SUMMIT
ONLINE

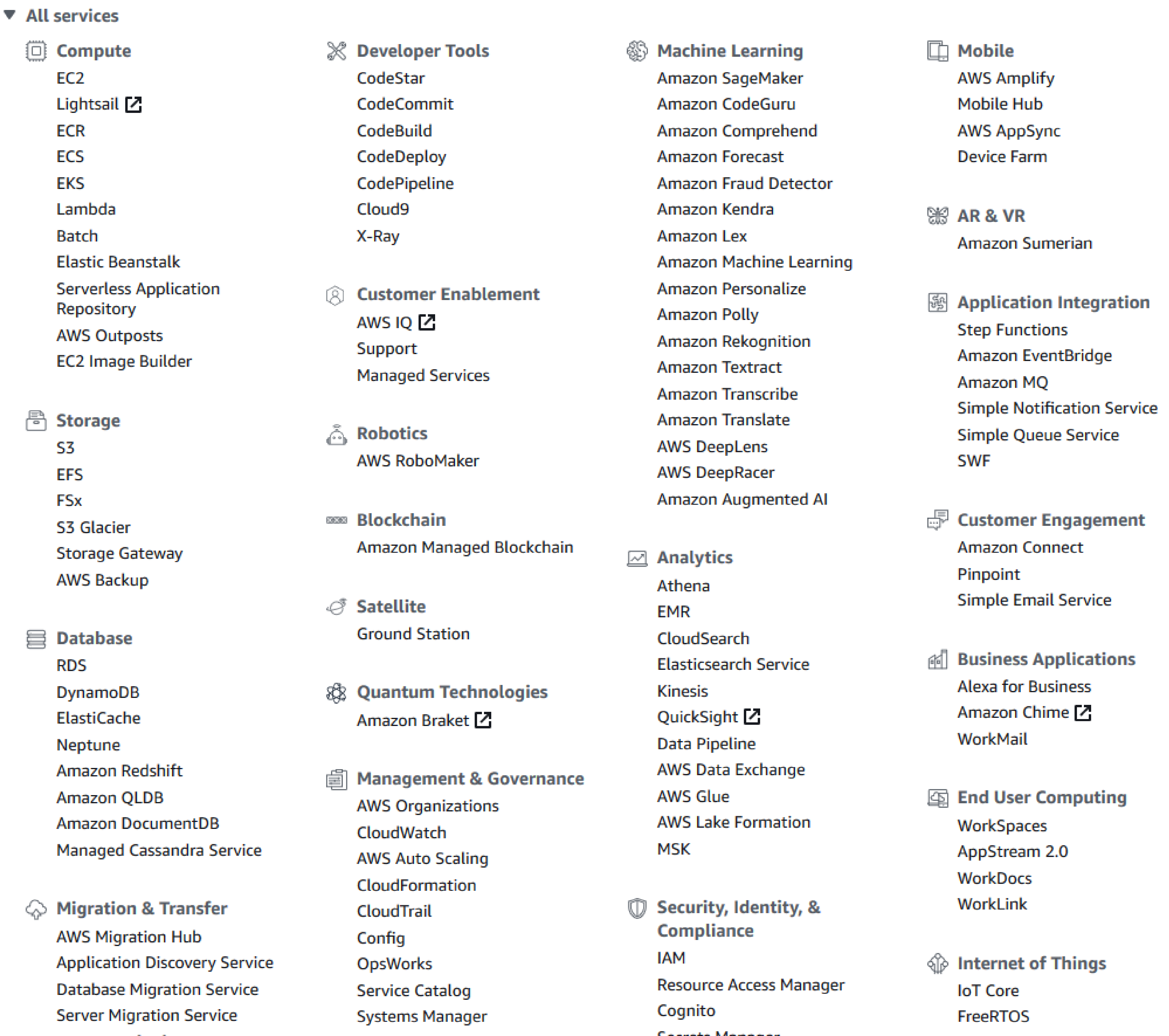
LAU03

# The fundamentals of AWS security

Pierre Liddle

Principal Security Specialist Solutions Architect
Amazon Web Services

aws SUMMIT ONLINE



▼ **All services**

**Compute**
- EC2
- Lightsail
- ECR
- ECS
- EKS
- Lambda
- Batch
- Elastic Beanstalk
- Serverless Application Repository
- AWS Outposts
- EC2 Image Builder

**Storage**
- S3
- EFS
- FSx
- S3 Glacier
- Storage Gateway
- AWS Backup

**Database**
- RDS
- DynamoDB
- ElastiCache
- Neptune
- Amazon Redshift
- Amazon QLDB
- Amazon DocumentDB
- Managed Cassandra Service

**Migration & Transfer**
- AWS Migration Hub
- Application Discovery Service
- Database Migration Service
- Server Migration Service

**Developer Tools**
- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- Cloud9
- X-Ray

**Customer Enablement**
- AWS IQ
- Support
- Managed Services

**Robotics**
- AWS RoboMaker

**Blockchain**
- Amazon Managed Blockchain

**Satellite**
- Ground Station

**Quantum Technologies**
- Amazon Braket

**Management & Governance**
- AWS Organizations
- CloudWatch
- AWS Auto Scaling
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Systems Manager

**Machine Learning**
- Amazon SageMaker
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Forecast
- Amazon Fraud Detector
- Amazon Kendra
- Amazon Lex
- Amazon Machine Learning
- Amazon Personalize
- Amazon Polly
- Amazon Rekognition
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS DeepLens
- AWS DeepRacer
- Amazon Augmented AI

**Analytics**
- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- QuickSight
- Data Pipeline
- AWS Data Exchange
- AWS Glue
- AWS Lake Formation
- MSK

**Security, Identity, & Compliance**
- IAM
- Resource Access Manager
- Cognito
- Secrets Manager

**Mobile**
- AWS Amplify
- Mobile Hub
- AWS AppSync
- Device Farm

**AR & VR**
- Amazon Sumerian

**Application Integration**
- Step Functions
- Amazon EventBridge
- Amazon MQ
- Simple Notification Service
- Simple Queue Service
- SWF

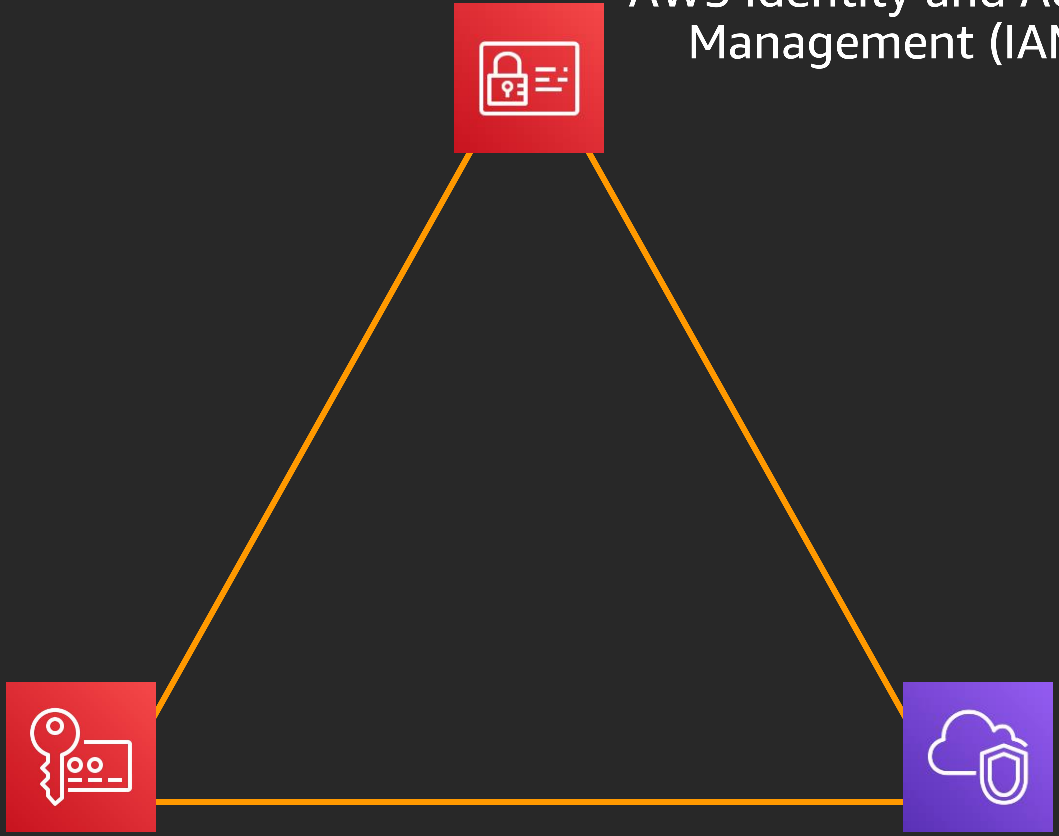
**Customer Engagement**
- Amazon Connect
- Pinpoint
- Simple Email Service

**Business Applications**
- Alexa for Business
- Amazon Chime
- WorkMail

**End User Computing**
- WorkSpaces
- AppStream 2.0
- WorkDocs
- WorkLink

**Internet of Things**
- IoT Core
- FreeRTOS

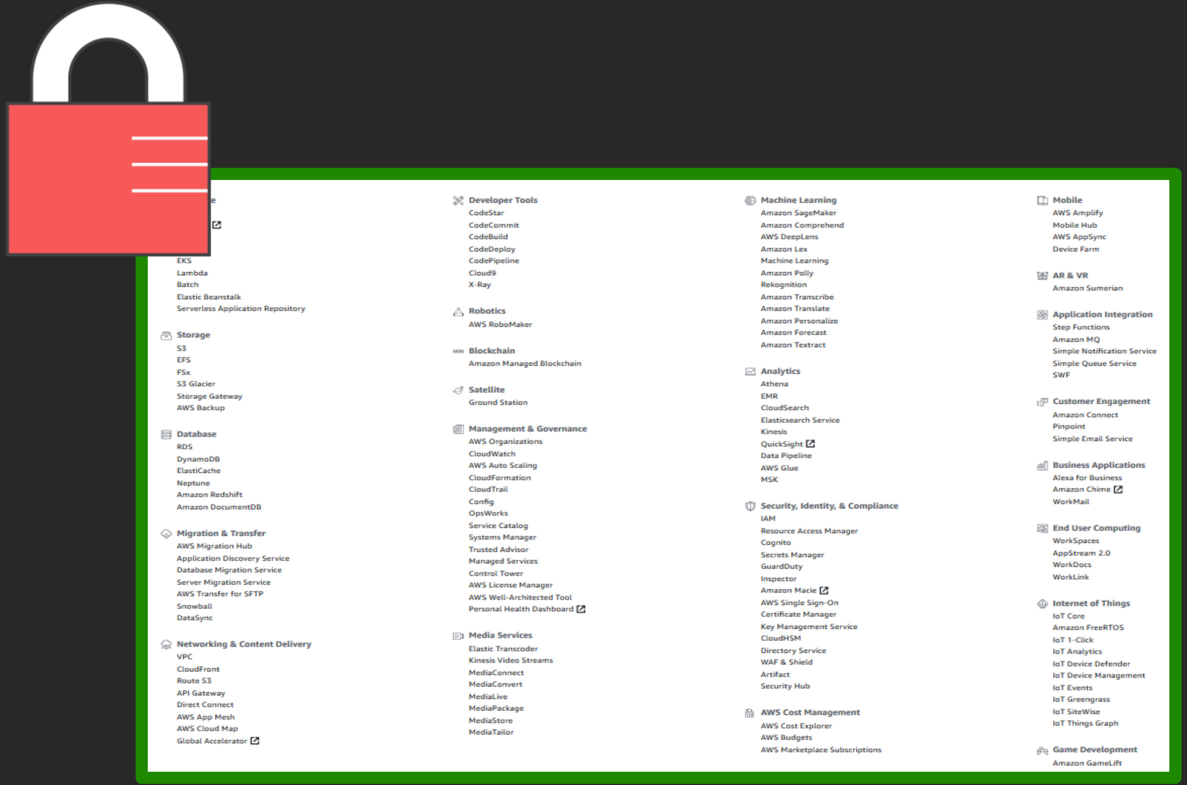
# Learn a few patterns, secure everything in AWS



**Permissions management**
AWS Identity and Access
Management (IAM)

**Data encryption**
AWS Key Management Service
(AWS KMS)

**Network security controls**
Amazon Virtual Private Cloud
(Amazon VPC)



EKS
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository

**Storage**
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

**Database**
RDS
DynamoDB
ElastiCache
Neptune
Amazon Redshift
Amazon DocumentDB

**Migration & Transfer**
AWS Migration Hub
Application Discovery Service
Database Migration Service
Server Migration Service
AWS Transfer for SFTP
Snowball
DataSync

**Networking & Content Delivery**
VPC
CloudFront
Route 53
API Gateway
Direct Connect
AWS App Mesh
AWS Cloud Map
Global Accelerator

**Developer Tools**
CodeStar
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
Cloud9
X-Ray

**Robotics**
AWS RoboMaker

**Blockchain**
Amazon Managed Blockchain

**Satellite**
Ground Station

**Management & Governance**
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Managed Services
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard

**Media Services**
Elastic Transcoder
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage
MediaStore
MediaTailor

**Machine Learning**
Amazon SageMaker
Amazon Comprehend
AWS DeepLens
Amazon Lex
Machine Learning
Amazon Polly
Rekognition
Amazon Transcribe
Amazon Translate
Amazon Personalize
Amazon Forecast
Amazon Textract

**Analytics**
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Glue
MSK

**Security, Identity, & Compliance**
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
Artifact
Security Hub

**AWS Cost Management**
AWS Cost Explorer
AWS Budgets
AWS Marketplace Subscriptions

**Mobile**
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

**AR & VR**
Amazon Sumerian

**Application Integration**
Step Functions
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

**Customer Engagement**
Amazon Connect
Pinpoint
Simple Email Service

**Business Applications**
Alexa for Business
Amazon Chime
WorkMail

**End User Computing**
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink

**Internet of Things**
IoT Core
Amazon FreeRTOS
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise
IoT Things Graph

**Game Development**
Amazon GameLift

# Agenda

A builder-focused introduction to AWS' security controls

- **Control your cloud infrastructure:** AWS IAM
- **Control your data:** AWS KMS
- **Control your network:** Amazon VPC

You will leave this session with the foundation you need to secure an AWS environment

# Identity and Access Management (IAM)

# Identity and Access Management

## What it is:

- **‘I’—Authentication.** Support for human and application caller identities
- **‘AM’—Authorisation.** Powerful, flexible permissions language for controlling access to cloud resources

## Why it matters to you:

Every AWS service uses IAM to authenticate and authorise API calls

## What builders need to know:

- How to make authenticated API calls to AWS from IAM identities
- Basic fluency in IAM policy language
- Where to find and how to understand service-specific authorisation control details

# AWS API calls recognise two kinds of IAM identities

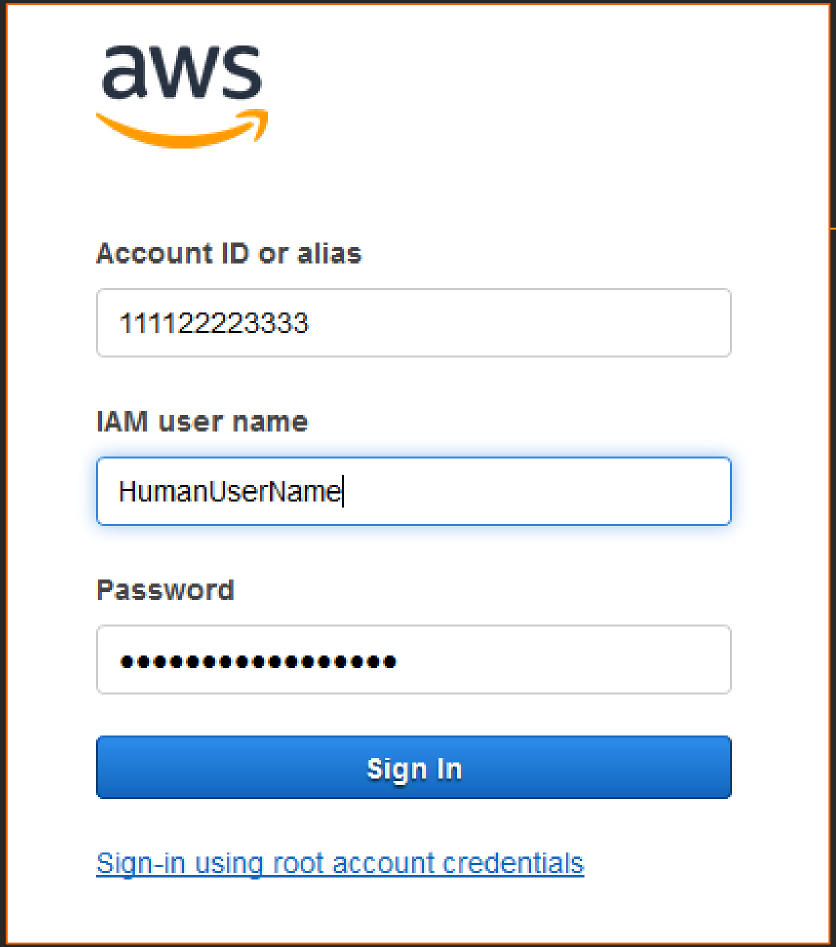
Long-term
credentials

IAM User

Short-term credentials
(sessions)

IAM Role

# AWS identities for human callers: IAM users



Account ID or alias

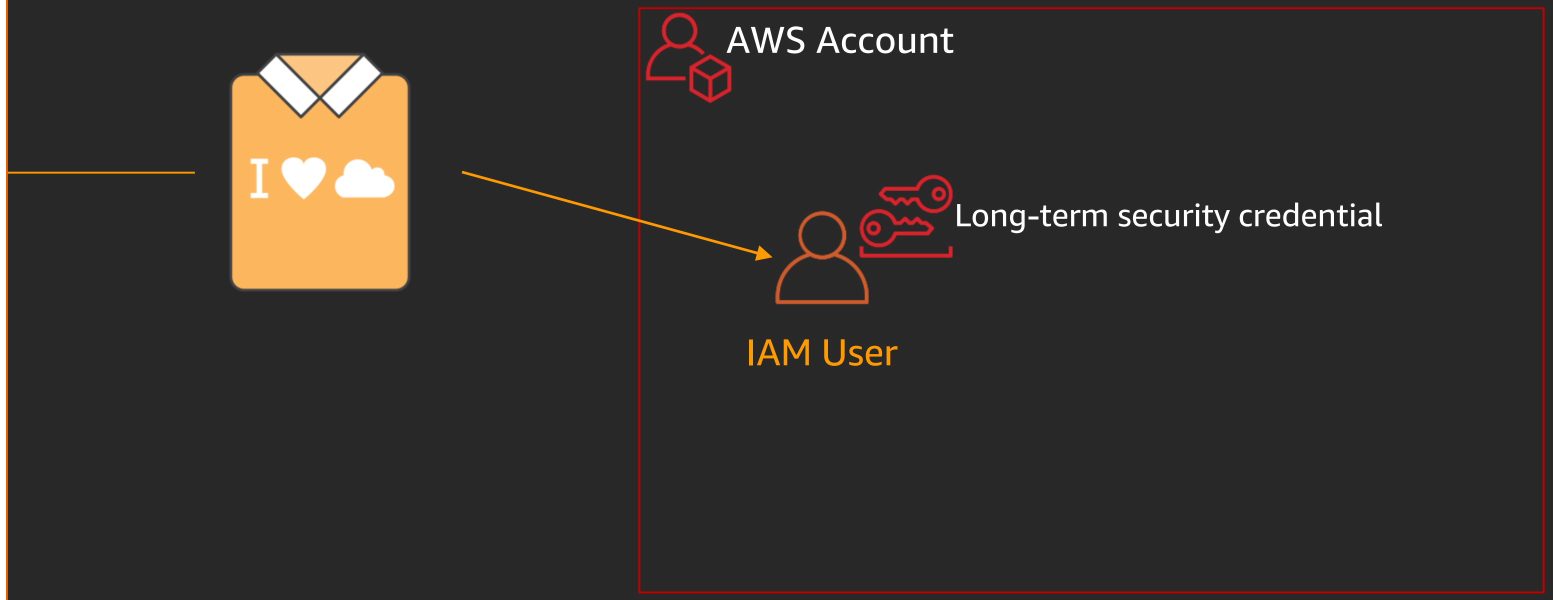
111122223333

IAM user name

HumanUserName

Password

•••••••••••••••••

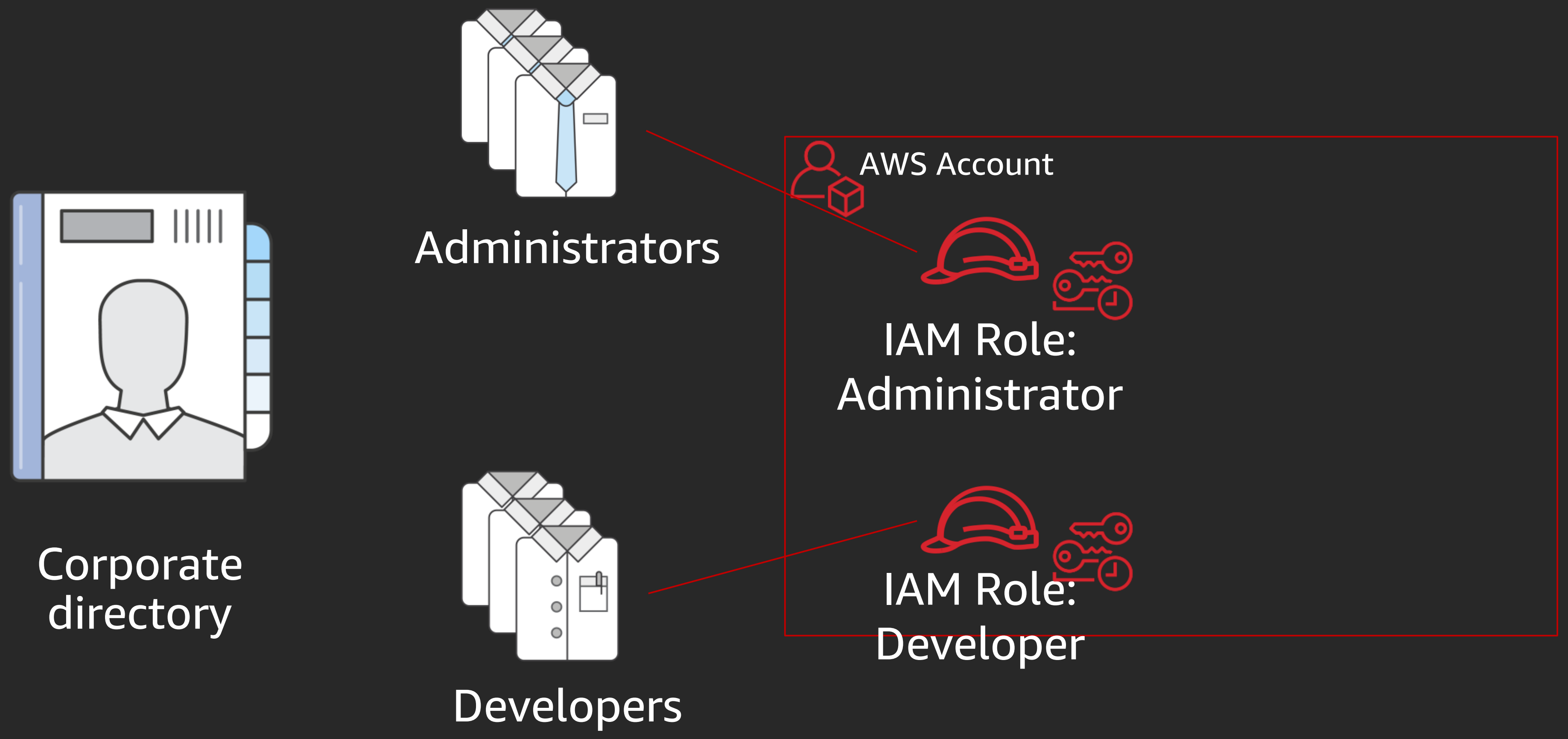


AWS Account

Long-term security credential

IAM User

# AWS identities for human callers: Federated identities



# AWS identities for non-human callers

EC2
Instance

Lambda
Function

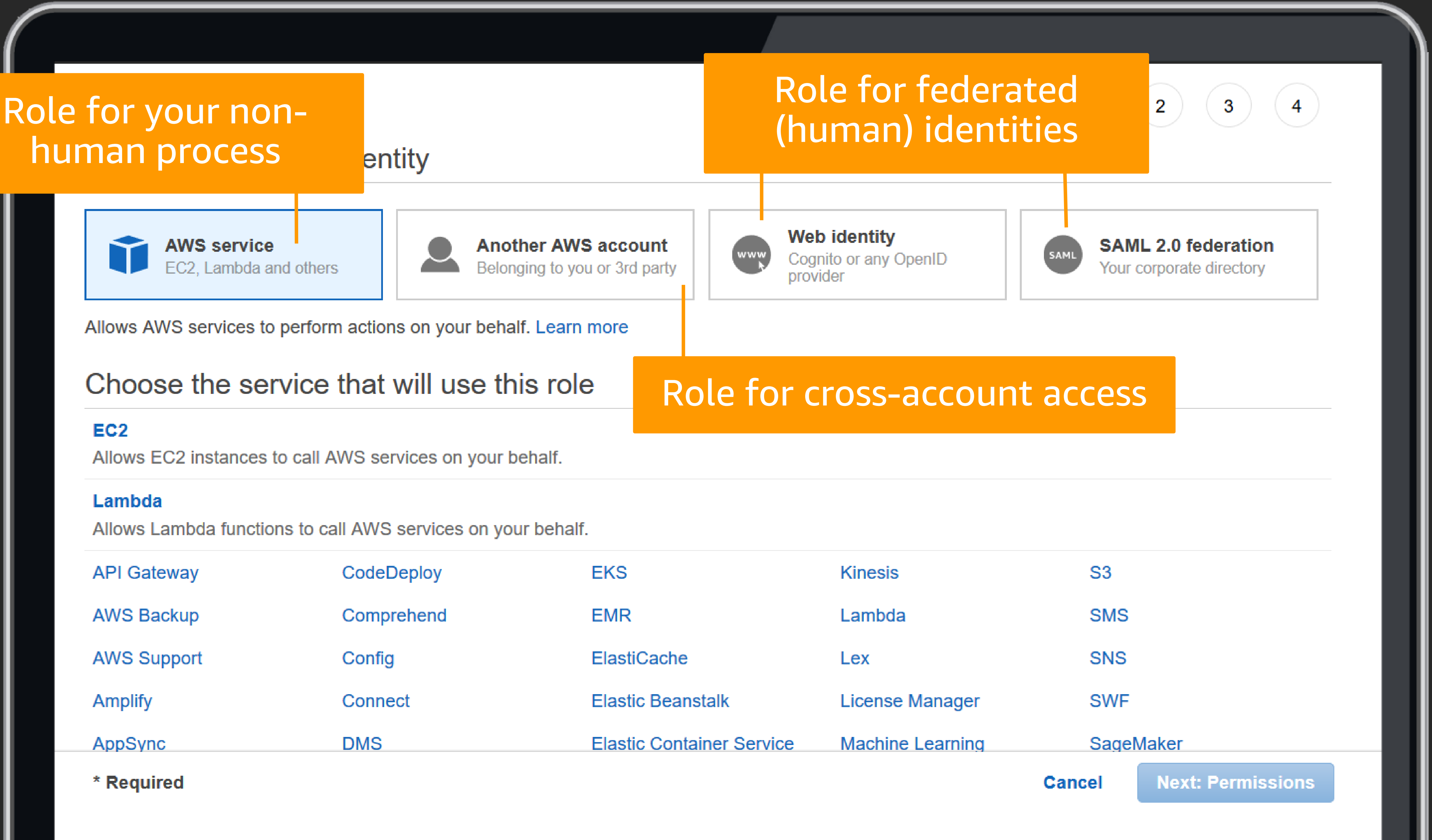
Amazon
SageMaker
Notebook

AWS Glue
Crawler

Amazon
ECS Task

… and many others

# Creating a role in the AWS Management Console



Role for your non-human process

Role for federated (human) identities

Role for cross-account access

entity

**AWS service**
EC2, Lambda and others

**Another AWS account**
Belonging to you or 3rd party

**Web identity**
Cognito or any OpenID provider

**SAML 2.0 federation**
Your corporate directory

Allows AWS services to perform actions on your behalf. Learn more

Choose the service that will use this role

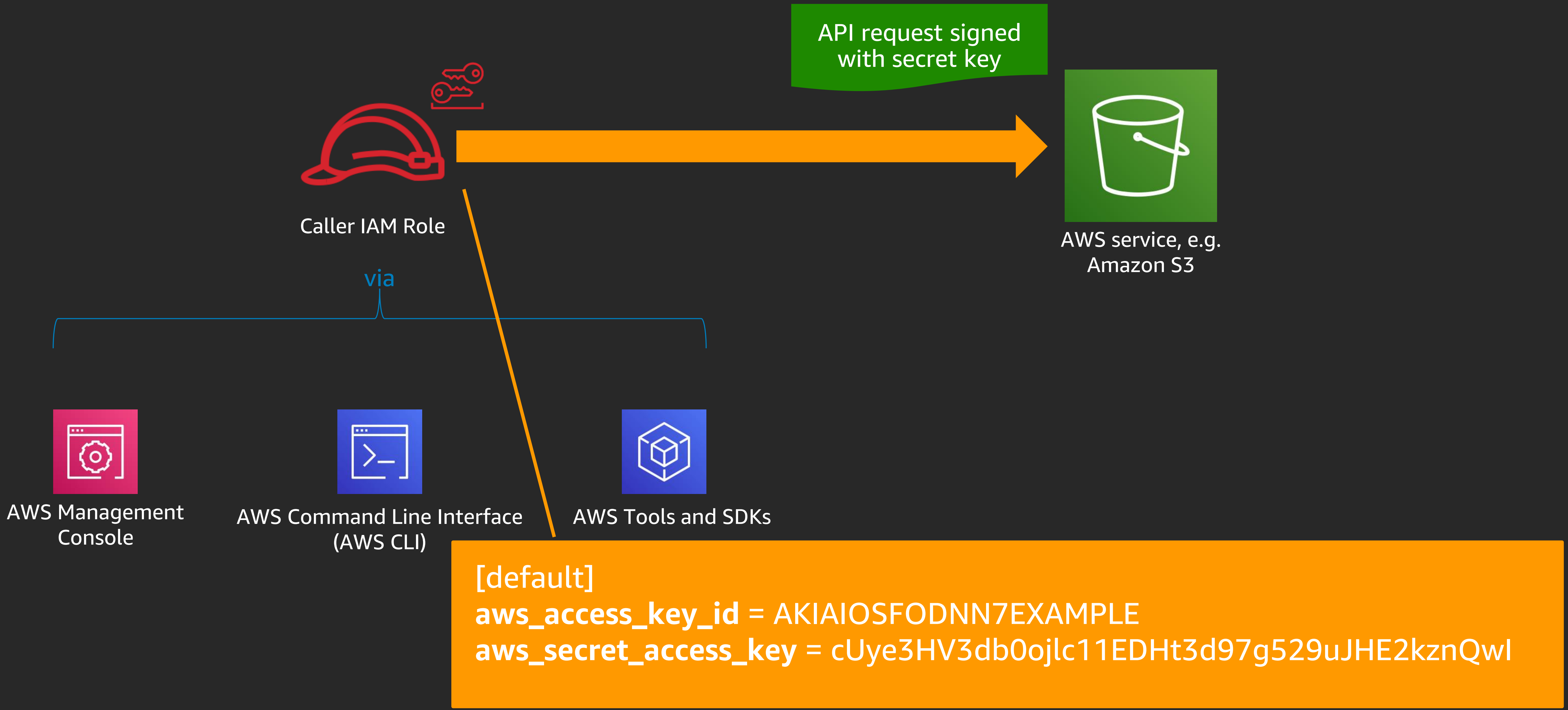
**EC2**
Allows EC2 instances to call AWS services on your behalf.

**Lambda**
Allows Lambda functions to call AWS services on your behalf.

| | | | | |
|---|---|---|---|---|
| API Gateway | CodeDeploy | EKS | Kinesis | S3 |
| AWS Backup | Comprehend | EMR | Lambda | SMS |
| AWS Support | Config | ElastiCache | Lex | SNS |
| Amplify | Connect | Elastic Beanstalk | License Manager | SWF |
| AppSync | DMS | Elastic Container Service | Machine Learning | SageMaker |

* **Required**

# How authentication works in AWS



API request signed with secret key

Caller IAM Role

AWS service, e.g. Amazon S3

via

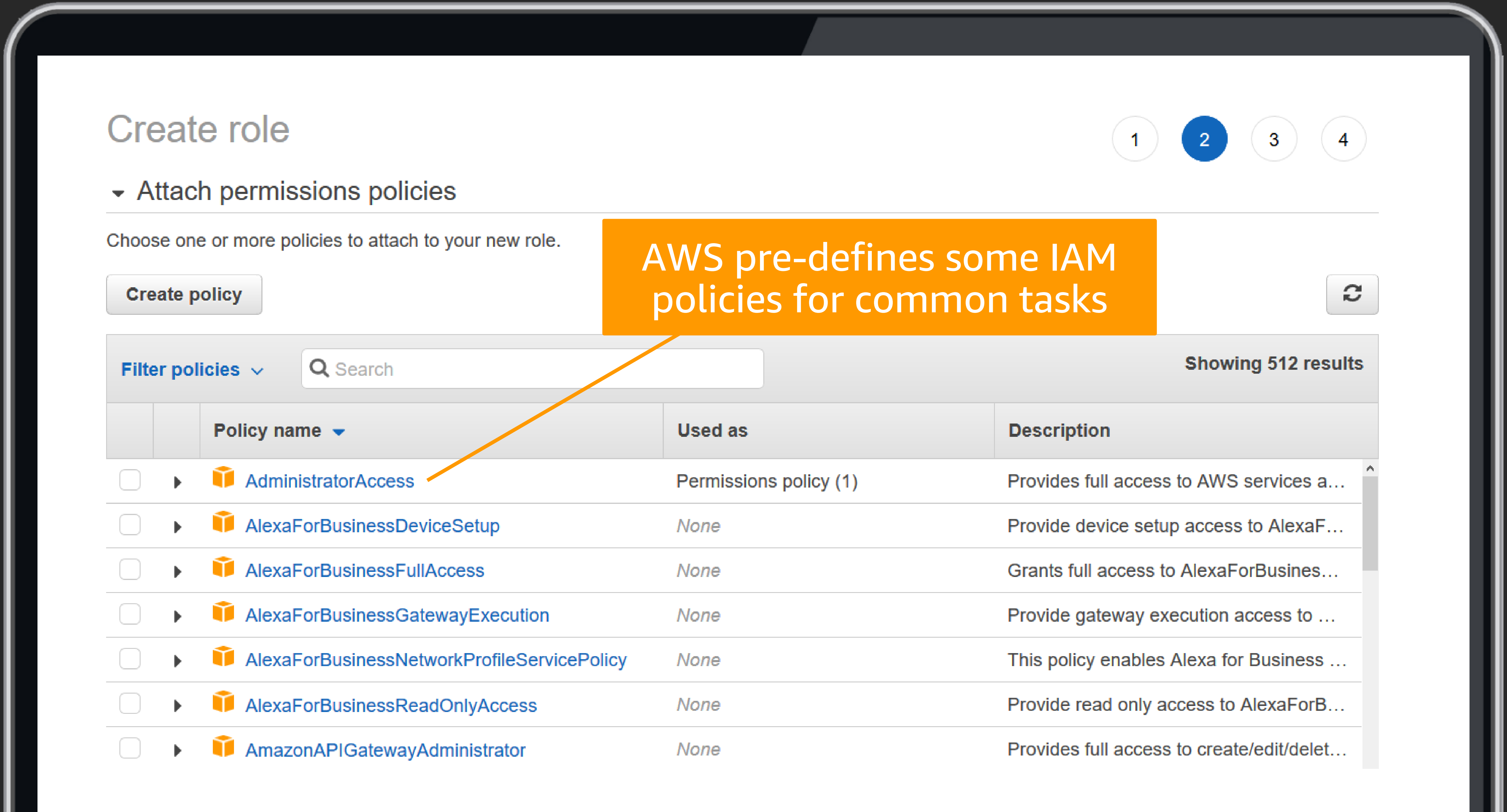
AWS Management Console

AWS Command Line Interface (AWS CLI)

AWS Tools and SDKs

```
[default]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = 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
```

# AWS-managed policies for common sets of permissions



Create role

1 2 3 4

Attach permissions policies

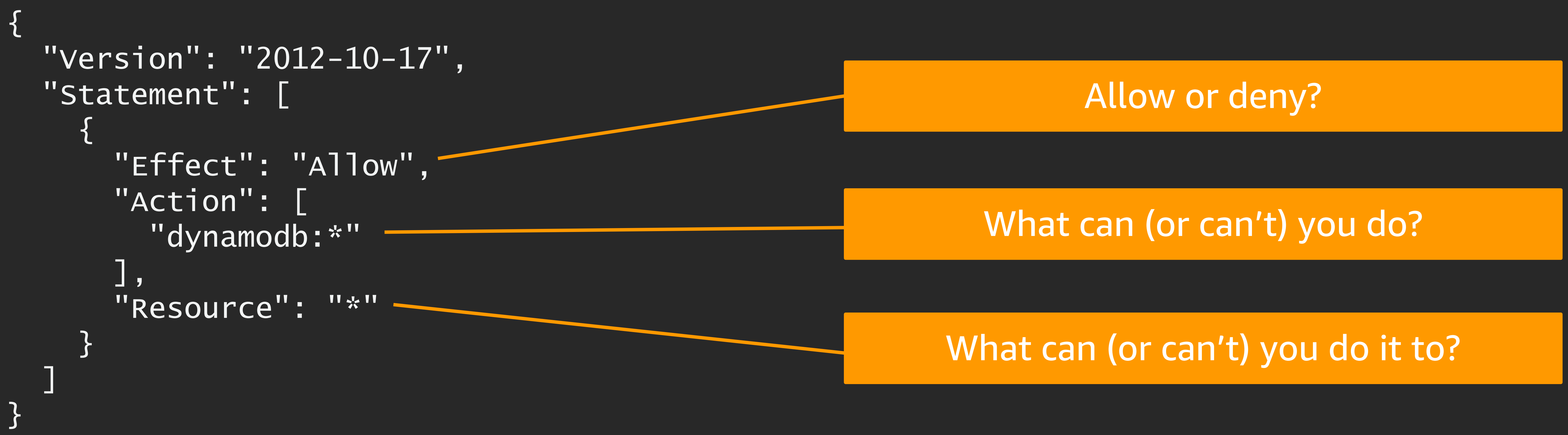
Choose one or more policies to attach to your new role.

Showing 512 results

| Policy name | Used as | Description |
|---|---|---|
| □ AdministratorAccess | Permissions policy (1) | Provides full access to AWS services a… |
| □ AlexaForBusinessDeviceSetup | *None* | Provide device setup access to AlexaF… |
| □ AlexaForBusinessFullAccess | *None* | Grants full access to AlexaForBusines… |
| □ AlexaForBusinessGatewayExecution | *None* | Provide gateway execution access to … |
| □ AlexaForBusinessNetworkProfileServicePolicy | *None* | This policy enables Alexa for Business … |
| □ AlexaForBusinessReadOnlyAccess | *None* | Provide read only access to AlexaForB… |
| □ AmazonAPIGatewayAdministrator | *None* | Provides full access to create/edit/delet… |

AWS pre-defines some IAM policies for common tasks

# Reading and writing IAM policy



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Allow or deny?

What can (or can’t) you do?

What can (or can’t) you do it to?

In English: Allowed to take all Amazon DynamoDB actions

# Reading and writing IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:PutItem"
      ],
      "Resource": "*"
    }
  ]
}
```

In English: Allowed to read and write individual items in DynamoDB

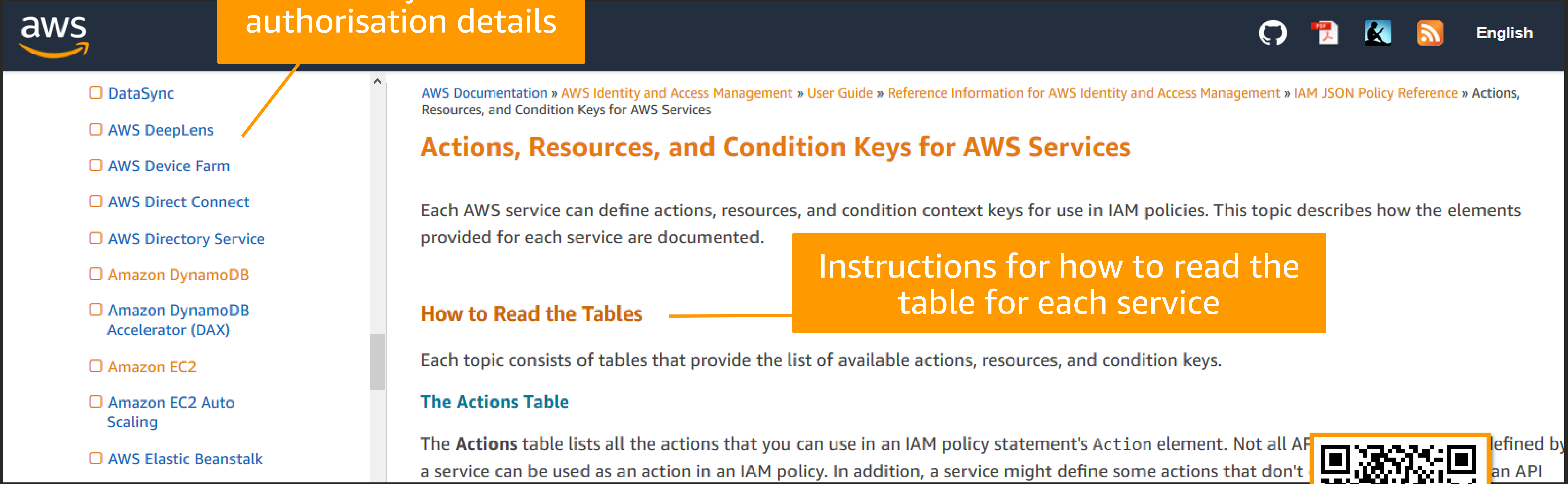
# Reading and writing IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:PutItem"
      ],
      "Resource": [
        "arn:aws:dynamodb:ap-southeast-2:111122223333:table/MyTableName"
      ]
    }
  ]
}
```

In English: Allowed to take specific DynamoDB actions on a specific table

This is an Amazon Resource Name (ARN).
All AWS services use them, and they follow this format.

# How to write a least-privilege IAM policy



Service-by-service authorisation details

Instructions for how to read the table for each service

□ DataSync
□ AWS DeepLens
□ AWS Device Farm
□ AWS Direct Connect
□ AWS Directory Service
□ Amazon DynamoDB
□ Amazon DynamoDB Accelerator (DAX)
□ Amazon EC2
□ Amazon EC2 Auto Scaling
□ AWS Elastic Beanstalk

AWS Documentation » AWS Identity and Access Management » User Guide » Reference Information for AWS Identity and Access Management » IAM JSON Policy Reference » Actions, Resources, and Condition Keys for AWS Services

## Actions, Resources, and Condition Keys for AWS Services

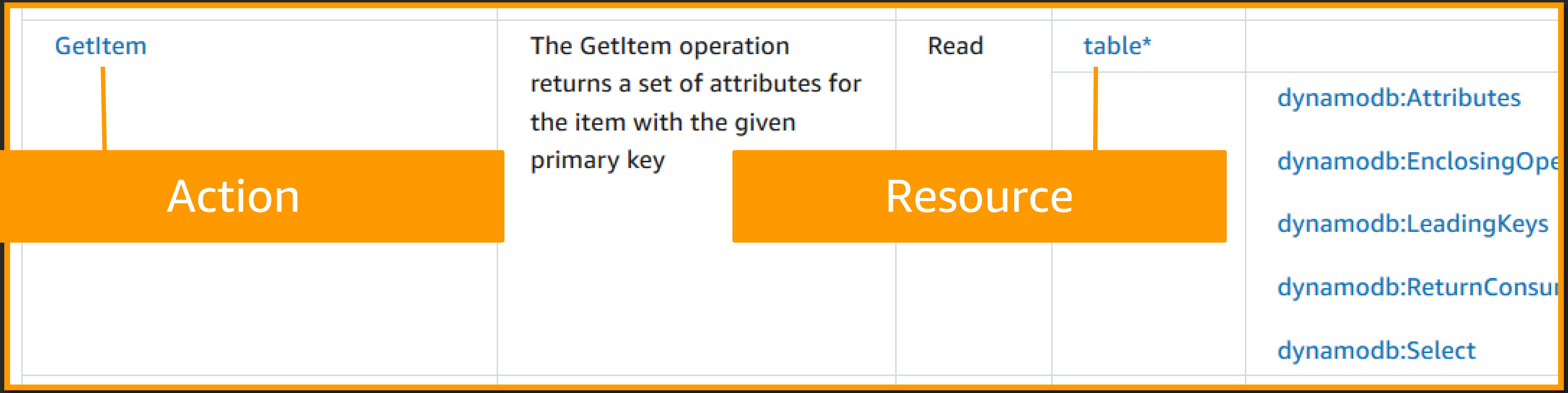
Each AWS service can define actions, resources, and condition context keys for use in IAM policies. This topic describes how the elements provided for each service are documented.

### How to Read the Tables

Each topic consists of tables that provide the list of available actions, resources, and condition keys.

### The Actions Table

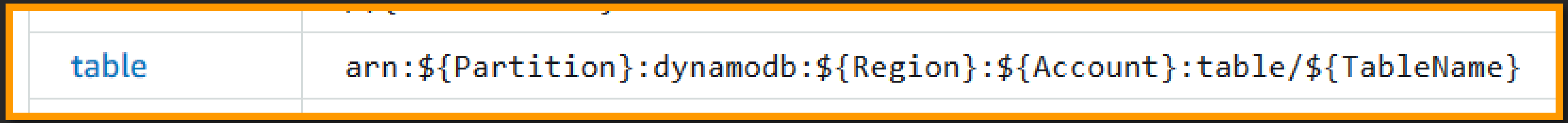
The **Actions** table lists all the actions that you can use in an IAM policy statement's `Action` element. Not all AP efined by a service can be used as an action in an IAM policy. In addition, a service might define some actions that don't an API



| | | | | |
|---|---|---|---|---|
| GetItem | The GetItem operation returns a set of attributes for the item with the given primary key | Read | table* | |
| | | | | dynamodb:Attributes<br>dynamodb:EnclosingOpe<br>dynamodb:LeadingKeys<br>dynamodb:ReturnConsu<br>dynamodb:Select |

Action

Resource

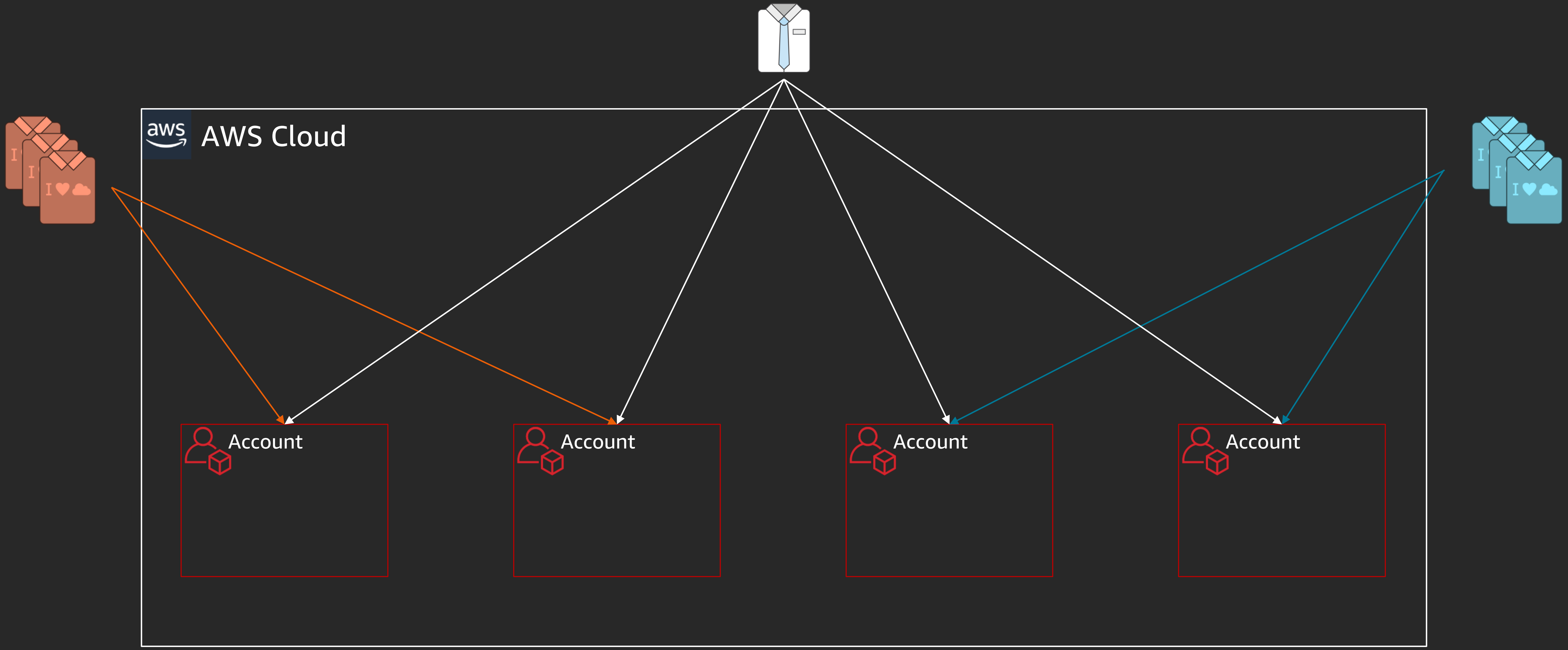


| | |
|---|---|
| table | `arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}` |

```
"arn:aws:dynamodb:ap-southeast-2:111122223333:table/MyTableName"
```

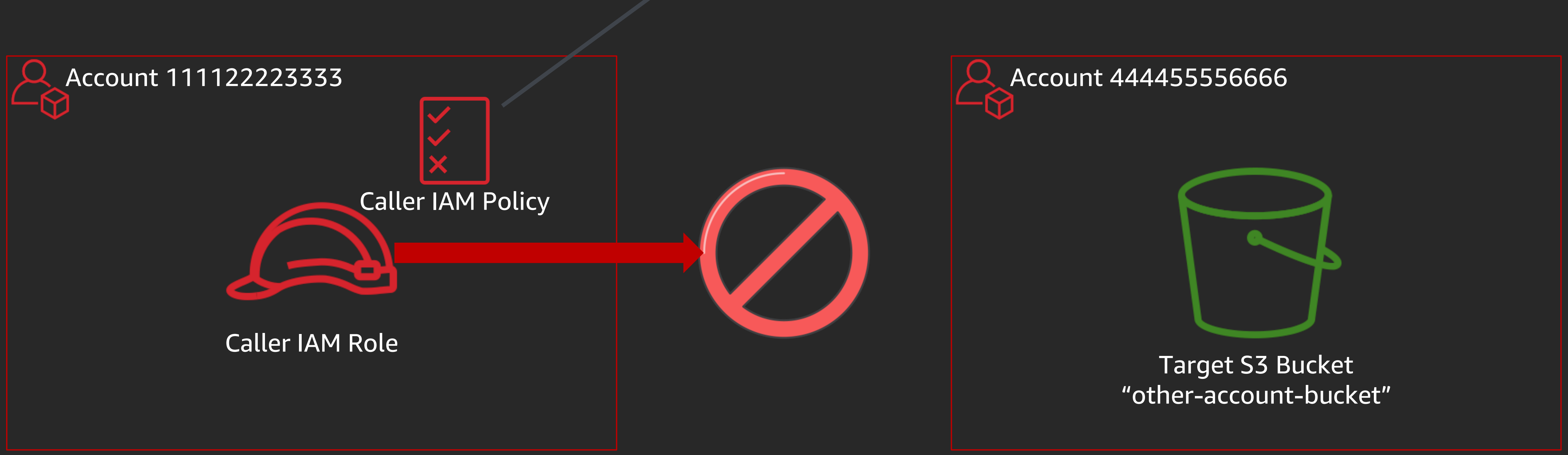
Resource ARN format

# IAM in an AWS enterprise environment



# Working across AWS account boundaries

```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::other-account-bucket/*"
}
```



Account 111122223333

Caller IAM Policy

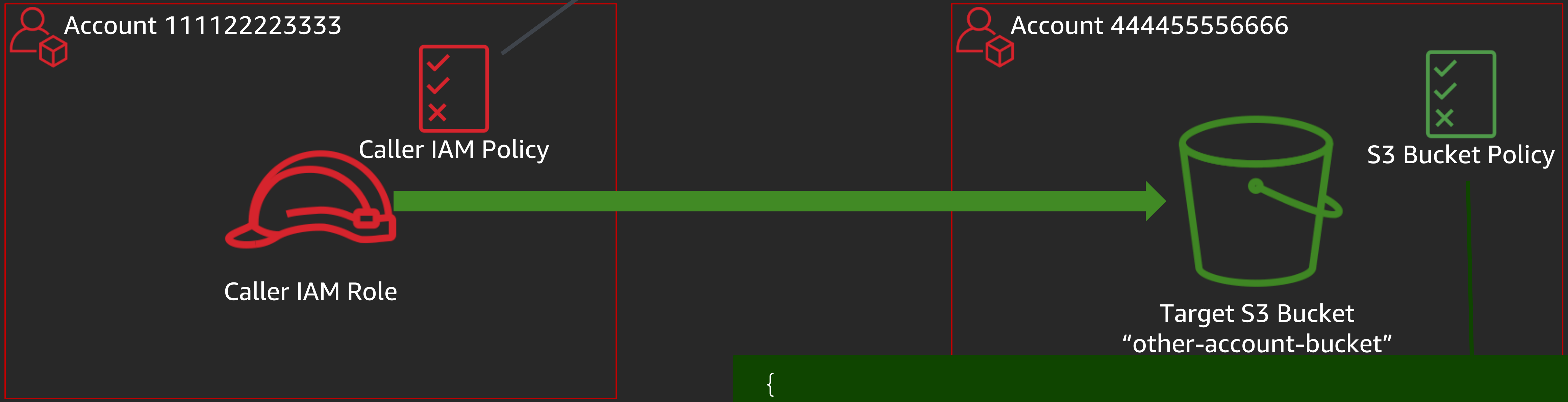
Caller IAM Role

Account 444455556666

Target S3 Bucket
“other-account-bucket”

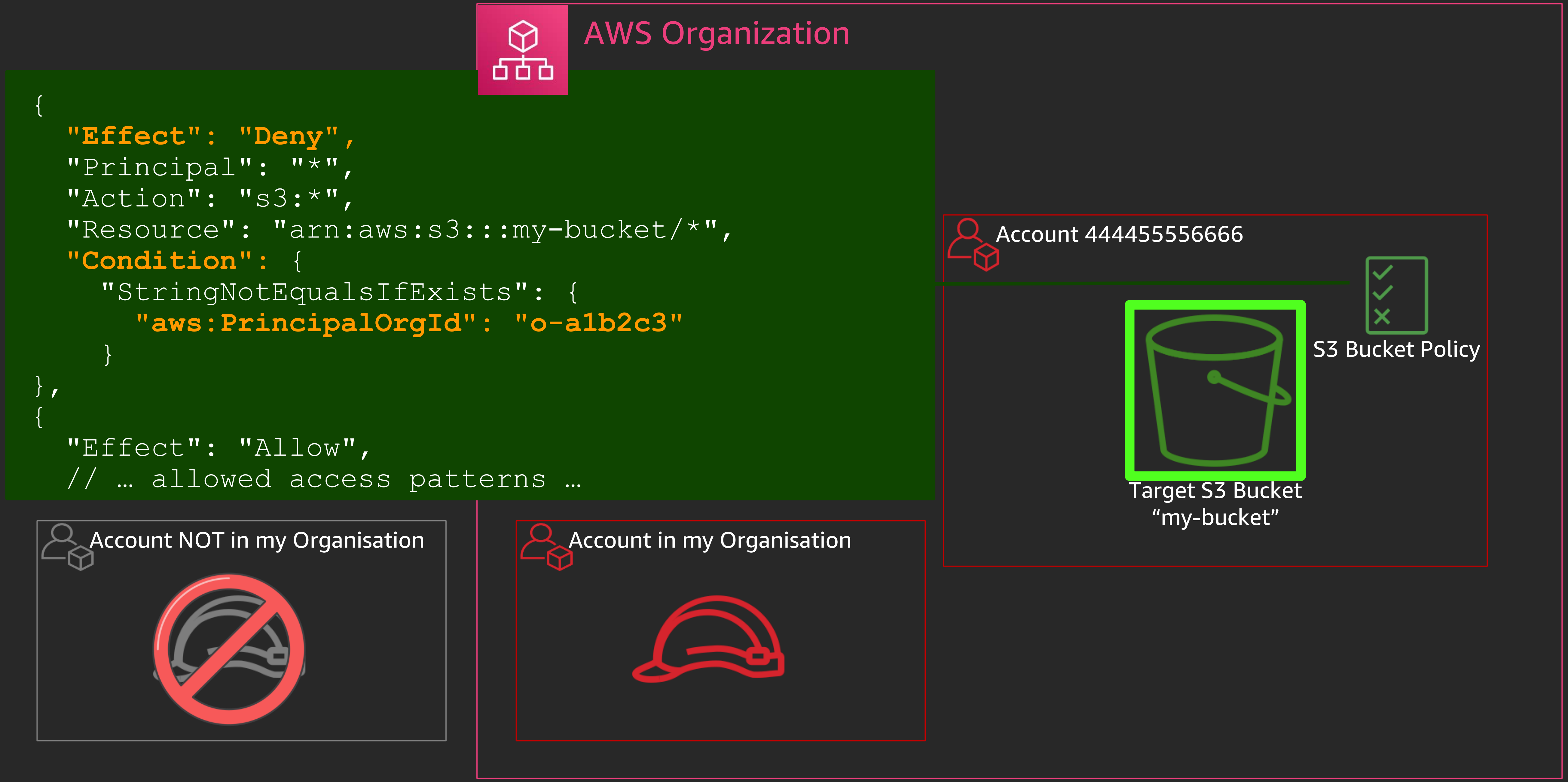
# Working across AWS account boundaries

```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::other-account-bucket/*"
}
```



```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "111122223333"
  }
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::other-account-bucket/*"
}
```

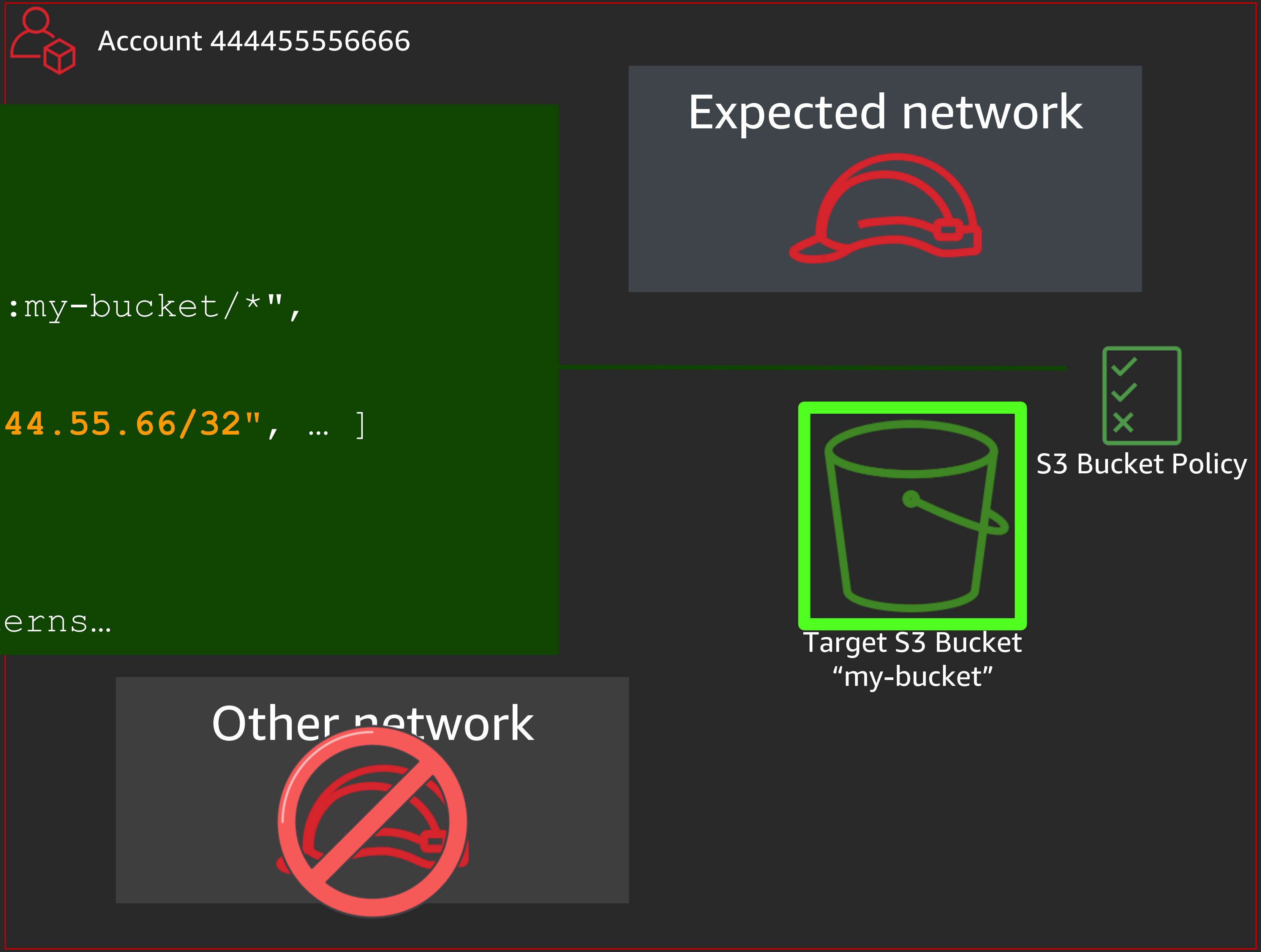
# Example: S3 Bucket Policies



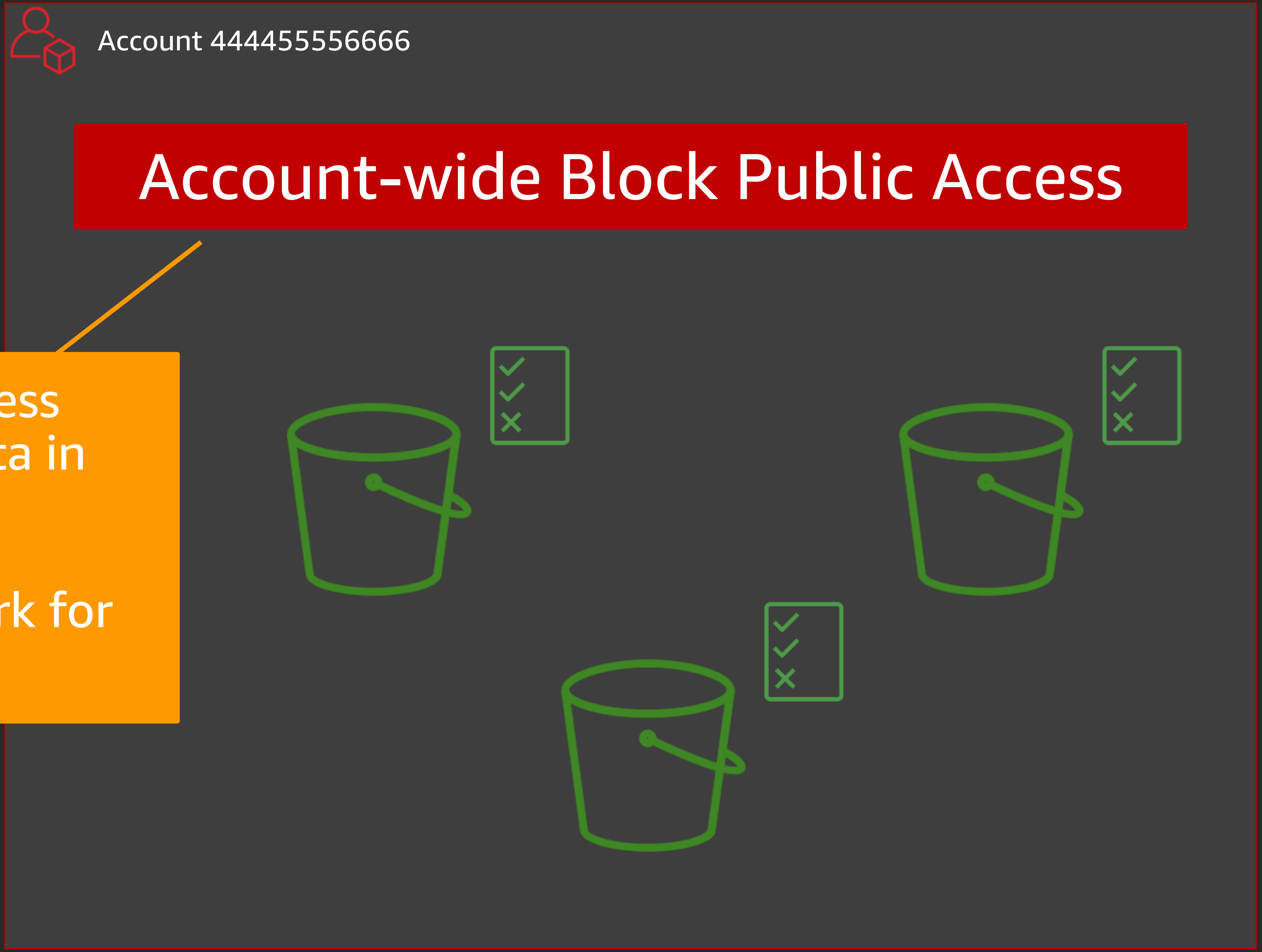
```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "arn:aws:s3:::my-bucket/*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:PrincipalOrgId": "o-a1b2c3"
    }
},
{
  "Effect": "Allow",
  // … allowed access patterns …
```

# Example: S3 Bucket Policies

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "arn:aws:s3:::my-bucket/*",
  "Condition": {
    "IpAddress": {
      "aws:SourceIp": [ "3.44.55.66/32", … ]
    }
},
{
  "Effect": "Allow",
  // … allowed access  patterns…
```



# Example: S3 Bucket Policies



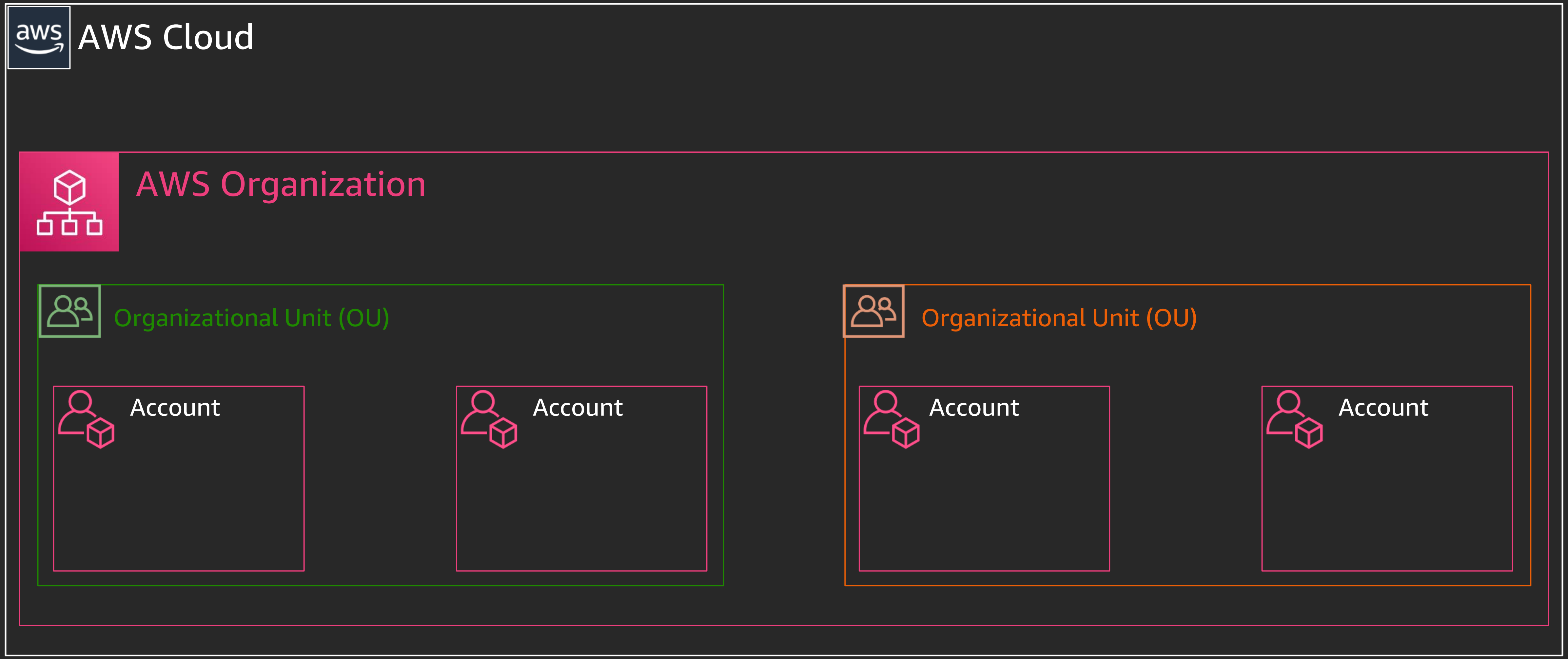
Account 444455556666

Account-wide Block Public Access

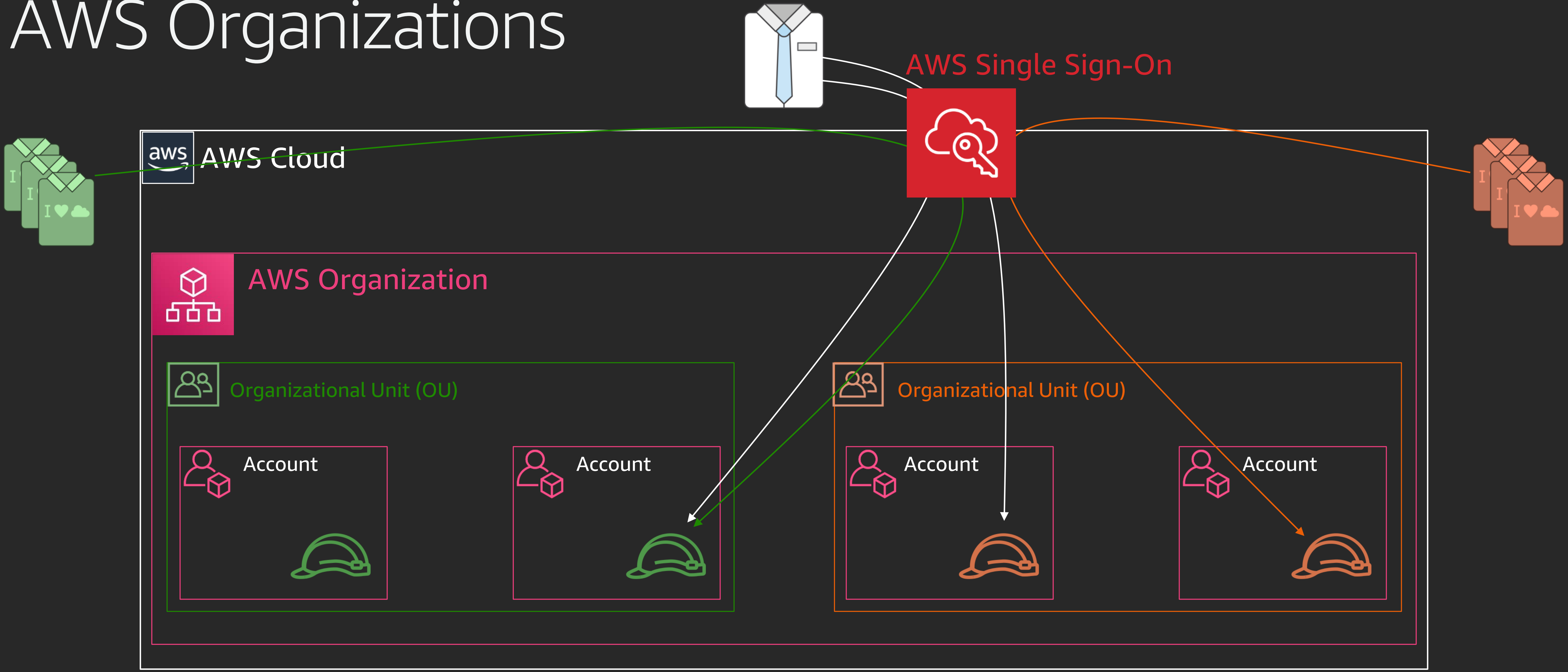
Enable Block Public Access unless you are hosting fully public data in your bucket (this is rare).

Your bucket policy will still work for specific cross-account access.

# Managing multi-account environments with AWS Organizations

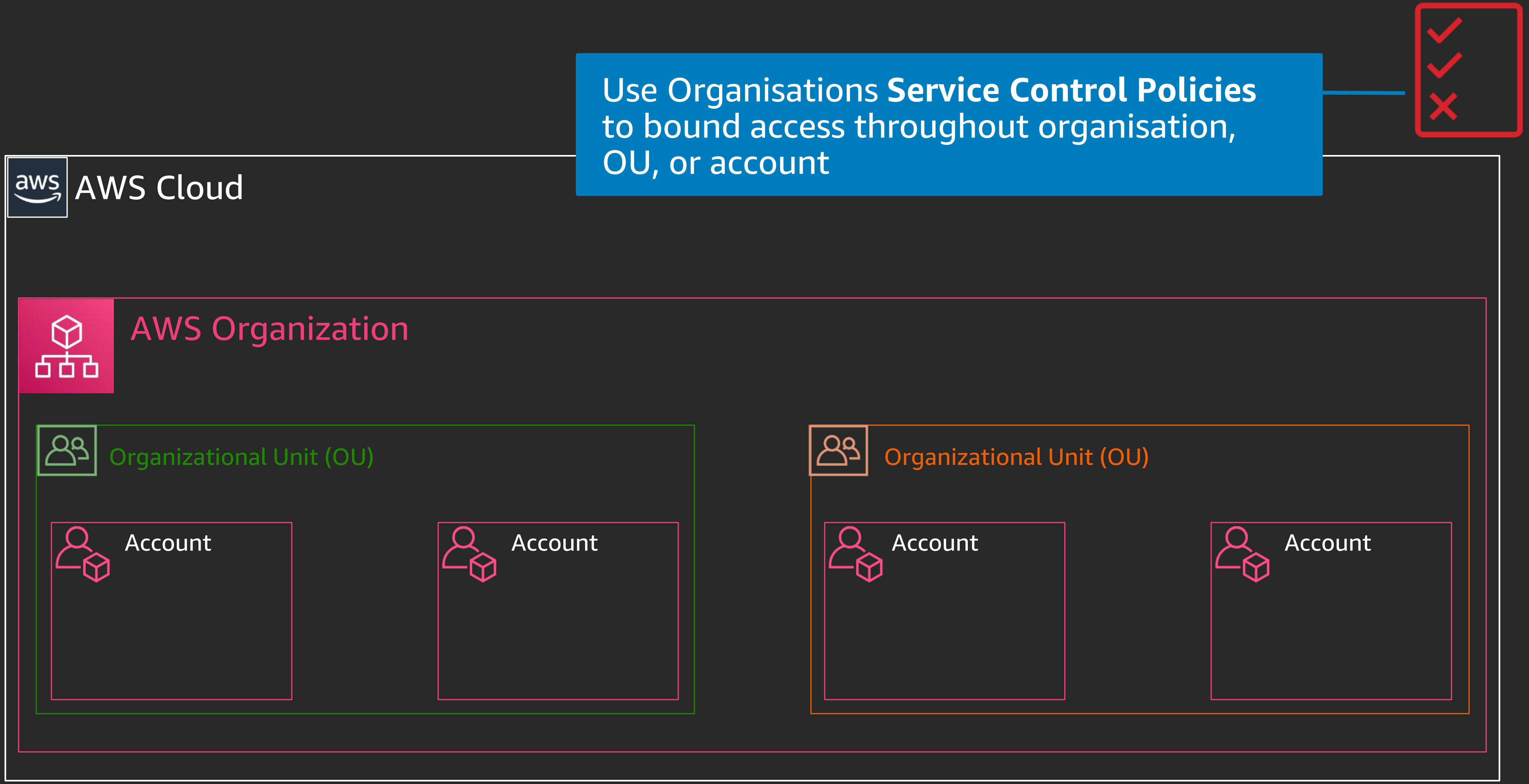


# Managing multi-account environments with AWS Organizations



# Organisations provides guardrails for IAM

Use Organisations **Service Control Policies** to bound access throughout organisation, OU, or account



# AWS Key Management Service

# AWS Key Management Service (AWS KMS)

## What it is:

AWS-managed encryption/decryption service

## Why it matters to you:

Many data-handling AWS services offer simple AWS KMS integrations. If you know how to use AWS KMS, you can protect your data at rest simply and with no management overhead.

## What builders need to know:

- The basics of how to use an AWS KMS key
- Familiarity with the AWS KMS integrations offered by many AWS data-handling services
- How to use IAM to control access to keys

# If you don’t understand the next slide, it’s OK

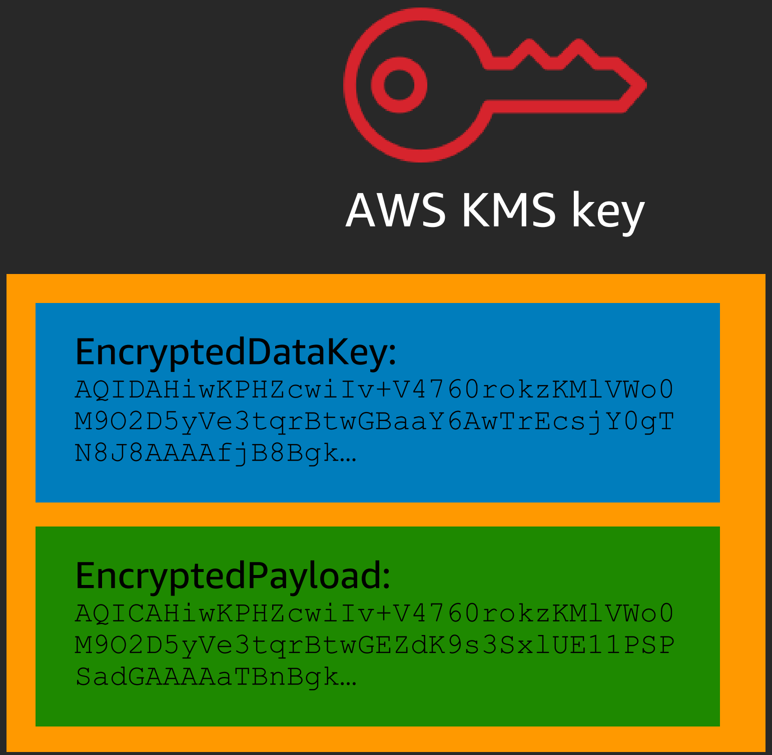
# The mechanics of an AWS KMS key

## For encrypting individual pieces of data (<=4KB):

- KMS.Encrypt(“hello world”) ➔ AQICAHiwKPHZcwiIv….
- KMS.Decrypt(“AQICAHiwKPHZcwiIv….”) ➔ “hello world”

## For encrypting application data, use envelope encryption:

- KMS.GenerateDataKey ➔ symmetric data key (plaintext and encrypted)
- Use plaintext data key to encrypt your data, then discard
- Store encrypted data key alongside your data
- To decrypt:
  - KMS.Decrypt(encryptedDataKey) ➔ plaintextDataKey
  - Then decrypt the data with the plaintext symmetric key



AWS KMS key

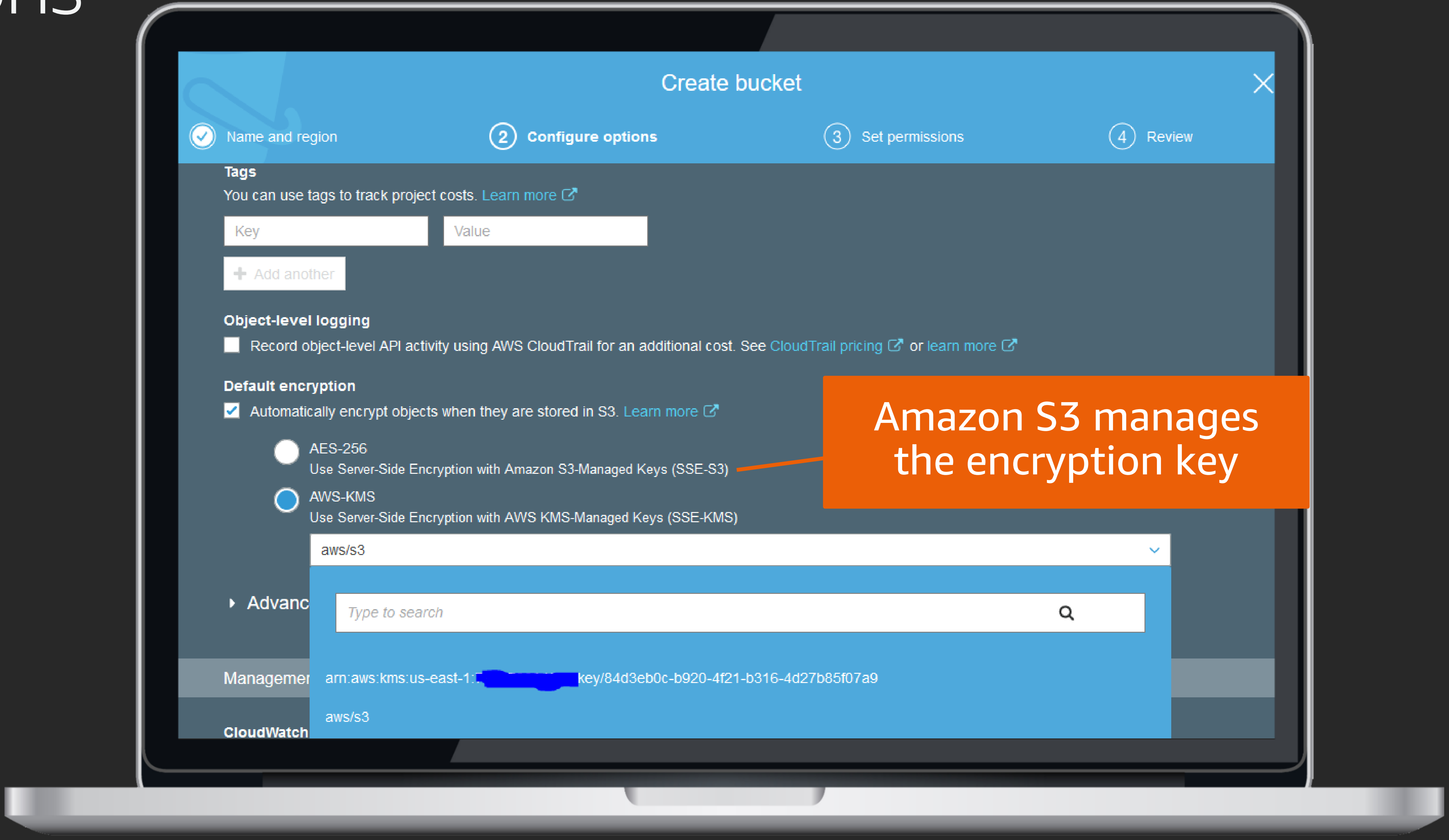
EncryptedDataKey:
AQIDAHiwKPHZcwiIv+V4760rokzKMlVWo0
M9O2D5yVe3tqrBtwGBaaY6AwTrEcsjY0gT
N8J8AAAAfjB8Bgk…

EncryptedPayload:
AQICAHiwKPHZcwiIv+V4760rokzKMlVWo0
M9O2D5yVe3tqrBtwGEZdK9s3SxlUE11PSP
SadGAAAAaTBnBgk…

# Why you didn’t need to understand that:

# AWS services manage the AWS KMS mechanics for you

# Encrypting the easy way with AWS Service Integrations



Create bucket

✓ Name and region   2 Configure options   3 Set permissions   4 Review

**Tags**

You can use tags to track project costs. Learn more

Key   Value

+ Add another

**Object-level logging**

□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

**Default encryption**

☑ Automatically encrypt objects when they are stored in S3. Learn more

○ AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

● AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

aws/s3

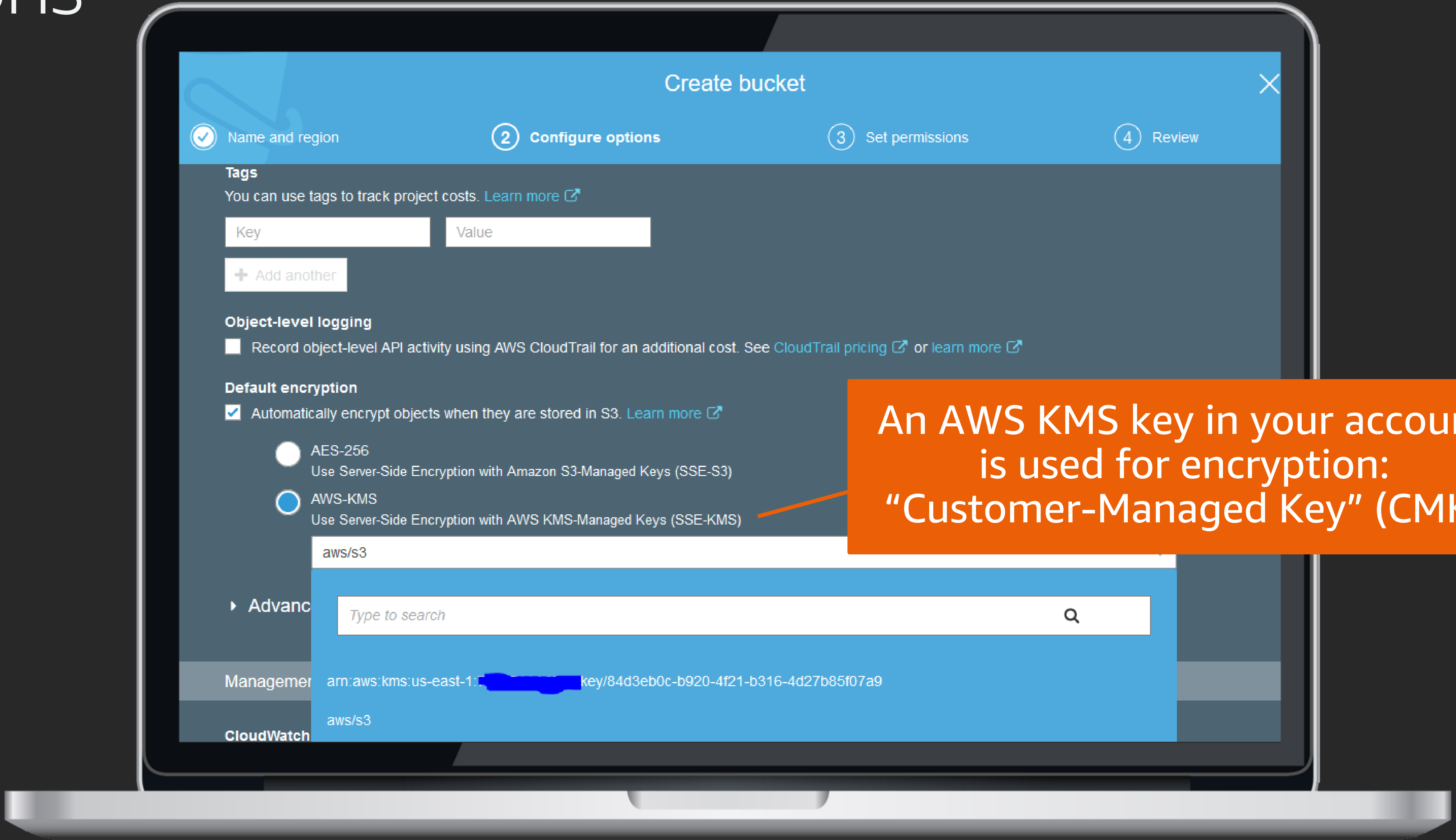
Type to search

arn:aws:kms:us-east-1:[redacted]key/84d3eb0c-b920-4f21-b316-4d27b85f07a9

aws/s3

Amazon S3 manages the encryption key

# Encrypting the easy way with AWS Service Integrations



Create bucket

✓ Name and region 2 **Configure options** 3 Set permissions 4 Review

**Tags**

You can use tags to track project costs. Learn more

Key | Value

+ Add another

**Object-level logging**

□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

**Default encryption**

☑ Automatically encrypt objects when they are stored in S3. Learn more

○ AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

● AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

aws/s3

Type to search

arn:aws:kms:us-east-1:[redacted]key/84d3eb0c-b920-4f21-b316-4d27b85f07a9

aws/s3

▸ Advanc

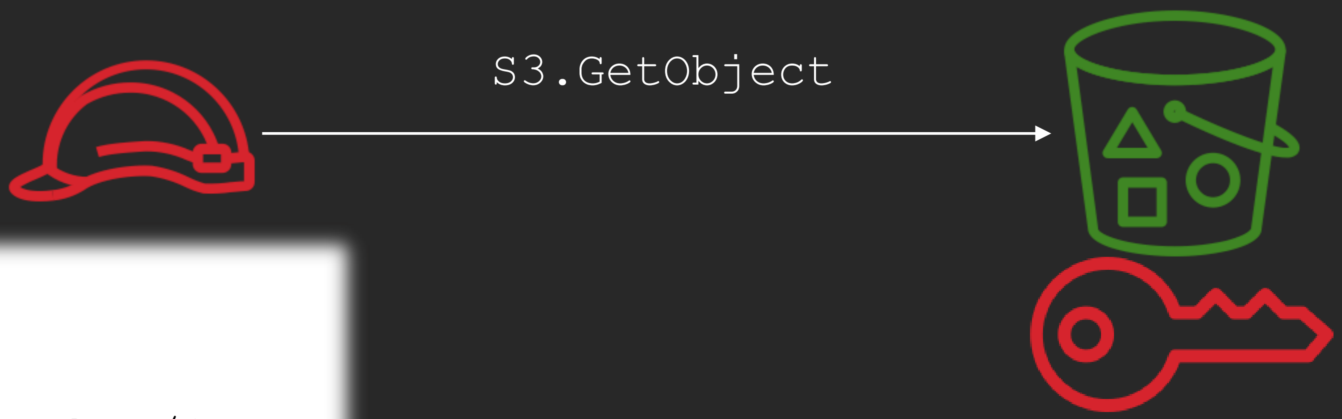
Managemen

CloudWatch

An AWS KMS key in your account is used for encryption: “Customer-Managed Key” (CMK)

# IAM permissions for AWS KMS keys

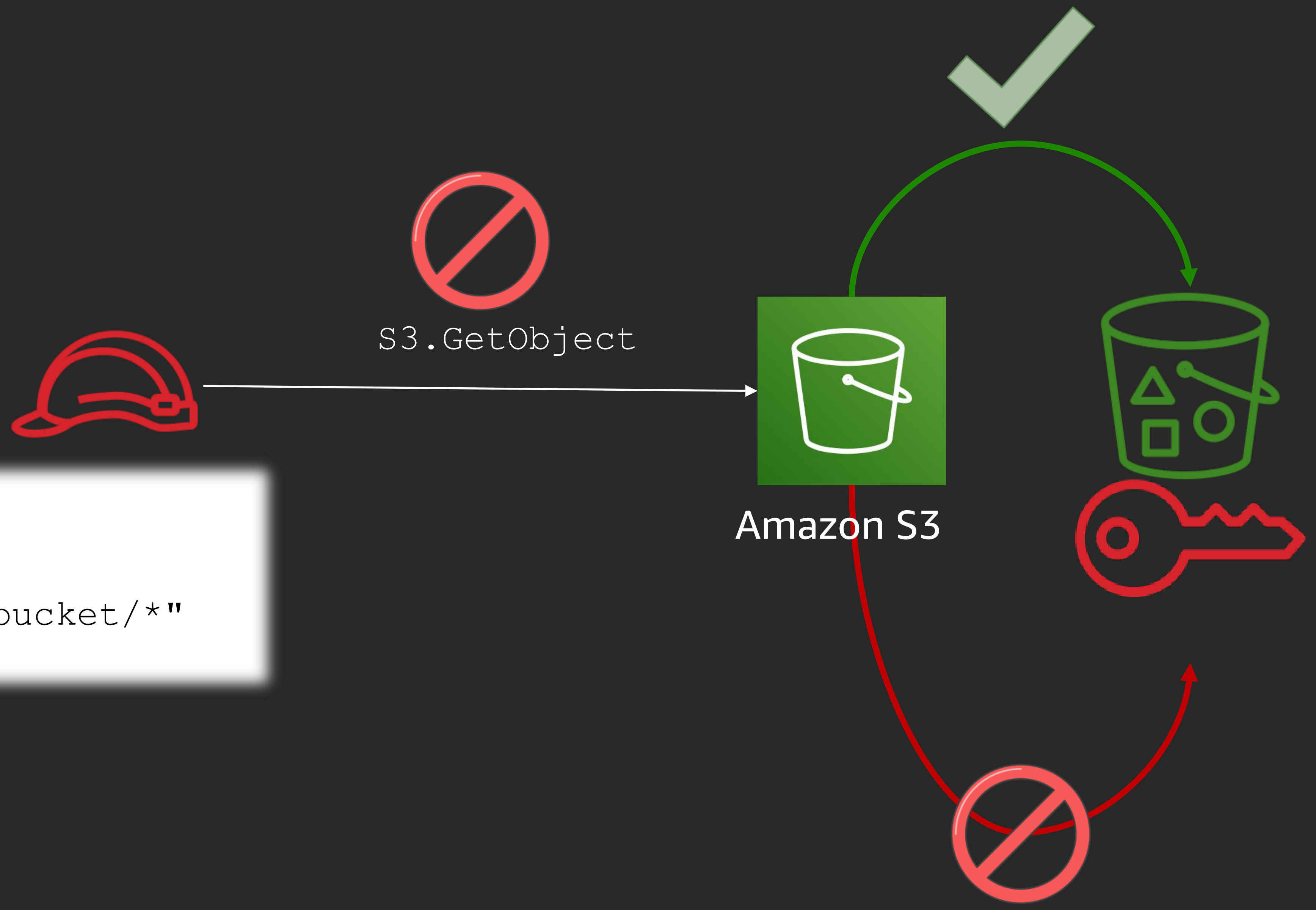
**Question: What happens here?**



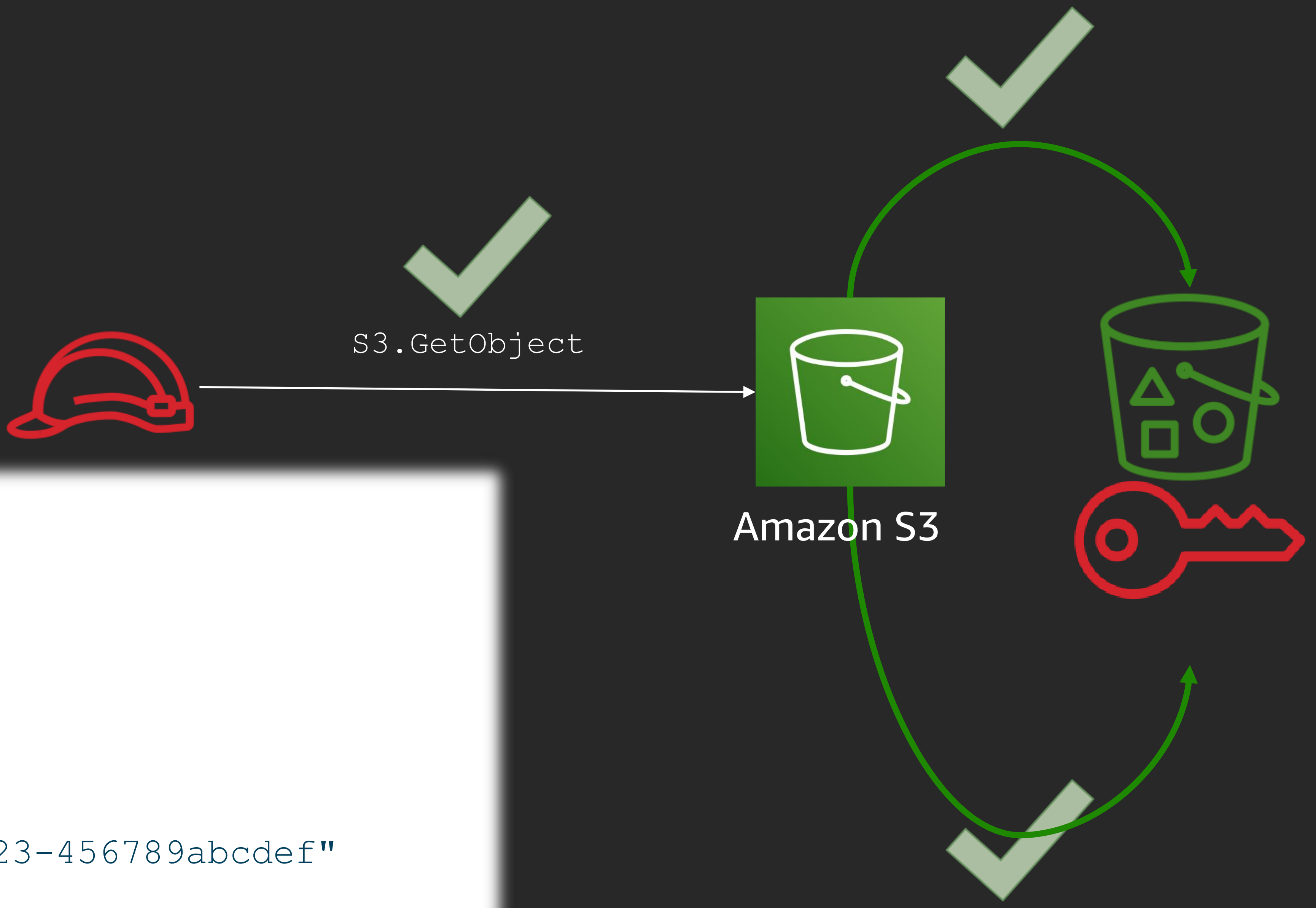
```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*"
}
```

# IAM permissions for AWS KMS keys

```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*"
}
```

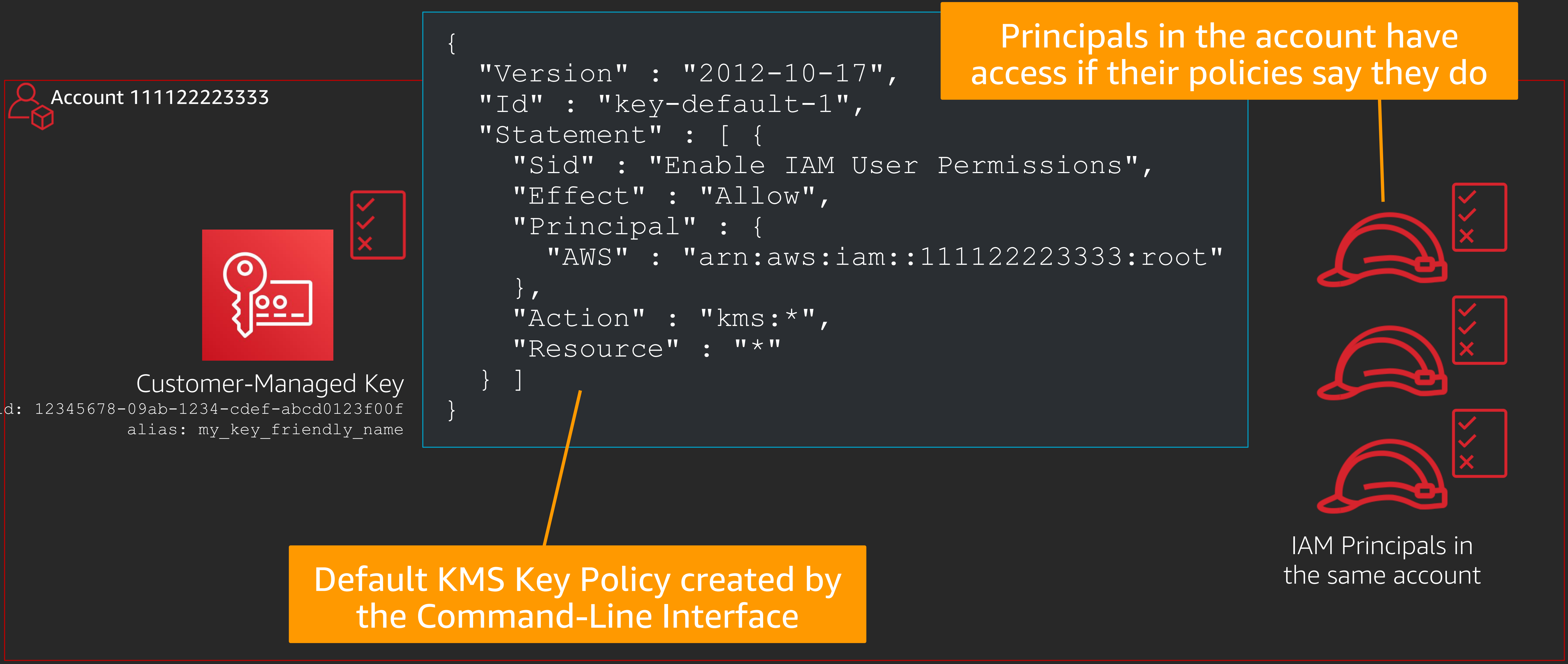


# IAM permissions for AWS KMS keys



```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*"
},
{
  "Effect": "Allow",
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:us-east-
2:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"
}
```

# The default KMS Key Policy


Account 111122223333
Customer-Managed Key
id: 12345678-09ab-1234-cdef-abcd0123f00f
alias: my_key_friendly_name
IAM Principals in the same account

```
{
  "Version" : "2012-10-17",
  "Id" : "key-default-1",
  "Statement" : [ {
    "Sid" : "Enable IAM User Permissions",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

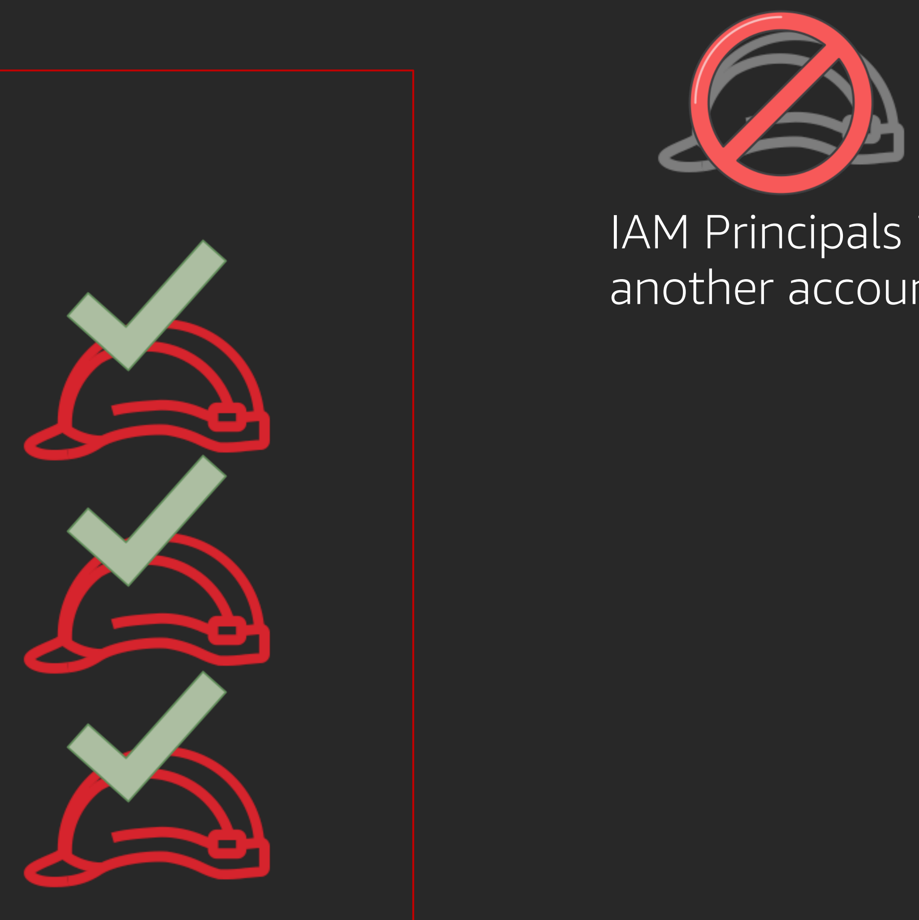
Principals in the account have access if their policies say they do

Default KMS Key Policy created by the Command-Line Interface

# AWS-Managed KMS Keys

```
{
  "Sid": "Allow access through SNS to all
principals in the account that are authorised
to use SNS",
  "Effect": "Allow",
  "Principal": { "AWS": "*" },
  "Action: [
    "kms:Decrypt",
    "kms:GenerateDataKey",
    … a couple others
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "sns.us-east-
2.amazonaws.com",
      "kms:CallerAccount": "111122223333"
    }
  }
}
```

AWS-Managed Key:
aws/sns



IAM Principals in
the same account

IAM Principals in
another account

# Amazon Virtual Private Cloud

aws SUMMIT ONLINE

# Amazon Virtual Private Cloud (Amazon VPC)

## What it is:

“Your virtual data center in the cloud,” i.e., the network for your cloud infrastructure

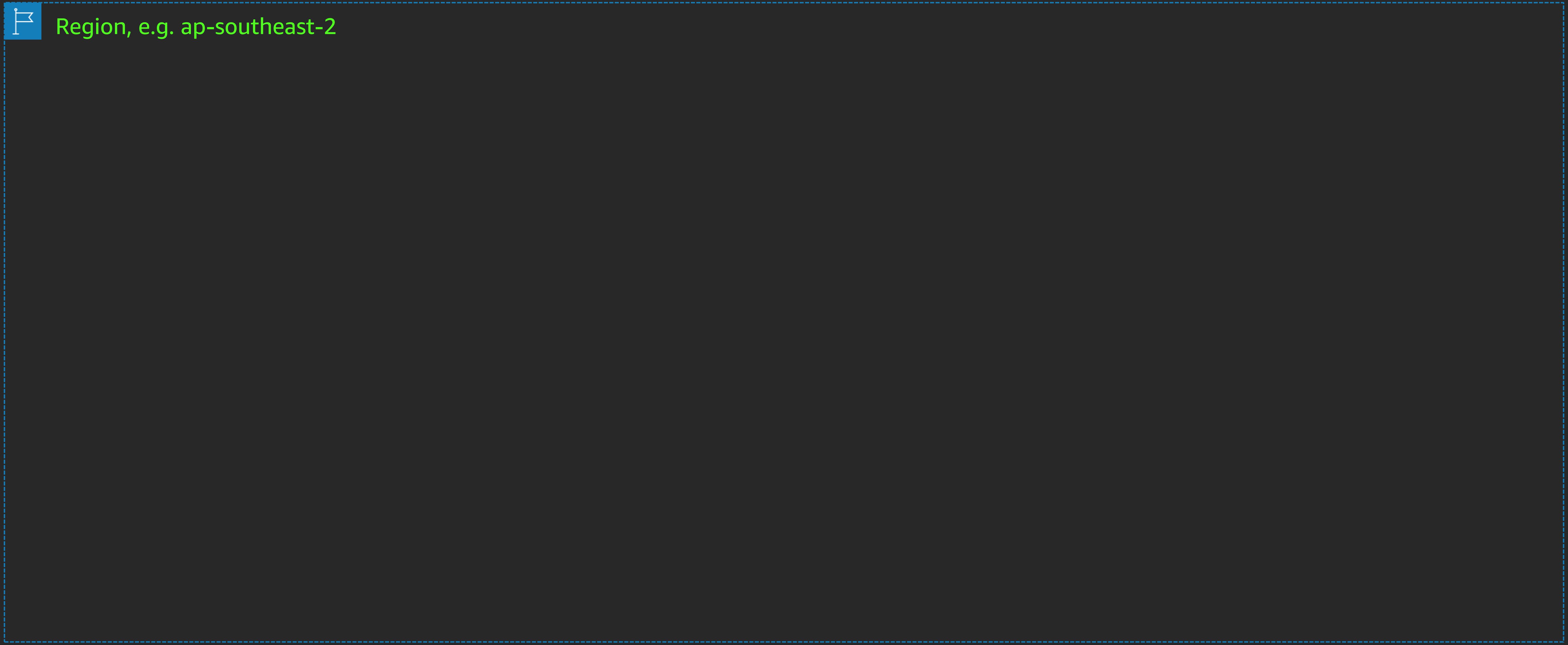
## Why it matters to you:

When you deploy cloud infrastructure, your VPC is the network that provides connectivity to and from that infrastructure

## What builders need to know:

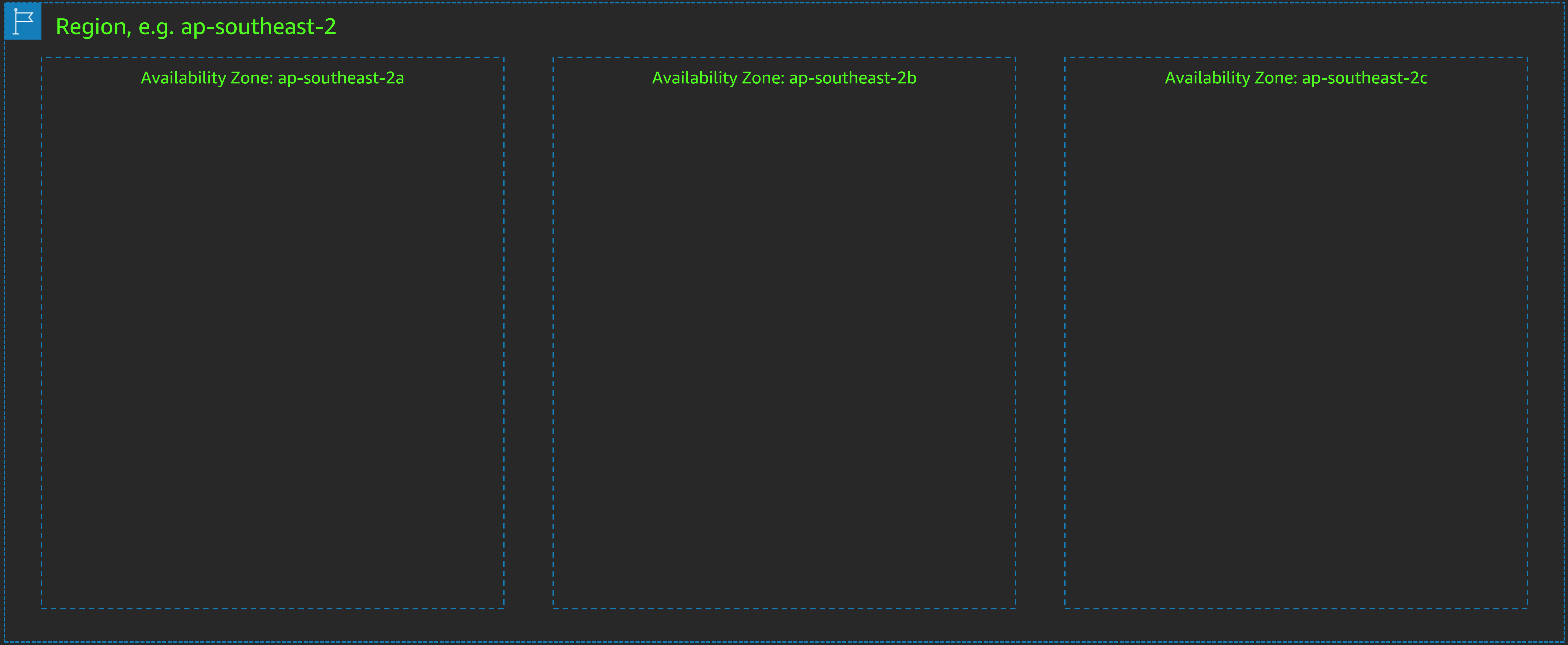
- VPC core concepts: Subnets and security groups
- Routing basics in VPC
- Private connectivity capabilities

# What a VPC is and what goes in it



Region, e.g. ap-southeast-2

# What a VPC is and what goes in it



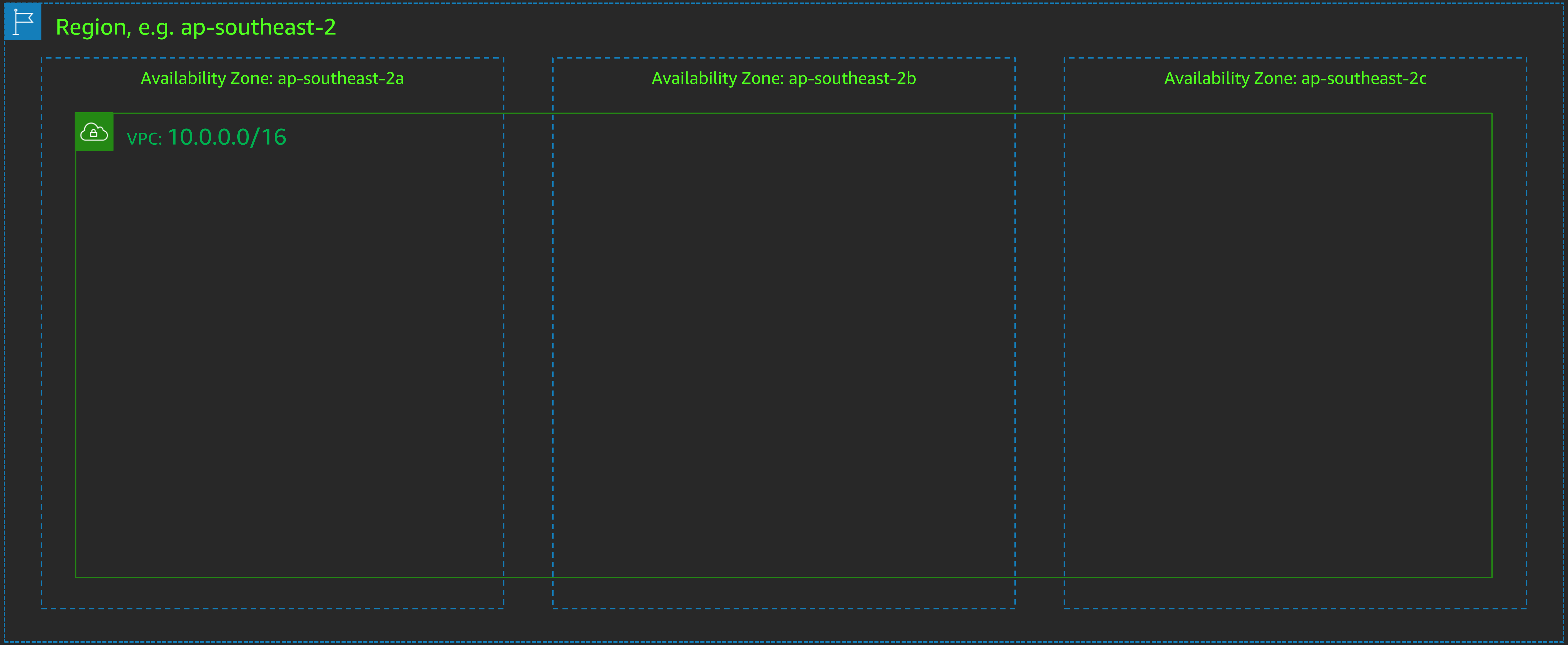
Region, e.g. ap-southeast-2

Availability Zone: ap-southeast-2a

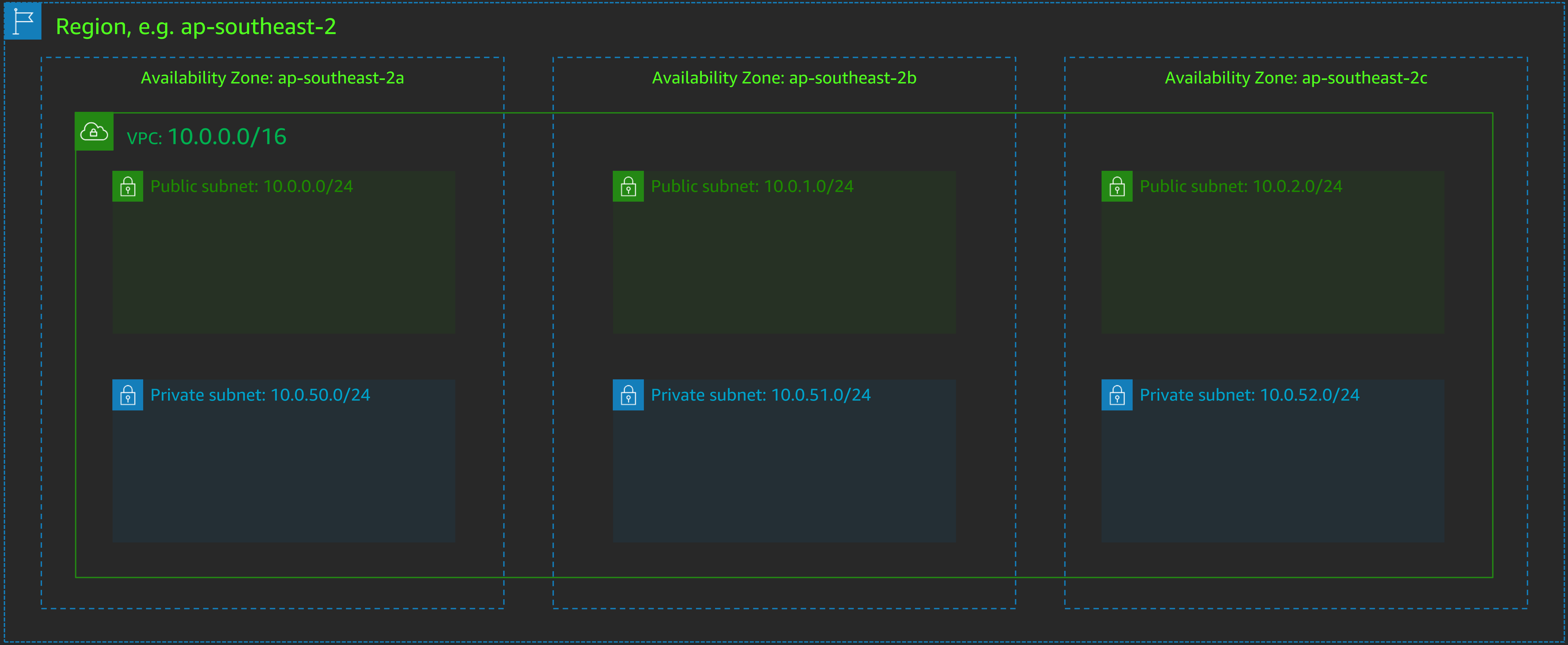
Availability Zone: ap-southeast-2b

Availability Zone: ap-southeast-2c

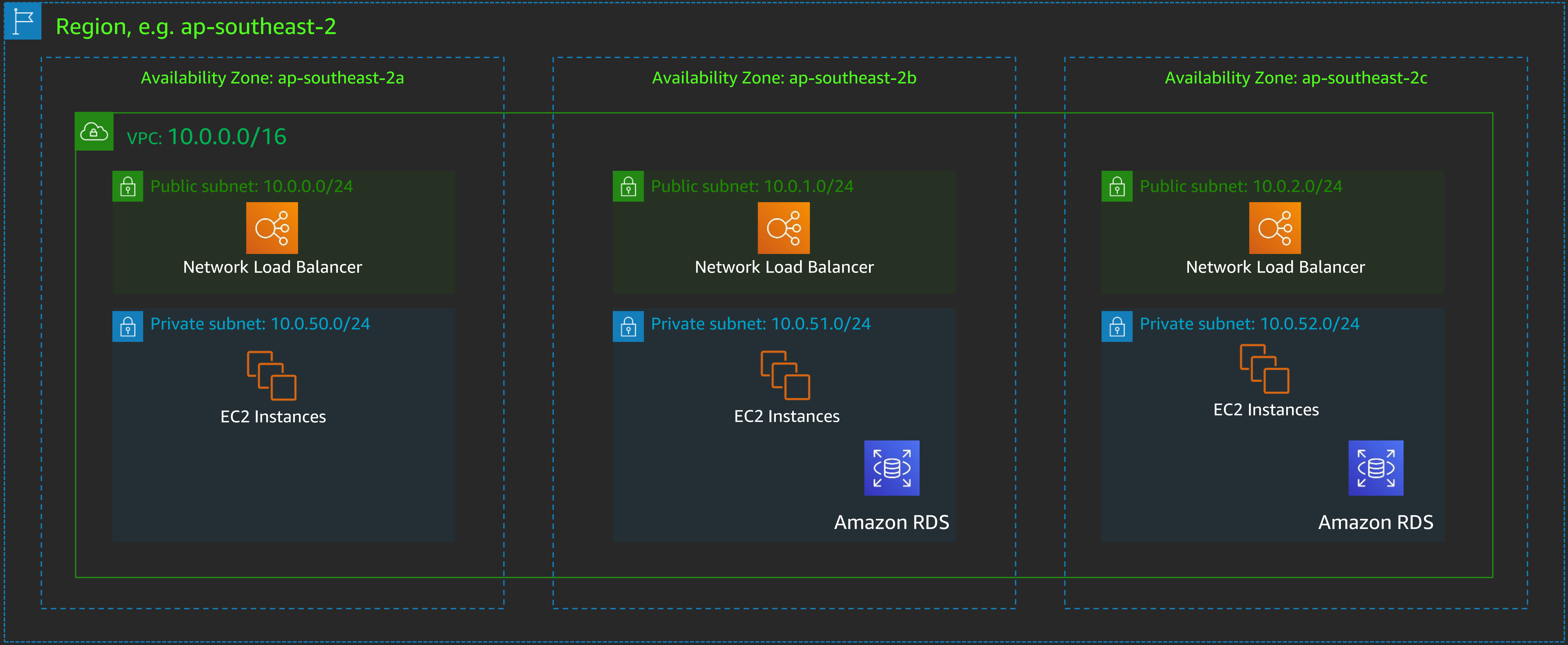
# What a VPC is and what goes in it


Region, e.g. ap-southeast-2
Availability Zone: ap-southeast-2a
Availability Zone: ap-southeast-2b
Availability Zone: ap-southeast-2c
VPC: 10.0.0.0/16

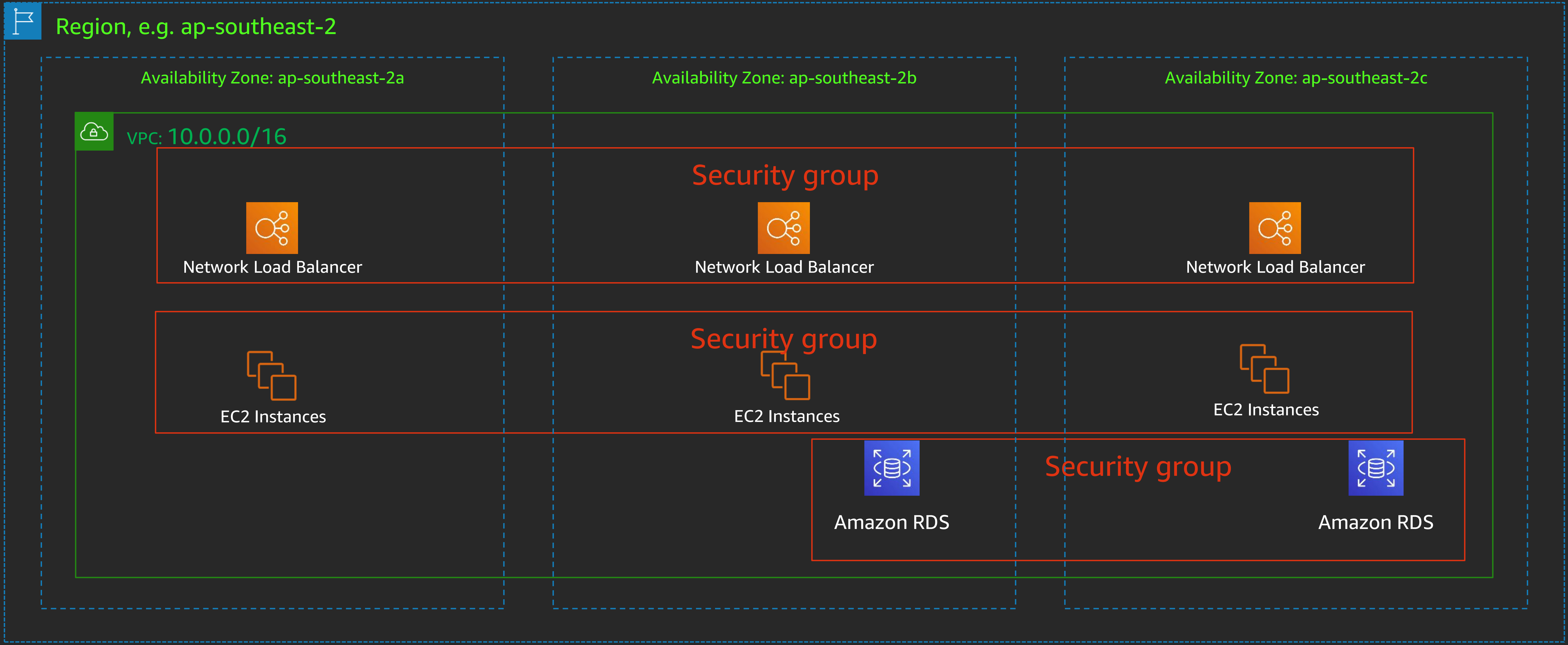
# What a VPC is and what goes in it


Region, e.g. ap-southeast-2
Availability Zone: ap-southeast-2a
Availability Zone: ap-southeast-2b
Availability Zone: ap-southeast-2c
VPC: 10.0.0.0/16
Public subnet: 10.0.0.0/24
Public subnet: 10.0.1.0/24
Public subnet: 10.0.2.0/24
Private subnet: 10.0.50.0/24
Private subnet: 10.0.51.0/24
Private subnet: 10.0.52.0/24

# What a VPC is and what goes in it

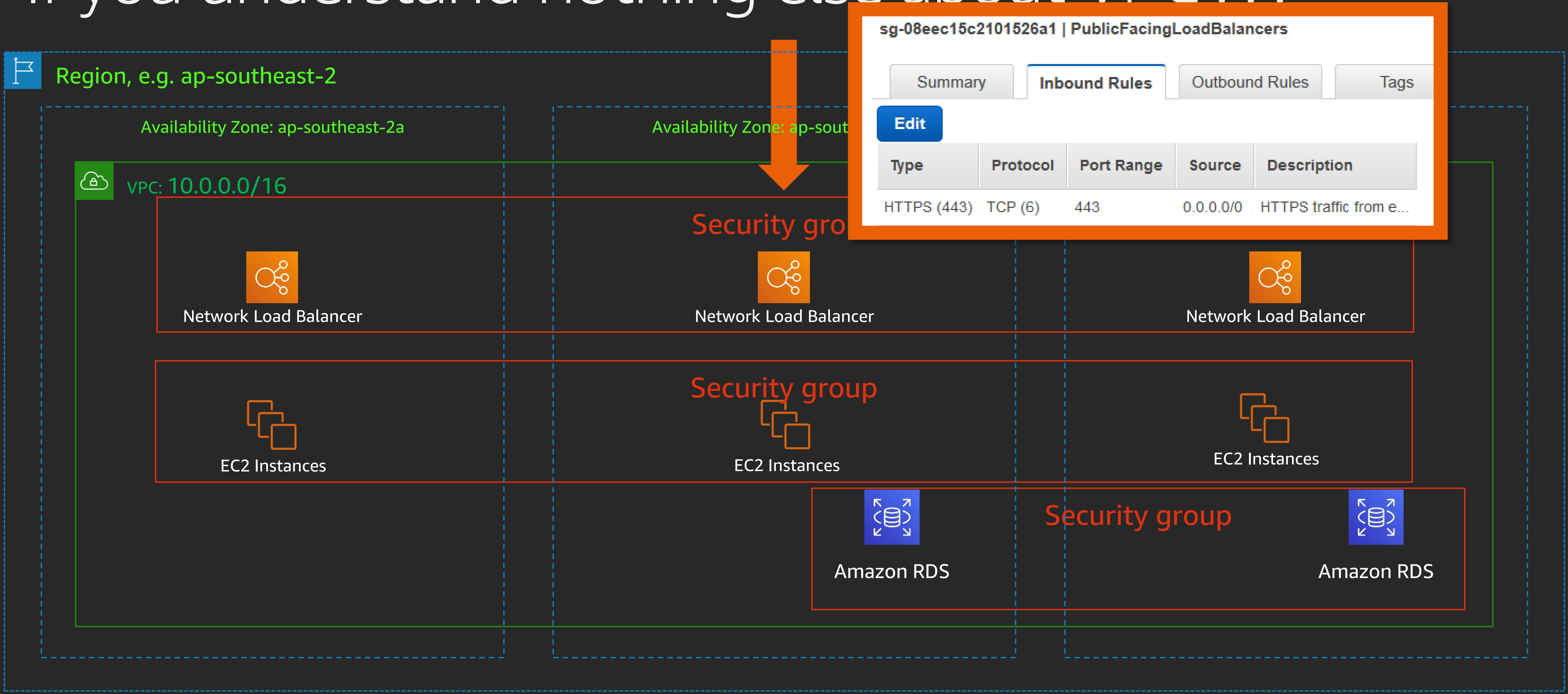

Region, e.g. ap-southeast-2
Availability Zone: ap-southeast-2a
Availability Zone: ap-southeast-2b
Availability Zone: ap-southeast-2c
VPC: 10.0.0.0/16
Public subnet: 10.0.0.0/24
Network Load Balancer
Public subnet: 10.0.1.0/24
Network Load Balancer
Public subnet: 10.0.2.0/24
Network Load Balancer
Private subnet: 10.0.50.0/24
EC2 Instances
Private subnet: 10.0.51.0/24
EC2 Instances
Amazon RDS
Private subnet: 10.0.52.0/24
EC2 Instances
Amazon RDS

# If you understand nothing else about VPC . . .



# . . . understand security groups

# If you understand nothing else about VPC . . .

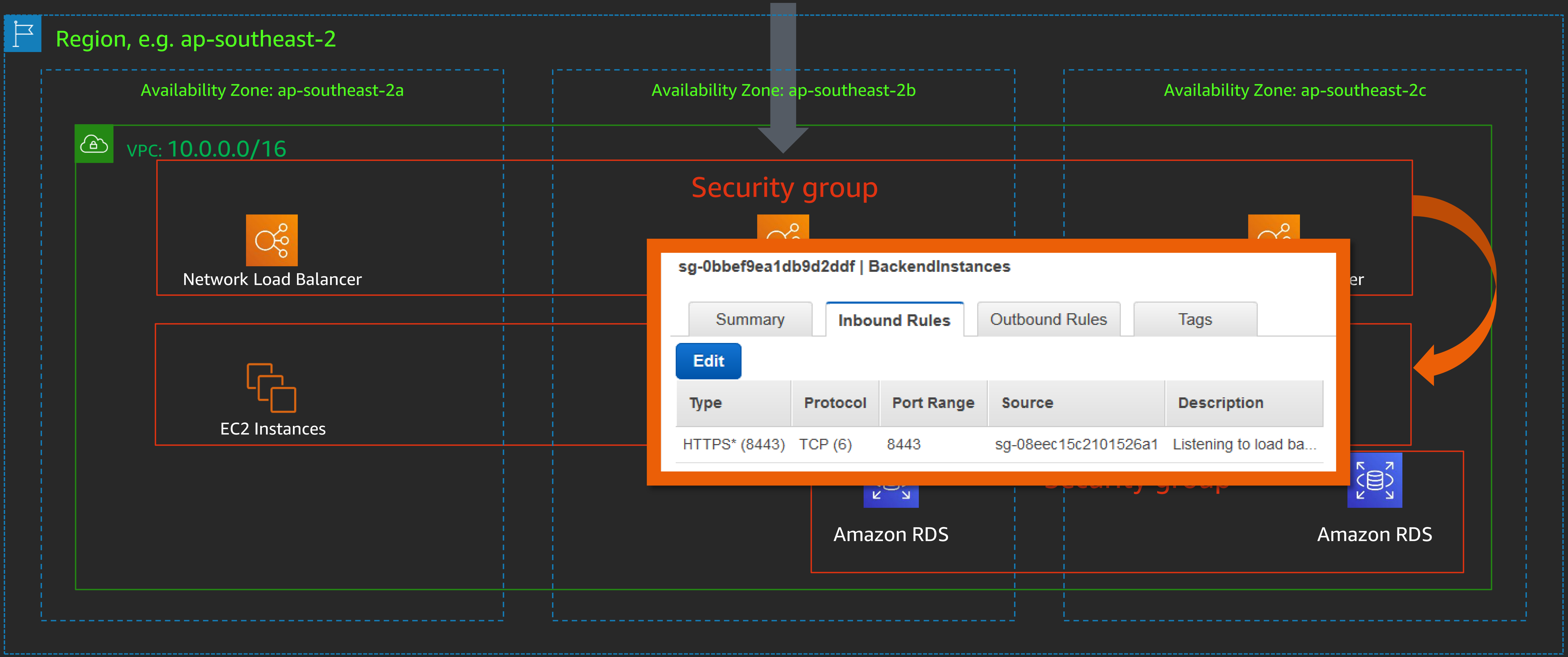


sg-08eec15c2101526a1 | PublicFacingLoadBalancers

| Type | Protocol | Port Range | Source | Description |
|---|---|---|---|---|
| HTTPS (443) | TCP (6) | 443 | 0.0.0.0/0 | HTTPS traffic from e... |

# . . . understand security groups

# If you understand nothing else about VPC . . .

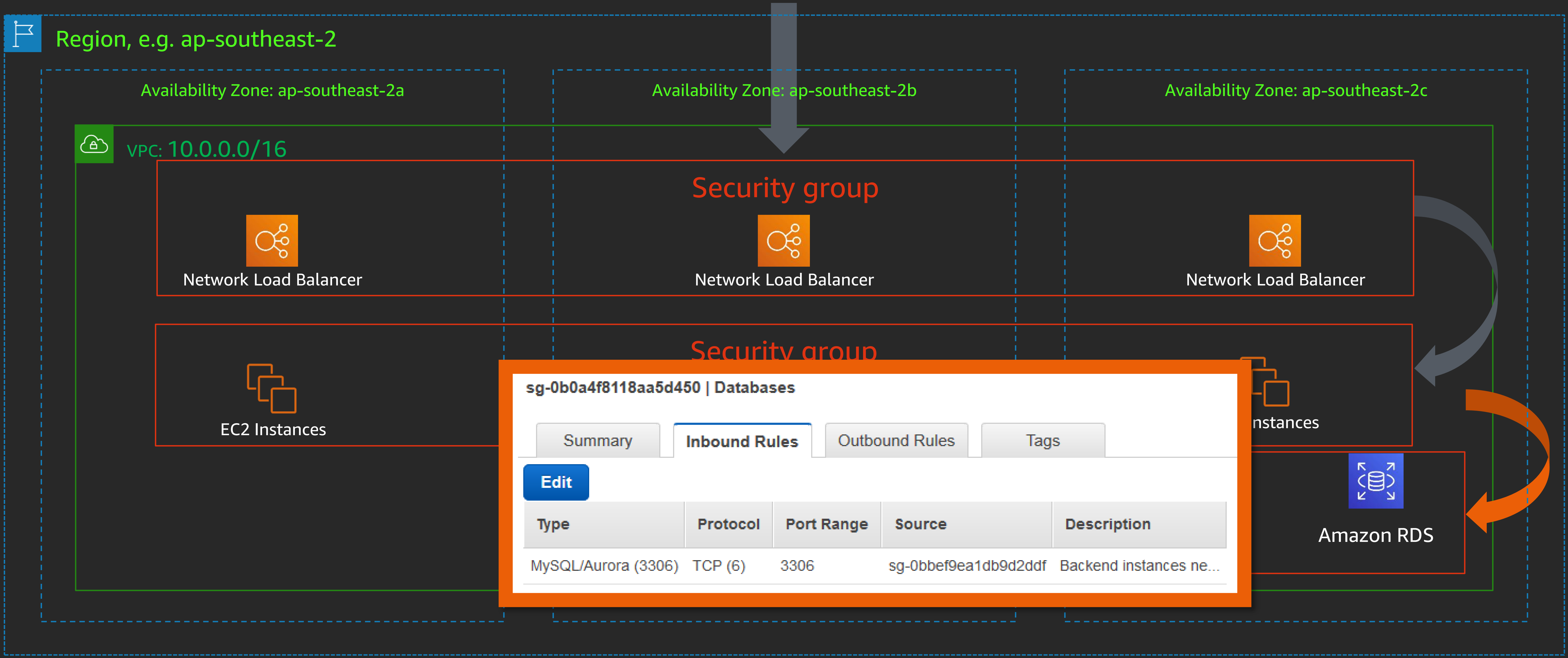

Region, e.g. ap-southeast-2
Availability Zone: ap-southeast-2a
Availability Zone: ap-southeast-2b
Availability Zone: ap-southeast-2c
VPC: 10.0.0.0/16
Security group
Network Load Balancer
er
EC2 Instances
Amazon RDS
Amazon RDS
Summary
Inbound Rules
Outbound Rules
Tags
Edit

sg-0bbef9ea1db9d2ddf | BackendInstances

| Type | Protocol | Port Range | Source | Description |
|---|---|---|---|---|
| HTTPS* (8443) | TCP (6) | 8443 | sg-08eec15c2101526a1 | Listening to load ba... |

# . . . understand security groups

# If you understand nothing else about VPC . . .

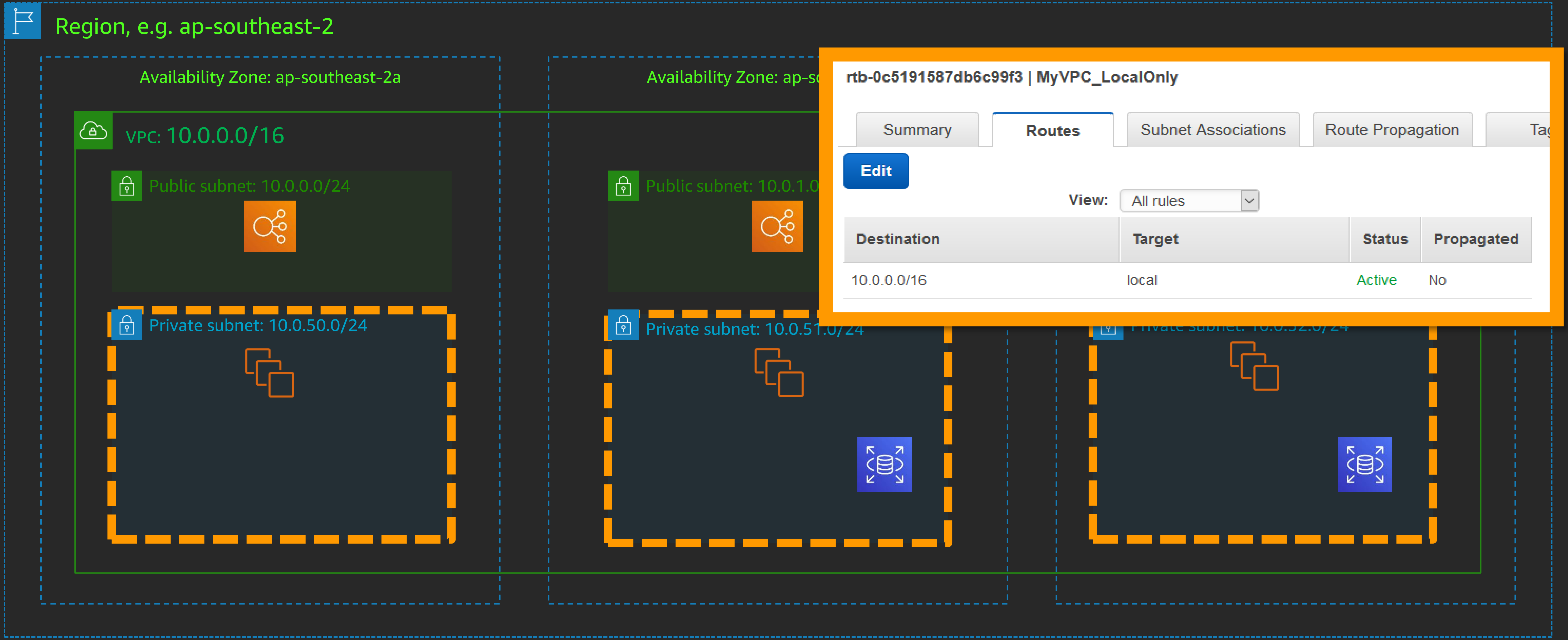


sg-0b0a4f8118aa5d450 | Databases

| Type | Protocol | Port Range | Source | Description |
|---|---|---|---|---|
| MySQL/Aurora (3306) | TCP (6) | 3306 | sg-0bbef9ea1db9d2ddf | Backend instances ne... |

# . . . understand security groups

# If you understand only two things about VPC . . .

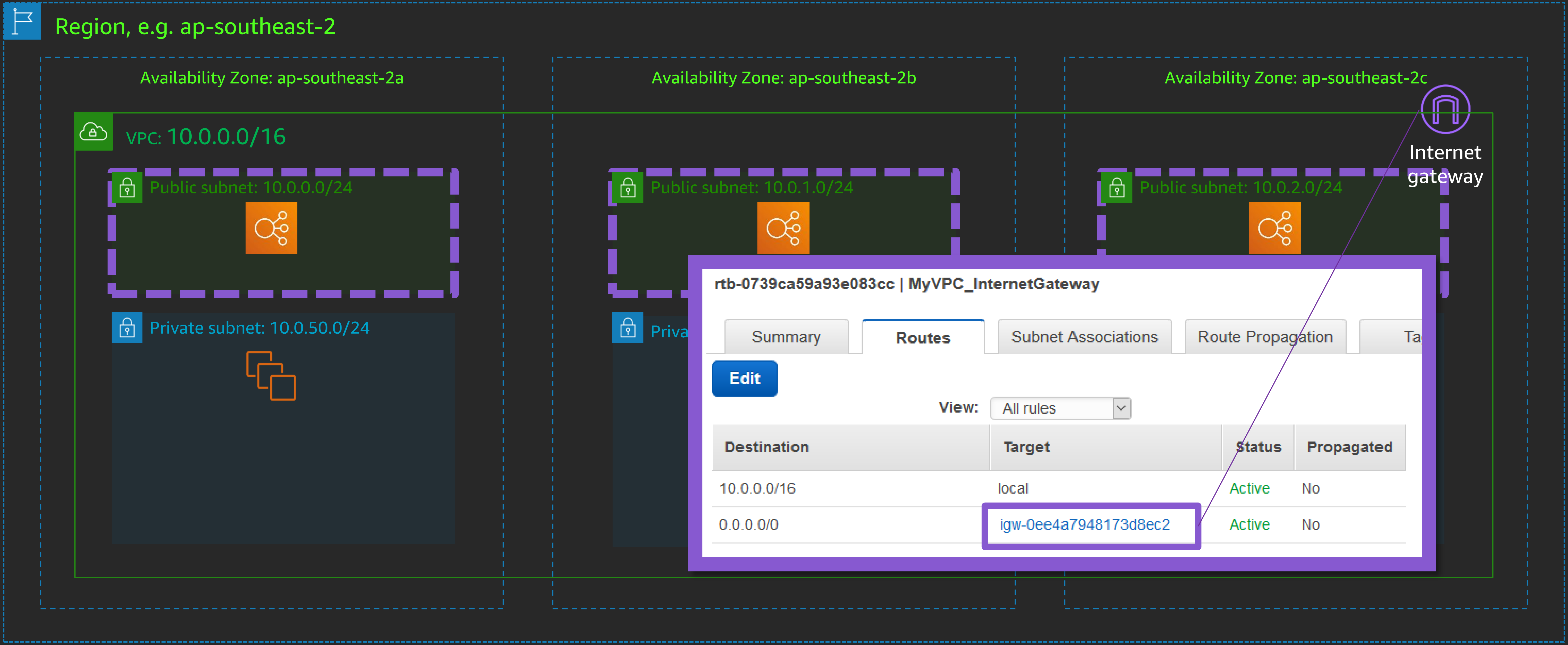

Region, e.g. ap-southeast-2
Availability Zone: ap-southeast-2a
Availability Zone: ap-s
VPC: 10.0.0.0/16
Public subnet: 10.0.0.0/24
Public subnet: 10.0.1.0
Private subnet: 10.0.50.0/24
Private subnet: 10.0.51.0/24
Private subnet: 10.0.52.0/24
Summary
Routes
Subnet Associations
Route Propagation
Tag
Edit
View: All rules

rtb-0c5191587db6c99f3 | MyVPC_LocalOnly

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.0.0.0/16 | local | Active | No |

# . . . understand routing

# If you understand only two things about VPC . . .

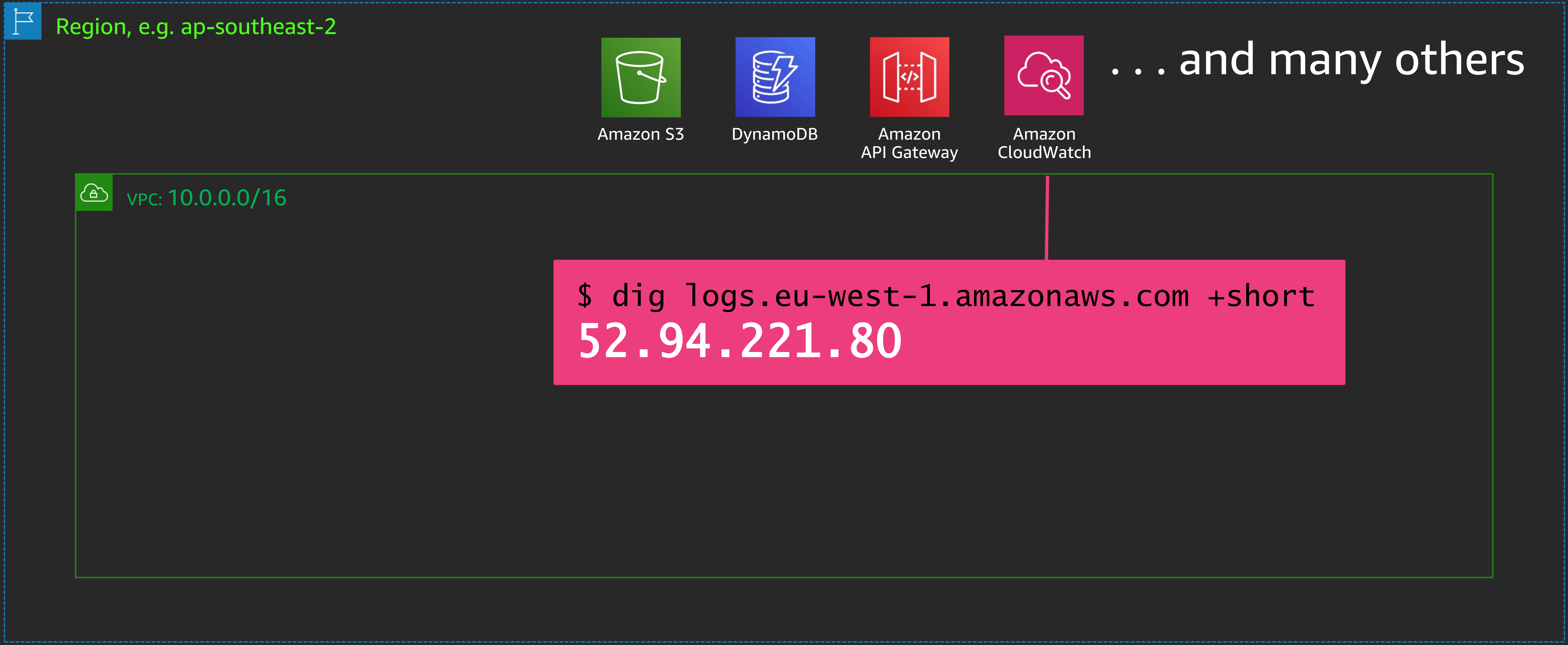

Region, e.g. ap-southeast-2
Availability Zone: ap-southeast-2a
Availability Zone: ap-southeast-2b
Availability Zone: ap-southeast-2c
VPC: 10.0.0.0/16
Internet gateway
Public subnet: 10.0.0.0/24
Public subnet: 10.0.1.0/24
Public subnet: 10.0.2.0/24
Private subnet: 10.0.50.0/24
Priva
Summary
Routes
Subnet Associations
Route Propagation
Ta
Edit
View: All rules

rtb-0739ca59a93e083cc | MyVPC_InternetGateway

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.0.0.0/16 | local | Active | No |
| 0.0.0.0/0 | igw-0ee4a7948173d8ec2 | Active | No |

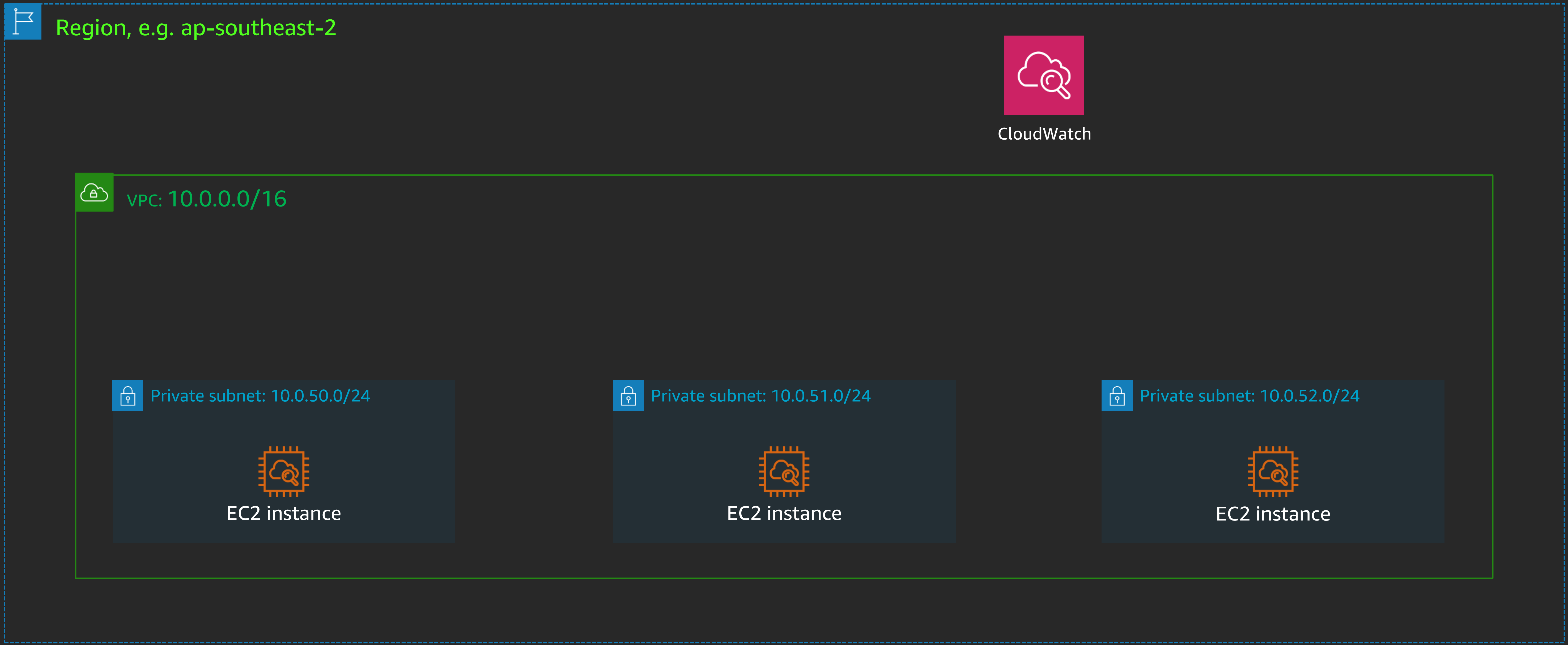
# . . . understand routing

# AWS resources not in your VPC

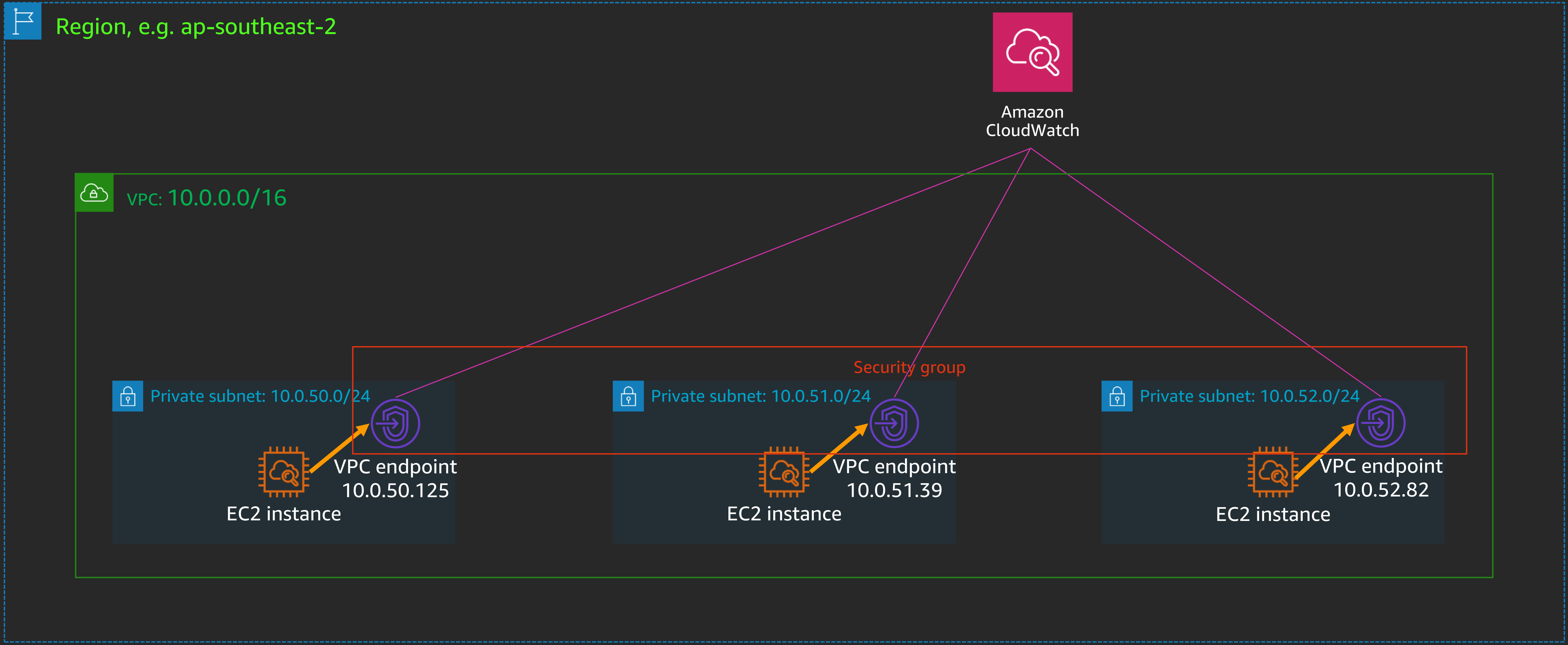


```
$ dig logs.eu-west-1.amazonaws.com +short
52.94.221.80
```

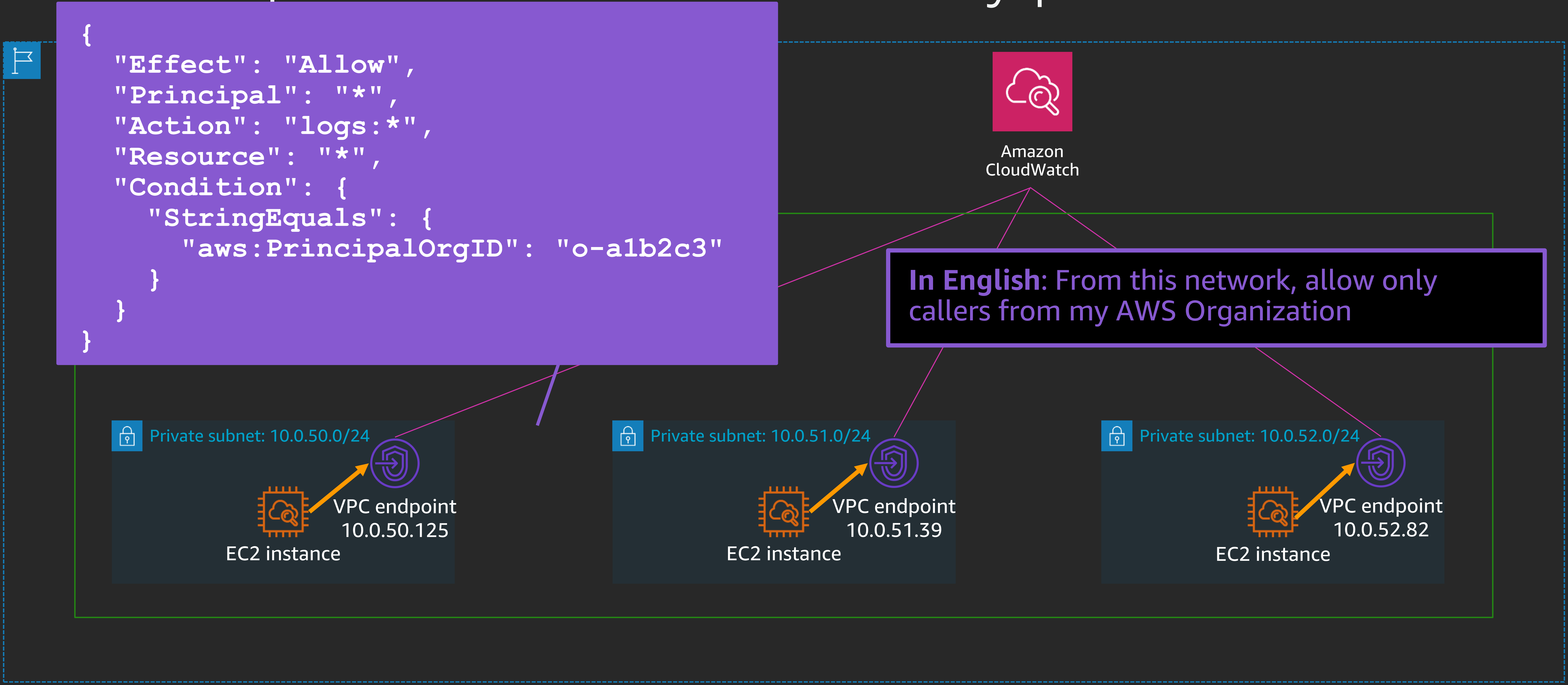
# VPC endpoints: Private connectivity to AWS services


Region, e.g. ap-southeast-2
CloudWatch
VPC: 10.0.0.0/16
Private subnet: 10.0.50.0/24
EC2 instance
Private subnet: 10.0.51.0/24
EC2 instance
Private subnet: 10.0.52.0/24
EC2 instance

# VPC endpoints: Private connectivity to AWS services



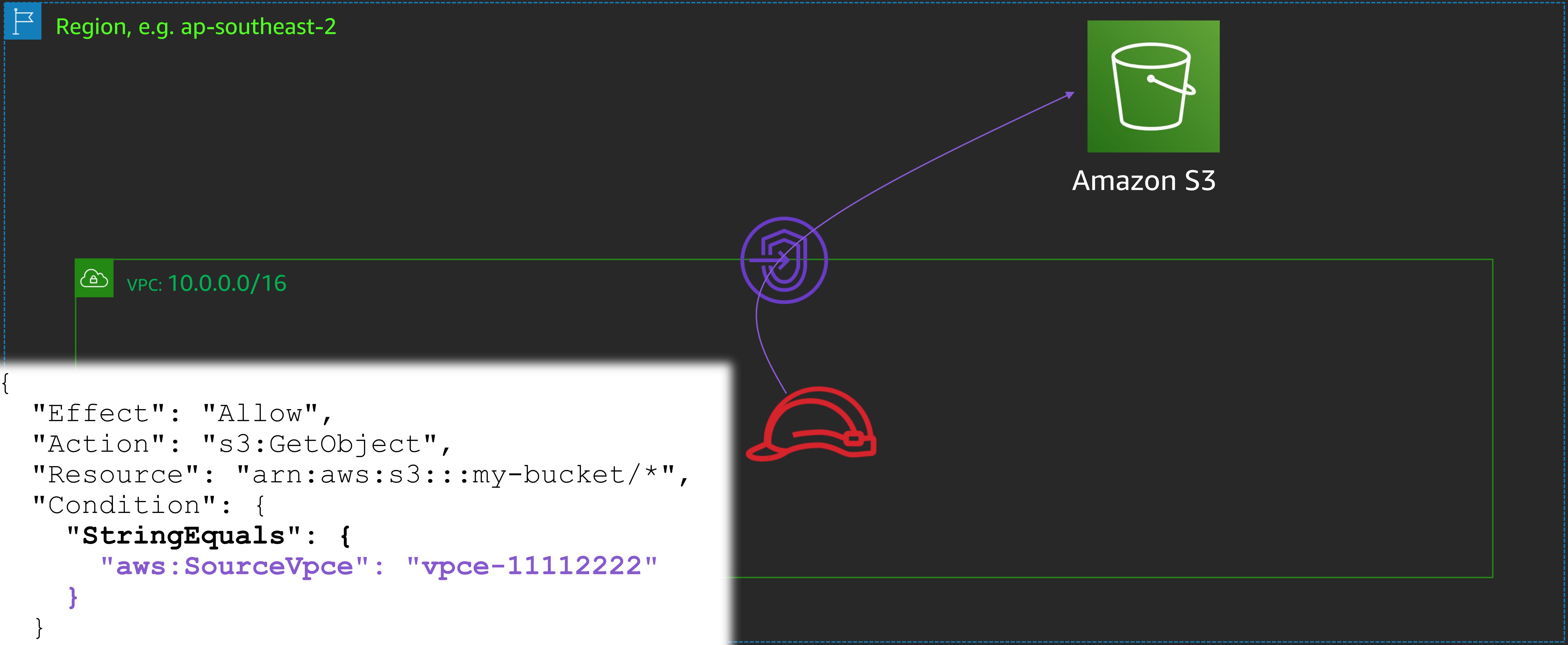
# VPC endpoints: Network as security perimeter



```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "logs:*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalOrgID": "o-a1b2c3"
    }
  }
}
```

**In English**: From this network, allow only callers from my AWS Organization

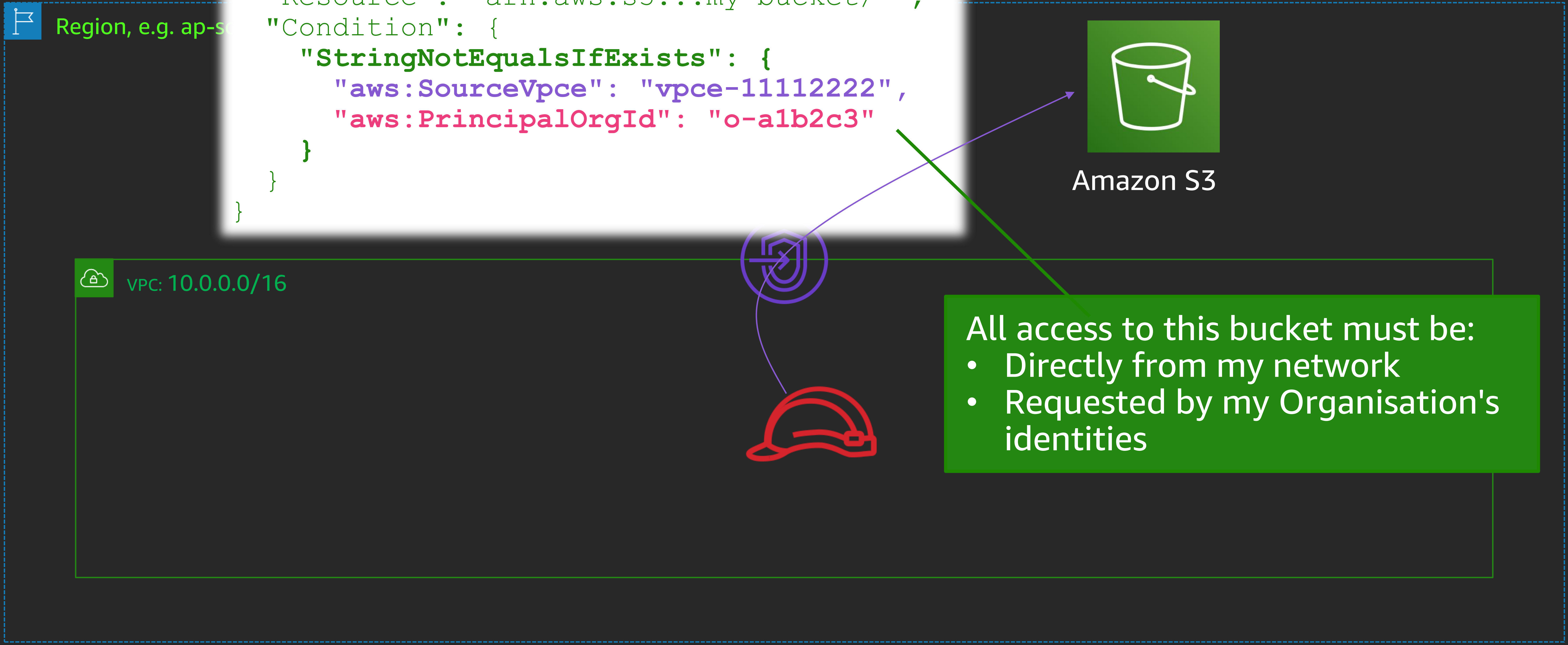
# VPC endpoints: Authorisation using network path



```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*",
  "Condition": {
    "StringEquals": {
      "aws:SourceVpce": "vpce-11112222"
    }
  }
}
```

# VPC en ng network path

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:SourceVpce": "vpce-11112222",
      "aws:PrincipalOrgId": "o-a1b2c3"
    }
  }
}
```

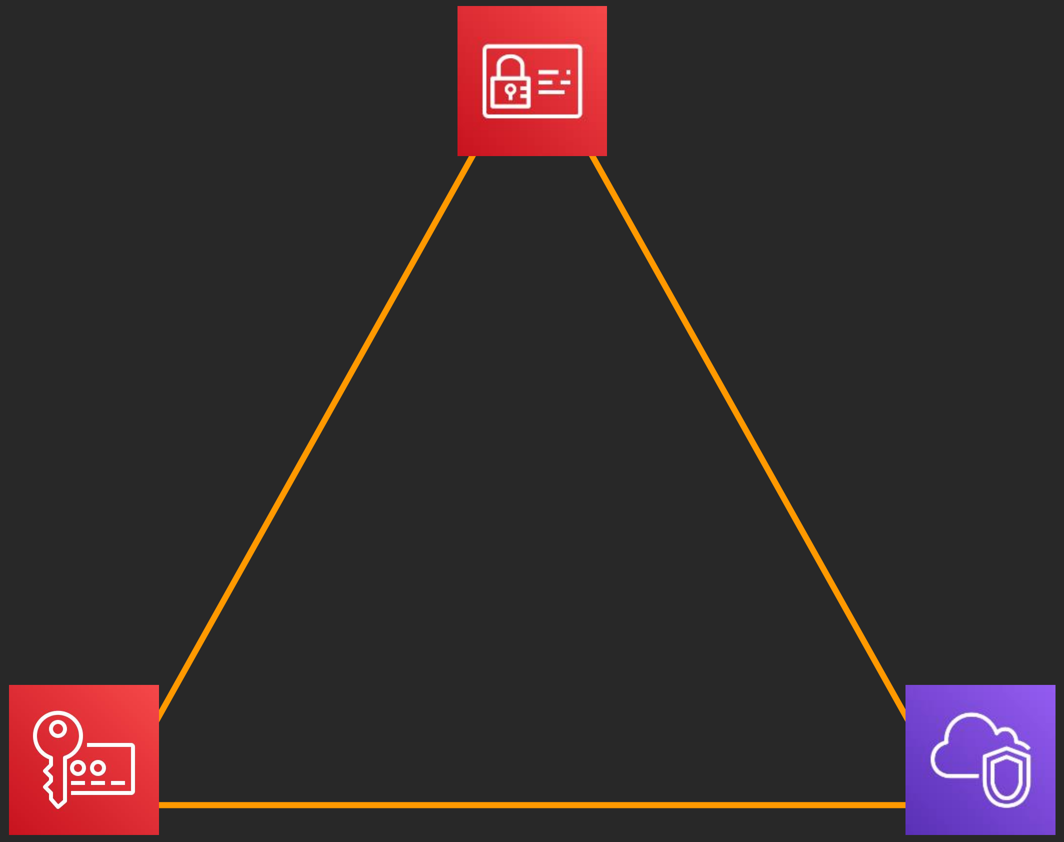


All access to this bucket must be:
- Directly from my network
- Requested by my Organisation's identities

# Wrapping up

# Learn a few patterns, secure everything in AWS

**Permissions management**
AWS IAM



**Data encryption**
AWS KMS

**Network security controls**
Amazon VPC

EKS
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository

**Storage**
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

**Database**
RDS
DynamoDB
ElastiCache
Neptune
Amazon Redshift
Amazon DocumentDB

**Migration & Transfer**
AWS Migration Hub
Application Discovery Service
Database Migration Service
Server Migration Service
AWS Transfer for SFTP
Snowball
DataSync

**Networking & Content Delivery**
VPC
CloudFront
Route 53
API Gateway
Direct Connect
AWS App Mesh
AWS Cloud Map
Global Accelerator

**Developer Tools**
CodeStar
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
Cloud9
X-Ray

**Robotics**
AWS RoboMaker

**Blockchain**
Amazon Managed Blockchain

**Satellite**
Ground Station

**Management & Governance**
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Managed Services
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard

**Media Services**
Elastic Transcoder
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage
MediaStore
MediaTailor

**Machine Learning**
Amazon SageMaker
Amazon Comprehend
AWS DeepLens
Amazon Lex
Machine Learning
Amazon Polly
Rekognition
Amazon Transcribe
Amazon Translate
Amazon Personalize
Amazon Forecast
Amazon Textract

**Analytics**
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Glue
MSK

**Security, Identity, & Compliance**
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
Artifact
Security Hub

**AWS Cost Management**
AWS Cost Explorer
AWS Budgets
AWS Marketplace Subscriptions

**Mobile**
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

**AR & VR**
Amazon Sumerian

**Application Integration**
Step Functions
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

**Customer Engagement**
Amazon Connect
Pinpoint
Simple Email Service

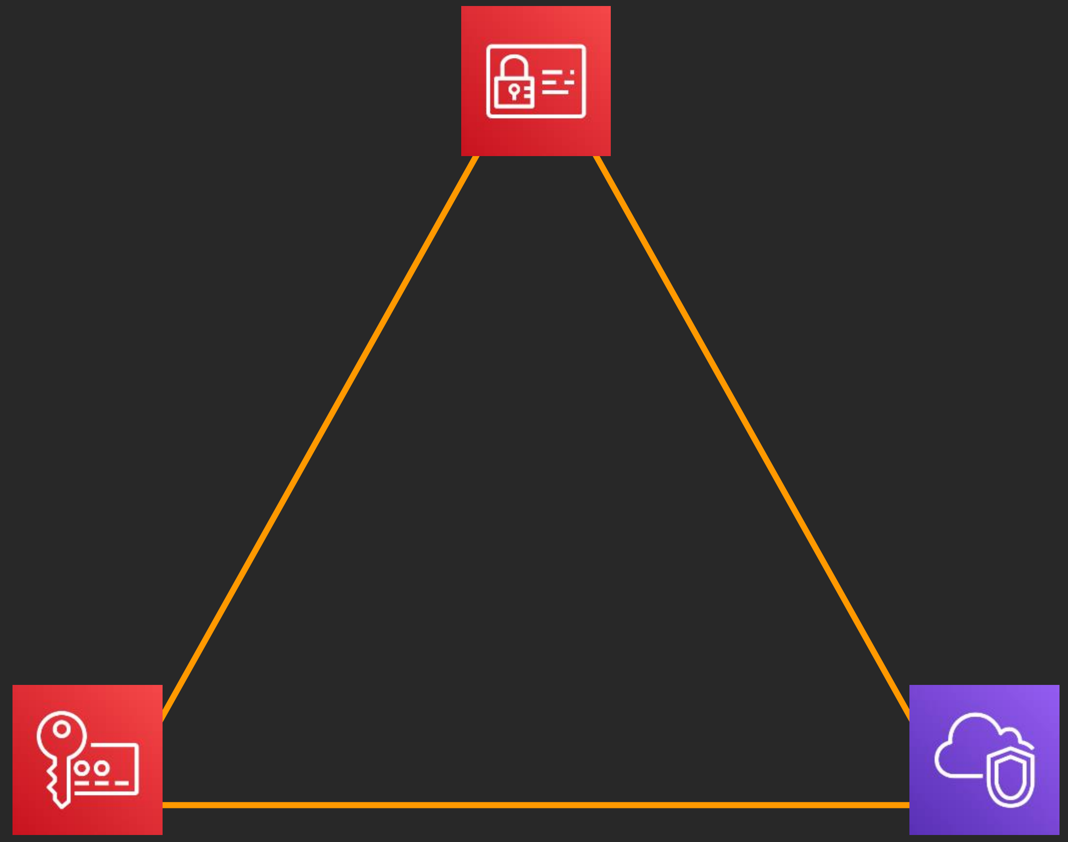
**Business Applications**
Alexa for Business
Amazon Chime
WorkMail

**End User Computing**
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink

**Internet of Things**
IoT Core
Amazon FreeRTOS
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise
IoT Things Graph

**Game Development**
Amazon GameLift

# Learn a few patterns, secure everything in AWS



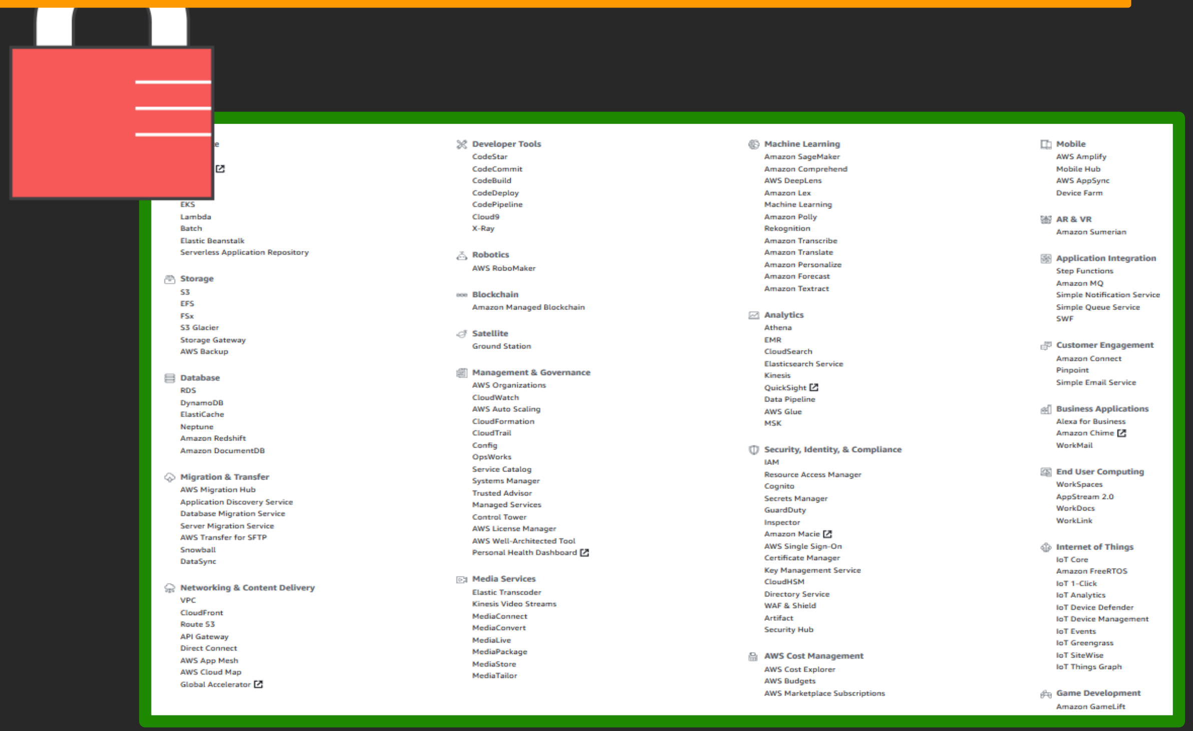
**Permissions management**
AWS IAM

**Data encryption**
AWS KMS

**Network security controls**
Amazon VPC

We learned:

- Identities that can make AWS calls
- How to read and write IAM policy



EKS
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository

Storage
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

Database
RDS
DynamoDB
ElastiCache
Neptune
Amazon Redshift
Amazon DocumentDB

Migration & Transfer
AWS Migration Hub
Application Discovery Service
Database Migration Service
Server Migration Service
AWS Transfer for SFTP
Snowball
DataSync

Networking & Content Delivery
VPC
CloudFront
Route 53
API Gateway
Direct Connect
AWS App Mesh
AWS Cloud Map
Global Accelerator

Developer Tools
CodeStar
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
Cloud9
X-Ray

Robotics
AWS RoboMaker

Blockchain
Amazon Managed Blockchain

Satellite
Ground Station

Management & Governance
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Managed Services
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard

Media Services
Elastic Transcoder
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage
MediaStore
MediaTailor

Machine Learning
Amazon SageMaker
Amazon Comprehend
AWS DeepLens
Amazon Lex
Machine Learning
Amazon Polly
Rekognition
Amazon Transcribe
Amazon Translate
Amazon Personalize
Amazon Forecast
Amazon Textract

Analytics
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Glue
MSK

Security, Identity, & Compliance
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
Artifact
Security Hub

AWS Cost Management
AWS Cost Explorer
AWS Budgets
AWS Marketplace Subscriptions

Mobile
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

AR & VR
Amazon Sumerian

Application Integration
Step Functions
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

Customer Engagement
Amazon Connect
Pinpoint
Simple Email Service

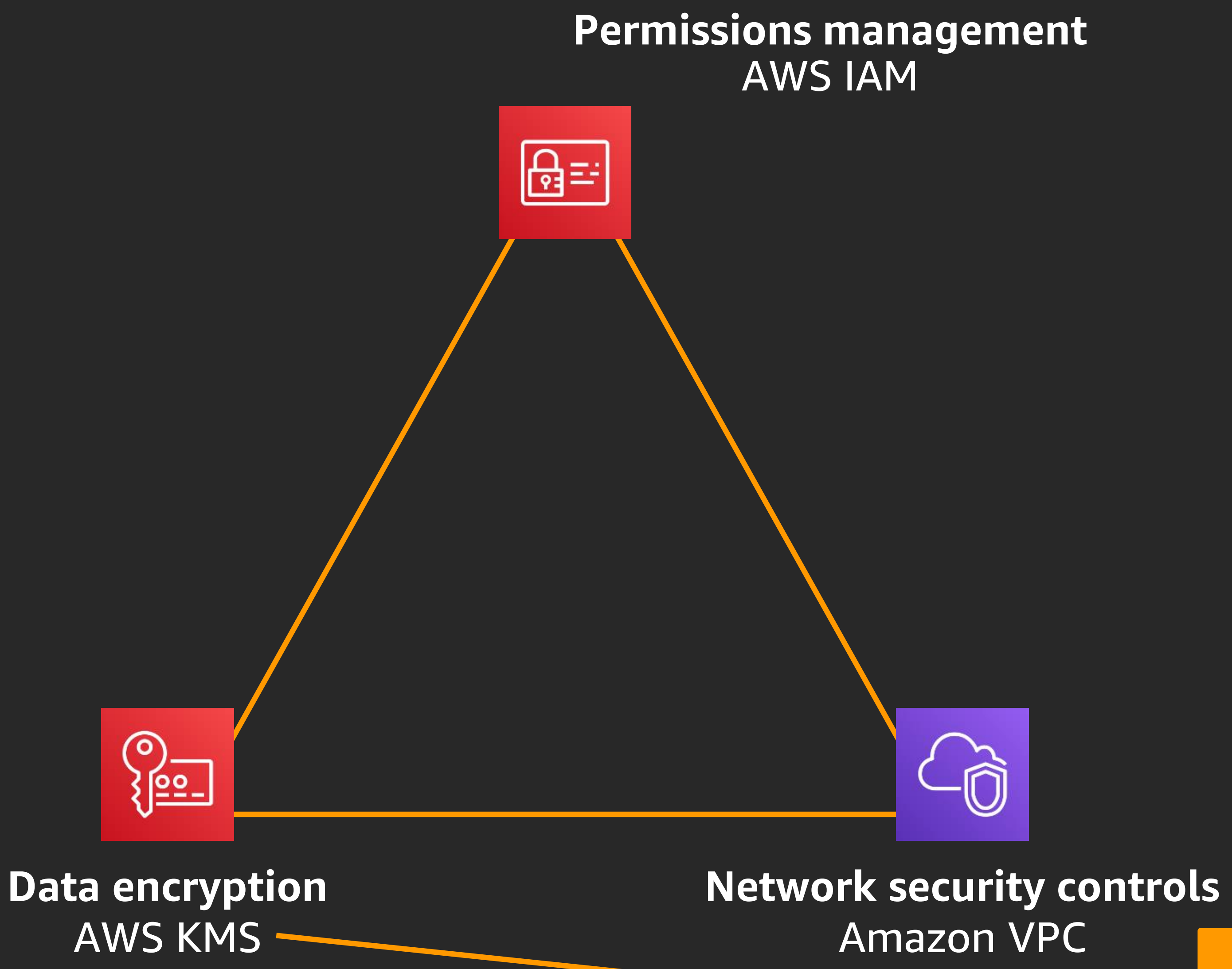
Business Applications
Alexa for Business
Amazon Chime
WorkMail

End User Computing
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink

Internet of Things
IoT Core
Amazon FreeRTOS
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise
IoT Things Graph

Game Development
Amazon GameLift

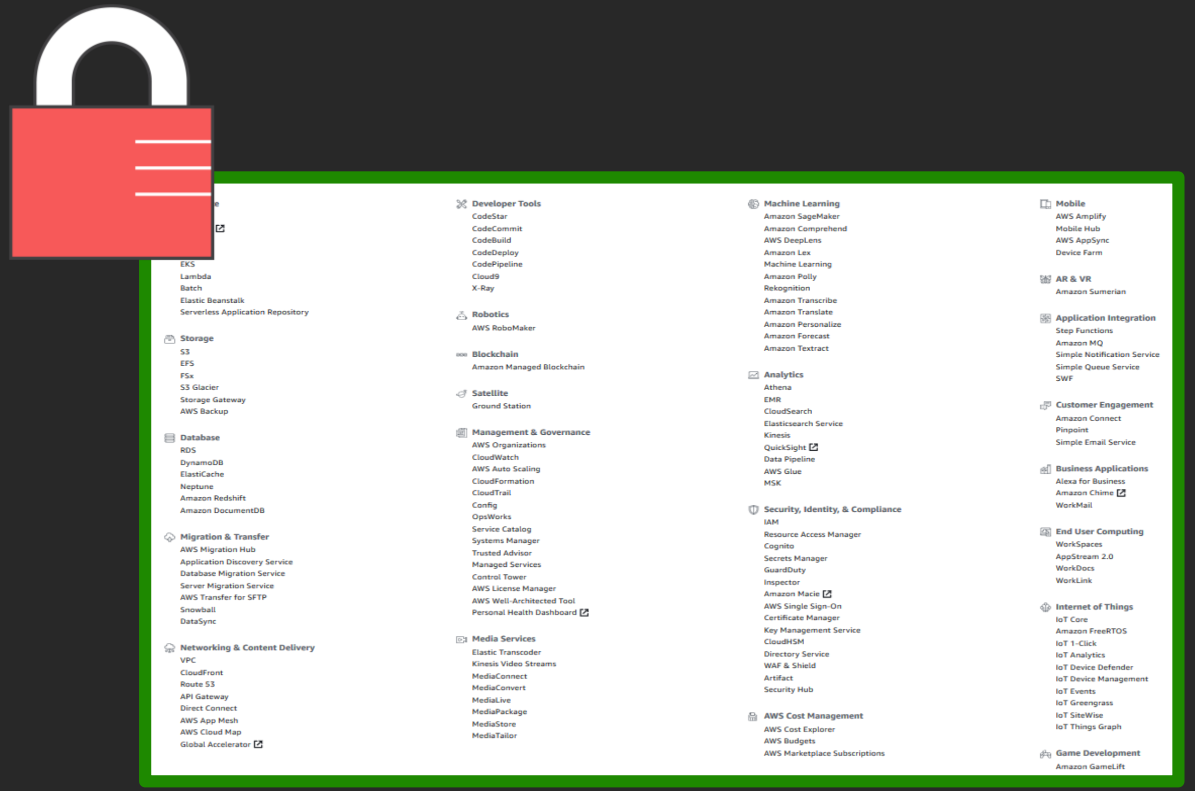
# Learn a few patterns, secure everything in AWS



**Permissions management**
AWS IAM

**Data encryption**
AWS KMS

**Network security controls**
Amazon VPC



e

EKS
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository

**Storage**
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

**Database**
RDS
DynamoDB
ElastiCache
Neptune
Amazon Redshift
Amazon DocumentDB

**Migration & Transfer**
AWS Migration Hub
Application Discovery Service
Database Migration Service
Server Migration Service
AWS Transfer for SFTP
Snowball
DataSync

**Networking & Content Delivery**
VPC
CloudFront
Route 53
API Gateway
Direct Connect
AWS App Mesh
AWS Cloud Map
Global Accelerator

**Developer Tools**
CodeStar
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
Cloud9
X-Ray

**Robotics**
AWS RoboMaker

**Blockchain**
Amazon Managed Blockchain

**Satellite**
Ground Station

**Management & Governance**
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Managed Services
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard

**Media Services**
Elastic Transcoder
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage
MediaStore
MediaTailor

**Machine Learning**
Amazon SageMaker
Amazon Comprehend
AWS DeepLens
Amazon Lex
Machine Learning
Amazon Polly
Rekognition
Amazon Transcribe
Amazon Translate
Amazon Personalize
Amazon Forecast
Amazon Textract

**Analytics**
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Glue
MSK

**Security, Identity, & Compliance**
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
Artifact
Security Hub

**AWS Cost Management**
AWS Cost Explorer
AWS Budgets
AWS Marketplace Subscriptions

**Mobile**
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

**AR & VR**
Amazon Sumerian

**Application Integration**
Step Functions
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

**Customer Engagement**
Amazon Connect
Pinpoint
Simple Email Service

**Business Applications**
Alexa for Business
Amazon Chime
WorkMail

**End User Computing**
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink

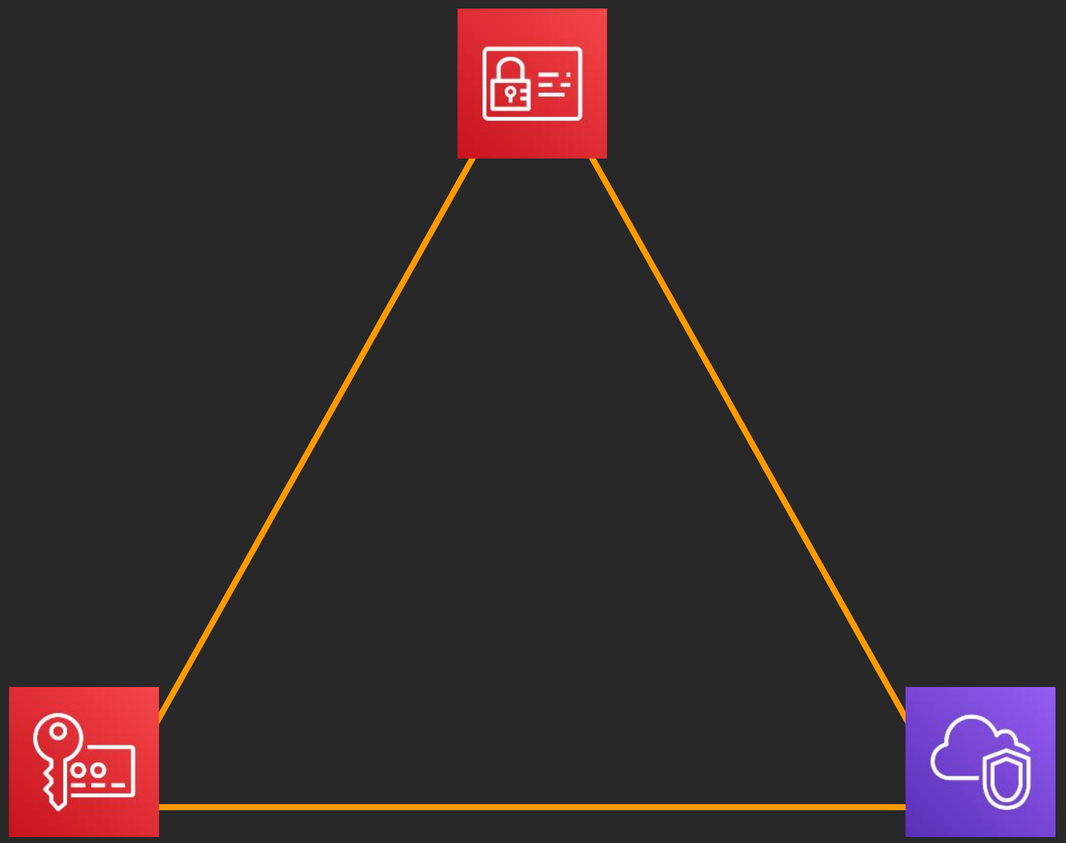
**Internet of Things**
IoT Core
Amazon FreeRTOS
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise
IoT Things Graph

**Game Development**
Amazon GameLift

We learned:

- How AWS KMS integrates with AWS services
- How to authorise access to AWS KMS keys

# Learn a few patterns, secure everything in AWS



**Permissions management**
AWS IAM

**Data encryption**
AWS KMS

**Network security controls**
Amazon VPC

e

EKS
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository

**Storage**
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

**Database**
RDS
DynamoDB
ElastiCache
Neptune
Amazon Redshift
Amazon DocumentDB

**Migration & Transfer**
AWS Migration Hub
Application Discovery Service
Database Migration Service
Server Migration Service
AWS Transfer for SFTP
Snowball
DataSync

**Networking & Content Delivery**
VPC
CloudFront
Route 53
API Gateway
Direct Connect
AWS App Mesh
AWS Cloud Map
Global Accelerator

**Developer Tools**
CodeStar
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
Cloud9
X-Ray

**Robotics**
AWS RoboMaker

**Blockchain**
Amazon Managed Blockchain

**Satellite**
Ground Station

**Management & Governance**
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Managed Services
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard

**Media Services**
Elastic Transcoder
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage
MediaStore
MediaTailor

**Machine Learning**
Amazon SageMaker
Amazon Comprehend
AWS DeepLens
Amazon Lex
Machine Learning
Amazon Polly
Rekognition
Amazon Transcribe
Amazon Translate
Amazon Personalize
Amazon Forecast
Amazon Textract

**Analytics**
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Glue
MSK

**Security, Identity, & Compliance**
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
Artifact
Security Hub

**AWS Cost Management**
AWS Cost Explorer
AWS Budgets
AWS Marketplace Subscriptions

**Mobile**
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

**AR & VR**
Amazon Sumerian

**Application Integration**
Step Functions
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

**Customer Engagement**
Amazon Connect
Pinpoint
Simple Email Service

**Business Applications**
Alexa for Business
Amazon Chime
WorkMail

**End User Computing**
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink

**Internet of Things**
IoT Core
Amazon FreeRTOS
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise
IoT Things Graph

**Game Development**
Amazon GameLift

We learned:
How to get least-privilege connectivity
How to use your network as a security perimeter

# Thank you!

Pierre Liddle

liddlep@amazon.com
https://www.linkedin.com/in/pierreliddle/

aws SUMMIT ONLINE