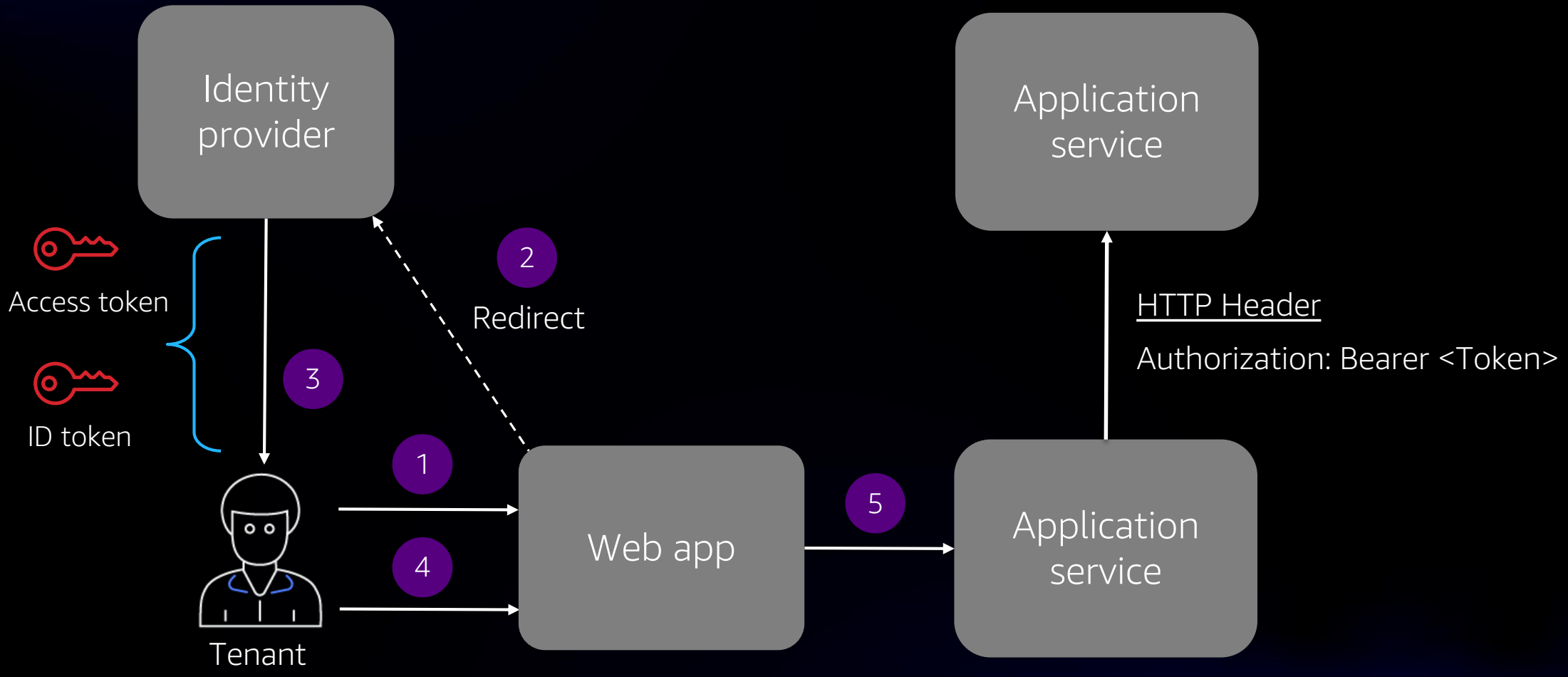
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tier-driven onboarding in action



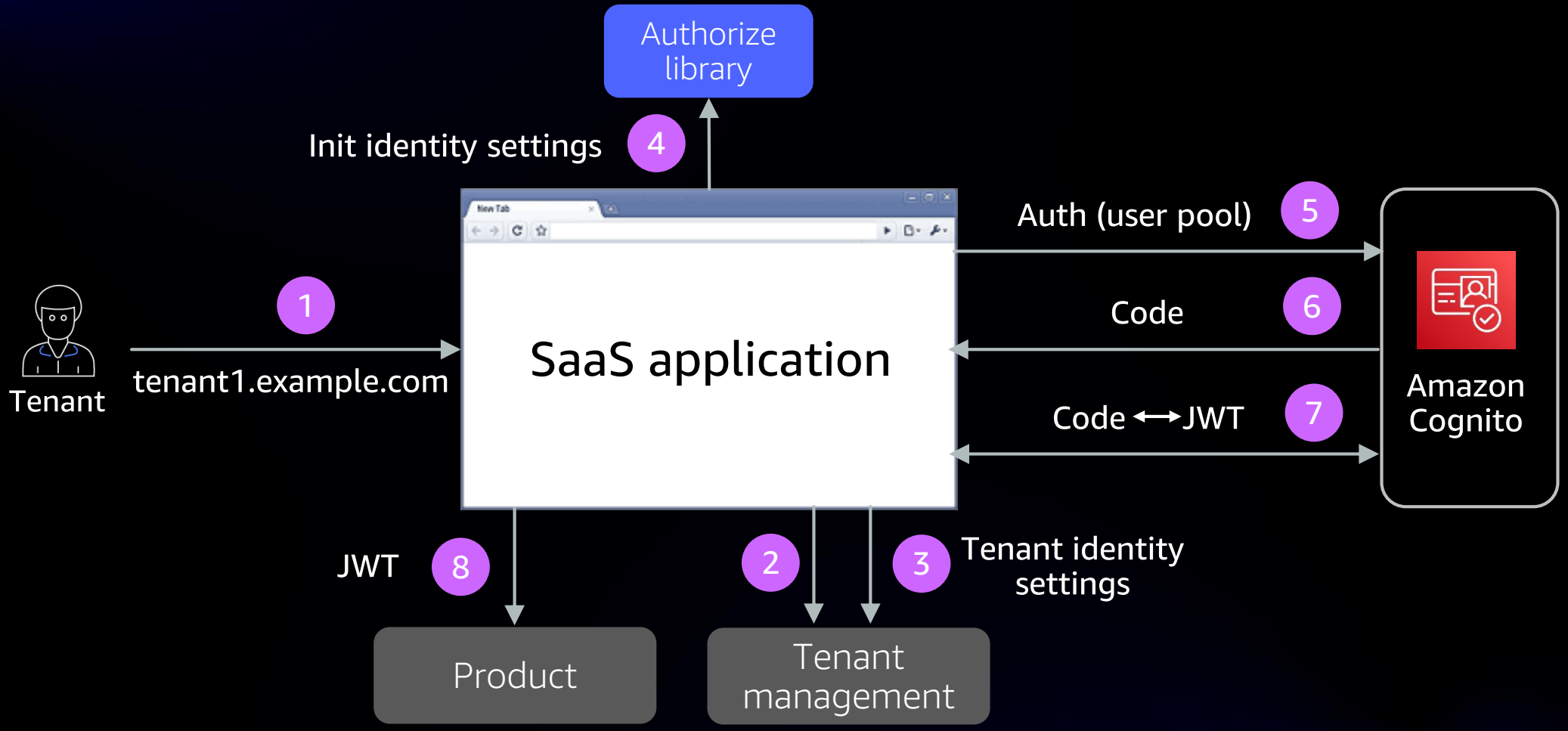
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tenant-aware identity



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

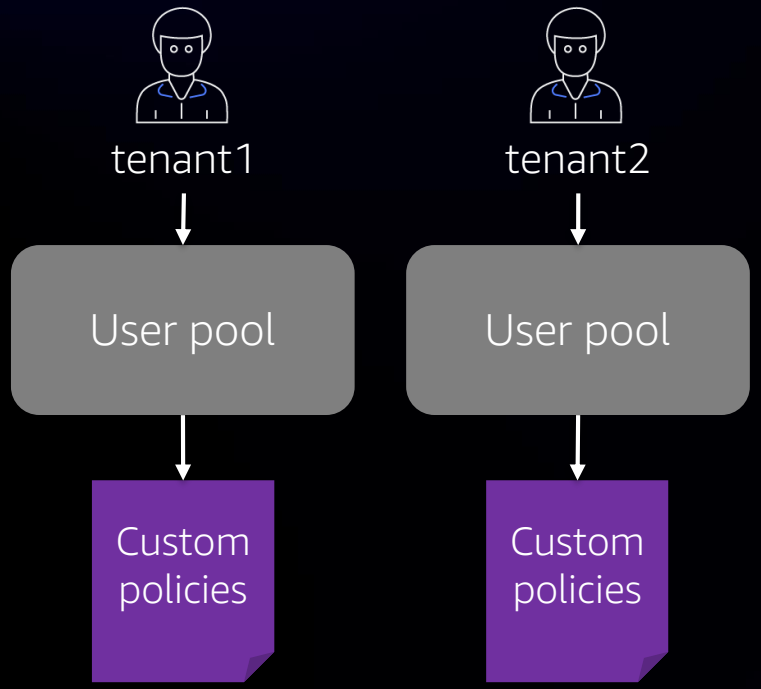
Tenant-aware identity flow



- Origin ⟶ company
- User pool mapping
- App ID

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tenant → User pool mapping

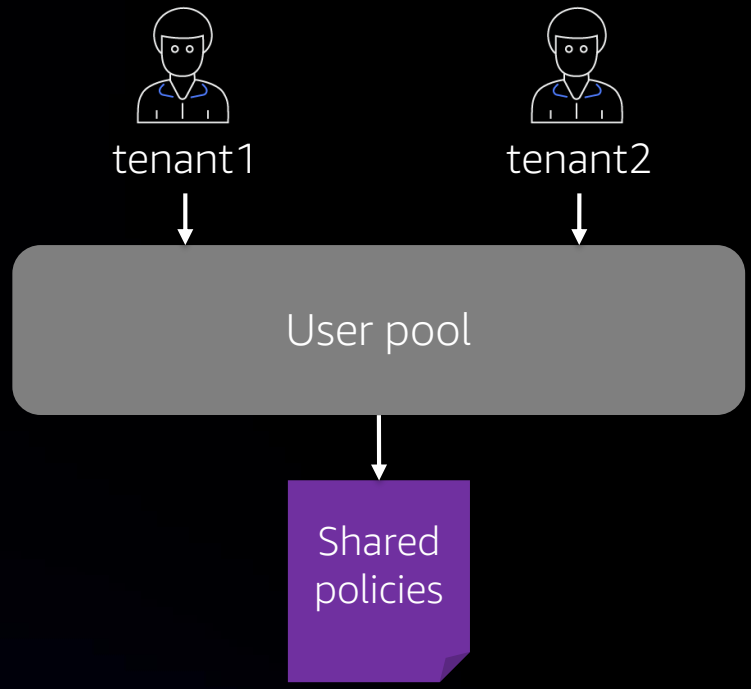


Pros

- Separate policies
- Better isolation

Cons

- Mapping required
- Scale
- Atypical OAuth flow



Pros

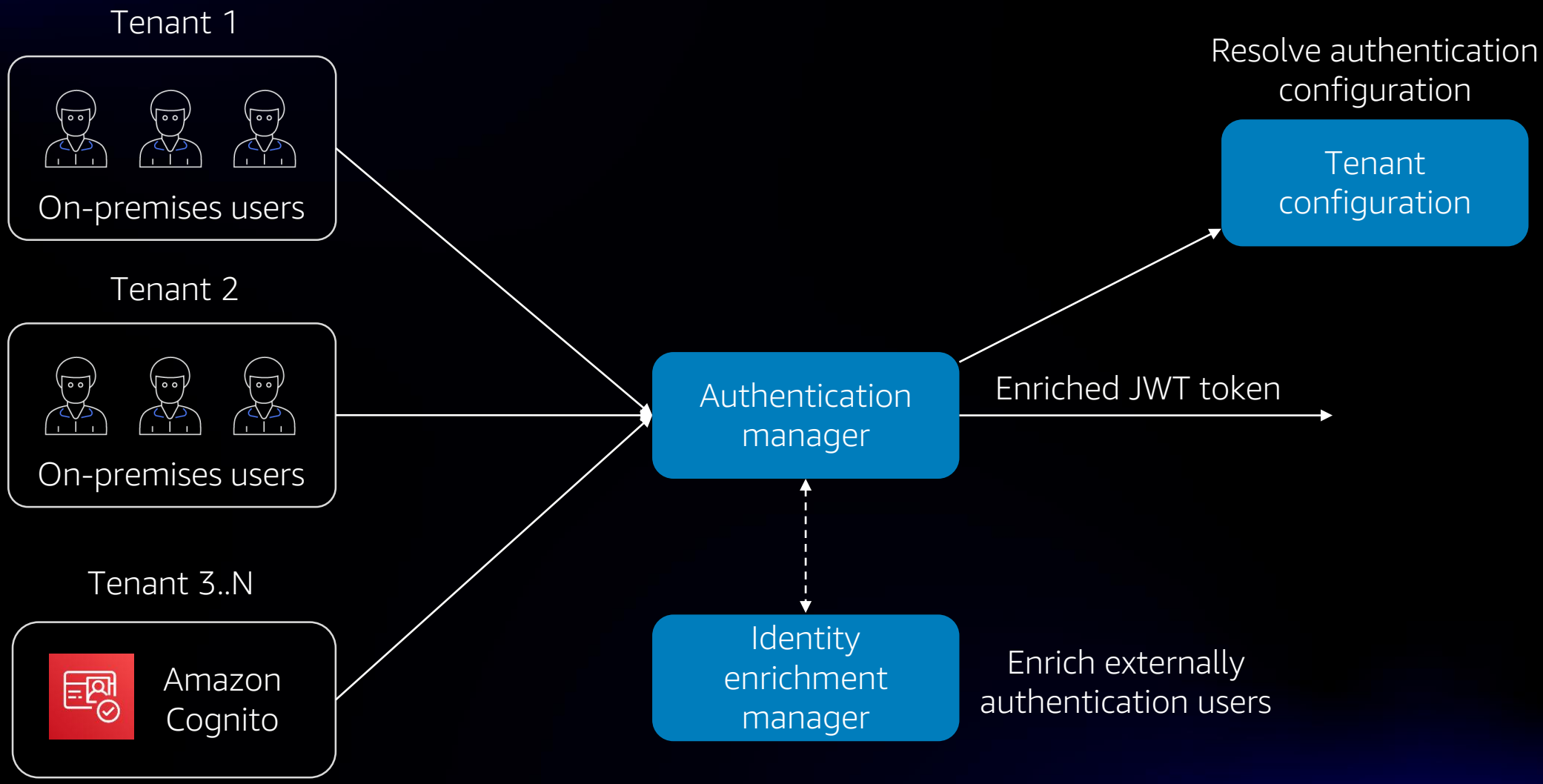
- No mapping
- Better OAuth flow
- Scale (maybe)

Cons

- No custom policies
- Isolation story

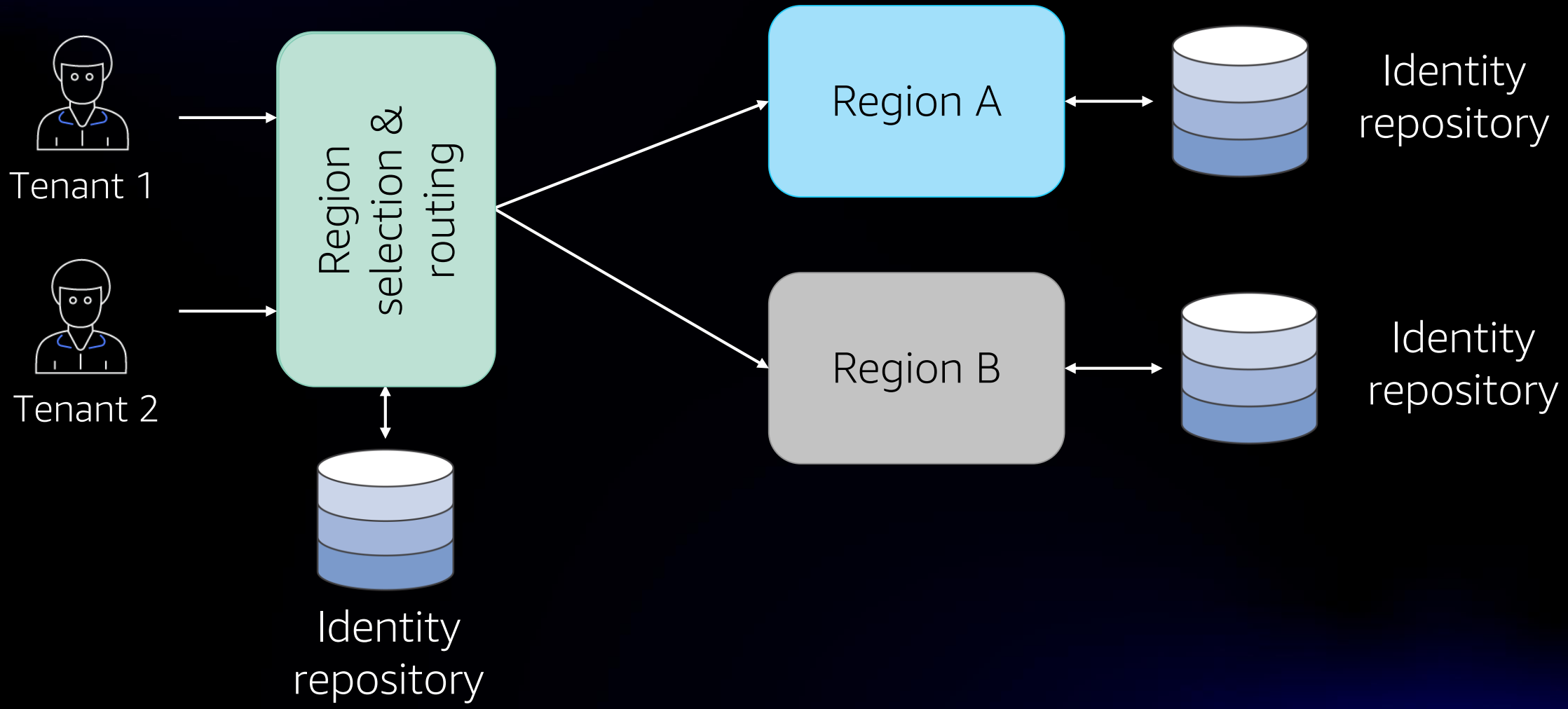
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hybrid identity model



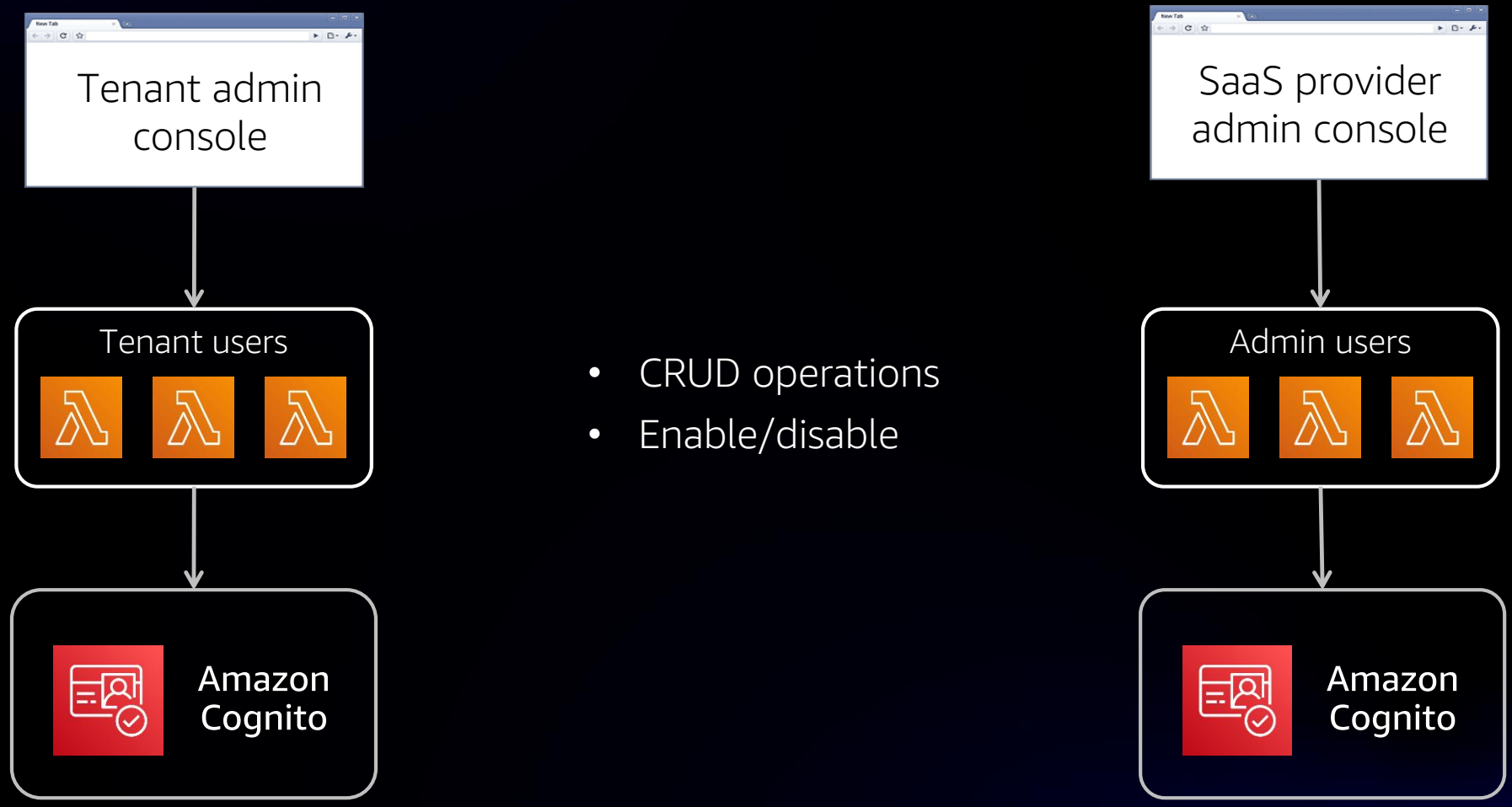
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-Region identity



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

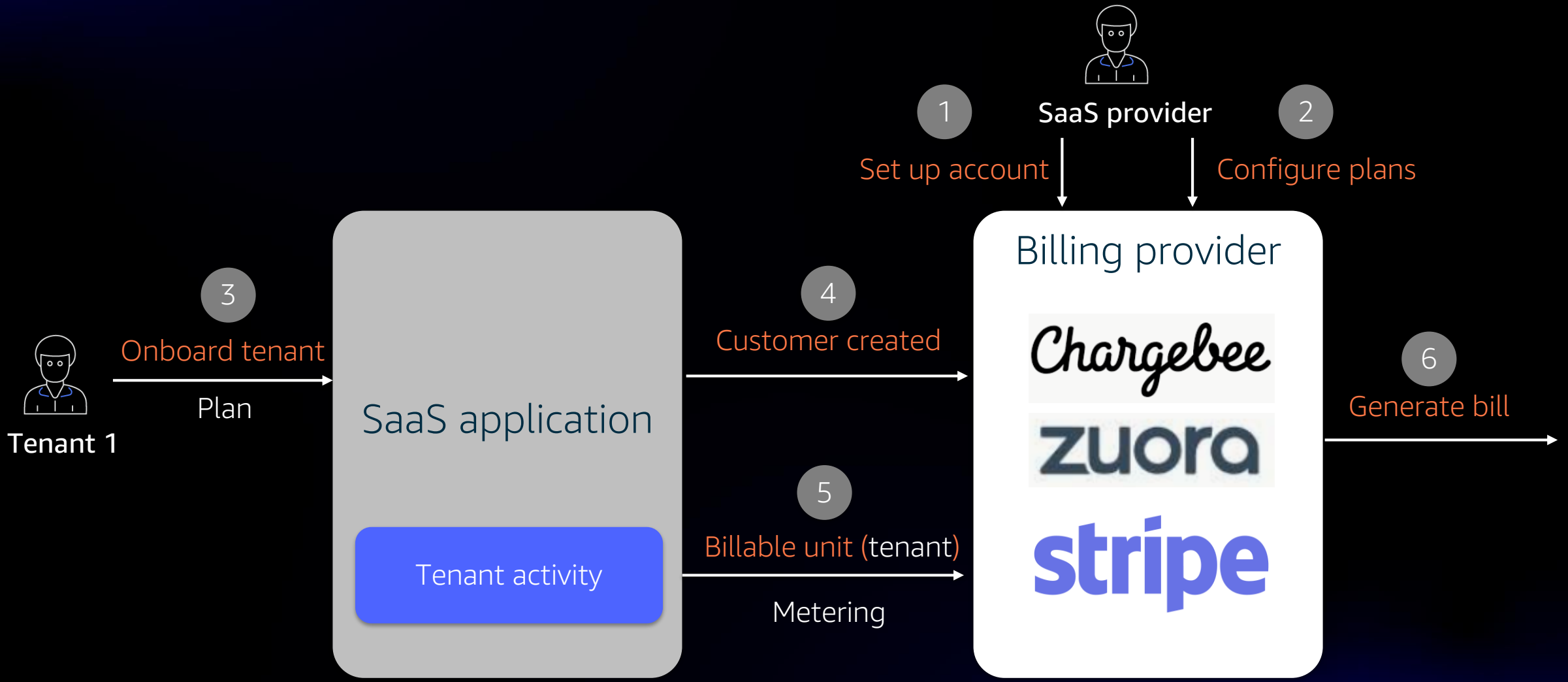
User management



- CRUD operations
- Enable/disable

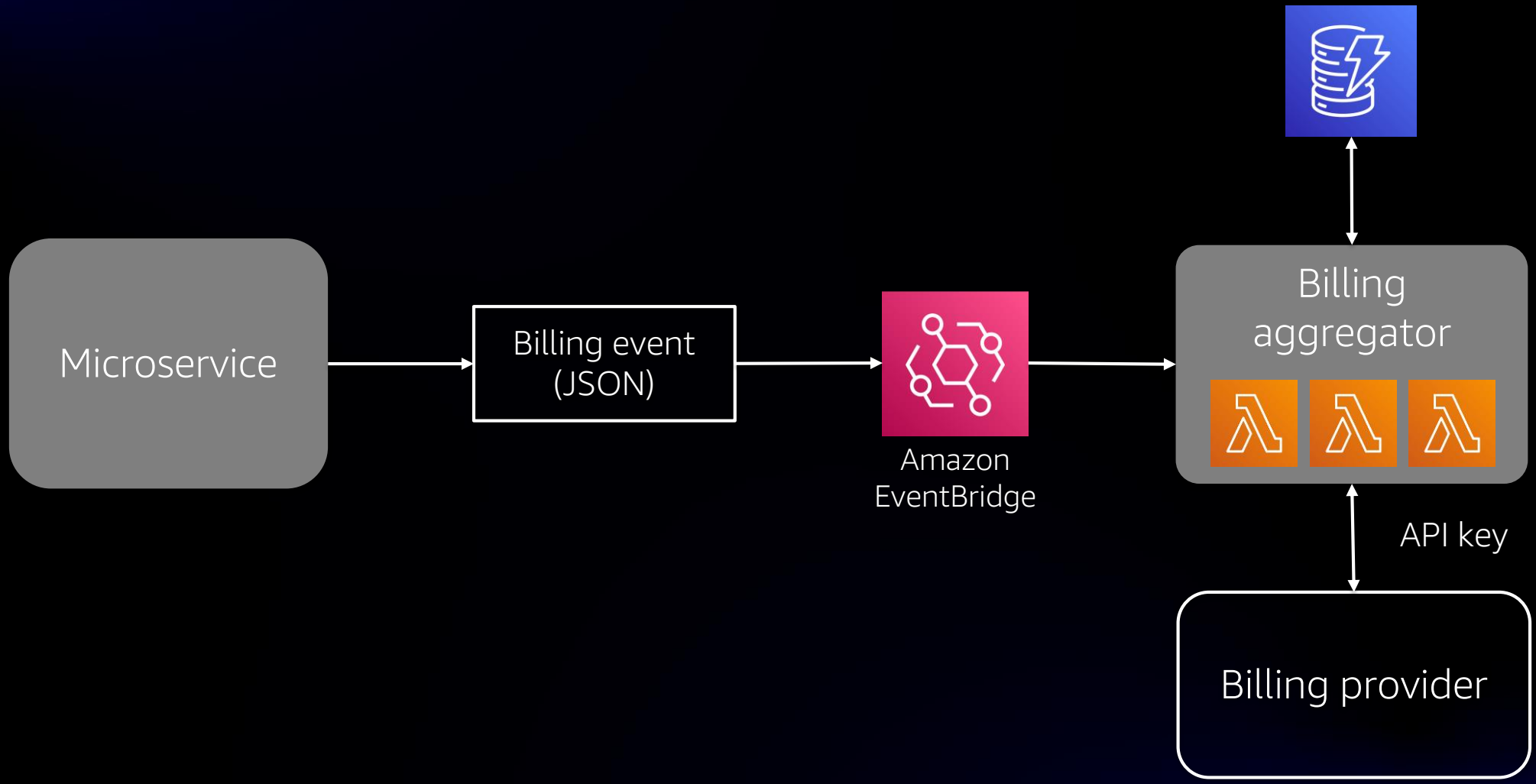
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Billing configuration and instrumentation



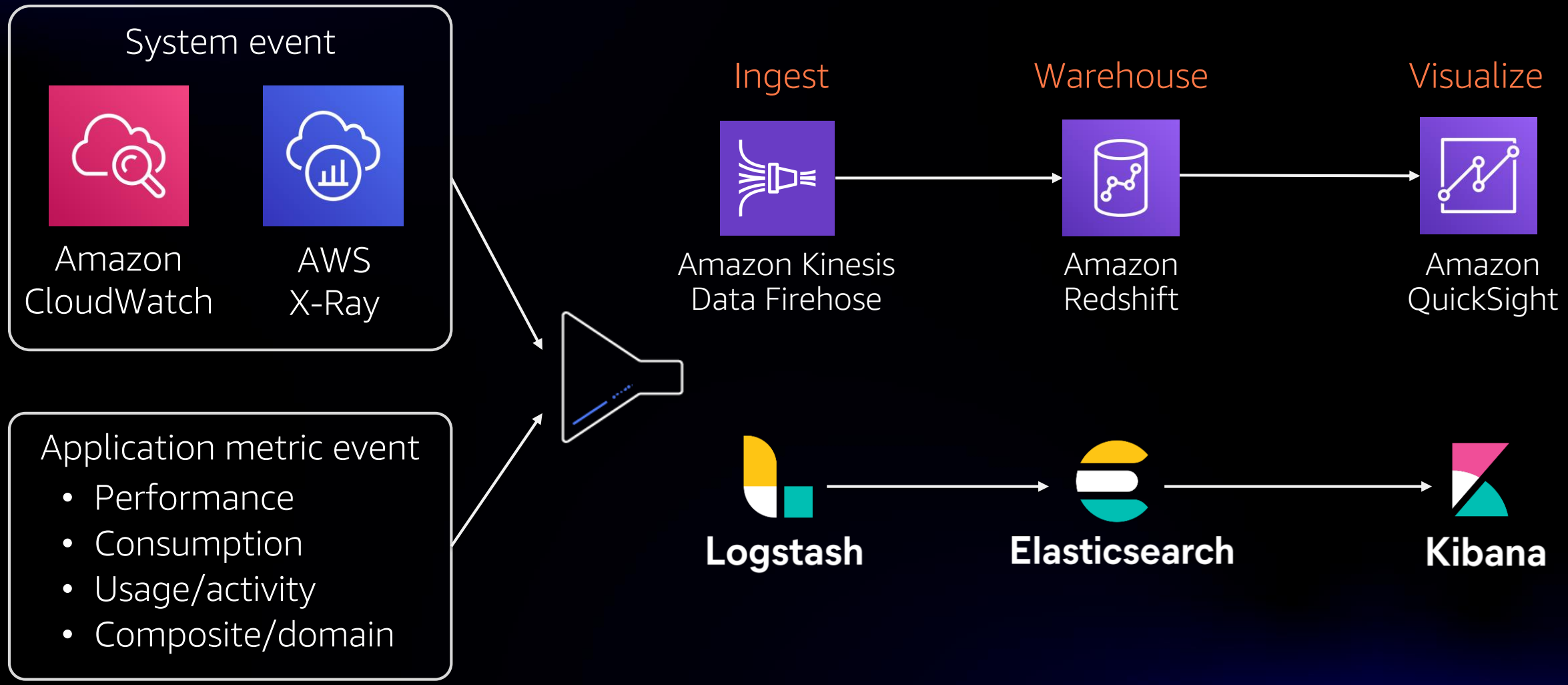
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Billable events



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

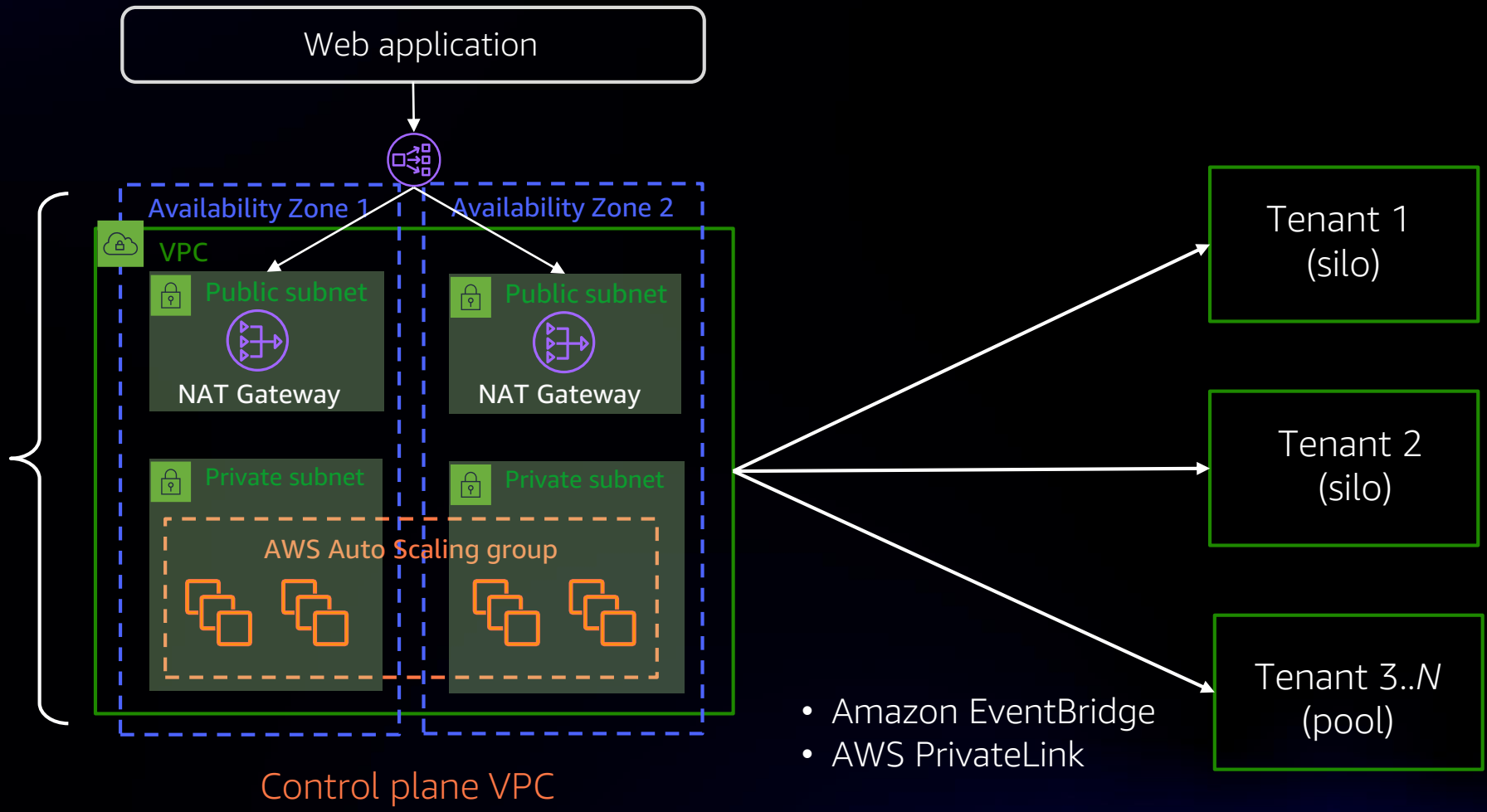
Metrics instrumentation and aggregation



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application plane integration

- Onboarding
- Identity
- Provisioning
- Management
- Metrics and analytics
- Tenant-aware logging
- Billing



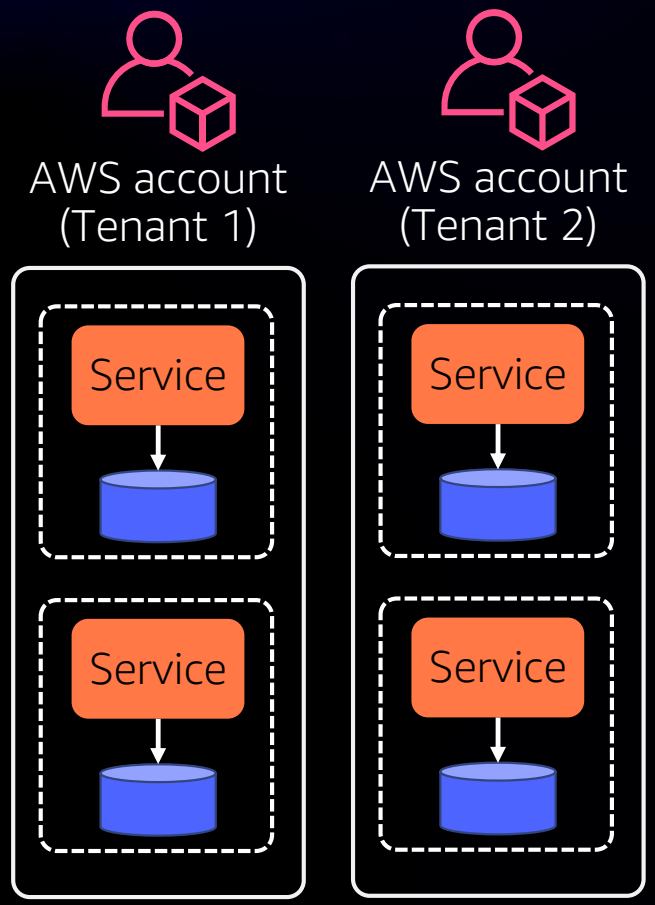
- Amazon EventBridge
- AWS PrivateLink

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

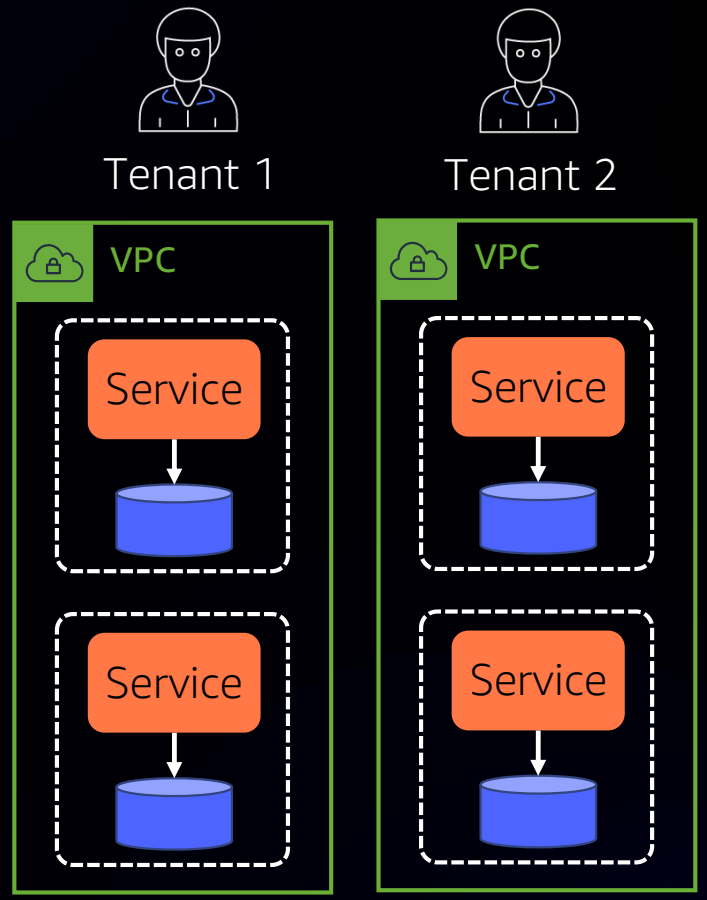
Application plane patterns

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

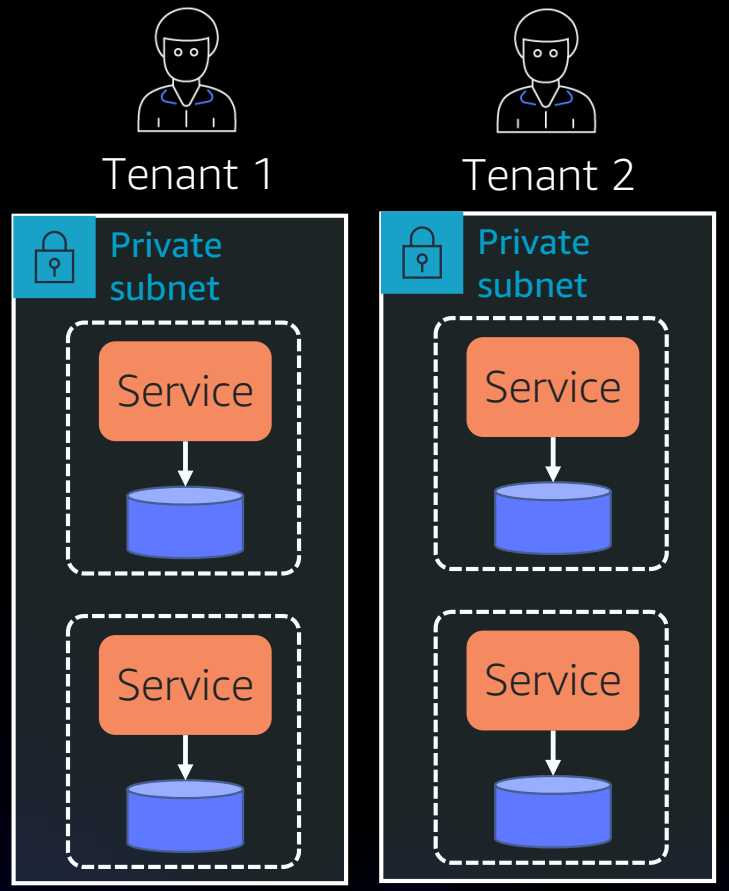
Coarse-grained full stack silo



Account per tenant



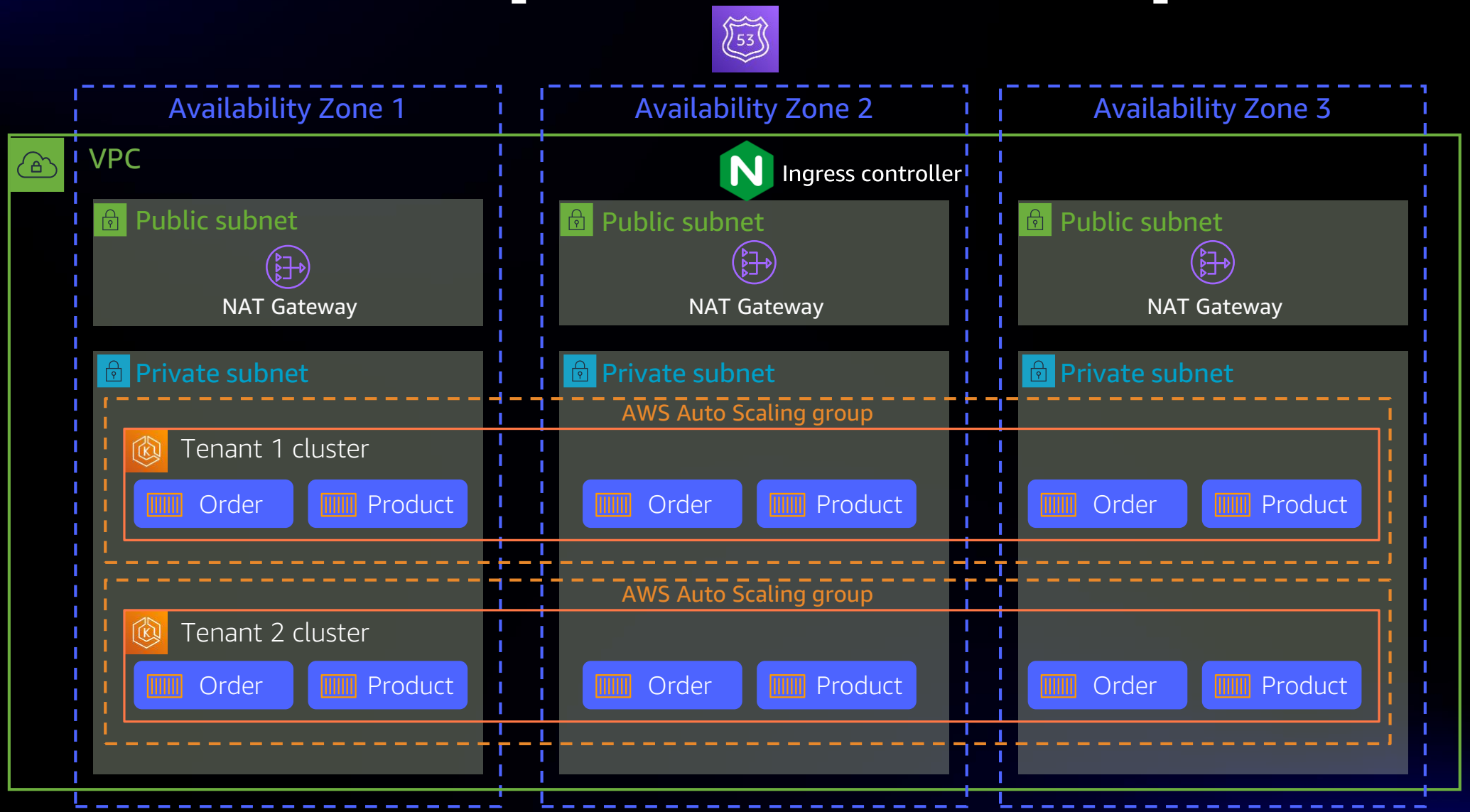
VPC per tenant



Subnet per tenant

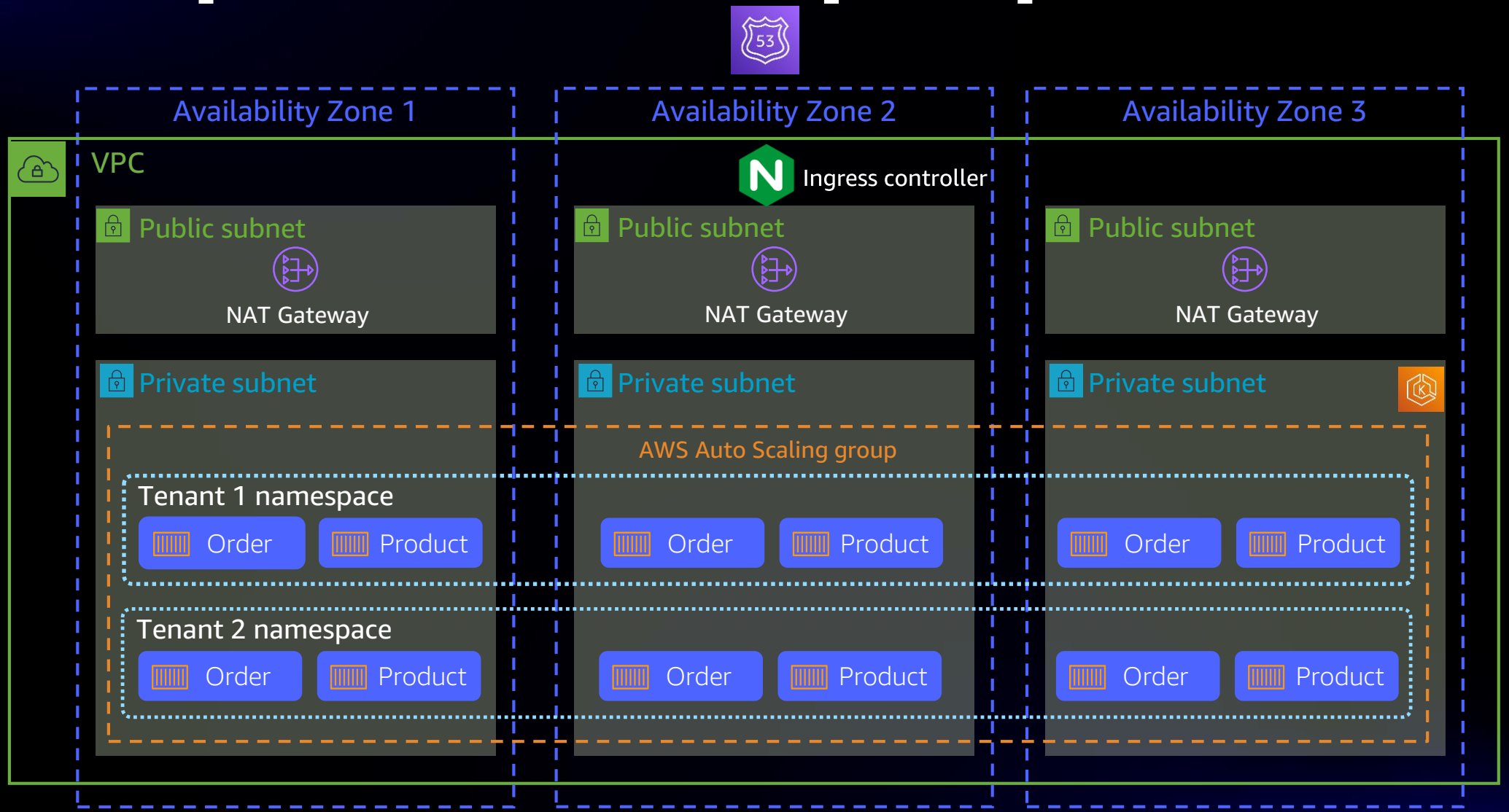
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EKS compute silo: Cluster per tenant



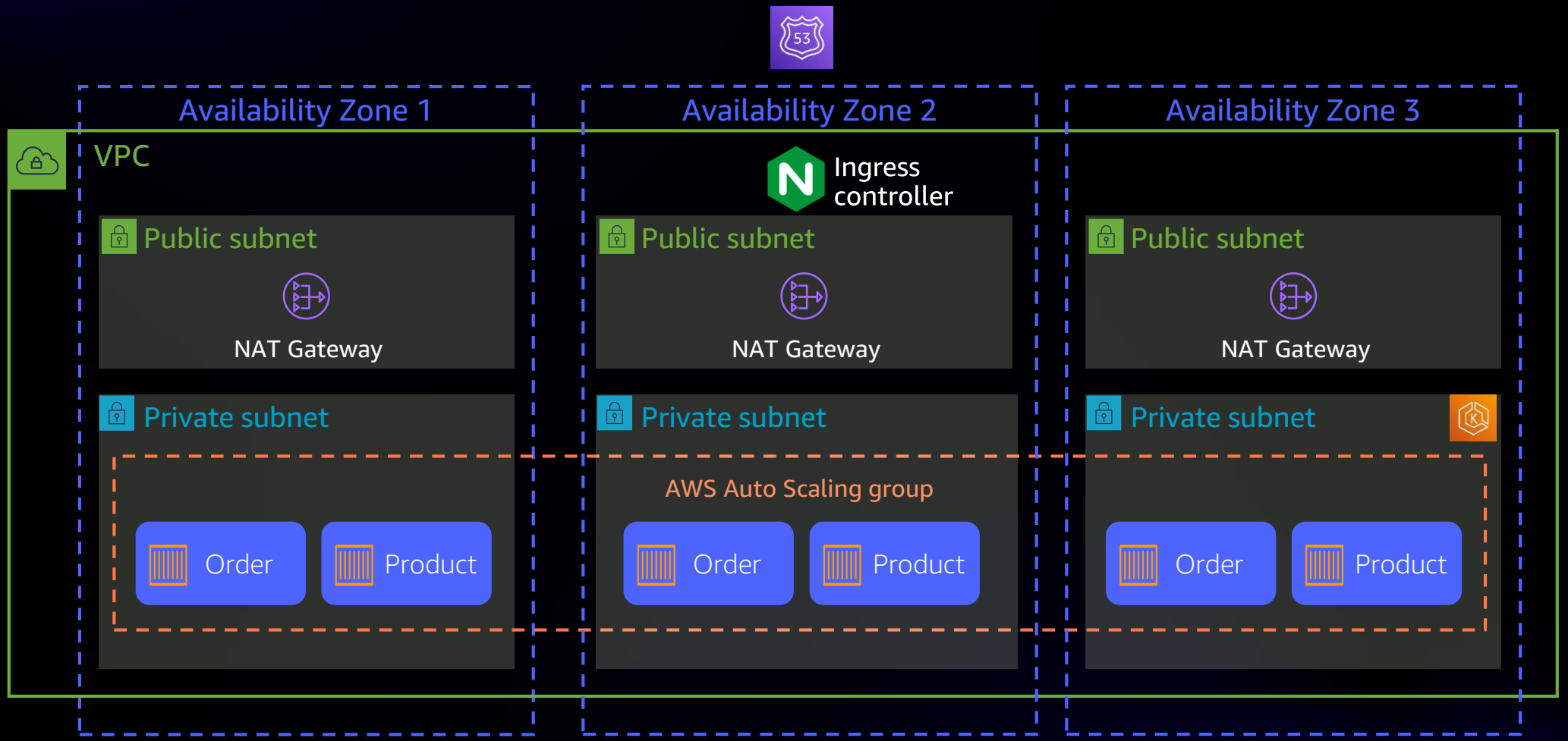
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

EKS compute silo: Namespace per tenant



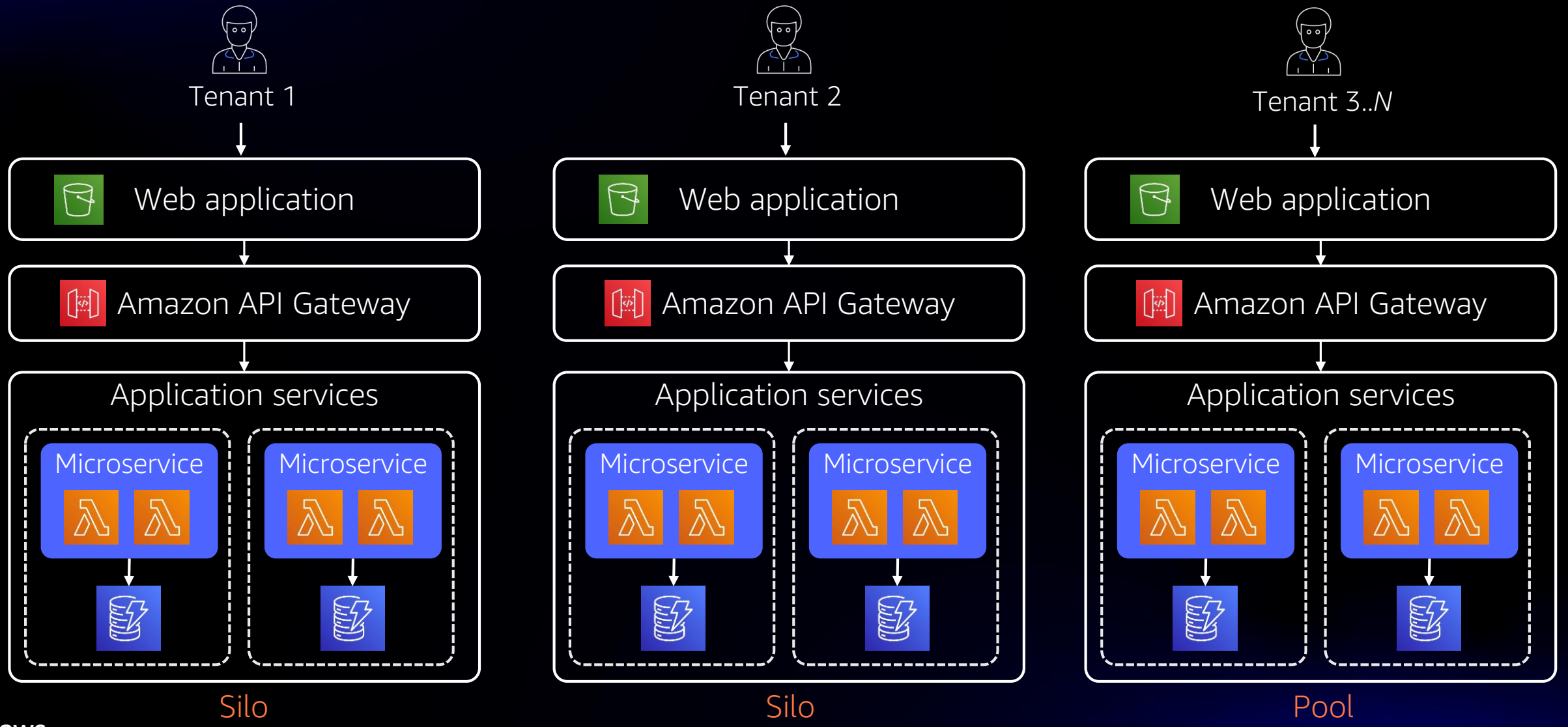
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

EKS compute pool



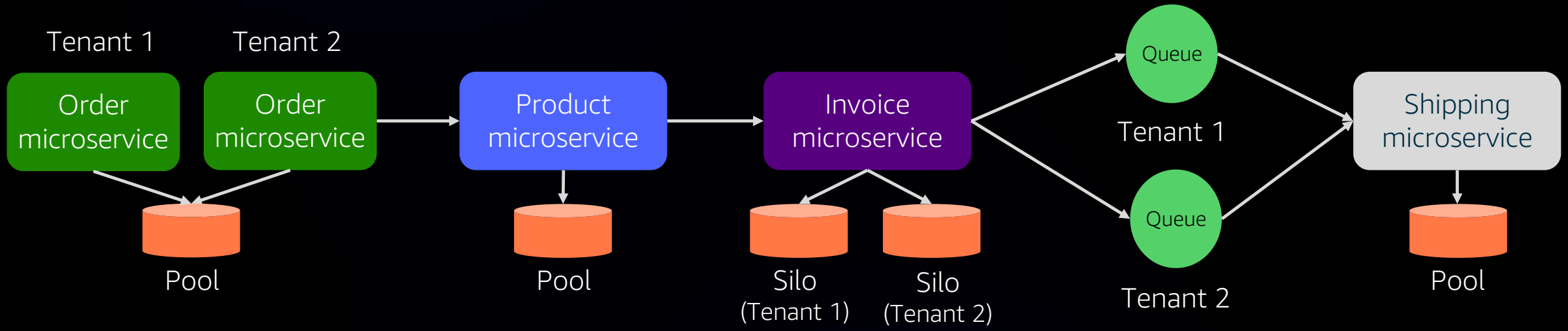
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Full-stack serverless silo and pool



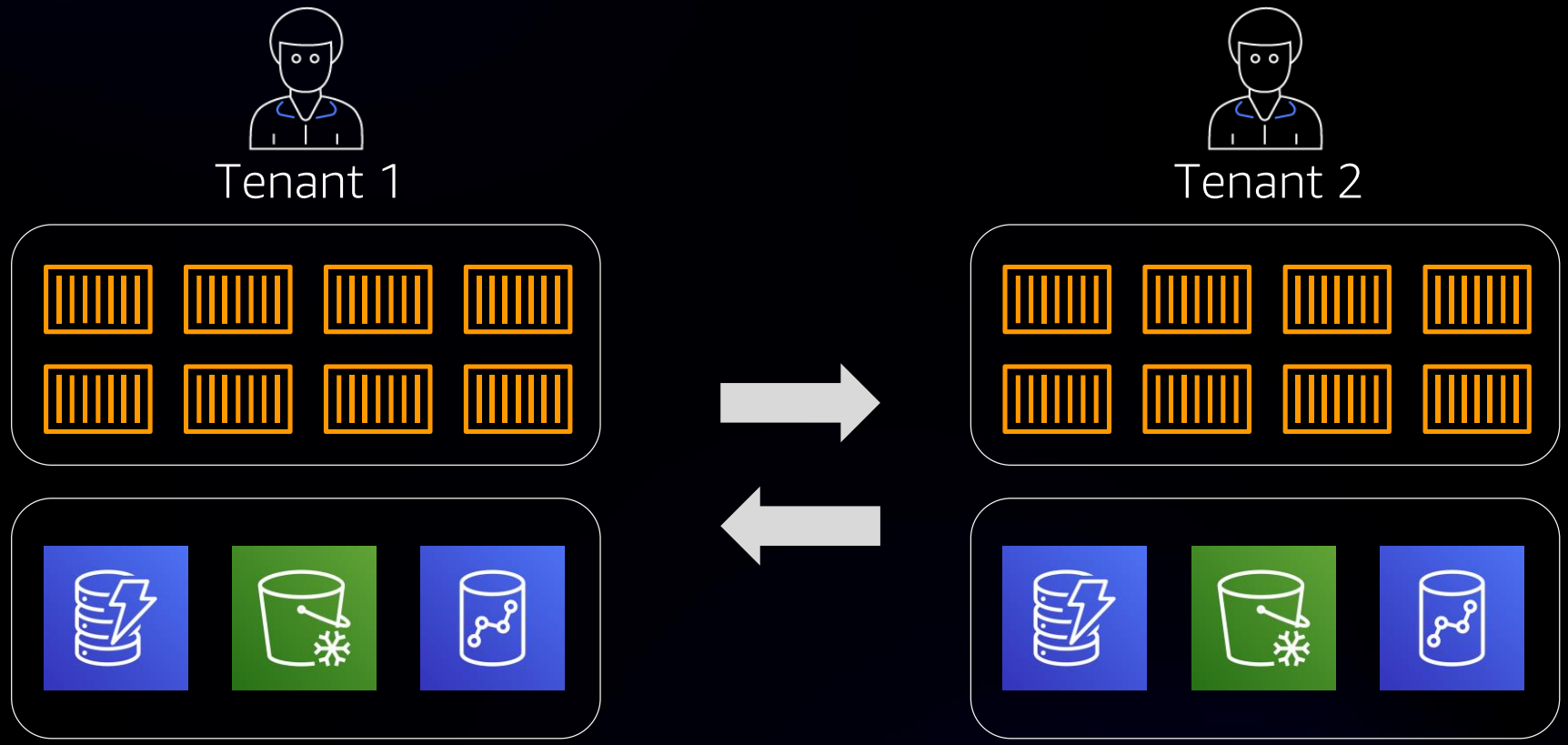
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resource-based silo and pool deployment



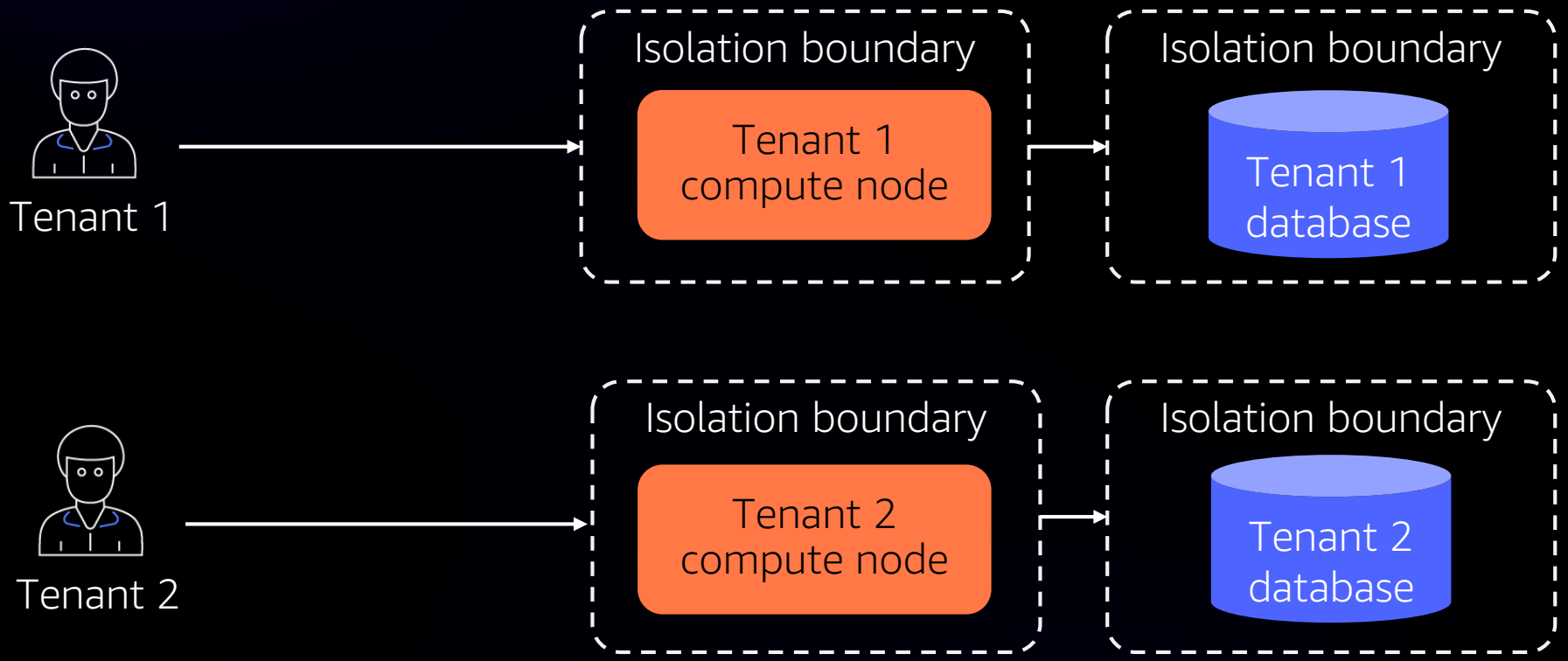
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tenant isolation



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resource-level isolation (silo)

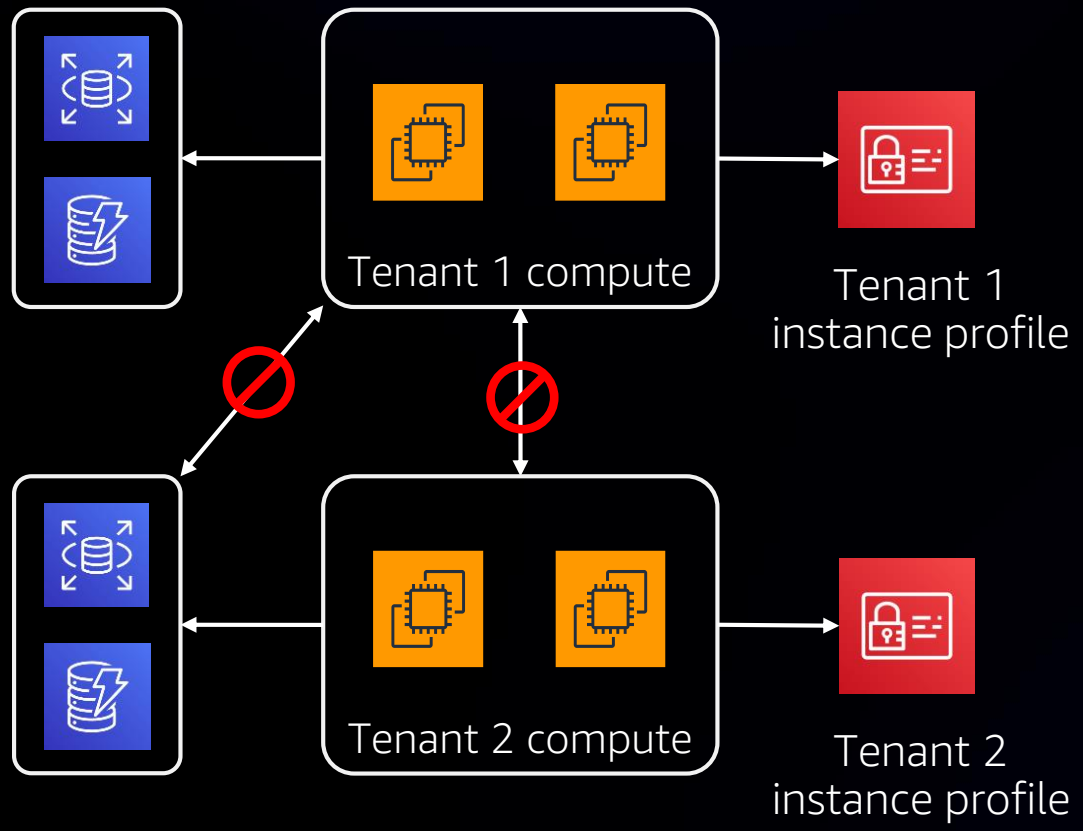


Unit of isolation is an entire resource level

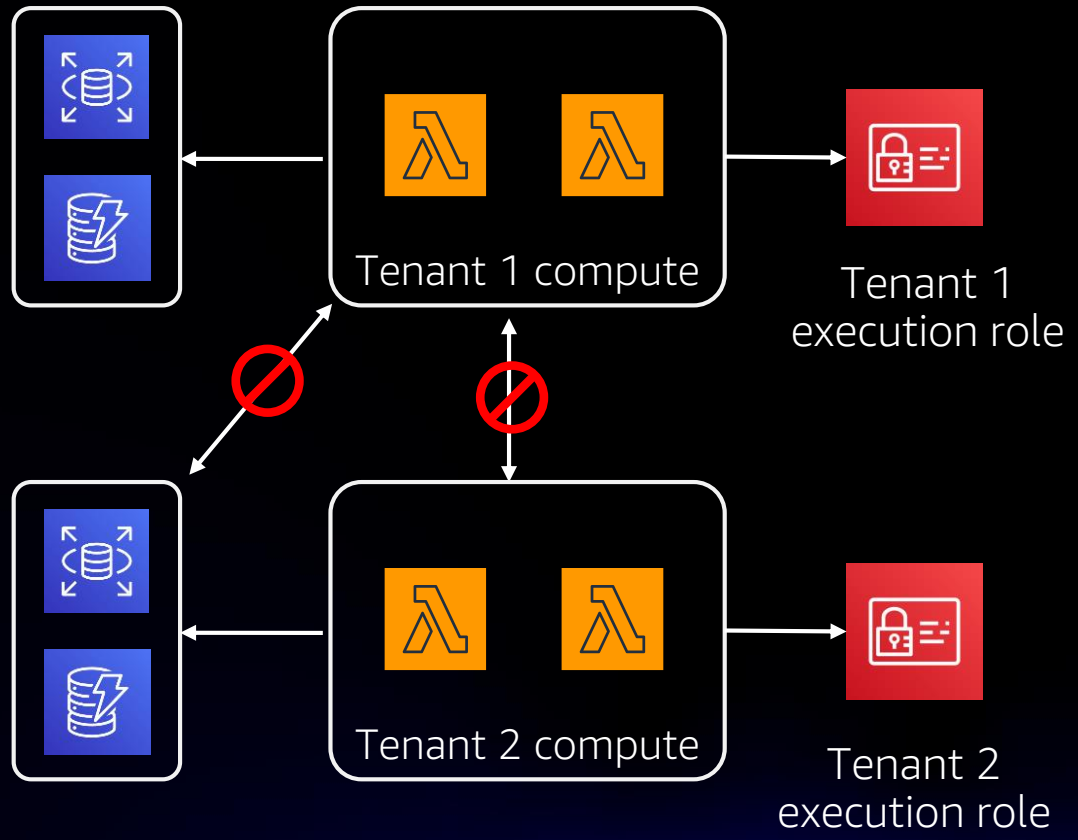
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deployment-driven resource isolation (silo)

Silo with Amazon EC2

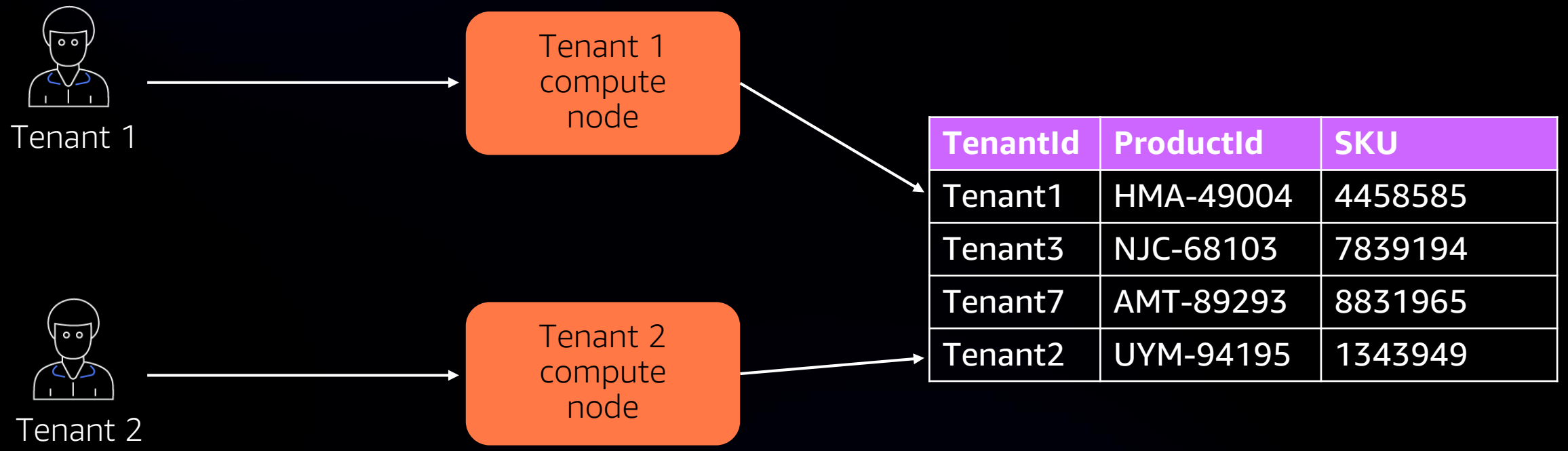


Silo with AWS Lambda



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Item-level isolation (pool)

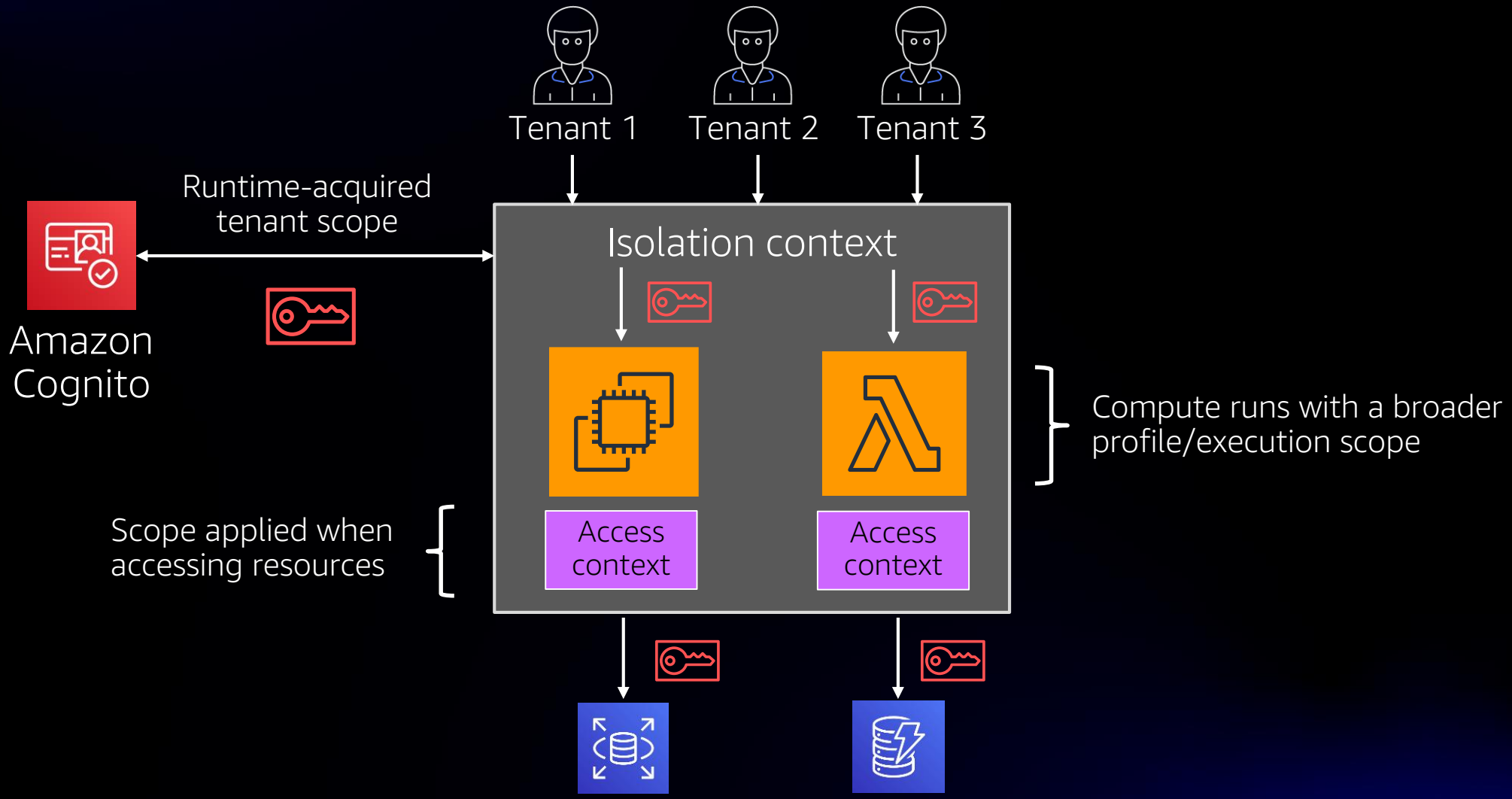


TenantId	ProductId	SKU
Tenant1	HMA-49004	4458585
Tenant3	NJC-68103	7839194
Tenant7	AMT-89293	8831965
Tenant2	UYM-94195	1343949

Unit of isolation is specific tenant item(s) within a resource

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Runtime enforced isolation



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Item-level isolation with Amazon DynamoDB

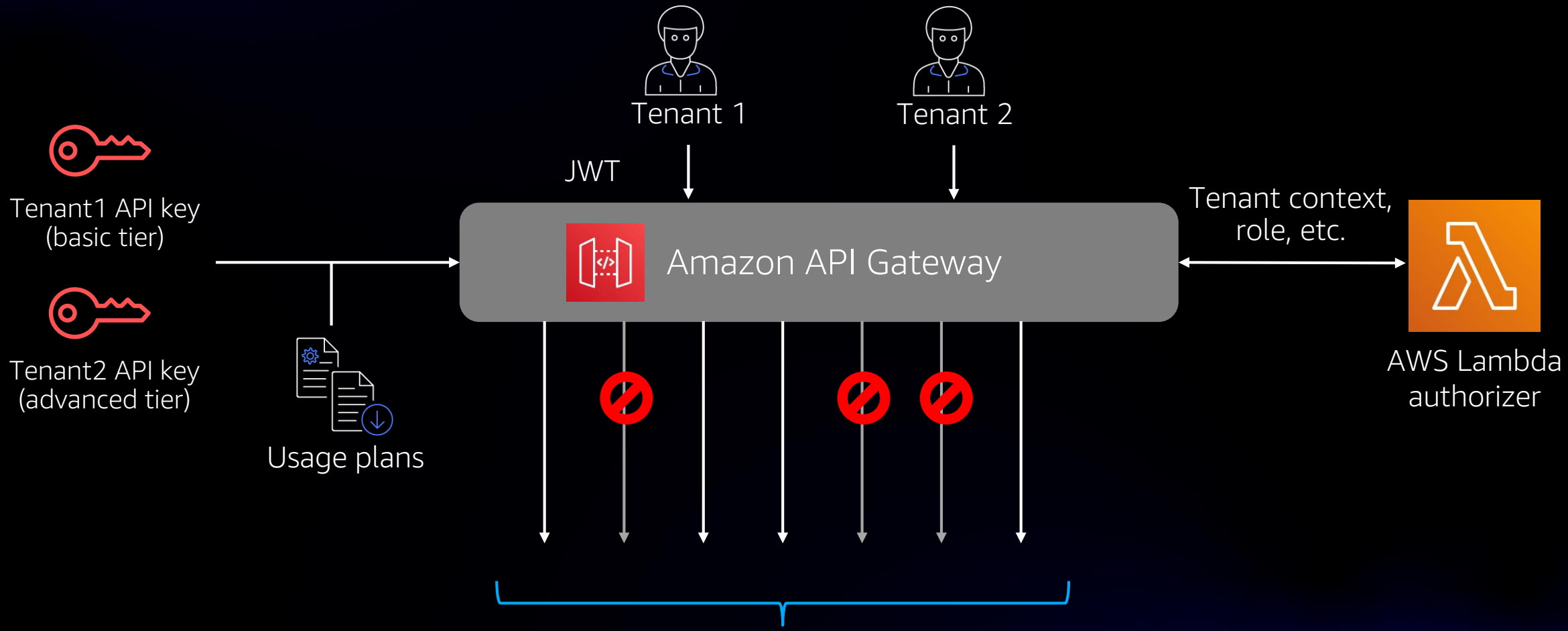
```
{
  "Sid": "TenantReadOnlyOrderTable",
  "Effect": "Allow",
  "Action": [
      "dynamodb:GetItem",
      "dynamodb:BatchGetItem",
      "dynamodb:Query",
      "dynamodb:DescribeTable"
  ],
  "Resource": [
      "arn:aws:dynamodb:[region]:table/Order"
  ],
  "Condition": {
      "ForAllValues:StringEquals": {
          "dynamodb:LeadingKeys": [
              "tenant1"
          ]
      }
  }
}
```

DynamoDB table

Partition key	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

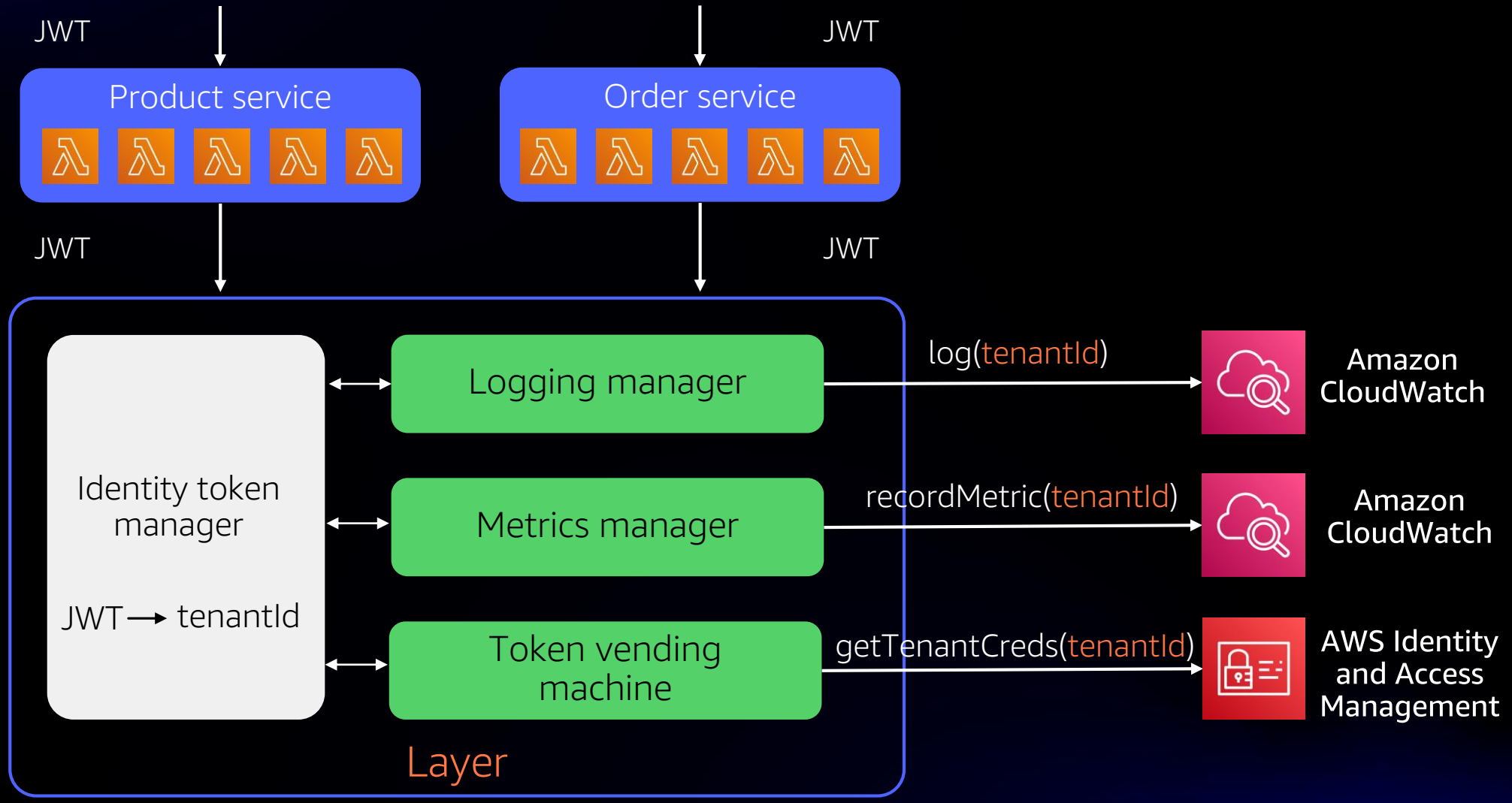
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tier-based throttling



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

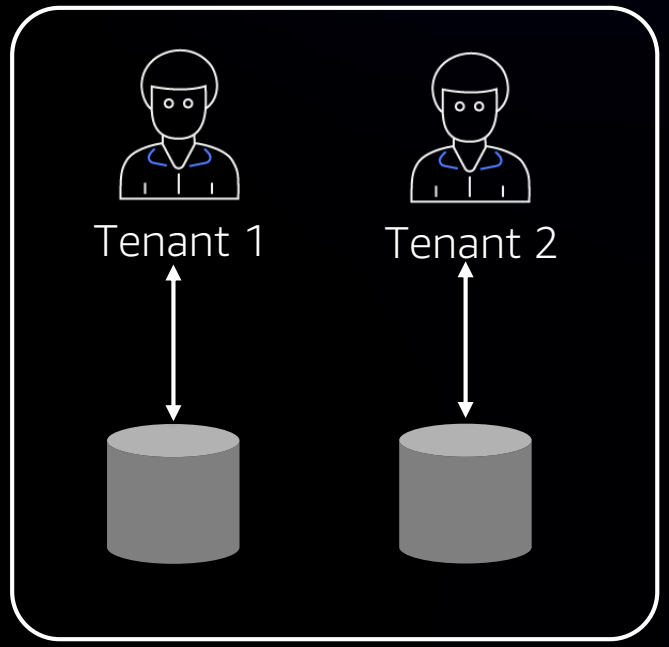
Multi-tenant microservice libraries



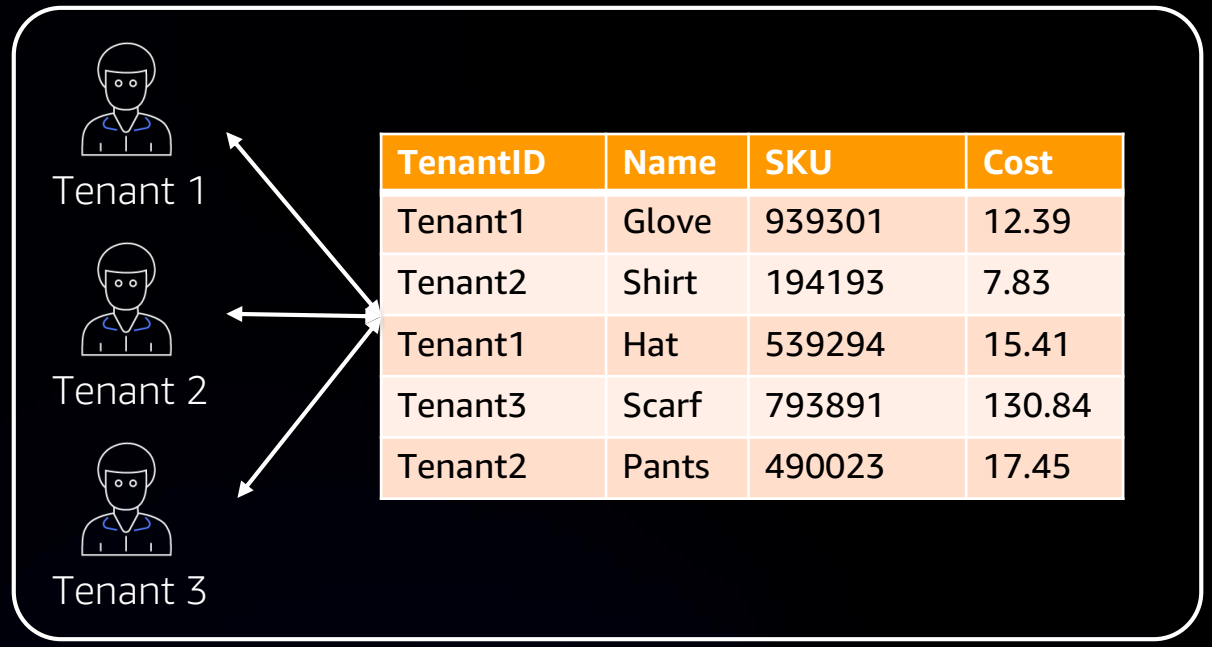
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data partitioning

Silo model



Pool model

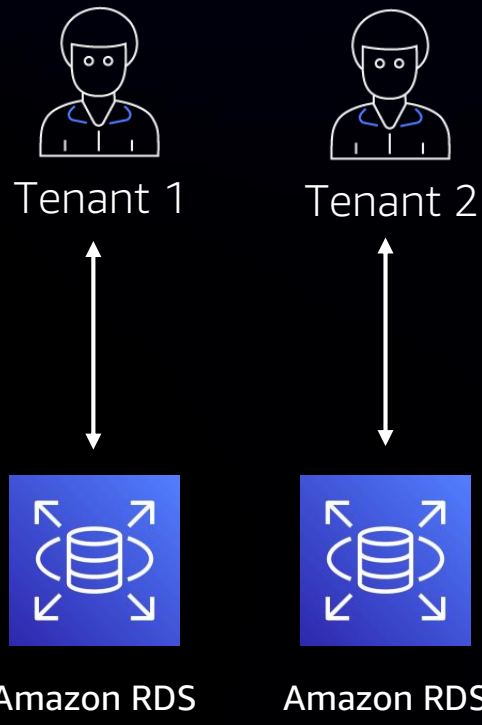


TenantID	Name	SKU	Cost
Tenant1	Glove	939301	12.39
Tenant2	Shirt	194193	7.83
Tenant1	Hat	539294	15.41
Tenant3	Scarf	793891	130.84
Tenant2	Pants	490023	17.45

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

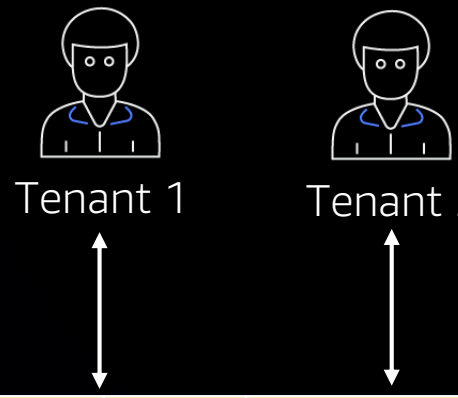
Data partitioning with Amazon RDS

Silo model



Separate instance/database per tenant

Pool model



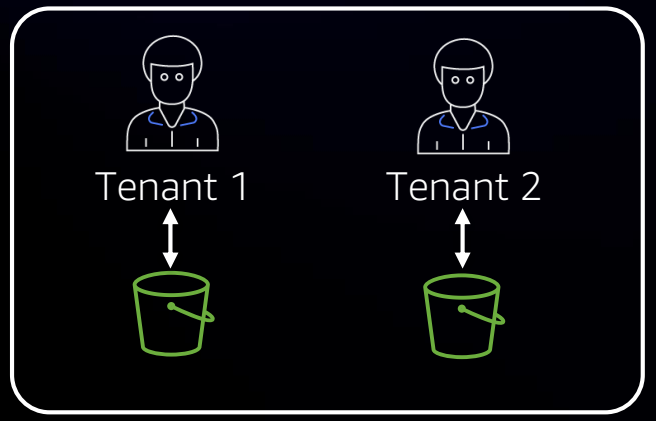
TenantID	Name	SKU	Cost
Tenant1	Glove	939301	12.39
Tenant2	Shirt	194193	7.83
Tenant1	Hat	539294	15.41
Tenant2	Pants	490023	17.45

One database with tenant-indexed data

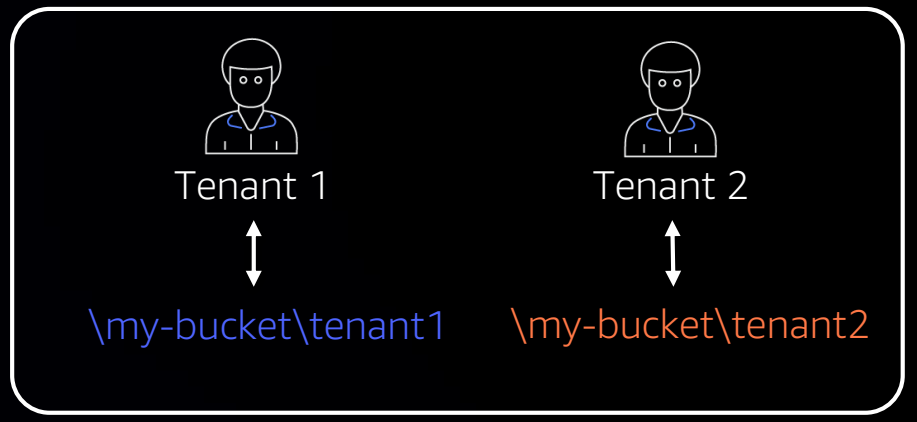
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data partitioning with Amazon S3

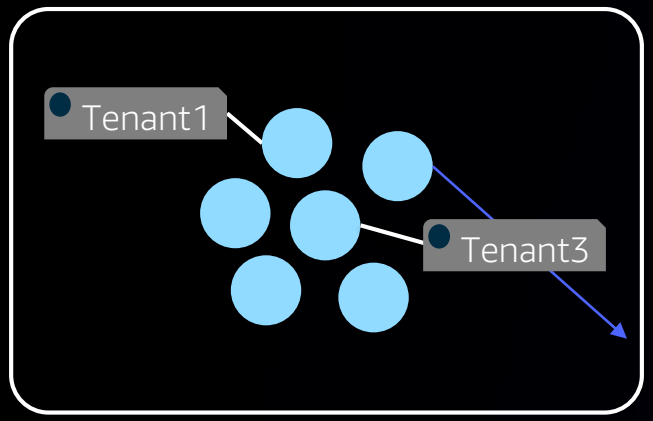
Bucket per tenant



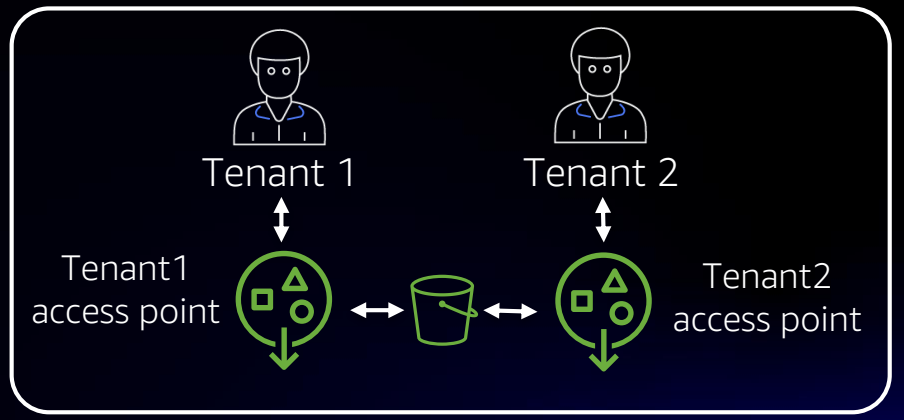
Prefix per tenant



Tag per tenant



Access point per tenant

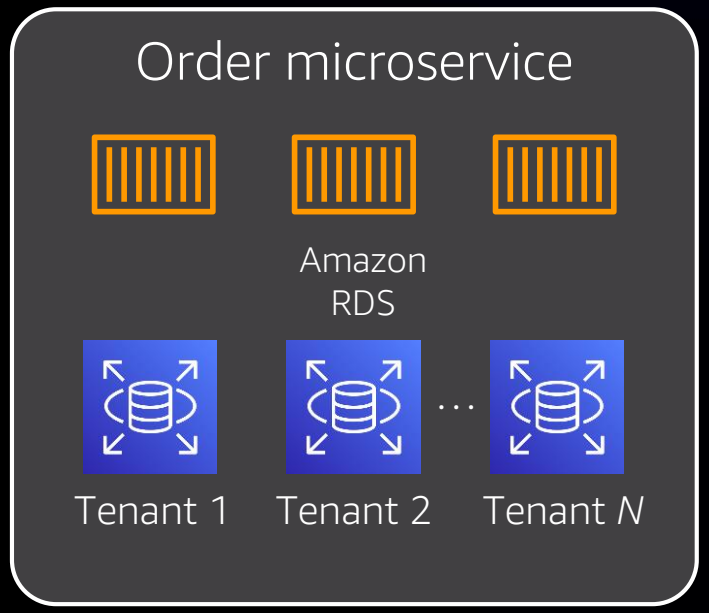


aws

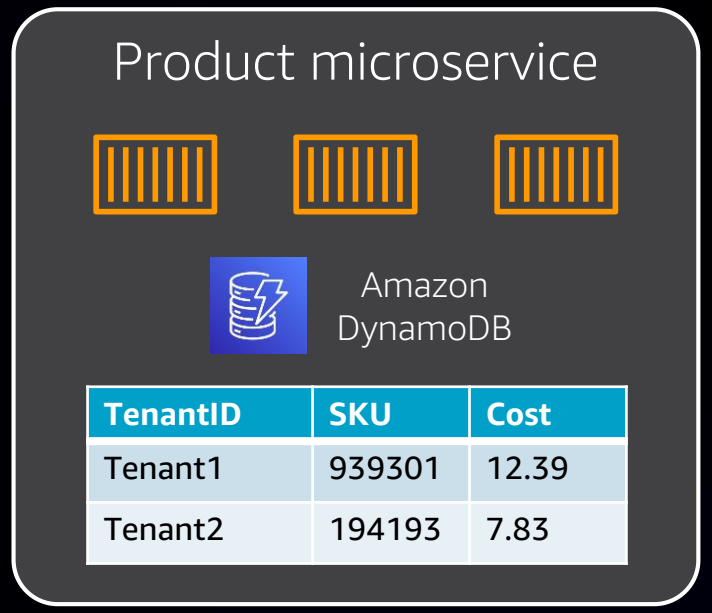
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Domain-driven data partitioning

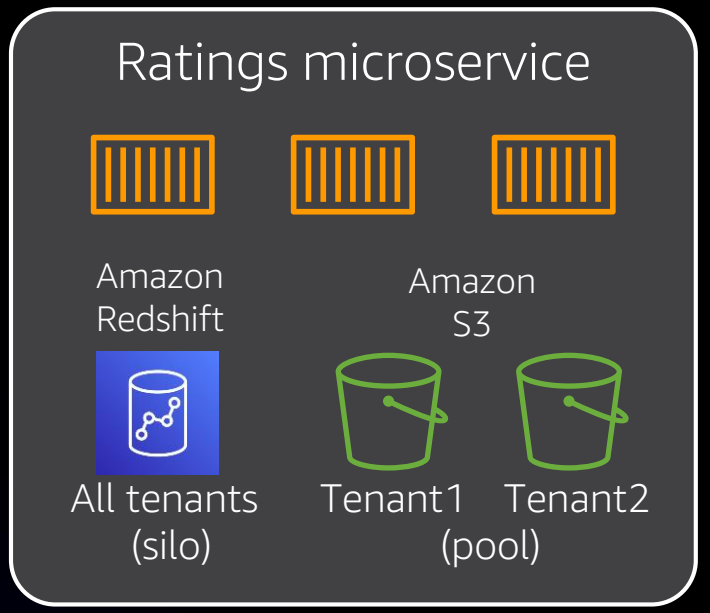
Partitioning and isolation strategy should be decided on a service-by-service basis



Database per tenant (silo)



Shared database for all tenants (pool)



Mixed mode – silo and pool models

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Takeaways

- There’s no universal SaaS blueprint
- Multi-tenancy does not require shared infrastructure
- Control plane services are essential to SaaS agility and innovation
- Each AWS stack/service may require a unique approach
- Silo and pool can be applied at the resource/microservice level
- Tiering, performance, and noisy neighbor will shape how and where you apply these patterns
- Find the combination of patterns that best matches your needs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Additional SaaS sessions

Breakout sessions

ARC306: SaaS architecture patterns: From concept to implementation

ARC405: Inside a working serverless SaaS reference solution

ARC402: Amazon EKS SaaS deep dive: A multi-tenant EKS SaaS solution

GPS209: How to grow your SaaS business and drive revenue with AWS Marketplace

Workshops

ARC403: Hands-on serverless SaaS: Building a serverless SaaS solution on AWS

ARC404: Hands-on Amazon EKS SaaS: Building a multi-tenant SaaS solution on AWS

Chalk talks

ARC320: From Monolith to SaaS: Discover the way

GPS311: Building multi-tenant-aware SaaS microservices on AWS

OPN309: AWS SaaS Boost vNext: Enabling new patterns and extensibility

ARC401: Serverless SaaS deep dive: Inside a multi-tenant serverless solution

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Tod Golding

todg@amazon.com



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.