
AWS
re:Invent

ARC314

# Inside Amazon EKS SaaS: Building multi-tenant solutions with EKS

Tod Golding

Principal Partner Solutions Architect

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS and SaaS: A natural fit



Rapid scaling



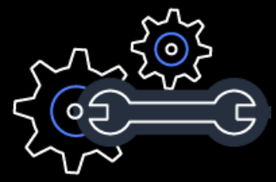
Security constructs



Cost efficiency



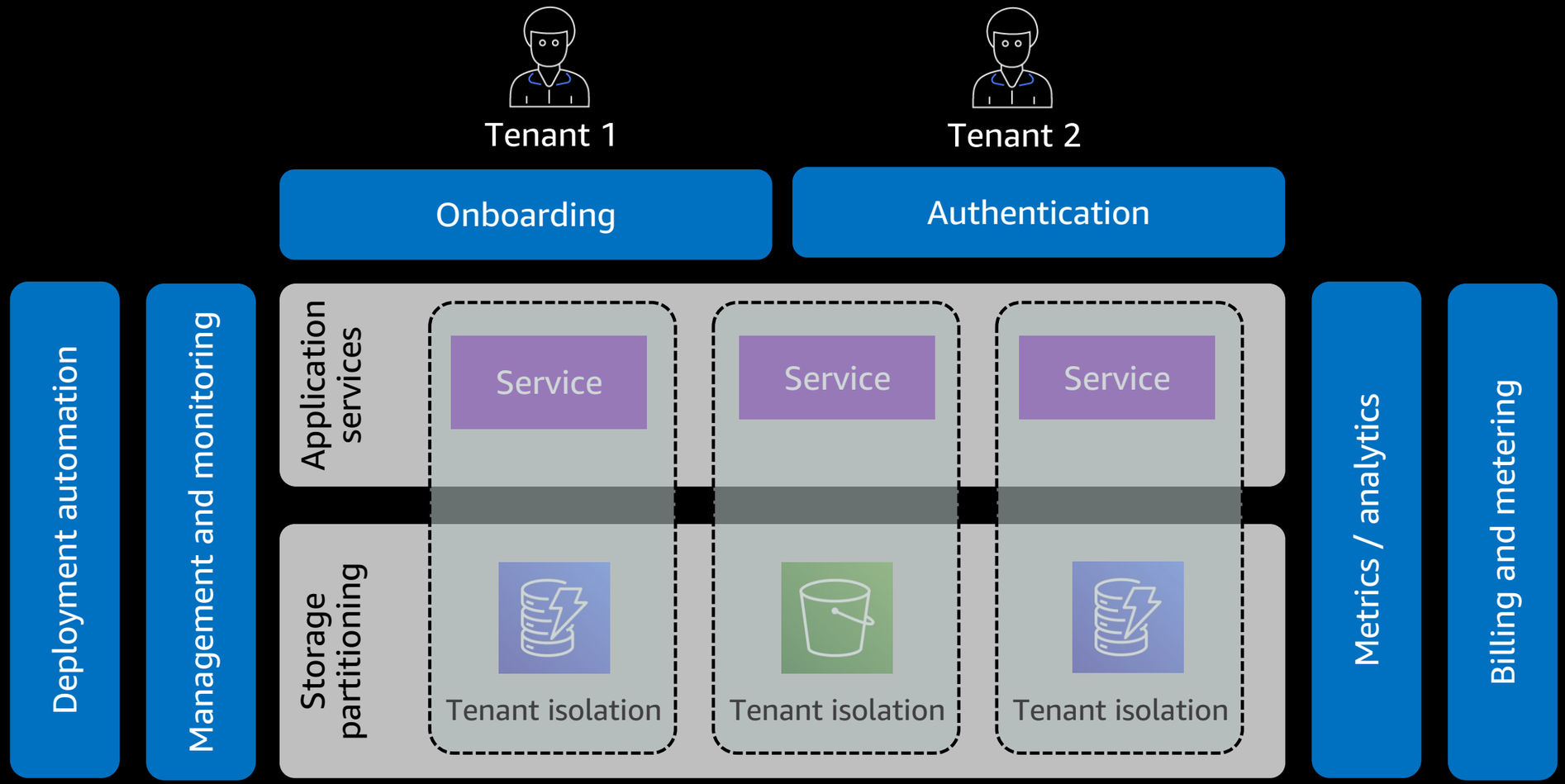
Community tooling



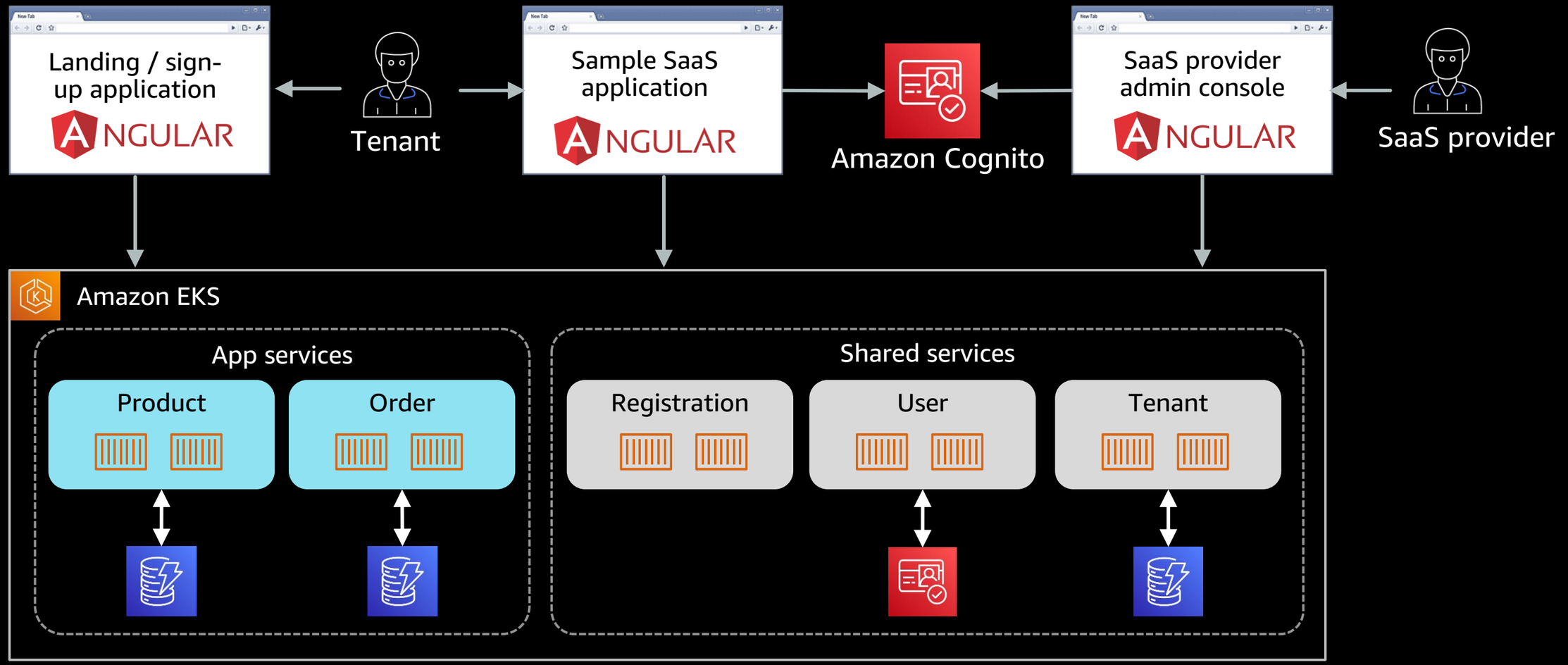
Developer learning curve

Amazon Elastic Kubernetes Service (Amazon EKS) and SaaS

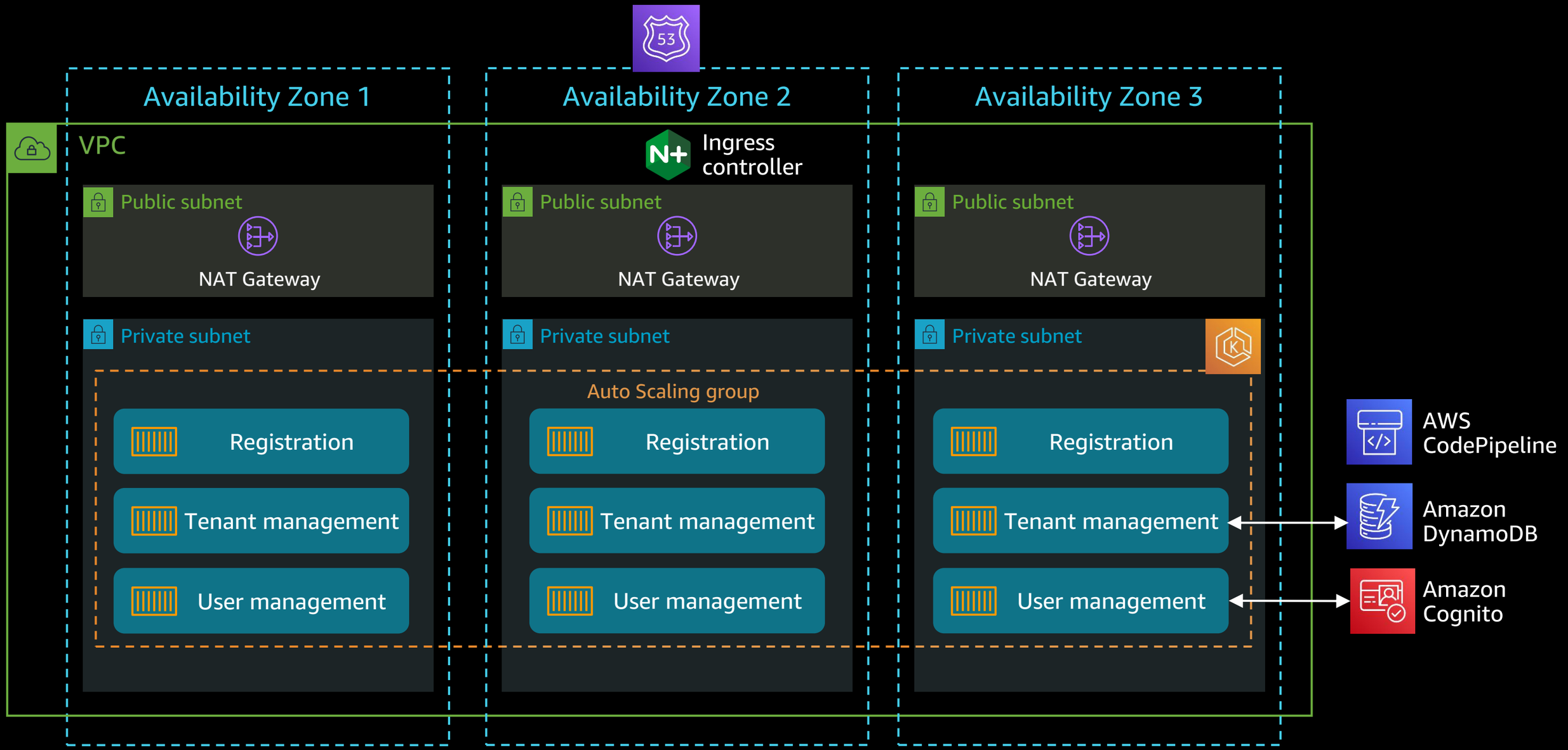
# Amazon EKS SaaS architecture landscape



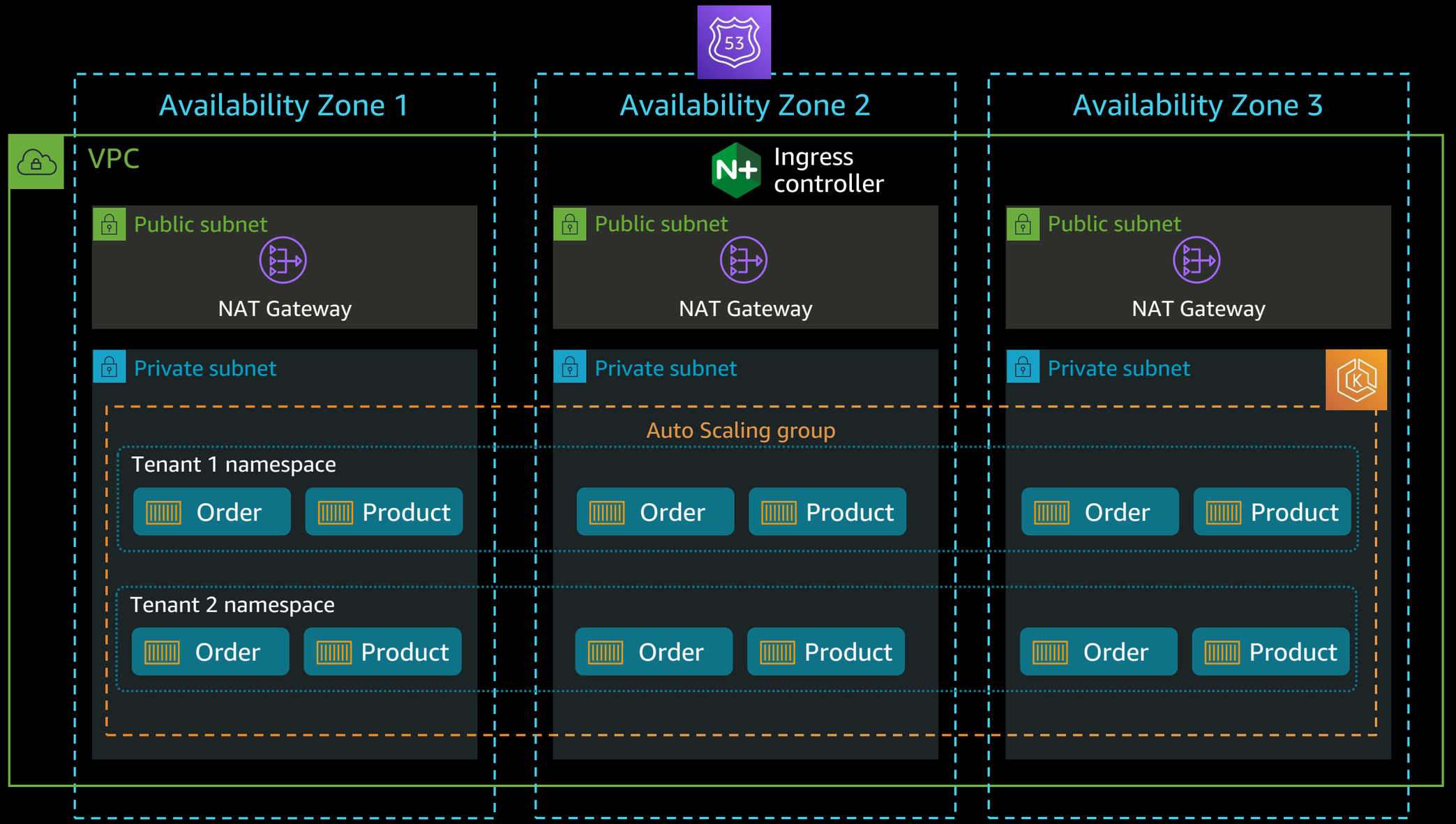
# Conceptual view of the stack



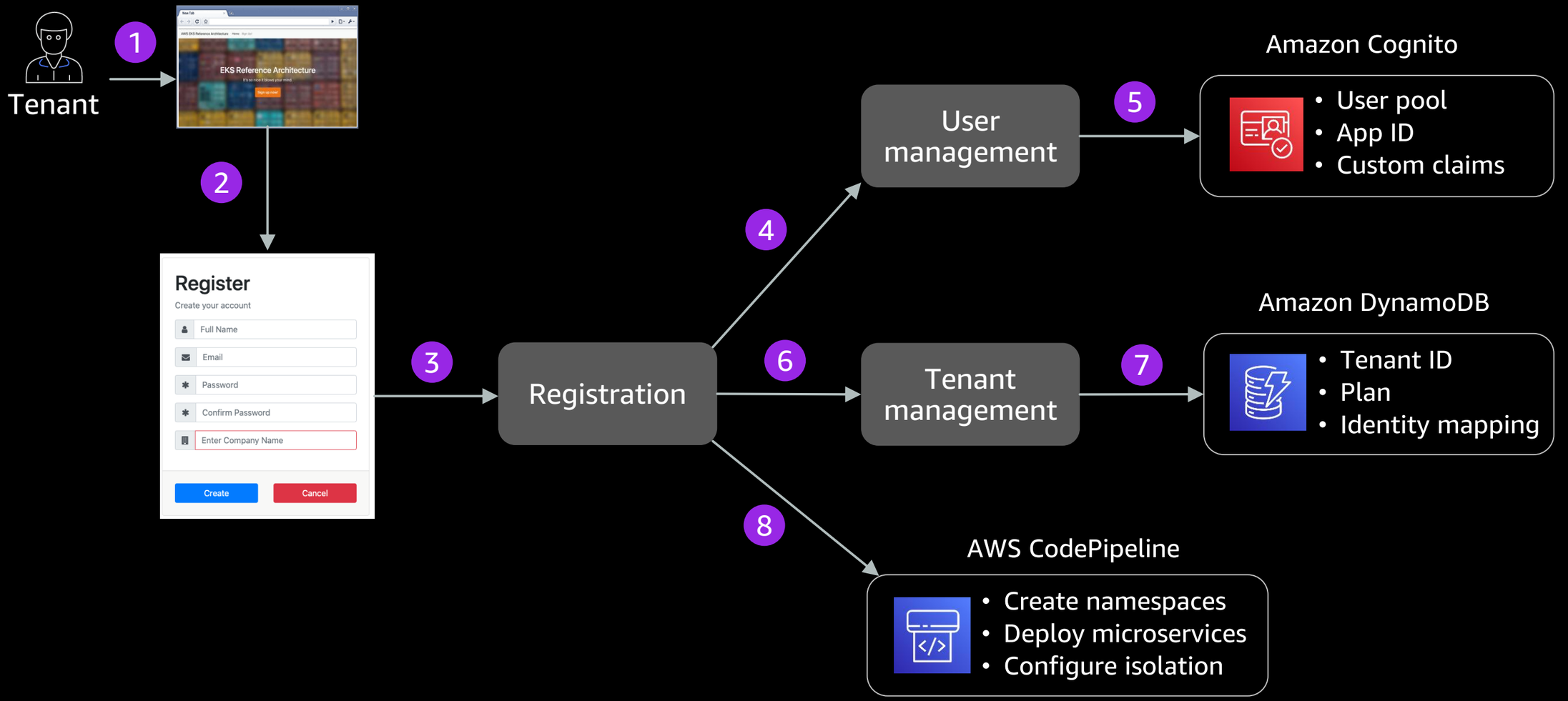
# Provisioning the baseline environment



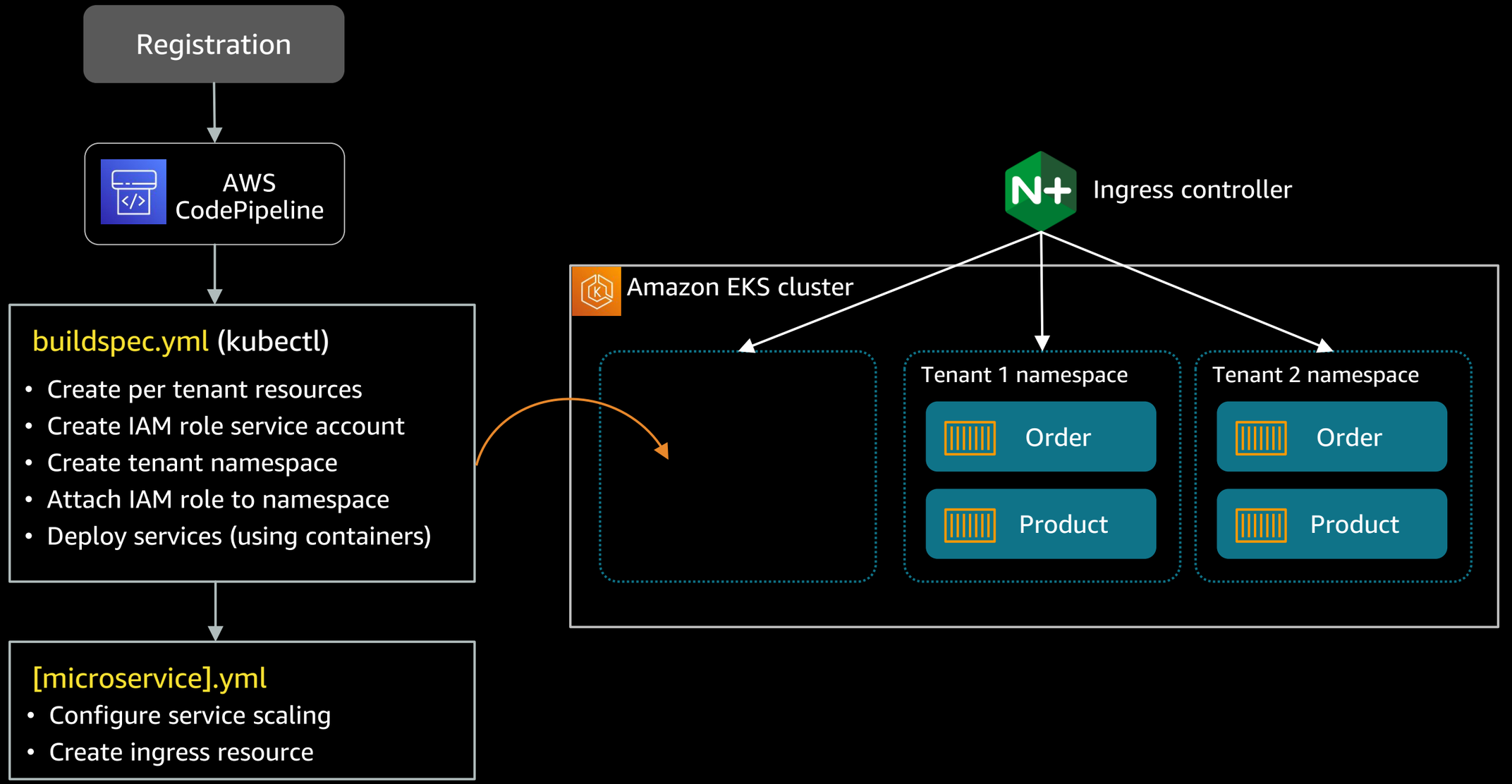
# Tenant environments



# Onboarding new tenants



# Tenant namespace provisioning



# Microservice configuration

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: order
spec:
  replicas: 1
  selector:
    matchLabels:
      app: order
  template:
    metadata:
      labels:
        app: order
    spec:
      containers:
      - name: order
        image: ORDER_SERVICE_ECR_REPO_URI:latest
        ports:
        - containerPort: 5001
          name: "http"
```

Deployment

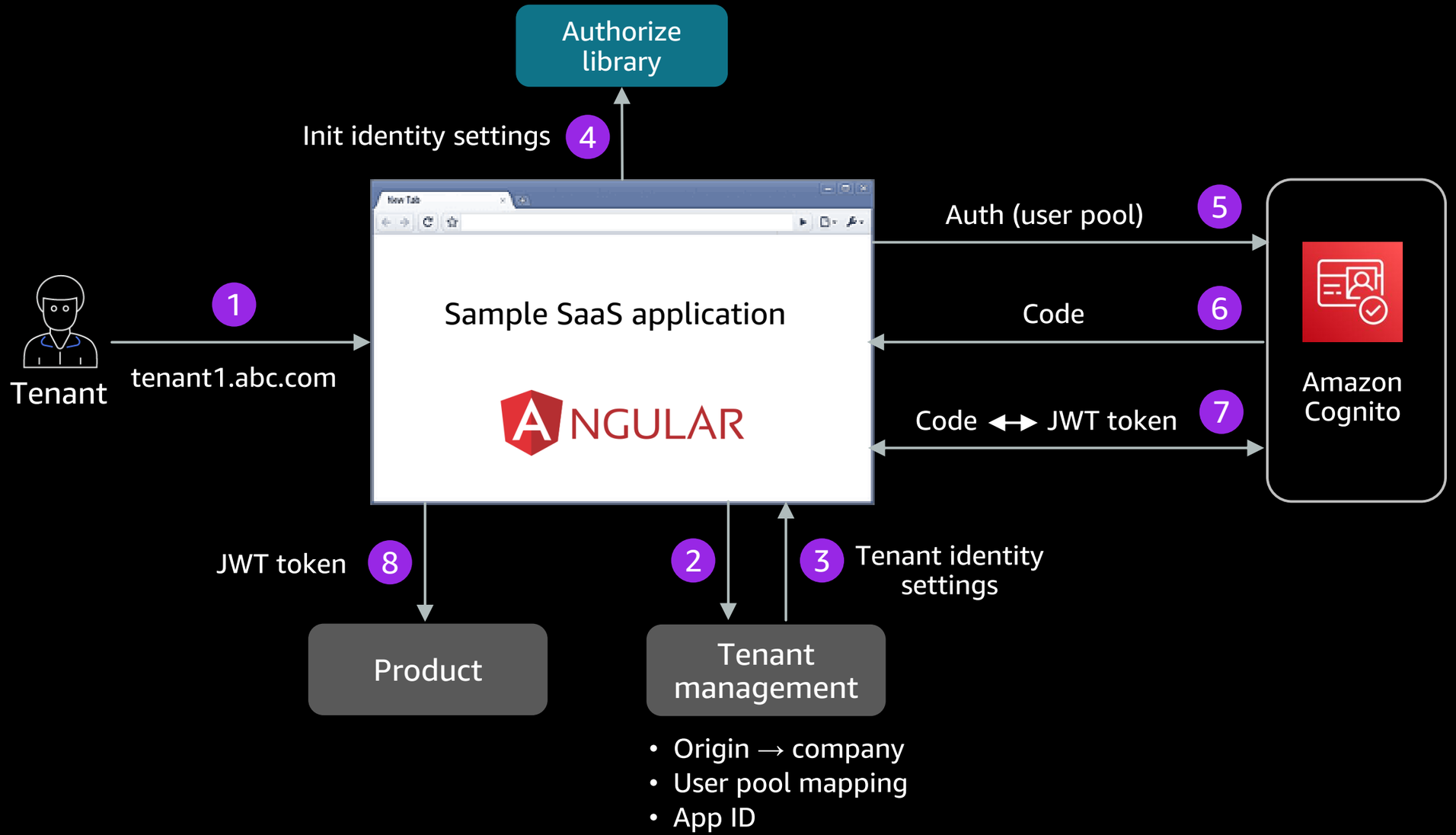
```yaml
apiVersion: v1
kind: Service
metadata:
  name: order-service
spec:
  selector:
    app: order
  ports:
  - name: http
    protocol: TCP
    port: 80
    targetPort: 5001
  type: NodePort
```

Service

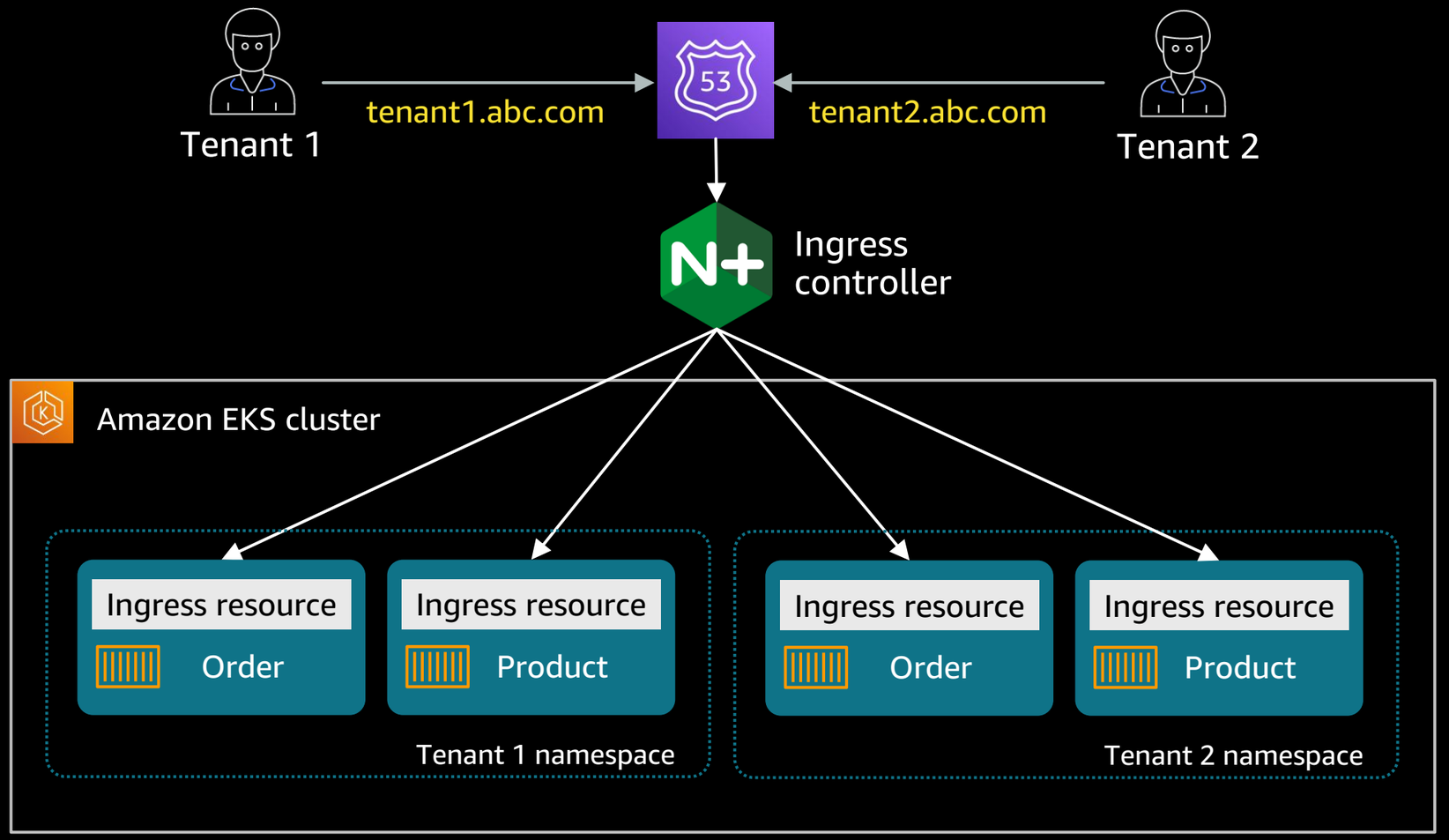
```yaml
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: order-service-ingress
  annotations:
    kubernetes.io/ingress.class: "nginx"
spec:
  rules:
  - host: api.CUSTOM_DOMAIN
    http:
      paths:
      - path: /TENANT_NAME/order
        backend:
          serviceName: order-service
          servicePort: 80
```

Ingress

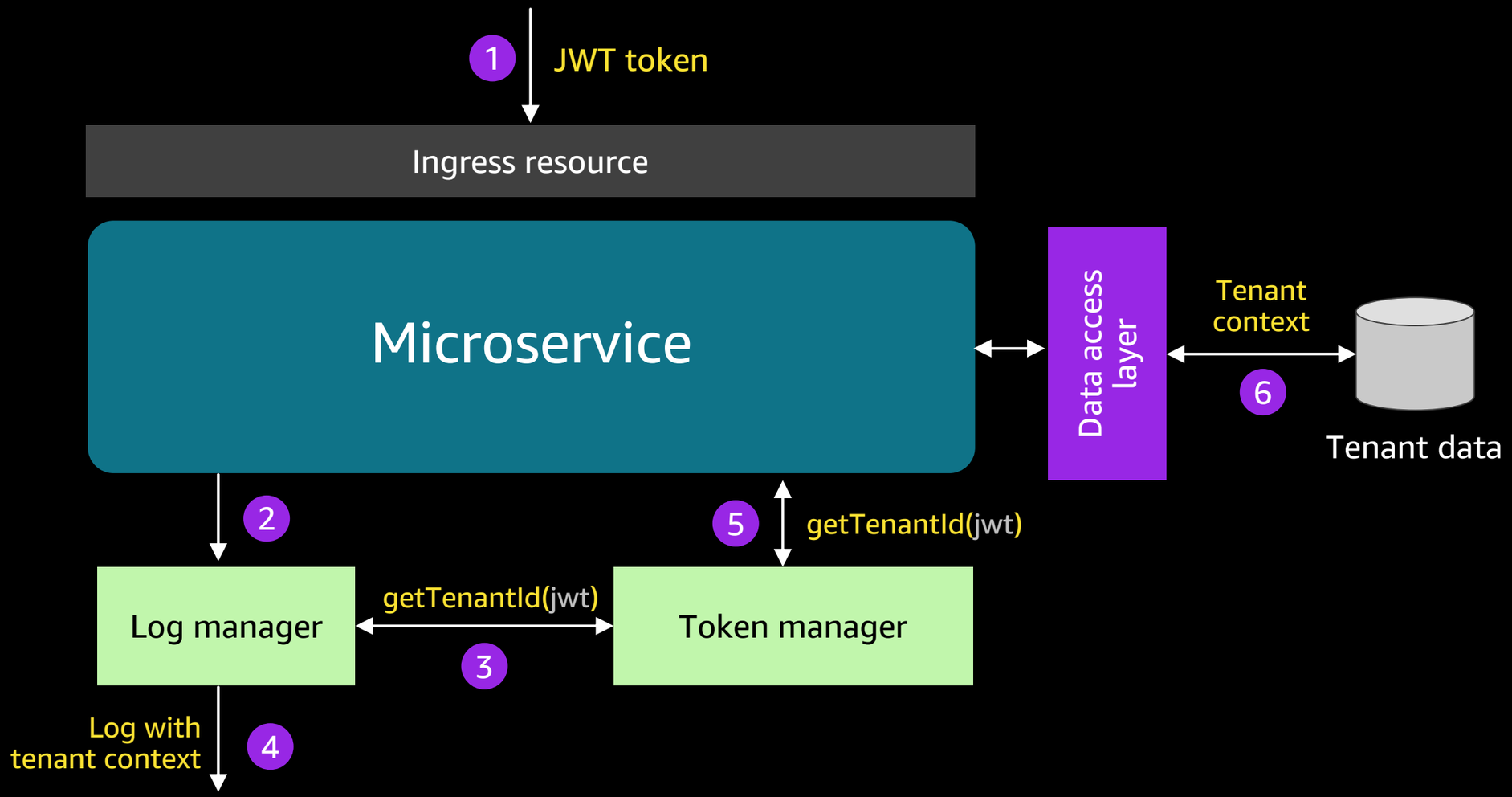
# Tenant authentication



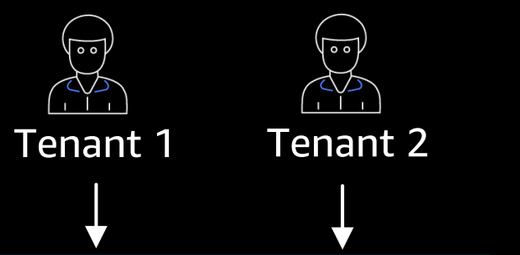
# Routing tenants to namespaces



# Inside the microservices



# Data partitioning



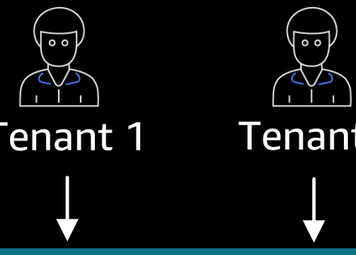

Order microservice

| Product ID | Price | Quantity |
|---|---|---|
| 33919 | $50.00 | 10 |
| 98194 | $29.99 | 34 |
| 73919 | $104.12 | 2 |

Order-Tenant1 table

| Product ID | Price | Quantity |
|---|---|---|
| 57181 | $219.45 | 11 |
| 10097 | $7.90 | 3 |
| 22414 | $431.94 | 23 |

Order-Tenant2 table

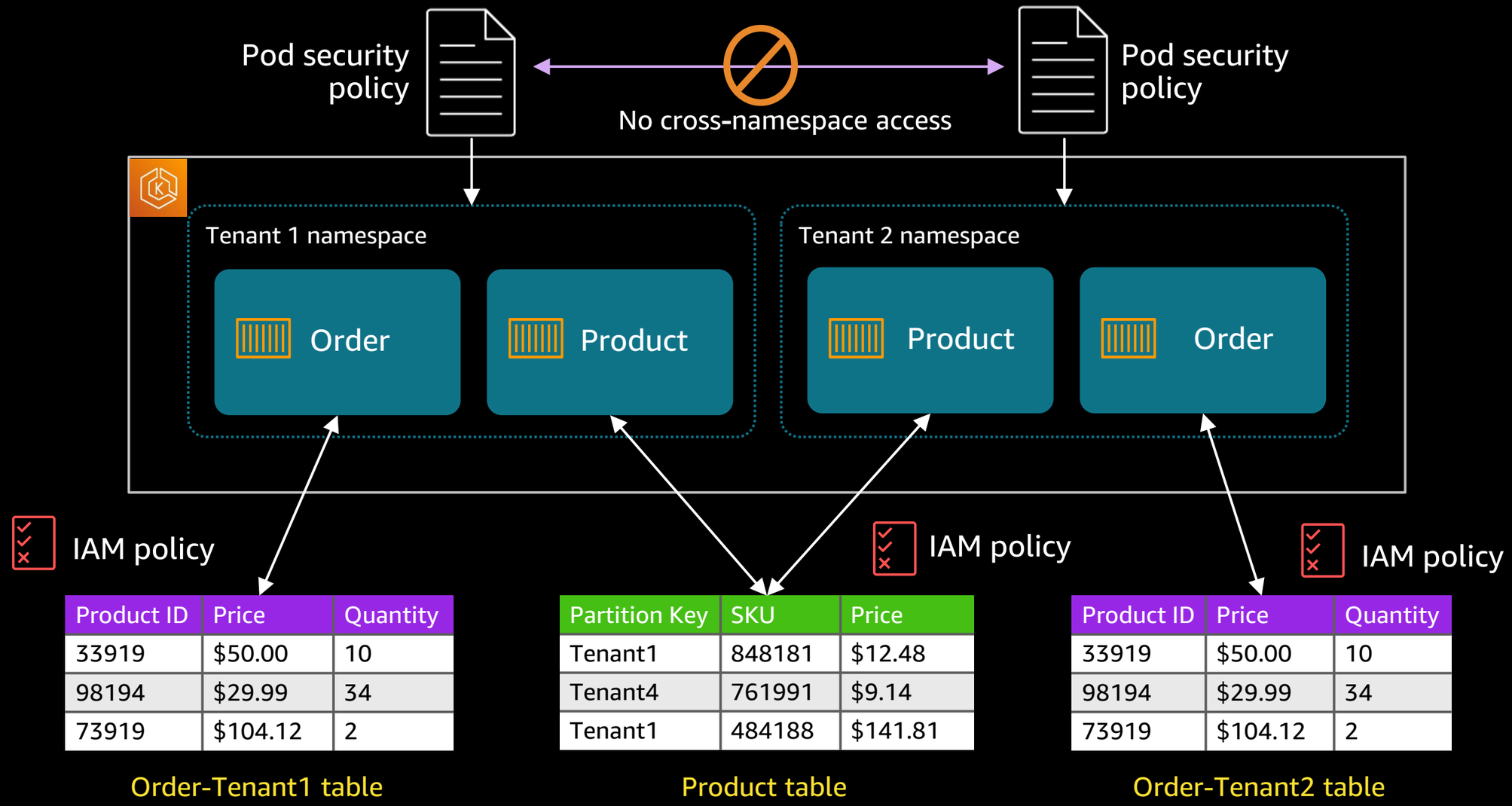



Product microservice

| Partition key | SKU | Price |
|---|---|---|
| Tenant1 | 848181 | $12.48 |
| Tenant4 | 761991 | $9.14 |
| Tenant1 | 484188 | $141.81 |

Product table

# Tenant isolation




| Product ID | Price | Quantity |
|---|---|---|
| 33919 | $50.00 | 10 |
| 98194 | $29.99 | 34 |
| 73919 | $104.12 | 2 |

Order-Tenant1 table

| Partition Key | SKU | Price |
|---|---|---|
| Tenant1 | 848181 | $12.48 |
| Tenant4 | 761991 | $9.14 |
| Tenant1 | 484188 | $141.81 |

Product table

| Product ID | Price | Quantity |
|---|---|---|
| 33919 | $50.00 | 10 |
| 98194 | $29.99 | 34 |
| 73919 | $104.12 | 2 |

Order-Tenant2 table

# Isolation policies

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TENANT_NAME",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:us-east-1:ACCOUNT_ID:table/Order-TENANT_NAME"
        }
    ]
}
```

Scope access to order table by Tenant ID

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  namespace: TENANT_NAME
  name: TENANT_NAME-policy-deny-other-namespace
spec:
  podSelector:
    matchLabels:
  ingress:
  - from:
    - podSelector: {}
```

Define network policy to limit access across namespaces

# Scaling and tiering considerations



# Takeaways

- Amazon EKS provides rich set of multi-tenant constructs
- Fine-grained scaling controls enable powerful tiering constructs
- Use and mix of IAM and K8s security mechanisms build robust tenant isolation model
- Create a single, unified model for provisioning and configuring namespaces
- Lean on rich community of partner solutions to address multi-tenant SaaS challenges

# Accessing the sample solution

Link to the repository with the working solution:

https://github.com/aws-samples/aws-saas-factory-eks-reference-architecture

# More SaaS sessions

Technical Sessions

OPN303 – Open source meets SaaS: Accelerating the path to SaaS adoption

API304 - Monolith to serverless SaaS: Migrating to multi-tenant architecture

GPS304 – SaaS Jump Start: Under the hood of an automated SaaS migration tool

Business sessions

GPS208 -  Insights and inspiration from those on the transformation path

# Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.