







FND209


The fundamentals of AWS cloud security


Becky Weiss
Senior Principal Engineer
AWS

 Lightsail 
ECR
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


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


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


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

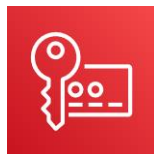
 **End User Computing**
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink

 **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

Snapshot
taken
04-19-2019

Learn a few patterns, secure everything in AWS

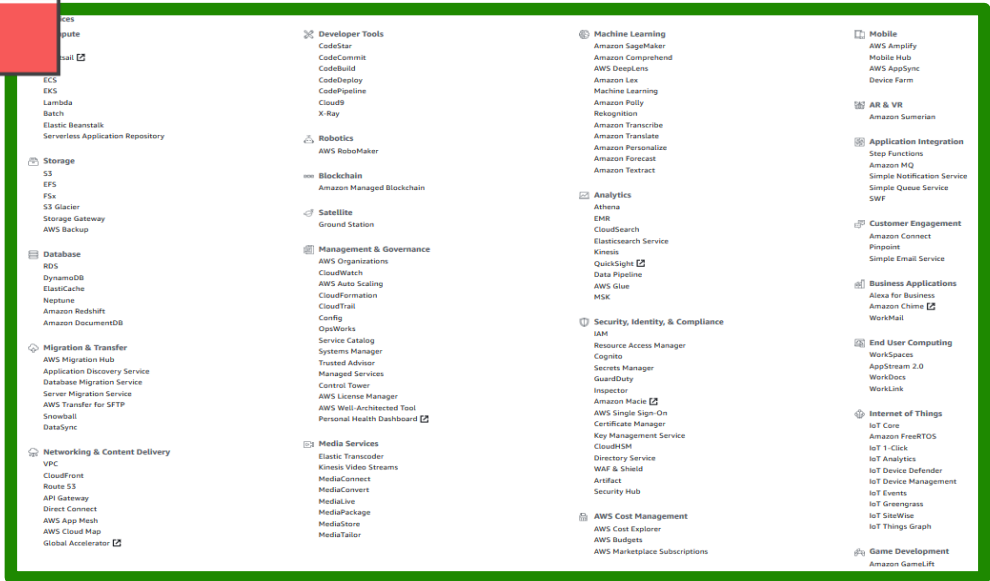
Permissions management:
AWS Identity and Access Management (IAM)



Data encryption:
AWS Key Management Service
(AWS KMS)



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



Agenda

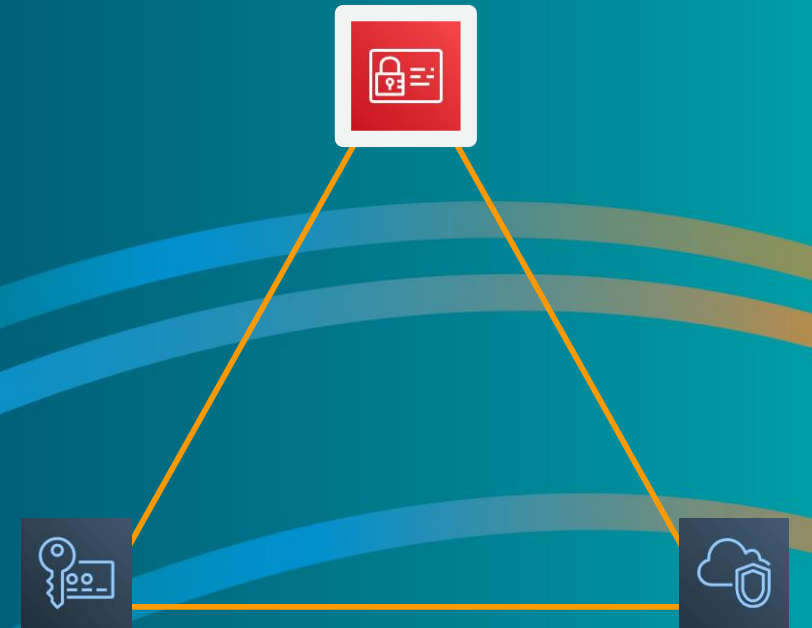


A builder-focused introduction to the AWS-wide security features

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

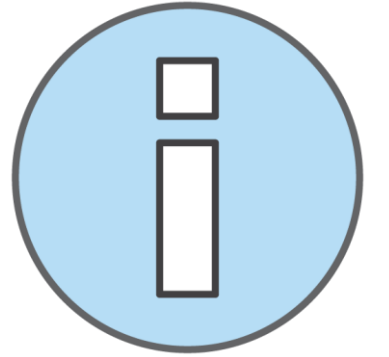
➔ You will leave this session with the foundation that you need to secure an AWS environment

AWS IAM



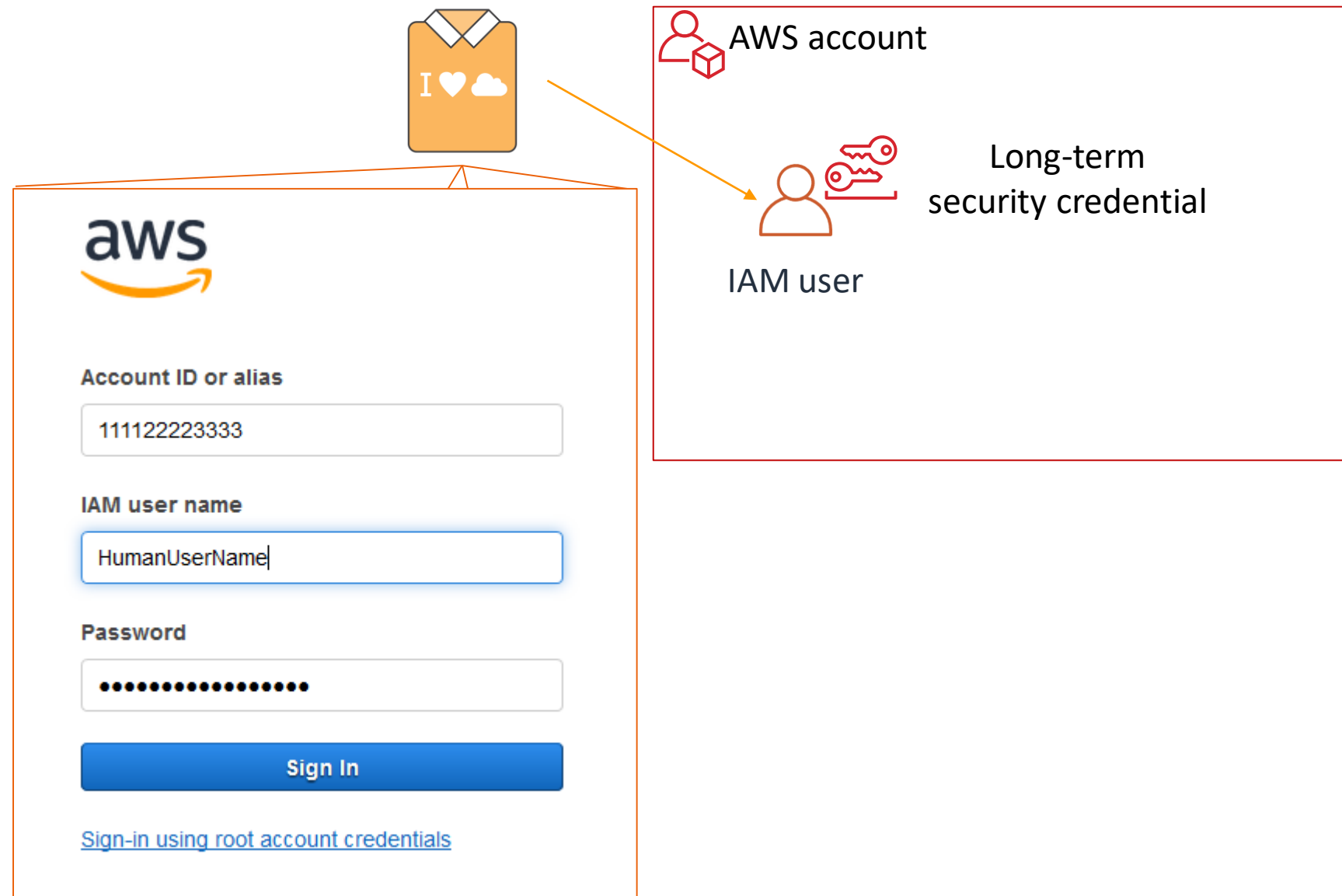
aws RE:INFORCE

AWS IAM

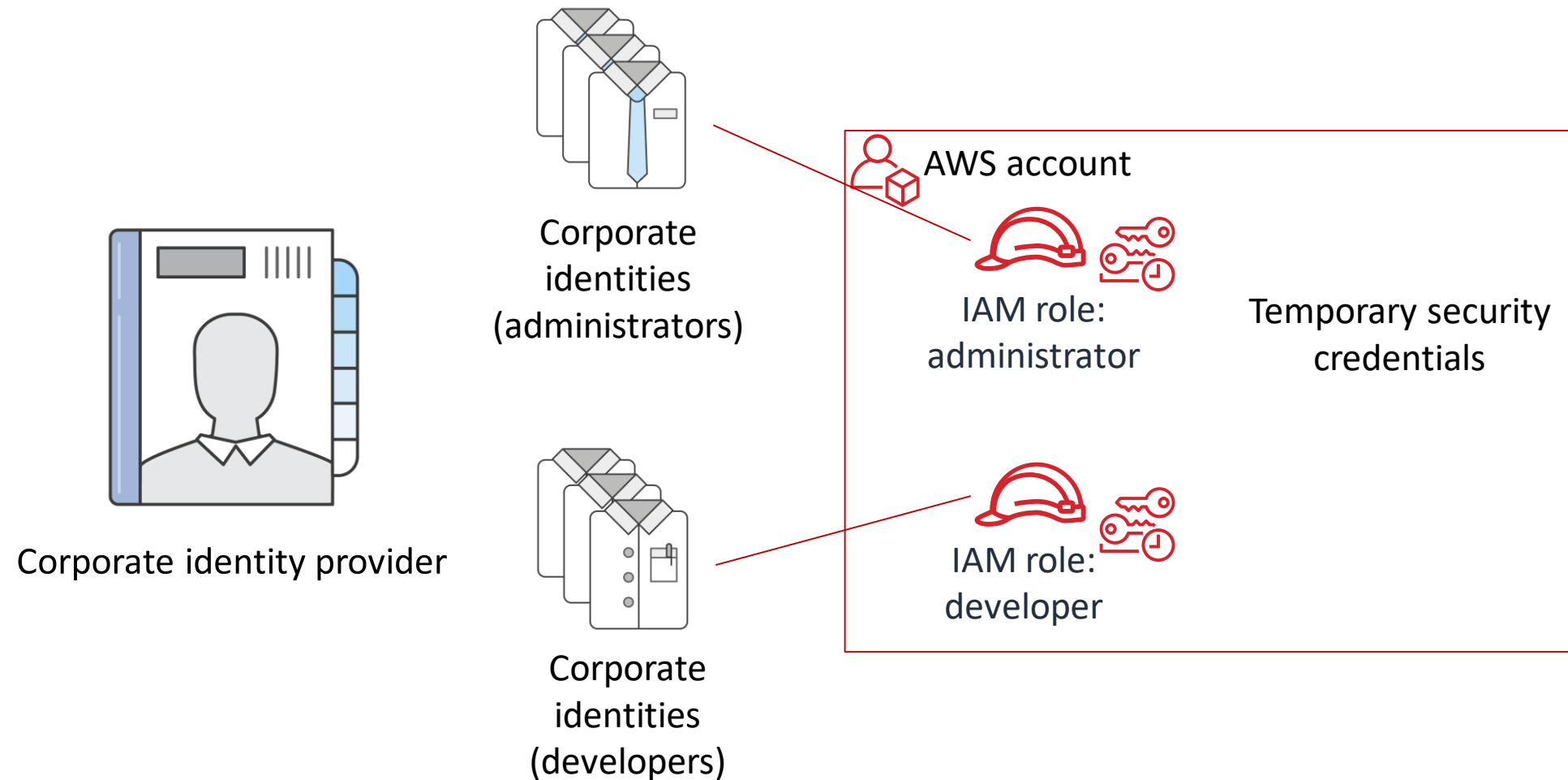


- **What it is**
 - I – Authentication: Support for human and application caller identities
 - AM – Authorization: Powerful, flexible permissions language for controlling access to cloud resources
- **Why it matters to you:** Every AWS service uses IAM to authenticate and authorize API calls
- **What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

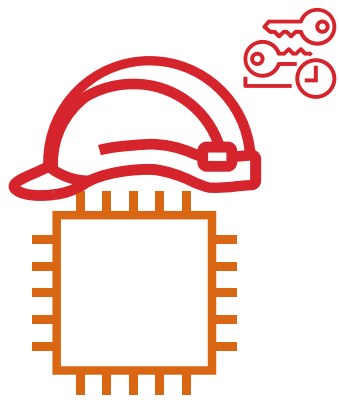
AWS identities for human callers: IAM users



AWS identities for human callers: Federated identities



AWS identities for non-human callers



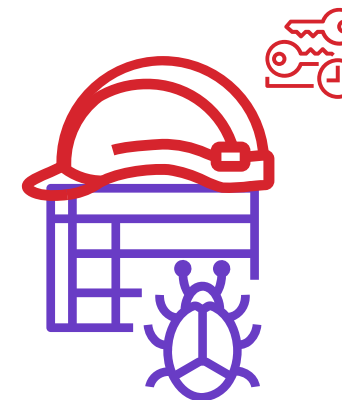
Amazon
EC2
instance



AWS 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


1


2


3

4

**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

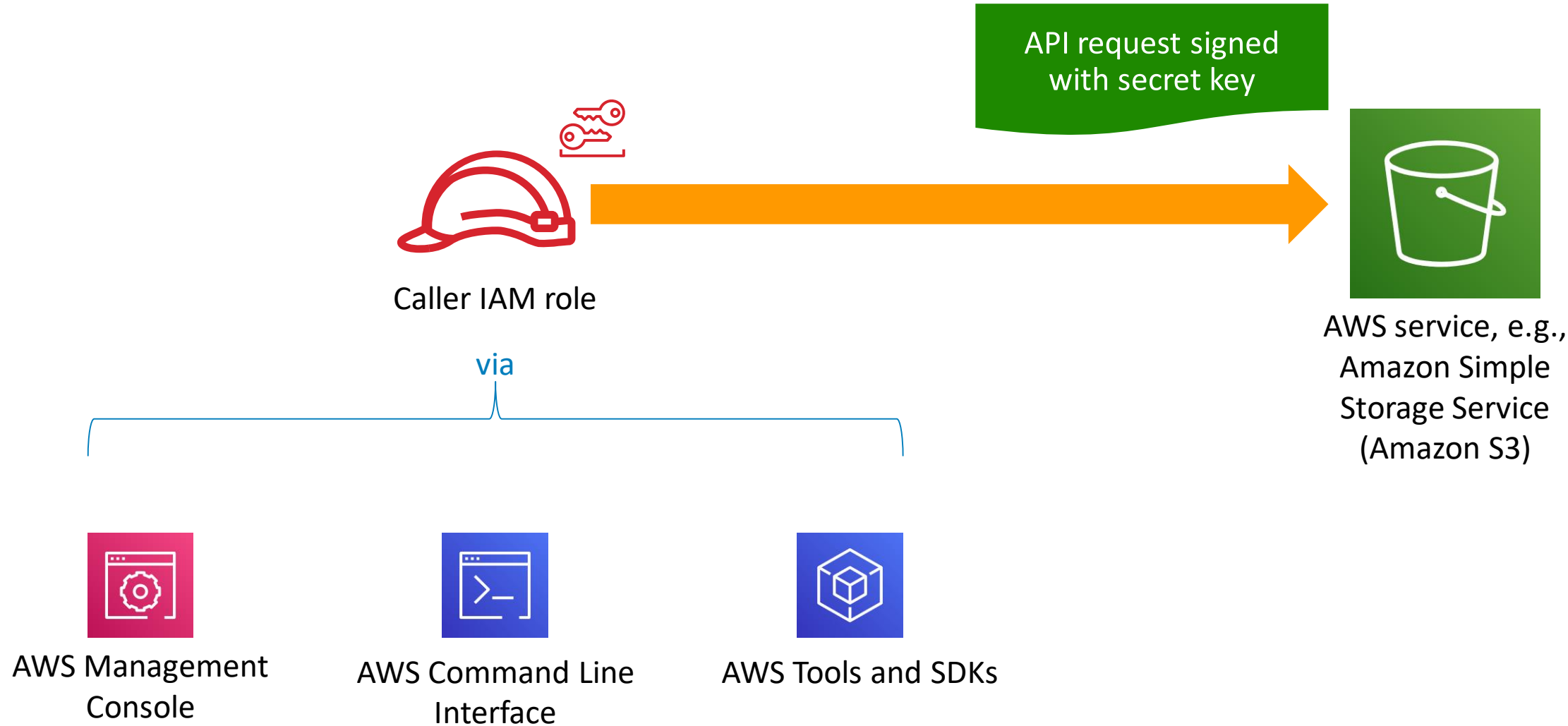
API Gateway	CodeDeploy	EKS	Kinesis	S3
AWS Backup	Comprehend	EMR	Lambda	SMS
AWS Support	Config	ElastiCache	Lex	SNS
Amplify	Connect	Elastic Beanstalk	License Manager	SWF
AppSync	DMS	Elastic Container Service	Machine Learning	SageMaker

* Required

[Cancel](#)[Next: Permissions](#)

Role for cross-account access

How an authentication works in AWS



AWS-managed policies for common sets of permissions

Create role

1234

▼ Attach permissions policies

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

Create policy

Filter policies ▼ Search

Showing 512 results

	Policy name ▼	Used as	Description
<input type="checkbox"/>	▶ AdministratorAccess	Permissions policy (1)	Provides full access to AWS services a...
<input type="checkbox"/>	▶ AlexaForBusinessDeviceSetup	None	Provide device setup access to AlexaF...
<input type="checkbox"/>	▶ AlexaForBusinessFullAccess	None	Grants full access to AlexaForBusines...
<input type="checkbox"/>	▶ AlexaForBusinessGatewayExecution	None	Provide gateway execution access to ...
<input type="checkbox"/>	▶ AlexaForBusinessNetworkProfileServicePolicy	None	This policy enables Alexa for Business ...
<input type="checkbox"/>	▶ AlexaForBusinessReadOnlyAccess	None	Provide read only access to AlexaForB...
<input type="checkbox"/>	▶ 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

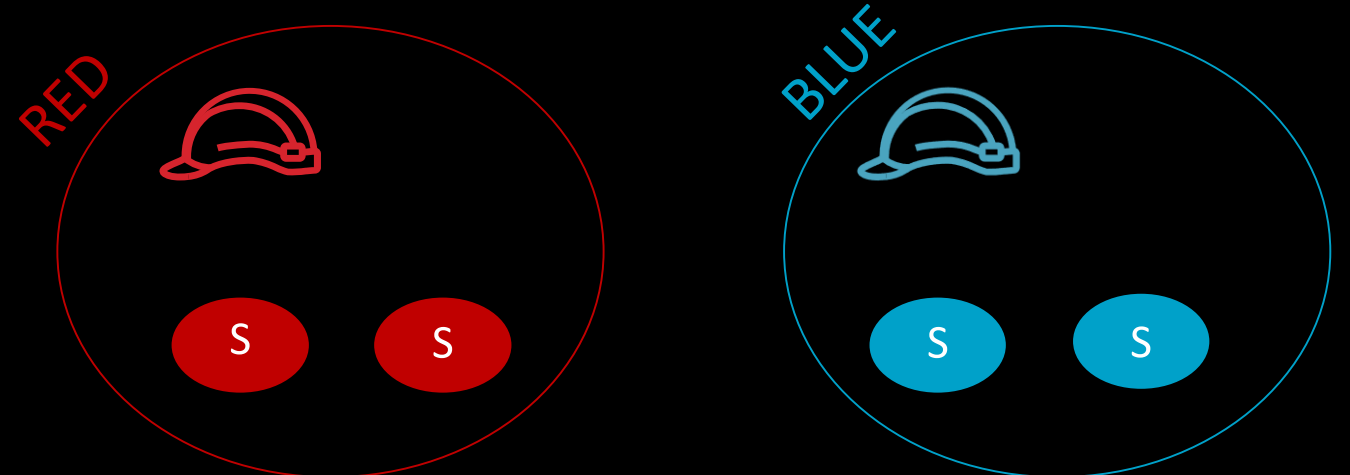
This is an Amazon Resource Name (ARN);
All AWS services use them, and they follow this format

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

- ☐ 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 its own set of actions, resources, and condition keys. This topic describes how the elements provided for each service are organized.

Instructions for how to read the
table for each service

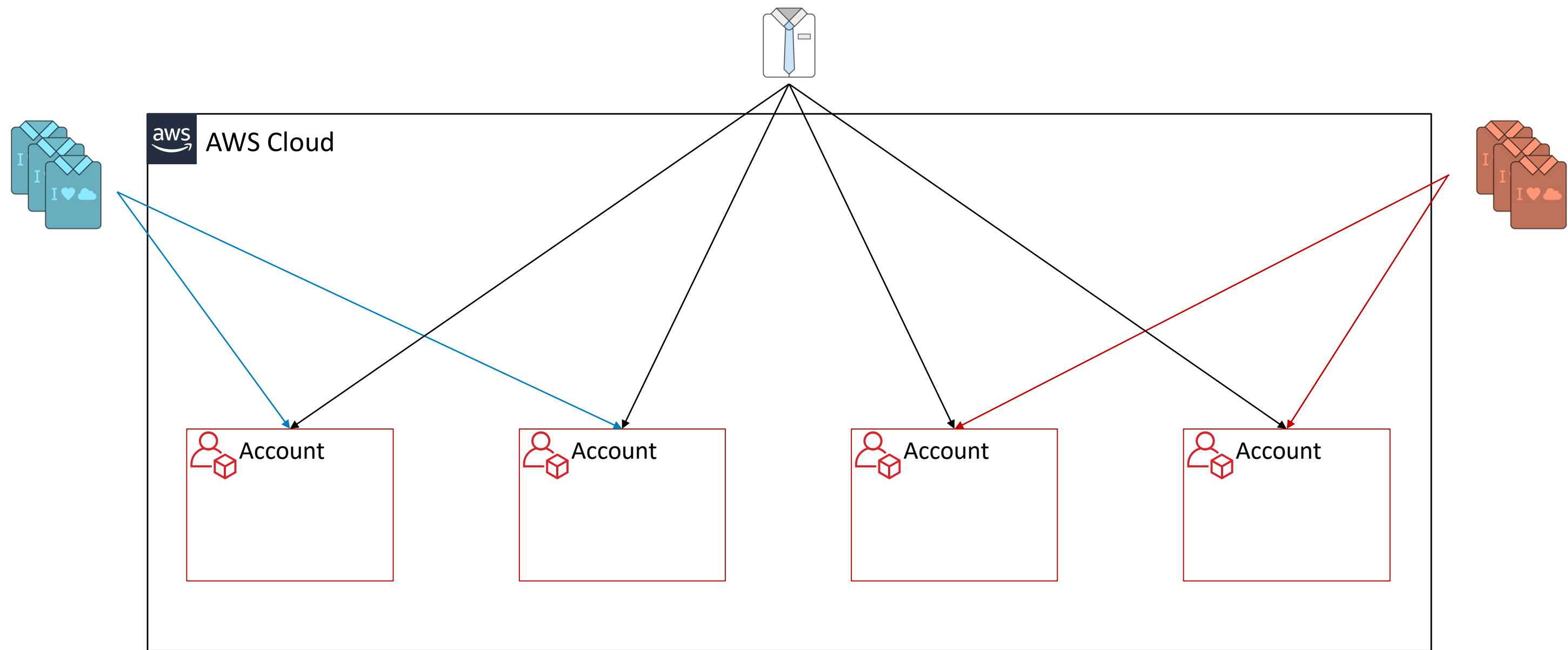
How to Read the Tables

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

The Actions Table

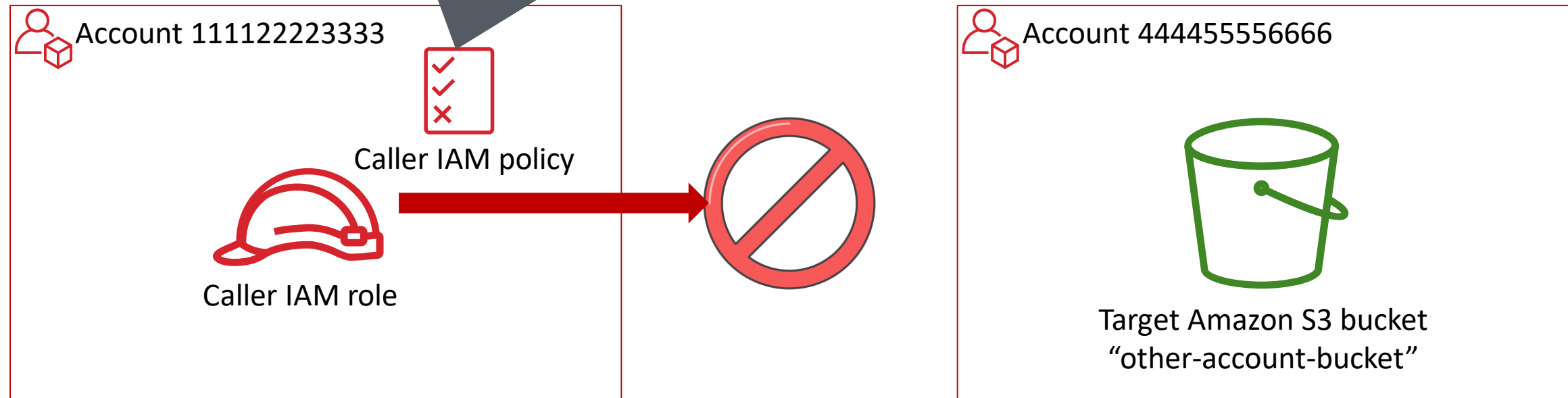
The **Actions** table lists all the actions that you can use in an IAM policy statement's Action element. Not all API operations that are defined by a service can be used as an action in an IAM policy. In addition, a service might define some actions that don't directly correspond to an API

IAM in an AWS enterprise environment



Working across AWS account boundaries

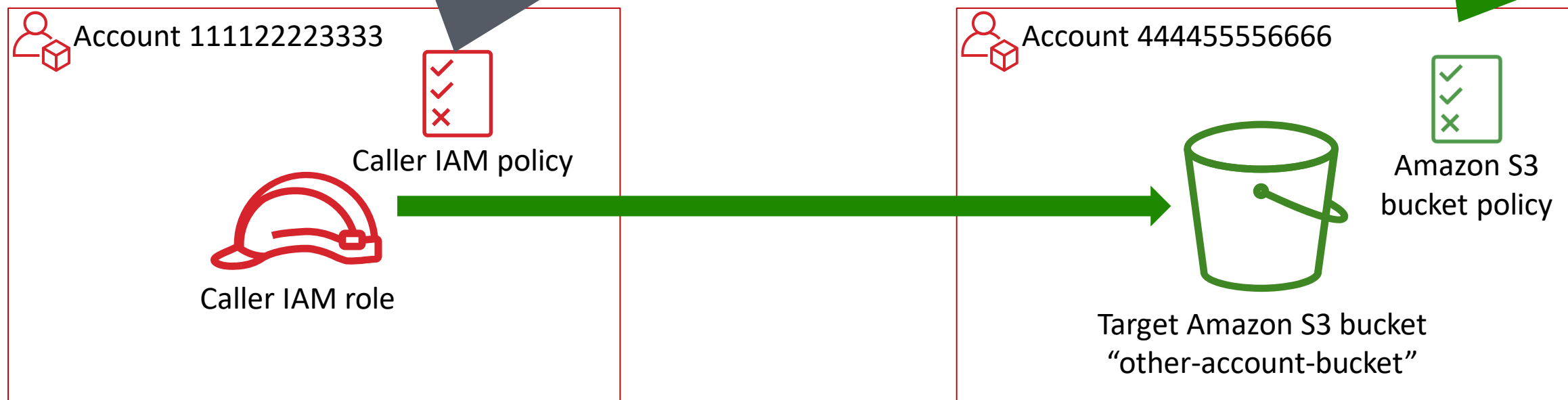
```
{  
  "Effect": "Allow",  
  "Action": "s3:GetObject",  
  "Resource": "arn:aws:s3:::other-account-bucket/*"  
}
```



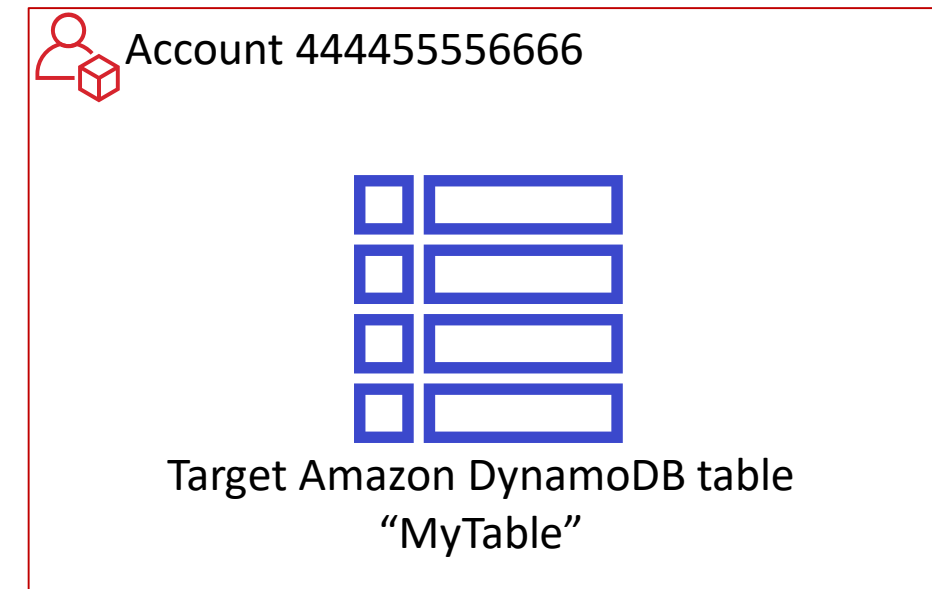
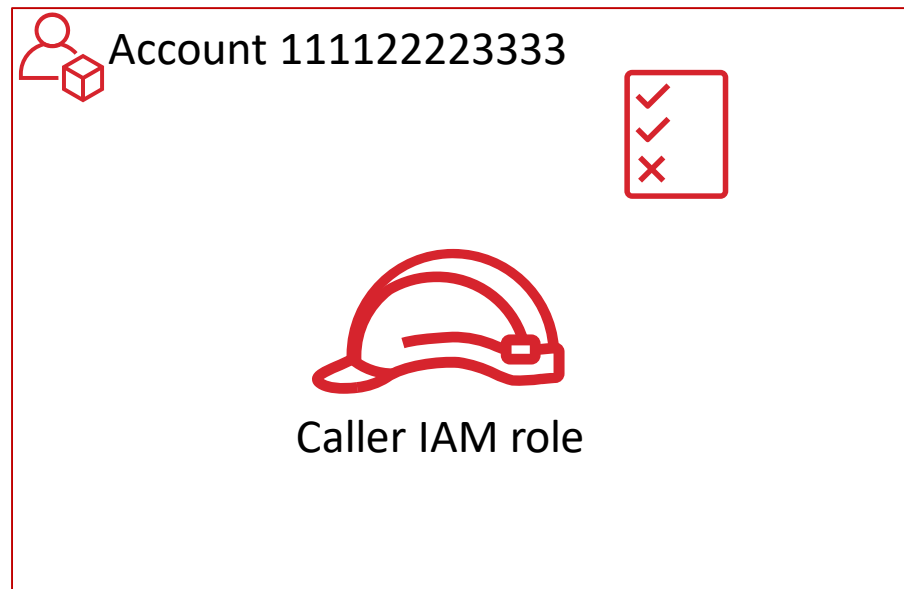
Working across AWS account boundaries

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

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

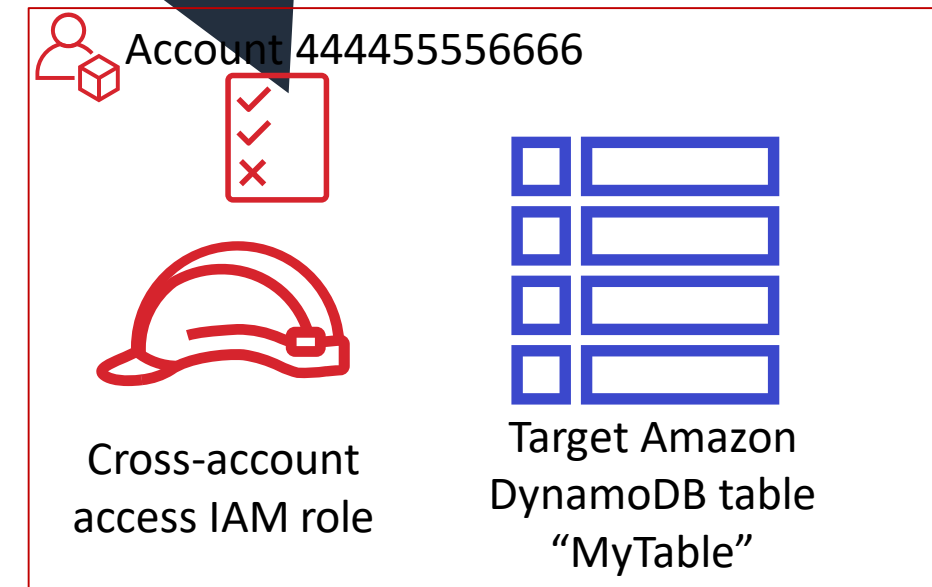
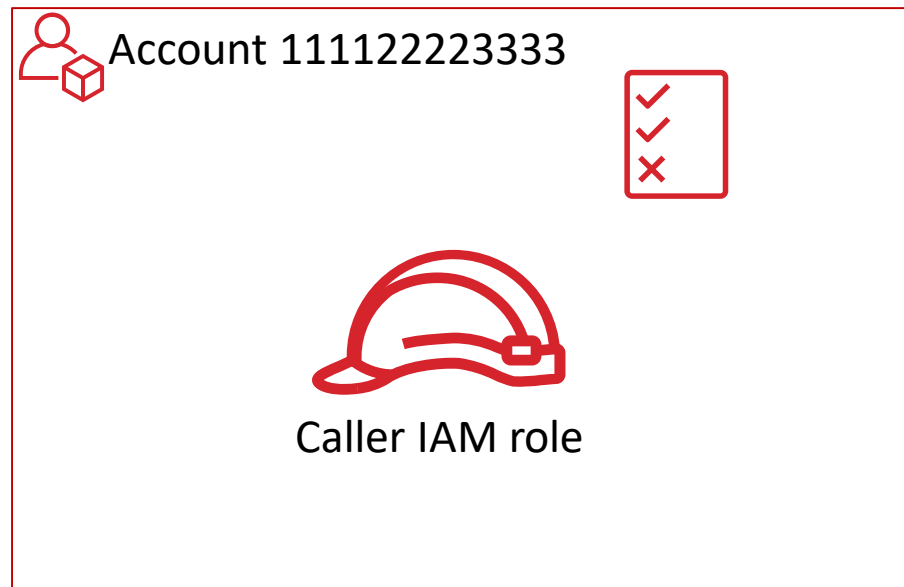


Working across AWS account boundaries




Working across AWS account boundaries

```
{  
  "Effect": "Allow",  
  "Action": "dynamodb:GetItem",  
  "Resource": "arn:aws:dynamodb:us-west-2:444455556666:table/MyTable"  
}
```



Working across AWS account boundaries

```
{  
  "Effect": "Allow",  
  "Action": "dynamodb:GetItem",  
  "Resource": "arn:aws:dynamodb:us-west-2:444455556666:table/MyTable"  
}
```

 Account 111122223333



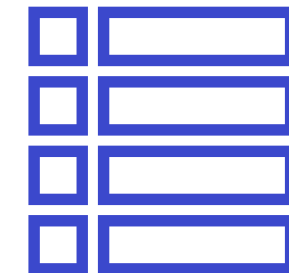
Caller IAM role

```
{  
  "Effect": "Allow",  
  "Action": "sts:AssumeRole",  
  "Principal": {  
    "AWS": "arn:aws:iam::111122223333:root"  
  }  
}
```

 Account 444455556666



Cross-account
access IAM role




Target Amazon
DynamoDB table
"MyTable"

Working across AWS account boundaries

```
{  
  "Effect": "Allow",  
  "Action": "sts:AssumeRole",  
  "Resource": "arn:aws:iam::444455556666:role/CrossAccountAccess"  
}
```

```
{  
  "Effect": "Allow",  
  "Action": "dynamodb:GetItem",  
  "Resource": "arn:aws:dynamodb:us-west-2:444455556666:table/MyTable"  
}
```

 Account 111122223333

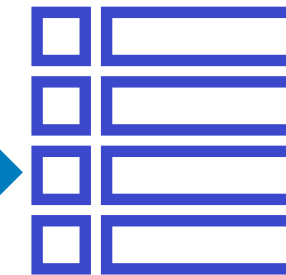


Caller IAM role

 Account 444455556666



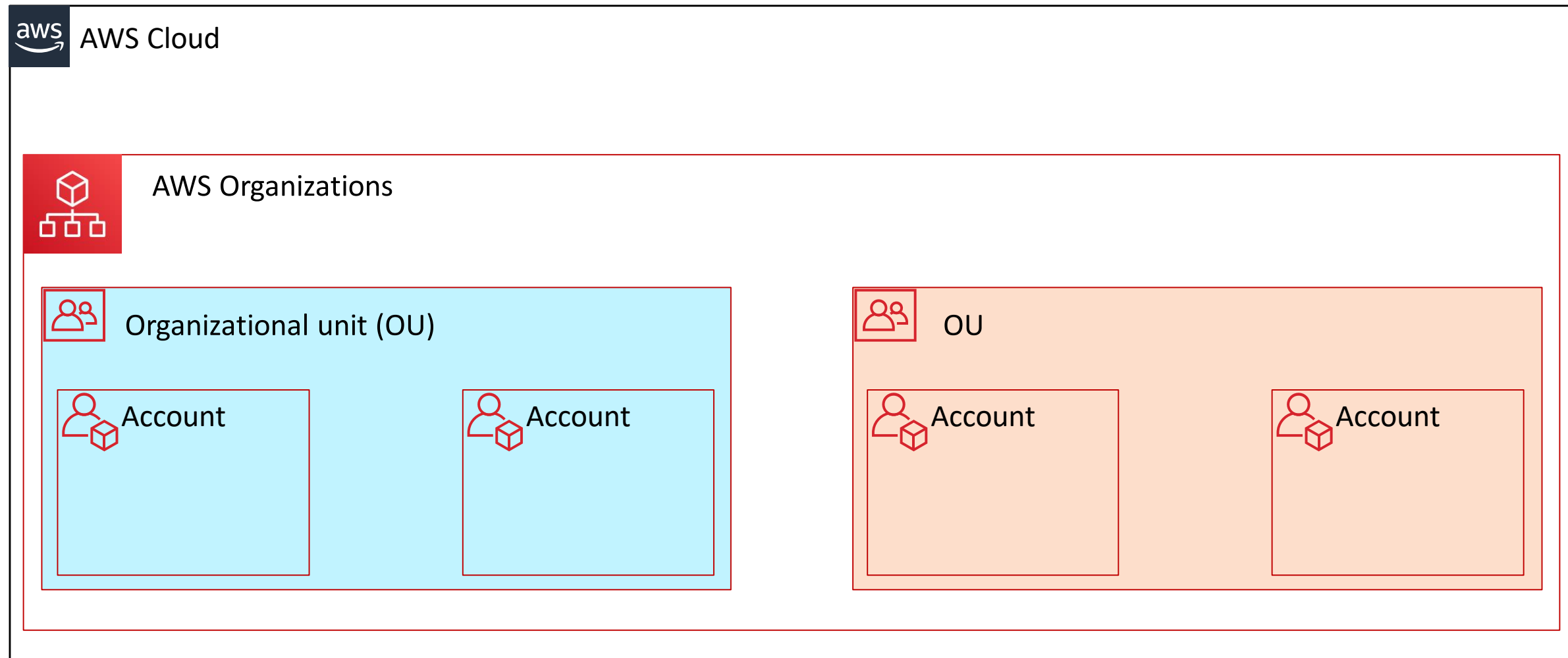
Cross-account
access IAM role



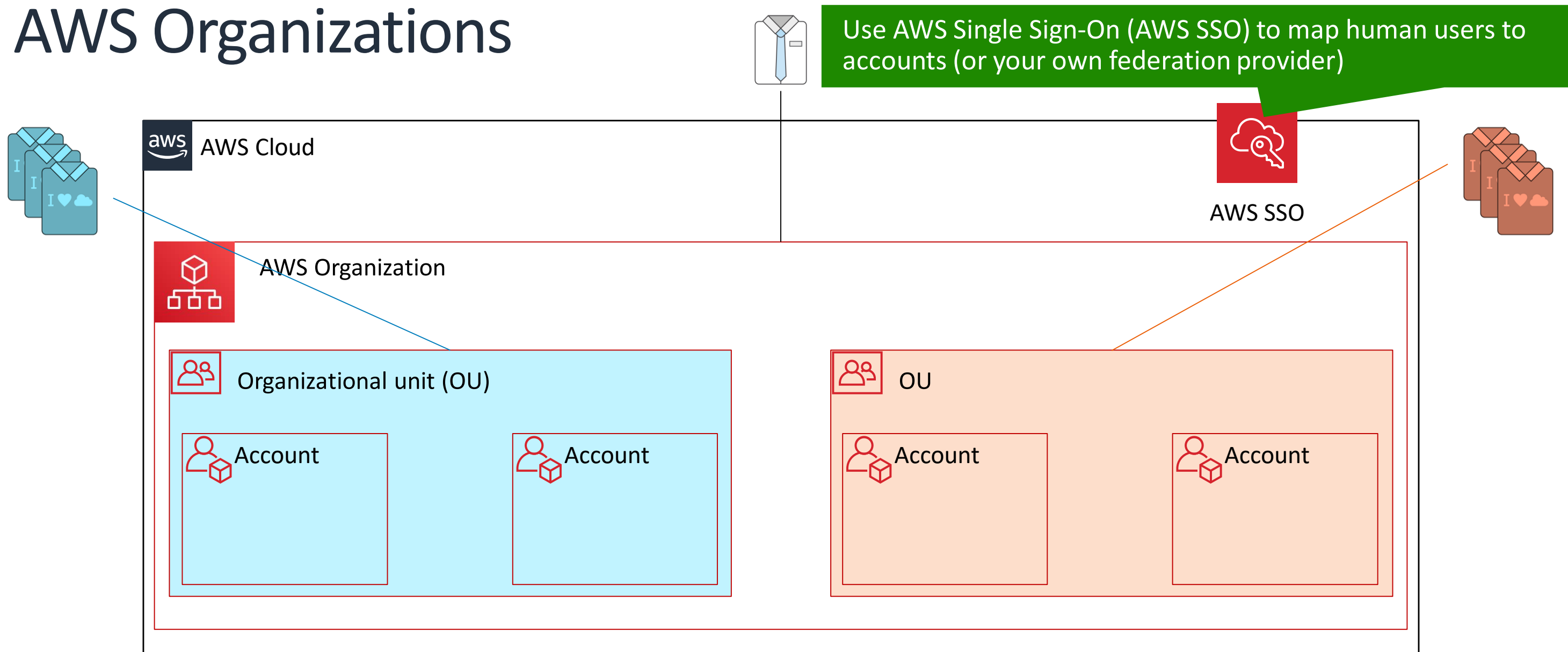
Target Amazon
DynamoDB table
"MyTable"

```
{  
  "Effect": "Allow",  
  "Action": "sts:AssumeRole",  
  "Principal": {  
    "AWS": "arn:aws:iam::111122223333:root"  
  }  
}
```


Managing multi-account environments with AWS Organizations

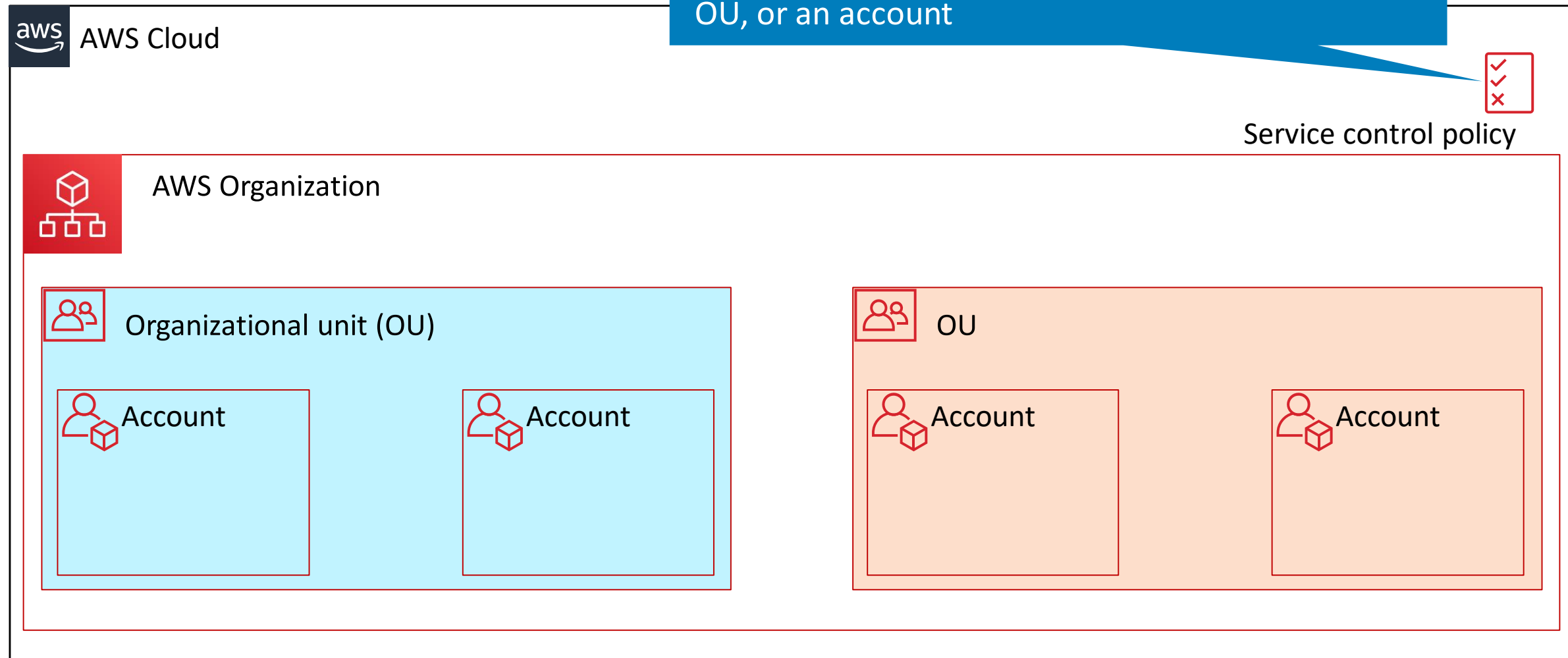


Managing multi-account environments with AWS Organizations

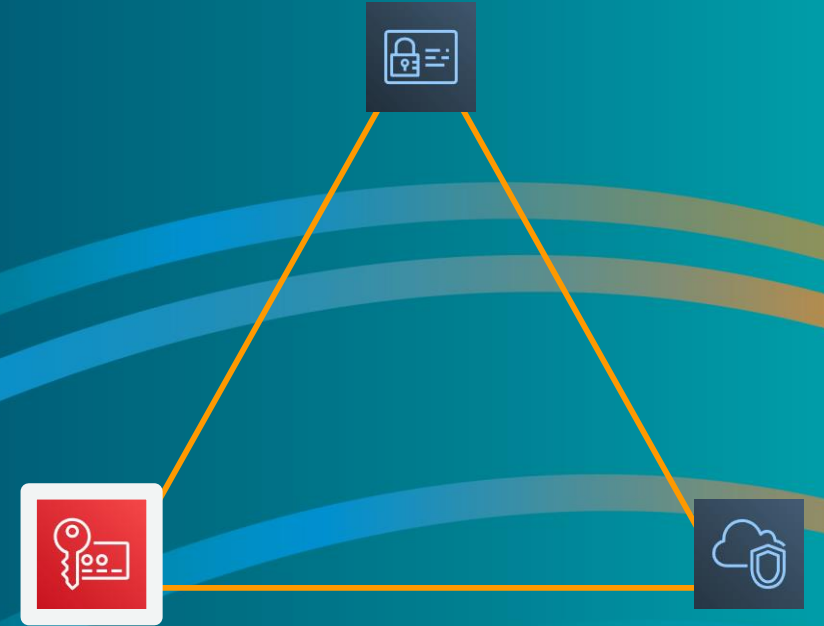


AWS Organizations provides guardrails for IAM

Use AWS Organizations service control policies to bound access throughout AWS Organizations, an OU, or an account

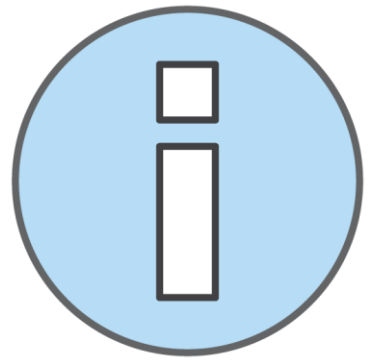


AWS KMS



aws RE:INFORCE

AWS KMS



- **What it is:** AWS-managed encryption and 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
 - 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 okay

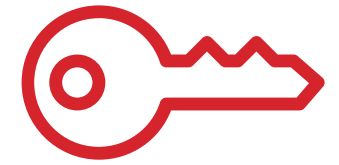
The mechanics of an AWS KMS key

For encrypting individual pieces of data ($\leq 4\text{KB}$)

- `KMS.Encrypt("hello world")` \rightarrow `AQICAHiwKPHZcwilv....`
- `KMS.Decrypt("AQICAHiwKPHZcwilv....")` \rightarrow `"hello world"`

For encrypting application data, use envelope encryption

- `KMS.GenerateDataKey` \rightarrow 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)` \rightarrow **plaintext**DataKey
 - Then decrypt the data with the **plaintext** symmetric key



AWS KMS key

EncryptedDataKey:
AQIDAHiwKPHZcwiIv+V4760rokzKM1vwo0M902D5yV
e3tqrBtwGBaaY6AwTrEcsjY0gTN8J8AAAFjB8Bgk...

EncryptedPayload:
AQICAHiwKPHZcwiIv+V4760rokzKM1vwo0M902D5yV
e3tqrBtwGEZdK9s3Sx1UE11PSPSadGAAAAaTBnBgk...

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

1 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 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

Type to search

arn:aws:kms:us-east-1:123456789012:key/84d3eb0c-b920-4f21-b316-4d27b85f07a9

aws/s3

Amazon S3 manages the encryption key

Encrypting the easy way with AWS service integrations

Create bucket

1 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 charge.

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

► Advanced options

Search: Type to search

arn:aws:kms:us-east-1:123456789012:key/84d3eb0c-b920-4f21-b316-4d27b85f07a9

aws/s3

IAM permissions for AWS KMS keys

Question: What happens here?

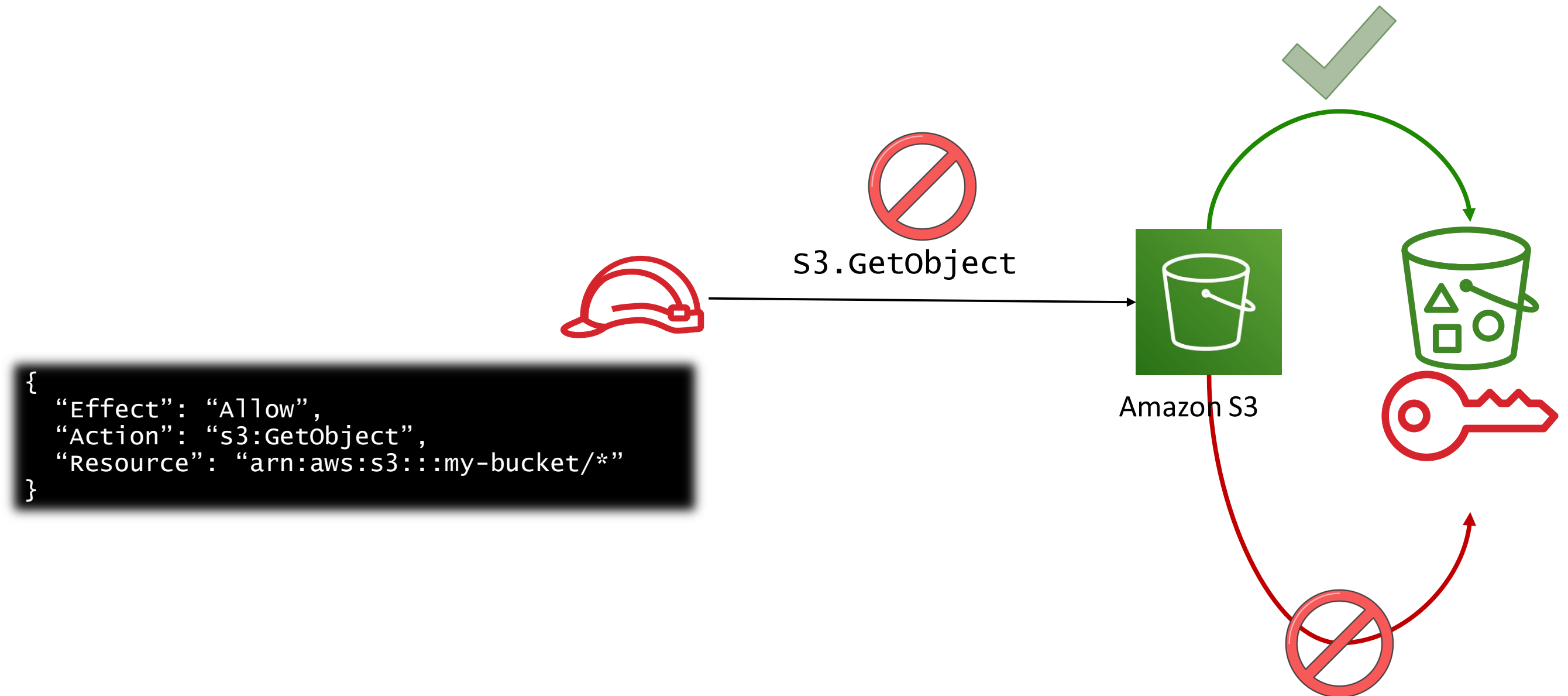
```
{  
  "Effect": "Allow",  
  "Action": "s3:GetObject",  
  "Resource": "arn:aws:s3:::my-bucket/*"  
}
```



s3.GetObject



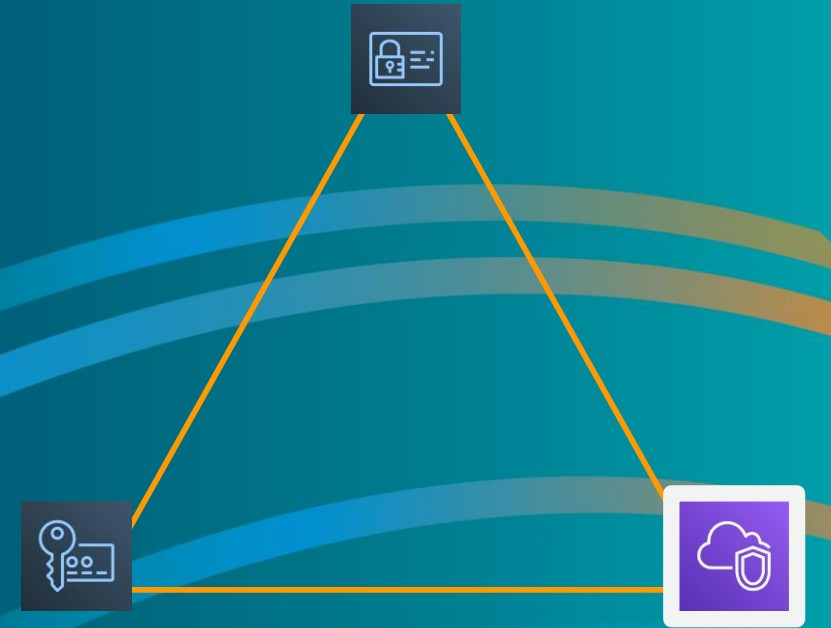
IAM permissions for AWS KMS keys



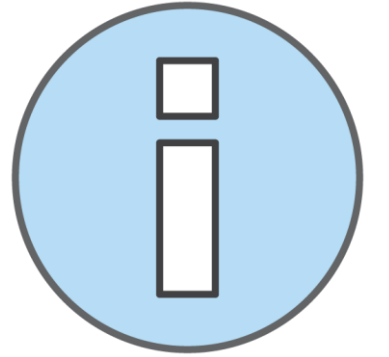
IAM permissions for AWS KMS keys



Amazon VPC



Amazon VPC



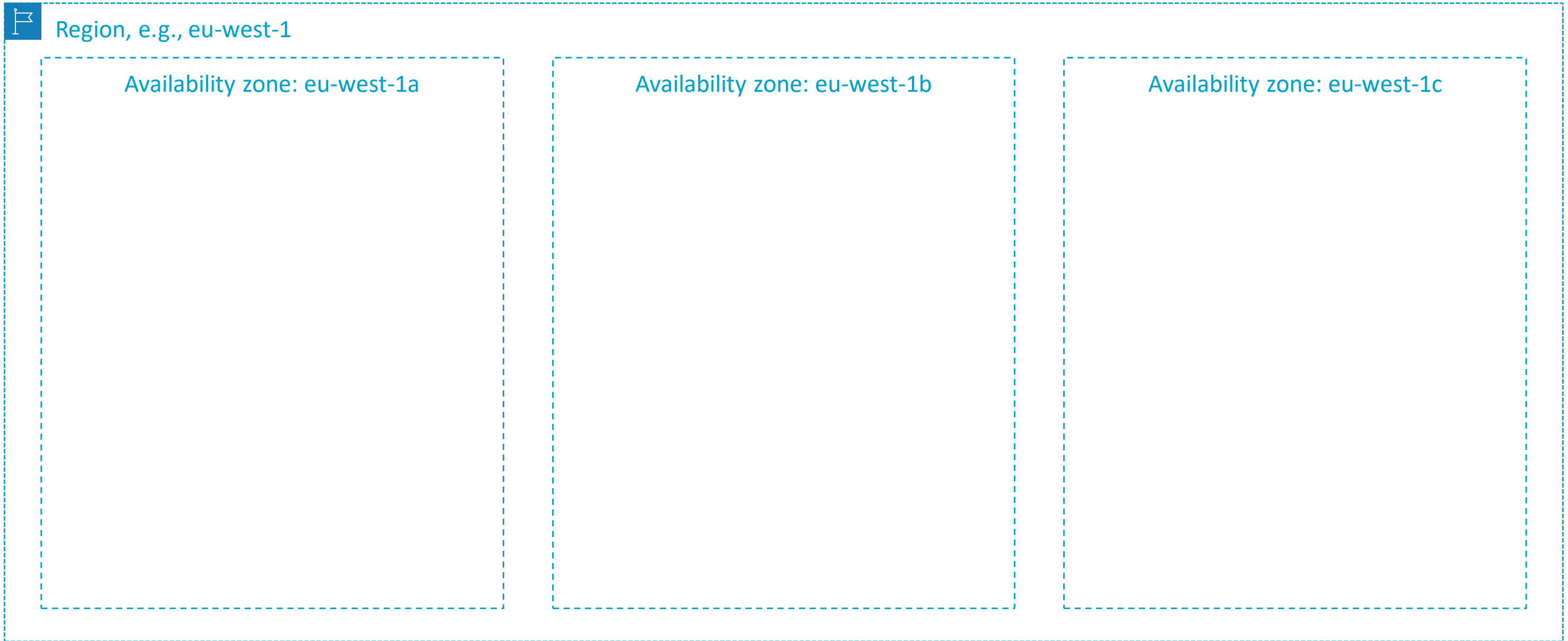
- **What it is:** Your virtual data center in the cloud, i.e., the network for your cloud infrastructure
- **Why it matters to you:** When you deploy cloud infrastructure, your VPC is the network that provides connectivity to and from that infrastructure
- **What builders need to know**
 - VPC core concepts: subnets and security groups
 - Routing basics in Amazon VPC
 - Private connectivity capabilities

What a VPC is and what goes in it

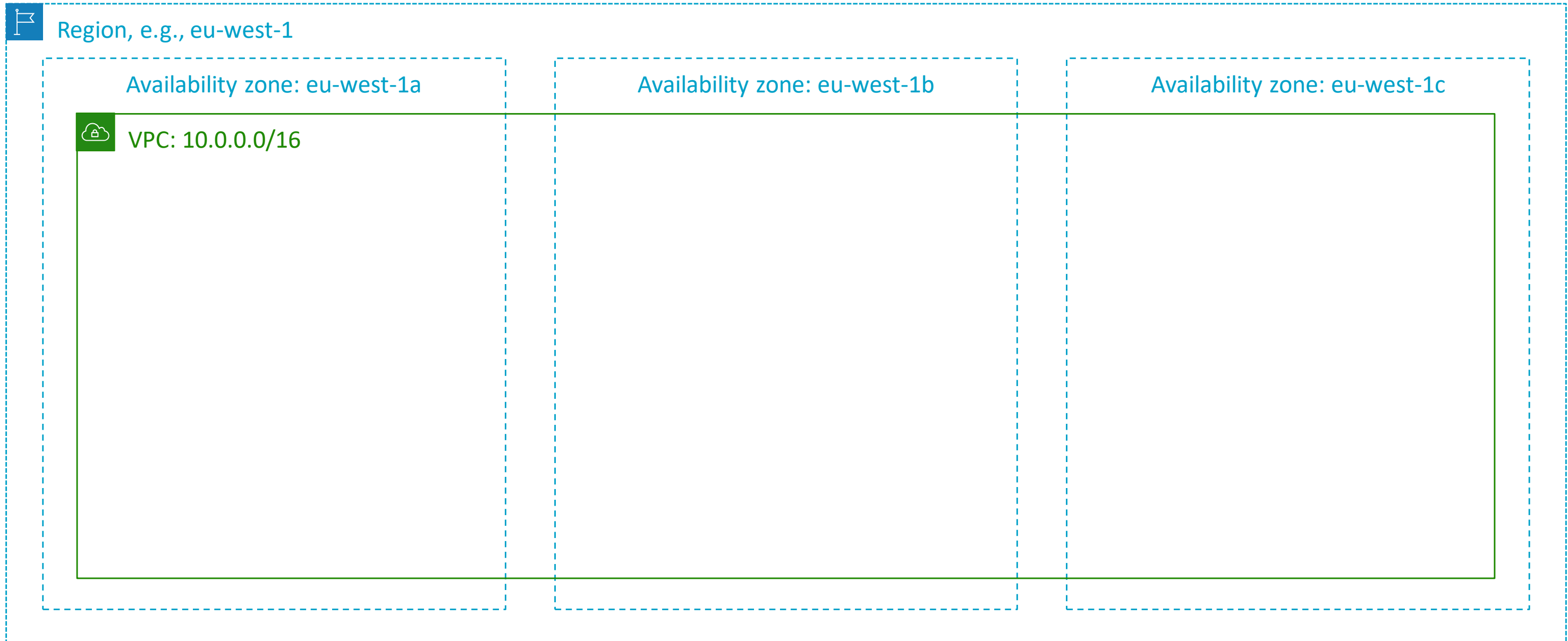


Region, e.g., eu-west-1

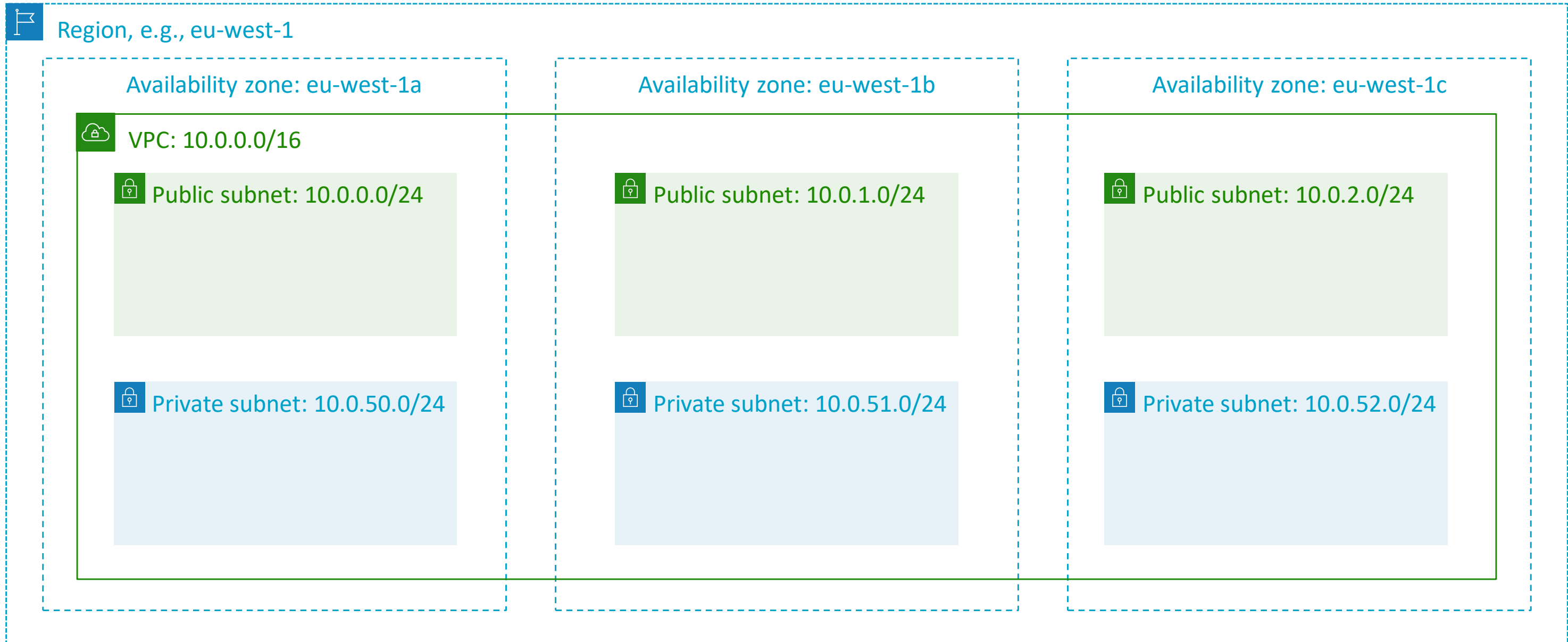
What a VPC is and what goes in it



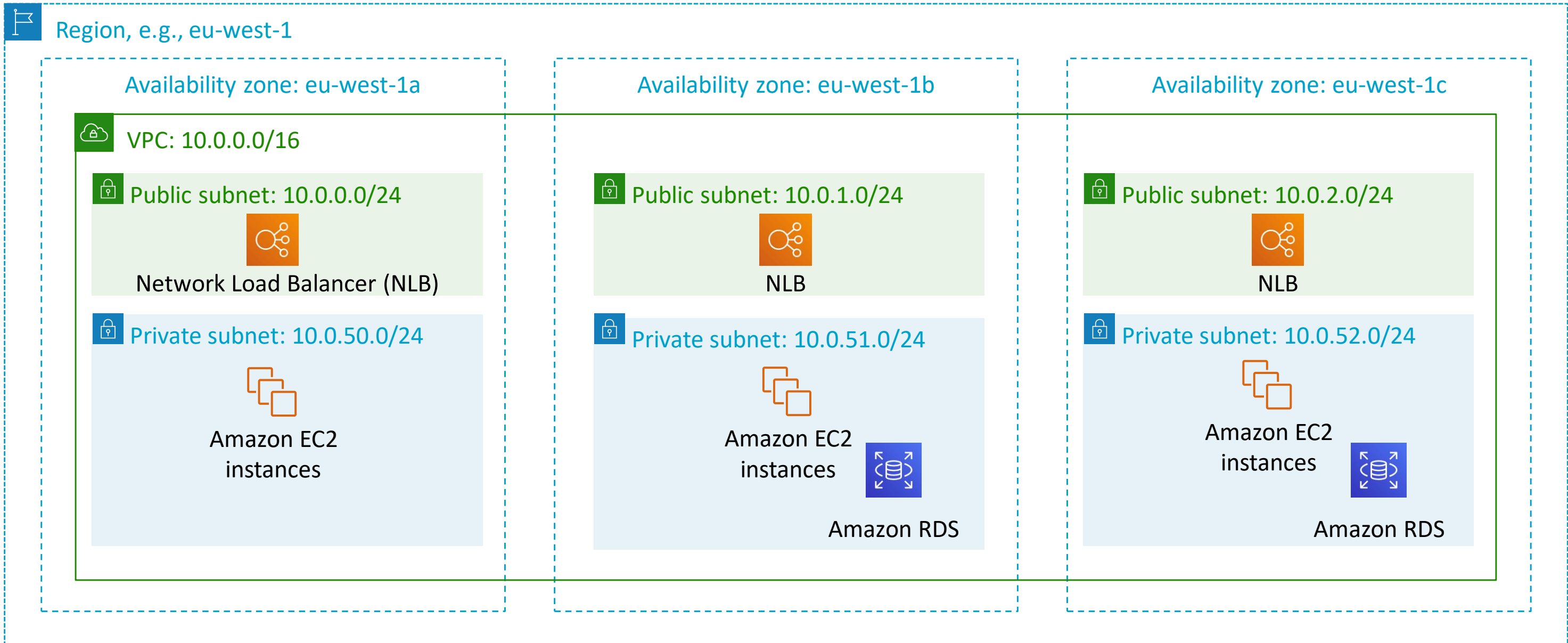
What a VPC is and what goes in it



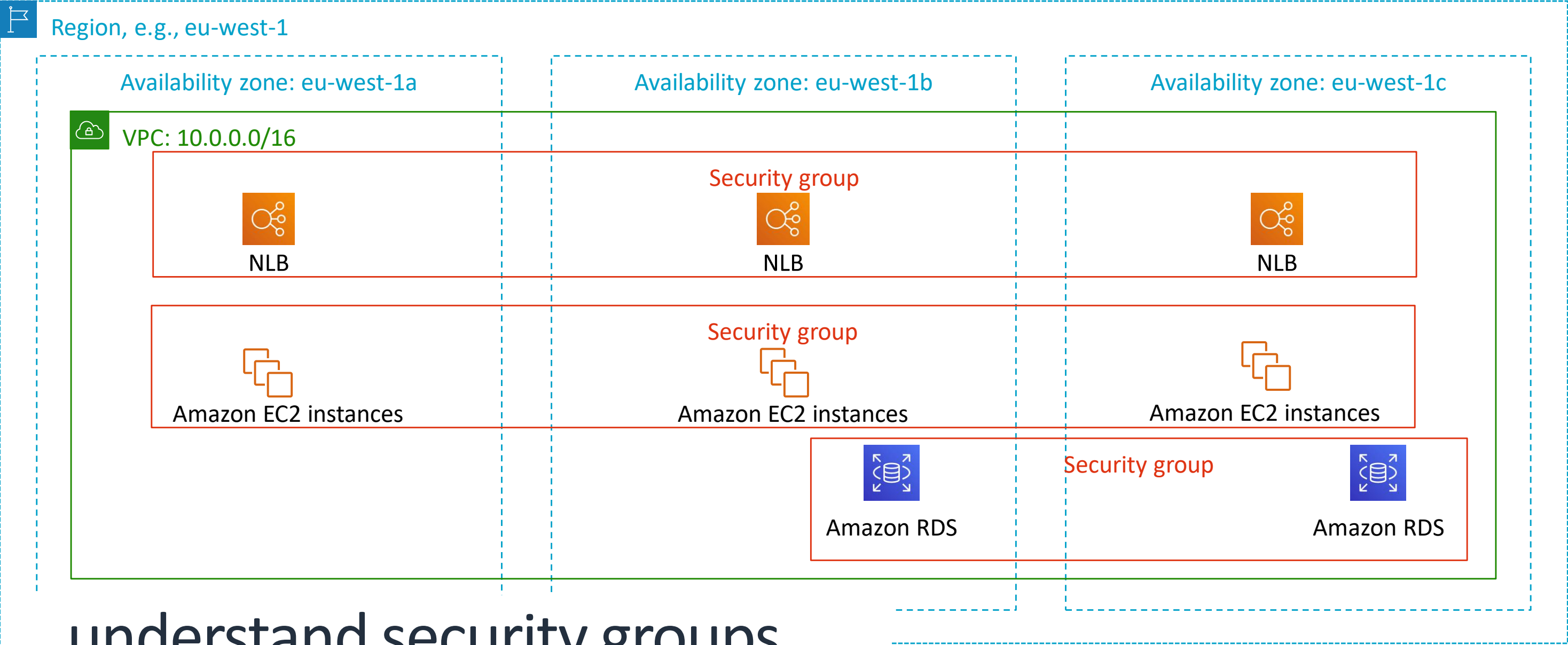
What a VPC is and what goes in it



What a VPC is and what goes in it

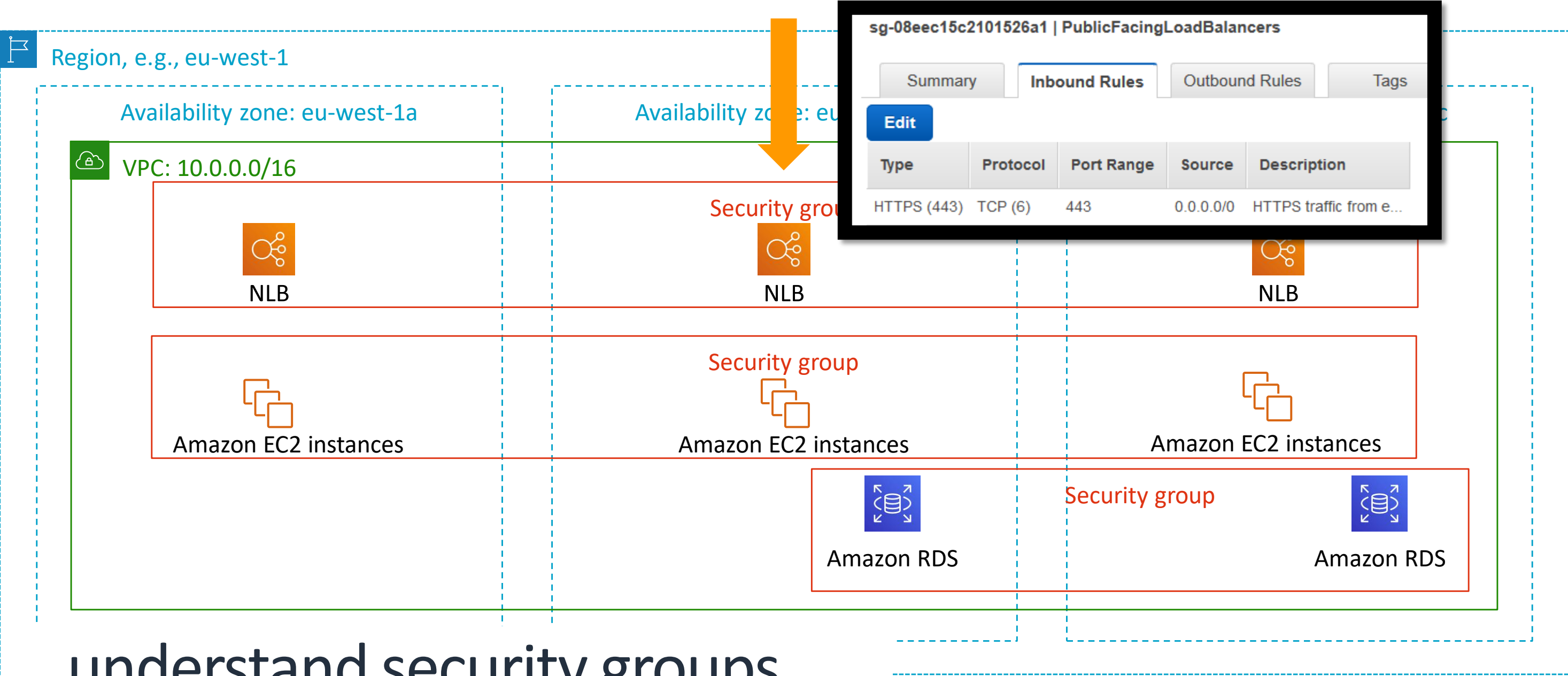


If you understand nothing else about Amazon VPC...



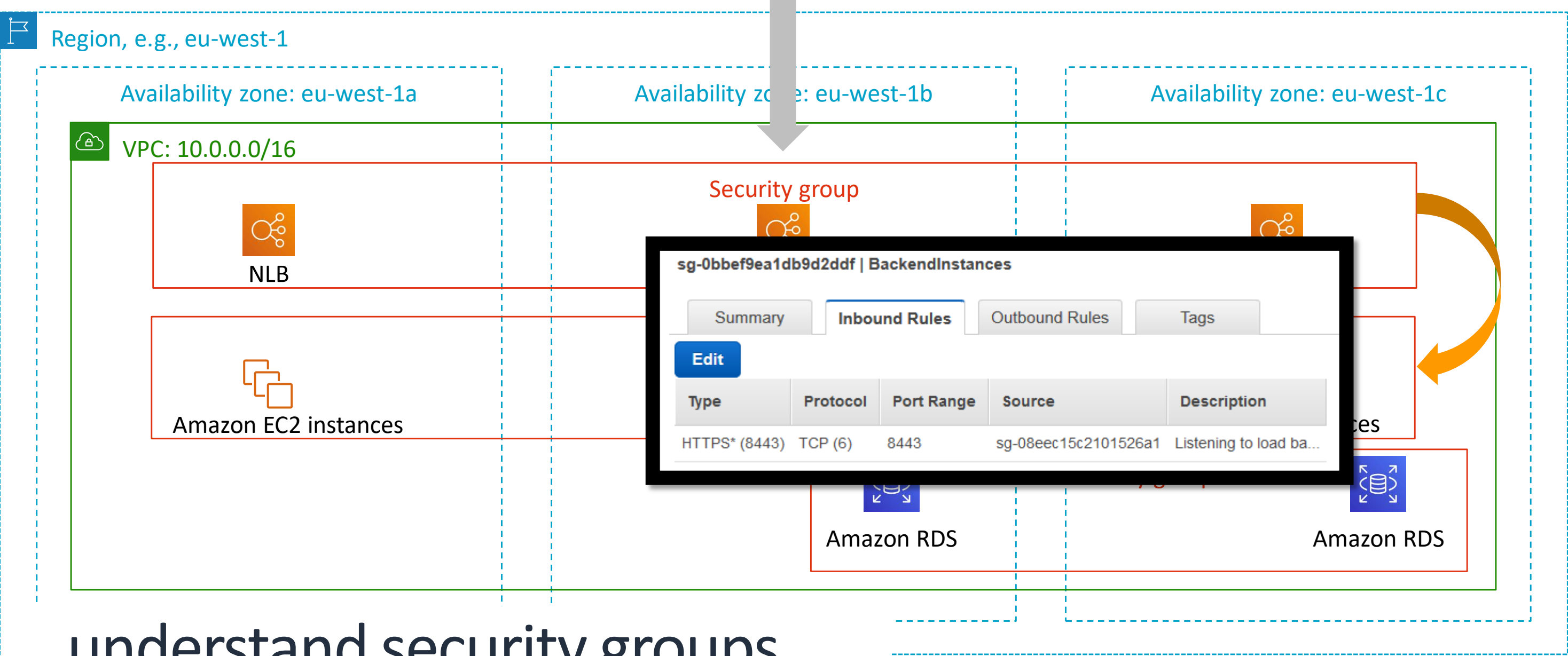
...understand security groups

If you understand nothing else about Amazon VPC...



...understand security groups

If you understand nothing else about Amazon VPC...



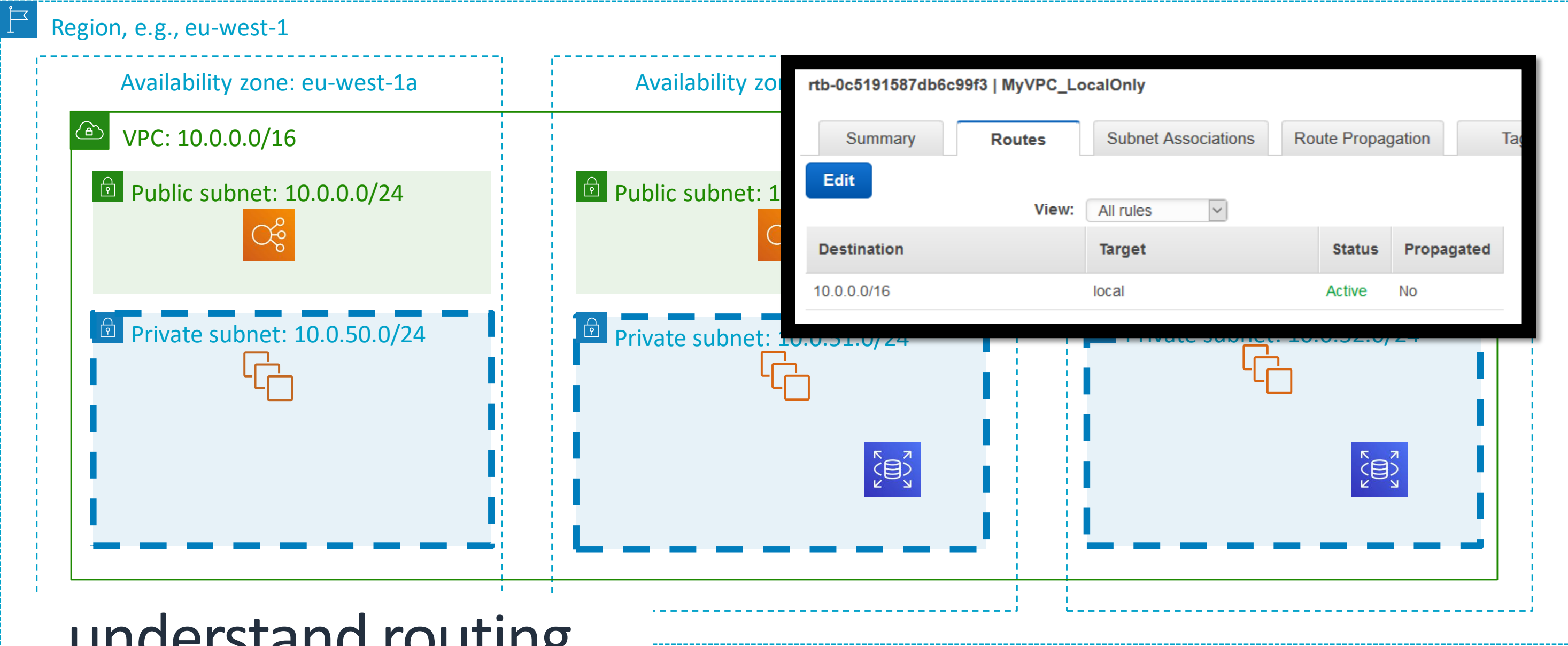
...understand security groups

If you understand nothing else about Amazon VPC...



...understand security groups

If you understand only 2 things about Amazon VPC...



If you understand only 2 things about Amazon VPC...



Region, e.g., eu-west-1

Availability zone: eu-west-1a

VPC: 10.0.0.0/16

Public subnet: 10.0.0.0/24

Private subnet: 10.0.50.0/24

Availability zone: eu-west-1b

Public subnet: 10.0.1.0/24

Private

Availability zone: eu-west-1c

Public subnet: 10.0.2.0/24



Internet gateway

rtb-0739ca59a93e083cc | MyVPC_InternetGateway

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

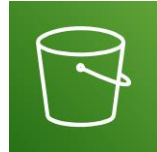
Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-0ee4a7948173d8ec2	Active	No

...understand routing

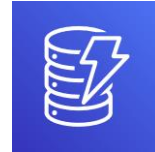
AWS resources **not** in your VPC



Region, e.g., eu-west-1



Amazon S3



Amazon
DynamoDB



Amazon
API Gateway



Amazon
CloudWatch

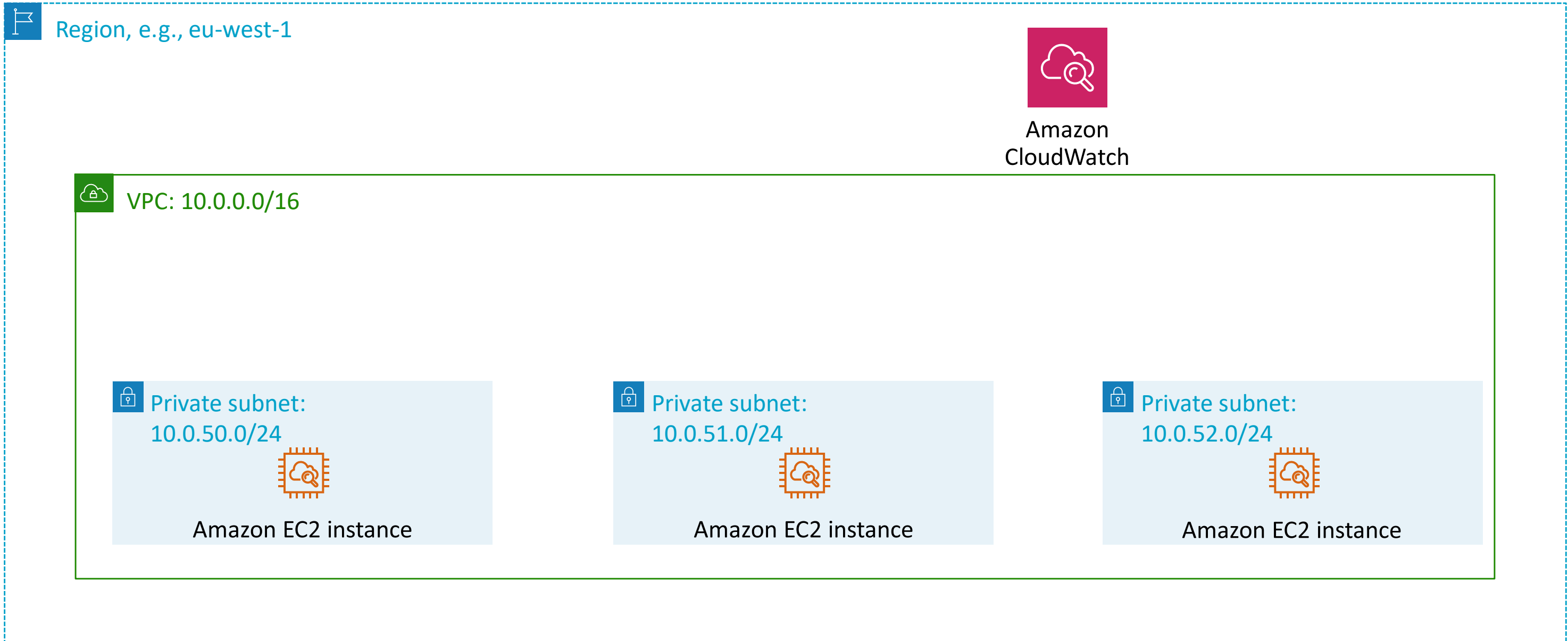
...and many others



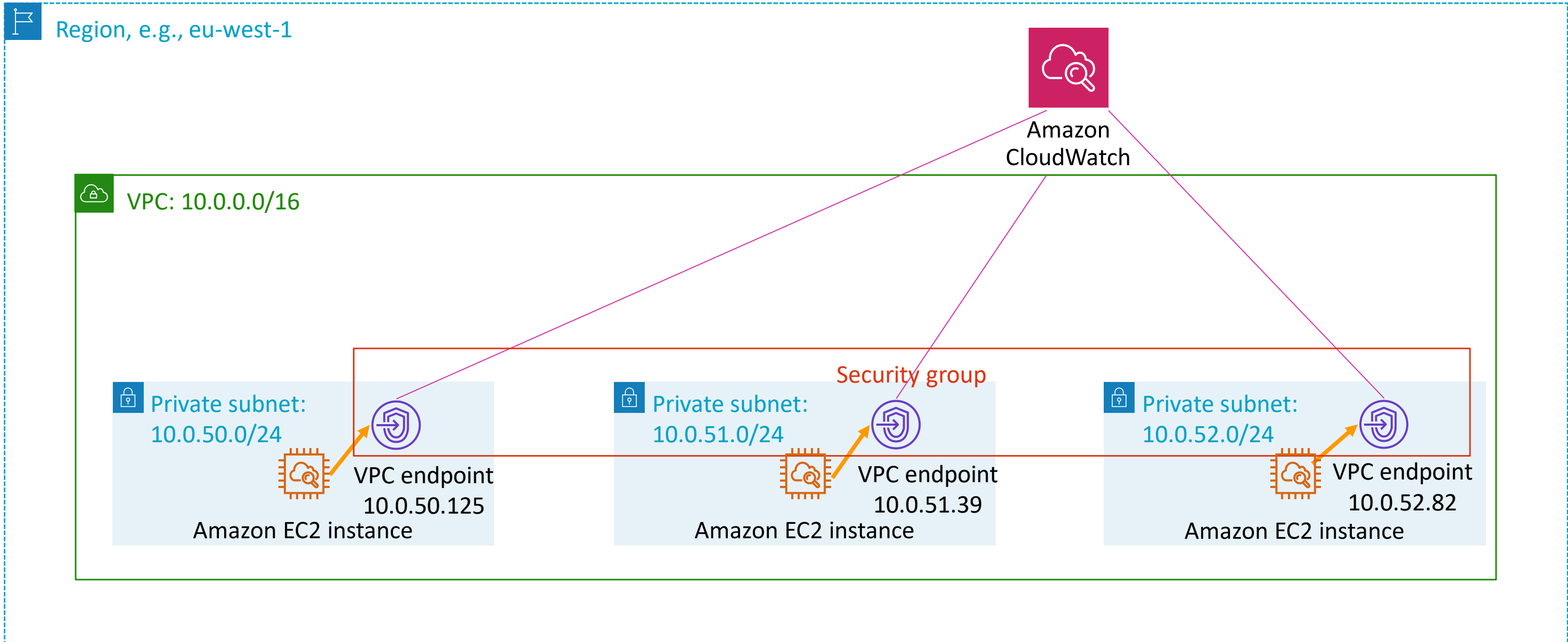
VPC: 10.0.0.0/16

```
$ dig logs.us-east-2.amazonaws.com +short  
52.95.18.51
```

VPC endpoints: Private connectivity to AWS services



VPC endpoints: Private connectivity to AWS services



VPC endpoints: Network as security perimeter

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "logs:*",
  "Resource": "arn:aws:logs:us-east-2:111122223333:*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalOrgID": "o-a1b2c3"
    }
  }
}
```

In English: From this network, allow only callers from my AWS Organizations, and allow only log groups from my account



Amazon CloudWatch



Amazon VPC endpoint policy



Private subnet:
10.0.50.0/24



VPC endpoint
10.0.50.125

Amazon EC2 instance



Private subnet:
10.0.51.0/24



VPC endpoint
10.0.51.39

Amazon EC2 instance



Private subnet:
10.0.52.0/24



VPC endpoint
10.0.52.82

Amazon EC2 instance

Wrapping up

aws RE:INFORCE

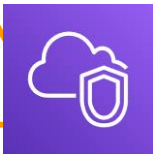
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learn a few patterns, secure everything in AWS

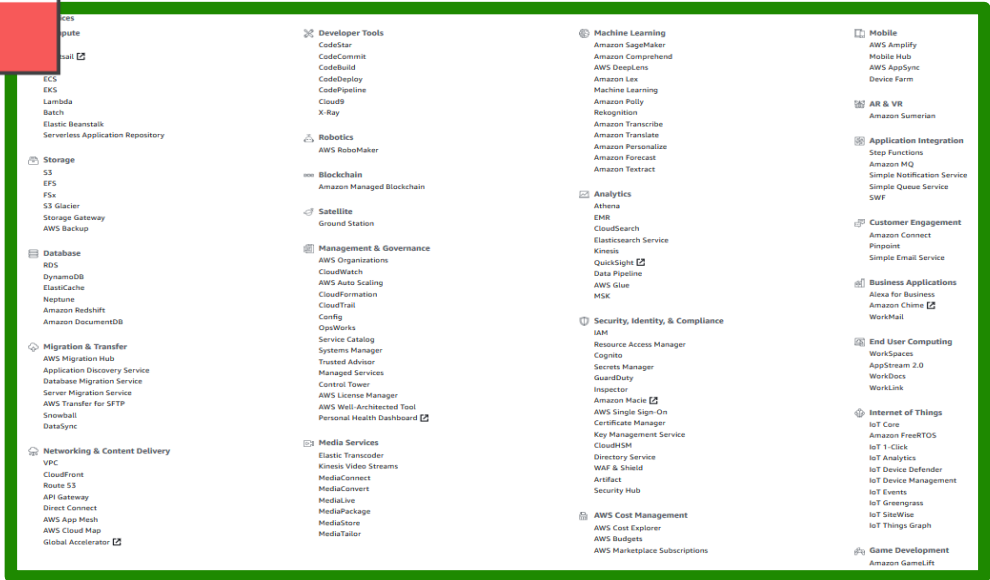
Permissions management:
AWS IAM



Data encryption:
AWS KMS



Network security controls:
Amazon VPC



Learn a few patterns, secure everything in AWS

Permissions management:
AWS IAM



We learned

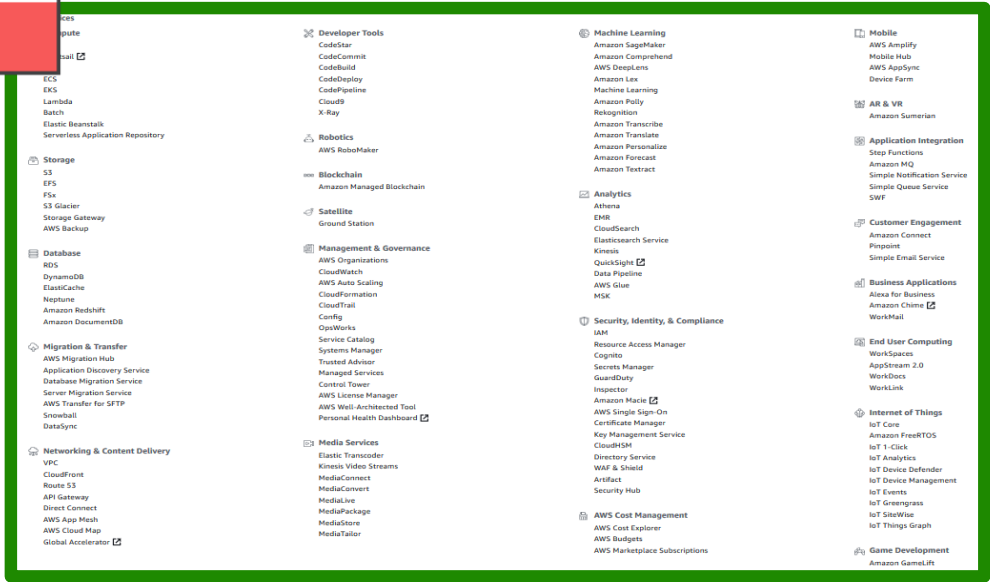
- Identities that can make AWS calls
- How to read and write IAM policy



Data encryption:
AWS KMS



Network security controls:
Amazon VPC



Learn a few patterns, secure everything in AWS

Permissions management: AWS IAM



We learned

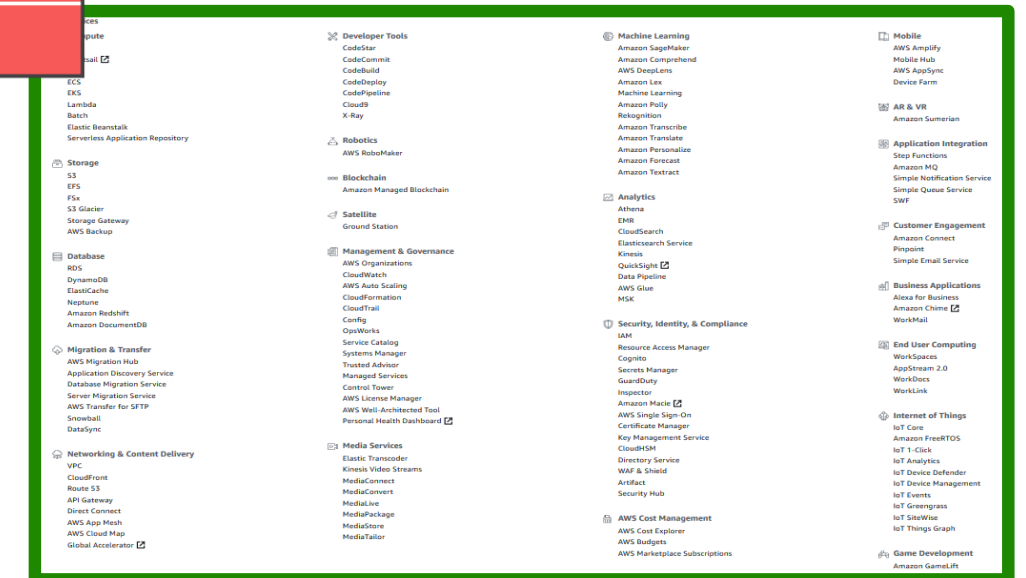
- How AWS KMS integrates with AWS services
- How to authorize access to AWS KMS keys



Data encryption: AWS KMS



Network security controls: Amazon VPC



Learn a few patterns, secure everything in AWS

Permissions management:
AWS IAM



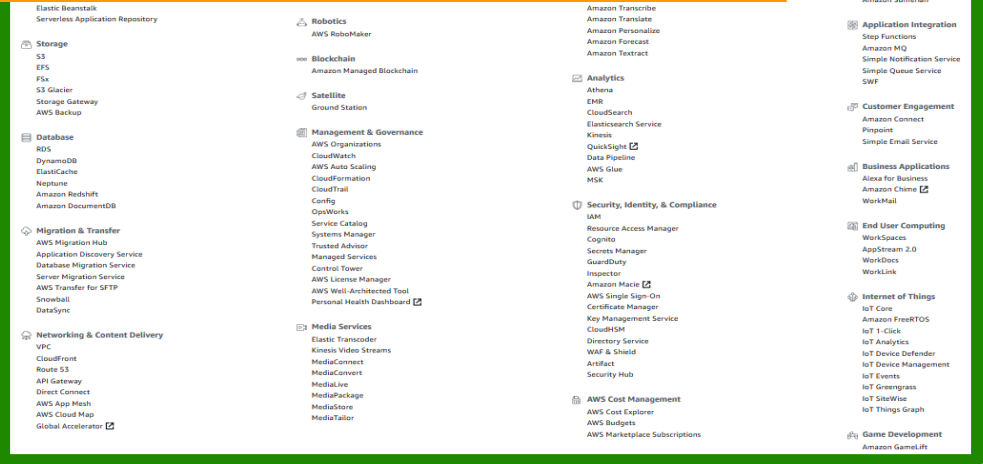
Data encryption:
AWS KMS



Network security controls:
Amazon VPC

We learned

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



Related breakouts

Wednesday, June 26

FND215: Best practices for choosing identity solutions for applications + workloads

2:45 – 3:45 PM | Level 3, Ballroom East

Wednesday, June 26

FND310-R1: How encryption works in AWS: What assurances do you have that unauthorized users won't access your data?

8:45 – 9:45 AM | Level 2, Room 253B

Wednesday, June 26

FND204-R1: Sharing services securely across VPCs and accounts

9:30 – 10:30 AM | Level 1, Room 151B, Table 1

Thank you!

Becky Weiss
becky@amazon.com

 RE:INFORCE