Welcome to AWS Builders Online Series

Gabe Hollombe
Senior Developer Advocate,
Amazon Web Services
in 🐦 @gabehollombe

Why cloud infrastructure?

Increase agility

Gain scalability

Improve reliability

Lower costs

Maximum security

Security is "job zero"

Cloud security is a shared responsibility

Security of the cloud

Managed by AWS

Security in the cloud

Managed by you

Agenda

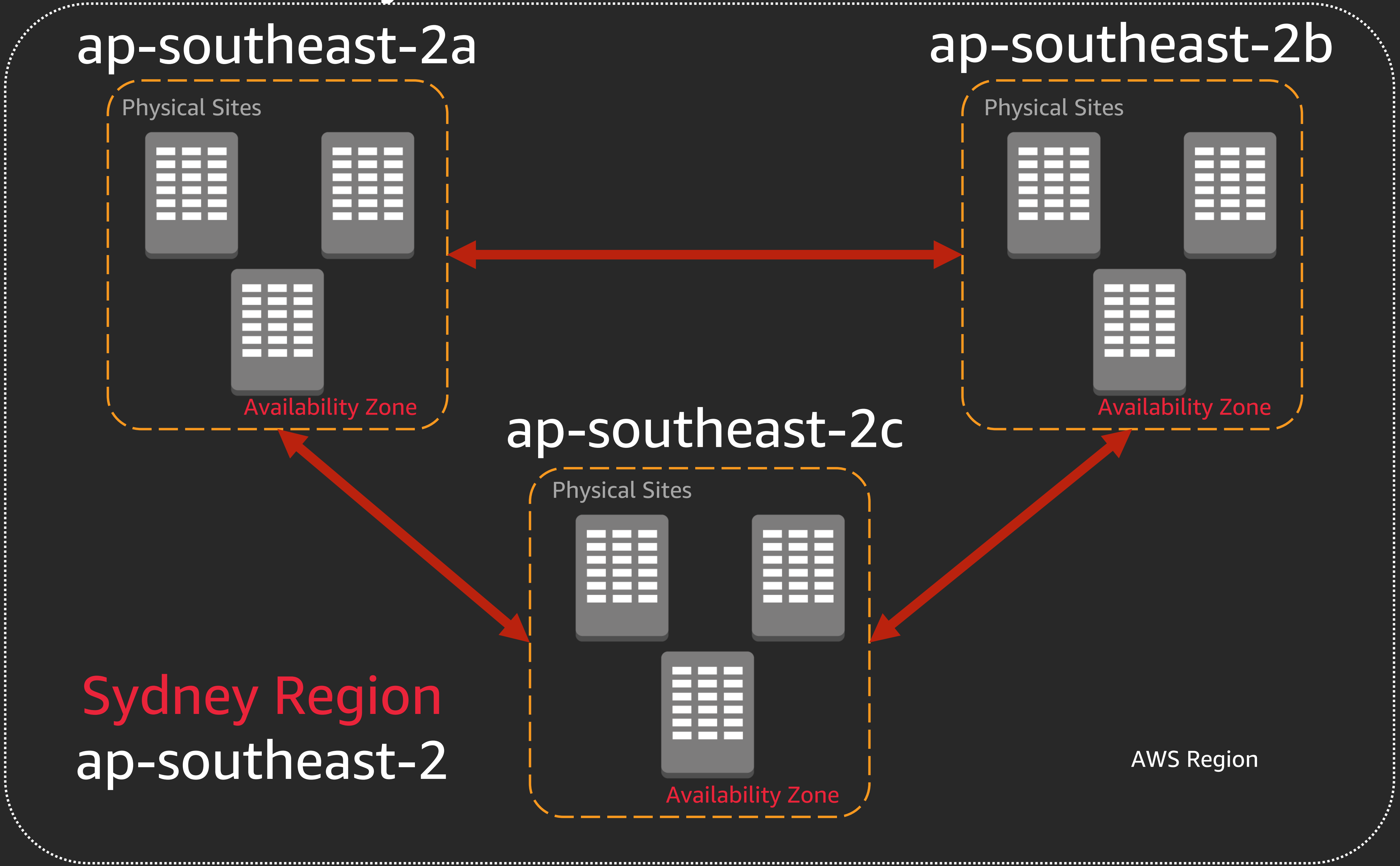
1. A builder-focused introduction to AWS's security controls
   - Understand what AWS takes care of and what you need to secure
   - Control your cloud infrastructure: AWS Identity and Access Management (IAM)
   - Control your data: AWS Key Management Service (KMS)
   - Control your network: Amazon Virtual Private Cloud (VPC)

2. An overview of what to expect from today's sessions

Security of the cloud

Managed by AWS

AWS Availability Zones



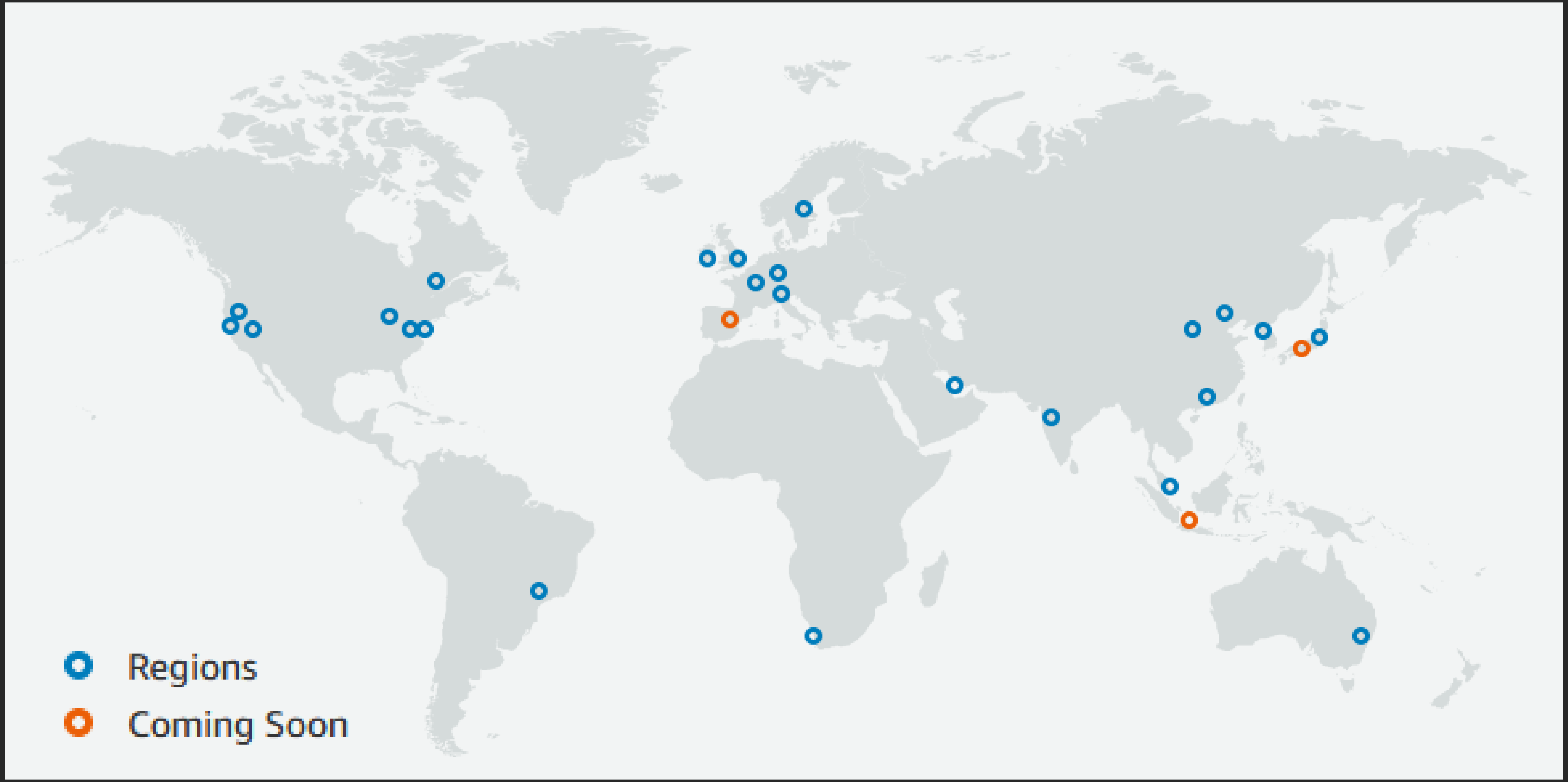
AWS global infrastructure

24 Regions

(+3 Announced Regions)

77 Availability Zones

216 Network Points of Presence



https://aws.amazon.com/about-aws/global-infrastructure/

AWS compliance programs

CSA
Cloud Security Alliance Controls

ISO 9001
Global Quality Standard

ISO 27001
Security Management Standard

ISO 27017
Cloud Specific Controls

ISO 27018
Personal Data Protection

PCI DSS Level 1
Payment Card Standards

CJIS
Criminal Justice Information Services

DoD SRG
DoD Data Processing

FedRAMP
Government Data Standards

FERPA
Educational Privacy Act

FIPS
Government Security Standards

FISMA
Federal Information Security Management

SOC 1
Audit Controls Report

SOC 2
Security, Availability, & Confidentiality Report

SOC 3
General Controls Report

FISC [Japan]
Financial Industry Information Systems

IRAP [Australia]
Australian Security Standards

MTCS Tier 3 [Singapore]
Multi-Tier Cloud Security Standard

GXP
Quality Guidelines and Regulations

HIPAA
Protected Health Information

SEC Rule 17a-4(f)
Financial Data Standards

ITAR
International Arms Regulations

MPAA
Protected Media Content

NIST
National Institute of Standards and Technology

Data Privacy

Australia Data Privacy

CISPE

EU Data Protection

EU-US Privacy Shield

Germany Privacy Considerations

India Privacy Considerations

Malaysia Privacy Considerations

New Zealand Privacy Considerations

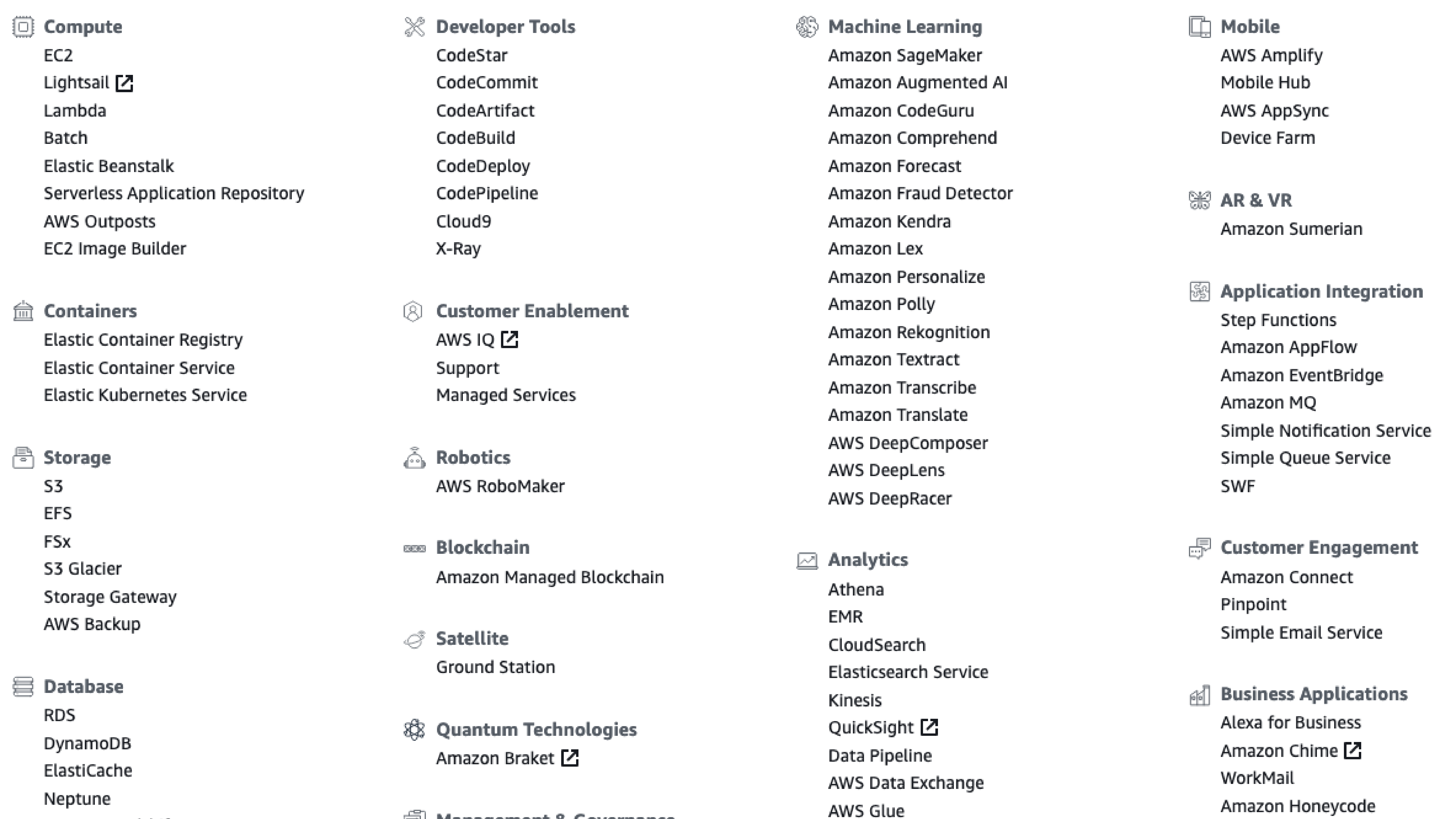
PIPEDA [Canada]

Singapore Privacy Considerations

Spanish DPA Authorization

Security in the cloud

Managed by you



Compute
EC2
Lightsail ↗
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository
AWS Outposts
EC2 Image Builder

Containers
Elastic Container Registry
Elastic Container Service
Elastic Kubernetes Service

Storage
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

Database
RDS
DynamoDB
ElastiCache
Neptune

Developer Tools
CodeStar
CodeCommit
CodeArtifact
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

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

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

Mobile
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

AR & VR
Amazon Sumerian

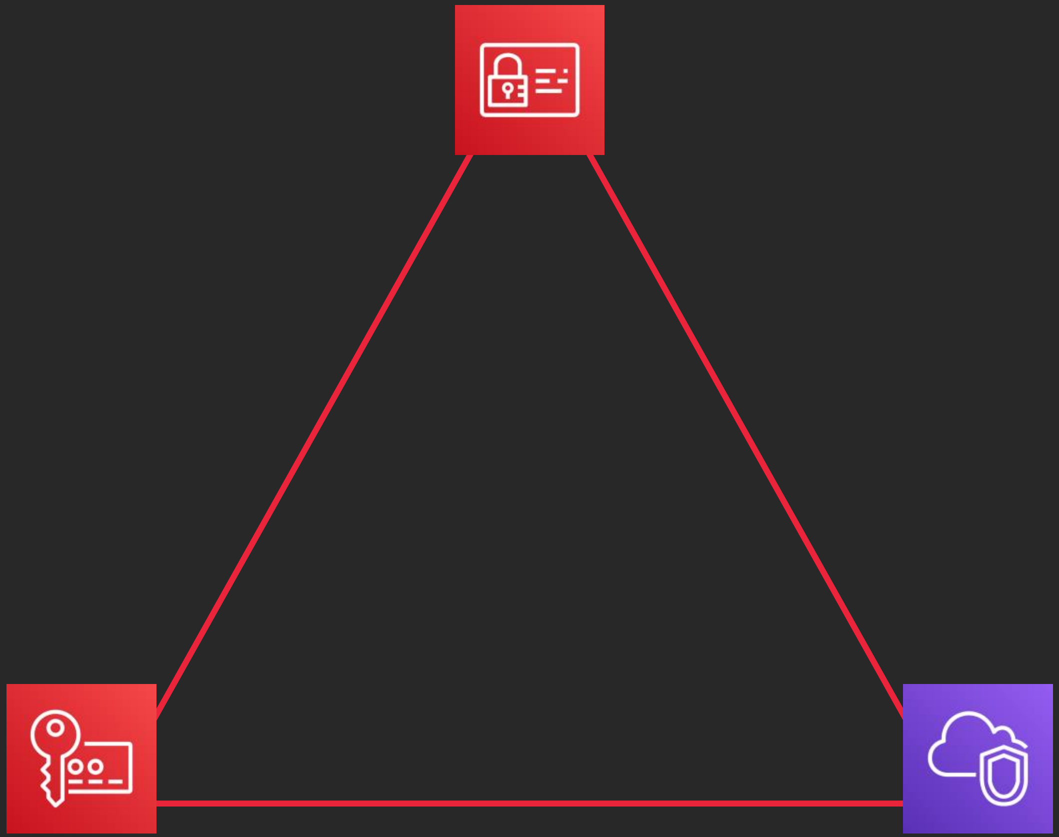
Application Integration
Step Functions
Amazon AppFlow
Amazon EventBridge
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

Customer Engagement
Amazon Connect
Pinpoint
Simple Email Service

Business Applications
Alexa for Business
Amazon Chime ↗
WorkMail
Amazon Honeycode

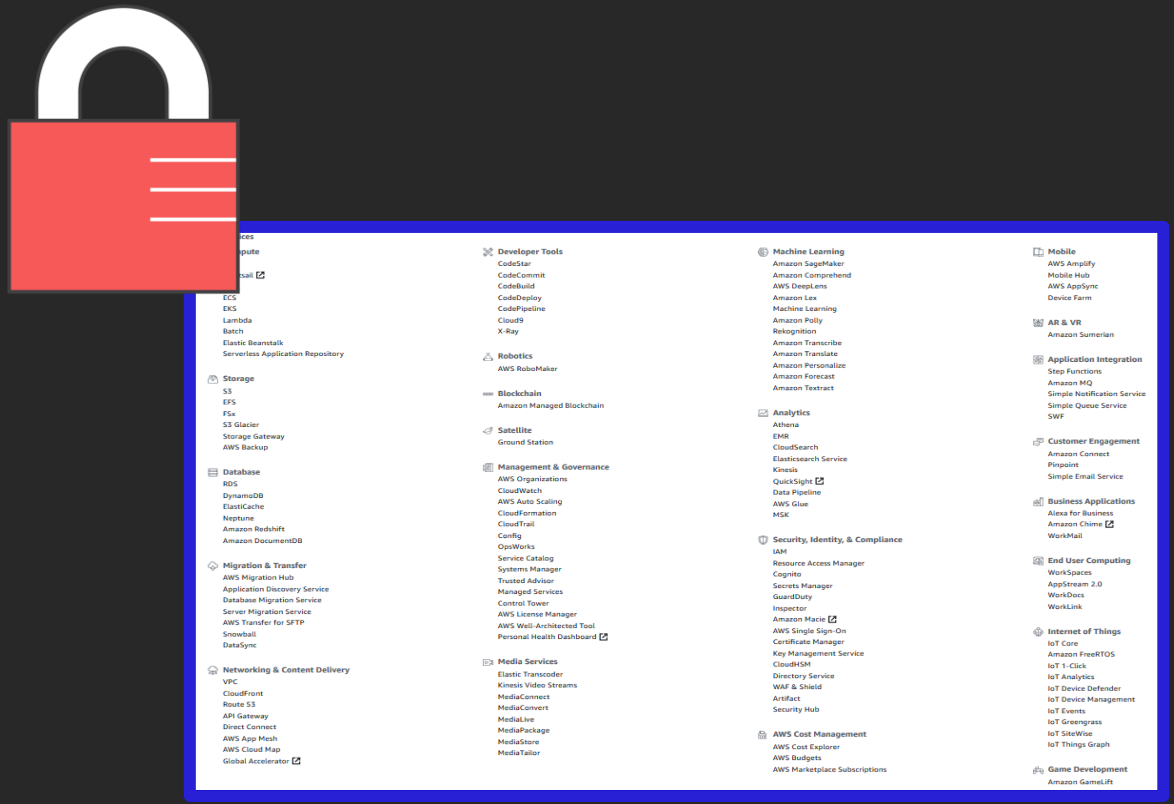
Learn a few patterns, secure everything in AWS

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)



ices

pute

tsail ↗
ECS
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

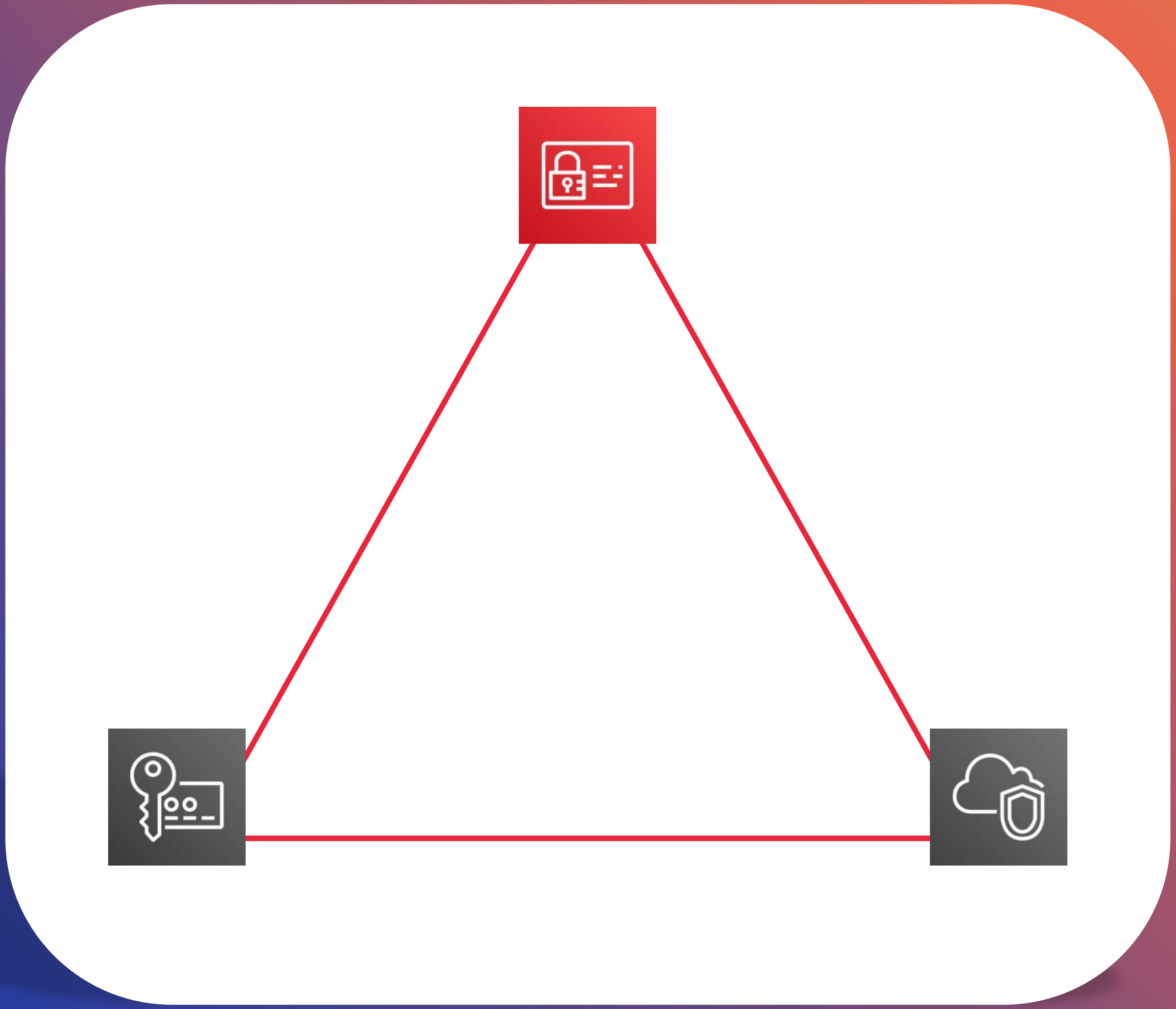
Business Applications
Alexa for Business
Amazon Chime ↗
WorkMail

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

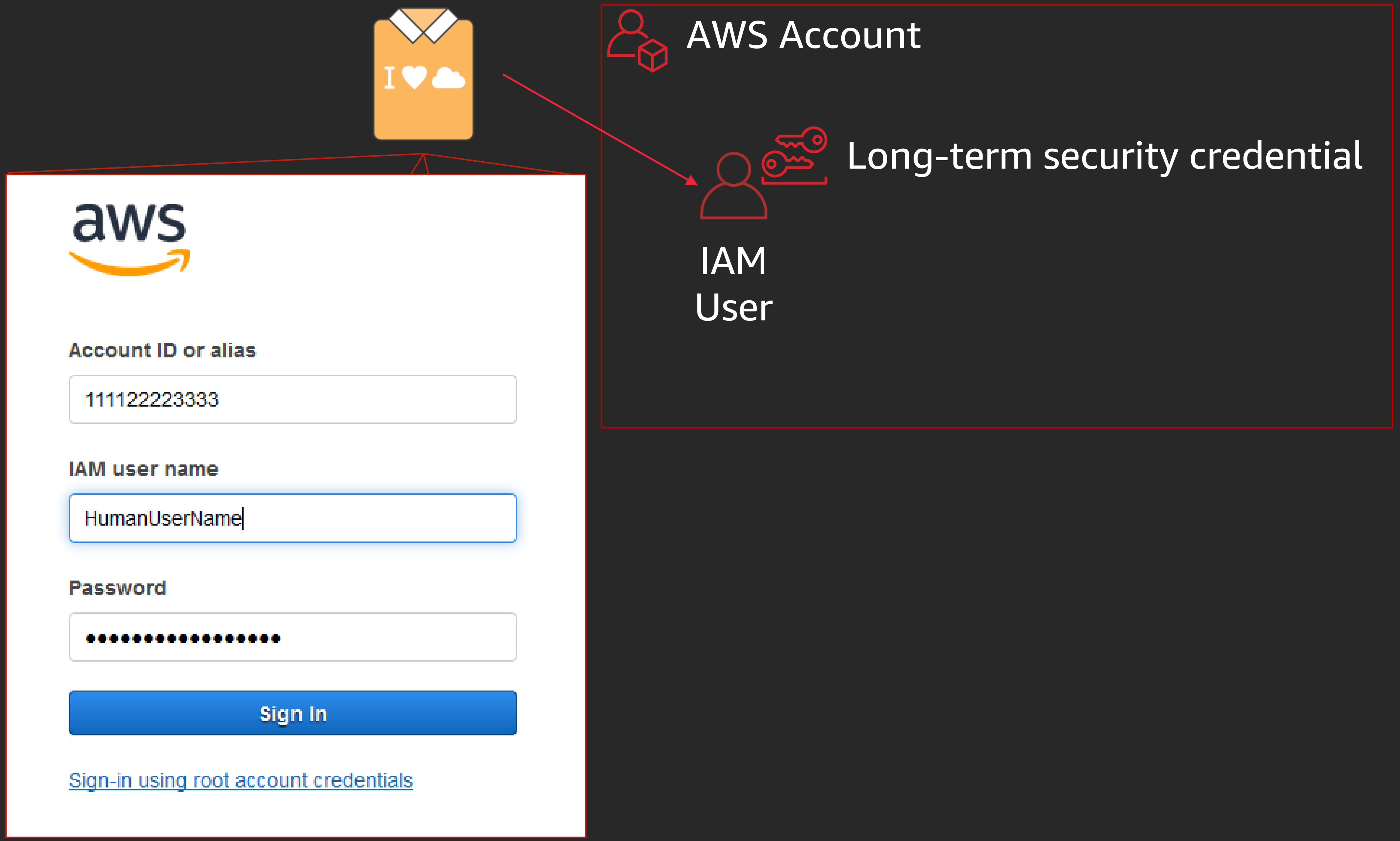
AWS Identity and Access Management (IAM)



AWS IAM

- **What it is:**
  - **'I'—Authentication.** Support for human and application caller identities
  - **'AM'—Authorization.** Powerful, flexible permissions language for controlling access to cloud resources
- **Why it matters to you:** Every AWS service uses IAM to authenticate and authorize 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 authorization control details

AWS identities for human callers: IAM users



I ♥ ☁
AWS Account
Long-term security credential
IAM User
aws

Account ID or alias

111122223333

IAM user name

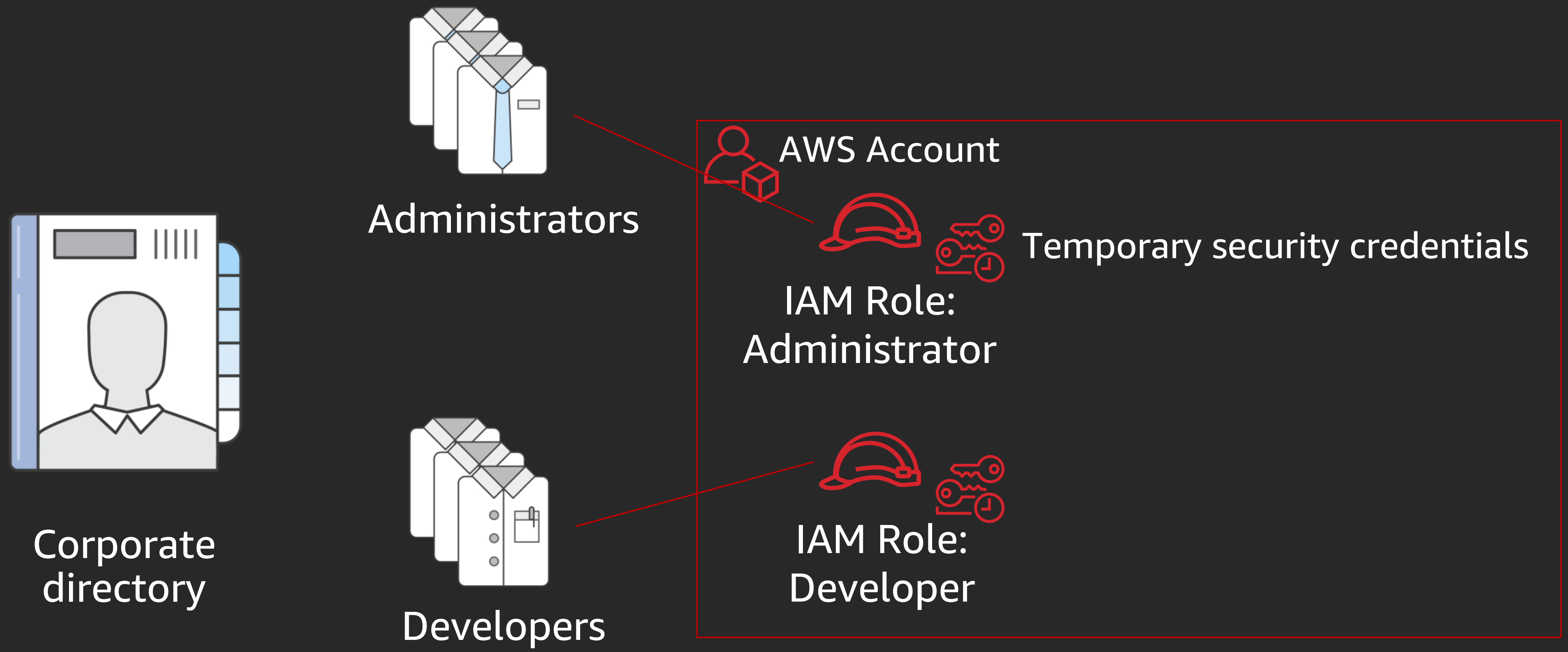
HumanUserName

Password

•••••••••••••••••

Sign In
Sign-in using root account credentials

AWS identities for human callers: Federated identities



AWS identities for non-human callers

EC2 Instance

Lambda Function

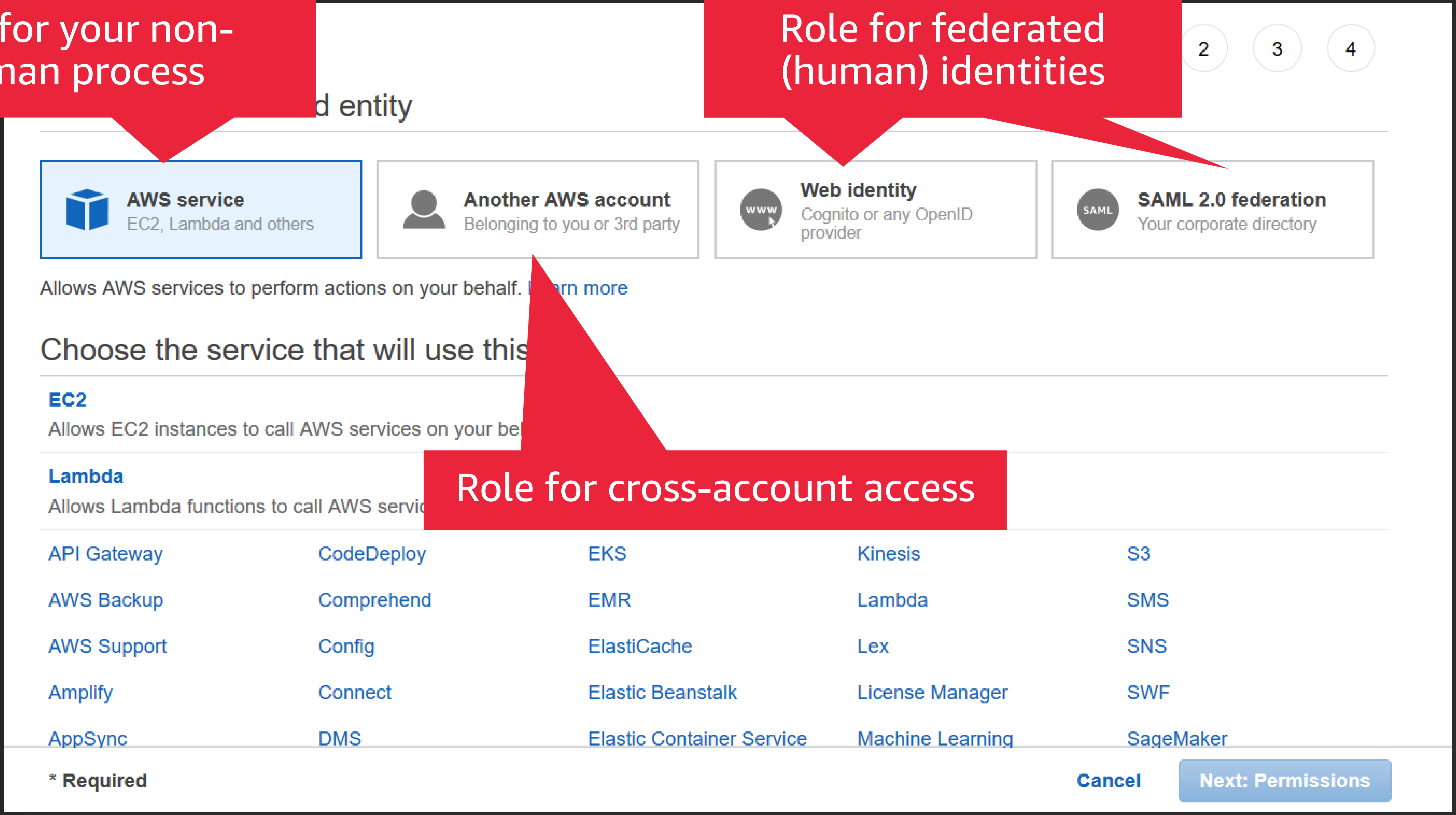
Amazon SageMaker Notebook

AWS Glue Crawler

Amazon ECS Task

… and many others

Creating a role in the AWS Management Console



2 3 4

d 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. L rn more

Choose the service that will use this

EC2
Allows EC2 instances to call AWS services on your be

Lambda
Allows Lambda functions to call AWS servic

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

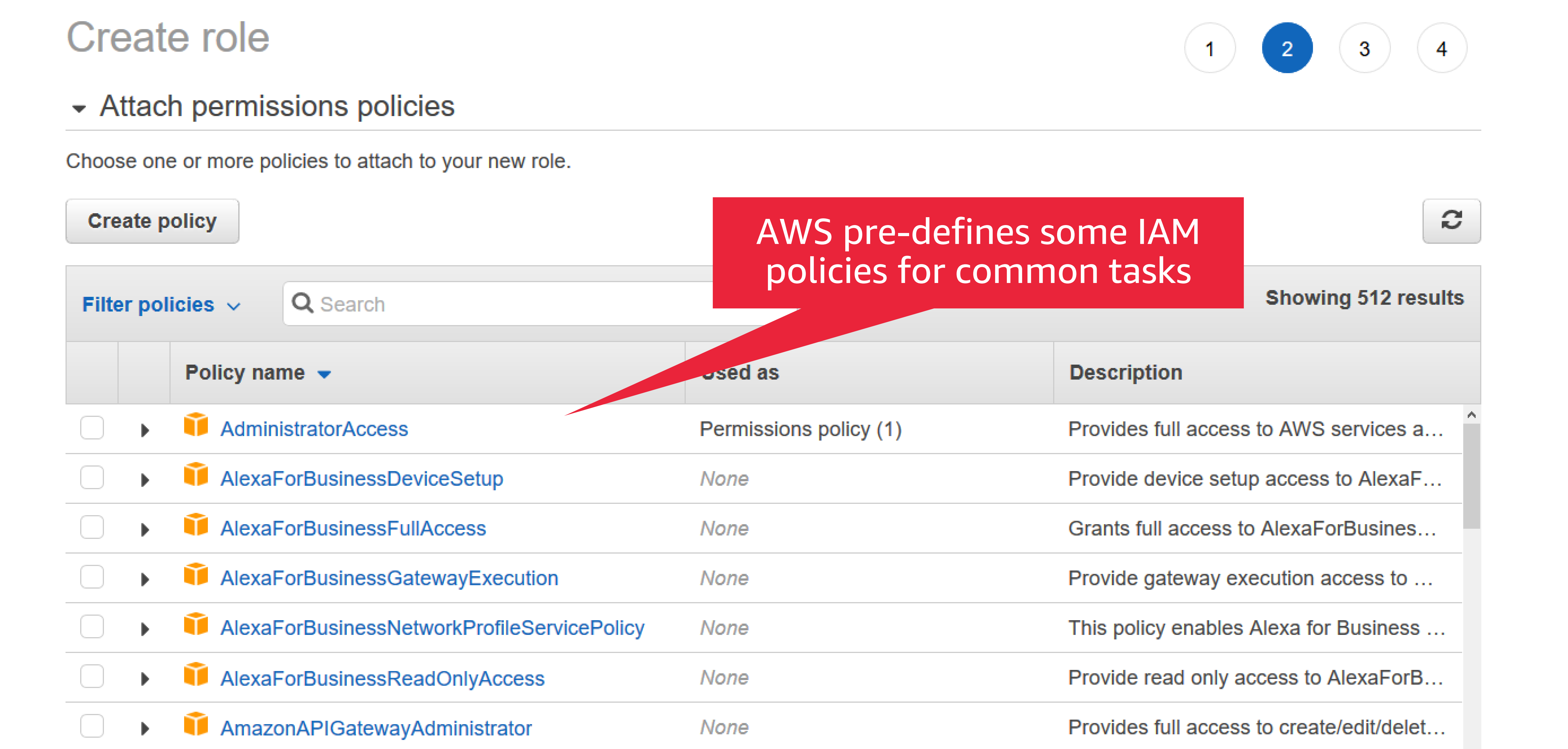
* **Required**

Role for your non-human process

Role for federated (human) identities

Role for cross-account access

AWS-managed policies for common sets of permissions



Create role

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:BatchGetItem",
        "dynamodb:GetItem",
        "dynamodb:Query"
      ],
      "Resource": "*"
    }
  ]
}
```

In English: Allowed to take only a few specific Amazon DynamoDB actions

Reading and writing IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:BatchGetItem",
        "dynamodb:GetItem",
        "dynamodb:Query",
      ],
      "Resource": [
        "arn:aws:dynamodb:us-east-2:111122223333:table/MyTableName",
        "arn:aws:dynamodb:us-east-2:111122223333:table/MyTableName/index/*"
      ]
    }
  ]
}
```

In English: Allowed to take specific Amazon DynamoDB actions on a specific table and its indexes

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

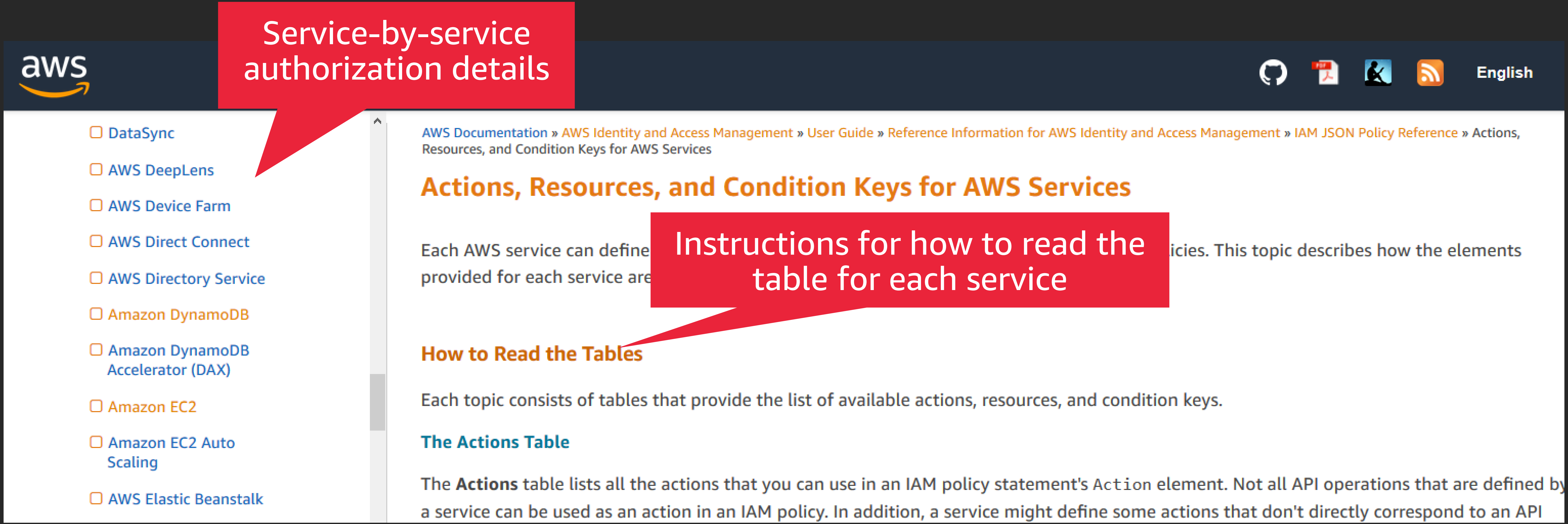
Reading and writing IAM policy

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "secretsmanager:ResourceTag/Project": "${aws:PrincipalTag/Project}"
    }
   }
  }
 ]
}
```

In English: You can read secrets whose project tag matches your own

Attribute-Based Access Control (ABAC)

How to write a least-privilege IAM policy



Service-by-service authorization 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 … icies. This topic describes how the elements provided for each service are

How to Read the Tables

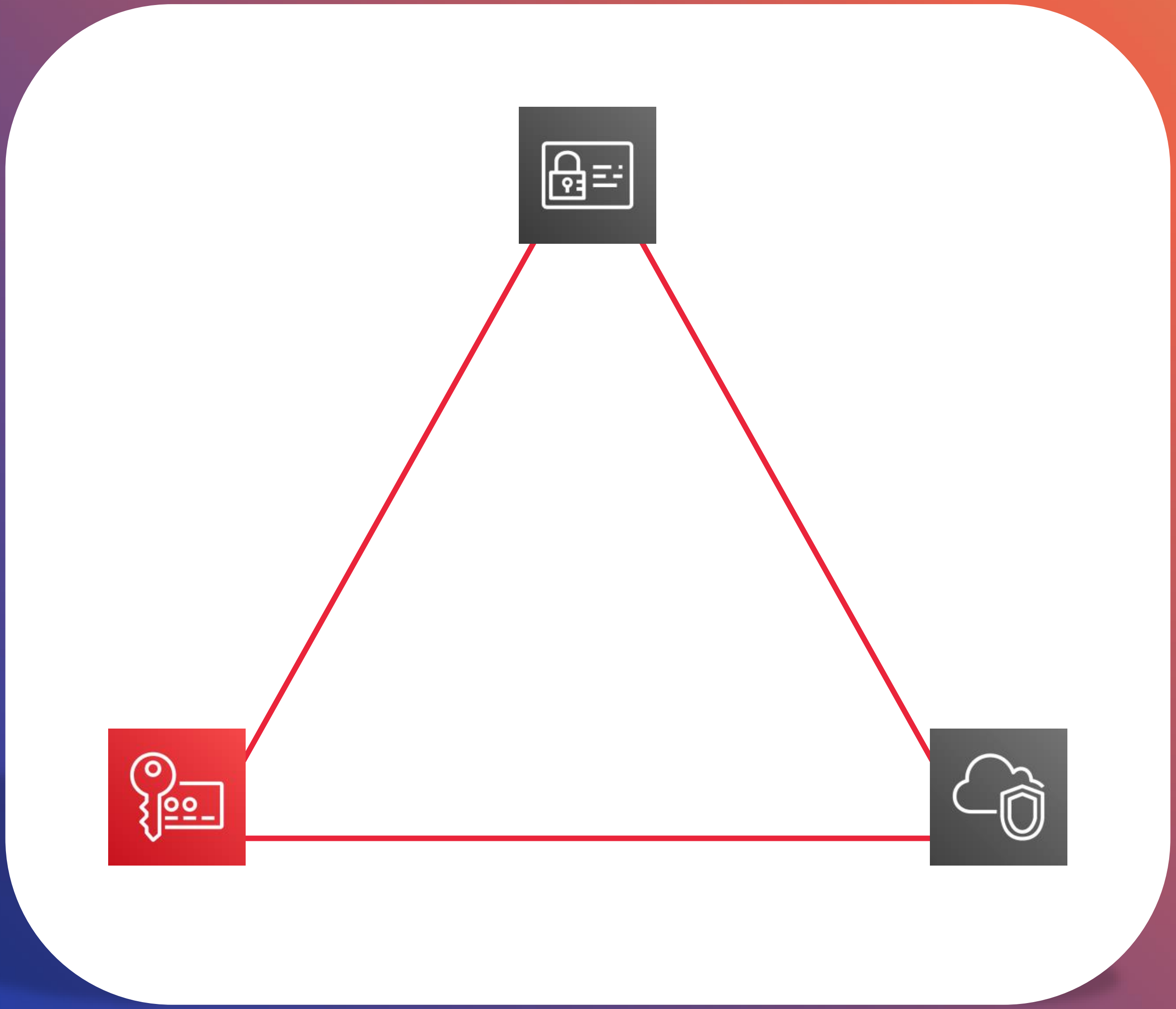
Each topic consists of tables that provide the list of available actions, resources, and condition keys.

The Actions Table

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

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_actions-resources-contextkeys.html

AWS Key Management Service (KMS)



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

It's OK if you don’t understand the next slide…

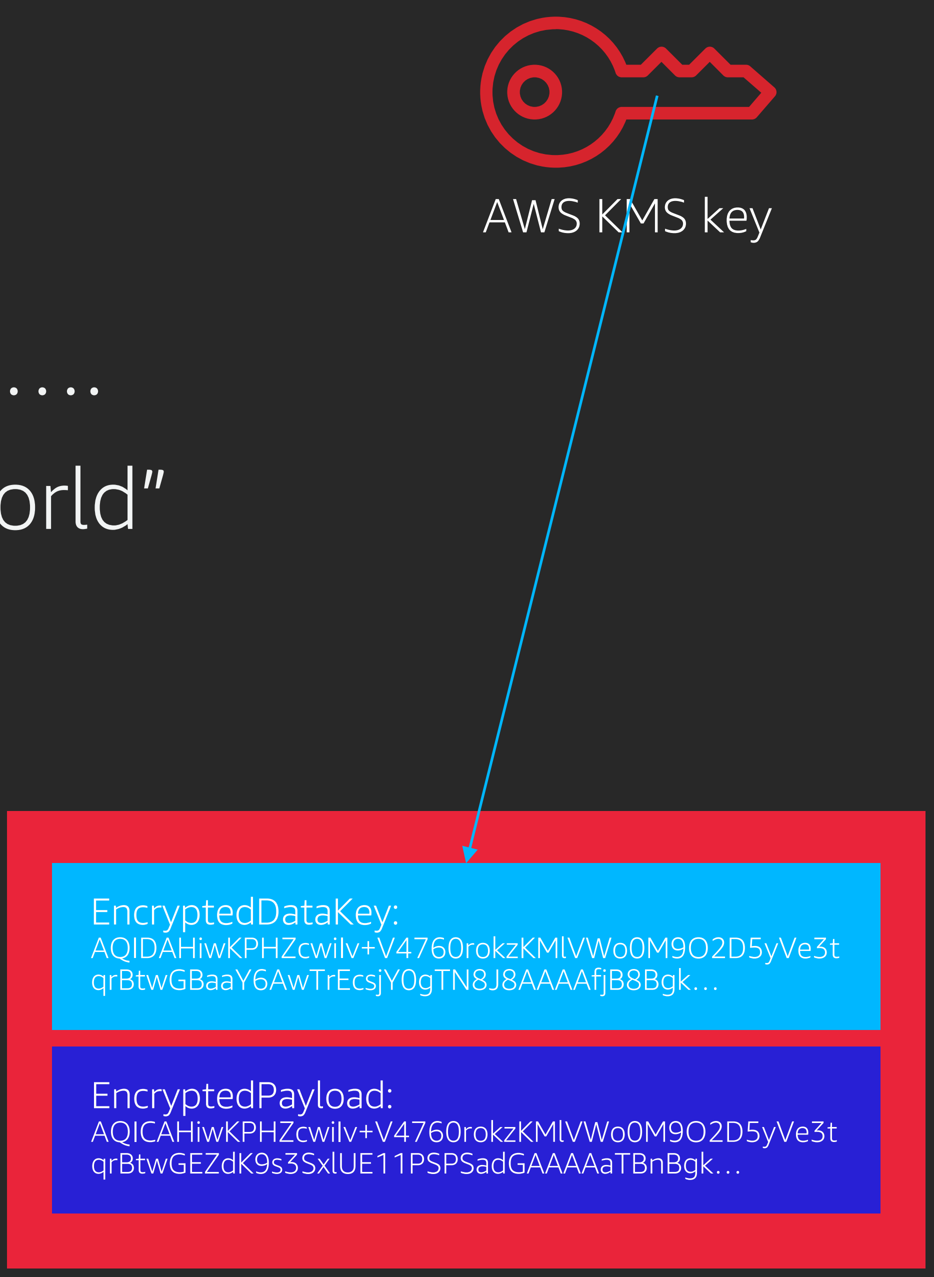
The mechanics of an AWS KMS key

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

- KMS.Encrypt("hello world") ➔ AQICAHiwKPHZcwilv….
- KMS.Decrypt("AQICAHiwKPHZcwilv….") ➔ "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



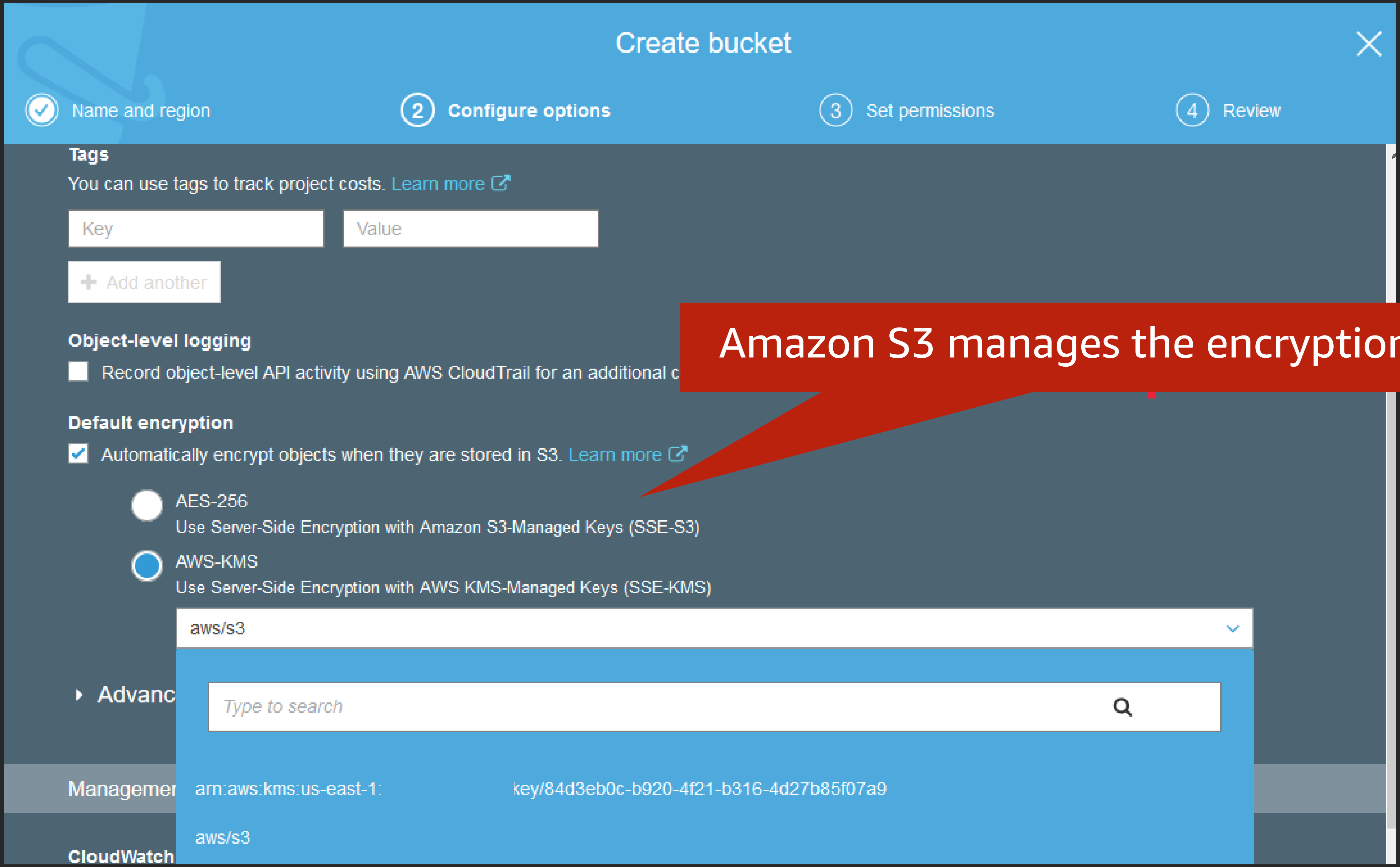
EncryptedDataKey:
AQIDAHiwKPHZcwilv+V4760rokzKMlVWo0M9O2D5yVe3t
qrBtwGBaaY6AwTrEcsjY0gTN8J8AAAAfjB8Bgk…

EncryptedPayload:
AQICAHiwKPHZcwilv+V4760rokzKMlVWo0M9O2D5yVe3t
qrBtwGEZdK9s3SxlUE11PSPSadGAAAAaTBnBgk…

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



Tags

You can use tags to track project costs. Learn more

Object-level logging

□ Record object-level API activity using AWS CloudTrail for an additional c

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)

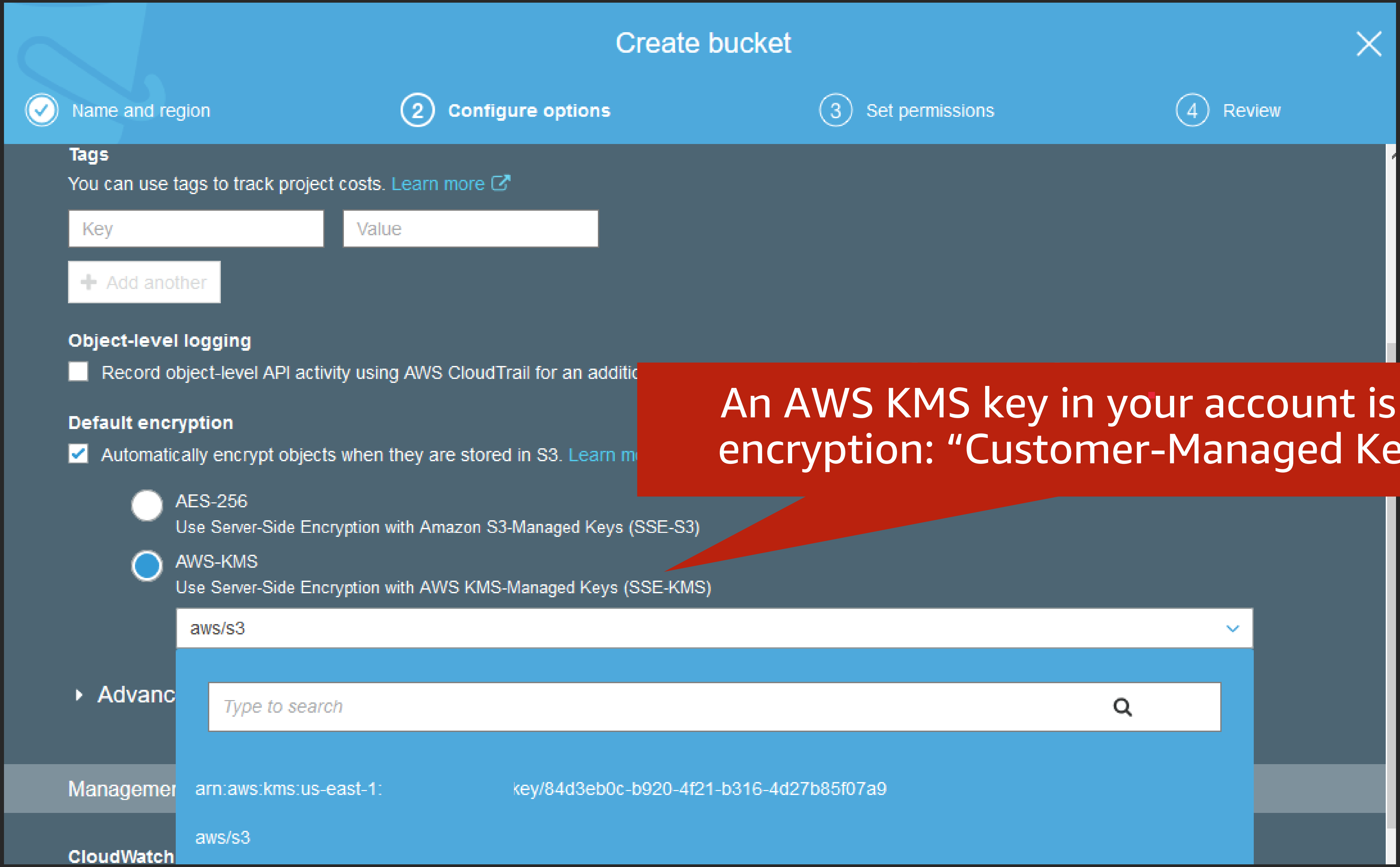
aws/s3

arn:aws:kms:us-east-1: 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 additic

Default encryption

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

○ 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

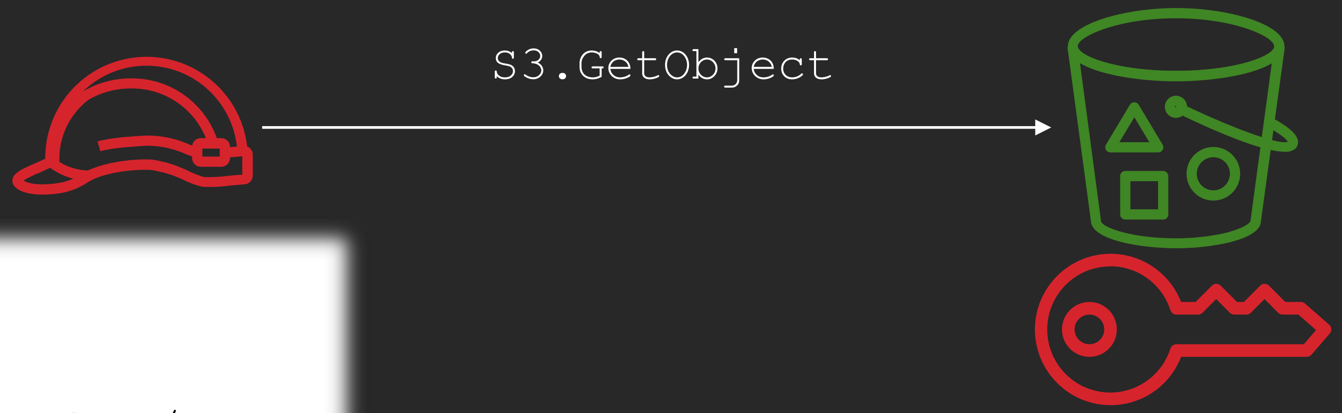
arn:aws:kms:us-east-1: key/84d3eb0c-b920-4f21-b316-4d27b85f07a9

aws/s3

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

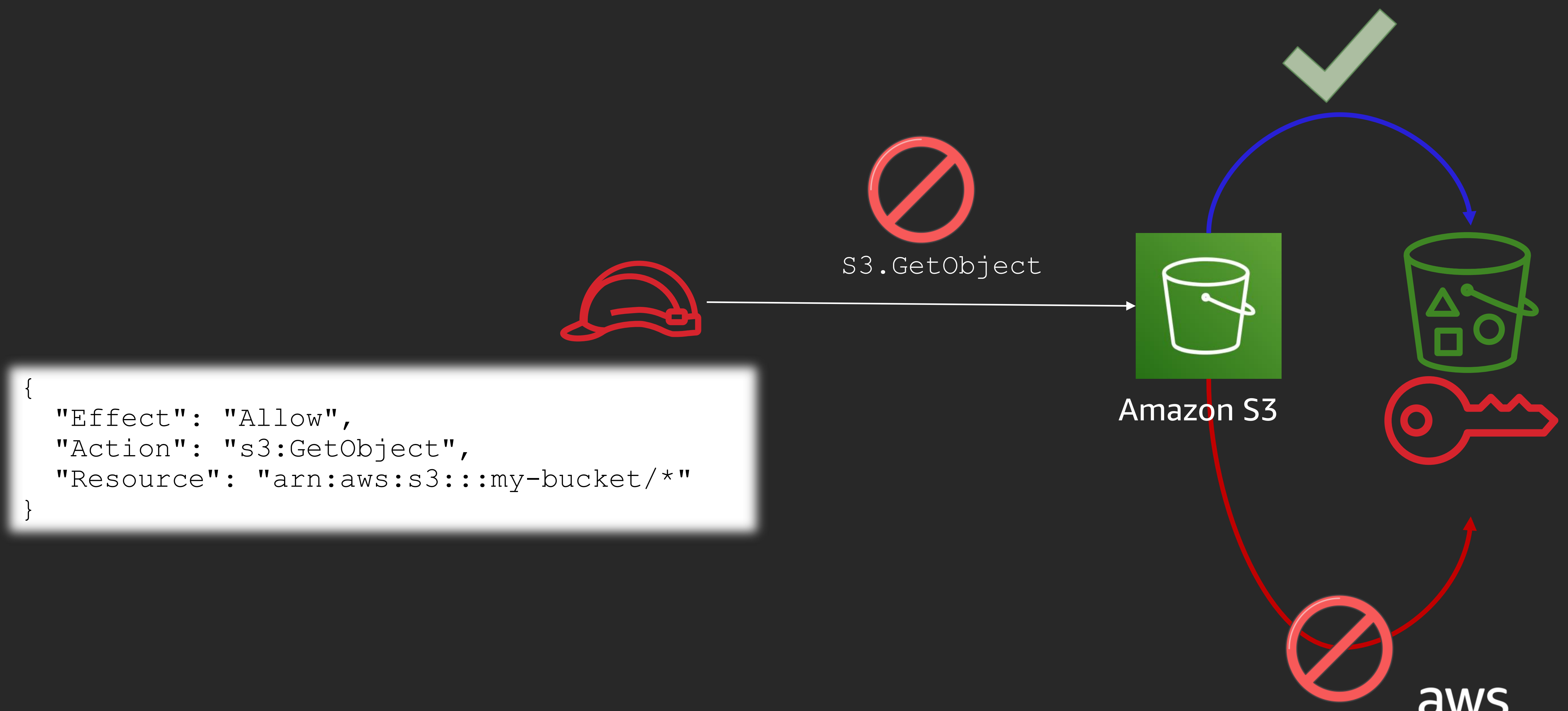
IAM permissions for AWS KMS keys

Question: What happens here?



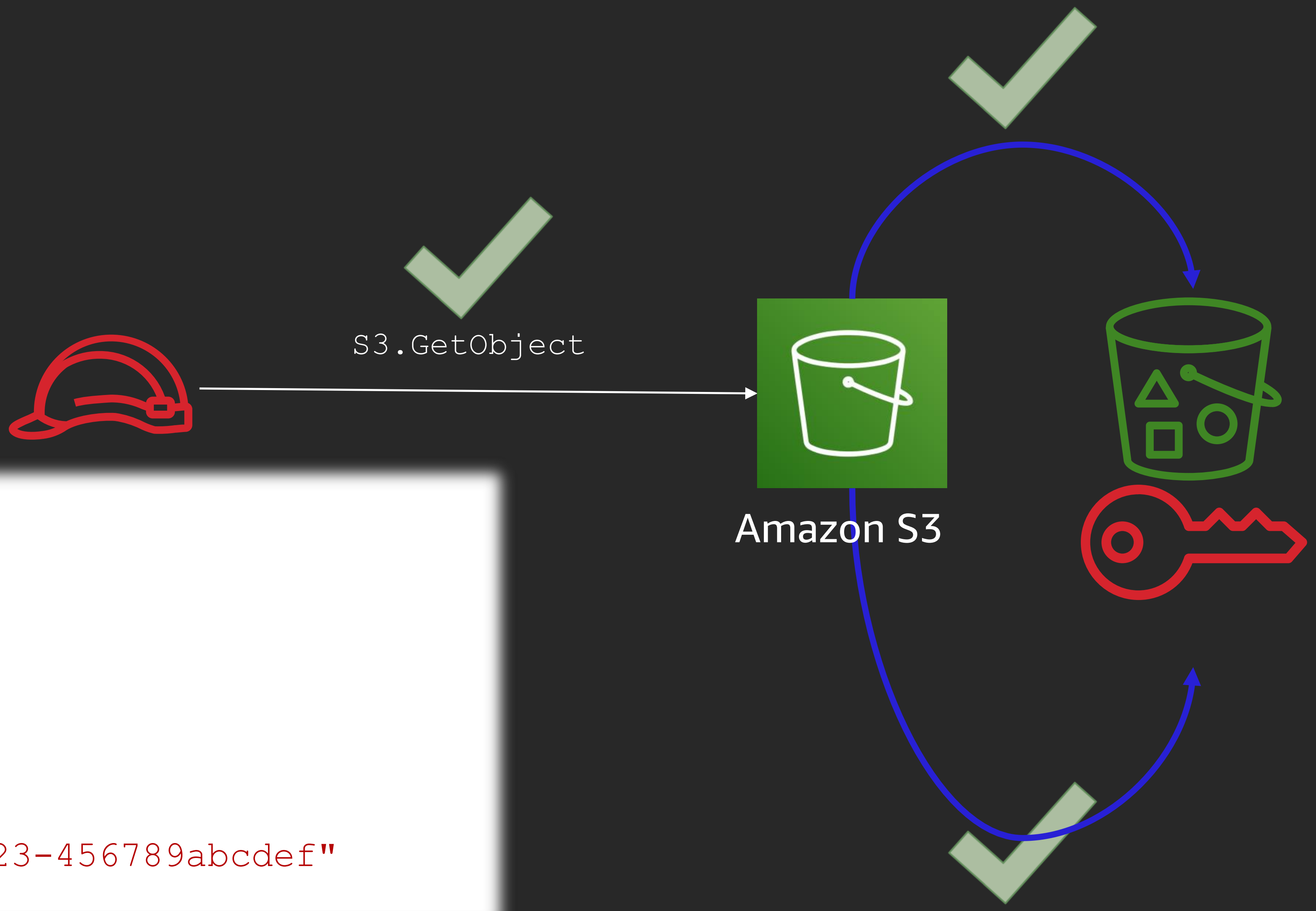
```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*"
}
```

IAM permissions for AWS KMS keys



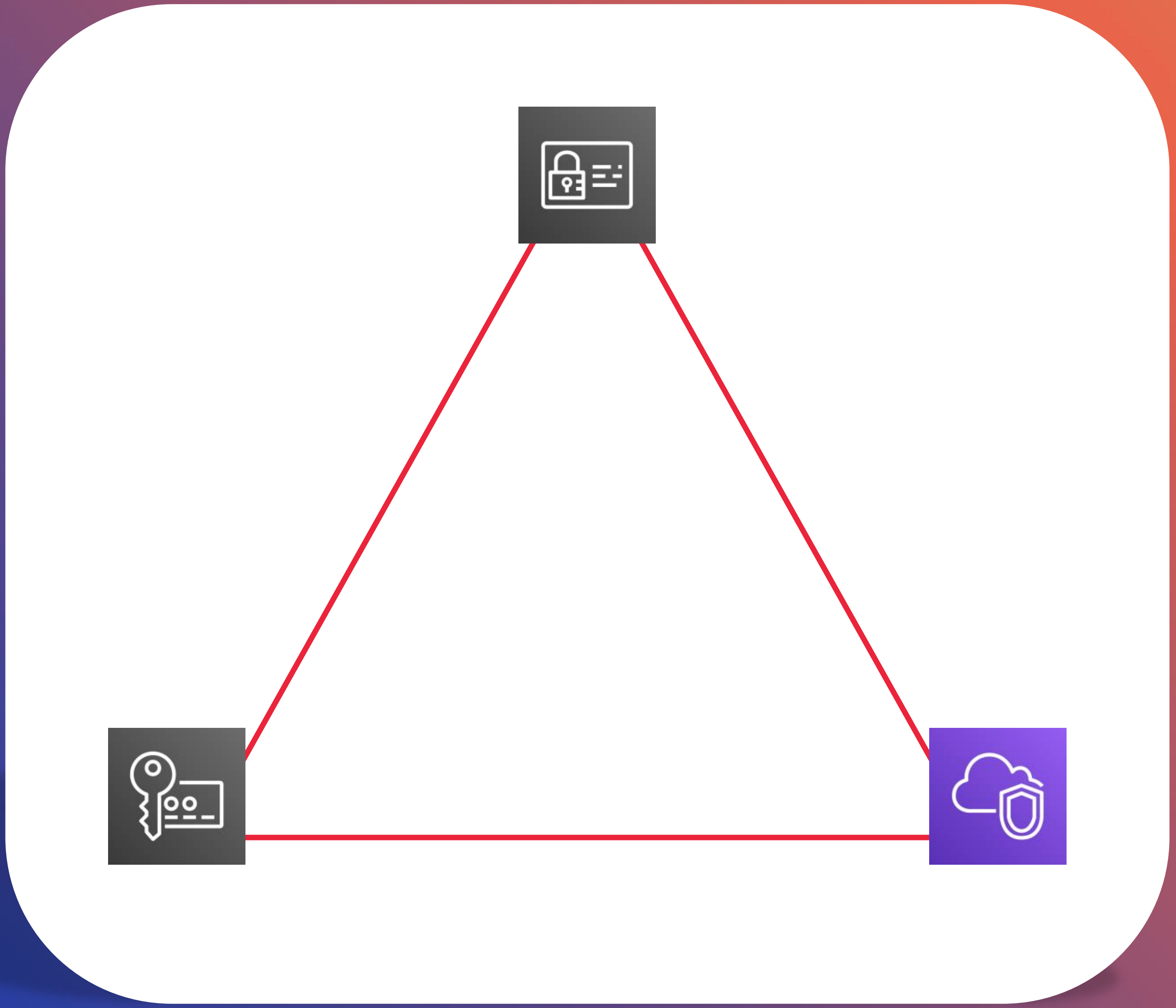
```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*"
}
```

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"
}
```

Amazon Virtual Private Cloud (VPC)



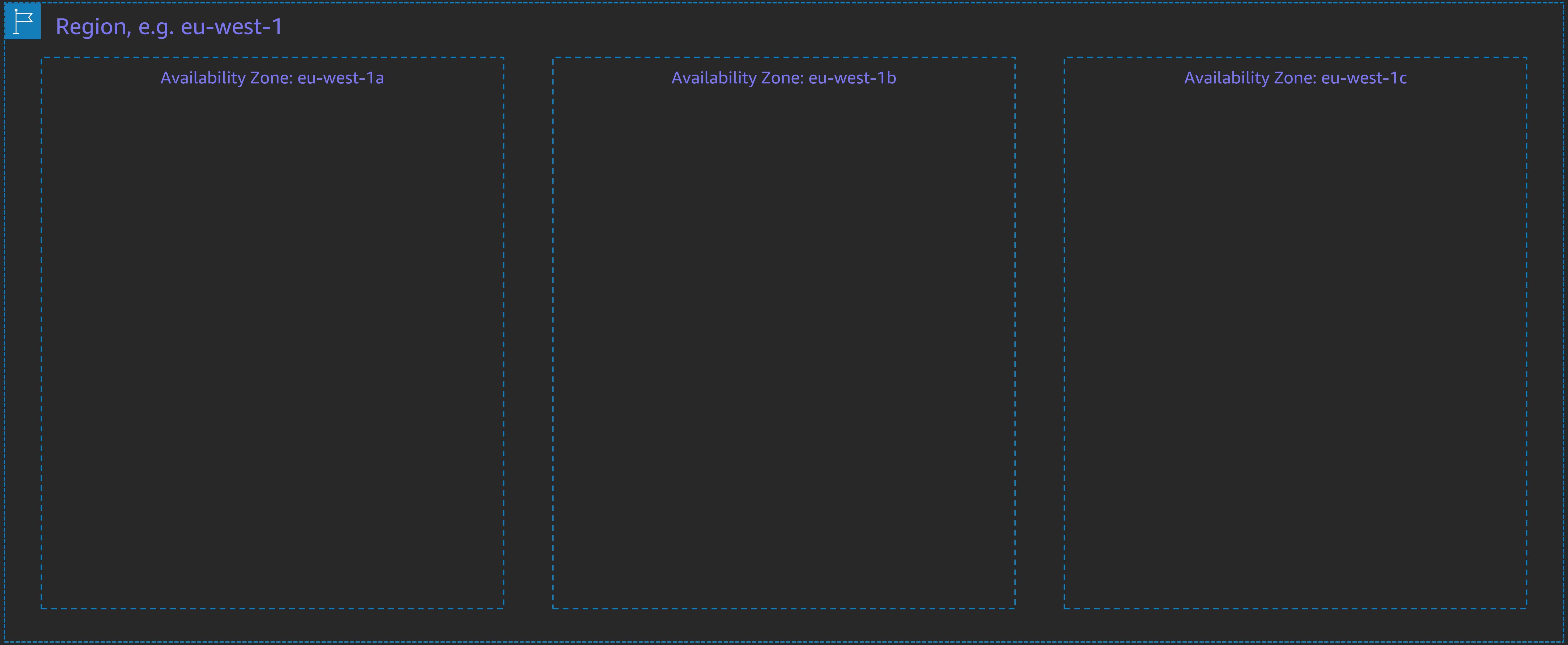
Amazon VPC

- **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. eu-west-1

What a VPC is and what goes in it



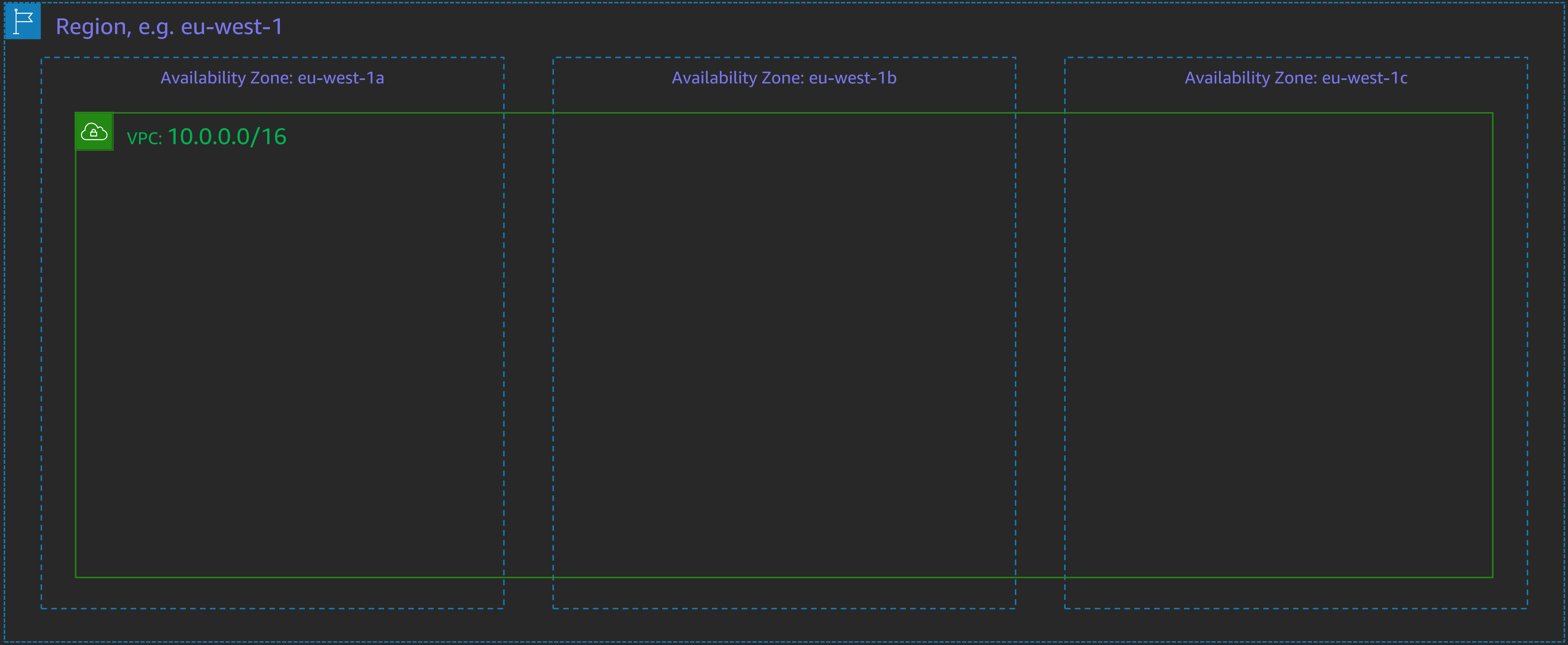
Region, e.g. eu-west-1

Availability Zone: eu-west-1a

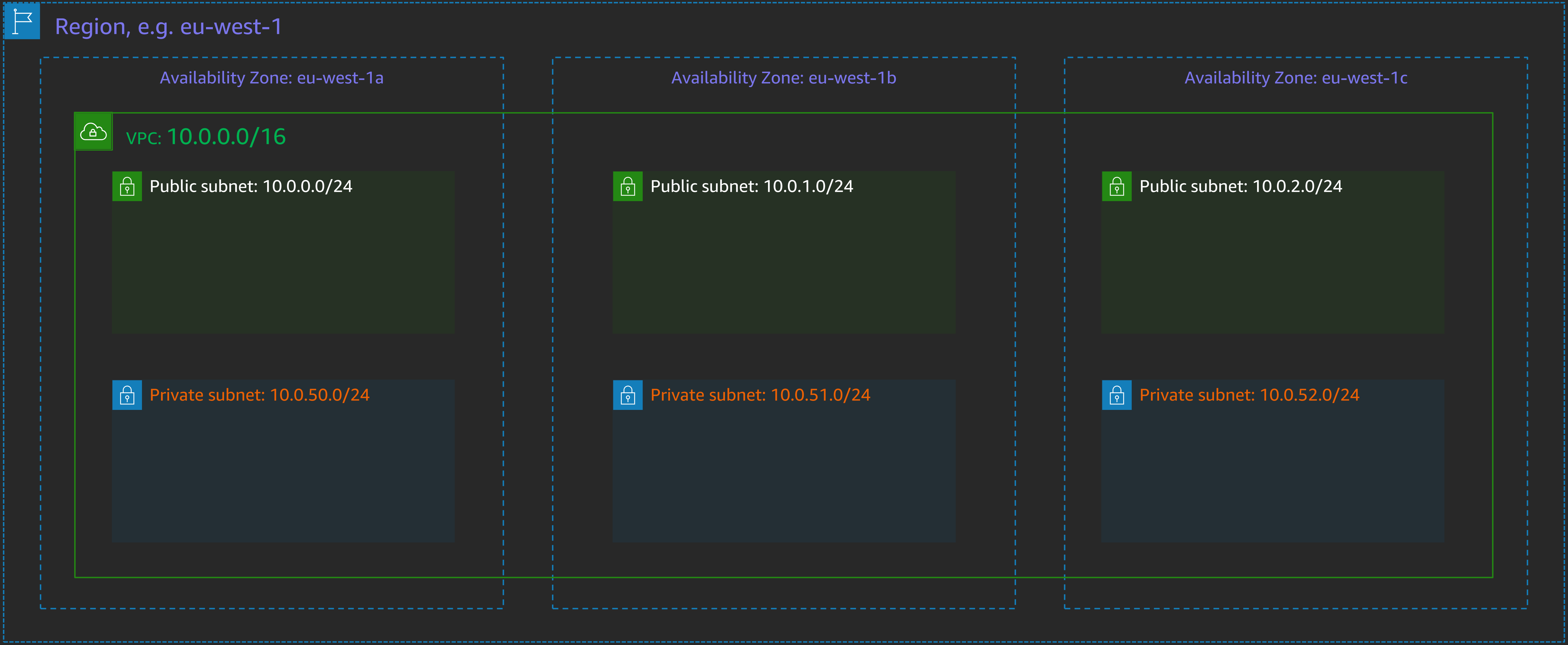
Availability Zone: eu-west-1b

Availability Zone: eu-west-1c

What a VPC is and what goes in it

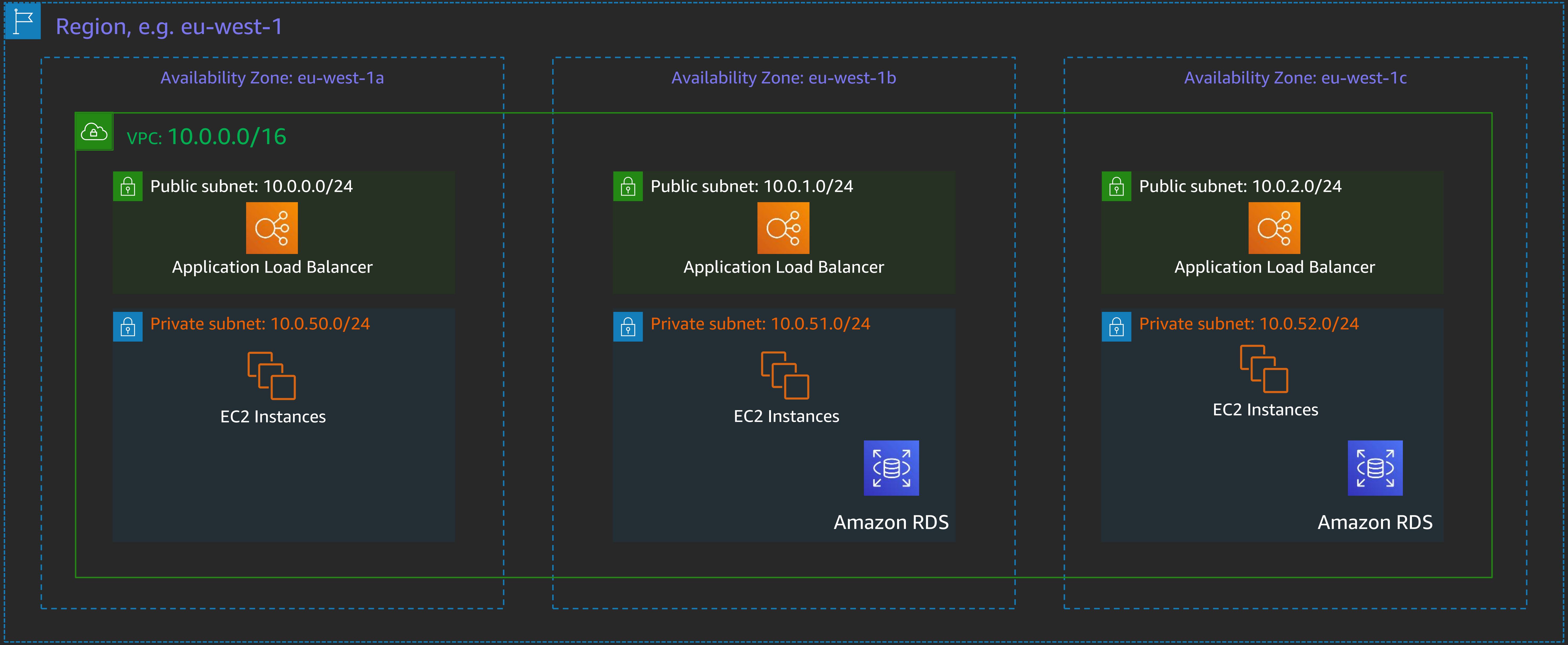

Region, e.g. eu-west-1
Availability Zone: eu-west-1a
Availability Zone: eu-west-1b
Availability Zone: eu-west-1c
VPC: 10.0.0.0/16

What a VPC is and what goes in it

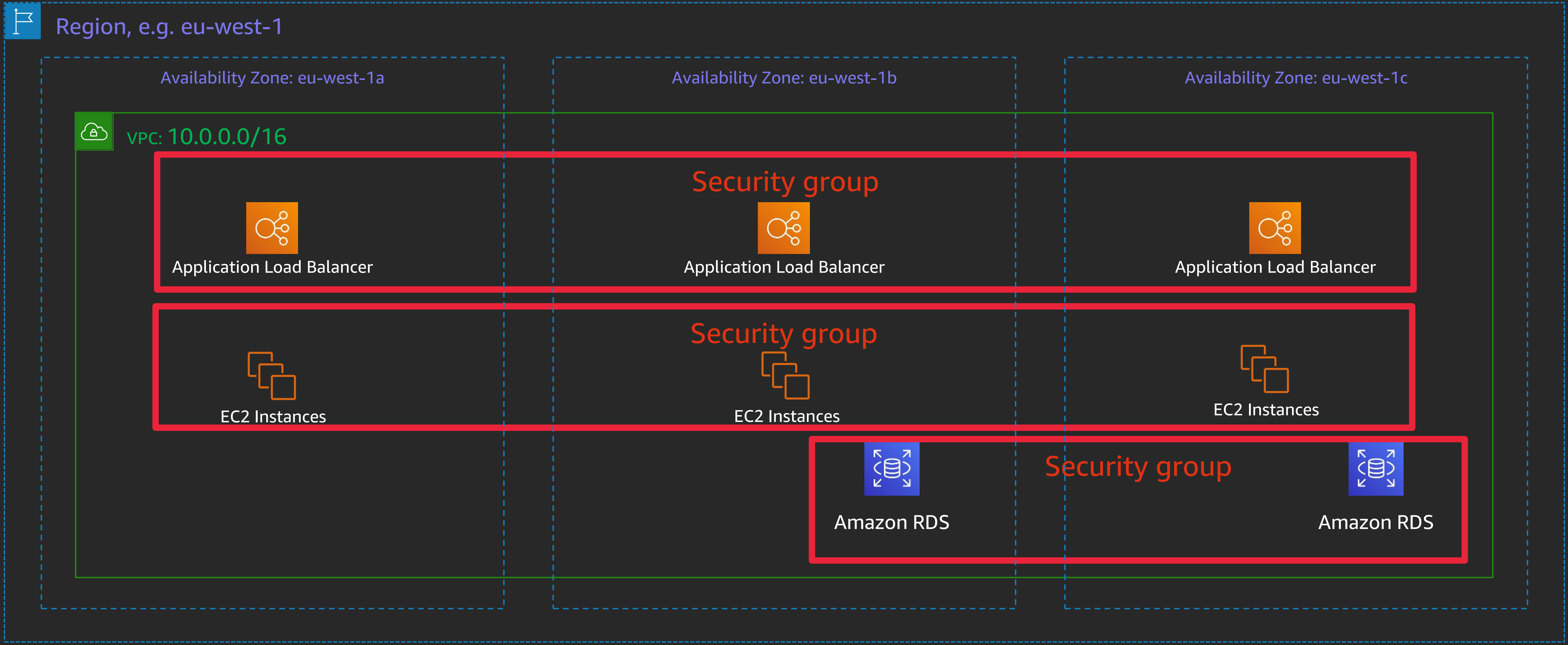


Region, e.g. eu-west-1
Availability Zone: eu-west-1a
Availability Zone: eu-west-1b
Availability Zone: eu-west-1c
VPC: 10.0.0.0/16
Public subnet: 10.0.0.0/24
Public subnet: 10.0.1.0/24
Public subnet: 10.0.2.0/24
Private subnet: 10.0.50.0/24
Private subnet: 10.0.51.0/24
Private subnet: 10.0.52.0/24

What a VPC is and what goes in it

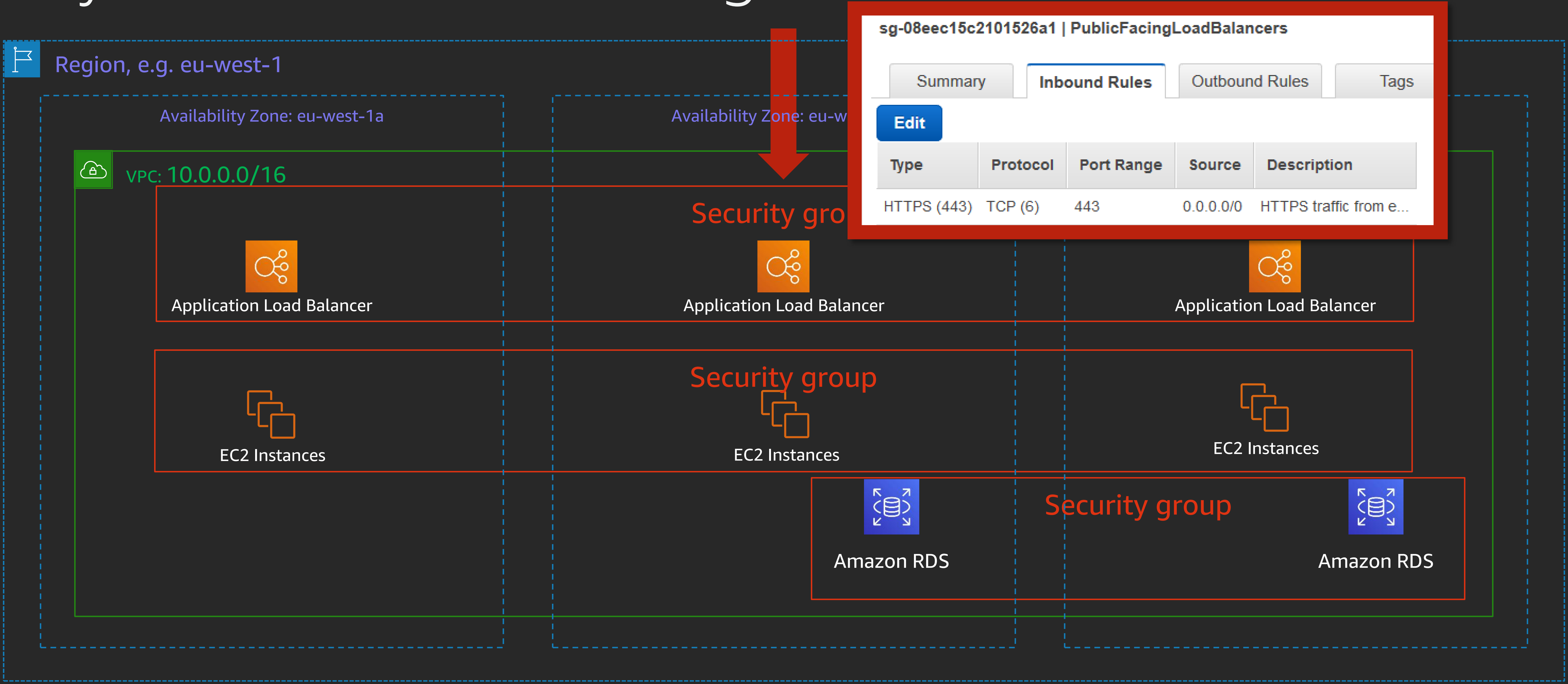

Region, e.g. eu-west-1
Availability Zone: eu-west-1a
Availability Zone: eu-west-1b
Availability Zone: eu-west-1c
VPC: 10.0.0.0/16
Public subnet: 10.0.0.0/24
Application Load Balancer
Public subnet: 10.0.1.0/24
Application Load Balancer
Public subnet: 10.0.2.0/24
Application Load Balancer
Private subnet: 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 . . .


Region, e.g. eu-west-1
Availability Zone: eu-west-1a
Availability Zone: eu-west-1b
Availability Zone: eu-west-1c
VPC: 10.0.0.0/16
Security group
Application Load Balancer
Application Load Balancer
Application Load Balancer
Security group
EC2 Instances
EC2 Instances
EC2 Instances
Amazon RDS
Security group
Amazon RDS

. . . understand security groups

If you understand nothing else about VPC . . .

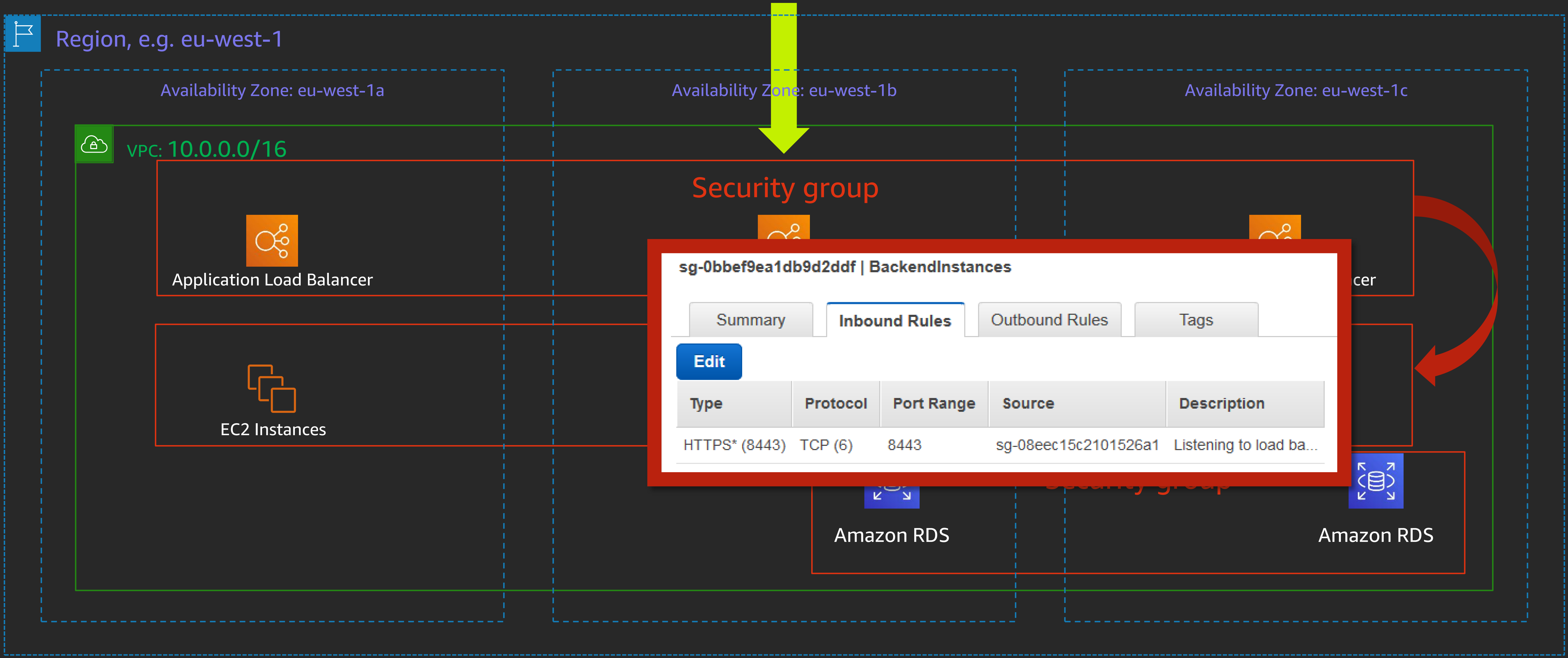


sg-08eec15c2101526a1 | PublicFacingLoadBalancers

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 . . .

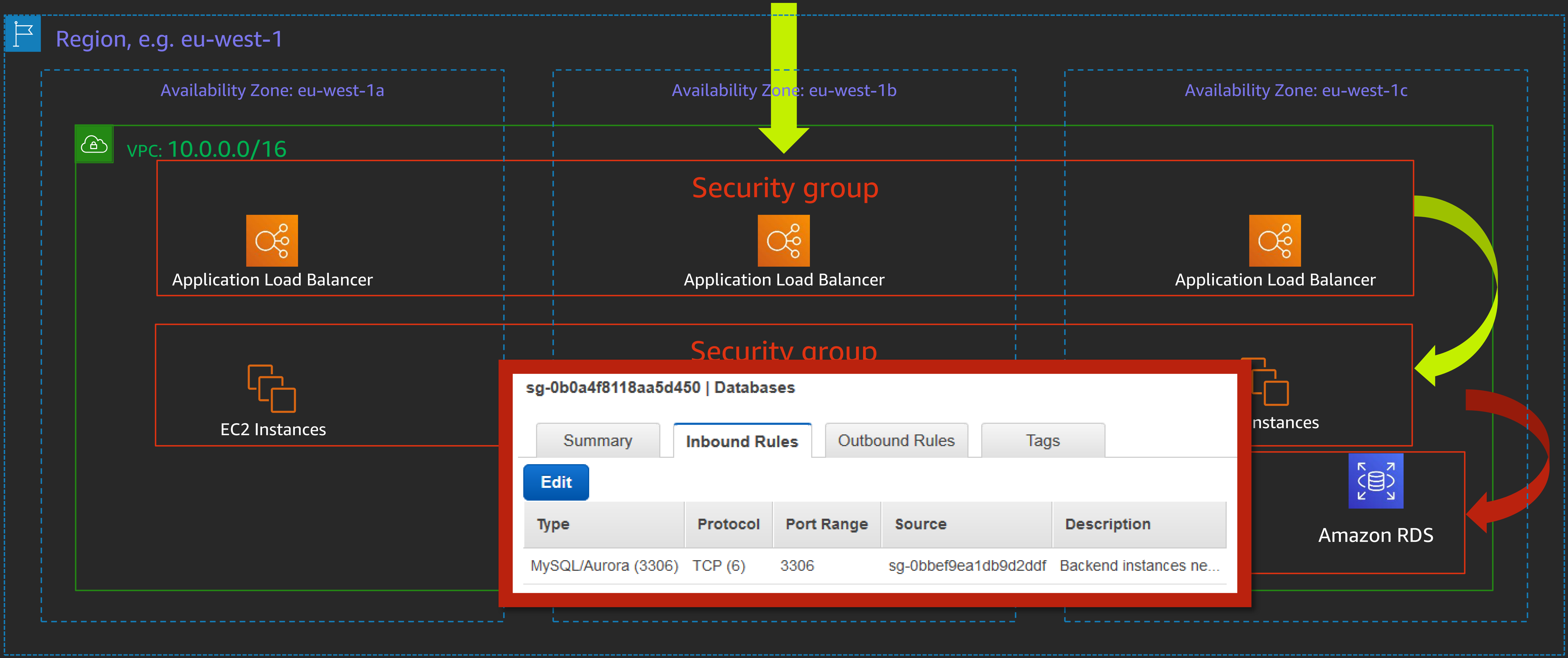


sg-0bbef9ea1db9d2ddf | BackendInstances

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 . . .

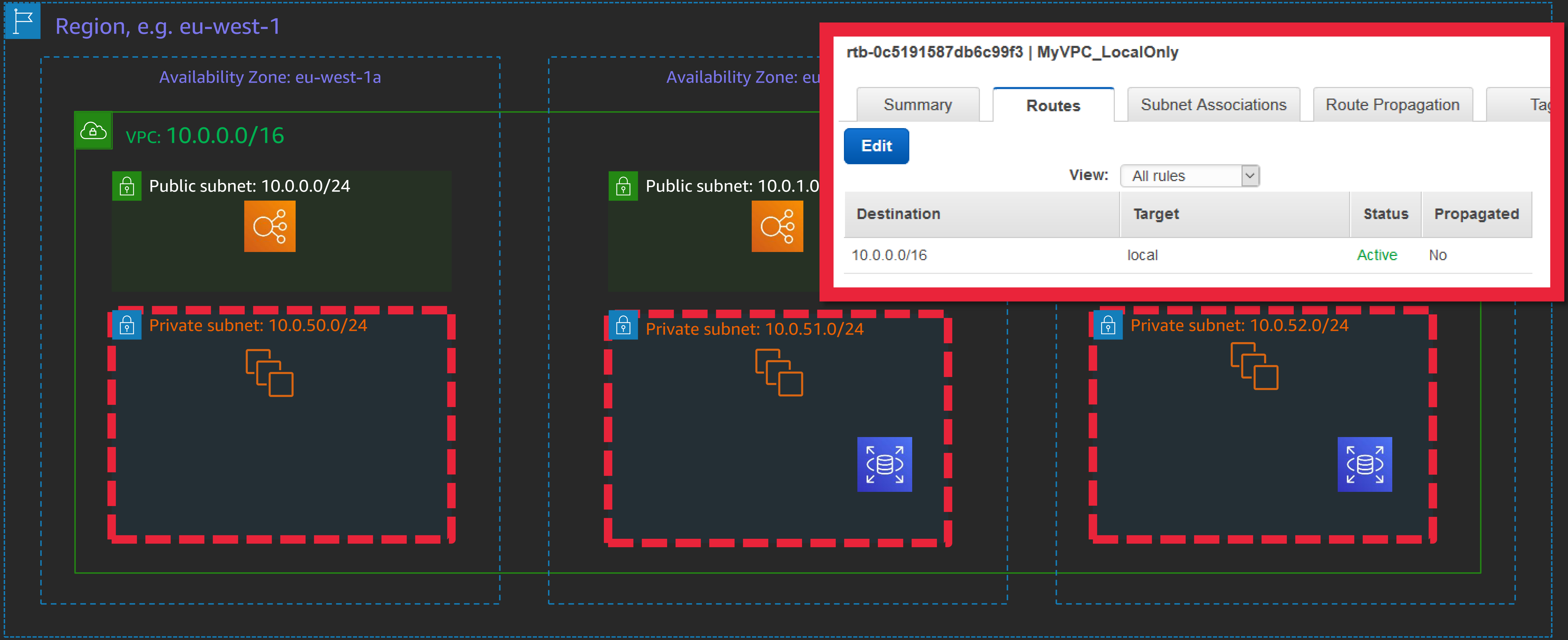

Region, e.g. eu-west-1
Availability Zone: eu-west-1a
Availability Zone: eu-west-1b
Availability Zone: eu-west-1c
VPC: 10.0.0.0/16
Security group
Application Load Balancer
Application Load Balancer
Application Load Balancer
Security group
EC2 Instances
nstances
Amazon RDS
Summary
Inbound Rules
Outbound Rules
Tags
Edit

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. eu-west-1
Availability Zone: eu-west-1a
Availability Zone: eu
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

rtb-0c5191587db6c99f3 | MyVPC_LocalOnly

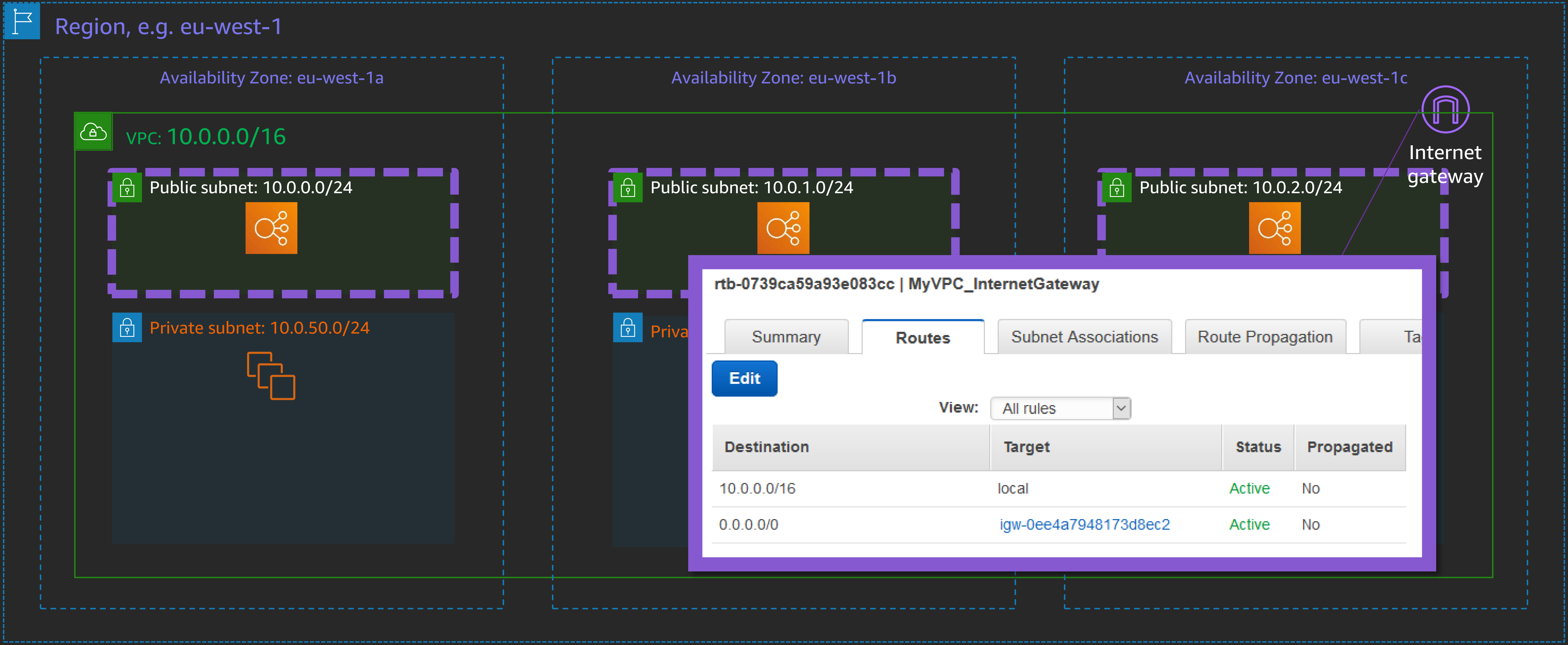
Summary
Routes
Subnet Associations
Route Propagation
Tag
Edit

View: All rules

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. eu-west-1
Availability Zone: eu-west-1a
Availability Zone: eu-west-1b
Availability Zone: eu-west-1c
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

rtb-0739ca59a93e083cc | MyVPC_InternetGateway

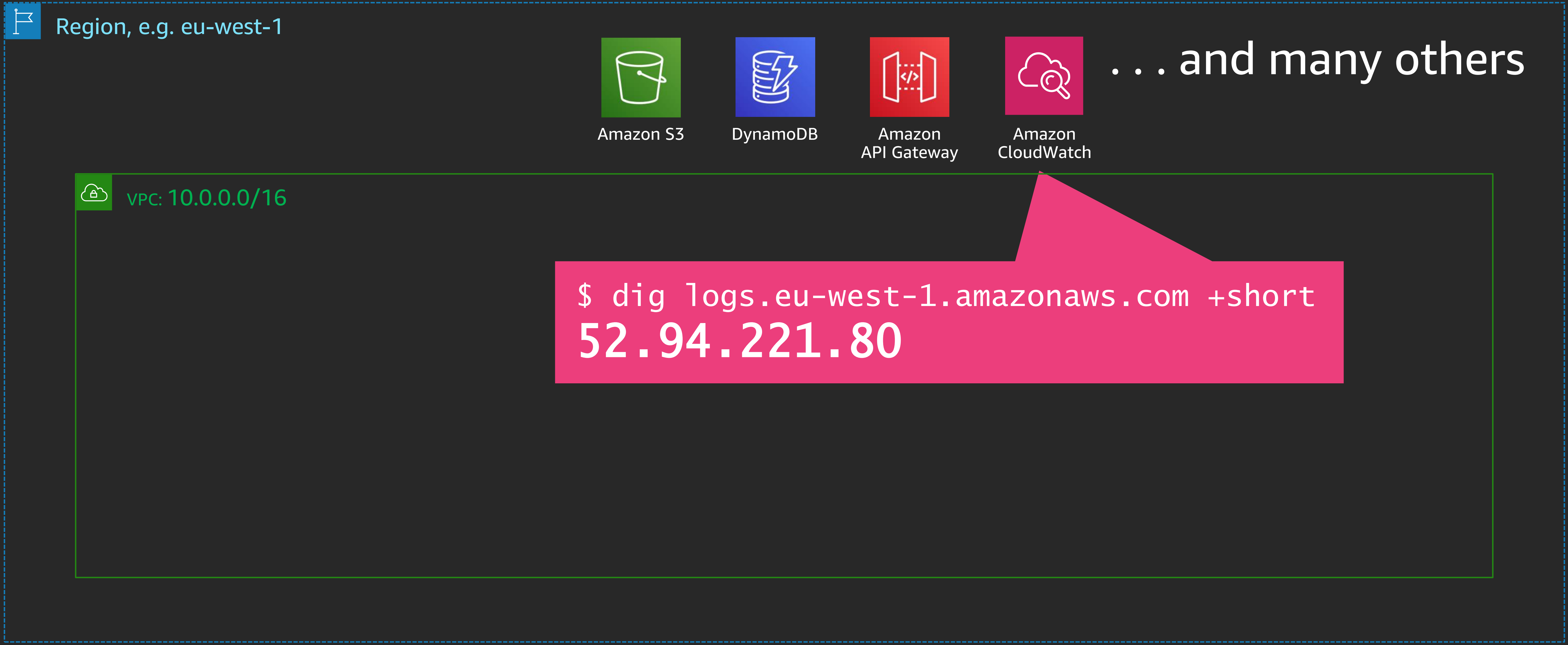
Summary
Routes
Subnet Associations
Route Propagation
Ta
Edit

View: All rules

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

. . . understand routing

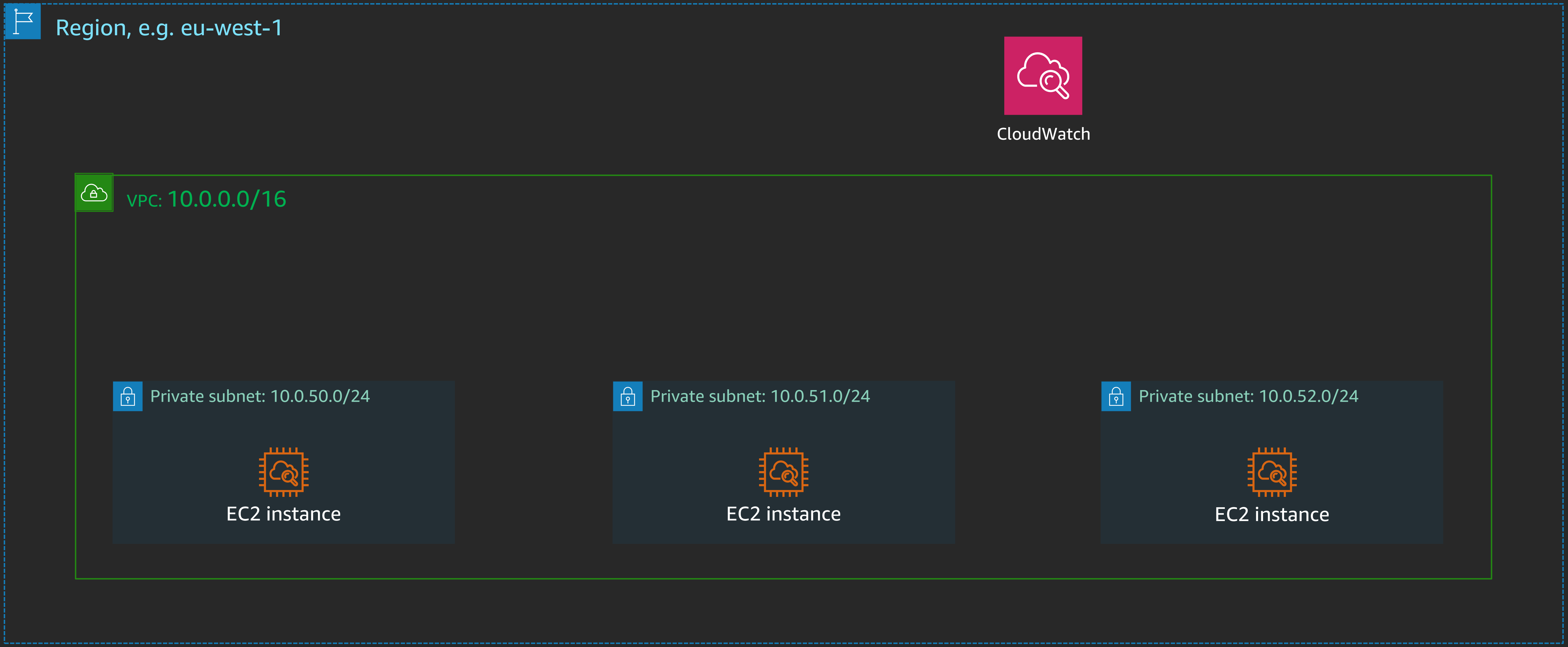
AWS resources **not** in your VPC



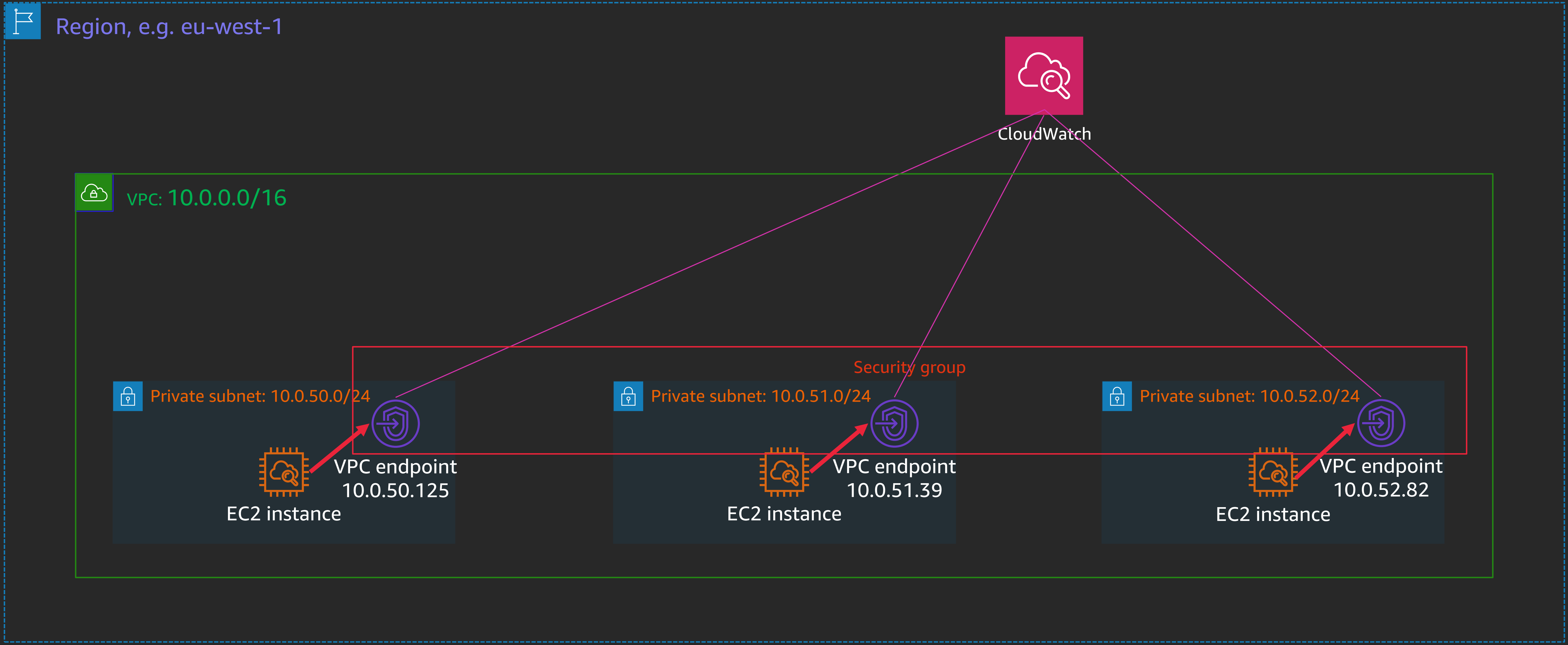
. . . and many others

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

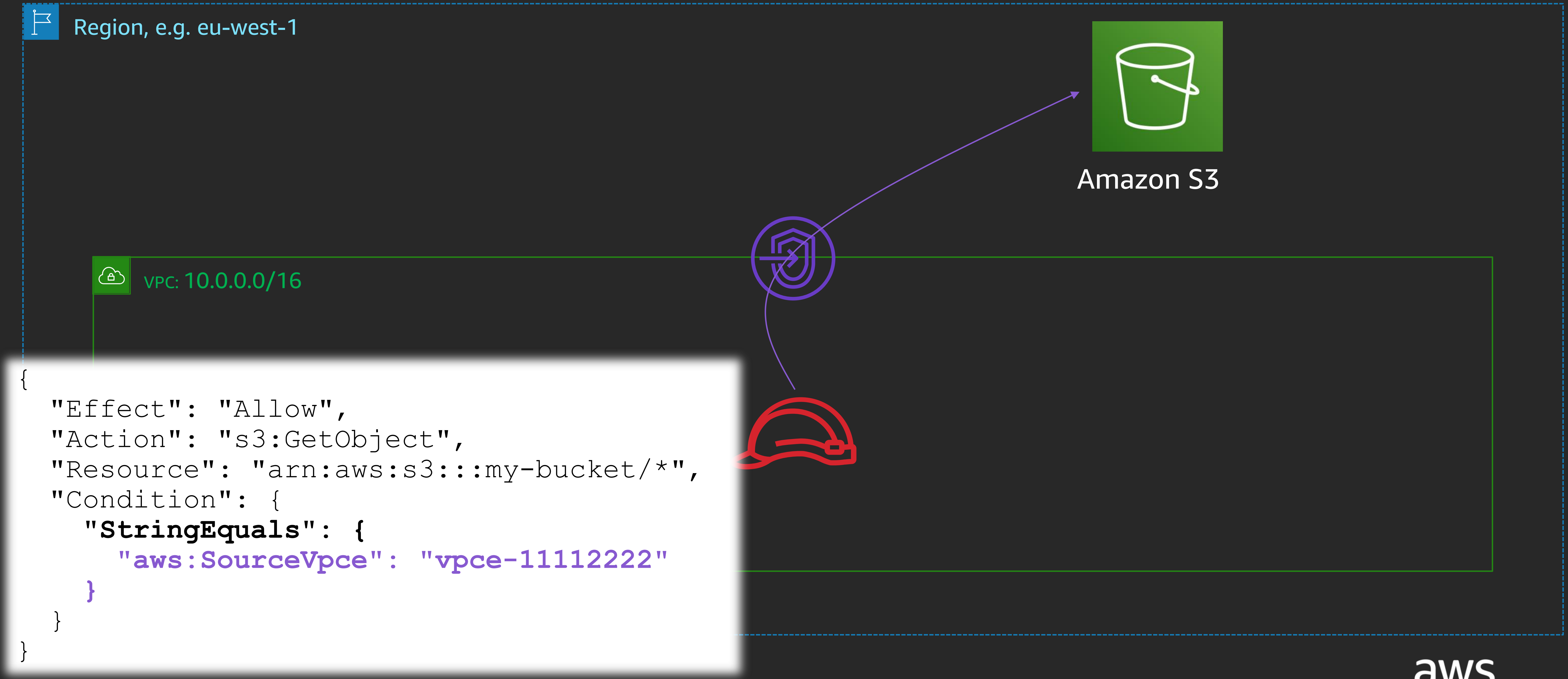
VPC endpoints: Private connectivity to AWS services


Region, e.g. eu-west-1
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



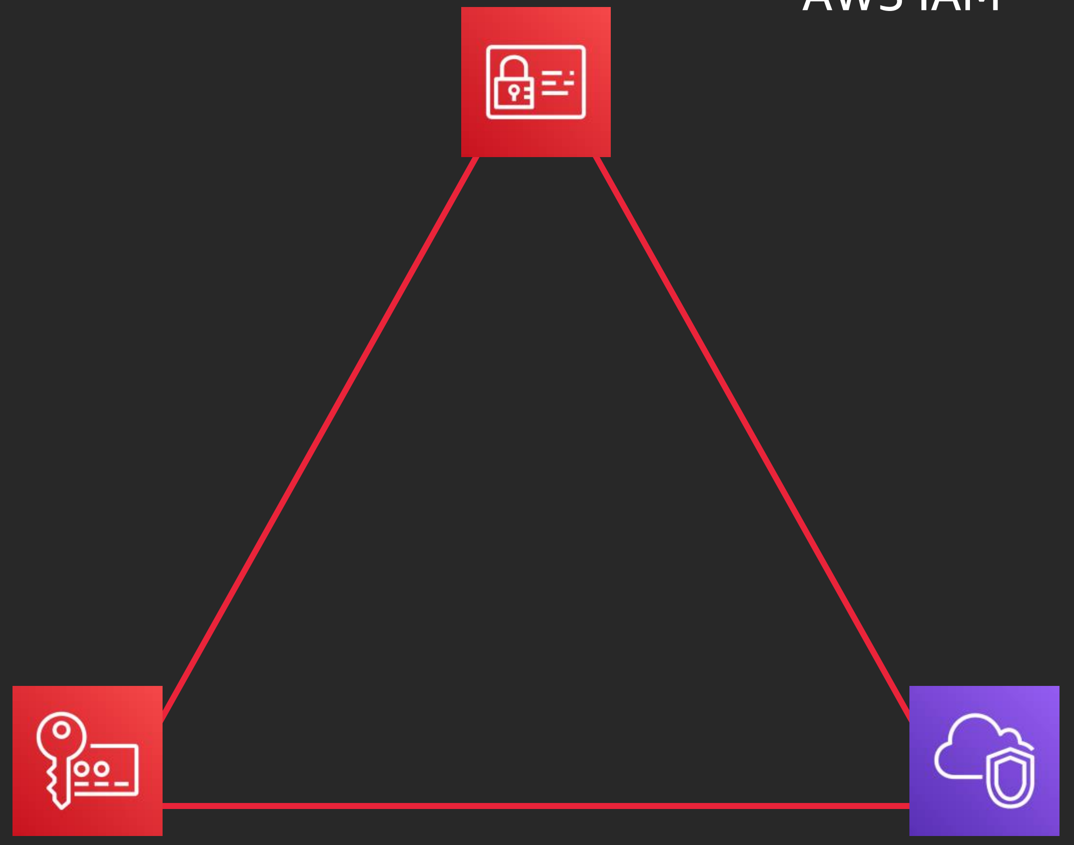
VPC endpoints: Authorization using network path



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

Wrapping up

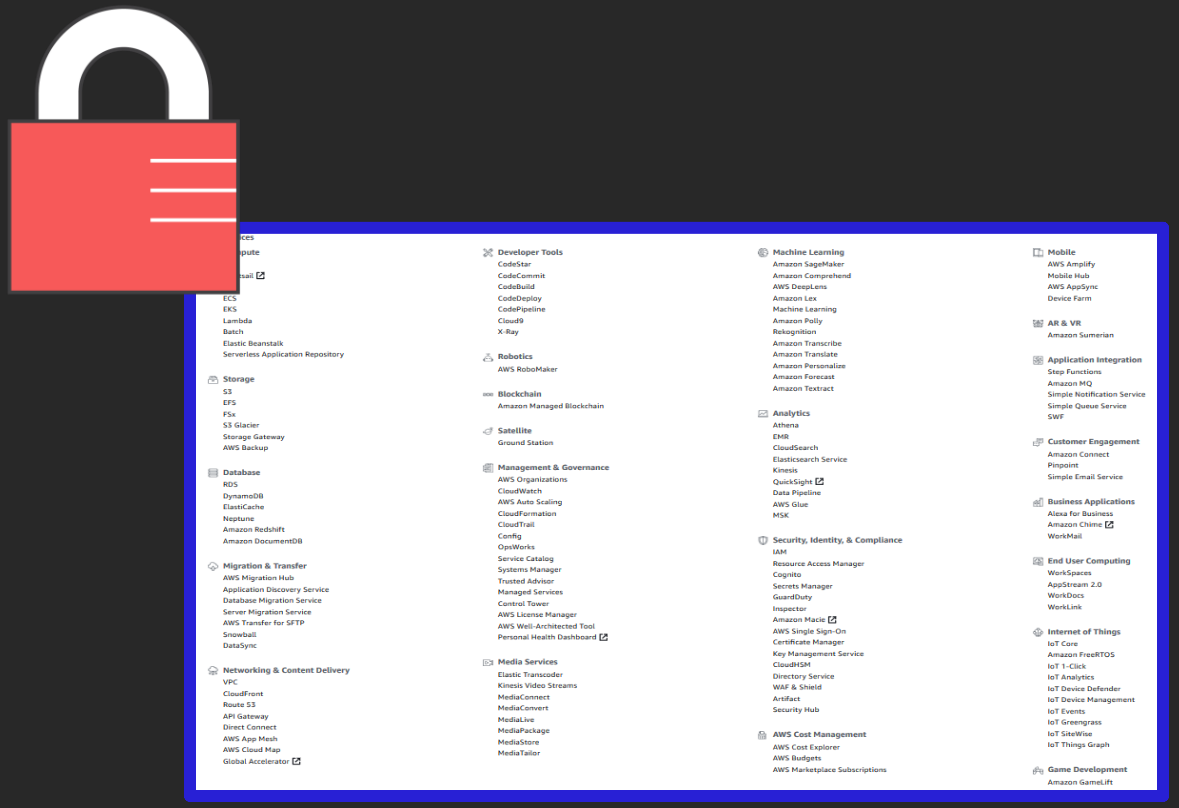
Learn a few patterns, secure everything in AWS



Permissions management:
AWS IAM

Data encryption:
AWS KMS

Network security controls:
Amazon VPC



ces

pute

tsail

ECS
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

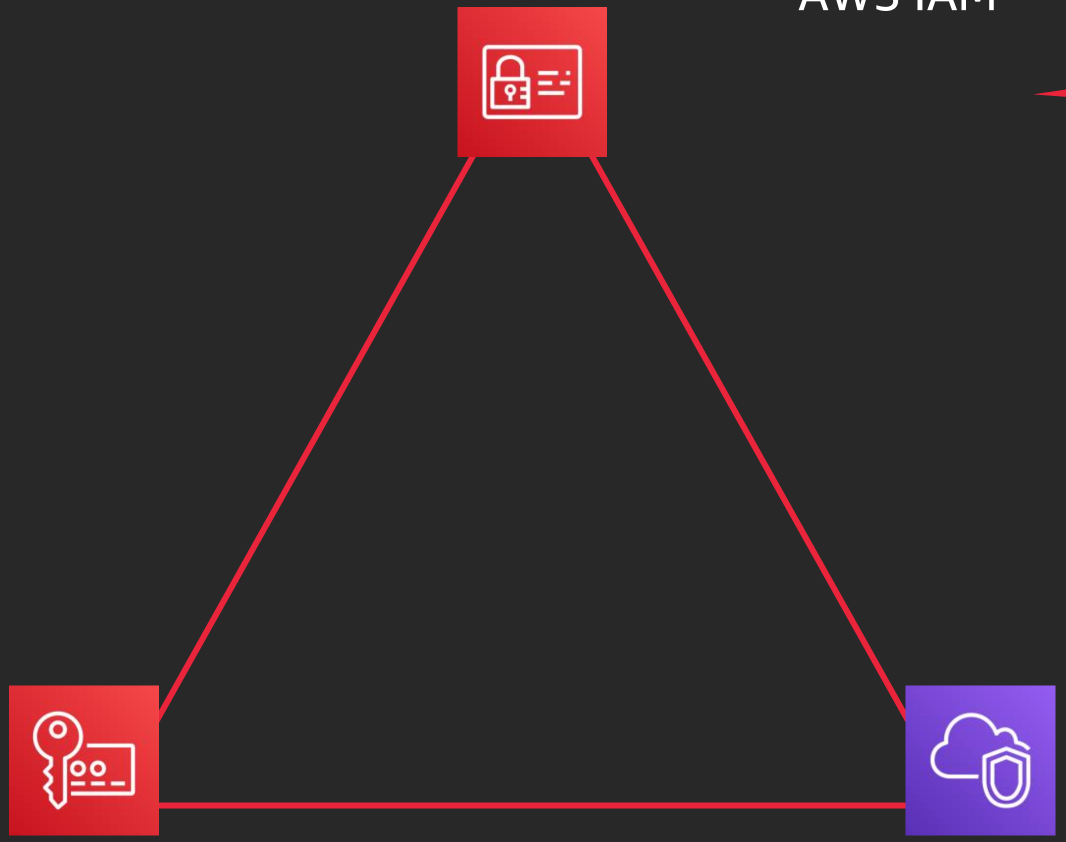
Business Applications
Alexa for Business
Amazon Chime
WorkMail

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

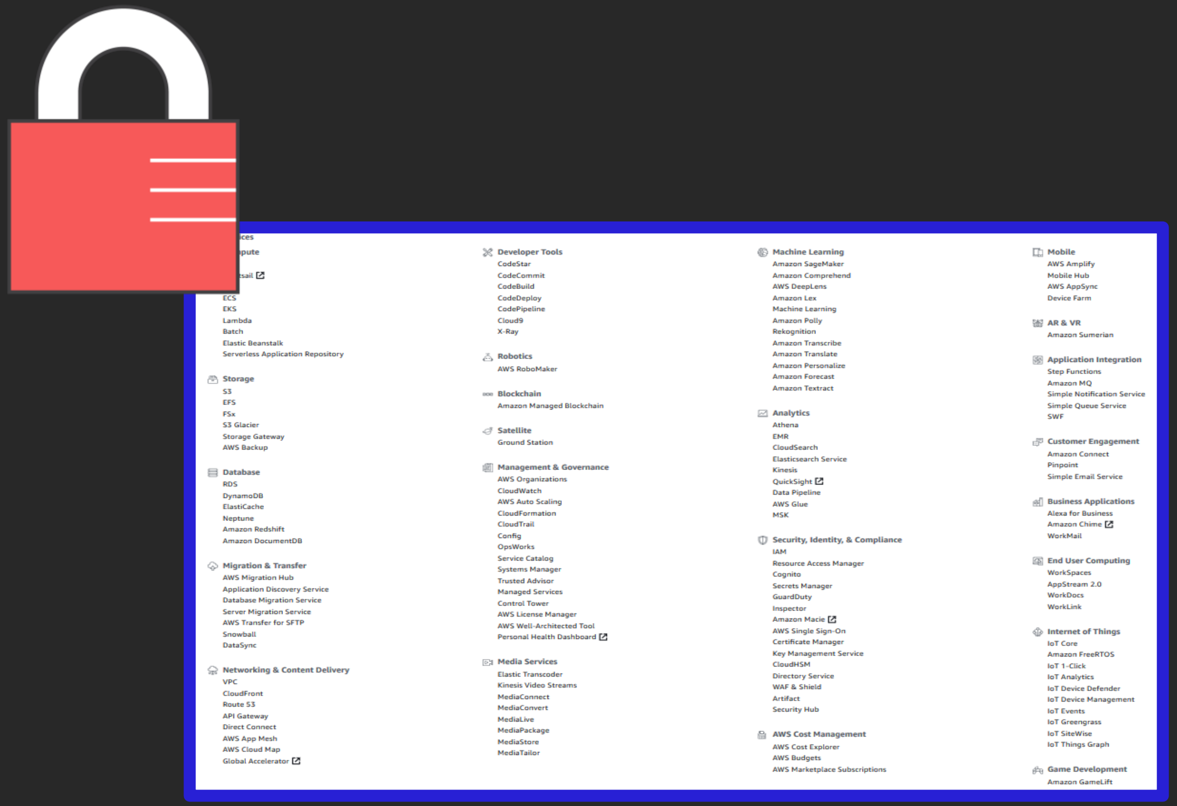


Permissions management:
AWS IAM

Data encryption:
AWS KMS

Network security controls:
Amazon VPC

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



ices

pute

tsail ↗
ECS
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

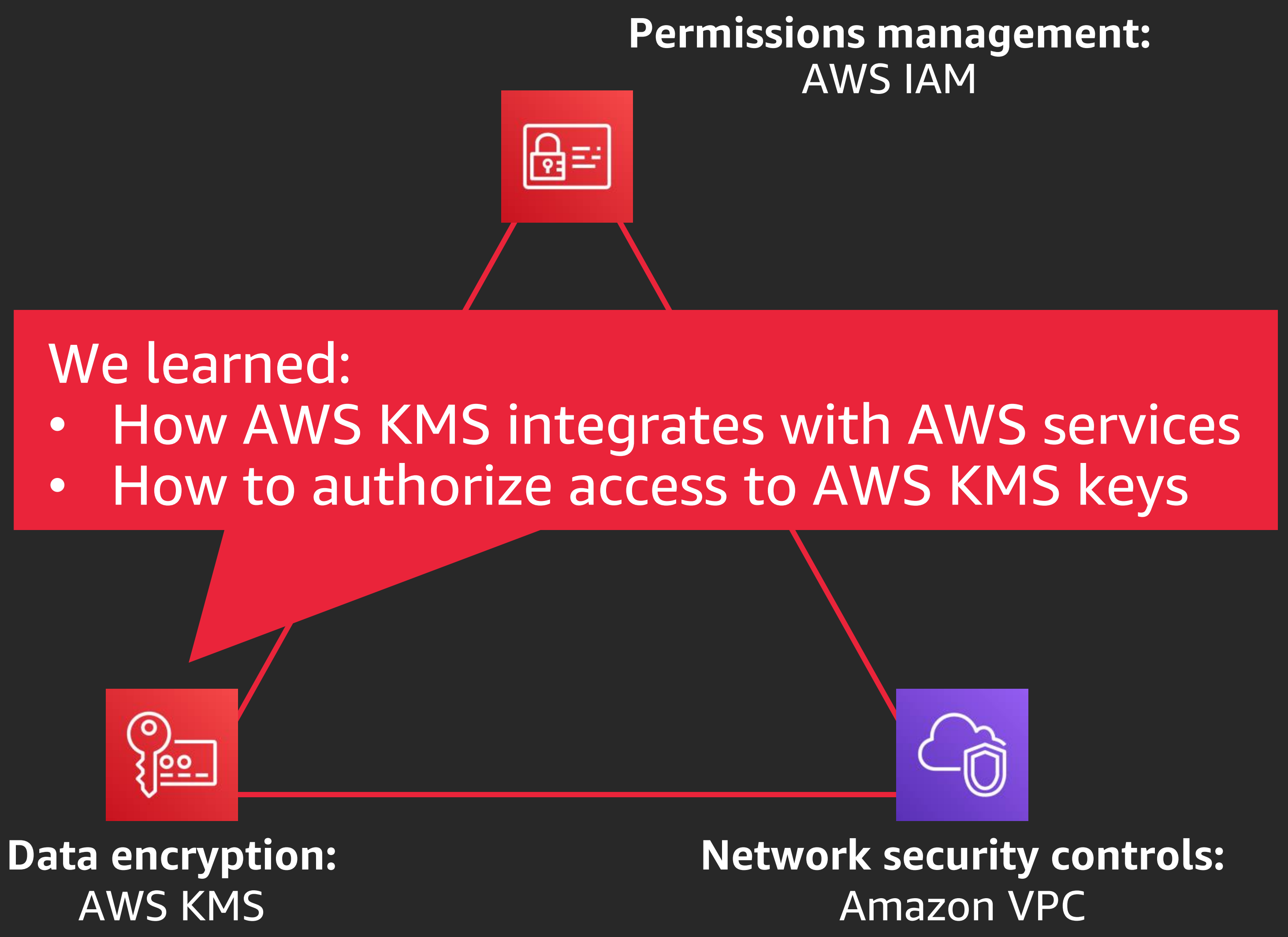
Business Applications
Alexa for Business
Amazon Chime ↗
WorkMail

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:

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

ces

pute

tsail

ECS
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

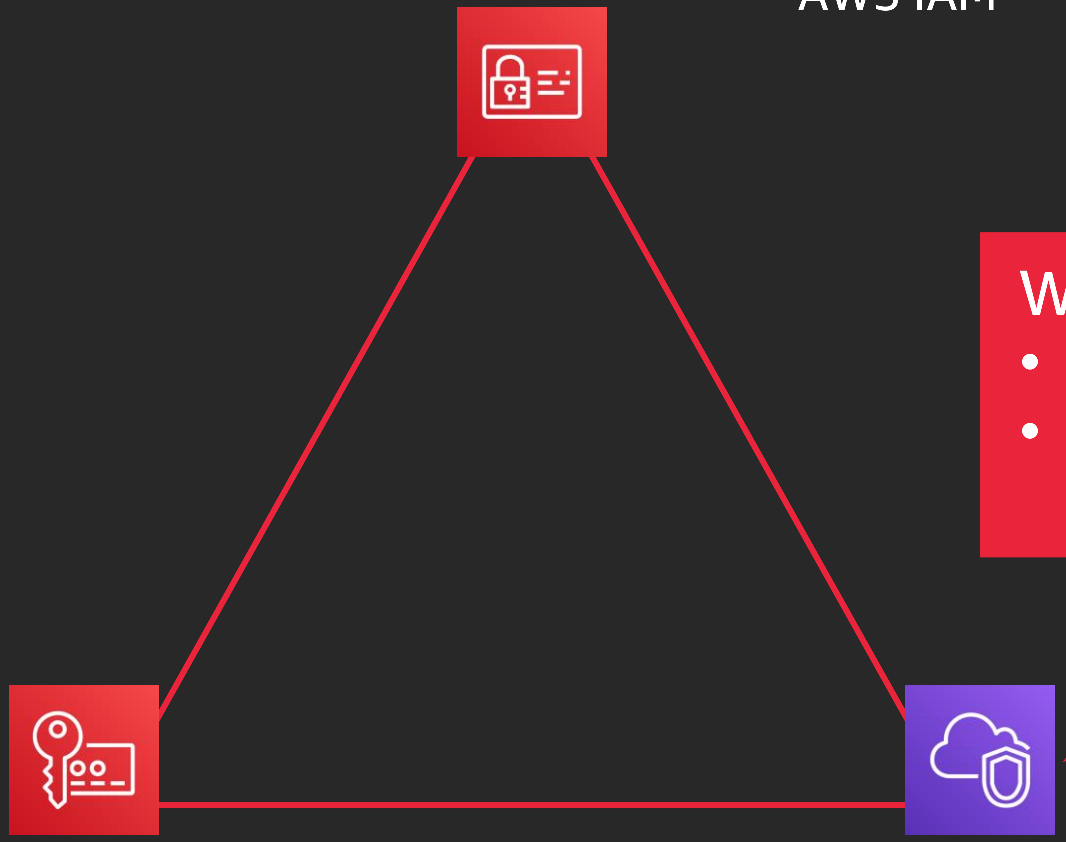
Business Applications
Alexa for Business
Amazon Chime
WorkMail

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:

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

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

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

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

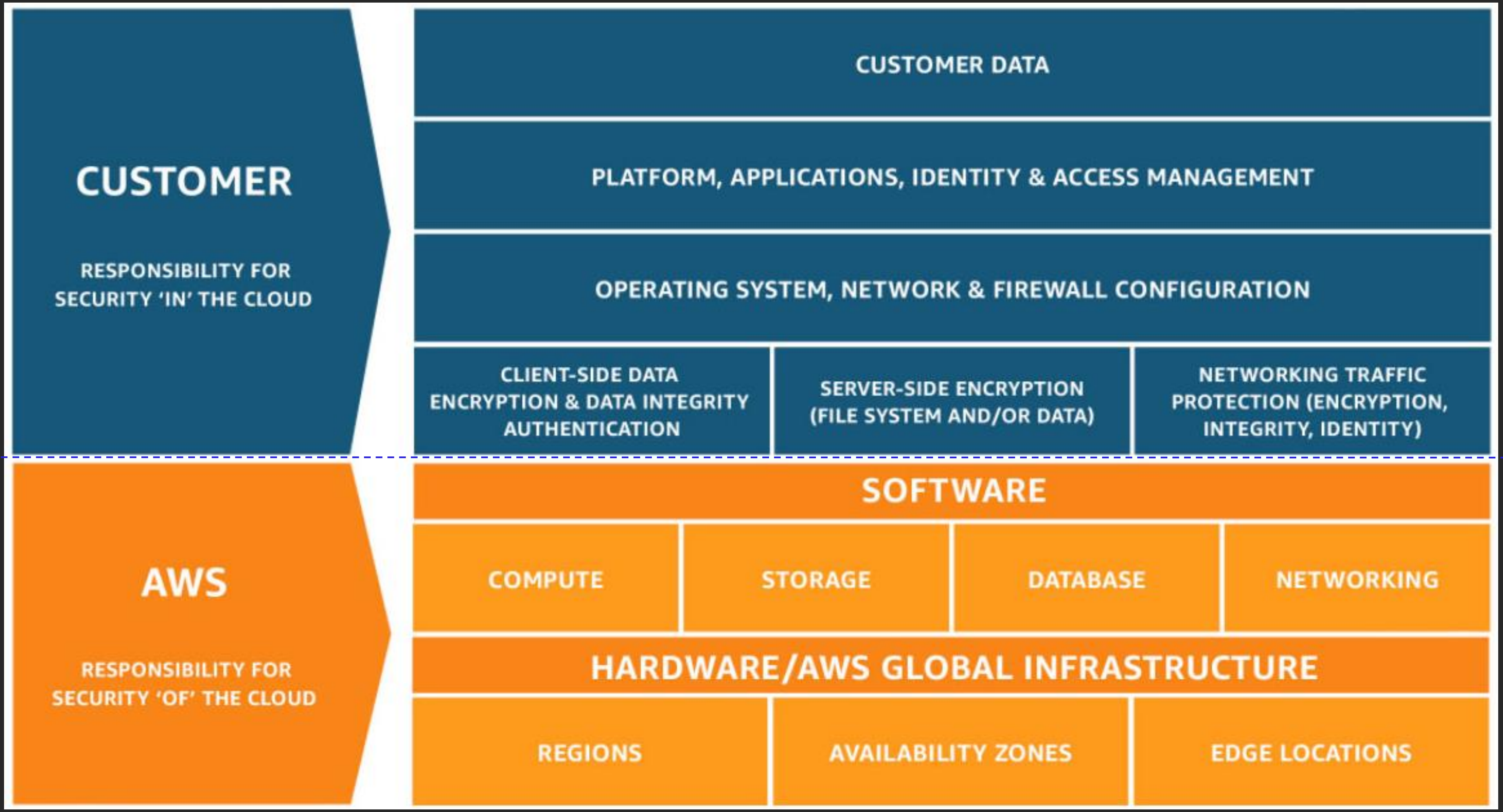
Business Applications
Alexa for Business
Amazon Chime
WorkMail

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

AWS shared responsibility model



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

Security in the cloud

Managed by **customers**

Security of the cloud

Managed by **AWS**

Ready to build?

Overview

LIVE OPENING & CLOSING LIVE Q&A

TRACKS

Track 1

- Performance Efficiency
- Operational Excellence
- Marketplace

Track 2

- Reliability
- Cost Optimization
- Startup – AWS Activate

4 LANGUAGES ACROSS 5 TRACKS

English Tracks

Korean Track

Bahasa Indonesia Track

Vietnamese Track

ACTIVITIES

Live Q&A with AWS Experts

20+ Sessions

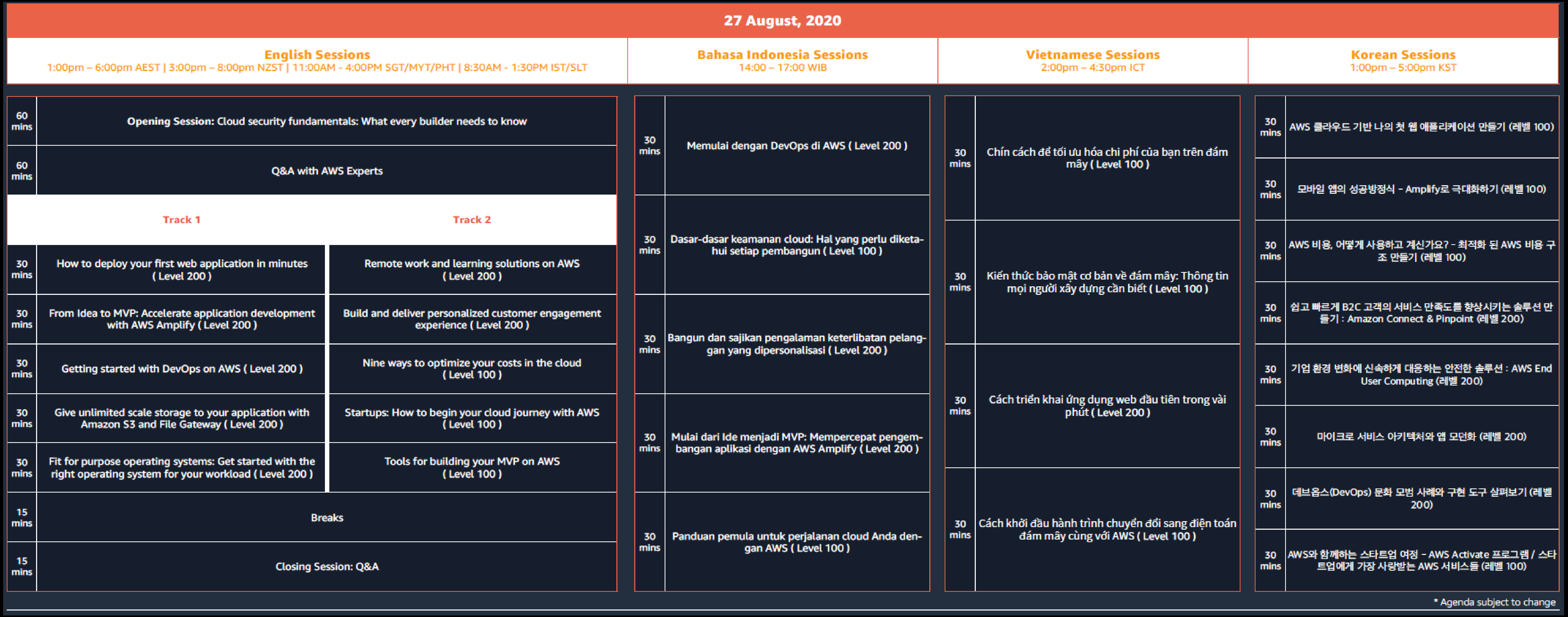
Technical Demos & Use Cases

Certificate of Attendance

aws

Agenda

(https://aws.amazon.com/events/builders-online-series/)



27 August, 2020

English Sessions
1:00pm – 6:00pm AEST | 3:00pm – 8:00pm NZST | 11:00AM - 4:00PM SGT/MYT/PHT | 8:30AM - 1:30PM IST/SLT

60 mins	Opening Session: Cloud security fundamentals: What every builder needs to know		
60 mins	Q&A with AWS Experts		
	Track 1		Track 2
30 mins	How to deploy your first web application in minutes (Level 200)		Remote work and learning solutions on AWS (Level 200)
30 mins	From Idea to MVP: Accelerate application development with AWS Amplify (Level 200)		Build and deliver personalized customer engagement experience (Level 200)
30 mins	Getting started with DevOps on AWS (Level 200)		Nine ways to optimize your costs in the cloud (Level 100)
30 mins	Give unlimited scale storage to your application with Amazon S3 and File Gateway (Level 200)		Startups: How to begin your cloud journey with AWS (Level 100)
30 mins	Fit for purpose operating systems: Get started with the right operating system for your workload (Level 200)		Tools for building your MVP on AWS (Level 100)
15 mins	Breaks		
15 mins	Closing Session: Q&A		

Bahasa Indonesia Sessions
14:00 – 17:00 WIB

30 mins	Memulai dengan DevOps di AWS (Level 200)
30 mins	Dasar-dasar keamanan cloud: Hal yang perlu diketahui setiap pembangun (Level 100)
30 mins	Bangun dan sajikan pengalaman keterlibatan pelanggan yang dipersonalisasi (Level 200)
30 mins	Mulai dari Ide menjadi MVP: Mempercepat pengembangan aplikasi dengan AWS Amplify (Level 200)
30 mins	Panduan pemula untuk perjalanan cloud Anda dengan AWS (Level 100)

Vietnamese Sessions
2:00pm – 4:30pm ICT

30 mins	Chín cách để tối ưu hóa chi phí của bạn trên đám mây (Level 100)
30 mins	Kiến thức bảo mật cơ bản về đám mây: Thông tin mọi người xây dựng cần biết (Level 100)
30 mins	Cách triển khai ứng dụng web đầu tiên trong vài phút (Level 200)
30 mins	Cách khởi đầu hành trình chuyển đổi sang điện toán đám mây cùng với AWS (Level 100)

Korean Sessions
1:00pm – 5:00pm KST

30 mins	AWS 클라우드 기반 나의 첫 웹 애플리케이션 만들기 (레벨 100)
30 mins	모바일 앱의 성공방정식 – Amplify로 극대화하기 (레벨 100)
30 mins	AWS 비용, 어떻게 사용하고 계신가요? – 최적화 된 AWS 비용 구조 만들기 (레벨 100)
30 mins	쉽고 빠르게 B2C 고객의 서비스 만족도를 향상시키는 솔루션 만들기 : Amazon Connect & Pinpoint (레벨 200)
30 mins	기업 환경 변화에 신속하게 대응하는 안전한 솔루션 : AWS End User Computing (레벨 200)
30 mins	마이크로 서비스 아키텍처와 앱 모던화 (레벨 200)
30 mins	데브옵스(DevOps) 문화 모범 사례와 구현 도구 살펴보기 (레벨 200)
30 mins	AWS와 함께하는 스타트업 여정 – AWS Activate 프로그램 / 스타트업에게 가장 사랑받는 AWS 서비스들 (레벨 100)

* Agenda subject to change

Builders Online Series

Thank you

Gabe Hollombe

in 🐦 @gabehollombe

gabehol@amazon.com