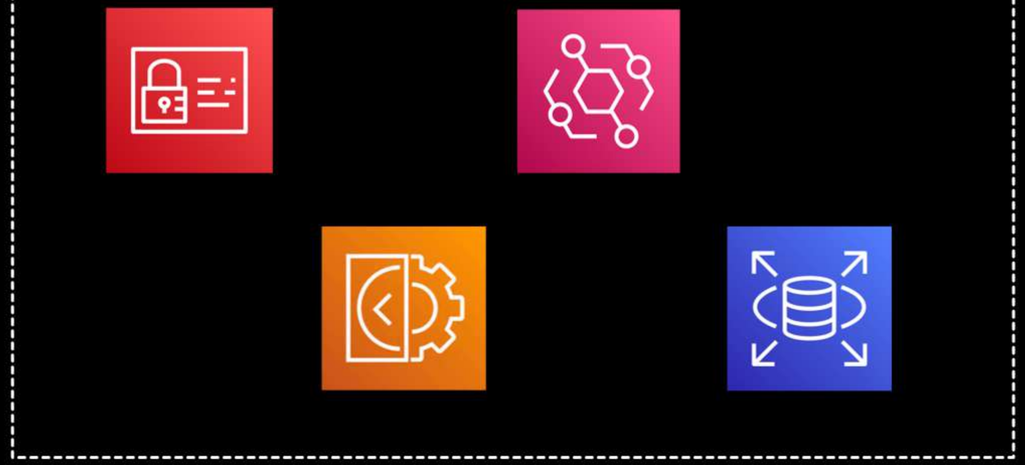


Exam Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

The AWS Global Certification Program

Amazon Web Services





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

The AWS Global Certification Program







NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Professional

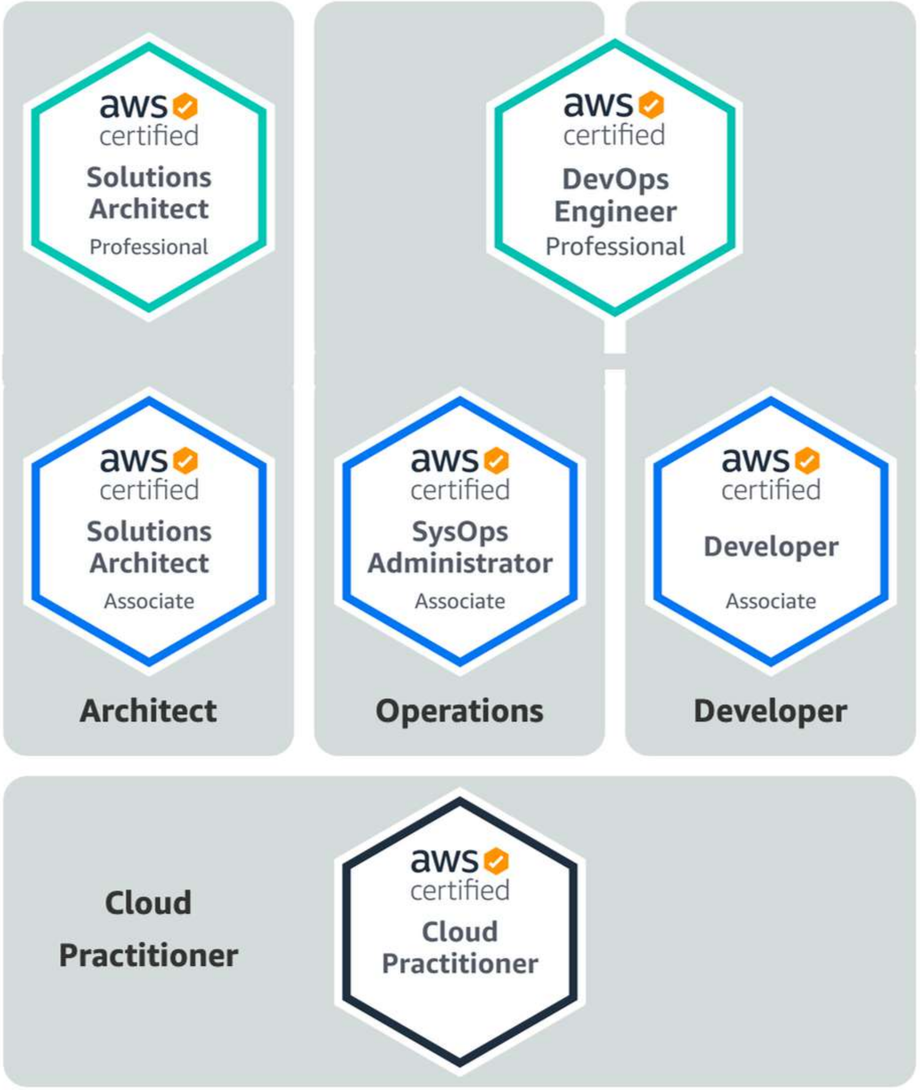
Two years of comprehensive experience designing, operating, and troubleshooting solutions using the AWS Cloud

Associate

One year of experience solving problems and implementing solutions using the AWS Cloud

Foundational

Six months of fundamental AWS Cloud and industry knowledge



Specialty

Technical AWS Cloud experience in the Specialty domain as specified in the **exam guide**



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Certified SysOps Administrator - Associate

- intended for DevOps Engineers or System Administrator roles
- preferably for professionals with 1 year experience using AWS cloud resources.
- helps organizations identify and develop talent for performing system administration tasks

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





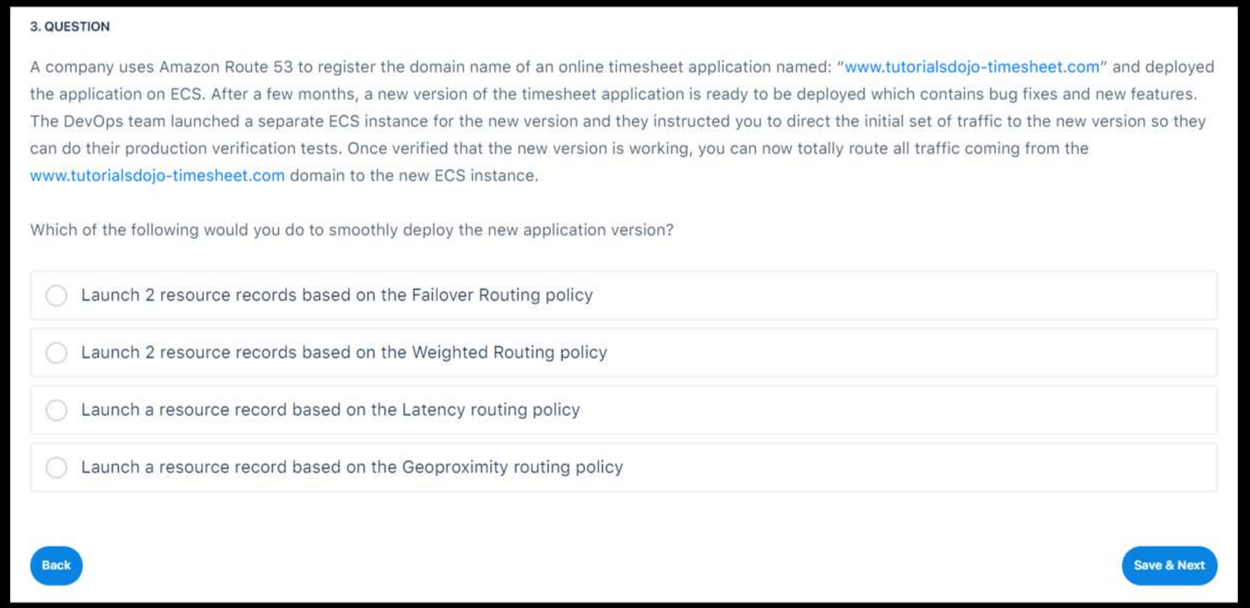
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SOA-C02 Question Formats

Multiple Choice

Multiple Responses

Exam Labs


3. QUESTION

A company uses Amazon Route 53 to register the domain name of an online timesheet application named: "www.tutorialsdojo-timesheet.com" and deployed the application on ECS. After a few months, a new version of the timesheet application is ready to be deployed which contains bug fixes and new features. The DevOps team launched a separate ECS instance for the new version and they instructed you to direct the initial set of traffic to the new version so they can do their production verification tests. Once verified that the new version is working, you can now totally route all traffic coming from the www.tutorialsdojo-timesheet.com domain to the new ECS instance.

Which of the following would you do to smoothly deploy the new application version?

- Launch 2 resource records based on the Failover Routing policy
- Launch 2 resource records based on the Weighted Routing policy
- Launch a resource record based on the Latency routing policy
- Launch a resource record based on the Geoproximity routing policy

Back

Save & Next

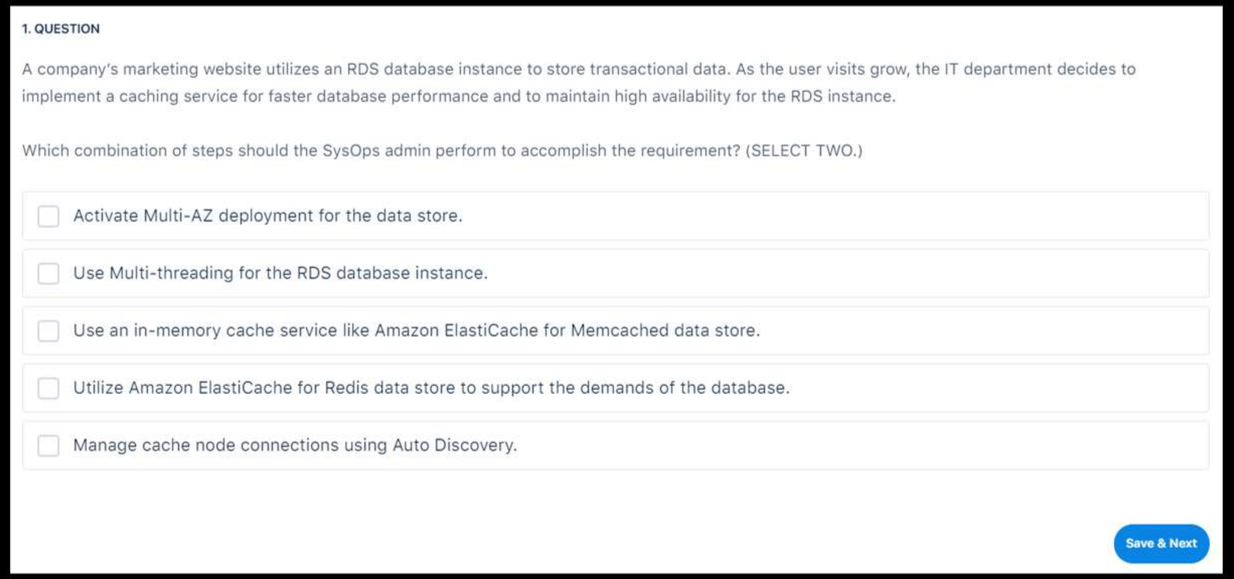
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SOA-C02 Question Formats

Multiple Choice

Multiple Responses

Exam Labs



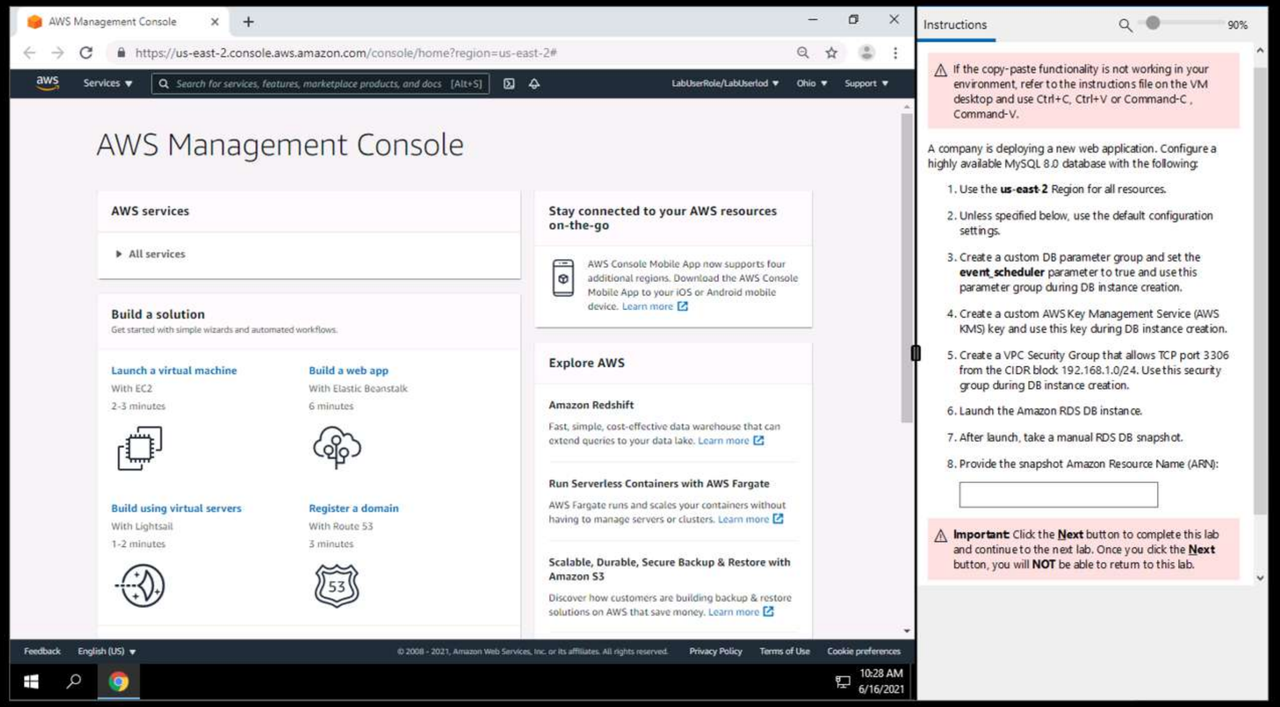
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SOA-C02 Question Formats

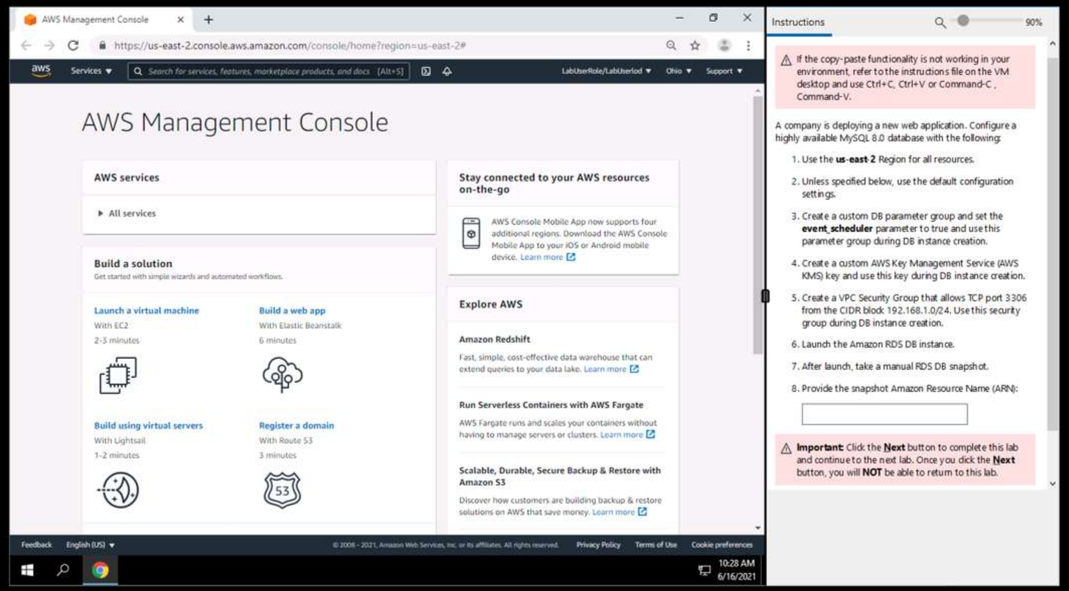
Multiple Choice

Multiple Responses

Exam Labs



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Exam Labs

- There may be more than one way to perform an exam lab.
- A full score is awarded if the correct end state to the scenario is achieved.
- Partial credit is awarded for partial completion of exam labs.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



The exam validates a candidate's ability to:

- Deploy, manage, and operate workloads on AWS,
- Support and maintain AWS workloads according to the AWS Well-Architected Framework
- Perform operations by using the AWS Management Console and the AWS CLI
- Implement security controls to meet compliance requirements
- Monitor, log, and troubleshoot systems

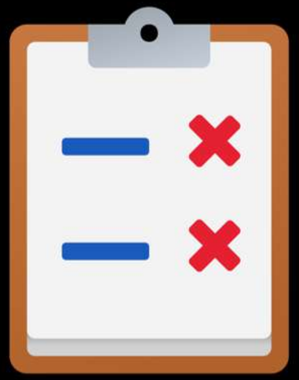
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



The exam validates a candidate's ability to

- Apply networking concepts
- Implement architectural requirements
- Perform business continuity and disaster recovery procedures
- Identify, classify, and remediate incidents.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



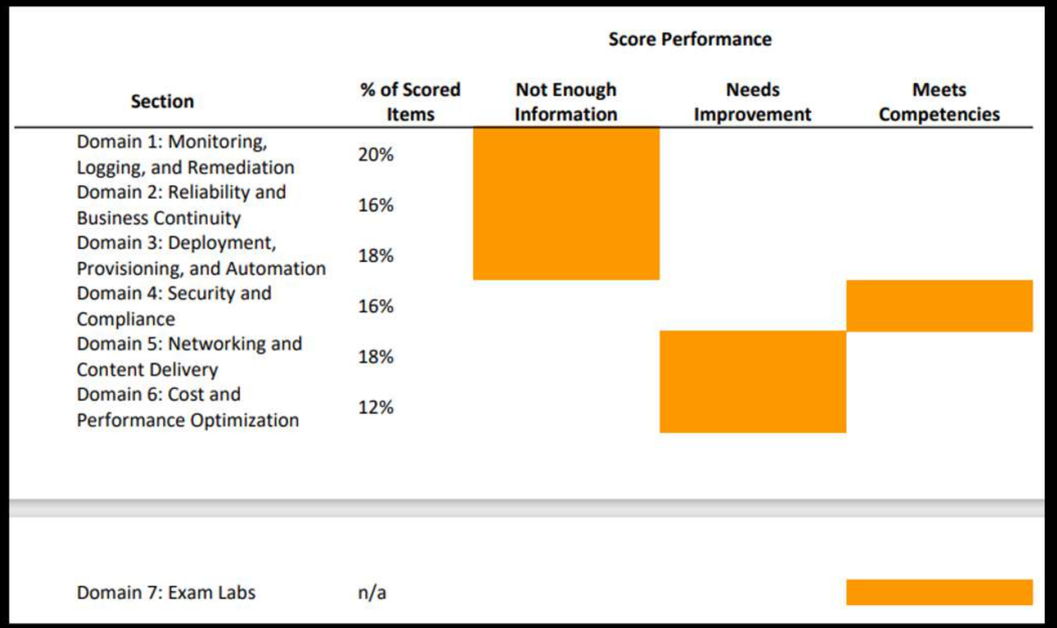
In case you fail the exam:

- You must wait 14 days before you ar allowed to retake the test
- NO hard limit on the number of exam attempts
- On each exam attempt, the full registration price of the exam must be paid
- Exam vouchers can still be applied when you retake the exam.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS is using a compensatory scoring model

- You will pass this exam as long as you get an overall score of 720 across 6 domains
- Each section has a specific score weighting
- Your Score Performance table highlights your strengths and weaknesses



Section	% of Scored Items	Score Performance: Not Enough Information	Score Performance: Needs Improvement	Score Performance: Meets Competencies
Domain 1: Monitoring, Logging, and Remediation	20%			
Domain 2: Reliability and Business Continuity	16%			
Domain 3: Deployment, Provisioning, and Automation	18%			
Domain 4: Security and Compliance	16%			
Domain 5: Networking and Content Delivery	18%			
Domain 6: Cost and Performance Optimization	12%			
Domain 7: Exam Labs	n/a			

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



SysOps Exam Domains

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

THE EXAM DOMAINS

- Monitoring, Logging, and Remediation
-
- Reliability and Business Continuity
- Deployment, Provisioning, and Automation
- Security and Compliance
- Networking and Content Delivery
- Cost and Performance Optimization

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DOMAIN 1 - 20%

Monitoring, Logging and Remediation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon
CloudWatch



Amazon
Simple Notification
Service (SNS)



Amazon
Cloud Trail



Amazon
EventBridge

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DOMAIN 1: Monitoring, Logging and Remediation

- Implement **metrics**, **alarms**, and **filters** by using AWS monitoring and logging services
- Remediate issues based on monitoring and availability metrics



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DOMAIN 2 - 16%

Reliability and Business Continuity

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DOMAIN 2: RELIABILITY AND BUSINESS CONTINUITY

- Implement **scalability** and **elasticity**
- Implement **high availability** and resilient environments
- Implement **backup** and **restore** strategies



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DOMAIN 3 - 18%

Deployment, Provisioning and Automation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS
CloudFormation



AWS
Config



AWS
Systems Manager



AWS
Resource Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DOMAIN 3: DEPLOYING, MONITORING, AND AUTOMATION

- Provision and maintain cloud resources
- Automate manual and repeatable process



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DOMAIN 4 - 16%

Security and Compliance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon
Cloud Trail



AWS
Key Management Service (KMS)



IAM
Access Analyzer



AWS
Certificate Manager



AWS
IAM Policy Simulator



Amazon Inspector

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DOMAIN 4: SECURITY AND COMPLIANCE

- Implement and manage security and compliance policies,
- Implement **data and infrastructure protection** strategies in AWS.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DOMAIN 5 - 18%

Network and Content Delivery

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Route 53



Amazon CloudFront



Amazon VPC

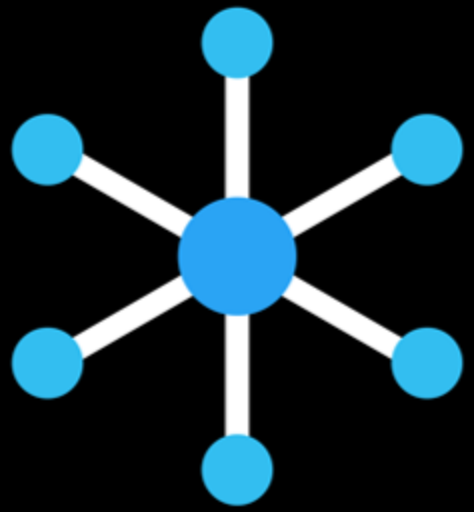


Hybrid Networks

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DOMAIN 5: NETWORK AND CONTENT DELIVERY

- Implement **networking features and connectivity**
- Configure domains, **DNS** services, and **content delivery**
- Troubleshoot network connectivity issues.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DOMAIN 6 - 12%

Cost and Performance Optimization

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DOMAIN 6: COST AND PERFORMANCE OPTIMIZATION

- Implement cost optimization strategies,
- implementing performance optimization strategies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Tutorials Dojo

SYSOPS Administrator Associate Exam

- Set up monitoring and logging for your resources,
- Perform architectural change for AWS workloads and networks based on metrics,
- Implement optimization strategies,
- Apply networking concepts like DNS, VPCs, Security Groups, Network ACLs,

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SYSOPS Administrator Associate Exam

- Implement security and compliance policies,
- Strategize and implement business continuity plans,
- Remediate accidents through various monitoring and availability metrics.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Exam Benefit

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



What benefits will you get?

- ✓ You will get two vouchers
  - ✓ 50% exam discount voucher for your next exam
  - Free access voucher to an official AWS practice exam
- AWS Digital Badge
- Access to AWS Certified Store
- Opportunity to join the AWS IQ program

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

aws training and certification

Get Help | Support & FAQs | English | Logout

Candidate ID: [redacted]

Testing Center Updates
Find more information on availability and procedures for testing centers near you.

AWS Certification Information & Policies
Learn more about what to expect before, during, and after your exam on our website.

Important: Identification Policy
Your name in your AWS Certification Account must match your government ID. Please review the Identification Policy Bulletin for details on how to verify your name and make updates if needed.

Your AWS Certification Account

Use your AWS Certification Account as a central management tool for AWS Certification, including scheduling exams and taking advantage of certification benefits.

Schedule New Exam

Request Exam Accommodations

Manage PSI Exams

Manage Pearson VUE Exams

Get Started

Click "Schedule New Exam" to schedule a certification exam or practice exam at either a PSI or Pearson VUE testing center.

Click "Request Exam Accommodations" to learn about applying for exam accommodations and to submit an accommodations request. Please request your Exam Accommodation before scheduling your exam at PSI or Pearson VUE.

Click "Manage PSI Exams" or "Manage Pearson VUE Exams" to manage a previously scheduled exam appointment or view/generate a receipt.

For candidates ages 13-17, please visit the Request Exam Accommodations page for specific instructions on registration and testing experience.

Take Advantage of Certification Benefits
Once you've achieved your first certification, you can take advantage of exclusive benefits, including AWS Certified merchandise, free practice exams, digital badges, and transcripts that you can use to showcase your expertise.

Confirm Your Accommodations - As a reminder, if you have requested an accommodation, please confirm that it is displayed on your account prior to taking your exam. Click "Request Exam Accommodations" to review your requested and approved accommodations.

If an ESL +30 accommodation is missing, please request the accommodation again.

If other accommodations have been approved and are missing, please contact PSI (1-800-367-1565 ex. 6701) and/or Pearson VUE (1-800-466-0450) and request that they re-approve the accommodations.

News

Aug 26, 2020

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Testing Center Updates



What benefits will you get?

- ✓ You will get two vouchers
  - ✓ 50% exam discount voucher for your next exam
  - ✓ Free access voucher to an official AWS practice exam
- ✓ AWS Certification Digital Badge
- Access to AWS Certified Store
- Opportunity to join the AWS IQ program

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

aws training and certification

Get Help | Support & FAQs | English | Logout

Candidate ID: [redacted]

My AWS Certification Benefits

If you hold one or more active AWS certifications, below you will find benefits for the earned certification(s) along with instructions for redemption. Note that redeeming some benefits requires access to third-party sites.

All benefits are non-transferable and intended for use solely by the individual who earned the benefit and by the AWS Certification account to which the benefit was originally assigned. If AWS, in its sole discretion, determines you misused or transferred a benefit, AWS may invalidate the exam result related to the misuse or transfer and the benefit will not be reinstated.

View My Certifications

View My Digital Badges

Share My Transcript

Active Benefits

Name	Type	Apply Link	Code	Claim Benefit
AWS Certified Store Benefit				
AWS Certified Associate: Store Access	Token	View	[redacted]	
AWS Certified Practice Exam Benefit				
AWS Free Practice Exam Voucher	Token			Claim Benefit
AWS Certification SME Program				
Apply to join our Subject Matter Expert (SME) Program	Link			Claim Benefit
AWS Certified Exam Discount Benefit				
50% Discount on your next Exam	Token			Claim Benefit
AWS Certified Global LinkedIn Community				
AWS Certified Global LinkedIn Community	Link	View		

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



What benefits will you get?

- You will get two vouchers
  - 50% exam discount voucher for your next exam
  - Free access voucher to an official AWS practice exam
- AWS Certification Digital Badge
- Access to AWS Certified Store
- Opportunity to join the AWS IQ program

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

aws training and certification

Get Help | Support & FAQs | English | Logout

Candidate ID: [redacted]

My AWS Certification Benefits

If you hold one or more active AWS certifications, below you will find benefits for the earned certification(s) along with instructions for redemption. Note that redeeming some benefits requires access to third-party sites.

All benefits are non-transferable and intended for use solely by the individual who earned the benefit and by the AWS Certification account to which the benefit was originally assigned. If AWS, in its sole discretion, determines you misused or transferred a benefit, AWS may invalidate the exam result related to the misuse or transfer and the benefit will not be reinstated.

View My Certifications

View My Digital Badges

Share My Transcript

Active Benefits

Name	Type	Apply Link	Code	Claim Benefit
AWS Certified Store Benefit				
AWS Certified Associate: Store Access	Token	View	[redacted]	
AWS Certified Practice Exam Benefit				
AWS Free Practice Exam Voucher	Token			Claim Benefit
AWS Certification SME Program				
Apply to join our Subject Matter Expert (SME) Program	Link			Claim Benefit
AWS Certified Exam Discount Benefit				
50% Discount on your next Exam	Token			Claim Benefit
AWS Certified Global LinkedIn Community				
AWS Certified Global LinkedIn Community	Link	View		

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



What benefits will you get?

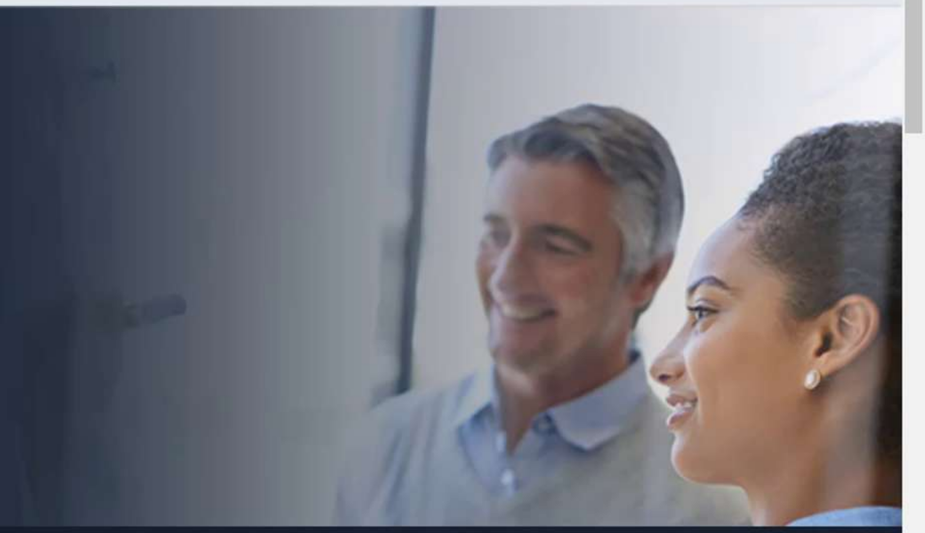
- You will get two vouchers
  - 50% exam discount voucher for your next exam
  - Free access voucher to an official AWS practice exam
- AWS Certification Digital Badge
- Access to AWS Certified Store
- Opportunity to join the AWS IQ program

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS IQ for Experts

Help customers and get paid for your AWS Certification expertise

Register now



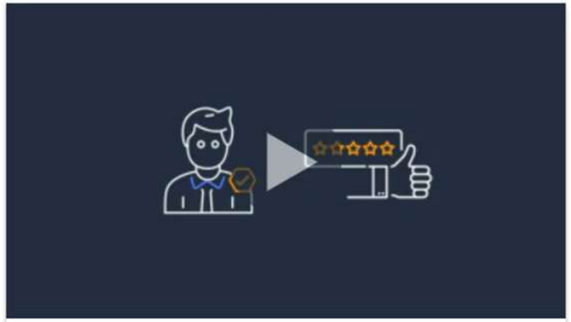
FEATURED

AWS Certification

Explore the resources available to help you prepare for your AWS Certification.

Learn more »

AWS IQ enables customers to quickly find, engage, and pay AWS Certified third-party experts for on-demand project work. AWS IQ also makes it easy for you to use your AWS Certifications to help AWS customers. With AWS IQ, you have a secure collaborative workspace for project consultations and an easy way to get paid.



Connect with AWS Customers, Demonstrate Your Expertise, and Get Paid (1:40)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS IQ Program

- Must be 18 years old and above
- Must be a US-based professional
- Shall possess an Associate, Professional, or Specialty Certification

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT

is AWS?

WHEN

did AWS start?

WHY

is AWS so popular?

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?

Amazon



Web Services

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?

Amazon







Web Services

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?

Amazon Web Services = Cloud Service Provider

- provides a cloud-based platform or cloud services
- Allows you to **rent out** virtual servers that you access remotely

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?

Cloud Service Provider is *like* a Car Rental



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?

Cloud Service Provider

With different types of **CPU**, **Storage**, **Network** and other components that you can choose from!



Virtual Machines



Physical Servers

Storage Appliances



Network Devices

Available for RENT and accessible online via *Web Service* interfaces (REST, SOAP etc...)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Car Rental









WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?



2004

- AWS started out as a department **within** Amazon Inc.
- Used only by early Amazon customers
- Web services are not available publicly

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?



2004



2006

- AWS officially started its operation as a **public cloud** service provider
- Released Amazon S3 (Simple Storage Service)
- Released Amazon SQS (Simple Queue Service)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?



2004



2006



Today

- Offers hundreds of fully-featured services that are available globally
- Provides a highly reliable, scalable, and **low-cost** infrastructure platform in the cloud
- Boasts a broad set of cloud-based products

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WHAT
is AWS?

WHEN
did AWS start?

WHY
is AWS so popular?



Today

aws is the **world's leading cloud platform**.

- Used by **millions** of customers
- Supports various workloads
- Significantly lower your operating costs
- Enables companies to scale globally in minutes!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Global Infrastructure

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Has thousands of servers!



These *physical* servers generate *virtual* machines or store your data!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Availability Zone

Region

Edge Networks



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

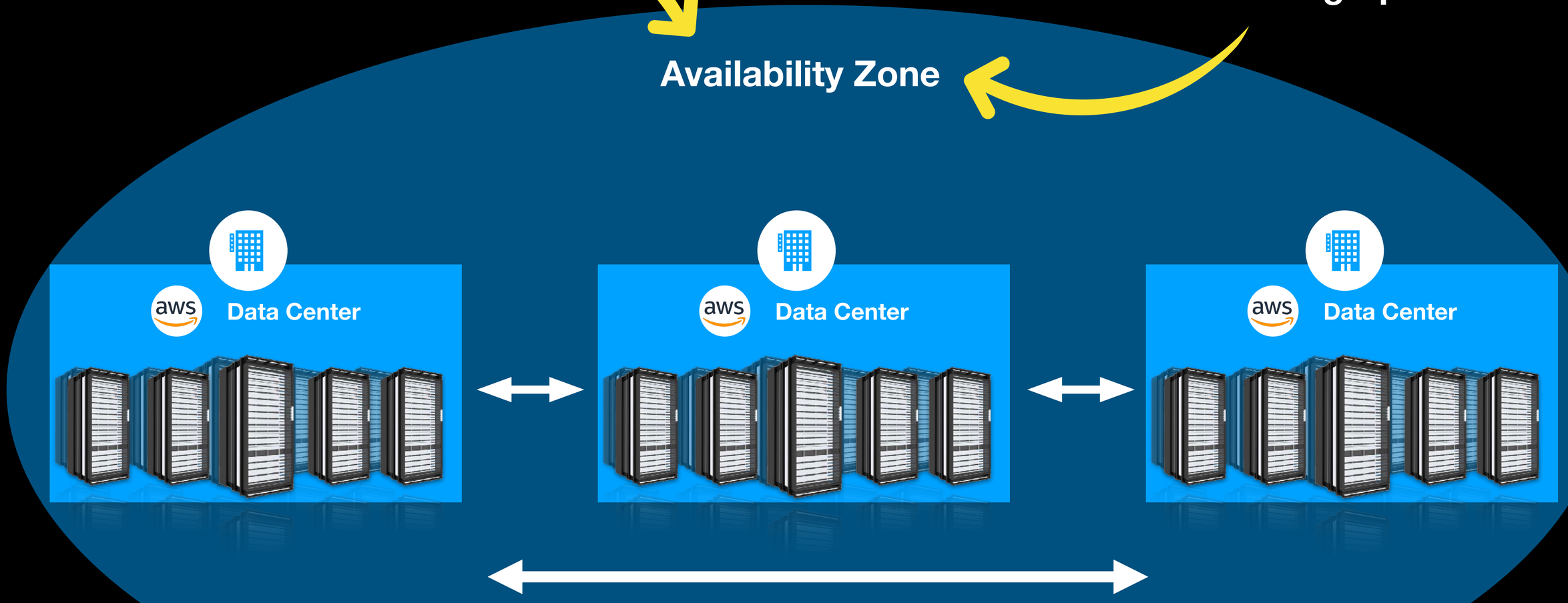
Edge Networks

Region

Improves the “Availability” of your systems

Literally a Geographic “Zone”

Availability Zone



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

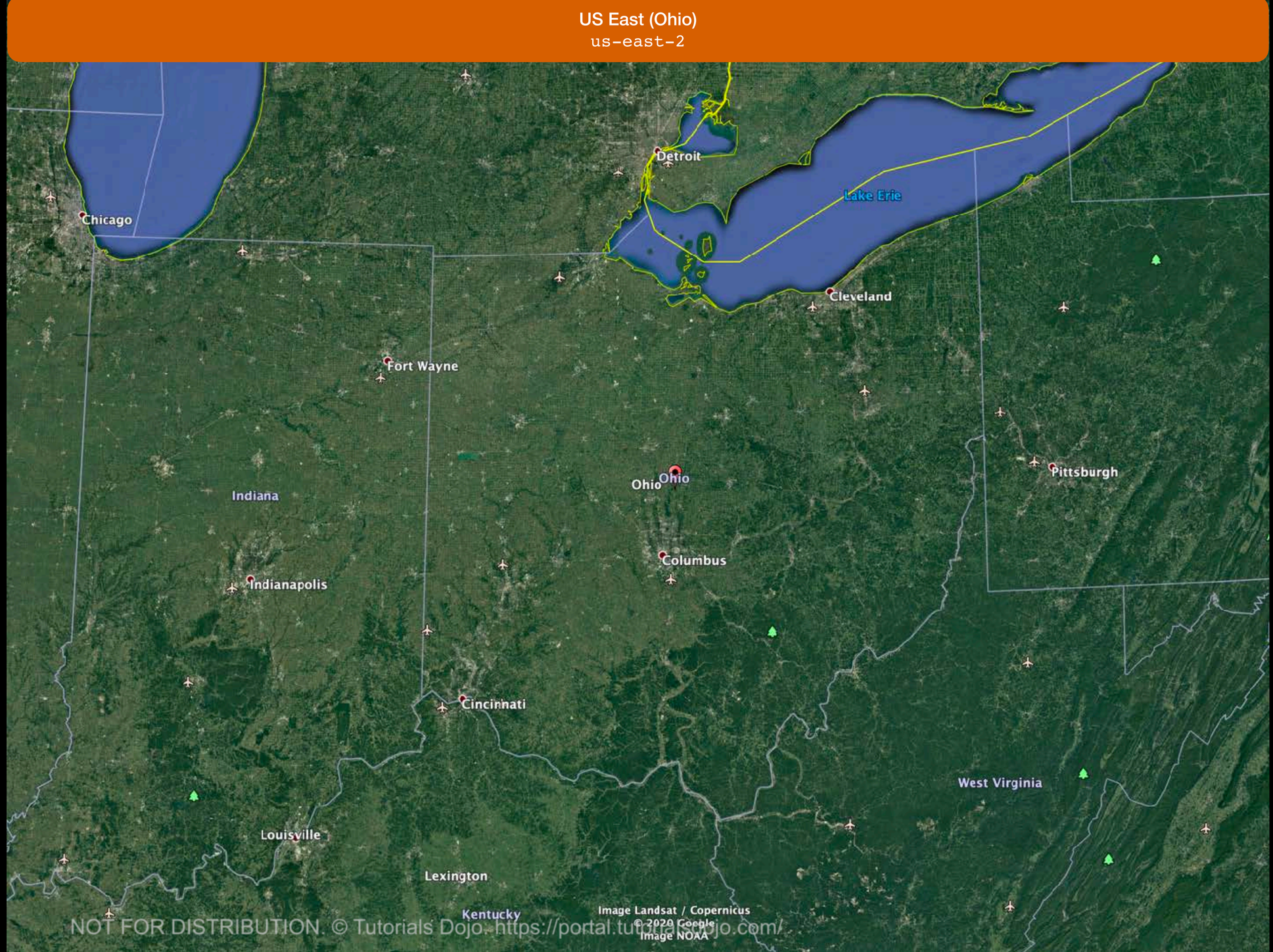
Edge Networks

Region

US East (Ohio)
us-east-2

Availability Zone





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Edge Networks

Region

US East (Ohio)
us-east-2

Availability Zone

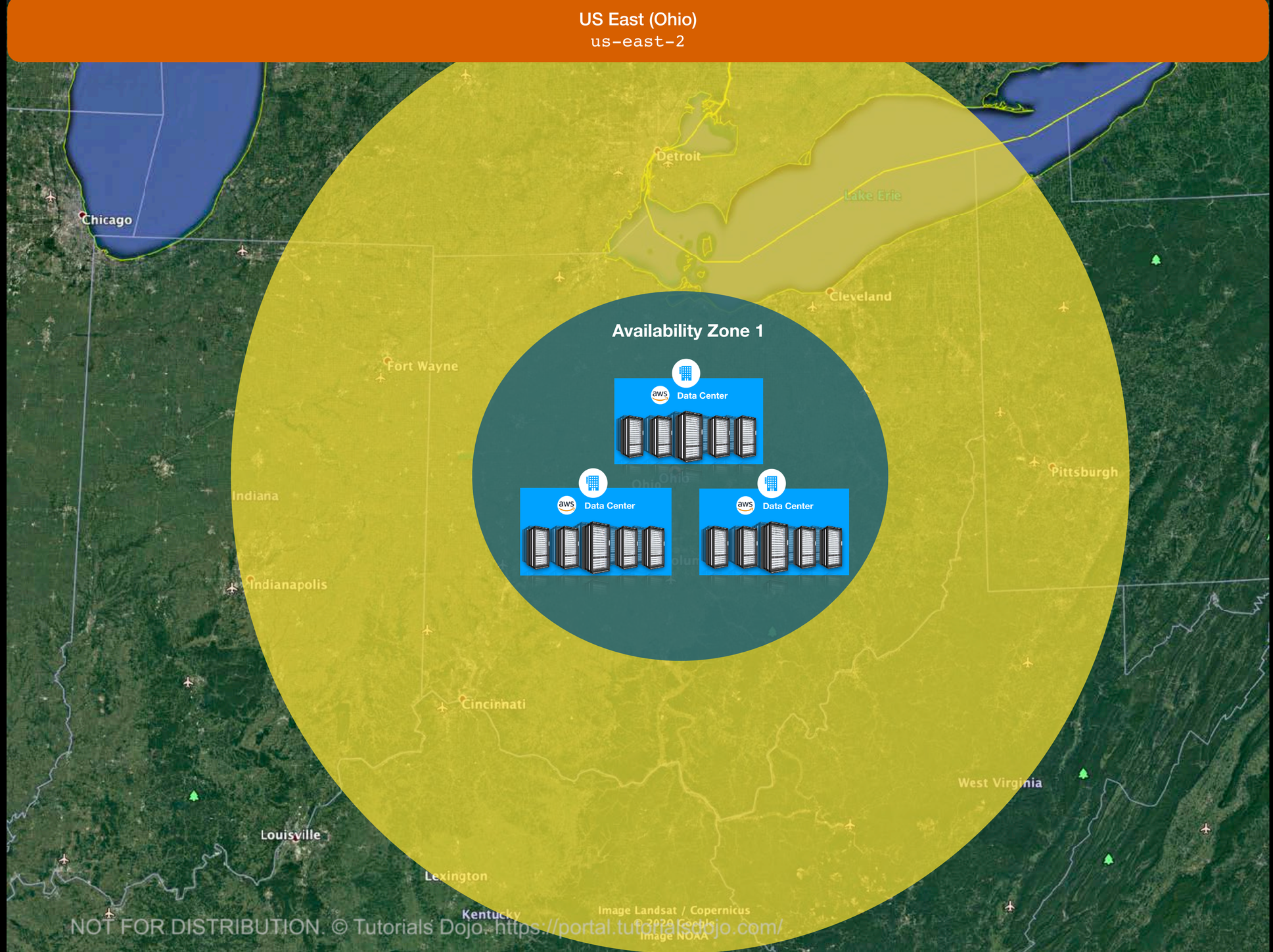


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Edge Networks

Region

Availability Zone

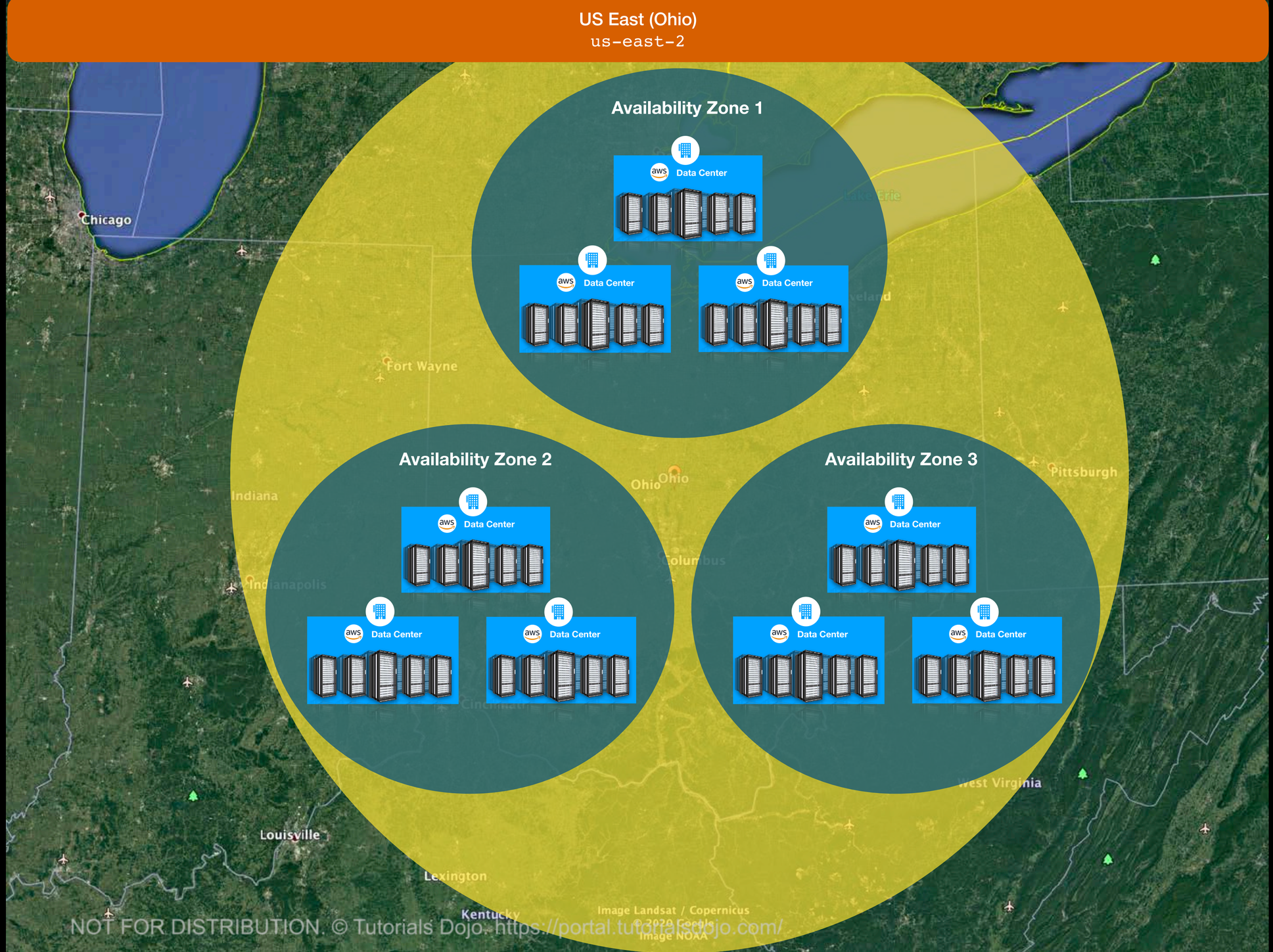


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Edge Networks

Region

Availability Zone



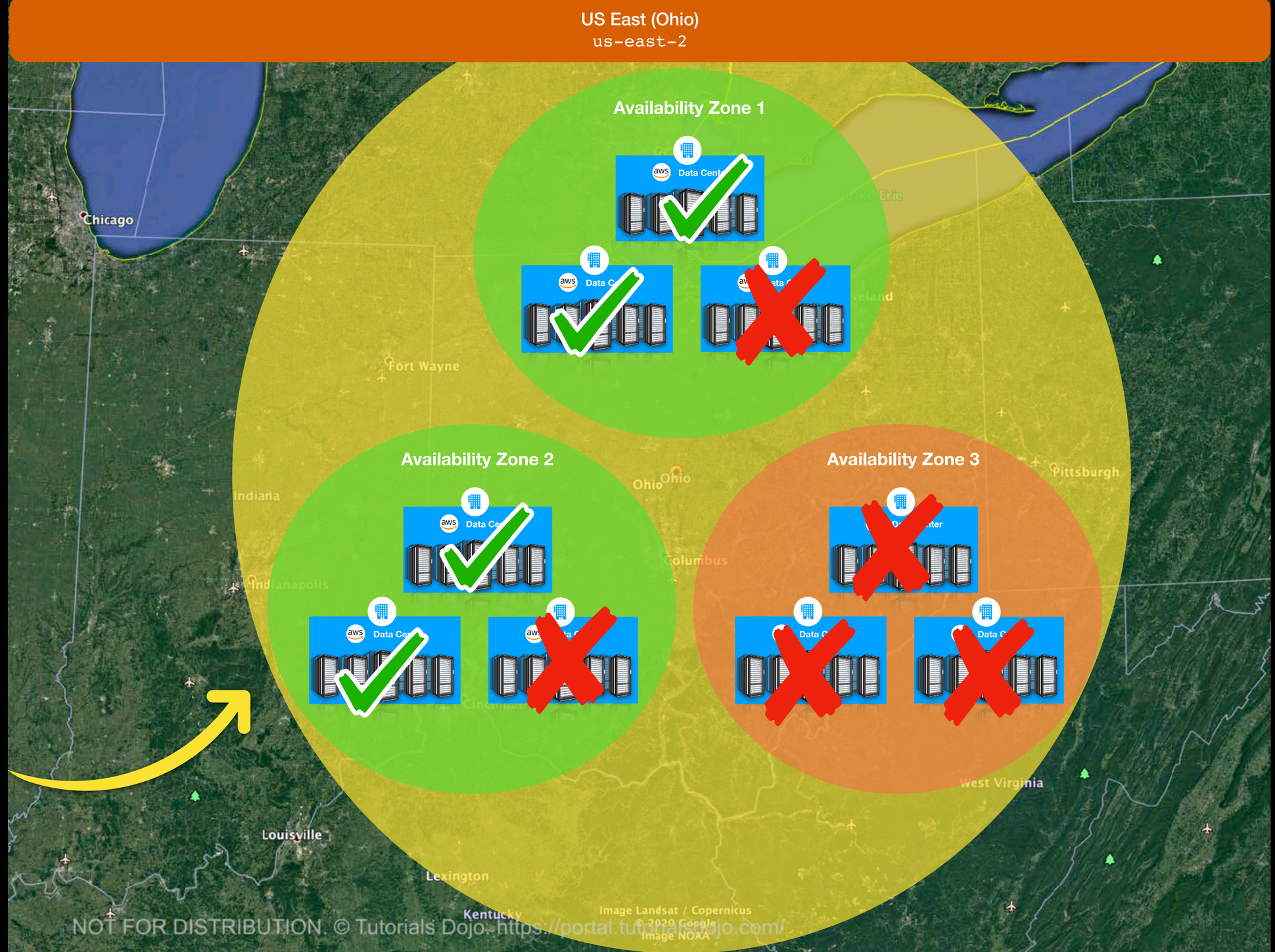
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Edge Networks

Region

Availability Zone

Your system will still run even if one or more data centers encountered an outage



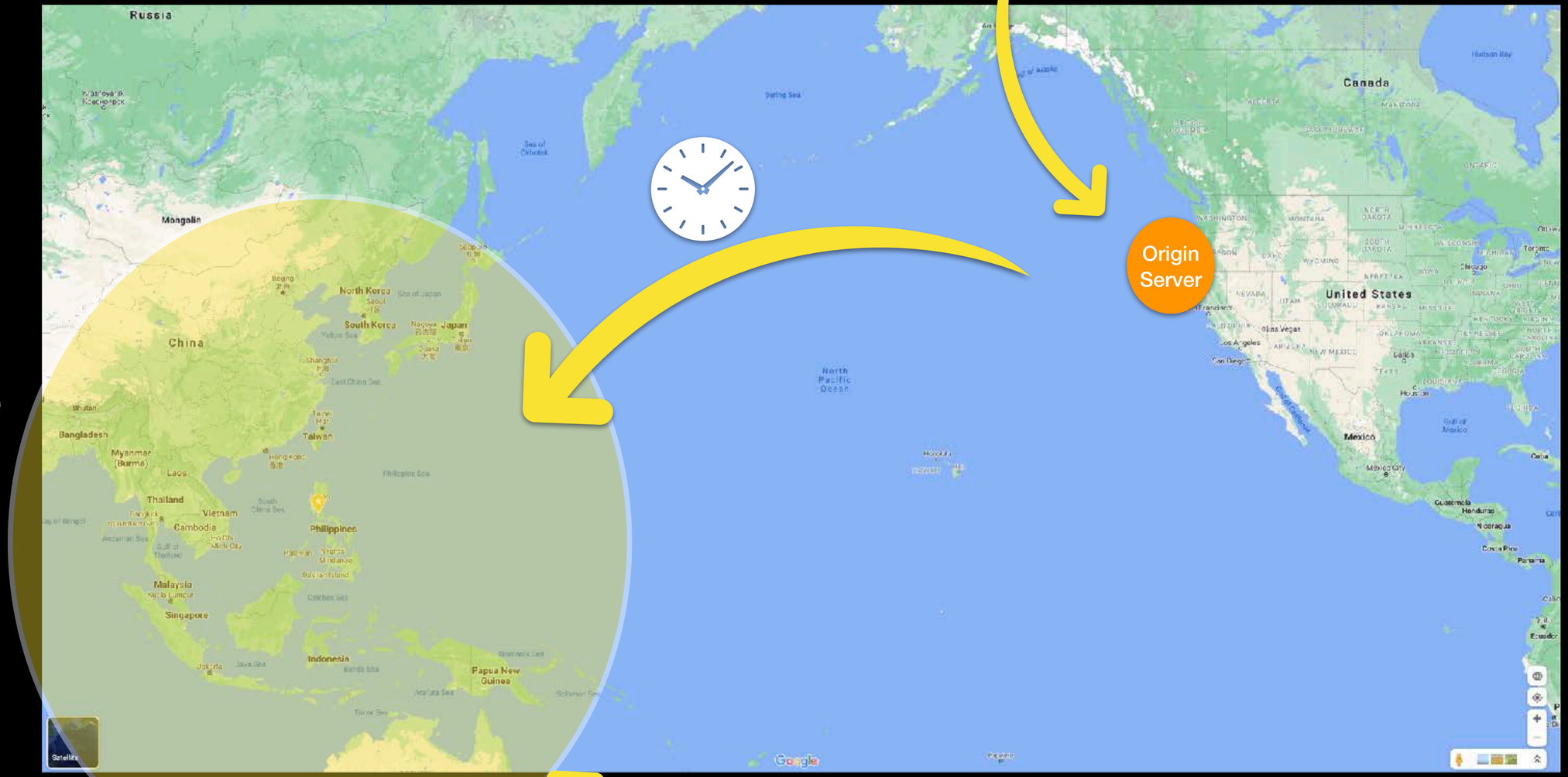
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Edge Networks

PoP Point of Presence / Edge Location

Region

Availability Zone



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



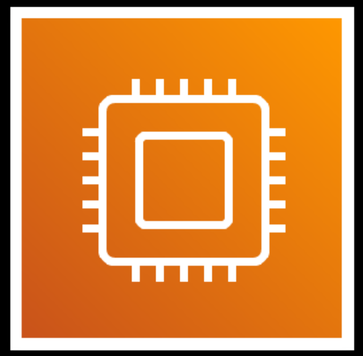
AWS Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



…and many more!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Host
Web Apps



Run Real-Time
Data Analytics



Develop
Mobile Apps



Store Data
for Backup

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Analytics



Application Integration



AWS Cost Management



Blockchain



Business Applications



Compute



Containers



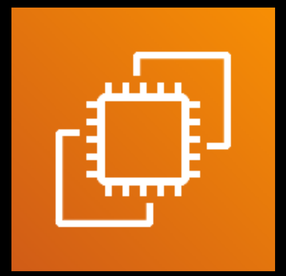
Customer Engagement

FOR REVIEW PURPOSES ONLY | https://portal.tutorialsdojo.com/

PER CATEGORY

- Analytics
- Application Integration
- AWS Cost Management
- Blockchain
- Business Applications
- Compute
- Containers
- Customer Engagement
- Database
- Developer Tools
- End User Computing
- Front-End Web & Mobile
- Game Tech
- Internet of Things
- Machine Learning
- Management & Governance
- Media Services
- Migration & Transfer
- Networking & Content Delivery
- Quantum Technologies
- Robotics
- Satellite
- Security, Identity & Compliance
- Serverless

COMPUTE SERVICES



Amazon EC2



AWS Lambda

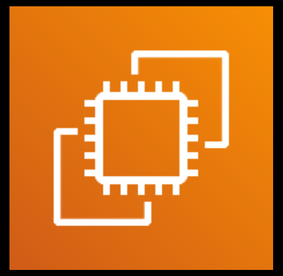


AWS Outposts



Amazon Lightsail

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2

Amazon Elastic **Compute** Cloud



Amazon S3

Amazon Simple **Storage** Service



Amazon RDS

Amazon **Relational Database** Service

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Fully Managed *By:* aws





Open Source Technology



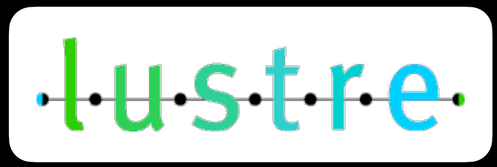
Amazon Elastic **Kubernetes** Service (EKS)







Amazon FSx for **Lustre** (FSx)

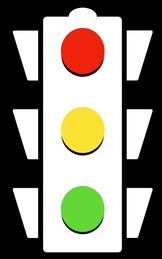




Amazon **Elasticsearch** Service



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Routes Traffic



Amazon Route 53

What's the meaning of this number?

The number **53** is the TCP and UDP **Port Number** used for the Domain Name System (**DNS**) protocol transport

PORT

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/


Featured Services


Analytics


Application Integration


AWS Cost Management

Blockchain


Business Applications


Compute


Containers


Customer Engagement


Database


Developer Tools


End User Computing


Front-End Web & Mobile


Game Tech


Internet of Things


Machine Learning


Management & Governance


Media Services


Migration & Transfer


Networking & Content Delivery


Quantum Technologies


Robotics


Satellite

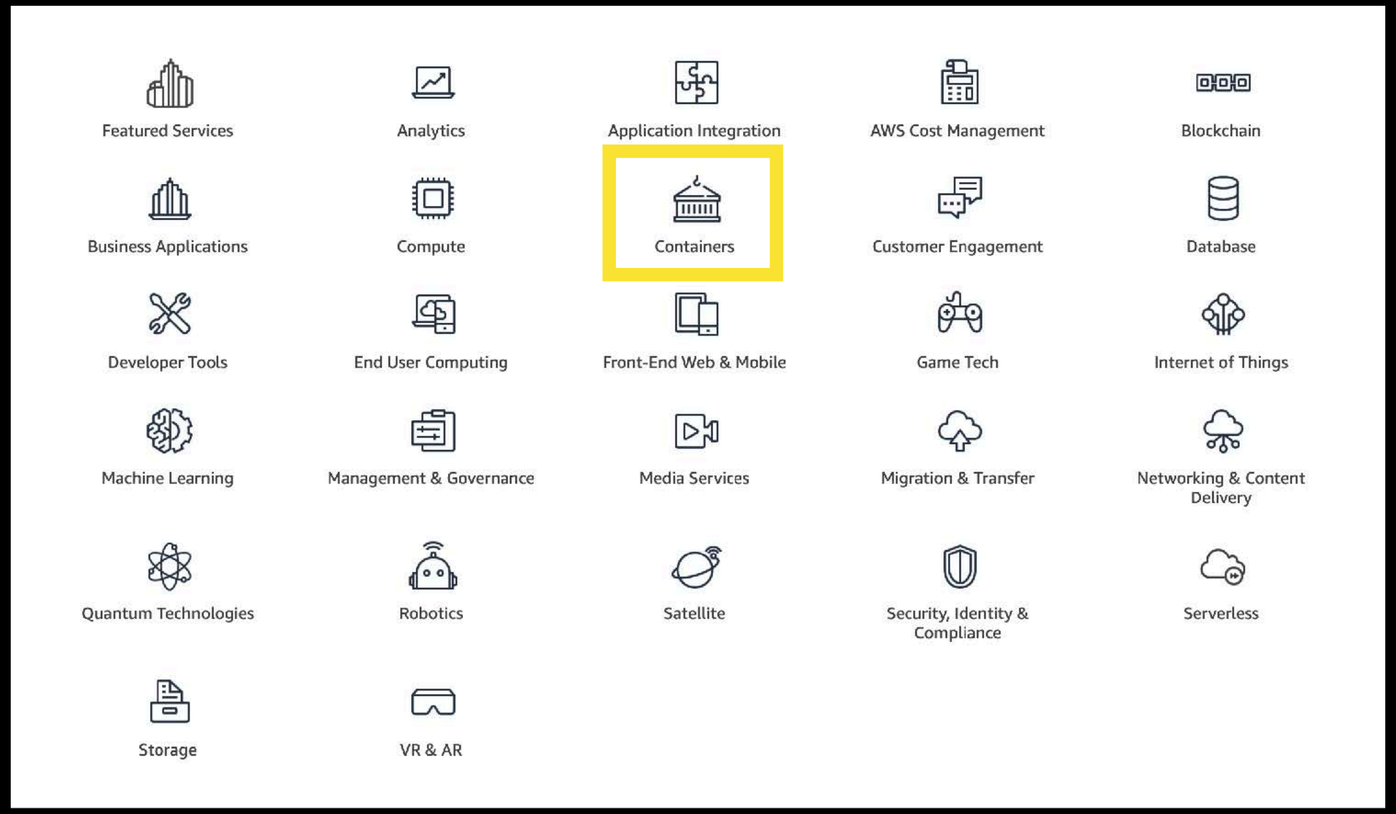

Security, Identity & Compliance


Serverless


Storage


VR & AR

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

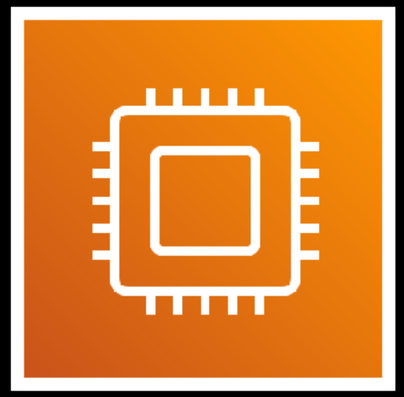


Amazon Elastic Container Service

Amazon EC2

Amazon Elastic Kubernetes Service

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

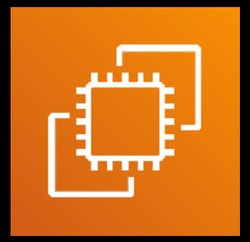


AWS Compute Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Compute Services

Virtual Machines



Amazon EC2



Amazon LightSail



AWS Outposts

Serverless



AWS Lambda



AWS Fargate

Orchestration



AWS Elastic Beanstalk



AWS Batch

Container



Amazon EKS



Amazon ECS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Virtual Machines



Windows



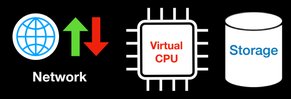
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



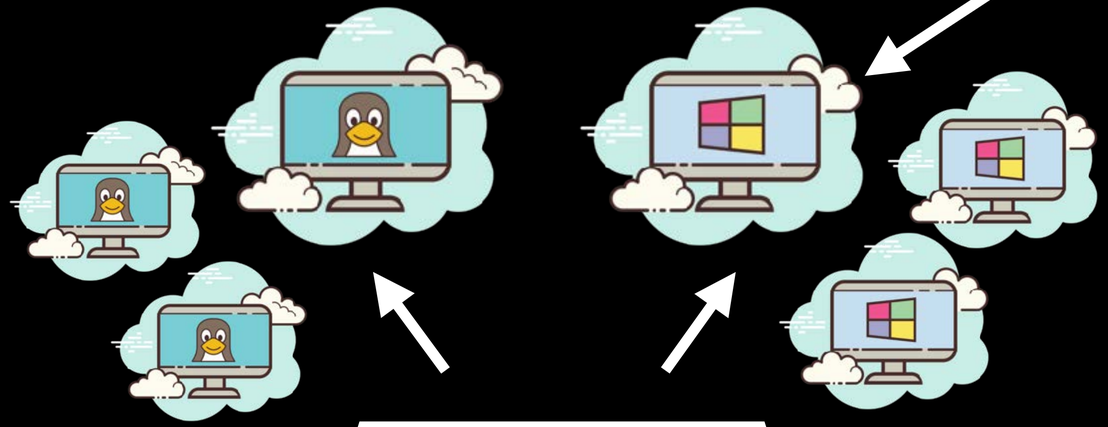
Used by MULTIPLE Tenants / Customers



Used by a SINGLE Customer

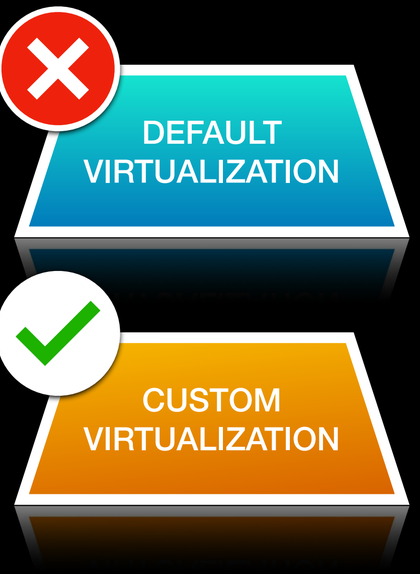


Instance









VIRTUALIZATION

Also called a
Virtual Machine Monitor
or a
Hypervisor



SHARED



DEDICATED

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Serverless

Fully Managed *By:* aws





NO DIRECT Server access via:

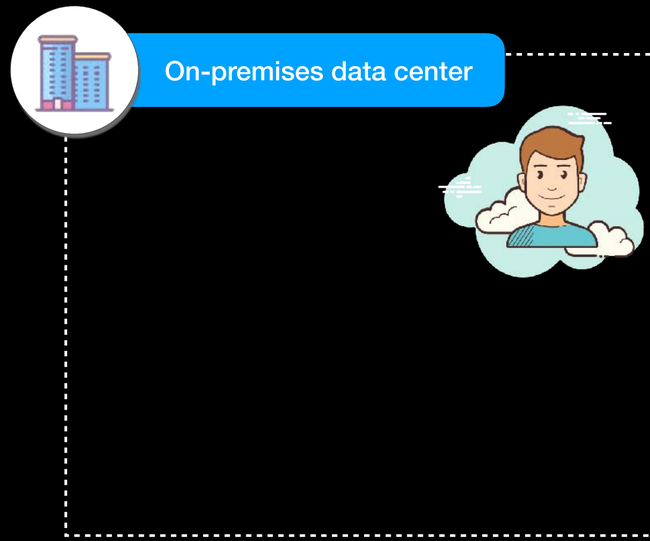
SSH or RDP

Unlike Amazon EC2

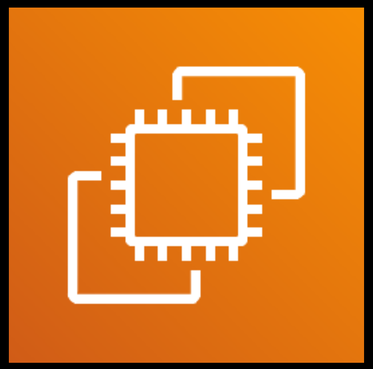


Hybrid





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

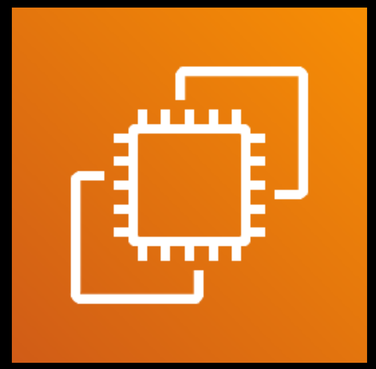


Amazon EC2

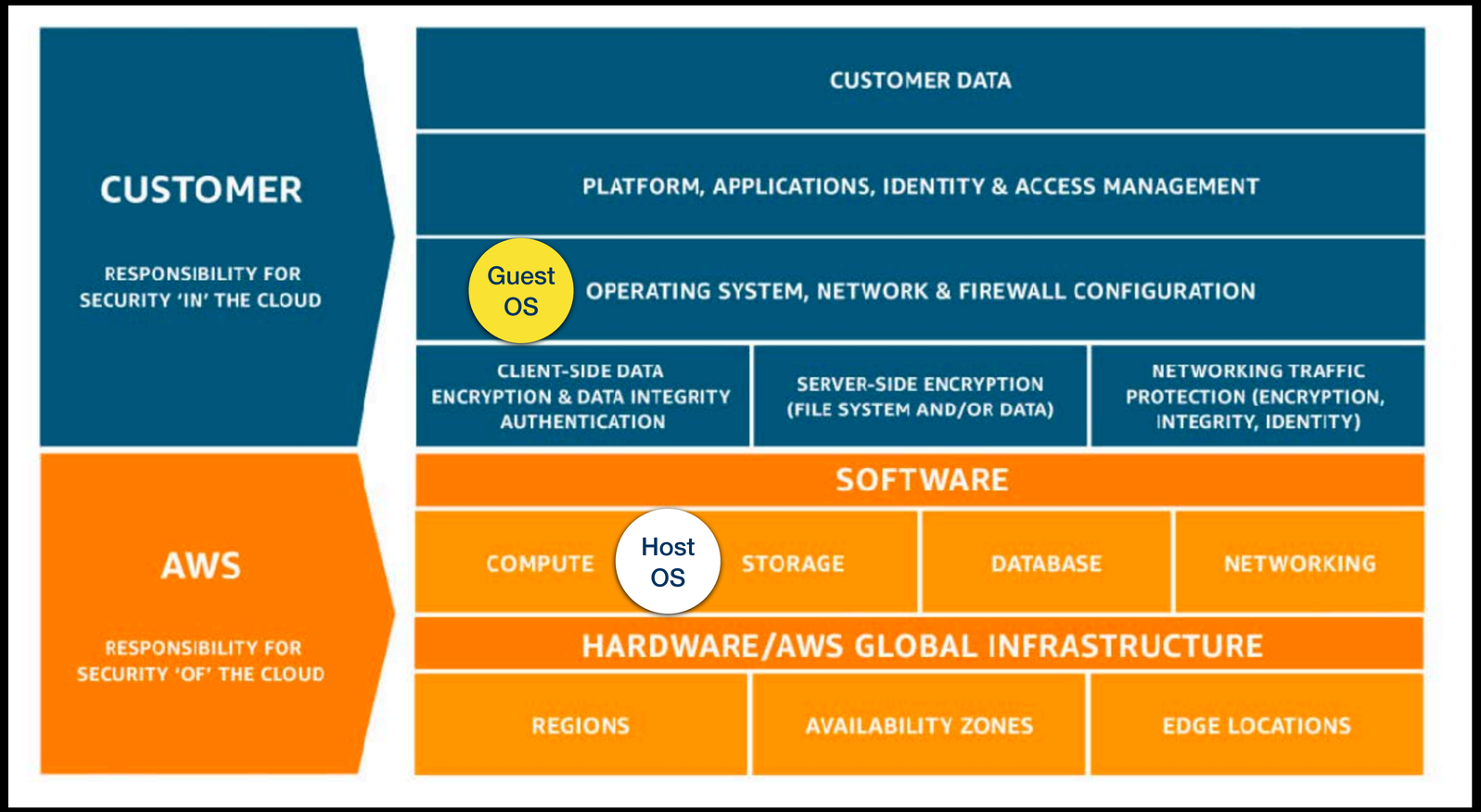
- A **computing service** that runs virtual servers in AWS
- Allows you to launch Windows, Linux or even MacOS virtual machines
- A type of an **Infrastructure as a Service (IaaS)**
- A basic building block for your cloud architecture
- Used by other AWS services as an underlying compute service

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

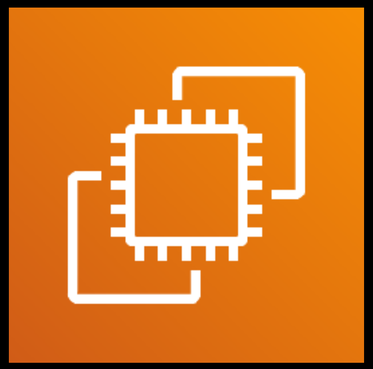
Shared Responsibility Model



Amazon EC2



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

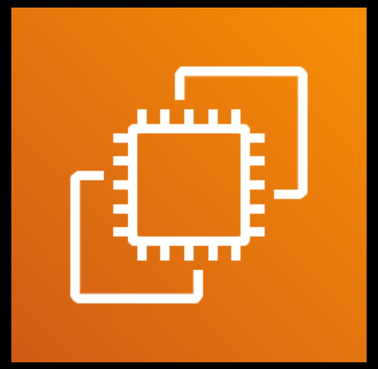


Amazon EC2

Elastic Compute Cloud

- Flexible
- Customizable
- Scalable

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2

Elastic Compute Cloud

EC2

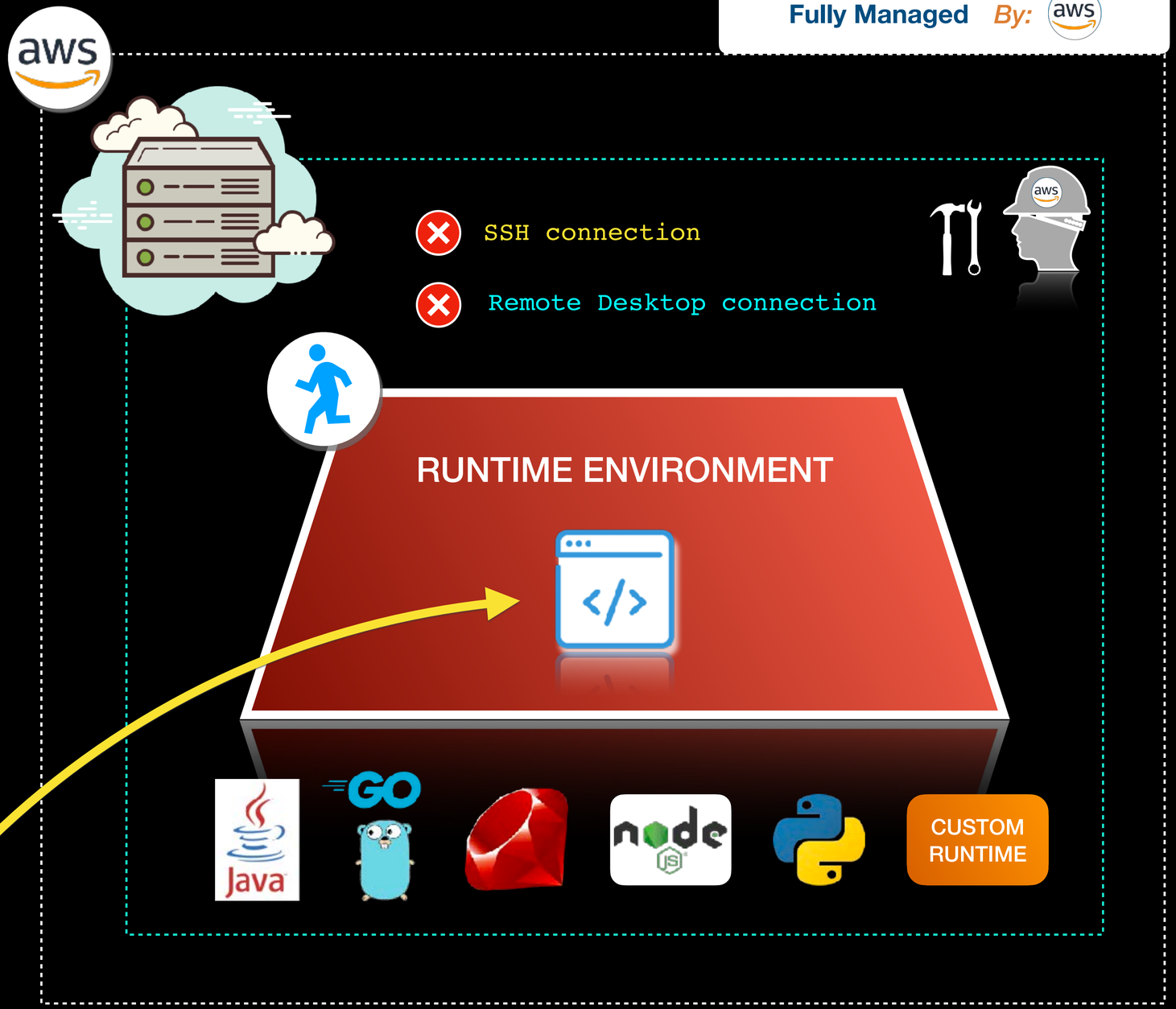
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Serverless



AWS Lambda

Lambda function



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Orchestration



AWS Batch



AWS Elastic Beanstalk

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Batch

- Enables you to run **batch** computing workloads
- Dynamically provisions the optimal quantity and type of compute resources, based on the volume and specific resource requirements.
- Does the planning, scheduling, and execution of your batch computing workloads **using Amazon EC2 instances.**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



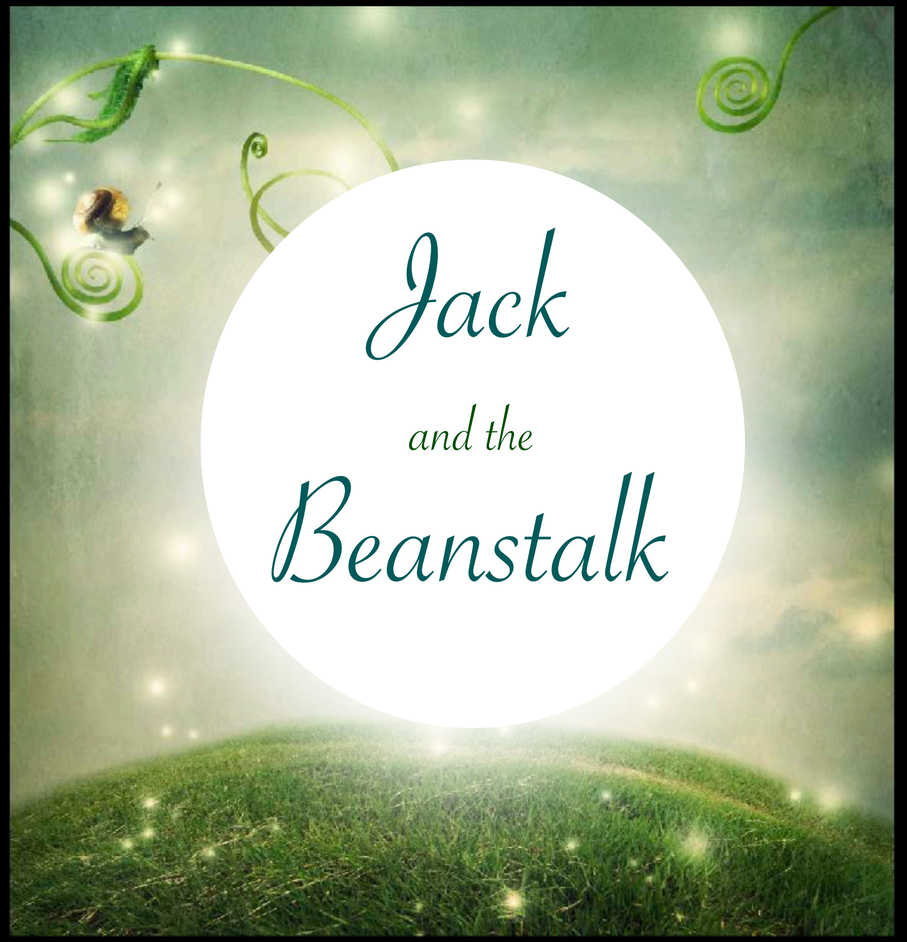
AWS Elastic Beanstalk

- Automates the deployment, management, scaling, and monitoring of your custom applications in AWS
- Just upload your application and it will automatically handle the common tasks to run your application.
- Handles capacity provisioning, load balancing, database management, auto-scaling, and health monitoring

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Elastic Beanstalk

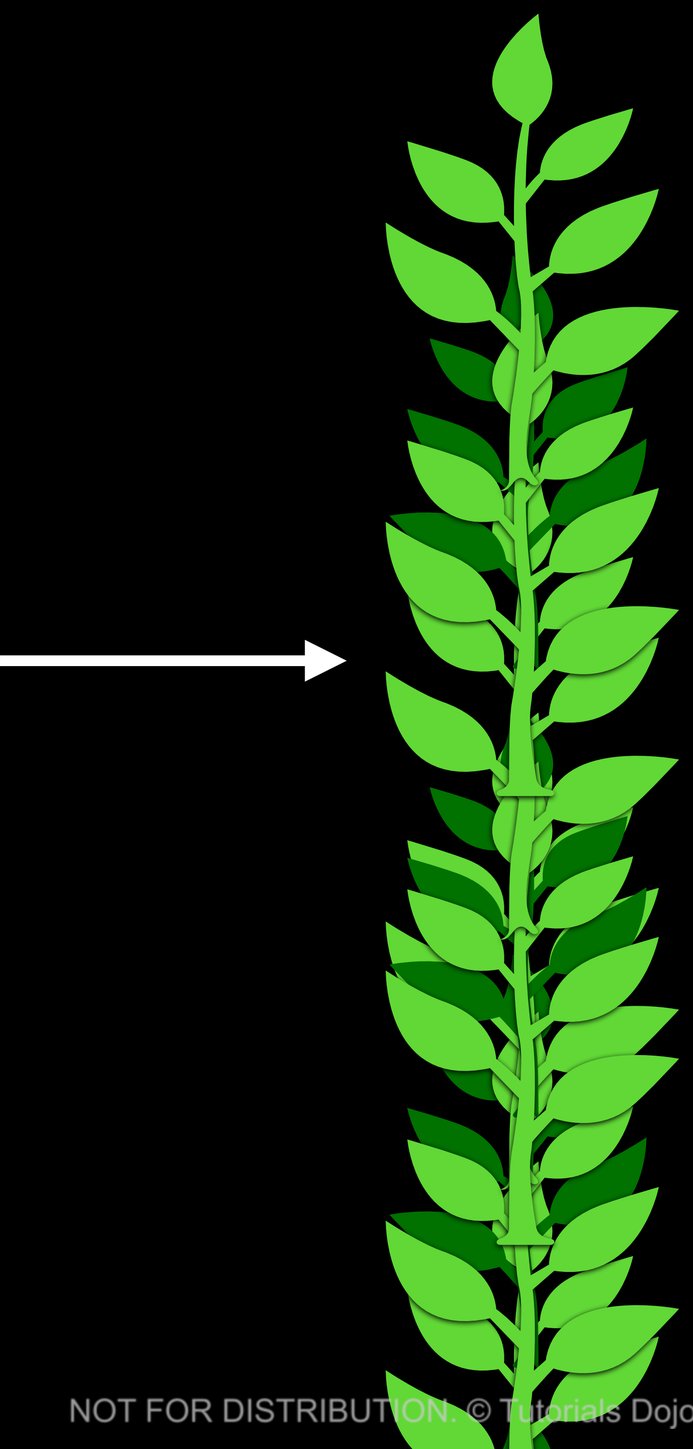




NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Elastic Beanstalk





Your Applications

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon LightSail

- An easy-to-use **Virtual Private Server** (VPS)
- Has its **own web management console**
- Also provides other services like databases, load balancers, DNS records and many more.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Outposts

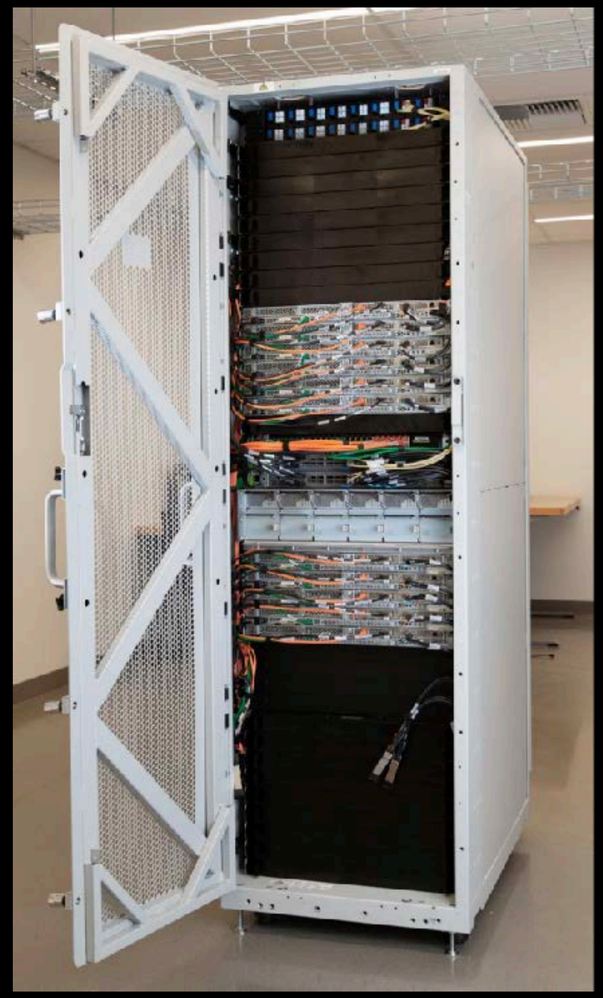
- A hybrid service that allows you to run AWS services, like Amazon EC2, in your on-premises data center

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Outposts





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Container Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Container Services



Amazon ECS



Amazon EKS



AWS Fargate



Amazon ECR

CLI Tools



AWS App2Container (A2C)



AWS Copilot

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Virtual Machine



Container

App Container 1

App Container 2

App Container 3

Guest OS

Can also run...

HYPERVISOR

Bare Metal

Hosted

Host OS

Windows

Firmware

App Container 1

App Container 2

CONTAINER ENGINE

kubernetes

docker

Host OS

Windows

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon ECS

- Amazon **E**lastic **C**ontainer **S**ervice (Amazon ECS)
- A **container orchestration service** that supports Docker containers.
- Allows you to easily install, operate, and scale your cluster management infrastructure in AWS
- Containers are defined in a **task definition** which you use to run an **ECS task** or are **grouped** together as an **ECS service**





- Runs your ECS tasks using:



Amazon EC2



AWS Fargate

- An **IAM Role** can be attached to your ECS task in the `TaskRoleArn` property of your task definition for security control
- Store your Docker Images to:



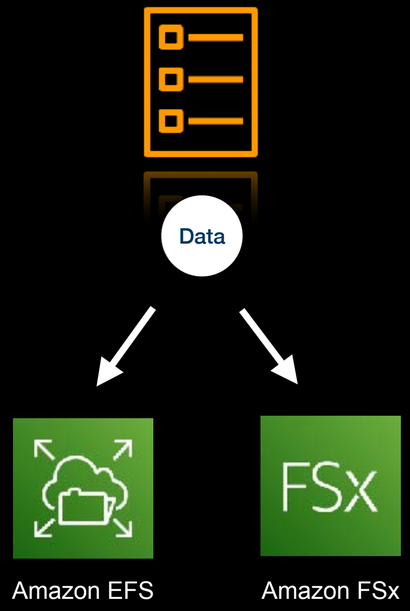
Amazon ECR

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon ECS

Storage



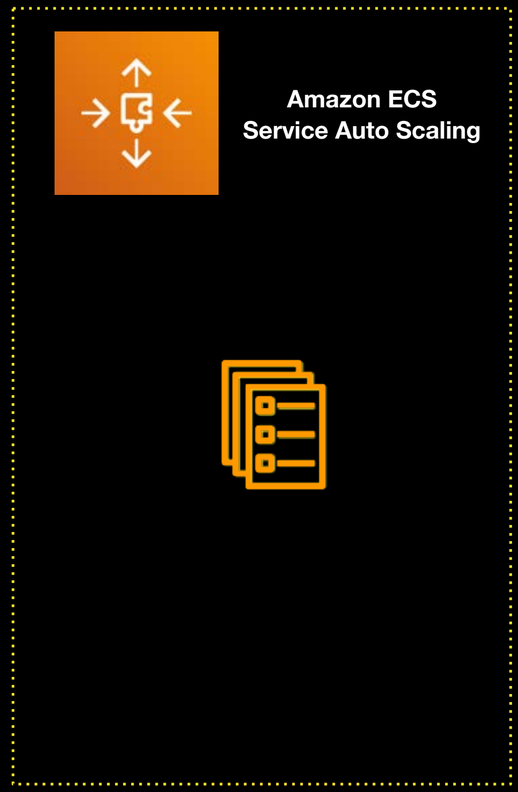
Amazon EFS

Amazon FSx

Integration



Scaling



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EKS

- Amazon **E**lastic **K**ubernetes **S**ervice (Amazon EKS)
- A fully-managed **Kubernetes** service
- Portable, extensible, and open-source platform for managing containerized workloads and services
- Containers are grouped into **Pods** — the basic operational unit for Kubernetes.
- Launches and orchestrates a cluster of compute resources using:



Amazon EC2



AWS Fargate

- Considered as **Cloud-agnostic** as it allows you to easily move your workloads to your on-premises network or to other cloud service providers like Microsoft Azure, Google Cloud Platform (GCP) et cetera.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Fargate

- A **serverless** compute engine
- Works on:



Amazon ECS



Amazon EKS

- Allows you to focus on building your applications without worrying about server provisioning, scaling, and management
- Provides a more **cost-effective** solution than a container running on **Amazon EC2 launch type**
- Runs each ECS task or Kubernetes pod in its own kernel.
- Provides the tasks and pods in their own isolated compute environment.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



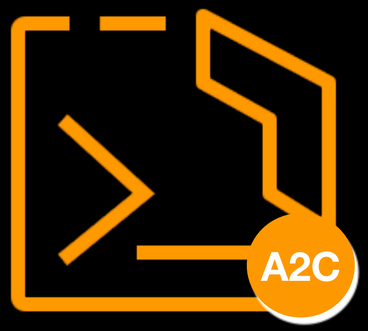
Amazon ECR

- Amazon **E**lastic **C**ontainer **R**egistry (Amazon ECR)
- A fully-managed **Docker container registry**
- Allows you to store, manage, and deploy Docker container images.
- Integrated with **Amazon ECS**



- **Stores your docker images** in a highly available and scalable architecture
- You can use IAM to provide resource-level control of each repository.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS App2Container
(A2C)

- A **command-line tool**
- Transforms .NET & Java applications to **containerized applications**
- Packages the application artifact and dependencies into container images.
- Configures the network ports and generates the ECS task and Kubernetes pod definitions.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Copilot

- Also a **command-line tool**, just like AWS App2Container (A2C)
- Transforms .NET & Java applications to **containerized applications**
- Enables you to quickly launch and easily manage containerized applications on AWS
- Automates the deployment lifecycle of your containers

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Database Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Relational

A C I D

- Atomicity
- Consistency
- Isolation
- Durability

Amazon RDS

Amazon Aurora

Data warehouse

Amazon Redshift

NoSQL

Amazon DynamoDB

Amazon DocumentDB

In-Memory

Amazon ElastiCache

redis

emcached

Other Databases

Amazon Keyspaces

Amazon Neptune

Amazon Timestream

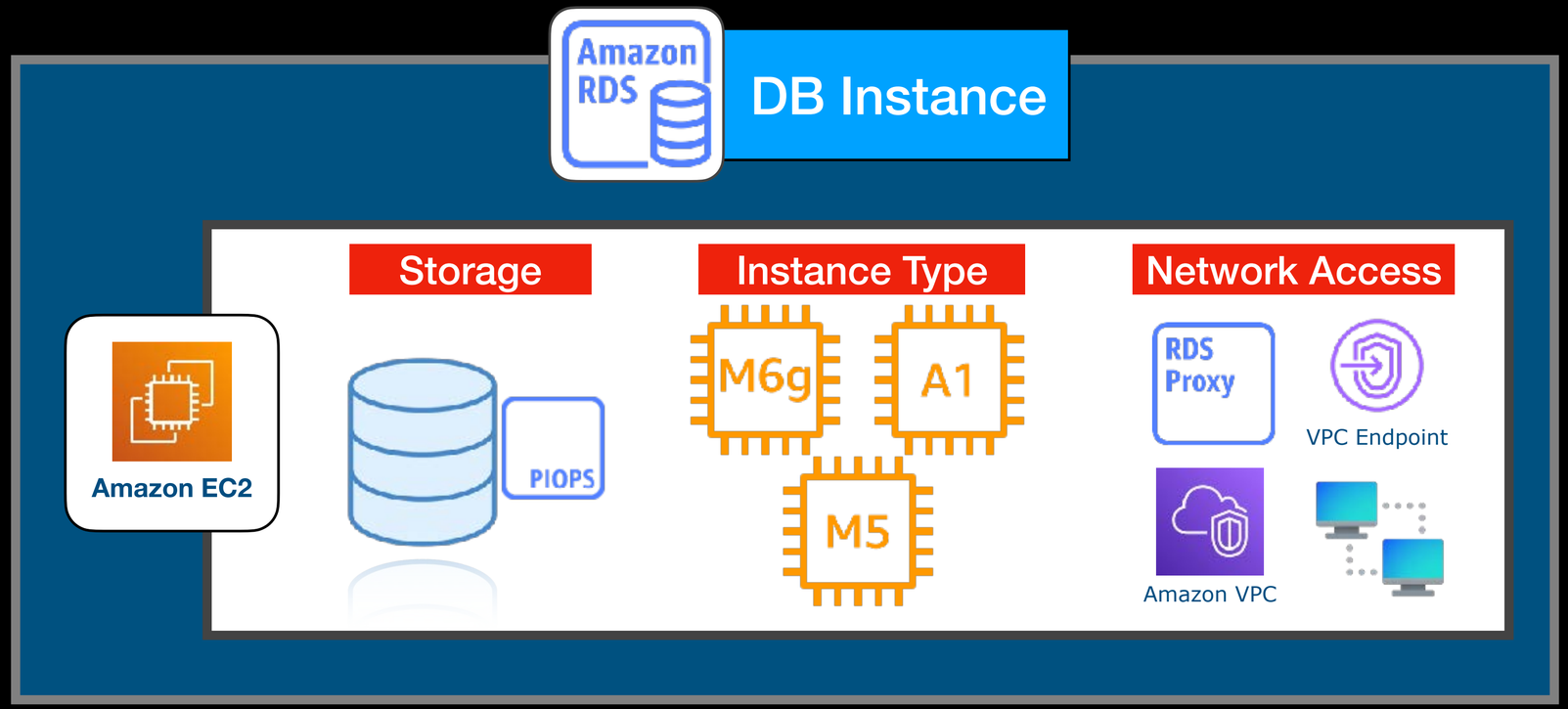
Amazon Quantum Ledger

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

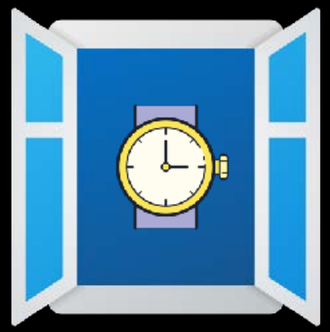


Amazon Relational Database Service
(Amazon RDS)

- A **relational** database that is managed by both you (limited access) and AWS.
- **The time-consuming tasks are handled by AWS** — such as hardware provisioning, patching, backups, and maintenance.
- You can **configure the underlying EC2 instance** used by Amazon RDS



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





- You decide the **actual time** for the patches to be applied on its **maintenance window**
- Can run various types of **database engines:**

Amazon Relational Database Service
(Amazon RDS)

Amazon RDS DB Instance

Microsoft SQL Server

MySQL

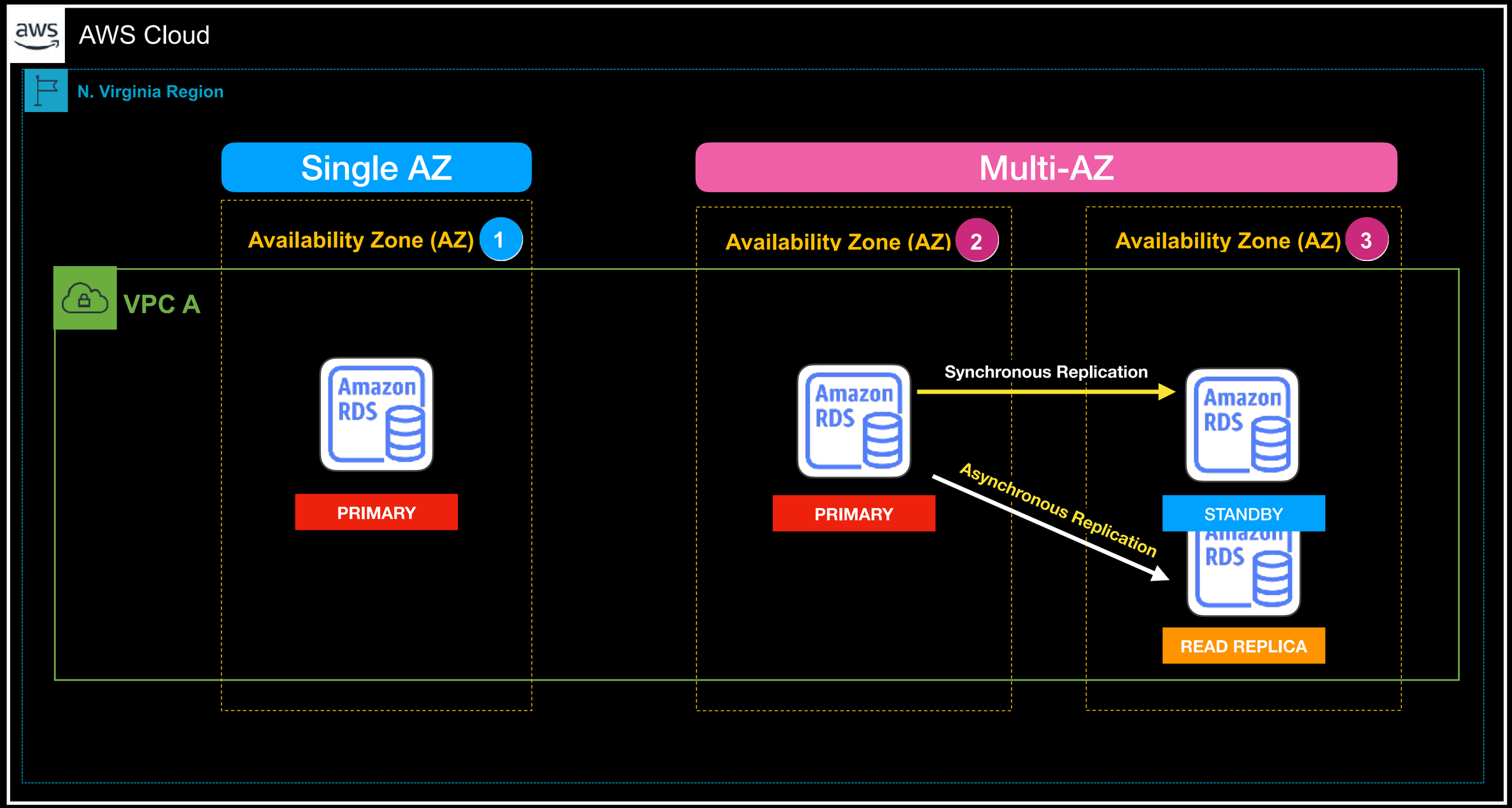
MariaDB

PostgreSQL

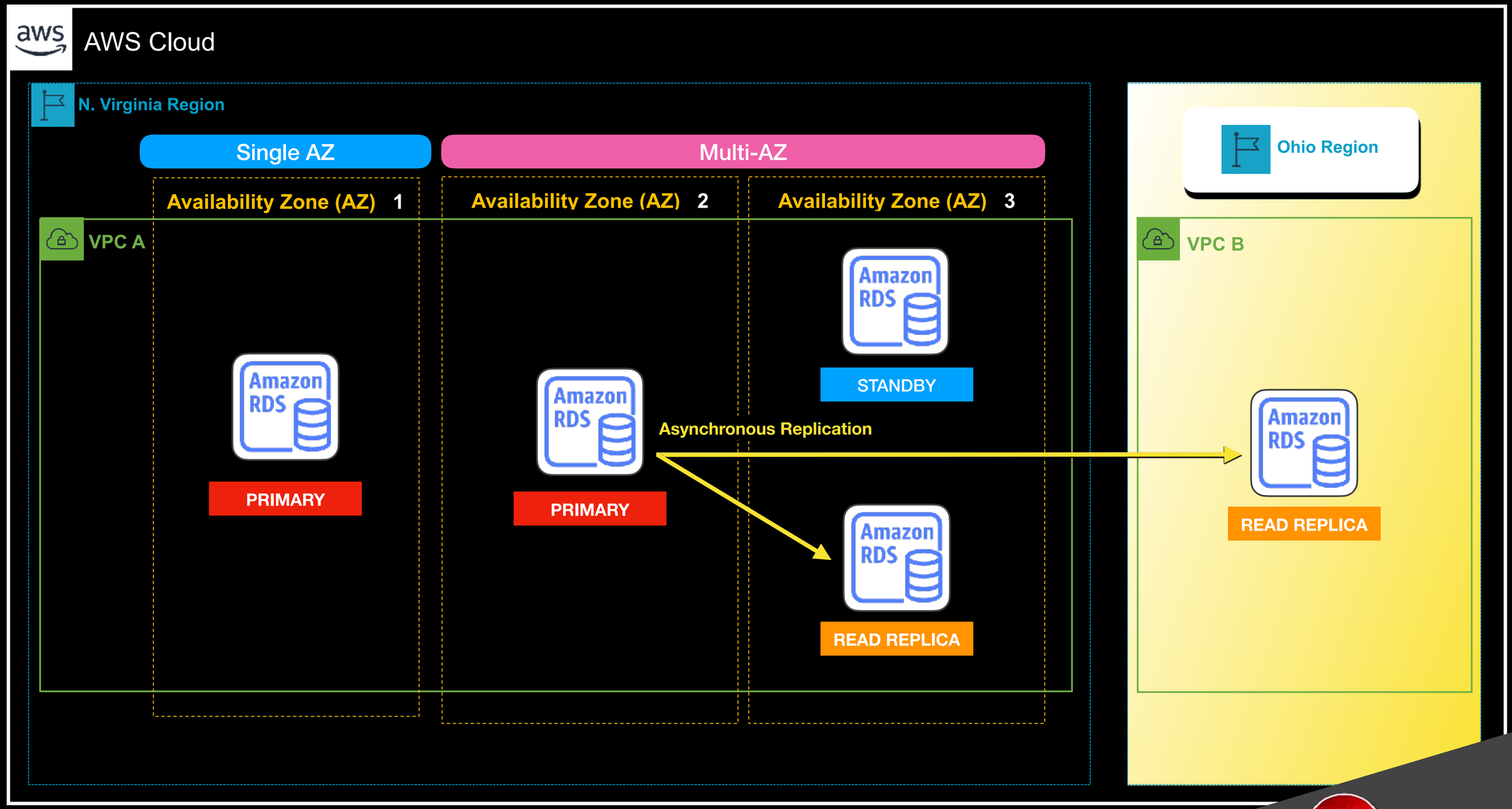
ORACLE

Amazon Aurora

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

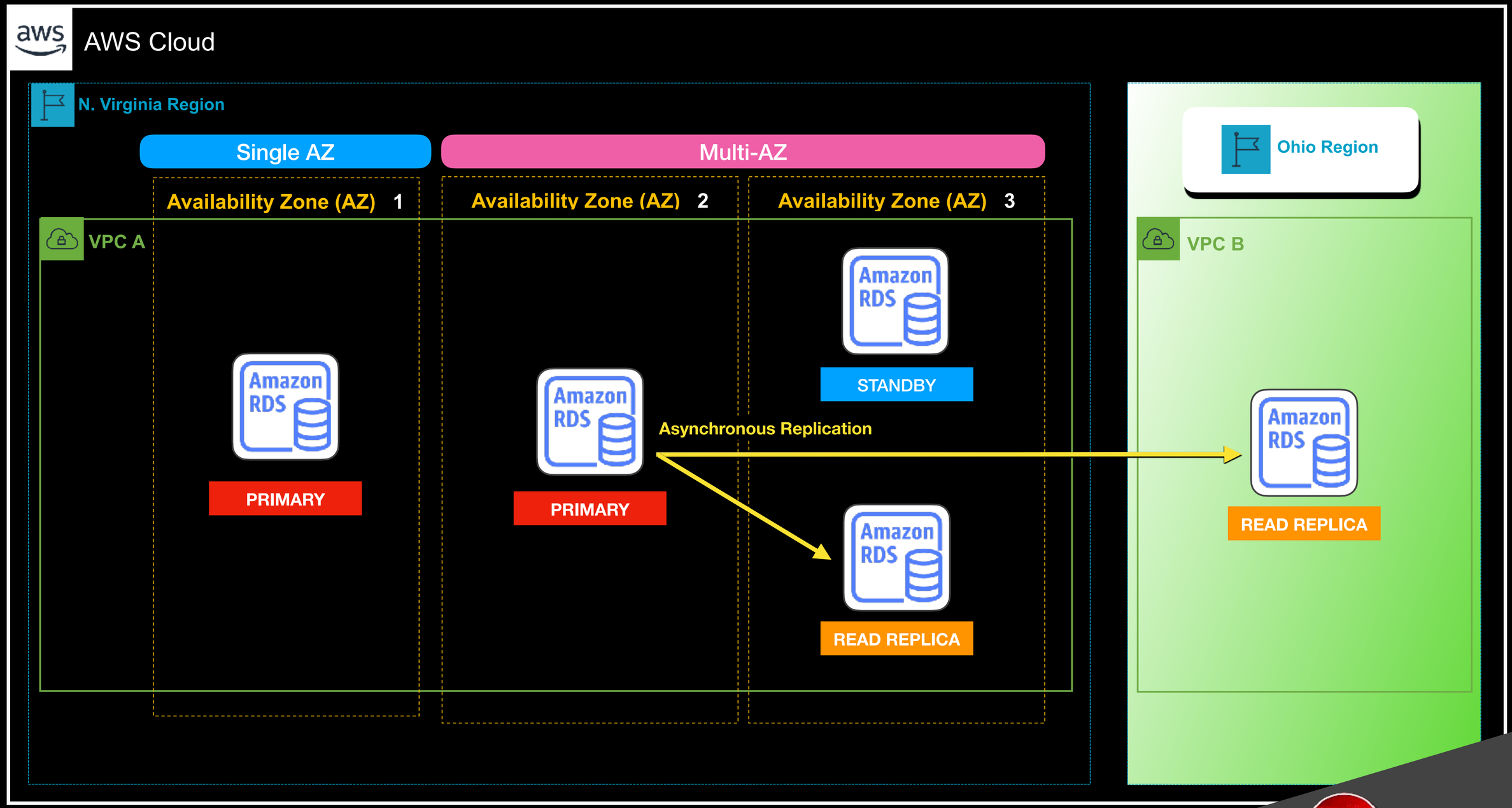


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Tutorials Dojo
www.tutorialsdojo.com



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Tutorials Dojo
www.tutorialsdojo.com



Amazon Aurora

- A type of a **database engine** (that you can run on Amazon RDS) and a **fully managed database** service.
- Compatible with: MySQL PostgreSQL
- Scales automatically, performs faster, and costs lower than other databases
- Can **automatically grow its data storage**
- Deployed as a **database cluster** that consists of:



- **Similar to Multi-AZ Deployments** in Amazon RDS
- A cluster has a **single-master configuration** where applications can only write data to a single, master DB instance.
- In a **multi-master cluster**, all DB instances have read/write capability.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora



Amazon Relational Database Service
(Amazon RDS)



- Suitable for applications that read or write **constantly changing data**, such as Online Transaction Processing applications or OLTP.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Data warehouse



Amazon Redshift

- A fully managed **data warehouse**
- Allows you to **analyze all your data using standard SQL** or through your existing Business Intelligence tools
- Optimized to **analyze relational data** coming from transactional systems, business applications, and other sources for fast SQL queries.
- Offers a **concurrency scaling** feature that supports virtually unlimited concurrent users and concurrent queries
- Has a feature called **Redshift Spectrum** that allows you to query and retrieve structured and semistructured data from files stored in:



Amazon S3

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Redshift



- Primarily used for **Online Analytical Processing or OLAP** applications like data reporting and analytics.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NoSQL Databases



Amazon DynamoDB



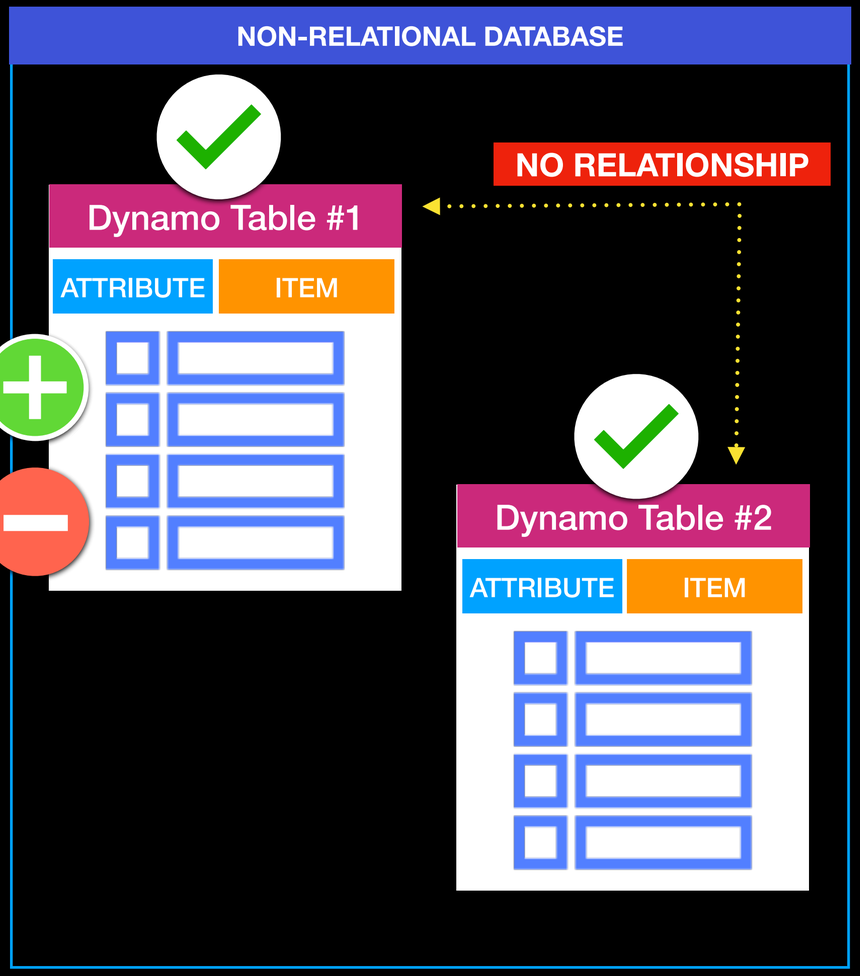
Amazon DocumentDB

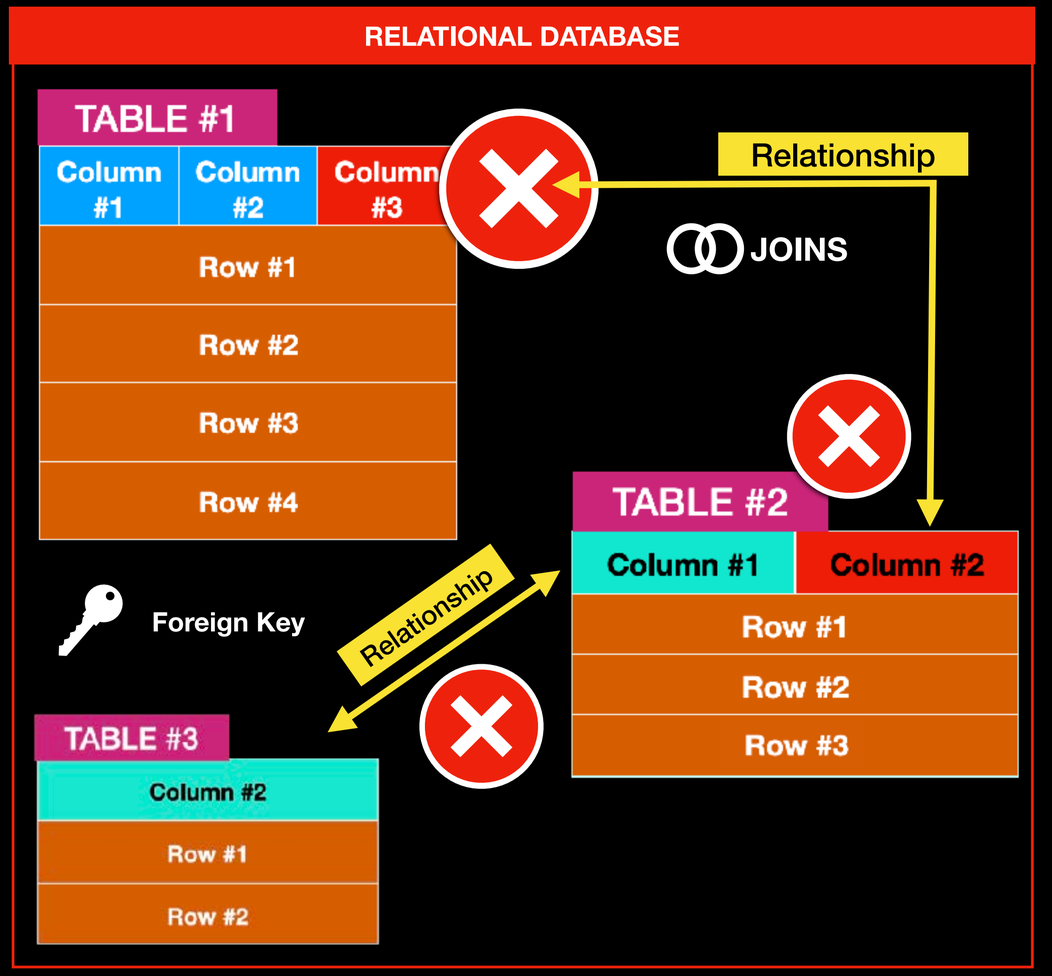
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

- A fully managed **NoSQL database** service
- A non-relational database that **does not have a rigid schema** or extensive table relationships.



Amazon DynamoDB





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DOCUMENT

```
{
  id: 1898,
  gid: “tutorialsdojo1898”,
  firstName: "Jose",
  lastName: "Rizal",
  profile: {
    nationality: “Filipino,
    country: “Philippines,
    birthPlace: “Laguna"
    }
}
```

- A fast, scalable, highly available **MongoDB-compatible database** service.

- A **document**-oriented database program
- Cross-platform, NoSQL database

- Each **document** contains fields and values in **JSON format** with no rigid schema enforced

Amazon DocumentDB

DOCUMENT DATABASE

COLLECTION

Document #1	Field #1	Value #1
	Field #2	Value #2
	Field #3	Value #3
Document #2	Field #1	Value #1
	Field #2	Value #2
	Field #3	Value #3
Document #3	Field #1	Value #1
	Field #2	Value #2
	Field #3	Value #3

RELATIONAL DATABASE

TABLE #1

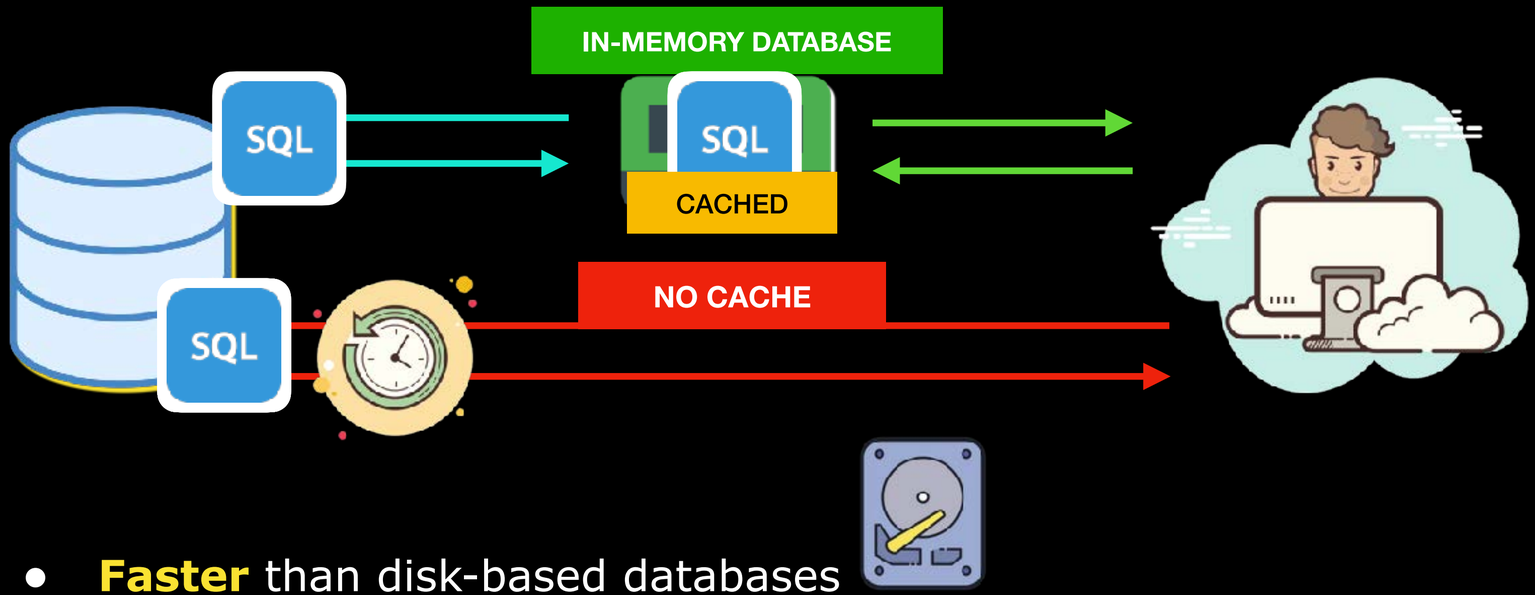
Column #1	Column #2	Column #3
Row #1		
Row #2		
Row #3		
Row #4		

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon ElastiCache

- A **caching service**
- Allows you to set up, run, and scale **open-source in-memory databases** like: emcached redis



- **Faster** than disk-based databases
- Useful for **database caching** that eliminates unnecessary frequent calls to the database just to **return identical datasets**
- Useful for real-time analytics, distributed session management, geospatial services, and many more

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon ElastiCache





emcached



Sub-millisecond latency



Data Partitioning



Can be integrated to your apps with minimal code change





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



emcached



Amazon ElastiCache for Memcached

- Based on the open-source **Memcached** in-memory data store.
- Suitable for building a simple, scalable caching layer for your data-intensive apps.
- **Multithreaded** — it can utilize multiple processing cores.
- **Lacks data replication capability**
- **Does not:**
  - Support Advanced Data Structures
  - Provide Highly Available Caching Layer

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



redis

stands for

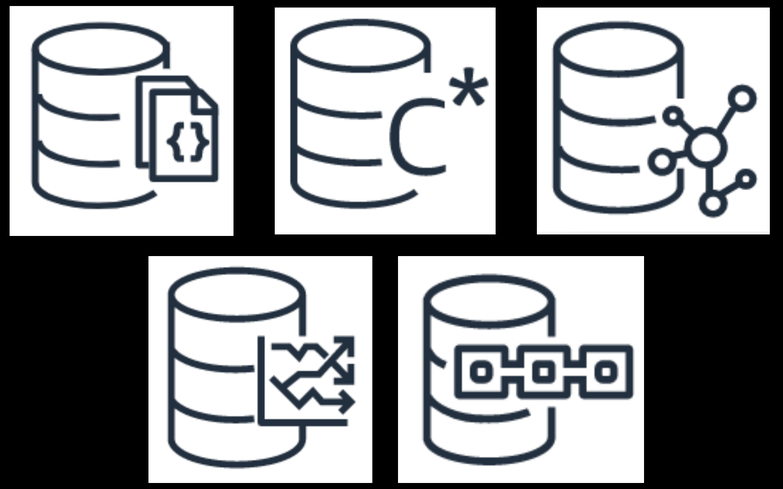
REmote **DI**ctionary **S**erver



Amazon ElastiCache for Redis

- Based on the open-source **Redis** in-memory data store.
- Provides:
  - Advanced Data Structures
  - Pub/Sub messaging
  - Geospatial support
  - Point-in-Time Snapshot support
- Has a **replication feature** that provides high availability via data replication.
- You can enable the **Cluster Mode** in Redis to have multiple primary nodes and replicas across two or more Availability Zones.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Other Databases

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon KeySpaces

- A scalable, highly available, and managed **Apache Cassandra**–compatible database service



- An open-source, **wide column data store** that is designed to handle large amounts of data.

- **Run your Cassandra workloads** on AWS without having to provision, patch, or manage servers.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





Amazon Neptune

- A fast, reliable, fully-managed **graph database** service
- Makes it easy for you to build and run applications that work with **highly connected datasets**
- Allows you to **store billions of relationships** and query your data graphs with **milliseconds latency.**
- **Uses nodes to store data entities and edges** to store relationships between entities.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





Amazon Timestream

- A fast, scalable, and **serverless time series database** service
- Primarily used **for Internet-of-Things and operational applications.**
- **Track the changes of your data**
- Can be used to track stock prices, temperature measurements, and the CPU utilization of an EC2 instance over a specific amount of time.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

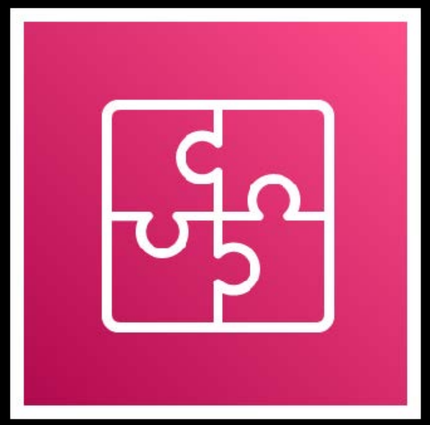


Amazon Quantum Ledger (Amazon QLDB)



- A fully managed **ledger database** service.
- Provides a transparent and **immutable transaction log** that is owned by a central trusted authority.
- Creates logs that are **cryptographically verifiable**
- Provide an **auditable history of all changes** made to your application data.
- Can be used to track each and every application data change.

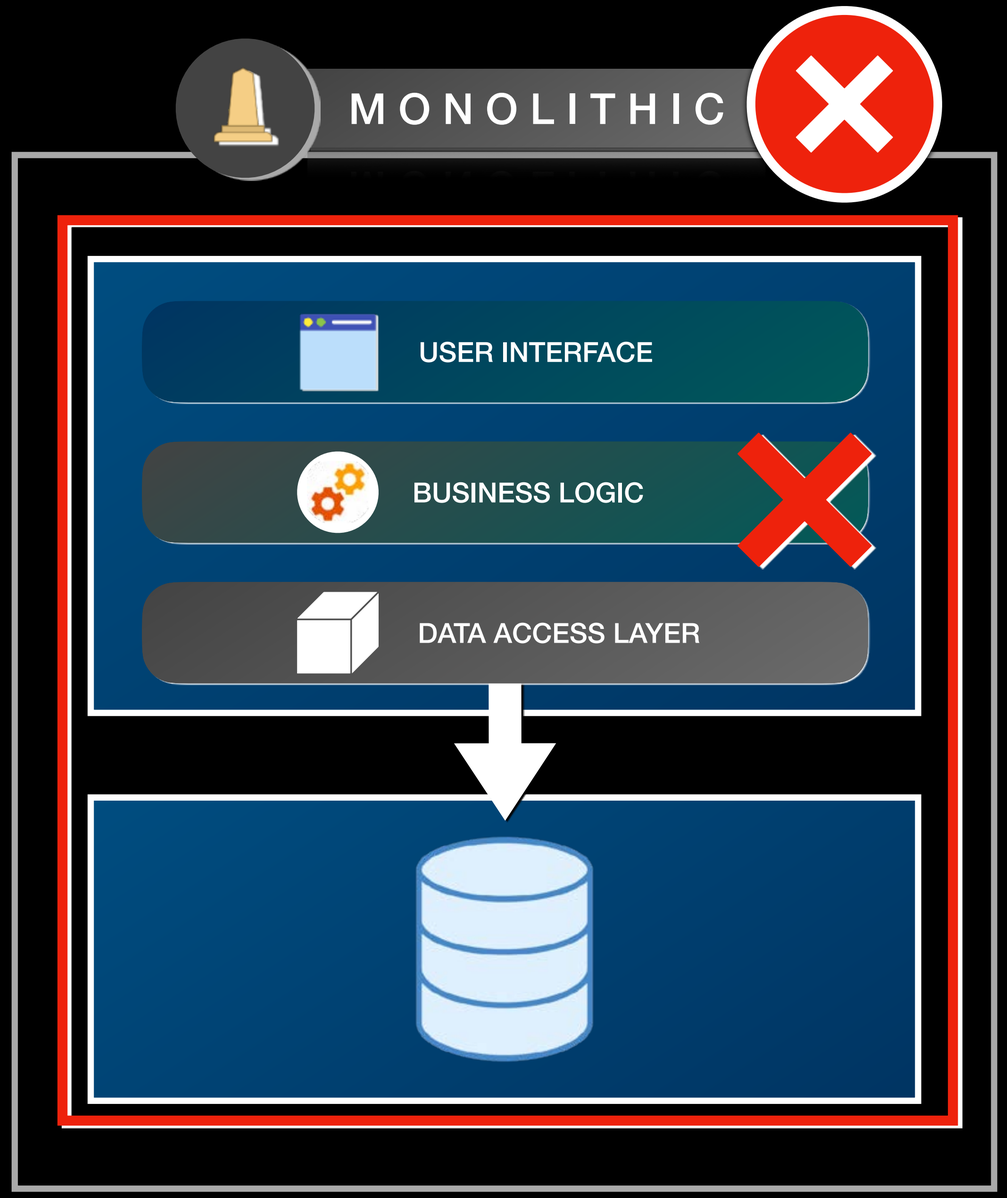
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

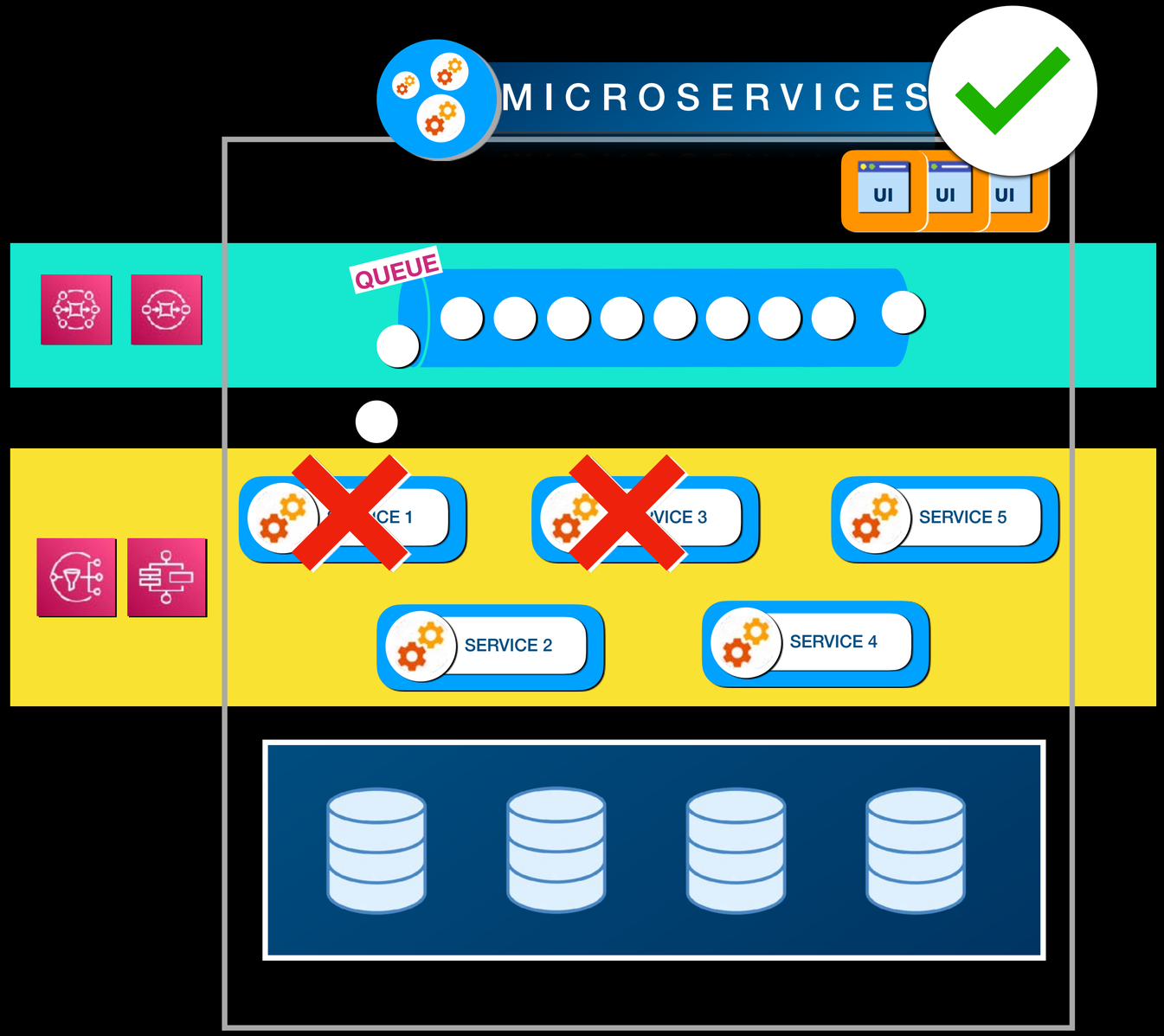


Application Integration Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Application Integration Services





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

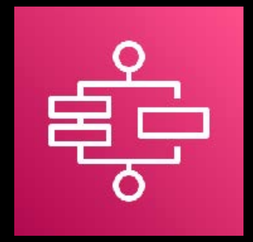
Application Integration Services



Amazon Simple Queue Service (Amazon SQS)



Amazon Simple Notification Service (Amazon SNS)



AWS Step Functions



Amazon MQ



Amazon EventBridge

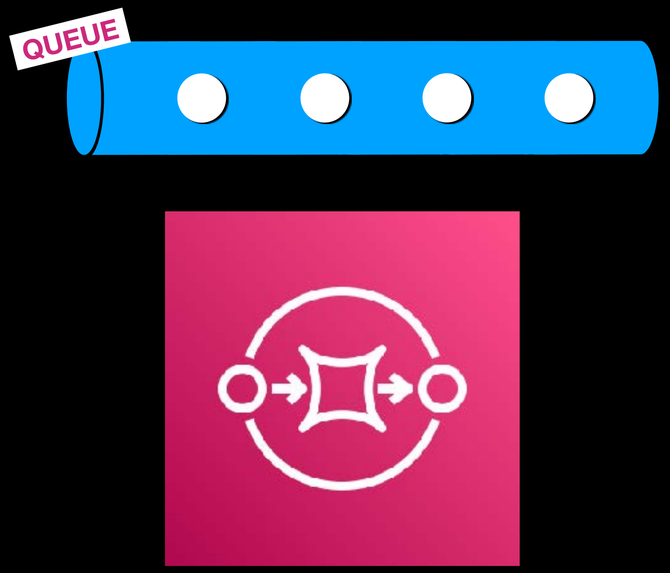


AWS AppSync



Amazon AppFlow

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Simple Queue Service (Amazon SQS)

- A fully managed message queueing service



- The messages can be consumed or processed by:


Amazon EC2

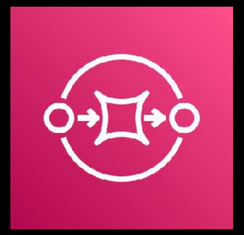

AWS Lambda


Amazon ECS


Other Consumers

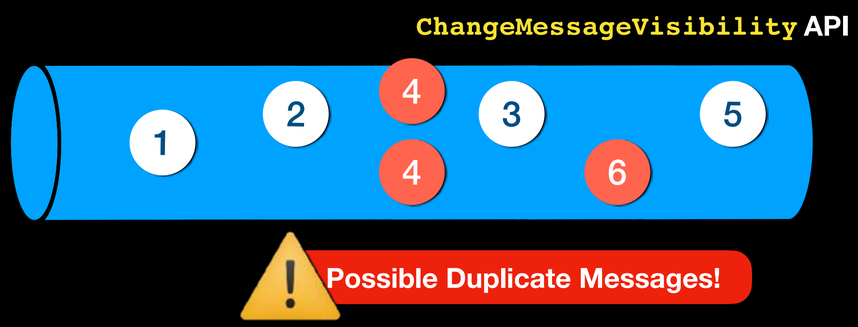
- Can replace your traditional message-oriented middleware without having to manage any servers or resources

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

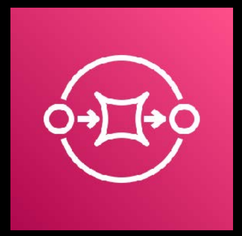


Amazon SQS

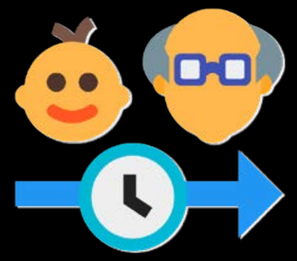
TYPES

	STANDARD	FIFO
		First In, First Out
DELIVERY	 At Least Once	 Exactly Once
ORDERING	**Best Effort** Messages might be delivered in a **different order**	**Preserves the exact order** **in which the messages are received**
THROUGHPUT	**HIGH** 	**LIMITED** 

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

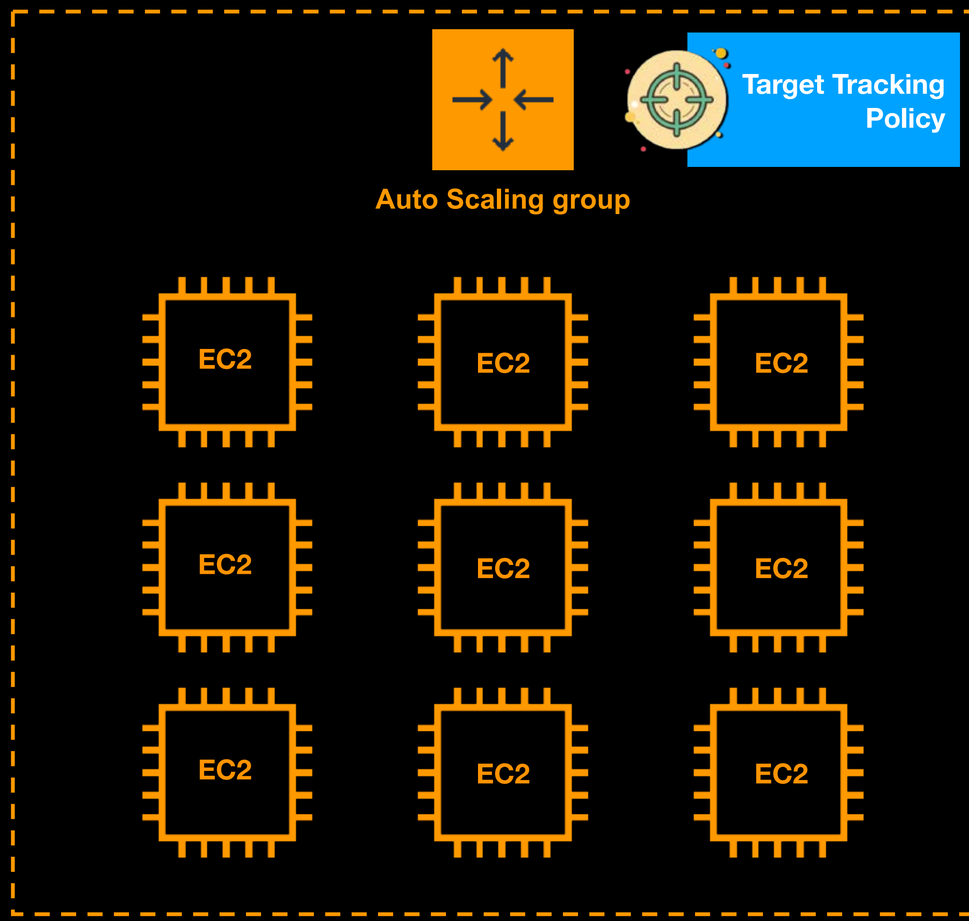


Amazon SQS

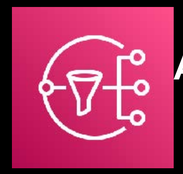




- **Age** of the Oldest Message
- **Queue Depth**
- **Number** of Messages



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



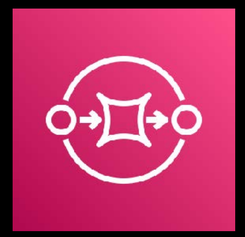
Amazon Simple Notification Service (Amazon SNS)



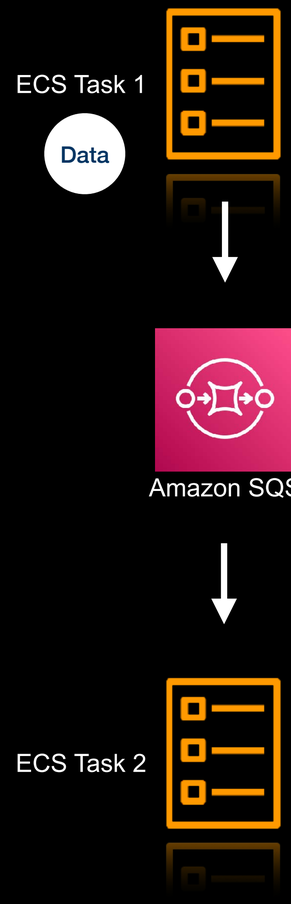
Amazon ECS



Amazon S3 Bucket



Amazon SQS

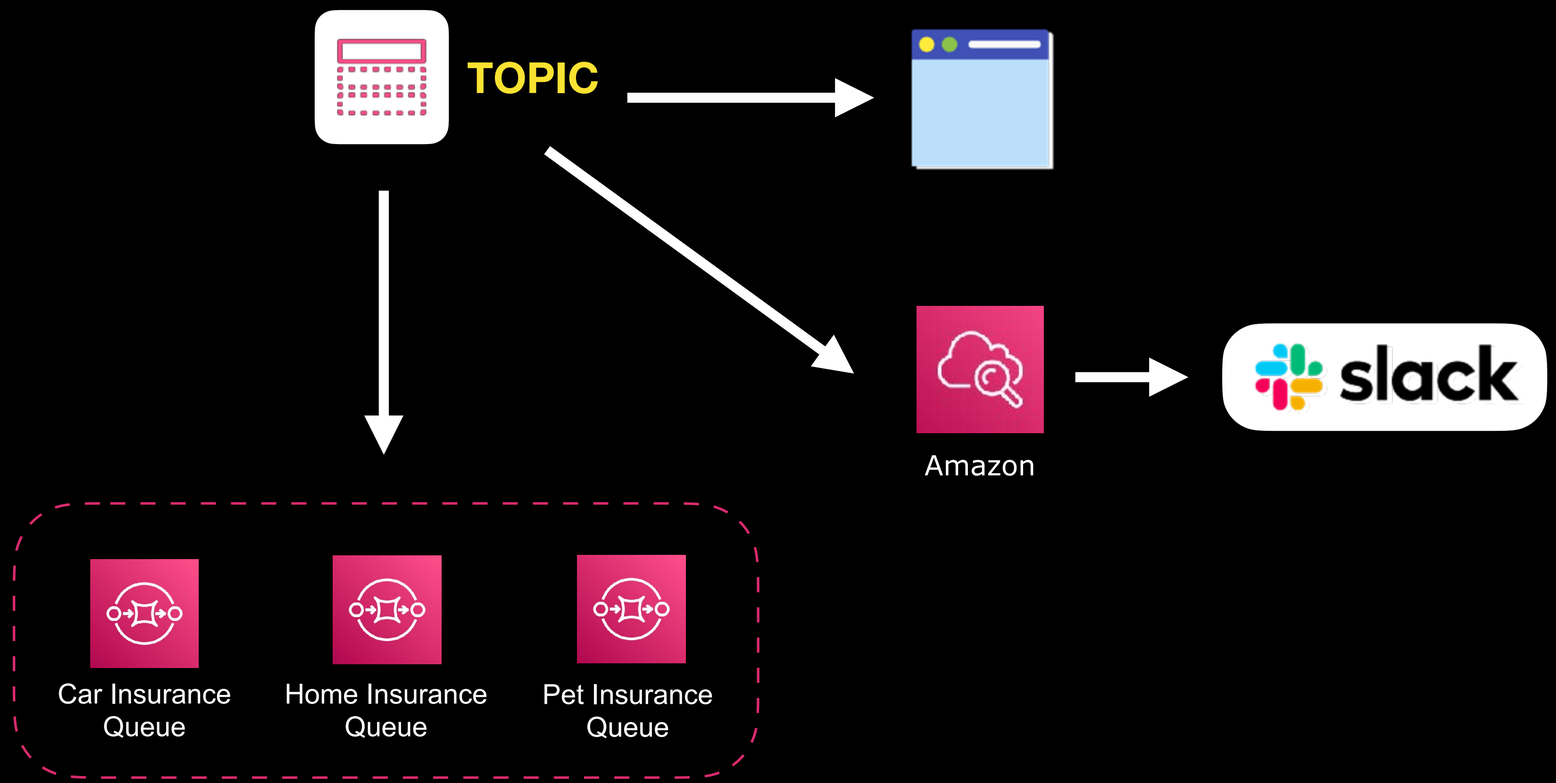


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Simple Notification Service (Amazon SNS)

- A fully managed **messaging and notification service**
- **Enables you to communicate between systems** through publish/subscribe patterns or pub/sub messaging
- Messaging via mobile push, email, or SMS



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

FANOUT EVENT NOTIFICATIONS



Amazon RDS Events



TOPIC

Message Filtering



Filter by

QUOTE Type



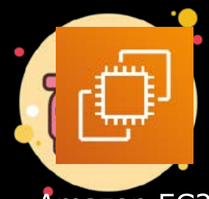
Car Insurance Queue



Home Insurance Queue



Pet Insurance Queue



Amazon EC2



Amazon ECS



AWS Lambda

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

FANOUT EVENT NOTIFICATIONS

SQS QUEUES

CONSUMERS

Amazon SNS with Message Filtering

Custom Events

SNS TOPIC

Message Filter

Filter by

QUOTE Type

Car Insurance Queue

Amazon EC2

Home Insurance Queue

Amazon ECS

Pet Insurance Queue

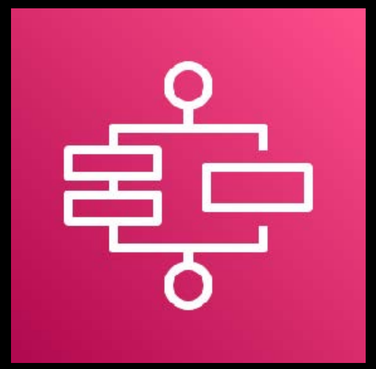
AWS Lambda

Amazon CloudWatch

slack

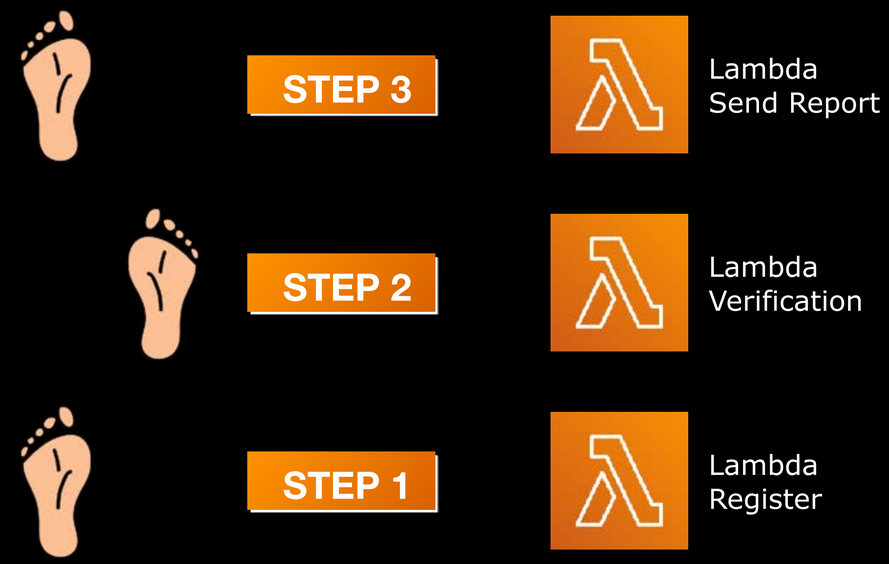
Tutorials Dojo
www.tutorialsdojo.com

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

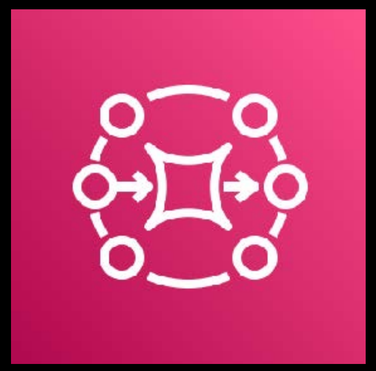


AWS Step Functions

- A **serverless function orchestrator** for AWS Lambda
- Allows you to **orchestrate multiple AWS Lambda functions**, in order to achieve a specific workflow
- Enables you to create a **state machine** containing a combination of steps, activities and service tasks



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon MQ

- A managed **message broker** service
- Uses the open-source Apache ActiveMQ message broker
- The "MQ" in Amazon MQ stands for **Message Queue**, which is a form of asynchronous communication
- Works like Amazon SQS but **supports more messaging protocol types**
- Supports Java Message Service (JMS), .NET Message Service (NMS), AMQP, MQTT, WebSocket and many others.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EventBridge

- A **serverless event bus** service
- Enables you to connect applications together using data from your own applications, Software-as-a-Service (SaaS) applications, and other AWS services.
- **Uses the same service API, endpoint,** and the underlying service infrastructure of:



- Recommended to be used for your own applications, 3rd party Software-as-a-Service apps, and other external sources
- Suitable for building **event-driven applications**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



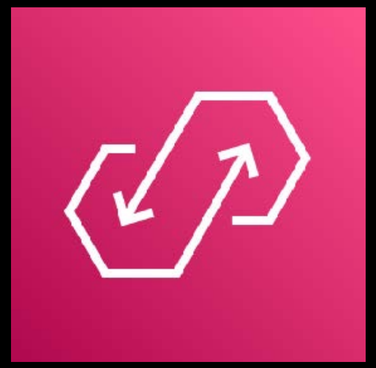
AWS AppSync

- A managed service that uses GraphQL
- GraphQL is a **data query language** that basically allows you to query your REST APIs
- Has different types of **schema**

QUERY	Read Data
MUTATION	Write Data
SUBSCRIPTION	Download/Upload Data

- Only fetches the data that you want and not the entire data set
- Unlike REST API, you can query different APIs or resources easily using a single API call
- Uses a **Resolver** which populates the data in your schema
- Simplifies application development by easily integrating GraphQL with your applications

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon AppFlow

- A fully managed **integration service**
- Enables you to **securely transfer data between various systems** such as your Software-as-a-Service (SaaS) applications and different AWS Services
- Supports different SaaS apps such as Salesforce, Marketo, Slack, ServiceNow and many more
- Can be integrated with other AWS services
- **Allows you to run your data flows** on-demand, by schedule or as a response to a business event
- Provides you with powerful data transformation capabilities like filtering and validation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Identity Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Identity Services



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Identity Services



AWS Identity & Access Management (IAM)



AWS Single Sign-On



Amazon Cognito



AWS Directory Service

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Identity & Access Management (IAM)

- The primary **identity service** in AWS
- Allows you to **manage access to various AWS services** and resources

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Identity & Access Management (IAM)



IAM USER



IAM GROUP



PASSWORD



ACCESS KEYS



IAM POLICY



Permission 1



Permission 2



Permission 3



Permission 4



IAM ROLE



Permission 1



Permission 2



Permission 3



Permission 4

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Let you **add user sign-up, sign-in, and access control** features to your web or mobile apps
- Allows users to log in to your application with their:

and other social media accounts!

Amazon Cognito

Microsoft **Active Directory**

SAML

Security Assertion Markup Language

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



USER POOL



IDENTITY POOL

Amazon Cognito

For **Authentication**

Users can sign in by authenticating through their **social identity providers**

For **Authorization**

Users can obtain **temporary and limited-privilege AWS credentials** that authorize access to other AWS services

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Single Sign-On



- A **single sign-on service** in AWS
- Allows a user to **log in with a single ID and password** to access multiple and independent, software systems
- Provides a **user portal** that allows users to access the roles that they can assume
- Offers pre-configured SAML integrations to many business applications

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Directory Service

- A managed Microsoft **Active Directory**
- Does not require you to synchronize or replicate data from your existing Active Directory to the cloud
- No need to install and manage an Active Directory domain controller
- Improves security and minimizes administrative overhead
- **Allows you to assign IAM roles** to your Active Directory users and groups
- Allows you to assign IAM roles to your on-premises Microsoft Active Directory using:



AD Connector

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

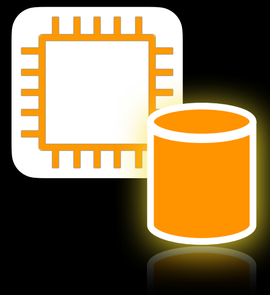


AWS Storage Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Storage Services

Built-in component and NOT a full-fledged AWS Service



Amazon EC2 Instance Store



Amazon Elastic Block Store (Amazon EBS)



Amazon Simple Storage Service (Amazon S3)



Amazon S3 Glacier



Amazon Elastic File System (Amazon EFS)



Amazon FSx for Lustre



Amazon FSx for Windows File Server



AWS Backup



AWS Storage Gateway

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Underlying Host Computer that powers your



Amazon EC2 Instances



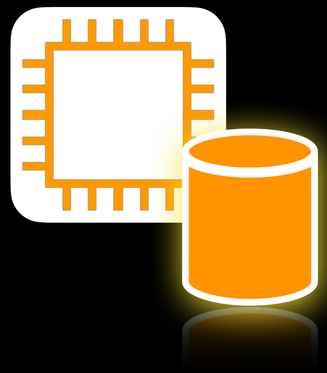
e·phem·er·al

/əˈfem(ə)rəl/

adjective

lasting for a very short time.
"fashions are ephemeral"

Similar: transitory | transient | fleeting | passing | short-lived | momentary



Amazon EC2 Instance Store

- A temporary or ephemeral block-level storage
- Uses the local disks or storage volumes that are physically attached to the underlying host computer of the Amazon EC2 instance.
- Provides low-latency access to your data
- Loses its stored data if:
  - The underlying local storage fails
  - The Amazon EC2 Instance:



Stops



Hibernates



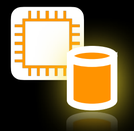
Terminates

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic Block Store
(Amazon EBS)

- A persistent block-level storage service
- Your data will still be there even if you stop, restart, or terminate your Amazon EC2 instance, unlike:



Amazon EC2
Instance Store

- Also called EBS Volumes
- Mounted or attached to your Amazon EC2 instances
- Zonal in scope — you can only attach a volume to any EC2 instances in the same Availability Zone.
- Can be encrypted at rest using:



AWS Key Management Service
(AWS KMS)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon Elastic Block Store
(Amazon EBS)



Solid State Drive (SSD)



Hard Disk Drive (HDD)

Read & Write Speeds	 Fast !	 Slow…
Use Case	For workloads with frequent read/write operations	For data archiving, backups or throughput-oriented storage
Dominant Performance Attribute	IOPS Input/Out operations Per Second	Throughput Megabit per second (Mbps)
Can be used as **Boot Volume** for  **Amazon EC2** ?	Yes	No

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Tutorials Dojo
www.tutorialsdojo.com

Amazon Elastic Block Store
(Amazon EBS)

TYPES

Faster data retrieval than:

Amazon S3

Amazon EFS



Solid State Drive (SSD)



Hard Disk Drive (HDD)

gp — General Purpose SSD

st — Throughput Optimized HDD

io — Provisioned IOPS SSD

sc — Cold HDD

Can only be attached to a **single** Amazon EC2 at a time

Can be used as **Boot Volume** for Amazon EC2

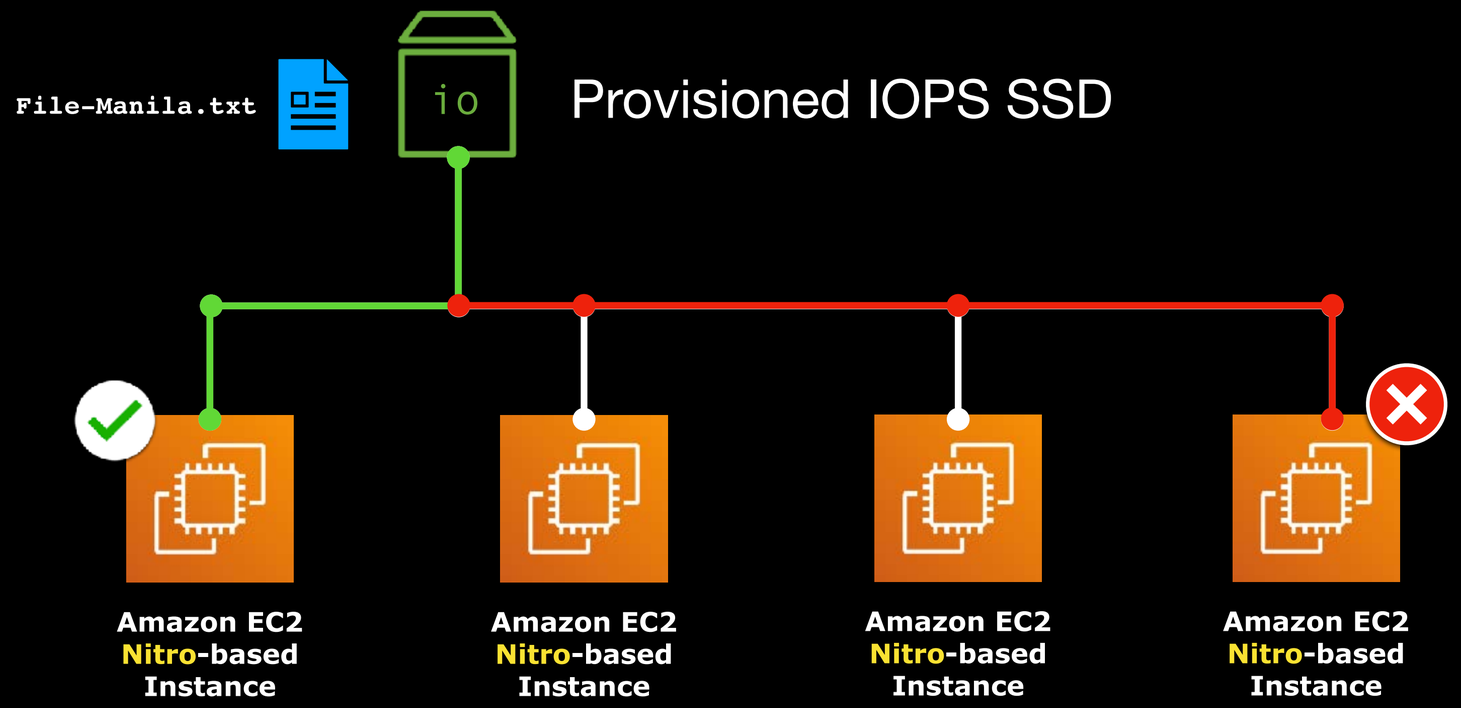
Cannot be used as a Boot Volume

Amazon EC2

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon Elastic Block Store
(Amazon EBS)

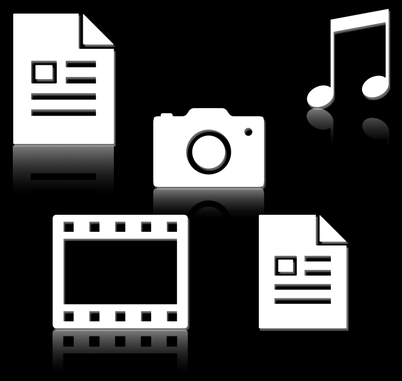
EBS Multi-Attach



No concurrent file modification

Amazon EFS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Simple Storage Service
(Amazon S3)

- An object storage service
- Highly durable and scalable
- Can store virtually unlimited amounts of data
- The files are called “objects” that you upload to an S3 Bucket
- Access files via a REST API call

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon S3 Storage Classes



S3 Standard

For **frequently accessed** data



S3 Intelligent-Tiering

For changing or
unknown access patterns



S3 Standard-IA
(Infrequent Access)



S3 **One** Zone-IA
(Infrequent Access)

For storing long-lived,
yet **less frequently accessed** data



S3 Glacier



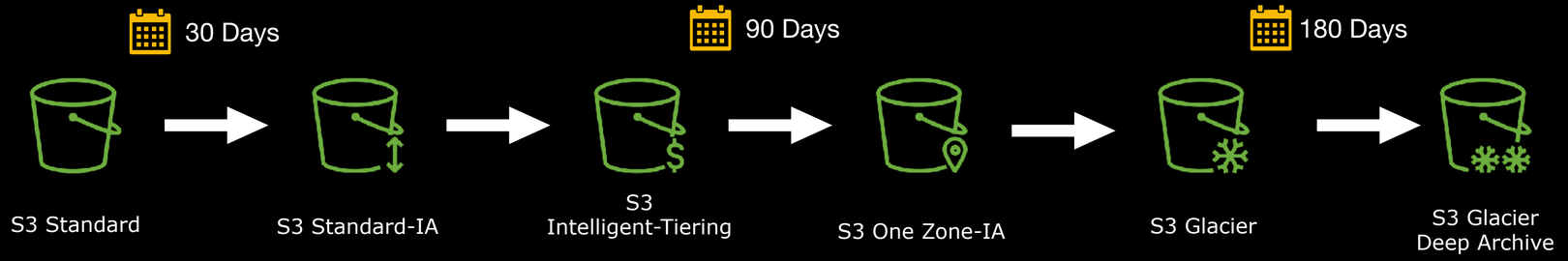
S3 Glacier **Deep** Archive

For **low-cost long-term storage**
and data archiving

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Lifecycle Policy





Access Control List
(ACL)

- Secure access to your S3 buckets and objects



Bucket Policy

- Control external access to your Amazon S3 bucket.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Versioning



Multi-Factor Authentication
(MFA)

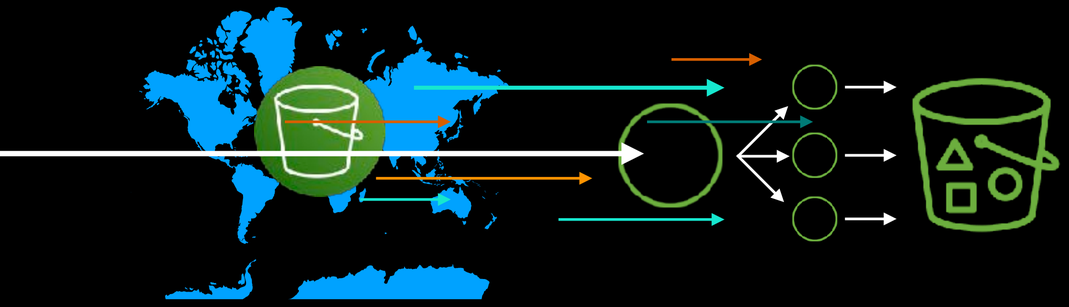
- Prevent accidental data deletion in Amazon S3.



Cross Region Replication (CRR)

- Automatically replicate objects to a different AWS Region for backup purposes

---



Transfer Acceleration

Multipart Upload

- Accelerate or expedite the data transfer (upload/ download) of S3 objects

…and many more S3 features!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3 Glacier

- One of the storage classes in Amazon S3
- Has its own web management console apart from Amazon S3
- Based on the word — **Glacier**:
  - Rarely Accessed Data (Cold)
  - Frequently Accessed (Hot)

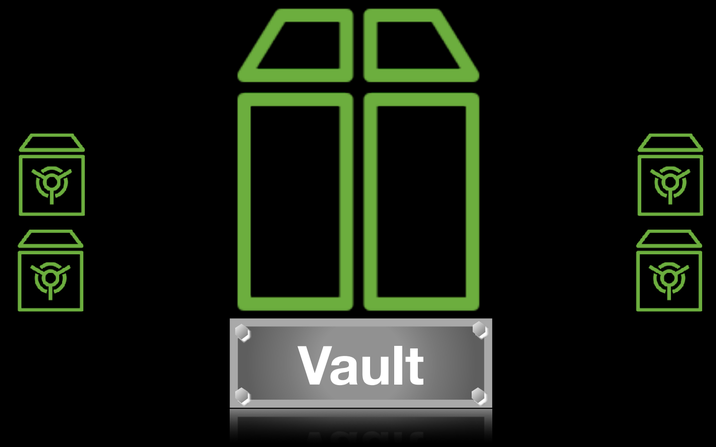


Cold HDD

- Low-cost storage for data archiving and long-term backup.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





S3 Glacier		S3 Glacier Deep Archive
LOW $ $	COST	LOWEST $
90 Days	MINIMUM STORAGE DURATION	180 days
You will be billed for the entire 90 Days	DATA DELETED AFTER 1 DAY (24 HOURS)	You will be billed for the entire 180 Days
Normal storage usage charge	DATA DELETED AFTER 90 DAY	You will be billed for the entire 180 Days
Normal storage usage charge	DATA DELETED AFTER 180 DAYS	Normal storage usage charge

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Standard

VS



S3 Glacier

HIGHEST $ $ $	**COST** Timed Storage - Byte Hours	**LOWEST $**
None	**MINIMUM STORAGE DURATION**	**90 days**
Regular storage usage charge (24 hours)	**DATA DELETED AFTER 1 DAY (24 HOURS)**	You will be billed for the **entire 90 Days**
Regular storage usage charge (30 days)	**DATA DELETED AFTER 30 DAYS**	You will be billed for the **entire 90 Days**
Regular storage usage charge (90 days)	**DATA DELETED AFTER 90 DAYS**	Regular storage usage charge (90 Days)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Archive Retrieval Options

	EXPEDITED	STANDARD	BULK
 **S3 Glacier**	1 - 5 minutes	3 - 5 hours	5 - 12 hours
 **S3 Glacier Deep Archive**	NOT AVAILABLE	Within 12 Hours	Within 48 hours

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic File System
(Amazon EFS)

- A scalable shared file storage service
- Provides a POSIX-compliant (Portable Operating System Interface) shared file system
- Can be simultaneously accessed by multiple Amazon Linux EC2 instances in different Availability Zones.
- Uses the Network File System (NFS) protocol. Works as a file share
- Only supports:



Linux Servers



=

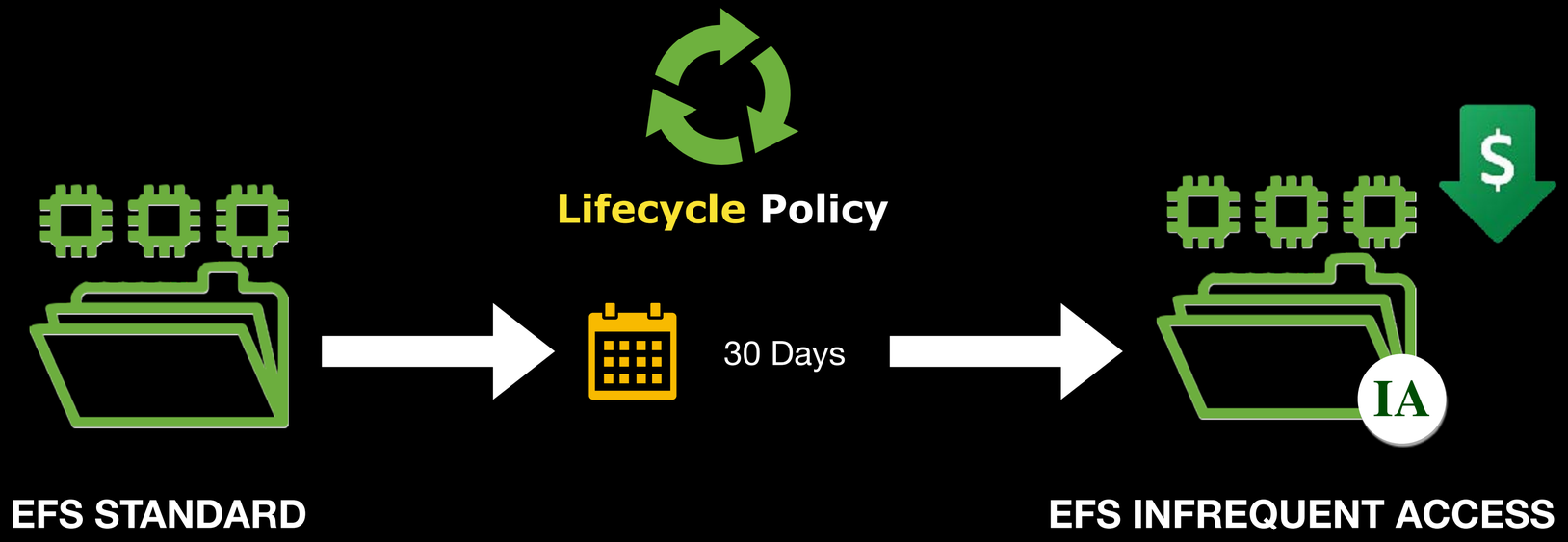


Amazon FSx for
Windows File Server

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic File System
(Amazon EFS)



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx



Amazon FSx for Lustre



Amazon FSx for
Windows File Server

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic File System
(Amazon EFS)

- A scalable shared file storage service
- Provides a POSIX-compliant (Portable Operating System Interface) shared file system
- Can be simultaneously accessed by multiple Amazon Linux EC2 instances in different Availability Zones.
- Uses the Network File System (NFS) protocol
- Only supports:



Linux Servers

Amazon FSx for Lustre

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

lustre®
open-source, parallel file system

= Linux Cluster



Amazon FSx for Lustre

- a parallel file system used for large-scale cluster computing.
- Primarily used for High-Performance Computing, Machine Learning, or HPC applications
- For workloads that need high-performance parallel storage for frequently accessed hot 🥵 data.
- Provides a throughput of hundreds of gigabytes per second
- Offers millions of IOPS
- You can mount an Amazon FSX for Lustre file share to:

Amazon EC2 Amazon ECS Amazon EKS

- Use the CSI Container Storage Interface (CSI) to connect to your Amazon EKS cluster.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx for Windows File Server

- A fully managed Microsoft Windows file server service
- Uses the Server Message Block (SMB) protocol
- Can be integrated to your existing:
  - Microsoft **Active Directory**
  - AWS Managed Microsoft AD
- Can be used as shared file storage for your:
  - Microsoft **SharePoint**
  - Microsoft **SQL Server**
  - Microsoft **Containers**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

- A fully managed backup service
- Automates your server and database backup processes.



AWS Backup

Service-level backups

- Amazon FSx
- Amazon EFS
- Amazon DynamoDB
- Amazon EC2

Service-level snapshots

- Amazon Aurora
- Amazon RDS
- Amazon EBS
- AWS Storage Gateway

7 Days (Default)

35 Days (Maximum)

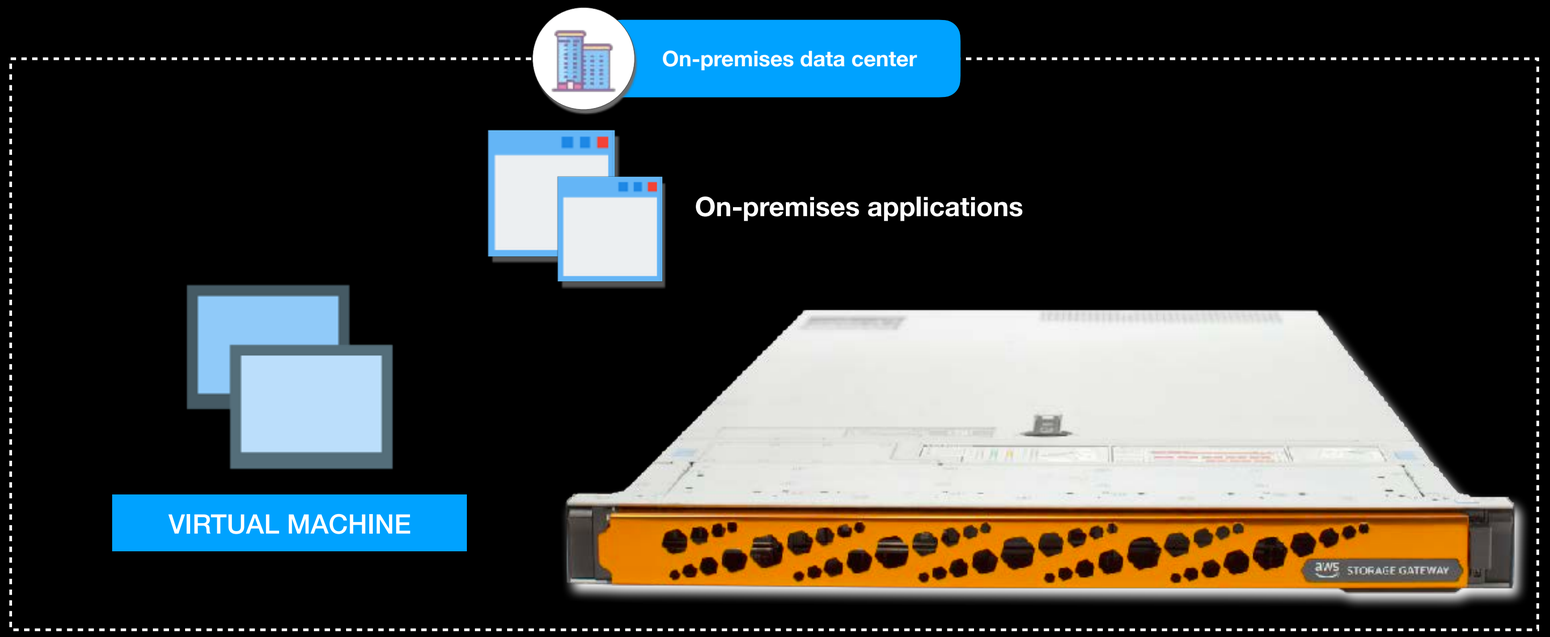
90 Days, One Year or even more!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Storage Gateway

- A hybrid cloud storage service
- Connects your on-premises applications and data storage to the AWS Cloud.
- Integrate your local & cloud storage systems by using a gateway.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

File Gateway

Store and retrieve objects in Amazon S3

using NFS and SMB protocols

Can be integrated with:

AWS Managed Microsoft AD

Microsoft **Active Directory**

Provides a hardware appliance hosted on-premises

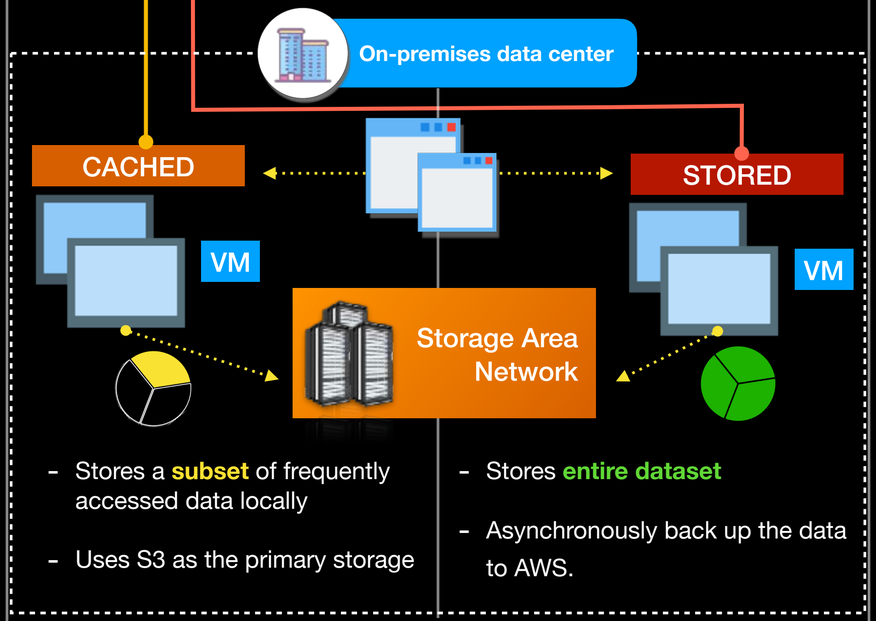


To replicate your local data to Amazon S3

Volume Gateway

Provides block storage to your on-premises apps with low-latency via the Internet Small Computer System Interface (iSCSI)

Uses Amazon S3 for point-in-time snapshots of your EBS Volumes



- Stores a **subset** of frequently accessed data locally
- Uses S3 as the primary storage

- Stores **entire dataset**
- Asynchronously back up the data to AWS.

Tape Gateway

A cloud-based Virtual Tape Library

Uses Amazon S3 to back up the tapes

Can store the archived tapes in:

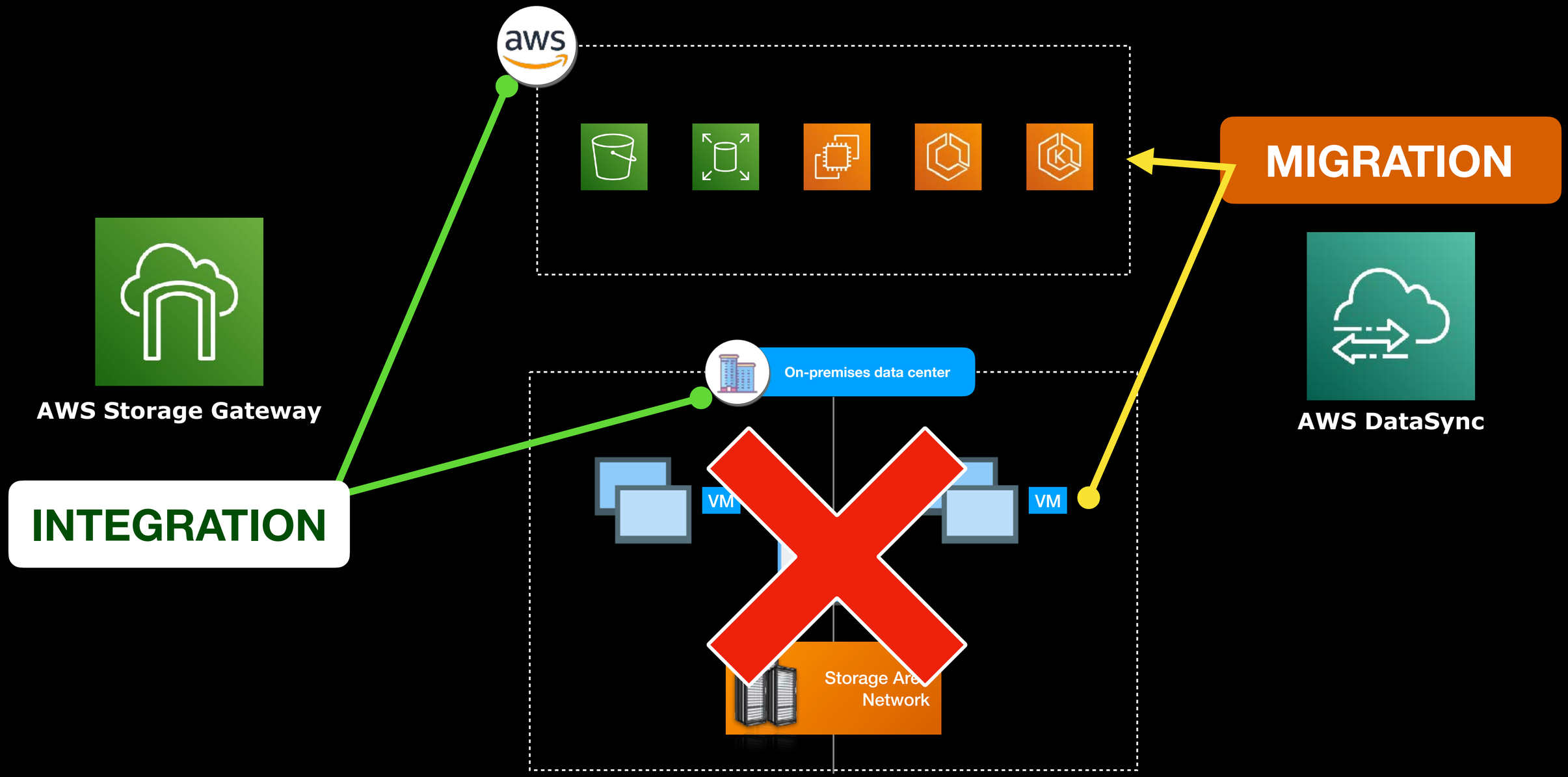
S3 Glacier

S3 Glacier Deep Archive

- On-premises apps can connect to the tape gateway as iSCSI devices

- Reduce costs by eliminating the use of physical backup tapes

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

REPLICATE DATA

INTEGRATION

MOVE DATA

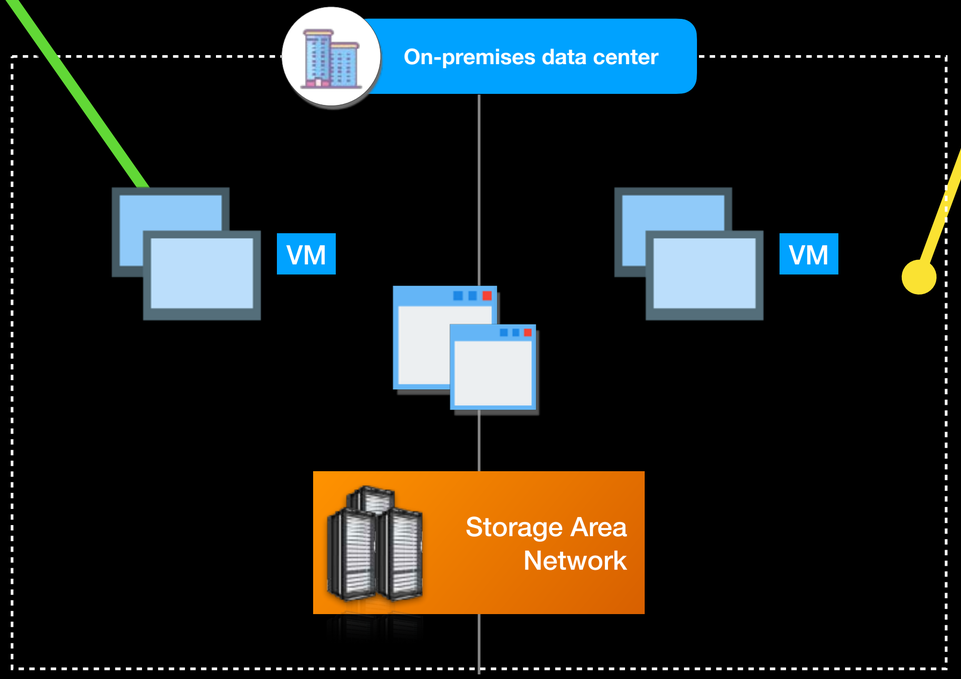
MIGRATION



AWS Storage Gateway



AWS DataSync



On-premises data will **still be actively used**

On-premises data would **not be utilized anymore**/ *will be decommissioned*

Tutorials Dojo

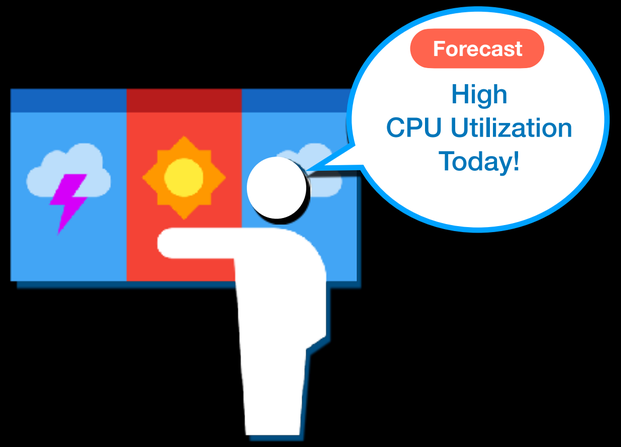
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Monitoring Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

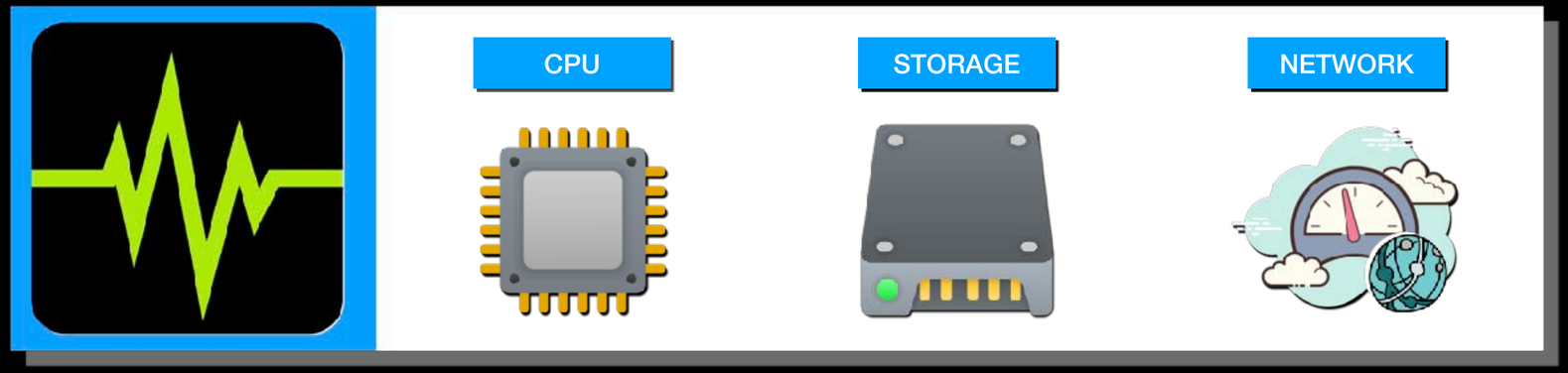
AWS Monitoring Services













NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Monitoring Services



Amazon CloudWatch



AWS Service Health Dashboard



AWS Personal Health Dashboard



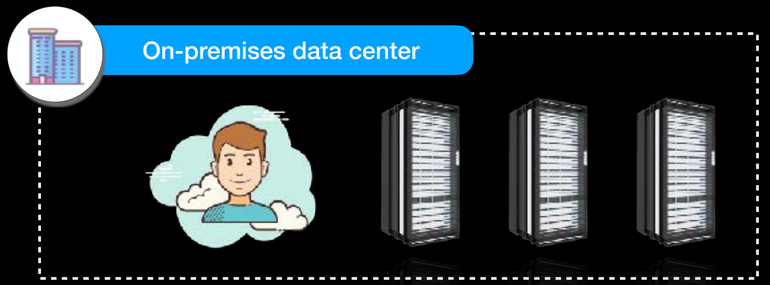
AWS Health API

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

- A **suite of AWS services** used in monitoring your systems on both:



- A **metrics repository** that collects system data from AWS services as well as your custom metrics
- **Monitors** and analyzes system metrics
- **Notifies** you if a certain threshold has been reached
- **Triggers an action** based on a specific threshold or events that you define

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



Metrics



Logs



Alarms



Events



Dashboards

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

METRICS

- **Collect metrics** from various AWS Services and your custom applications
- **Aggregate (combine) metrics** across multiple resources
- Most AWS services send metric data to CloudWatch every 1 minute by default
- For Amazon EC2, the default frequency is every **5 minutes**
- **Detailed Monitoring** sends EC2 metrics data every **1 minute**



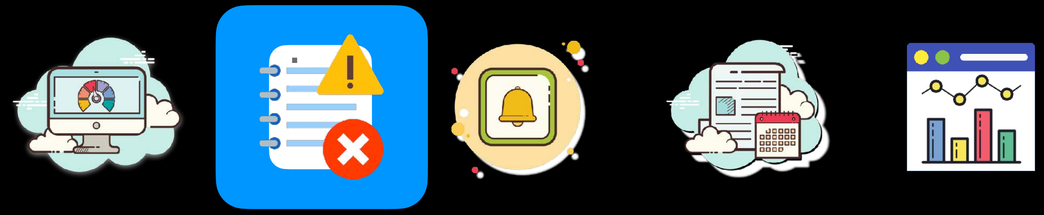
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

LOGS

- Primarily used for **logs** monitoring
- Allows you to **monitor, store, access, analyze or query the logs** from your AWS resources or from your custom applications
- Install **CloudWatch Logs agent** to your EC2 instances to automatically collect and publish your application logs to CloudWatch



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

ALARMS

- Allows you to create **alarms** for your monitoring
- Performs one or more actions based on a system metric and a **specific threshold**
- Can **notify you or other systems/services** using Amazon SNS
- Can **trigger a custom action**, such as:
  - Auto Scaling your EC2 instances
  - Sending a billing alert
  - Invoking a Lambda function
  - … and many more!



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

CloudWatch Events and Amazon EventBridge have the **same underlying service and API**, but the latter provides more features.



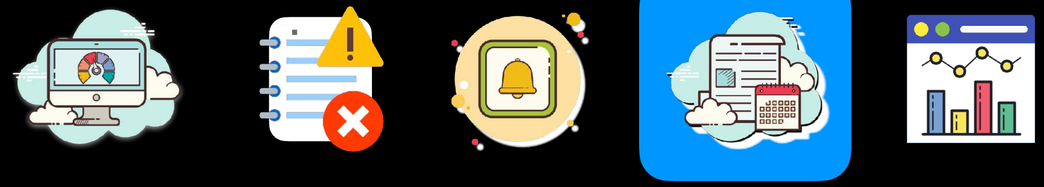
Amazon EventBridge



Amazon CloudWatch

EVENTS

- **Monitors and responds to the system/service events** of your AWS resource in near real-time
- Allows you to **create a CloudWatch Event rule** to track the changes or the state of your services
- **Invokes a certain action** if a specific event matched your Event rule
- Allows you to create a **scheduled job** that invokes a Lambda function on a regular basis, like every hour, every day, every week, or any schedule that you like.



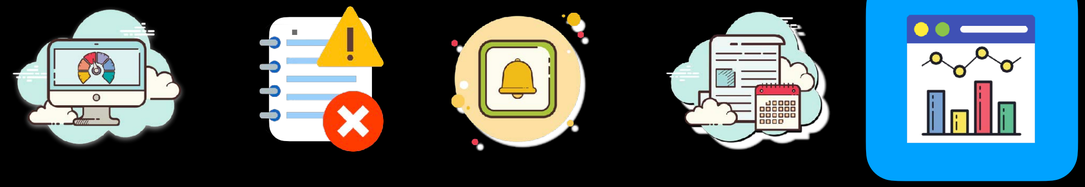
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

DASHBOARDS

- A customizable **dashboard** containing your AWS system metrics
- **Monitor your resources in a single view**, even if those resources are located across different AWS Regions
- Allows you to publish and view your **custom metrics**



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



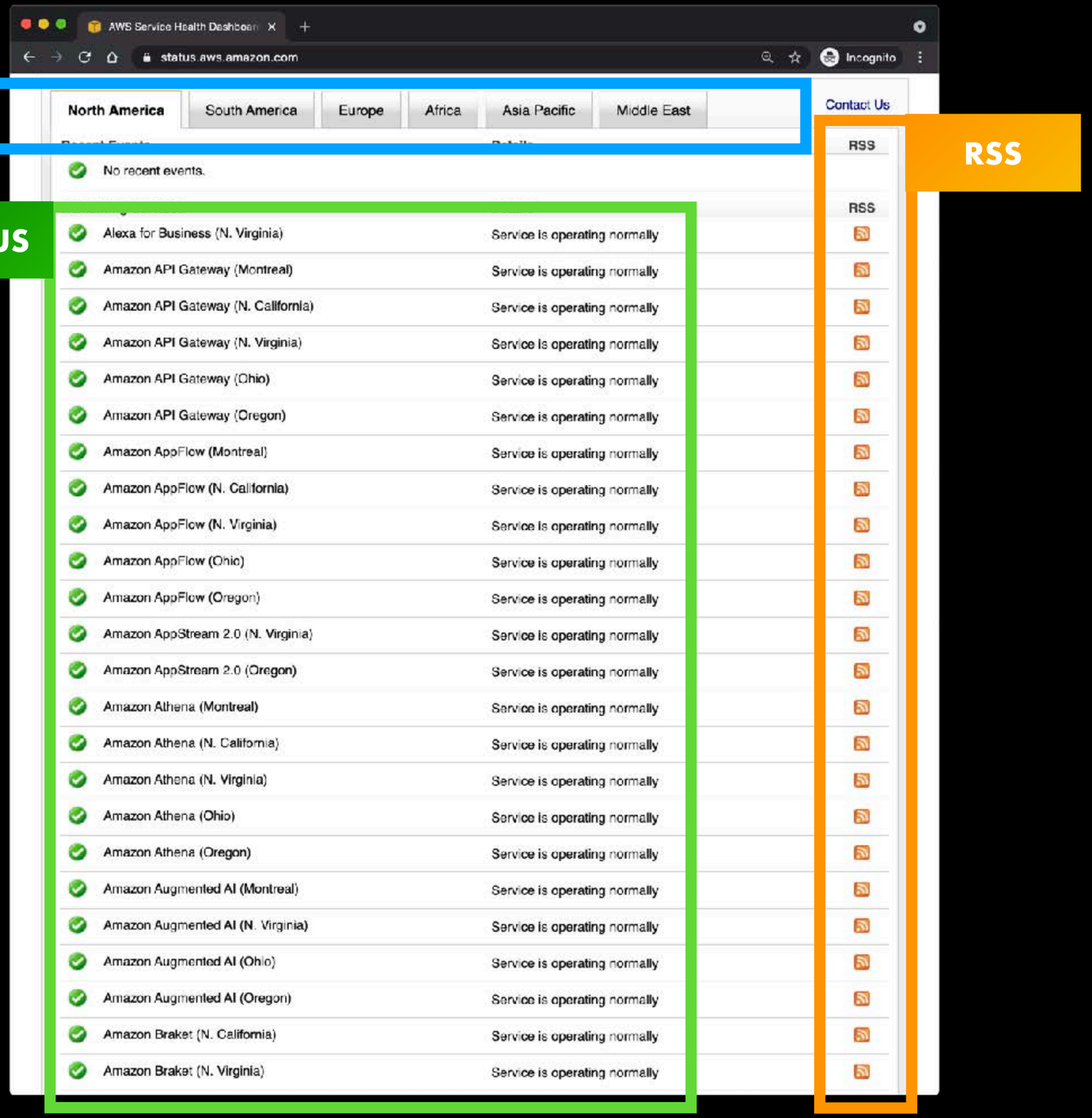




NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Service Health Dashboard



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Personal Health Dashboard

- A **personalized** dashboard that shows the **status of the AWS services that you are using**
- Does **NOT** show you the status of all the AWS services globally but only the status of the AWS services that you have in your account.
- **Shows the AWS Health events** that might affect your applications running on AWS such as scheduled maintenance or system outages
- **Allows you to create alerts and notifications** based on the health of your AWS resources

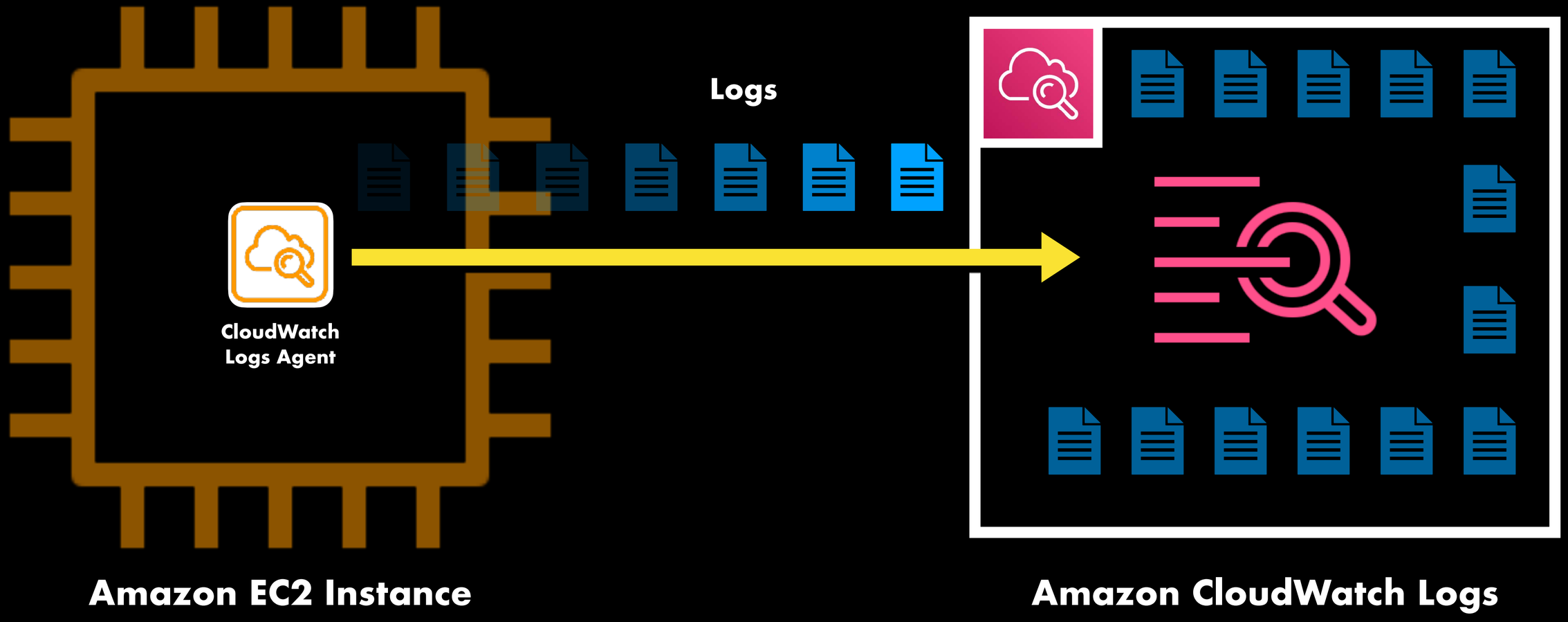
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Health API

- Provides **programmatic access to the AWS Health** information that appears in your AWS Personal Health Dashboard
- A **RESTful web service** that you can access via HTTPS
- **NOT** available by default
- Only available in **Business or Enterprise support plans**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Tutorials Dojo
www.tutorialsdojo.com
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Audit & Compliance Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Audit & Compliance Services



aws API

RESOURCE CHANGES

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Audit & Compliance Services



AWS CloudTrail



AWS Artifact



AWS Security Hub

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



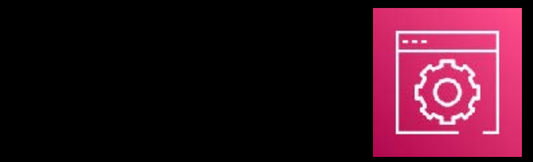
AWS CloudTrail

- **Tracks user activity and API usage** in your AWS account
- **Stores the audit log data** in:



Amazon S3 Bucket

- **Enables risk auditing** by continuously monitoring and logging account activities, such as user actions:



AWS Management Console



AWS SDK



AWS API



AWS Command Line Interface (CLI)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudTrail

MANAGEMENT EVENTS

Control Plane

Provide information about the management operations performed on your AWS resources

- **Attaching an IAM Role**
- **Creating a new VPC**
- **Creating a subnet**

DATA EVENTS

Data Plane

Provide information about the resource operations performed ON (e.g. S3 bucket) your resources or performed IN (e.g. S3 objects) your resources

- **Amazon S3 object-level API activities**
- **Invoking an AWS Lambda function**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Artifact

- Provides on-demand **AWS security and compliance reports**
- Acts as a self-service portal to find compliance-related information and reports for:
    - ISO Reports
    - Payment Card Industry (PCI) reports
    - Service Organization Control (SOC) reports
    - . . . and many more!
- Allows you to download AWS security and compliance documents such as **SOC 1 report, ISO certifications, and other reports**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Security Hub

- Provides a **centralized & comprehensive view of the security posture** of your cloud infrastructure across multiple AWS accounts
- Helps you to comply with your company's specific security standards and best practices
- **Collects security alerts and findings** from:



Amazon GuardDuty



Amazon Inspector



Amazon Macie



AWS IAM Access Analyzer



AWS Firewall Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Networking & Content Delivery Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Networking & Content Delivery Services



Amazon VPC



Elastic Load Balancing



Amazon Route 53



AWS Global Accelerator



Amazon CloudFront



AWS PrivateLink



AWS VPN



AWS Direct Connect



AWS Transit Gateway



Amazon API Gateway



AWS App Mesh

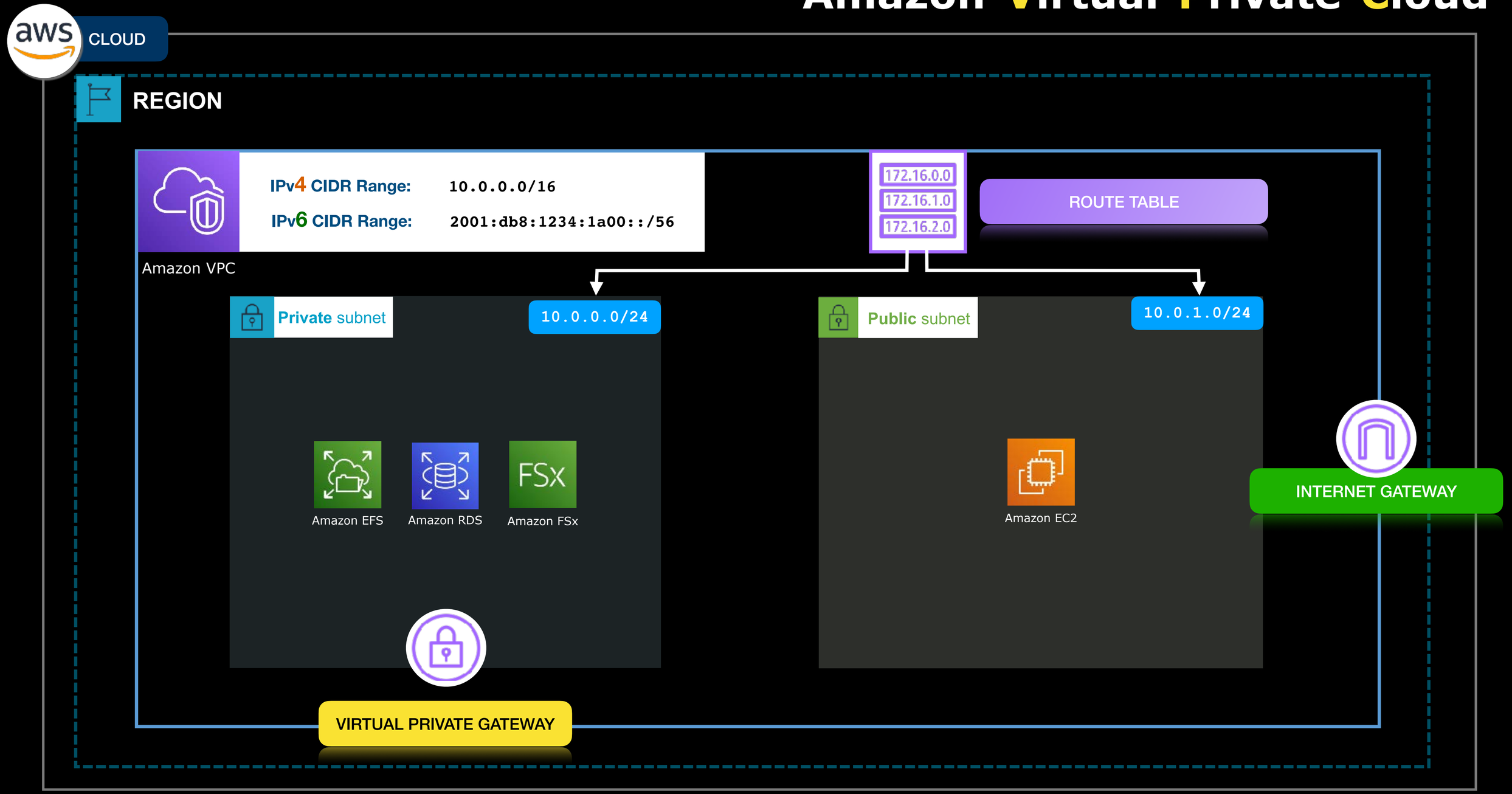


AWS Cloud Map

Also categorized as an Application Integration Service

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon Virtual Private Cloud



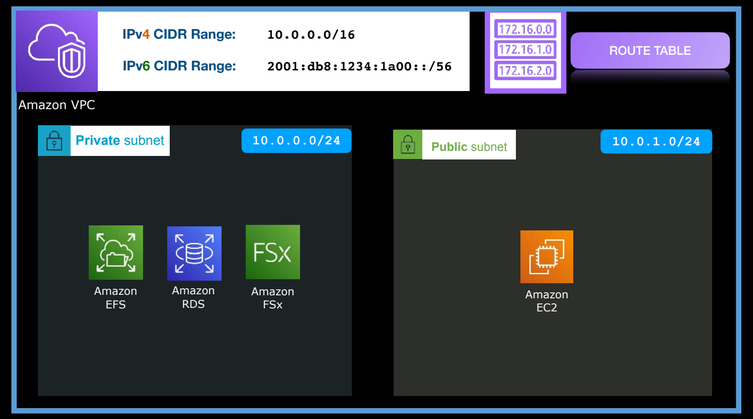
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon Virtual Private Cloud

aws CLOUD

ASIA PACIFIC (Singapore)

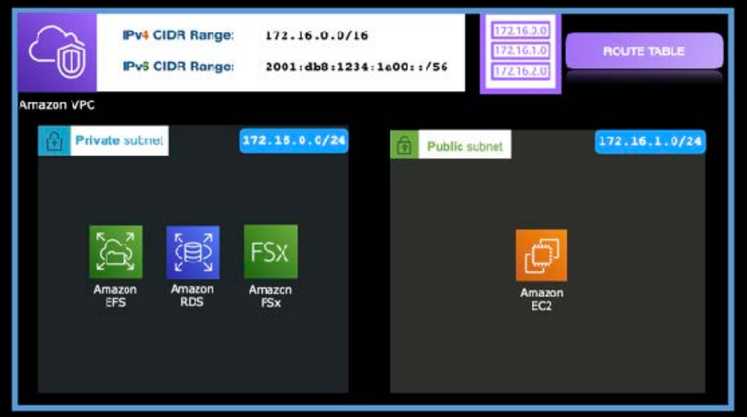
VPC A - Manila Branch



VPC Peering

US EAST (Northern Virginia)

VPC B - New York Branch



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Virtual Private Cloud

Amazon VPC

Virtual Devices

VIRTUAL IP address MAC address Firewall

VIRTUAL IP address MAC address Firewall

VIRTUAL IP address MAC address Firewall

NETWORK VIRTUALIZATION

Physical Devices

PCIe Network Interface Card

Nitro Card for VPC





aws Data Center

aws Data Center

aws Data Center

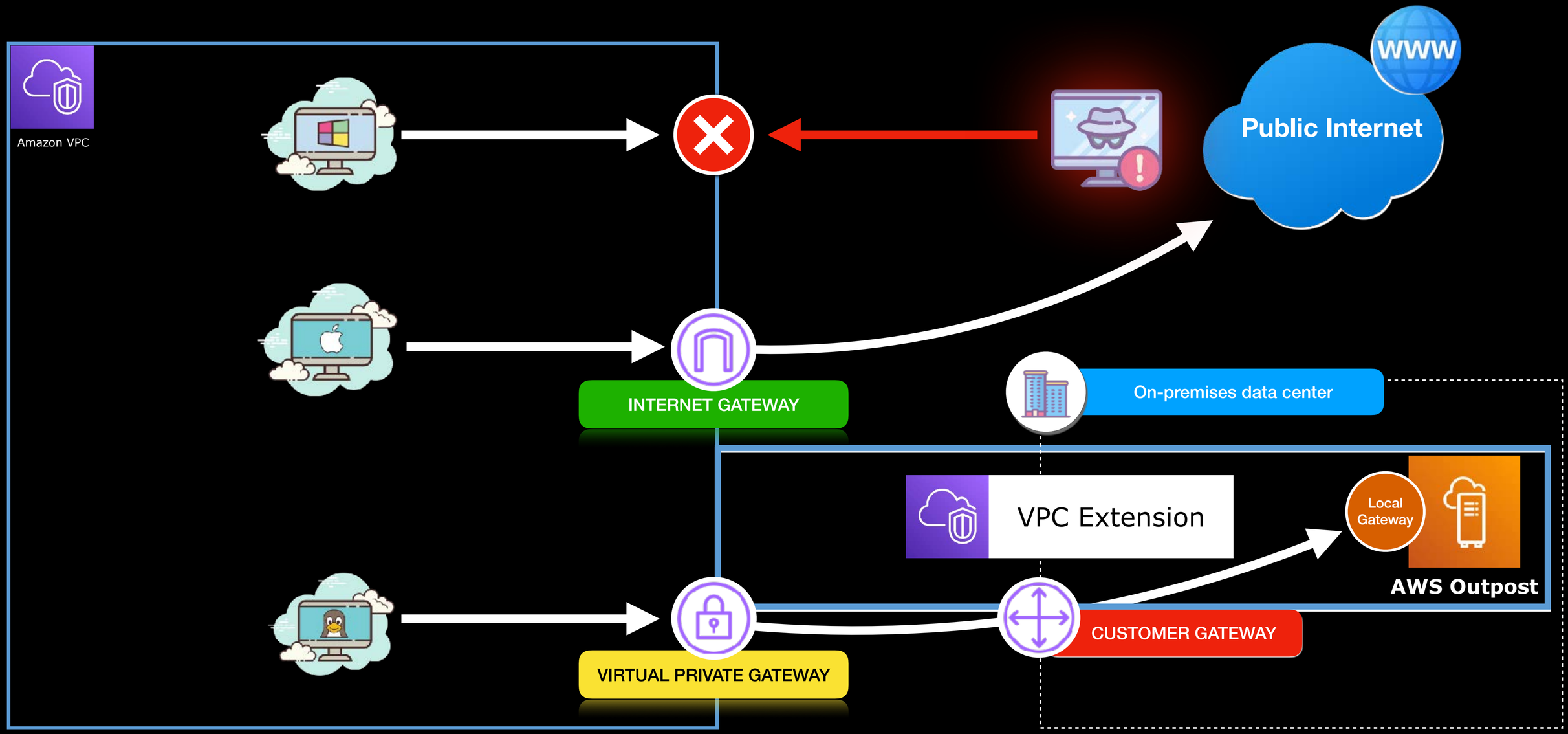
aws Data Center

aws Data Center

aws Data Center

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Virtual Private Cloud

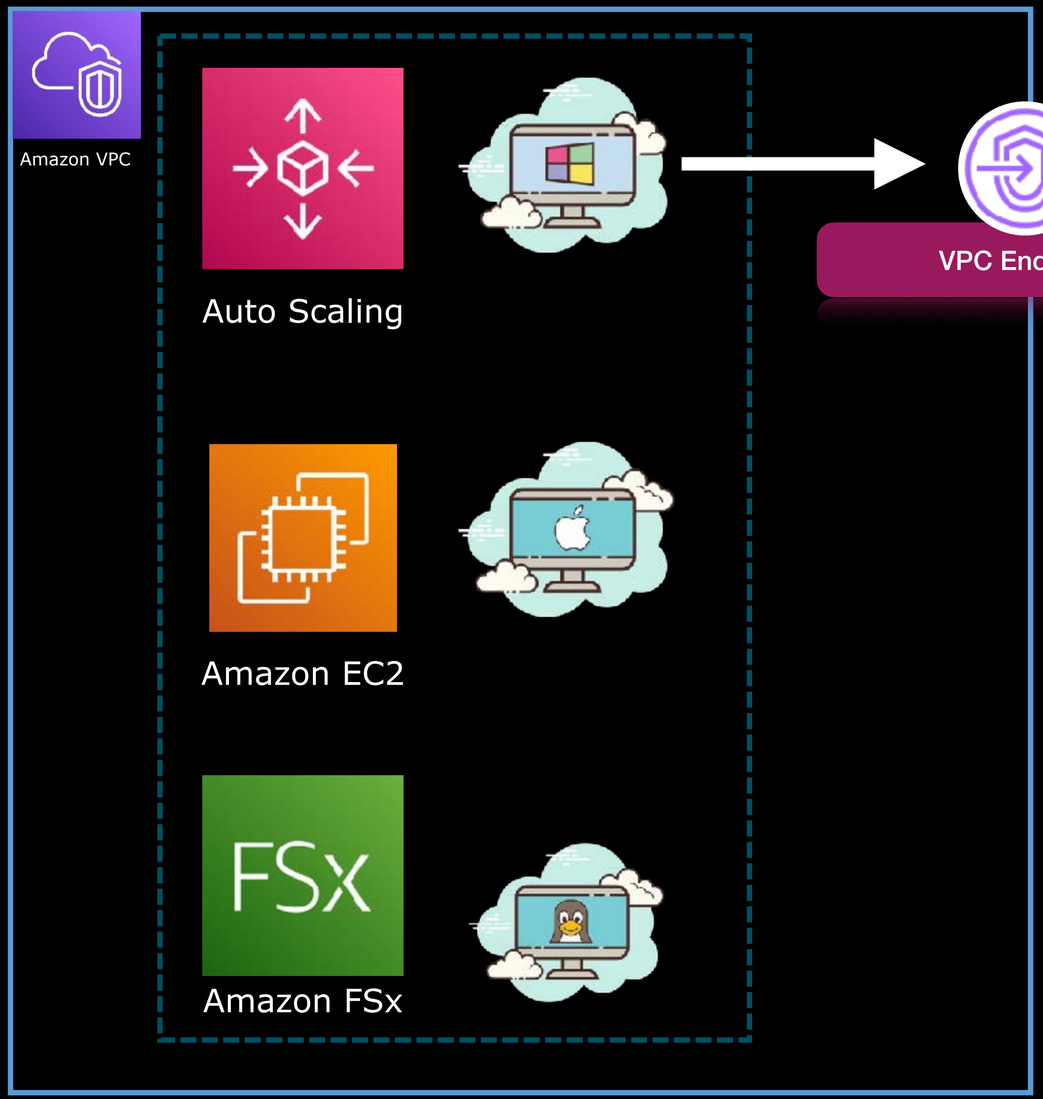


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Virtual Private Cloud







Auto Scaling

Amazon EC2

Amazon FSx



VPC Endpoint





Amazon S3



Amazon DynamoDB

Other aws Services

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Elastic Load Balancing

- Automatically distributes incoming traffic across **multiple targets** such as:


Amazon EC2 Instance


Amazon ECS Task


AWS Fargate Task


AWS Lambda Function


IP Address

- It **distributes** (*load balances*) the incoming traffic to your underlying resources
- Provides **high-availability** to your web applications
- if one of your servers or EC2 instances fails (*unhealthy resource*), the request will be routed to another server (*healthy resource*)
- Routes incoming traffic across multiple Availability Zones, within a **single** AWS Region only.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Elastic Load Balancing TYPES

	Application Load Balancer (ALB)	Network Load Balancer (NLB)	Gateway Load Balancer (GWLB)	Classic Load Balancer (CLB)
PROTOCOL LISTENERS	HTTP / HTTPS gRPC	TCP / UDP TLS	IP	HTTP / HTTPS TCP SSL/TLS
USE CASES	For **web apps**, microservices & containers	Handling **millions of requests per second** while maintaining **ultra-low latencies**	Running third-party **virtual appliances** in AWS	For **legacy** applications in AWS For implementing **Custom Security Policies** and **TCP passthrough configuration**

Tutorials Dojo
www.tutorialsdojo.com

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Route 53

- A **Domain Name System** (DNS) web service
- DNS is a system that routes a **domain name** to a particular **IP address**
- **Map** domain names to:



Elastic IP address



Amazon EC2 Instance



Amazon S3 Static Website



Elastic Load Balancers



Amazon CloudFront Web Distributions

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Route 53

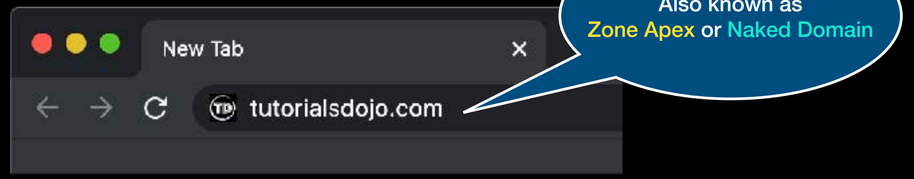


Buy Domains



Manage Domains

Root Domain



Subdomains

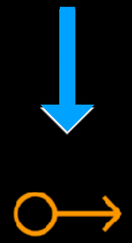
philippines.tutorialsdojo.com

blog.tutorialsdojo.com

portal.tutorialsdojo.com

cdn.tutorialsdojo.com

manila-datacenter.tutorialsdojo.com



Elastic IP address



Amazon EC2 Instance



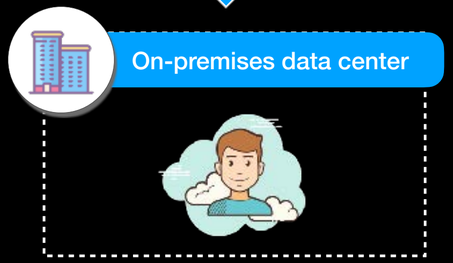
Amazon S3 Static Website



Elastic Load Balancers



Amazon CloudFront Web Distributions



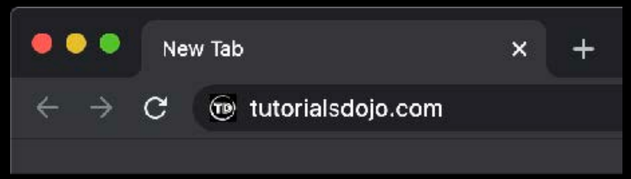
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ROUTING POLICIES

Amazon Route 53

Simple | Failover | Geolocation | Geoproximity | Latency-Based | Multivalue Answer | Weighted

Root Domain



Subdomains

philippines.tutorialsdojo.com

blog.tutorialsdojo.com

portal.tutorialsdojo.com

cdn.tutorialsdojo.com

manila-datacenter.tutorialsdojo.com

Elastic IP address

Amazon EC2 Instance

Amazon S3 Static Website

Elastic Load Balancers

Amazon CloudFront Web Distributions

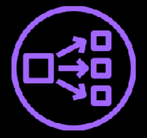
On-premises data center

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Global Accelerator

- Provides a set of **static anycast IP** addresses
- The static IP address serves as a **single fixed entry point** to:



Network
Load Balancer



Application
Load Balancer

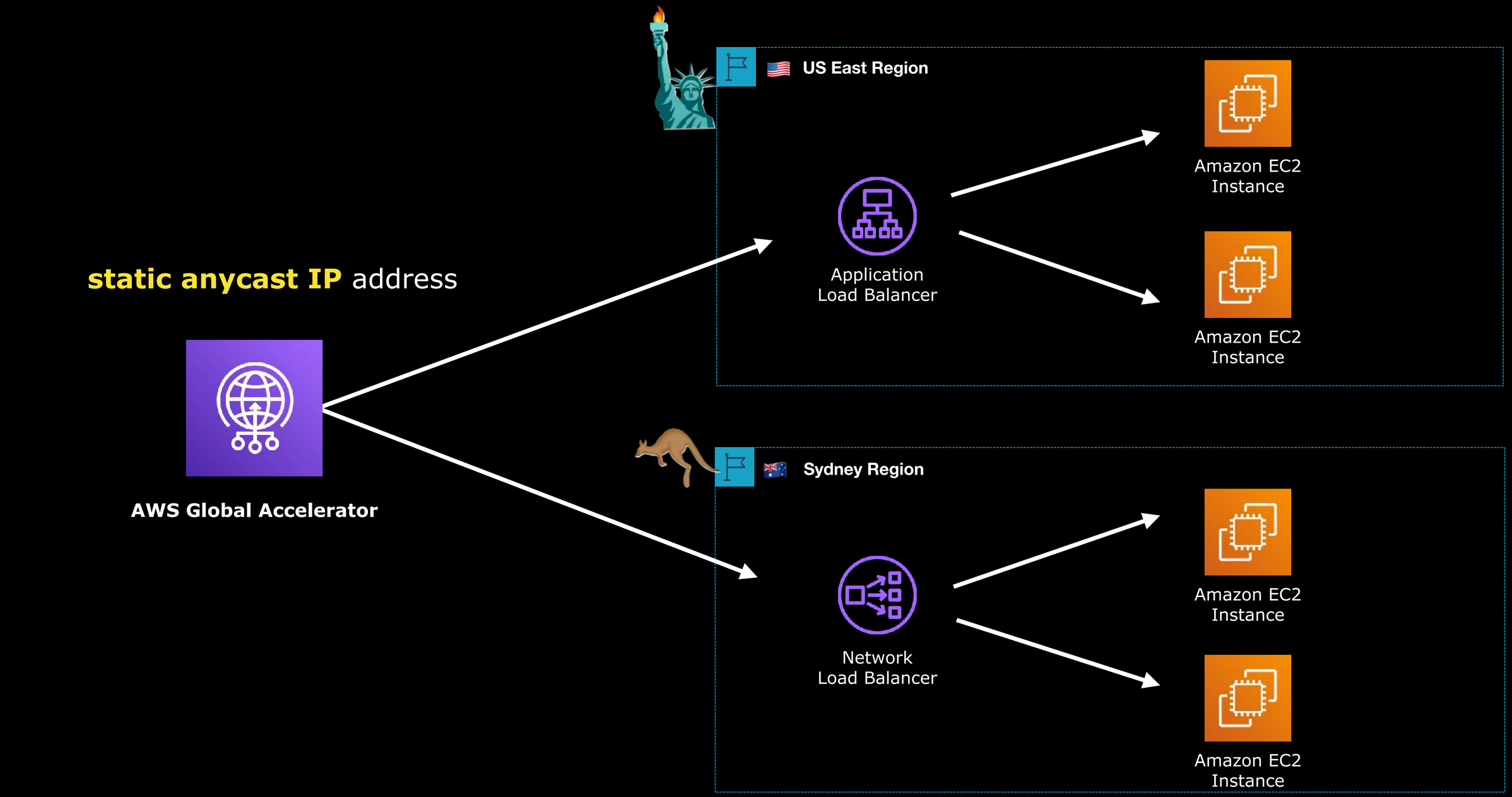


Amazon EC2
Instance



Elastic IP
address

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudFront

- A **content delivery network** (CDN) service
- Quickly delivers static content and video stream to your clients.
- A CDN is a **globally-distributed network** of services/servers spread around the globe that stores or **caches** your files.
- **Reduces latency** by shortening the time it takes to deliver your data to your users
- **Improves the response time** of your application.
- **Caches** your images, videos, media files, or software packages

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS PrivateLink

- Allows **private connectivity** to various AWS services
- **Does not pass through the public Internet.**
- Provides a **private endpoint** that you can use for your:



Amazon VPC



Amazon EC2



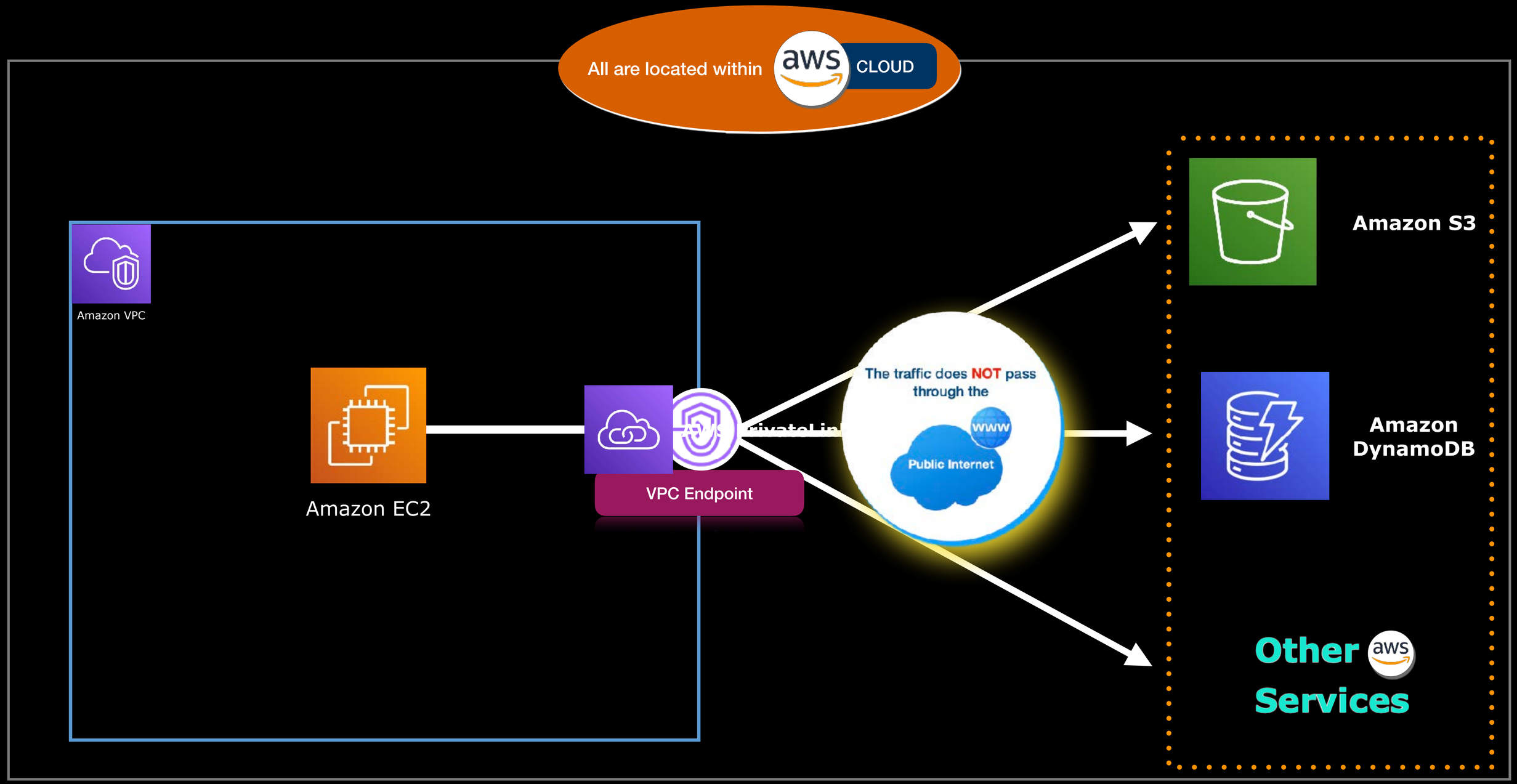
Amazon S3



Amazon DynamoDB

Other Services

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



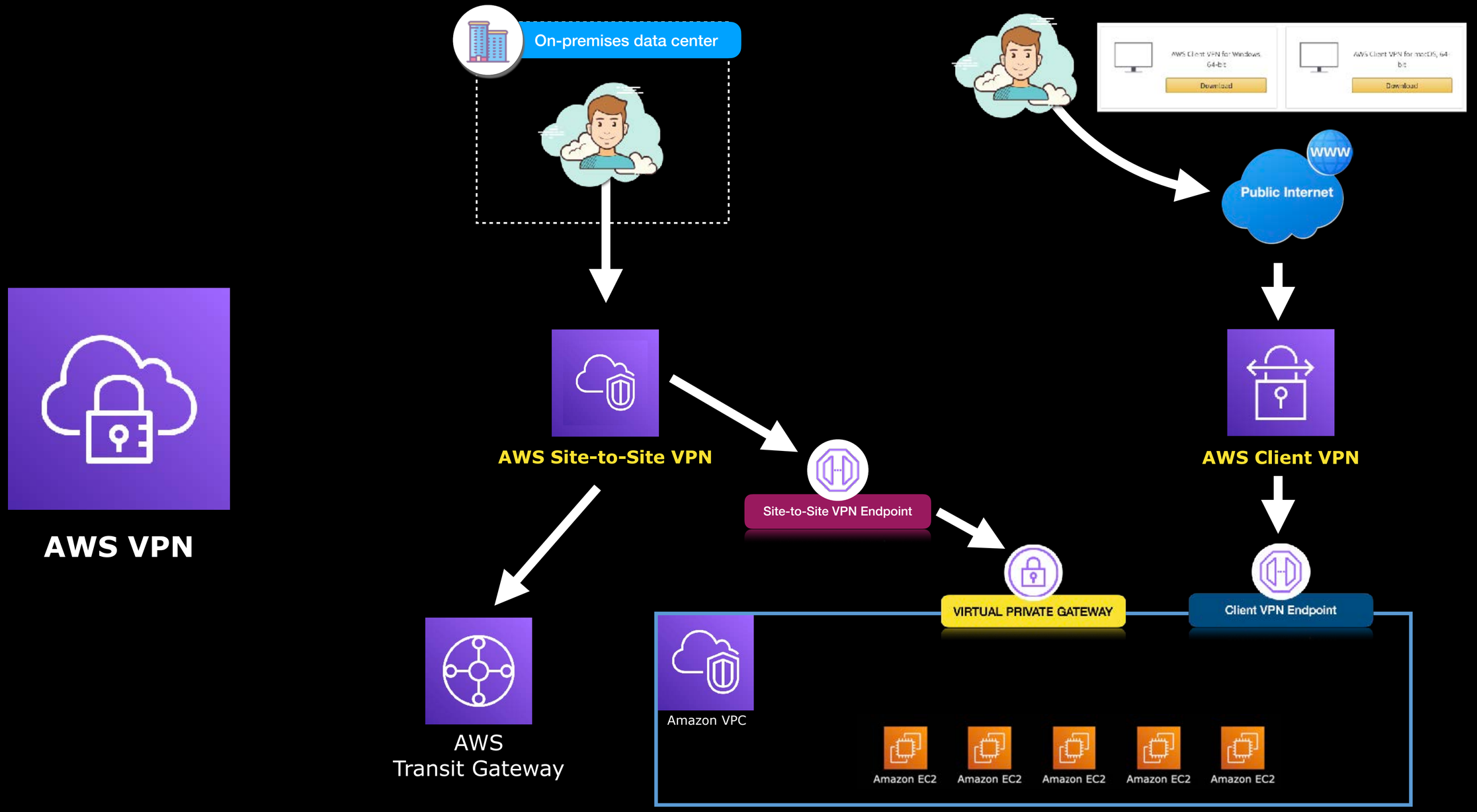
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



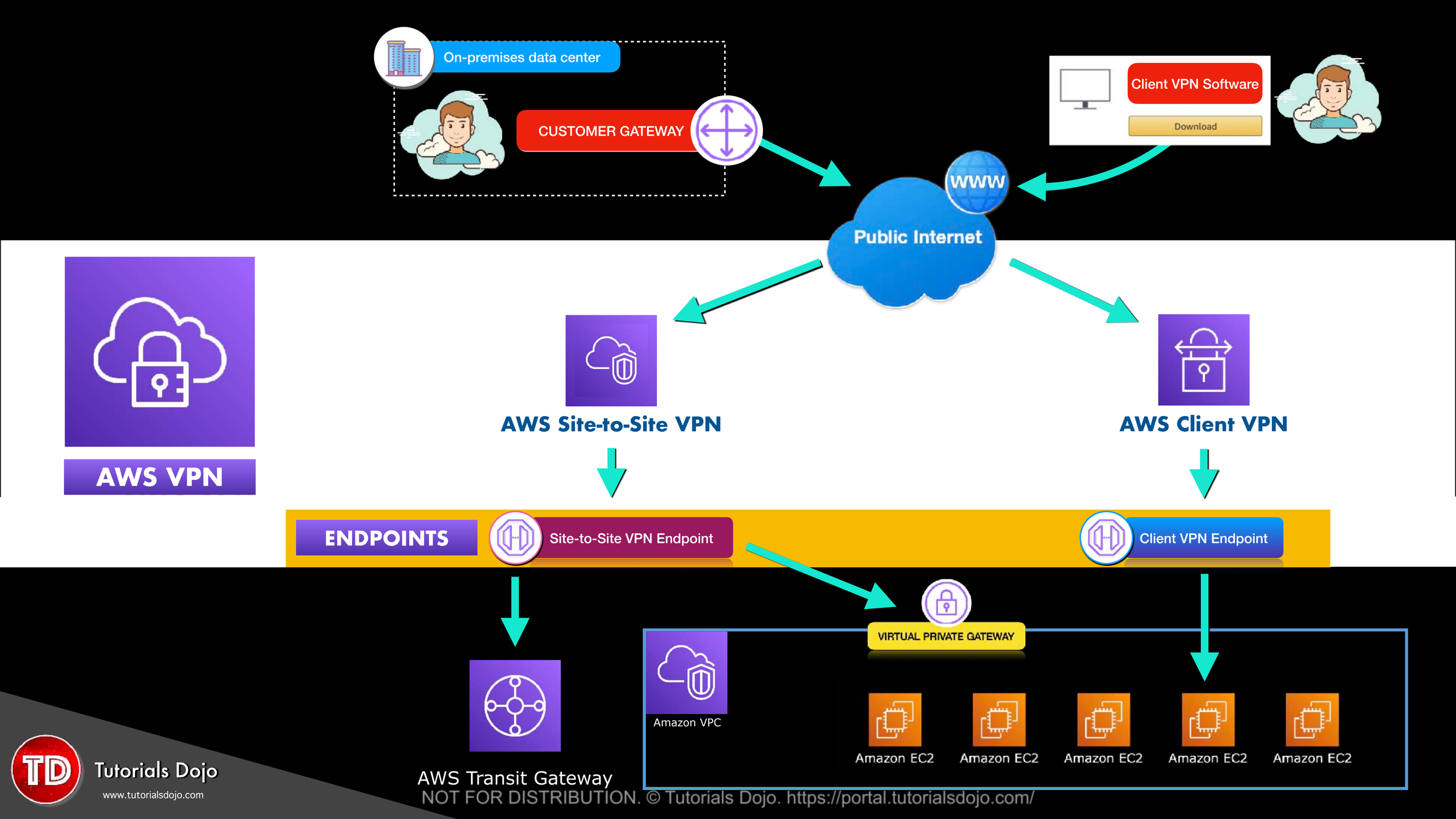
AWS VPN

- AWS **V**irtual **P**rivate **N**etwork, or AWS VPN
- Enables you to **connect your on-premises network to AWS.**
- An encrypted connection that **passes through the public Internet.**
- Uses the **IPsec protocol** to authenticate and encrypt your data in transit.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

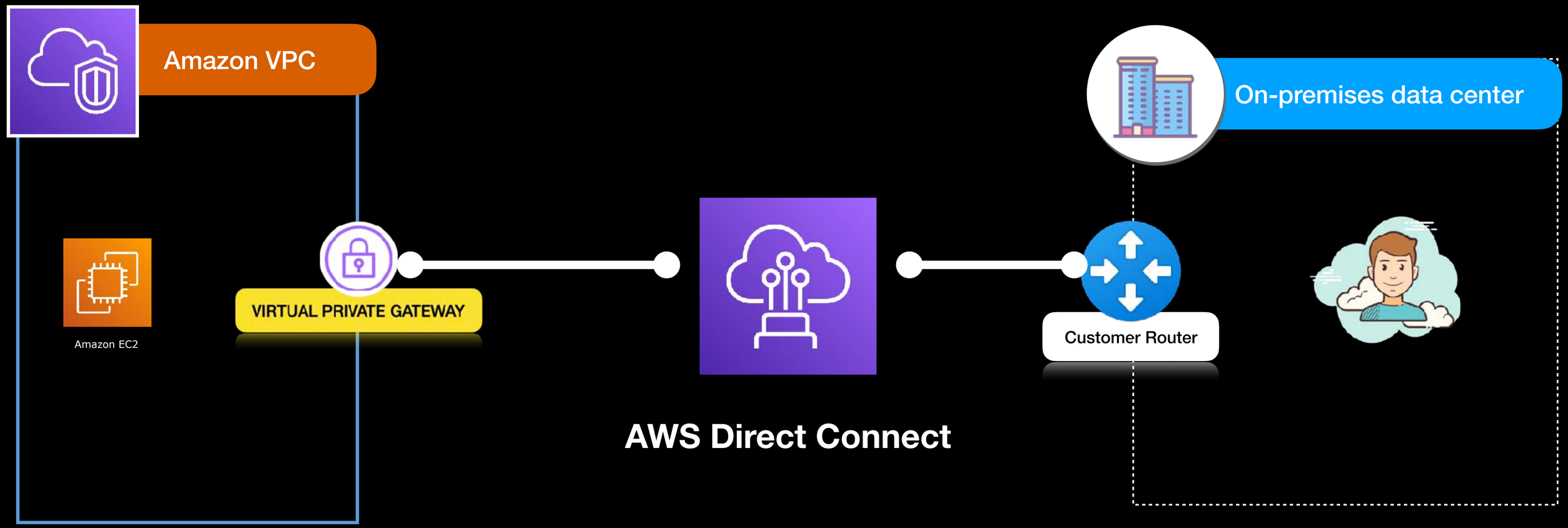


Tutorials Dojo
www.tutorialsdojo.com
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

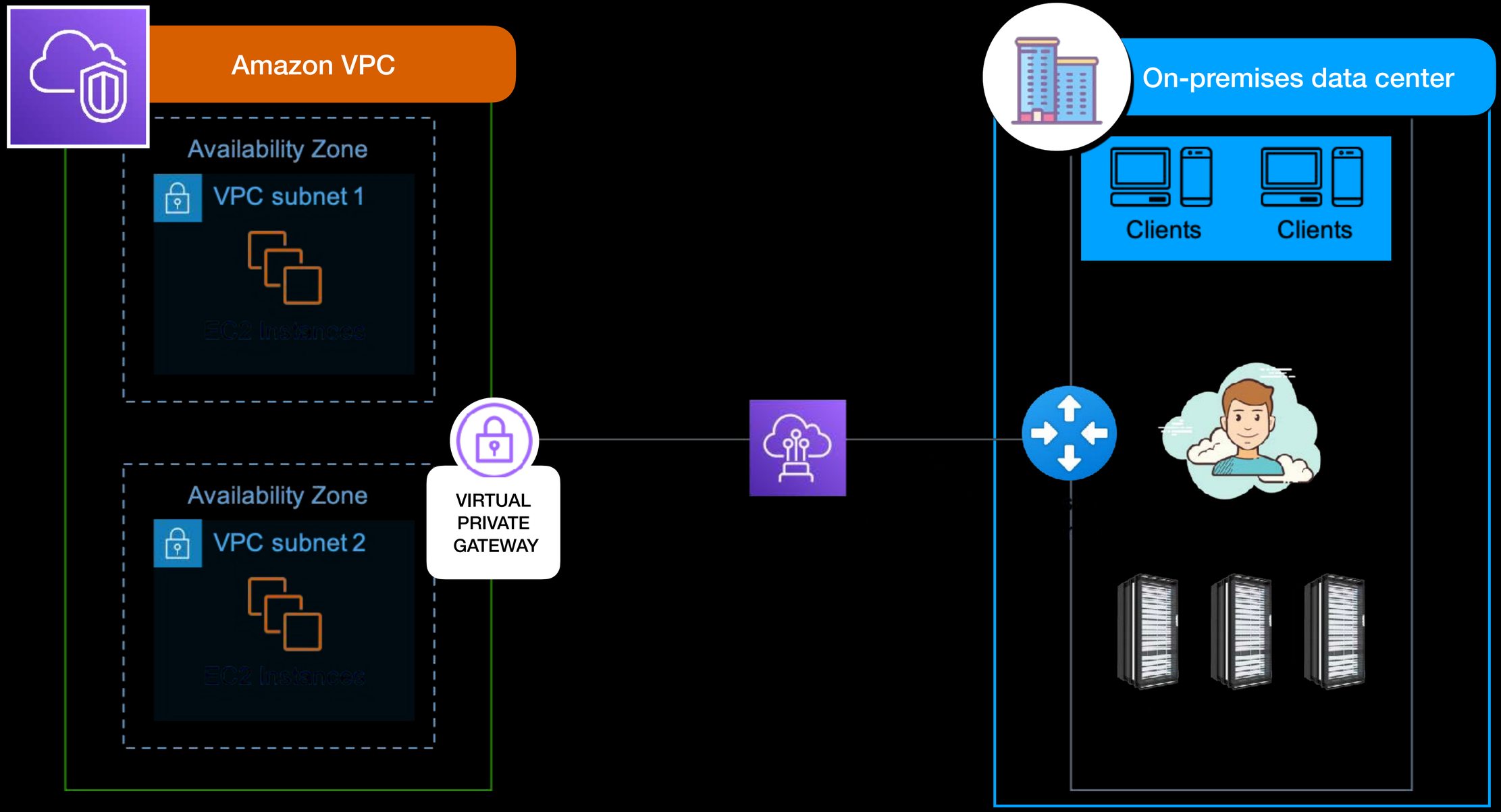


- Allows you to establish a **dedicated network connection** from your on-premises network to AWS
- Provides a **more consistent network experience** over Internet-based connections such as a VPN, and a **higher bandwidth**.
- You can create a **private virtual interface** to enable your on-premises servers to connect to the virtual private gateway of your Amazon VPC.
- You can group your virtual private gateways and private virtual interfaces using a **Direct Connect Gateway**.
- You can also use a **public virtual interface** to connect to your Amazon S3 buckets and other public resources in AWS.
- **The traffic does NOT pass through the public Internet.**

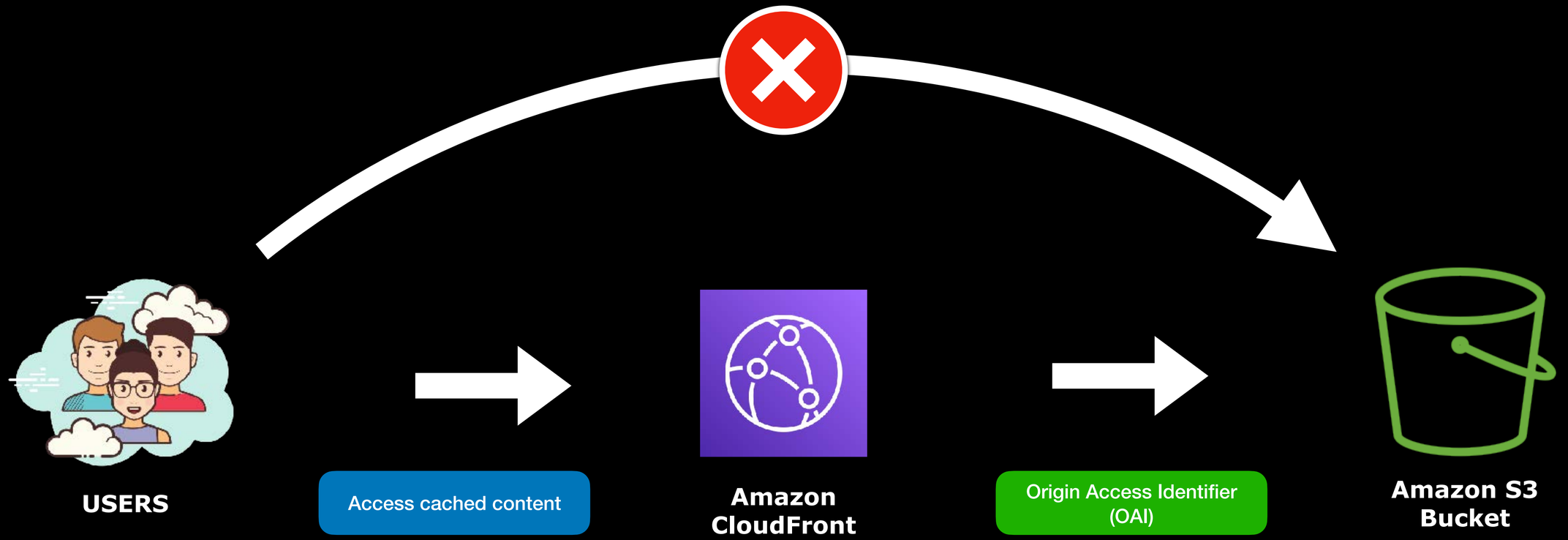
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



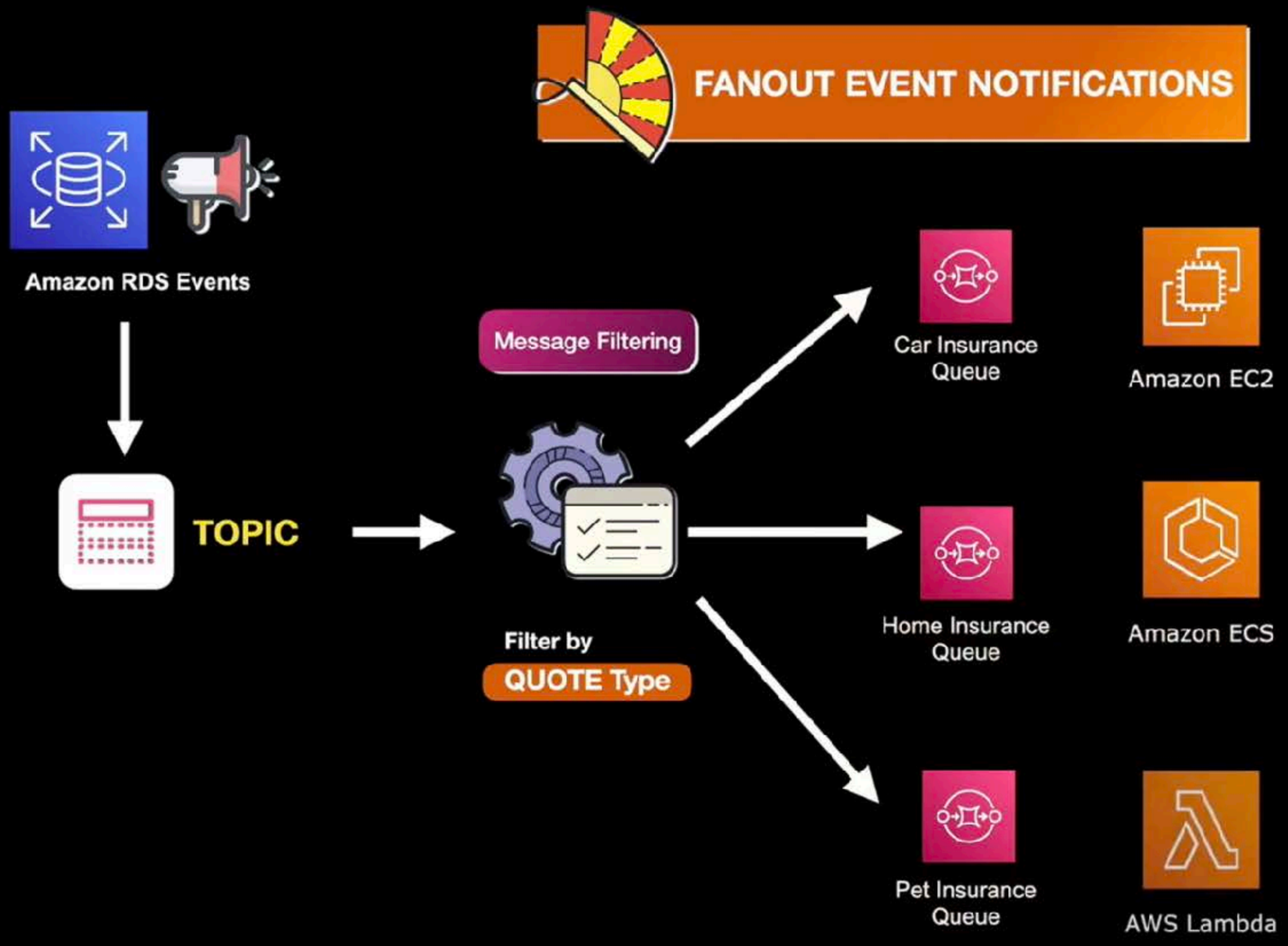
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



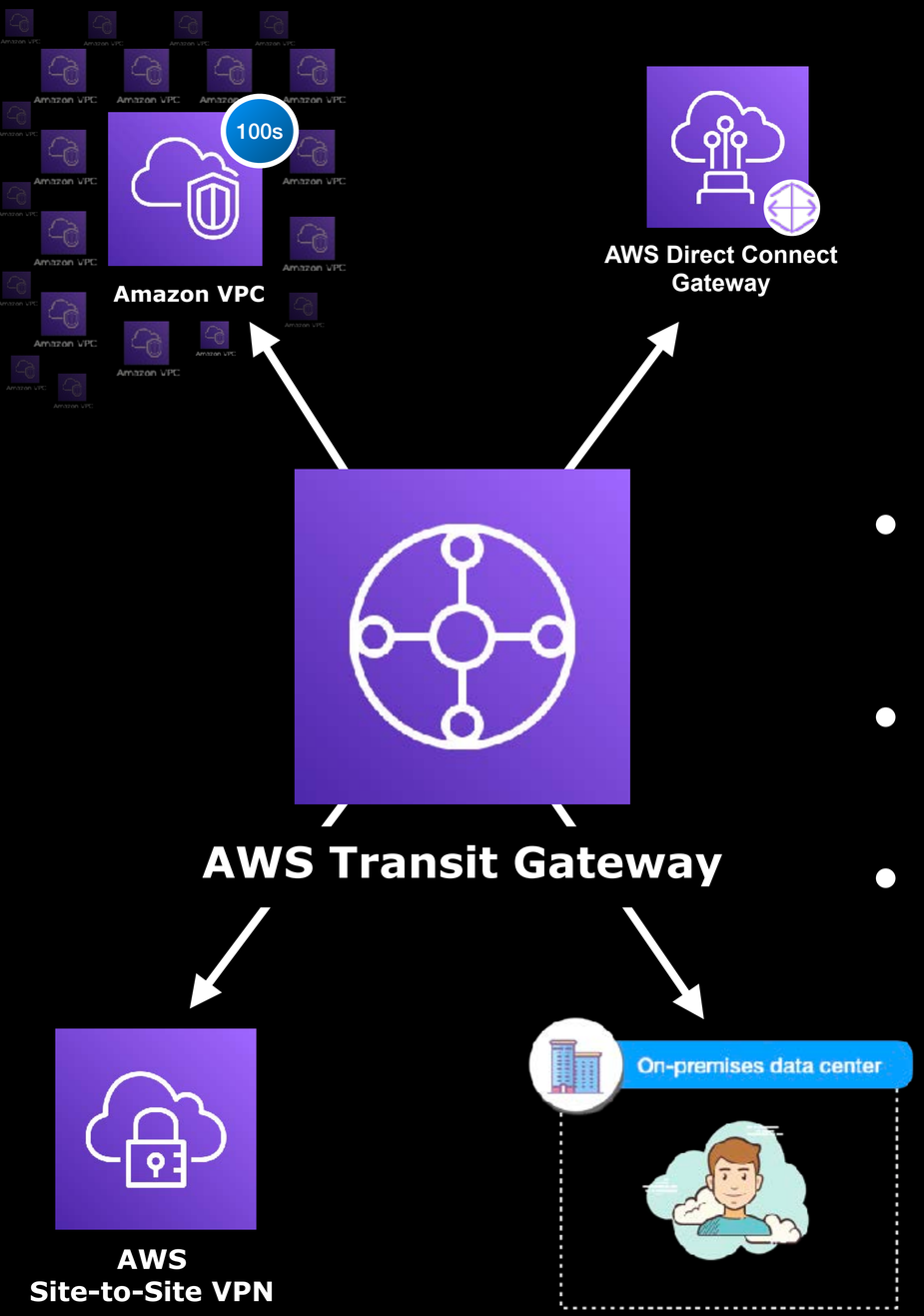
Tutorials Dojo
www.tutorialsdojo.com
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Tutorials Dojo
www.tutorialsdojo.com
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

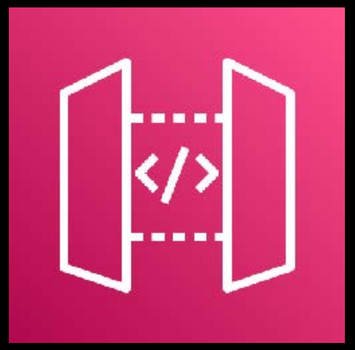


Tutorials Dojo
www.tutorialsdojo.com
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- **Connects your cloud networks** (e.g. Amazon VPCs, VPNs, Direct Connect Gateways, and on-premises networks) **to a single gateway.**
- Recommended for large organizations with 100s **hundreds of Amazon VPCs, site-to-site VPNs, and external networks.**
- Reduces the complexity of your infrastructure and makes scaling easier

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon API Gateway

- Allows you to publish, maintain, monitor, and secure your **RESTful APIs.**
- Also supports **WebSockets** for real-time message communication
- **Acts as a front door for your back-end services** that are running on:


Amazon EC2


Amazon ECS


AWS Fargate


AWS Lambda


AWS Elastic Beanstalk

- Works as a **Proxy** — similar to APIGEE, Mulesoft and other proxies/integration platforms

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS App Mesh

- A **service mesh** *(an infrastructure layer that handles communication between microservices)*
- Provides application-level networking for the different types of **containerized applications** in AWS**.**
- **Allows your services to communicate with each other** across multiple types of computing infrastructure.
- Uses envoy *(an open-source service mesh proxy)*
- Can be used with microservice containers managed by:



Amazon ECS



Amazon EKS



AWS Fargate



Amazon EC2

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Cloud Map

- A **cloud resource discovery** service.
- Commonly used in microservices and containerized applications that have **dynamically changing resources.**
- You can **name your containerized application resources** with **custom names.**
- Improves your containerized applications in AWS by always discovering the **most up-to-date locations of your resources**
- **Improves the availability** of your system.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Security Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Security Services

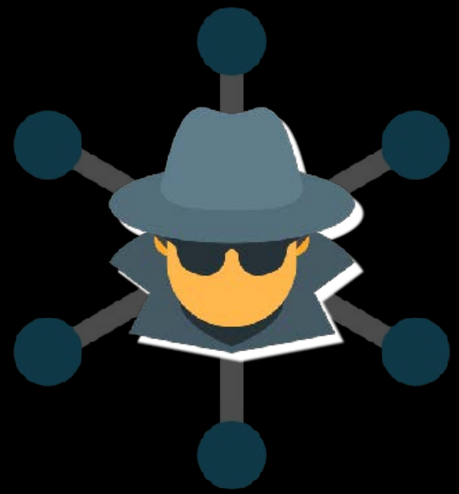












NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

7 Open Systems Interconnection (OSI) Model Layers





DDOS

Distributed **D**enial-**O**f-**S**ervice Attack

UDP TCP

IP

SYN SYN SYN SYN SYN SYN SYN SYN SYN



SYN ACK



ACK ACK ACK

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Security Services



AWS Web Application Firewall (AWS WAF)



AWS Firewall Manager



AWS Shield



Amazon GuardDuty



AWS CloudHSM



AWS Key Management Service (AWS KMS)



AWS Secrets Manager



AWS Certificate Manager (AWS ACM)



Amazon Macie



Amazon Inspector



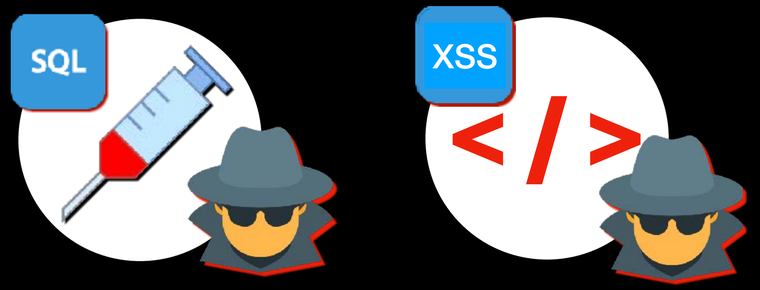
Amazon Detective

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Web Application Firewall (AWS WAF)

- A **web application firewall** service
- Protects your web applications from **common web exploits**
- Allows you to create **custom rules** that block common attack patterns such as:



- **Can be integrated with**:



Amazon CloudFront



Application Load Balancer



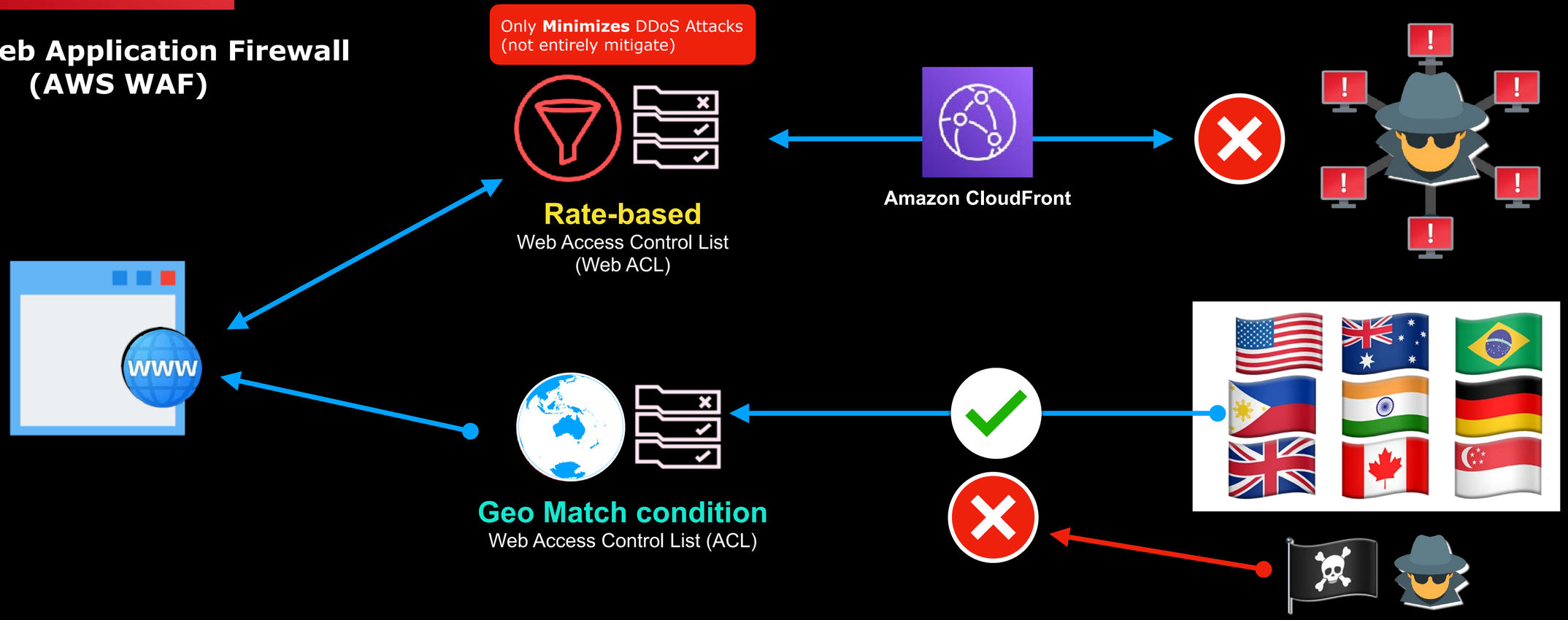
Amazon API Gateway

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Web Application Firewall (AWS WAF)

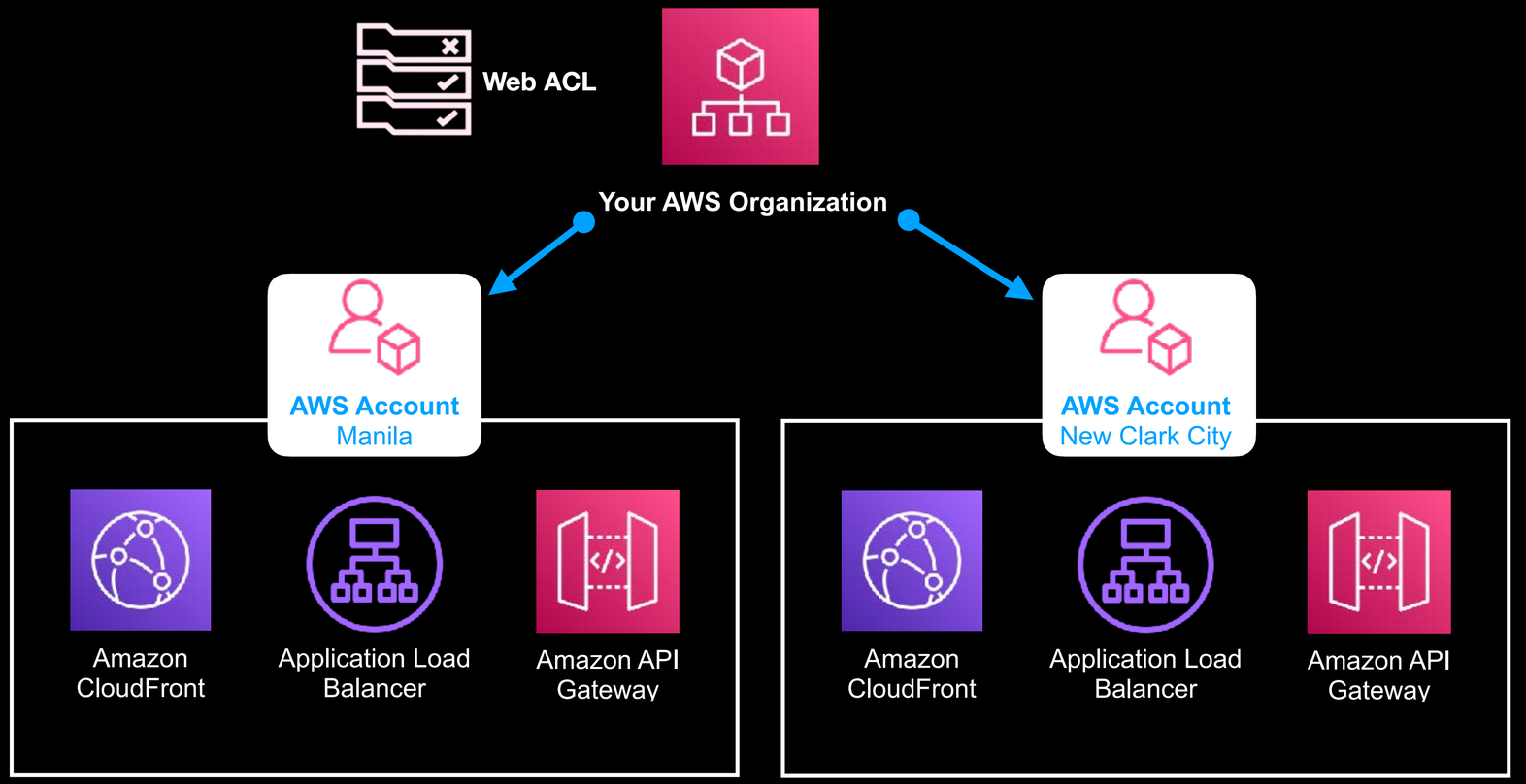
- Has an **IP Match condition** feature, you can block malicious requests from a recurring set of IP addresses.
- Can protect your application from **illegitimate requests** sent by illegitimate external systems, through its **rate-limiting rule.**



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

- A **security management service** designed for: AWS WAF Rules
- Allows you to **centrally configure and manage WAF rules across multiple AWS accounts** and applications.
- Enables you to roll out your custom rules to your **AWS Organization**

AWS Firewall Manager



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Shield

- A **managed DDoS protection** service
- Provides **detection and automatic mitigations** that minimize application downtime and latency.
- **Mitigate different types of flood attacks** such as UDP reflection, SYN flood, DNS Query flood, and HTTP flood attacks.
- Protects your applications that use:


Amazon EC2


Elastic Load Balancer


Amazon CloudFront


AWS Global Accelerator



Amazon Route 53

- Two Tiers:
  - **Standard**
    - Built-in by default
    - No extra charge
  - **Advanced**
    - Has an additional charge
    - Provides access to real-time DDoS attack notification
    - DDoS Response Team (DRT) supports you during DDoS Attack

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon GuardDuty

- A **managed threat detection** service
- **Identifies malicious or unauthorized activities** in your AWS accounts and workloads.
- **Monitors activities** such as unusual API calls, cryptocurrency mining, or potentially unauthorized deployments that indicate a possible account compromise.
- Also detects potentially compromised:



Amazon EC2 Instances

- Produces security reports called:



Findings

- Able to **send notifications using CloudWatch Events** when a change was detected
- **NOT capable of doing any resource changes** by itself, like rate-limiting protection or DDoS attack mitigation.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudHSM



AWS Key Management Service (AWS KMS)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

- A fully managed, **cloud-based hardware security module** or HSM.
- The **HSM** in Cloud**HSM** means: **Hardware Security Module**



AWS CloudHSM



- Enables you to easily **generate and use your own encryption keys.**
- Encryption keys can be in 128-bit or 256-bit

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

HSM

Hardware Security Module



- A **physical hardware device**
- Performs **cryptographic operations**
- Securely stores cryptographic **key material**



AWS CloudHSM

Leading HSM Providers

THALES

utimaco®

IBM

SWIFT

yubico

Hewlett Packard Enterprise

- A random, **Base64 or hexadecimal string**
- **Binary** format (`.bin`)
- Used by your **encryption key.**



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudHSM

- The **CloudHSM clients** is installed and **hosted in your**:



Amazon EC2 Instances

- The HSM cluster is **deployed in your:**



Amazon VPC

- **Single Tenant** — Only used by one tenant or user (you)



- Can be used to:
  - Offload SSL Processing
  - Enabling Transparent Data Encryption (TDE) for Oracle databases
  - Protecting the private keys for an Issuing Certificate Authority (CA).

- Integrate CloudHSM and  AWS KMS to create a **custom key store.**



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Key Management Service (AWS KMS)

- A managed service that **works like:** **AWS CloudHSM**
- Internally, it **also uses hardware security modules (HSMs)** for creating and controlling your encryption keys.
- Has **multi-tenant access**

You **share** the HSM with other tenants or AWS customers

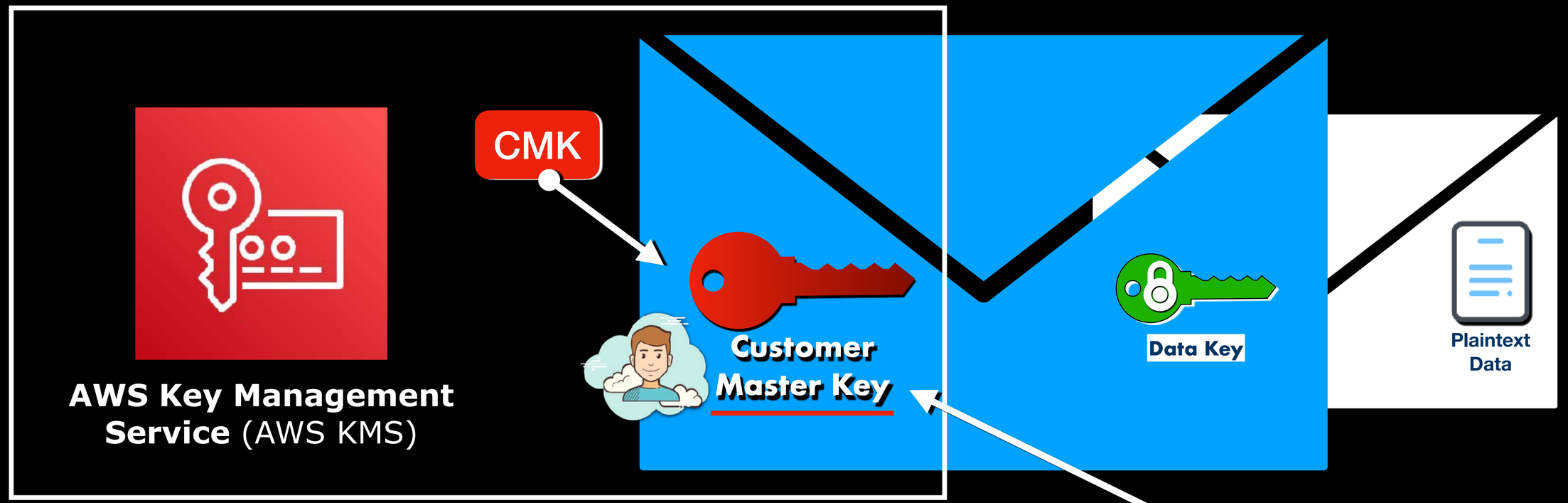


- Unlike CloudHSM, you **cannot launch the HSM to Amazon VPC or EC2 instances** *(as clients with direct HSM access)* that you own.
- Can be integrated with other AWS services to help you protect the data you store with these services.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ENVELOPE ENCRYPTION



- AWS KMS **automatically rotates** your CMK

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Key Management Service (AWS KMS)

- You can also create a **custom key store** in AWS KMS with



AWS CloudHSM



- Provides complete control over your **encryption key lifecycle management**
- Allows you to **remove the key material** of your encryption keys.



- You can **audit key usage independently** of:



AWS CloudTrail



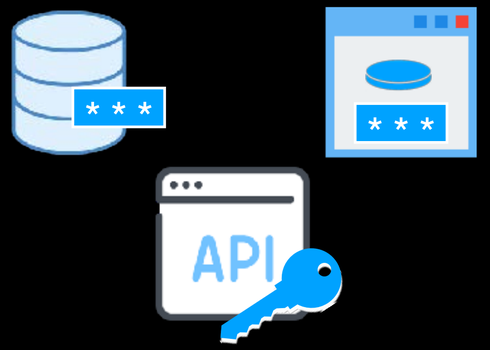
AWS KMS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Secrets Manager

- Protect the **secrets** of your applications, services, and IT resources.
- Enables you to easily **rotate, manage, and retrieve** your secrets
- A **secret** can be:
  - A database password
  - API key
  - Authentication token
  - Other sensitive data



- Eliminates hardcoded sensitive information in plain text in:



AWS Lambda

- Offers **secret rotation** with built-in integration for:



Amazon RDS



Amazon Redshift



Amazon DocumentDB



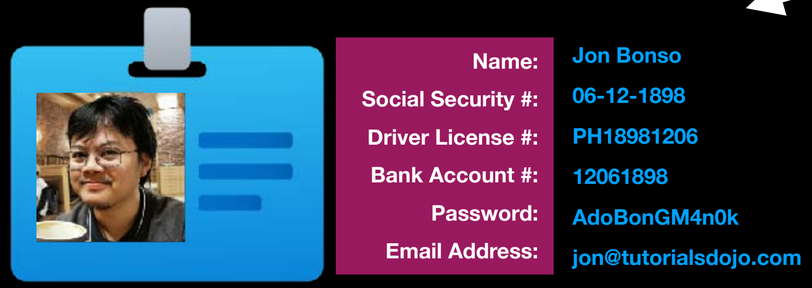
Other Services

- **Control access to secrets** using fine-grained permissions and centrally audit your secrets.
- **Not recommended** for storing encryption keys or key materials since it does not use an HSM

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Macie



- A fully managed **data security and data privacy** service
- Automatically **recognizes and classifies sensitive data** or intellectual property
- **Uses machine learning** to automatically discover, classify, and protect sensitive data stored in your:



Amazon S3 bucket



Other Services

- Recognizes sensitive data such as **personally identifiable information** or PII.
- **Provides dashboards and alerts** that give visibility into how sensitive data is being accessed or moved.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Certificate Manager
(AWS ACM)

- Provisions, manages, and deploys public and private Secure Sockets Layer/Transport Layer Security **(SSL/TLS) certificates**
- Enables you to **create private certificates** for your internal resources and **manage the certificate lifecycle centrally**
- SSL Certificates are **free of charge for ACM-integrated services** such as:



Amazon API Gateway



Elastic Load Balancing

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Inspector

- An **automated security assessment** service
- Improves the security and compliance of applications deployed on your AWS cloud infrastructure
- **Automatically assesses applications for vulnerabilities** or deviations from best practices.
- Produces a detailed list of security findings prioritized by level of security risk severity
- Provides an **automated security assessment report** that will identify unintended network access to your:



Amazon EC2 Instances

- The detailed assessment reports are available via the Amazon Inspector console or API

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Detective

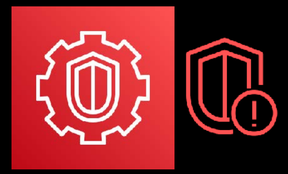
- Helps you **detect the root cause of your security issues** easier
- It analyzes, investigates, and quickly identifies the potential security issues or suspicious activities in your AWS infrastructure
- **Automatically collects log data from various AWS resources** such as:



AWS CloudTrail



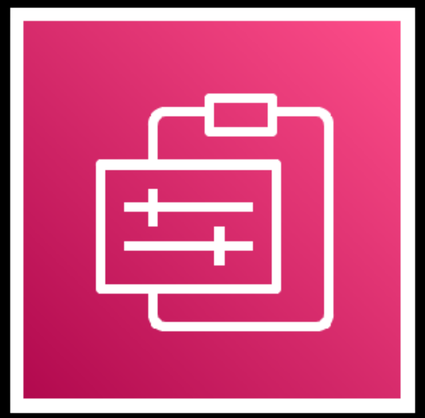
VPC Flow Logs



GuardDuty Findings

- **Uses machine learning** to analyze and conduct security investigations.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Management & Governance Services Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Management & Governance Services



SOP

Standard Operating Procedures



HIPAA

Health Insurance Portability and Accountability Act of 1996



GDPR

General Data Protection Regulation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Management & Governance Services

MANAGE

– control resources

AWS Management Console

AWS Command Line Interface (AWS CLI)

AWS Console Mobile Application

AWS Resource Access Manager

AWS Systems Manager (SSM)

GOVERN

– enforce standards
– ensure compliance

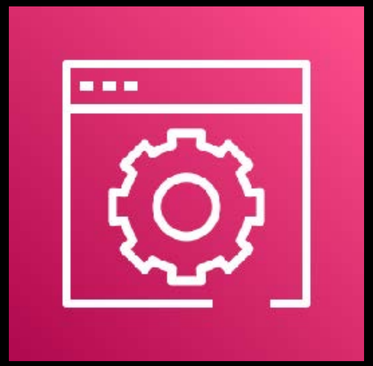
AWS Config

AWS Organizations

AWS Service Catalog

AWS Control Tower

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Management Console

- A **web interface** to control your AWS resources
- Accessible through your **web browser**
- Log in using your IAM username and password
- Supports **Multi-Factor Authentication** (MFA)
- Accessible via this URL: `https://console.aws.amazon.com`

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Command Line Interface
(AWS CLI)

- A **command-line interface** to control your AWS resources
- Accessible through your terminal, command prompt or Windows PowerShell





- Allows you to **develop custom shell scripts** that invoke different AWS CLI commands

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Console Mobile Application

- The **official mobile app** provided by Amazon Web Services
- Allows you to monitor your resources through a dedicated dashboard
- Enables you to view your configuration details, metrics, and alarms of **select AWS services** (not all services) on your mobile device
- Provides an overview of the account status, real-time CloudWatch metrics, Personal Health Dashboard, and AWS Billing
- Has **limited capabilities** compared with:



AWS Management Console



AWS CLI

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager
(SSM)

- A **suite of services** that allows you to manage your resources
- Allows you to **control both of your AWS Cloud and on-premises** infrastructure
- Composed of:



Session Manager



State Manager



Patch Manager



Automation



Maintenance Windows



Run Command



Parameter Store



Others

- Also has an **SSM agent** that you can install on your EC2 instances or on-premises servers to centrally manage your resources



Amazon EC2 Instances



On-premises Servers

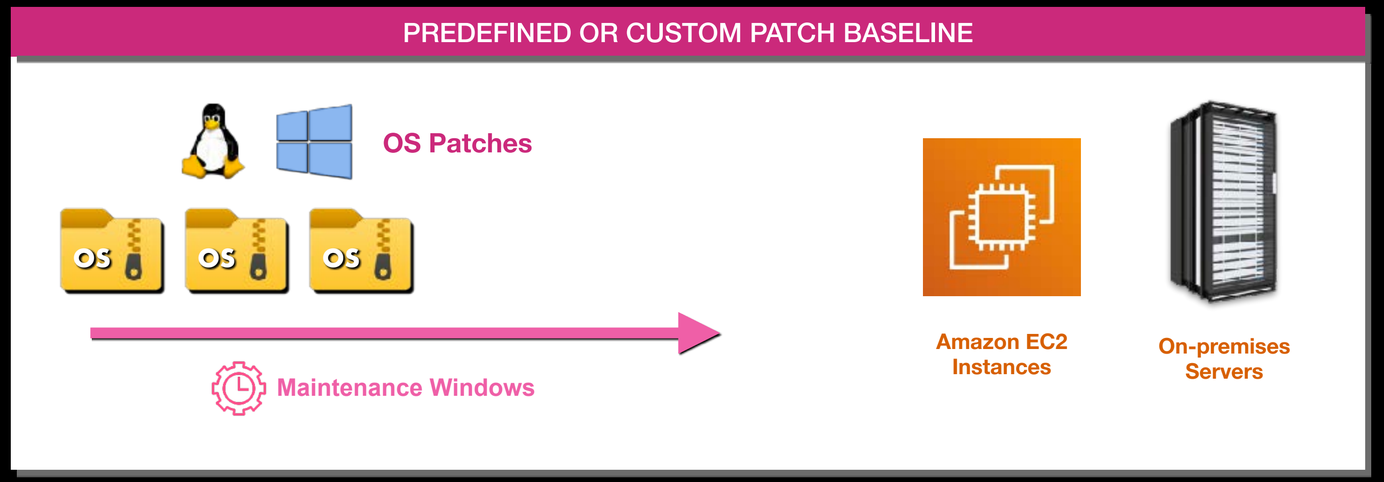
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager
(SSM)



Patch Manager





State Manager

STATE

- Installed softwares (e.g. startup script, antivirus etc)
- Server configurations
- Firewall settings
- Associate Ansible playbooks, Chef recipes, PowerShell modules, and other SSM Documents



Parameter Store

PARAMETER

- Passwords
- Database Strings
- Amazon Machine Image (AMI) IDs
- License Codes
- Environment Variables



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

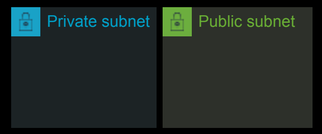


AWS Resource Access Manager (AWS RAM)

- Enables you to easily and **securely share your AWS resources** with any AWS account or within your AWS Organization
- Allows you to share:



AWS Transit Gateway



Subnets



AWS License Manager



Amazon Route 53 Resolver

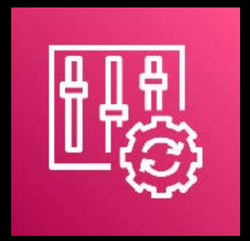


Other AWS Resources

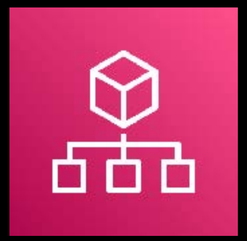
- **Eliminates the need to create duplicate resources** in multiple accounts
- **Reduces the operational overhead** of managing multiple resources in each and every single account you own.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





AWS Config



AWS Organizations

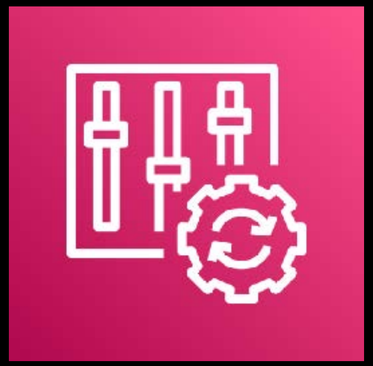


AWS Service Catalog



AWS Control Tower

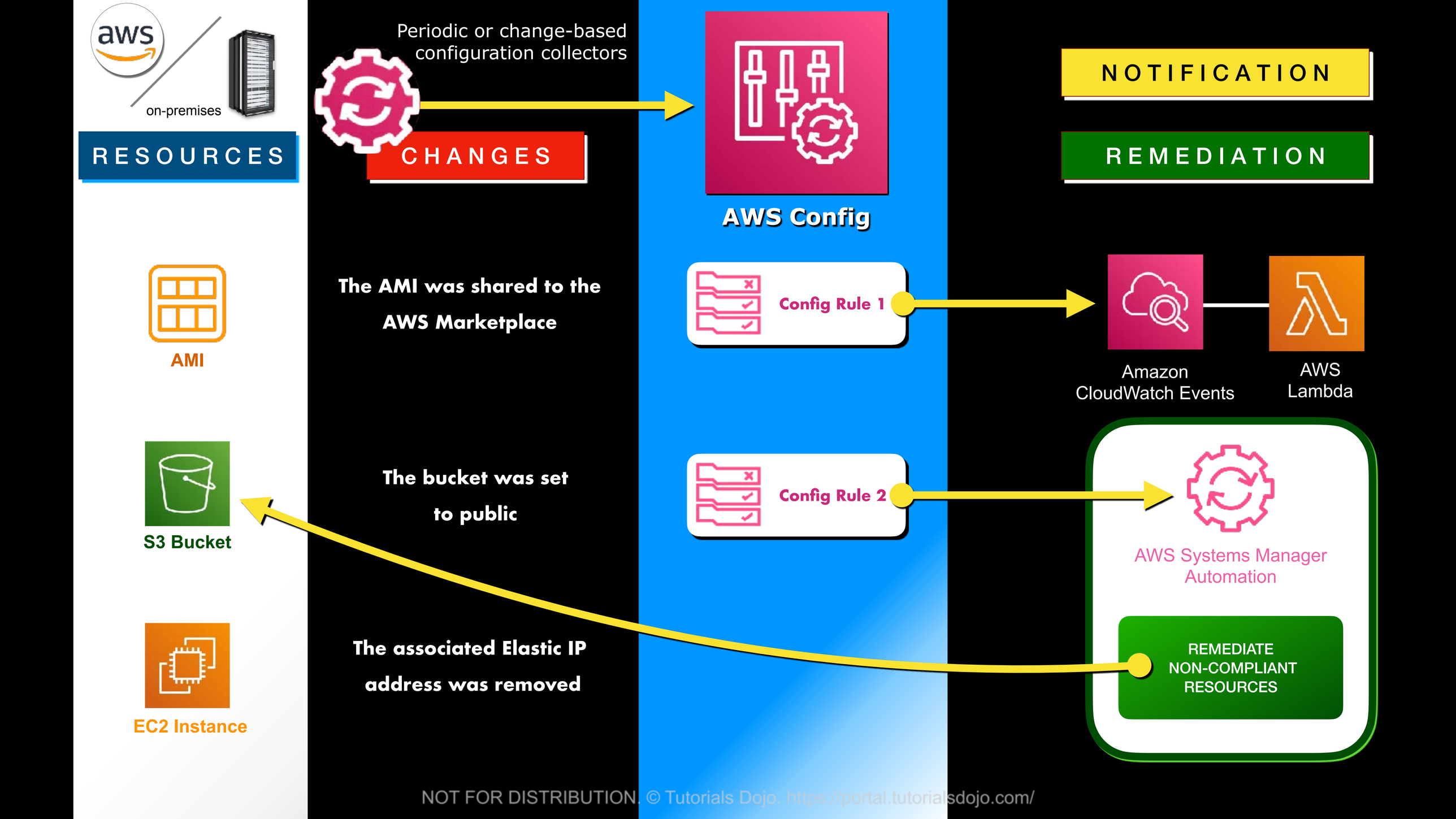
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



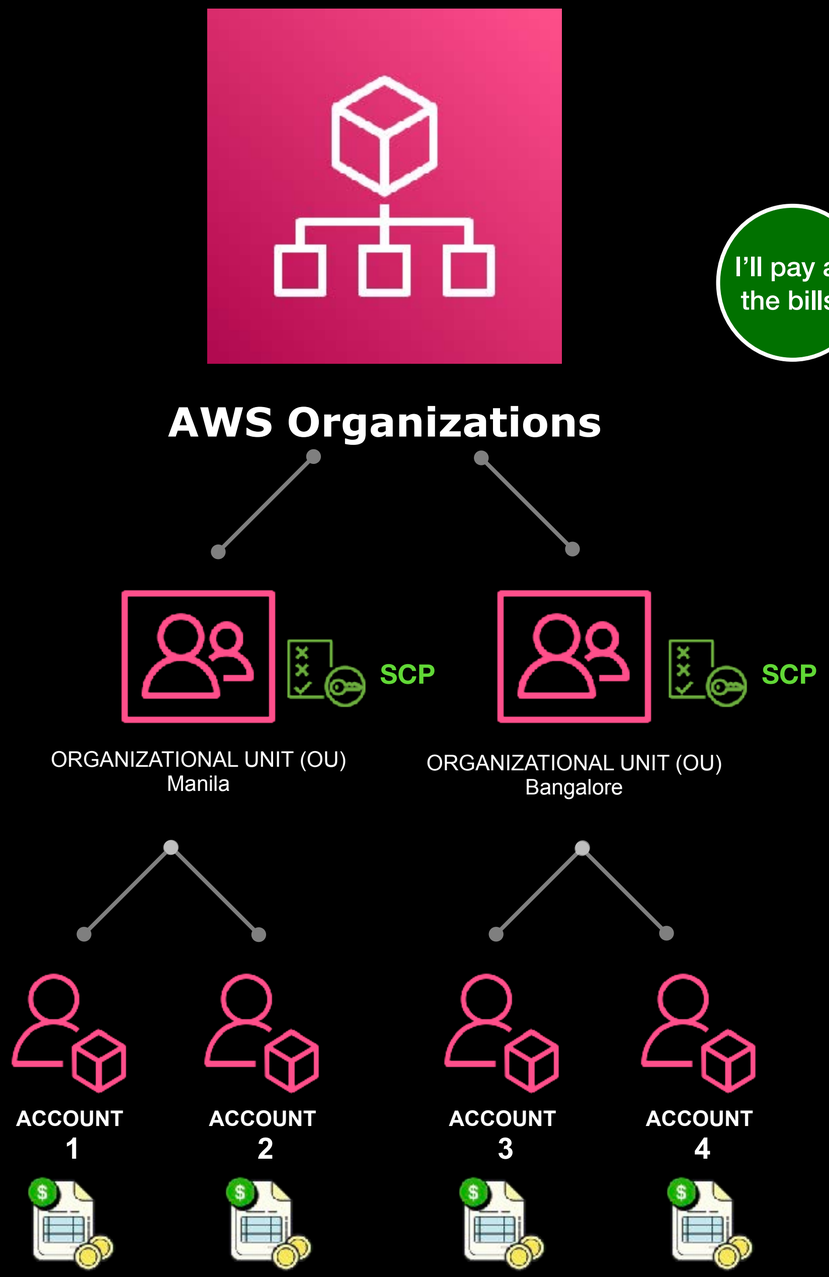
AWS Config

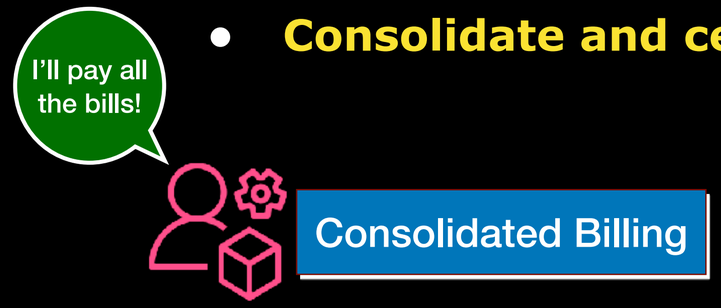
- Enables you to **assess, audit, and evaluate the configurations** of your AWS resources
- Automates your **compliance assessment** process
- **Provides visibility on the existing configurations** of your various AWS services and third-party resources (such as your on-premises servers)
- Enables you to **identify the changes** made to a specific resource over time

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

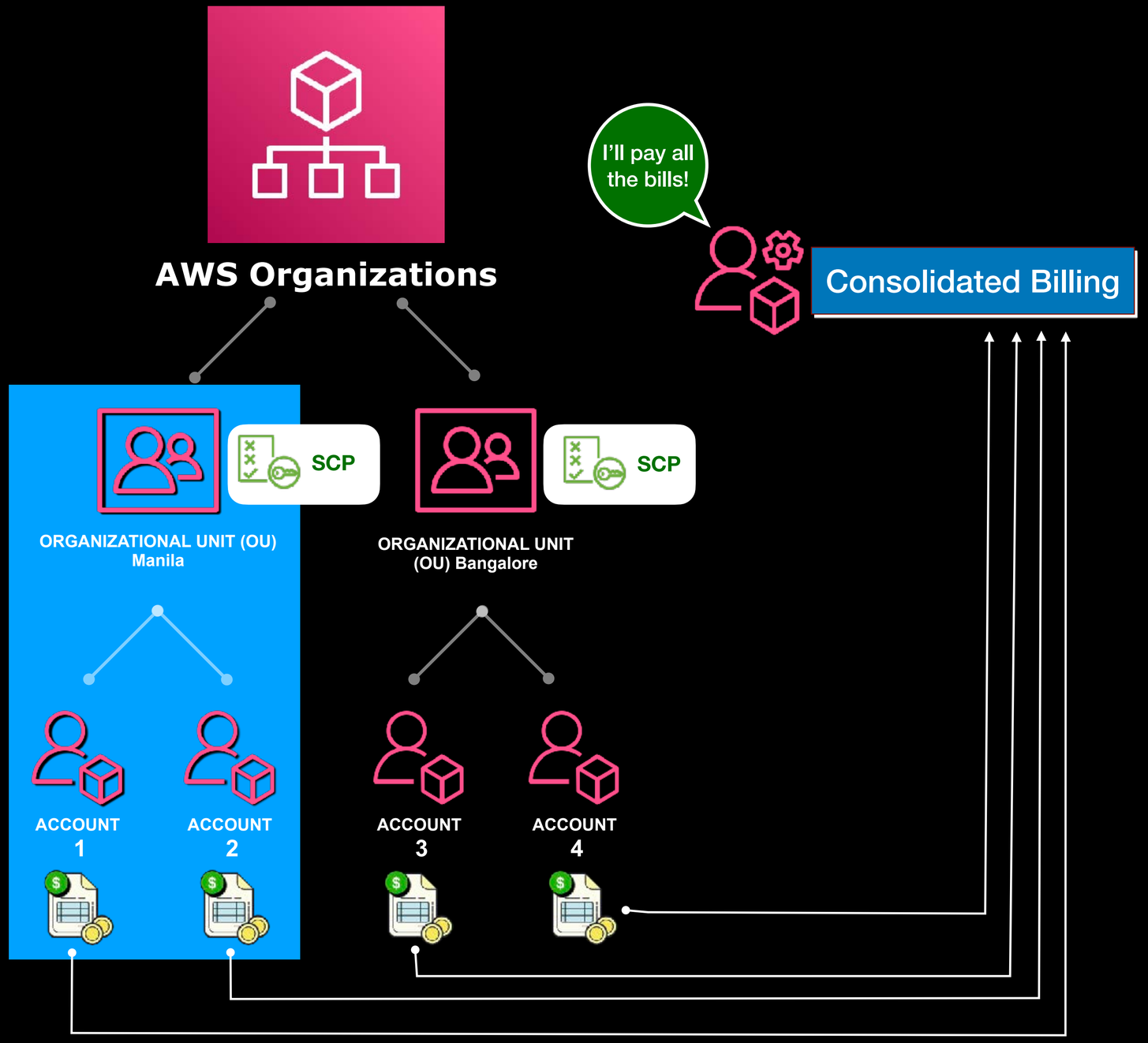




- **Consolidate and centrally manage** multiple AWS accounts
  - Combines the bills of multiple AWS accounts
  - Provides **volume discounts** to further lower down your costs
- Uses **Service Control Policies (SCP)** to control access and ensure organizational compliance across your AWS accounts
- Offers **Central Logging** to monitor all activities performed across your organization using AWS CloudTrail
- **Aggregate data from all your AWS Config rules** to quickly audit your environment for compliance.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

A single AWS Organization can have two or more Organizational Unit (OU) and underlying AWS accounts with Service Control Policies (SCPs) attached



Tutorials Dojo
www.tutorialsdojo.com
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Service Catalog

- Empowers you to **set up and centrally manage catalogs** of approved IT services
- Allows you to manage various IT services, referred to as "**products**" in Service Catalog then group them in a portfolio

PRODUCT

- Machine image (AMI)
- Application server
- Program
- Tool
- Database
- Other services

- Assists you in meeting your compliance requirements
- **Enforce granular access control** to your resources

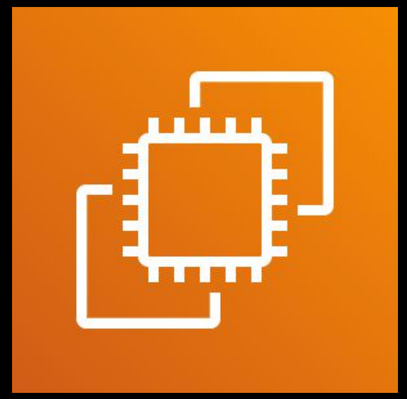
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Control Tower

- Helps you **set up and govern a secure multi-account** AWS environment
- Automates the setup of your multi-account AWS environment
- Uses **blueprints** that follow AWS best practices for security and management
- Provides mandatory high-level rules called **guardrails**
- Help enforce your policies using service control policies (SCPs)
- **Detect policy violations** using AWS Config rules

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2 Overview

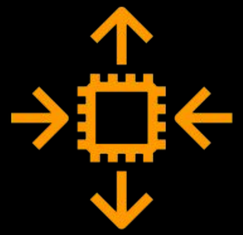
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

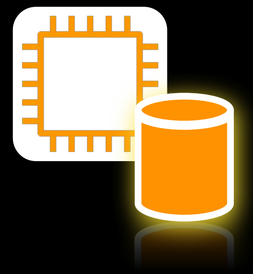


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

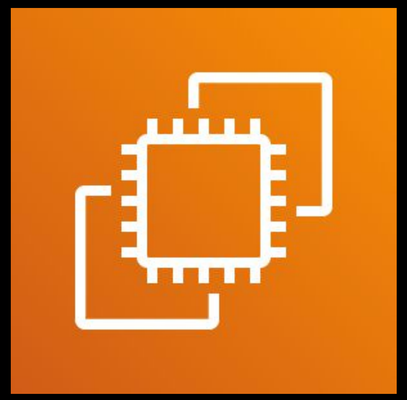






Can be integrated with a lot of AWS Services

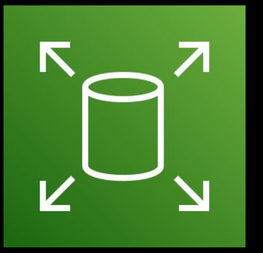


Amazon EC2







NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon VPC



Elastic IP Address



Elastic Network Interface (ENI)



Elastic Network Adapter (ENA)



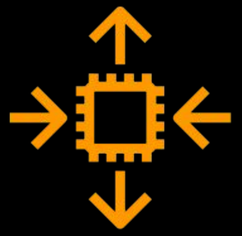
Placement Groups



Elastic Fabric Adapter (EFA)



Your Computer

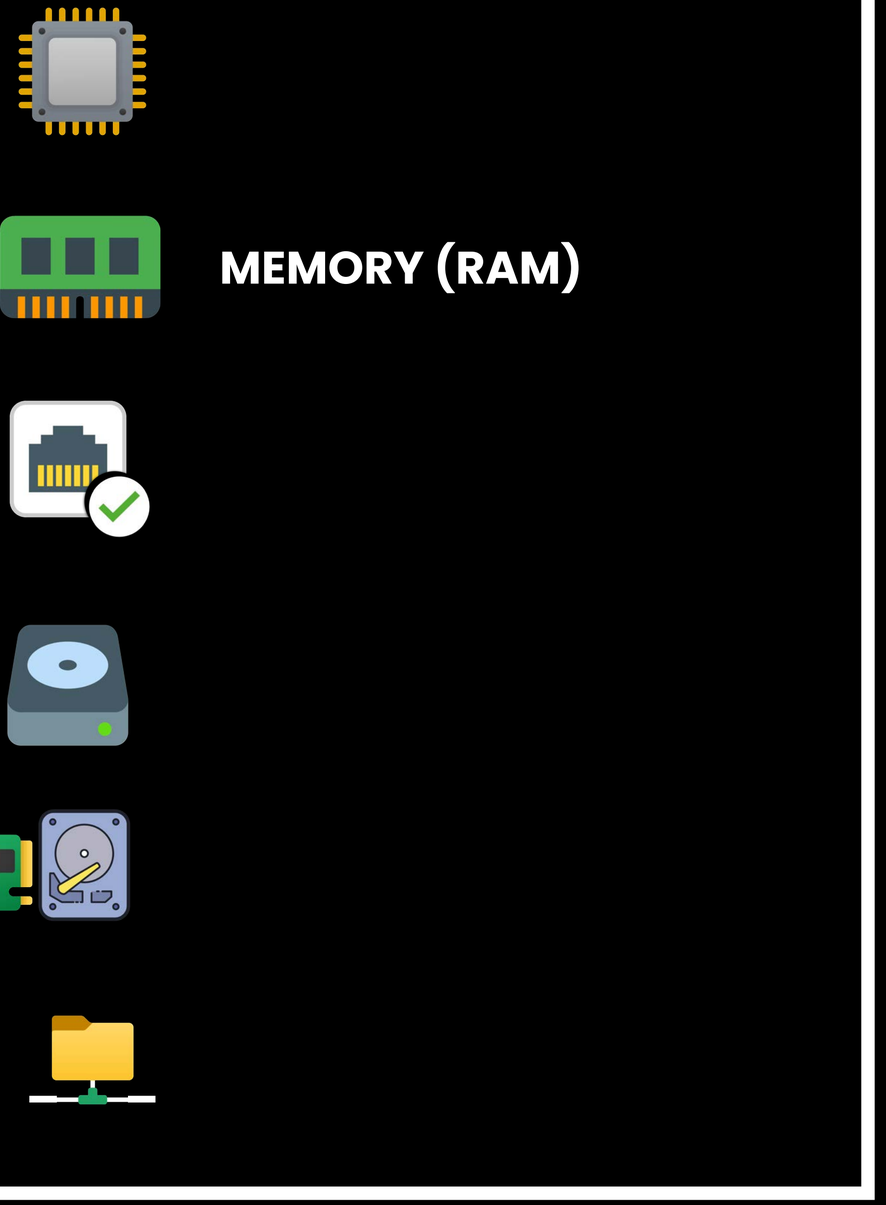




Amazon EC2

both have





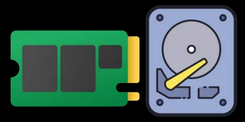
MEMORY (RAM)

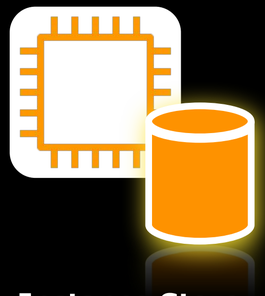






NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





Instance Store



Amazon EBS





Amazon EFS



Amazon FSx for Lustre



Amazon FSx for Windows File Server



OBJECT STORAGE



Amazon S3

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NETWORK



Amazon VPC



Elastic IP Address



Elastic Network Interface (ENI)



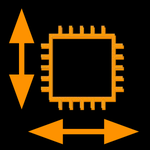
Placement Groups



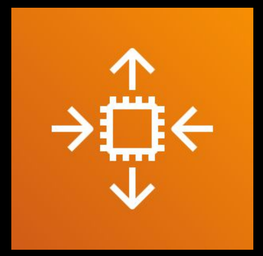
Elastic Network Adapter (ENA)



Elastic Fabric Adapter (EFA)



AUTO SCALING



Amazon EC2 Auto Scaling





Amazon Machine Image (AMI)

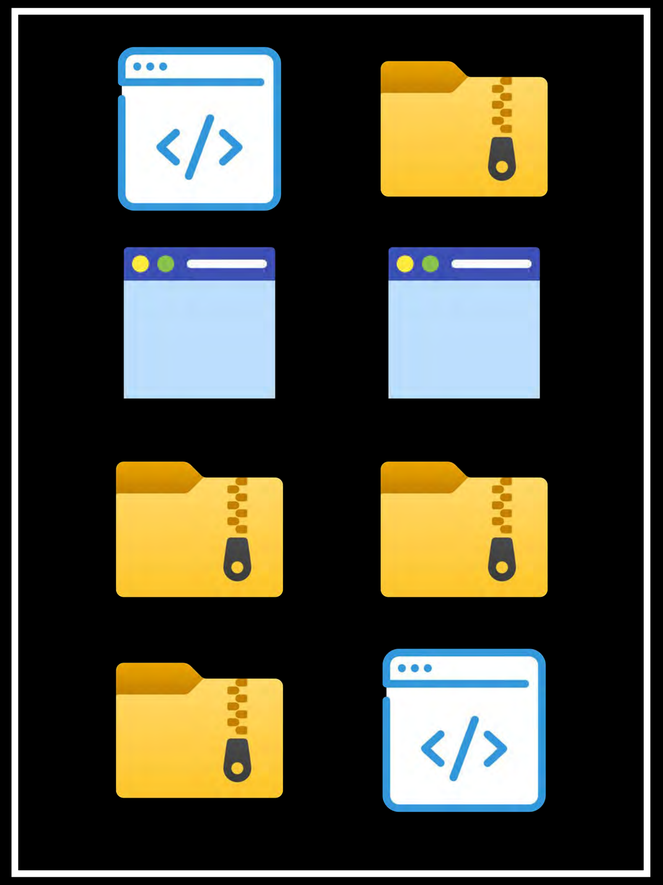
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Machine Image (AMI)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

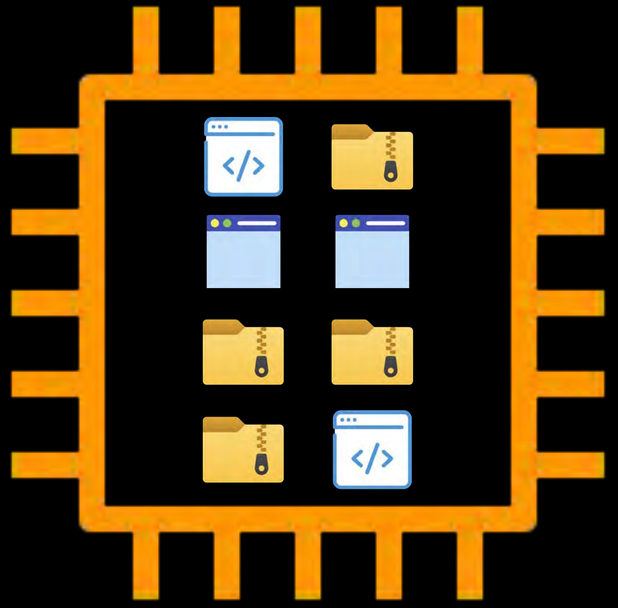
apps & configurations



AMI

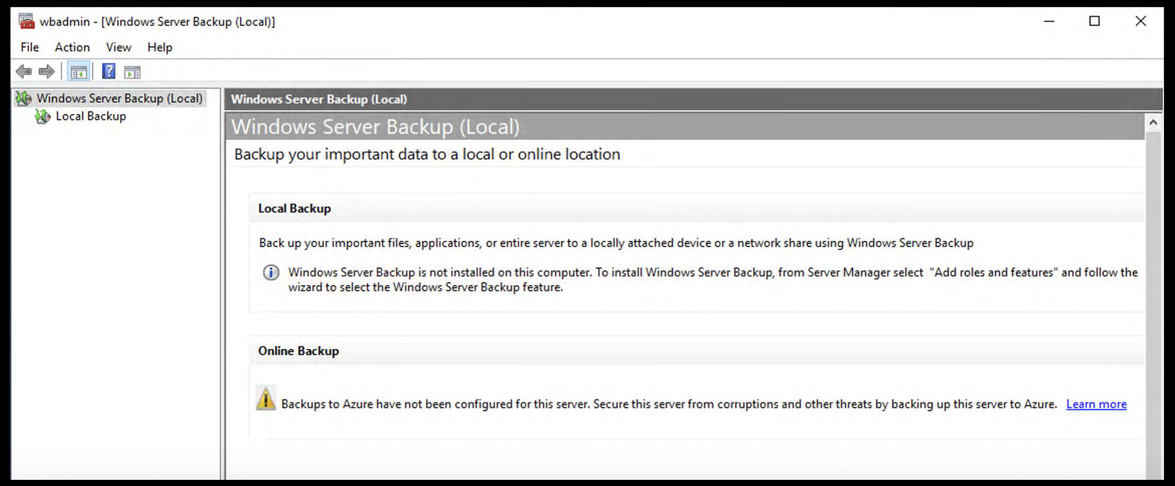


EC2 Instance



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

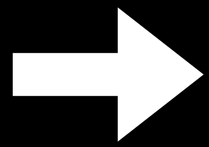






NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/







Amazon Machine Image (AMI)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Machine Image (AMI)

Volume Snapshots

Block Device Mapping

Launch Permissions

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

BLOCK STORE TYPE



Amazon Machine Image (AMI)

	Volume Snapshots	Block Device Mapping	Launch Permissions
Amazon EBS	 EBS Snapshots	 Amazon EBS Volumes mapping	• Public • Explicit • Implicit
Amazon EC2 Instance Store	 Template for the root volume	N/A	

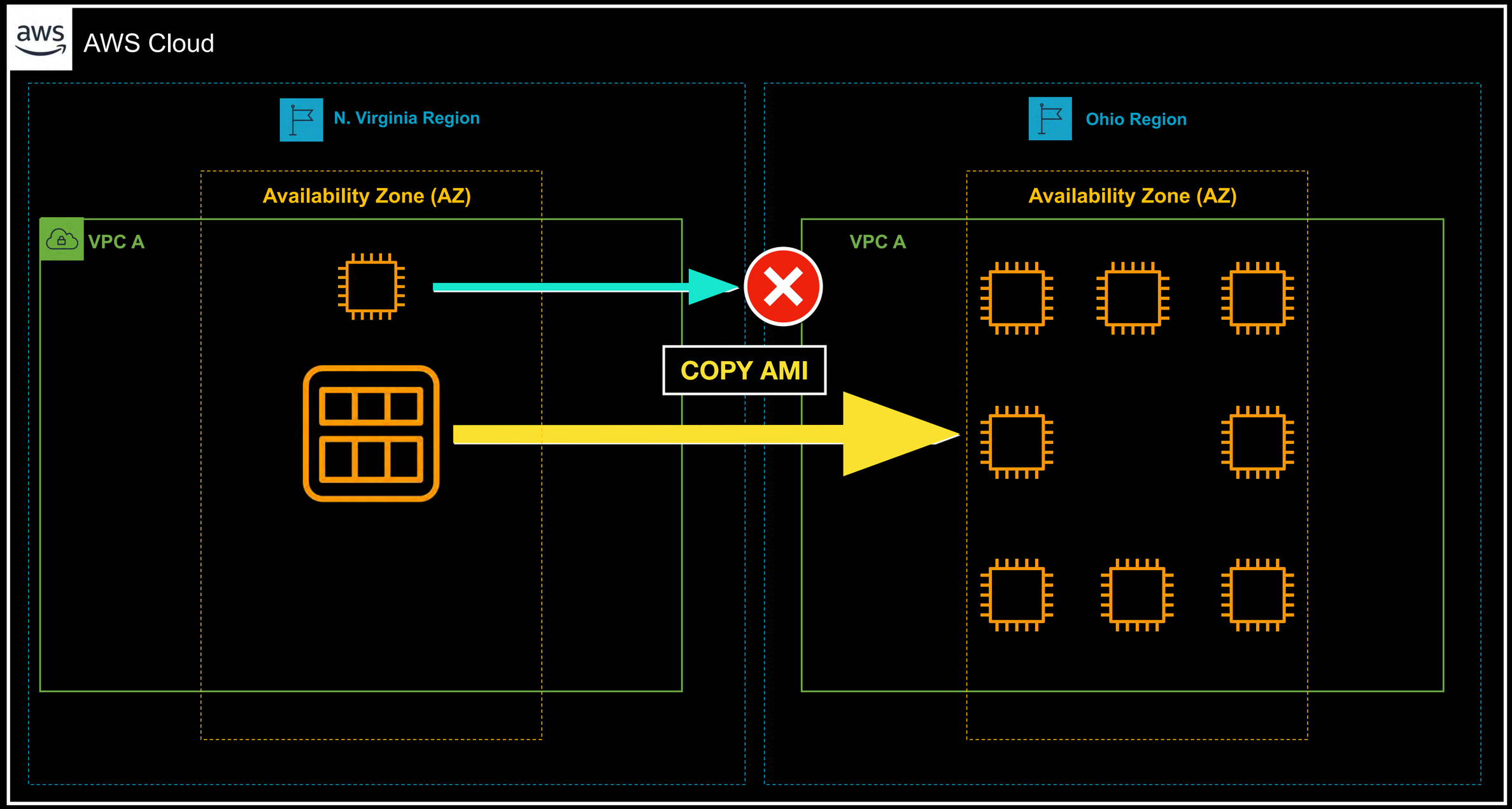
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Machine Image (AMI)

- **Regional** in scope
- You can **copy your AMI to another AWS Region**
- You can also copy your AMI to **another AWS account**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Marketplace



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Machine Image (AMI)

VIRTUALIZATION TYPE

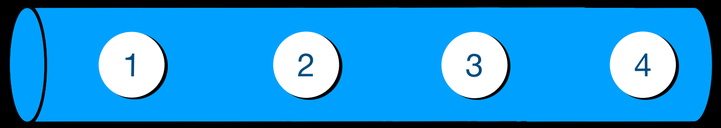
VIRTUALIZATION TYPE	BOOT UP PROCESS	SUPPORT FOR SPECIAL HARDWARE EXTENSIONS
PV Paravirtual	Uses special boot loader called **PV-GRUB**	**N/A**
HVM Hardware Virtual Machine	Executes the master boot record of the root block device of your image	Uses several special hardware extensions such as **enhanced networking** or **GPU processing**

PV Paravirtual

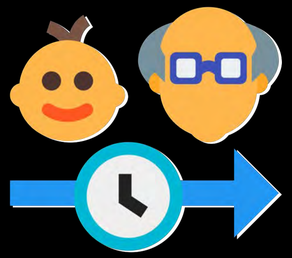
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon SQS

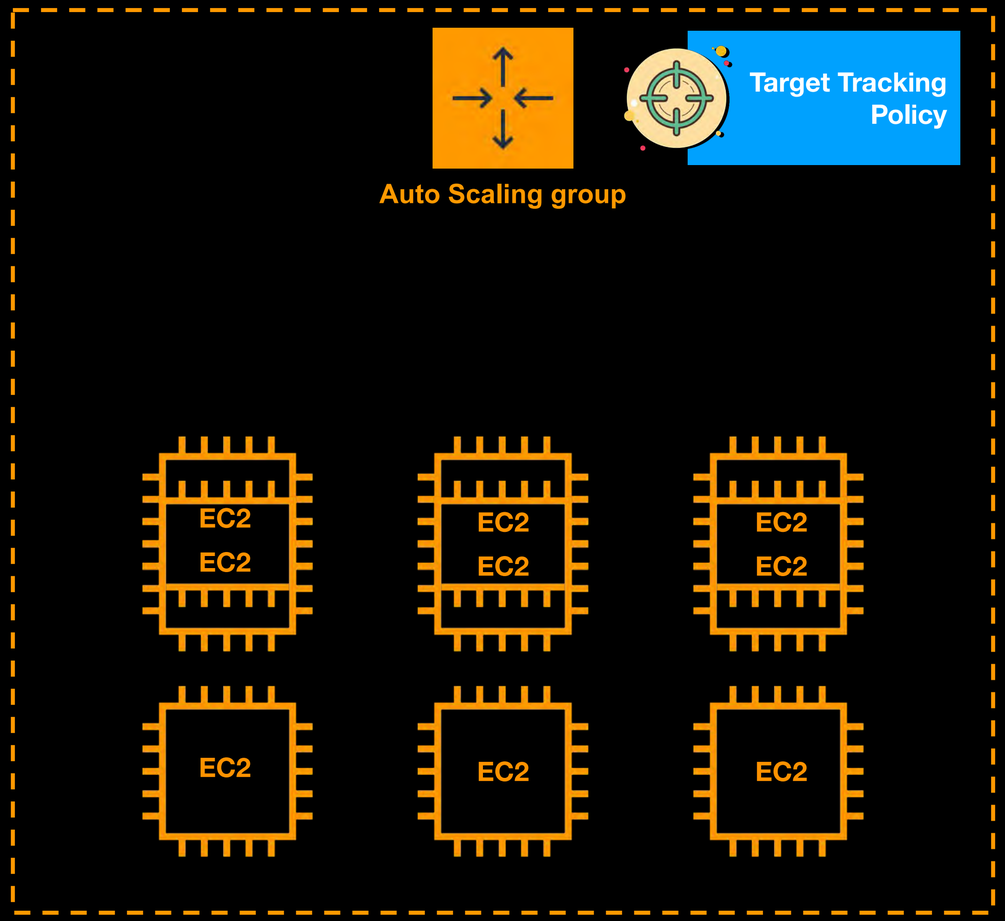


- **Age** of the Oldest Message

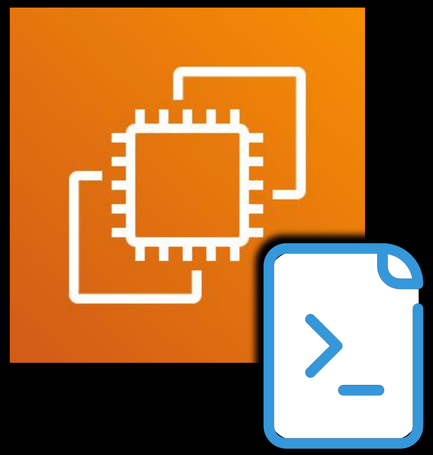


Amazon Machine Image (AMI)





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Instance User Data

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

```
#!/bin/bash
yum update -y
mkdir tdojologs
systemctl start httpd
echo “tutorialsdojo OK!”
```



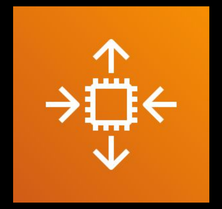
User Data

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EFS





Auto Scaling Group

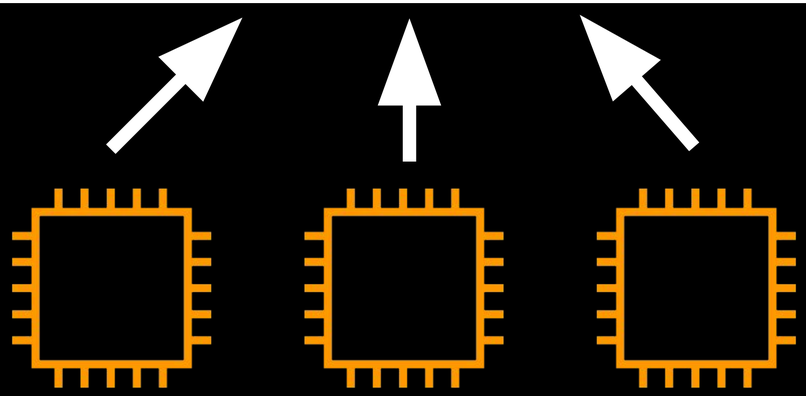
```
mkdir ~/tutorialsdojo-efs

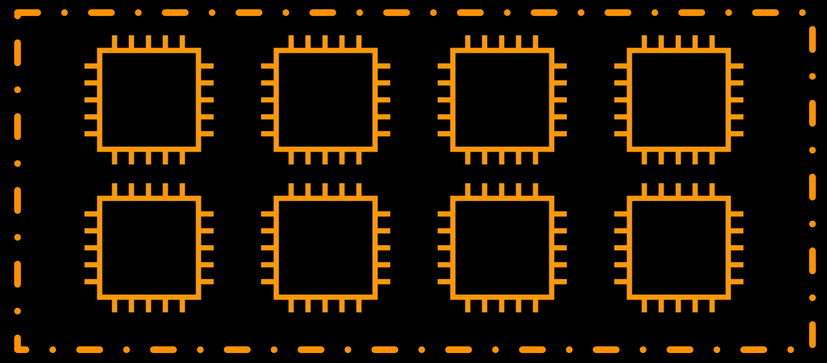
sudo mount -t nfs -o nfsvers=4.1,\
rsize=1048576,wsize=1048576,hard,\
timeo=600,retrans=2,noresvport \
awsjonbonsoefs:/    ~/tutorialsdojo-efs
```



```
#!/bin/bash
curl
https://s3.amazonaws.com/aws-cloudwatch/dow
nloads/latest/awslogs-agent-setup.py -O
chmod +x ./awslogs-agent-setup.py
./awslogs-agent-setup.py -n -r us-east-1 -c
s3://tutorialsdojo
```

User Data





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



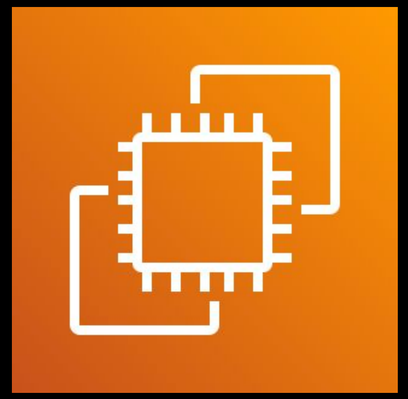
User Data

- Must be in a **base64-encoded format**
- Limited to **16 KB only when in raw form**
- Accessible from the Instance Metadata using this URI:

```
http://169.254.169.254/latest/user-data
```

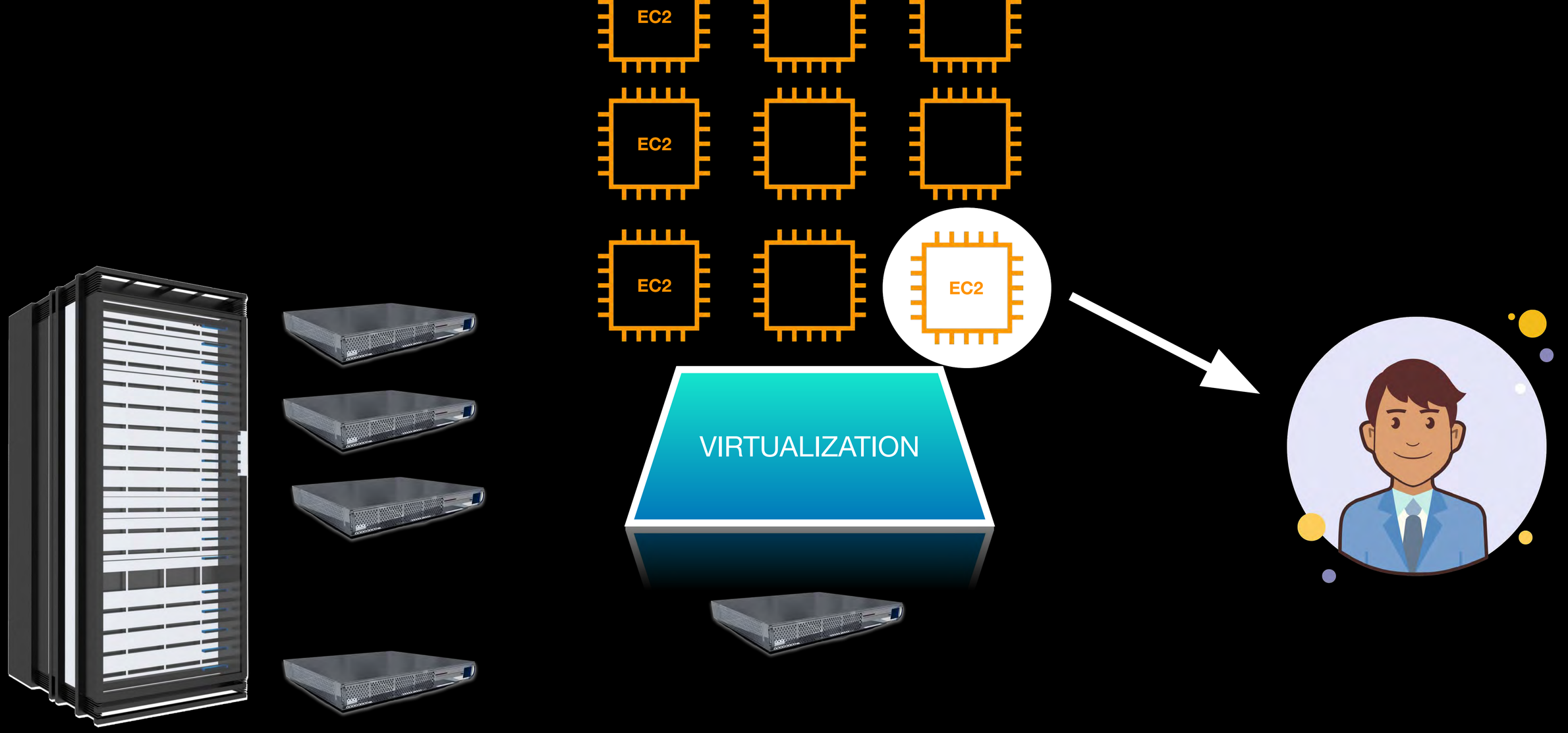
- **Only run once** upon the first EC2 Instance Launch
- Modifying the User Data and restarting the instance won’t affect the initial User Data

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Instance Metadata

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



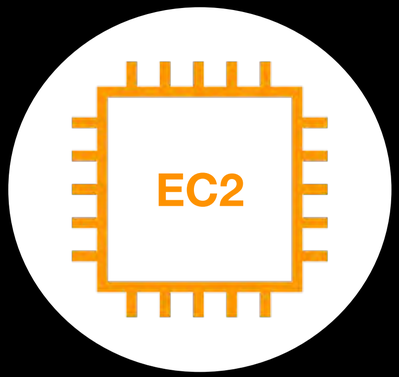
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

MANIFEST





METADATA



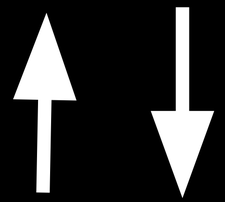
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

- AMI
- Hostname
- Public IP address
- Private IP address
- Instance type
- MAC address
- Security groups
- Security credentials
- IAM Roles of your instance
- . . . and many more!

INSTANCE METADATA



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Link-local Address

INSTANCE METADATA SERVICE

http://169.254.169.254/latest/meta-data/

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

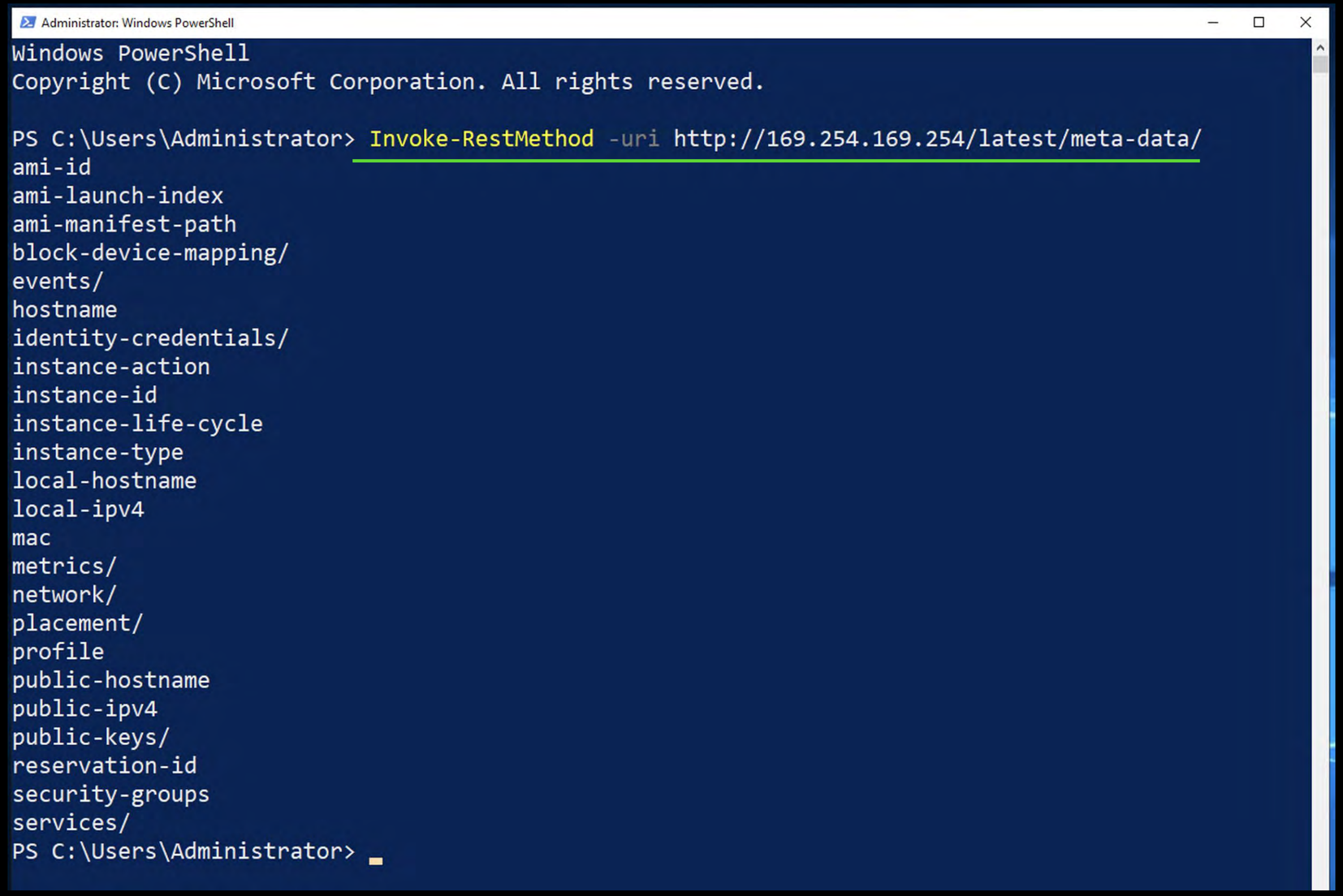


```
jonbonso — Philippines - Amazon EC2 Instance - Cebu, Davao, Palawan, Cagayan De Oro, Tarlac, Pangasinan — Tutorials Dojo Manila Server — ssh -i ~/

jonbonso@tutorialsdojo >curl http://169.254.169.254/latest/meta-data
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Windows



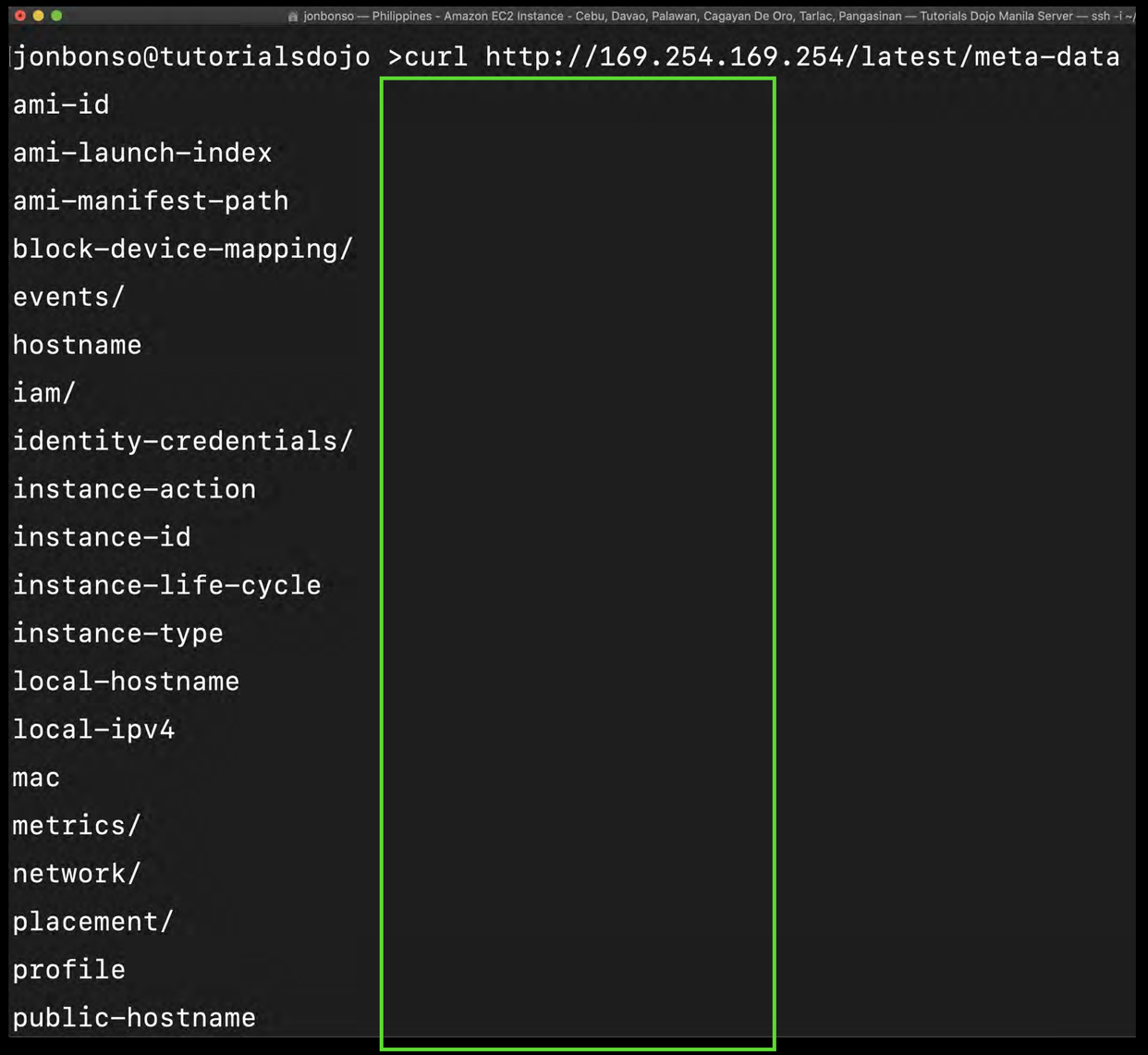
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

INSTANCE METADATA SERVICE version 2

Session Oriented

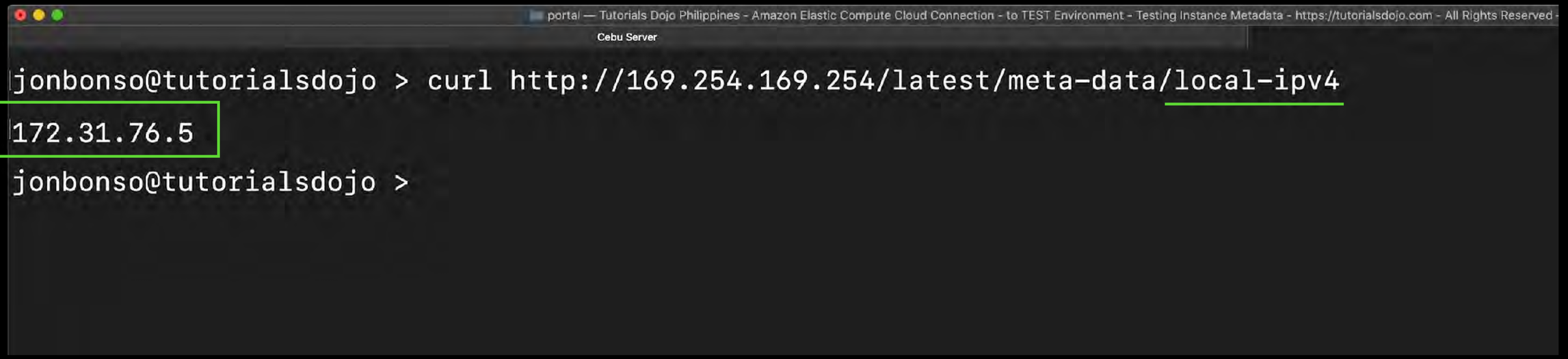
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

CATEGORIES



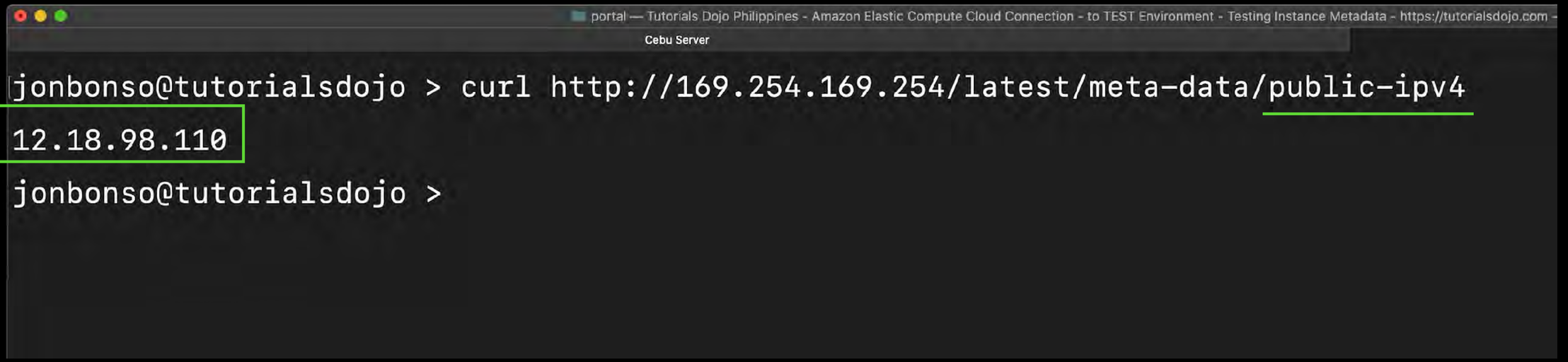
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Private IP Address



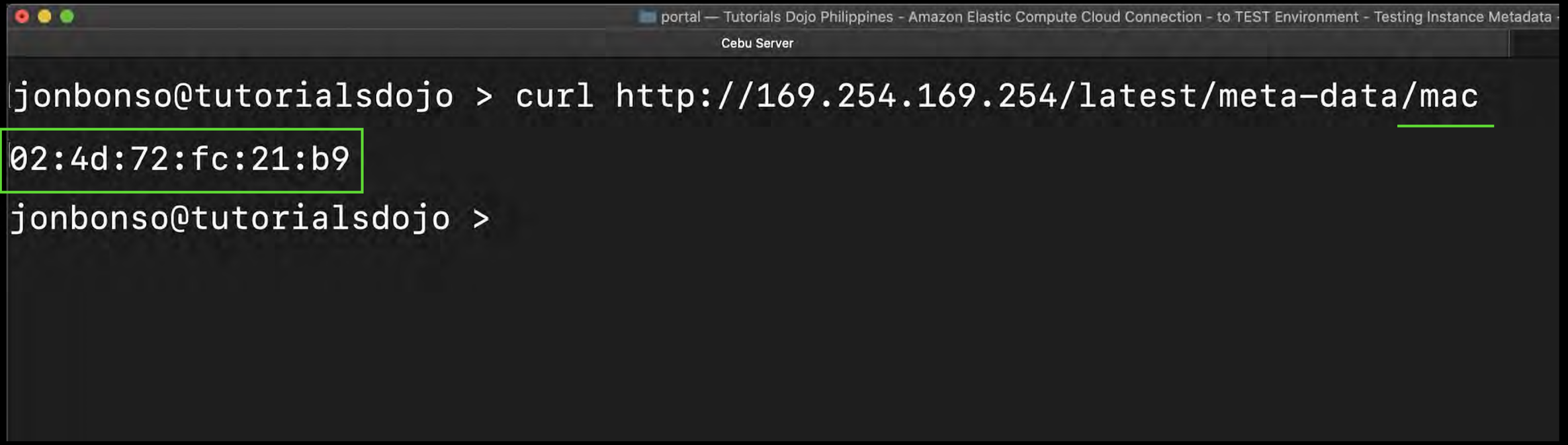
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Public IP or Elastic IP Address



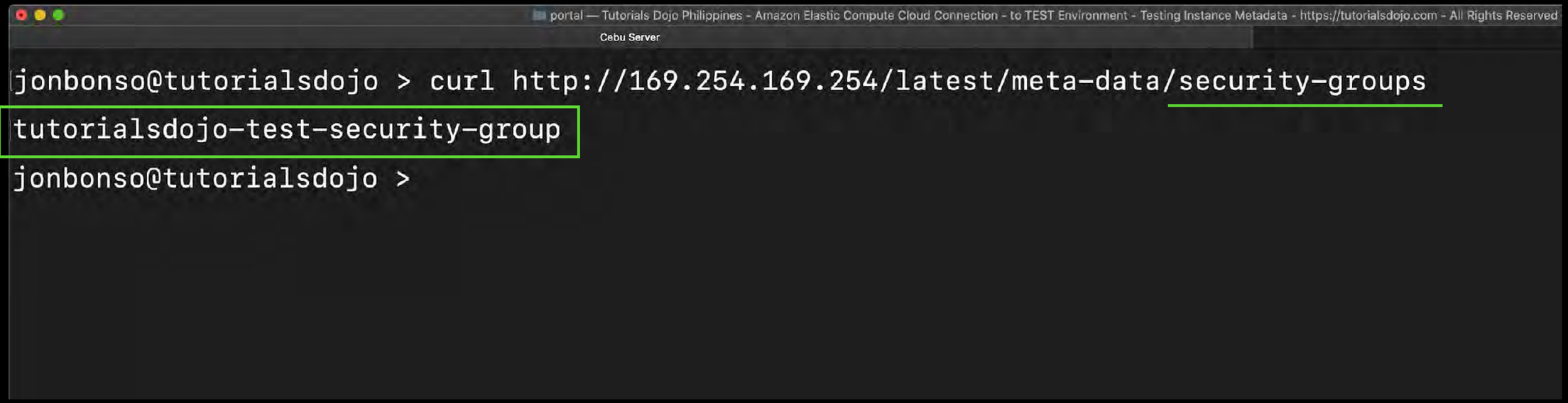
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Media Access Control (MAC) Address



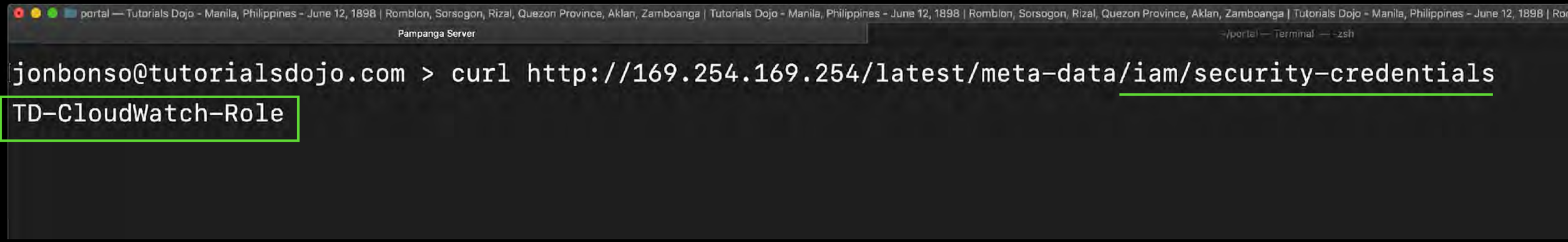
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Security Groups

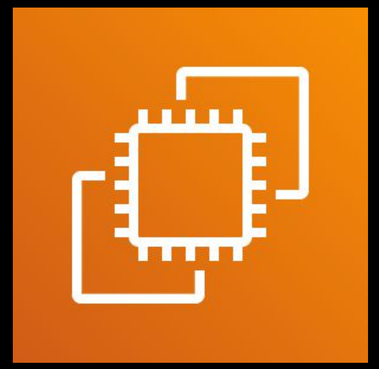


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Instance Profile



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2

Instance Purchasing Options

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Underlying Physical Servers of Amazon EC2

Virtual Machines



Rack



Rack-mounted servers

A **single** server can instantiate **multiple** EC2 Instances



Shared by MULTIPLE Tenants / Customers across the globe!







NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

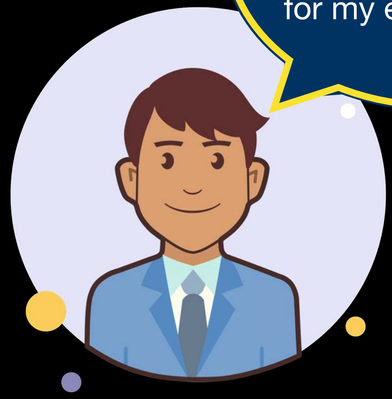
Spare or Unused Server





Amazon EC2 Service

INTERRUPTION



I would like to rent the entire server without any virtualization & is **dedicated** for my exclusive use!



I would like to **reserve** this instance for 1 year at **$1.5** / hour

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

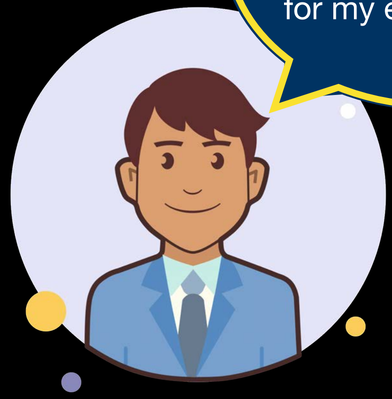
Spare or Unused Server





Amazon EC2 Service

INTERRUPTION

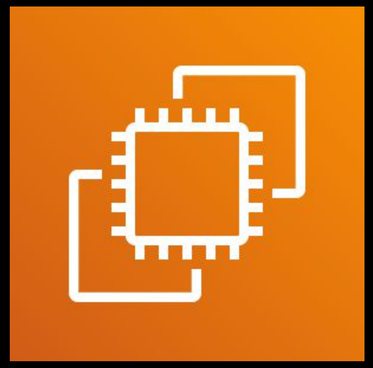


I would like to rent the entire server without any virtualization & is **dedicated** for my exclusive use!

I want to order an EC2 Instance for **$2** / hour



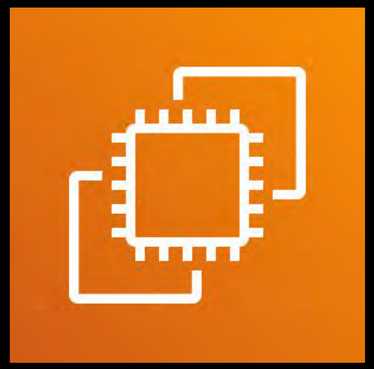
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2
Instance Purchasing Options

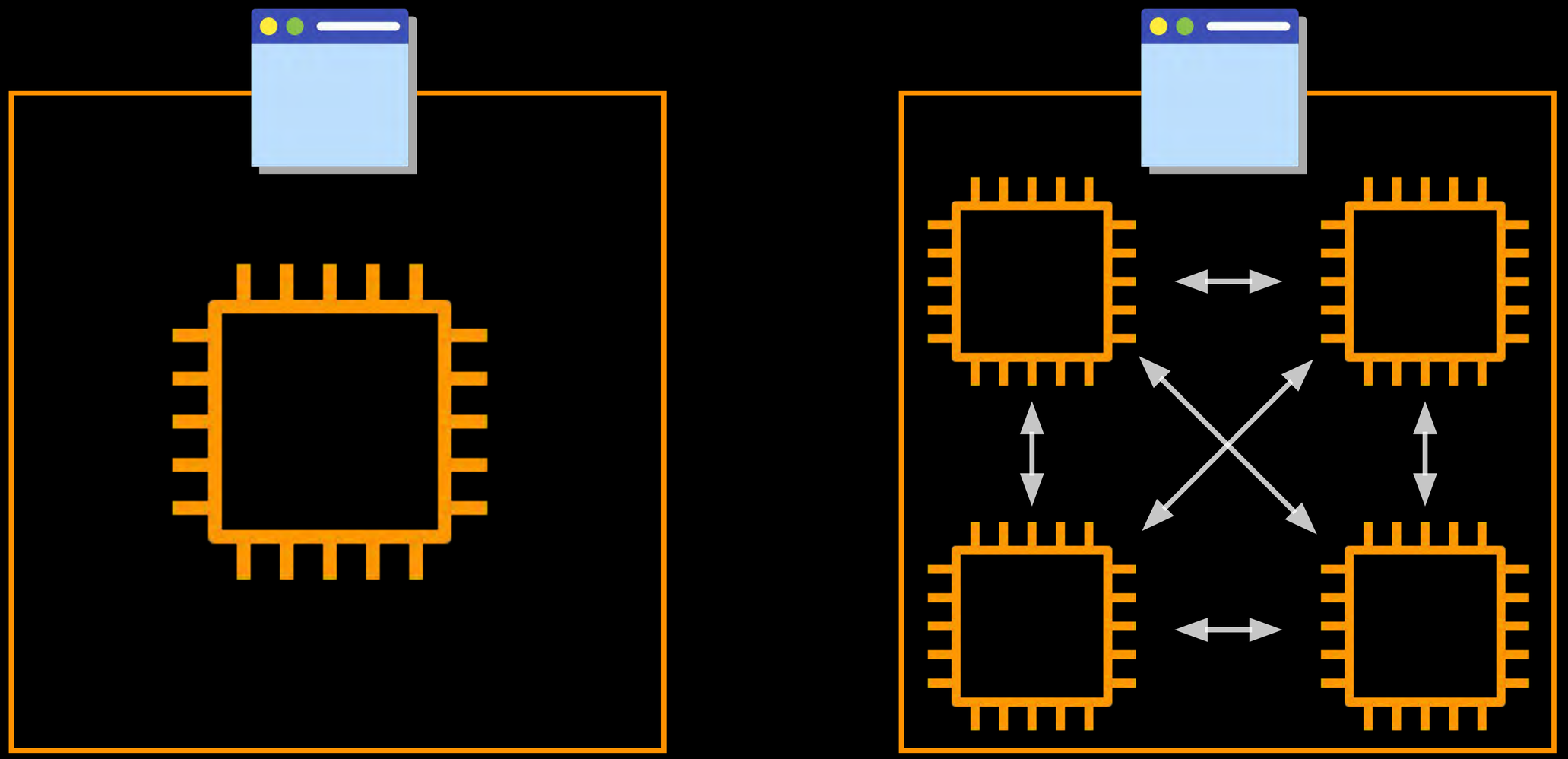
- **On-Demand**
- **Spot**
- **Reserved**
- **Dedicated**
- **Savings Plans**
- **Capacity Reservation**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Placement Groups

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

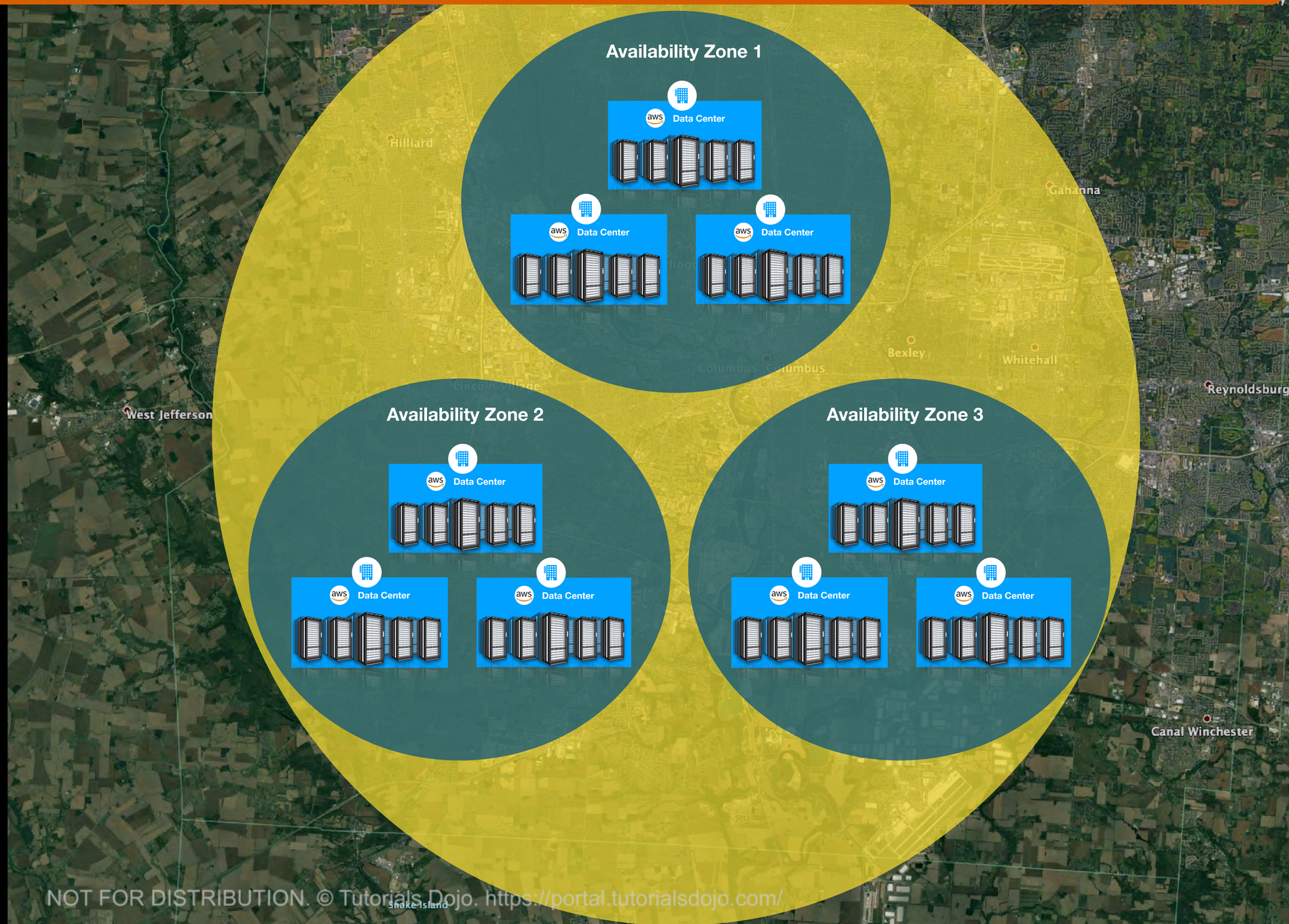


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

US East (Ohio)
us-east-2



Amazon EC2 Service



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

US East (Ohio)
us-east-2

I'll place you…

EC2

Amazon EC2 Service

Franklin

Gahanna

Upper Arlington

Bexley

Whitehall

Columbus

Columbus

Lincoln Village

Grove City

Availability Zone 3

aws Data Center



aws Data Center



aws Data Center

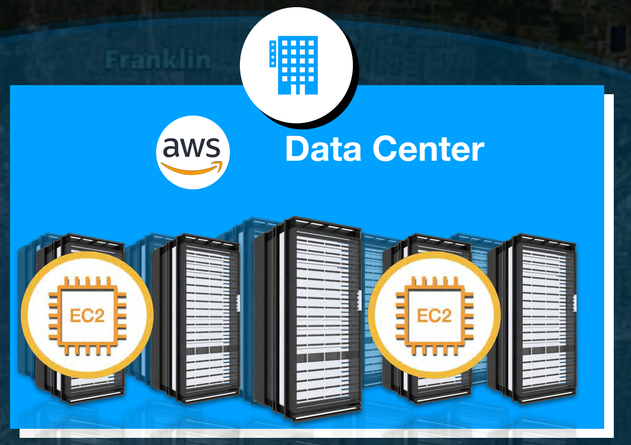


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

US East (Ohio)
us-east-2

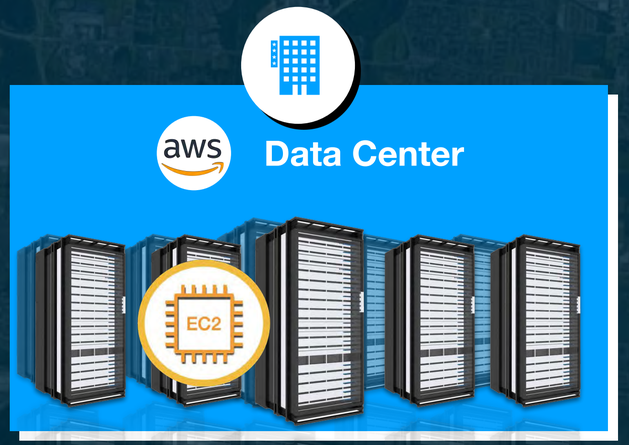


Amazon EC2 Service

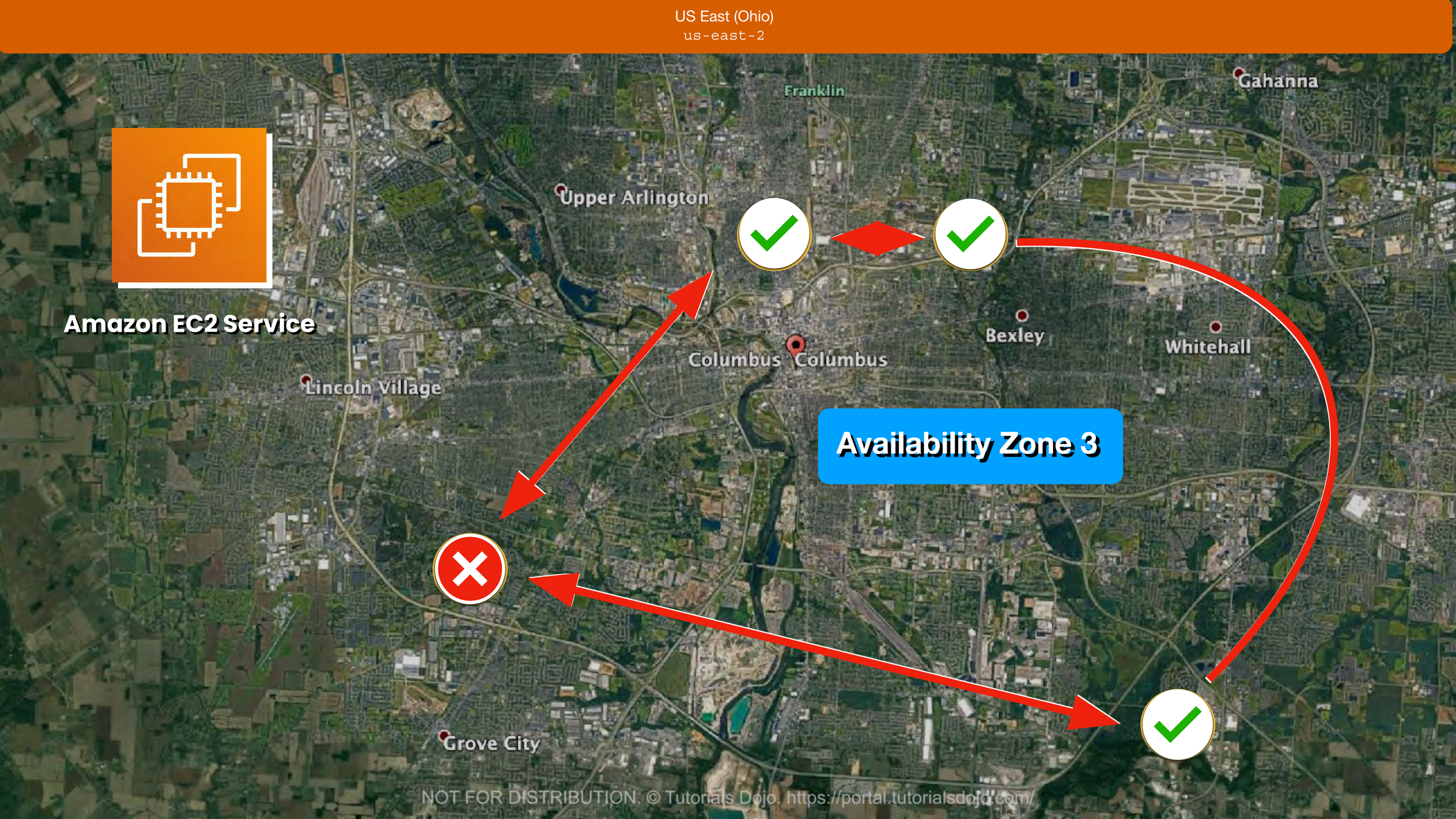




Availability Zone 3



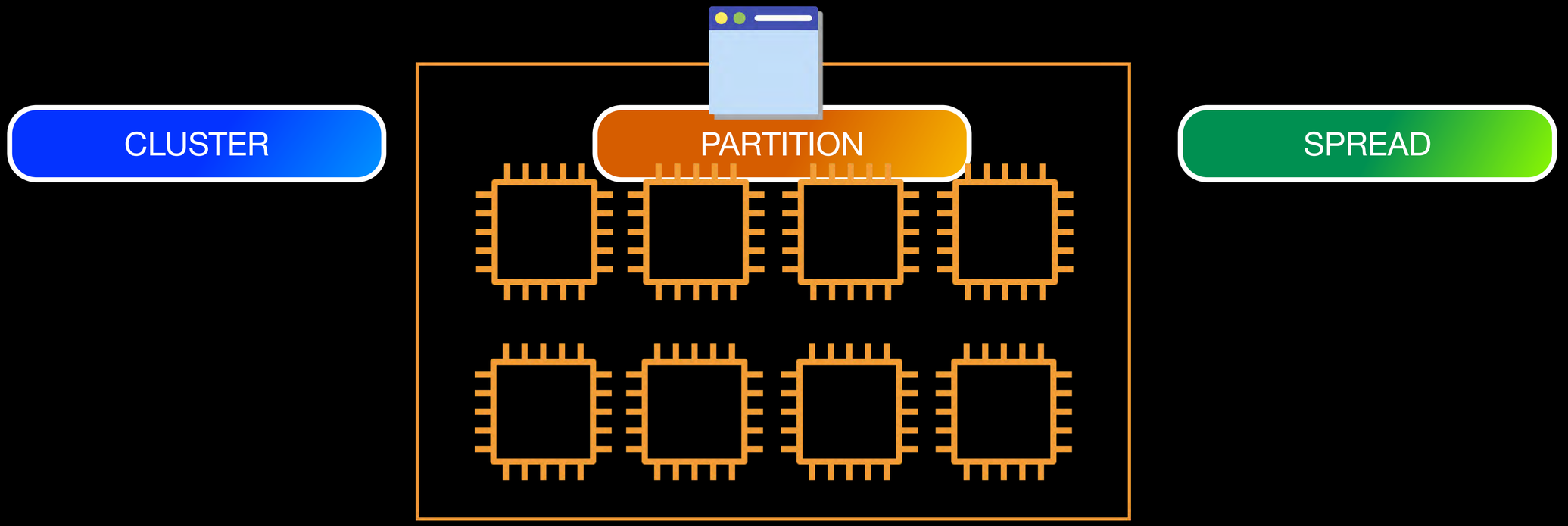
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/


US East (Ohio)
us-east-2
Amazon EC2 Service
Franklin
Gahanna
Upper Arlington
Bexley
Whitehall
Columbus
Columbus
Lincoln Village
Availability Zone 3
Grove City
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Placement Groups

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

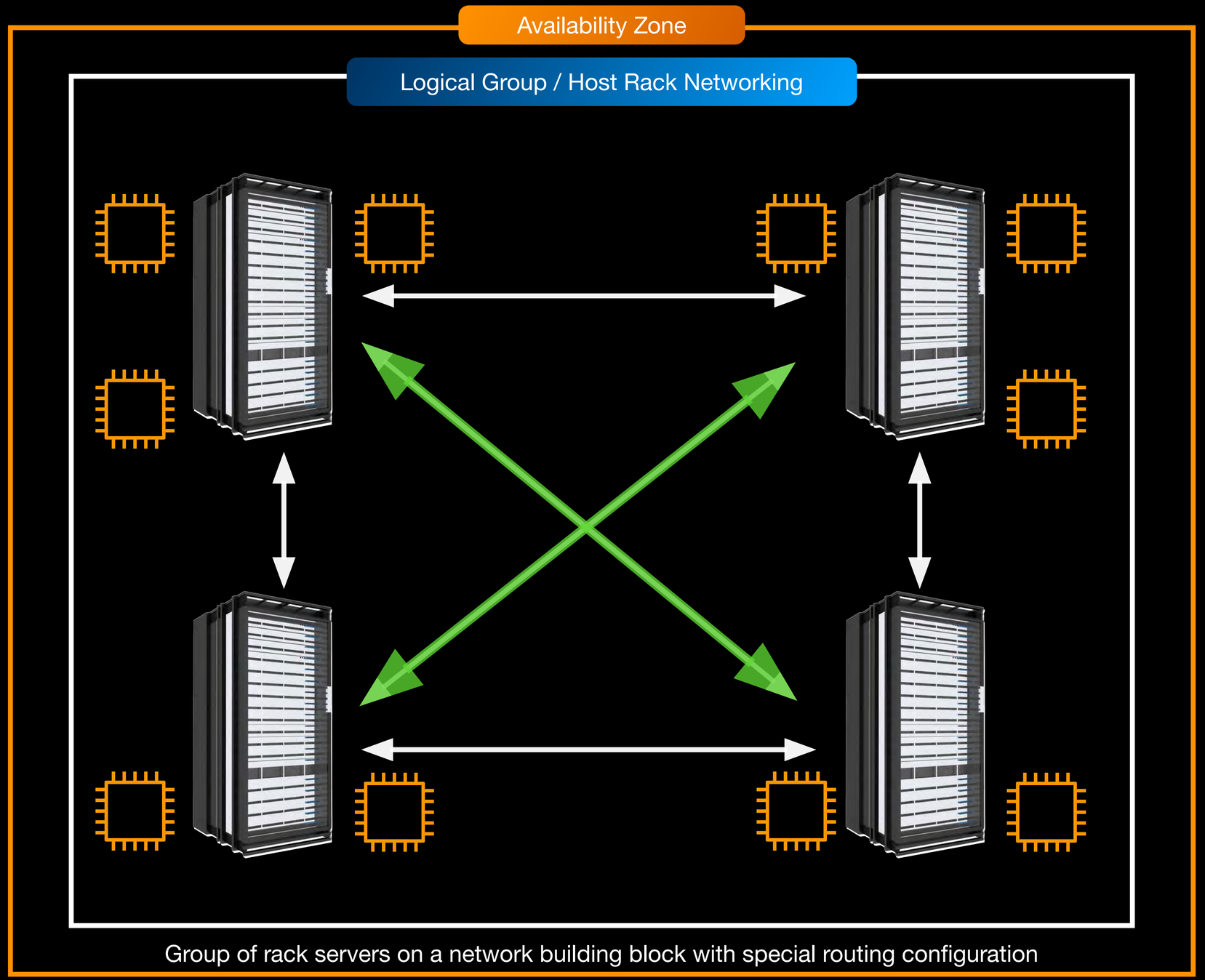
Placement Groups



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

CLUSTER

Provide low-latency network performance and high network throughput

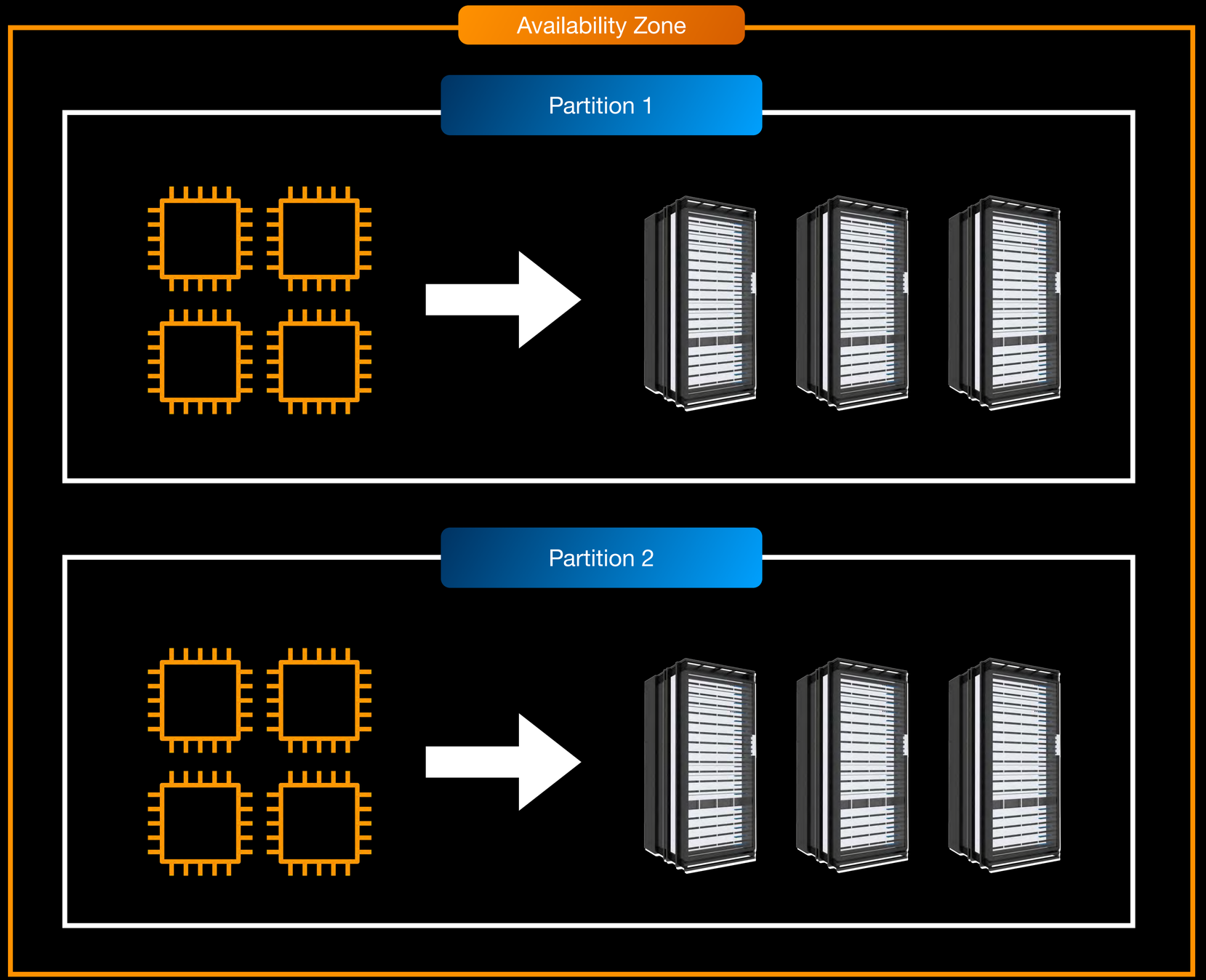


Group of rack servers on a network building block with special routing configuration

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

PARTITION

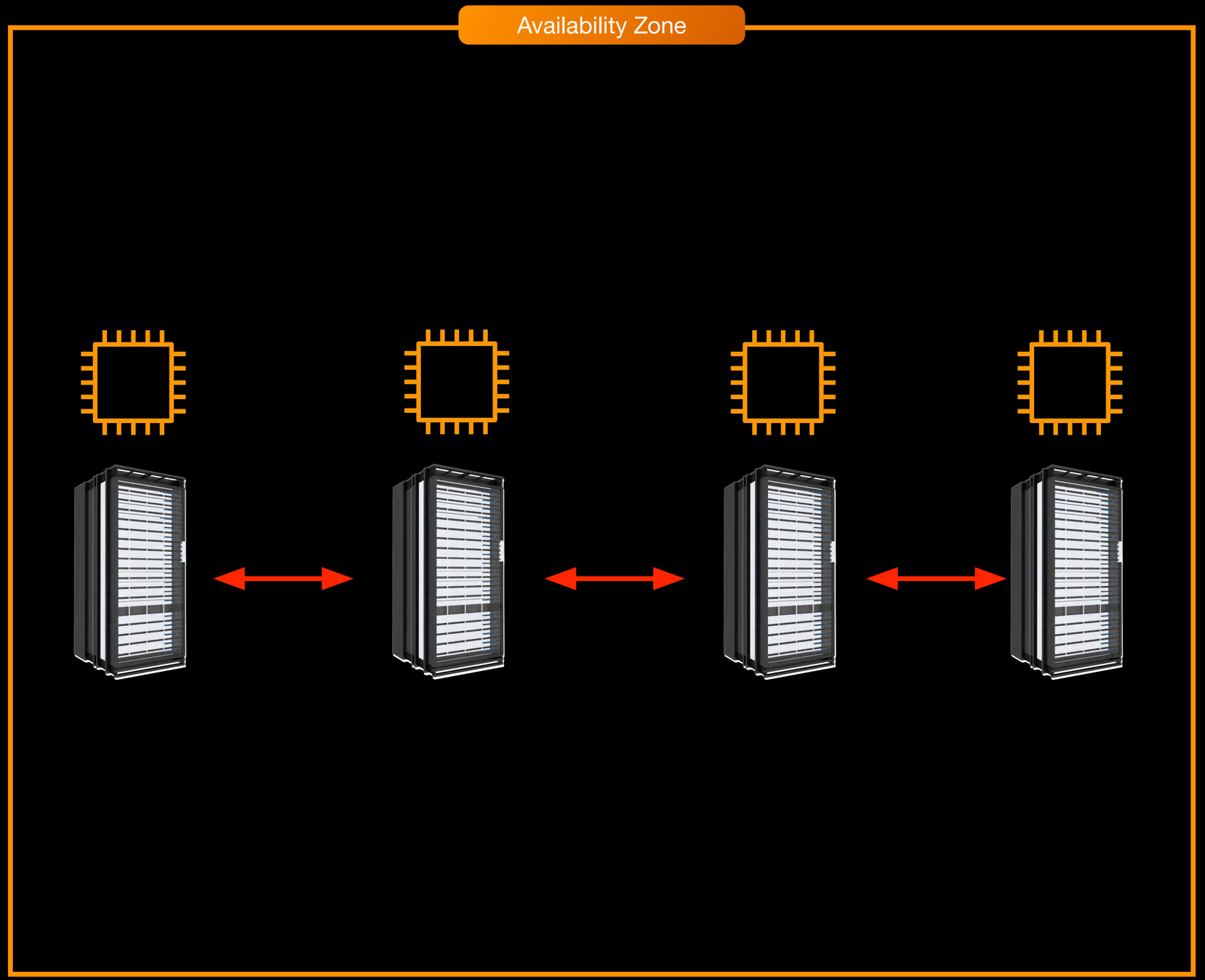
Commonly used on large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

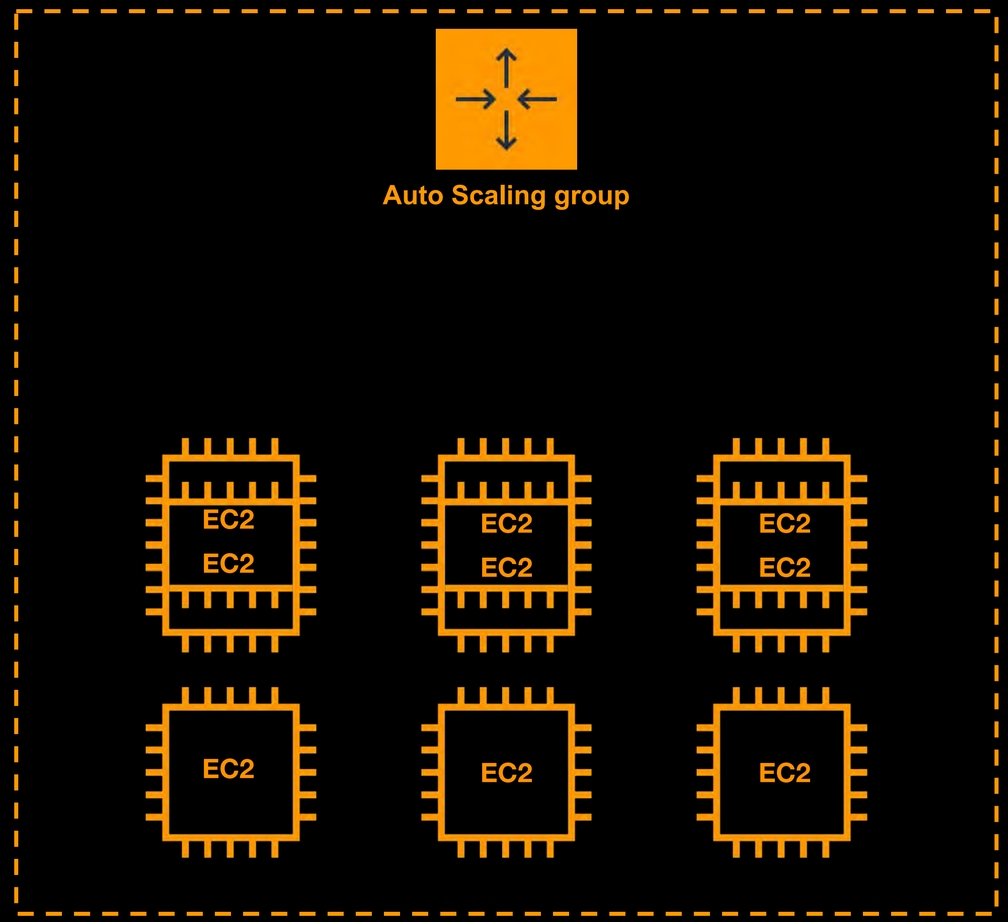
SPREAD

Reduces correlated failures and improves availability

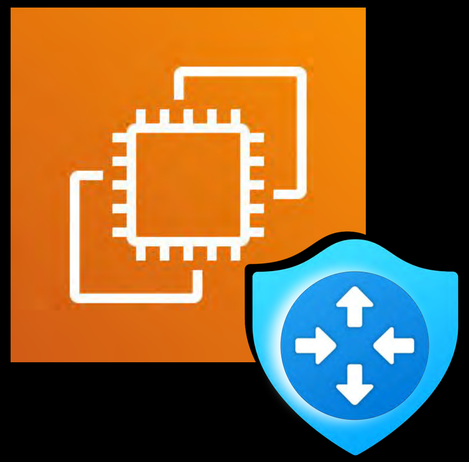


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Placement Group



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2 Network Security

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

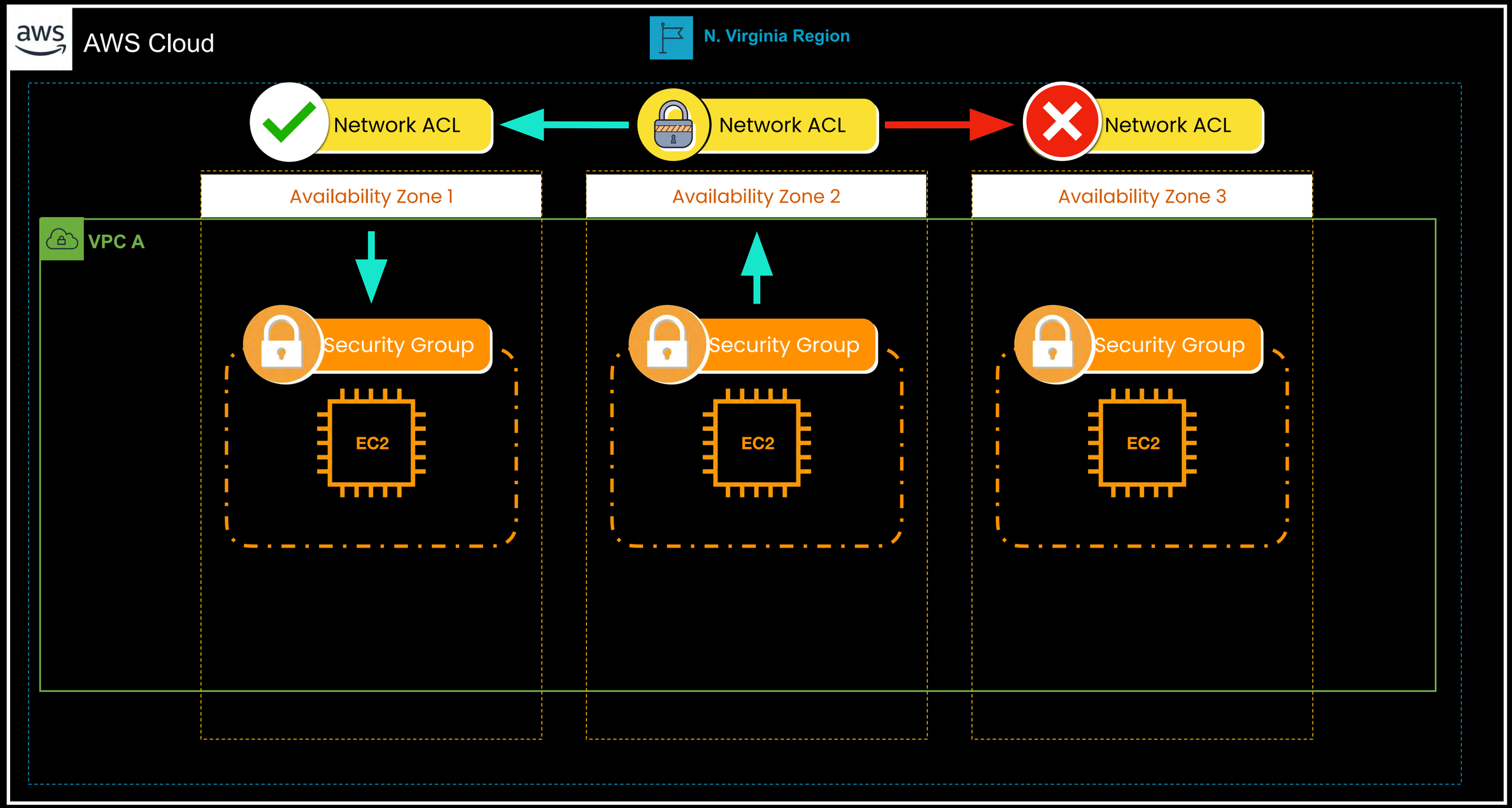


Security Groups



Network Access Control List
(Network ACL)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Cloud

N. Virginia Region

VPC A

Default Network ACL

- Already exists by default
- Can be modified
- Allows all inbound and outbound traffic by default

Custom Network ACL

- You manually have to create
- Can be modified
- Denies all inbound and outbound traffic by default

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

State

You can:

- Allow Traffic
- Deny Traffic





Inbound Rules

TYPES



Outbound Rules

Rule #	Type	Protocol	Port range	Source	Allow/Deny
10	HTTP	TCP	80	172.31.1.2/32	DENY
20	HTTPS	TCP	443	192.0.2.0/24	DENY
30	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
40	All IPv6 traffic	All	All	::/0	ALLOW

- An address prefix of **/32** denotes a single IP address
- The /24 denotes the CIDR block which contains **256** different IP addresses

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Network ACL



Outbound Rules

Ephemeral Ports

- Short-lived port numbers
- The range varies depending on the Operating System

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





Inbound Rules

Type	Protocol	Port range
HTTP	TCP	80



Outbound Rules



- 32768 – 61000



- 49152 – 65535
- 1024 – 65535

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





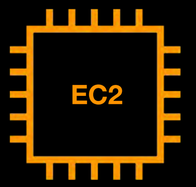
Inbound Rules



Outbound Rules







NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Security Groups

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Security Groups

- A **virtual firewall** that controls the incoming and outgoing traffic of one or more EC2 instances
- **1 EC2 instance** can have **one or more security groups**
- Cannot have an explicit DENY Rule (unlike Network ACL)
- Aside from EC2 Instances, it **can also be attached to Amazon RDS, Amazon ElastiCache and other AWS resources**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Security Groups



Inbound Rules

- Allows incoming traffic
- Can't explicitly DENY traffic
- Not affected by Outbound Rules



Outbound Rules

- Allows outgoing traffic
- Controls traffic originated from the EC2 instance itself
- Does not affect the outgoing response traffic
- Examples:
  - EC2-initiated API call
  - Scheduled OS Patches

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

7 Open Systems Interconnection (OSI) Model Layers



TCP UDP

	Protocol	Port range	Description
	TCP	80	Allow inbound HTTP access from all IPv4 addresses
	TCP	80	Allow inbound HTTP access from all IPv6 addresses
	T	443	Allow inbound HTTPS access from all IPv4 addresses
	T	443	Allow inbound HTTPS access from all IPv6 addresses
	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the internet gateway)
	TCP	3389	Allow inbound RDP access to Windows instances from IPv4 IP addresses in your network (over the internet gateway)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

7 Open Systems Interconnection (OSI) Model Layers



HTTP : 80

HTTPS : 443

MSSQL : 1433

MySQL : 3306

RDP : 3389

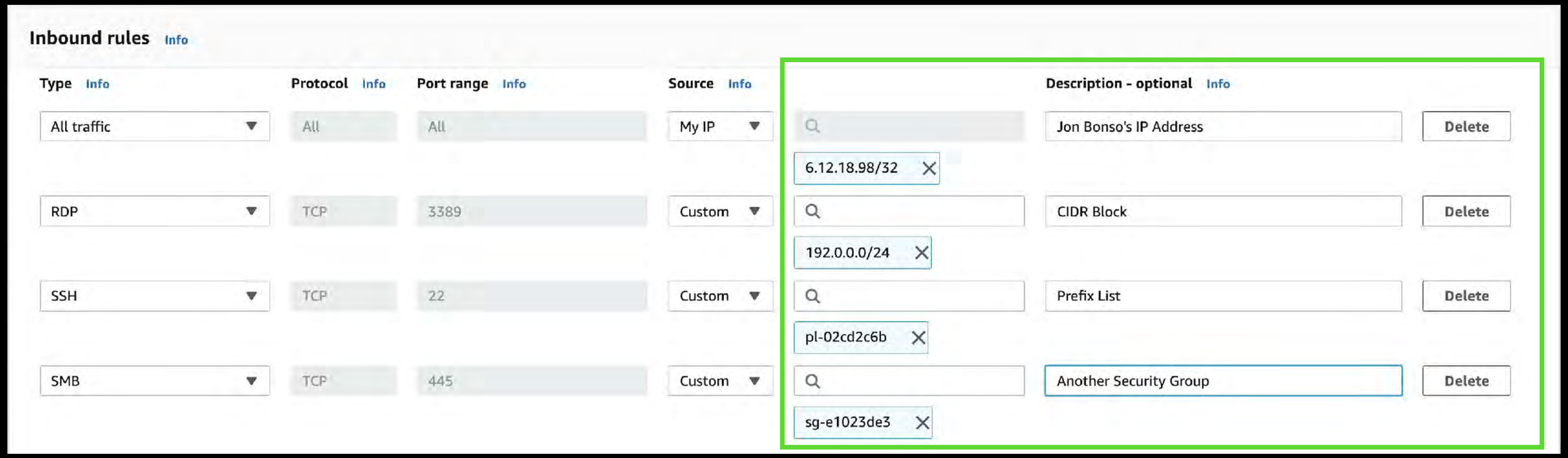
SSH : 22

SMB : 445

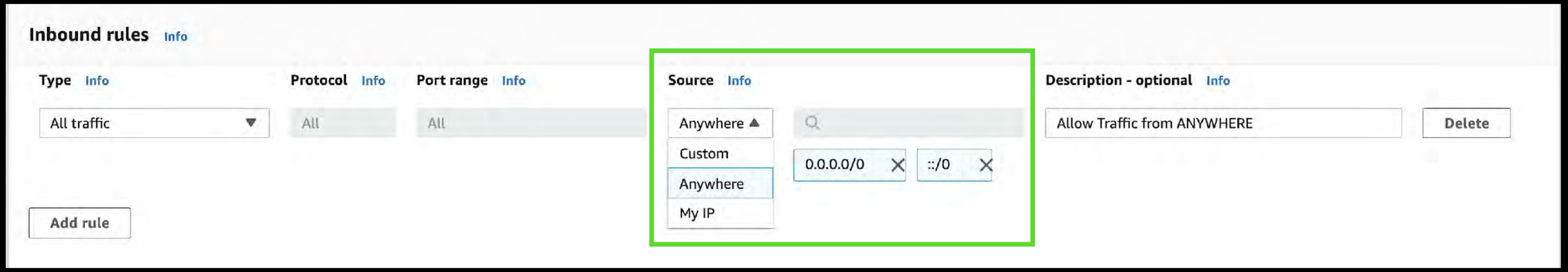
TCP

ICMP - `Ping`

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

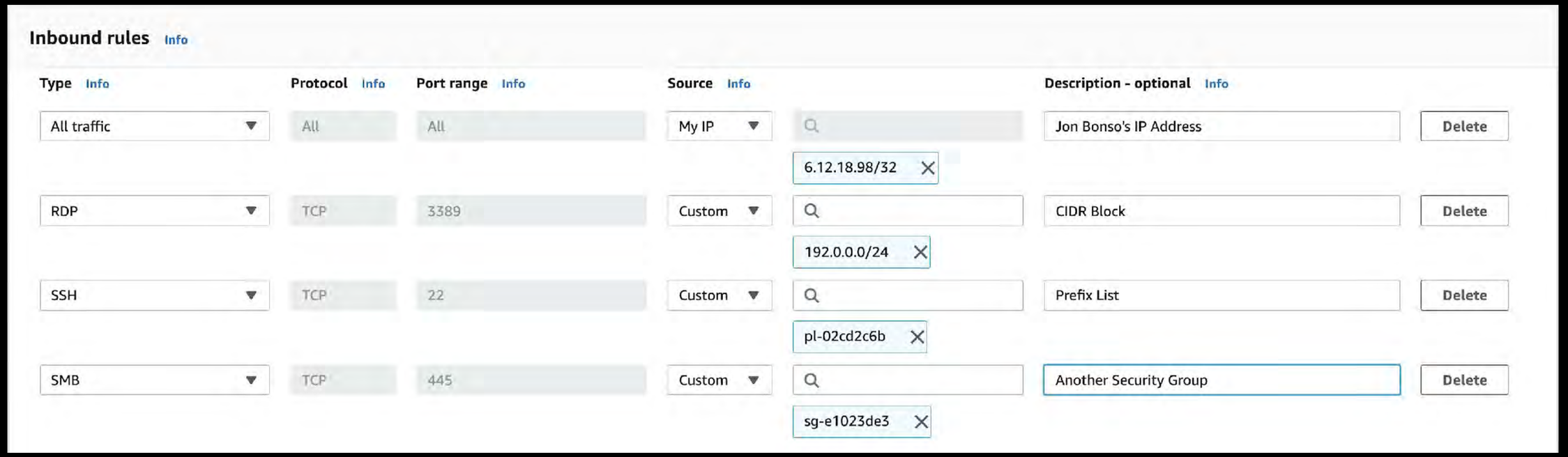


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Whitelisting

You can only

- Allow Traffic



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Default Security Group

- Already exists on your default VPC
- Has one inbound rule and one outbound rule by default
- Will be attached to your EC2 instance if you didn't specify a particular security group
- Automatically allows incoming traffic from any resource that also uses the default security group
- Allows all outgoing traffic that originated from the instance itself



Custom Security Group

- You manually have to create
- Has a default outbound rule that allows all traffic
- Doesn't have a default inbound rule
- Denies all inbound and outbound traffic by default

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

You can only

- Allow Traffic



Security Groups

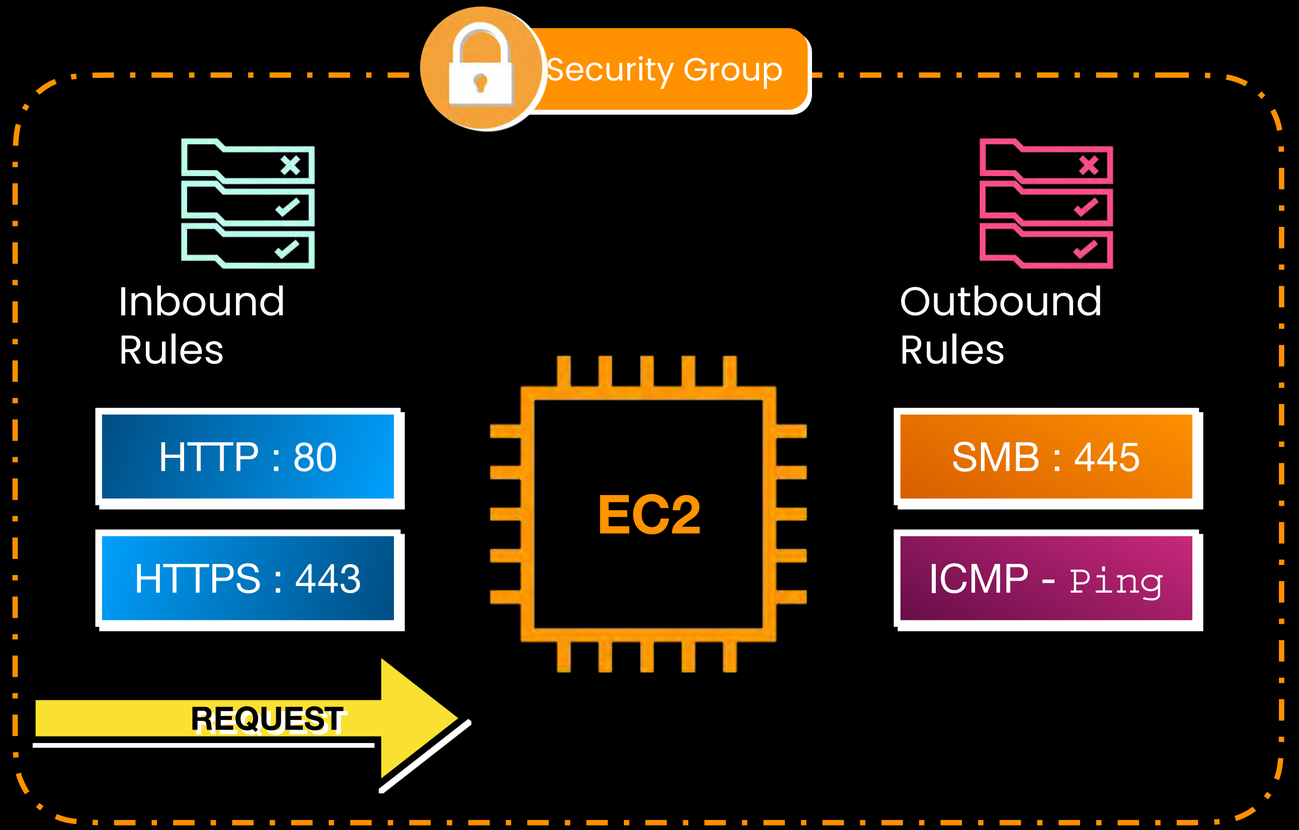
```
root@ip-172-31-3-100:~# iptables -nL INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  77.126.68.20         0.0.0.0/0
2    DROP       all  --  0.0.0.0/0            0.0.0.0/0
root@ip-172-31-3-100:~#
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

STATEFUL



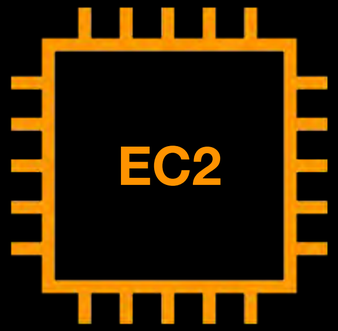
Security Groups



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Security Groups



Amazon EC2



Amazon RDS



Amazon Aurora



Amazon ElastiCache

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Security Groups

+



Network Access Control List
(Network ACL)



AWS Web Application Firewall (AWS WAF)

- You can’t apply a security group or network ACL to your Amazon S3 buckets
- Both of these features do not provide enough protection against Cross-Site Scripting or SQL Injection attacks
- These two are also inefficient in geographic match conditions or blocking certain countries

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

VPC Flow Logs



Security Groups

+



Network Access Control List
(Network ACL)

Selected resources Info

Name	Resource ID	State
Tutorials Dojo Manila VPC	vpc-4ba22d36	Available

Flow log settings

Name - *optional*

tutorialsdojo-flow-logs

Filter
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

- (•) Accept
- ( ) Reject
- ( ) All

Maximum aggregation interval Info
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

- (•) 10 minutes
- ( ) 1 minute

Destination
The destination to which to publish the flow log data.

- (•) Send to CloudWatch Logs
- ( ) Send to an Amazon S3 bucket

Destination log group Info
The name of the Amazon CloudWatch log group to which the flow log is published. A new log stream is created for each monitored network interface.

IAM role Info
The IAM role that has permission to publish to the Amazon CloudWatch log group.

The IAM role must have permission to publish to the CloudWatch log group. Set up permissions

Log record format
Specify the fields to include in the flow log record.

- (•) AWS default format
- ( ) Custom format

Format preview

```
${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}
```

Copy

NOT FOR DISTRIBUTION. © Tutorials Dojo Manila Software Solutions Corp.



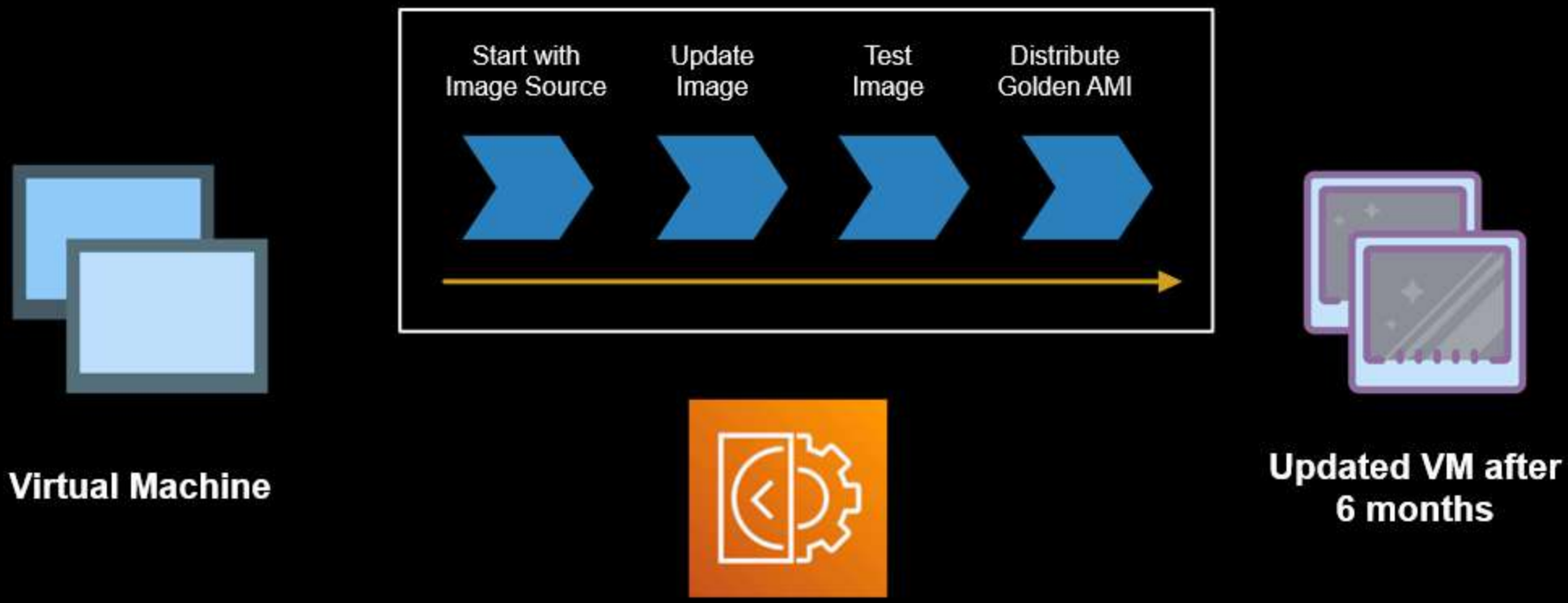
EC2 Image Builder

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

At the end of the video, you will be able to:

- Understand the value of using EC2 Image Builder
- Familiarize which AWS services integrate with EC2 Image Builder

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



EC2 Image Builder

The **EC2 Image Builder** allows you to:

- Create **image pipelines**
- Customize **recipes** with **OS and components** you need
- Perform **tests on your images**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

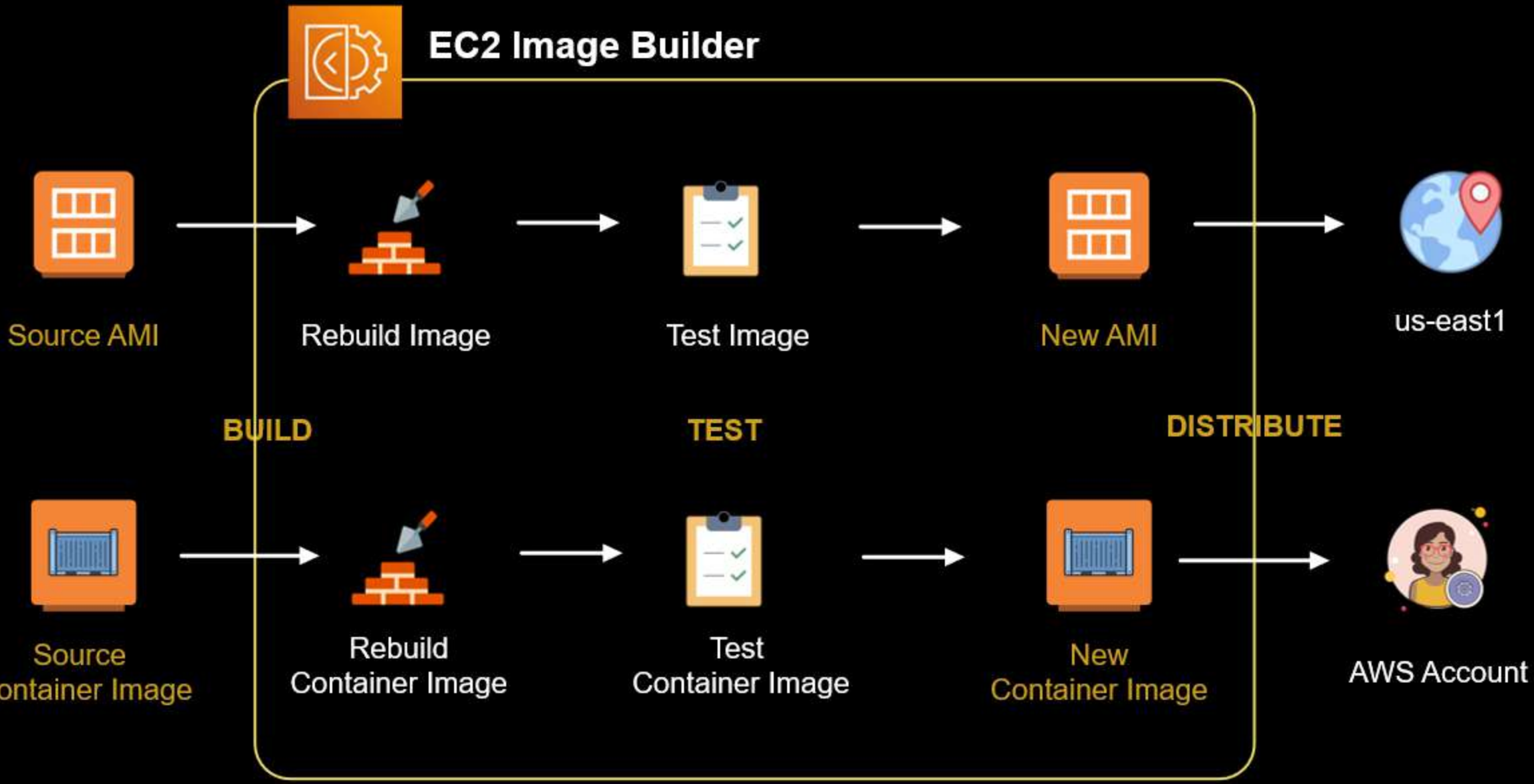


EC2 Image Builder

The **EC2 Image Builder** provides tests like:

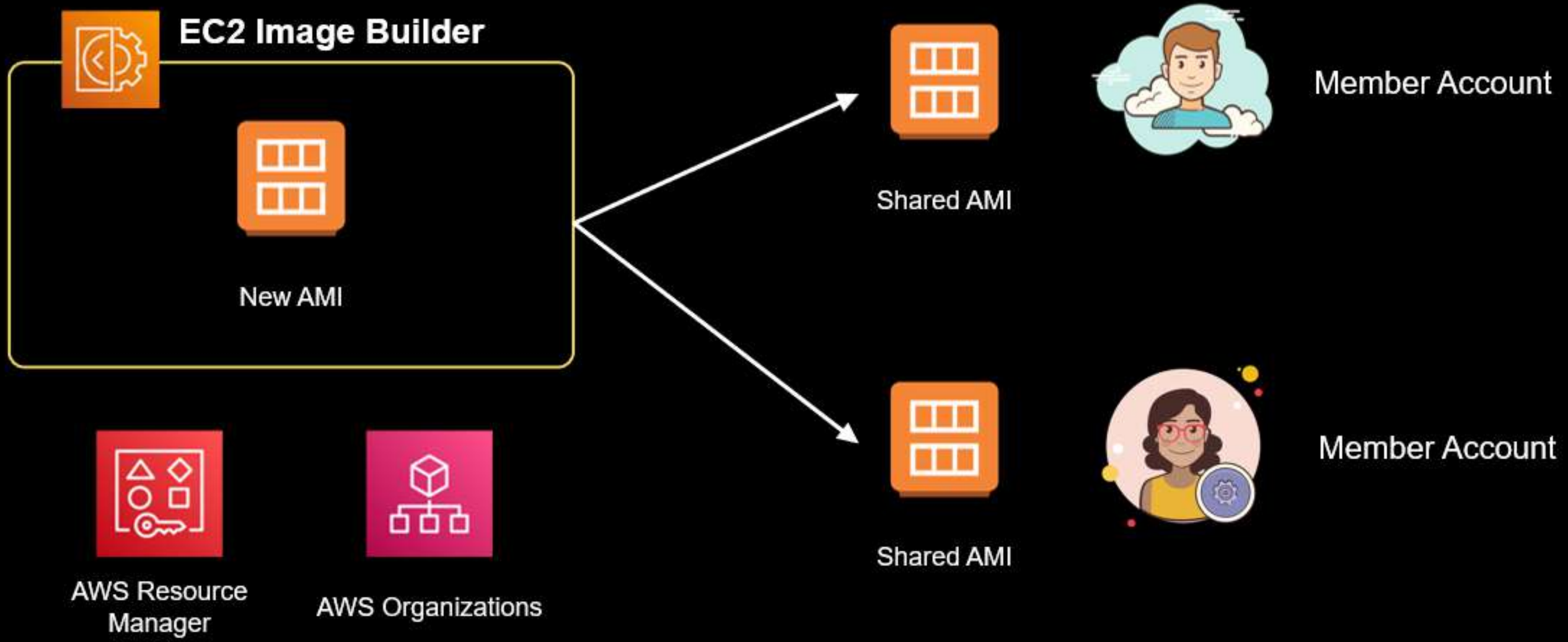
- if **images boot**
- if required **drivers are installed**
- if images are **hardened to CIS standards**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

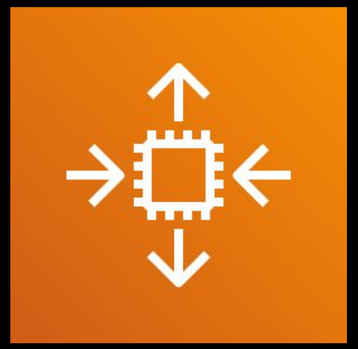


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sharing of images in EC2 Image Builder



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2 Auto Scaling Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Number of requests: 1

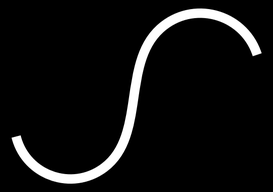
Public subnet

Auto Scaling group

EC2 EC2 EC2 EC2 EC2 EC2

EC2 EC2 EC2 EC2 EC2 EC2

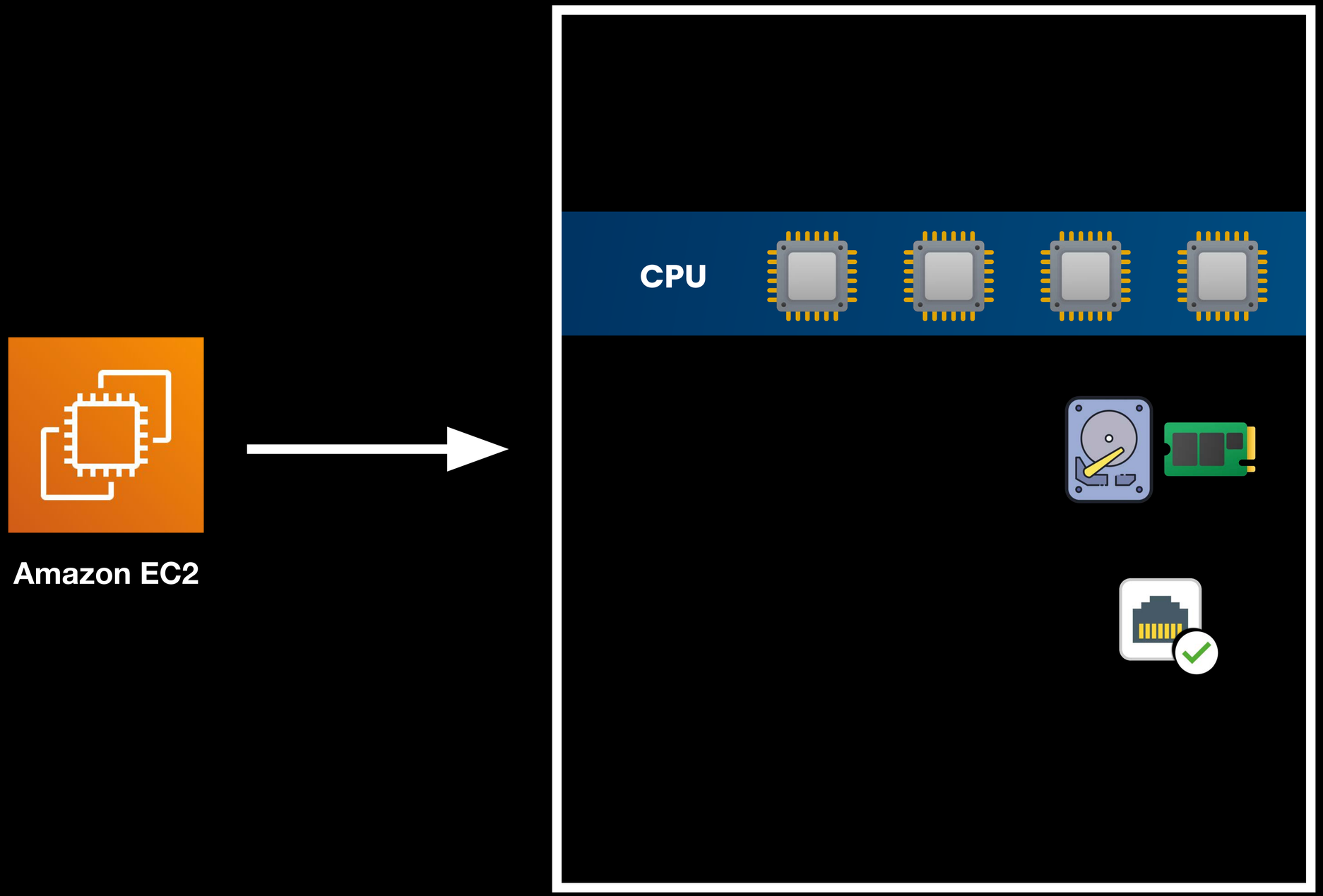
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



ELASTICITY

- The ability to **dynamically acquire or release resources** when you need them
- Can be easily done in the cloud since it has hundreds of thousands of servers
- **Improves the performance of your application** when it is experiencing a surge of requests
- **Avoids over-provisioning** of your resources
- **Lowers down your operating costs** significantly by eliminating idle resources

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



On-premises data center



RIGID and NOT FLEXIBLE

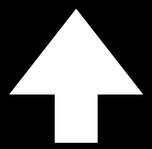
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SCALING TYPES

VERTICAL SCALING

HORIZONTAL SCALING

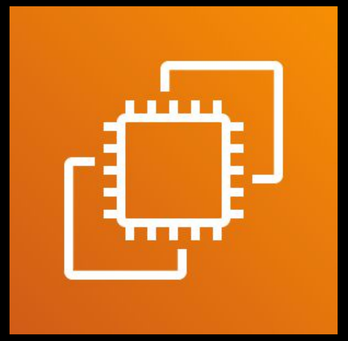
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



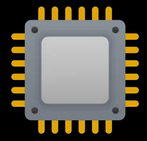
SCALE **UP**

VERTICAL SCALING

SCALE **DOWN**



Large Amazon EC2
Instance Type



30 vCPU

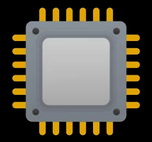


300 GB





Small Amazon EC2
Instance Type



10 vCPU



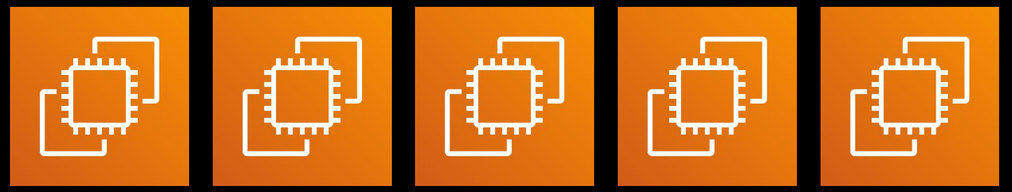
100 GB

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SCALE OUT

HORIZONTAL SCALING

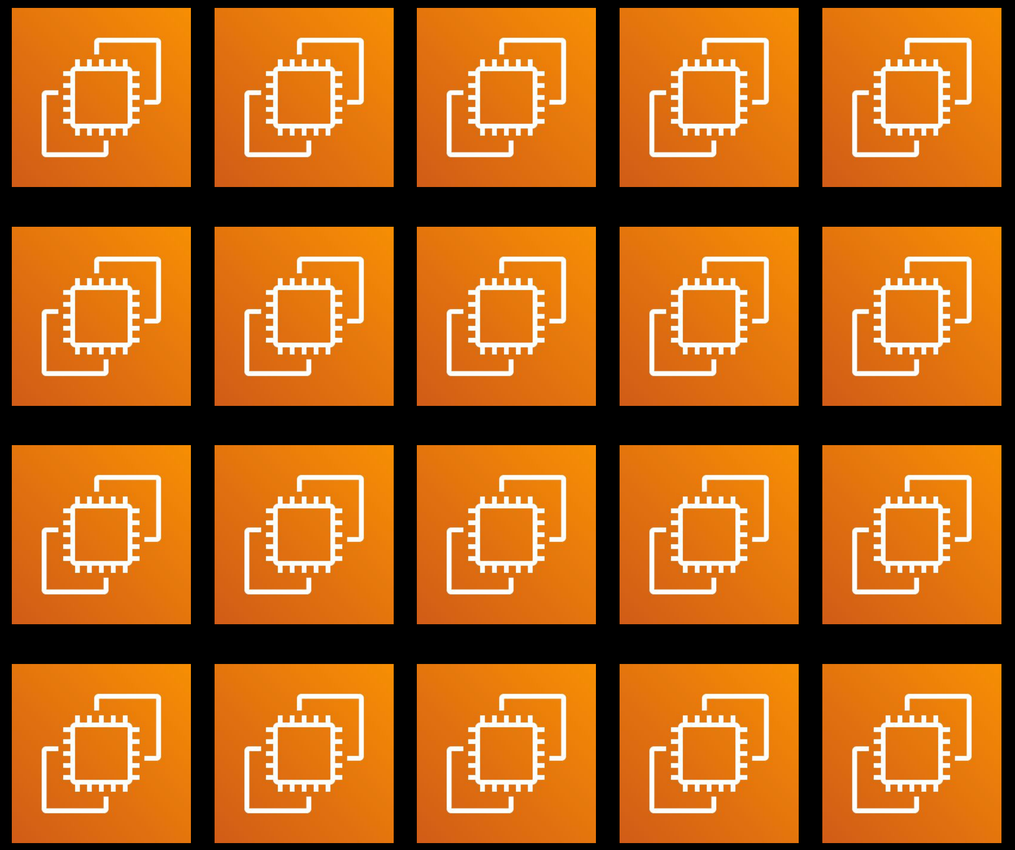
SCALE IN



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Machine Image (AMI)



SCALE OUT

HORIZONTAL SCALING

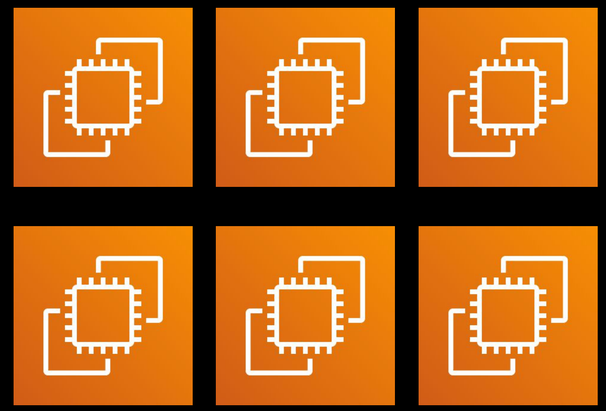
SCALE IN

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

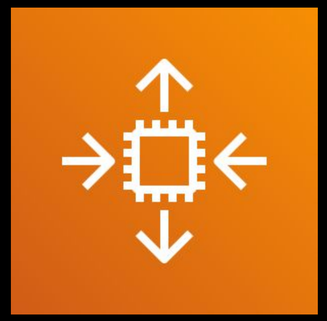
SCALE OUT

HORIZONTAL SCALING

SCALE IN



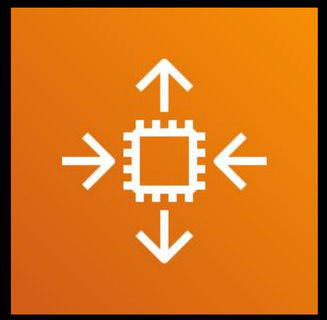
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2 Auto Scaling

HORIZONTAL SCALING

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2 Auto Scaling

AUTO SCALING GROUP

CONFIGURATION TEMPLATE

SCALING OPTION

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AUTO SCALING GROUP

- Organizes your Amazon EC2 instances into groups
- **A logical unit for scaling** and management
- Must have a setting for the minimum, maximum, and desired number of Amazon EC2 instances

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

CONFIGURATION TEMPLATE

- **Types:**
  - Launch Template
  - Launch Configuration
- Acts as a **template** for your Auto Scaling Group, containing the AMI ID, the instance type, the key pair, the security groups, block device mapping and others
- It is recommended to use a **Launch Template**, rather than a Launch Configuration, as the latter only offers limited features

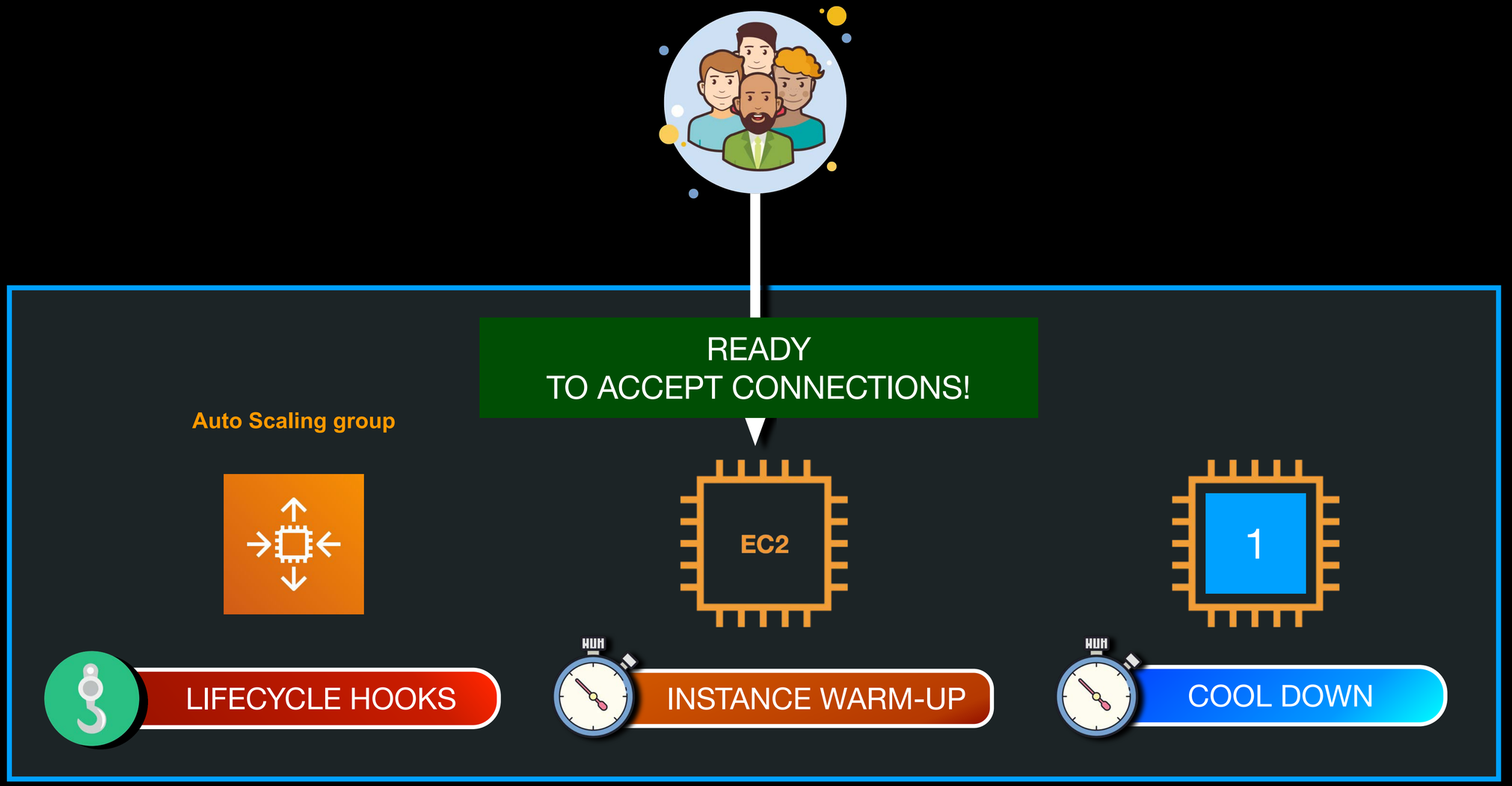
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SCALING OPTION

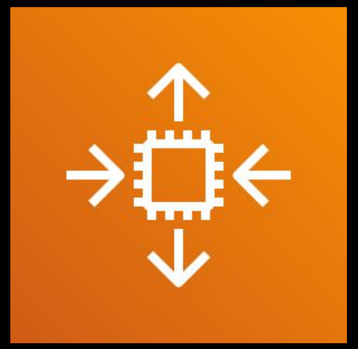
- Allows you to choose the suitable **scaling behavior** of your Auto Scaling Group.

- **Types:**
  - Dynamic
  - Predictive
  - Scheduled

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



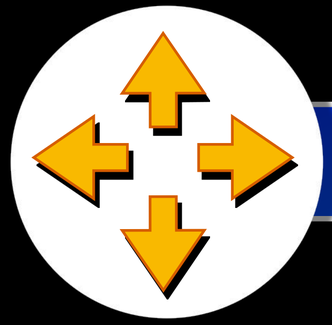
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



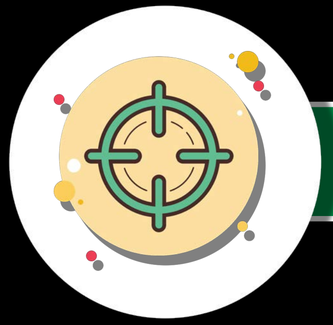
Amazon EC2 Auto Scaling Types

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AMAZON EC2 AUTO SCALING TYPES



SIMPLE SCALING



TARGET TRACKING



STEP SCALING

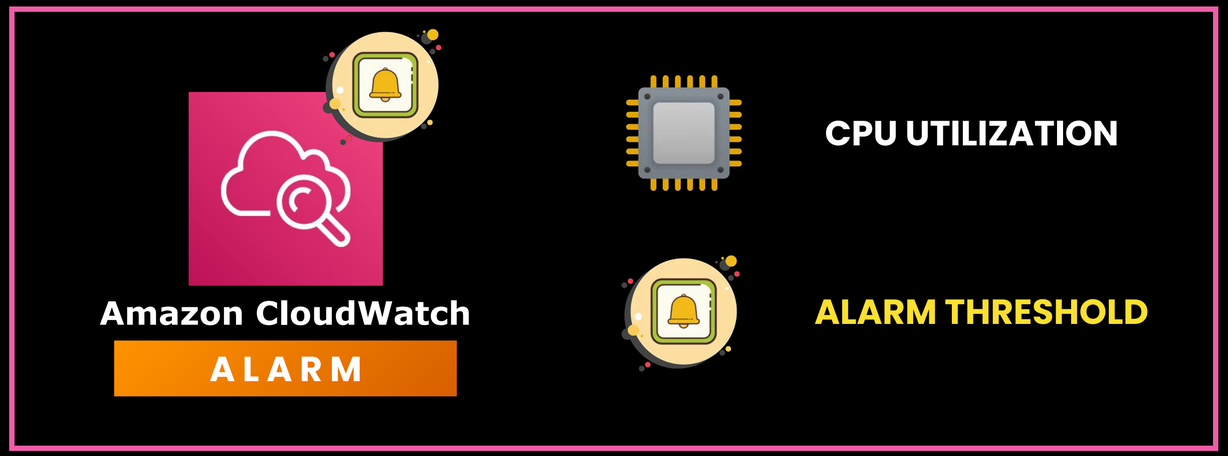


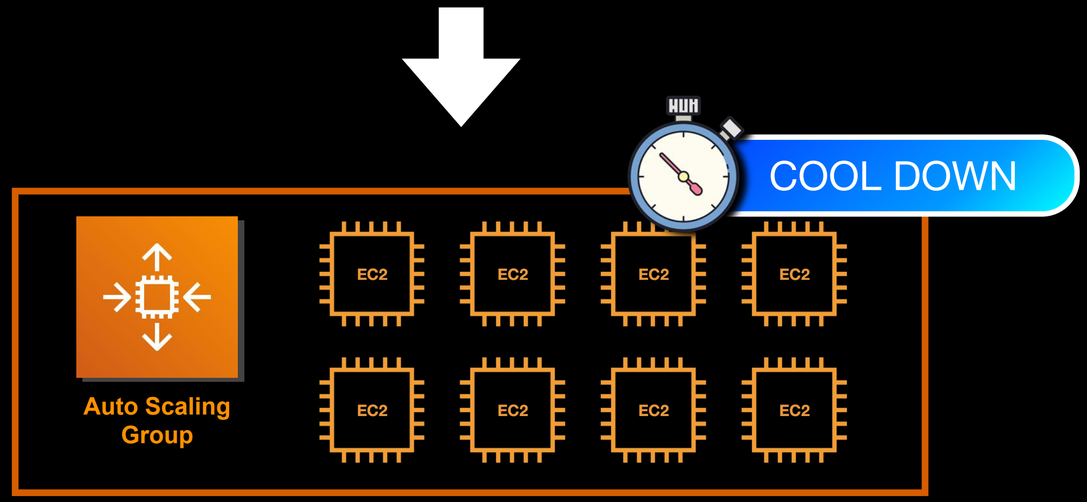
SCHEDULED SCALING

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Automatically increases or decreases the current capacity of your Auto Scaling Group based on a **single scaling adjustment**





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Automatically increases or decreases the current capacity of your Amazon EC2 Auto Scaling group **based on a set of scaling adjustments**, also known as **step adjustments**

- Also requires the use of CloudWatch alarms with specified high and low thresholds as well as a defined action that either adds or removes instances

- Also supports setting the Auto Scaling group to an **exact size or a fixed capacity unit** in the event that your CloudWatch alarm threshold was breached

- Unlike Simple Scaling policy, it **can continue to respond to additional CloudWatch alarms**, even if the current scaling activity or health check replacement is already in progress

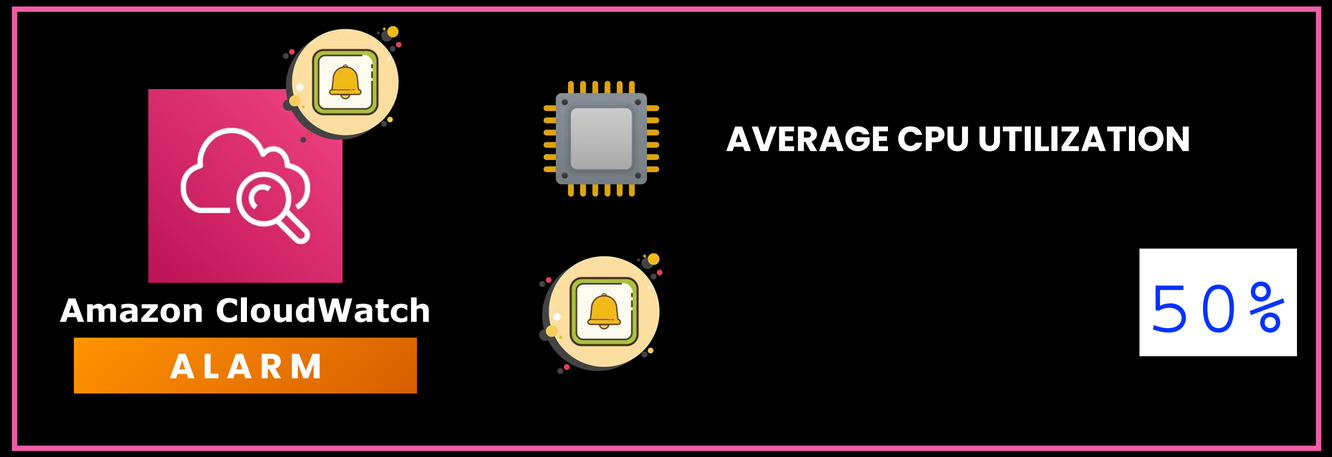
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

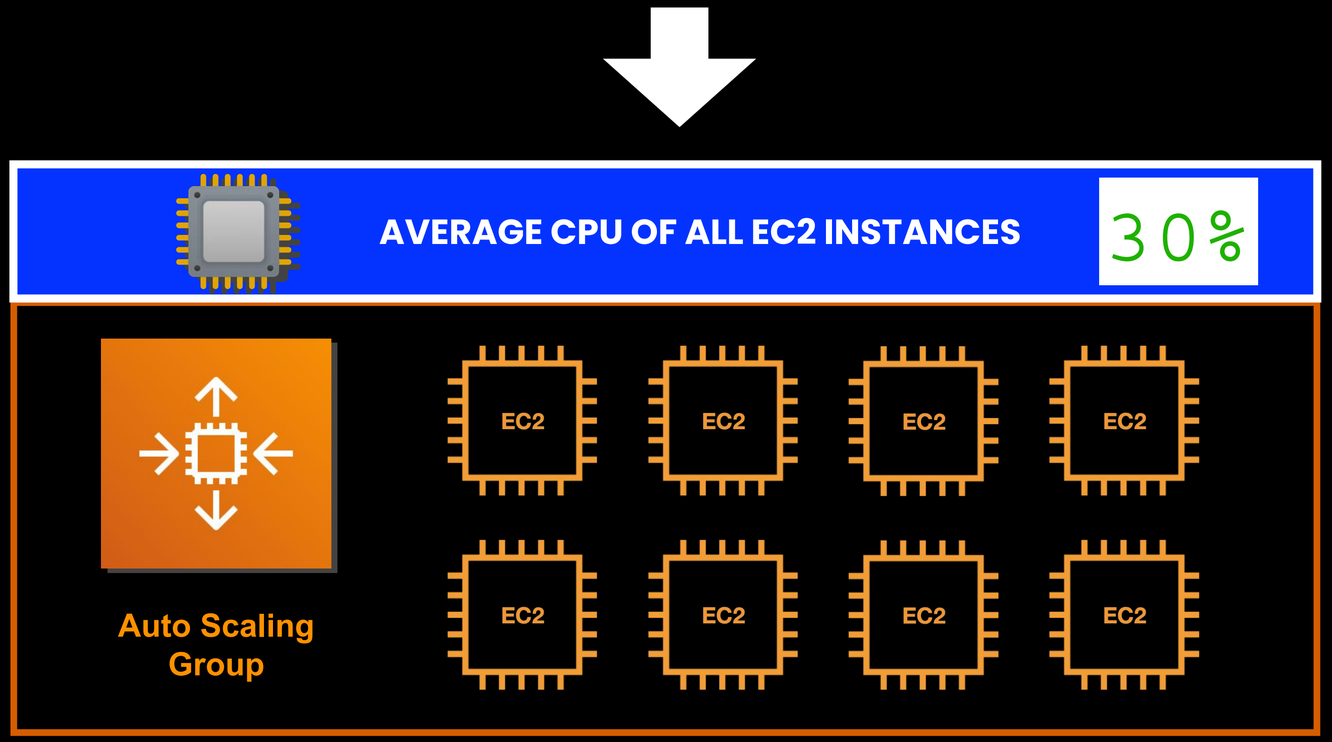


- Automatically increases or decreases the current capacity of your Auto Scaling group **based on a target value for a specific metric**
- **Maintains and adjusts the number of EC2 instances** in your Auto Scaling group based on the target that you specify

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

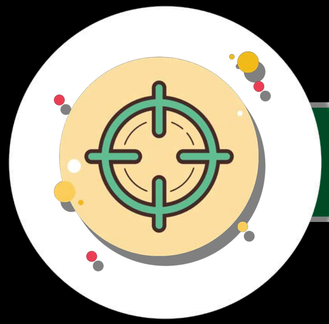






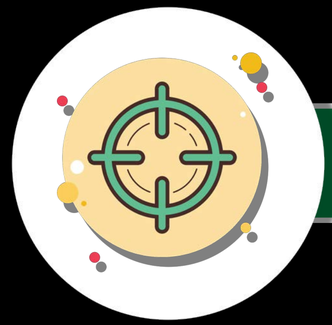
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

WORKS LIKE A THERMOSTAT!



TARGET TRACKING

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



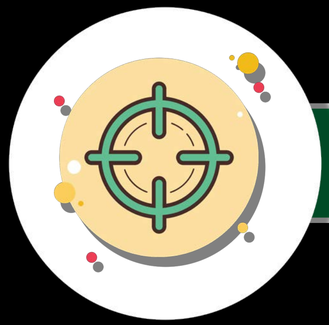
TARGET TRACKING

USE CASES

- If you've determined the **optimal performance** of your web application and you want to **maintain its desired performance across** all EC2 instances of your Auto Scaling group

- If your application works best when the combined CPU utilization of your Amazon EC2 instances is at or near a certain percentage (e.g. 40%). You can set up a target tracking policy with a metric type of "`Average CPU utilization`" and a 40% target value

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



TARGET TRACKING

USE CASES

- Tracking of a certain metric that is produced by your application. You can track the **average network in or network out** of all your instances
- You can use the **request count per target** (`ALBRequestCountPerTarget`) metric of your Application Load Balancer as the metric type for your Target Tracking policy

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Automatically increases or decreases the current capacity of your Auto Scaling group **based on a set schedule that you define**
- Allows you to set up your own scheduled scaling based on the **predictable load changes** of your application.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



SCHEDULED SCALING

USE CASES

Month-end Batch Processing Scenario



- **Performs significantly slower** when the month-end financial calculation batch executes
- Causes the CPU utilization of your Amazon EC2 instances to immediately peak to 100% on that period
- **Always happens on the first day of every month** at the stroke of midnight.

- Set a scheduled scaling policy with a **monthly schedule**
- **Scale out before the clock hits 12 midnight** on the first day of the month so there would be **more EC2 instances deployed to handle the peak load**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



SCHEDULED SCALING

USE CASES

Holidays and Public Announcements





- Provides a **consistent user experience** by scaling your Auto Scaling group a few hours before your event or specific holidays
- Scaling out your compute capacity takes time due to the **cooldown period.** It may take an hour or more to fully scale your compute capacity to match the current load. This is the reason why **you have to scale-out early!**
- Setting up a scheduled scaling activity beforehand can reduce the performance issues of your application

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



SCHEDULED SCALING

USE CASES

Slow site every morning when work day begins…





- Sluggish application performance right **when the workday begins** (e.g. 8 AM) but usually runs well by mid-morning (e.g. 10 AM) or at lunchtime
- There is a **delay in launching new instances** as opposed to the number of incoming requests
- For example, your Auto Scaling group scales up to 20 or 25 instances during work hours, but scales down to just 2 instances overnight
- In the morning, **it takes a few hours** for the scaling process to complete – extending to mid-morning or till lunchtime, since there are only 2 instances at the start of the day

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic Load Balancing
Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Incoming Elastic Load Balancing

of traffic

the distribution of traffic to underlying resources





Amazon EC2 Instances



AWS Lambda Functions



Amazon EKS Clusters



Amazon ECS Tasks



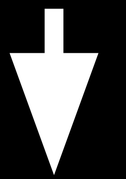
AWS Fargate Tasks



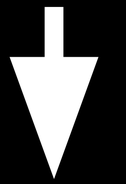
Custom IP Addresses

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/









52.44.107.223



OS Patching or
System Maintenance

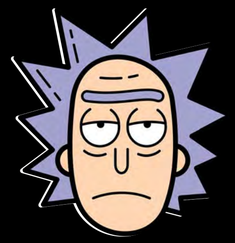




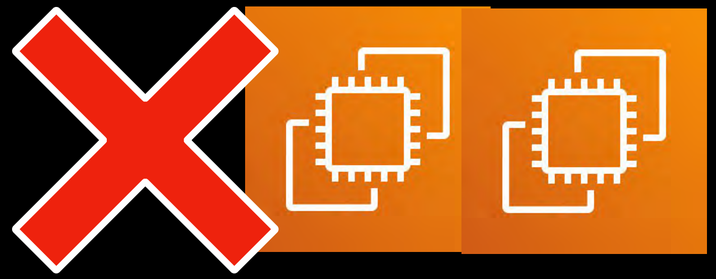
Critical Application
or System Errors



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

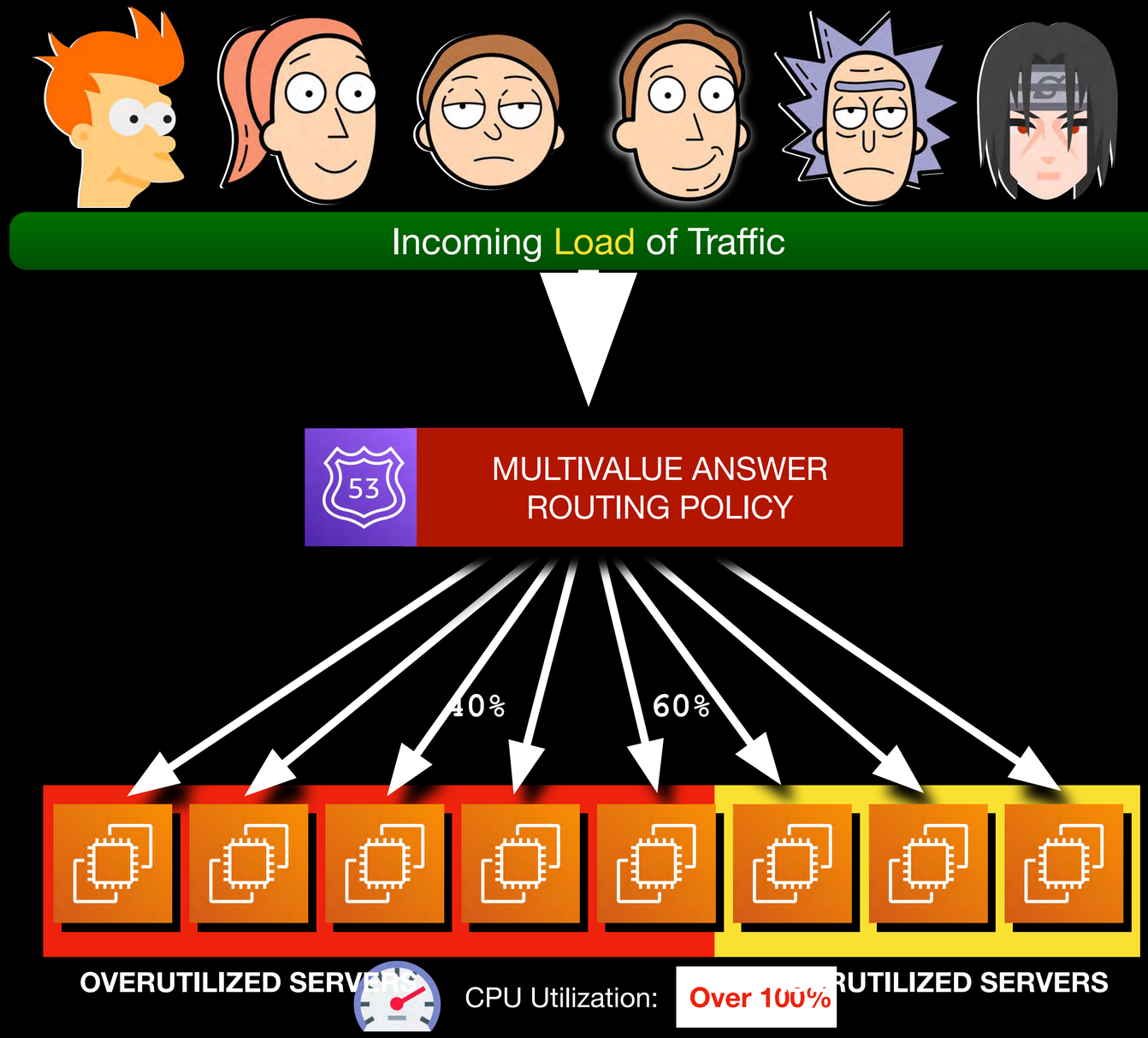


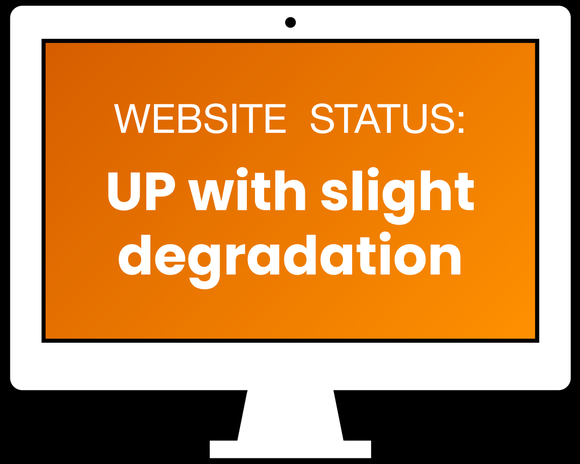






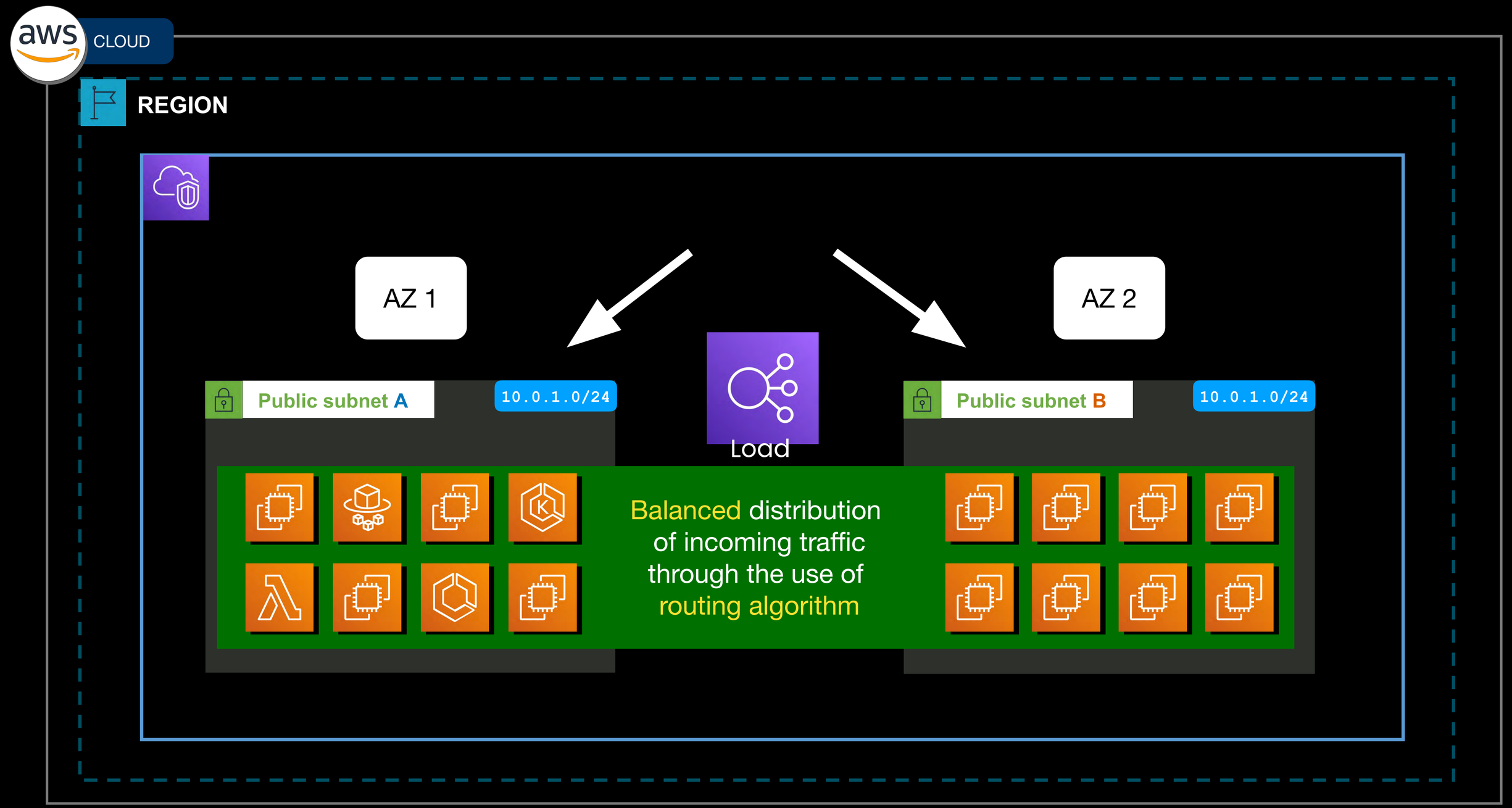
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





- The distribution of the **incoming load traffic is not balanced** across the underlying servers
- The traffic is distributed **randomly**
- **Unbalanced** - Some servers are overutilized while others are underutilized
- **No routing algorithm**
- **Lacks security features**

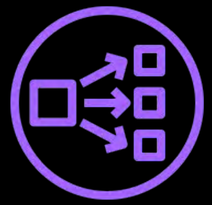
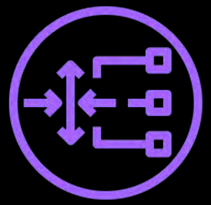
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Elastic Load Balancing TYPES

	 **Application Load Balancer (ALB)**	 **Network Load Balancer (NLB)**	 **Gateway Load Balancer (GWLB)**	 **Classic Load Balancer (CLB)**
ROUTING ALGORITHM	Round Robin Least Outstanding Requests (LOR)	Flow Hash	IP Listener Routing that leverages on GENEVE protocol	Round Robin Least Outstanding Requests (LOR)

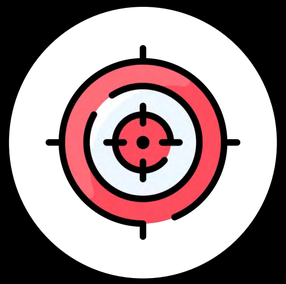
PROTOCOL LISTENERS	`HTTP / HTTPS`
	`gRPC`
		`TCP / UDP`
		`TLS`
			`IP`	`HTTP / HTTPS`
				`TCP`
				`SSL/TLS`

USE CASES	For **web apps**, microservices & containers	Handling **millions of requests per second** while maintaining **ultra-low latencies**	Running third-party **virtual appliances** in AWS	For **legacy** applications in AWS For implementing **Custom Security Policies** and **TCP passthrough configuration**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

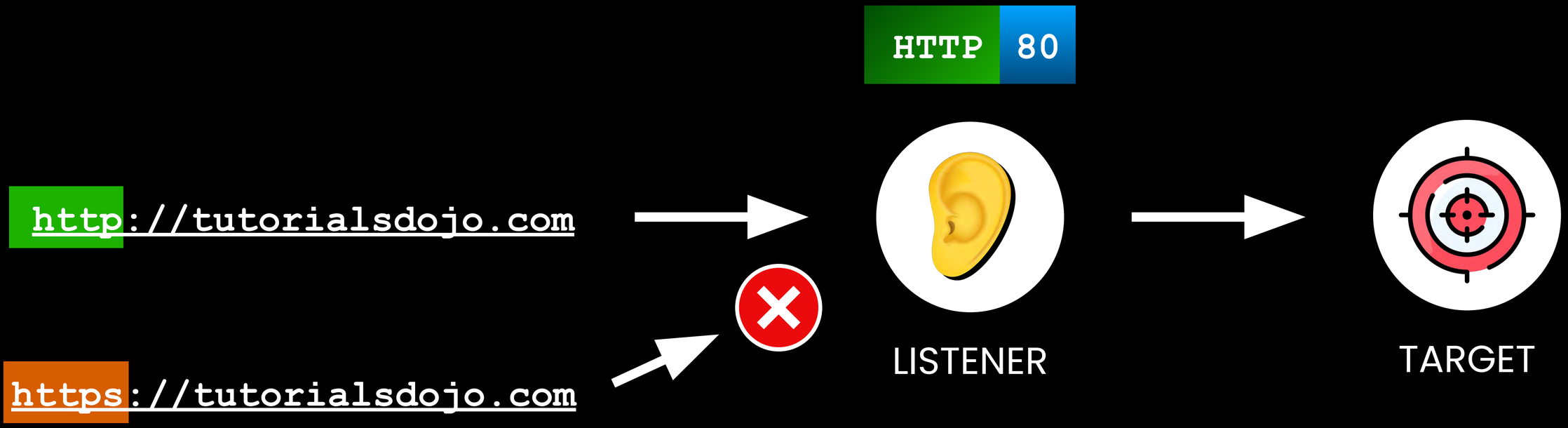


LISTENER

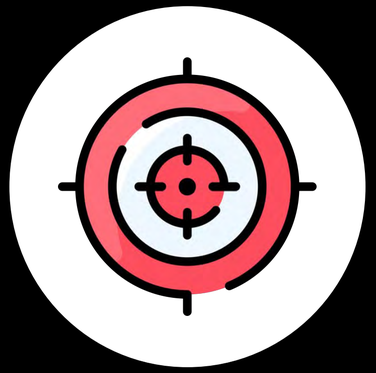


TARGET

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



TARGET



Amazon EC2 Instances



AWS Lambda Functions



Amazon EKS Clusters



Amazon ECS Tasks

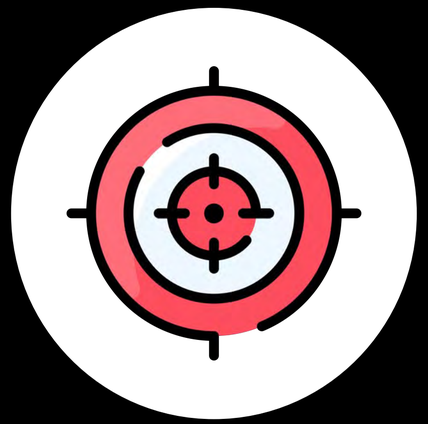


AWS Fargate Tasks



Custom IP Addresses

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



TARGET GROUP



Amazon EC2 Instances



AWS Lambda Functions



Amazon EKS Clusters



Amazon ECS Tasks

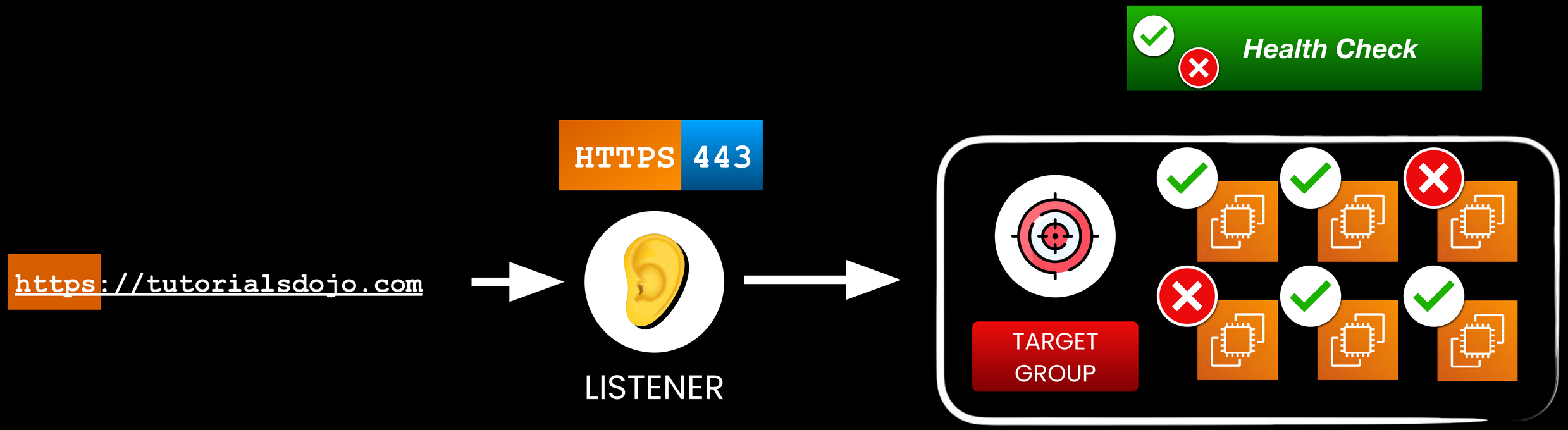


AWS Fargate Tasks

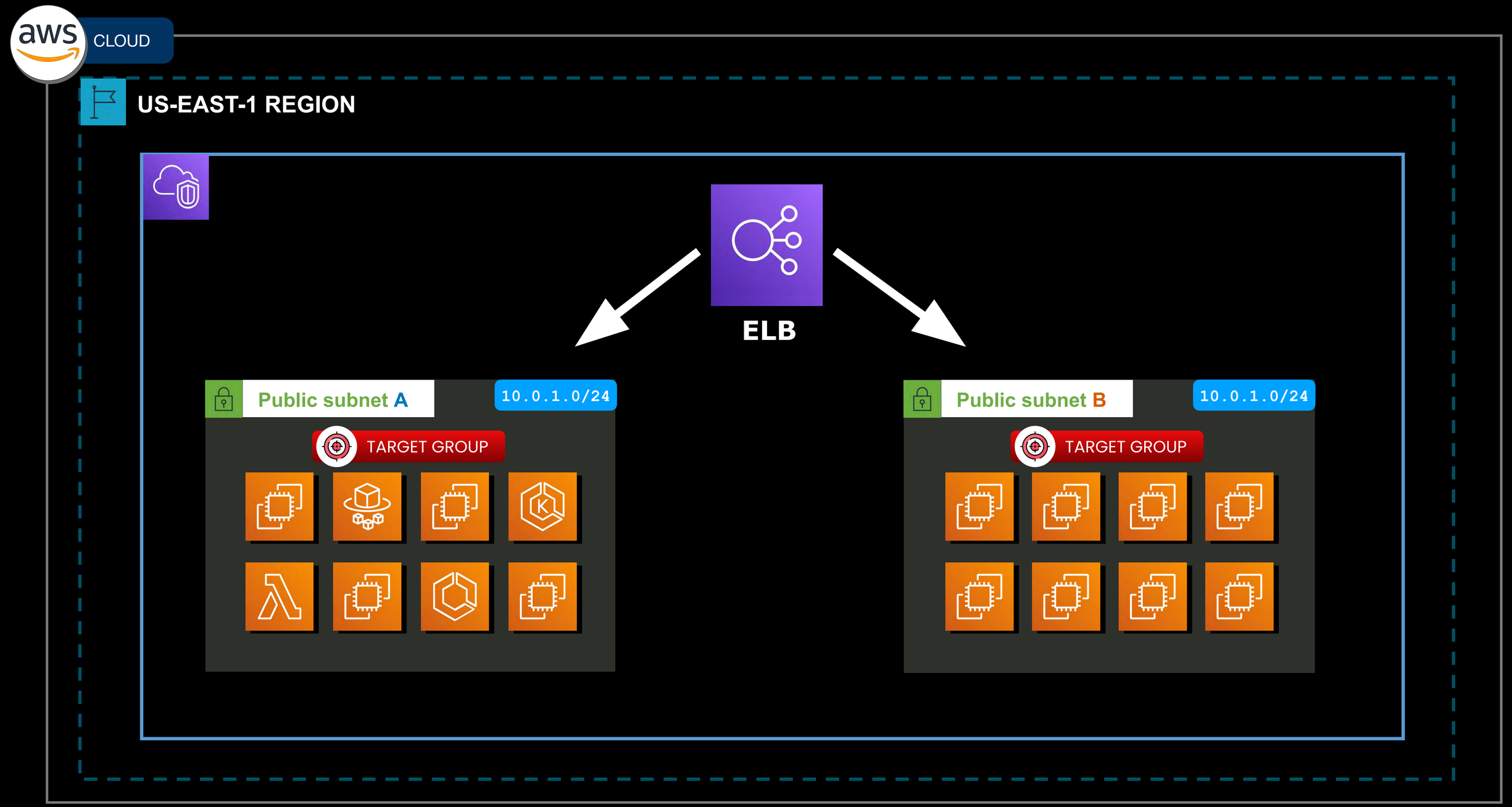


Custom IP Addresses

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

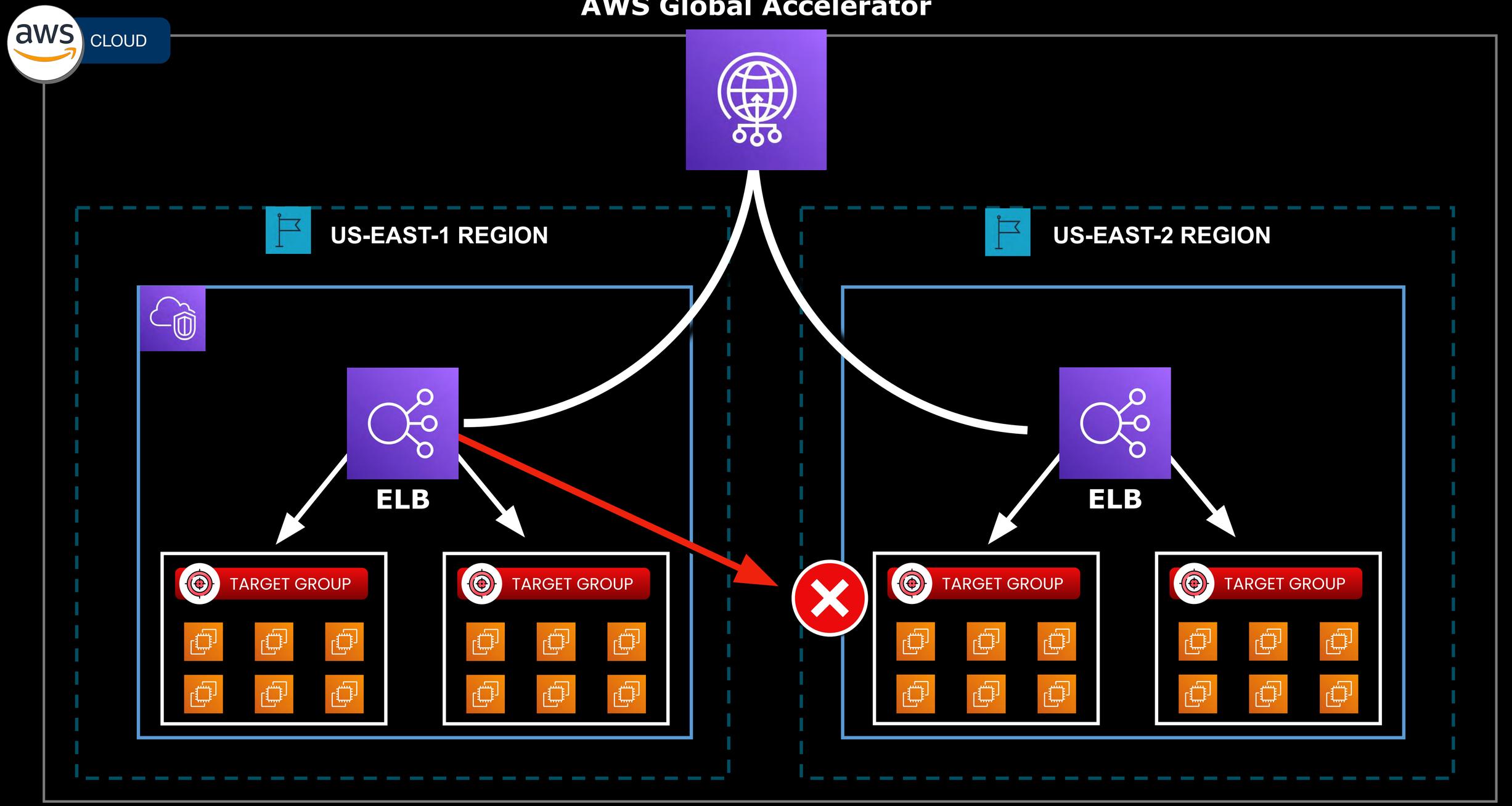


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

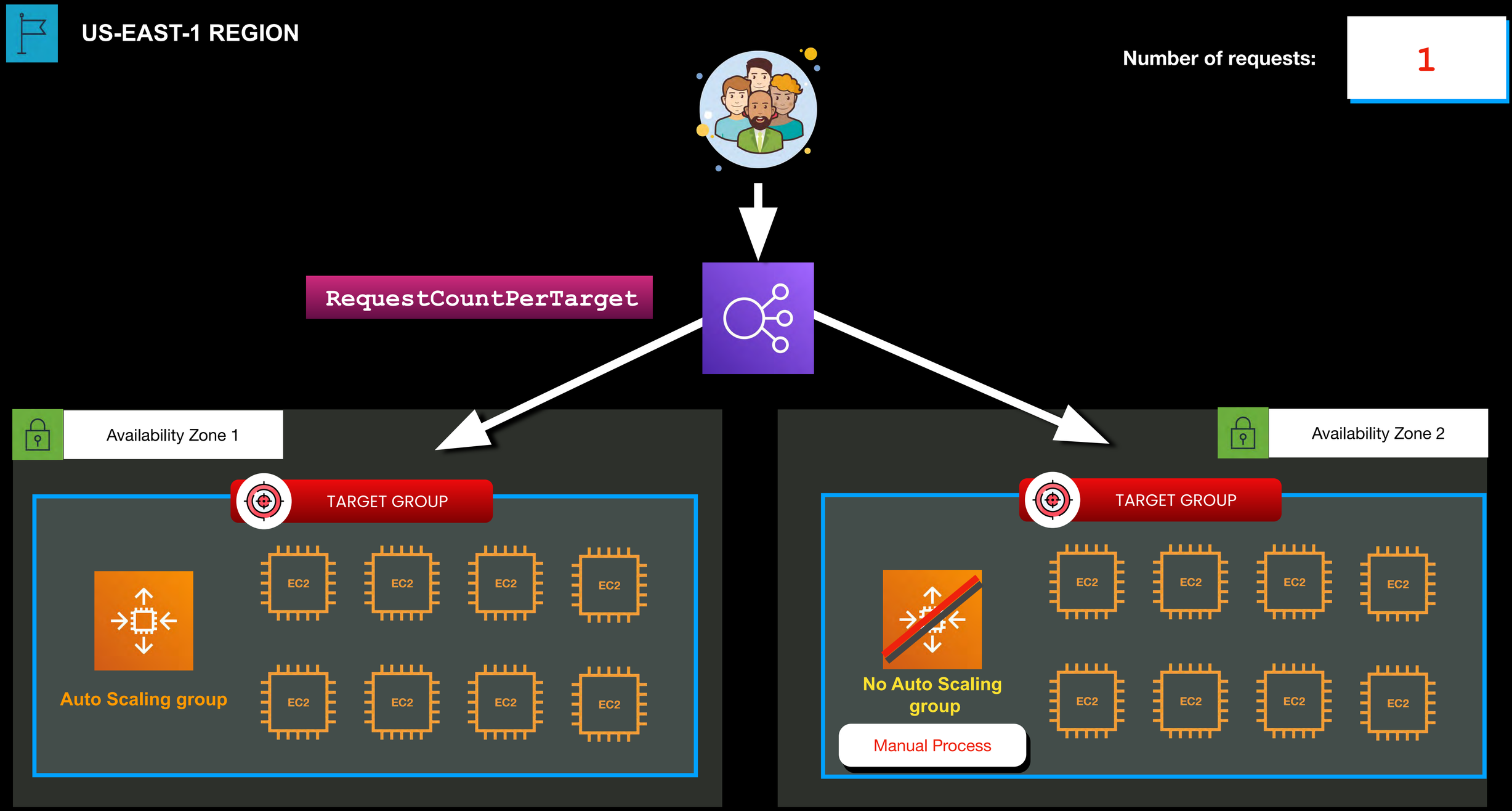


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Global Accelerator



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



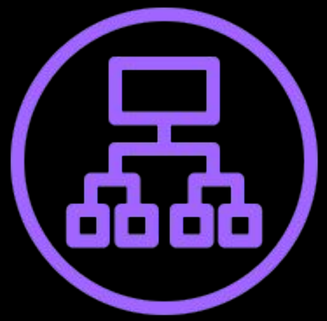
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



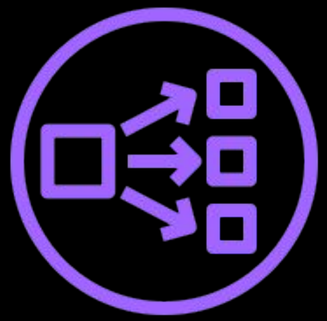
Amazon Elastic Load Balancing

T Y P E S

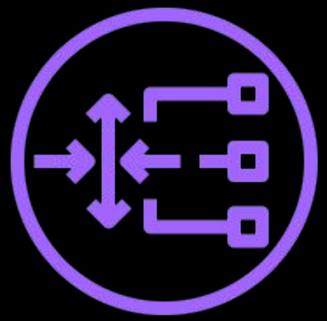
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Application Load Balancer



Network Load Balancer

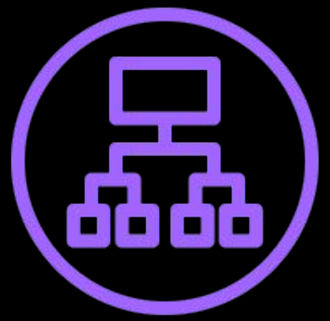


Gateway Load Balancer



Classic Load Balancer

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Application Load Balancer

- Primarily used for load balancing HTTP and HTTPS traffic
- Suitable for web applications
- Works on the Layer 7 (Application Layer) of the OSI Model
- Supports Round Robin (default) and Least Outstanding Requests (LOR) routing algorithms
- Target types:



Amazon EC2 Instance

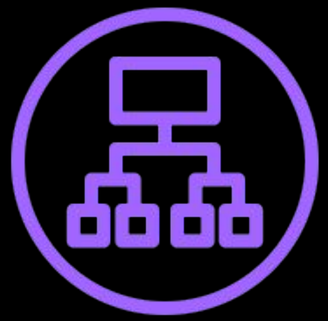


AWS Lambda Function



- Supported Protocol listeners: HTTP, HTTPS, and gRPC
- Also supports WebSockets and HTTP2
- Can be integrated with AWS Global Accelerator, AWS Config, AWS WAF and other features

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

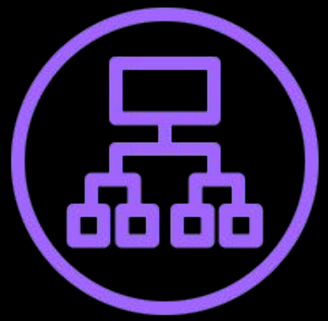


Application Load Balancer

- Notable features:
  - Advanced routing via listener rule condition types
  - Connection Draining
  - Idle connection timeout
  - Cross-zone Load Balancing
  - Preserving Source IP address
  - Slow Start
- Has different security features such as:
  - SSL Offloading
  - Server Name Indication (SNI)
  - Back-end Server Encryption
  - User Authentication
  - Application-Layer Protocol Negotiation (ALPN)
  - Integration with Security Group and AWS WAF

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

LISTENER RULE CONDITION TYPES



Application Load Balancer

- **Host condition**

```
tutorialsdojo.com
portal.tutorialsdojo.com
app.tutorialsdojo.com
*.tutorialsdojo.com
```

- **HTTP Header**

```
User-Agent
Content-Type
```

- **HTTP Request Method**

```
GET, POST, PUT, DELETE
```

- **Path**

```
/img/
/doc/cebu
/pdf/*/report
```

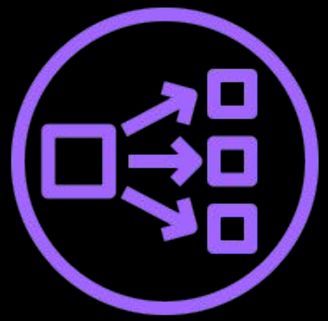
- **Query String**

```
/info?version=1
/health?status=manila
/account?id=123&alias=pogi
```

- **Source IP**

```
192.0.2.0, 198.51.100.10
```

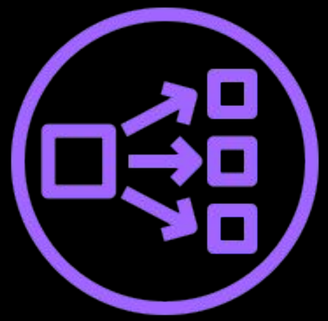
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Network Load Balancer

- For load balancing TCP, UDP, and TLS traffic
- Can handle millions of requests per second
- Routes the traffic while maintaining ultra-low latencies
- Works on the Layer 4 (Transport Layer) of the OSI Model
- Uses the flow hash routing algorithm
- Can be directly associated with an Elastic IP address
- Supports direct integration with: AWS Global Accelerator, AWS Config, VPC Endpoint Services and Traffic Mirroring

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



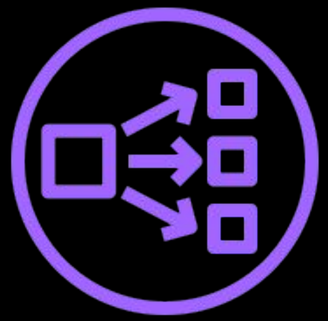
Network Load Balancer

- Notable features:
  - Connection Draining
  - Cross-zone Load Balancing
  - Preserving Source IP address
  - WebSockets support
  - Long-lived TCP connection

- Has different security features such as:
  - SSL Offloading
  - Server Name Indication (SNI)
  - Back-end Server Encryption
  - Application-Layer Protocol Negotiation (ALPN)
  - Integration with AWS Global Accelerator

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

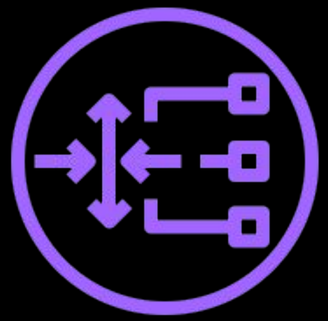
Notable differences between ALB and NLB



Network Load Balancer

- Does not have a selection of rule condition types unlike ALB
- Uses the TCP and UDP transport protocols not HTTP and HTTPS
- Suitable for various networking use cases, or for real-time multiplayer games that uses UDP
- Can support millions of requests per second while maintaining ultra-low latencies unlike ALB
- Can be directly integrated with an Elastic IP address, unlike ALB

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Gateway Load Balancer

- Primarily used for running third-party virtual appliances
- Suitable for custom firewalls, deep packet inspection systems, intrusion detection & prevention systems and many other virtual appliances
- Uses the Internet Protocol (IP) to pass the OSI Layer 3 traffic to its registered targets
- Works on both Layer 3 (Network Layer) and Layer 4 (Transport Layer) of the OSI Model
- Uses the Generic Network Virtualization Encapsulation (GENEVE) protocol to exchange application traffic
- You can use GWLB endpoints to exchange traffic across different VPC boundaries
- The access is configured using the route tables of your VPC, instead of virtual IP addresses

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Classic Load Balancer

- Intended for legacy applications that are still using the EC2-Classic network
- Not recommended for modern applications
- Supports both the transport layer protocols (TCP, SSL) as well as the application layer protocols (HTTP, HTTPS)
- Works on both Layer 4 (Transport Layer) and Layer 7 (Application Layer) of the OSI Model
- For applications with custom security policies and TCP passthrough configuration
- Can provide end-to-end security for your data-in-transit

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Identity and Access Management

AUTHENTICATION

AUTHORIZATION

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Identity

AUTHENTICATION

IAM ENTITIES



IAM USER



IAM GROUP



IAM ROLE

TYPES:

- Root User
- Regular IAM User

Access Management

AUTHORIZATION



IAM POLICY



AWS-managed Policy

Customer-managed Policy

Inline Policy

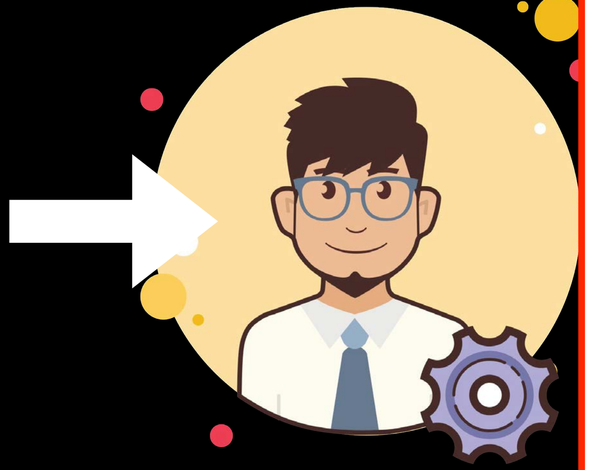
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Grant Least Privilege

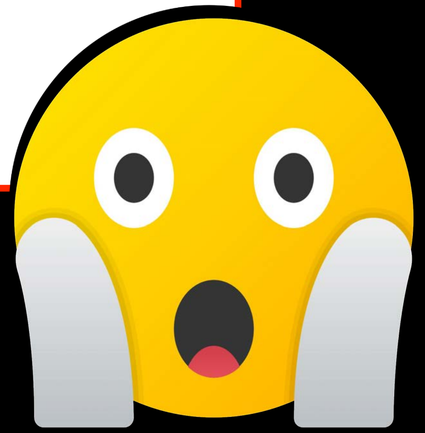
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Does not grant the least privilege

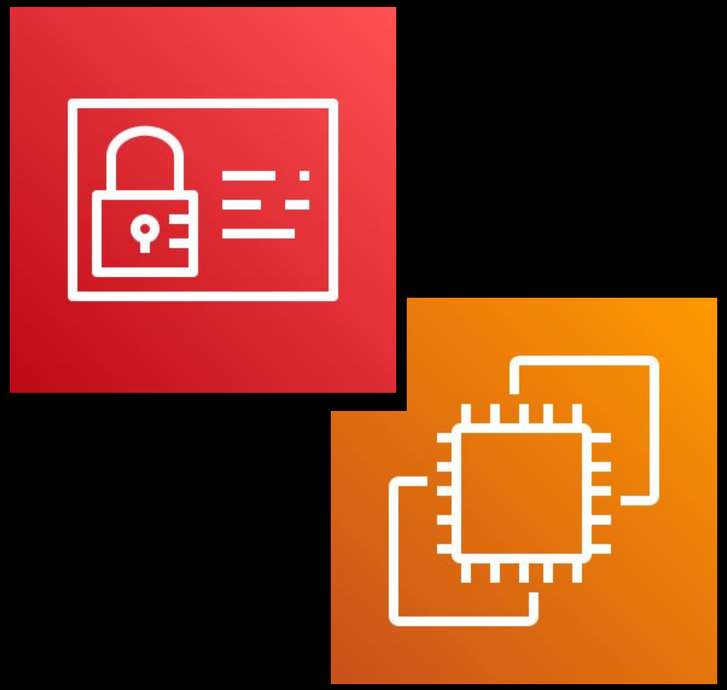


IAM ROLE

ROOT USER ACCESS



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EC2 and AWS IAM

- Use the **Instance Profile** to pass a specific IAM role to your Amazon EC2 instance for it to perform certain actions

- IAM roles attached to your instance can also be viewed on your EC2 metadata.

```
curl http://169.254.169.254/latest/meta-data/iam/info
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3 and AWS IAM

- You can set up a **bucket policy** to grant IAM users and other AWS accounts the access permissions for your bucket and its objects.

- In AWS Organization, you can set up an S3 bucket policy that allows cross-account access to other departments of your organization.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Databases and AWS IAM

- For DynamoDB, you can design an IAM policy that allows access to put, update, and delete items in one specific table.
- **IAM DB Authentication** is a feature available for Amazon RDS and Aurora. This allows you to use IAM to centrally manage access to your database resources

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon SQS and AWS IAM

- An **Access Policy** can be provisioned to control external access to your SQS queue.
- Helps you grant permissions to an external company to access your queue.
- An SQS access policy can allow external companies to poll the queue without giving up the permissions of your own account.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

IDENTITY-BASED POLICY

IAM ENTITIES



IAM USER

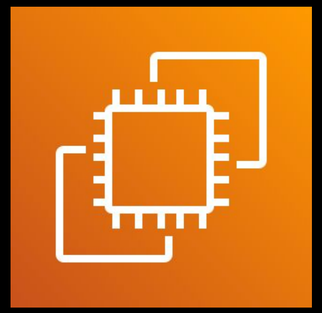


IAM GROUP

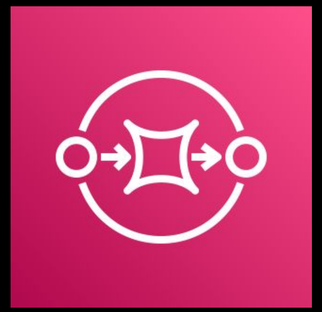


IAM ROLE

RESOURCE-BASED POLICY









NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

PERMISSIONS BOUNDARY

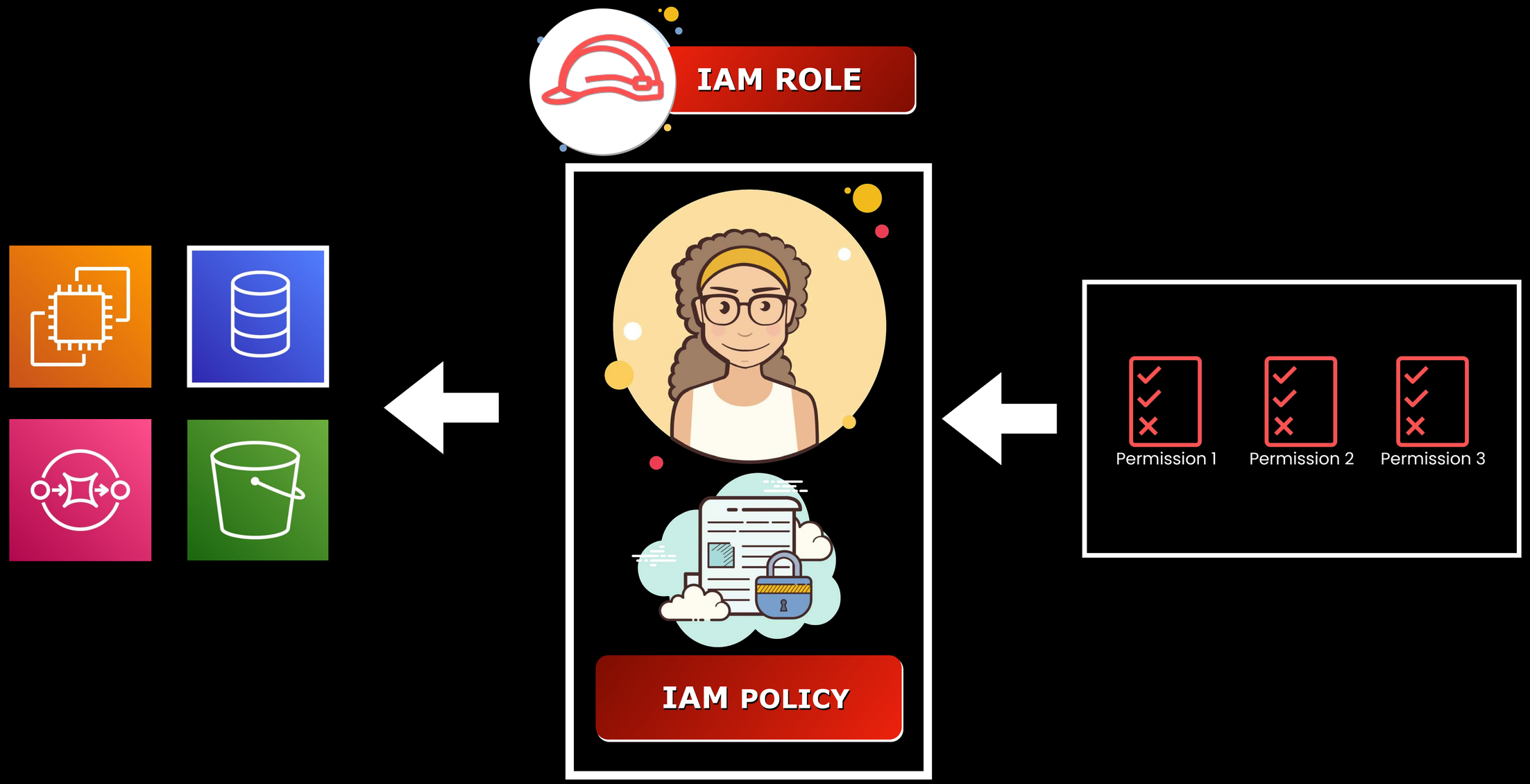
- Allows you to set the **maximum permissions** that an identity-based policy can grant to an IAM entity.
- Ensure that the entity can only perform the actions that are allowed by both its identity-based policies and its permissions boundaries.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM Identities

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

IAM IDENTITIES



IAM USER



IAM GROUP



IAM ROLE

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- An entity that **represents an actual person or a service**
- **Can interact with your AWS resources** using the AWS command-line interface, AWS API, or through the AWS management web console
- Provides someone the ability to sign in to the AWS Management Console and programmatic access to AWS APIs

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM USER

Consists of:

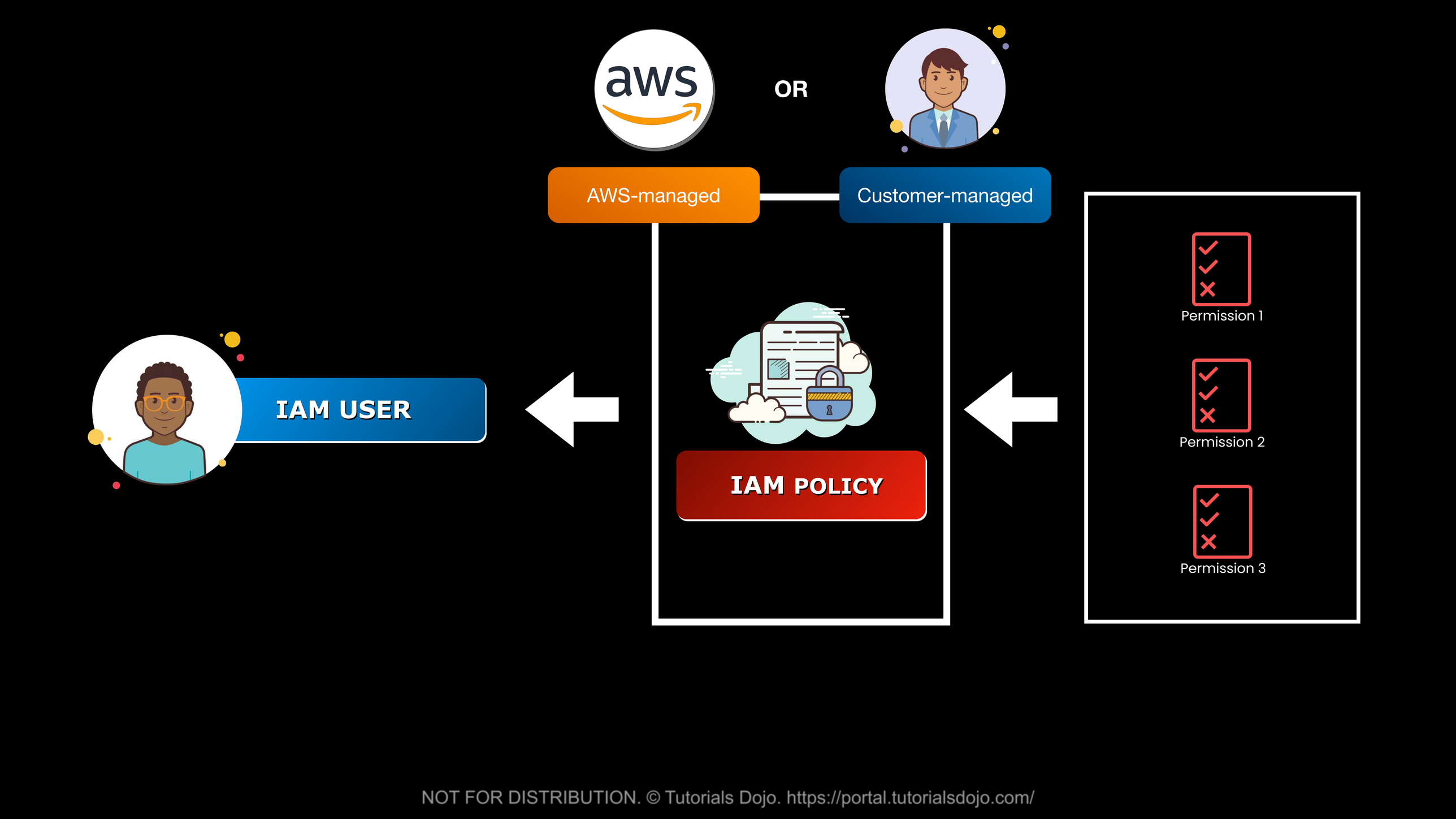
- **NAME**
- **PASSWORD**



- **ACCESS KEY PAIR**
  - **Access Key ID**
  - **Secret Access Key**

- **AWS CLI**
- **AWS APIs**
- **AWS SDKs**
- **AWS CDKs**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

IAM POLICY TYPES

AWS-managed

- Managed by **AWS**
- **Cannot** be fully customized
- Has AWS Managed-Policies for Job Functions that you can readily use:
  - Administrator
  - Support User
  - Security Auditor
  - Network Administrator
  - Developer Power User
  - Billing
  - …and others

Customer-managed

- Managed by **you** (the customer)
- **Can** be fully customized
- You have to manually create a policy for a particular job function



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM USER





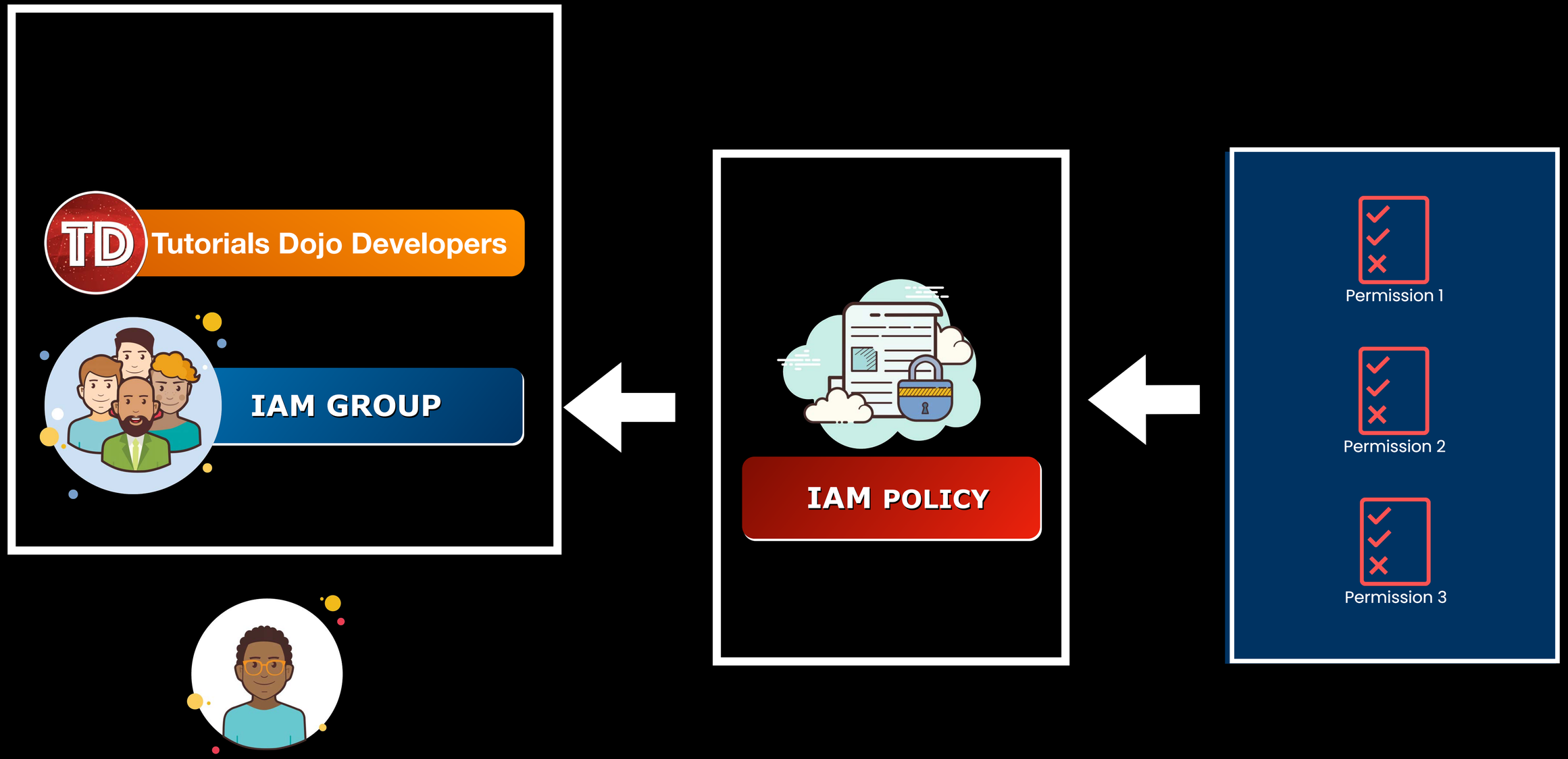
IAM GROUP

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Can **contain multiple IAM Users**
- A single IAM User can belong to multiple IAM Groups
- **Cannot be nested**
- It can only contain IAM users and not other IAM Groups
- There is no default user group that automatically includes all of the IAM Users in your AWS account

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

assumed by





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM ROLE

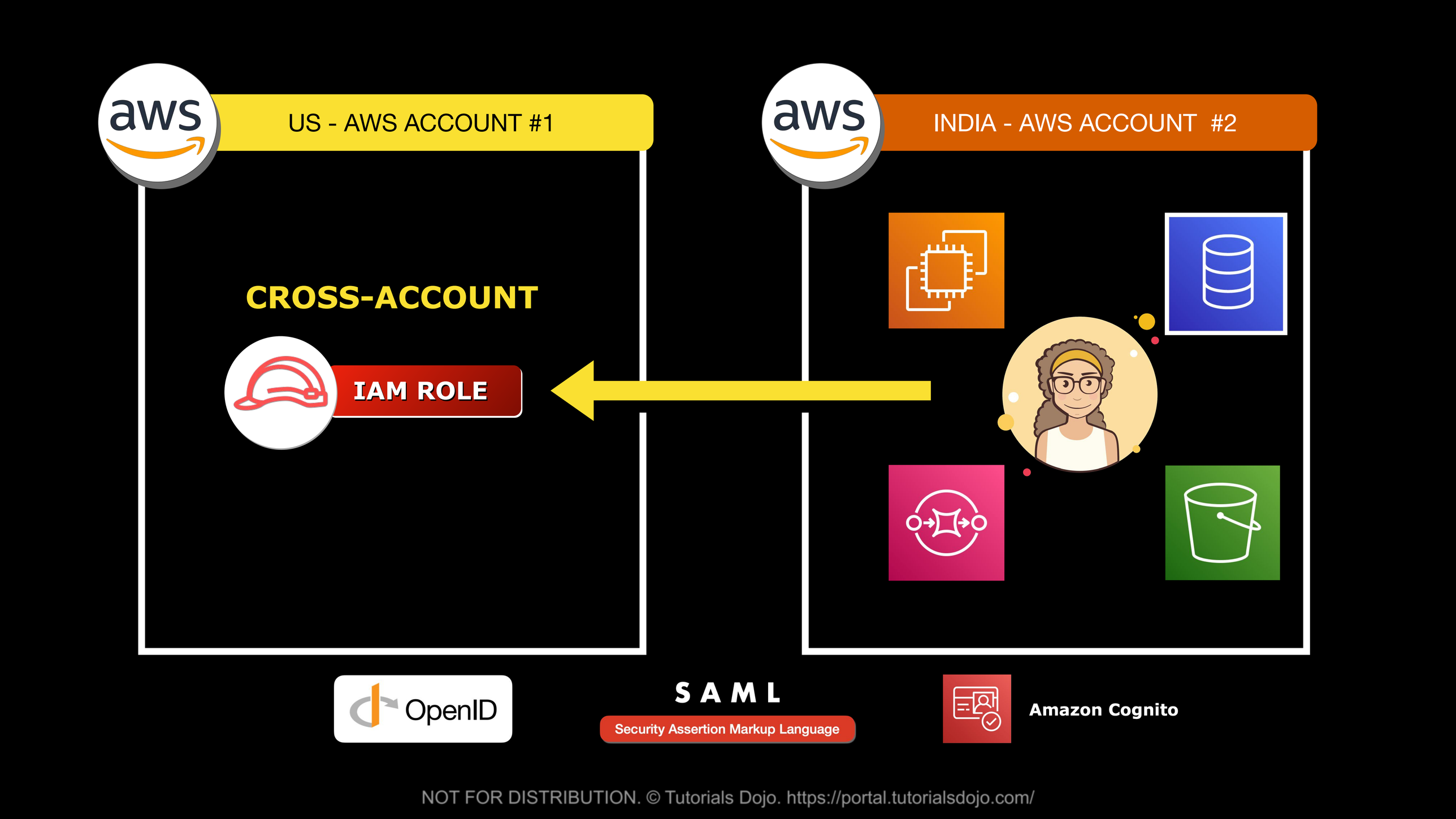
- Intended to be **assumed** by one or more AWS resources
- No long-term credentials



IAM USER

- Uniquely **associated** with one single person only
- Has long-term credentials:
  - AWS Management Console password
  - Access Keys

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CROSS-ACCOUNT

- Grants access to your resources in one account to a trusted principal in a **different AWS account**

AWS SERVICE ROLE

- **Assumed by an AWS service** or applications running in your EC2 instance
- Limited within your AWS account only
- The **custom applications hosted in Amazon EC2 can assume** an AWS service role to perform certain actions

AWS SERVICE-LINKED ROLE

- A predefined role that is **directly linked to an AWS service**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM Policy Types

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM USER



IAM GROUP

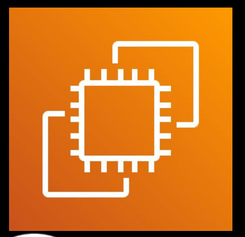


IAM ROLE

IAM IDENTITIES



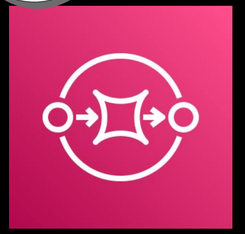
IAM POLICY





aws

RESOURCES





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM POLICY

- Contains permissions that **explicitly ALLOW or DENY access** to certain AWS services
- It provides fine-grained **access control to specific API actions** as well as the AWS resources that the policy should be applied to

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM POLICY

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TutorialsDojo",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::tutorialsdojo-manila/*"
        }
    ]
}
```

ALLOWS THE API ACTIONS YOU SPECIFY

API action

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM POLICY

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "tutorialsdojo",
        "Effect": "Deny",
        "Action": [
            "lambda:CreateFunction",
            "lambda:DeleteFunction"
            ],
        "Resource": "*",
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": "220.110.16.0/20"
            }
        }
    }
}
```

DENIES THE API ACTIONS

API actions

IP Condition

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM POLICY

Multi-Factor Authentication
(MFA)

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "tutorialsdojo",
        "Effect": "Deny",
        "Action": [
            "lambda:CreateFunction",
            "lambda:DeleteFunction"
        ],
        "Resource": "*",
        "Condition": {
            "BoolIfExists": {
                "aws:MultiFactorAuthPresent": "false"
            }
        }
    }
}
```

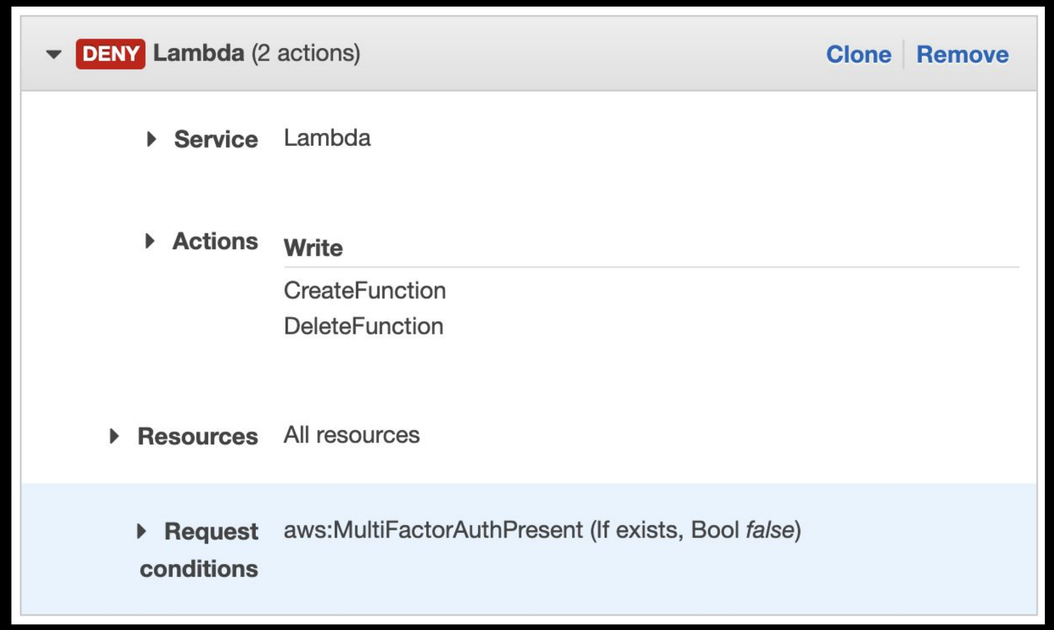
MFA Condition

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

JSON EDITOR

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "tutorialsdojo",
        "Effect": "Deny",
        "Action": [
            "lambda:CreateFunction",
            "lambda:DeleteFunction"
            ],
        "Resource": "*",
        "Condition": {
            "BoolIfExists": {
                "aws:MultiFactorAuthPresent": "false"
            }
        }
    }
}
```

VISUAL EDITOR



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Standalone Policy



Inline Policy

- **Remains unchanged** even if you delete its associated IAM identity
- It doesn’t have a strict one-to-one relationship to its associated IAM identity

- **Will be automatically be deleted** if you delete its associated identity
- Has a strict one-to-one relationship to its associated IAM identity

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM Policy Types

- Identity-based Policies
- Resource-based Policies
- Permissions Boundaries
- AWS Organizations SCPs
- S3 Access Control Lists (ACLs)
- Session Policies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Identity-Based Policy

- A policy that you **attach to an IAM Identity**
- Two Types:

Managed Policies

- A type of a standalone policy
- Can either be AWS managed or Customer-managed

Inline Policies

- Maintains a strict one-to-one relationship between a policy and an IAM identity.
- Tightly-coupled with its associated IAM Identity

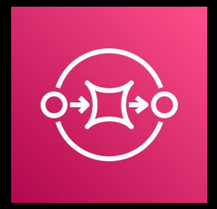
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Resource-Based Policy

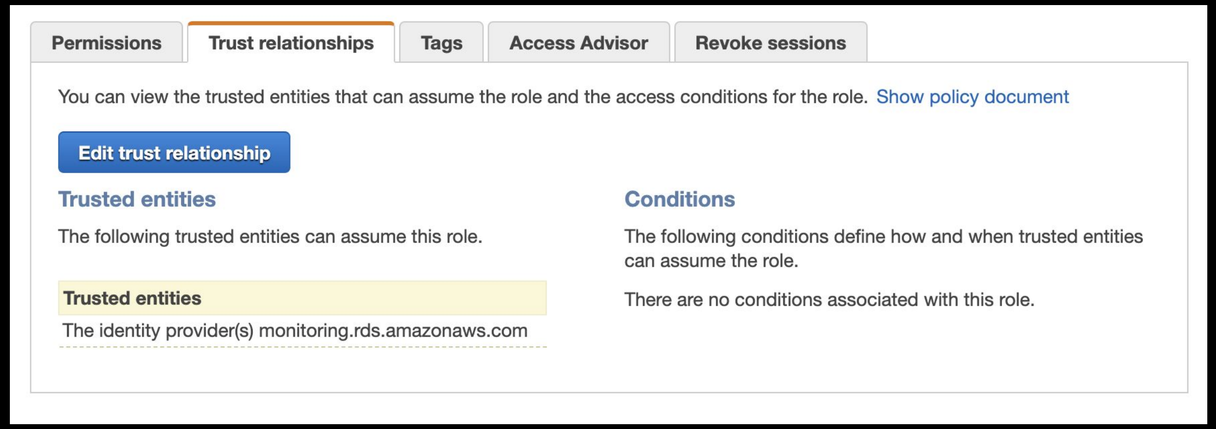
- Attaches an inline policy to a **specific AWS Resource**
- Types:



S3 Bucket Policy



SQS Access Policy



IAM ROLE Trust Policy

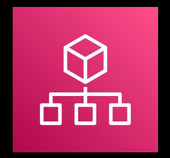
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Permissions Boundaries

- Defines the **maximum permissions** that an identity-based policy can grant to an IAM entity
- Does not explicitly grant permissions
- **Sets a clear boundary** to ensure that a given IAM policy will not over-provision the permissions to your AWS resources

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Service Control Policies
(SCPs)

- Primarily used in:  **AWS Organizations**
- Defines the **maximum permissions for account members** of an organization or organizational unit.
- Limits the permissions that identity-based policies or resource-based policies grant to the IAM users or roles within the AWS account
- IAM policies can't restrict the AWS account root user. In the contrary, the specified actions from an attached SCP can affect all IAM identities, including the root user, of the member account

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Access Control List
(ACL)

- Primarily used in: **Amazon S3**
- Controls which principals in other AWS accounts can access a particular bucket
- These are **cross-account permission policies** that grant certain permissions to a specified principal that you define
- ACLs cannot grant permissions to entities within the same account

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sessions Policies

- Limits the permissions that an identity-based policy grants to a **particular session**
- Works like **Permissions Boundaries**
- **Sets a limit of what kind of permission a session has**, without granting any permissions.
- Aside from an identity-based policy, the permissions of a session policy can also come from a resource-based policy
- If there’s an explicit deny in any of the policies, then it will effectively override any allowed permissions

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM Policy Basics

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Policy-wide Information

Statements

```
{
    "Id": "TutorialsDojoPolicy1",
    "Version": "2012-10-17",

    "Statement": [
        {
            "Sid": "AllowAllActionsOnBooksTable",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        },
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": ["s3:ListBucket", "s3:DeleteObject"],
            "Resource": ["arn:aws:s3:::tutorialsdojo-manila"]
        }
    ]
}
```

Logical **OR**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

IAM Statement Elements

```
{
    "Sid"       : "AllowActionsOnBooksTable",
    "Effect"    : "Allow",
    "Principal" : { "AWS": "arn:aws:iam::123456789012:root" }
    "Action"    : [
                      "dynamodb:*",
                      "s3:*",
    "Resource"  :    arn:aws:s3:::tutorialsdojo/*
    "Condition" :  {
        "IpAddress": {
            "aws:SourceIp": "220.110.16.0/20"
    }
}
```

Statement ID

ALLOW or DENY

CONDITION ELEMENT

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

CONDITION ELEMENT

- String
- Numeric
- Date
- Boolean
- Binary
- ARN
- IfExists
- IpAddress
- …and many more!

```
"Condition" : { "{condition-operator}" : { "{condition-key}" : "{condition-value}" }}
```

StringEquals
StringNotEquals
StringEqualsIgnoreCase
StringNotEqualsIgnoreCase
StringLike
StringNotLike

DateEquals
DateNotEquals
DateLessThan
DateLessThanEquals
DateGreaterThan
DateGreaterThanEquals

NumericEquals
NumericNotEquals
NumericLessThan
NumericLessThanEquals
NumericGreaterThan
NumericGreaterThanEquals

ArnEquals, ArnLike
ArnNotEquals, ArnNotLike

IpAddress
NotIpAddress

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

CONDITION ELEMENT

IfExists

- StringEqualsIfExists
- NumericEqualsIfExists
- BoolIfExists
- IpAddressIfExists
- etc…

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Shares the Amazon S3 bucket named **`tutorialsdojo-manila`** with an external vendor while ensuring that the **bucket owner** is still be able to access all objects

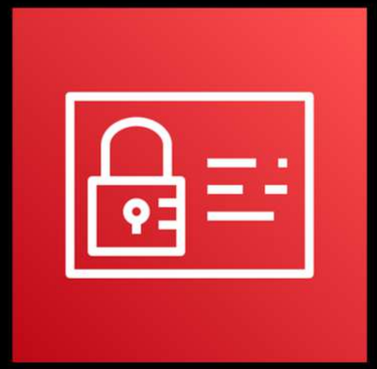
```
. . .
        "Action": [
            "s3:PutObject"
        ],
        "Resource": “arn:aws:s3:::tutorialsdojo-manila/*”,
        "Condition": {
            "StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control"
            }
        }
. . .
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Users will be denied of all API actions *(except for the **s3:PutObject** action)* if their **multi-factor authentication (MFA)** is not enabled

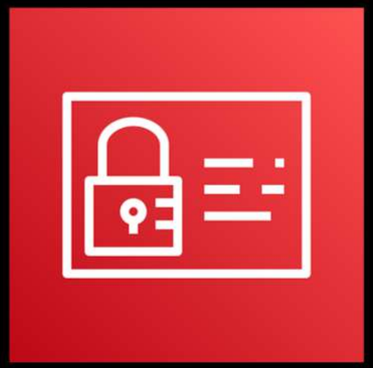
```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DenyAllTDojoUsersNotUsingMFA",
        "Effect": "Deny",
        "NotAction": “s3:PutObject",
        "Resource": "*",
        "Condition": {
            "BoolIfExists": {
                "aws:MultiFactorAuthPresent": "false"}
            }
    }]
}
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM Access Analyzer

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

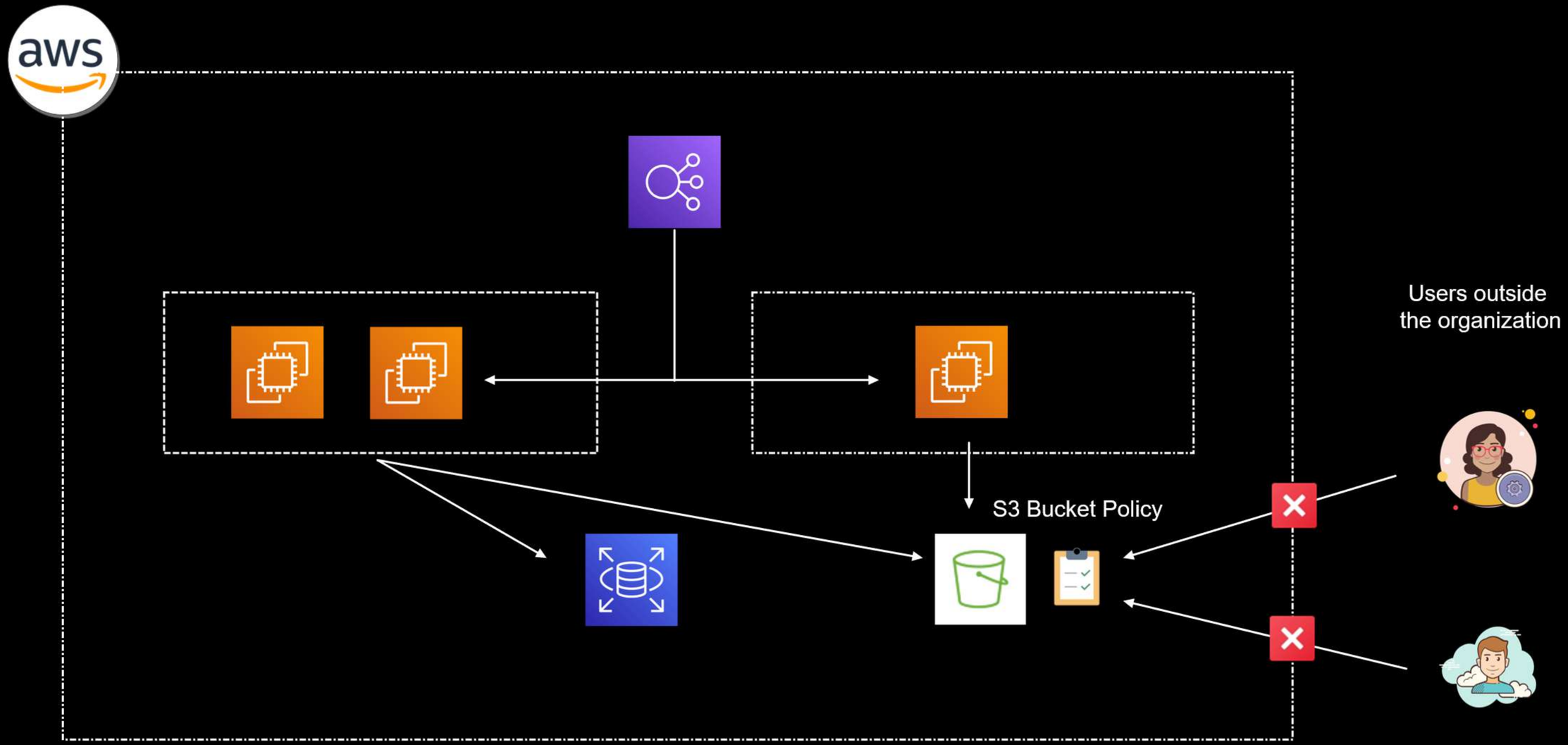


IAM Access Analyzer

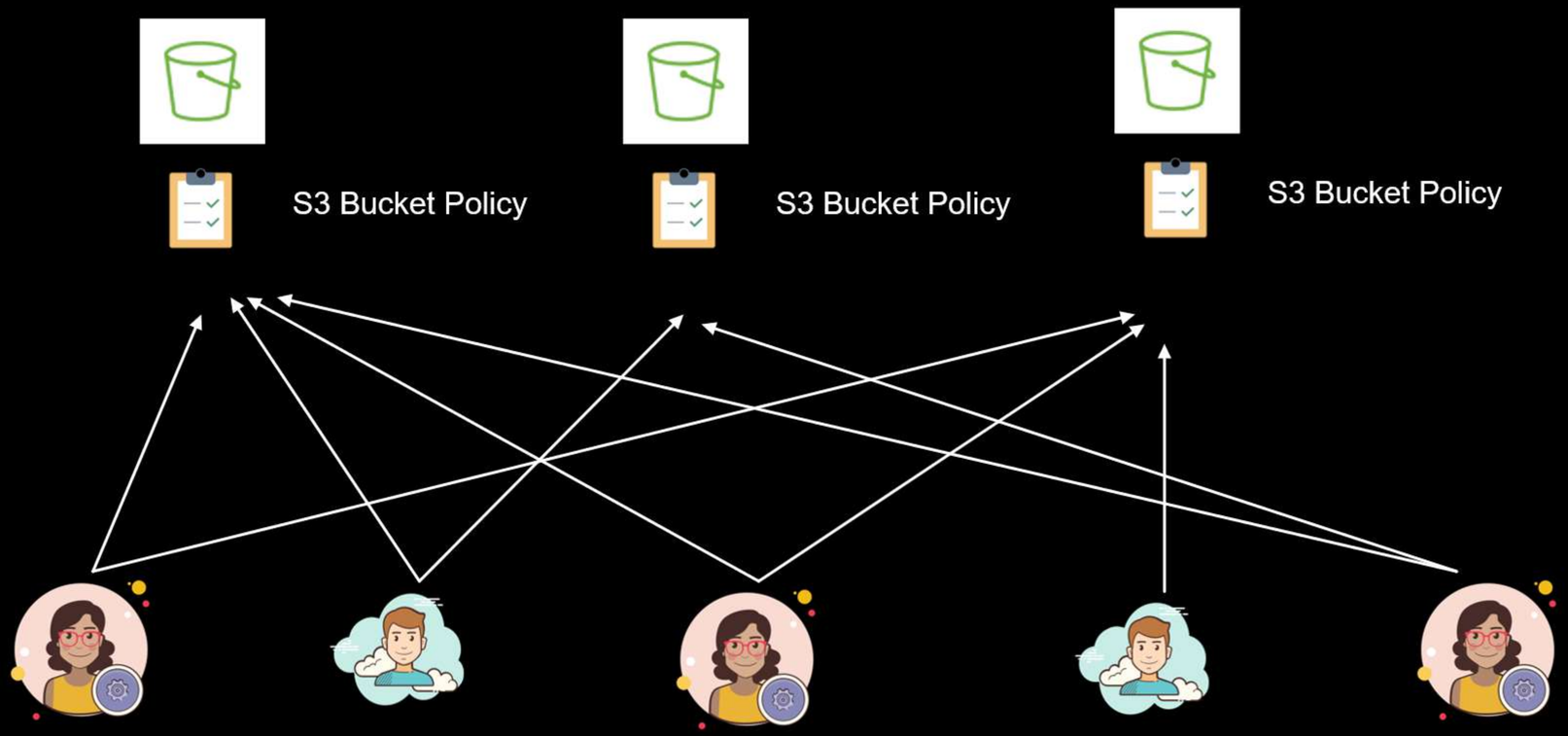
Questions we will try to answer in this lecture.

- What problem does IAM Access Analyzer solve?
- How does it fit in the enterprise scenario?

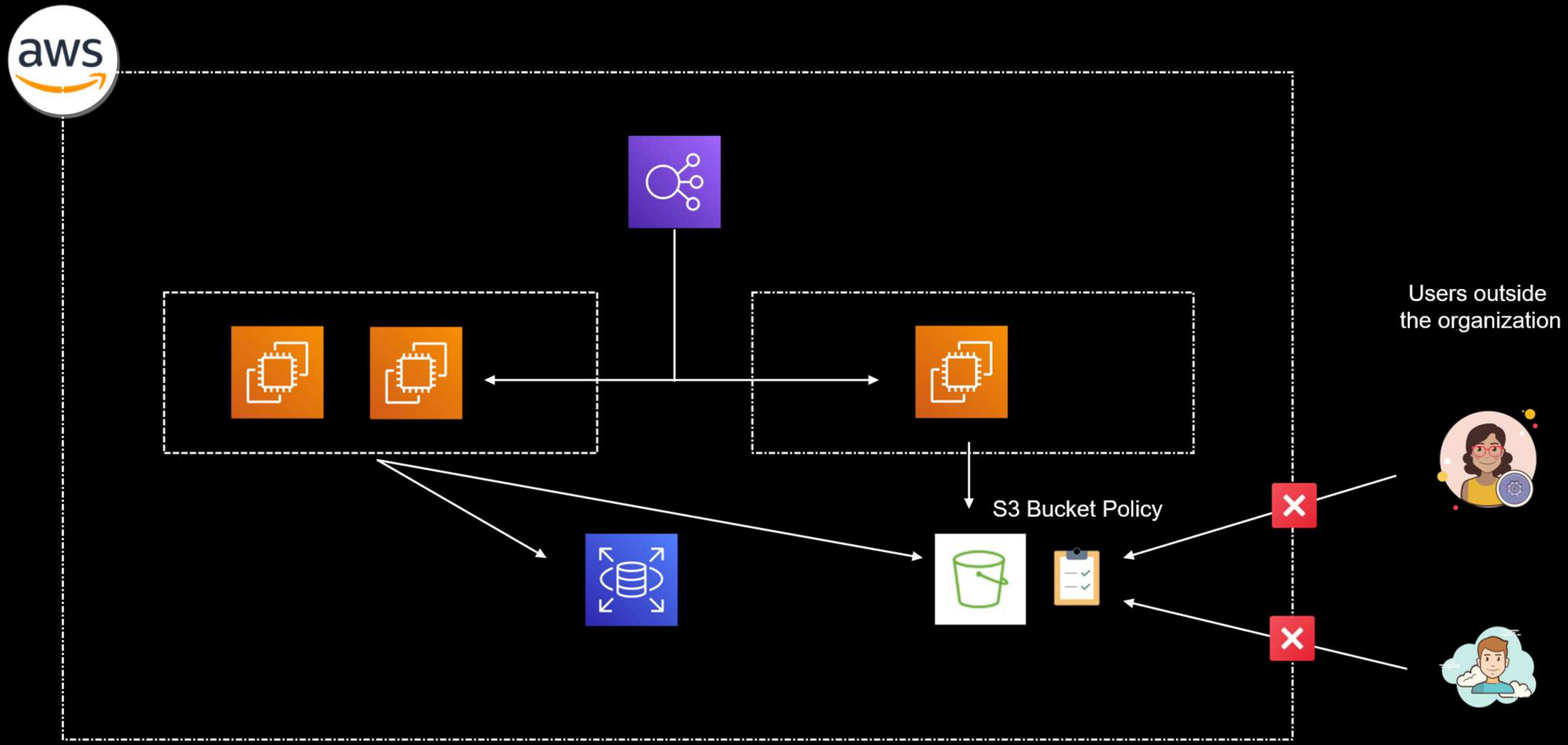
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



analyze resource-based policies

IAM Access Analyzer

- generates findings for each instance of a resource that is shared outside the organization
- allows you to analyze access for resources that belong to your organization, even if another AWS account owns the resource.

Users outside the organization

S3 Bucket Policy







NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



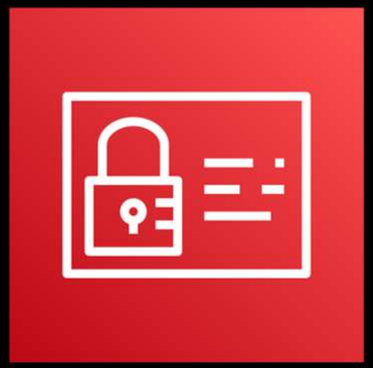
IAM Access Analyzer

Generate findings for resource types like:

- S3 buckets
- IAM roles
- KMS keys
- Lambda functions and layers
- SQS queues
- Secrets Manager secrets

→ all services support resource-based policies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



IAM Access Analyzer

IAM Access Analyzer can send an event to EventBridge:

- for each generated finding
- for a change to the status of an existing finding
- when a finding is deleted

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

IAM Access Analyzer



Generates findings

sends findings

Amazon EventBridge



Create an event rule to receive findings, with a target action that publishes message to an SNS topic

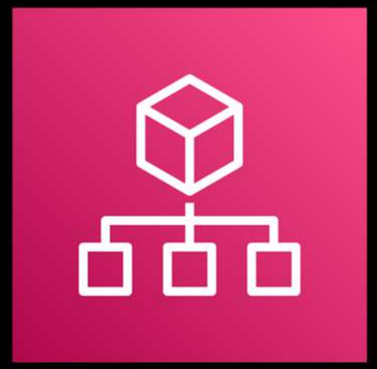
sends message

Amazon SNS



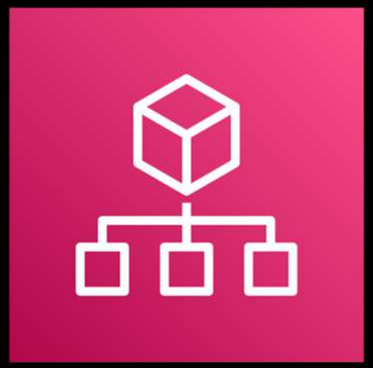
Receives message from the Amazon EventBridge event rule

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Organizations Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Organizations

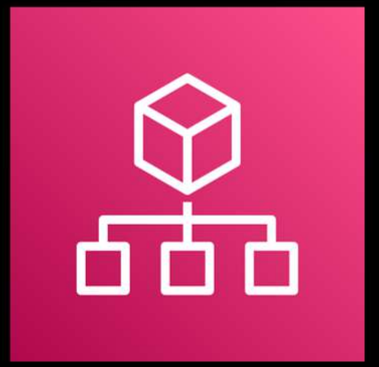
At the end of the video, you will be able to:

- Differentiate AWS IAM against AWS Organizations
- Explain basic terminology and concepts when using AWS Organizations like:
  - root
  - accounts
  - organizational units
  - service control policies (or SCPs)
- Learn best practices when you are using AWS Organizations

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Identity Access Management



AWS Organizations

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Identity Access Management

- used to provide permissions to access the AWS API
- you create IAM accounts within a specific AWS account to provide access resources to that account.

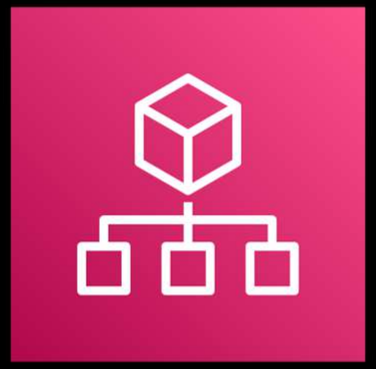
AWS Organizations

- allows you to manage multiple AWS accounts from a management AWS account
- you can limit what services can be used in multiple AWS accounts and monitor their compliance

❌ **An AWS account is NOT the same as a user account.**

- An AWS user is an identity that you create using the AWS IAM.
- An AWS account typically contains multiple IAM users and roles.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Organizations

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

root



master

Management Account

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Management Account

- Used to create an AWS organization
- Use this AWS account solely for the purpose of managing your organization only and NOT to provision resources
- The fewer users that can access this account, the better.

Carries senstitive administrative capabilities like:

- creating additional AWS accounts within your organization
- inviting other AWS accounts to join your organization
- removing accounts
- applying policies for security compliance
- deleting AWS accounts when you no longer need them

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Management Account

- used to create an AWS organization
- Use this AWS account solely for the purpose of managing your organization only and NOT to provision resources
- The fewer users that can access this account, the better.

AWS Organizations

SUPPORT ALL FEATURES

CONSOLIDATED BILLING ONLY

billing

payments

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

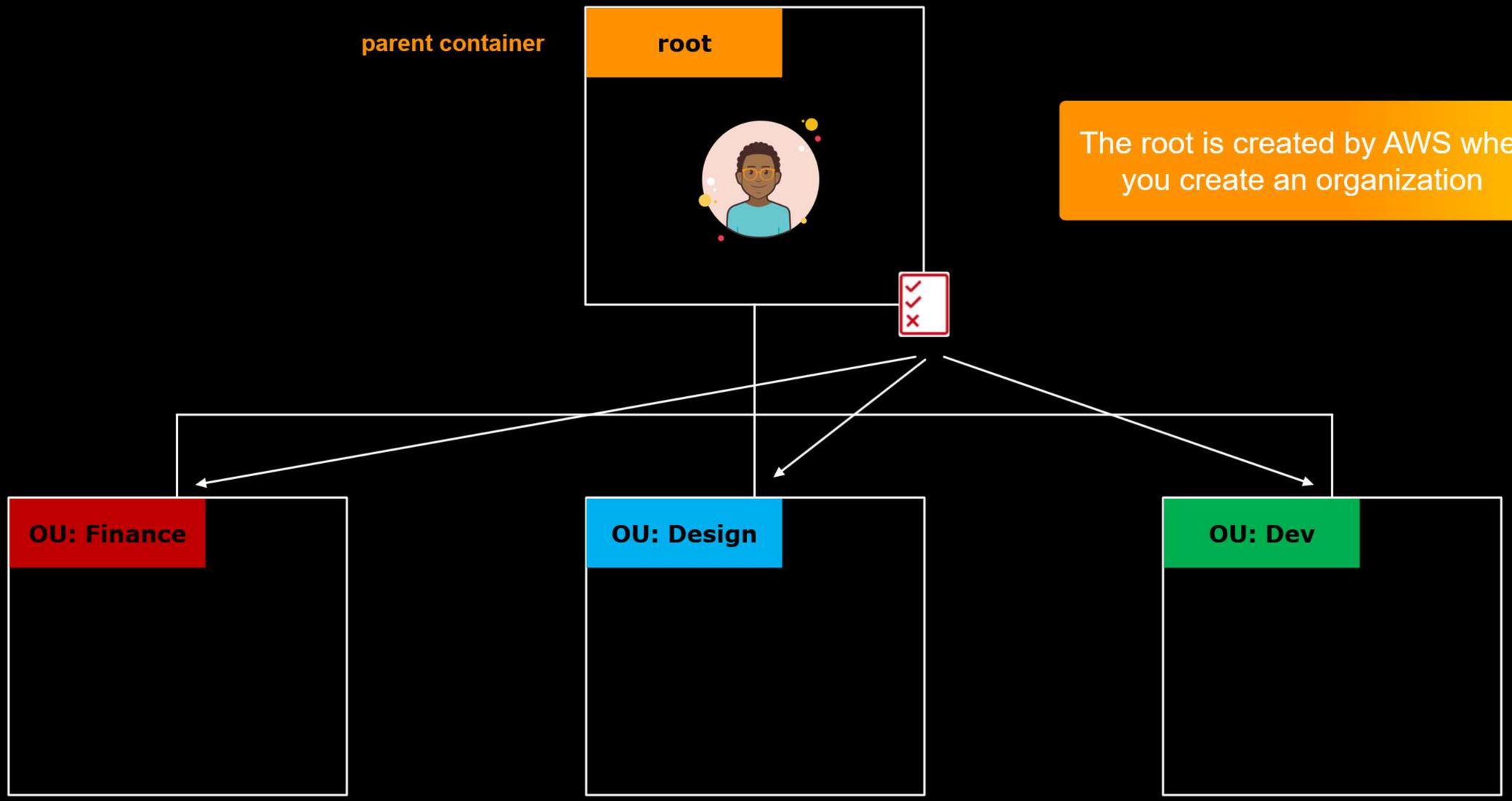


Management account can start creating Organization Units (OUs)

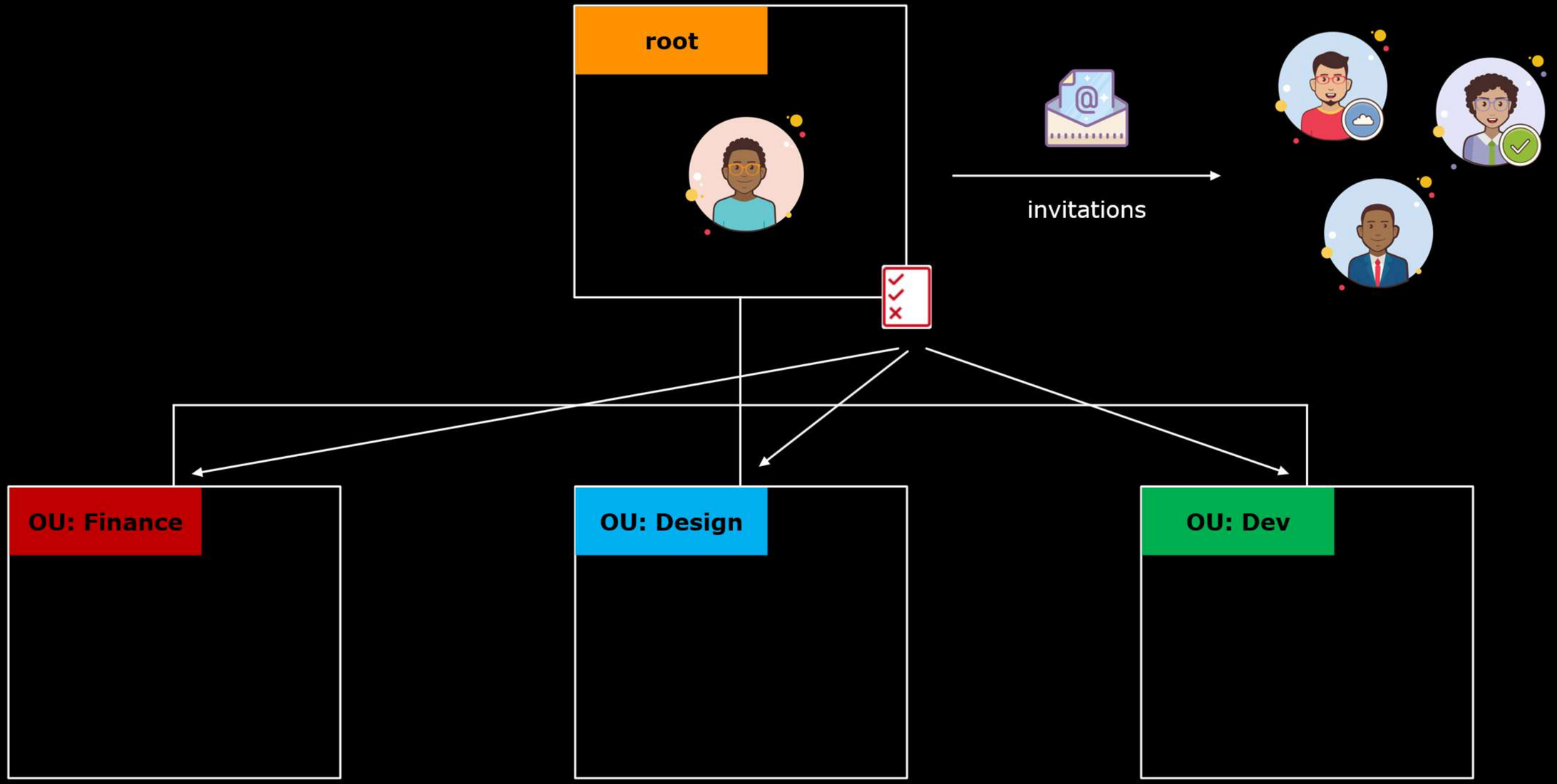
Management Account

- Think of Organizational Units (OUs) as a container for AWS accounts
- Creates a hierarchical structure in organizing your AWS account

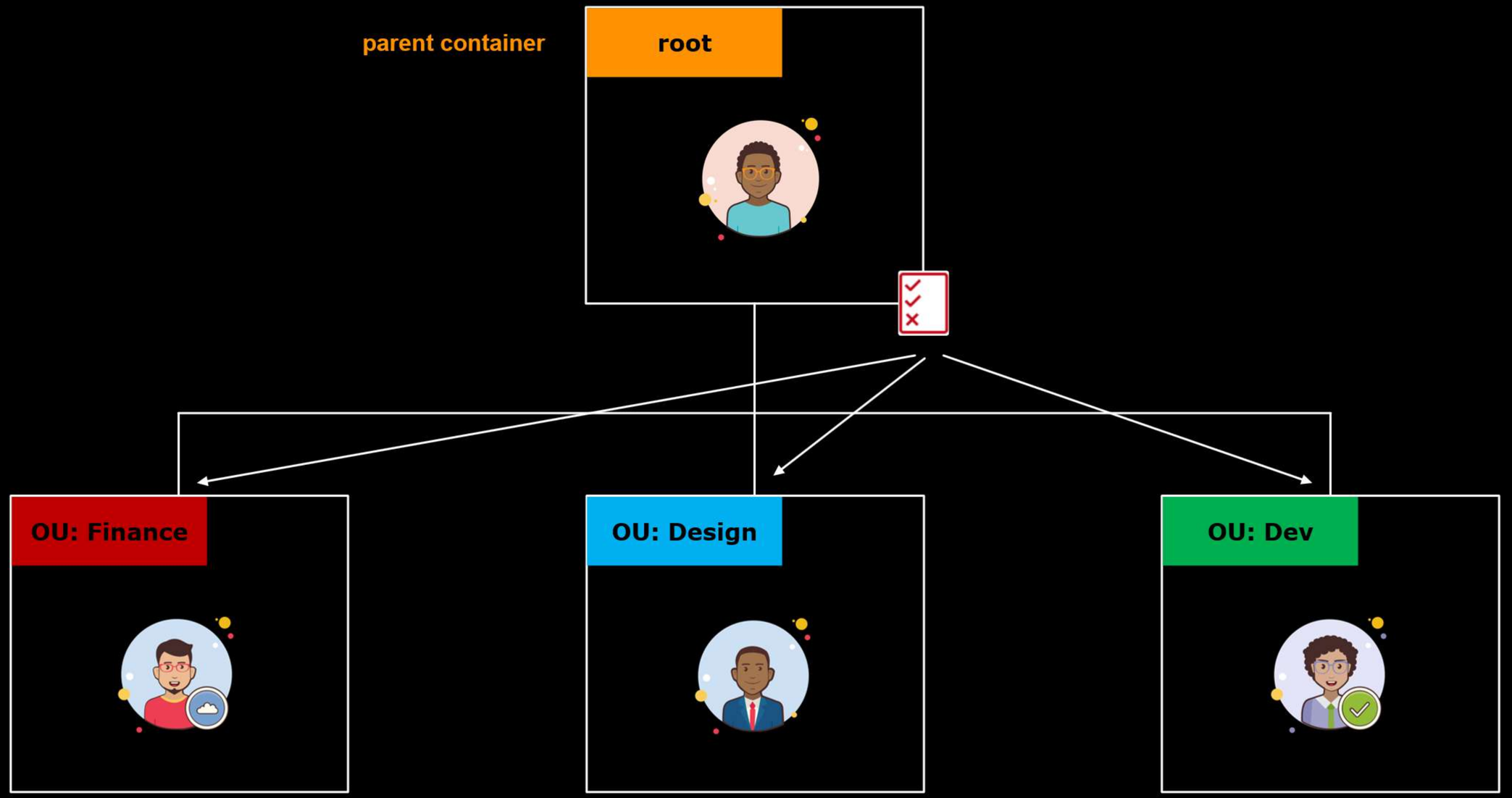
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



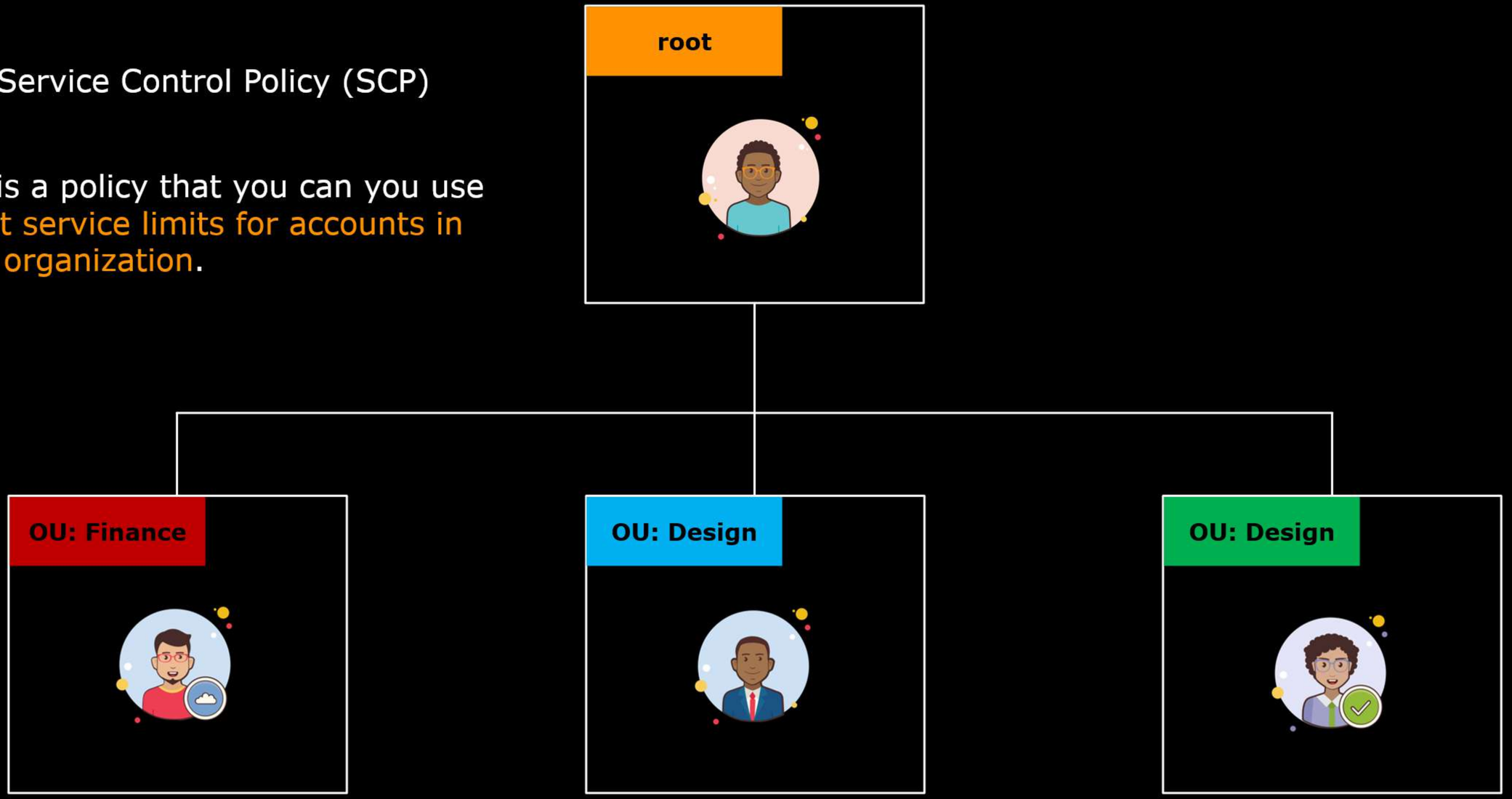
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Service Control Policy (SCP)

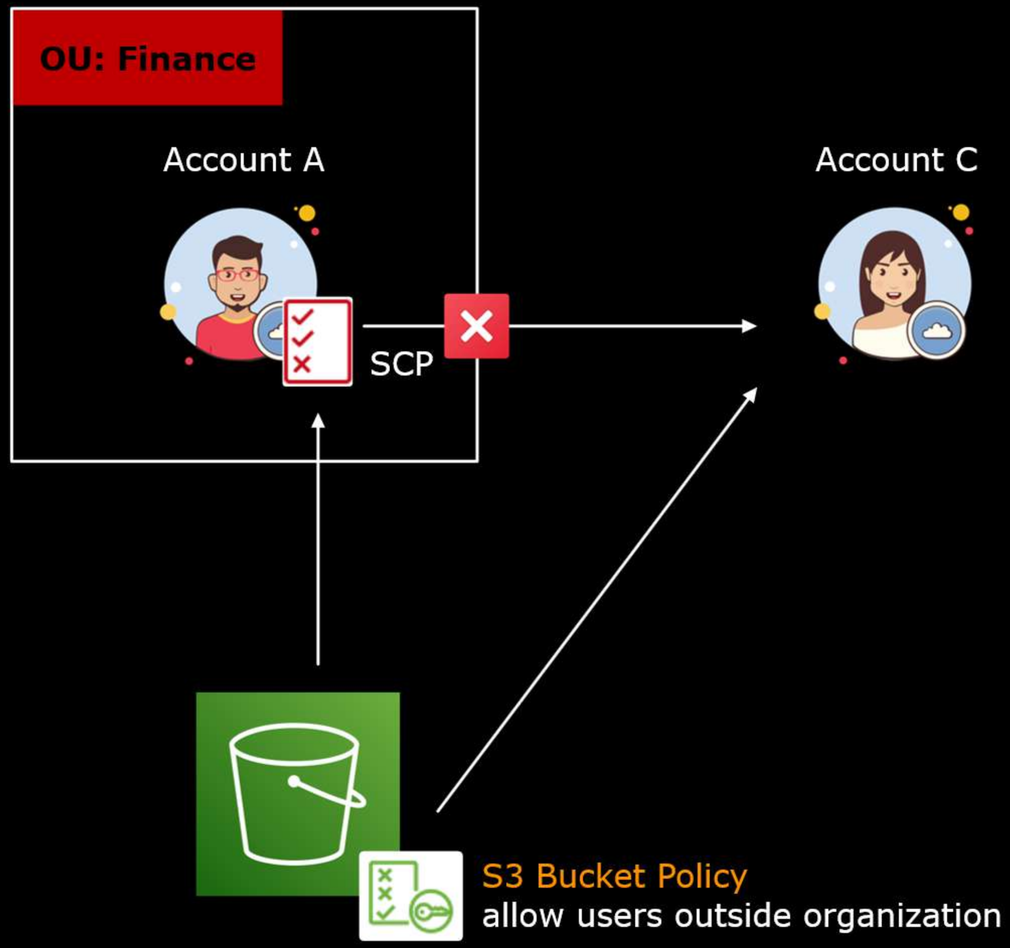
SCP is a policy that you can you use to set service limits for accounts in your organization.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SCP Policies

- Affects IAM users and roles that are managed by accounts that are part of the organization only
- They don't affect resource-based policies directly.

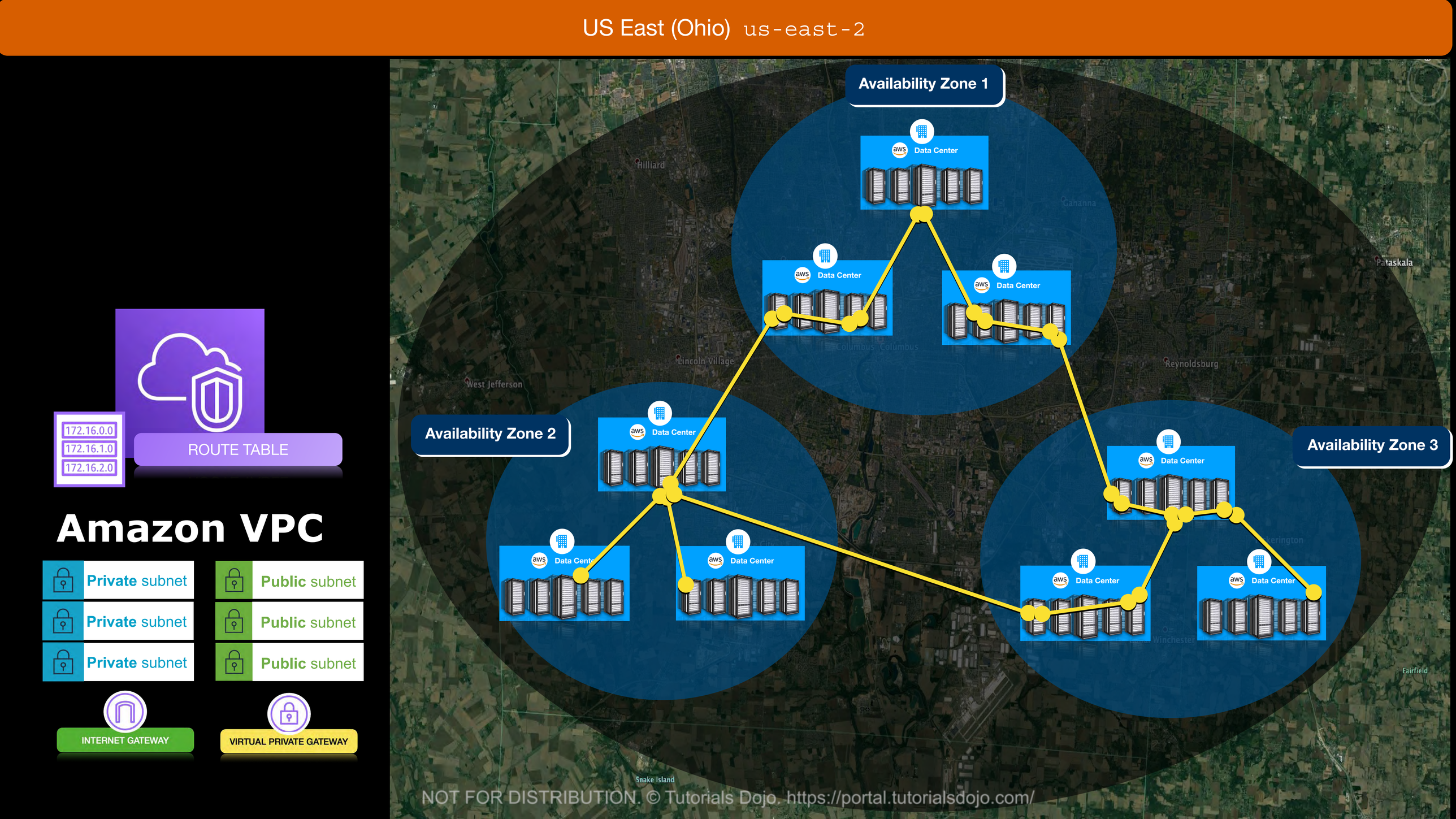


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

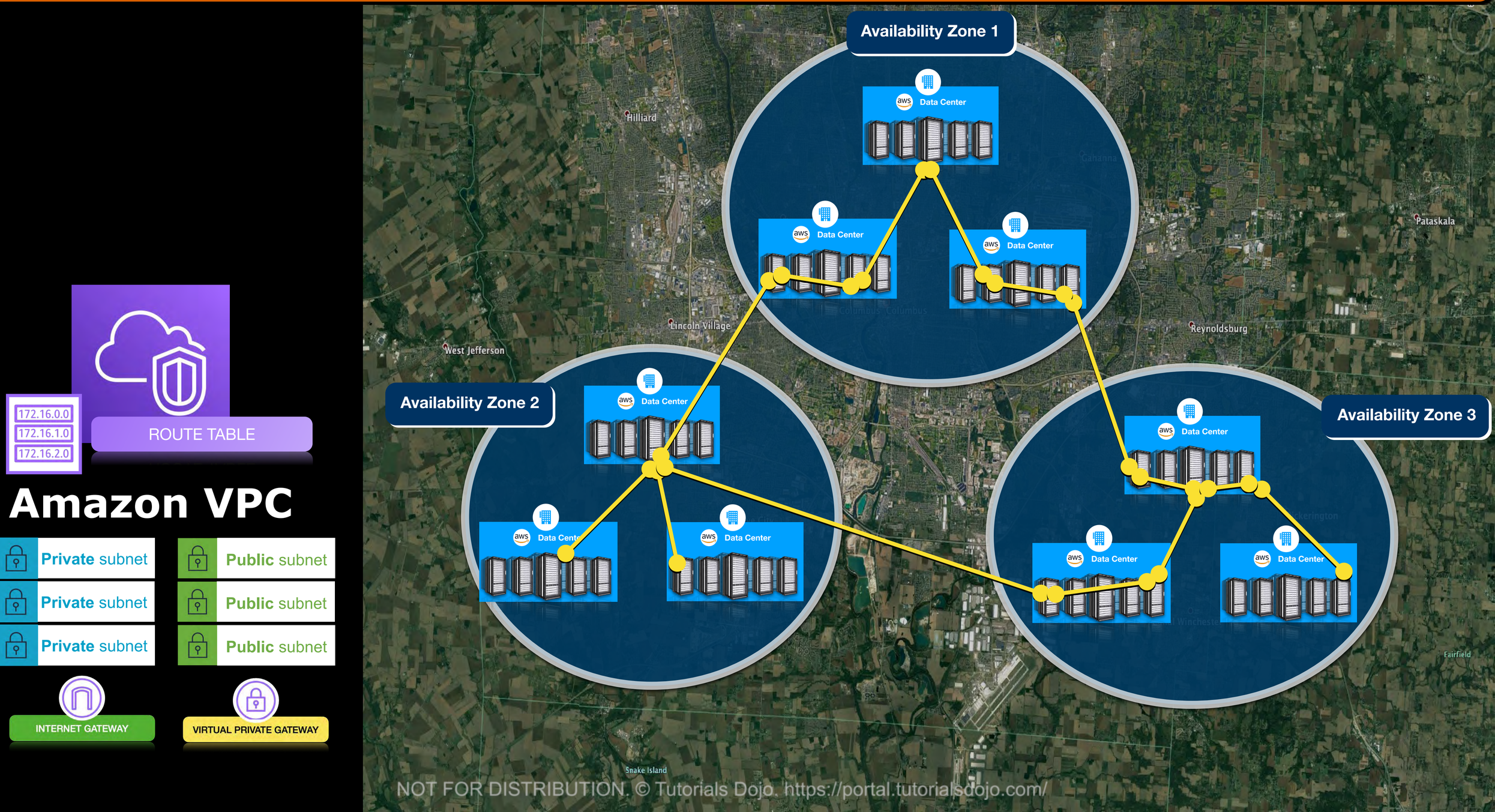


Amazon VPC Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/


US East (Ohio) us-east-2
Availability Zone 1
Availability Zone 2
Availability Zone 3
Data Center
172.16.0.0
172.16.1.0
172.16.2.0
ROUTE TABLE
Amazon VPC
Private subnet
Private subnet
Private subnet
Public subnet
Public subnet
Public subnet
INTERNET GATEWAY
VIRTUAL PRIVATE GATEWAY
Hilliard
Gahanna
Pataskala
Lincoln Village
West Jefferson
Reynoldsburg
Columbus
Snake Island
Fairfield
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

US East (Ohio) us-east-2



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

aws CLOUD

REGION

Amazon VPC

IPv4 CIDR Range: 10.0.0.0/16

IPv6 CIDR Range: 2001:db8:1234:1a00::/56

172.16.0.0
172.16.1.0
172.16.2.0

ROUTE TABLE

Private subnet

10.0.0.0/24

- A subnet **must reside entirely within one Availability Zone** only
- One subnet **cannot span to two or more AZs**.



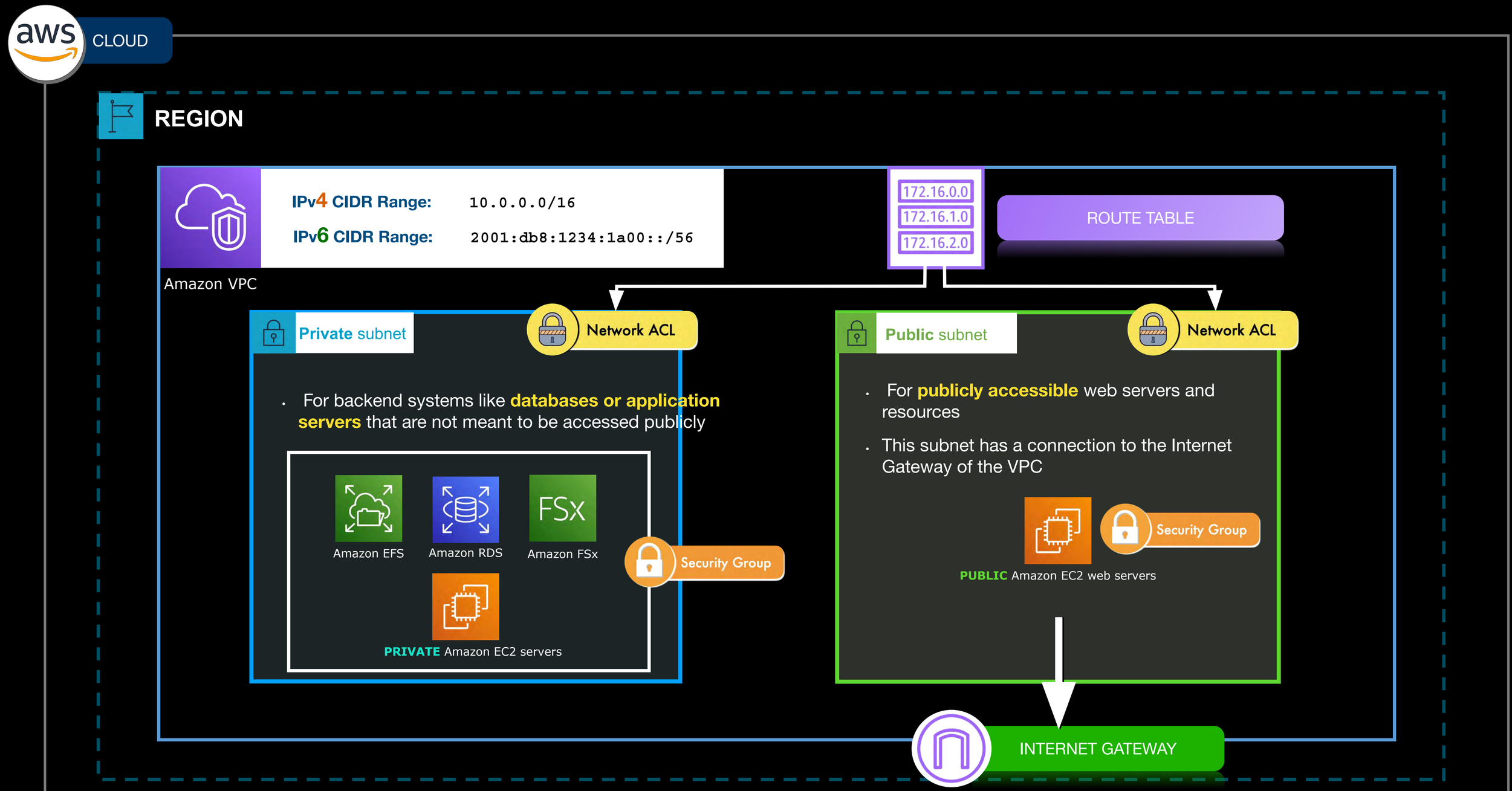
Public subnet

10.0.1.0/24

- You can **have multiple subnets in the same** Availability Zone.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Anatomy of an Amazon VPC

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

aws CLOUD

AWS IAM

REGION

Amazon VPC

IPv4 CIDR Range: 10.0.0.0/16

IPv6 CIDR Range: 2001:db8:1234:1a00::/56

172.16.0.0
172.16.1.0
172.16.2.0

ROUTE TABLE

Private subnet

Network ACL

Amazon EFS

Amazon RDS

Amazon FSx

Security Group

PRIVATE Amazon EC2 servers

Public subnet

Network ACL

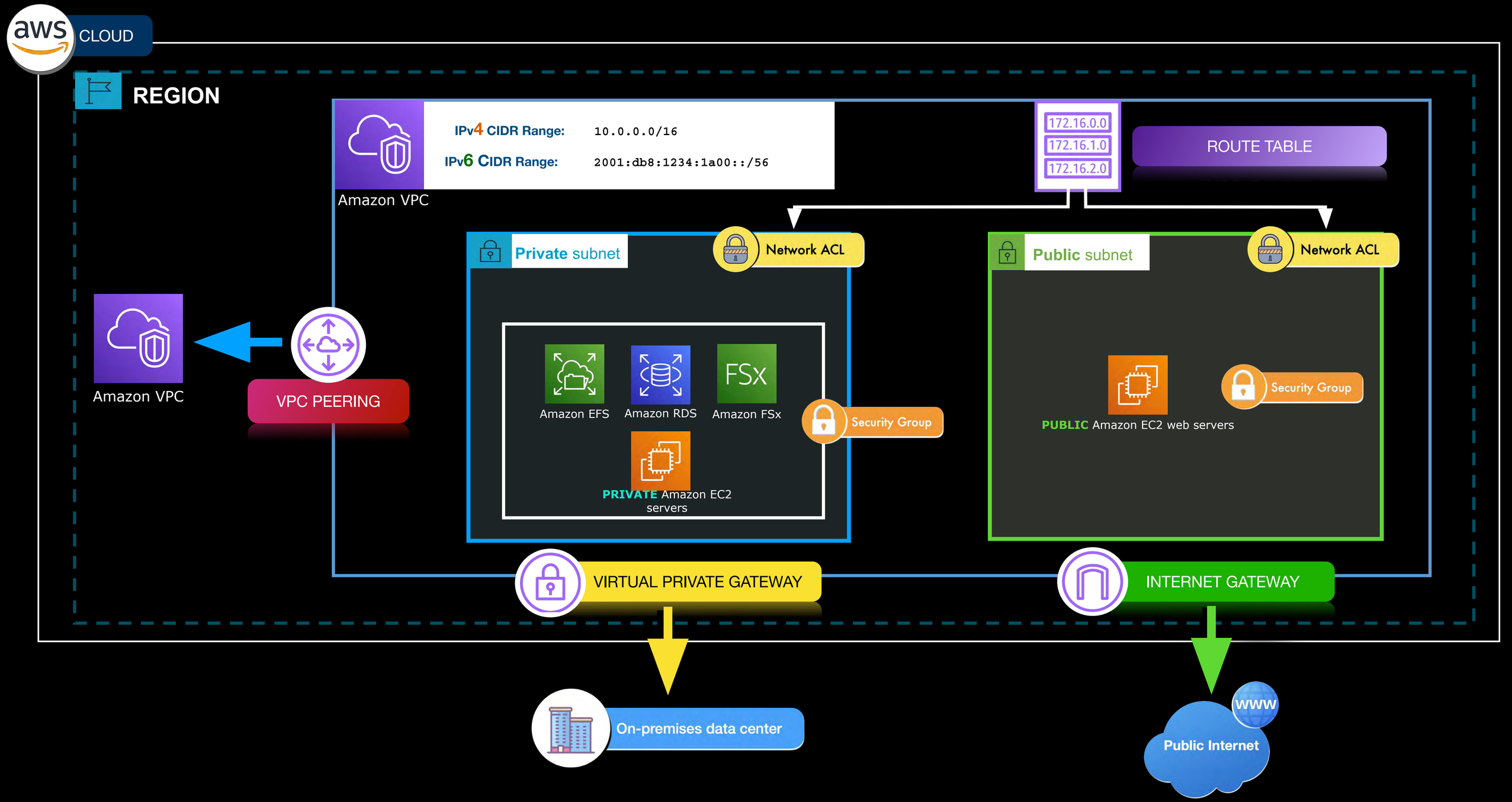
Security Group

PUBLIC Amazon EC2 web servers

VIRTUAL PRIVATE GATEWAY

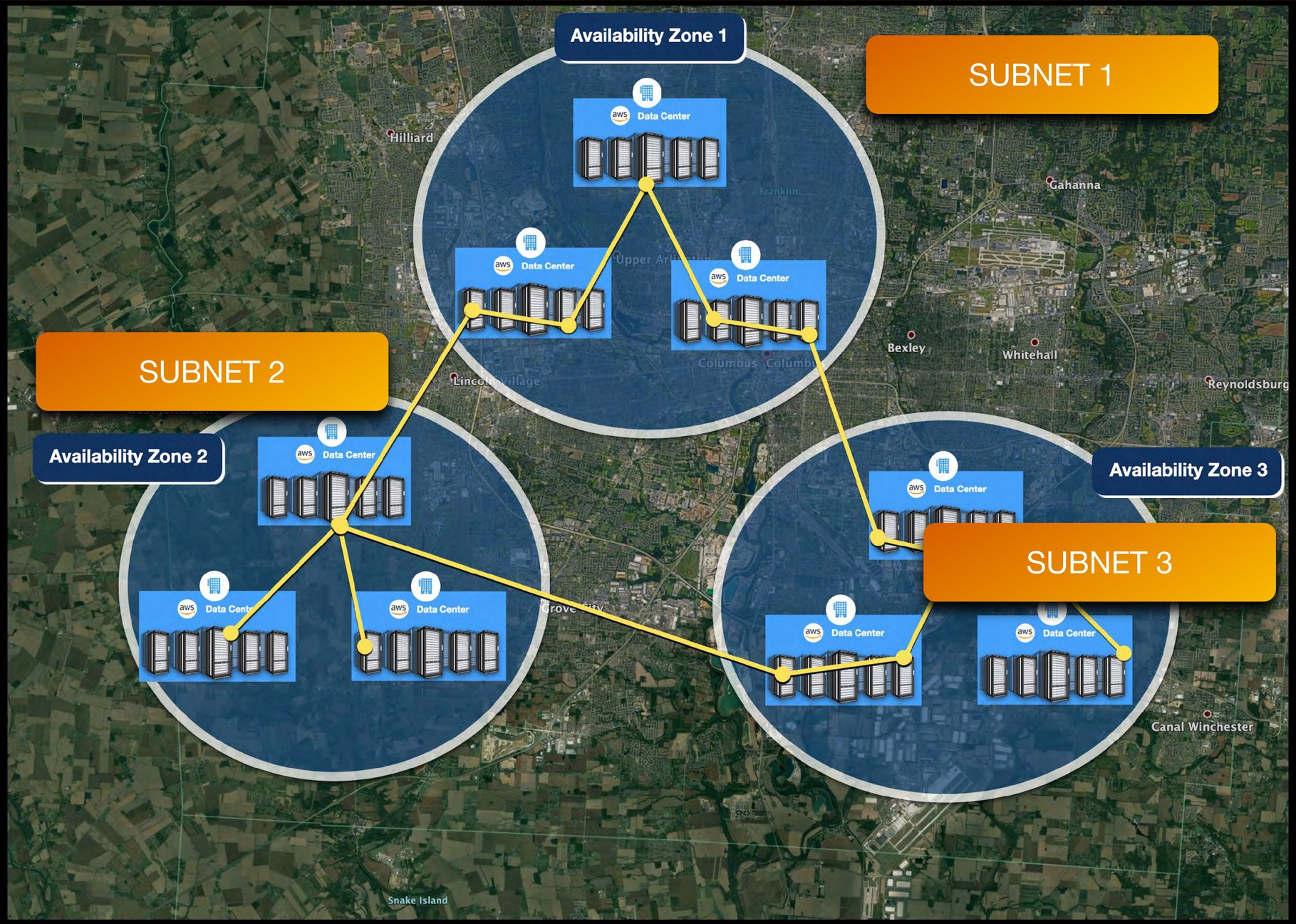
INTERNET GATEWAY

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

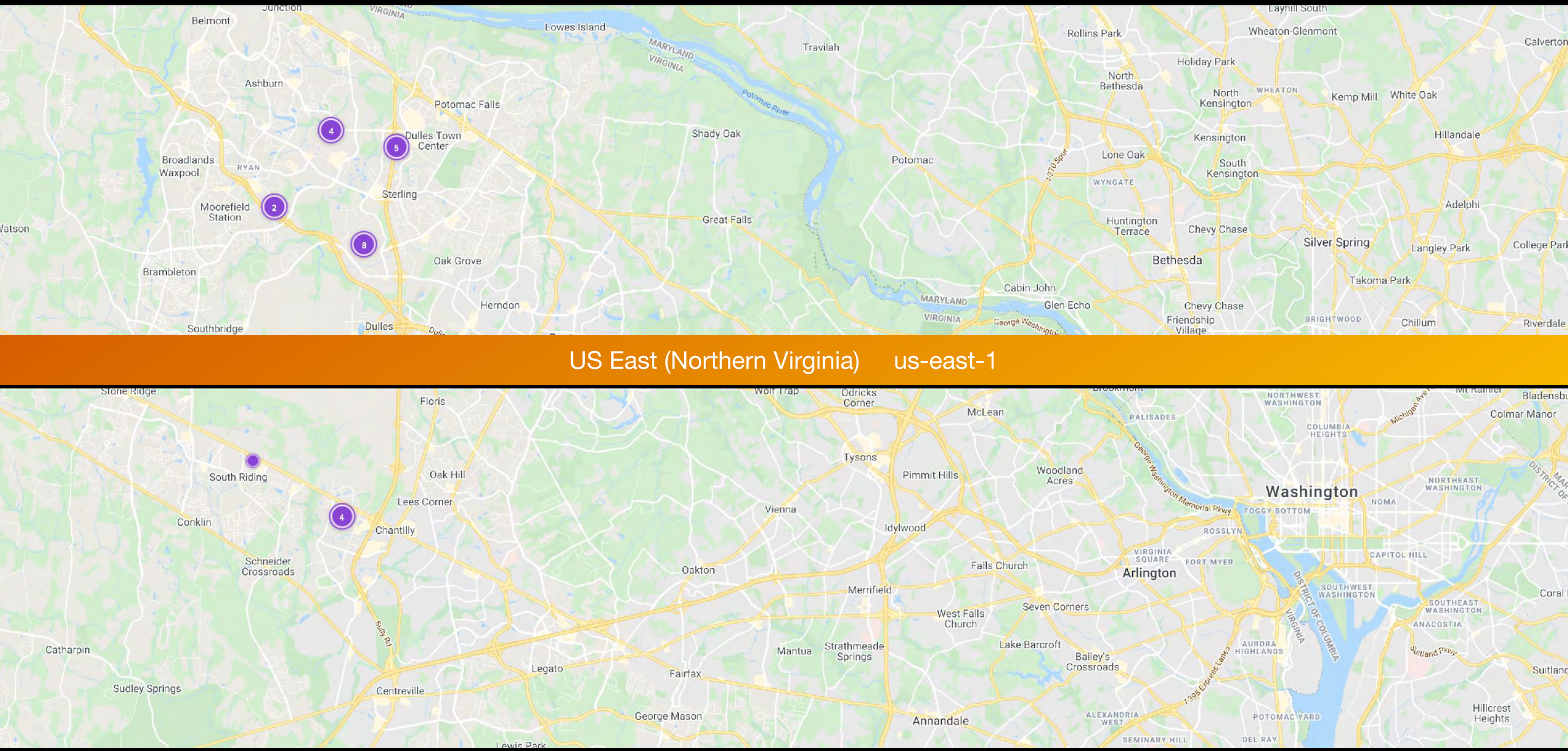


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

US East (Ohio) us-east-2



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



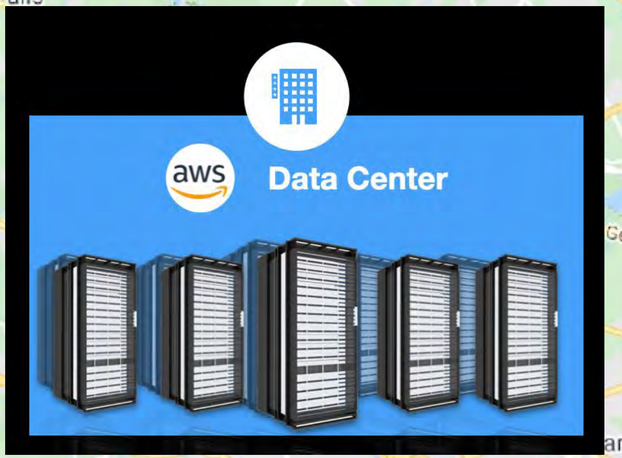
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

US East (Northern Virginia) us-east-1

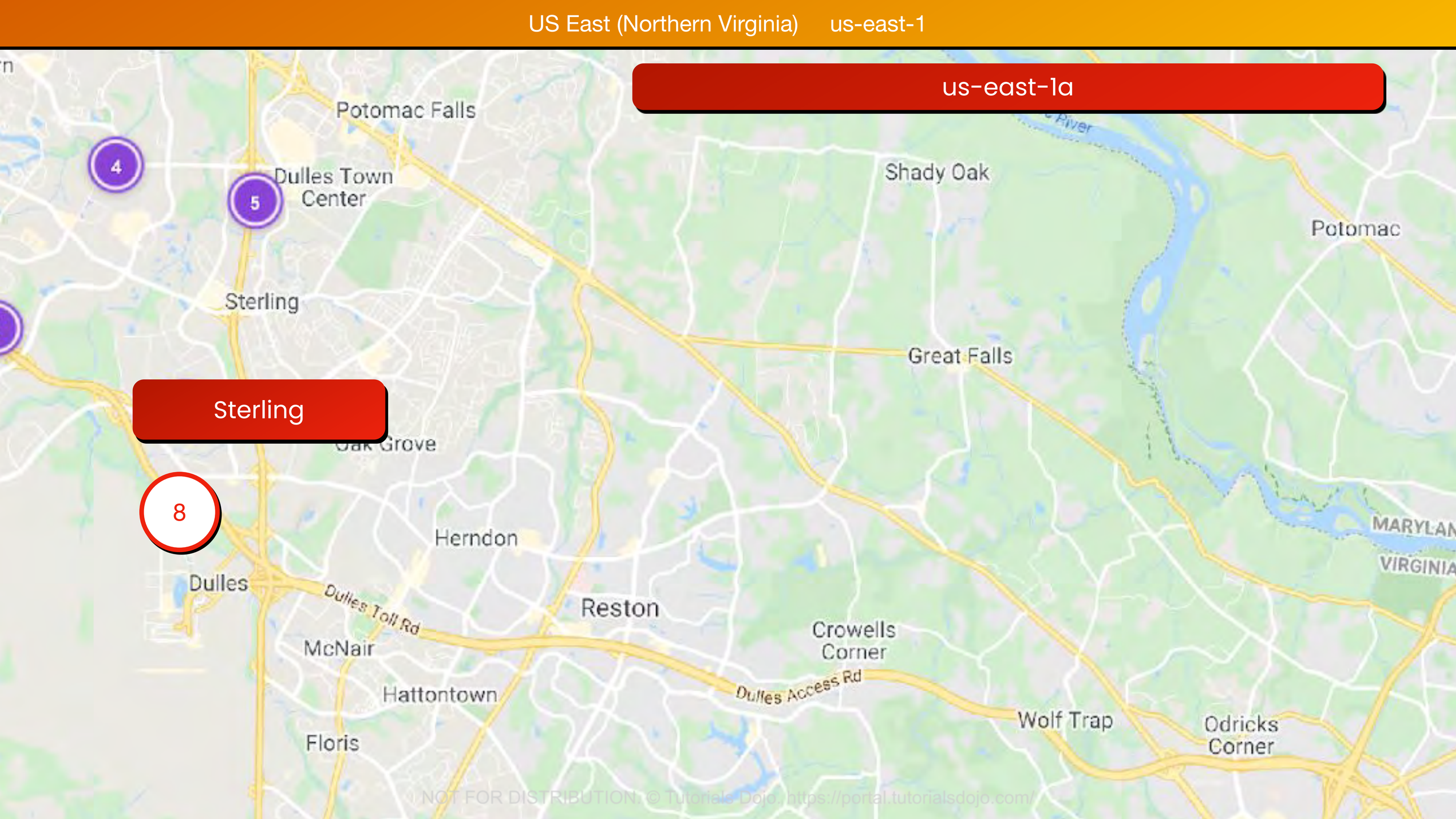
us-east-1b 4

us-east-1a 8

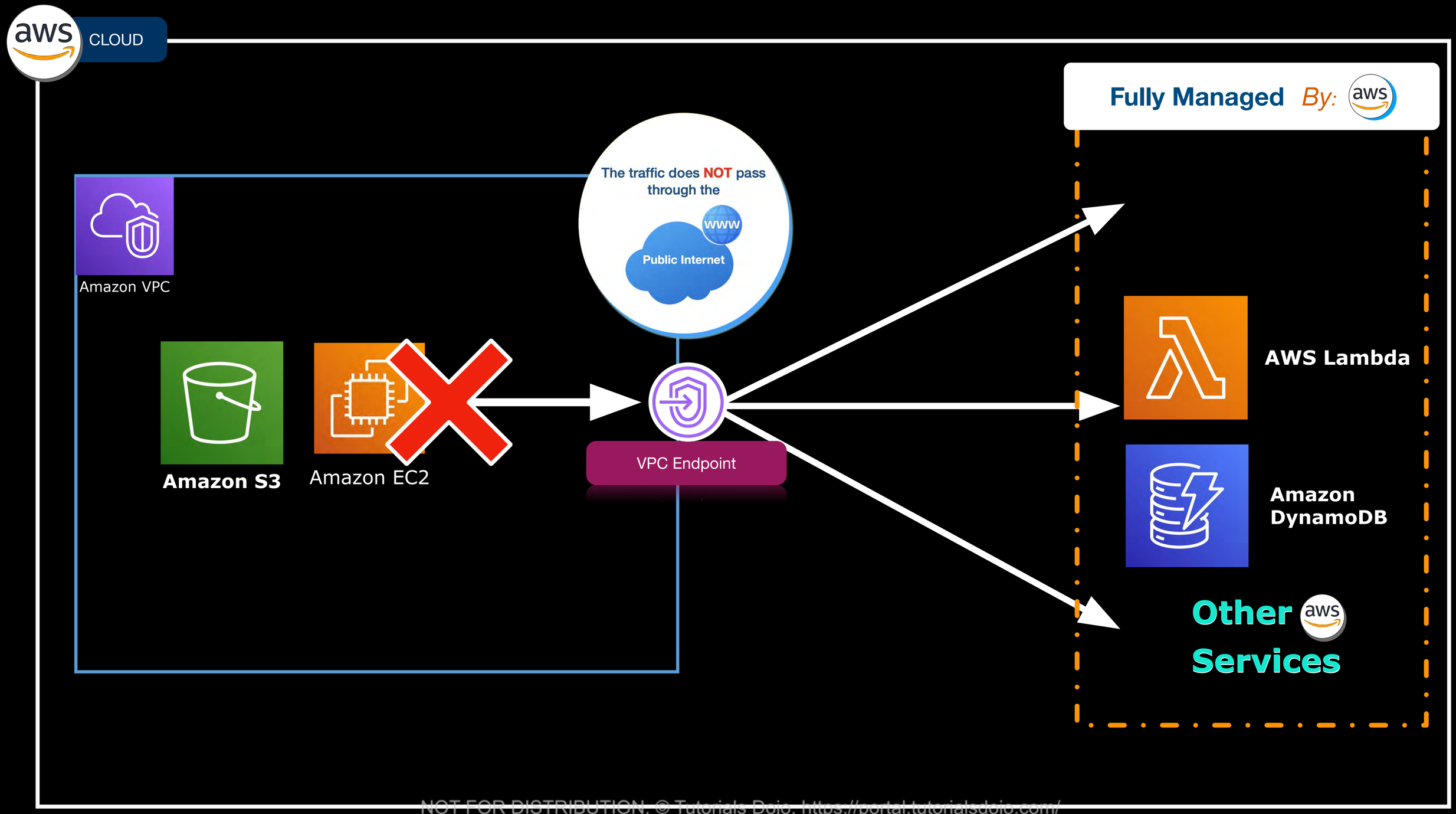
us-east-1c 4



NOT FOR DISTRIBUTION. © Tutorials Dojo https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon VPC
Components

- CIDR Block
- Subnets
- Route Table
- DHCP Options Set
- NAT Devices
- Network ACLs
- Security Groups
- Different types of Gateways

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CIDR BLOCK

- Allows you to specify the **size** of your network
- The allowed block size for a VPC is between **/16 to /28 netmask**
- A netmask (subnet mask) tells you the **total number of available hosts** for your network

/16	= **65,536** IP addresses
/17	= **32,768** IP addresses
/18	= **16,384** IP addresses
/28	= **16** IP addresses

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CIDR BLOCK

- AWS reserves a total of **5 IP addresses** from your CIDR block
- The **first four IP addresses** and the **last IP address** in each subnet CIDR block are reserved

CIDR `10.0.0.0/24`

`10.0.0.0`	– Network Address
`10.0.0.1`	– VPC Router
`10.0.0.2`	– DNS Server
`10.0.0.3`	– Reserved for Future Use
`10.0.0.255`	– Network Broadcast Address

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CIDR BLOCK

IPv4 CIDR Range:	`10.0.0.0/16`
IPv6 CIDR Range:	`2001:db8:1234:1a00::/56`

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- The **implicit router** in Amazon VPC
- **Controls the network traffic** in your VPC through subnet routing
- All subnets in your VPC must be associated with a route table.
- A route table can either be the **main route table or a custom route table**
- A subnet in your VPC can only be associated with one route table at a time but you can associate multiple subnets with the same subnet route table.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DHCP OPTIONS SET

- A set of options that **controls the automatic provisioning of IP addresses** to your Amazon EC2 instances and other resources
- Uses the **Dynamic Host Configuration Protocol**
- Allocates an IP address to every host, virtual machine, EC2 instance, RDS database, load balancer, or any other AWS resources in your VPC
- Configures your DNS, NetBios Name Server, and Network Time Protocol (NTP)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



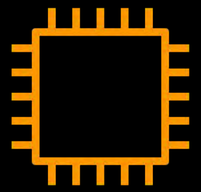
NAT DEVICES

- Uses **Network Address Translation (NAT)**
- Enable Amazon EC2 instances that are in a private subnet to connect to the public Internet or other AWS services
- **Prevents the public Internet from initiating connections** with your private EC2 instances.
- Works like a **one-way street** which means only the traffic initiated within your VPC is allowed but not vice versa

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NAT DEVICES



NAT Instance

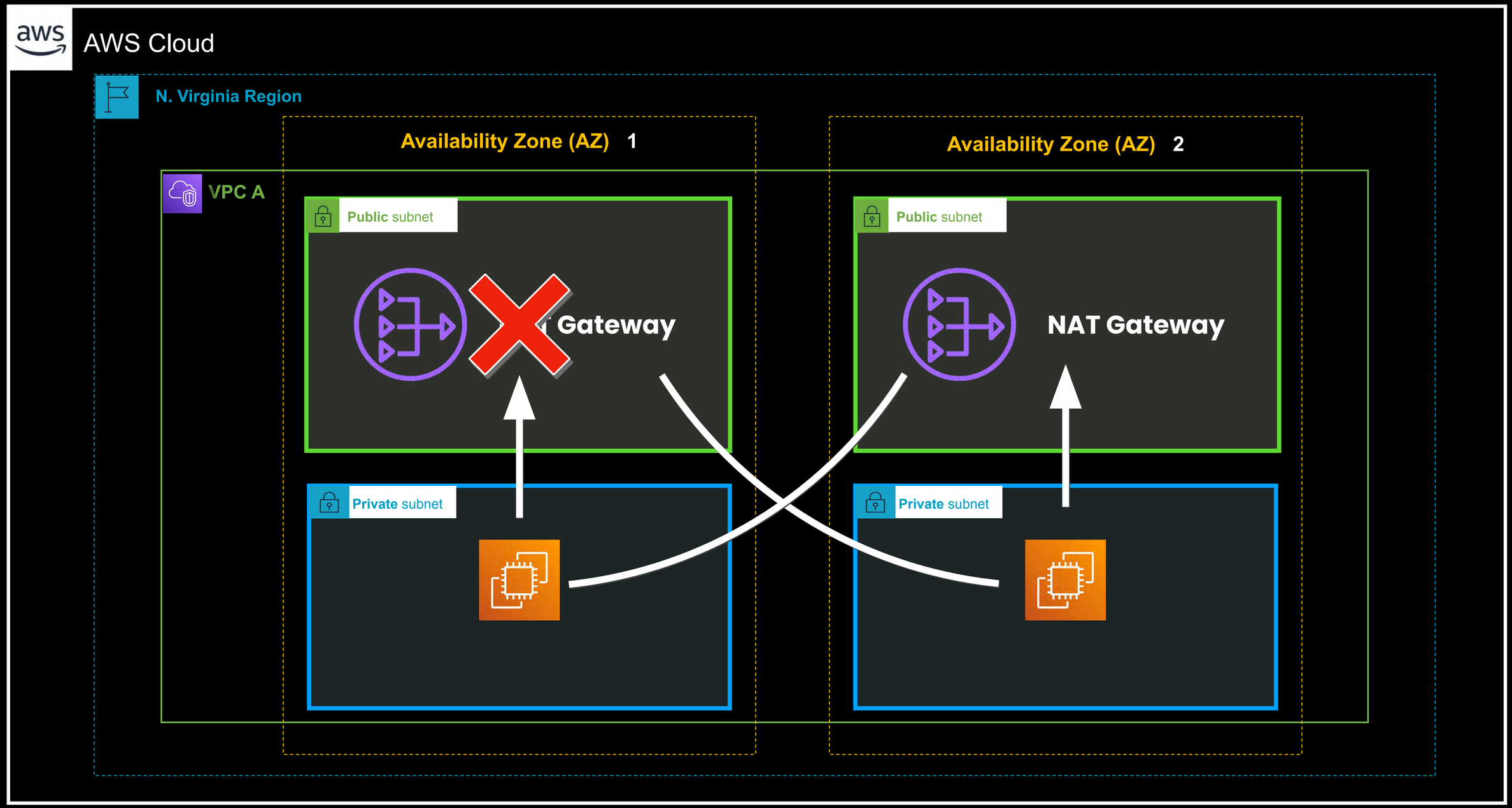
- A virtualized NAT device running in an EC2 instance within your VPC
- Managed by the customer (you)
- Not highly available nor scalable



NAT Gateway

- An advanced NAT device that is not running in your VPC
- Managed by AWS
- Highly available and scalable

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

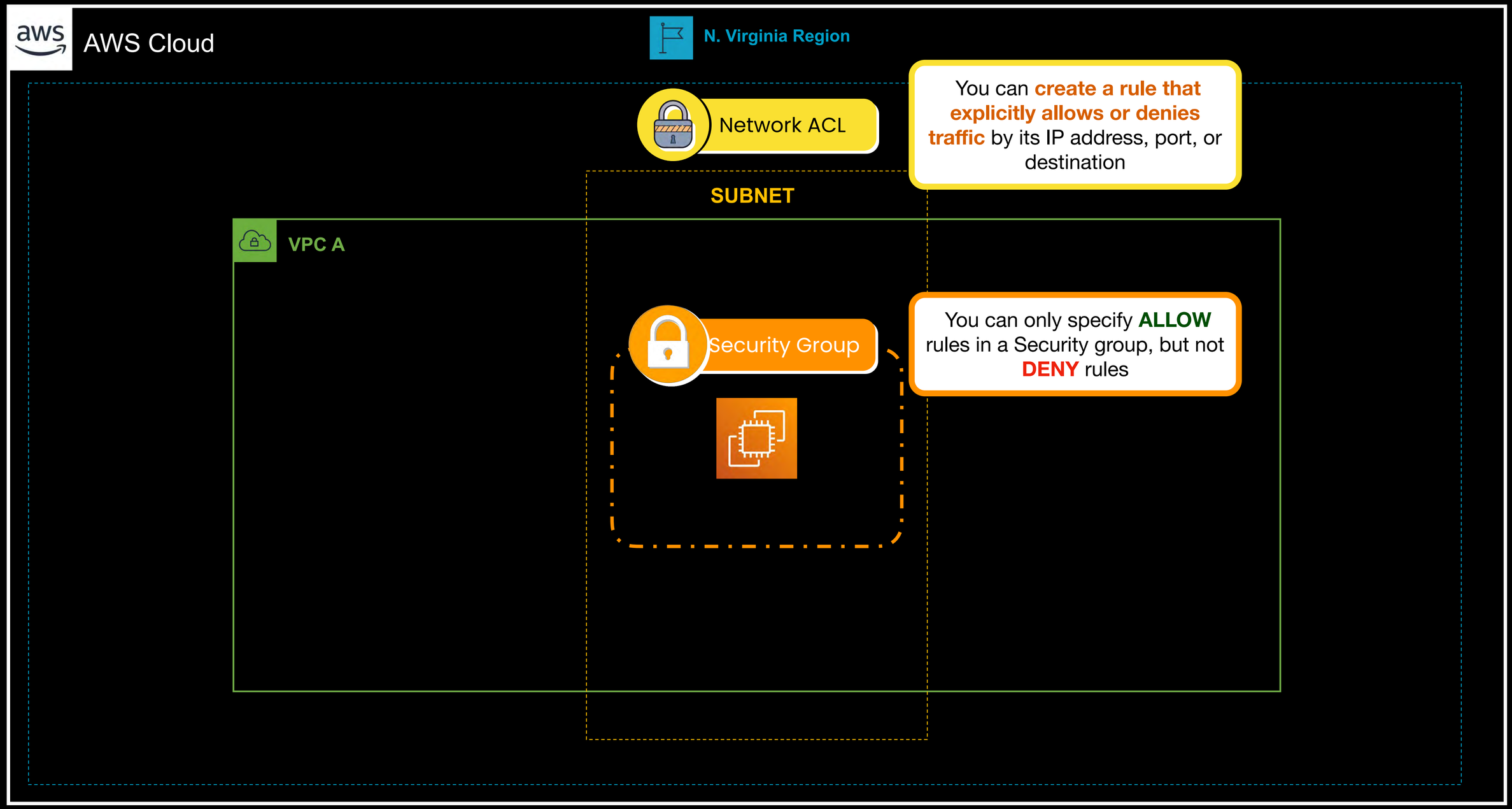


Security Groups

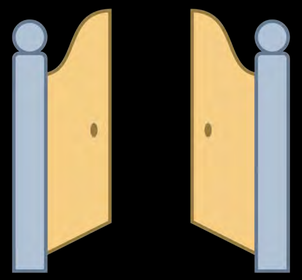


Network Access Control List
(Network ACL)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



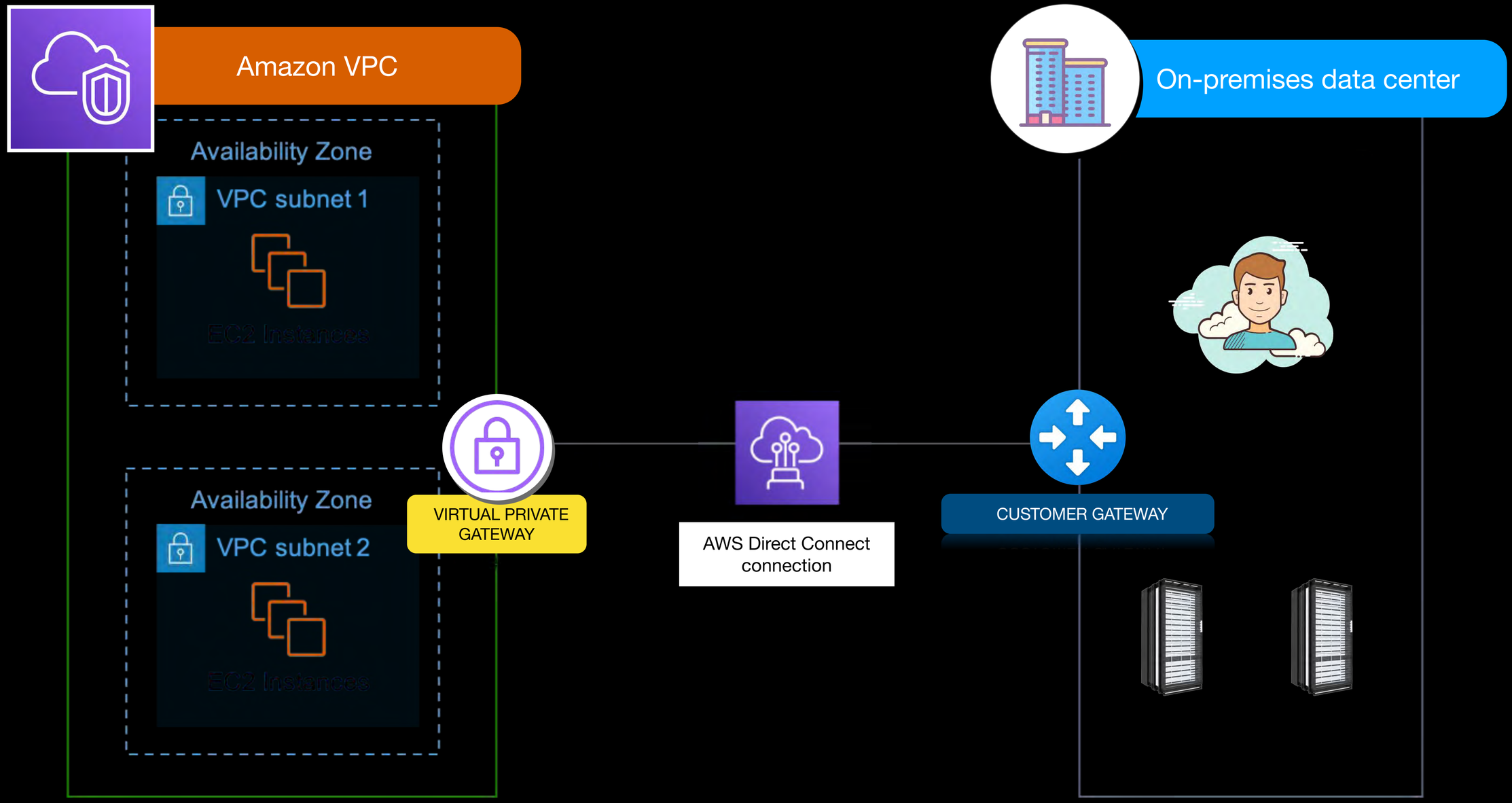
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Gateways

- Internet Gateway
- Customer Gateway
- Virtual Private Gateway
- Carrier Gateways
- Egress-only Internet Gateway

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



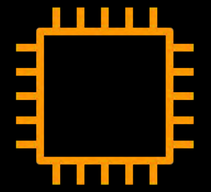
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

IPv6

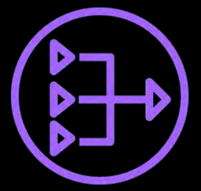
IPv4



Egress-only Gateway



NAT Instance



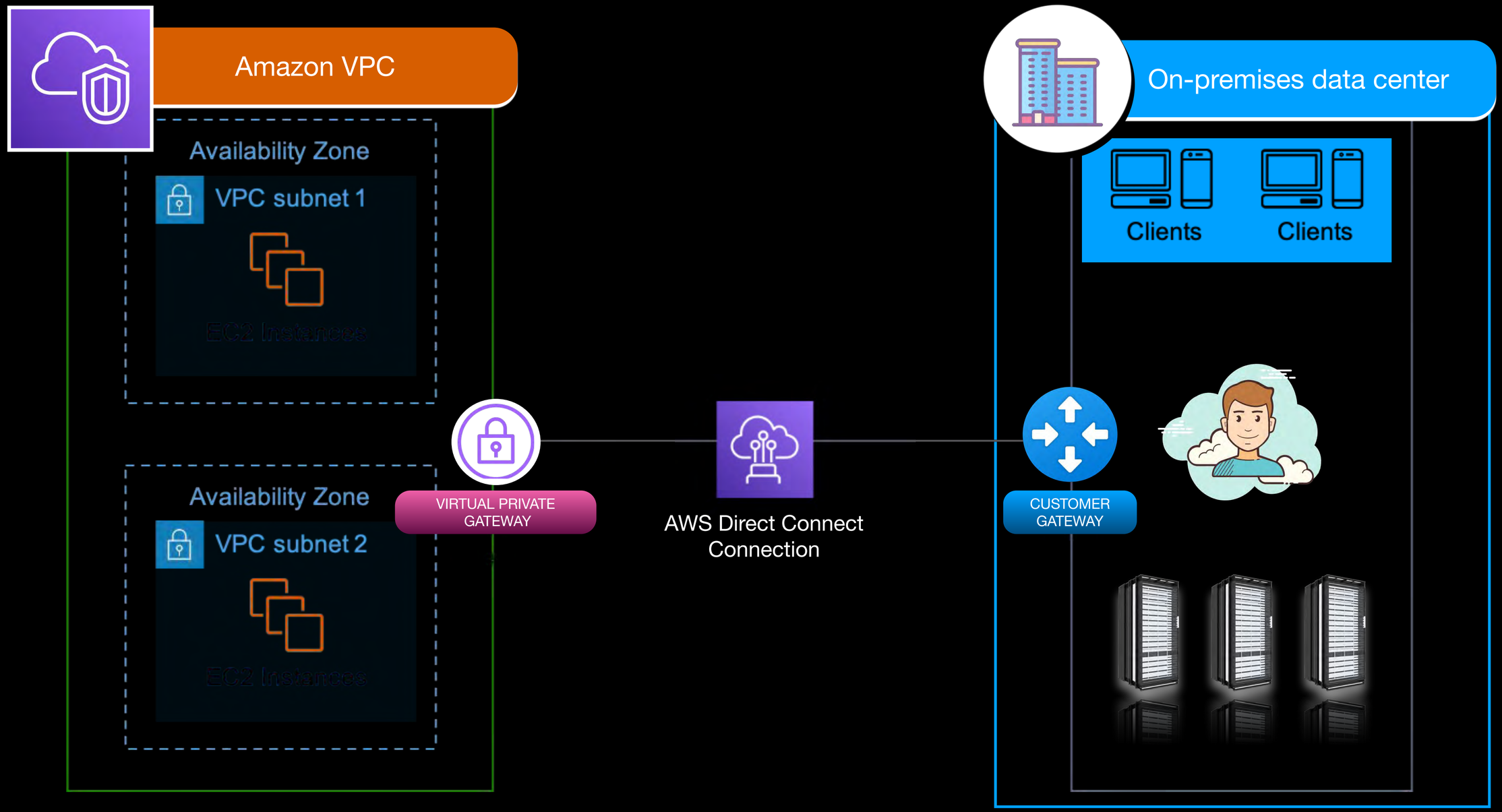
NAT Gateway

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- For VPCs that use **AWS Wavelength** to deliver ultra-low latency applications for 5G devices.
- Allows incoming traffic from a carrier network in a specific location
- Allows outgoing traffic to the carrier network and to the public Internet.
- Only available for VPCs that contain subnets in a **Wavelength Zone**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

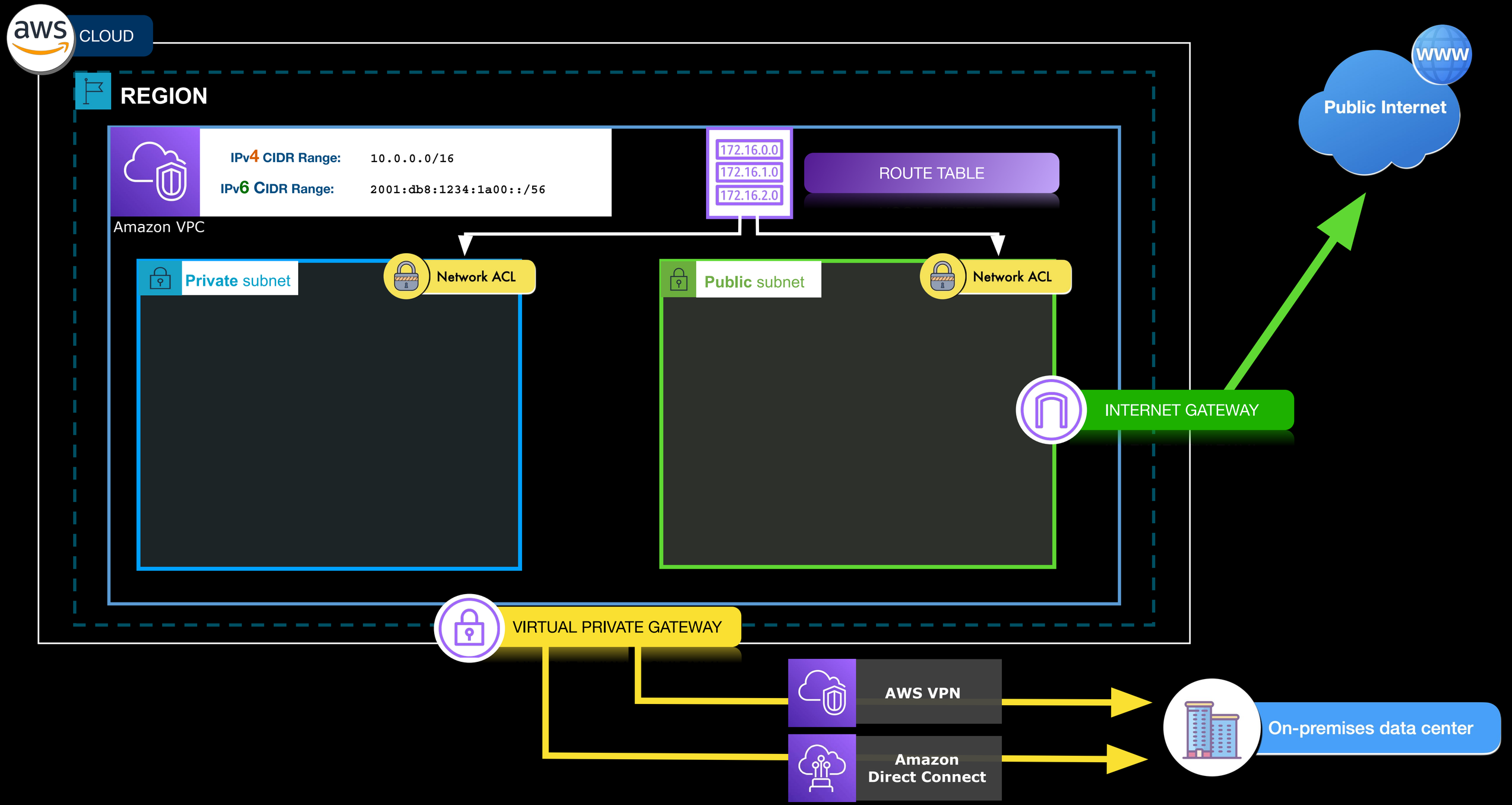


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon VPC Network Architectures

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- There is a default VPC **in each AWS Region**
- A default VPC can immediately be used to launch your Amazon EC2 instances, Elastic Load Balancers, Amazon RDS databases, and other resources.
- Perfect for quickly launching simple public websites or applications
- The existing components of your default VPC **can be configured**
- Has an attached **Internet Gateway** by default

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Default VPC

IPv4 CIDR Range: `172.31.0.0/16`

/16

= **65,536** IP addresses

`172.31.0.0` – **Network Address**

`172.31.0.1` – **VPC Router**

`172.31.0.2` – **DNS Server**

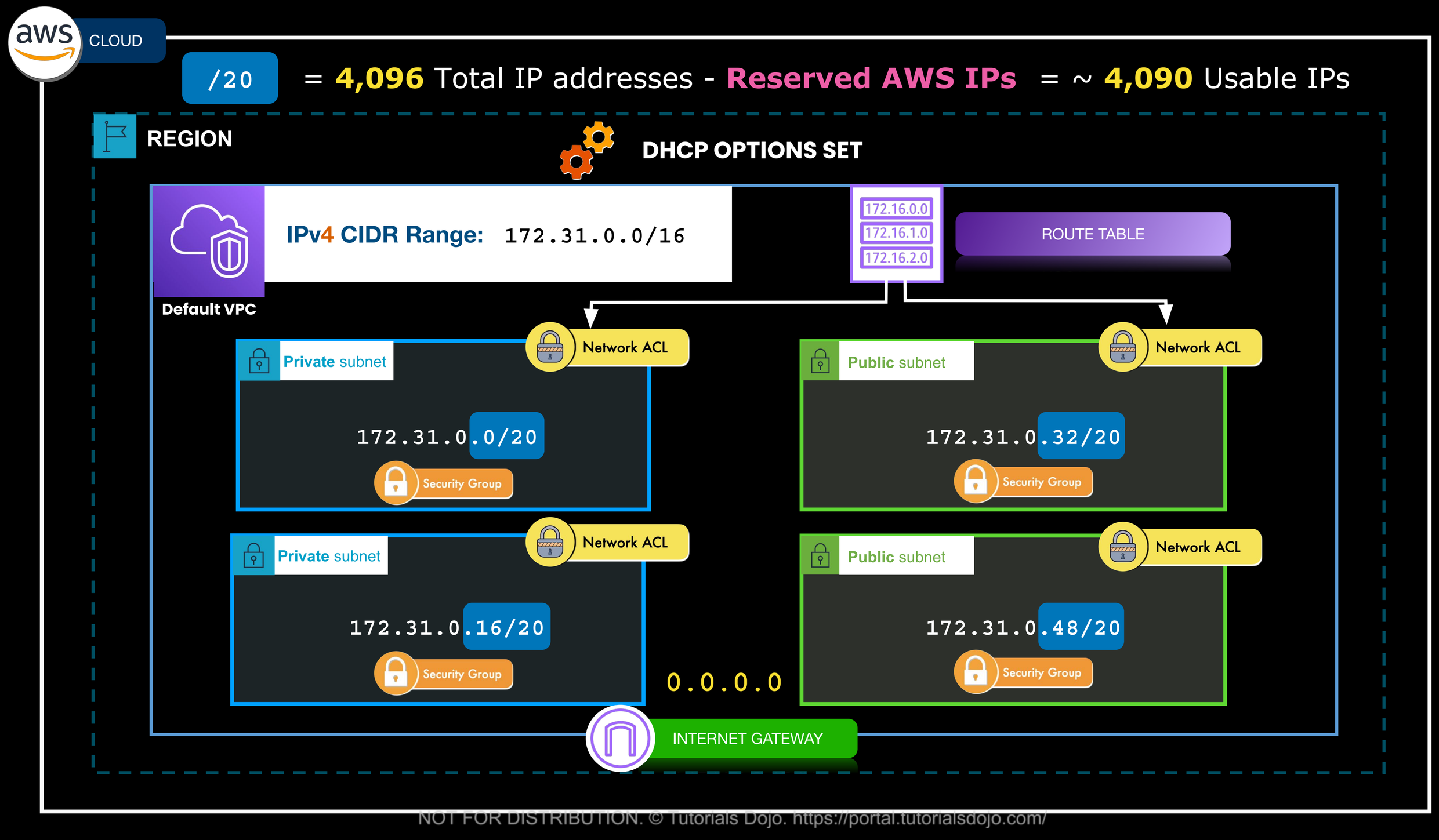
`172.31.0.3` – **Reserved for Future Use**

`172.31.0.255` – **Network Broadcast Address**

The first 4 IP addresses and the last IP address of that range are reserved.

You have a total of **5 IP addresses** that are not usable

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

CUSTOM AMAZON VPC



/28 = **16** Total IP addresses - **5 Reserved AWS IPs** = **11** Usable IPs

IPv4 CIDR Range: 10.0.0.0 /28

172.16.0.0
172.16.1.0
172.16.2.0

ROUTE TABLE

Private subnet

Auto Scaling group

EC2 EC2 EC2 EC2 EC2 EC2

Auto Scaling group

EC2 EC2 EC2 EC2 EC2

Tutorials Dojo
www.tutorialsdojo.com

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon VPC

Network Architecture Types

- A VPC with a single **public** subnet
- A VPC with **public** and **private** subnets
- A VPC with **public** and **private** subnets and **Hardware VPN Access**

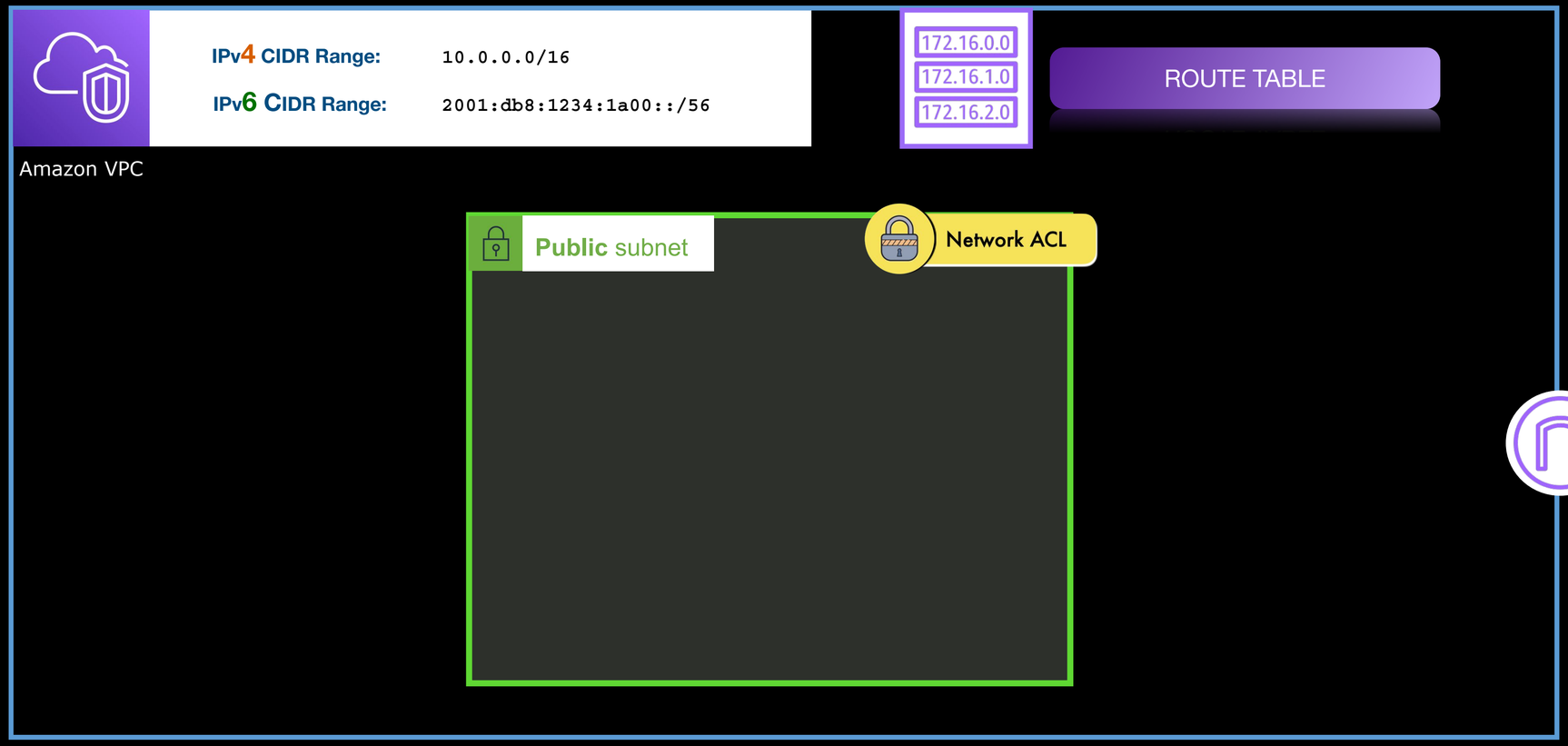


- A VPC with a **private** subnet only and **Hardware VPN Access**



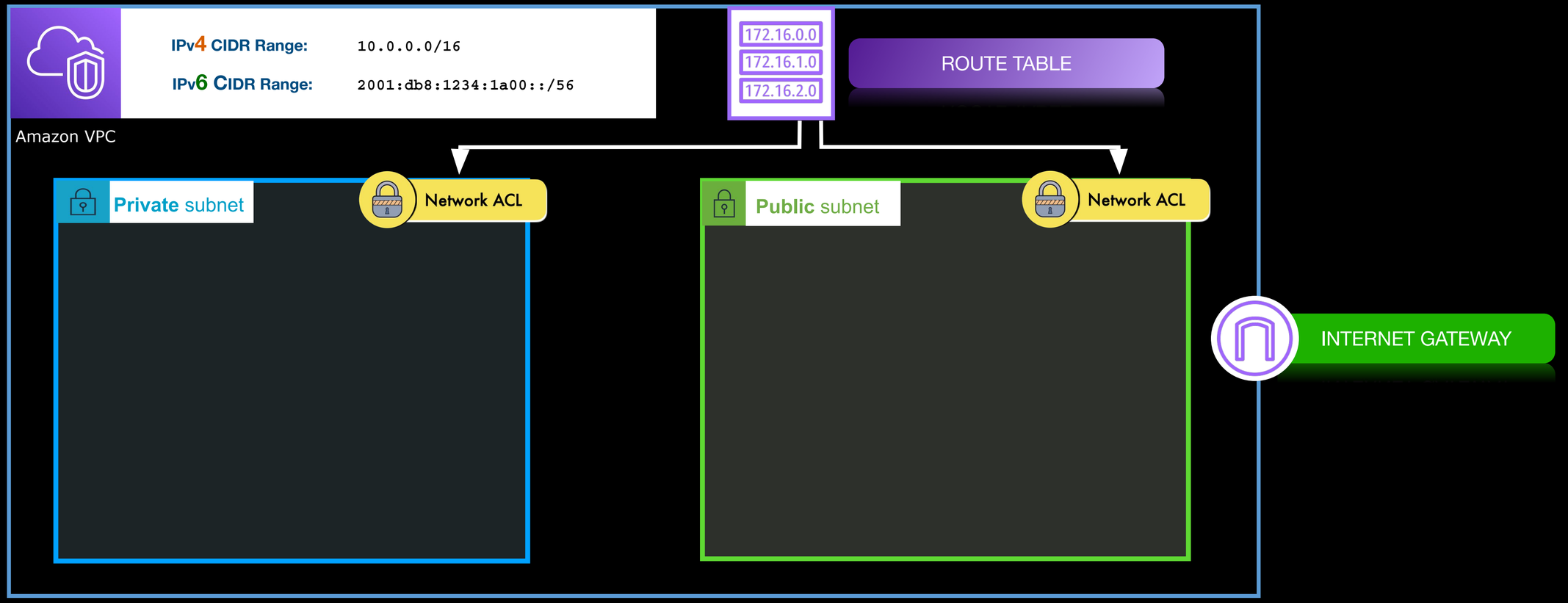
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

A VPC with a single public subnet



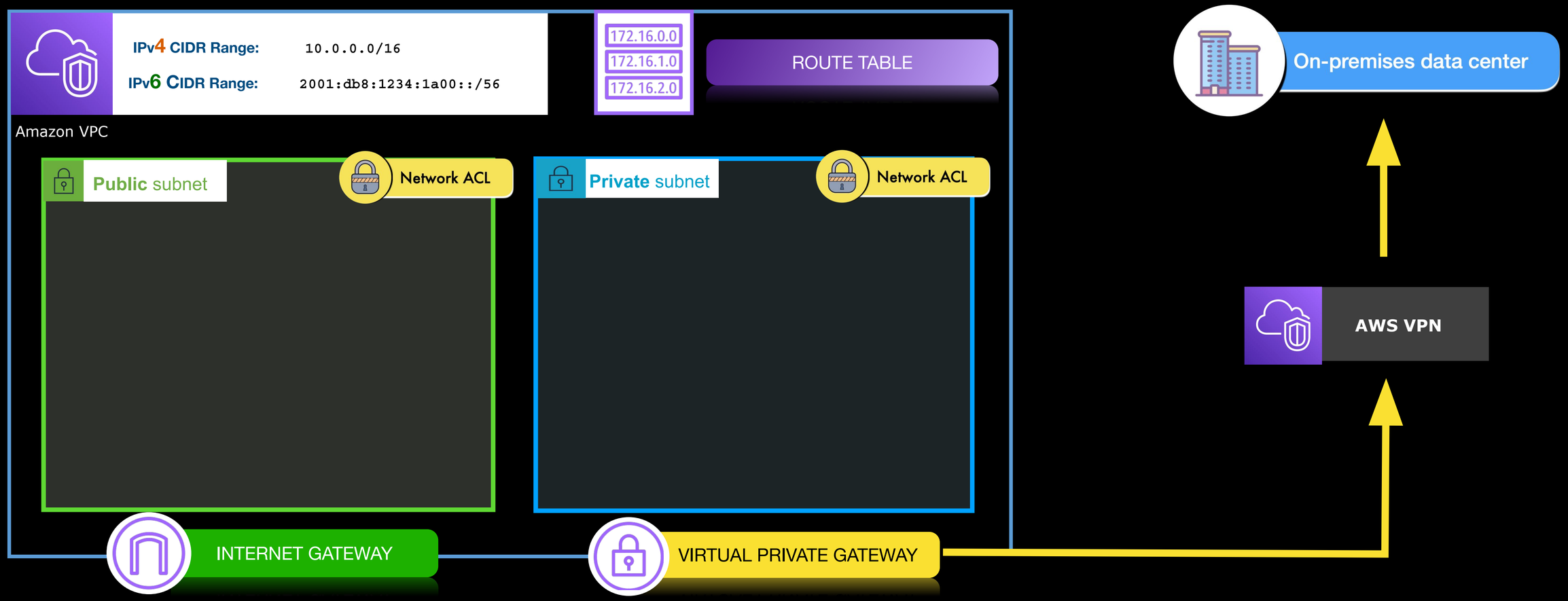
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

A VPC with public and private subnets



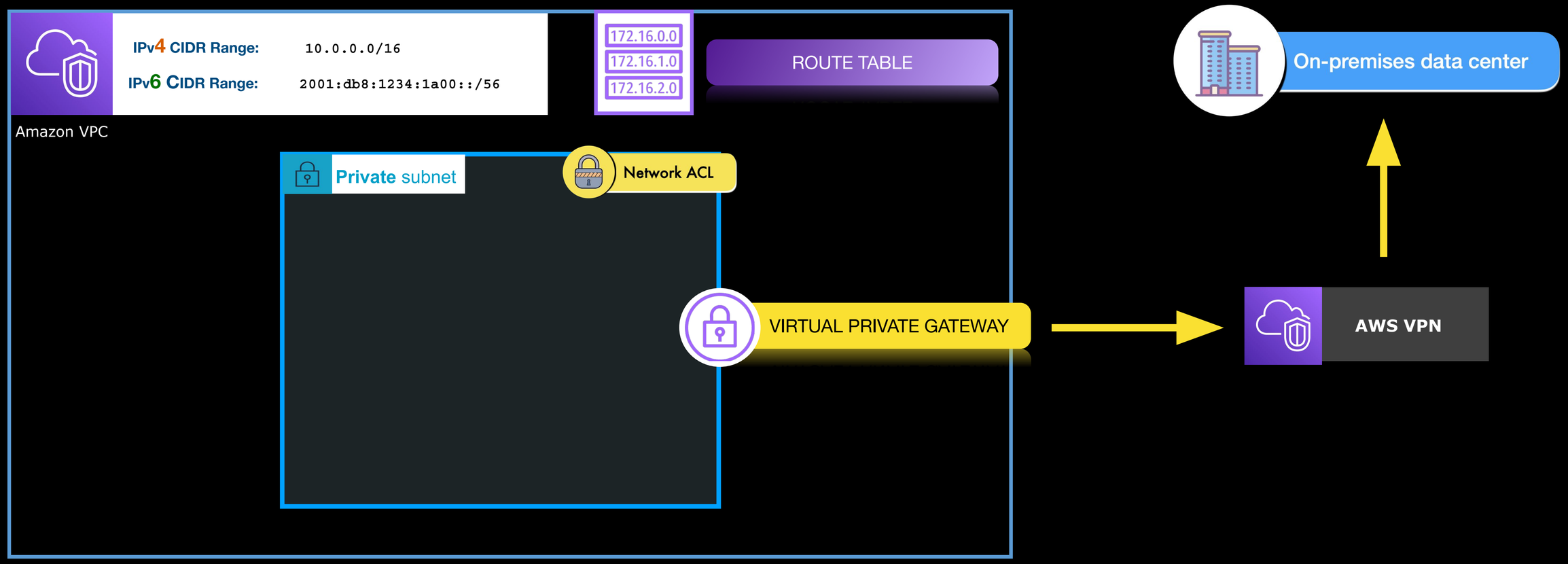
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

A VPC with public and private subnets and Hardware VPN Access

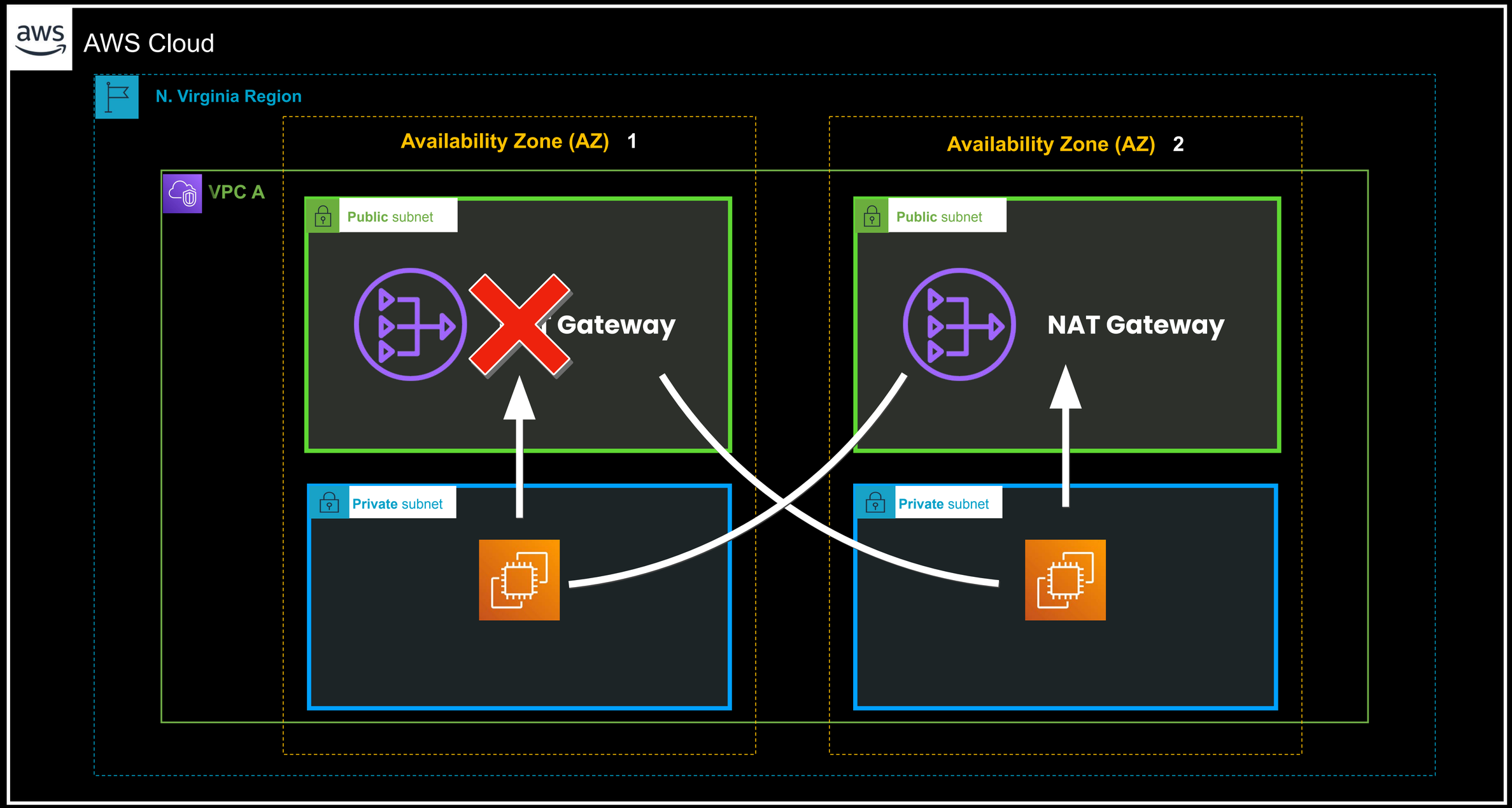


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

A VPC with private subnet and Hardware VPN Access



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Route 53 Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- A global **Domain Name System (DNS)** service
- Provides different **Routing Policies**

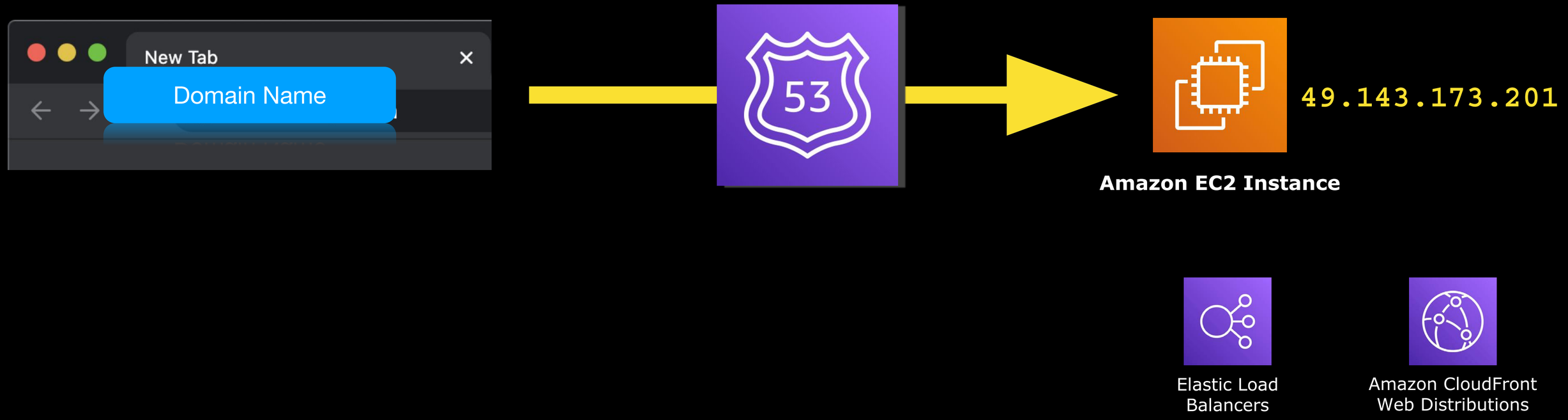


- Allows you to **register your own domain name**
- Transfer a domain from another domain registrar
- Create **health checks**



- Route **traffic flows**
- Configure **DNS resolvers**
- . . . and many more!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



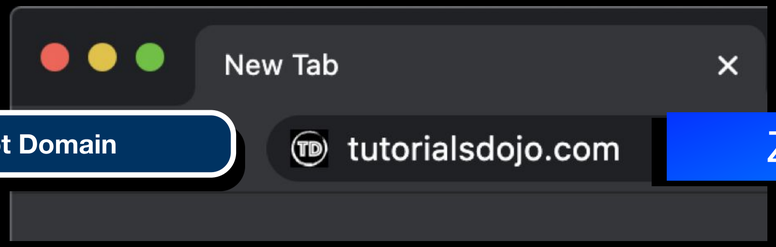
DNS Spoofing Attacks



DNSSEC
DNS Security Extensions



Man-In-The-Middle Attacks



Root Domain

Zone Apex

- The "**apex**" (summit) of the Hosted **Zone**
- Also known as **Naked Domain**

Subdomains

Hosted Zone

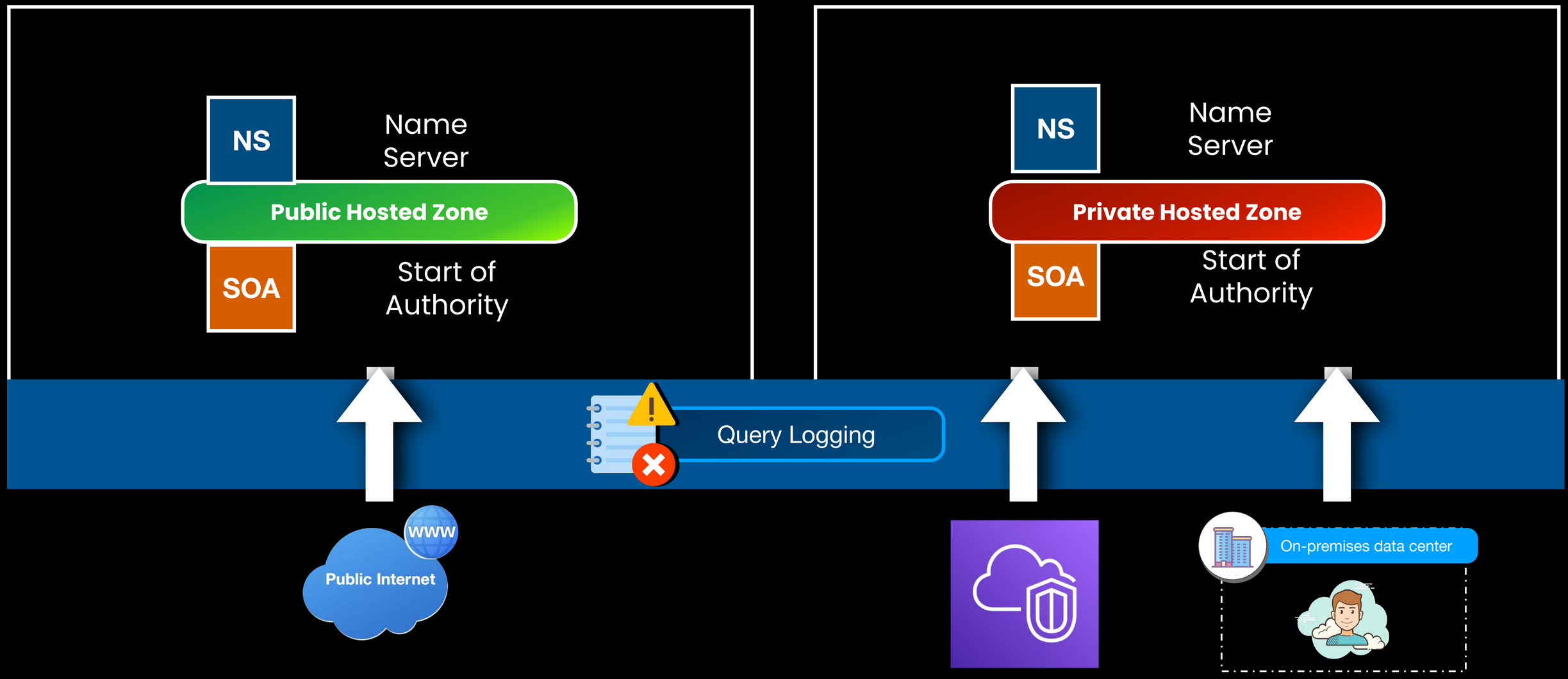
www.tutorialsdojo.com

portal.tutorialsdojo.com

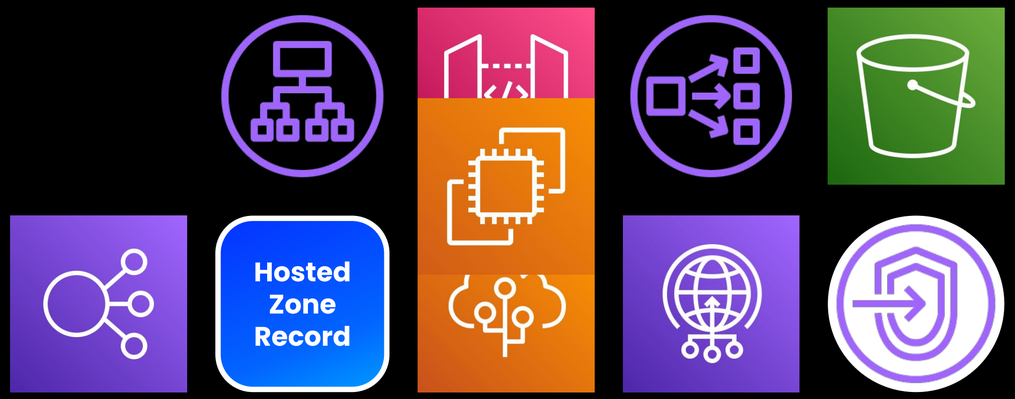
cebu.tutorialsdojo.com

bengaluru.tutorialsdojo.com

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



49.143.173.201

ALIAS RECORD

- Route traffic to selected **AWS resources**
- Works like a **CNAME** (Canonical Name) Record
- Not visible to DNS resolvers
- Points to a **specific AWS resource**

NON-ALIAS RECORD

- Allows you to specify the **IP addresses or the custom domain names** of your servers or resources
- Visible to DNS resolvers
- Points to a **particular IP address**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DNS RECORD TYPES

ALIAS

A — **IPv4** Host Address

ALIAS

AAAA — **IPv6** Host Address

NS — Name Server

SOA — Start of Authority

CNAME — Canonical Name

MX — Mail Exchange

TXT — Tex t

PTR — Pointer

SRV — Service Locator

SPF — Sender Policy Framework

NAPTR — Naming Authority Pointer

CAA — Certification Authority Authorization

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

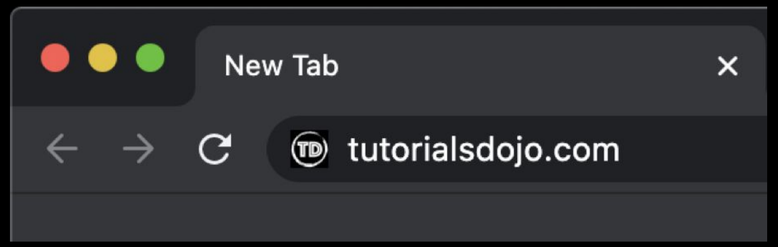
A — **IPv4** Host Address

AAAA — **IPv6** Host Address

CNAME — Canonical Name



Root Domain / Zone Apex



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- **An open-source program** that you can use as a fully customizable domain name server
- Usually launched by companies as their **internal DNS service**
- Stands for **Berkeley Internet Name Domain** server
- Has a **BIND DNS forwarder** that allows you to resolve the domain names in the private hosted zones in AWS from your on-premises network
- Can be migrated to Amazon Route 53 by **importing the BIND zone file**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ACTIVE

Live Traffic

PASSIVE

Failover

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ACTIVE ACTIVE

- **Improves fault tolerance and performance** of your applications
- Entails **additional cost**
- Has **several active environments** that accepts live production traffic
- Ensures the high availability and resiliency of your global applications
- Can be implemented by using a single policy, or a combination of routing policies such as:

Latency

Geolocation

Geoproximity

Multivalue Answer

Weighted

...other routing types!

ACTIVE PASSIVE

- Provides a **basic fault tolerance**
- More **cost-effective** than ACTIVE ACTIVE
- Has **one active environment** and one backup environment on standby
- Primarily implemented by using the:



Failover Policy

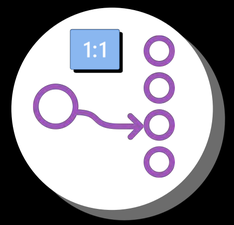
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Route 53
Routing Policies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ROUTE 53 ROUTING POLICY TYPES



SIMPLE



GEOLOCATION



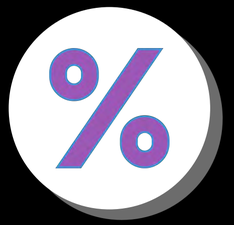
LATENCY-BASED



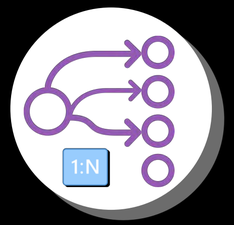
FAILOVER



GEOPROXIMITY

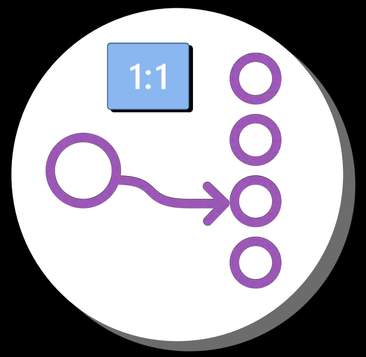


WEIGHTED



MULTIVALUE ANSWER

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

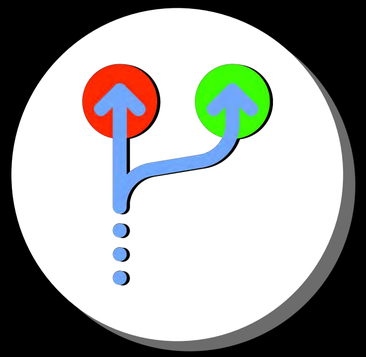


SIMPLE

- Routes to **a single resource**
- Example:
  - Routes all traffic from the `tutorialsdojo.com` apex domain to an NGINX web server, which is running on a **single Amazon EC2 instance**
- **Does not have a health check**
- **Establishes a one-to-one relationship** between the DNS record and the target

1:1

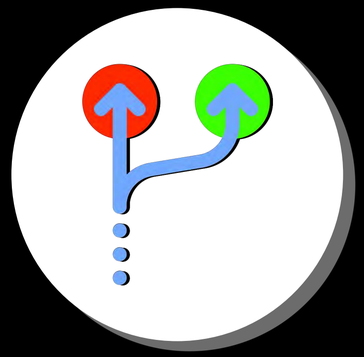
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



FAILOVER

- Primarily used to set up an **active-passive failover** for your network architecture
- Consists of 2 Failover record types:
  - **Primary** records
  - **Secondary** records
- Suitable if you want to automatically **redirect the incoming requests to a backup website** in the event that your primary site goes down

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



FAILOVER

USE CASES

- Also applicable for **setting up a static S3 website as a failover site**:
  - Set up a backup website that shows an announcement, a contact number, or a piece of information for your users
  - Host the backup website using the Amazon S3 static website hosting
  - Use the Failover Routing Policy to **automatically route incoming requests to the static S3 website if the primary website goes down**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOLOCATION

- Leverages on Amazon Route 53's capability to **detect the geographical location where the DNS queries originated**
- Lets you choose the specific resources that serve incoming traffic **based on the geographic location of your users**
- A single geolocation record is only **mapped to one continent or to a specific country**
- **Maps the client IP addresses to the geographical areas** using EDNS0 (Extension Mechanisms for DNS version 0)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOLOCATION

- Allows you to **ensure that each user location is consistently routed to the same endpoint**
- **Enables you to localize your content** and present the partial or entire content of your application in the respective language of your users
- Can **restrict the distribution of your content to certain locations only**, in which you have distribution rights

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOLOCATION

USE CASES

- Routing the traffic based on the **geographic location or region of your clients**
- For example, you have a web application hosted in multiple Amazon EC2 instances across different AWS Regions:
  - Application content is specifically associated with each geographic region
  - **User requests need to be routed to the correct EC2 instance that hosts the content for the appropriate region**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOLOCATION

USE CASES

- If your company has **legal distribution rights to digital content**
  - The digital content is hosted in an online content repository that is behind multiple Application Load Balancers across different AWS Regions
  - Your company holds various distribution rights for its content around the world
  - Need to ensure that the **users are properly served the right content without violating distribution rights**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOLOCATION

USE CASES

- For scenarios where you have **multiple environments that are hosted in different AWS Regions**
- Geolocation Policy provides **multi-region support for your application** to a certain degree

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOLOCATION

LIMITATIONS

- **Not fully capable of providing low-latency** and high performance to your users around the world and not just for several AWS Regions. Use Amazon CloudFront instead

- **Cannot dynamically shift traffic** from AWS resources in one region to another. If you need this feature, use this policy instead:



GEOPROXIMITY

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOPROXIMITY

- Similar to the  **GEOLOCATION** policy with notable differences:
  - It concentrates on the **proximity of the resource in a given geographic** area rather than its exact location
  - It **uses the Traffic Flow** feature of the Amazon Route 53 service
  - Uses a **BIAS** in shifting traffic to your AWS service

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOPROXIMITY

- Enables you to **keep track of all of the relationships among the records** in your Route 53 console
- Its **Traffic Flow feature simplifies the process of creating and maintaining your DNS records** for your extensive and complex configurations
- **The use of Traffic Flow is mandatory** if you want to implement geoproximity routing

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOPROXIMITY

- Allows you to **specify a bias in order to shift traffic** from your resources in one region to another region
- **Provides an option to shift more or less traffic** to your AWS services in one geographical location based on the numerical value of your bias and the specific geographical coordinates that you define
- The coordinates are the **latitude and longitude of the Endpoint Location**
- The actual bias **depends on the number of AWS resources that you currently have** and how close these resources are to one another

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOPROXIMITY

USE CASES

- Example:
  - A web application needs to be accessible to users in multiple geographic locations
  - The web application is currently deployed in an Auto Scaling group of EC2 instances behind an Application Load Balancer
  - The company needs to **direct traffic to the EC2 instance in the closest Region** and have the ability to shift traffic from resources in one region to another.
- In this case, you have to **deploy your application in multiple AWS Regions and set the bias to control the traffic**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



GEOPROXIMITY

LIMITATIONS

- This policy is **not fully capable of reducing Internet latency** to your applications
- It can improve the performance of your applications but it is **not on par with the level that Latency-based routing policy provides**
- If your application is expected to have millions of users around the world, it is better to use Amazon CloudFront or the Global Accelerator service instead

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



LATENCY-BASED

- Suitable for companies that **have resources in multiple AWS Regions**
- Improves the performance of your application by **serving the requests from the AWS Region that provides the lowest latency**
- The latency between users and your AWS resources is entirely **based on the traffic between your users and the physical AWS data centers** that are scattered around the world

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



LATENCY-BASED

USE CASES

- **The latency is not always lower even if the user is in close geographic proximity to a specific region.** The underlying network bandwidth and other factors must be considered.

- The request will be **served on the AWS region with the lowest latency**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



LATENCY-BASED

USE CASES

- Your company has an enterprise web application that is **running on a multi-region architecture**
  - The application is hosted on three AWS Regions, where each region has an Auto Scaling group of EC2 instances with an Application Load Balancer in front
  - You have to configure Route 53 to effectively **distribute traffic between these regions**
  - Need to improve the performance of your application by **selecting the specific AWS Region that provides the lowest latency**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



LATENCY-BASED

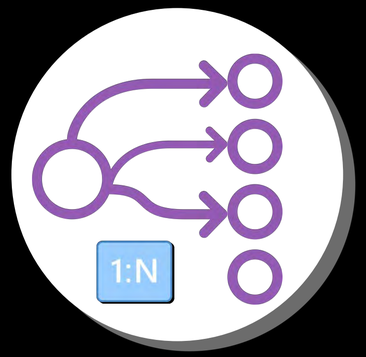
LIMITATIONS

- **Not entirely capable of shifting traffic from one region to another using a bias**. If you need this functionality, you have to use a different routing policy like:



GEOPROXIMITY

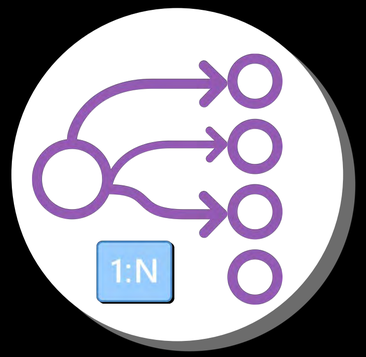
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



MULTIVALUE ANSWER

- Allows you to **configure a single Route 53 record to return multiple values** in response to DNS queries.
- Enables you to **add multiple IP addresses of your EC2 instances and map them to one DNS record**
- Can **route traffic to numerous resources** that can go up to eight active records or so, which are selected randomly

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



MULTIVALUE ANSWER

USE CASES

- Allows you to **configure an active-active failover for your network**
- Checks the health of each resource that you define to **ensure that Route 53 will route the live traffic to your healthy resources only**
- **Works like a load balancer** but not as powerful as a full-fledged elastic load balancer in AWS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



WEIGHTED

- Allows you to **route traffic to multiple resources in specific proportions** that you specify
- Acts as a load balancer that **routes requests to different records based on the relative percentage of traffic or weight** that you specified

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



WEIGHTED

USE CASES

- If you want to **route a small portion of your traffic to one resource and the rest to another resource**
  - You can specify the corresponding weights for each resource.
  - A “weight” in this policy is a **numerical value between 0 to 255**
  - If you specify 0, then Route 53 will stop responding to DNS queries using this record

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



WEIGHTED

USE CASES

- This is also **useful for migration activities**, such as blue/green deployment
- You can **shift the traffic to another resource partially or entirely by configuring the weight of each record**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3 Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3

- An **object storage** service
- S3 stands for **"Simple Storage Service"**
- **Highly durable, available & scalable** storage service
- Primarily **used to store static data** that does not change frequently
- Allows your files to be publicly available via the Internet

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



a set of name-value pairs



OBJECT

Highly scalable and allows you to store **virtually unlimited** amounts of files



BUCKET

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



BUCKET NAMING GUIDELINES

- The S3 bucket name is **globally unique**
- The namespace is **shared by all AWS accounts** around the world
- Example:
  - If you created an S3 bucket named "`tutorialsdojo`", then no other AWS user can **create a bucket with that same name**
  - If someone tries to create a new bucket called "`tutorialsdojo`", then that request will fail

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3 Folders and Prefixes

- Helps you organize or group your objects
- S3 has a **flat structure**
- The concept of a "folder" is not hierarchical unlike Amazon EFS
- Example:

Object key name

`tutorialsdojo/aws.jpeg`

Prefix | Filename



- Amazon S3 does NOT support POSIX, including:
  - Concurrent file modification
  - File system access semantics
  - File locking

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Cloud

N. Virginia Region

Automatically replicates your objects to **all Availability Zones** of the AWS region by default





Availability Zone (AZ) 2

Availability Zone (AZ) 3

YOUR VPC



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AVAILABILITY 99.99%

DURABILITY 99.999999999%

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

- The probability that an object remains intact and accessible after a period of one year



DURABILITY

100%	Absolutely no data loss per year
99%	1% chance of data loss per year
99.99%	**0.01%** chance of data loss per year
99.999999999%	0.000000001% chance of data loss per year or one lost data every 10 million years

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon S3 Storage Classes



S3 Standard

For **frequently accessed** data



S3 Intelligent-Tiering

For changing or
unknown access patterns



S3 Standard-IA
(Infrequent Access)



S3 **One** Zone-IA
(Infrequent Access)

For storing long-lived,
yet **less frequently accessed** data



S3 Glacier

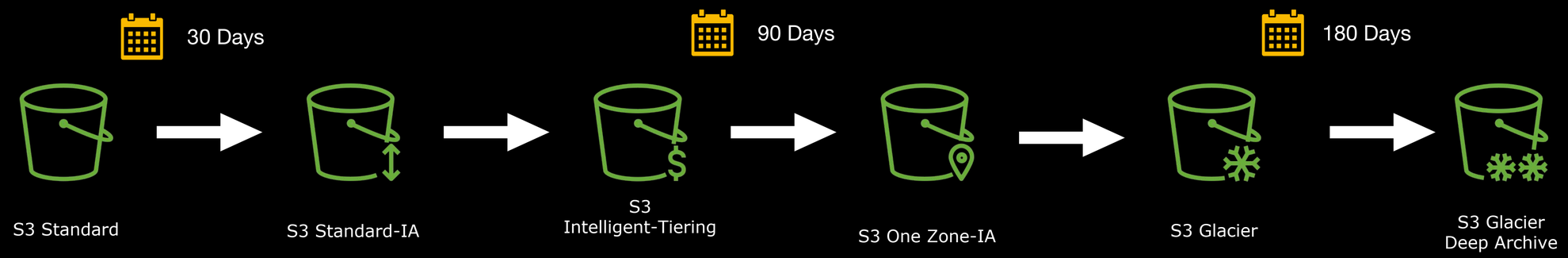


S3 Glacier **Deep** Archive

For **low-cost long-term storage**
and data archiving

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Lifecycle Policy



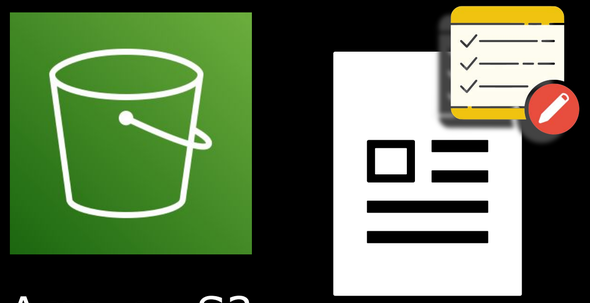
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



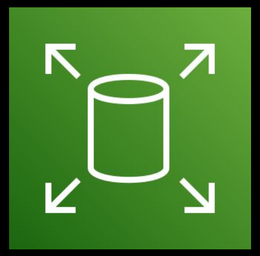
Static Website Hosting

- Launch a **static website** with HTML pages, downloadable packages, images, media files, or other **client-side scripts**
- **Cost-effective solution** for hosting your static websites with no server management required (serverless)
- **Cannot be used for running server-side scripts** such as PHP, JSP, ASP.NET etc…

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3

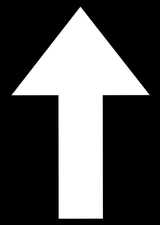


Amazon EBS

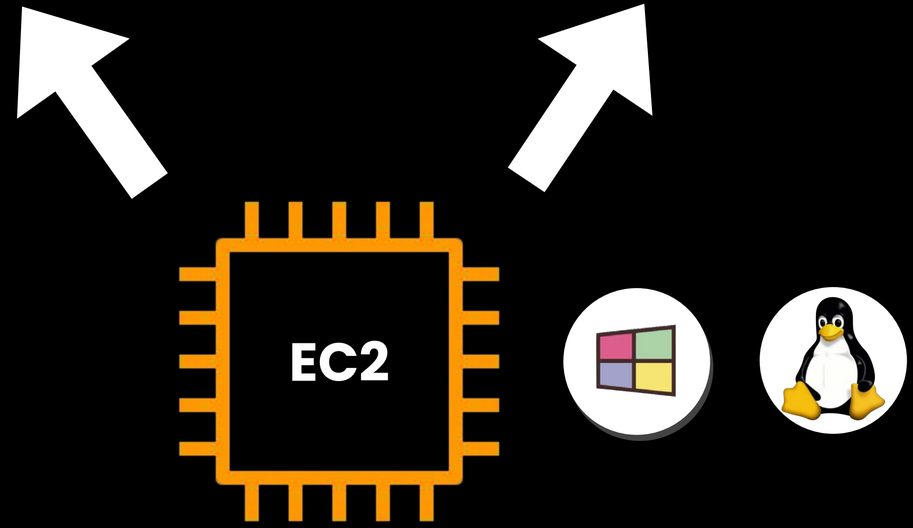


Amazon EFS









- Invoked via a **REST API** request call

- **Attached/Mounted** to the Amazon EC2 instance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Versioning



Multi-Factor Authentication
(MFA)

- Prevent accidental data deletion in Amazon S3



Access Control List
(ACL)

- Secure access to your S3 buckets and objects



Bucket Policy

- Control external access to your Amazon S3 bucket

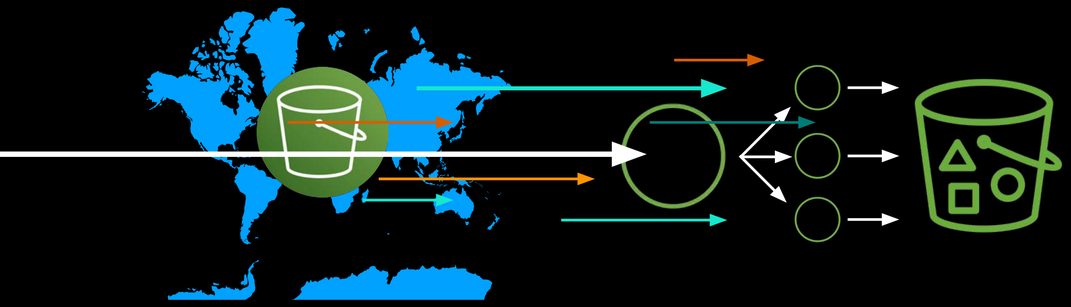
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Cross Region Replication (CRR)

- Automatically replicate objects to a different AWS Region for backup purposes

---



Transfer Acceleration

Multipart Upload

- Accelerate or expedite the data transfer (upload/download) of S3 objects

…and many other S3 features!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3 Storage Classes

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon S3 Storage Classes



S3 Standard



S3 Intelligent-Tiering



S3 Standard-Infrequent Access (Standard-IA)



S3 One Zone-Infrequent Access (One Zone-IA)



S3 Glacier



S3 Glacier Deep Archive

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Standard

- Primarily used for storing your data that are **frequently accessed**
- Highly durable, highly available, and high performance object storage
- Replicates your data to **3 or more** Availability Zones
- **99.99%** Availability
- **No minimum storage duration charge**
- **No data retrieval fee**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Standard

USE CASES

- For setting up a highly available and durable **static web hosting**
- As a **temporary storage service** for storing the nightly log processing of your application, where the logs are meant to be stored for 1 day (24 hours) only. It is a cost-effective option for this case since it has **no minimum storage duration charge**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Standard

LIMITATIONS

- **Not cost-effective** as this storage class is the **most expensive** among all other classes
- **Not recommended for data archiving, for infrequently access files** or for any workloads that require a cost-effective storage

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Standard-IA

- Primarily used for storing **infrequently accessed data** but provides a way to **rapidly retrieve the stored files**
- Replicates your data to **3 or more** Availability Zones
- **99.99%** Availability
- **30-day** minimum storage duration charge
- Has a data retrieval fee that is measured per gigabyte (GB)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Standard-IA

USE CASES

- As a long-term storage for **long-lived, but infrequently accessed data**
- For data backups
- As a data store for your Disaster Recovery (DR) files
- For storing the **primary backup copies** of your on-premises dataset

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 One Zone-IA

- For storing **less frequently accessed and easily reproducible data** that requires **immediate retrieval** when needed
- **30-day** minimum storage duration charge
- Cheaper than:  **S3 Standard-IA**
- Only uses **1 Availability Zone**
- **99.95% Availability** (*the **lowest** among all other Amazon S3 storage classes*)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 One Zone-IA

USE CASES

- If you require a **cost-effective option to store infrequently accessed data**
- For **workloads that do not require the availability and resilience** of the Amazon S3 Standard or S3 Infrequent Access class
- For storing **secondary backup copies of rarely-accessed on-premises dataset**
- For storing easily **recreatable data**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 One Zone-IA

LIMITATIONS

- The data is replicated in a **single AZ** only
- **Not recommended for storing your company's primary backup copies or any critical business data** that is difficult to reproduce

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Intelligent-Tiering

- Delivers **automatic cost savings**
- **Automatically moves your objects between different access tiers** whenever your access pattern changes
- **30-day** minimum storage duration charge
- **No data retrieval fee**
- Moves data to the most cost-effective access tier **without any operational overhead**
- Stores the objects in four access tiers:
  - 2 **low-latency** access tiers
  - 2 optional **archive** access tiers

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Intelligent-Tiering

USE CASES

- Suitable if your data has an **unpredictable access pattern**
- For buckets with a mix of frequent and infrequent accessed data
- If the access patterns to **your data vary all the time**
- If some of your files are accessed frequently while the **others are rarely accessed** (move to Glacier)
- If some of your data are **accessed less frequently** than others (move to IA tier)
- If **you are unsure** of how frequently your data will be accessed

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Intelligent-Tiering

USE CASES

- If you want to **keep costs low by automatically moving your data** to the appropriate S3 storage class
- If your data will be **accessed by users over variable periods of time**
- If you need storage with **no management overhead**
- If you want to **avoid lifecycle policies that are not consistently implemented** or are partially implemented

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Glacier

- A secure, durable, and low-cost storage
- Suitable for **data archiving**
- A cost-effective storage solution **for rarely accessed data and does not require a fast retrieval time**
- Replicates your data to **3 or more** Availability Zones
- **99.99%** Availability
- **90 day**-minimum storage duration charge
- **High data retrieval fee** (expensive)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Glacier

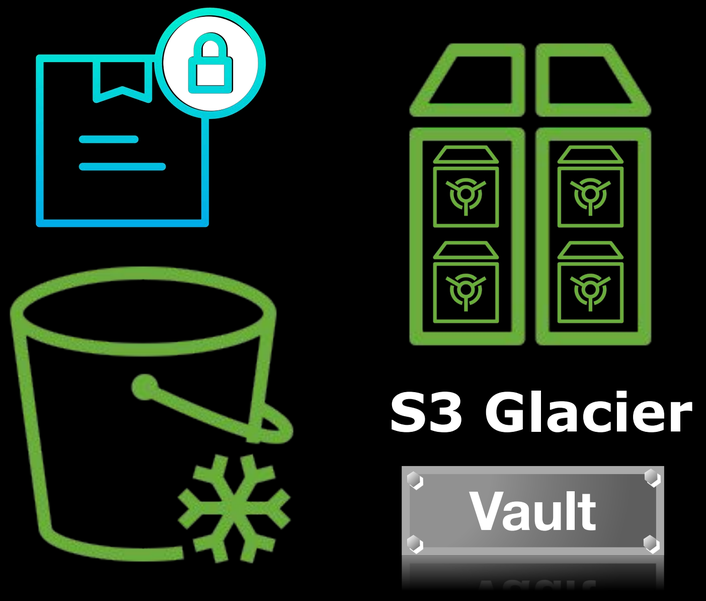
- **Has its own management console** apart from the regular Amazon S3 console
- 2 Ways to store your data:
  - Using the Amazon S3 console
  - Using the Amazon Glacier console
- Automatically move your data from S3 Standard or S3 Standard-IA to Amazon S3 Glacier by using a **lifecycle policy**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



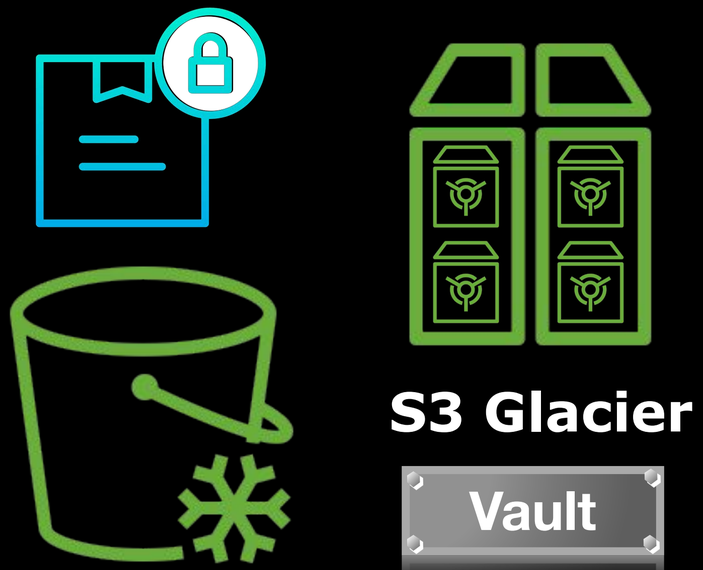
- Has a resource called: **Vault**
- A vault is a **container for storing your data archives**
- Base unit of storage in S3 Glacier, containing a **unique ID** and **an optional description**
- Can only be created in the Amazon S3 Glacier console
- You must provide the vault name and its corresponding AWS Region

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Use a **Vault Lock** to ensure data integrity and access control to your Amazon S3 Glacier Vaults
- A Vault Lock is an access policy that helps you **enforce regulatory and compliance requirements**
- You can specify a **"Write Once Read Many" (WORM)** control to lock your Glacier vault policy from future edits
- A Glacier vault access policy **can no longer be changed** when the vault lock process has been completed after 24 hours

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



USE CASES

- Applicable if your company wants to **retain its archives for a specific number of years** before the files can be deleted

- If you want to **deny users from modifying or deleting an archive** until after 1 year, 3 years, 7 years et cetera

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Glacier Archival Retrieval Options

EXPEDITED

- Quickly access a **subset of your data archives**
- Allows you to access your archived data within **1 - 5 minutes** (file size should **NOT** exceed **250 MB**)
- Ensure sufficient retrieval capacity for your *Expedited* retrieval operations by purchasing **provisioned capacity**

STANDARD

- **Default option** for retrieval requests
- Allows you to access any of your glacier archives within **3 – 5 hours**

BULK

- **Lowest-cost** retrieval option
- Retrieves large amounts of data archive in less than half a day
- Typically completes the process within **5 – 12 hours**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Glacier Deep Archive

- The **lowest-cost** storage class in Amazon S3.
- Supports **long-term retention and digital preservation** for your data
- Primarily used to retain your data sets for **7 to 10 years or longer to meet regulatory compliance requirements**
- Replicates your data to **3 or more** Availability Zones
- **99.99%** Availability

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Glacier Deep Archive

- **180-day** minimum storage duration charge (*roughly* ***6 months***)
- Should be used for data archiving only
- The data stored here should be **rarely accessed with no strict retrieval time**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



S3 Glacier Deep Archive - Retrieval Options

STANDARD

- **Default option** for retrieval requests
- Data will be restored within **12 hours**

BULK

- **Costs lower** than the Standard retrieval option
- Data will be restored within **48 hours**

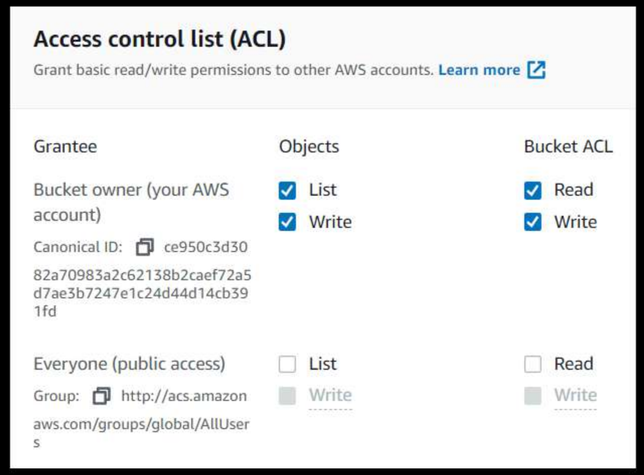
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon S3 Resource-based policies

Access Control List

- Less commonly used (legacy feature)

- Grants basic read/write permissions





Amazon S3 Bucket

Bucket Policies

- a JSON document that grants users access to an S3 bucket and the objects inside it

- You can write more complex rules with bucket polices than ACLs

- Unlike Identity-based policies, the Principal field is required for a bucket policy

- A newly created S3 bucket does not have a bucket policy

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sample S3 Bucket Policy

```
{
  "Statement":
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::tdojo-bucket/*",
      "Principal": "*"
    }
}
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sample S3 Bucket Policy

```
{
  "Statement":
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::tdojo-bucket/*",
      "Principal": "*"
    }
}
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sample S3 Bucket Policy

```
{
  "Statement":
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::tdojo-bucket/*",
      "Principal": "*"
    }
}
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sample S3 Bucket Policy



```
{
  "Statement":
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::tdojo-bucket/*",
      "Principal": "*"
    }
}
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sample S3 Bucket Policy

```
{
  "Statement":
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::tdojo-bucket/*",
      "Principal": "*"
    }
}
```

tdojo-bucket/images/*

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sample S3 Bucket Policy

```
{
  "Statement":
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::tdojo-bucket/*",
      "Principal": "*"
    }
}
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sample S3 Bucket Policy

```
{
  "Statement":
    {
      "Sid": "IPAllow",
      "Action": ["s3:GetObject"],
      "Effect": "Deny",
      "Principal": "*",
      "Resource": "arn:aws:s3:::TDOJO-BUCKET/*",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": "180.123.156.13"
        }
      }
    }
}
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3 Encryption

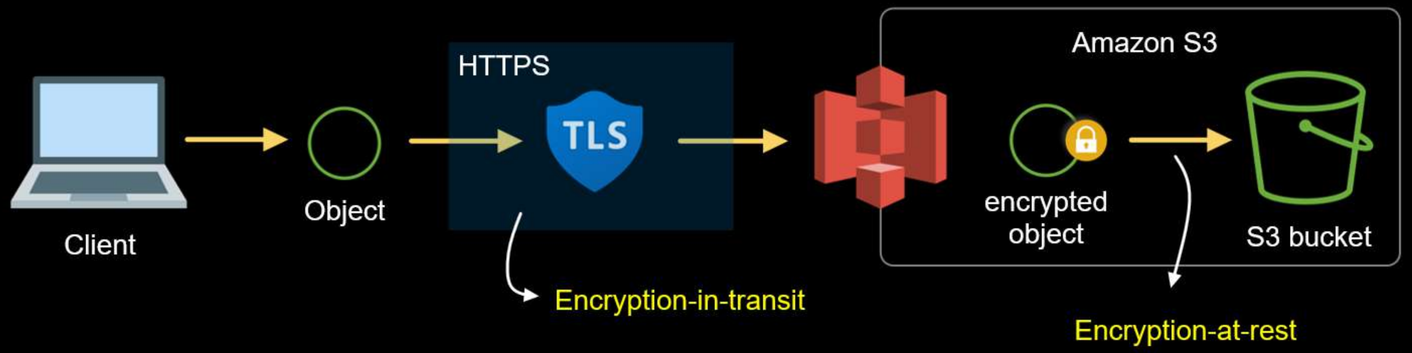
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3 Encryption

1. Server-side encryption (SSE)

- Amazon S3 encrypts object before saving it to disk storage and then decrypts it when you download the object



Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon S3
Encryption

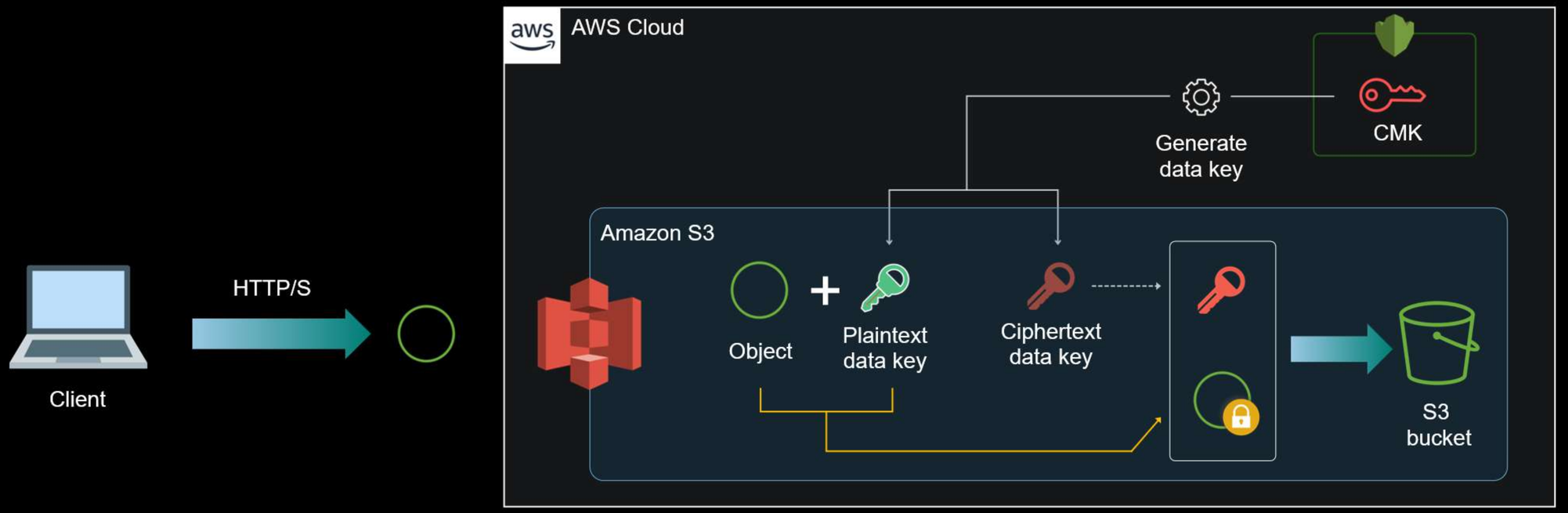
3 types of server-side encryption

- SSE-KMS
- SSE-S3
- SSE-C

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SSE-KMS

- You can specify an AWS-managed CMK (S3) or a customer-managed CMK
- S3 encrypts your data using a data key generated from the CMK that you specified
- The kms:GenerateDataKey and kms:Decrypt permissions are required if you're using a customer-managed CMK
- Set the header *x-amz-server-side-encryption: aws:kms* to use SSE-KMS
- Use the header *x-amz-server-side-encryption-aws-kms-key-id* to set your CMK ID. Don't use this header if you want to use the Amazon S3-managed CMK



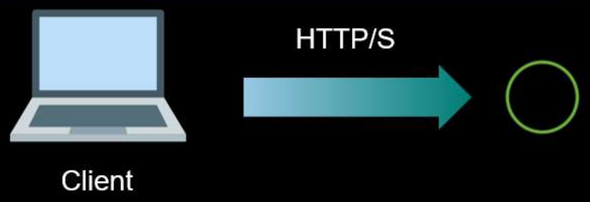
Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

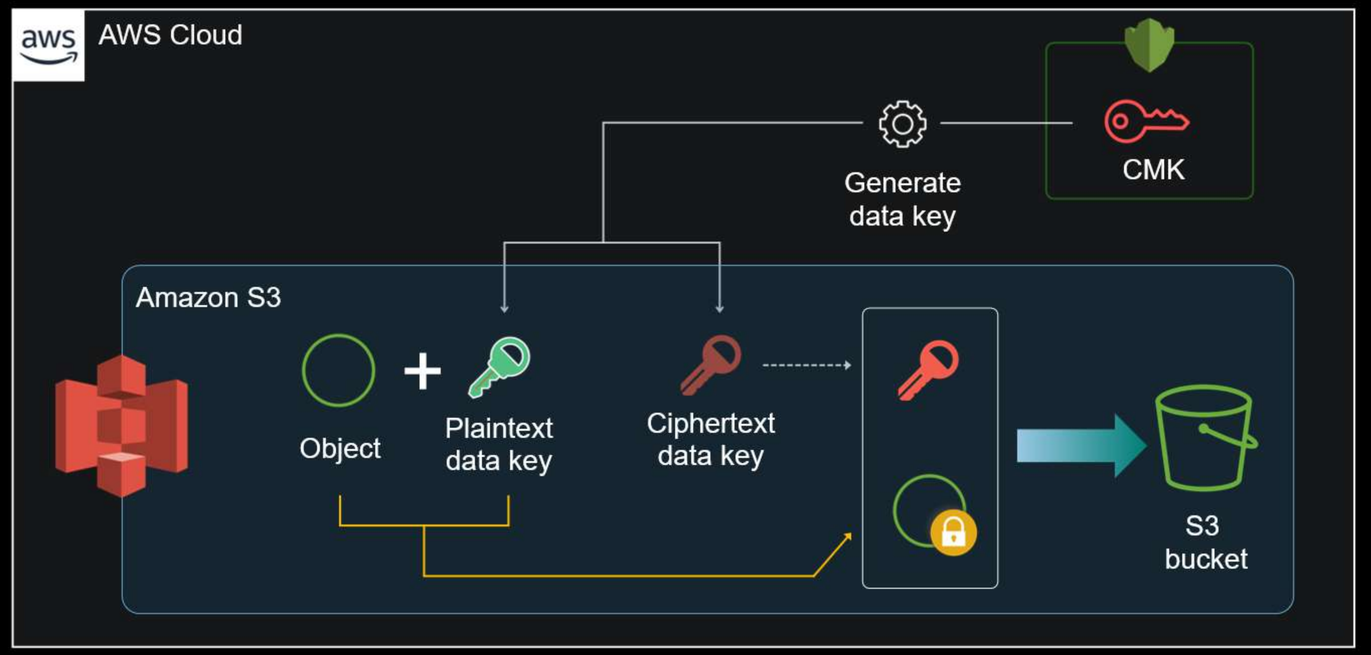
SSE-KMS

- You can specify an AWS-managed CMK (S3) or a customer-managed CMK
- S3 encrypts your data using a data key generated from the CMK that you specified
- The kms:GenerateDataKey and kms:Decrypt permissions are required if you're using a customer-managed CMK
- Set the header *x-amz-server-side-encryption: aws:kms* to use SSE-KMS
- Use the header *x-amz-server-side-encryption-aws-kms-key-id* to set your CMK ID. Don't use this header if you want to use the Amazon S3-managed CMK

Enforcing SSE-KMS

```
"Statement":[{
      "Sid":"DenyUnEncryptedObjectUploads",
      "Effect":"Deny",
      "Principal":"*",
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::awsexamplebucket1/*",
      "Condition":{
         "StringNotEquals":{
            "s3:x-amz-server-side-encryption":"aws:kms"
```





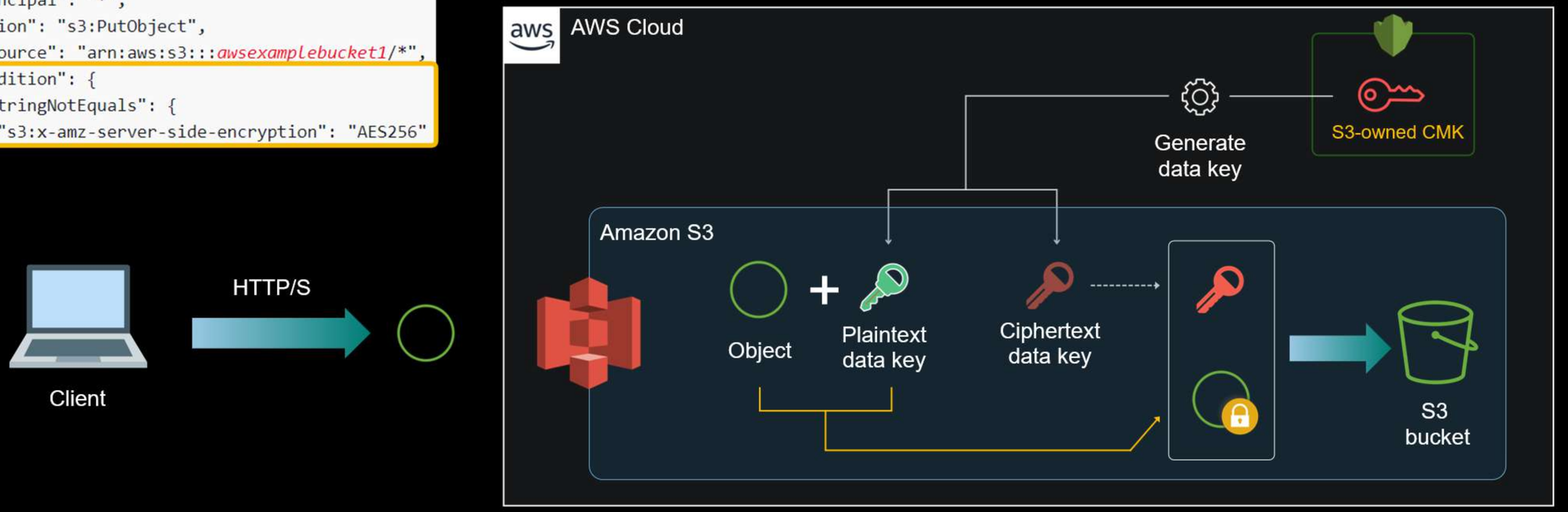
Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SSE-S3

- Uses an AES-256 Amazon S3-owned CMK
- Just like SSE-KMS, Amazon S3 manages the encryption and decryption of your data
- Set the header *x-amz-server-side-encryption: AES256* to use SSE-S3

Enforcing SSE-S3

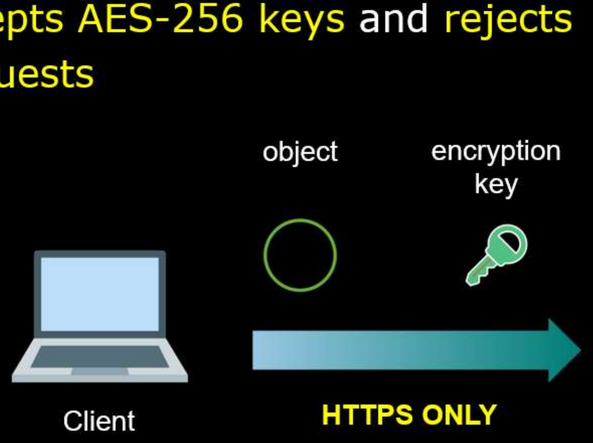
```
"Statement": [
  {
    "Sid": "DenyIncorrectEncryptionHeader",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::awsexamplebucket1/*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
```

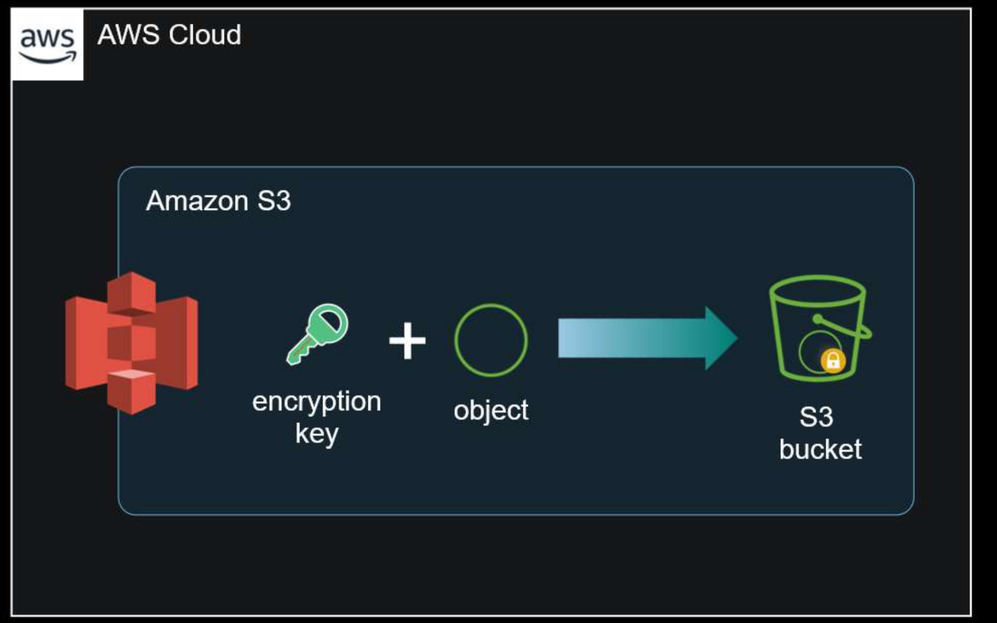


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SSE-C

- Amazon S3 manages the encryption and decryption of data
- You must provide the actual encryption key along with the data as part of your request
- You must include the same encryption key in your request to retrieve the encrypted data
- If you lose your encryption keys, you lose your data
- Requires 3 headers: *x-amz-server-side-encryption-customer-algorithm*, *x-amz-server-side-encryption-customer-key* and *x-amz-server-side-encryption-customer-key-MD5*
- Only accepts AES-256 keys and rejects HTTP requests

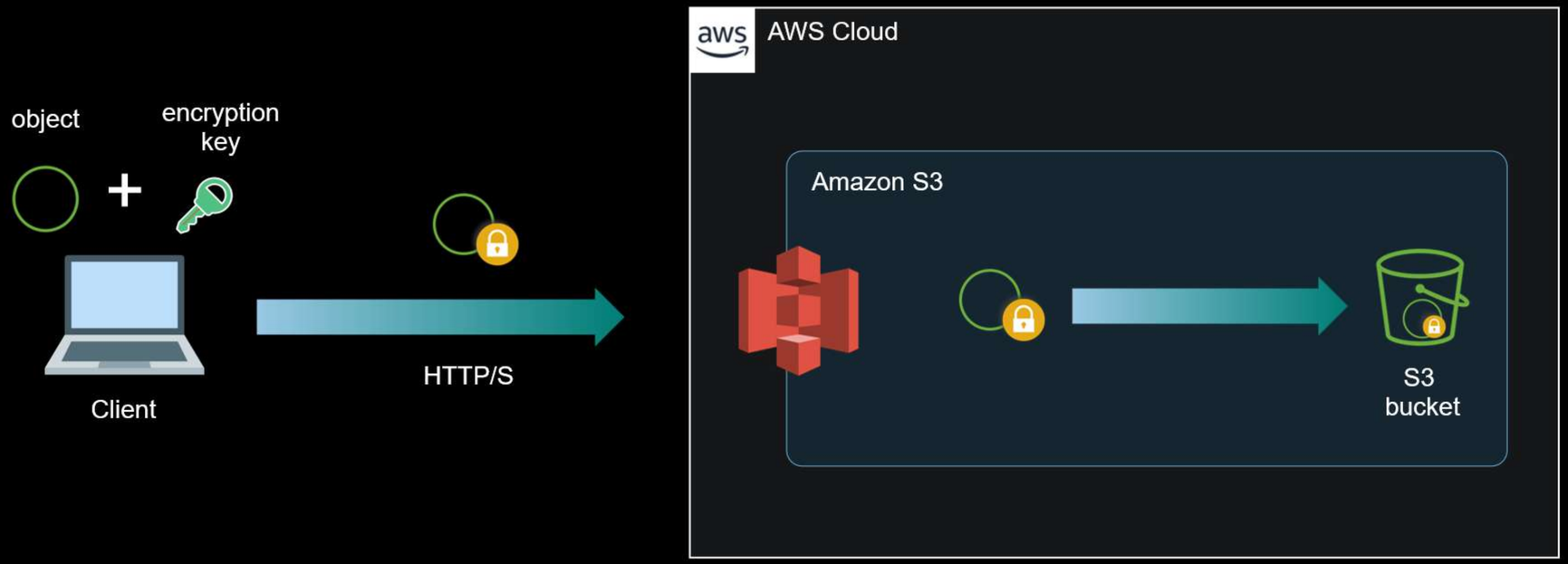




Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Client-side encryption

- Data is encrypted first before sending it to Amazon S3
- Amazon does not handle encryption and decryption for you
- You're responsible for data encryption and decryption
- You can use the AWS Encryption SDK to encrypt and decrypt data using industry standards and best practices



Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EBS Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EBS

- EBS stands for **Elastic Block Store**
- A type of a **block** storage like the Amazon EC2 Instance Store
- Its data is more persistent and **will not get lost even if the EC2 instance was stopped, restarted, or terminated**
- Zonal in scope, which means it **only exists in a single Availability Zone**
- Can be attached to any EC2 instances in the same Availability Zone only
- Can be encrypted at rest using **AWS KMS**
- You can attach one or more Amazon EBS volumes in a single EC2 instance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EBS

- Suitable for a **variety of workloads** such as databases, enterprise applications, big data analytics engines, file systems, media workflows, and others
- Allows you to store and retrieve your data with high throughput and low latency
- The Amazon EC2 instance and its attached EBS volumes are logically attached together and are both **located within a single Availability Zone**, which significantly reduces latency
- Since the underlying physical resources that power your Amazon EC2 instance and EBS volumes are located within the same city or geographic area, Amazon EBS is **capable of providing low latency read or write access to your data**
- Mainly operates on the **hardware level**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

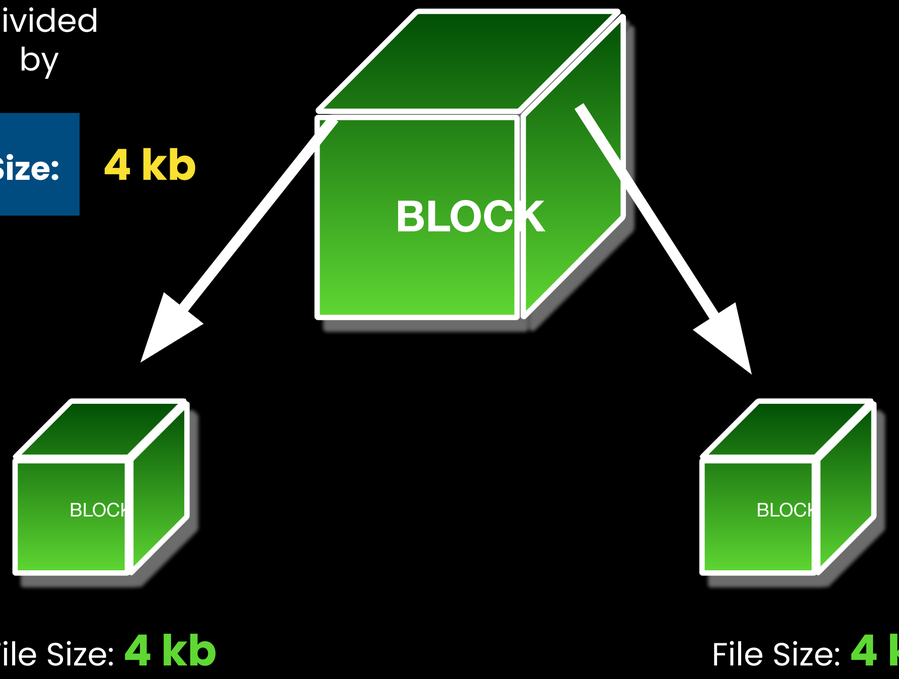


Amazon EBS

Total File Size: **8 kb**

divided by

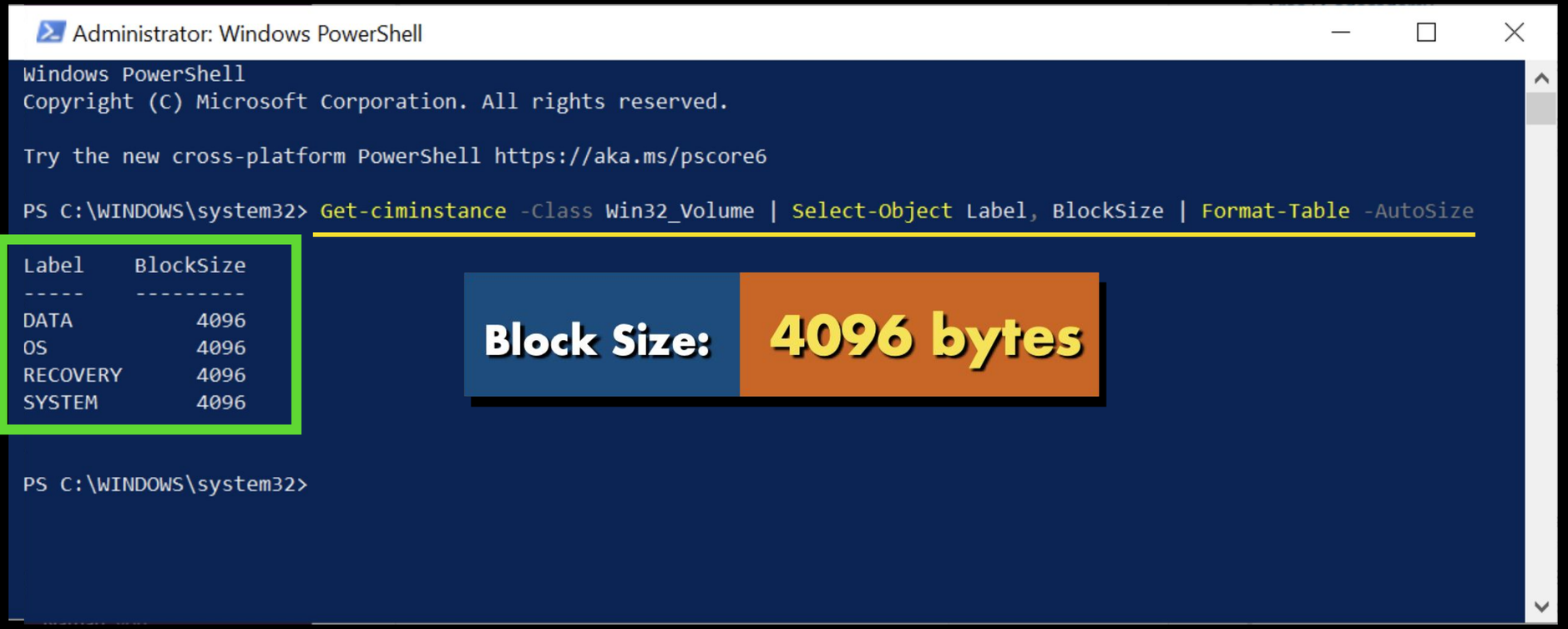
Block Size: **4 kb**



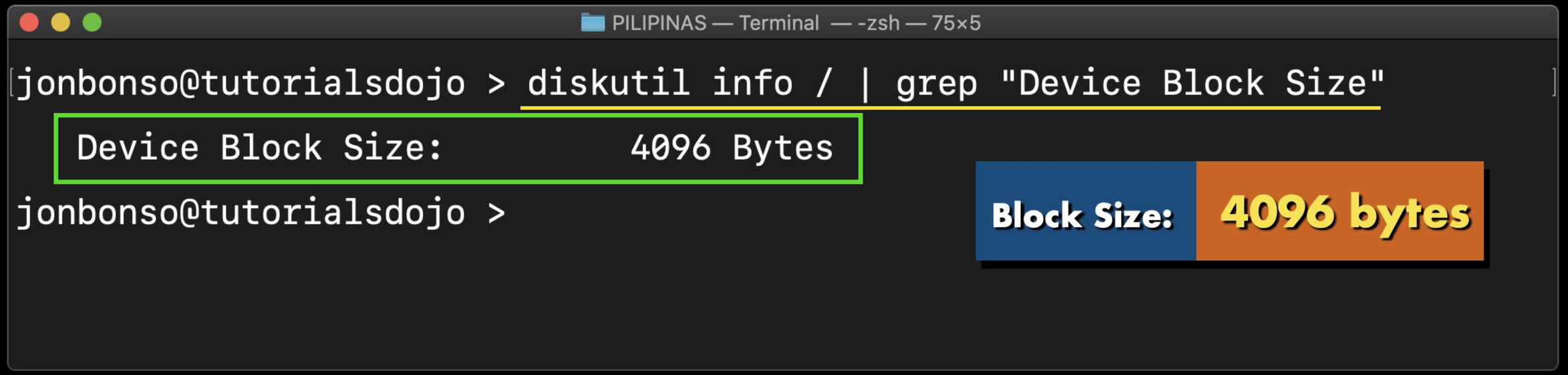
File Size: **4 kb**

File Size: **4 kb**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

RAID

Redundant **A**rray of **I**ndependent **D**isks

RAID 0

- **Stripes** multiple volumes together
- Provides **greater I/O performance**
- **Divides a body of data into blocks** and then spreads the data blocks across multiple storage devices
- Suitable if I/O performance is your priority

RAID 1

- **Mirrors** two or more volumes together
- Provides **on-instance redundancy**
- **Duplicates data** to provide more durability and availability
- Suitable if data redundancy is your focus

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon Elastic Block Store
(Amazon EBS)

	Solid State Drive (SSD)	
Read & Write Speeds	Fast !	Slow…
Use Case	For workloads with frequent read/write operations	For data archiving, backups or throughput-oriented storage
Dominant Performance Attribute		
Can be used as **Boot Volume** for Amazon EC2 ?		

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



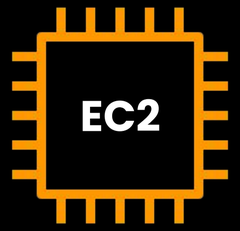
Amazon EBS Snapshots

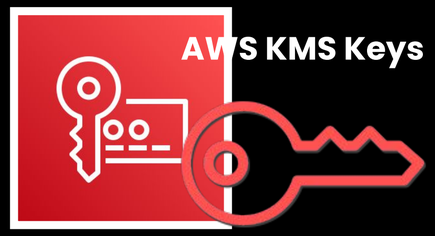
- **An incremental backup** that internally uses Amazon S3 to persist your data
- It only saves the data blocks that have changed after your most recent snapshot
- Allows you to **restore the state of your EBS volume in the event of data loss**
- Enables you to **copy your EBS volume to another AWS Region** for your data migration, disaster recovery activities
- Can be used to encrypt an unencrypted Amazon EBS volume.
- Automate the creation, retention, and deletion of your EBS snapshots and EBS-backed AMIs using the **Amazon Data Lifecycle Manager (Amazon DLM) service**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ENCRYPTION IN TRANSIT

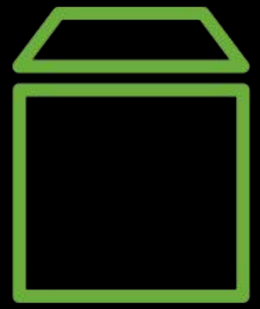
ENCRYPTION AT REST





Amazon EBS Encryption by Default

Must be manually enabled per AWS Region







AMAZON EBS VOLUME

AMAZON EBS SNAPSHOT

INTERNAL AMAZON S3 BUCKET

Exclusively managed by AWS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

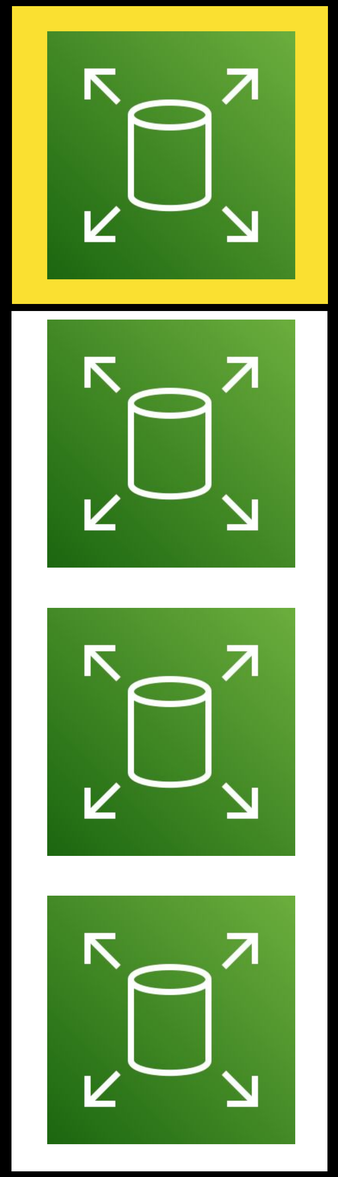


Amazon EBS Types

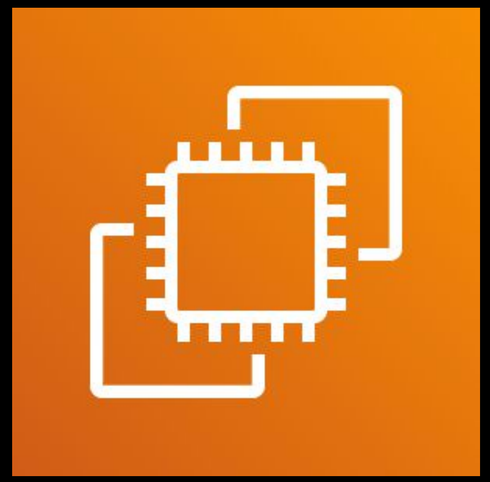
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ROOT EBS VOLUME

OTHER DATA VOLUMES



* contains the system image for booting the EC2 instance



Amazon EC2 Instance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Solid State Drive (SSD)





General Purpose SSD



Provisioned IOPS SSD

- Suitable for **transactional workloads**
- For various types of applications and systems with **frequent read/write operations with small I/O sizes**
- Performance Attribute: **IOPS**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Solid State Drive (SSD)



General Purpose SSD



Provisioned IOPS SSD

- Provides a **balance of price and performance** for your workloads
- Recommended for **most workloads**
- Also suitable for apps with **unpredictable or unknown access patterns**
- **Provides a configurable and consistent IOPS** to allow you to accommodate the changes in your data storage requirements

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Solid State Drive (SSD)



General Purpose SSD



Provisioned IOPS SSD

- Suitable for **low-latency interactive apps** in production as well as your development and test environments
- For your **infrquently accessed applications or systems that:**
  - Only peaks during certain times of the day
  - Has a varying Disk I/O operations
- Provides ample IOPS for your applications but **not on par** with what a Provisioned IOPS type can give
- The **most cost-effective storage option that does NOT sacrifice performance**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Solid State Drive (SSD)



General Purpose SSD



Provisioned IOPS SSD

- Primarily used for **mission-critical, low-latency, or high-throughput workloads**
- Provides **sub-millisecond latency and consistent IOPS performance**
- Allows you to set the amount of available IOPS of your EBS volume

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Solid State Drive (SSD)



General Purpose SSD



Provisioned IOPS SSD

- For hosting data to your **applications that makes small reads and writes** to a small file system
- For applications that **require a number of high read and write IOPS performance**
- For **fixing latency issues**
- For scenarios where your database storage performance is the bottleneck
- For storage systems that **require a configurable and consistent IOPS**
- . . . and many more!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon EBS Multi-Attach



Solid State Drive (SSD)

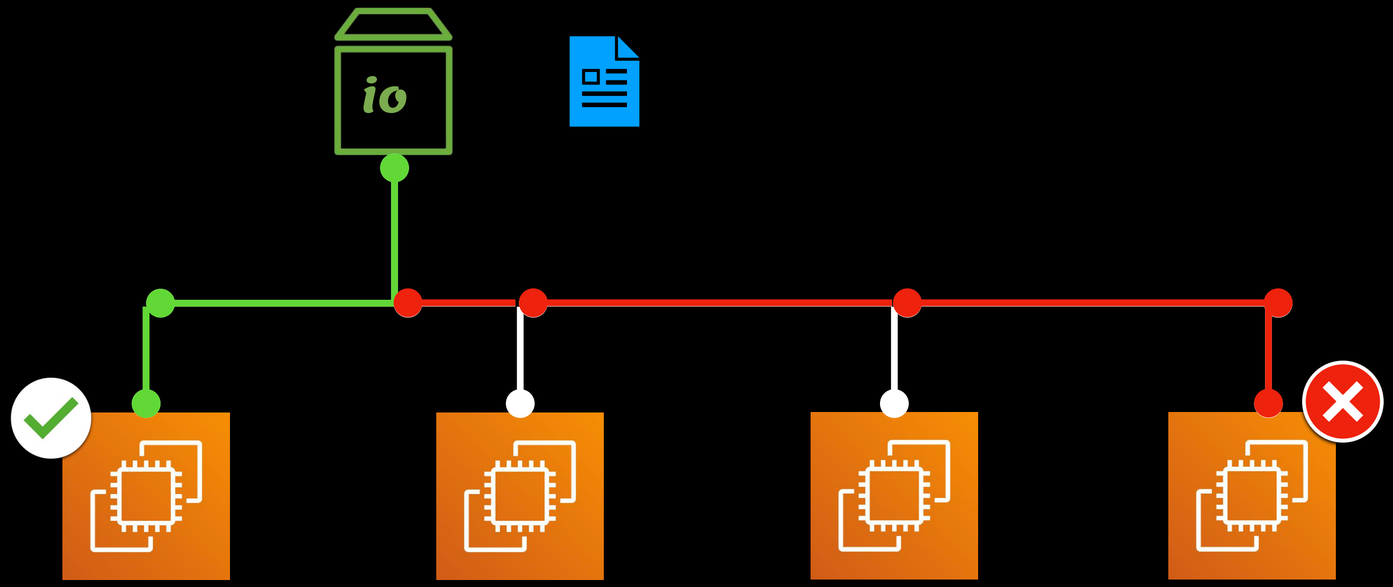


General Purpose SSD





Provisioned IOPS SSD



No concurrent file modification

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





Throughput Optimized HDD



Cold HDD

- Optimized for **large streaming workloads**
- For various types of applications and systems with **large, sequential I/O operations**
- Performance Attribute: **Throughput** `(MB/s)`

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



st

Throughput Optimized HDD

sc

Cold HDD

- A low-cost HDD designed for **frequently accessed, throughput-intensive workloads**
- Can be used for your Big data applications, Data Warehouses, and Log Processing
- **Cannot** be used as your boot (root device) volume

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





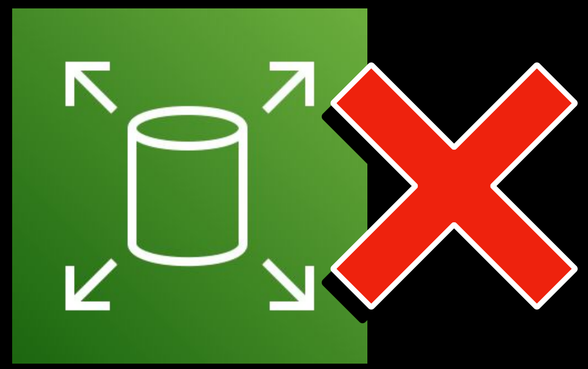
Throughput Optimized HDD



Cold HDD

- **Lowest-cost HDD storage type**
- Meant for storing **less frequently accessed** workloads
- The **most cost-effective storage EBS type** option for data archiving only since its throughput performance is substantially low
- Suitable for **throughput-oriented storage for data that is infrequently accessed**
- Perfect for scenarios where the **lowest storage cost is of the utmost importance**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



ANTI-PATTERNS

- If you just need a **temporary storage** for your data, use EC2 Instance Store instead
- If you have to store your application or system data in a **POSIX-compliant hierarchical directory structure** (use Amazon EFS instead)
- If you have multiple applications that are **concurrently accessing the same files at the same time**, it is better to use the Amazon EFS or Amazon FSx service instead
- If you need to **store your static data in the most cost-effective way**, it’s more appropriate and cheaper to store them in Amazon S3

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon RDS Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon RDS

- A **relational** database service
- Managed by both you (limited access) and AWS
- Allows you to run various database engines:

Microsoft **SQL Server**

MySQL

MariaDB

PostgreSQL

ORACLE

Amazon Aurora

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon RDS

- **Can be deployed using:**



AWS CloudFormation



AWS Management Console



AWS CLI



Amazon RDS API

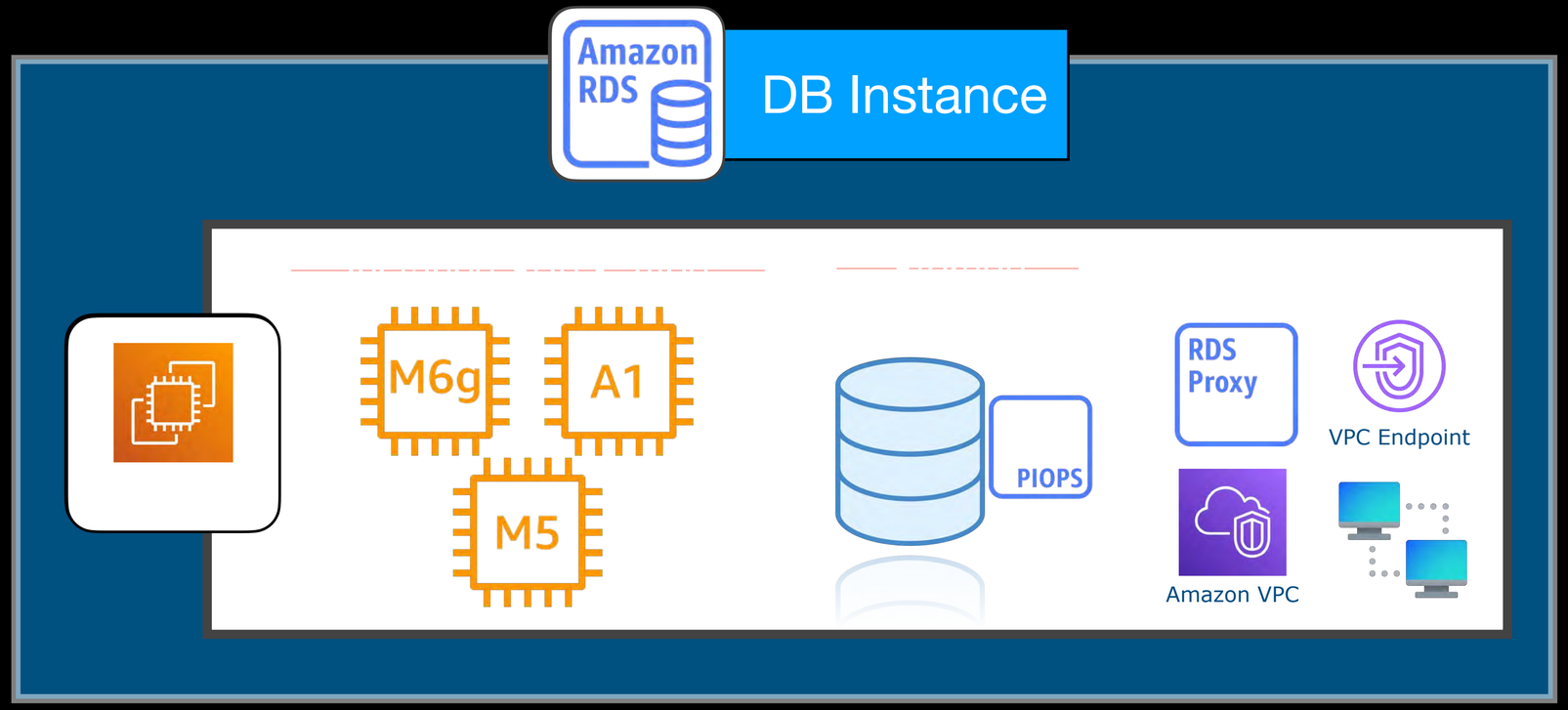
- **Eliminates the time-consuming tasks** of hardware provisioning, patching, backups, and maintenance for your database

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon RDS

- You can **configure the underlying EC2 instance** used by your Amazon RDS database such as its size, instance type & storage
- Purchase a **Reserved DB instance** to lower down your RDS costs
- Allows you to choose the Availability Zone where your database will be hosted, including its associated security group



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Self-Hosted Database



Amazon RDS Database

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

MANAGED BY	Self-Hosted Database	Amazon RDS Database
YOU *(AWS Customer)*	• Patching • Sc • Taking backups • Ensuri ailability • Re on • Monitoring	• Minimal maintenance work
aws	• Physical Infrastructure • Virtualization layer • Host OS of the EC2 instance	• Patching • Scaling • Taking database backups • Ensuring high availability • Replication • Monitoring

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Self-Hosted Database

- **Can be directly accessed** via SSH, RDP or other connections

- Allows direct access and modification of your **database configuration files** such as:

  - `/etc/mysql/my.cnf`
  - `ConfigurationFile.ini`
  - `INIT.ORA, TNSNAMES.ORA, *.ORA`



Amazon RDS Database

- The underlying EC2 instance **CANNOT** be directly accessed via SSH or RDP

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Self-Hosted Database

- **Can be directly accessed** via SSH, RDP or other connections
- Allows direct access and modification of your **database configuration files** such as:
  - /etc/mysql/**my.cnf**
  - **ConfigurationFile.in**
  - **INIT.ORA, TNSNAMES.O**

Amazon RDS Database

- The underlying EC2 instance **CANNOT** be directly accessed via SSH or RDP

my.cnf

```
# Default MySQL Server config for Tutorials Dojo Tarlac
[mysqld]

# Only allow connections from localhost
bind-address = 127.0.0.1
mysqlx-bind-address = 127.0.0.1

read_only = 1
```

Read-Only setting

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Self-Hosted Database

- **Can be directly accessed** via SSH, RDP or other connections
- Allows direct access and modification of your **database configuration files** such as:
  - /etc/mysql/**my.cnf**
  - **ConfigurationFile.ini**
  - **INIT.ORA, TNSNAMES.ORA, *.ORA**



Amazon RDS Database

- The underlying EC2 instance **CANNOT** be directly accessed via SSH or RDP

INIT.ORA

```
#############################################################################
# INIT.ORA file - Oracle Database
#############################################################################

# Change '<ORACLE_BASE>' to point to the oracle base (the one you specify at
# install time)

db_name='ORCL'
memory_target=1G
processes = 150
audit_file_dest='<ORACLE_BASE>/admin/orcl/adump'
audit_trail ='db'
db_block_size=8192
db_domain=''
db_recovery_file_dest='<ORACLE_BASE>/flash_recovery_area'
db_recovery_file_dest_size=2G
diagnostic_dest='<ORACLE_BASE>'
dispatchers='(PROTOCOL=TCP) (SERVICE=ORCLXDB)'
open_cursors=300
remote_login_passwordfile='EXCLUSIVE'
undo_tablespace='UNDOTBS1'

# You may want to ensure that control files are created on separate physical
# devices
control_files = (ora_control1, ora_control2)
compatible ='11.1.0'
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Self-Hosted Database

- You have **full access** to the virtual machine and the underlying database
- You are responsible for making your database highly available, fault-tolerant and secure
- You have to apply the OS patches as well as the Database Engine patches regularly
- You will handle all of the database administrative tasks



Amazon RDS Database

- Modify the database configuration via:

Parameter Group

Options Group

- You can choose the actual time when Amazon RDS will apply the DB patches in its **maintenance window**
- Database maintenance tasks are handled automatically

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



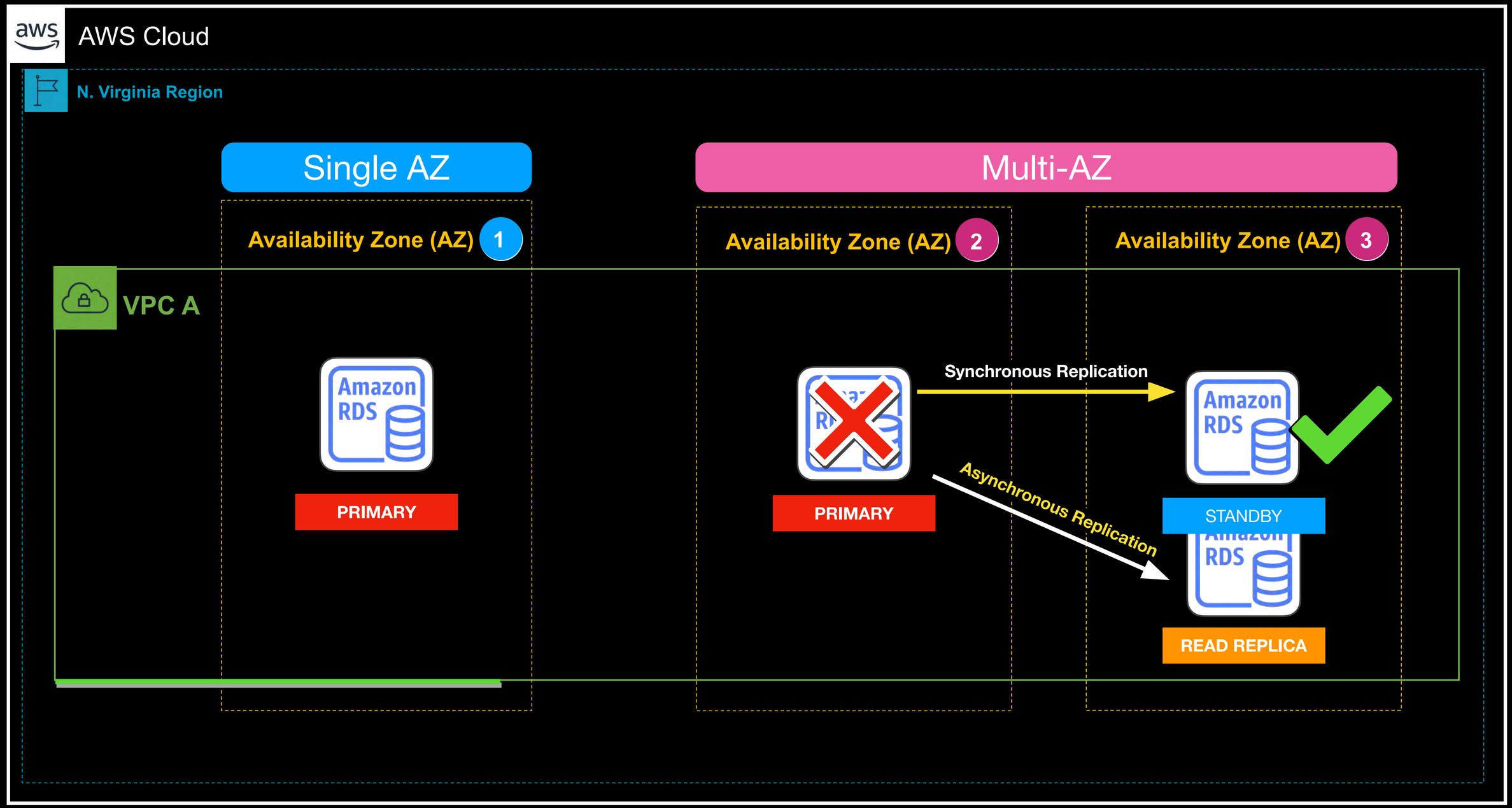
Self-Hosted Database



Amazon RDS Database

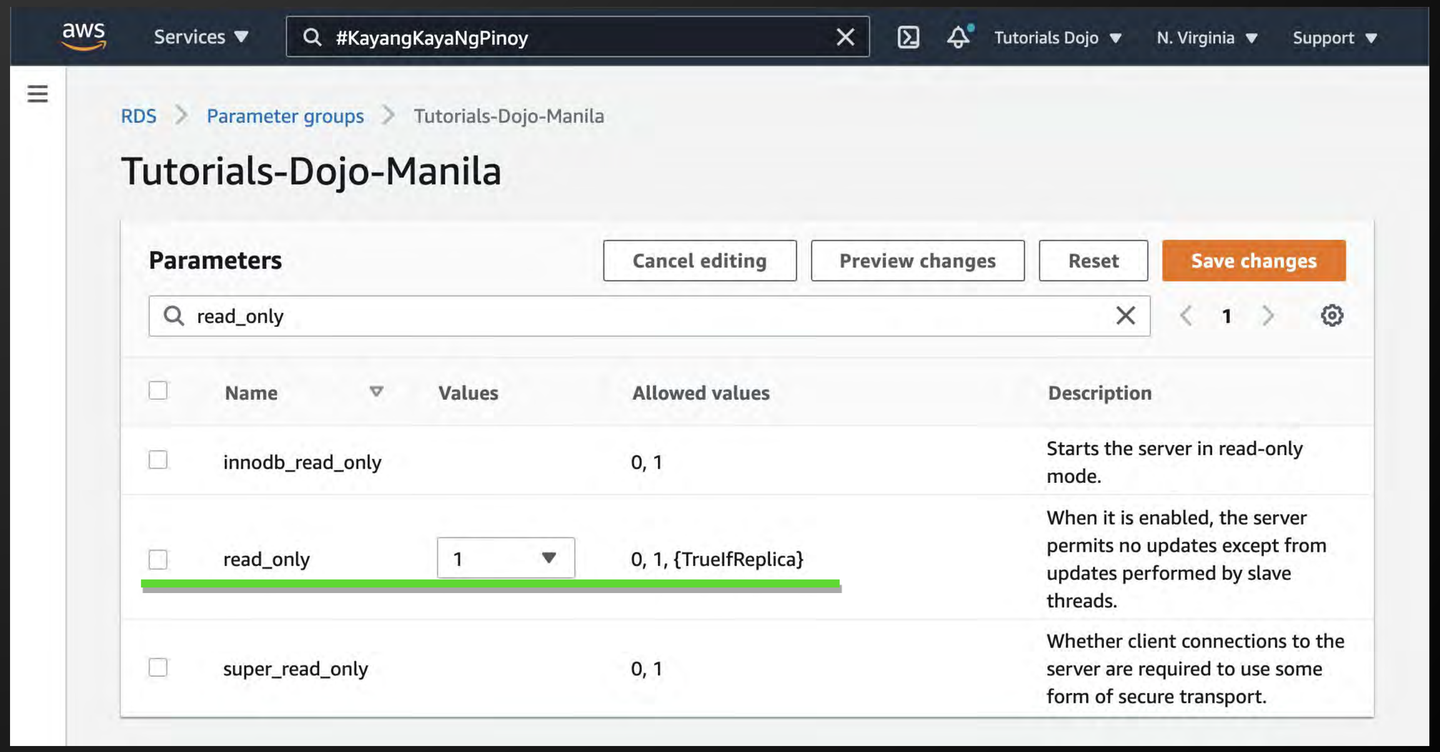


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

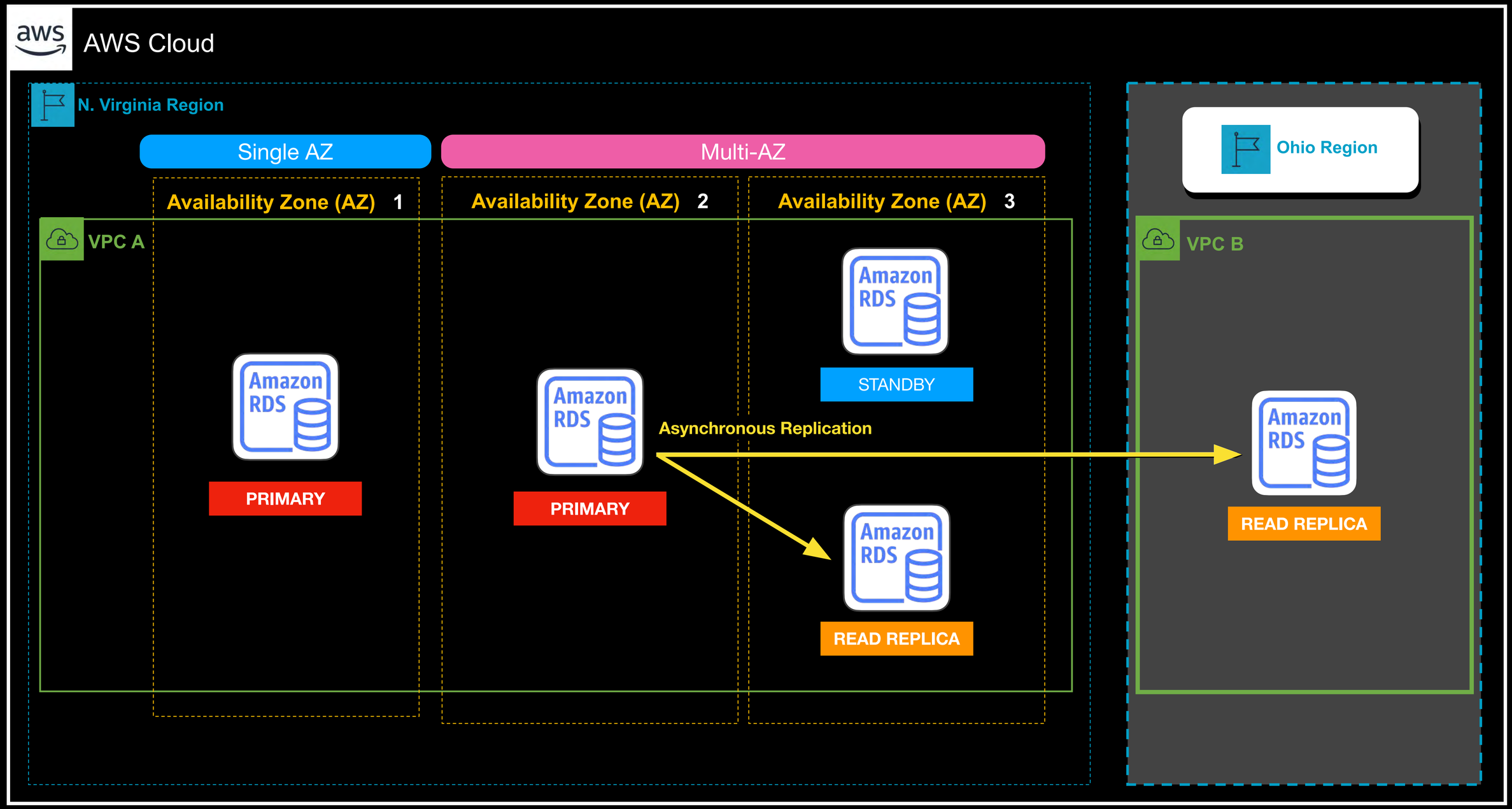


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

read_only



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon RDS



OLTP Applications

- Suitable for applications that read or write **constantly changing data**, such as Online Transaction Processing **OLTP** applications

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



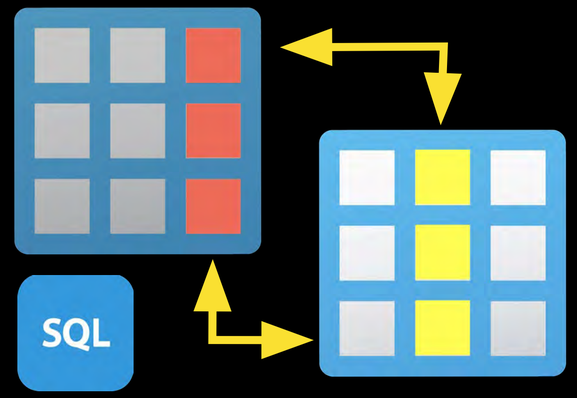
Amazon RDS

A TOMIC

C ONSISTENT

I SOLATED

D URABLE



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- A fully managed, highly available **database proxy**
- Automatically **connects your application to a new DB instance** while preserving its application connections
- **Minimizes downtime** by instantly routing the incoming requests directly to the new database instance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- A **fully managed database service** and also a type of **database engine** within Amazon RDS
- Scales automatically, performs faster, and costs lower
- A relational database that is compatible with:

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora

- Can automatically grow or scale its storage
- Usually deployed as a **database cluster**
- A cluster consists:

ONE PRIMARY



MULTIPLE REPLICAS



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora

CLUSTER TYPES

Single-master

Multi-master

STANDALONE TYPE

Single primary DB instance with no replica

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora

- **Performs faster** than other databases
- Can scale the computing components and storage automatically **without any manual intervention**
- The database cluster typically lags behind the primary instance by a **few milliseconds** only
- Provides **less than 1 second of read replication latency** for Aurora Replicas in the same or different AWS Region

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora
ENDPOINTS

Cluster endpoint

Reader endpoint

- **Group the individual DB instances and associate them with a particular endpoint**

Custom endpoint

Instance endpoint

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora
Serverless

- Recommended for **sporadic usage workloads** or with **unpredictable usage**
- Pay your database usage **on a per-second basis**
- Provides a **more cost-effective option** than the regular Amazon RDS or Amazon Aurora databases

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora Serverless

- For **migrating legacy applications** hosted on-premises that needs to be re-architected and reduce operating costs
- If it is required to re-architect your application by using technologies that **do not require any IT administration team to regularly manage your servers or clusters**
- If you need to turn your monolithic application into microservices architecture with serverless resources
- **Can be used for serverless stack** with the application containers running on AWS Fargate and your database on Aurora Serverless

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora
Serverless

- For **sporadic usage patterns**
- If your application has:
  - Extremely high usage at the beginning of each month
  - An unpredictable usage at the start of each week
  - A moderate usage over the weekend
- For situations where it is **difficult to predict the application demand or to choose the most suitable instance size** of your database due to the constantly changing usage
- If a cost-effective database platform is required which does not require any database modifications
- If you need to automatically scale the capacity up or down based on your application's needs

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora Serverless

- For applications with **infrequent access patterns**
- **Automatically scales down** your database capacity if there's less incoming traffic coming in, without any manual intervention
- For migrating your on-premises database to AWS Cloud **without having to worry about its particular database instance type**
- If you need to **eliminate the need to manually modify your database instance type** in anticipation of the changes in the number of your users or workloads

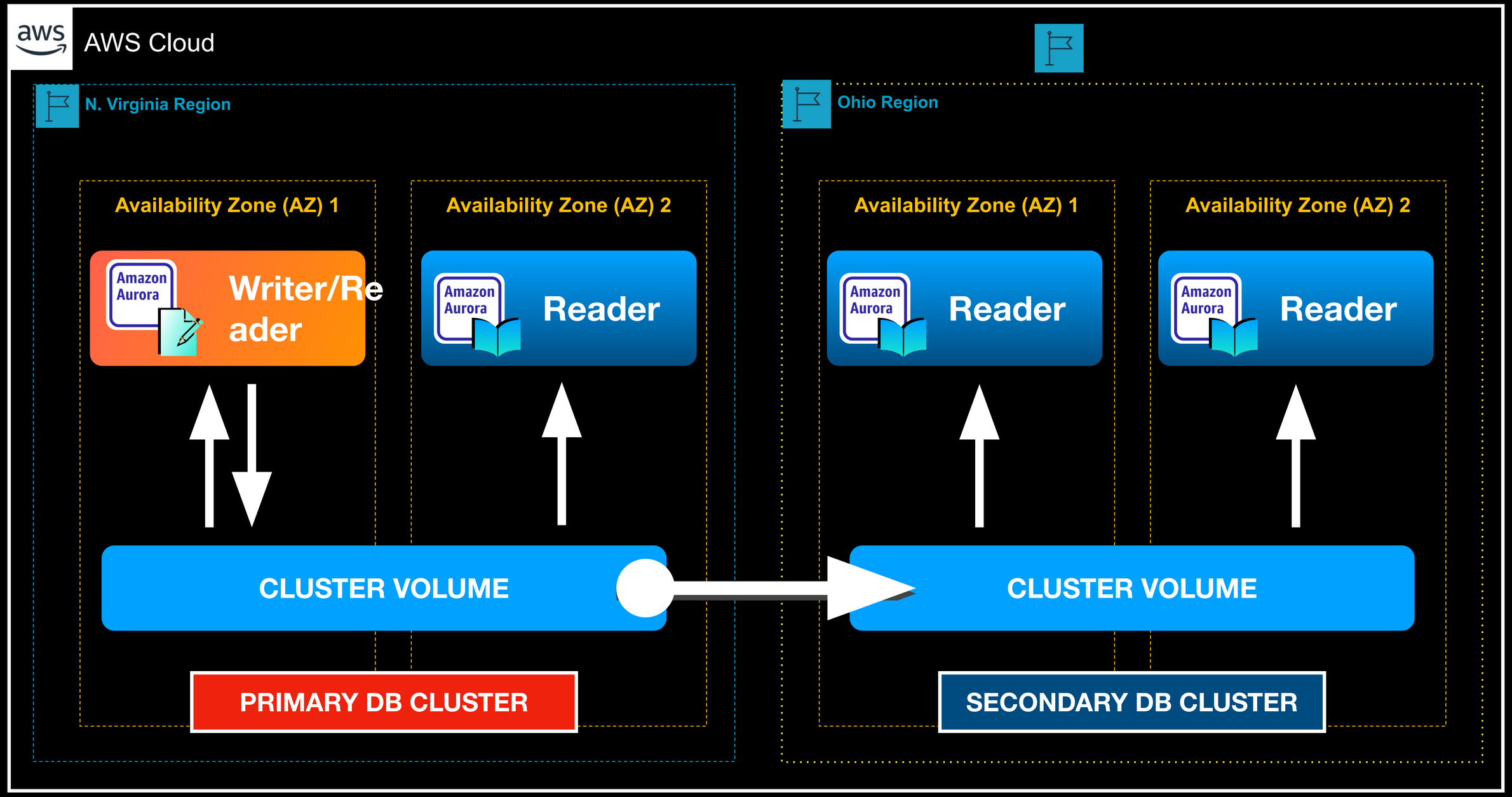
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora Global Databases

- Designed for **globally distributed applications**
- Allows a single Amazon Aurora database to span multiple AWS Regions
- Offers **faster physical replication** between Aurora clusters
- Eliminates the need to manually create cross-region Aurora Replicas yourself

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Aurora Global Databases



= 1 second



RTO

Recovery **Time** Objective

= 1 minute

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

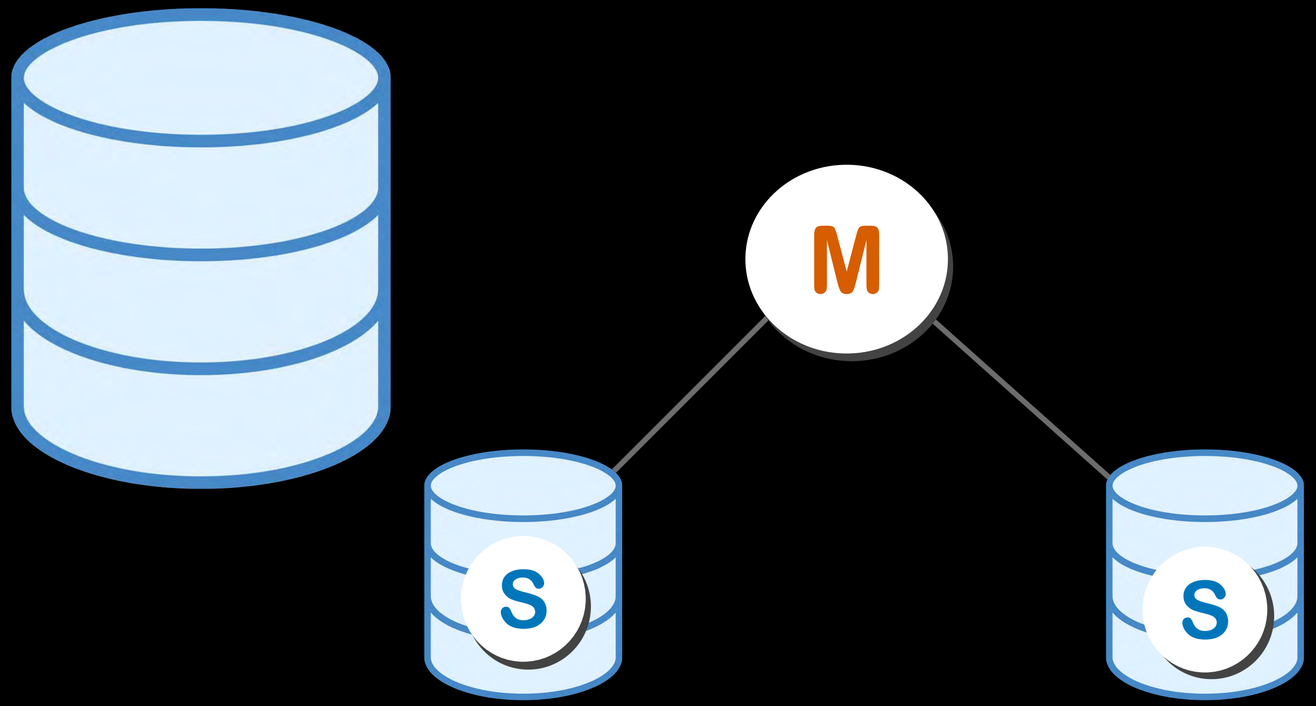


Amazon RDS Read Replica

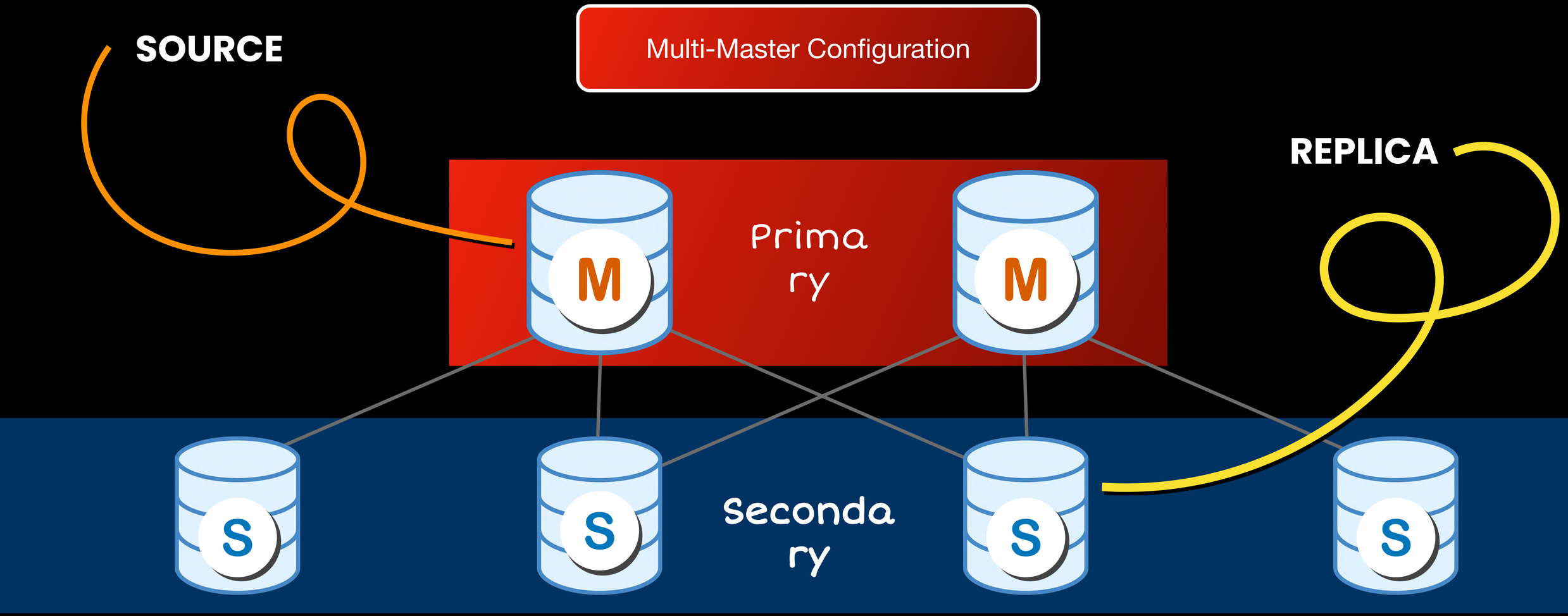
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

STANDALONE

MASTER-SLAVE CONFIGURATION



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

READ REPLICA

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



STANDBY REPLICA

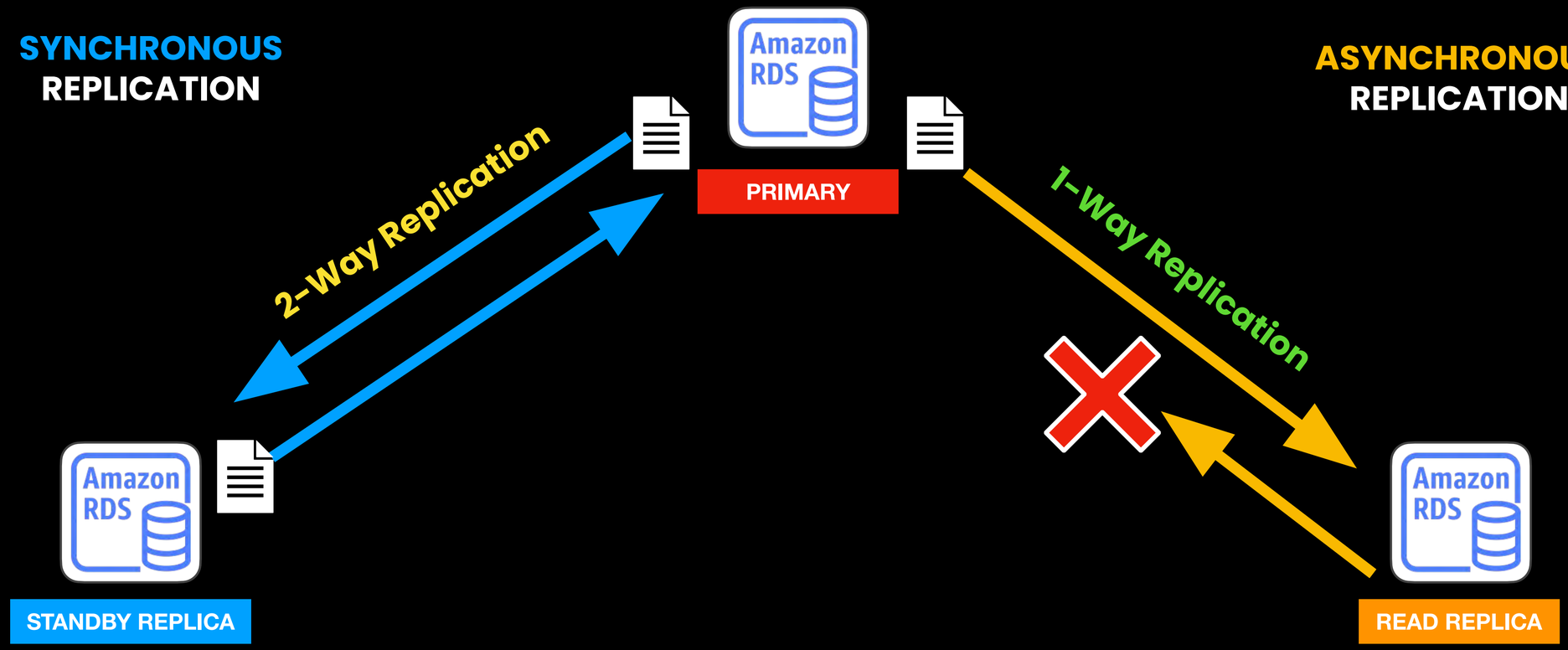
REPLICA

a copy of something



READ REPLICA

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Does not accept live traffic without failover
- **Cannot be seen** in the Amazon RDS Console as a separate DB instance
- The DB Endpoint is the **same** as the primary DB instance

- Can accept live traffic
- **Can be seen** in the Amazon RDS Console as a separate DB instance
- The DB Endpoint is **different** from the primary DB instance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA

- Based on the **built-in replication** functionality of:

MariaDB

Microsoft SQL Server

MySQL

ORACLE

PostgreSQL

- Just a regular database with a **read-only configuration**
- Under the hood, Amazon RDS creates this by cloning your source database, setting up the replication parameters, and disabling any write operations

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA

my.cnf

```
# Default MySQL Server config for Tutorials Dojo Divisoria
[mysqld]

# Only allow connections from localhost
bind-address = 127.0.0.1
mysqlx-bind-address = 127.0.0.1


# Set the database to read-only
read_only = 1

# Block any write operations from DB Administrators
super_read_only = 1
```



CREATE

INSERT

UPDATE

DELETE

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA

Other required parameters for binary logging to be set:

- `log_bin`
- `binlog-format`
- `sync_binlog`
- `...and many more!`

```
my.cnf

# Default MySQL Server config for Tutorials Dojo Divisoria
[mysqld]

# Only allow connections from localhost
bind-address = 127.0.0.1
mysqlx-bind-address = 127.0.0.1


# Set the database to read-only
read_only = 1


# Block any write operations from DB Administrators
super_read_only = 1
```

- A **binary log**
  - Also known as '***binlog***'
  - A set of log files that contain information about the recent SQL modifications
  - Contains all of the `CREATE`, `INSERT`, `UPDATE`, `DELETE`, `ALTER`, and other SQL statements that were made in your primary database
  - The actual data that is being transferred from the source database to the database replica

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA



READ REPLICA

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



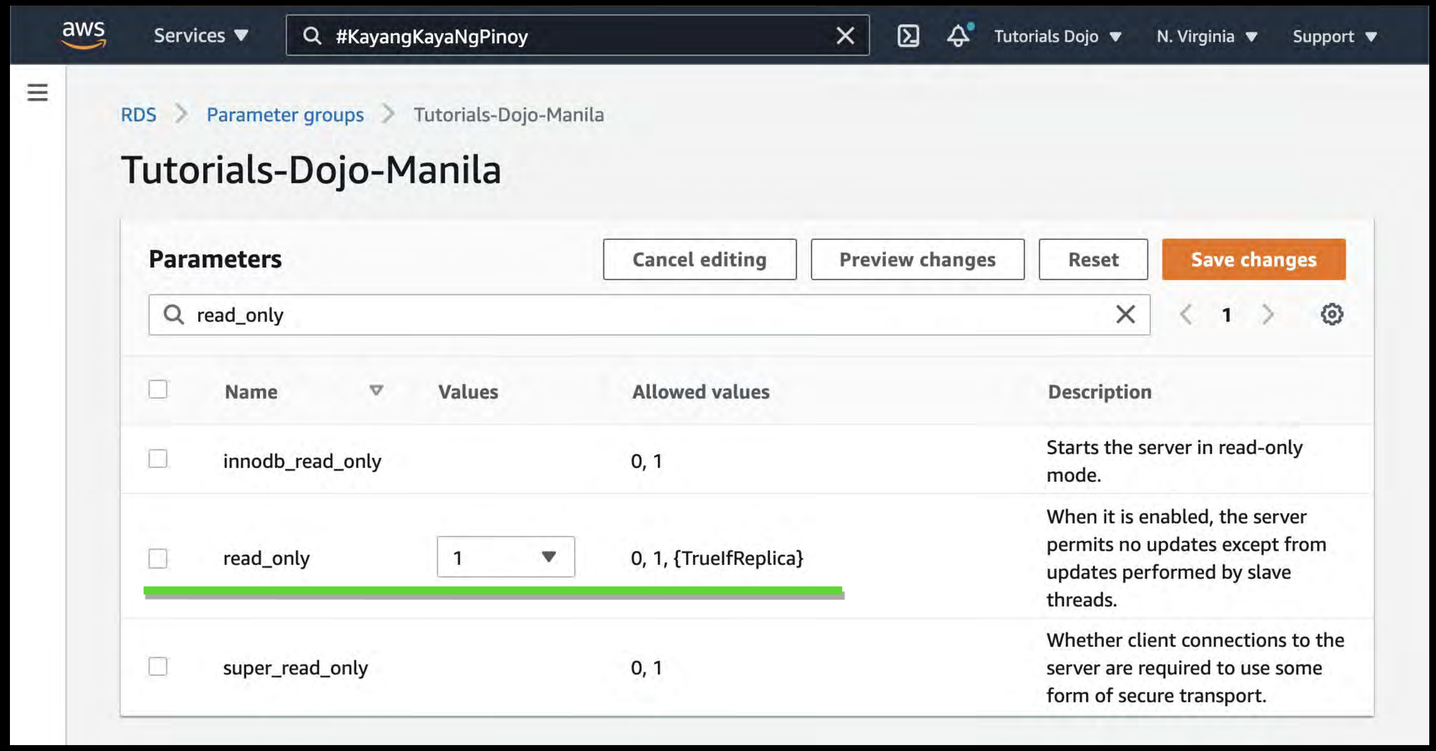
READ REPLICA

- Can be launched two ways:
  - On the **same** AWS Region of your primary DB
  - On a **different** AWS region
- **Does NOT provide the capability of directly accessing the actual configuration files** – `my.cnf` (MySQL), `ConfigurationFile.ini` (MS SQL) and others in Amazon RDS
- View and modify the DB configuration of the replica using a **parameter group**

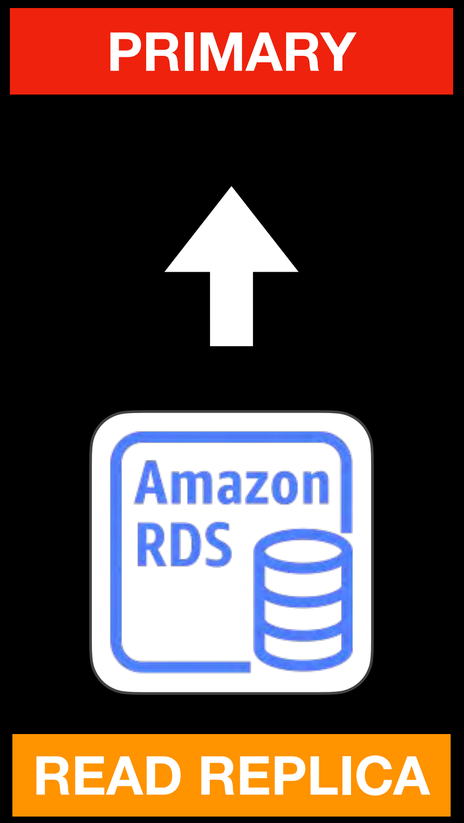
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Can be promoted to be a standalone DB instance
- Useful for:
  - Database sharding
  - Implementing failure recovery
  - Performing Data Definition Language (DDL) operations
- **Lessens the impact to the primary DB** instance brought by rebuilding indexes, scheduled jobs, and other processing
- Helpful if your primary AWS Region experiences an outage
- **Can be deployed to a different AWS Region** and be promoted as the primary DB instance in the event that the AWS Region of your source/primary database experiences a downtime

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA

- **Cannot directly create an encrypted Read Replica** from an unencrypted database instance
- Can be created from your encrypted database instances but not from the unencrypted ones
- An **encrypted cross-region read replica** can be launched as long as the target region and an encryption key in AWS KMS for that particular region are supplied
- Allows the use of a **custom encryption key** or the default encryption key for Amazon RDS that is created by AWS KMS in each region

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA

USE CASES

- Suitable if your company has a web application with a **built-in reporting** module
- If your department or application **runs large SQL queries every month that impact your database's performance** due to high usage
- If you need to minimize the impact that the reporting activity has on your application by **offloading the read requests**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA

USE CASES

- If you need to **separate the read requests from the write requests** of your application
- If you have an application wherein the **read operations are causing high I/O usage to your primary RDS database instance** which then results in high latency to the write requests in your production environment
- If you have application modules or reporting tools that only send `SELECT` queries. You can **configure the reporting module to use the Read Replica endpoint** and direct the transactional operations to the primary database instance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA

USE CASES

- If you have **3rd-party applications** or other internal systems that query your database instance heavily
- If you have an internal batch processing job that fetches reporting data from your RDS DB instance.
- **If your entire database slows down significantly** whenever your batch runs which impacts the overall read and write performance of your application
- If you need to configure your internal systems to fetch data from the replica instead of the primary instance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



READ REPLICA

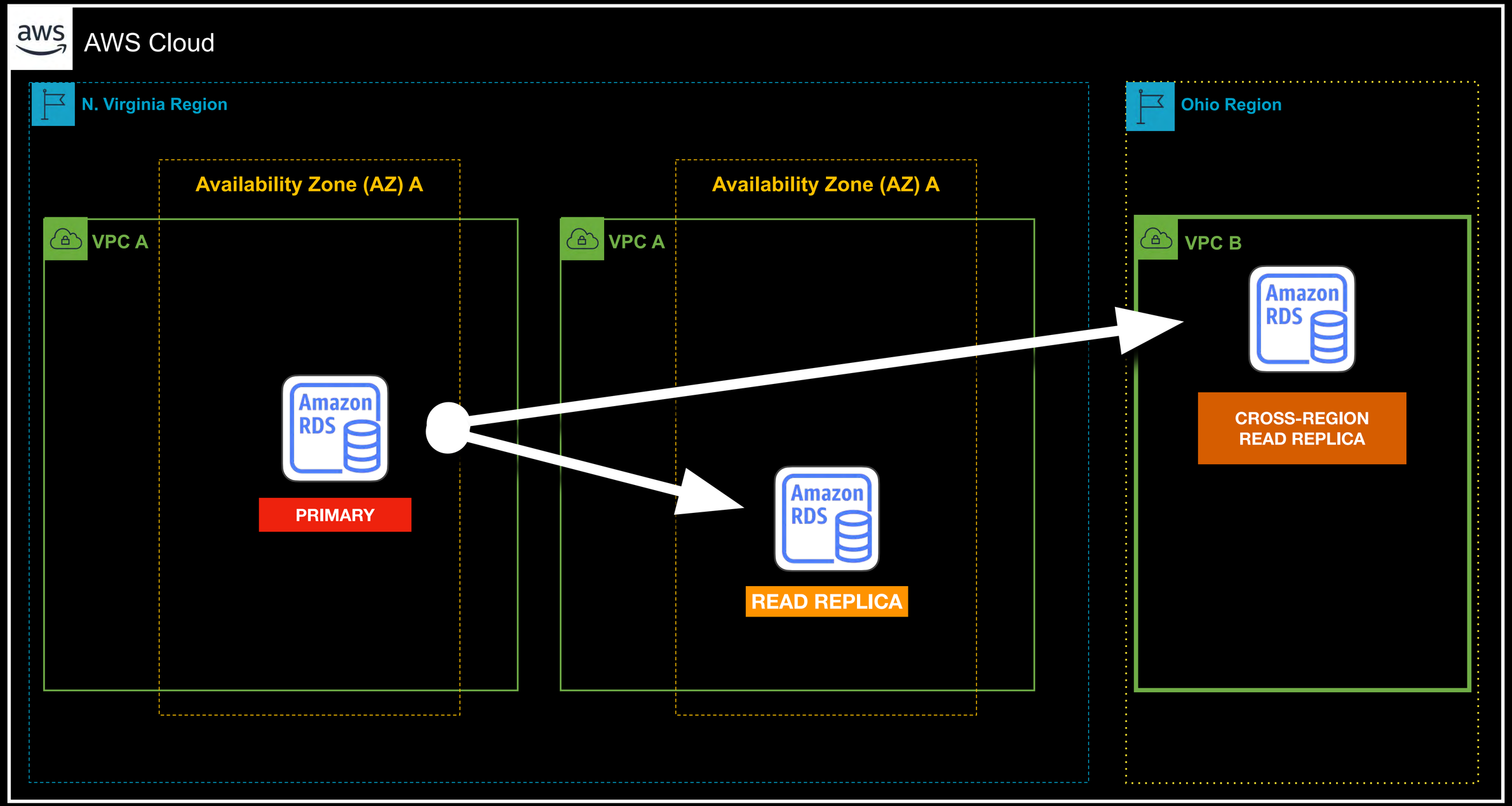
ANTI-PATTERNS

- A Read Replica is primarily used to **improve the scalability of your application** in terms of read operations and not for improving the availability of your database

- Cannot be used for ensuring that the database will be highly available in the event of an outage. You have to use the Multi-AZ Deployments configuration instead

- Unlike Multi-AZ RDS, a Read Replica doesn't have an automatic failover. If the primary DB instance experienced an outage, the incoming requests are not automatically routed to the Read Replica by default

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon RDS
Multi-AZ Deployments

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SYNCHRONOUS REPLICATION



STANDBY REPLICA

REPLICA

a copy of your primary database

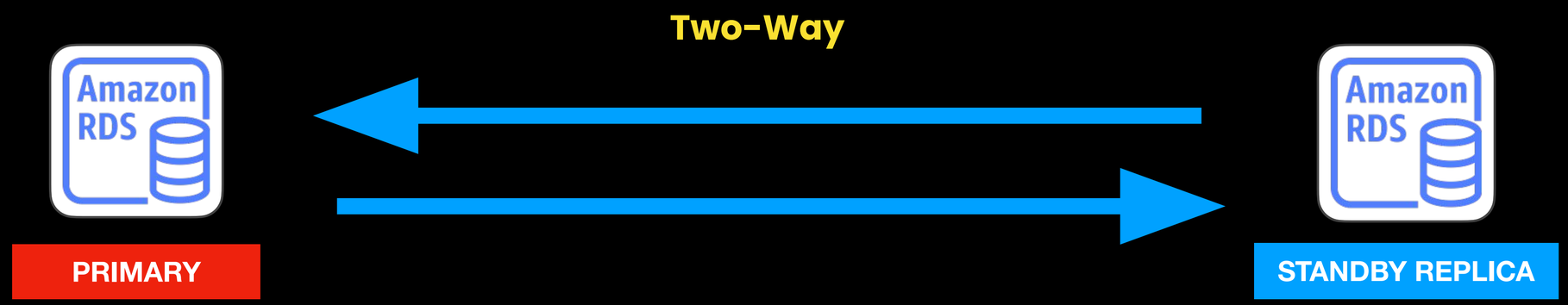
ASYNCHRONOUS REPLICATION



READ REPLICA

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SYNCHRONOUS REPLICATION



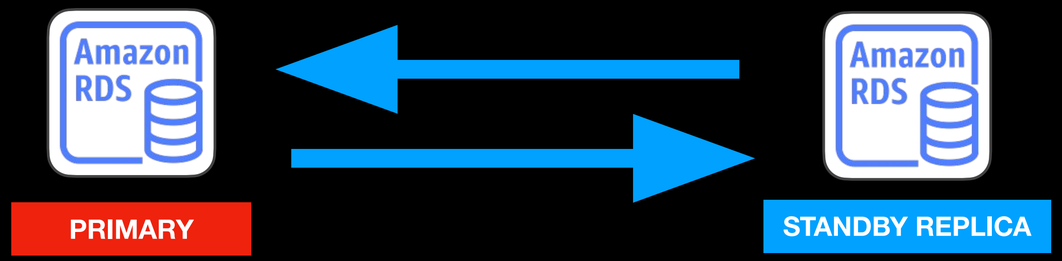

```
INSERT INTO CITIES (Name, Country)
VALUES ('Manila', 'Philippines');
```

```
INSERT INTO CITIES (Name, Country)
VALUES ('Toronto', 'Canada');
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SYNCHRONOUS REPLICATION

Two-Way



ASYNCHRONOUS REPLICATION

One-Way




```
UPDATE CITIES
SET City= 'Mumbai'
WHERE CITY_ID = 1;
```

```
UPDATE CITIES
SET City= 'Chicago'
WHERE CITY_ID = 2;
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

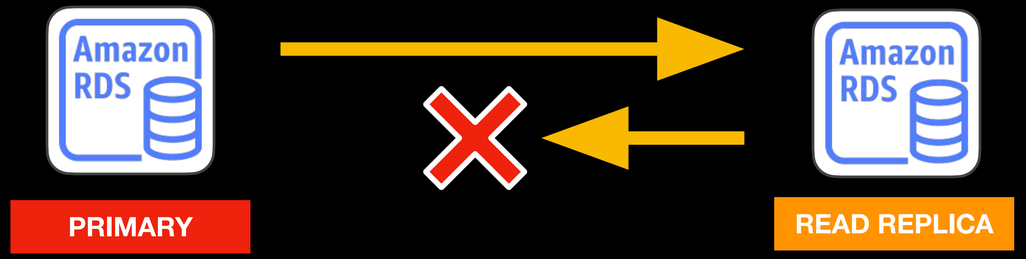
STANDALONE

Single DB Instance (*Single AZ*)

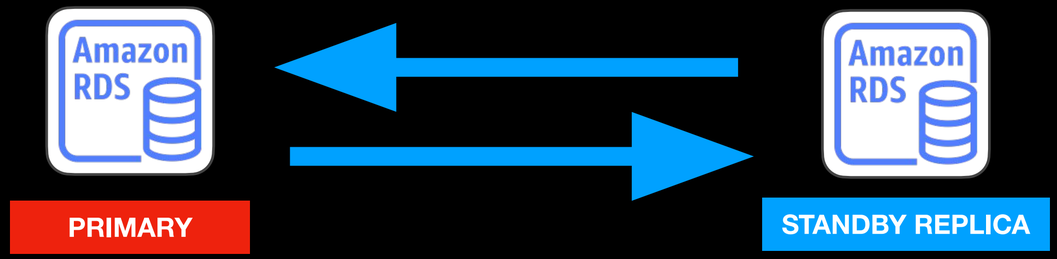


MASTER-SLAVE CONFIGURATION

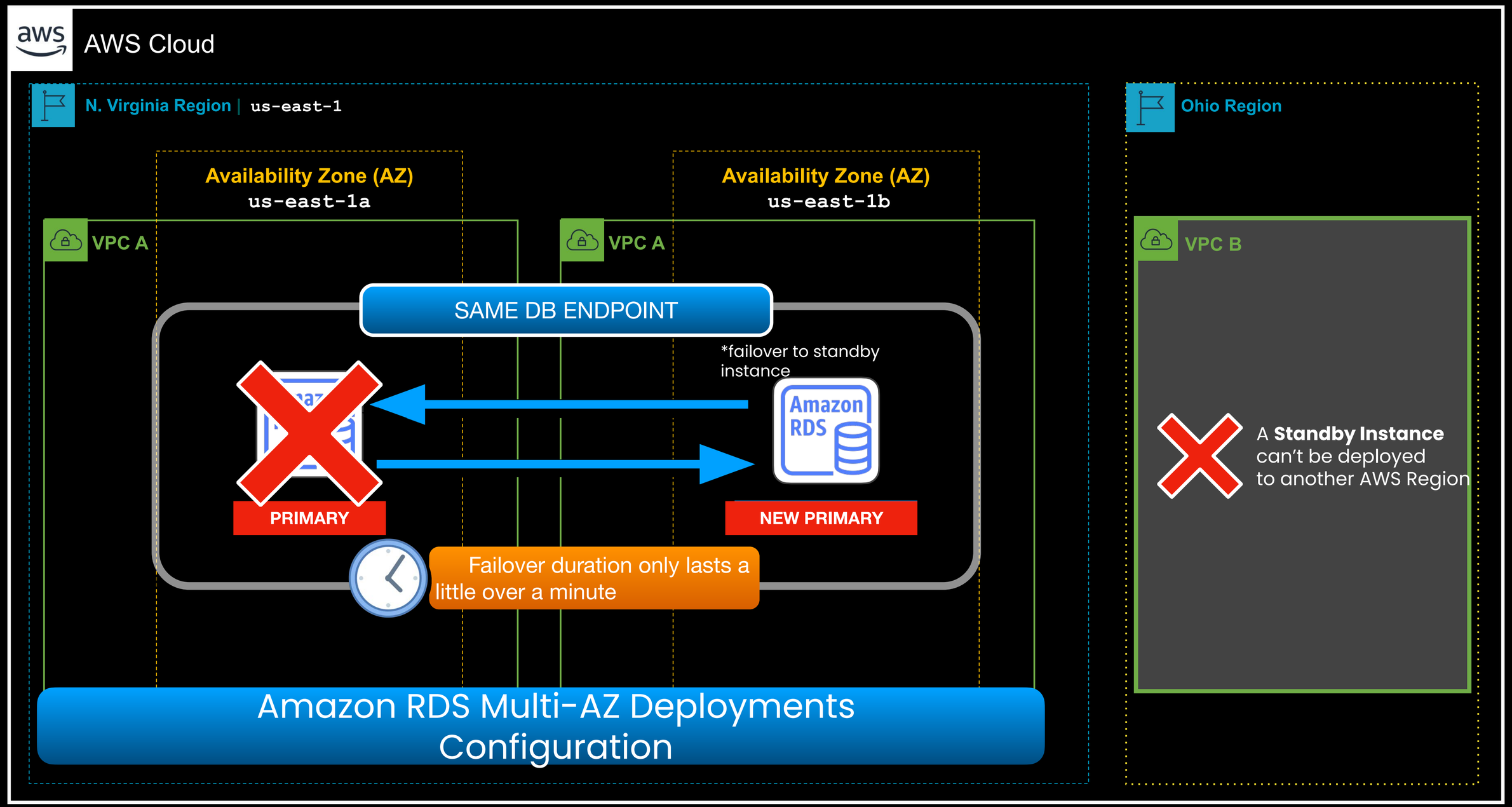
Read Replica



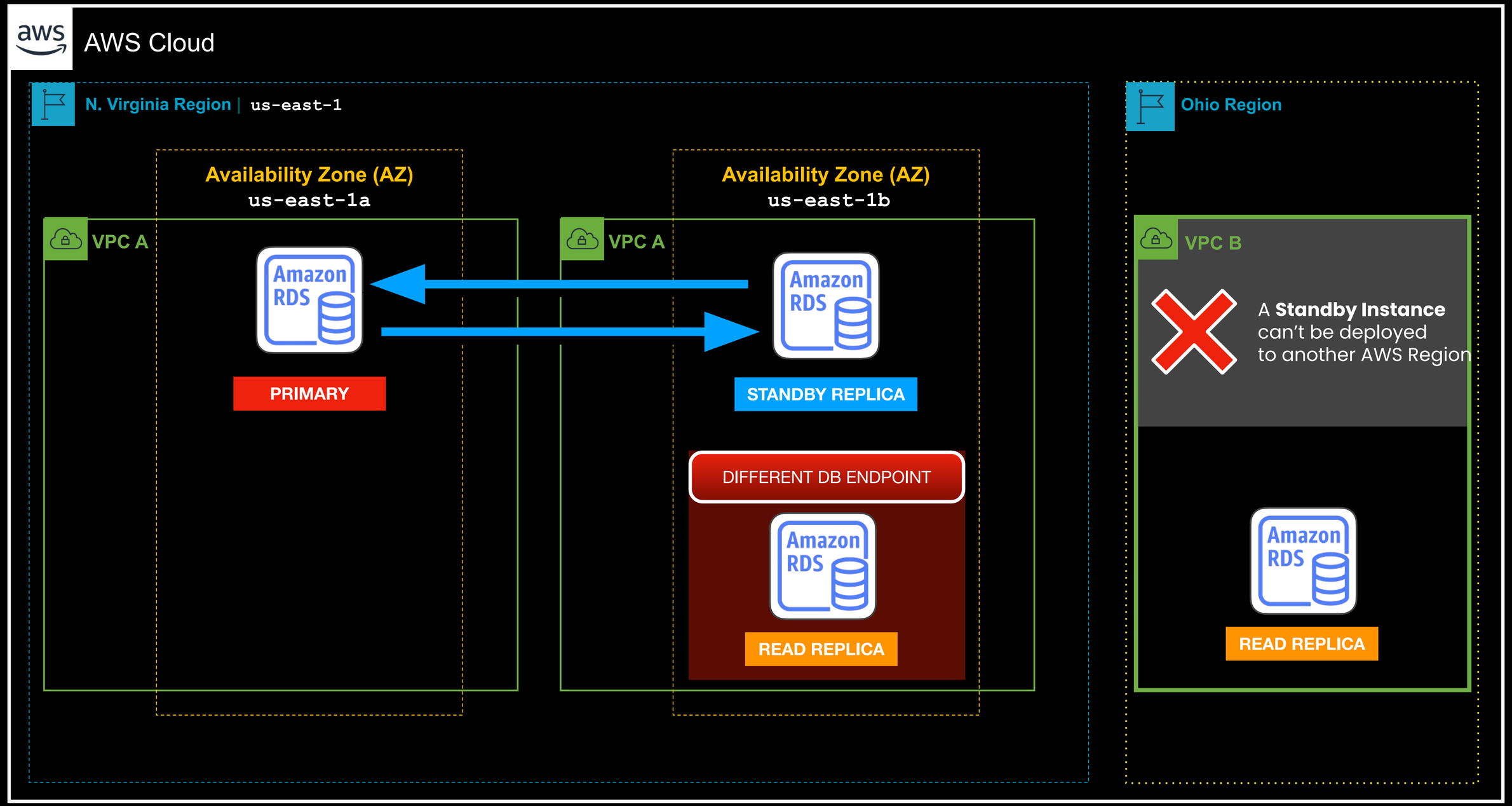
Multi-AZ Deployments



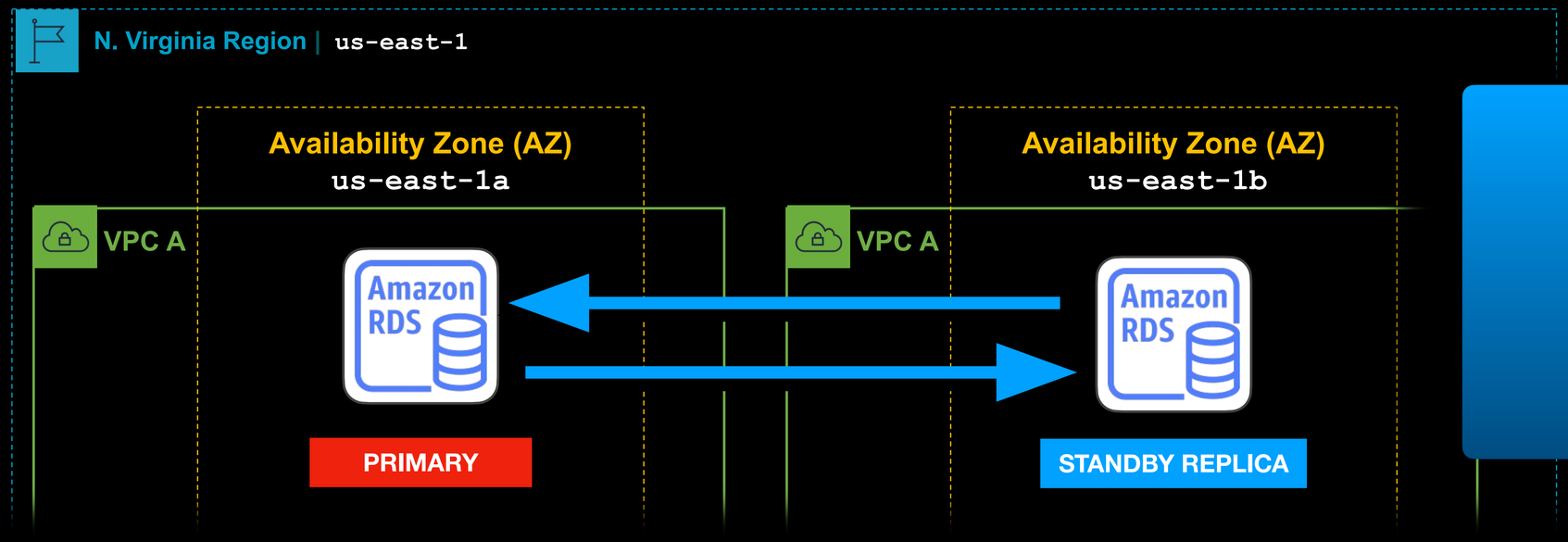
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



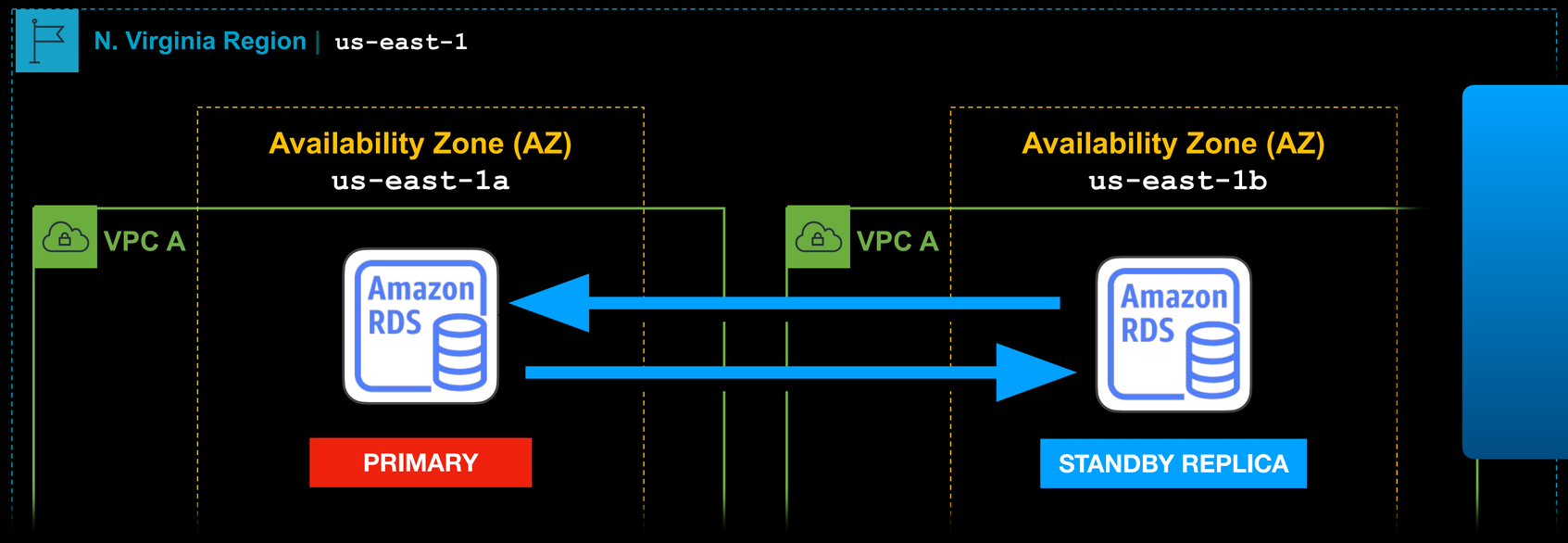
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon RDS Multi-AZ Deployments Configuration

- **Provides High Availability**
- **Improves Data Redundancy**
- **Minimizes latency spikes during system backups**
- **Keeps your database available on your planned system maintenance or DB Engine upgrade**
- **Protects your database against DB instance failure and disruptions when an Availability Zone outage occurs**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

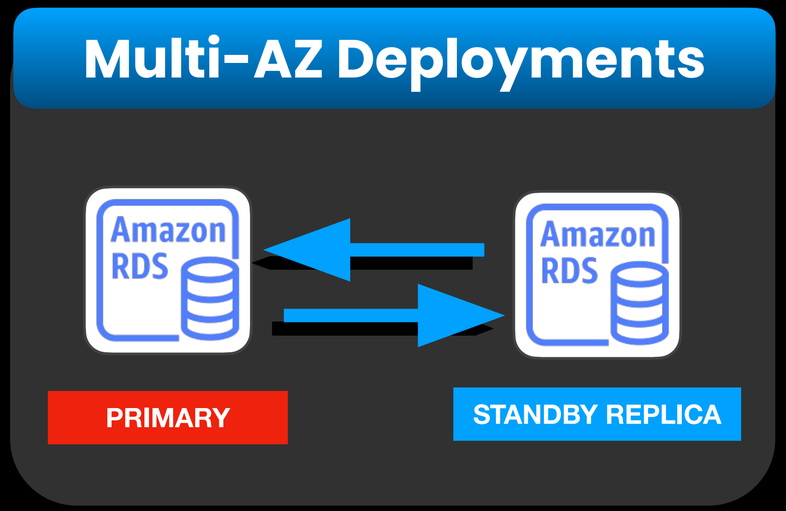


Amazon RDS Multi-AZ Deployments Configuration

Multi-AZ Deployments Configuration – Internal Steps

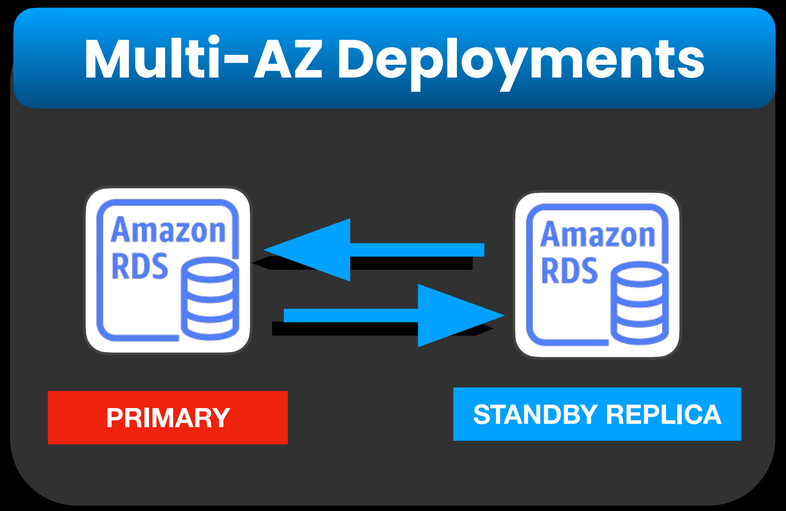
1. **Takes a snapshot of your primary DB instance**
2. **Launch a new Standby Instance in a different Availability Zone**
3. **Automatically configure synchronous replication between the primary and standby instances**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



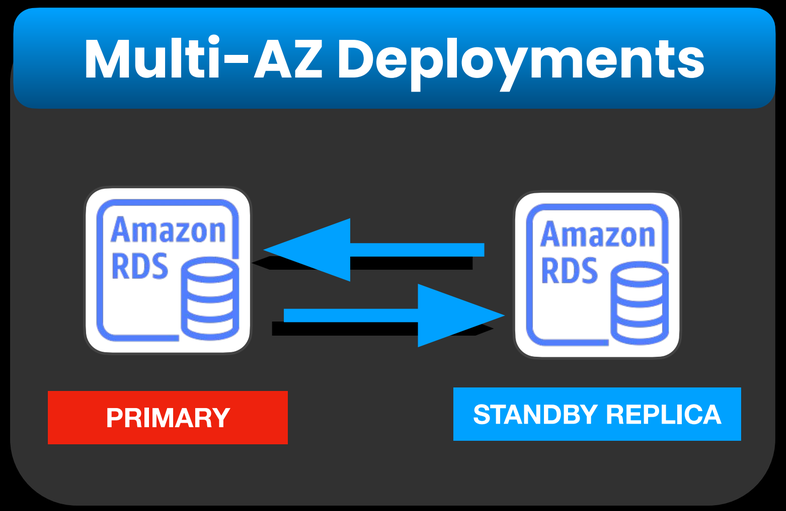
- Amazon RDS uses an internal Amazon EC2 instance that has its own operating system and attributes
- **Maintains database performance while the regular process of patching the database engine** is on-going
- **Ensures the availability of your database** when the OS and its underlying hardware go through its scheduled maintenance activities

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- During an AWS-initiated hardware maintenance, a Multi-AZ database will only have a **minimal disruption** unlike a Single-AZ database
- Your database will only be unavailable during the primary DB instance **failover to the Standby Replica**
- The duration of the failover process to the Standby Replica is only about 1 minute or so

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



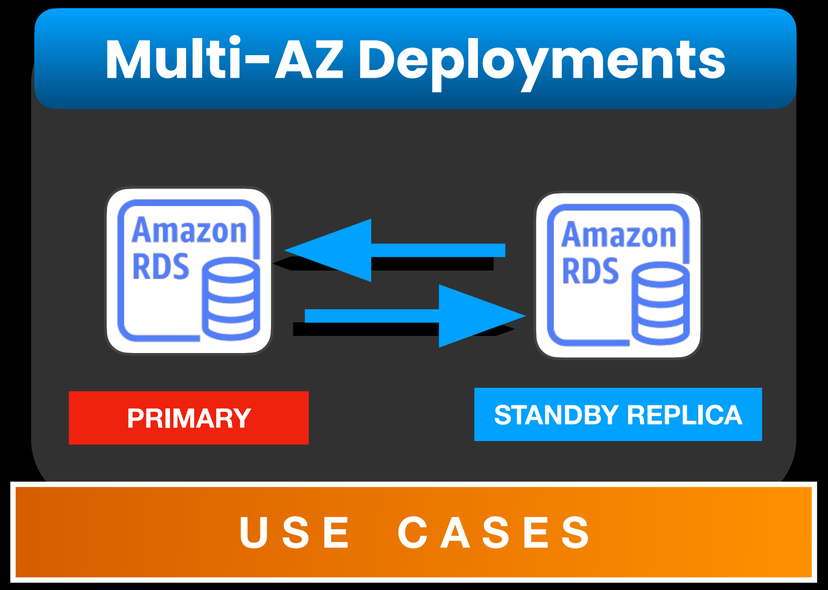
- When the automatic failover in Amazon RDS occurs, the **Canonical Name record (CNAME)** of your DB instance is automatically altered to point to the newly promoted Standby Instance

- If **AWS conducts a hardware maintenance on the Availability Zone where your Standby Replica is hosted**, your Multi-AZ RDS database will not experience any failover or downtime

- The **Operating System (OS) patch will be applied to the Standby Replica** first before it is installed to the primary instance

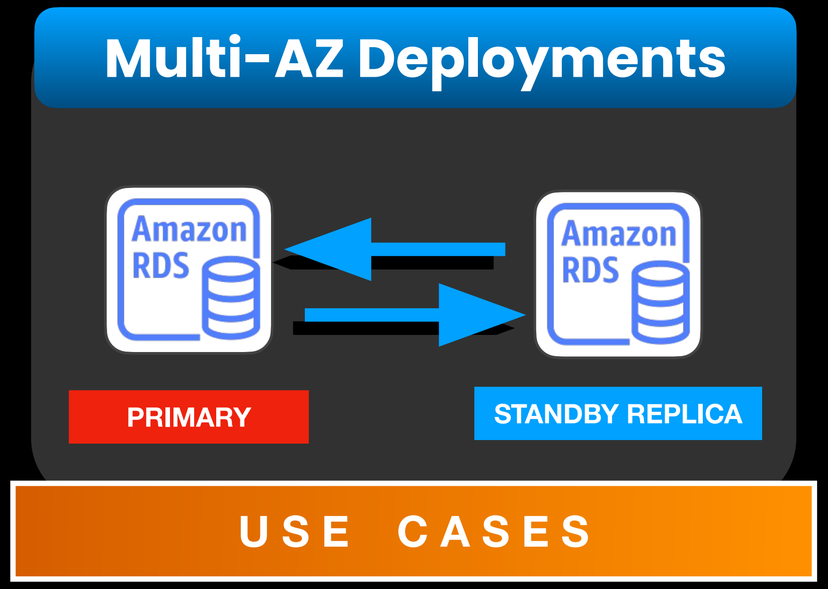
- The only downtime would be the failover process

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



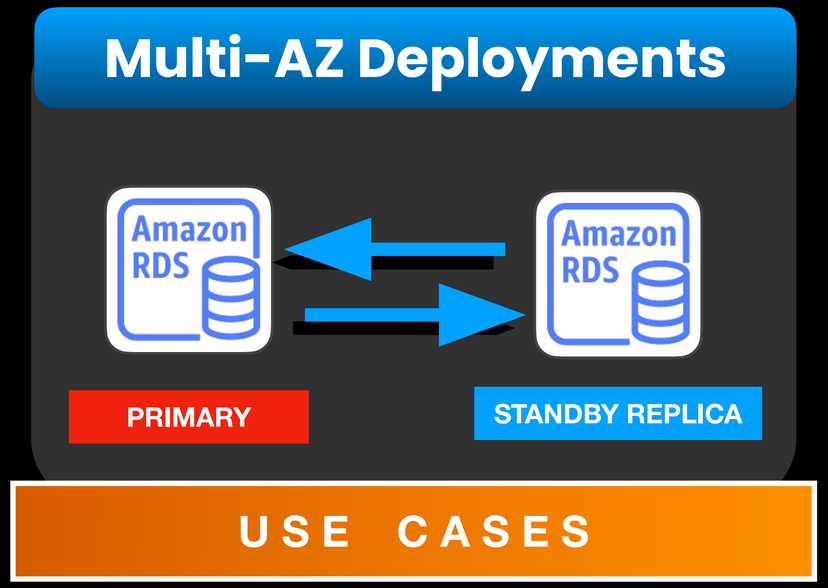
- Suitable for **mission-critical applications where you need the highest availability** while minimizing your operational and management overhead.
- Applicable if you have an application running in your production environment that uses a single-instance RDS database
- If you want to migrate your existing database running on your on-premises network, that is running on a single database configuration
- If you are required to **eliminate single points of failure in your architecture**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- For minimizing database downtime **without requiring any changes to your application code**
- For enterprise systems that need to be **highly available with low operational complexity**
- For any scenario where **the availability of your database is the highest priority/most important requirement** and not its scalability

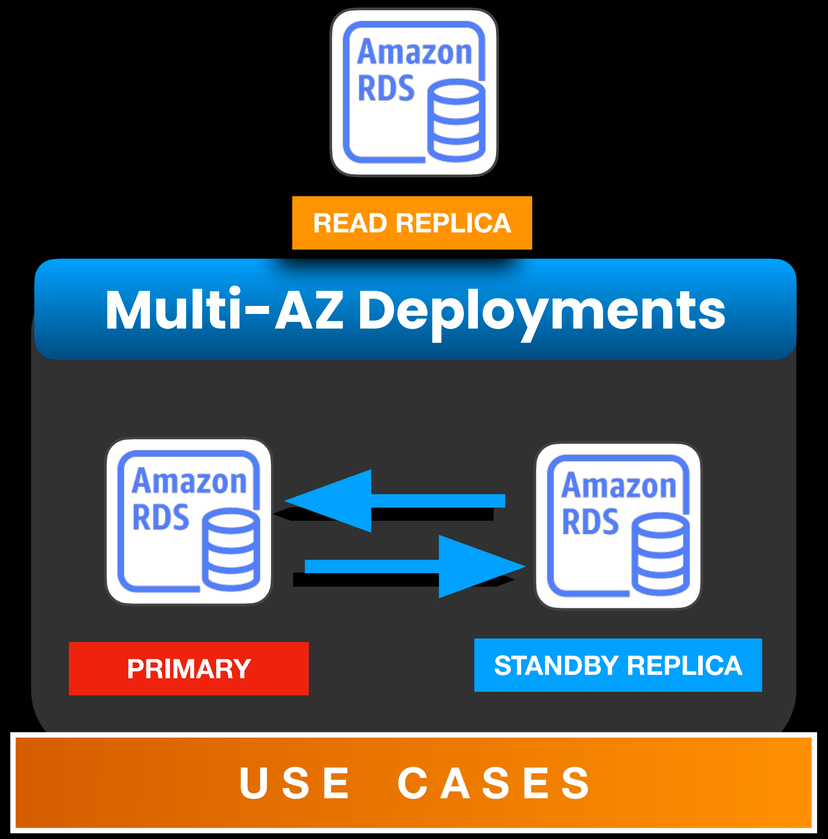
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- **For poorly-designed architectures that needs to be re-designed/refactored, such as:**
  - A three-tier application architecture runs in public and private subnets
  - The application is running on a **single Amazon EC2 instance** that is hosted in the public subnet
  - A **single Amazon RDS database** running on the private subnet

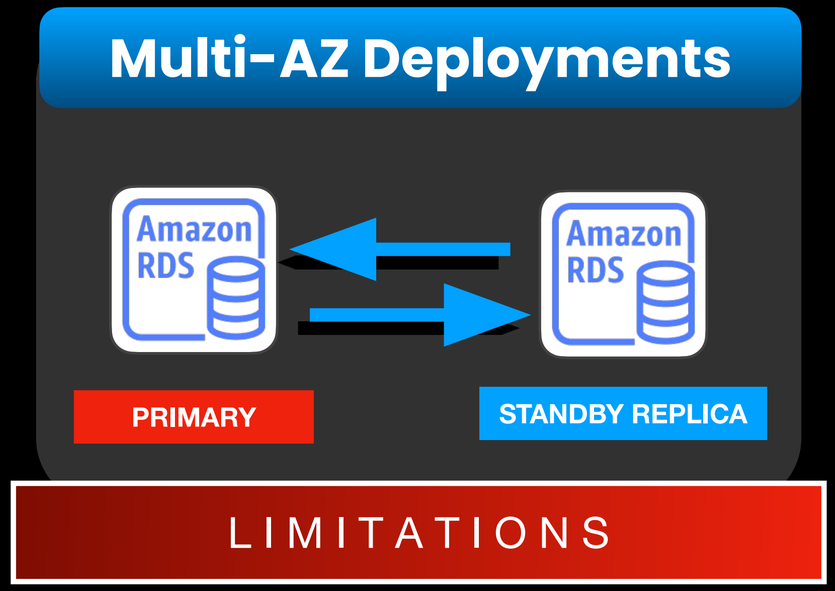
- **Improved architecture:**
  - Launch an Auto Scaling group of EC2 instances behind an Application Load Balancer that spans multiple AZs
  - Enable the Multi-AZ Deployments configuration in Amazon RDS to **make the database tier highly available**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



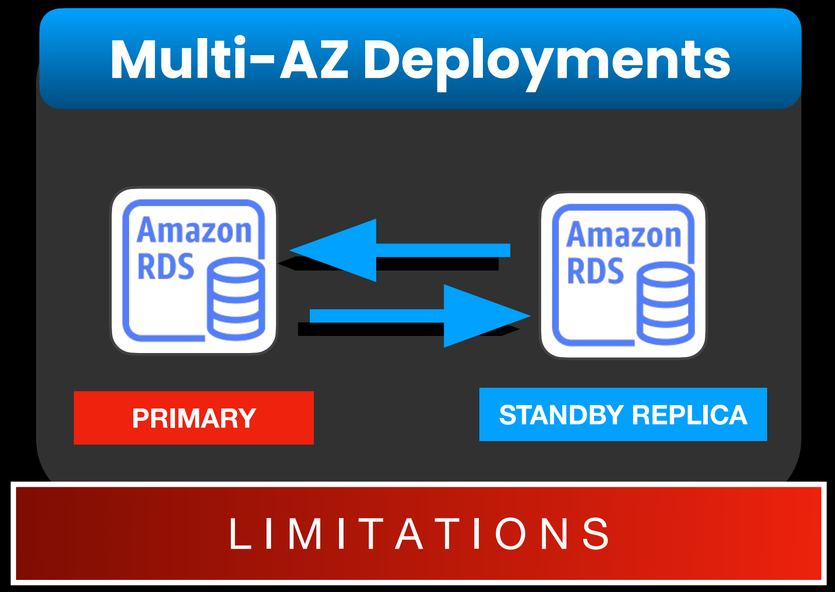
- You can **combine Multi-AZ Deployments configuration with Read Replicas**
- A Read Replica can provide **cross-region database replication for multi-Region disaster recovery**, which a Multi-AZ Deployment configuration can't provide
- Having both Standby and Read Replica ensures both high availability and scalability of your database tier

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- A Multi-AZ database can provide high availability in a **single AWS Region only**
- You cannot deploy a Standby Replica to another AWS Region
- **Does not provide multi-region disaster recovery**
- The Standby Replica cannot be used to read or write your application data, or accept live traffic
- **Cannot be used this to scale your application** in terms or read performance or handle the increased number of queries to your database

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Not suitable if the required Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are quite short

- **It cannot provide an RPO of 1 second and an RTO of 1 minute**

- If you have this requirement, you have to use:

Amazon Aurora Global Databases

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



RDS Proxy

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

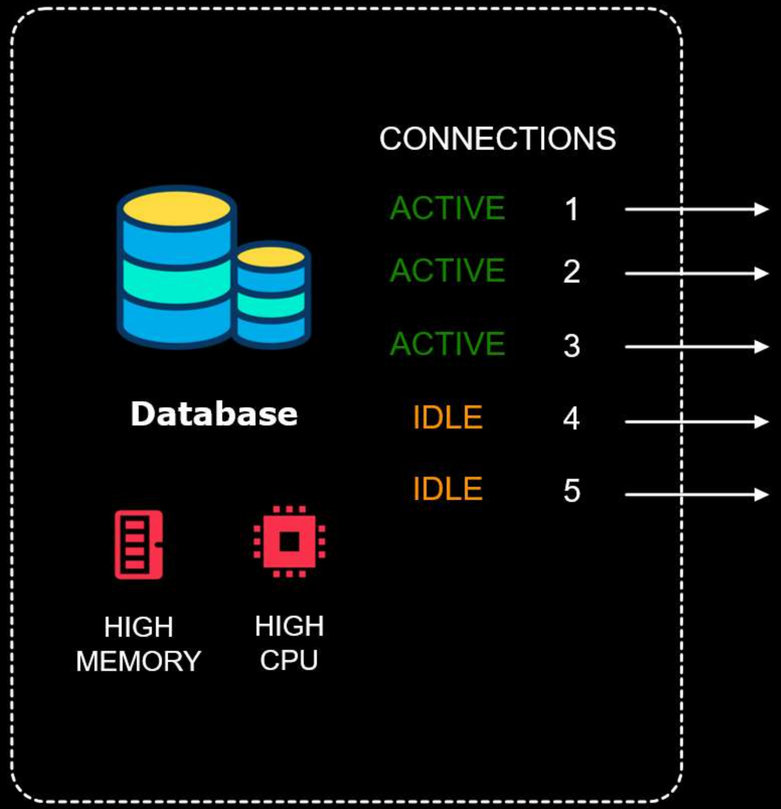


RDS Proxy

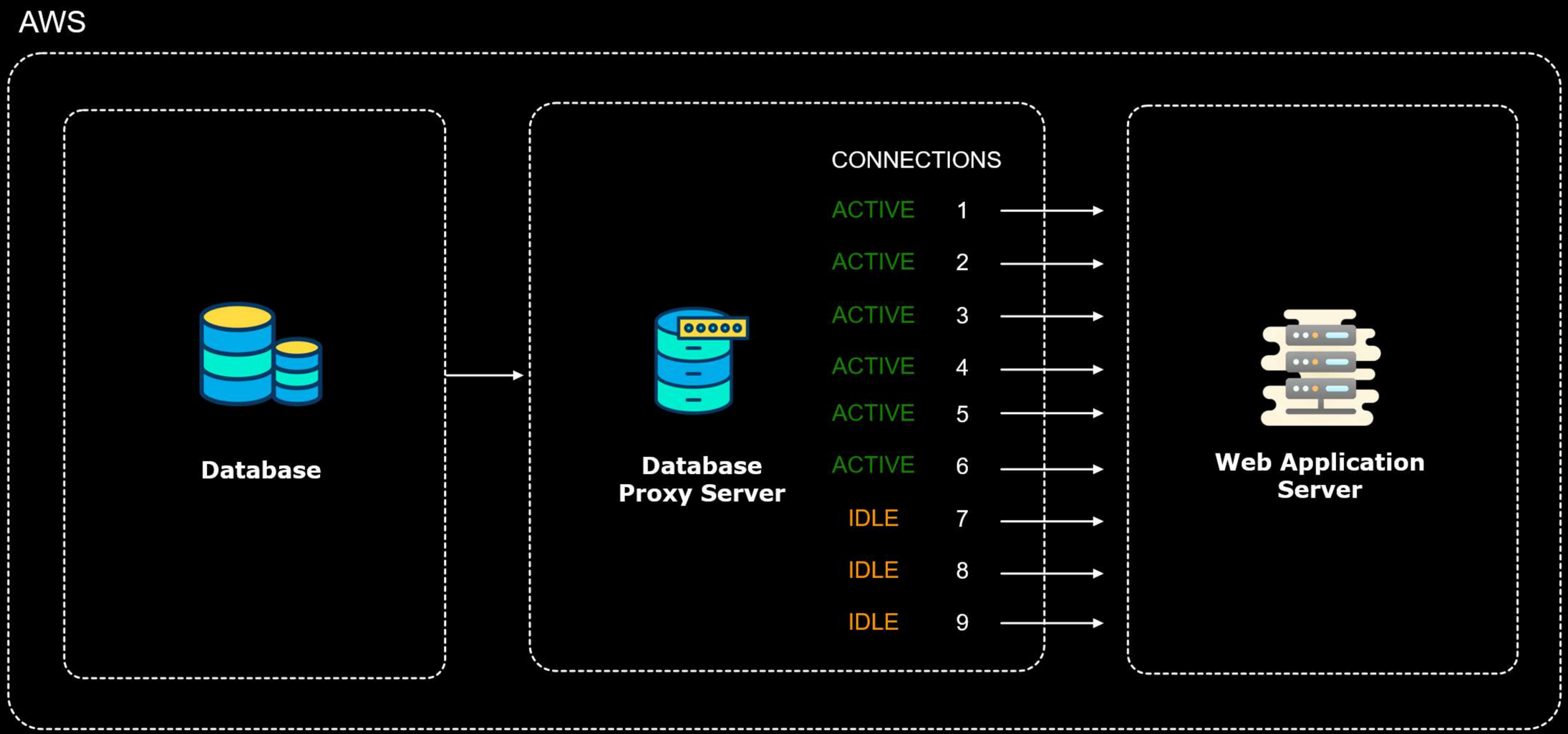
In this lecture, you will be able to:

- learn what is a database proxy server
- understand the benefits of using RDS Proxy
- analyze when to use RDS Proxy in an infrastructure

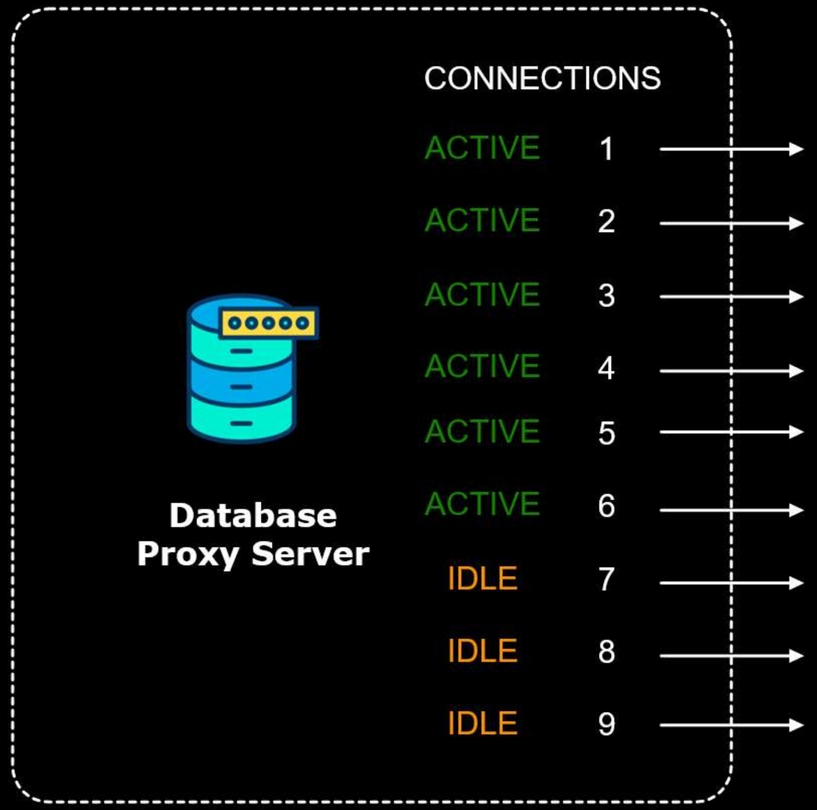
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Database Proxy Server

- enables scaling by providing a pool of established connections to the backend databases
- the pool of connections helps in reducing the stress of the database's compute and memory resources
- helps reduce database failover time

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

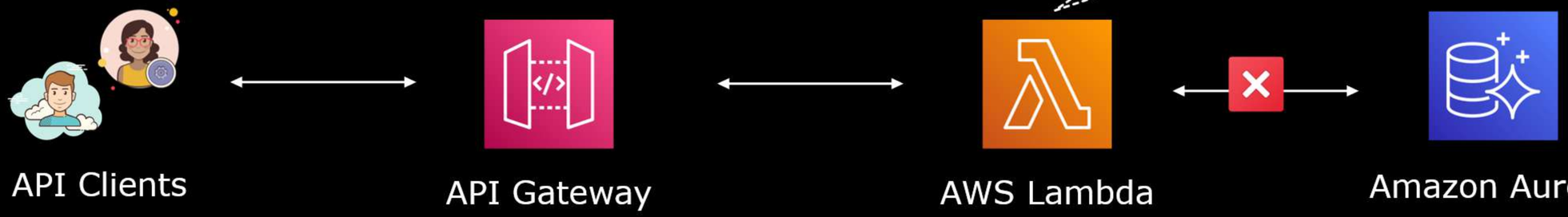


RDS Proxy

What is RDS Proxy?

- a fully managed AWS database proxy server
- has capabilities of a database proxy server without the need to patch and manage a physical server.
- it works with serverless application, container applications, EC2, and ECS instances

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

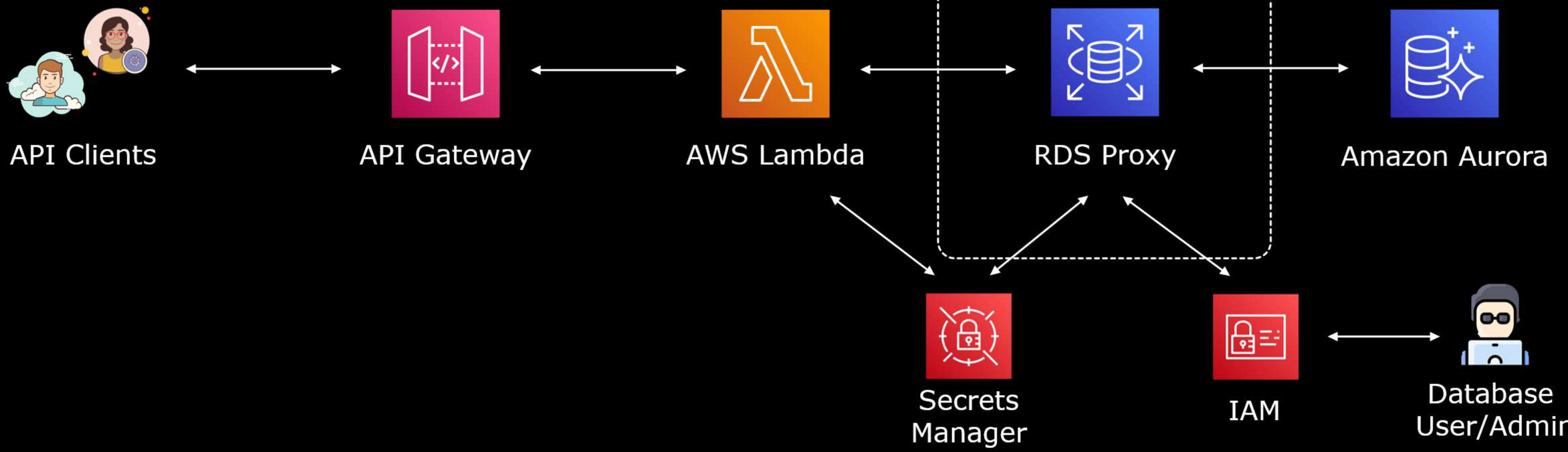


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

You just need to modify the DB connection string in the Lambda function to point to RDS Proxy



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic File System Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic File System

At the end of the lecture, you will be able to:

- explain what Amazon Elastic File System is
- evaluate scenarios where you can use the service

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

OBJECT STORAGE

store and manage data as objects



Simple Storage Service (S3)

BLOCK STORAGE

store your data into blocks



Elastic Block Store (EBS)

FILE SYSTEM STORAGE

allow sharing of files



Elastic File System (EFS)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

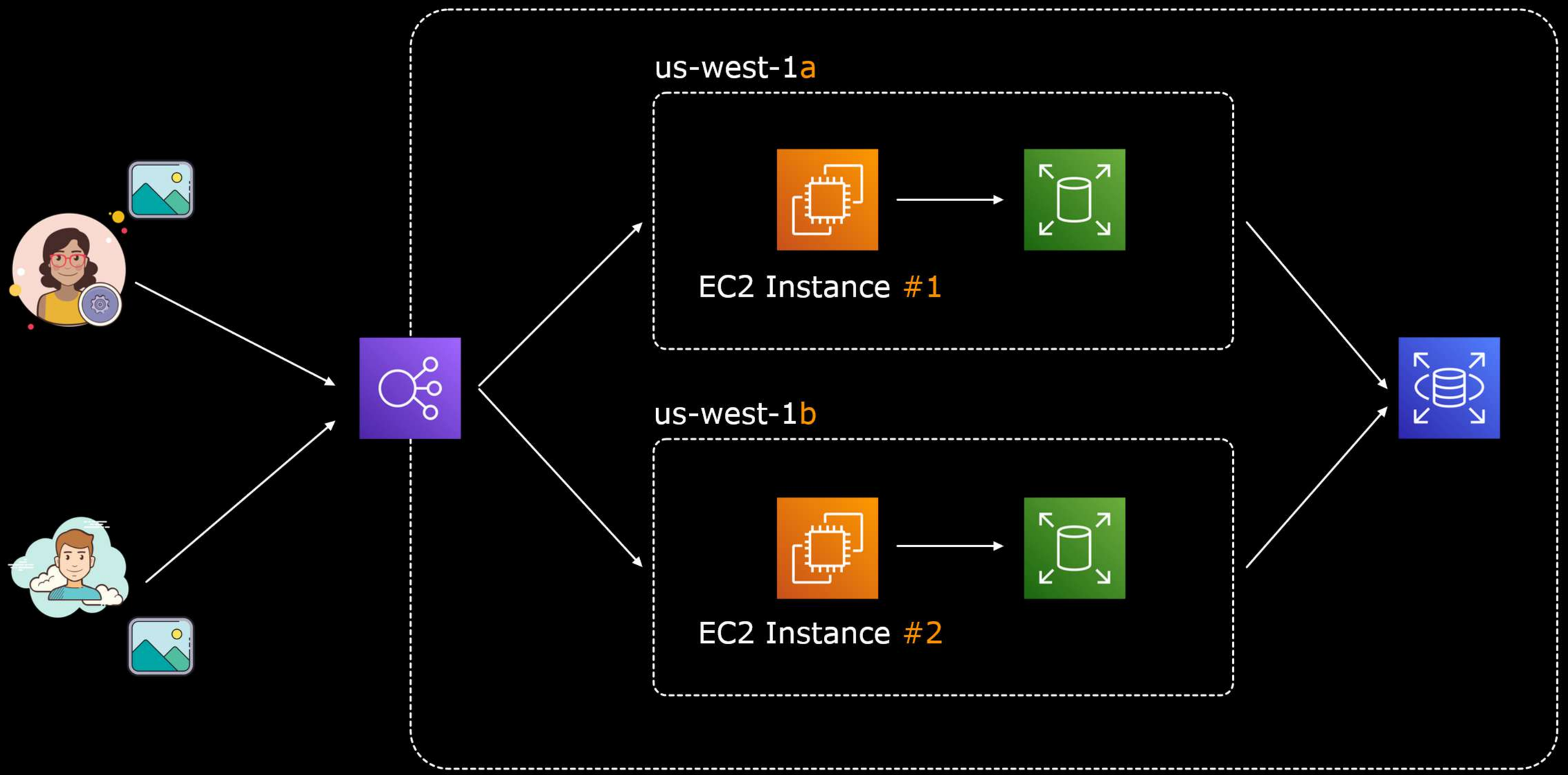


But when exactly would you use the Elastic File System?

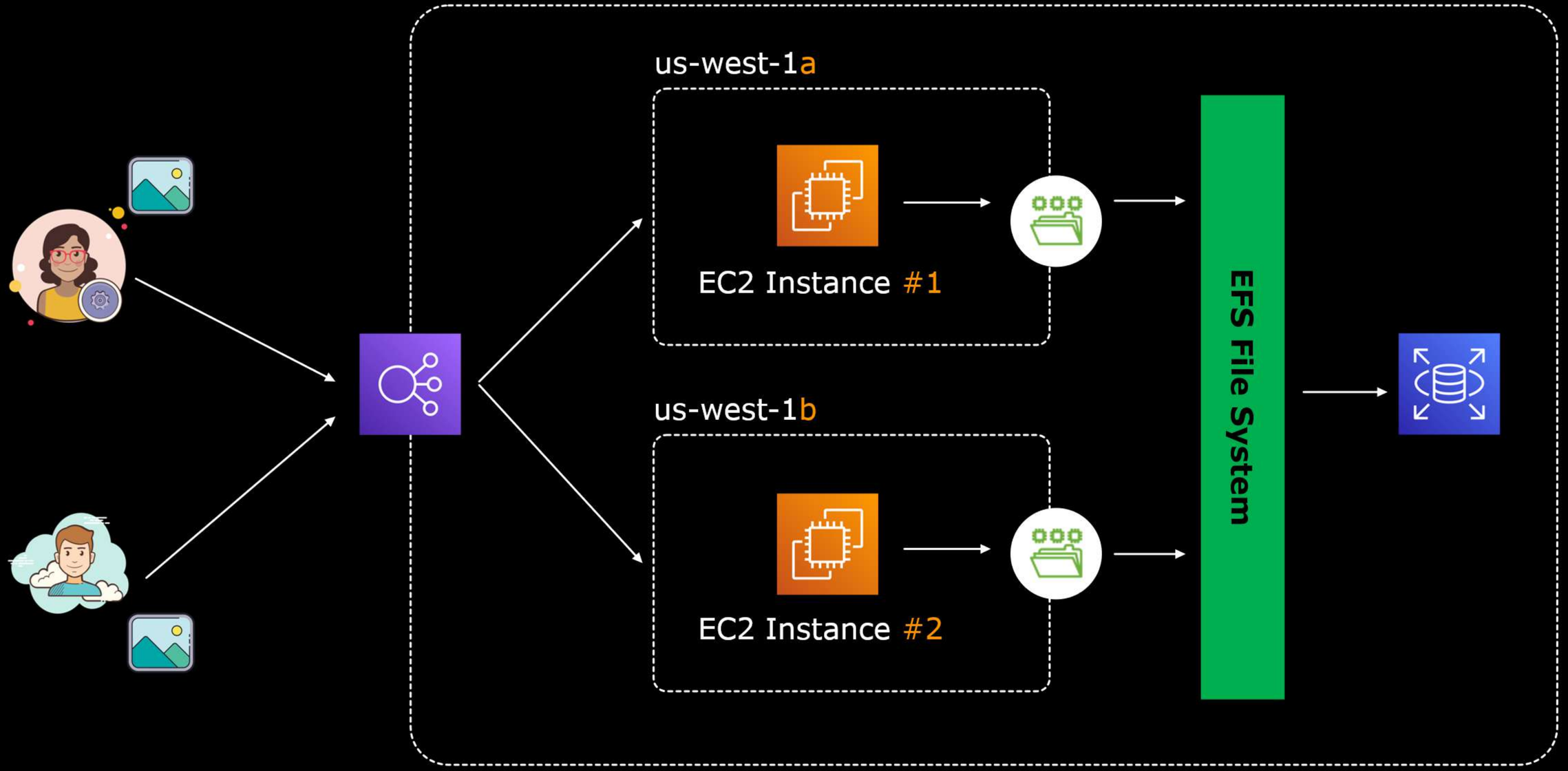
EFS can be used for applications that require a shared file system that can be accessed by multiple computers at the same time.

It can also be used by applications that access data using the standard file system interface provided through the operating system.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic File System

- Amazon EFS provides file systems storage for Linux workloads
- EFS removes the complexity of deploying, patching, and maintaining the underlying infrastructure for the file system
- You can also scale your EFS file system without provisioning new physical servers
- Integrates with AWS KMS to secure your data by encrypting your data at-rest and in-transit.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx for Lustre

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx for Lustre

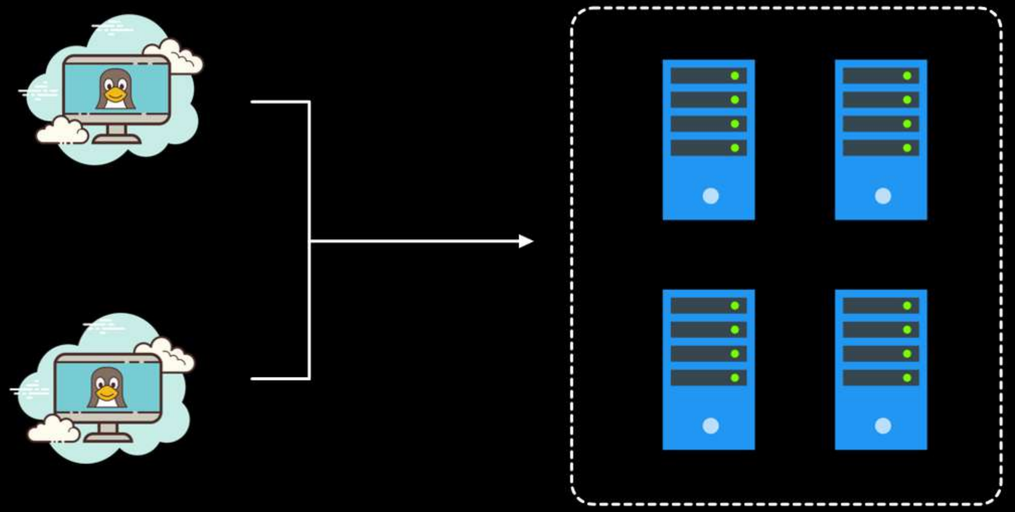
At the end of the video, you will be able to:

- Understand the significance of high-performance computing
- Explain what Amazon FSx for Lustre is

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

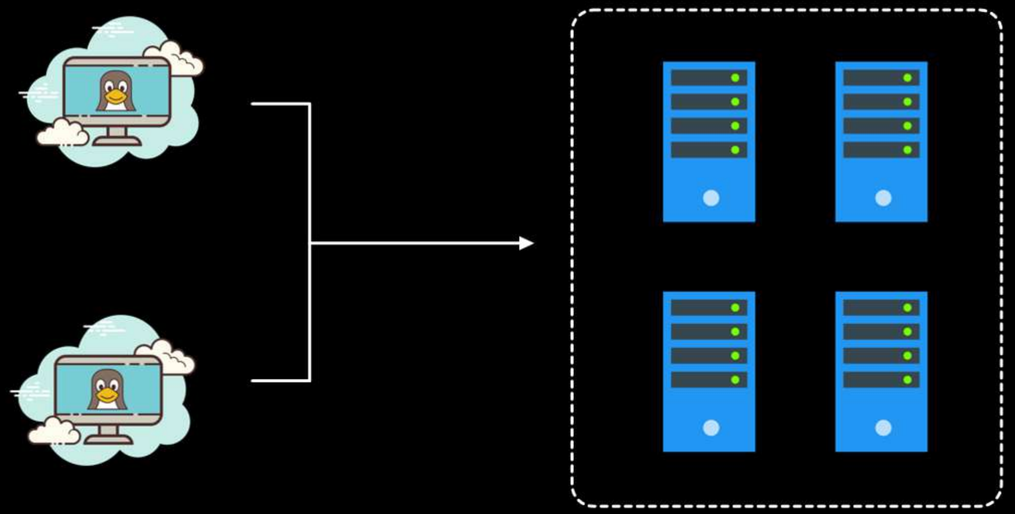


Amazon FSx for Lustre



HIGH PERFORMANCE COMPUTING

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

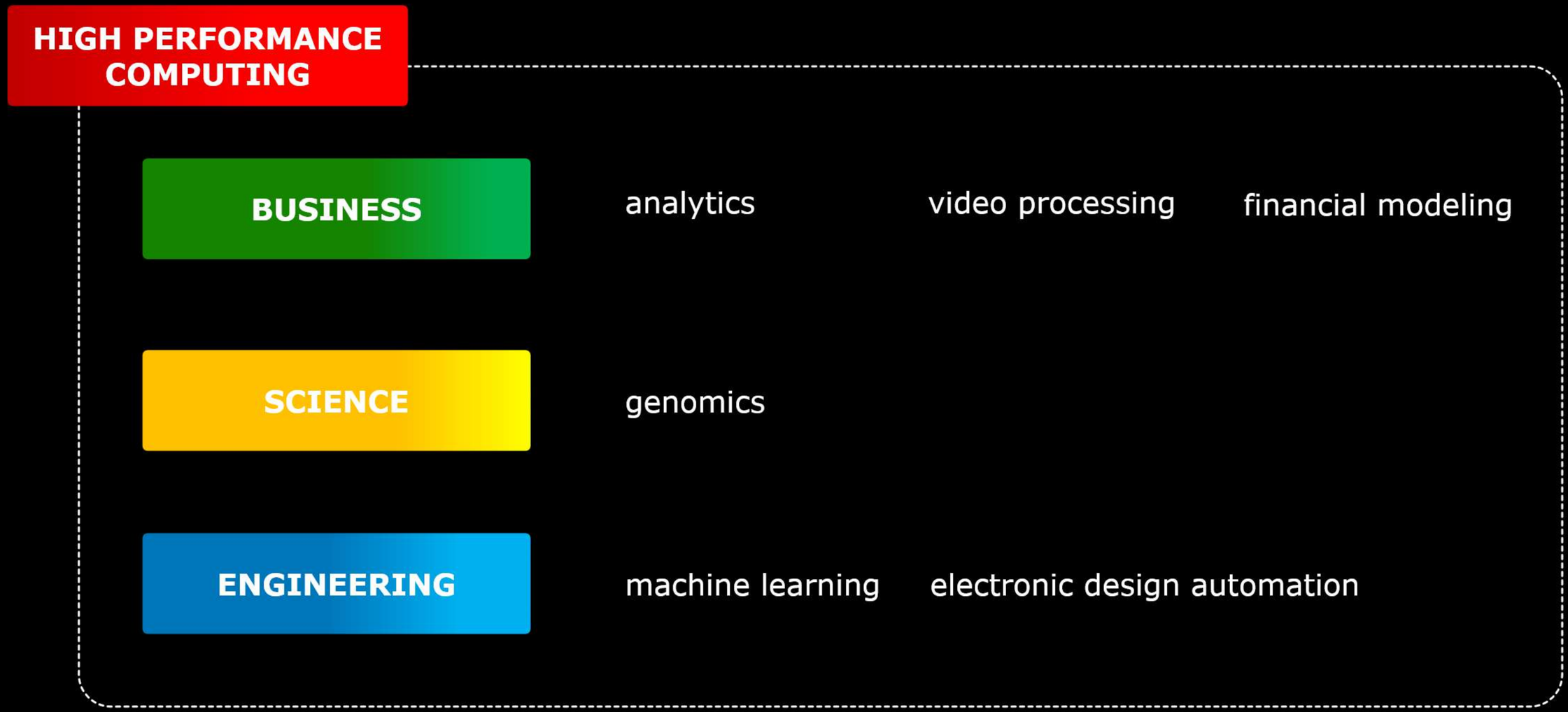


HIGH PERFORMANCE COMPUTING

What is HPC or high-performance computing?

- It's like your everyday computing, only it’s more powerful.
- Refers to the practice of aggregating computing power to deliver much higher “horsepower” than what traditional computers and servers can offer.
- Solves the problem of processing huge volumes of data at very high speeds using multiple computers and storage devices

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

machine learning

analytics

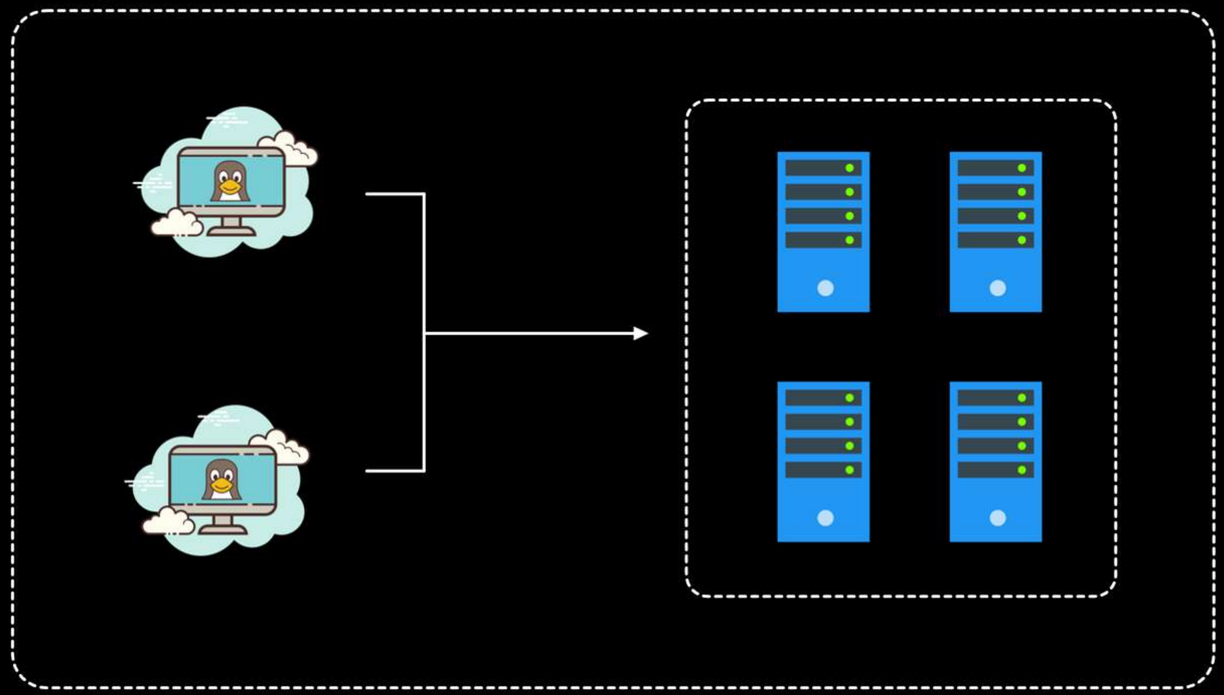
genomics

video processing

financial modelling

electronic design automation

Requires resources that can accommodate high performance computing



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

machine learning

analytics

genomics

video processing

financial modelling

electronic design automation

Requires resources that can accommodate high performance computing



Amazon FSx for Lustre

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx for Lustre

What is Amazon FSx for Lustre?

- a fully managed service by AWS that provides high-performance and scalable file system storage for your HPC workloads

It's basically a **high-performant file system**

- provides a native file system interface that works as any file system does with your Linux operating system.

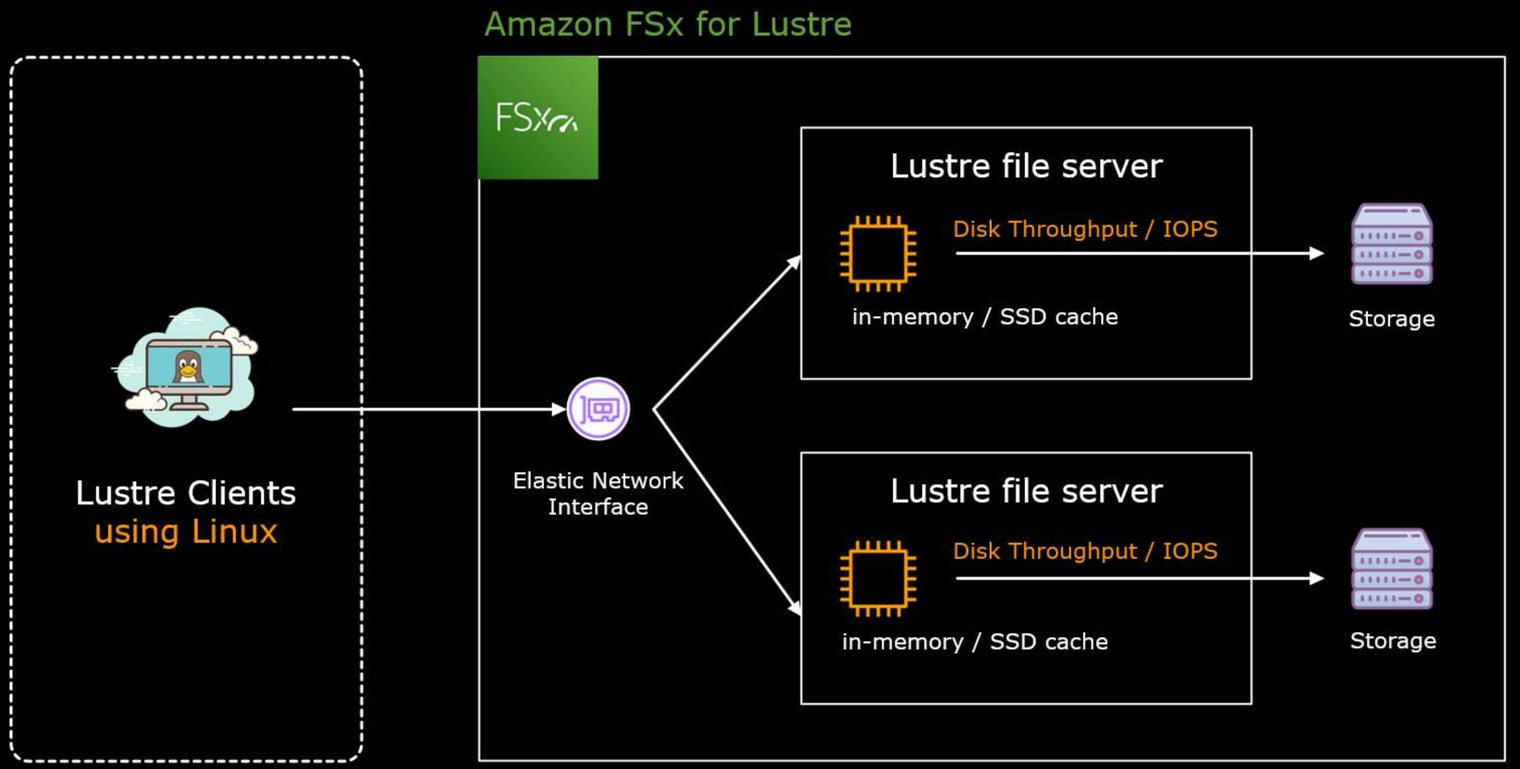
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx for Lustre

Significant features you need to know:

- offers sub-millisecond latencies, up to hundreds of gigabytes per second of throughput, and millions of IOPS
- Amazon FSx is POSIX compliant

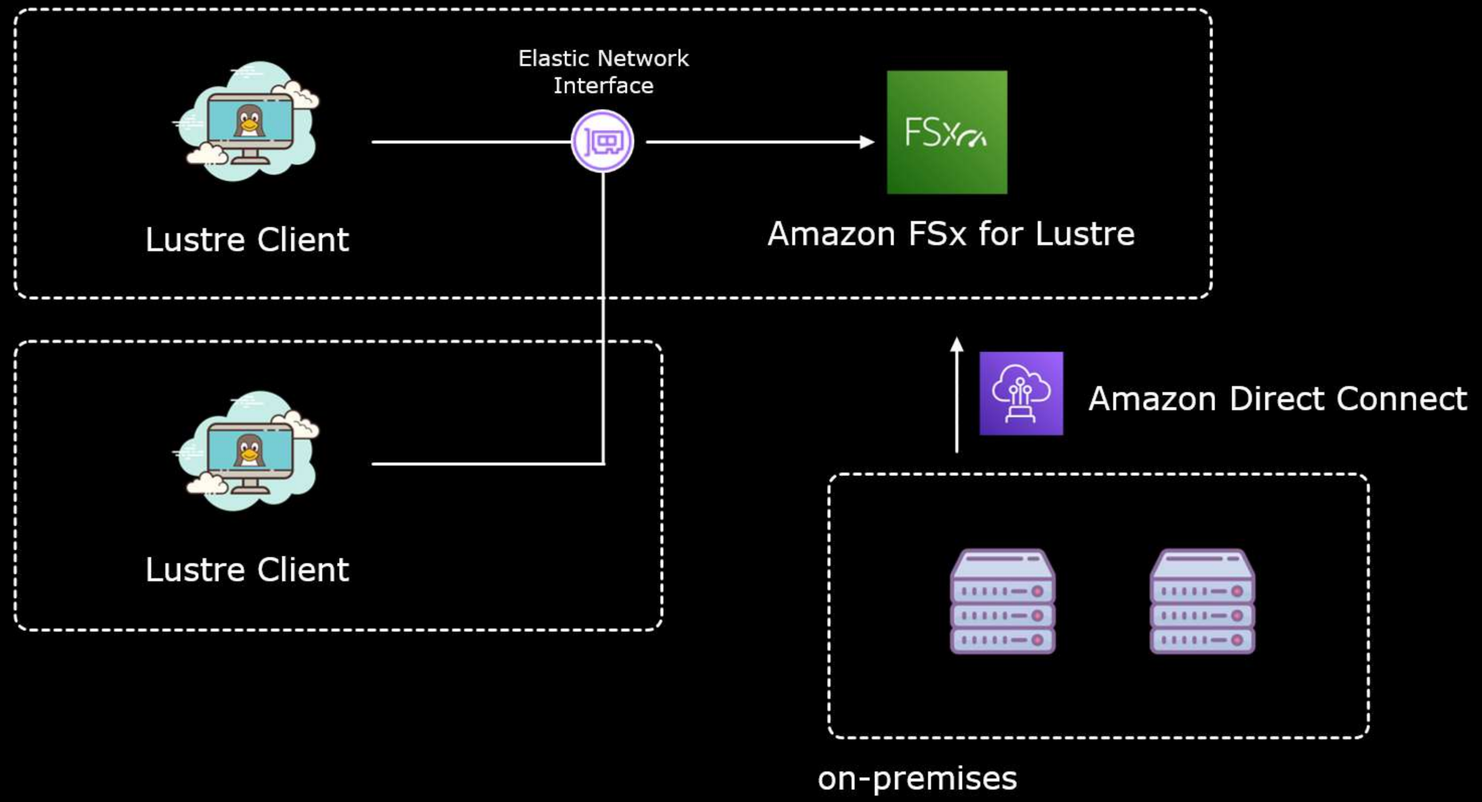


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon FSx for Lustre

Significant features you need to know:

- Link your Amazon FSx for Lustre file systems to data repositories like Amazon S3 or to an on-premises data store.



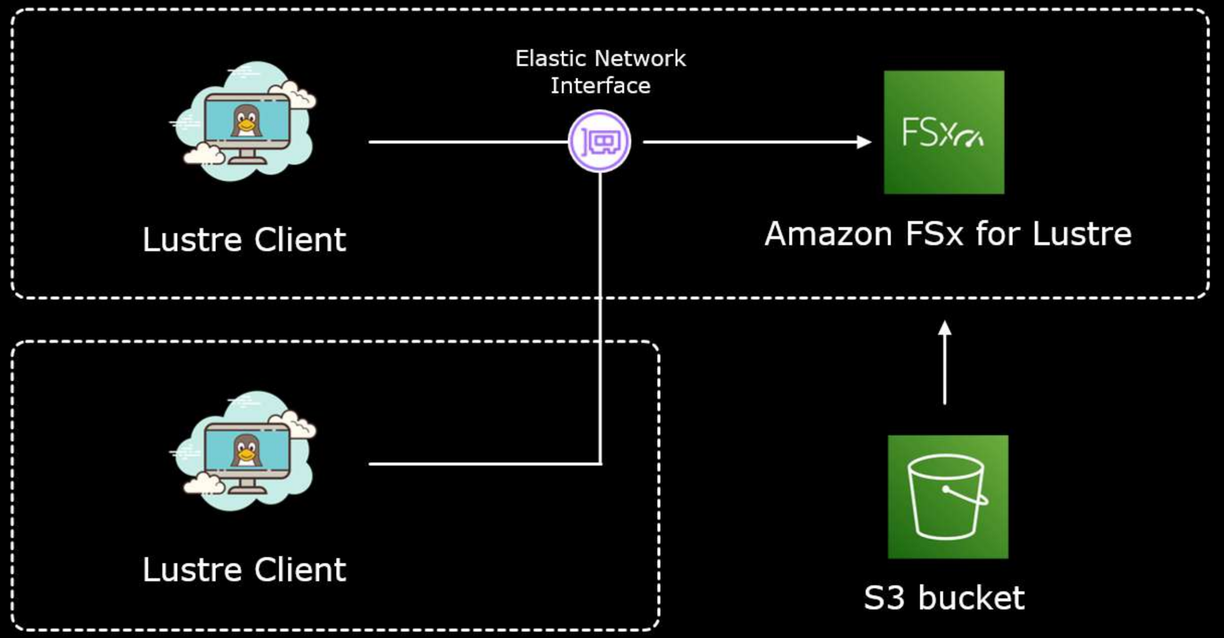
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx for Lustre

Significant features you need to know:

- Link your Amazon FSx for Lustre file systems to data repositories like Amazon S3 or to an on-premises data store.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx for Lustre

Significant features you need to know:

- You can use an SSD or HDDs to store your data
- Integrates well with AWS KMS to encrypt your data at rest using customer-managed keys

Data in transit is also automatically encrypted in certain AWS Regions only when accessed from supported EC2 instances.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx Windows File Server

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

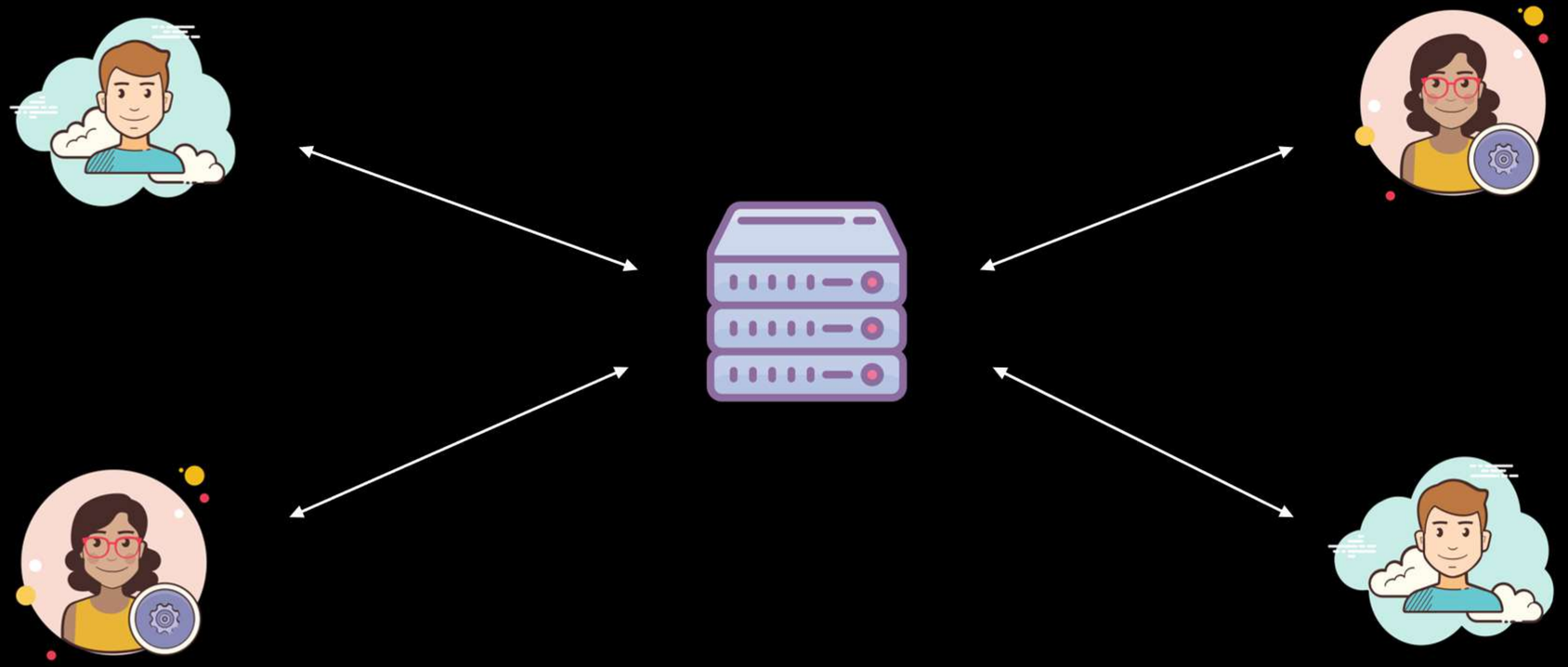


Amazon FSx Windows File Server

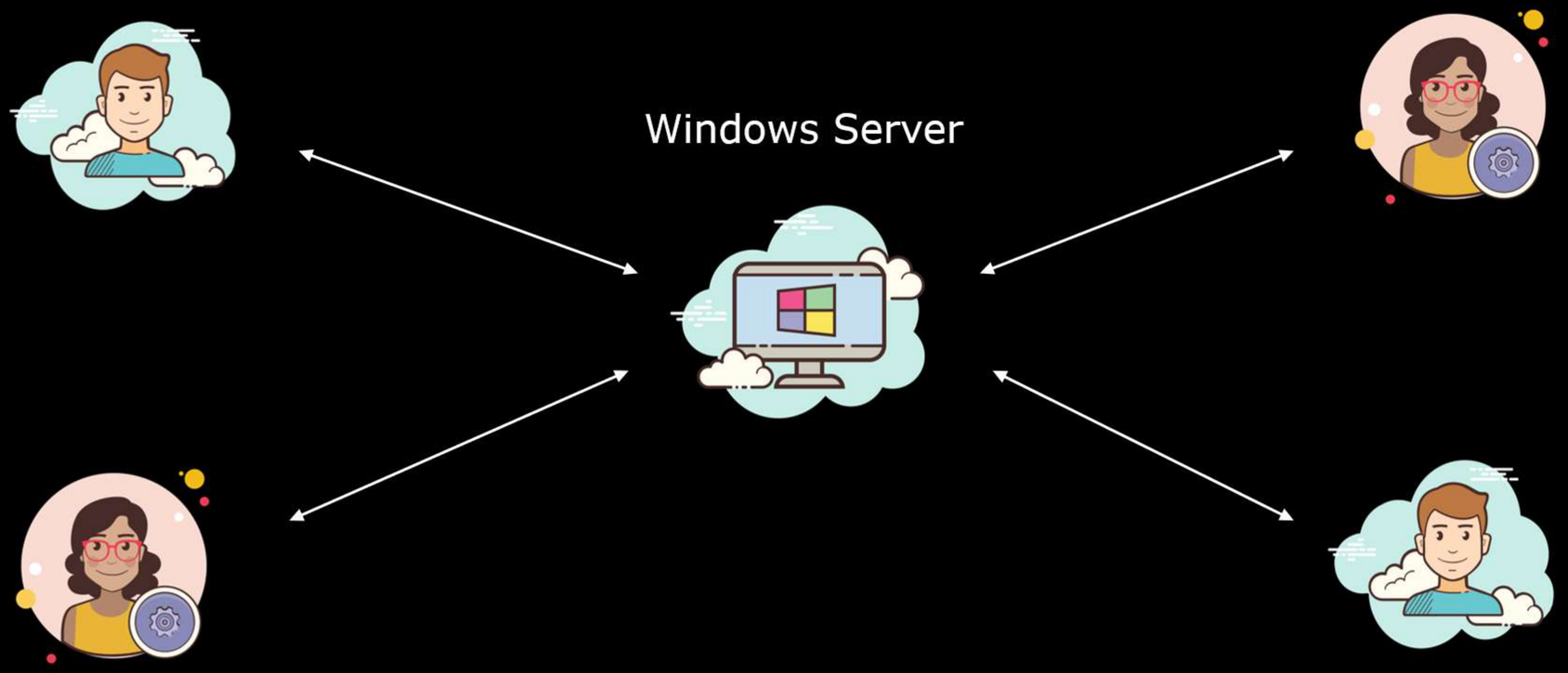
At the end of the video, you will be able to:

- explain when to use the Amazon FSx Windows File Server
- evaluate scaling, availability, and backup options
- understand how you can migrate your files from your existing file server to Amazon FSx

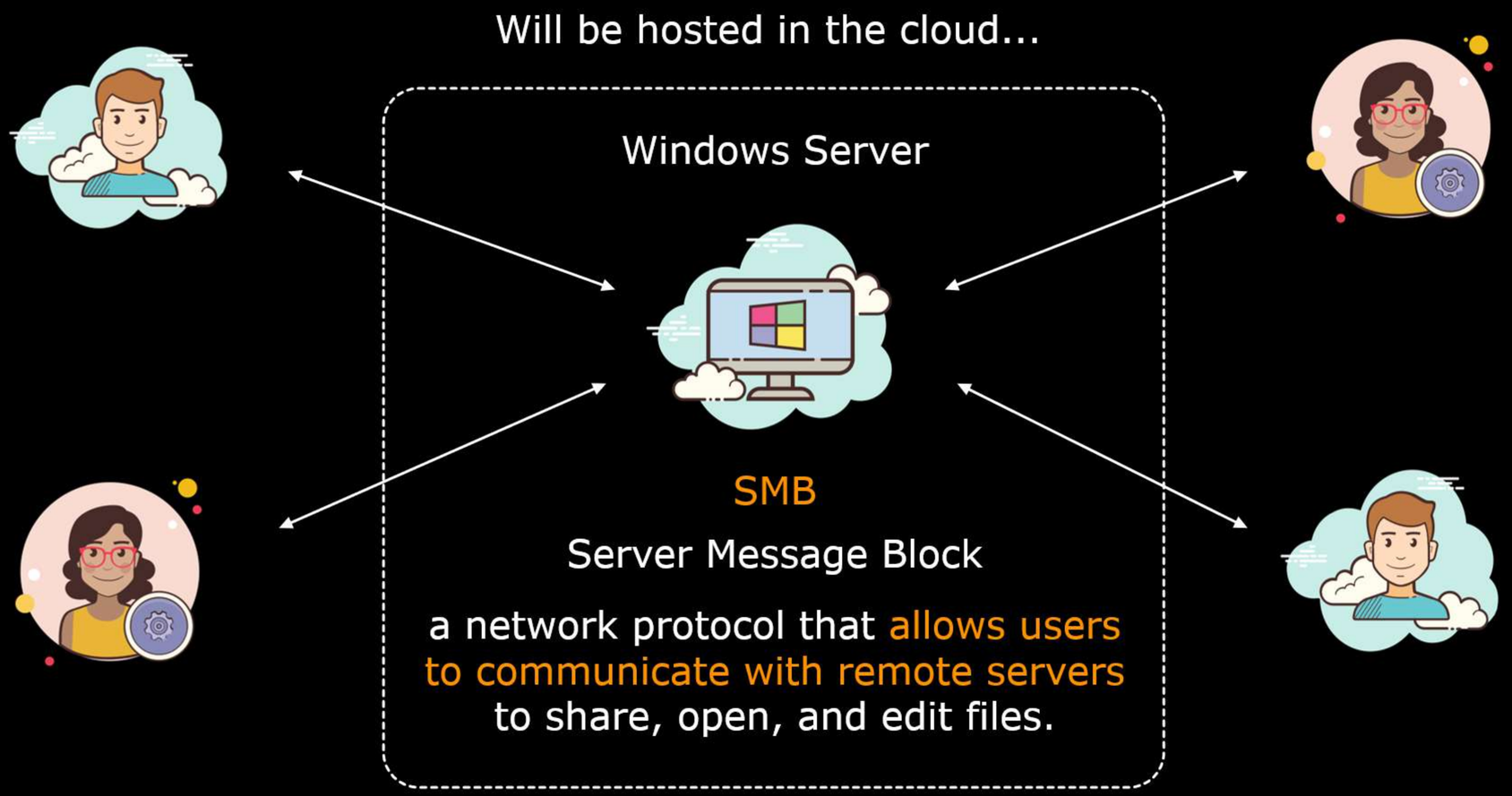
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx
Windows File Server

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx Windows File Server

- is a fully managed AWS storage designed to provide a high performant file system
- fully compatible shared Windows file service that is based on Windows Server
- The files on an Amazon FSx file system can be accessed from a Windows machine, Linux, macOS, EC2, VMWare, ECS, EKS, and even Lambda functions.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon FSx Windows File Server

- Integrates well with other AWS services
- Scalable and flexible to store and run data on the cloud

You can only increase the amount of storage capacity for a file system; you are not allowed to decrease storage capacity.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

	Single-AZ 1	Single-AZ 2	Multi-AZ
HDD Storage	✗	✓	✓
SSD Storage	✓	✓	✓
Microsoft Distributed File System Replication (DFSR)	✓	✗	✗
High-Availability	Provision two Single-AZ 1 file systems in separate AZs and replicate data synchronously using Microsoft DFSR.	✗	✓

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

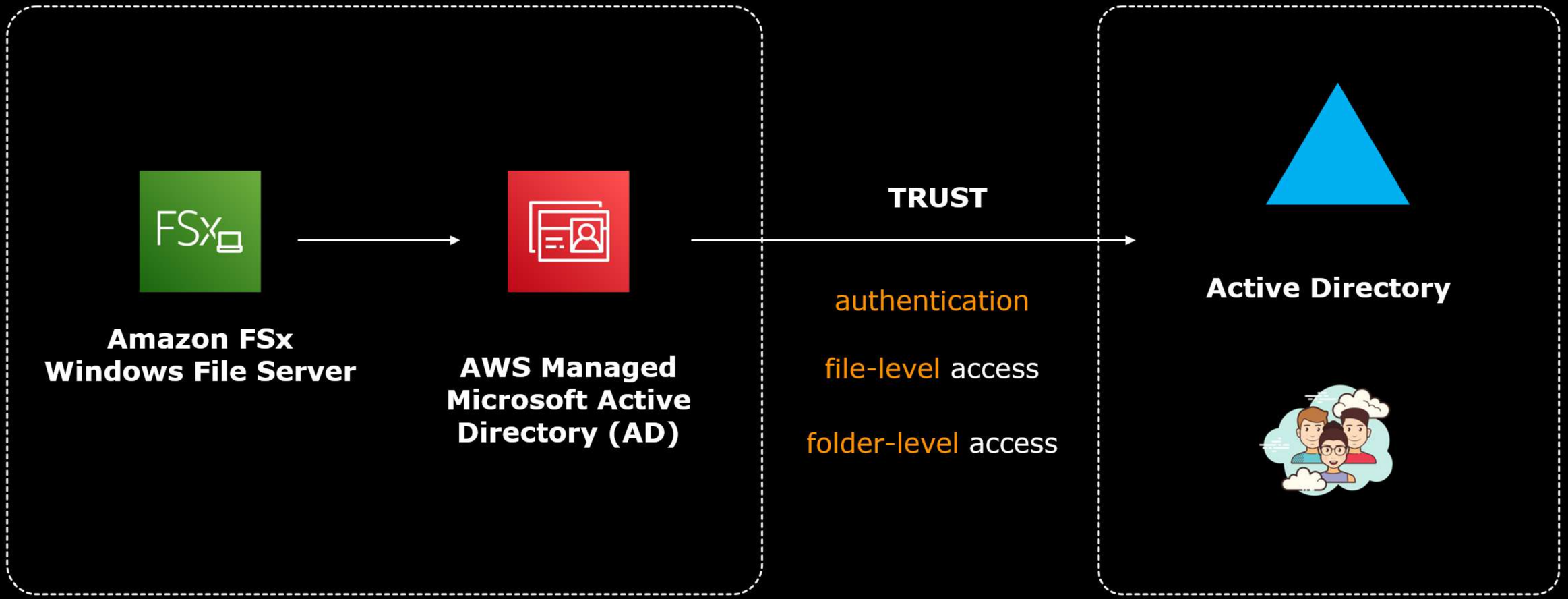


Amazon FSx
Windows File Server

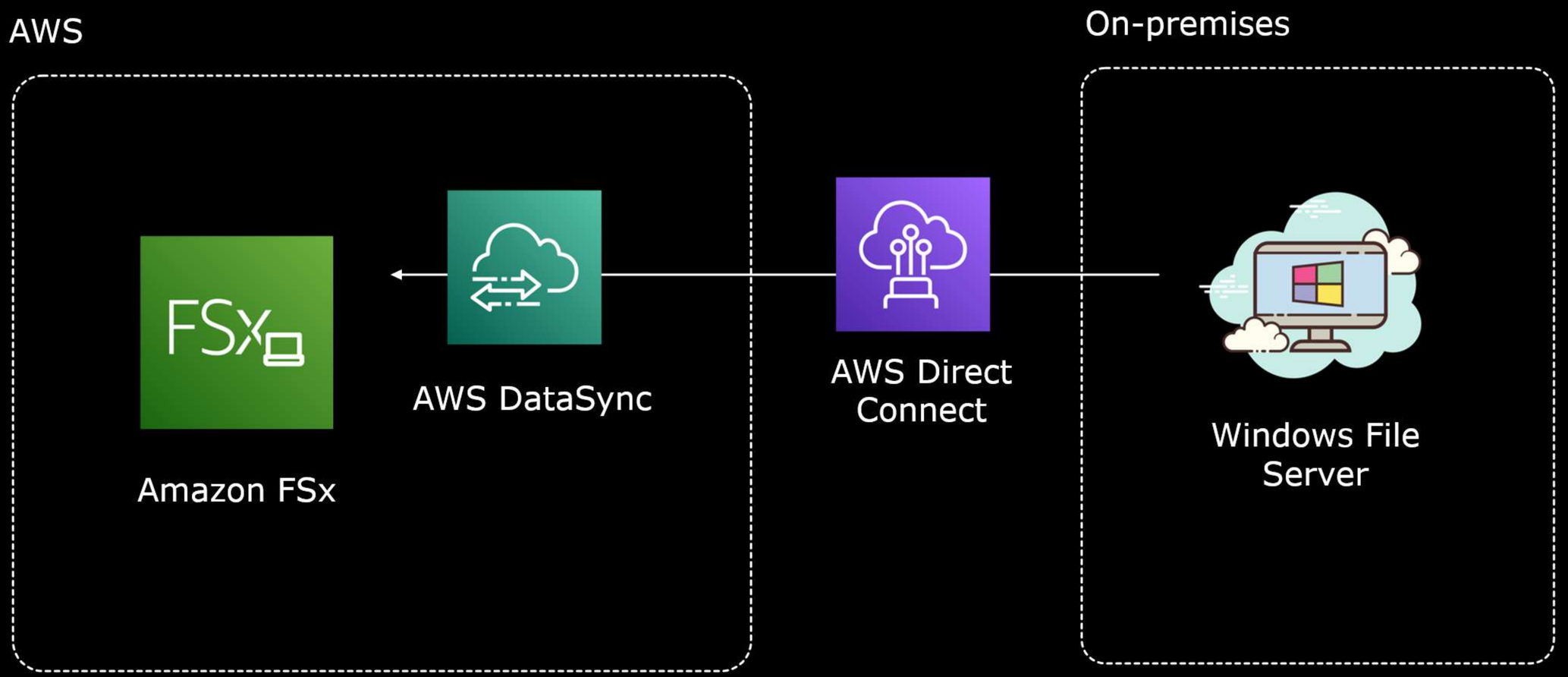
Other Amazon FSx features:

- taking native Amazon FSx backups
- creating backups through AWS Backup service
- taking Windows shadow copy to easily undo file changes and compare file versions
- schedule replication on AWS DataSync to a second file system

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

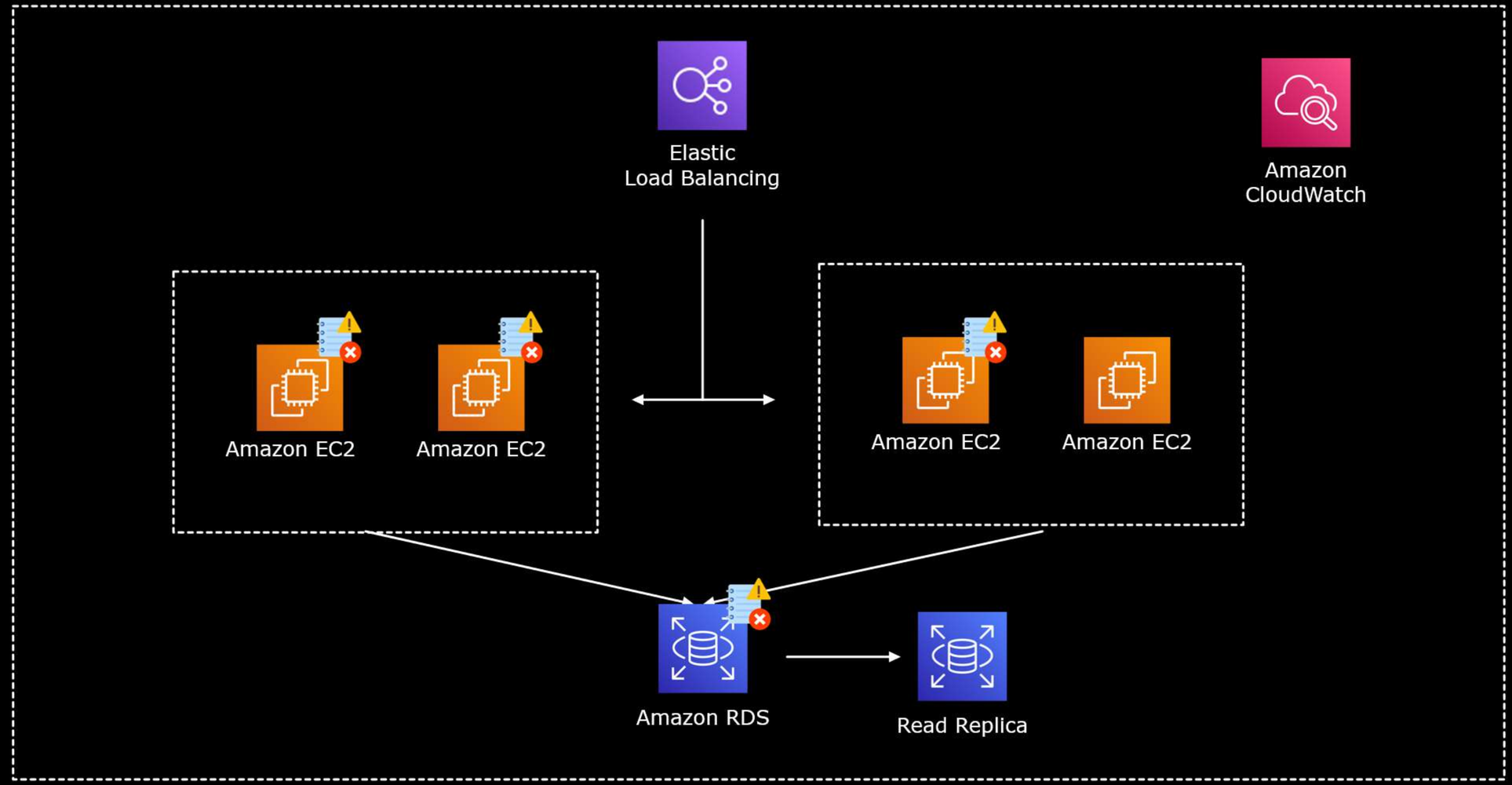


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon CloudWatch



Collect

Collect metrics and logs from your AWS resources, application and on-premises servers



Monitor

Visualize your operational data using dashboards and set up alerts to notify you.



Act

Automate the process of responding to operational changes and alarms.



Analyze

Extended data retention up to 15 months with real-time analytics.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



Collect

Collect metrics and logs from your AWS resources, application and on-premises servers



Monitor

Visualize your operational data using dashboards and set up alerts to notify you.



Act

Automate the process of responding to operational changes and alarms.



Analyze

Extended data retention up to 15 months with real-time analytics.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



Collect

Collect metrics and logs from your AWS resources, application and on-premises servers

- collect operational data like logs, metrics, and events
- use the data to improve performance of your applications and resources

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



Collect

Collect metrics and logs from your AWS resources, application and on-premises servers



Monitor

Visualize your operational data using dashboards and set up alerts to notify you.



Act

Automate the process of responding to operational changes and alarms.



Analyze

Extended data retention up to 15 months with real-time analytics.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



Monitor

Visualize your operational data using dashboards and set up alerts to notify you.

- setup monitoring solutions
- unified view of your application and resource's operational health
- create dashboards to get graphical view of your systems
- setup alerts to get notified

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



Collect

Collect metrics and logs from your AWS resources, application and on-premises servers



Monitor

Visualize your operational data using dashboards and set up alerts to notify you.



Act

Automate the process of responding to operational changes and alarms.



Analyze

Extended data retention up to 15 months with real-time analytics.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon CloudWatch



Act

Automate the process of responding to operational changes and alarms.

- automatically respond when things go wrong for your application and resources
- trigger actions like Auto Scaling, stopping instances to reduce overages, and trigger other workflows with services like Lambda, SNS, and CloudFormation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon CloudWatch



Collect

Collect metrics and logs from your AWS resources, application and on-premises servers



Monitor

Visualize your operational data using dashboards and set up alerts to notify you.



Act

Automate the process of responding to operational changes and alarms.



Analyze

Extended data retention up to 15 months with real-time analysis.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



Analyze

Extended data retention up to 15 months with real-time analysis.

- deep dive and analyze existing metrics and logs
- come up with a strategy and implement them
- create metrics and logs again to verify and monitor the performance of the improvement

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon CloudWatch



Collect

Collect metrics and logs from your AWS resources, application and on-premises servers



Monitor

Visualize your operational data using dashboards and set up alerts to notify you.



Act

Automate the process of responding to operational changes and alarms.



Analyze

Extended data retention up to 15 months with real-time analytics.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudWatch



Metrics



Logs



Alarms



Events



Dashboard

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Metrics



Logs



Alarms

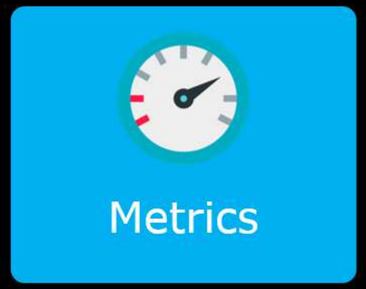


Events



Dashboard

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/




Logs


Alarms


Events


Dashboard

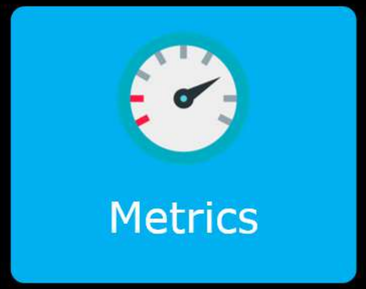


Amazon CloudWatch

Metrics - data that describes your the performance of your application or resources

- By default, many AWS services already provide free metrics for resources like EC2, EBS, and RDS.
- Most AWS services send metric data to CloudWatch every one minute.
- EC2 instances send metrics data to CloudWatch every 5 minutes by default but you can also enable detailed monitoring to send metric data at a 1-minute interval.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/




Logs


Alarms


Events


Dashboard



Amazon CloudWatch

- You can publish your own custom metrics
- Metric data in CloudWatch is kept for 15 months

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Metrics



Logs



Alarms



Events



Dashboard



Amazon CloudWatch

- Helps you monitor, store, and access your log files from:
  - Amazon EC2 instances
  - AWS CloudTrail
  - Route 53
  - on-premises servers, and other sources.
- Think of CloudWatch Logs as a highly scalable log repository that allows you to centralize your logs.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Metrics

Logs

Alarms

Events

Dashboard



Amazon CloudWatch

- view logs
- query for specific error codes
- filter logs based on specific fields
- archive logs for future analysis or investigation

Vended Logs





Published by AWS







and more..

Logs from on-premises server



CloudWatch Agent or **PutLogData API**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Metrics



Logs



Alarms



Events



Dashboard



Amazon CloudWatch

Alarms - triggers one or more actions based on the value of the metric relative to the threshold you set

Actions can be in the form of:

- sending notification to an Amazon SNS topic
- performing an Amazon EC2 action
- scaling an Auto Scaling Group
- creating an incident in Systems Manager
- sending a billing alert
- invoking a Lambda function

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Metrics | Logs | Alarms | **Events** | Dashboard



Amazon CloudWatch

Events - near real-time stream of system events that describe changes in your AWS resources

Rules - matches events that you want to monitor and route them to one or more targets

Targets - can be an EC2 instance action, triggering a Lambda function, invoking ECS task, setting off a Systems Manager Automation document, publishing a message to an SNS topic, and many more

Once a rule is set up, CloudWatch Events becomes aware of operational changes once they occur

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Metrics



Logs



Alarms



Events



Dashboard



CloudWatch Events



Amazon EventBridge

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Metrics



Logs



Alarms



Events



Dashboard



Alarms

take actions when a metric reaches a certain threshold



Events

reacts to real-time system events performed on your AWS resources

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Metrics



Logs



Alarms



Events



Dashboard



Amazon CloudWatch

- creates a reusable graphs and visualize your resources in a unified view
- graph metrics and logs data into a single dashboard which helps you to resolve issues and understand the root cause



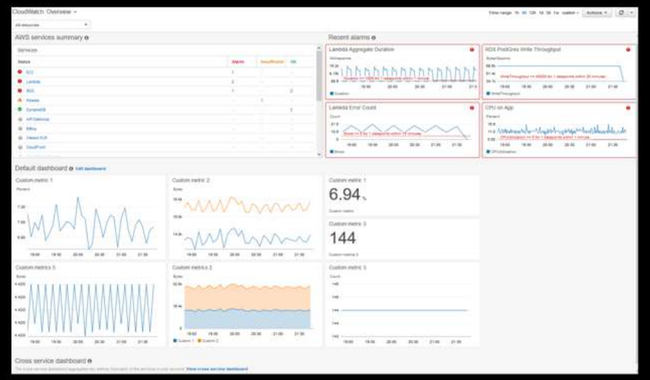
Amazon EC2



CPU Utilization



Memory Usage

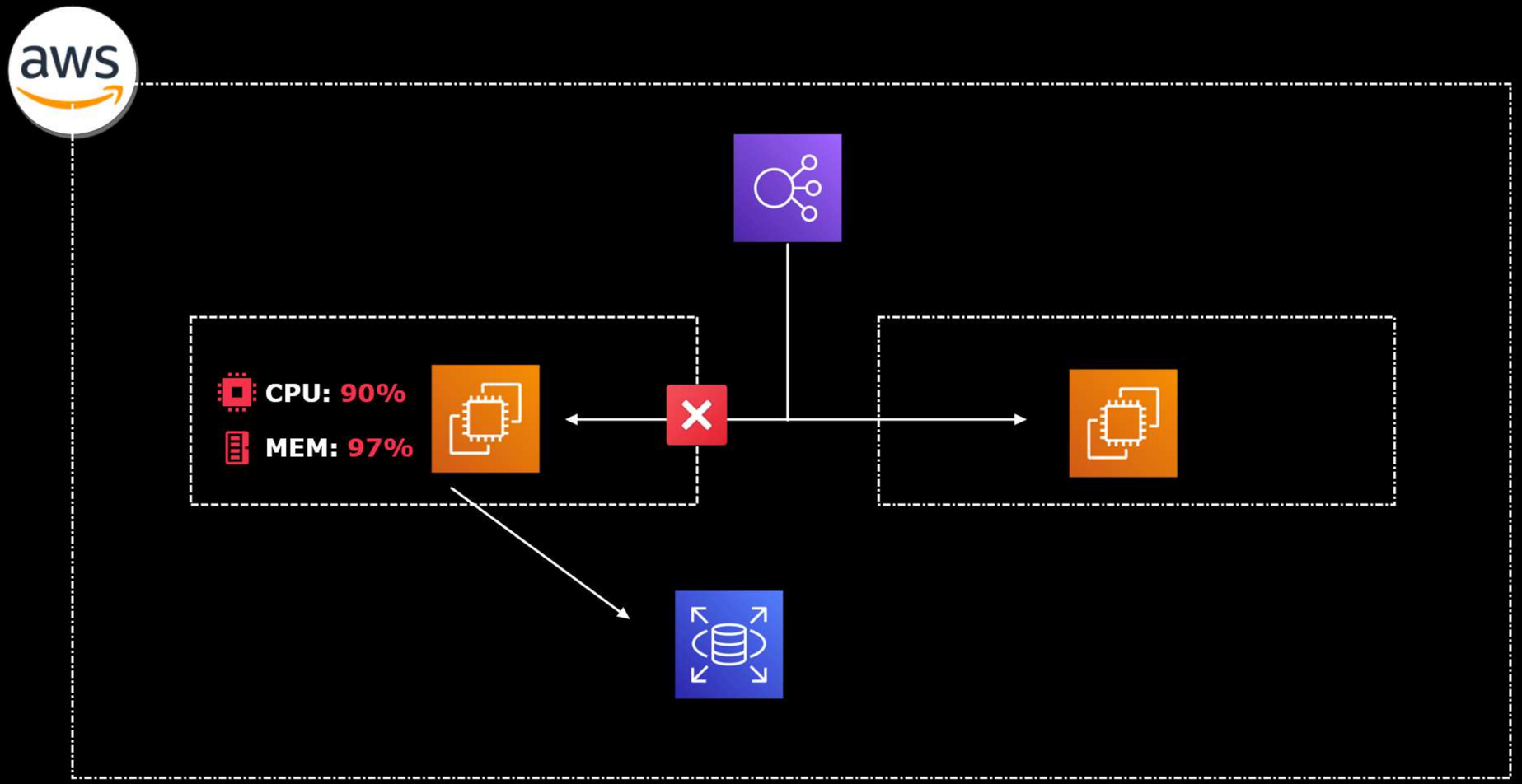


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CloudWatch Metrics for EC2 Instances

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



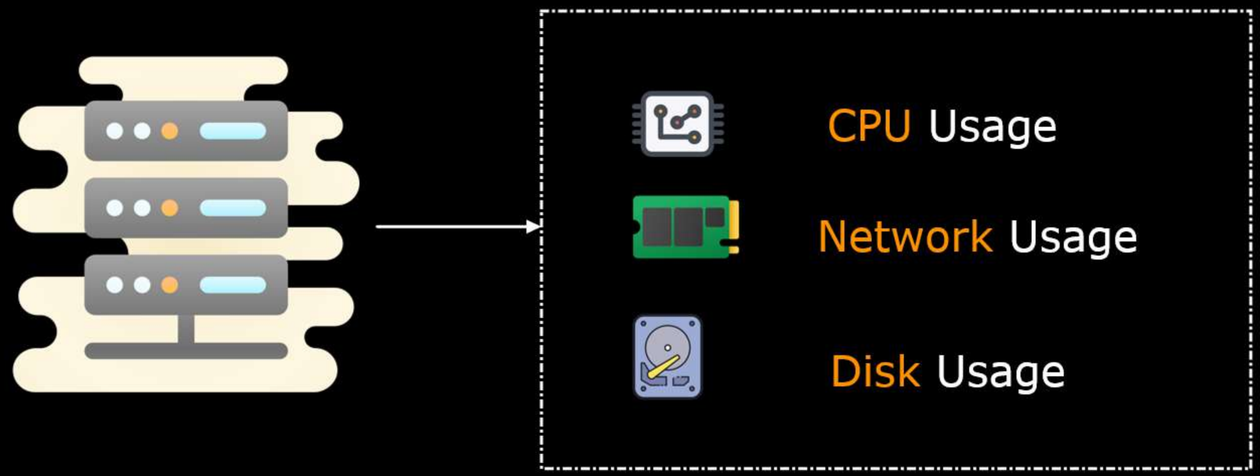
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch Metrics

What is a metric?

- Data that describes your resource



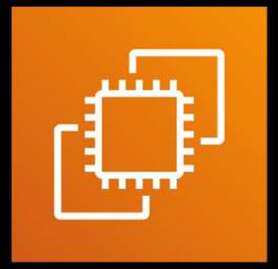
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

What is a metric?

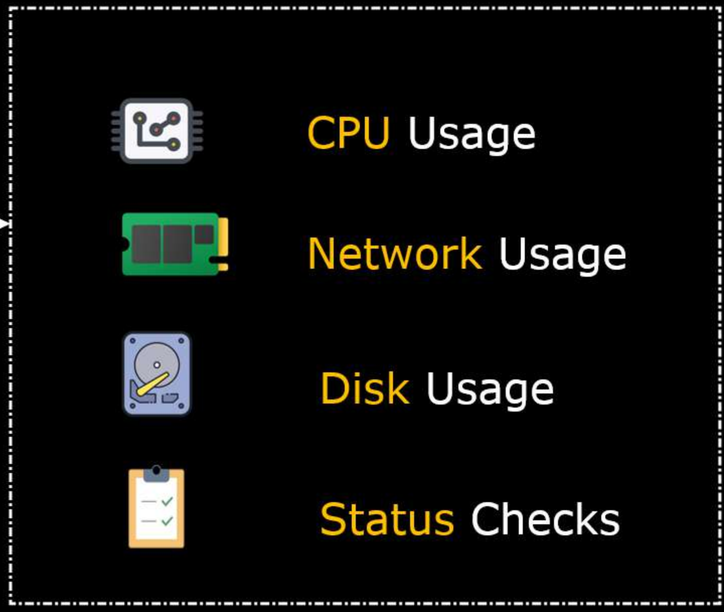
- Data that describes your resource



Amazon CloudWatch Metrics



EC2 Instance



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch Metrics

AWS-provided metrics can be set to monitor metrics using:

Basic Monitoring (default behavior for all metrics)

- Free of Charge
- Collects metrics data every **5 minutes**

Detailed Monitoring

- Charges apply
- Collects metrics data at **1 minute interval**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch Metrics

CUSTOM metrics can be set to monitor metrics using:

Basic Resolution (default behavior for all metrics)

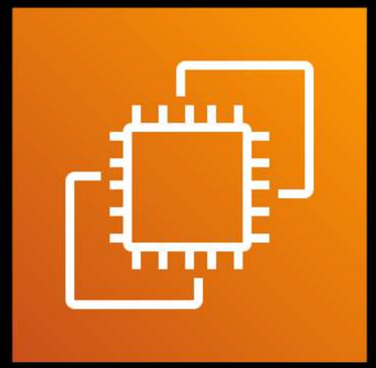
- Charges apply
- Pushes metrics every 1 minute

High Resolution

- Charges apply
- Can send metrics as frequent as per second

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS-PROVIDED METRICS



AWS-provided Metrics for EC2 instances

CPU related metrics

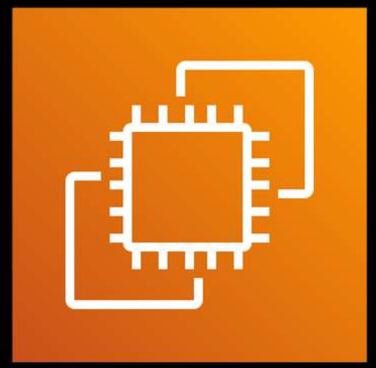
- CPU Utilization (compute units used)
- CPU Credit Usage & CPU Credit Balance (for burstable instances only like T2 & T3 instances)

NETWORK related metrics

- NetworkIn (bytes received by instance)
- NetworkOut (bytes sent out by instance)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS-PROVIDED METRICS



AWS-provided Metrics for EC2 instances



Disk related metrics (for instances backed by instance store)

- DiskReadOps and DiskWriteOps
- DiskReadBytes and DiskWriteBytes

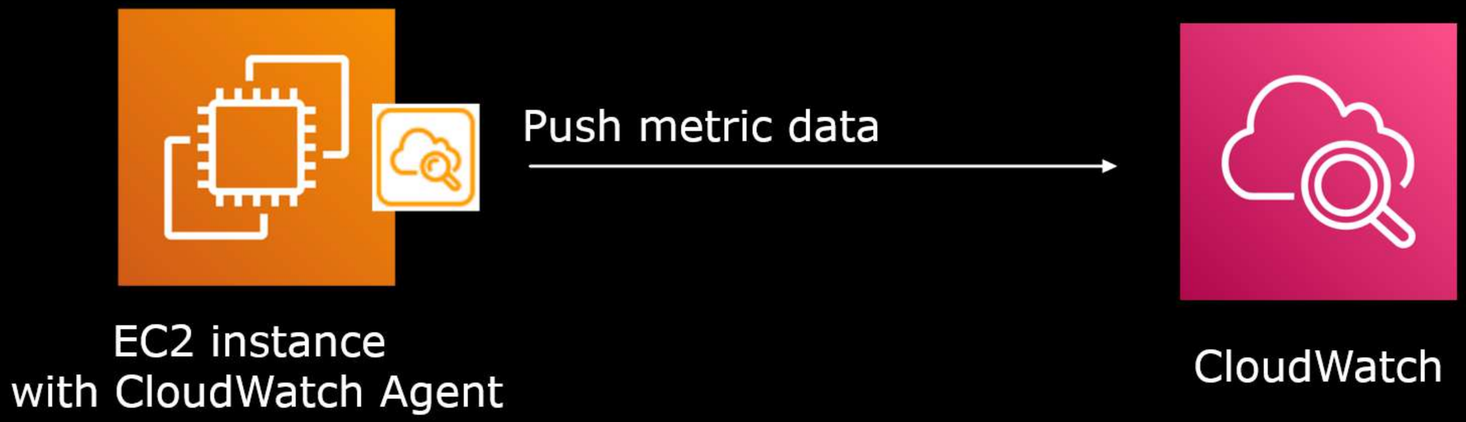


Status Check metrics

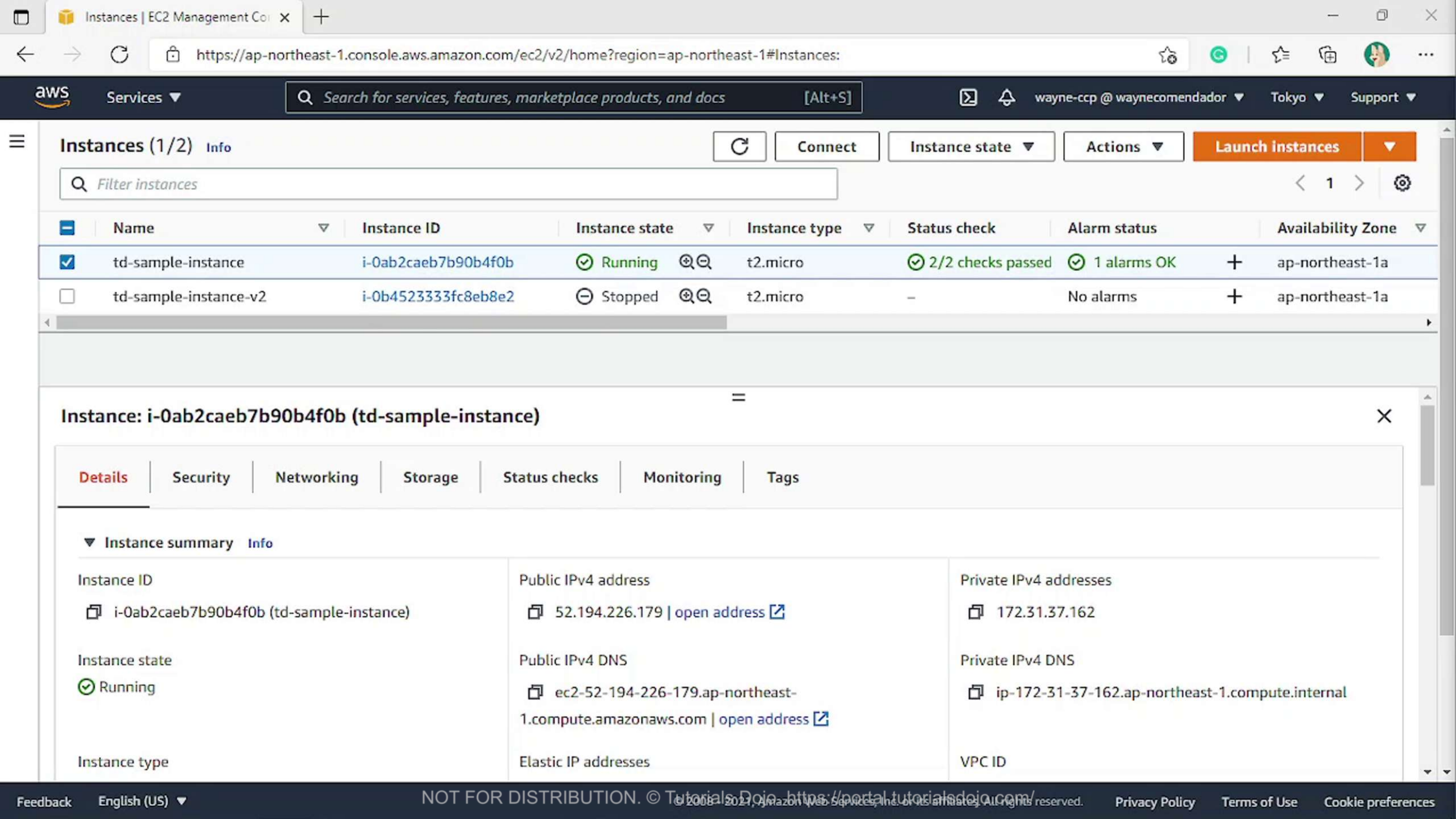
- Instance Status (monitors software and network configuration)
- System Status (refers to health of underlying hardware)
- Status Check Failed (refers to the status of both instance status and system status)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Remember: MEMORY metrics is NOT provided by AWS!



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

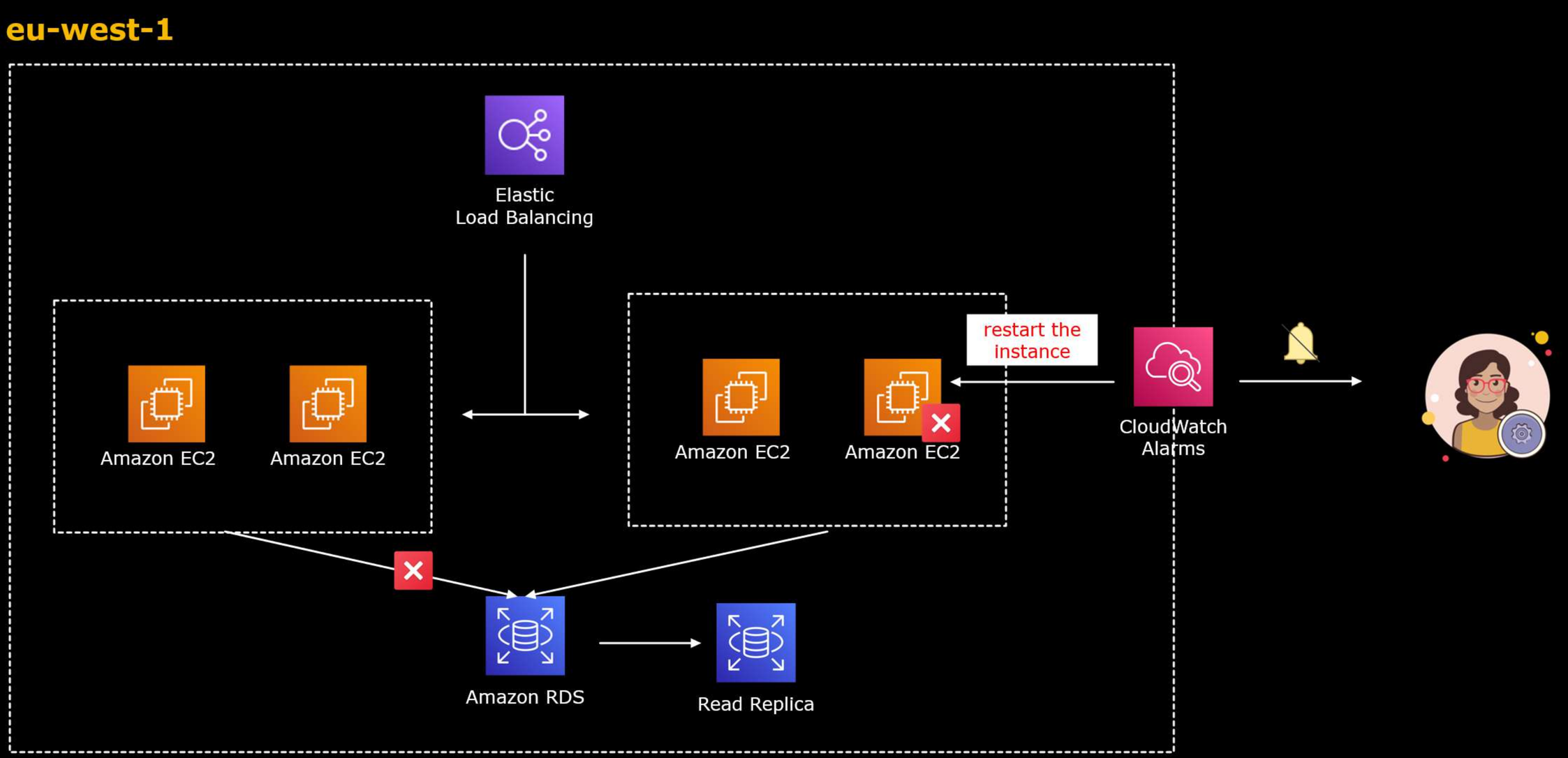


NOT FOR DISTRIBUTION. © Tutorials Dojo, https://portal.tutorialsdojo.com/



Amazon CloudWatch Alarms

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

Metrics you can use in CloudWatch Alarms

- Metric Alarm

  - Watches a single CloudWatch metric or the result of a math expression based on CloudWatch metrics

- Composite Alarms

  - trigger an alarm based on the alarm states of other alarms that you have created.

Alarms allow you to receive notifications when metrics or other alarms fall outside of the threshold that you set.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Two steps to create a metric alarm:



Amazon CloudWatch



Specify the metric



Configure actions to take after an alarm is triggered

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Specify the metric



Configure actions to trigger



Amazon CloudWatch

- AWS provides metrics for your resources
- But you can also use the metric filters that you created in CloudWatch Logs.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Specify the metric



Configure actions to trigger



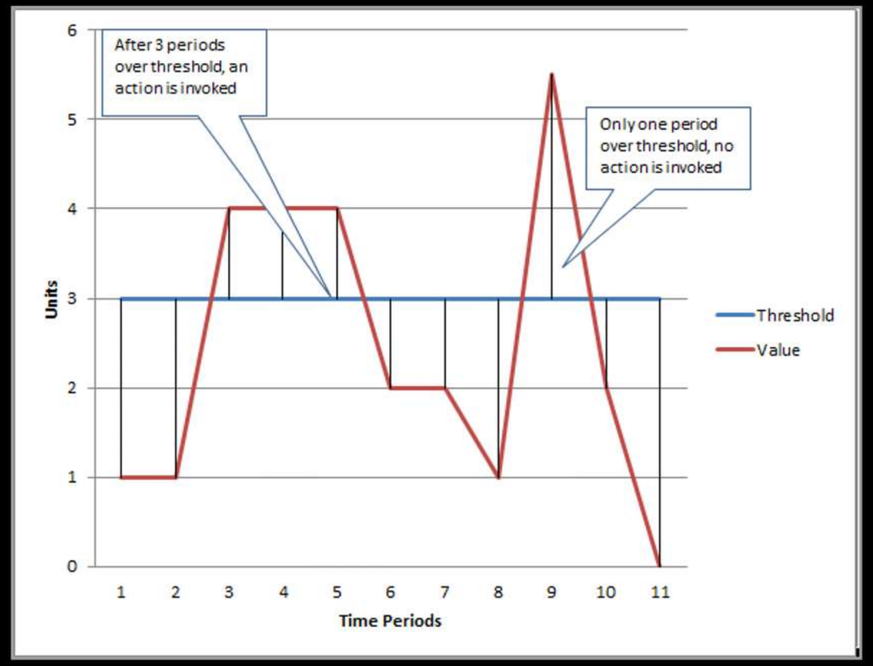
Amazon CloudWatch

- AWS provides metrics for your resources
- But you can also use the metric filters that you created in CloudWatch Logs.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Specify the metric

Configure actions to trigger



- Period - defines the length of time to evaluate a metric expressed in seconds

  For example, if you choose 5 minutes as a period, then the alarm evaluates the metric every 5 minutes.

- Evaluation Periods - defines the number of most recent periods, or data points, that you want to evaluate when determining alarm state.

- Datapoints to Alarm - specifies the number of data points within the Evaluation Periods that should be breached to trigger the ALARM state.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Specify the metric



Configure actions to trigger



Amazon CloudWatch

- Conditions - which determine the threshold for the alarm to trigger



Amazon EC2

Condition

StatusCheckFailed_System > 0

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Specify the metric

Configure actions to trigger



Amazon CloudWatch



OK

- the metric is within the defined threshold



ALARM

- the metric or expression is outside the defined threshold



INSUFFICIENT_DATA

- does not have enough data available for the metric to determine the alarm state

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Specify the metric



Configure actions to trigger



Amazon CloudWatch



OK

- the metric is within the defined threshold



ALARM

- the metric or expression is outside the defined threshold



INSUFFICIENT_DATA

- does not have enough data available for the metric to determine the alarm state

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Specify the metric



Configure actions to trigger



Amazon CloudWatch

- You can define an SNS topic to receive messages based on the different alarm states.
- You can also configure how resources will react once an alarm is triggered.



Amazon EC2

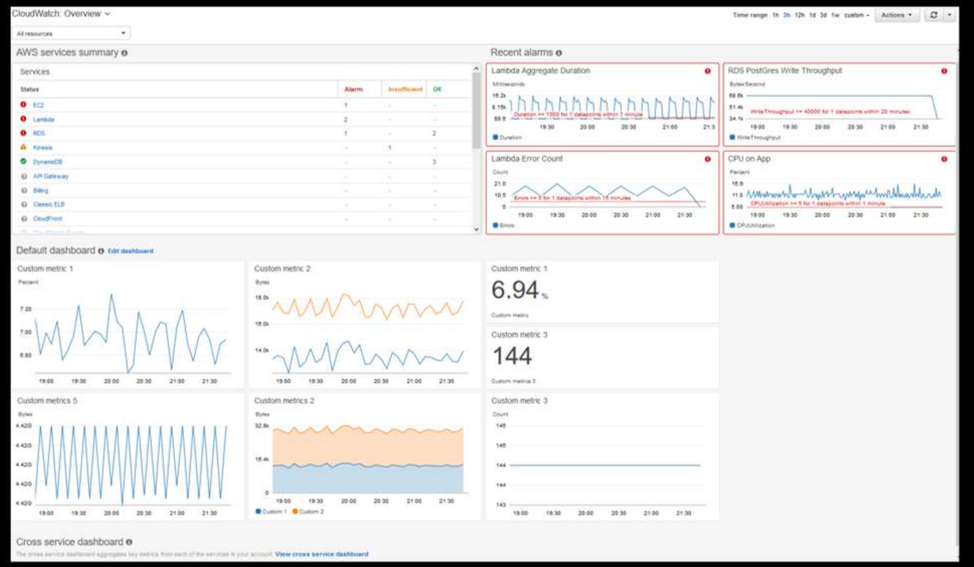
Stop and start instance to recover

StatusCheckFailed_System > 0

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch



- You can also add alarms to CloudWatch dashboards to monitor resources visually.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CloudWatch Logs and Metric Filters

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CloudWatch Logs

At the end of this lecture, you will be able to:

- understand what type of logs can you store in CloudWatch
- understand how metric filters help you gain better insights into your logs.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CloudWatch Logs

CloudWatch Logs is a log repository where you can:

- store log streams
- monitor logs
- perform query
- analyze your logs

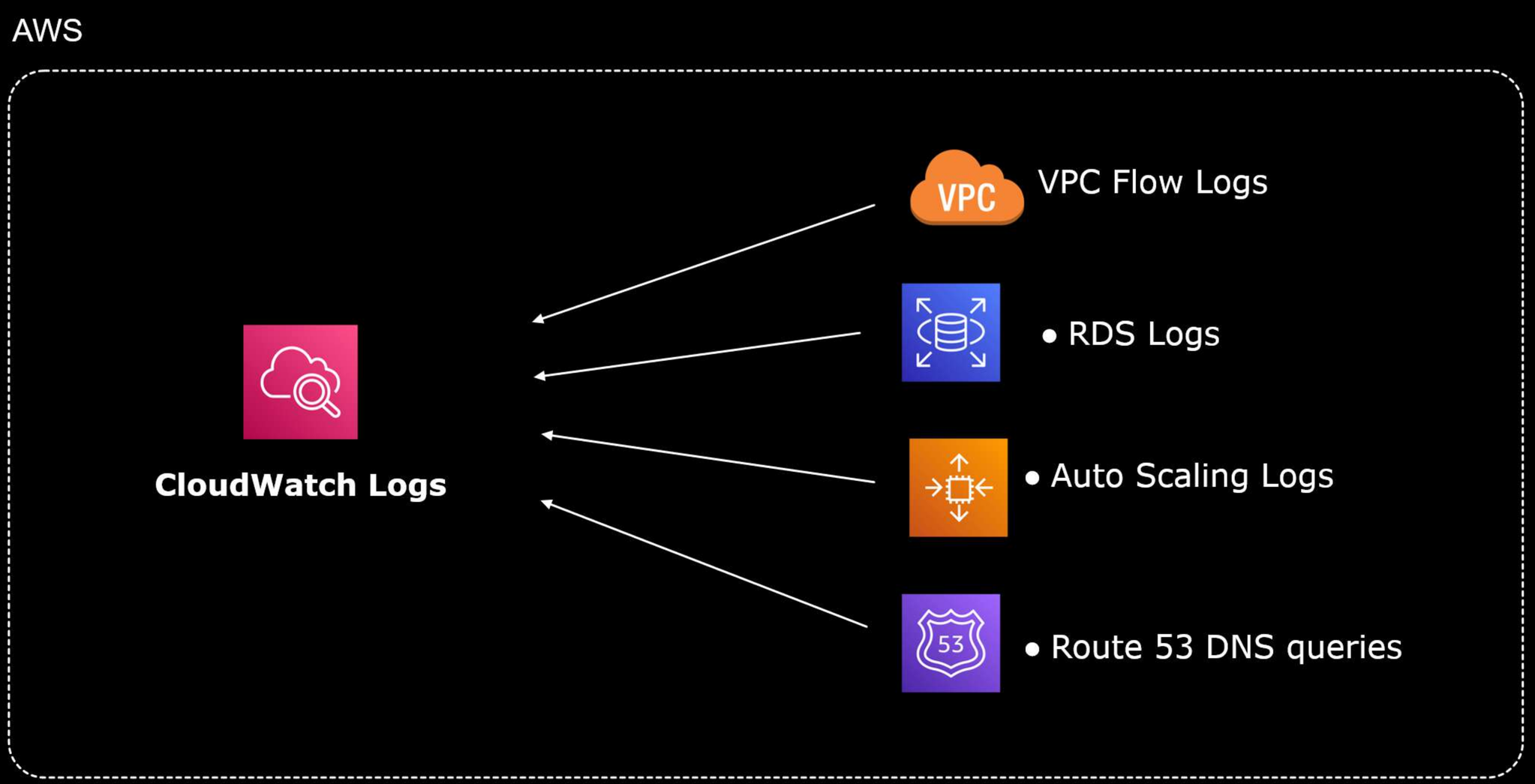
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



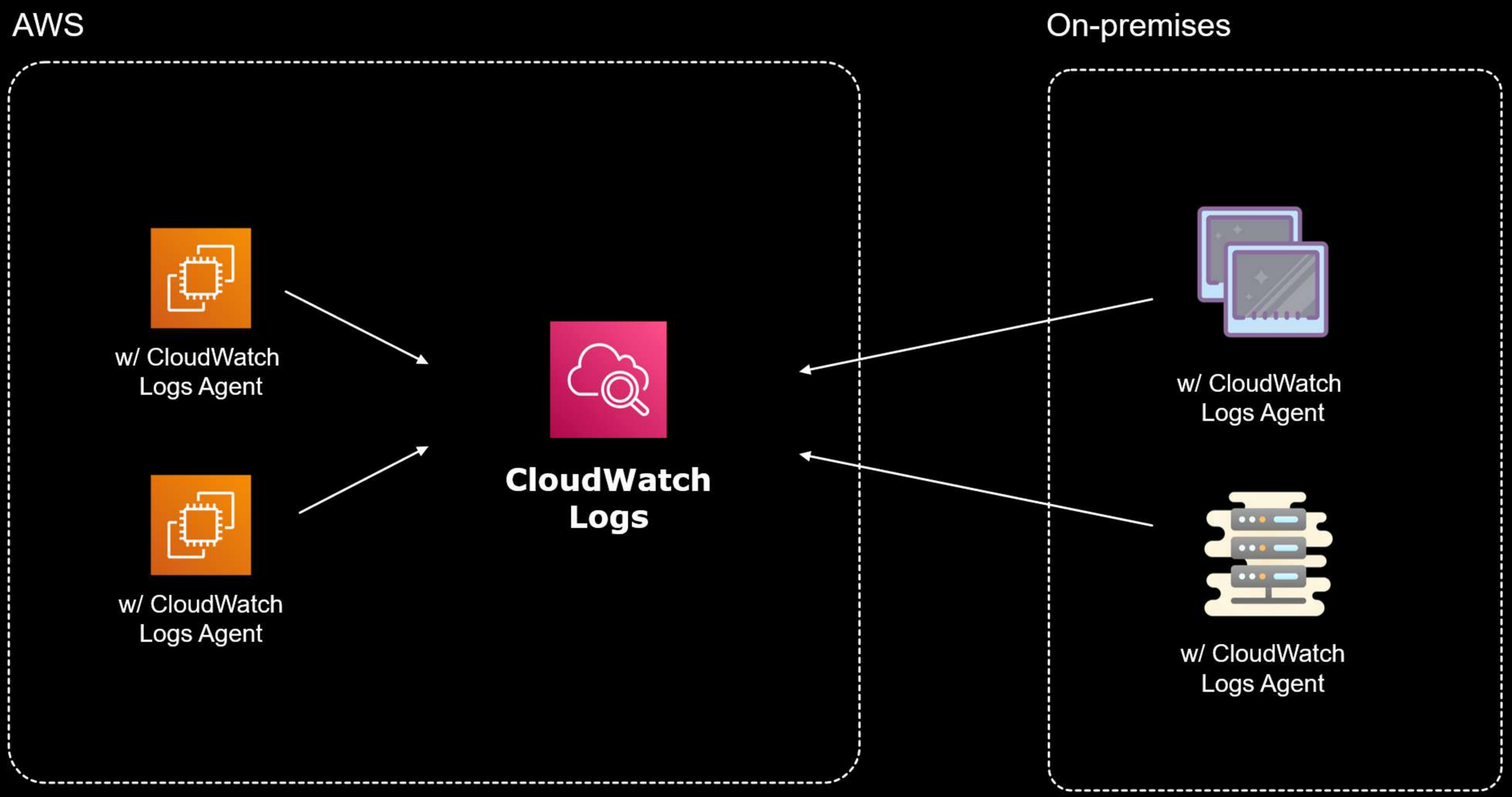
What are logs?

- it's like a list of activities performed by a server
- serves as a red flag that can help you investigate when there are malicious activities on your resources
- automatically created and maintained by a server

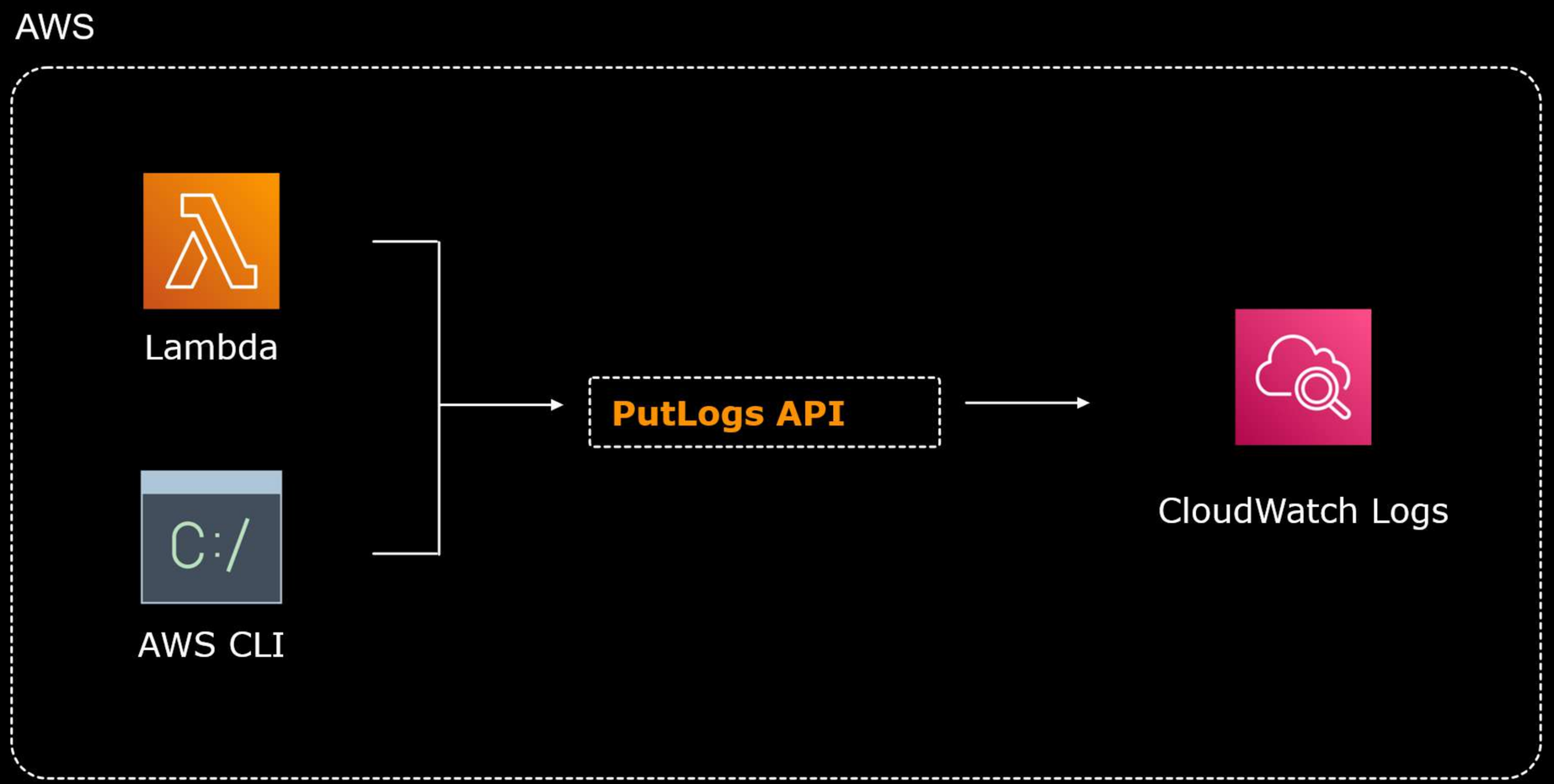
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

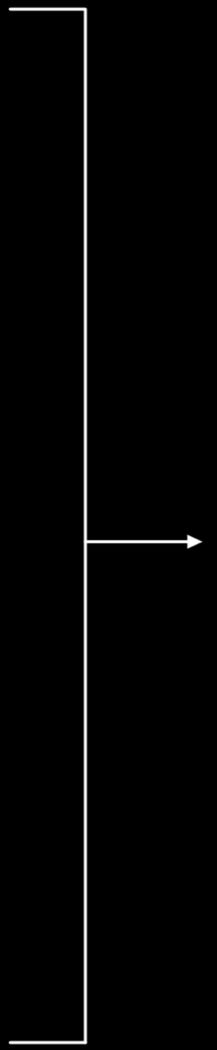


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

```
127.0.0.1 - - [24/Sep/2013:11:49:52 -0700] "GET /index.html HTTP/1.1" 500 287
127.0.0.1 - - [24/Sep/2013:11:50:52 -0700] "GET /index.html HTTP/1.1" 500 287
127.0.0.1 - - [24/Sep/2013:11:51:51 -0700] "GET /~test/ HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:52:51 -0700] "GET /favicon.ico HTTP/1.1" 501 308
127.0.0.1 - - [24/Sep/2013:11:53:51 -0700] "GET /favicon.ico HTTP/1.1" 503 308
127.0.0.1 - - [24/Sep/2013:11:54:34 -0700] "GET /~test/index.html HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:55:52 -0700] "GET /index.html HTTP/1.1" 500 287
127.0.0.1 - - [24/Sep/2013:11:56:52 -0700] "GET /index.html HTTP/1.1" 500 287
127.0.0.1 - - [24/Sep/2013:11:57:51 -0700] "GET /~test/ HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:58:51 -0700] "GET /favicon.ico HTTP/1.1" 501 308
127.0.0.1 - - [24/Sep/2013:11:59:01 -0700] "GET /favicon.ico HTTP/1.1" 501 308
127.0.0.1 - - [24/Sep/2013:11:50:02 -0700] "GET /favicon.ico HTTP/1.1" 503 308
127.0.0.1 - - [24/Sep/2013:11:51:03 -0700] "GET /~test/index.html HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:50:04 -0700] "GET /favicon.ico HTTP/1.1" 501 308
127.0.0.1 - - [24/Sep/2013:11:50:05 -0700] "GET /favicon.ico HTTP/1.1" 503 308
127.0.0.1 - - [24/Sep/2013:11:51:06 -0700] "GET /~test/index.html HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:49:07 -0700] "GET /index.html HTTP/1.1" 500 287
127.0.0.1 - - [24/Sep/2013:11:49:08 -0700] "GET /index.html HTTP/1.1" 500 287
127.0.0.1 - - [24/Sep/2013:11:50:09 -0700] "GET /~test/ HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:50:11 -0700] "GET /favicon.ico HTTP/1.1" 501 308
127.0.0.1 - - [24/Sep/2013:11:50:12 -0700] "GET /favicon.ico HTTP/1.1" 501 308
127.0.0.1 - - [24/Sep/2013:11:50:13 -0700] "GET /favicon.ico HTTP/1.1" 503 308
127.0.0.1 - - [24/Sep/2013:11:51:14 -0700] "GET /~test/index.html HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:50:15 -0700] "GET /favicon.ico HTTP/1.1" 501 308
127.0.0.1 - - [24/Sep/2013:11:50:16 -0700] "GET /favicon.ico HTTP/1.1" 503 308
127.0.0.1 - - [24/Sep/2013:11:51:17 -0700] "GET /~test/index.html HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:49:18 -0700] "GET /index.html HTTP/1.1" 500 287
```



- too vague to understand
- generated logs is usually too large
- too impractical to review

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CloudWatch Logs

CloudWatch Logs also allows you to query and analyze your logs using metric filters. To create one, you need to:

1. Create a filter pattern

   - defines the terms and patterns you want to look for in a log data

   Ex. error codes, warnings, or IP addresses

2. Assign a metric based on the filter pattern.

   - turn the filtered data into a numerical CloudWatch metric that you can graph or set an alarm on.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch Events

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

- is a resource monitoring service
- used for monitoring and describing changes in an AWS environment.
- automate response when events happen

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

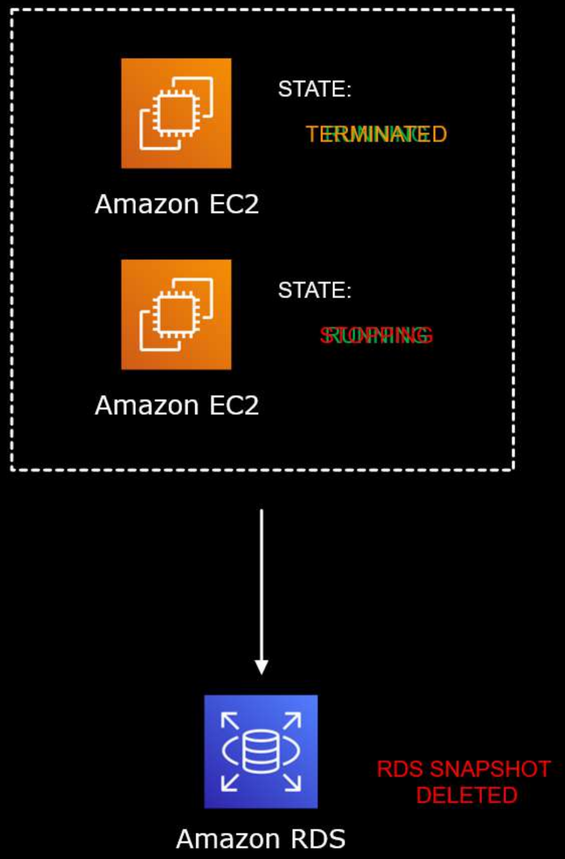
EVENTS

EVENT RULES

TARGETS

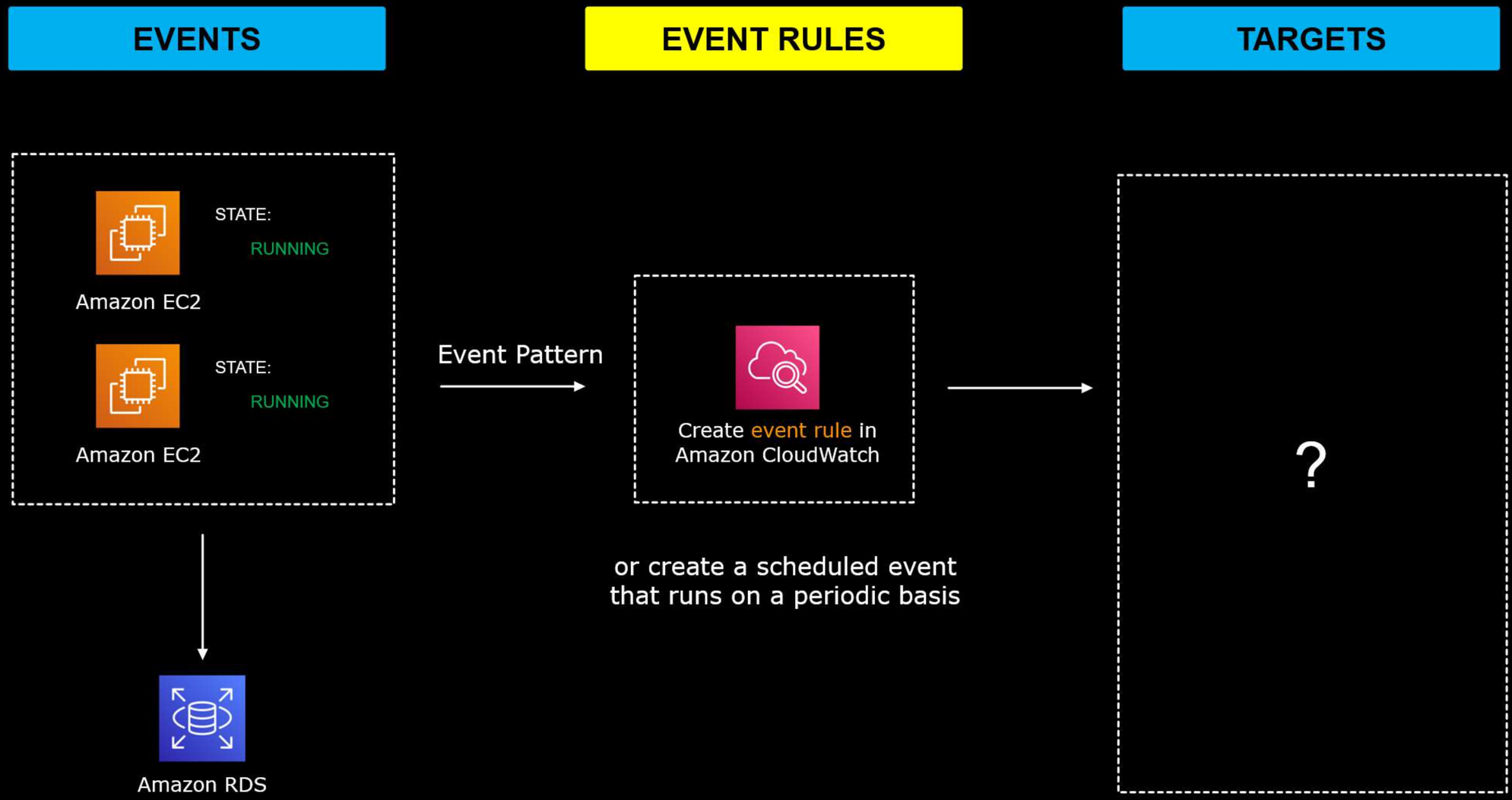
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

EVENTS | **EVENT RULES** | **TARGETS**

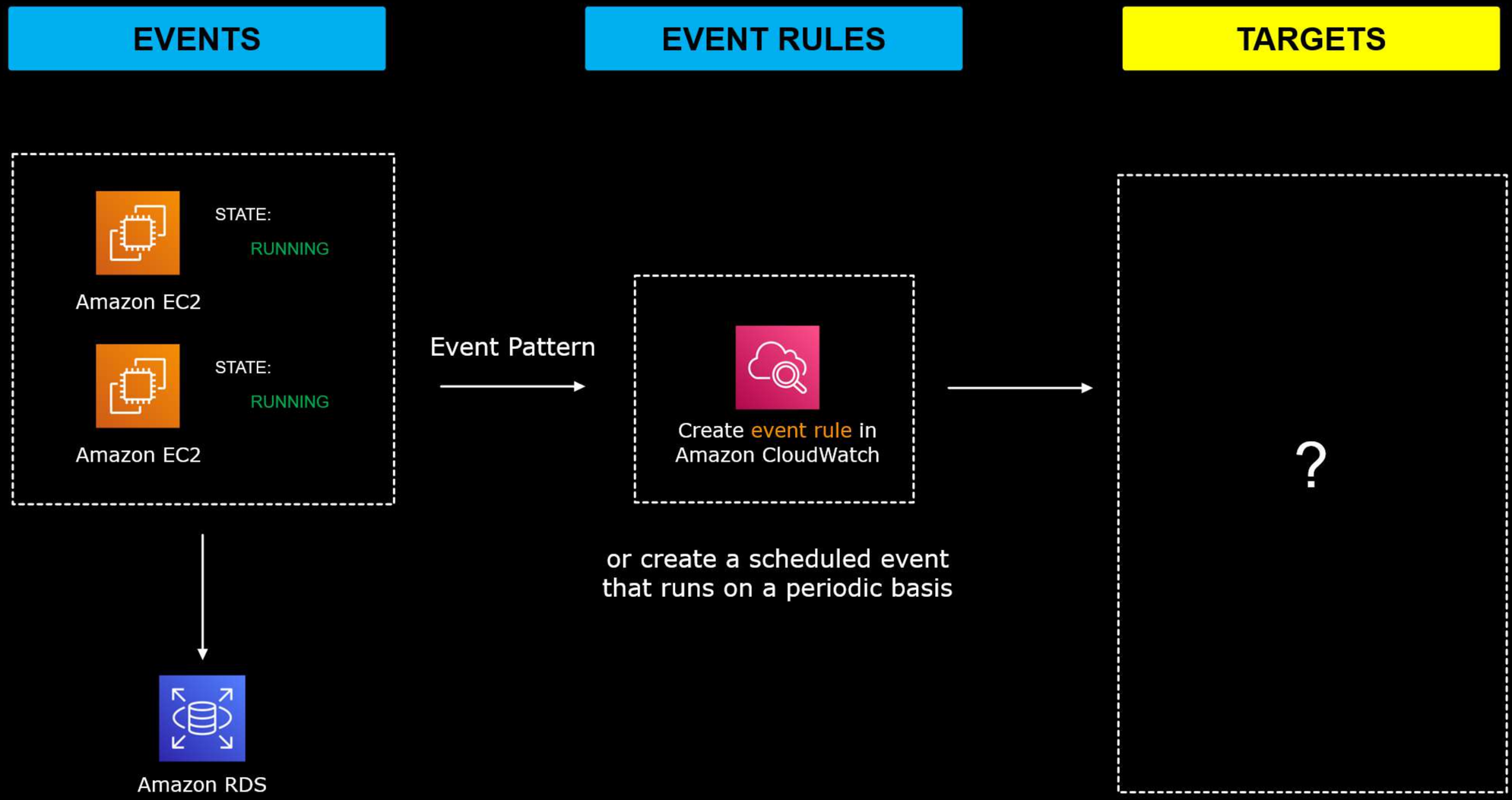


- Events that indicate changes in your AWS environment
- You can also set up scheduled events that are executed on a periodic basis

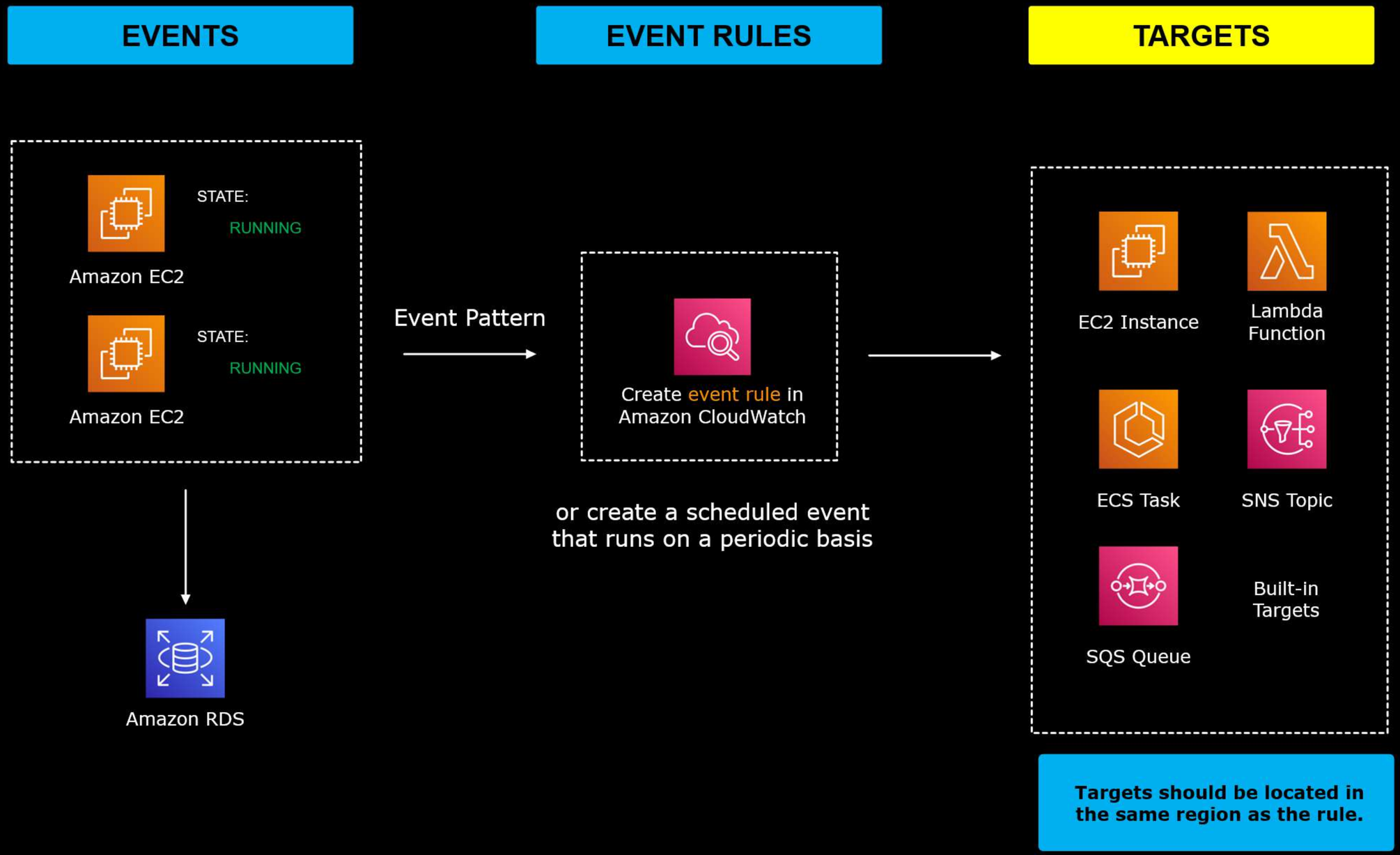
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

Services that integrate with CloudWatch Events:

- CloudTrail
- CloudFormation
- Config

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

Services that integrate with CloudWatch Events:

- IAM
- Lambda

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

Services that integrate with CloudWatch Events:

- CloudTrail
  - CloudTrail captures API calls made by or on behalf of your AWS account.
- CloudFormation
  - You can declare event rules in CloudFormation templates.
- Config
  - Detect and react to changes in the status of AWS Config events.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch

Services that integrate with CloudWatch Events:

- IAM
  - Create an event rule that sends a message to an SNS topic when a CreateUser and DeleteUser API call is made.
- Lambda
  - You can set Lambda functions as targets when creating a n event rule

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CloudWatch Events



Amazon EventBridge

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon CloudWatch Events

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

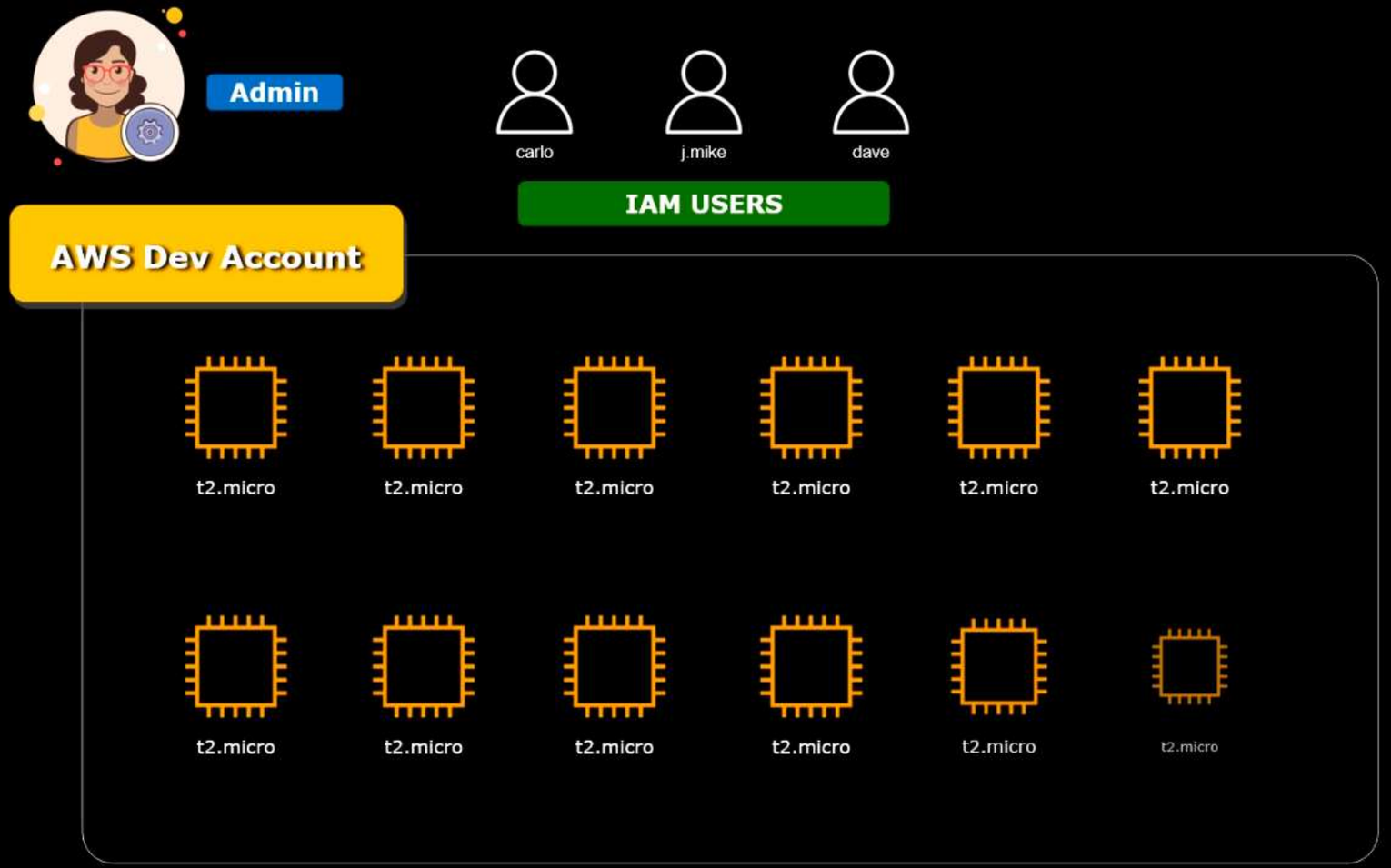


AWS CloudTrail

- A managed service for monitoring and logging account activities
- AWS Management Console, API, or CLI actions are recorded as events
- It can help you facilitate governance, compliance, operational auditing, and risk auditing of your AWS account

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Admin

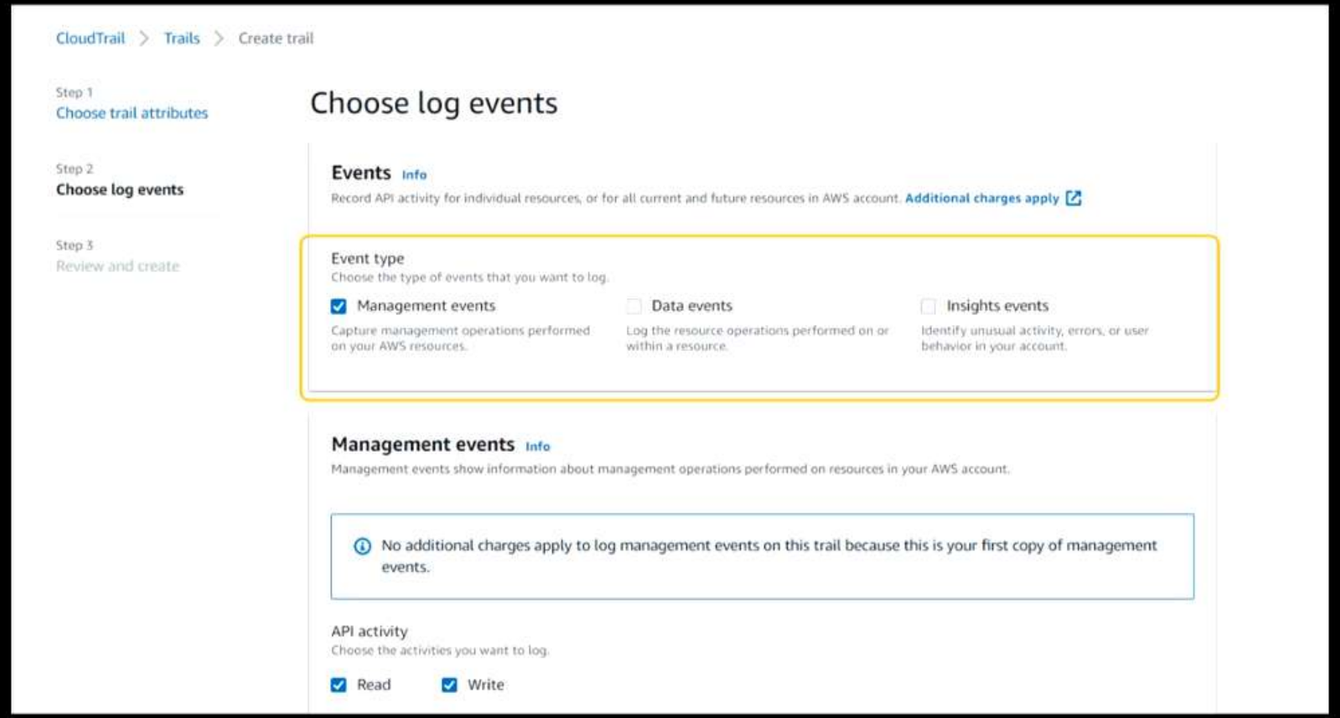
CloudTrail log


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAS2OSY7CBGGXUXXKGJ",
        "arn": "arn:aws:iam::194051115896:user/carlo",
        "accountId": "194051115896",
        "accessKeyId": "ASIAS2LSY7CBL6QTYY4N",
        "userName": "carlo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2021-06-28T16:07:31Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-06-28T16:14:56Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "RunInstances",
    "awsRegion": "ap-southeast-1",
    "sourceIPAddress": "230.205.213.212",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "instancesSet": {
            "items": [
```




IAM USERS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

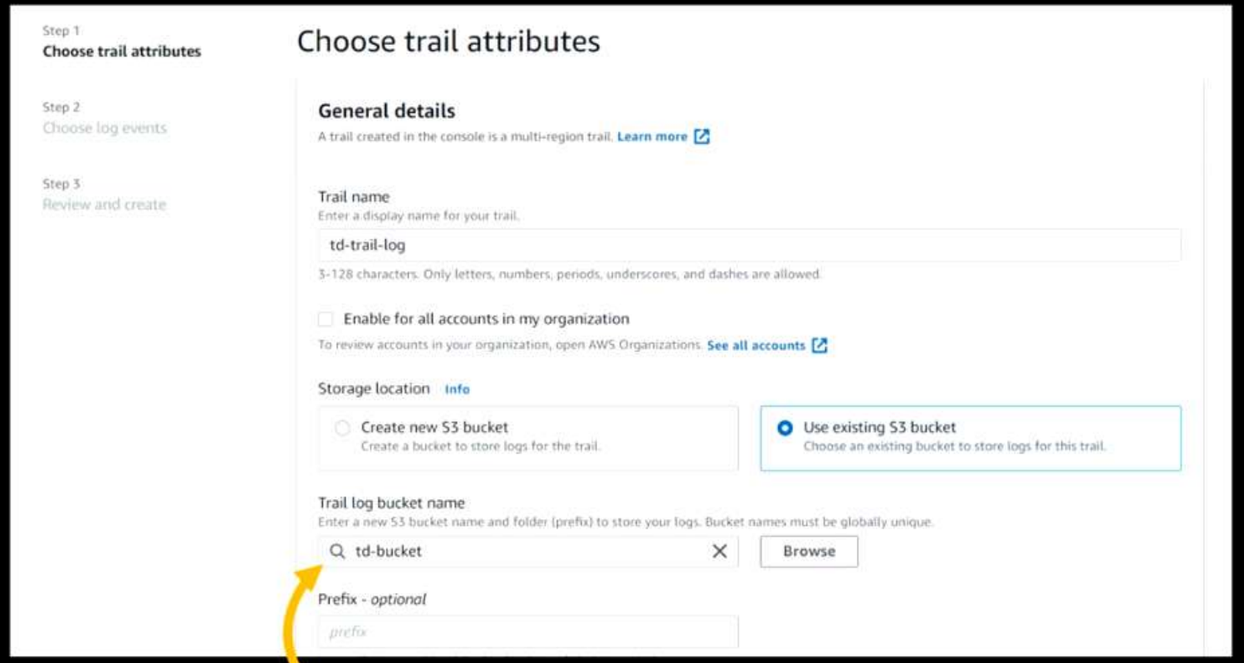


Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Event types

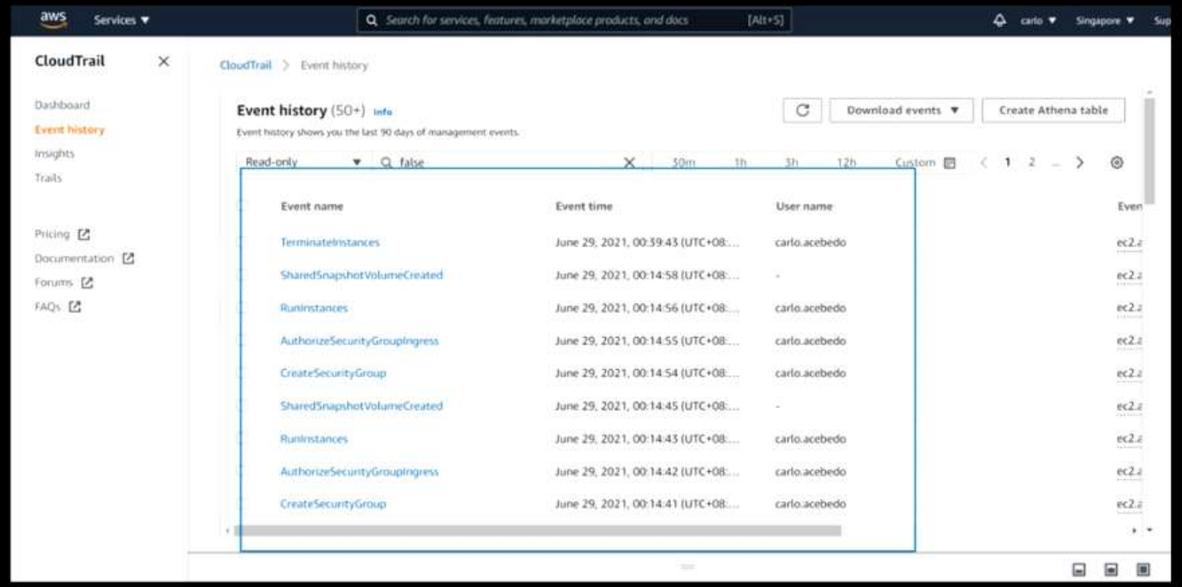
1. Management events
   - management operation events such as user logins
   - enabled by default
2. Data events
   - S3 object-level API events (ex., `GetObject`, `PutObject`)
   - Lambda function Invoke API
   - DynamoDB object-level API activity (ex., `PutItem`, `DeleteItem`)
   - Additional charges apply
3. Insight events
   - Unusual write API calls

Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Trail logs are stored on Amazon S3

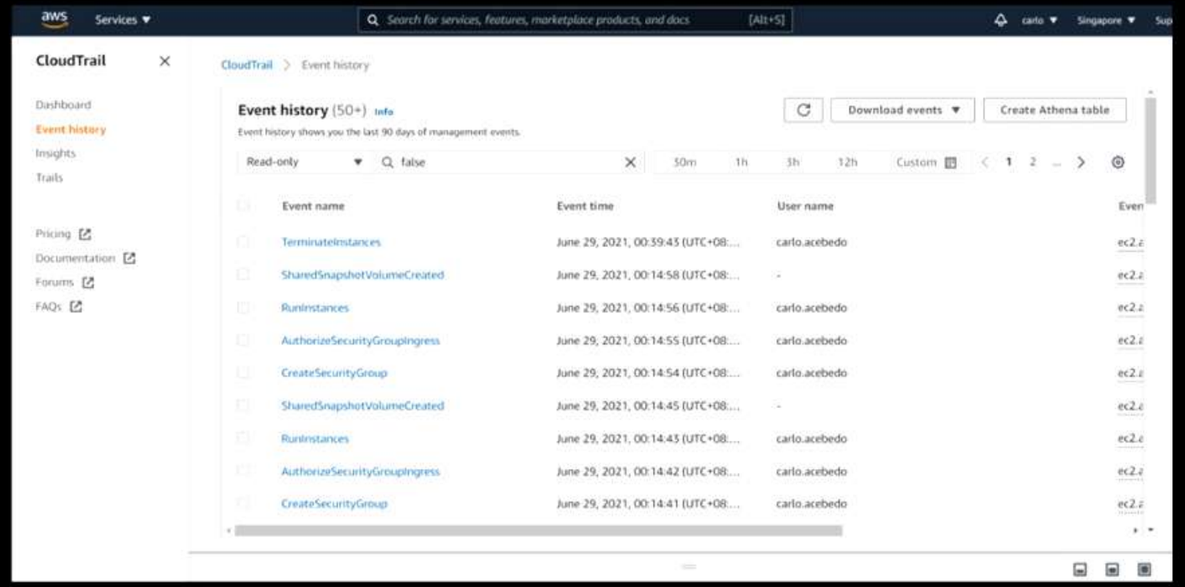
Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Event history

- Gives immediate visibility to management events over the past 90 days
- Data older than 90 days are deleted
- Create a trail to persist logs on an S3 bucket

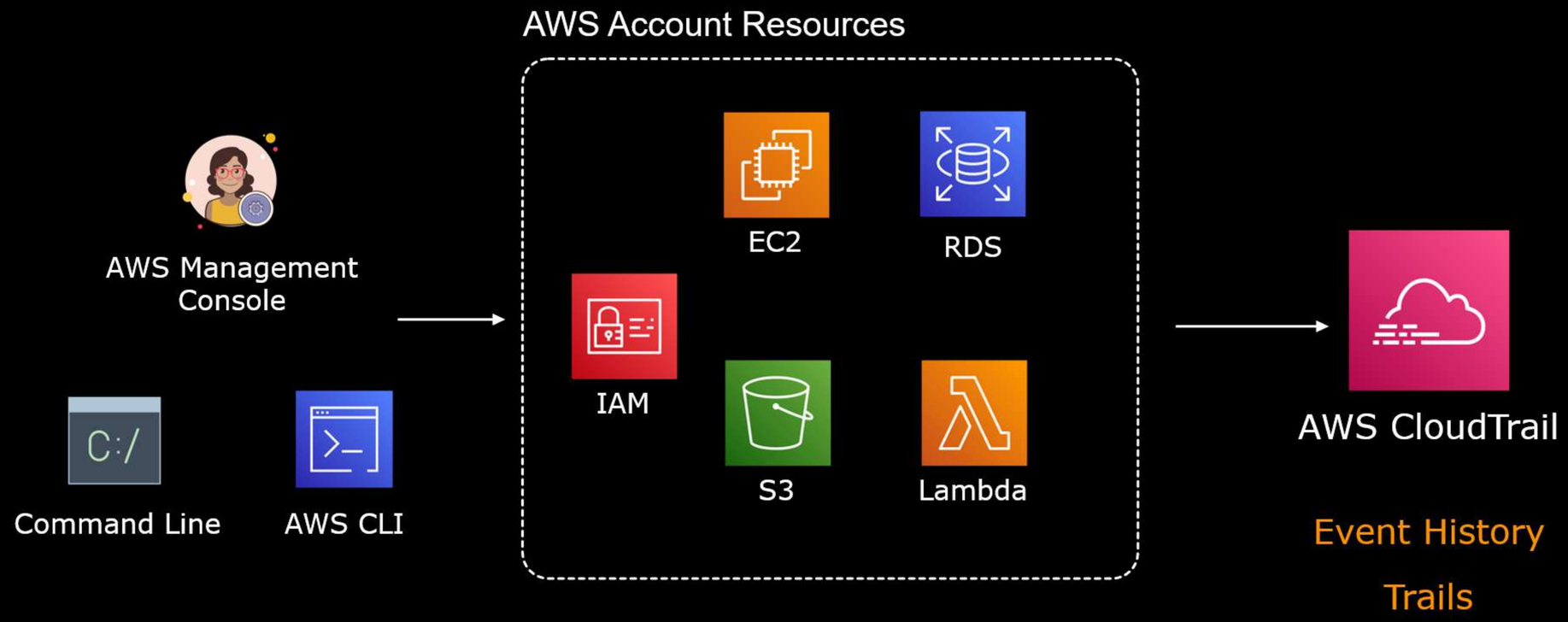


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CloudTrail Integrations

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudTrail

When you create trails:

- By default, trail logs events in all Regions. BEST PRACTICE!
- But you can also log events for individual region.
- Logs collected by the trail will be stored on an S3 bucket.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudTrail

Types of events when creating a trail:



Management Events



Data Events

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Management Events

- refer to the management-related operations performed on your resources
  - attaching policies to a role

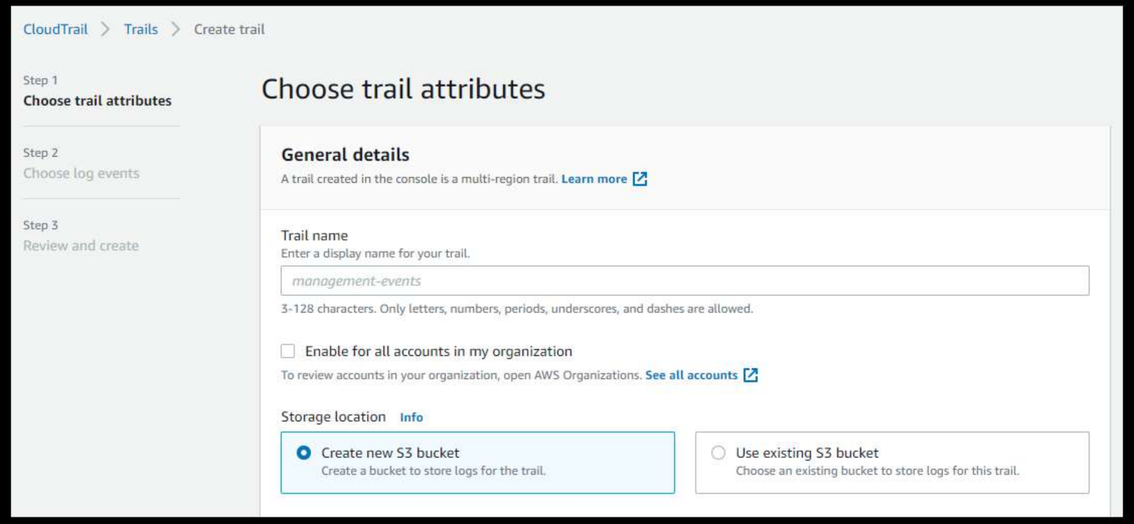


Attach policies to roles

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Management Events

- refer to the management-related operations performed on your resources
  - attaching policies to a role
  - setting up trails in CloudTrail.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Management Events

- refer to the management-related operations performed on your resources
  - attaching policies to a role
  - setting up trails in CloudTrail.
- also include non-API events that occur in your account
  - when a user signs in to your account



AWS Management Console



Command Line

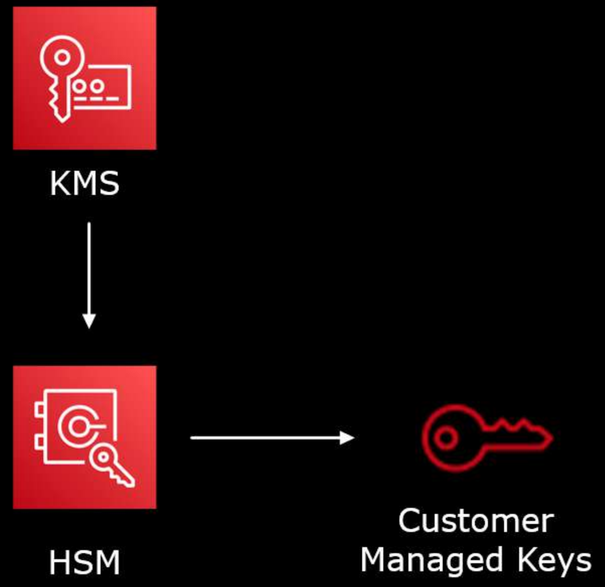


AWS CLI

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Management Events

- refer to the management-related operations performed on your resources
  - attaching policies to a role
  - setting up trails in CloudTrail.
- also include non-API events that occur in your account
  - when a user signs in to your account
  - when AWS automatically rotates a customer-managed key in KMS



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Management Events

- Create a trail using the management account for an organization in AWS Organizations. This is called an organization trail.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Data Events

- information about operations performed in resources you manage like:
  - S3 bucket and object-level activities
  - Lambda function is invoked
  - A DynamoDB object-level activity was performed on tables
  - when an EBS snapshot was taken

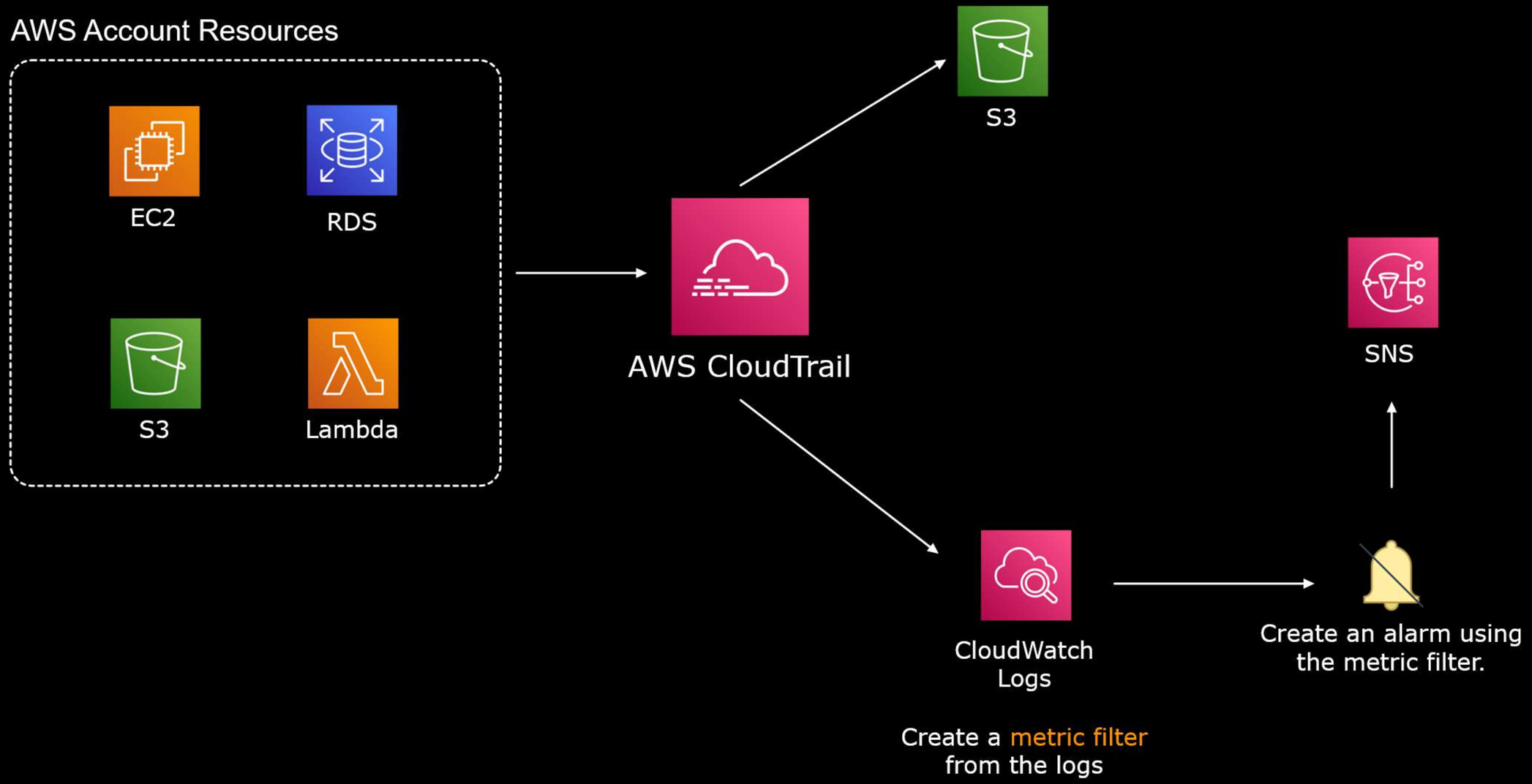

S3


Lambda

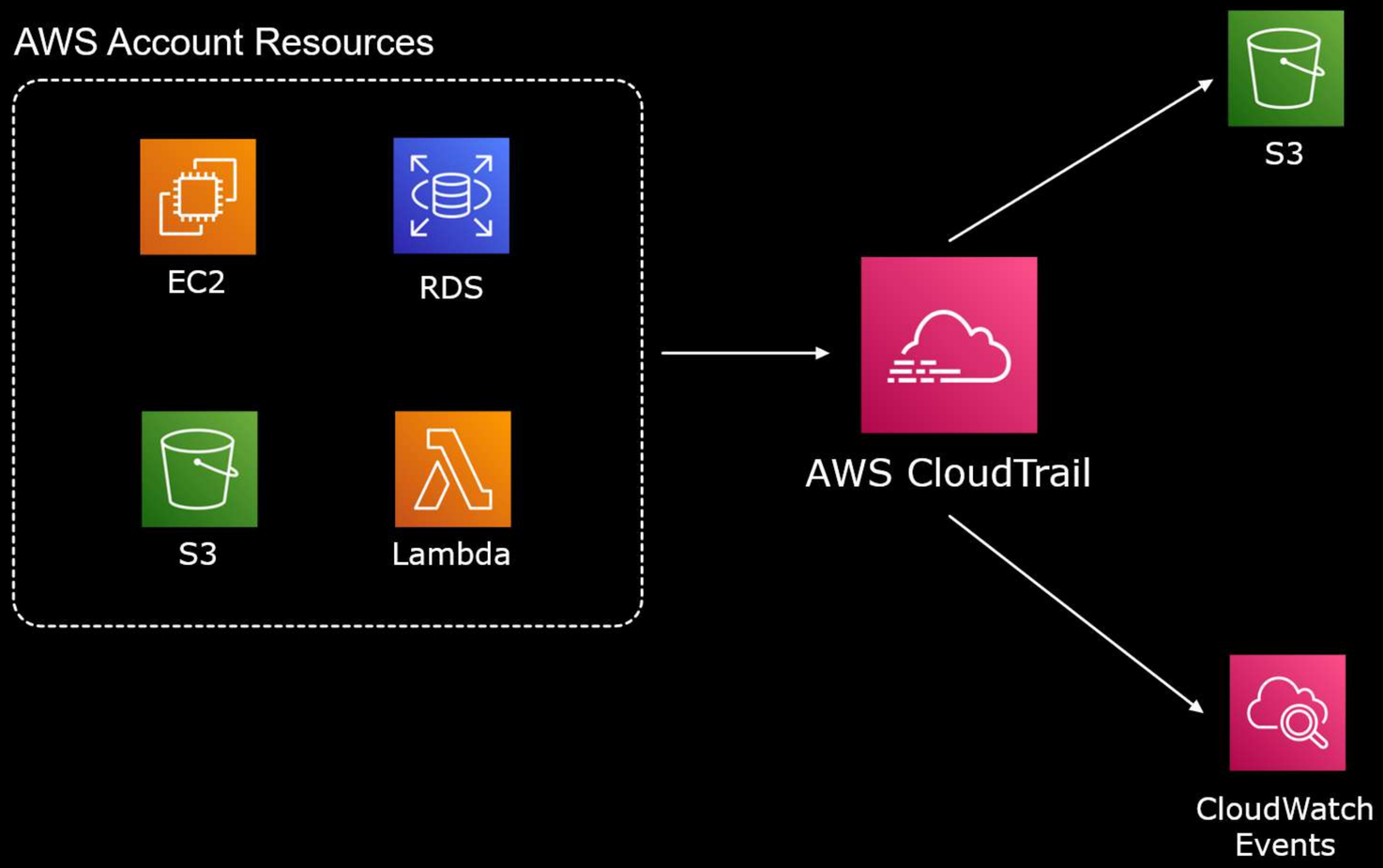

DynamoDB


EBS

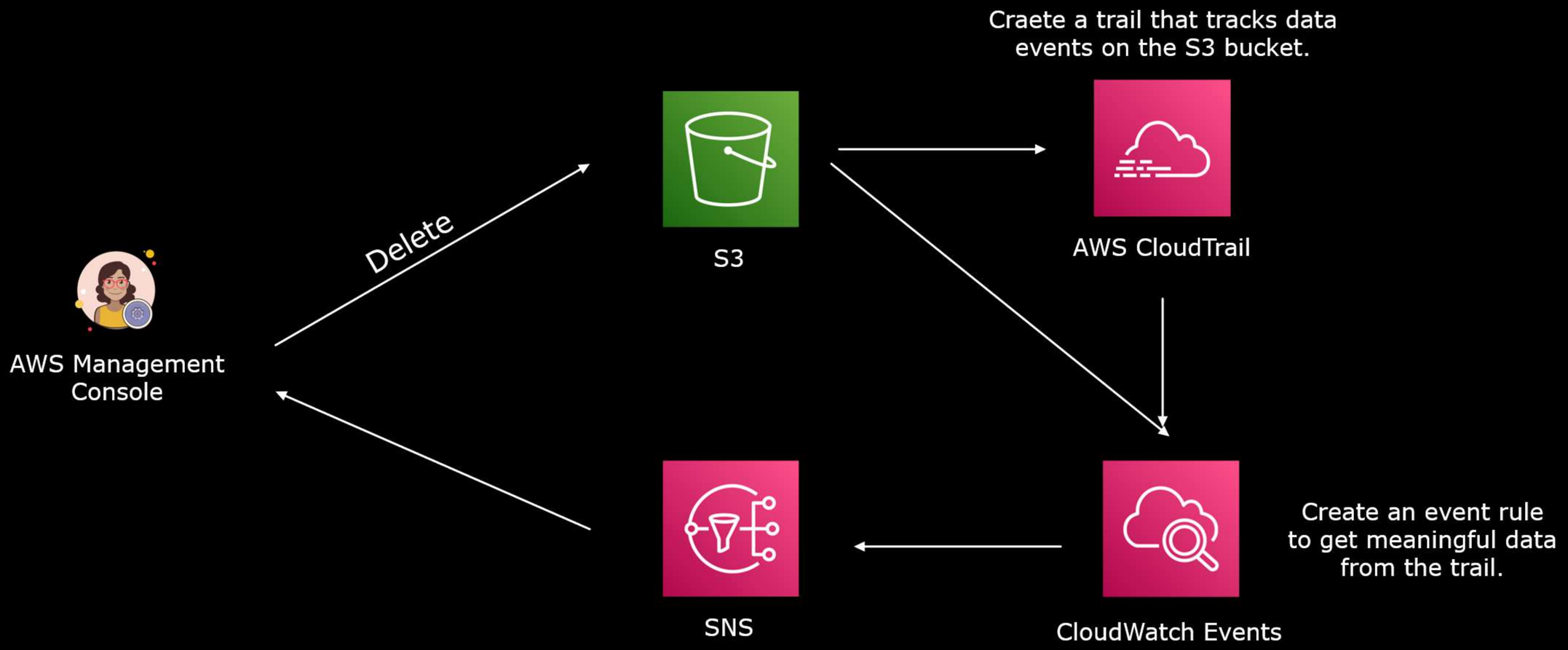
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

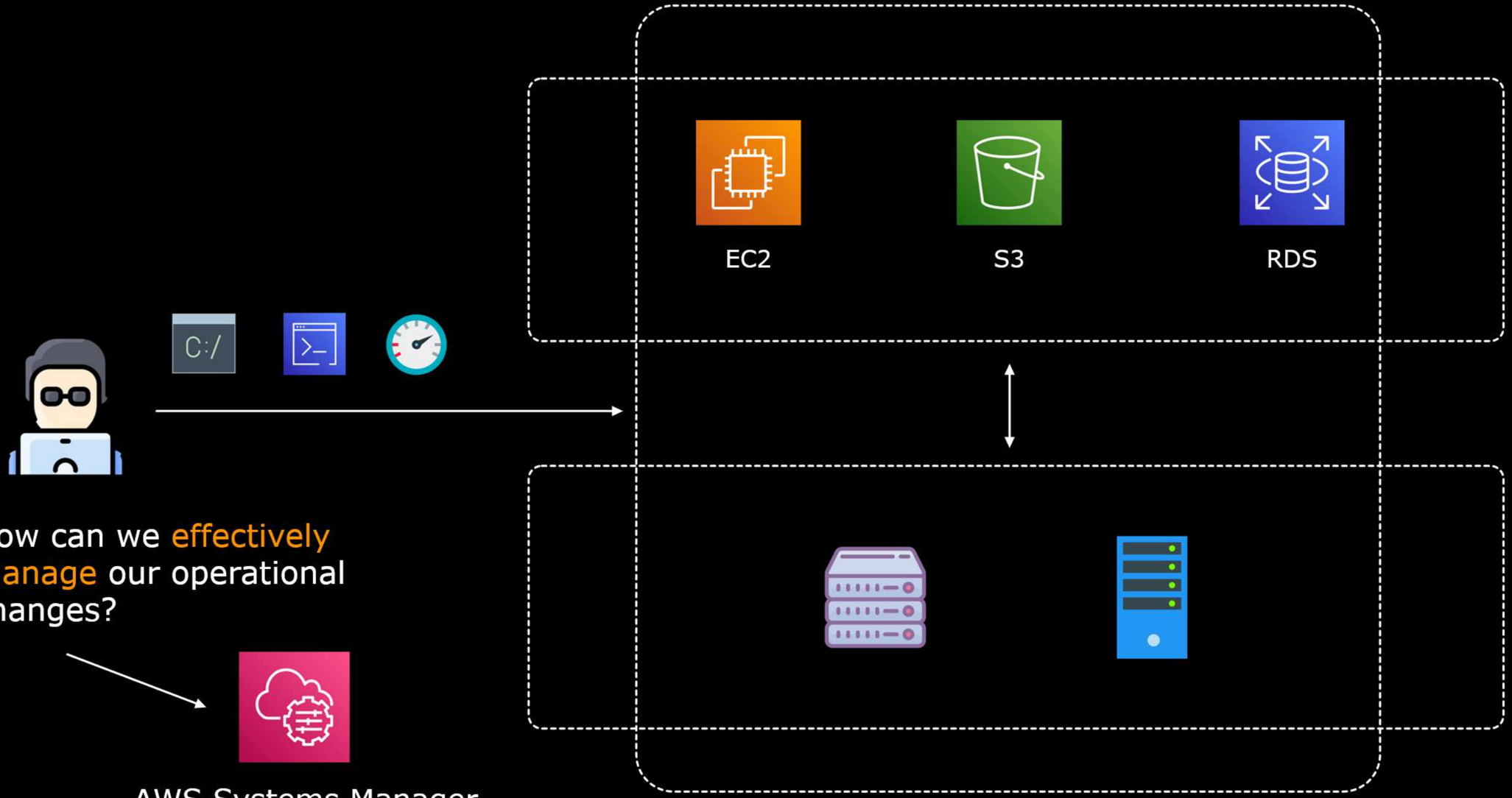


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Systems Manager Parameter Store

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

At the end of the video, you will be able to:

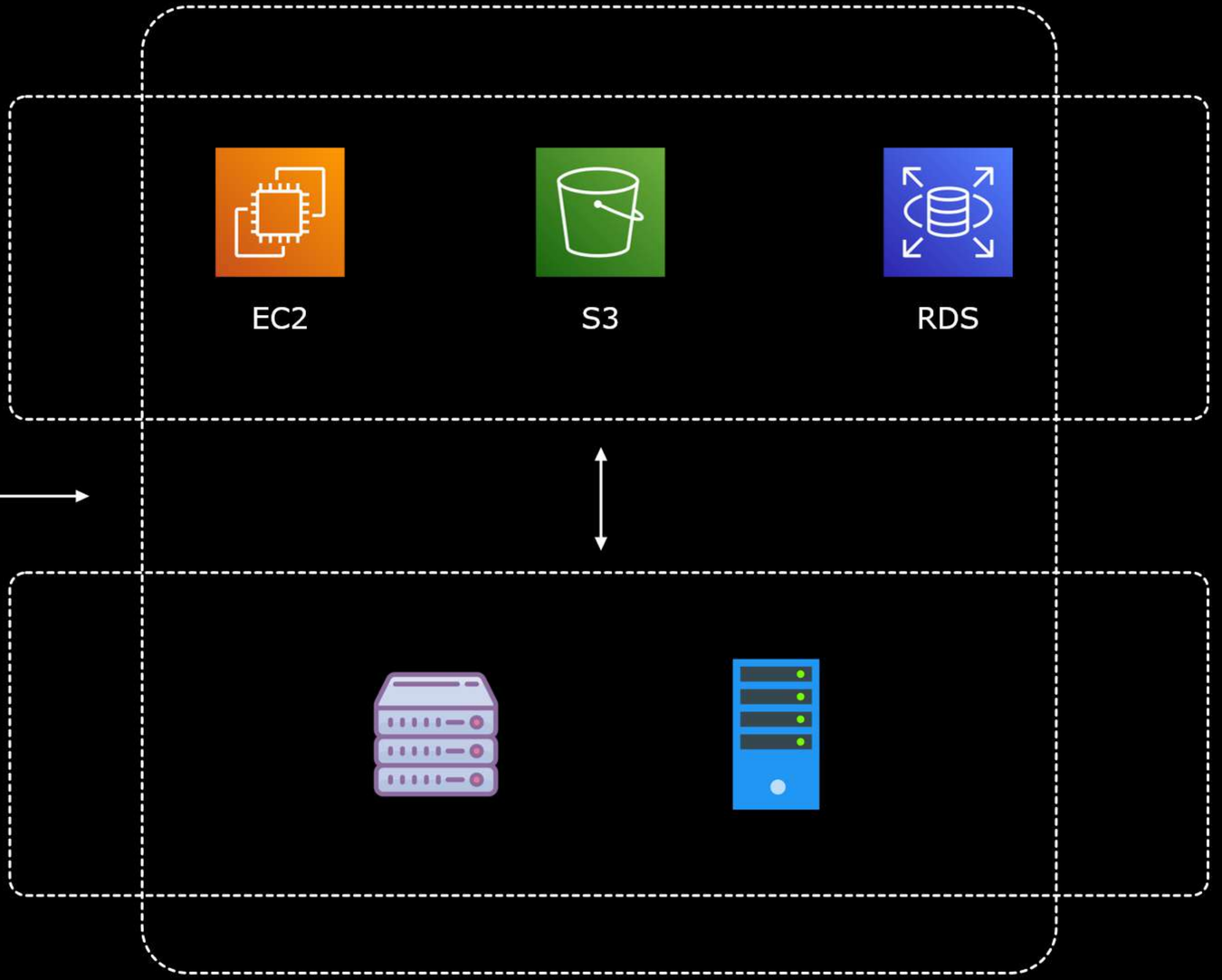
- explain what is AWS Systems Manager
- discuss the use cases, features, and limitations for the Parameter store

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





- simplifies the process of resource and application management
- shortens the time to detect and resolve operational problems
- makes it easier to operate and manage your infrastructure at scale.



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

- Parameter Store
- Change Manager
- Automation
- Patch Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

- Parameter Store
- Automation
- Change Manager
- Patch Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

What is AWS Systems Manager Parameter Store?

- It is one of the capabilities of the AWS Systems Manager
- Allows you to store and access data like:
  - digital authentication credentials
  - configuration data
  - passwords
  - keys
  - APIs
  - tokens

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



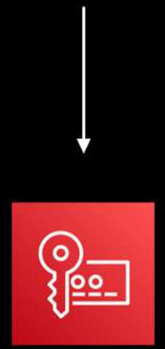
AWS Systems Manager

- tightly coupled with AWS KMS
- version tracking
- integrates with IAM

Parameter Store



`SecureString`



AWS KMS



RDS

Database Strings



On-premises Server

Tokens

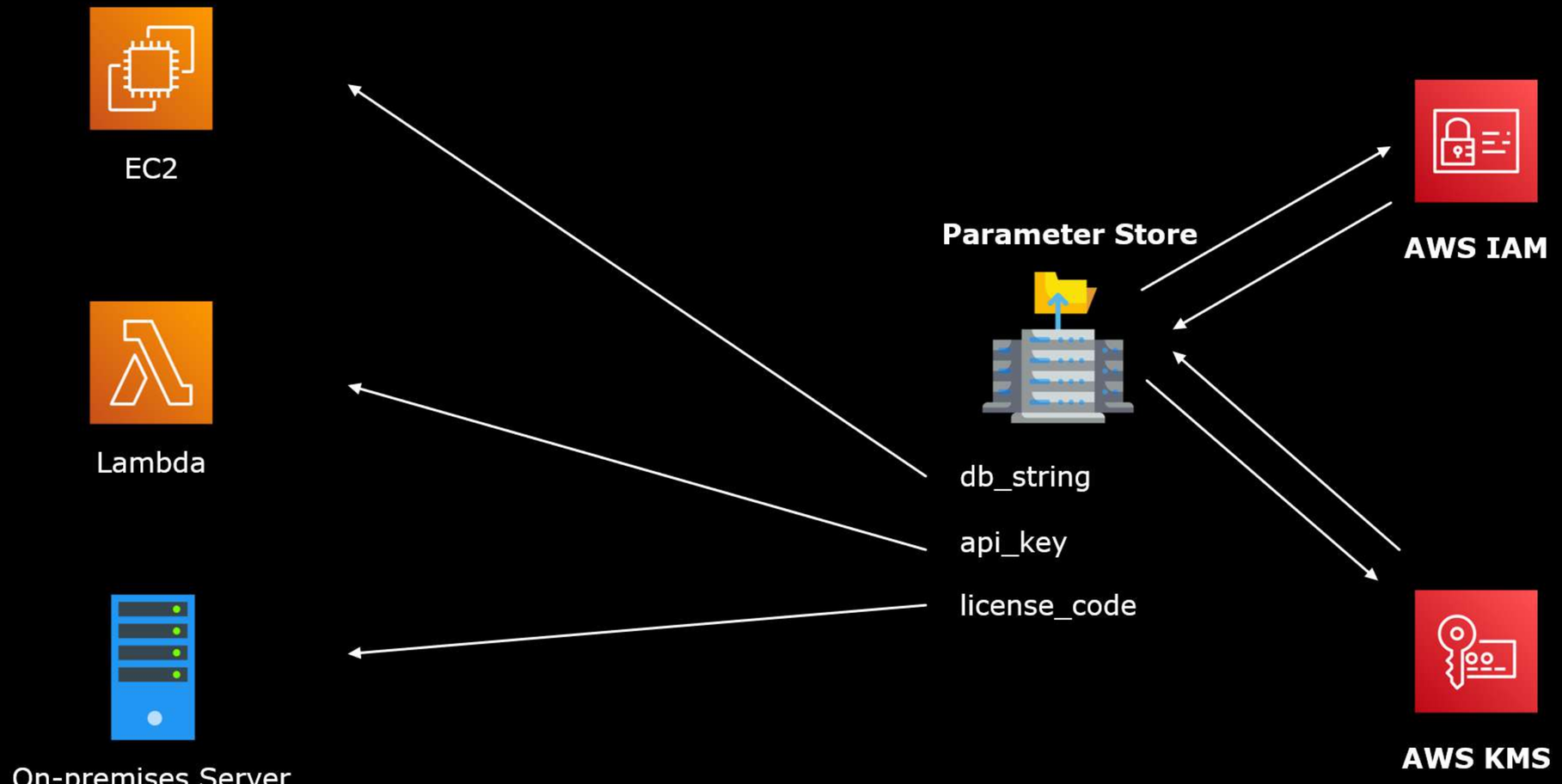
License Codes



EC2

Secrets

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

Parameter Hierarchies

- great when you are working on a large organization
- resolves the issue of having too many parameters
  - prone-to-error and time consuming
  - can cause accidentally deletion or use the wrong parameter
  - create duplicate parameters that use the same configuration data
- A hierarchy is simply a parameter name that includes a path that you define by using forward slashes (/)

PROD	/Prod/DBServer/MySQL/db-string-connection
DEV	/Dev/DBServer/MySQL/db-string-connection

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation



AWS Systems Manager Parameter Store

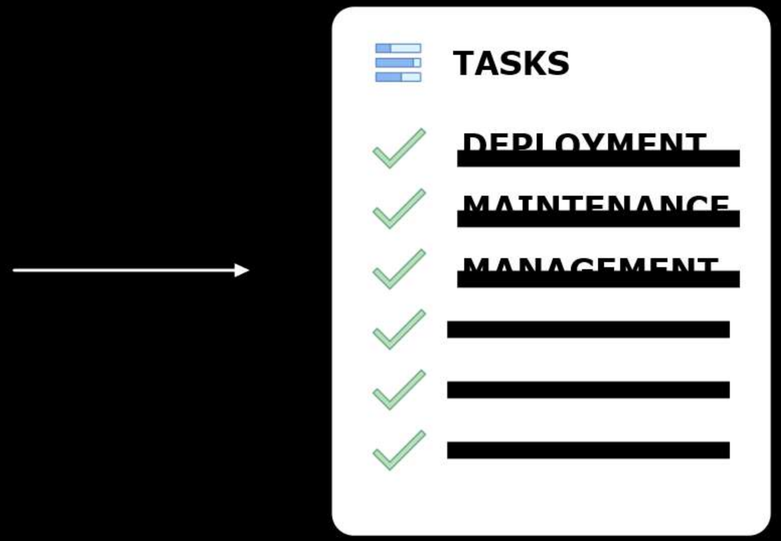
```
"Parameters" : {
  "InstanceTypeParameter" : {
    "Type" : "String",
    "Default" : "t2.micro",
    "AllowedValues" : ["t2.micro", "m1.small", "m1.large"],
    "Description" : "Enter t2.micro, m1.small, or m1.large. Default is t2.micro."
  }
}
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Systems Manager Automation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





Automation

accelerates the delivery of resources and applications by automating manual and repetitive processes that can be prone to issues

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Let's restart the instance via AWS Management Console!

AWS Management Console

Systems Manager

Managed Instances

EC2

Status Checks

System Status Check

Instance Status Check

Issue caused by underlying hardware

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Management Console

Systems Manager

Managed Instances

EC2

Status Checks

System Status Check

Instance Status Check

EC2

Status Checks

System Status Check

Instance Status Check

EC2

Status Checks

System Status Check

Instance Status Check

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

What can Systems Manager Automation do for you?

- simplifies the process of implementing maintenance and deployment tasks on Amazon EC2 instances like:
  - applying OS patches or application update
  - creating and updating Amazon Machine Images (AMIs)
  - applying driver and agent updates
  - resetting passwords on Windows Server instances
  - recovering an unreachable instance
  - resetting SSH keys on Linux instances

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

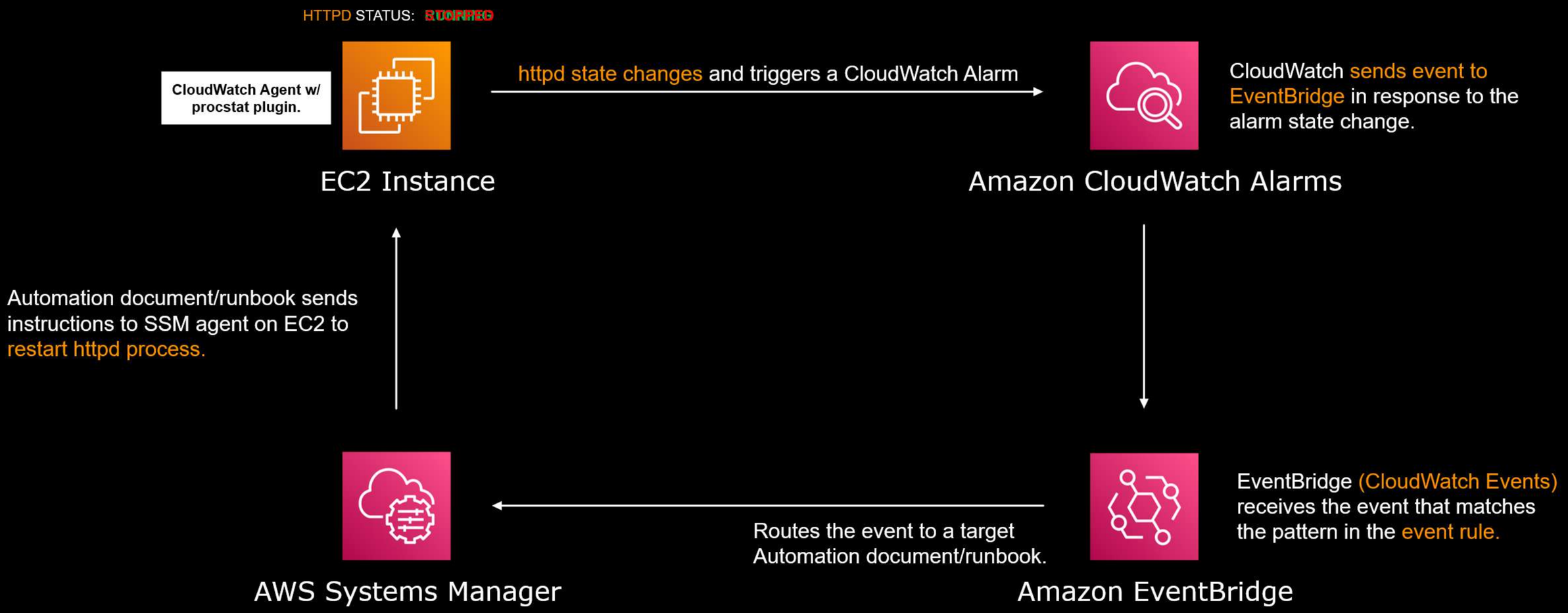


AWS Systems Manager

Systems Manager Automation document (now referred to as runbook)

- An automation document contains one or a series of actions that run in:
  - sequential order
  - conditionally branched
- The process of running actions and their steps is called the automation workflow
- You can either use predefined Automation documents or you can create your own custom documents
- Integrates with CloudWatch Events (or EventBridge)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Systems Manager
Change Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

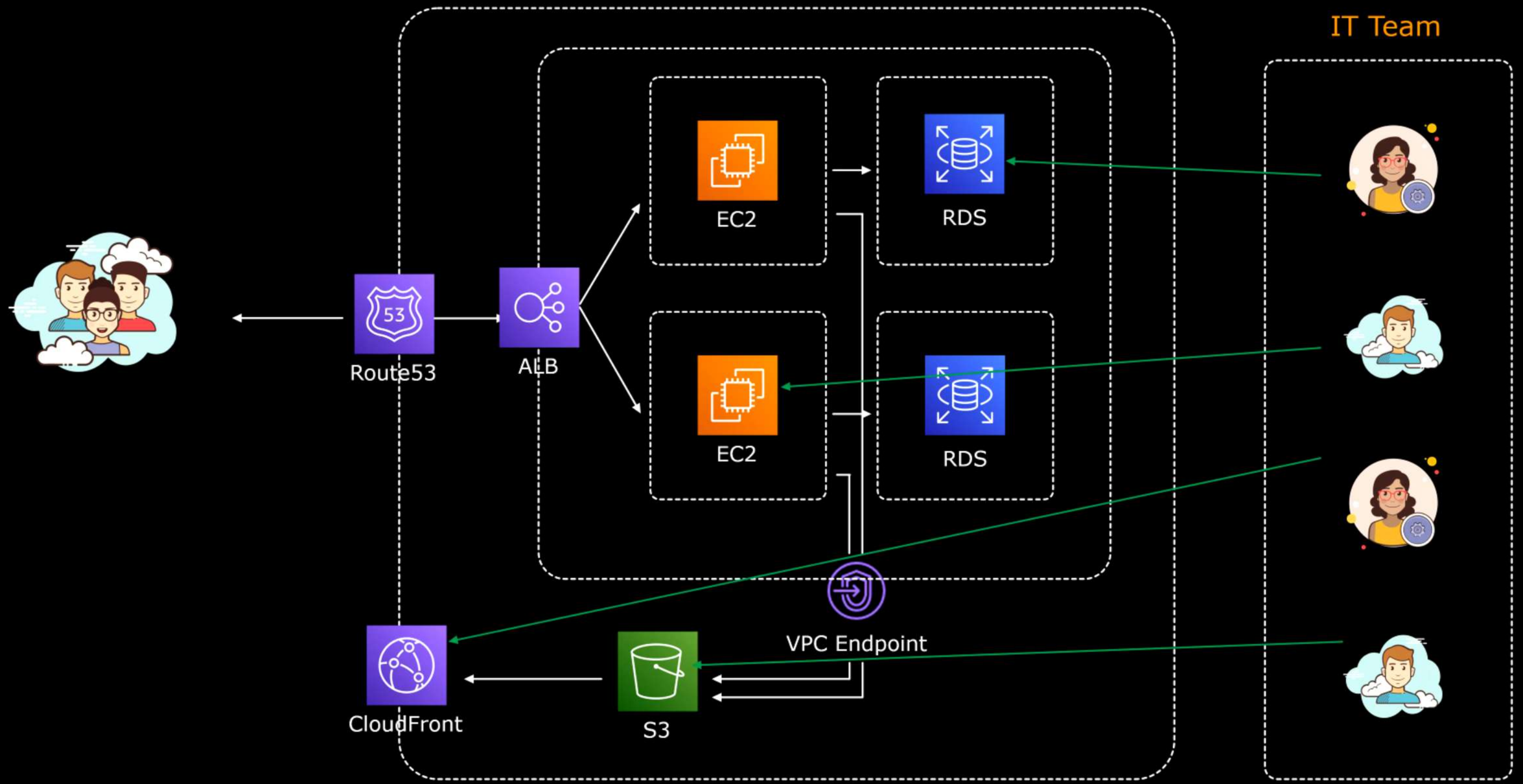


AWS Systems Manager

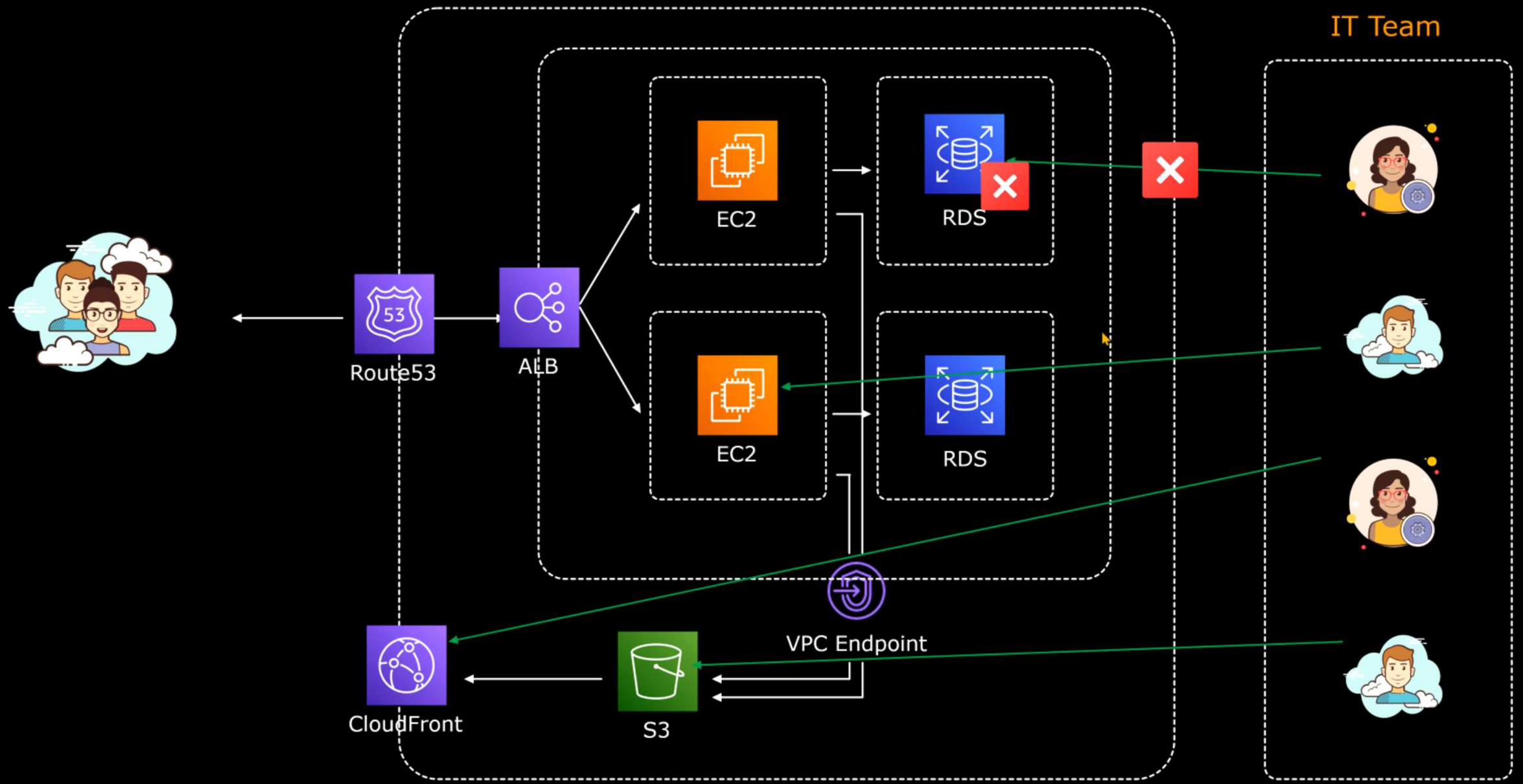
At the end of the video, you will be able to:

- Understand the problems that Change Manager solves in your organization
- Get a general idea of the key concepts like change templates, change requests, and automation runbooks

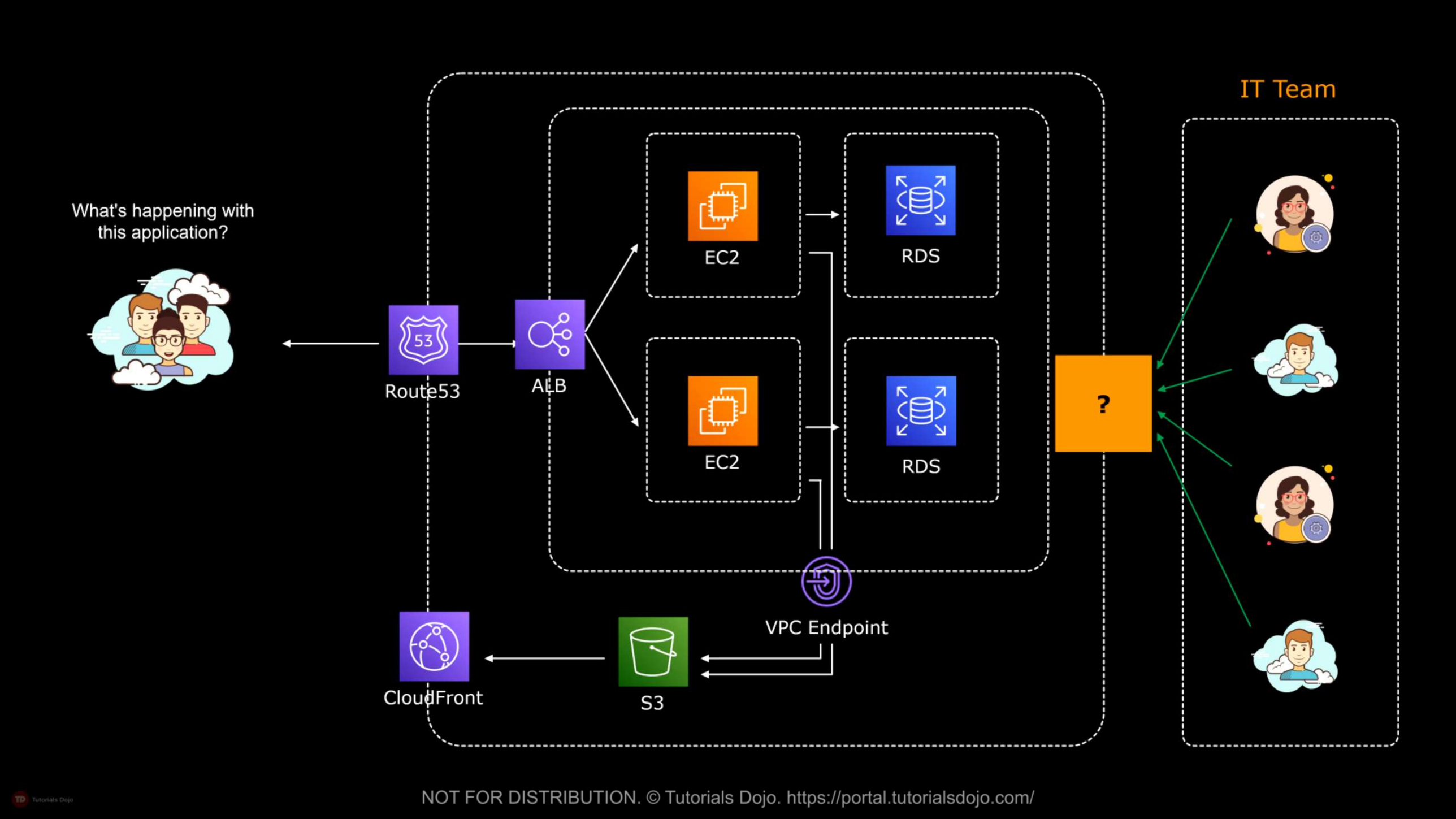
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



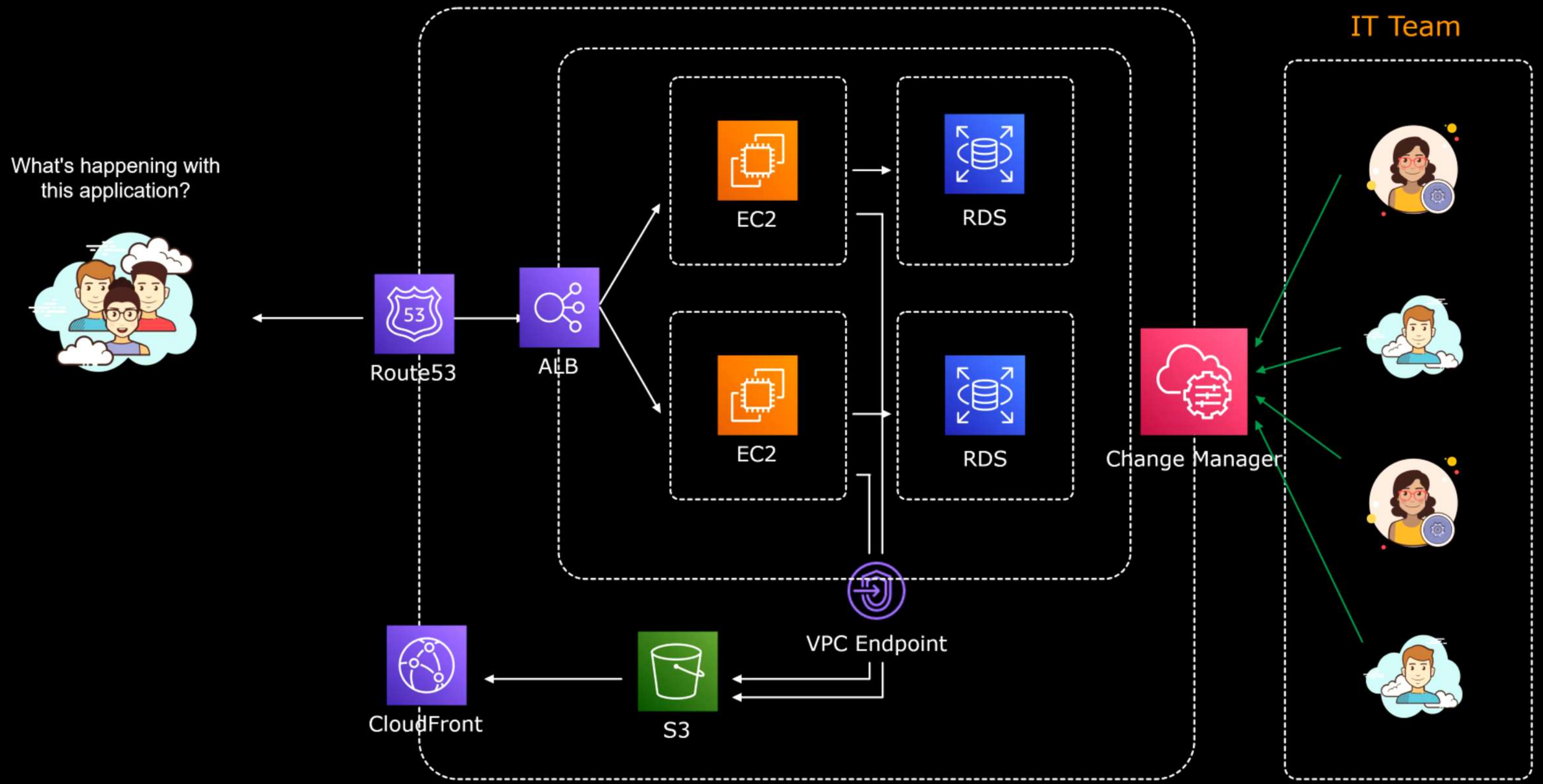
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



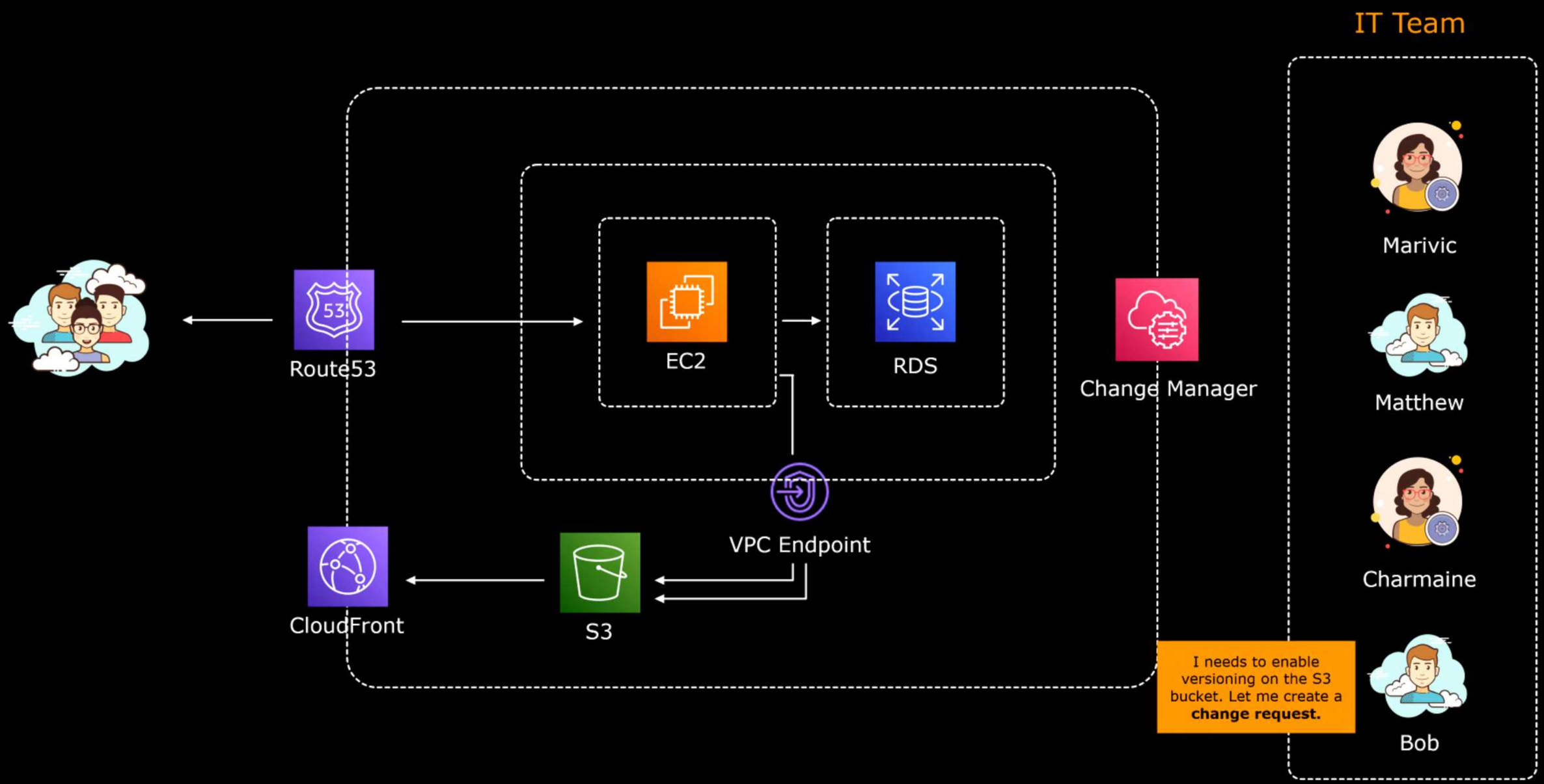
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



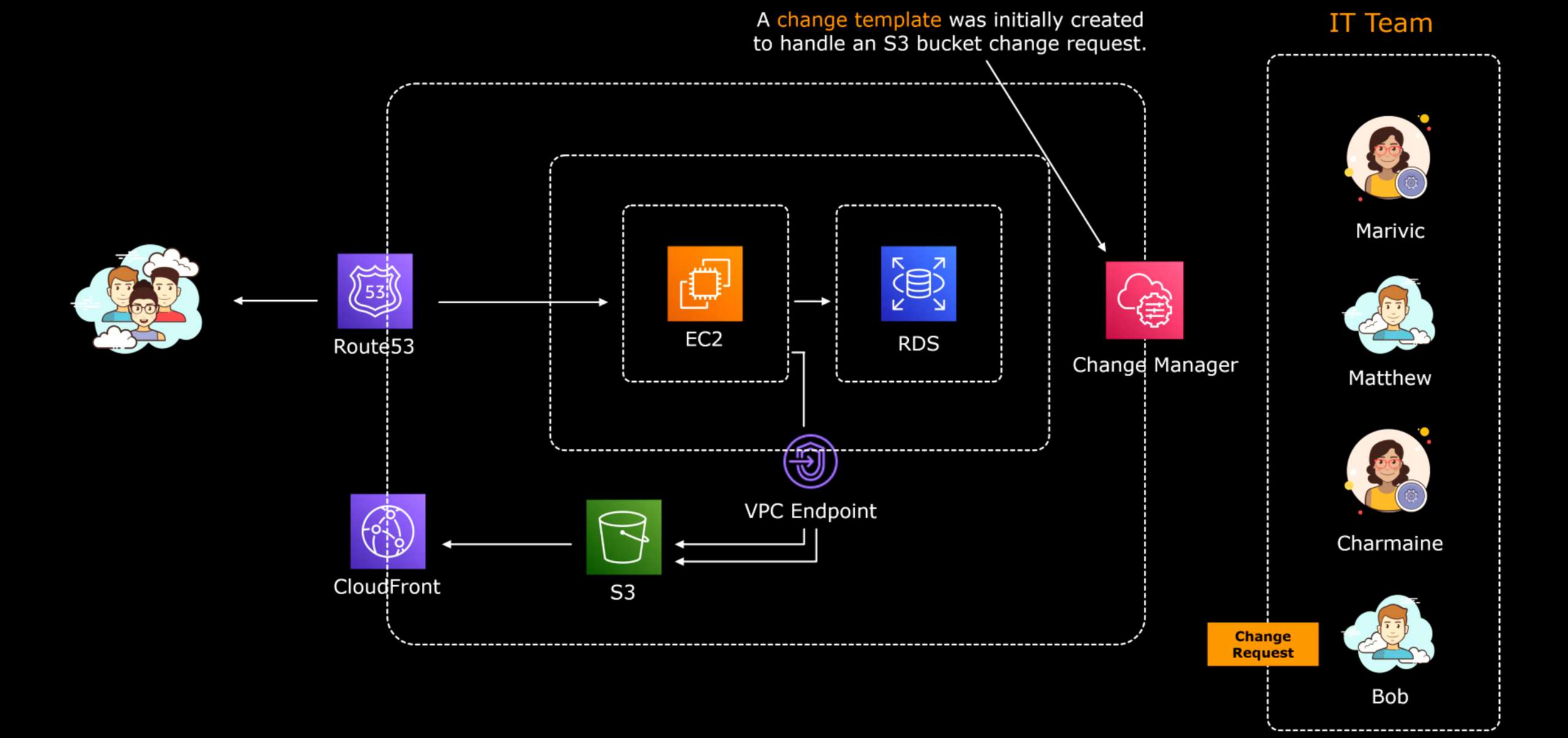
AWS Systems Manager
Systems Manager

- is a capability of AWS Systems Manager service mainly used to request, approve, implement, and report on operational changes to your application configuration and infrastructure

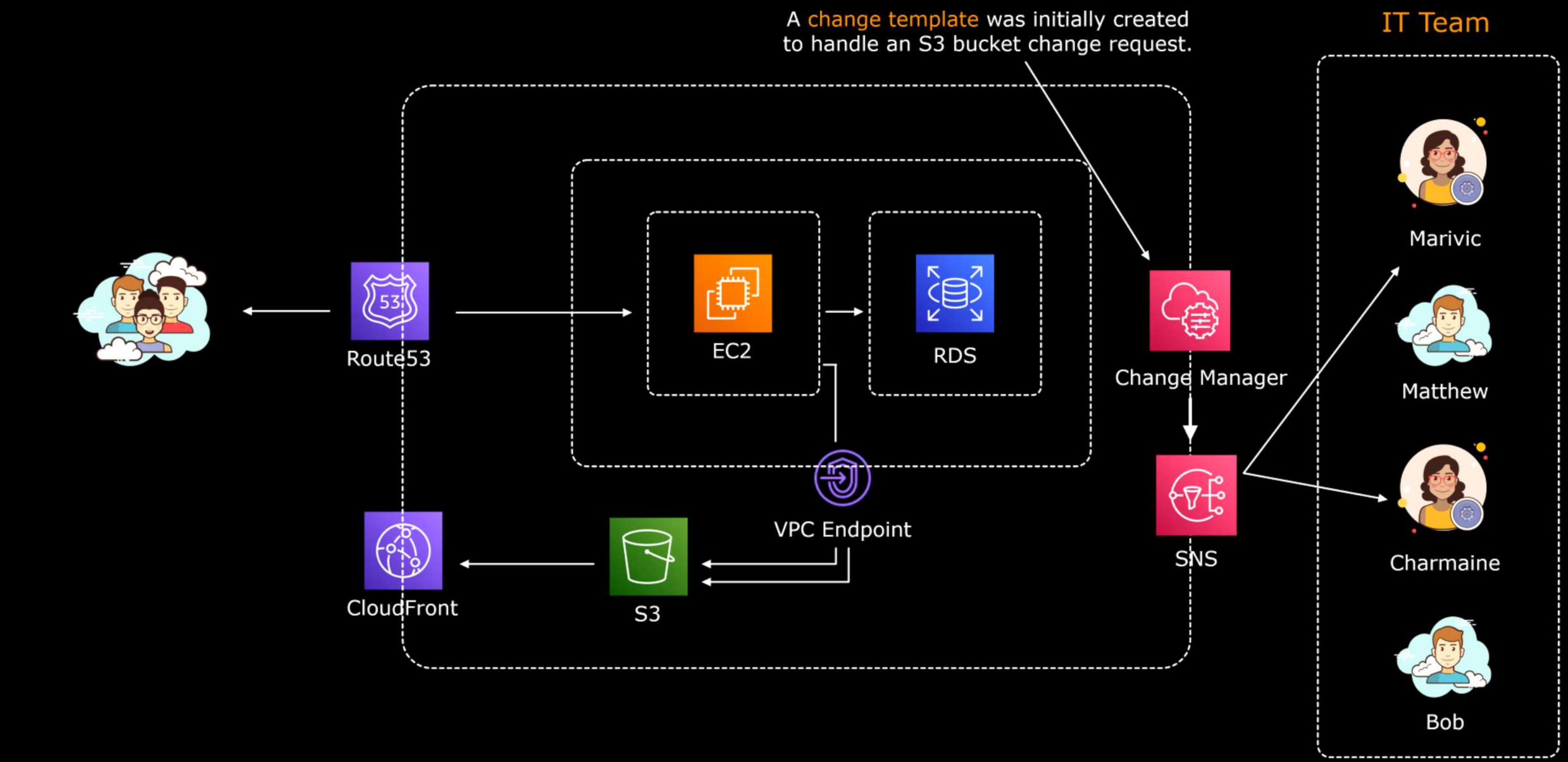
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

Systems Manager Change Manager

- Users across your organization or in a single AWS account can perform change-related tasks on which they have been granted the necessary permissions.
- Flexibility to assign approvers for change requests in the change template, or even let users assign approvers for the change request itself.
- You can configure Change Manager based on the active change calendar for your organization.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

Requirements in creating a change template:

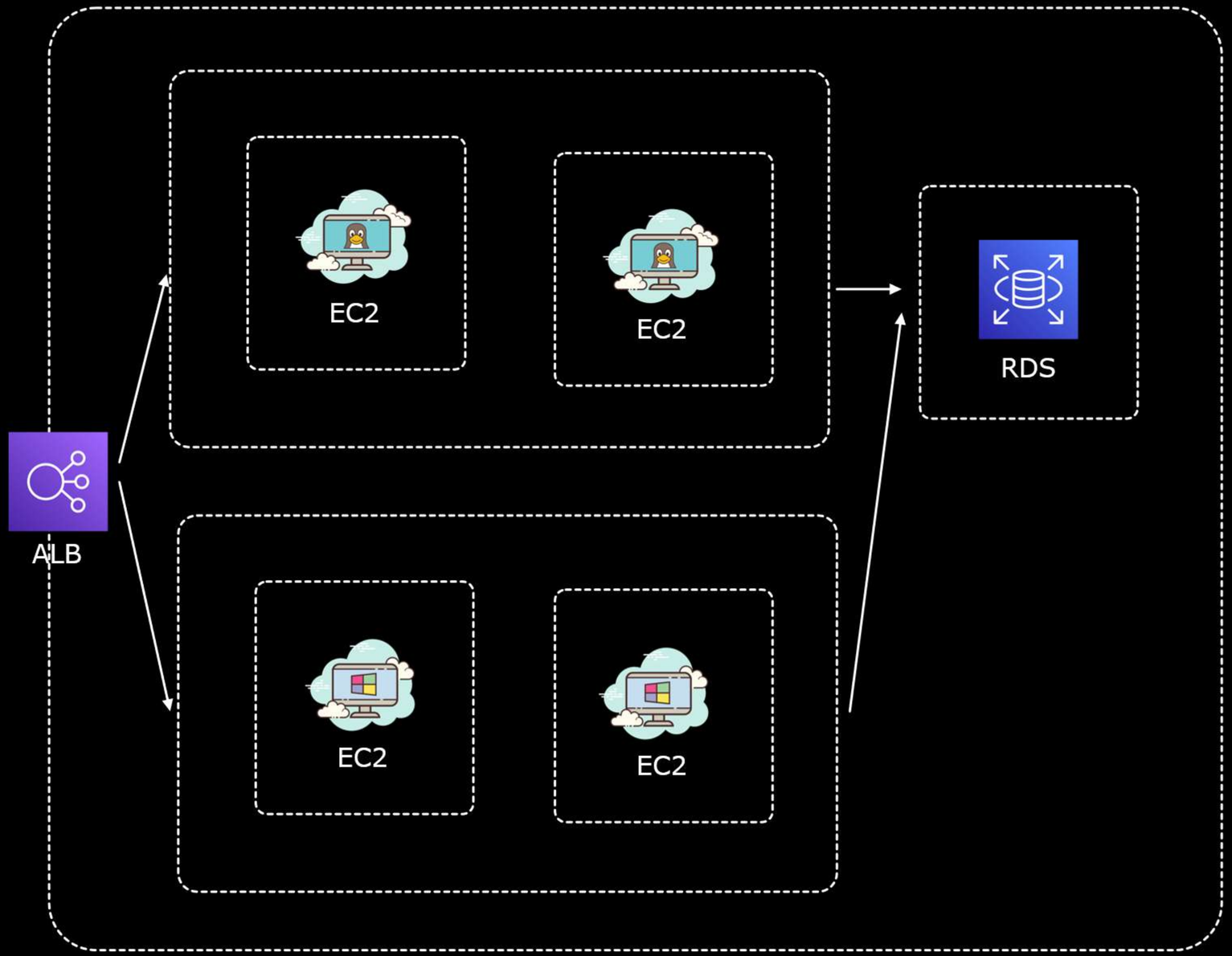
- One or more Automation runbooks for a user to choose when creating a change request.
- The Approvers
- An SNS topic to notify assigned approvers when a change request is ready
- A CloudWatch alarm that will monitor the runbook workflow
- An SNS topic to send notifications about status changes for change requests
- The auto-approved request setting which defines whether change request can be run without an approval step

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Systems Manager Patch Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





I need to update the operating system of the instances.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager Patch Manager

- allows you to automate the process of patching the operating system of your EC2 instances

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

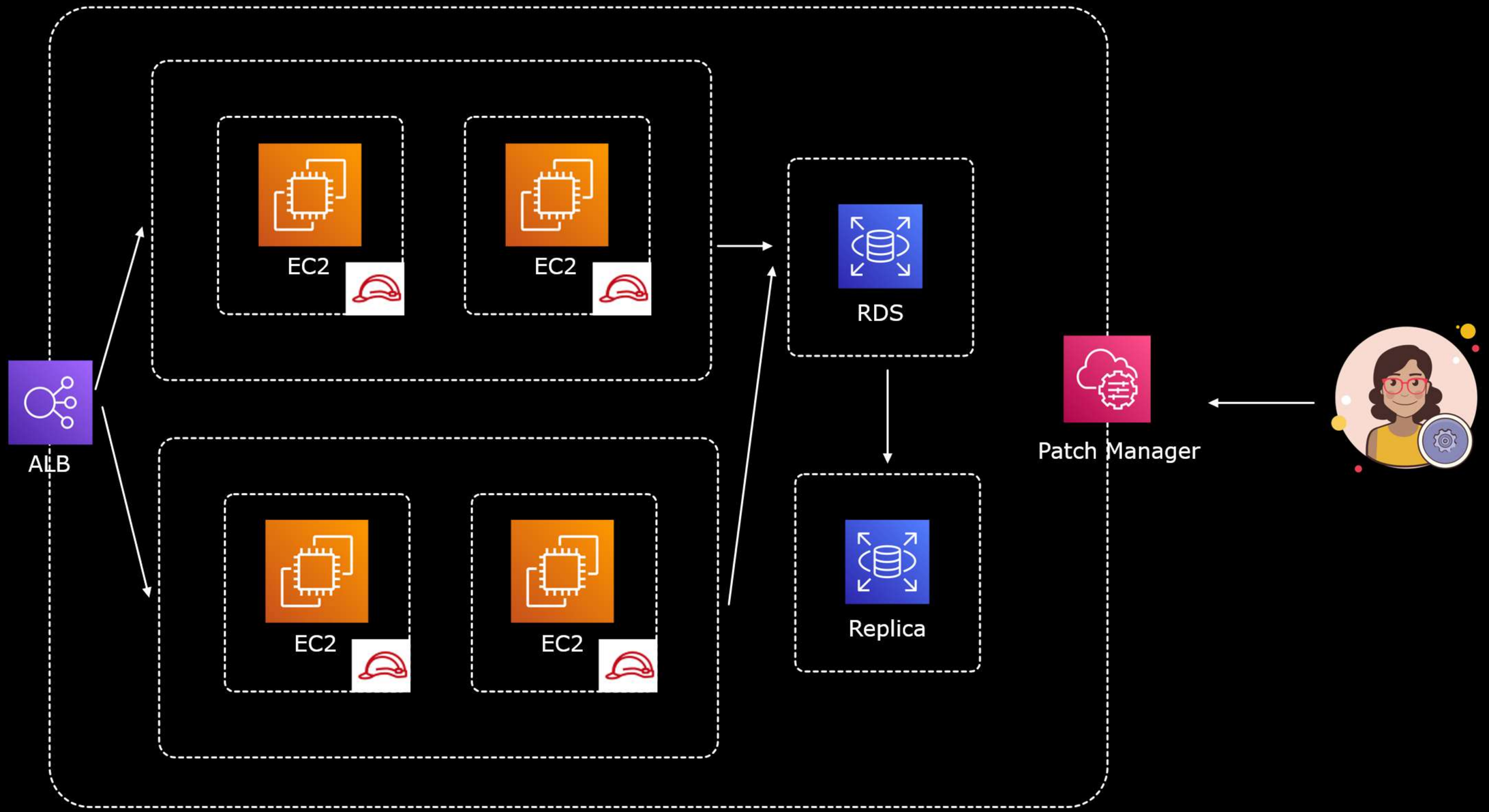
How to patch an instance?

- Attach an IAM role on the instances that allow Systems Manager to manage the Instance



AWS Systems Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

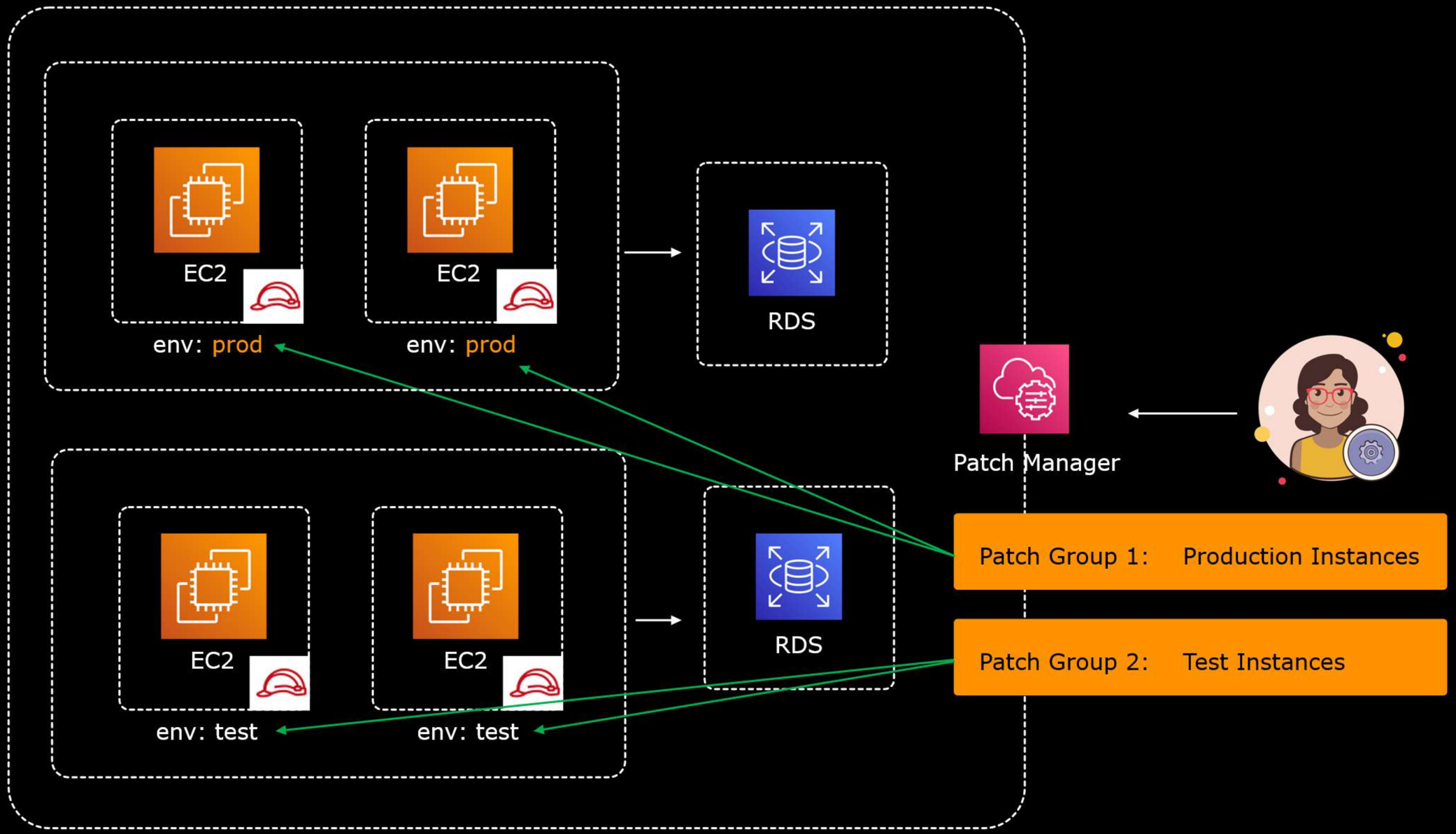


AWS Systems Manager

How to patch an instance?

- Attach an IAM role on the instances that allow Systems Manager to manage the Instance
- Create a patch baseline
  - defines which patches are approved for patching on your instances
  - AWS provides patch baselines but you can create custom patch baselines
  - Includes approval rule that indicates when patches should be approved or installed
- Create a patch group
  - Organize instances using EC2 tags

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

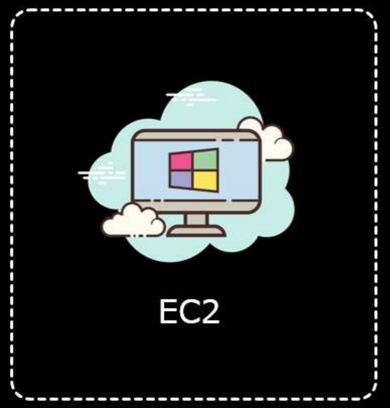


AWS Systems Manager

How to patch an instance?

- Attach an IAM role on the instances that allow Systems Manager to manage the Instance
- Create a patch baseline
  - defines which patches are approved for patching on your instances
  - AWS provides patch baselines but you can create custom patch baselines
  - Includes approval rule that indicates when patches should be approved or installed
- Create a patch group
  - Organize instances using EC2 tags
- Create a patch
  - Specify the patch group and the patching schedule

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/





Windows Update API

Patch Manager **doesn't install all available patches**, it only installs minor patches that are focused on security.





Yum Package Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

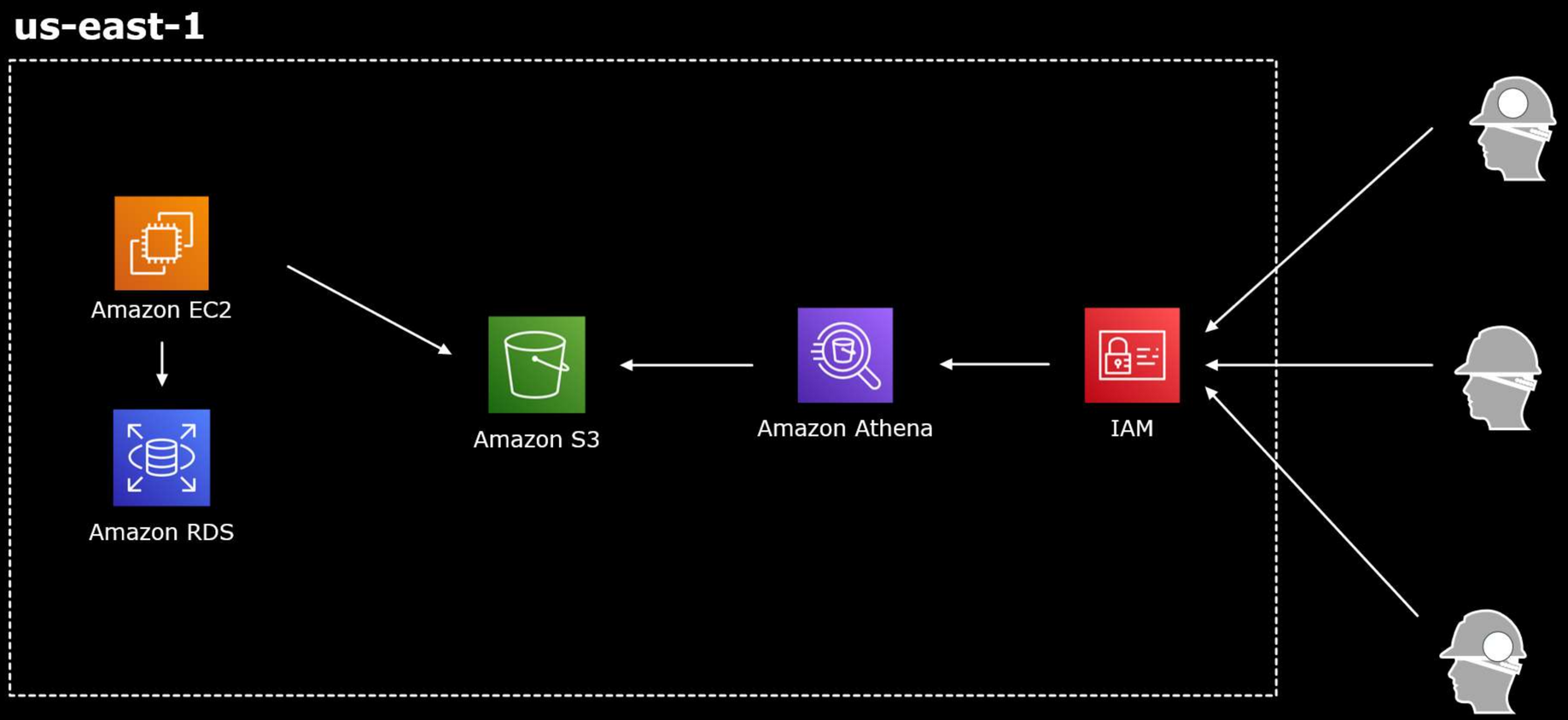


AWS CloudFormation

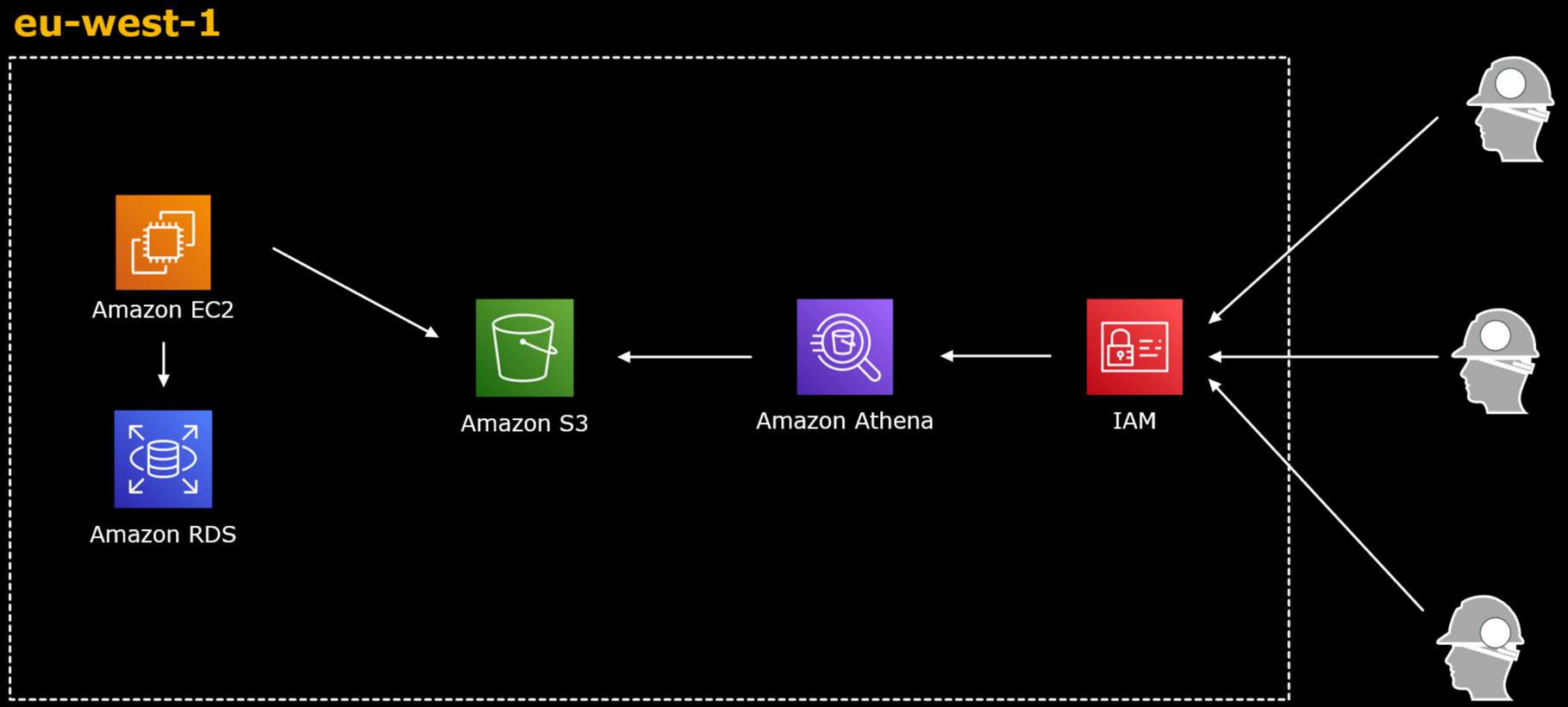
At the end of the video, you will be able to:

- understand how AWS CloudFormation can help you build your cloud infrastructure
- explain key concepts like templates, stacks, and changesets.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



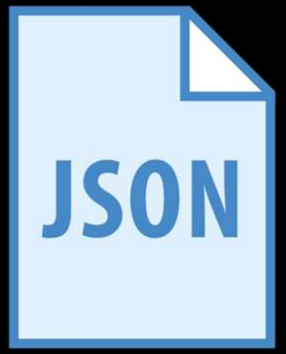
Deployment Documentation

- EC2 instance configuration
- RDS database configuration
- S3 bucket Configuration
- IAM permissions for Athena

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



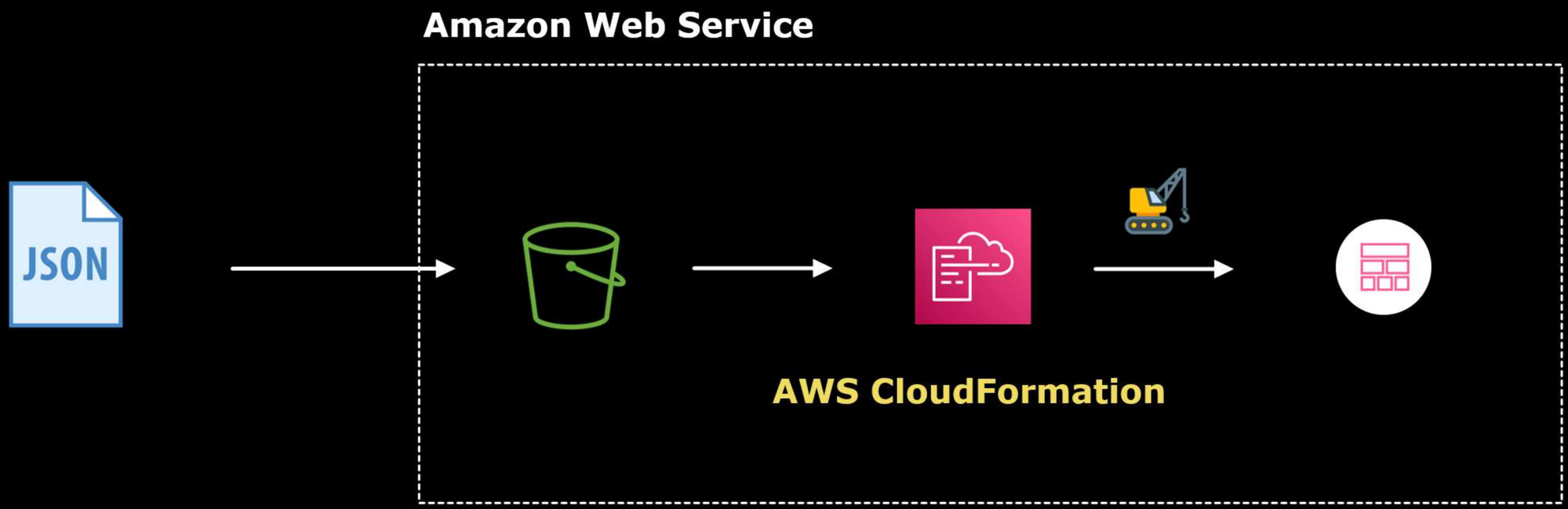
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Wouldn't it be nice to write a document or a template file where you can:

- define how resources are constructed
- define the connections between resources
- define permissions needed
- write infrastructure in CODE.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation

AWS CloudFormation helps you:

- simplify infrastructure management by building your infrastructure using code in templates
- quickly replicate your infrastructure by reusing CloudFormation templates that you created
- easily control and track changes to your infrastructure by using rollback actions and version control on your templates.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

JSON

```
"Ec2Instance" : {
    "Type" : "AWS::EC2::Instance",
    "Properties" : {
      "ImageId" : "ami-26190097123",
      "KeyName" : { "Ref" : "KeyName" },
      "InstanceType" : "t3.medium",
      "SecurityGroups" : [{ "Ref" : "Ec2SecurityGroup" }],
      "BlockDeviceMappings" : [
        {
          "DeviceName" : "/dev/sda1",
          "Ebs" : { "VolumeSize" : "50" }
        },{
          "DeviceName" : "/dev/sdm",
          "Ebs" : { "VolumeSize" : "100" }
        }
      ]
    }
}
```

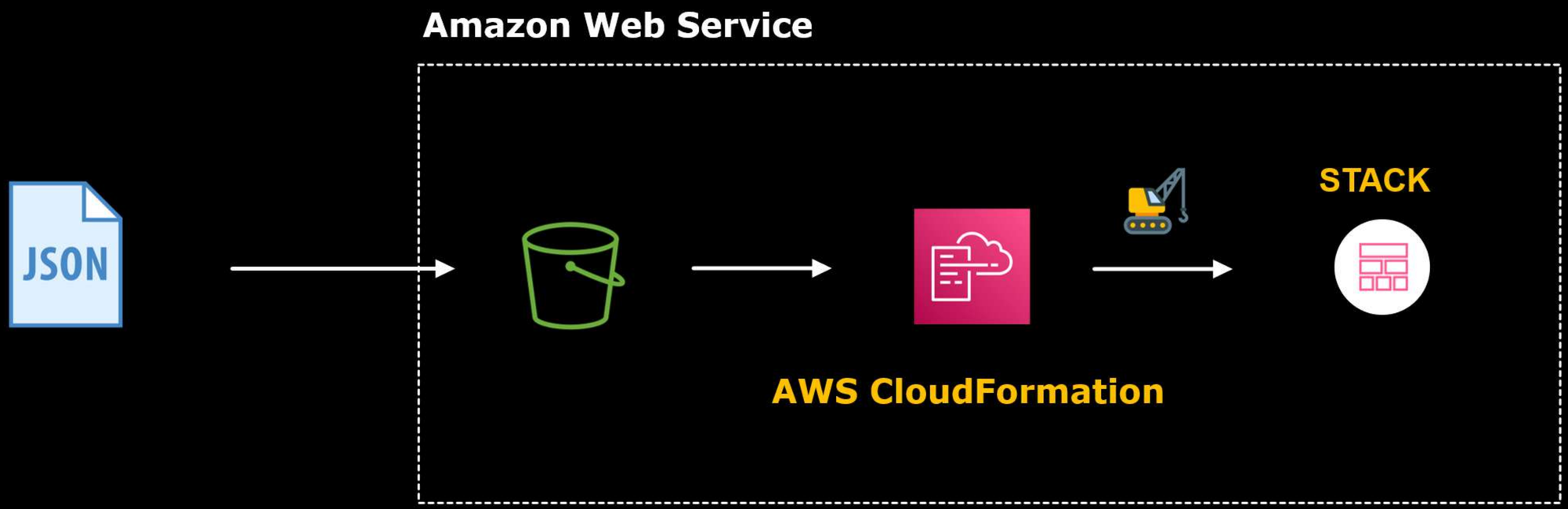
YAML

```
EC2Instance:
    Type: AWS::EC2::Instance
    Properties:
        ImageId: ami-26190097123
        KeyName: !Ref KeyName
        InstanceType: t3.medium
        SecurityGroups:
        - !Ref Ec2SecurityGroup
        BlockDeviceMappings:
        -
          DeviceName: /dev/sda1
          Ebs:
            VolumeSize: 50
        -
          DeviceName: /dev/sdm
          Ebs:
            VolumeSize: 100
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

```yaml
EC2Instance:
    Type: AWS::EC2::Instance
    Properties:
        ImageId: ami-26190097123
        KeyName: !Ref KeyName
        InstanceType: t3.medium
        SecurityGroups:
        - !Ref Ec2SecurityGroup
        BlockDeviceMappings:
        -
          DeviceName: /dev/sda1
          Ebs:
            VolumeSize: 50
        -
          DeviceName: /dev/sdm
          Ebs:
            VolumeSize: 100
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation

What is a Stack?

- when you use CloudFormation, you manage related resources as a single unit called a stack.
- all the resources provisioned in a stack are defined by the stack's CloudFormation template.
- you can create a stack by submitting a template to AWS CloudFormation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation

How do you update a stack?

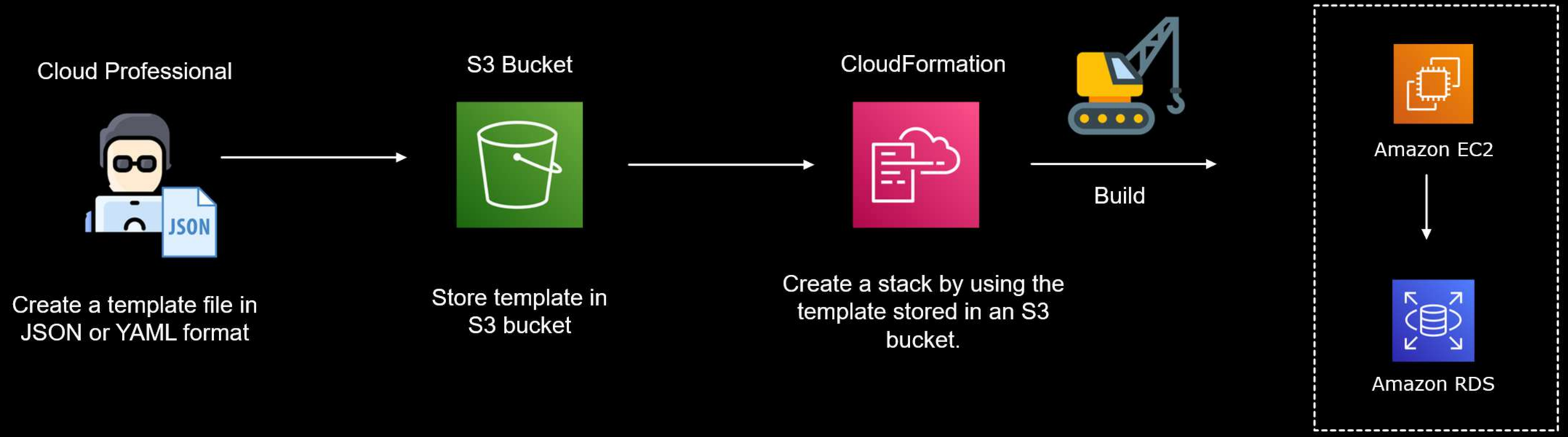
- before making changes to your resources, you should generate a change set.
- a change set is like a summary of your proposed changes.
- change sets allow you to see how your changes might impact the resources in your current stack

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Anatomy of a CloudFormation Template

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation

At the end of this video, you will be able to:

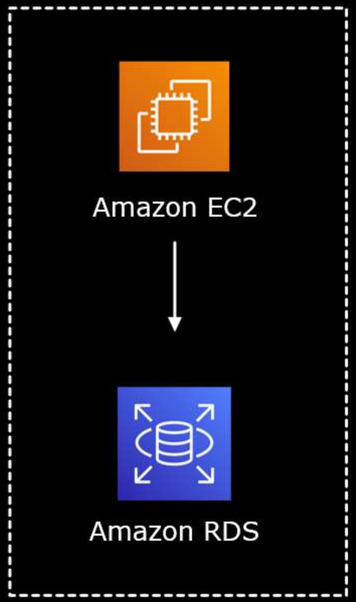
- understand basic template sections like resources, versions, description, and metadata
- explain the differences between Parameters, Mappings, and Outputs
- and ultimately, be comfortable reading CloudFormation templates

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Use JSON/YAML format files to create templates

Templates describes the resources that you want to provision



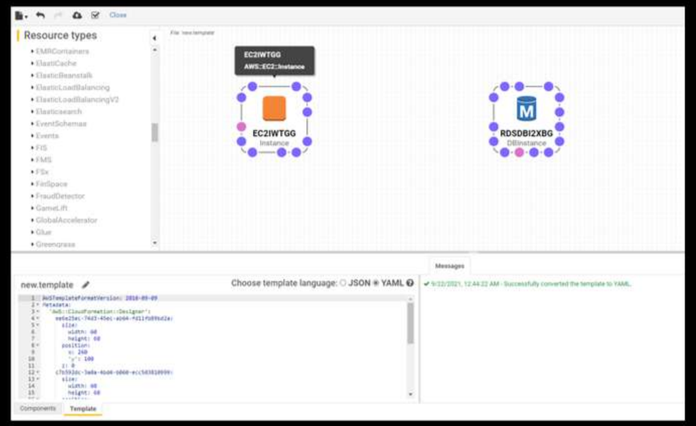
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

TEMPLATE





Use JSON/YAML format files to create templates



CloudFormation Designer

Templates describes the resources that you want to provision

CREATE

UPDATE

DELETE

STACK



Amazon EC2



Amazon RDS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

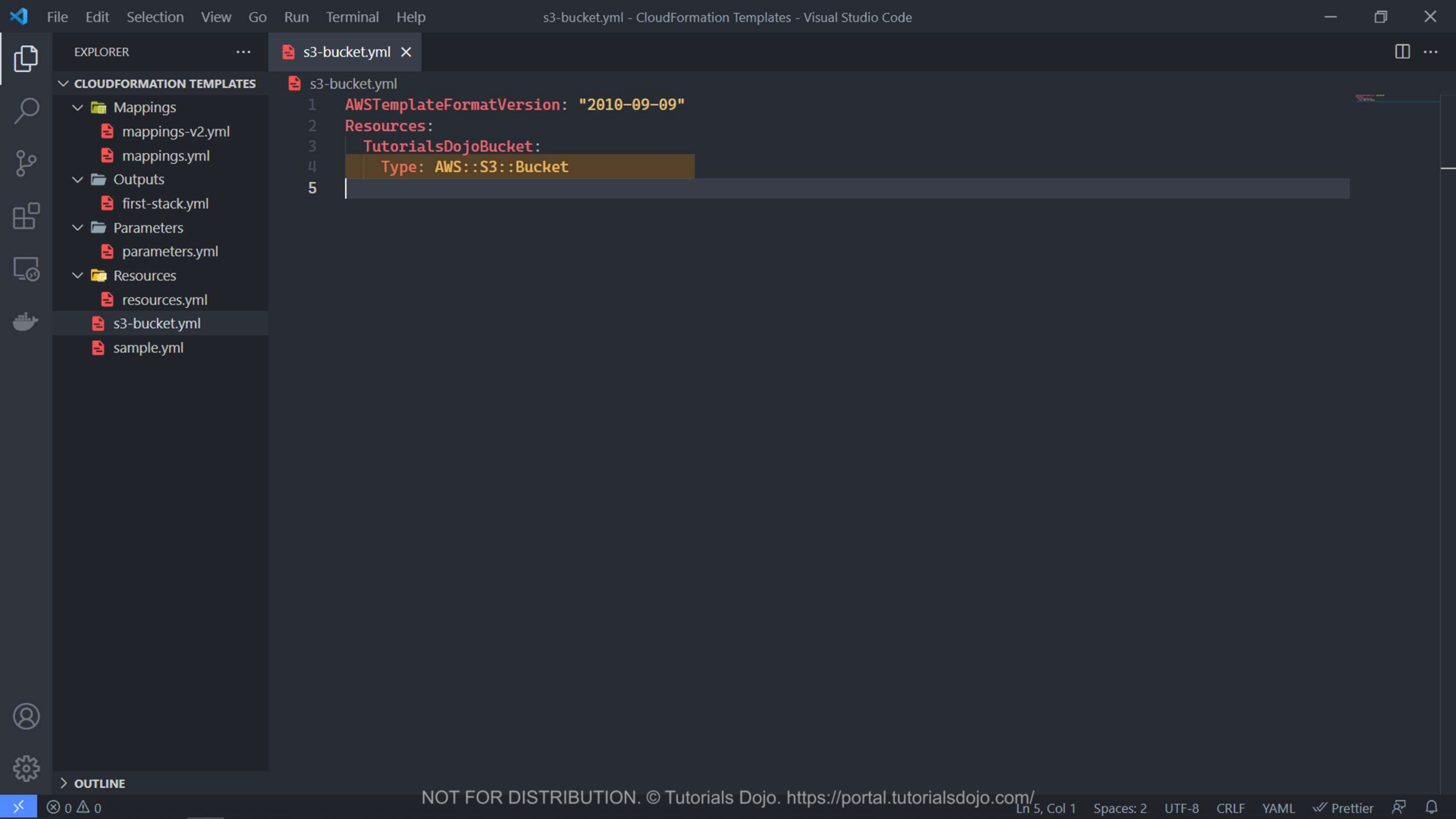


AWS CloudFormation

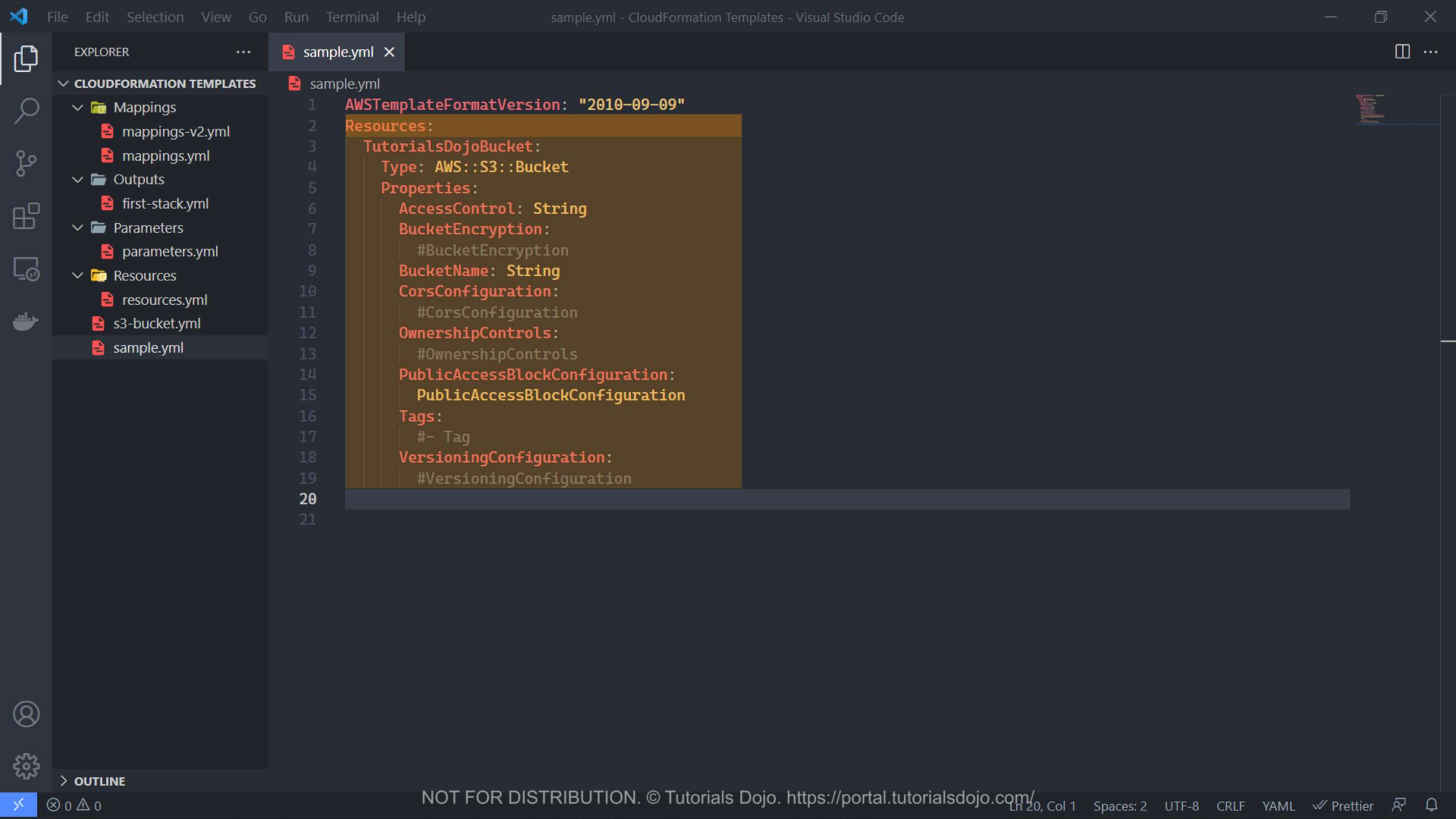
Template sections in CloudFormation:

- Resources
- Version
- Description
- Metadata
- Parameters
- Rules
- Mappings
- Conditions
- Outputs

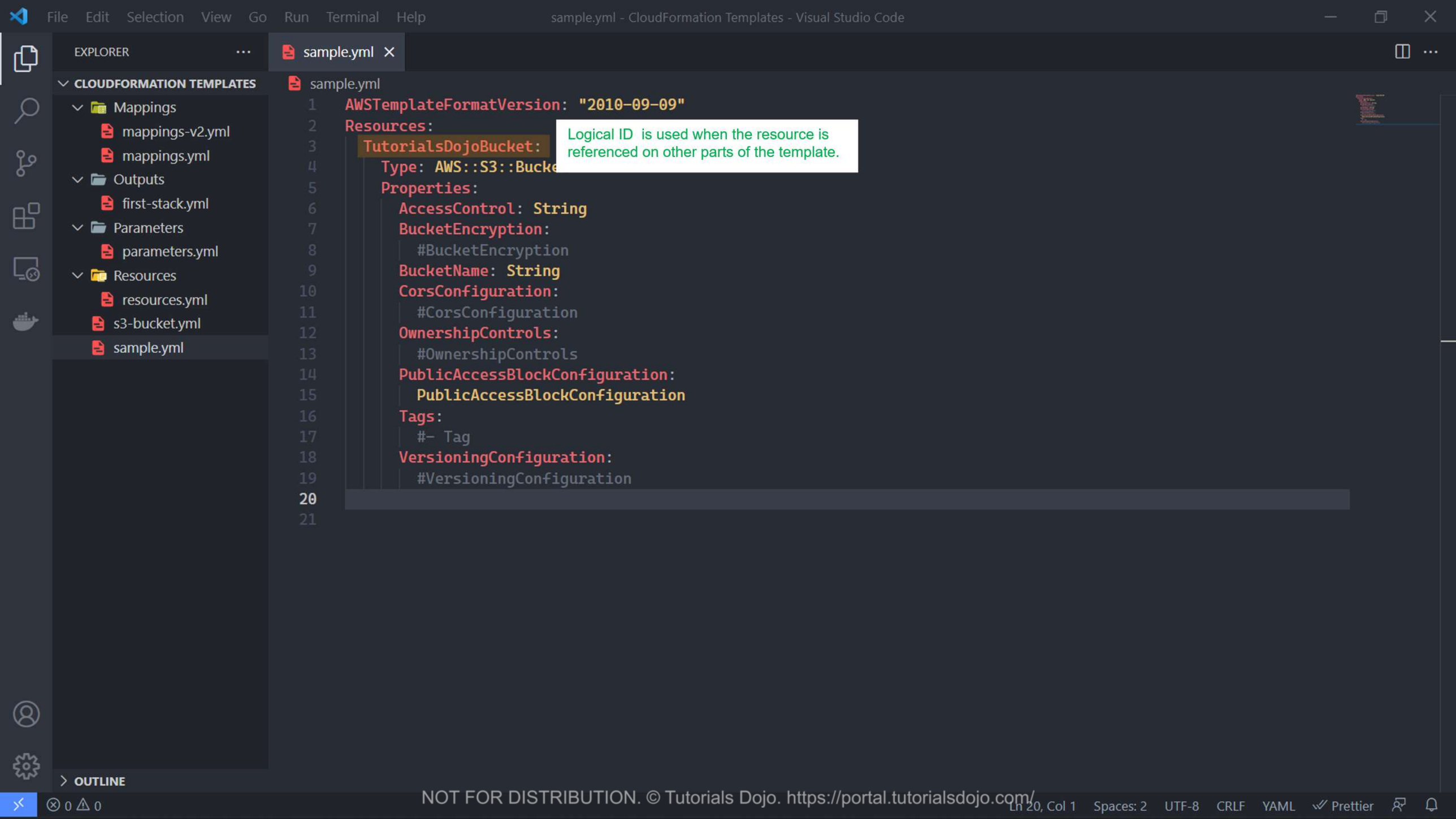
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



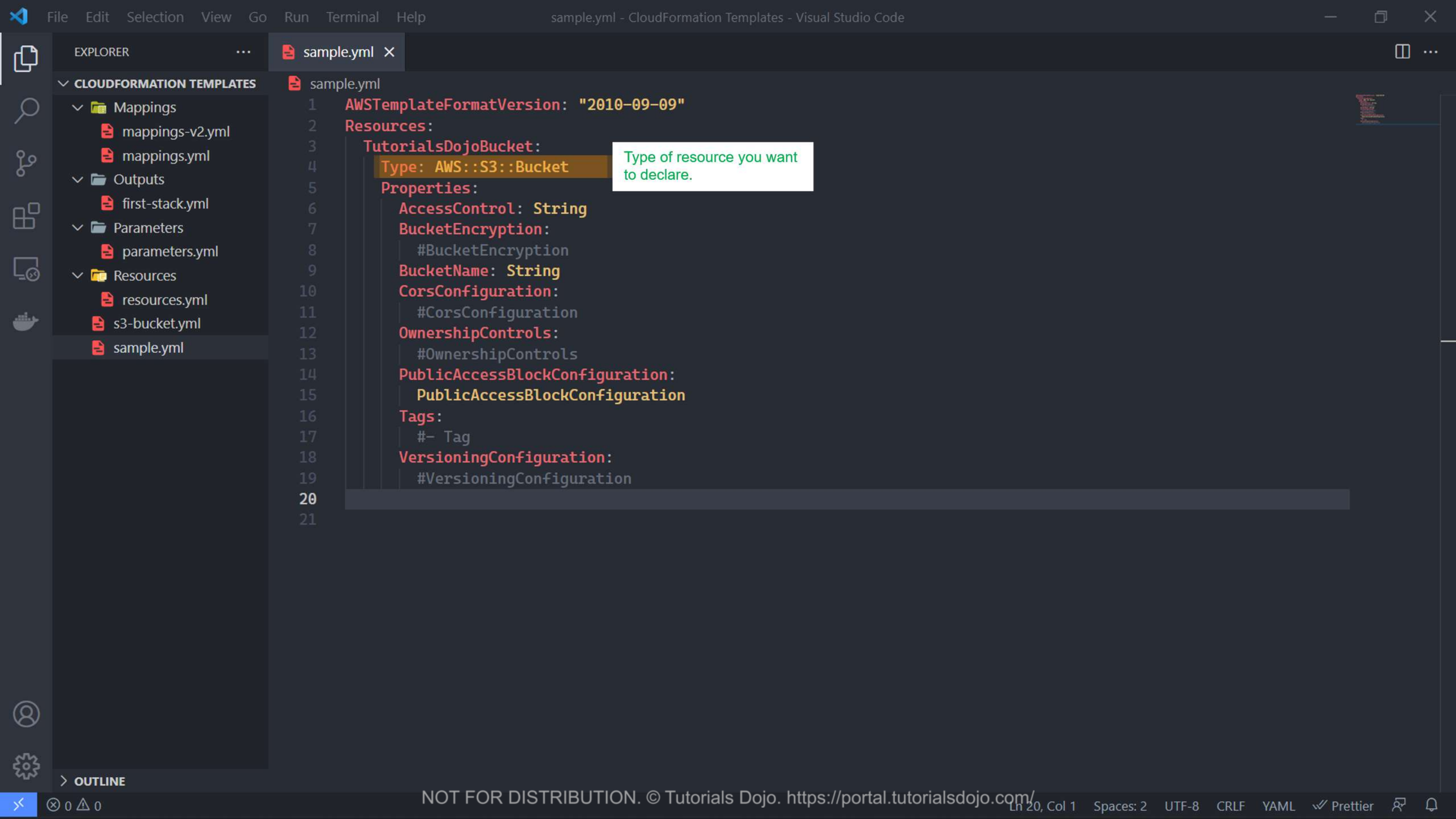
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



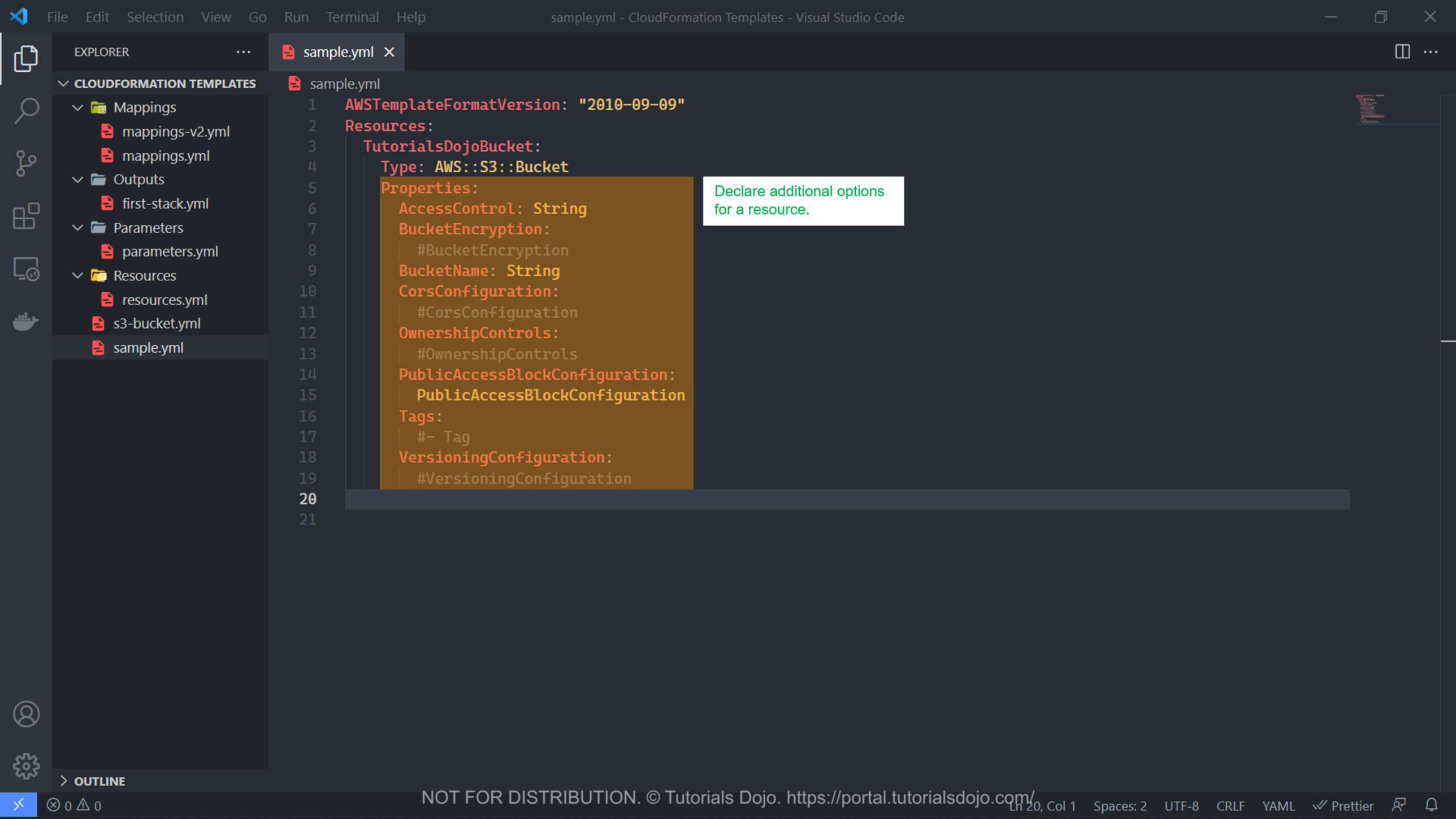
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



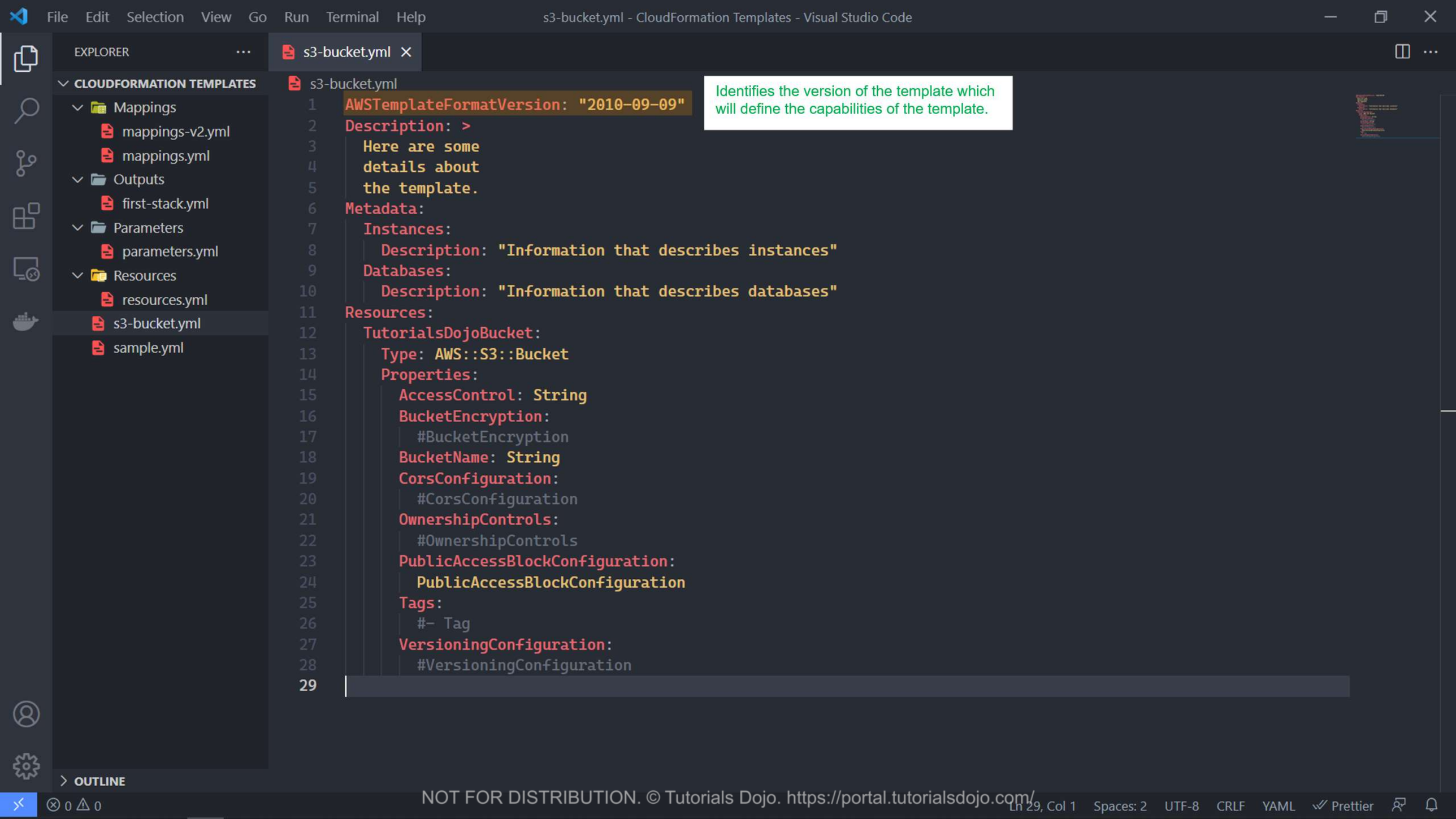
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



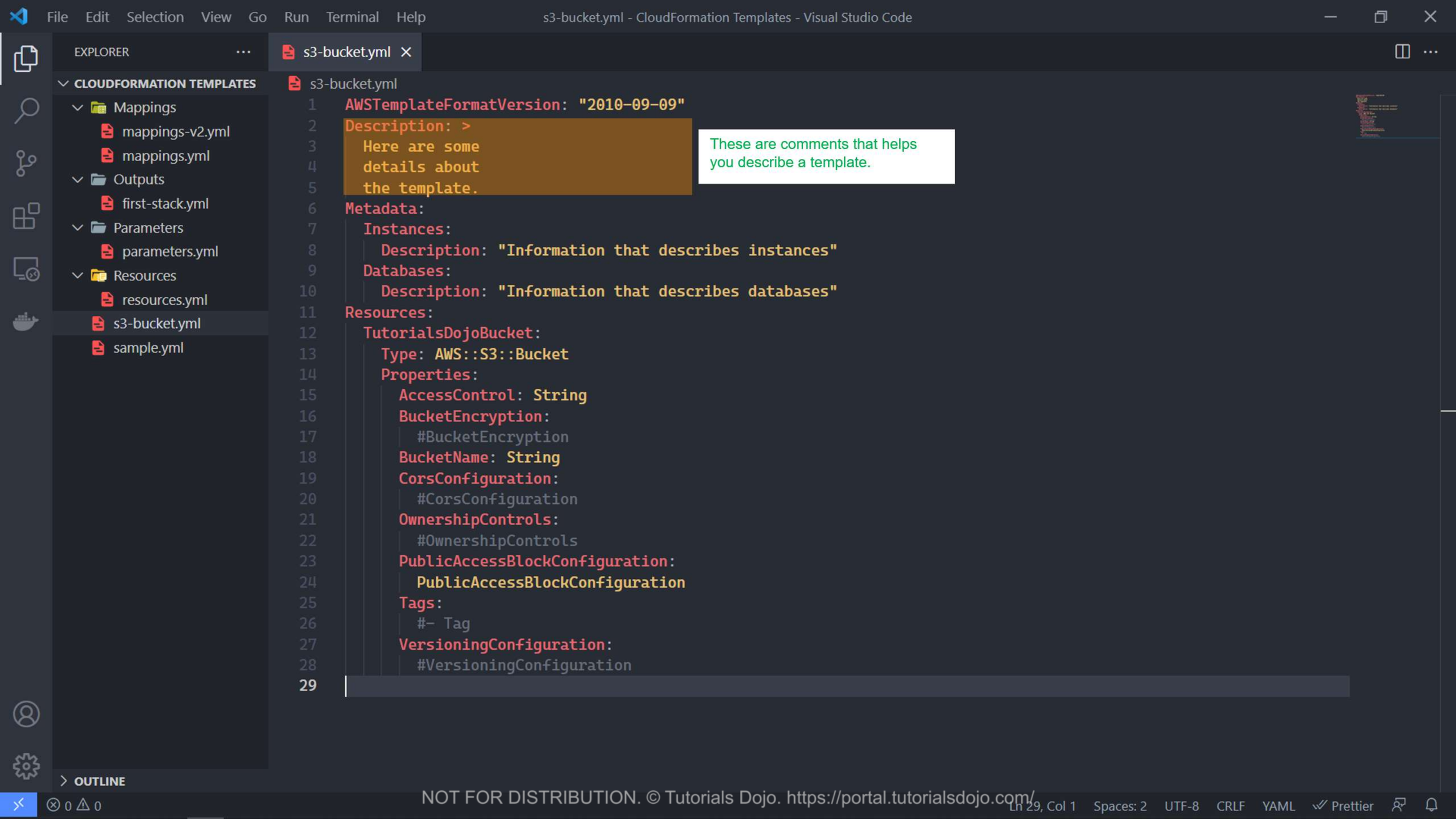
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



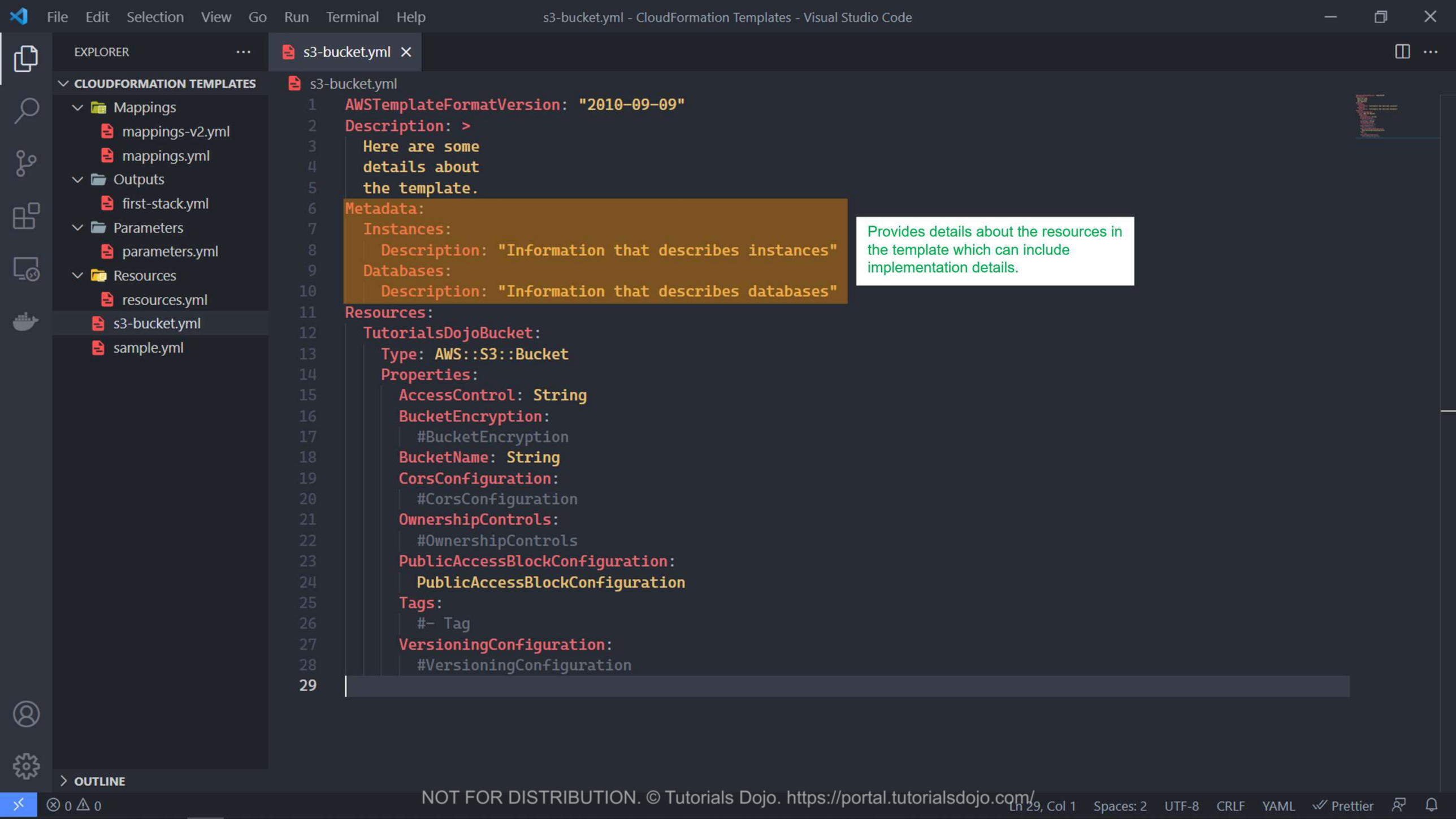
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Parameters

Mappings

Outputs

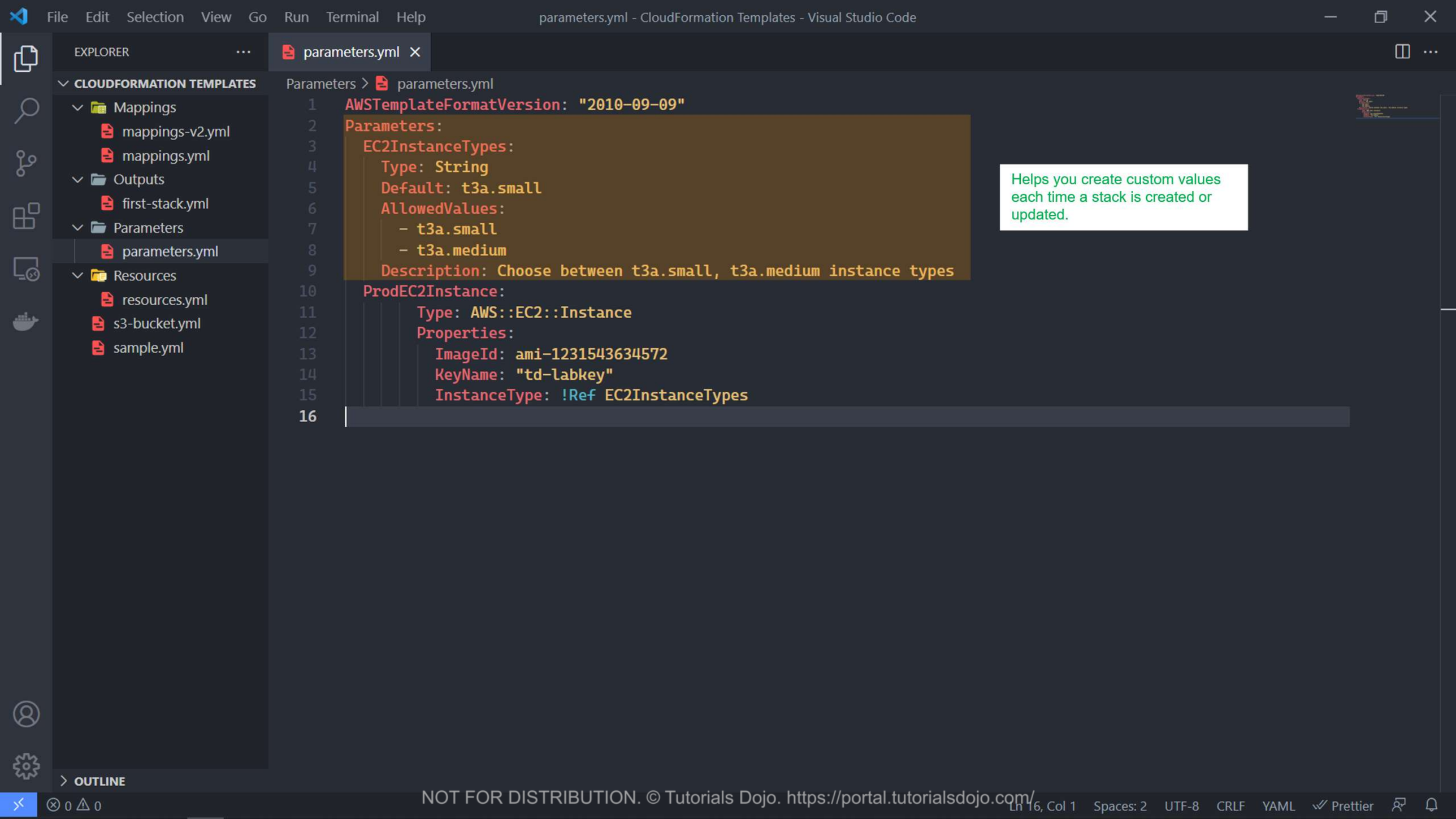
All of these allows you to store reusable values in CloudFormation.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

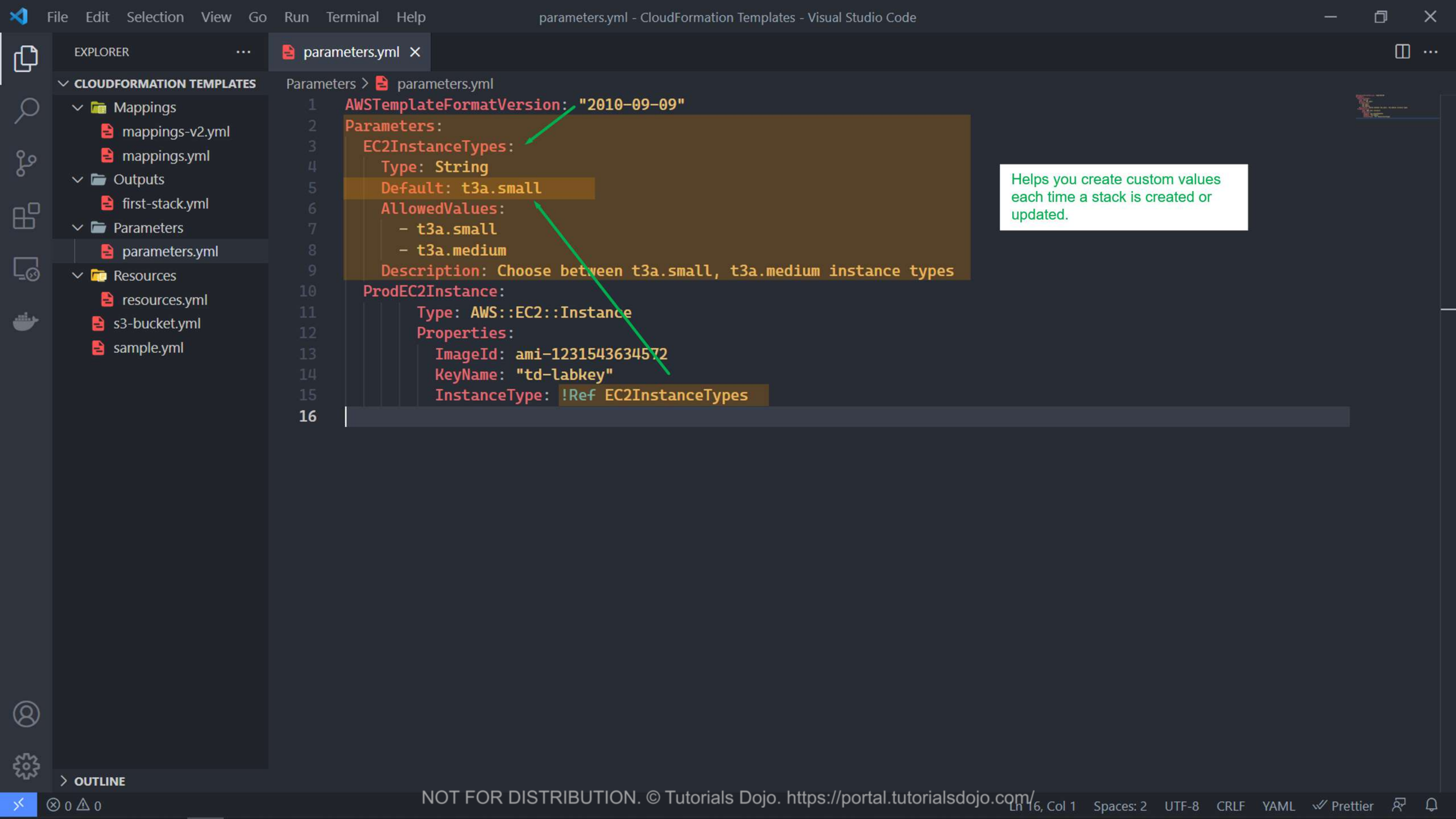
Parameters	Mappings	Outputs
Mainly for associating values to a parameter	Mainly used if you want to use a single key to a corresponding set of values	Exports values with a unique export name
Enables you to input custom values and call it using a Logical ID	Matches a key to a corresponding set of named values	Values can be exported to other stacks using the export field to perform cross-stack references
Uses Ref intrinsic function to reference a parameter	Use the Fn::FindInMap intrinsic function to retrieve values in a map	Uses the intrinsic function Fn::ImportValue to import values

Should **NOT** be used to store secrets and passwords.

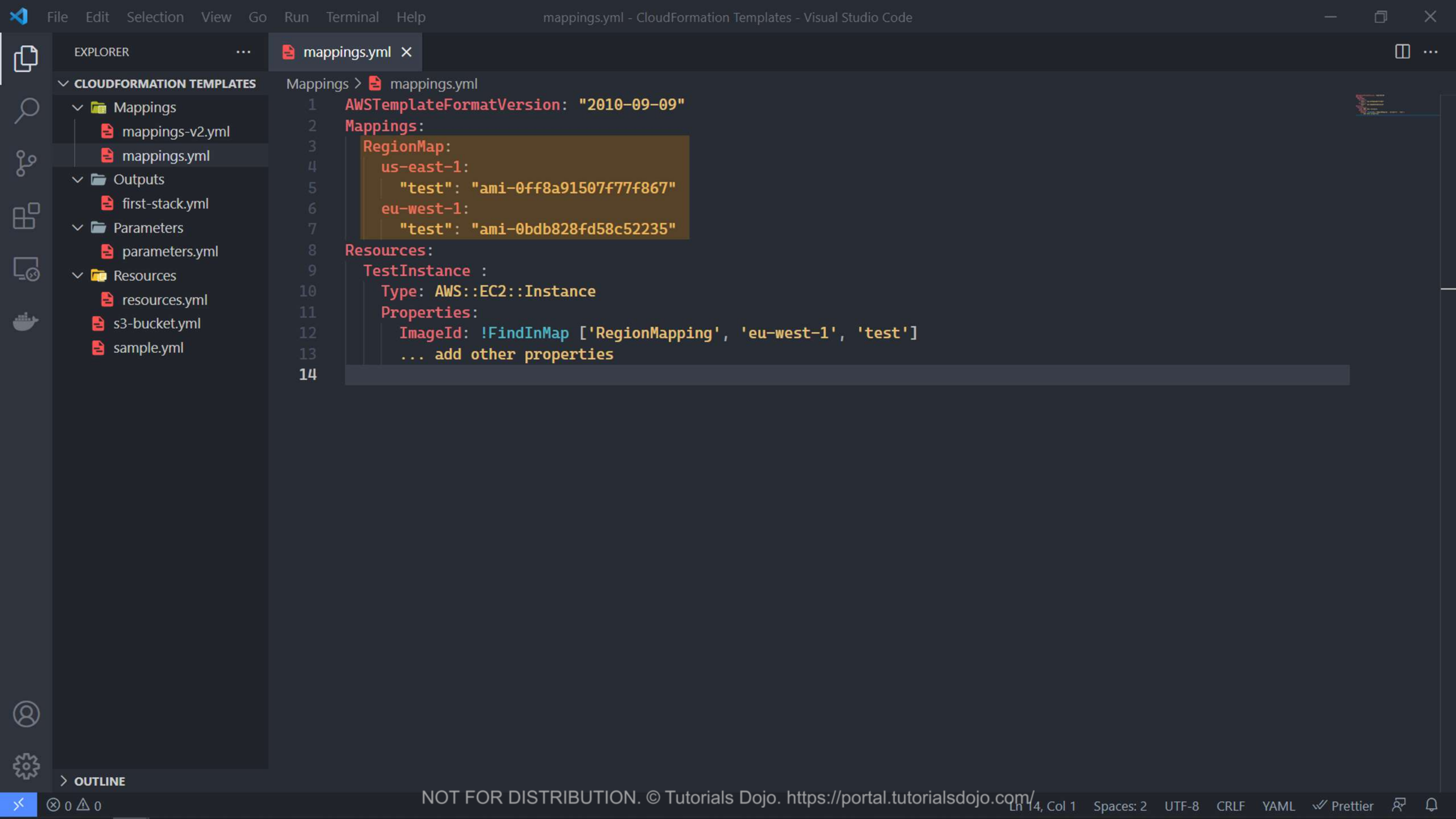
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



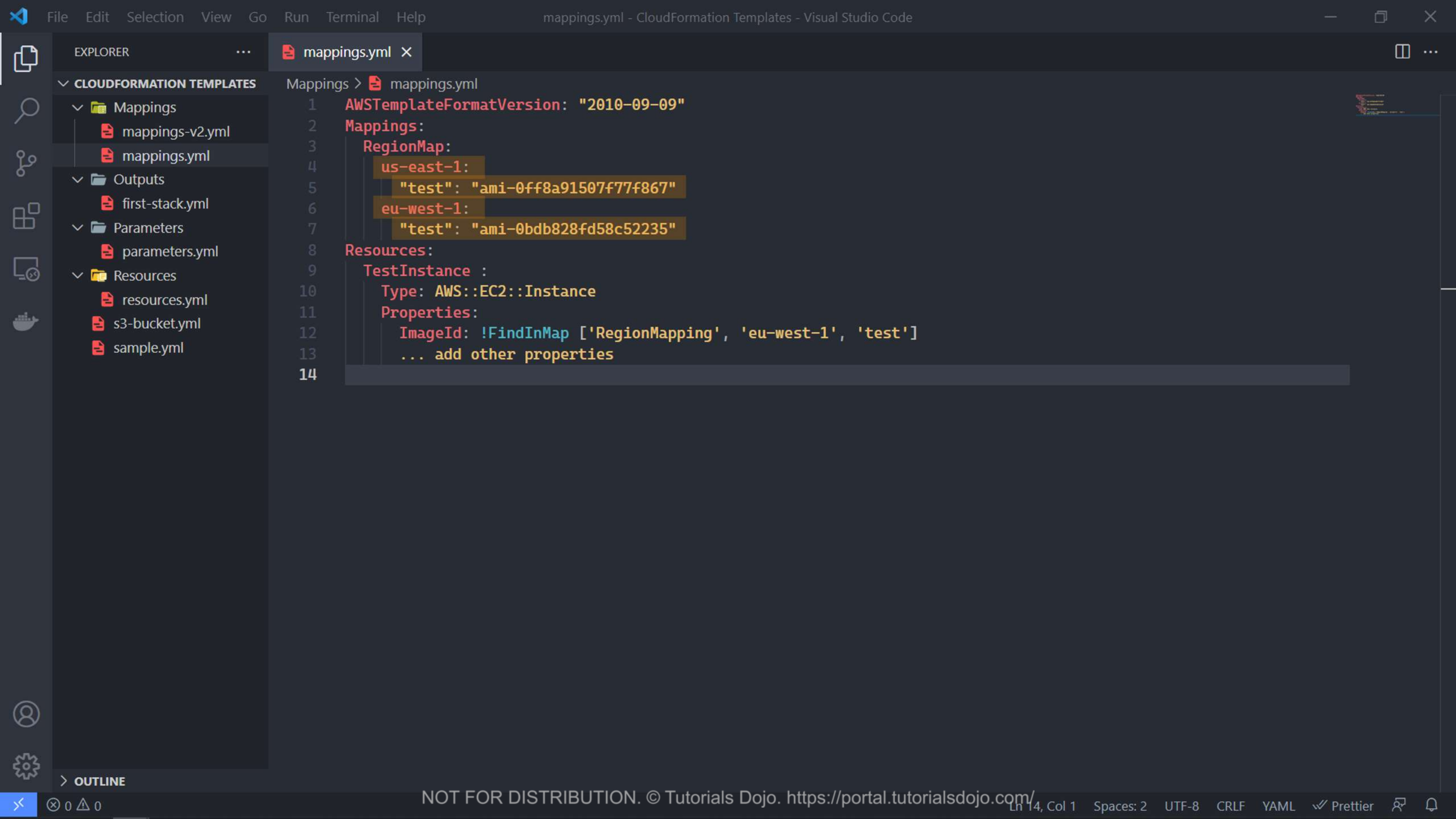
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



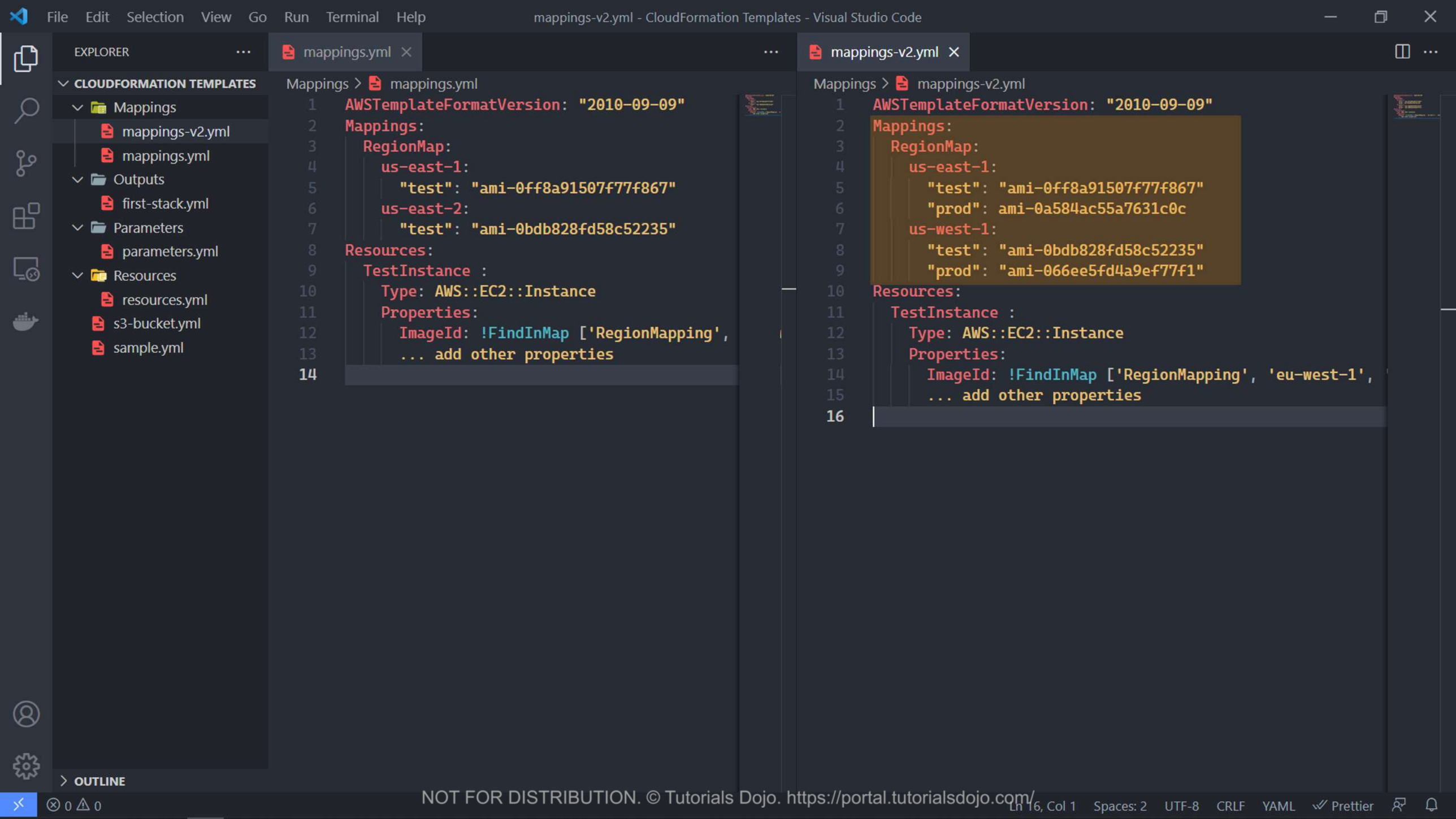
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



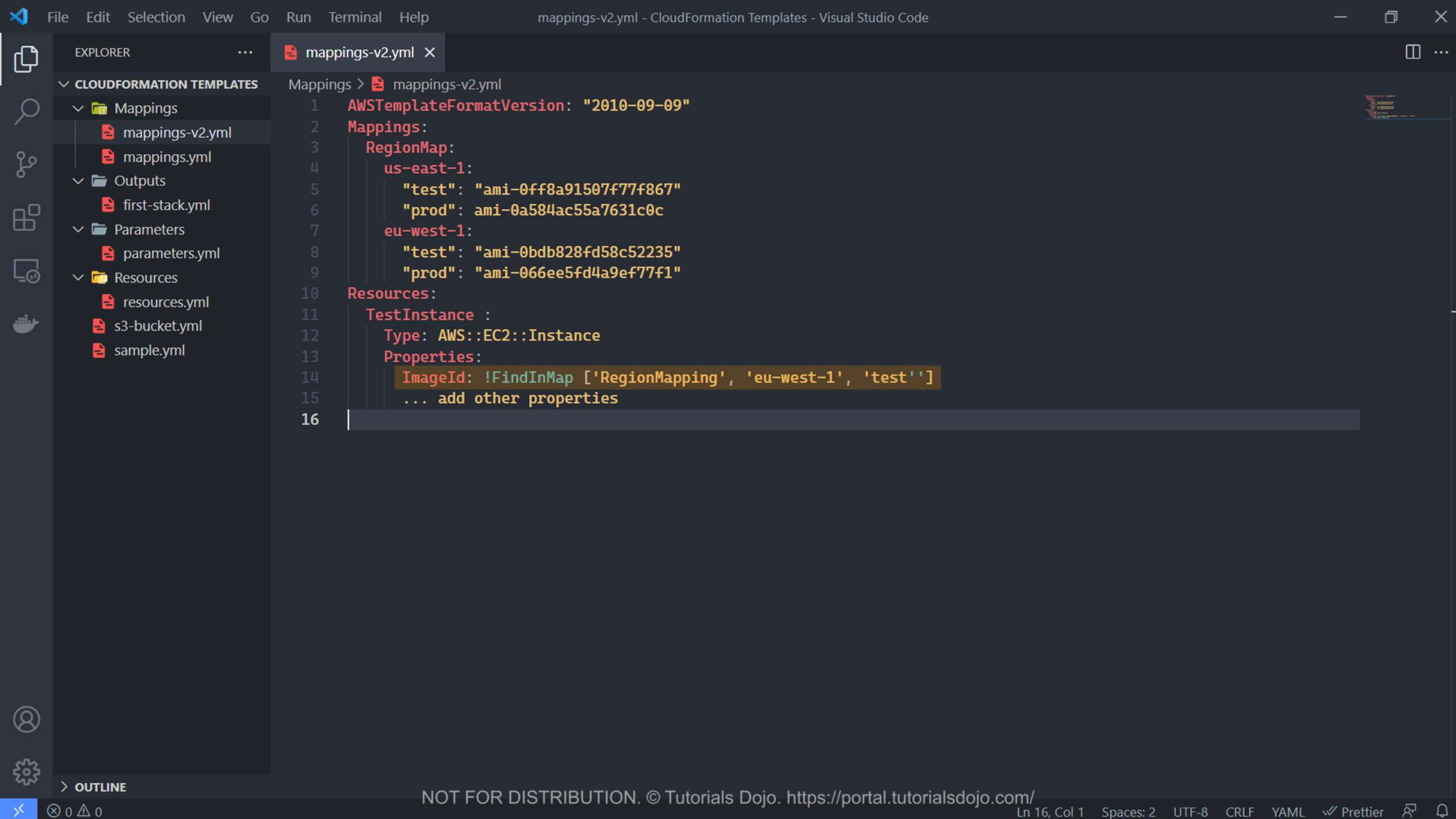
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



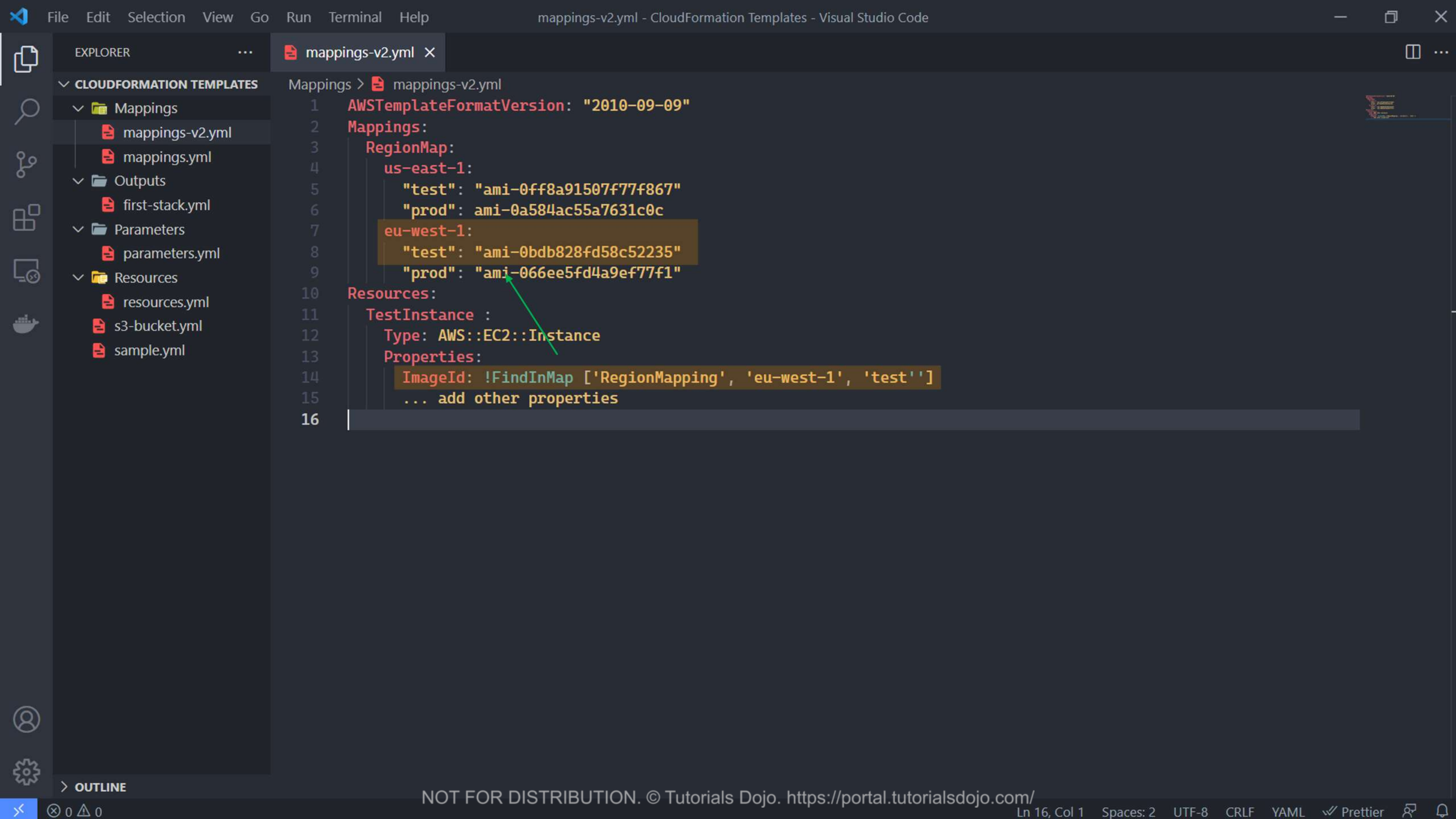
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



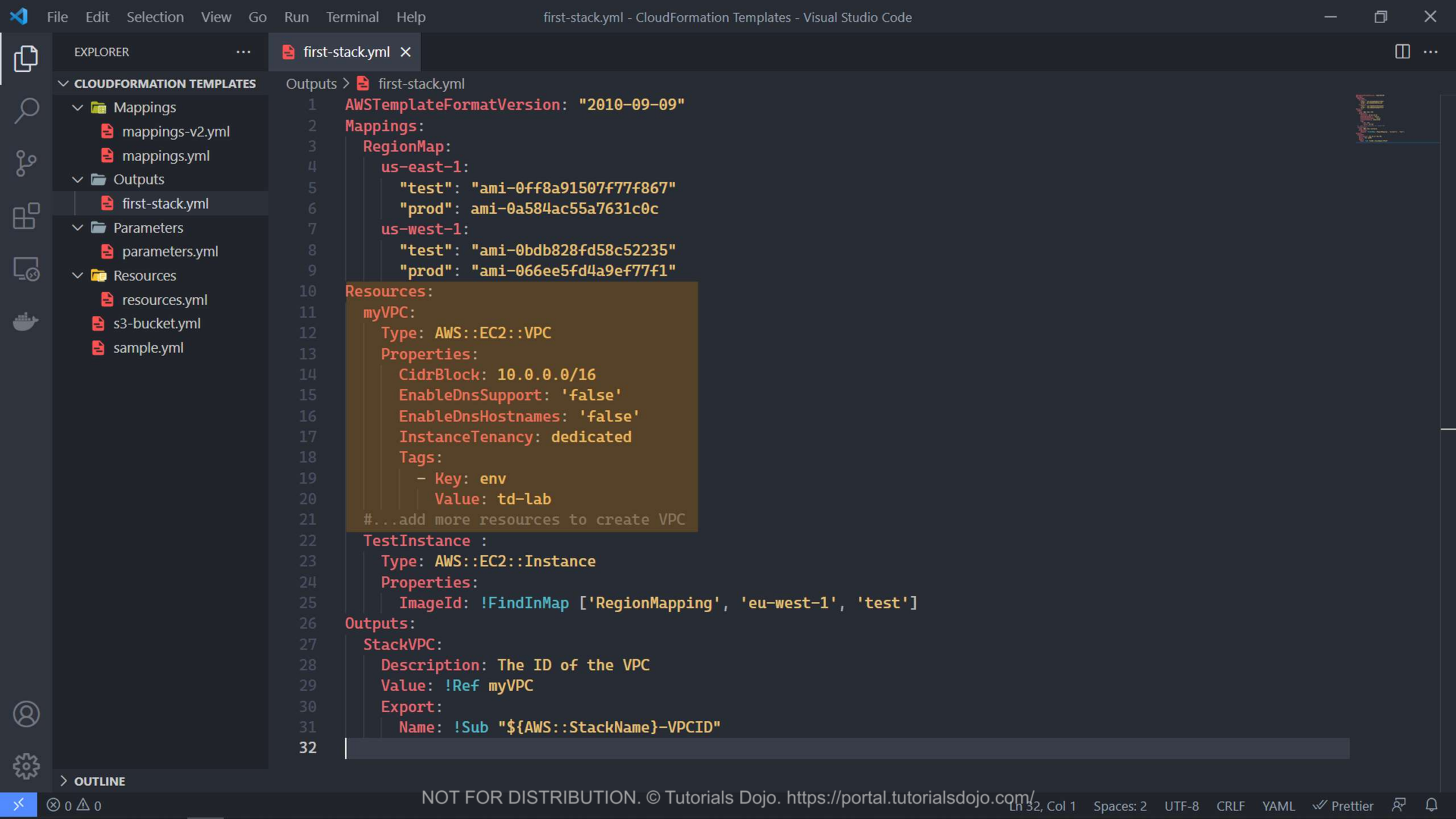
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



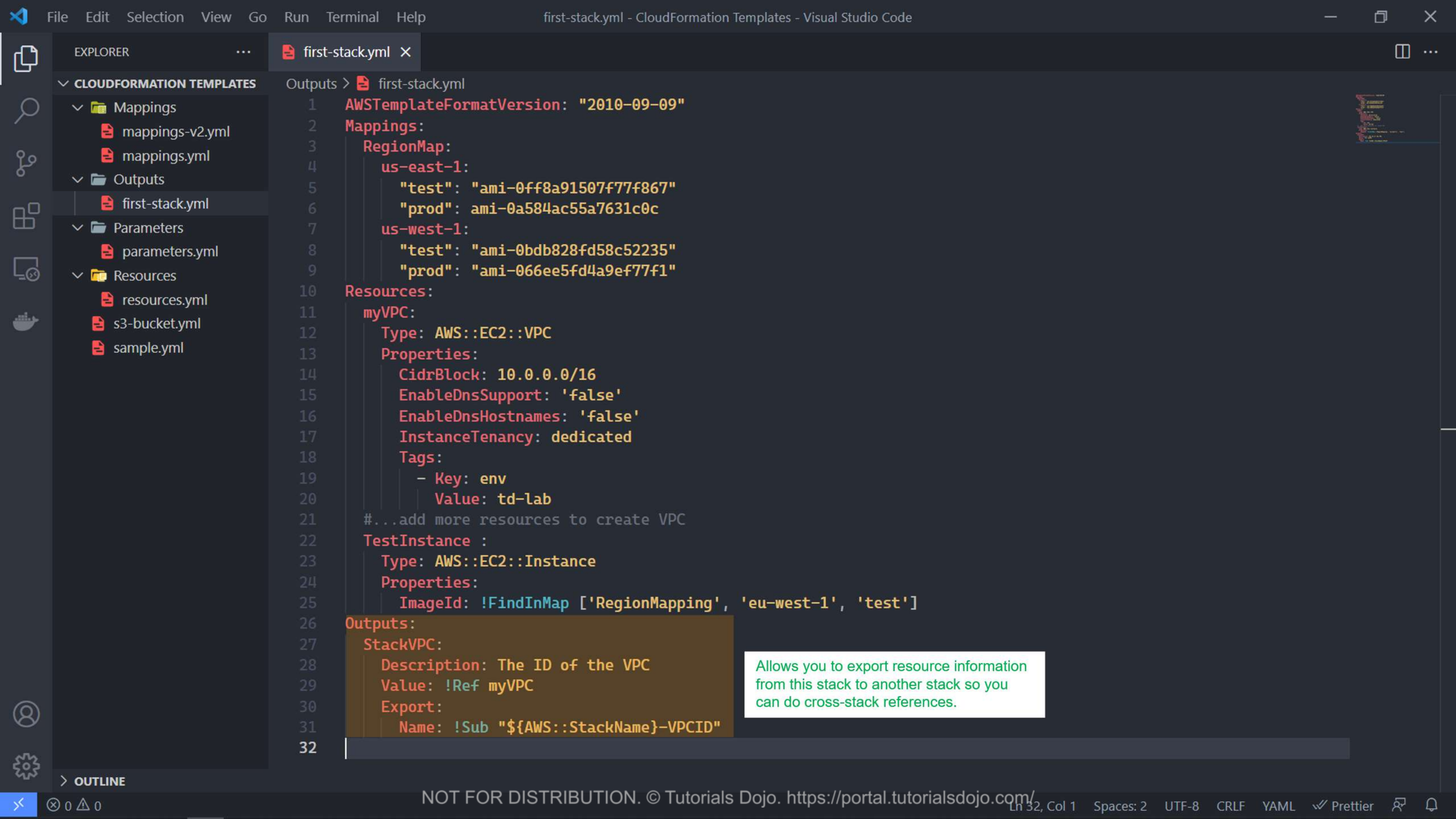
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



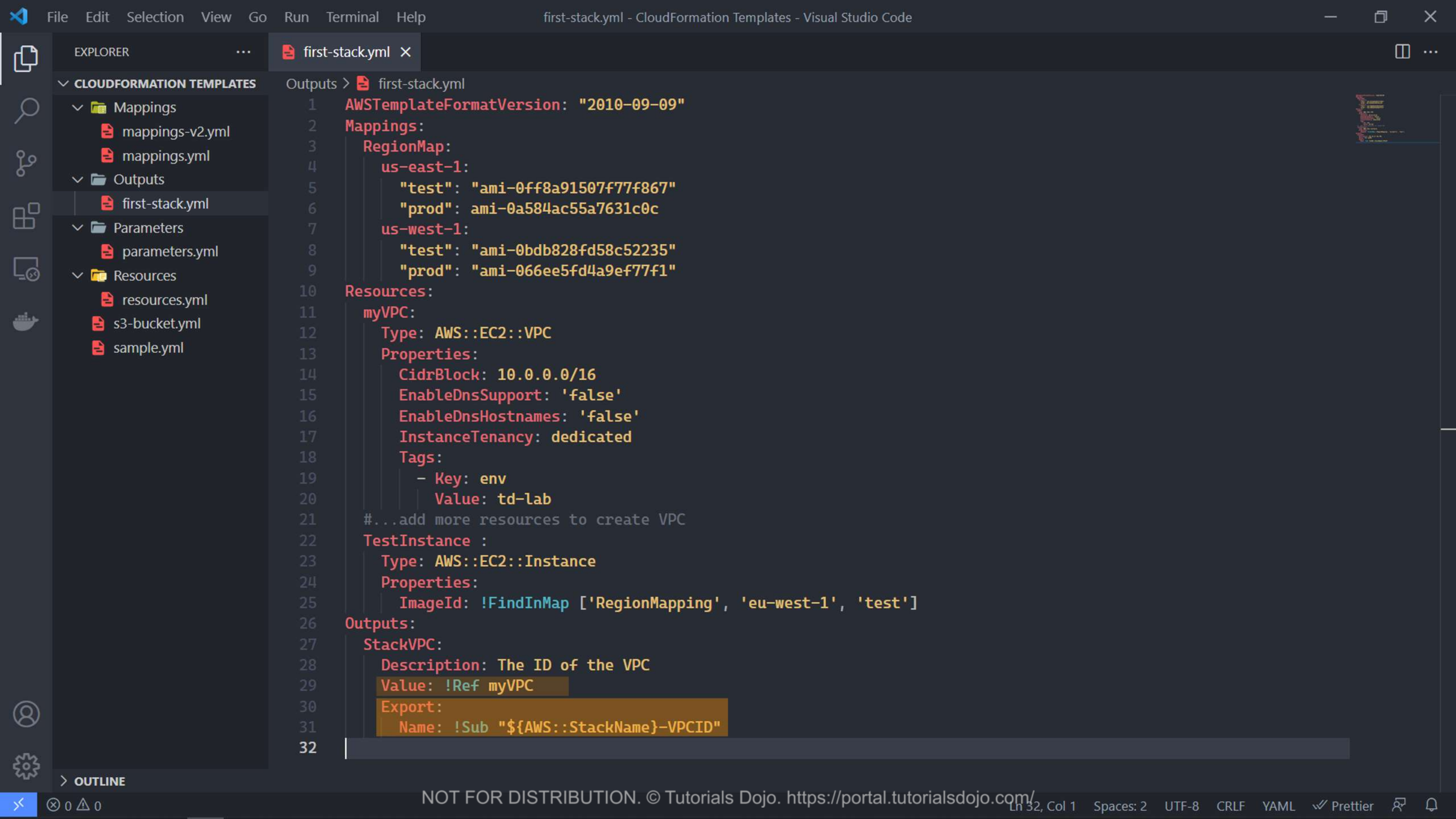
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



CloudFormation Helper Scripts

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



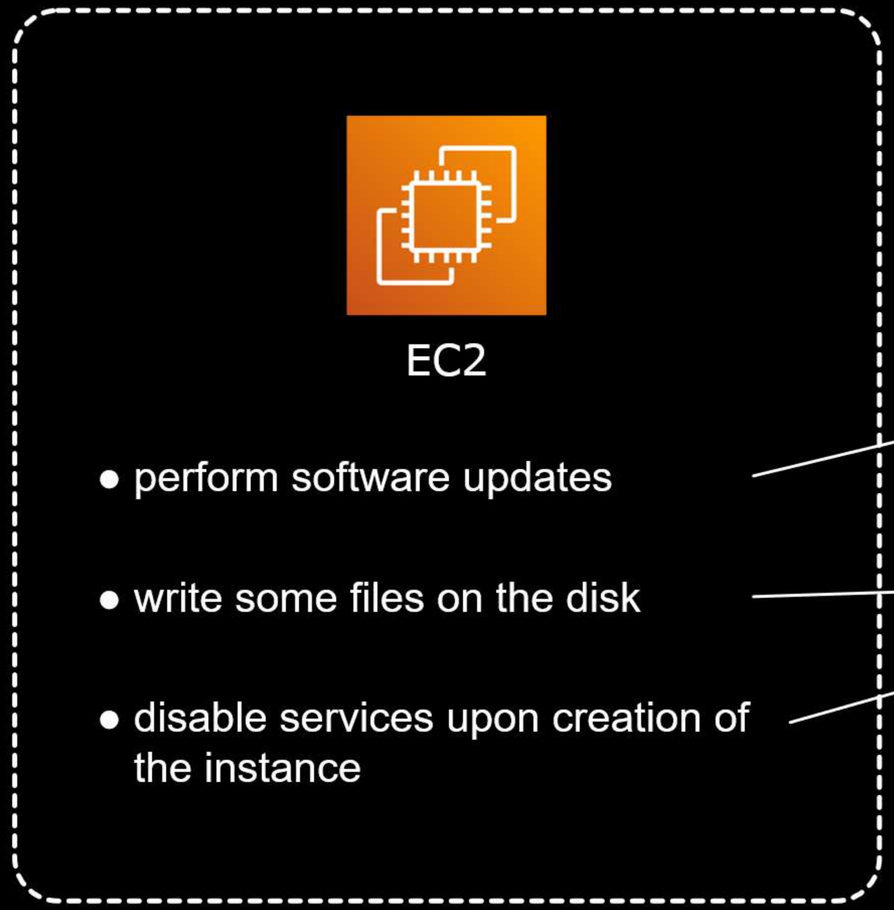
AWS CloudFormation

At the end of the video, you will be able to:

- Learn how to configure UserData property on an EC2 instance in AWS CloudFormation
- Understand how to create the metadata section for your EC2 instances
- Use cfn-signal and cfn-init helper scripts.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

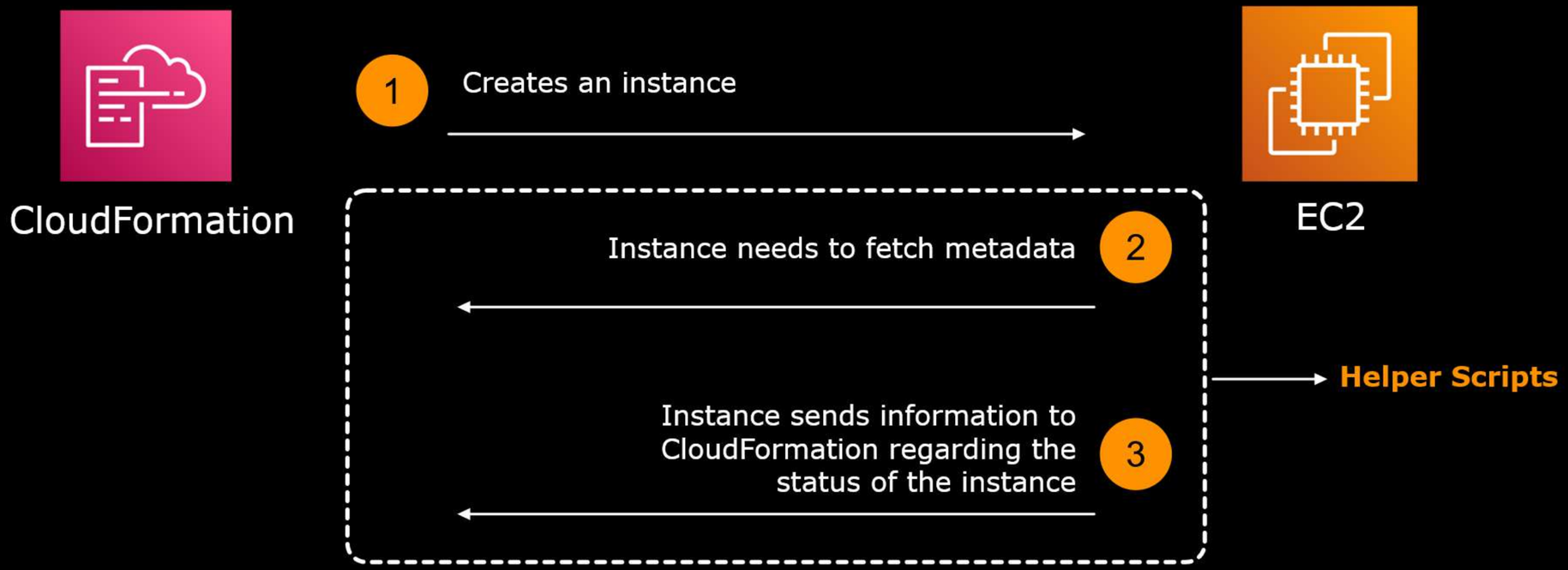
Scenario: You need to create an instance and upon instance creation, you need to:



User Data

```
#!/bin/bash
yum update -y
apt-get update && apt-get upgrade
apt-get install software-properties-common
add-apt-repository ppa:ondrej/php
apt-get update
apt-get install php8.0
sudo apt install php8.0-fpm
cd /etc/php/7.4/fpm/pool.d
sudo sed -i "/^pm.max_children/c\pm.max_children = 20" www.conf
sudo apt purge '^php7.4.*'
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation

CloudFormation Helper Scripts

- allow you to install software and start services on an Amazon EC2 instance
- are readily available on Amazon Linux AMIs
- can be installed using the aws-cfn-bootstrap package if not available on the instance

cfn-init

cfn-signal

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



cfn-init

- helps you read template metadata from the AWS::CloudFormation::Init key and then perform some actions according to that metadata.

```
NewInstance:
    Type: AWS::EC2::Instance
    Metadata:
      AWS::CloudFormation::Init:
        configSets:
          InstallAndConfigure :
            - Install
            - Configure
        Install:
          packages:
            ...Packages to install
          files:
            ...Files to create
        Configure
          commands
            ...Commands to perform
    Properties:
```

These values mean nothing unless they are invoked in via cfn-init in the UserData.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



cfn-signal

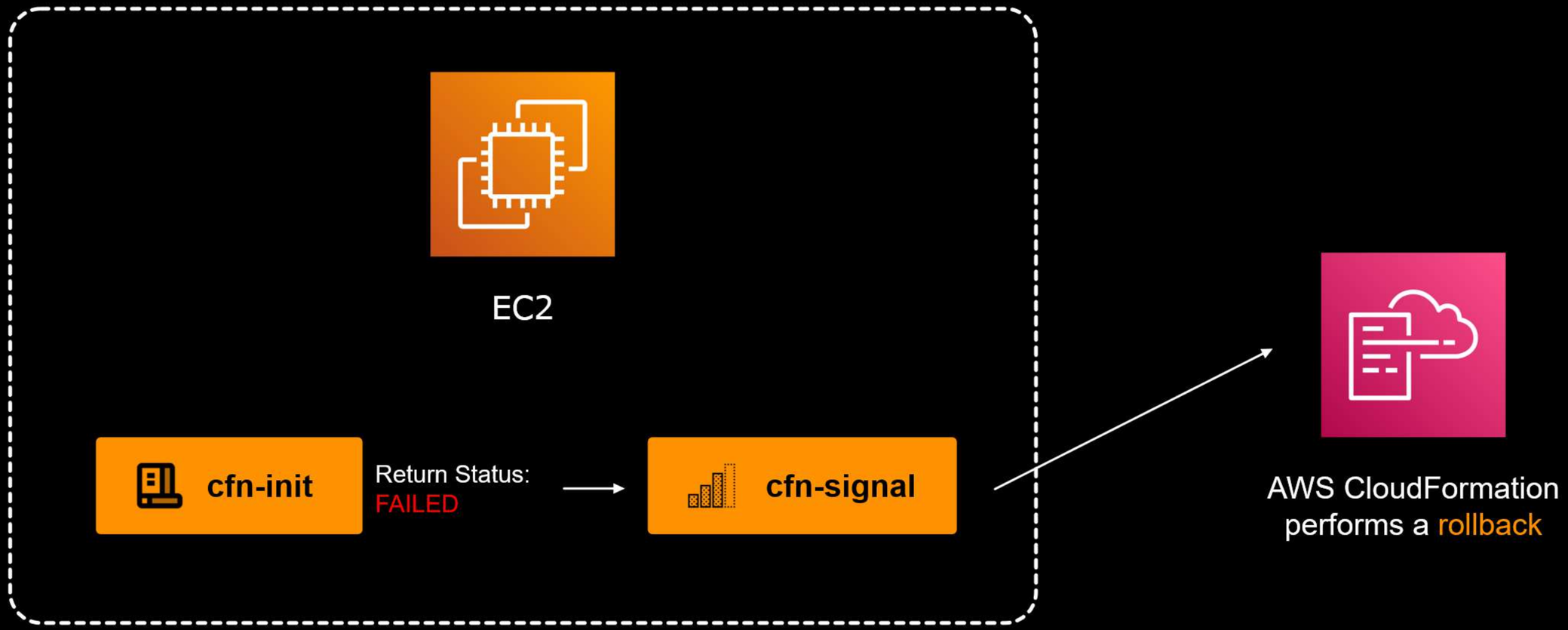
- signals CloudFormation to indicate whether an Amazon EC2 instance has been successfully created or updated.
- signals AWS CloudFormation that software applications are ready and installed

```
UserData: !Base64
  'Fn::Join':
    - ''
    - - |
        #!/bin/bash -xe
      - |
        # Install the files and packages from the metadata
      - yum install -y aws-cfn-bootstrap\n
      - '/opt/aws/bin/cfn-init -v '
      - '         --stack '
      - !Ref 'AWS::StackName'
      - '         --resource NewInstance '
      - '         --configsets InstallAndConfigure '
      - '         --region '
      - !Ref 'AWS::Region'
      - |+
```

signal CloudFormation after all the commands and configurations we performed with cfn-init.

```
        # Signal the status from cfn-init
      - '/opt/aws/bin/cfn-signal -e $? '
      - '         --stack '
      - !Ref 'AWS::StackName'
      - '         --resource NewInstance '
      - '         --region '
      - !Ref 'AWS::Region'
      - |+
```

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DependsOn and WaitConditions

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation

At the end of the lecture, you will be able to:

- Understand how DependsOn and WaitConditions help you manage the order of creating resources in a stack

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



DependsOn

- is a resource attribute that helps you specify that a resource shall only be created upon the successful launch of another resource.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

When to use DependsOn?

- when you want to avoid parallelism when creating, updating, and deleting instances.

```
DBInstance:
    Type: AWS::RDS::DBInstance
    ... RDS Properties here
ProdInstance:
    Type: AWS::EC2::Instance
    ... EC2 Properties
S3ImageBucket:
    Type: AWS::S3::Buc
    ... S3 Bucket Properties here
PublicVPC:
    Type: AWS::EC2::VPC
    ... VPC Properties here
```



AWS CloudFormation

CREATE_IN_PROGRESS

Oh wait, we can create the EC2 Instance too!

CREATE_IN_PROGRESS

Wait, no! The **RDS has to be launched completely first** before the instance is created.

Perfect! Use DependsOn to wait for the RDS to be completed.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

When to use DependsOn?

- when you want to avoid parallelism when creating, updating, and deleting instances.
- is when you want to explicitly declare dependencies among resources so you can control the order of instructions to create them.

RDS should exist first before the EC2 instance is created.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



WaitCondition

- Allows you to pause the creation of a stack and wait for a signal before CloudFormation continues to create the stack.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation

CREATE_IN_PROGRESS



EC2

Done launching the instance.
Should be COMPLETE status.

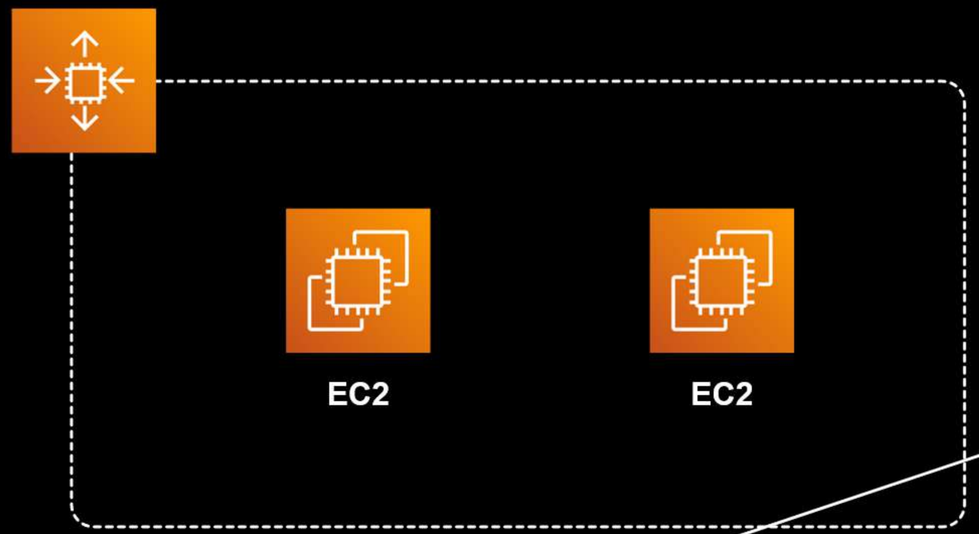
But we still need to download some applications and configure them accordingly.

Should not be in COMPLETE status yet.

```
MyInstance:
    Type: AWS::EC2::Instance
    Properties:
     ... EC2 Properties Here
WaitHandle:
  Type: AWS::CloudFormation::WaitConditionHandle
WaitCondition:
  Type: AWS::CloudFormation::WaitCondition
  DependsOn: MyInstance
  Properties:
    Handle: !Ref 'WaitHandle'
    Timeout: '300'
```

Will trigger only after the creation of MyInstance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/




```
EC2ScalingGroup:
  Type: AWS::AutoScaling::AutoScalingGroup
  Properties:
    MinSize: '1'
    MaxSize: '5'
    DesiredCapacity: 2
    LoadBalancerNames:
      - !Ref 'ElasticLoadBalancer'
WaitHandle:
  Type: AWS::CloudFormation::WaitConditionHandle
WaitCondition:
  Type: AWS::CloudFormation::WaitCondition
  DependsOn: EC2ScalingGroup
  Properties:
    Handle: !Ref 'WaitHandle'
    Timeout: '300'
    Count: 2
```

WaitCondition waits for the desired number of instances in the EC2ScalingGroup.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation StackSets

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

At the end of the video, you will be able to:

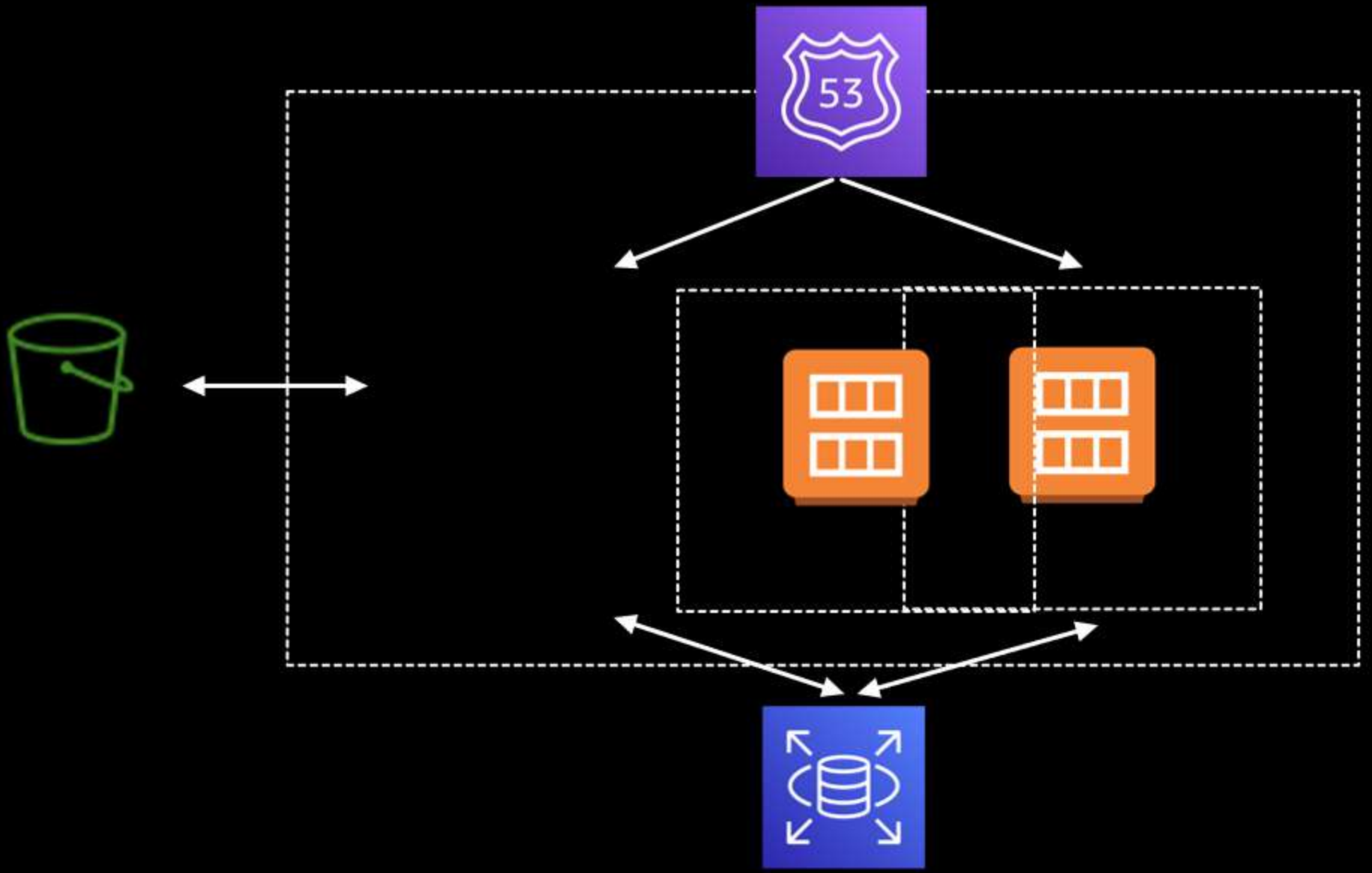
- Understand how StackSets help achieve consistency for your deployments across accounts and regions
- Understand the operations that you can perform with StackSets
- Learn which additional options you can use to control a StackSet deployment

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

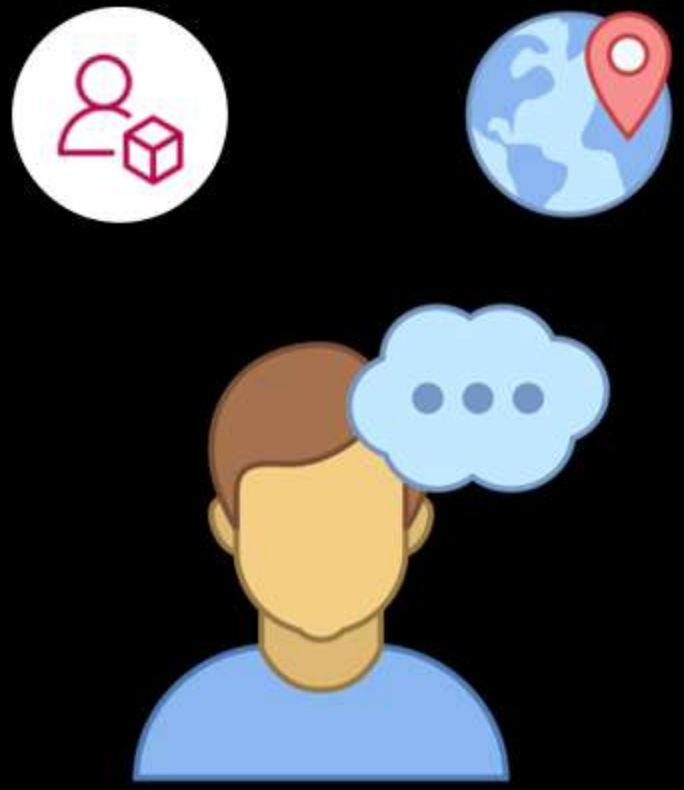
AWS CloudFormation



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



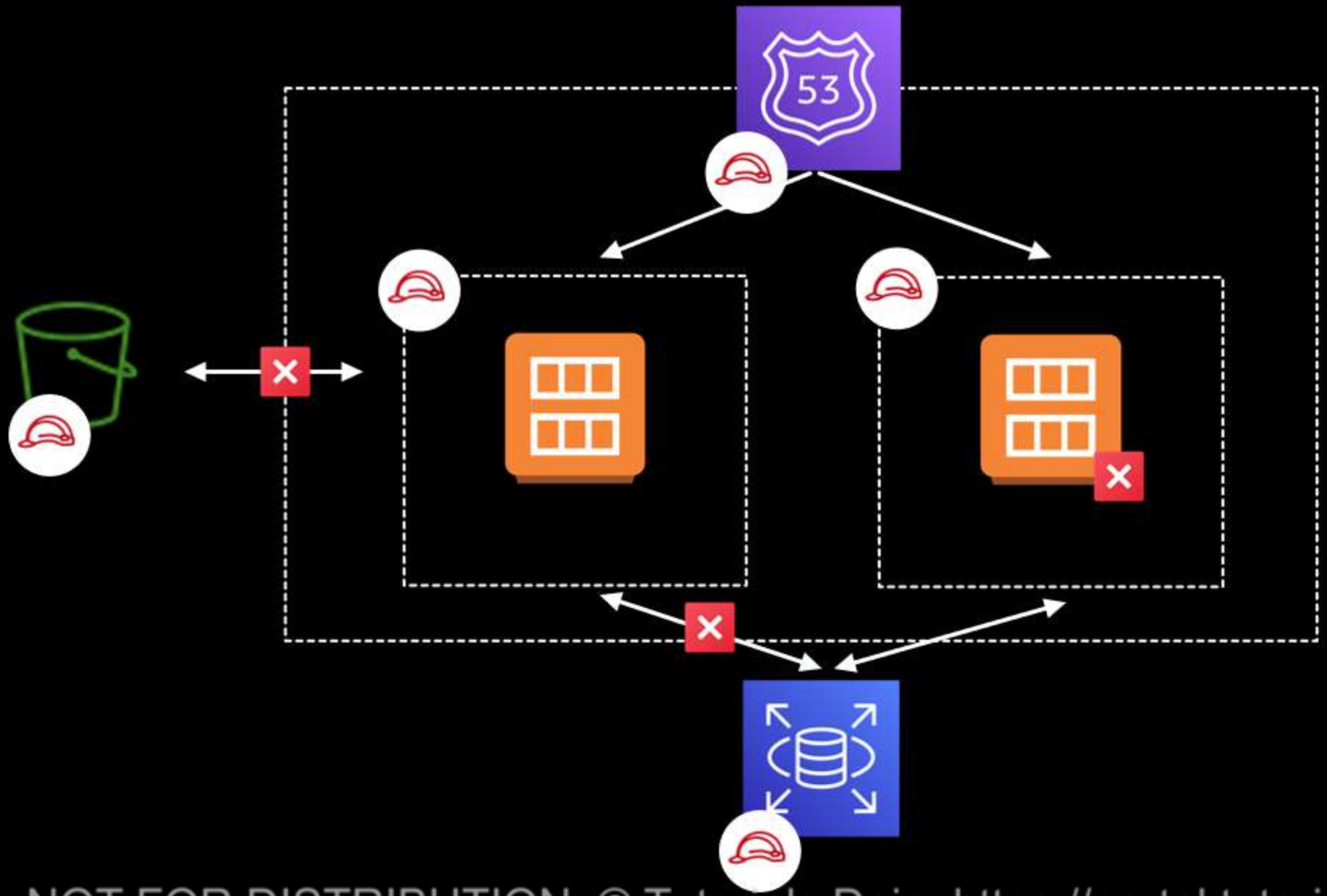
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



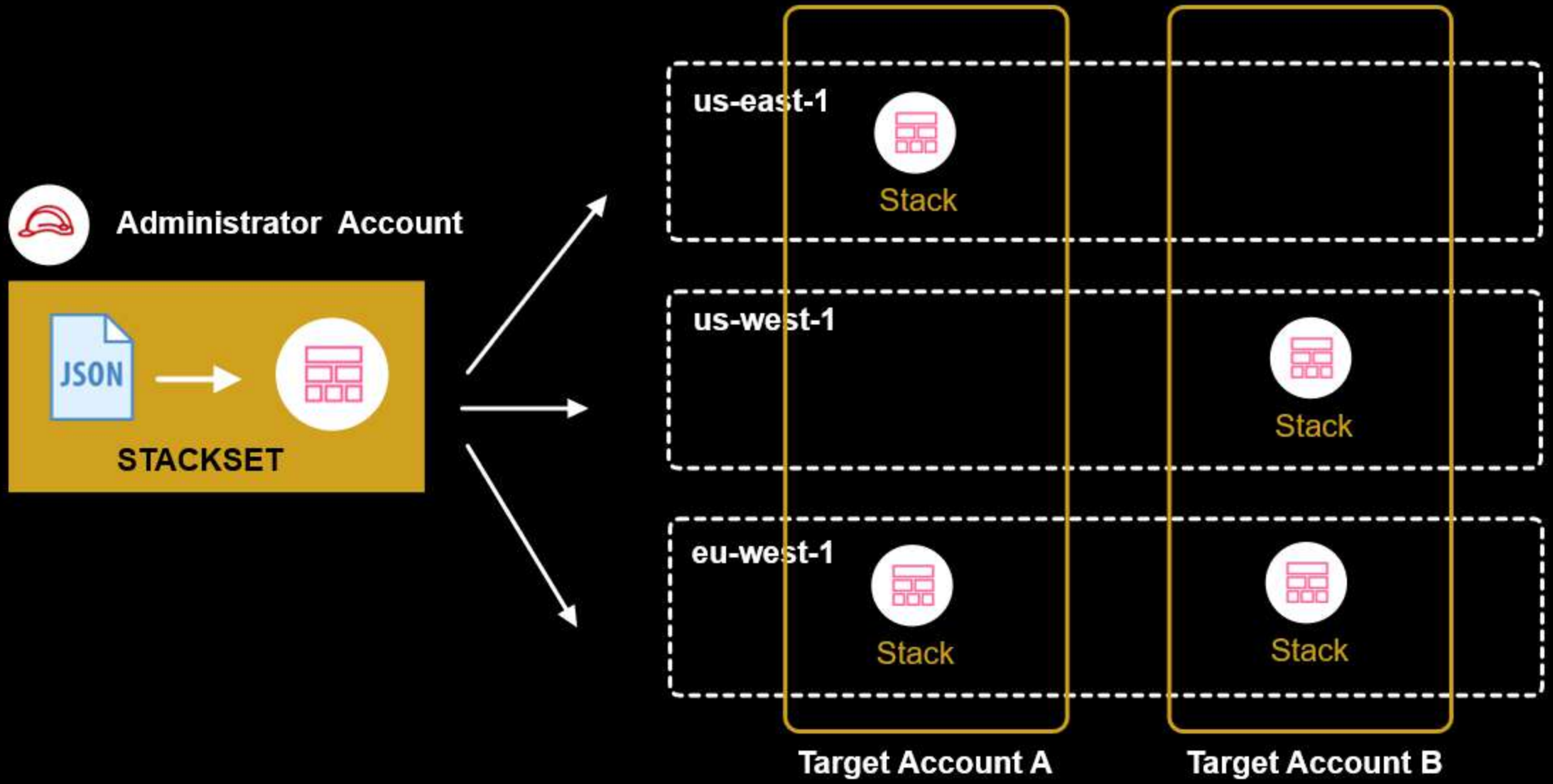
You may want to:

- isolate critical resources from test environments
- **restrict resources to regions or accounts**
- spread resources geographically for high availability

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

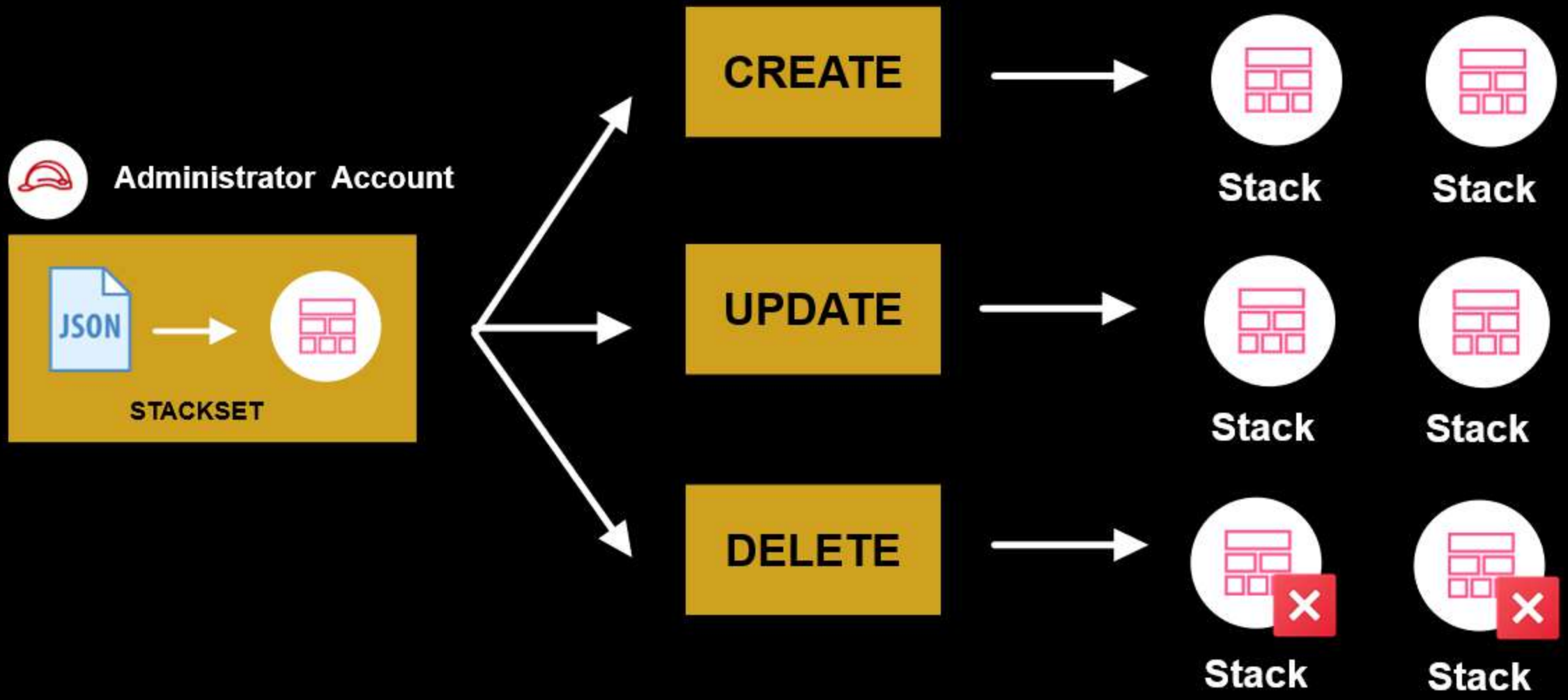


AWS CloudFormation Stacksets

STACK INSTANCES

- is a reference to a stack in a target account you defined within a given Region
- it can exist without a stack and it is associated with only one stack set.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Stacksets

To CREATE a stack set, you need to:

- specify a CloudFormation **TEMPLATE**
- **specify TARGET ACCOUNTS**
- identify REGIONS you will use

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Stacksets

When **UPDATING a stack set:**

- you cannot selectively update the template for some stacks
- an update always affects all stacks

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Stacksets

When **DELETING** **a stack set:**

- you are allowed to delete a single stack
- and you can also delete the entire stack set

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Stacksets

Additional Options you can use:

- Maximum Concurrent Accounts
- Failure Tolerance
- Retain Stacks
- Region Concurrency

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

TAGS

Key-Value Pairs

env : test

key value

used as filters for Billing and Cost Allocation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Permission Models

Self-managed

- **you define the IAM roles required** by StackSets to deploy resources across accounts and Regions
- StackSets can **deploy to any AWS account in which you have permissions** to create an IAM role

Service-managed

- you will be able to deploy stack instances to accounts managed by **AWS Organizations**
- **NO NEED** to create the necessary IAM roles anymore; StackSets will create the IAM roles that you need on your behalf.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation
Nested Stacks

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

At the end of the video, you will be able to:

- Explain what is a nested stack and what it allows you to do.
- Understand the relationship between a nested stack and change sets.

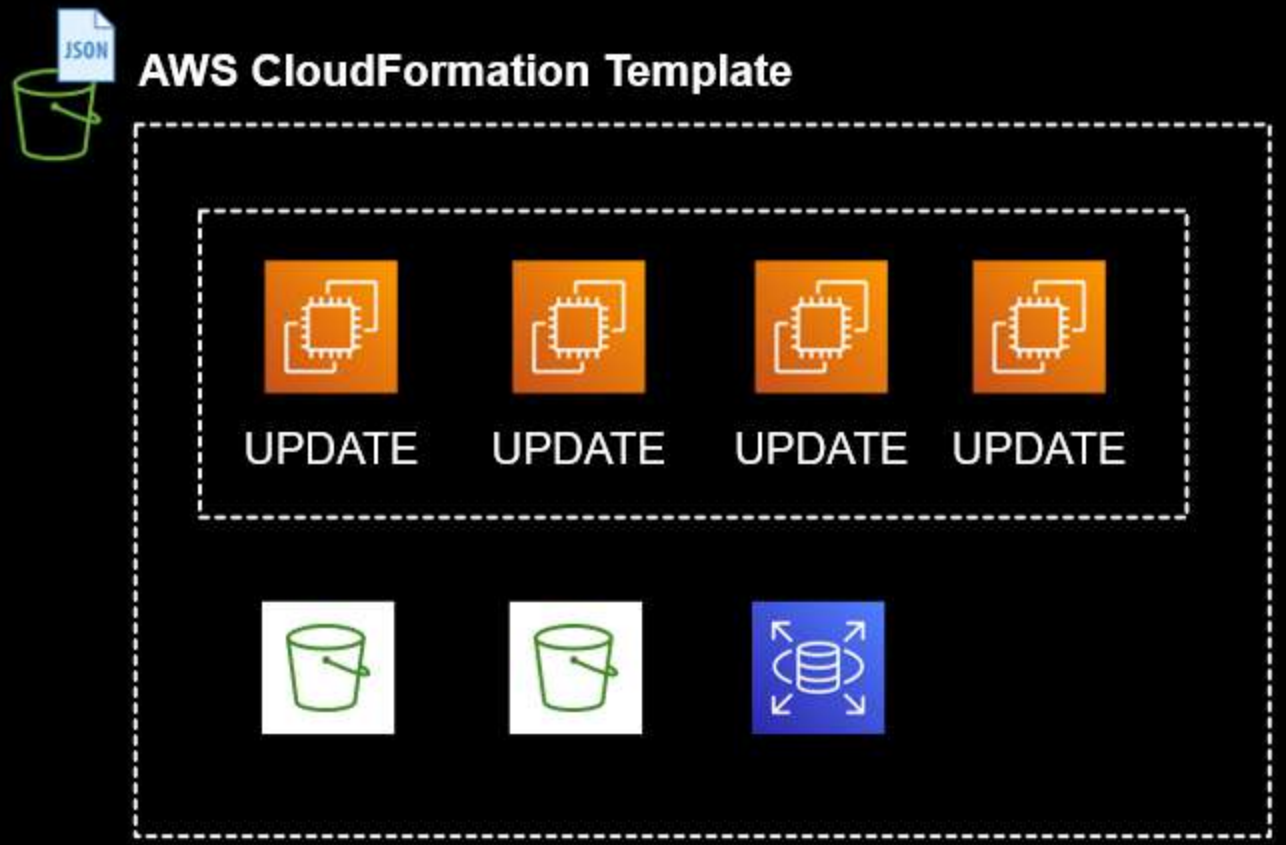
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS CloudFormation



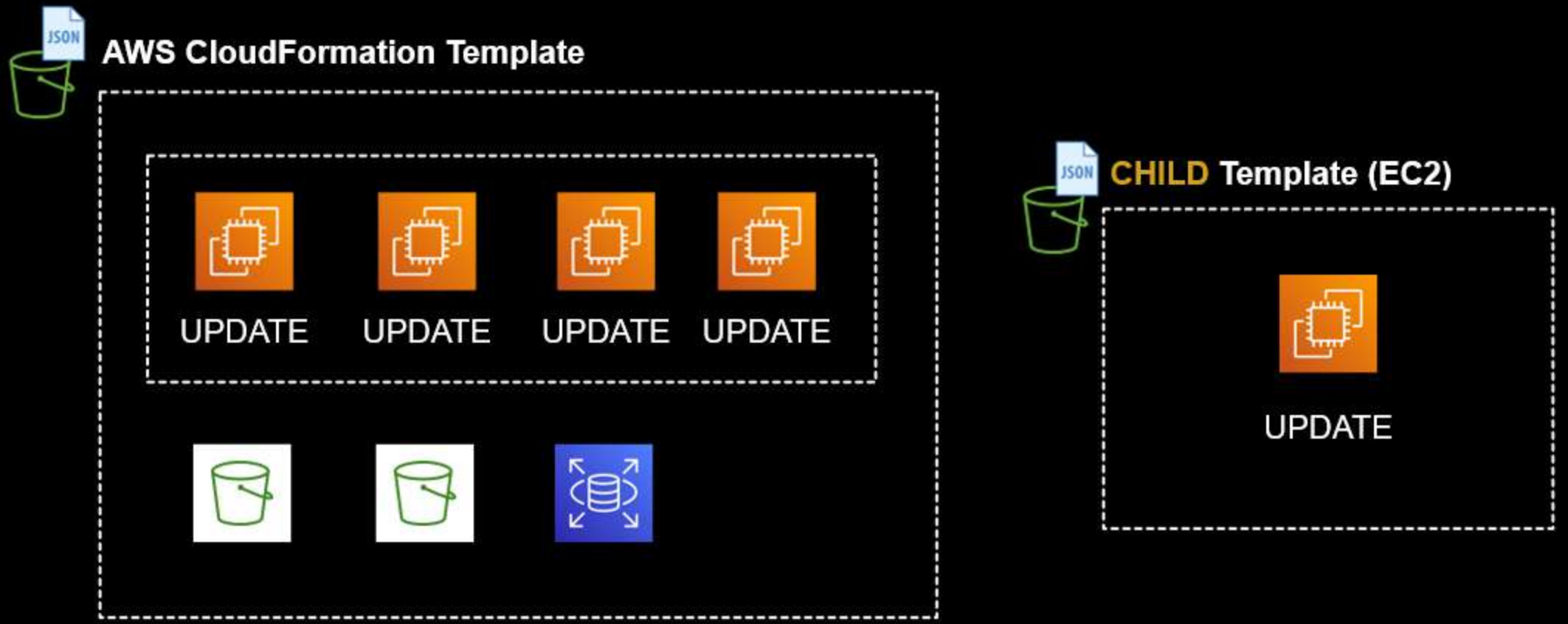
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS CloudFormation



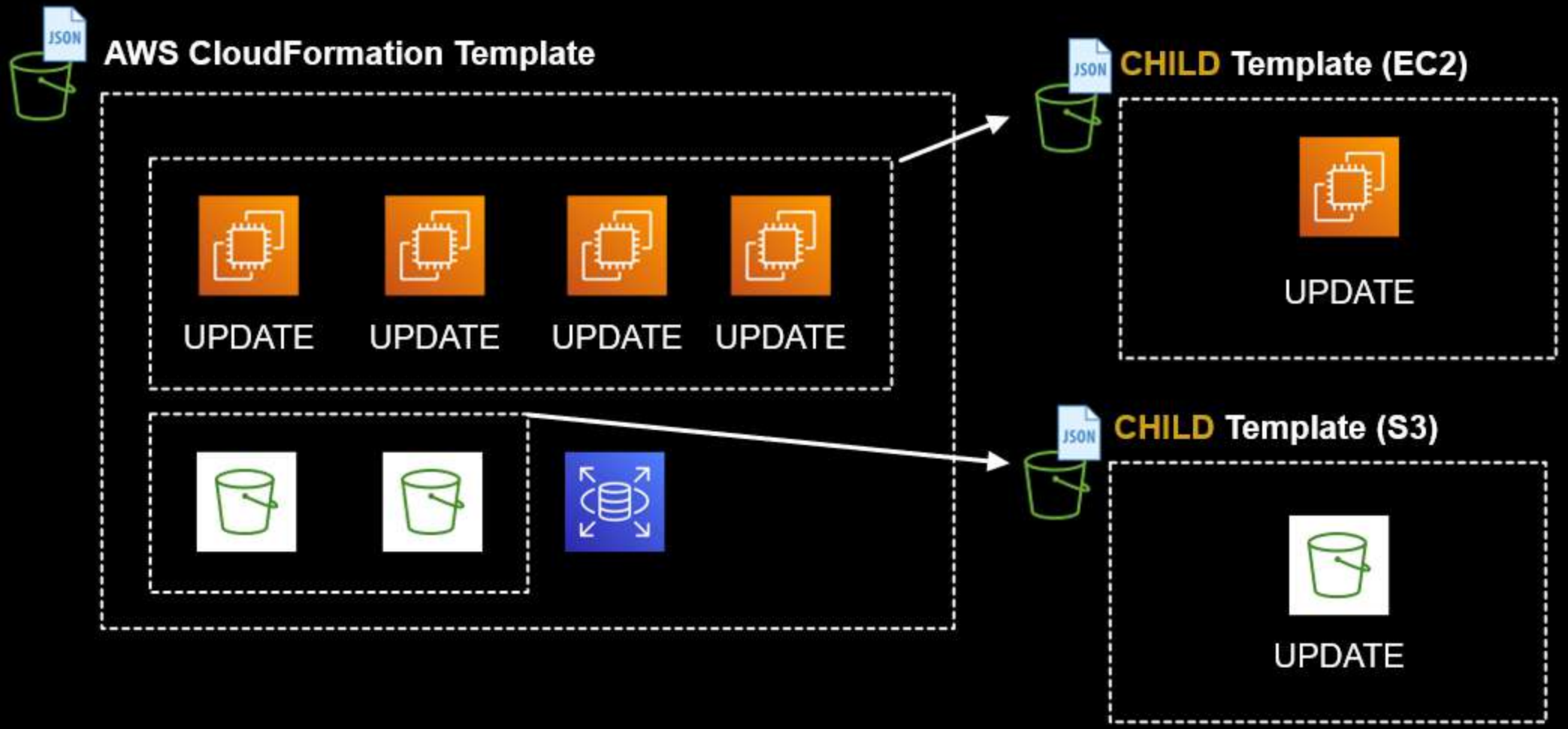
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS CloudFormation



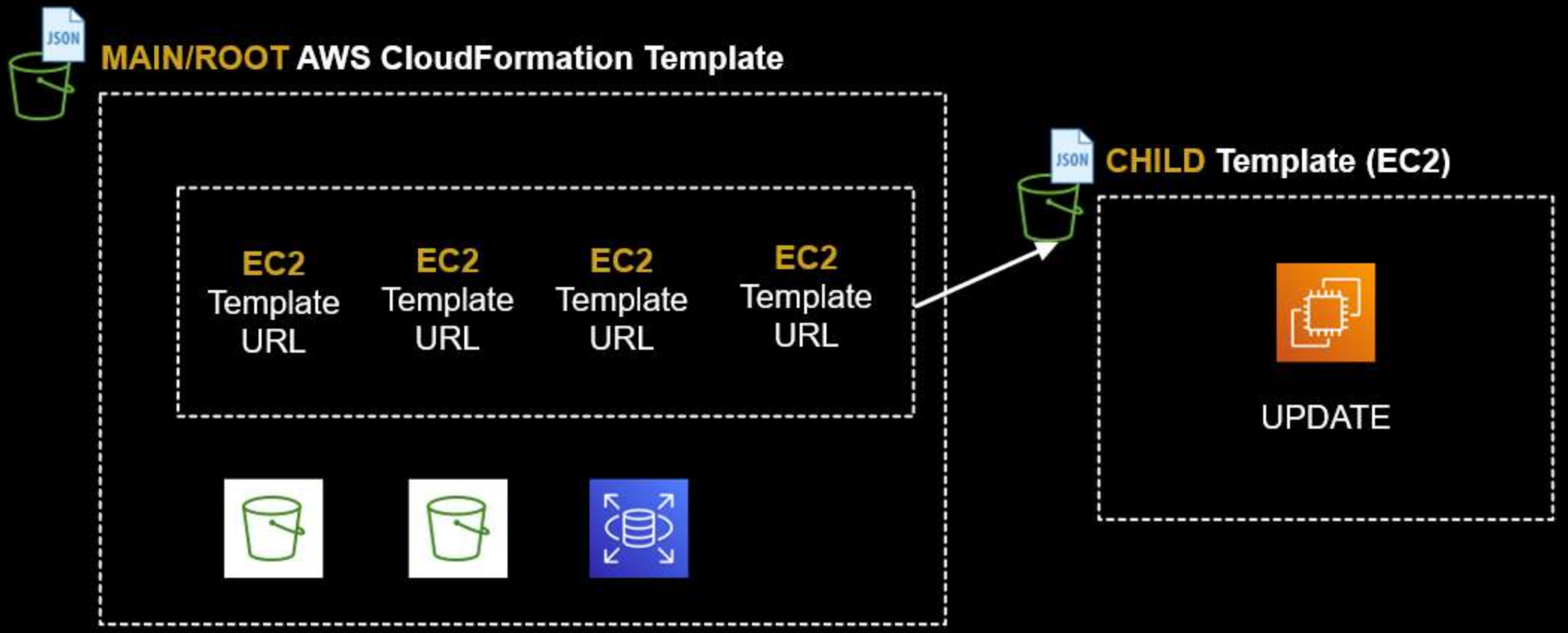
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS CloudFormation



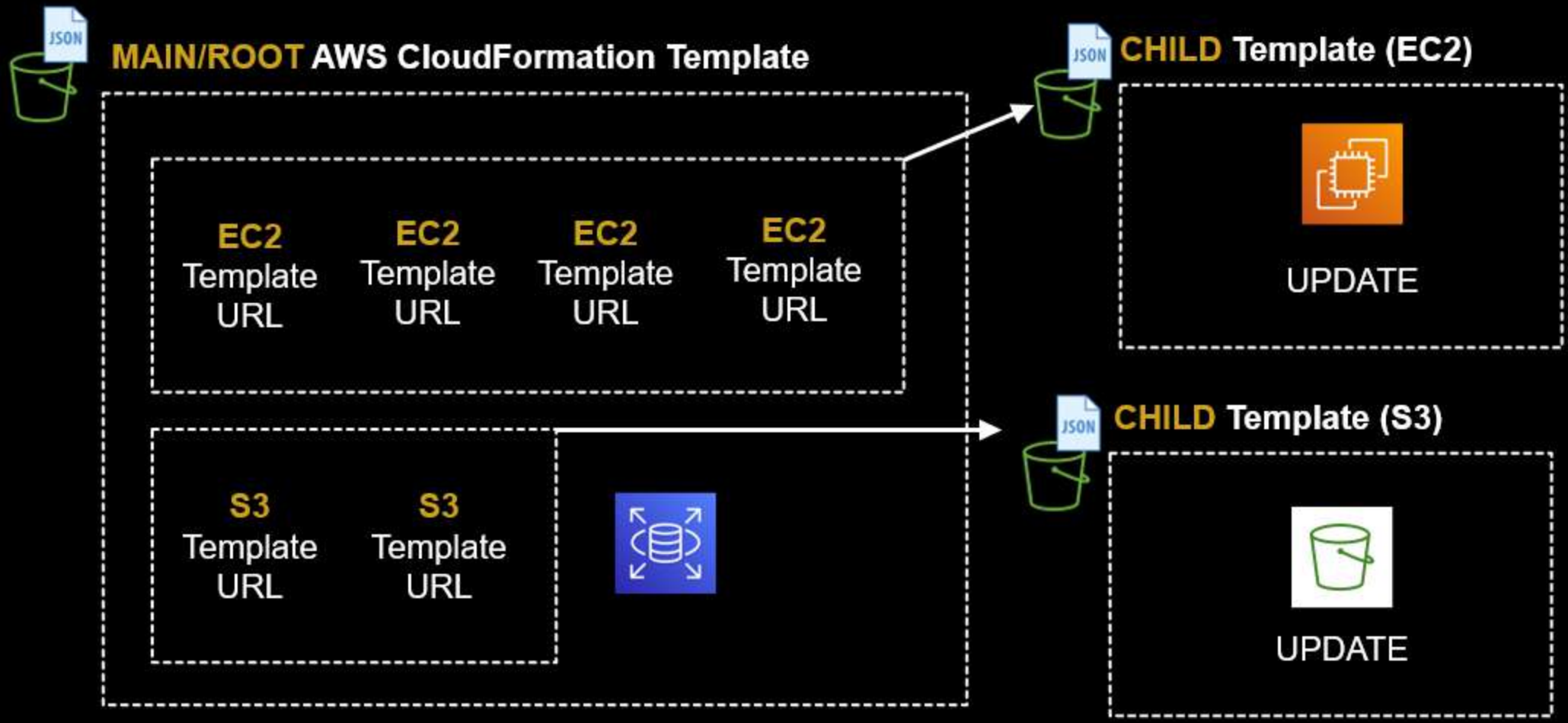
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS CloudFormation



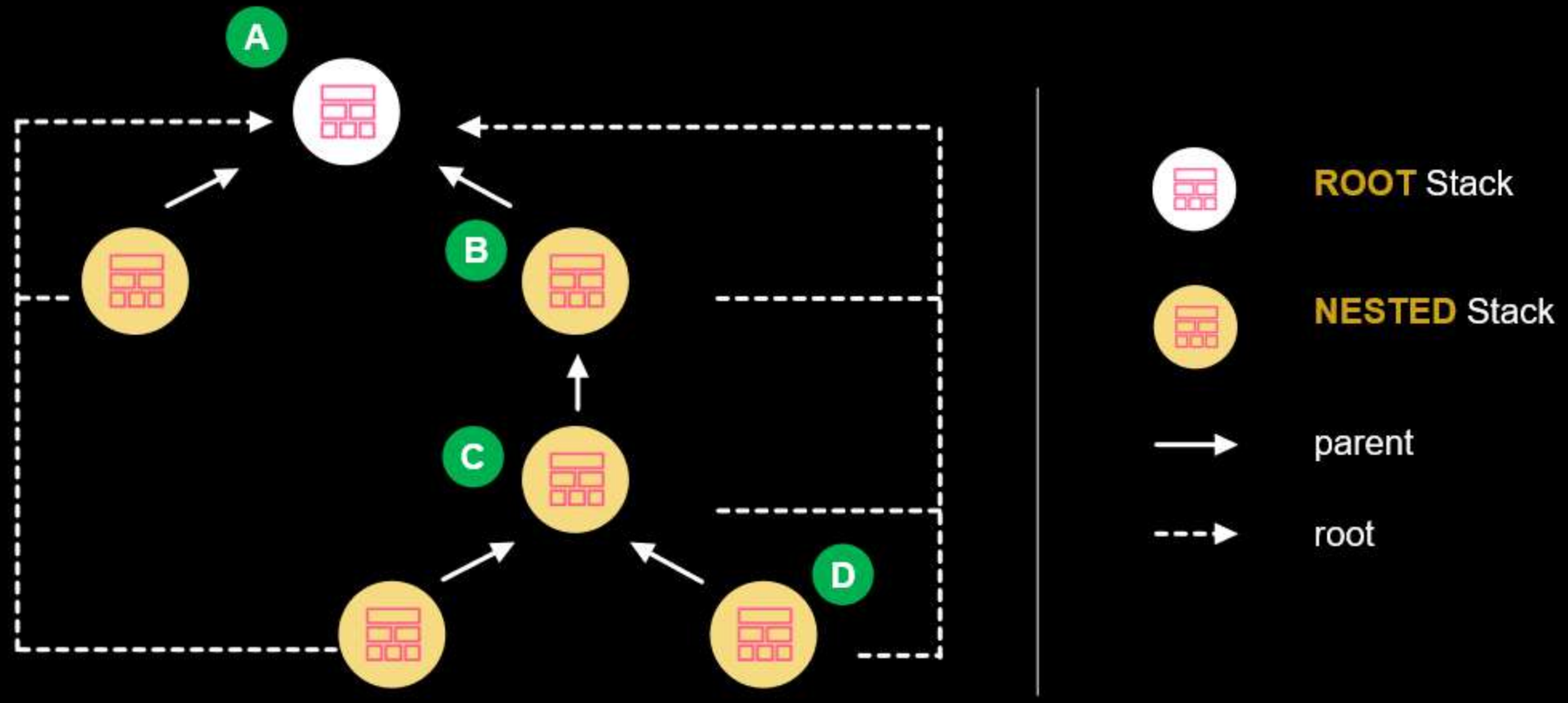
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS CloudFormation



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Sample Hierarchy of Nested Stacks



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Stacksets

Change Sets for Nested Stack Sets

- You can preview the changes to your application and infrastructure resources across the entire nested stack hierarchy prior to actual deployment
- **You can create change sets from any level of the stack hierarchy.**
- **If you need to execute or delete change sets for nested stacks, you need to do it from root change set.**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Custom Resource

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

At the end of the video, you will be able to:

- Understand when to use a custom resource in your CloudFormation templates.
- Learn how a custom resource works and how AWS Lambda and SNS integrates with it.
- Explain what makes a custom resource different from CloudFormation Registry.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Custom Resources

CloudFormation Custom Resources

- are **bits of logic that you declare to run during the provisioning phase** of your CloudFormation template.
- extends the features of CloudFormation to perform operations it could not normally do like:

    1. Provisioning resources that are not available as AWS CloudFormation resource type

    2. Provisioning non-AWS resources

    3. Performing provisioning steps not related to infrastructure

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

How does it work?



Template Developer

- creating template
- specify **service token** and input data / parameters in the template

Custom Resource Provider

- **owns** the custom resource
- determines how to respond to AWS CloudFormation requests
- provides **service token**

AWS CloudFormation

- sends request for a service token
- waits for a response before taking the next action

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Custom Resources

- **Custom resources require one property: the service token**, which specifies where AWS CloudFormation sends requests to, such as an Amazon SNS topic or an AWS Lambda function.

- **Associating Lambda** with custom resources:
  - the function is invoked whenever the custom resource is created, updated, or deleted
  - AWS CloudFormation calls a Lambda API to invoke the function and to pass all the request data to the function

- **Associating SNS** with custom resources:
  - you are able to perform scenarios like adding new resources to a stack and injecting dynamic data or information into a stack.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Associating SNS with Custom Resource



AWS CloudFormation

A custom resource was created during stack creation.

SNS

Triggers the application in an EC2 instance

EC2 (Subscriber)

Performs additional provisioning tasks

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS CloudFormation Registry

- **lists private and public extensions** that you can use in your CloudFormation account.
- extensions as artifacts registered in the CloudFormation registry and **can be written by Amazon, APN partners, Marketplace sellers, or even by the developer community**.
- The CloudFormation registry offers several advantages over custom resources like:
  - modeling, provisioning, and managing third-party application resources
  - Create, Read, Update, Delete, and List (CRUDL) operations
  - Drift detection on private and third-party resource types

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Data Lifecycle Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Data Lifecycle Manager

At the end of the lecture, you will be able to:

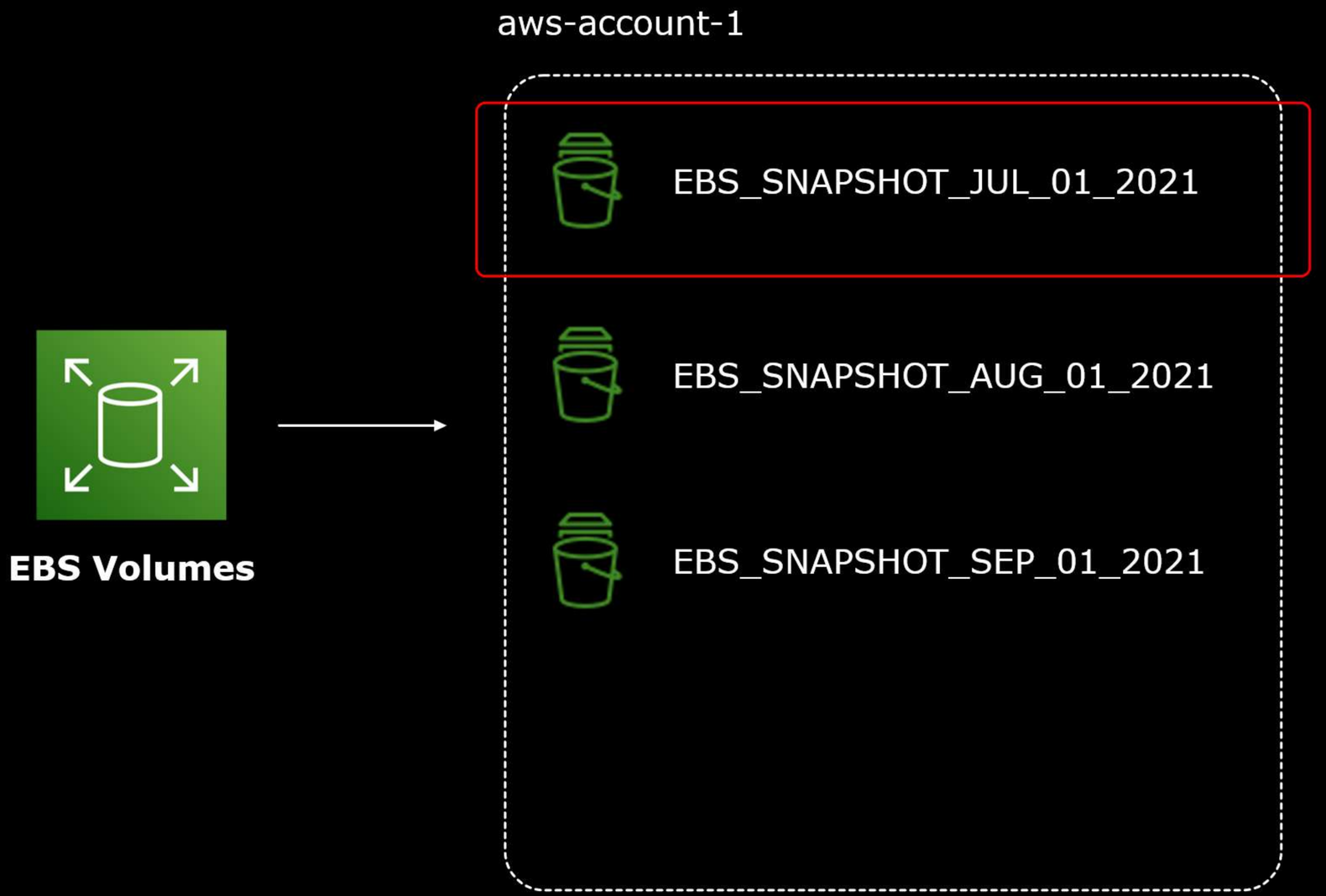
- explain how the Amazon Data Lifecycle Manager service helps you manage your EBS volume backups.



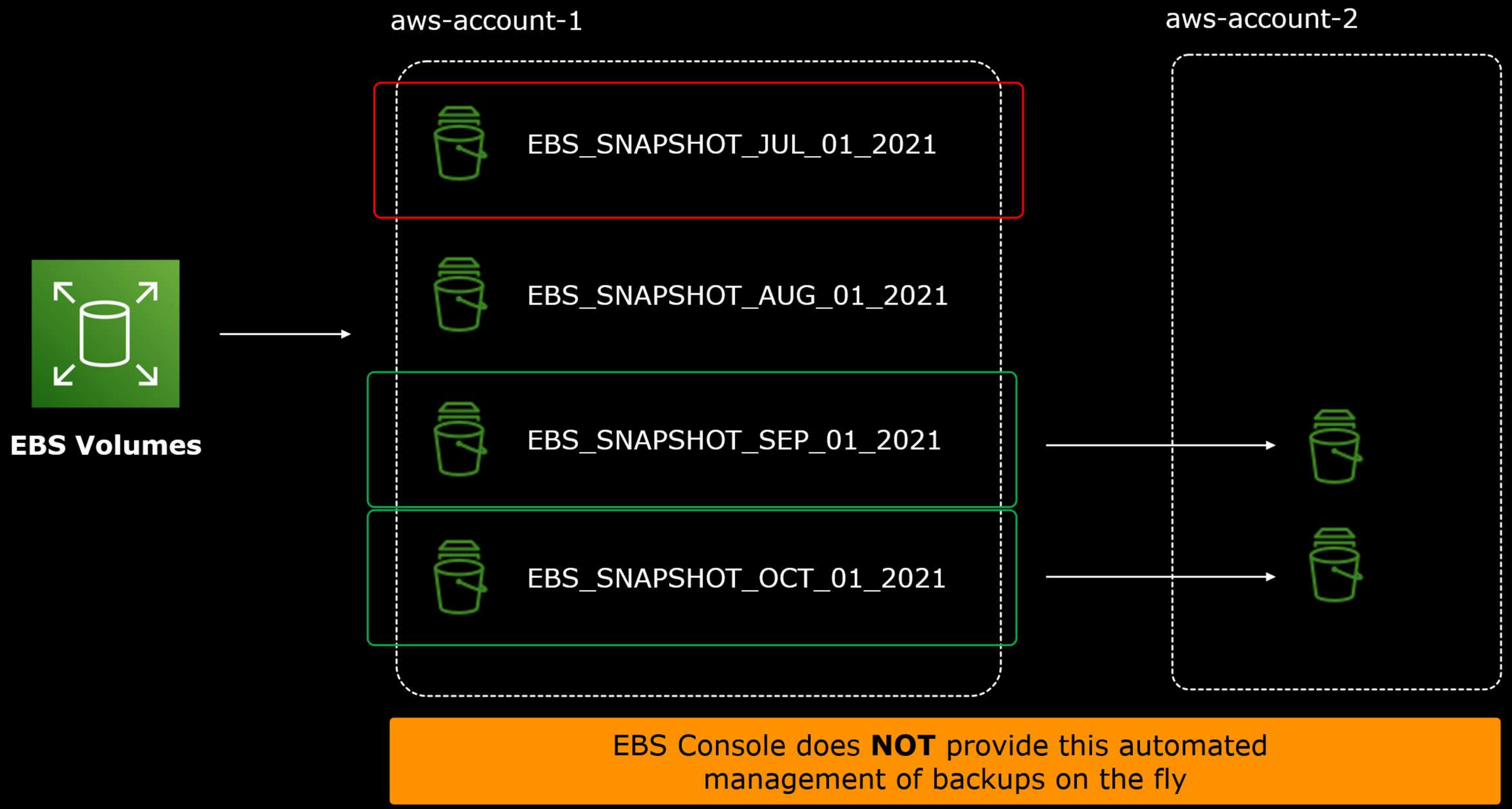
EBS Volumes



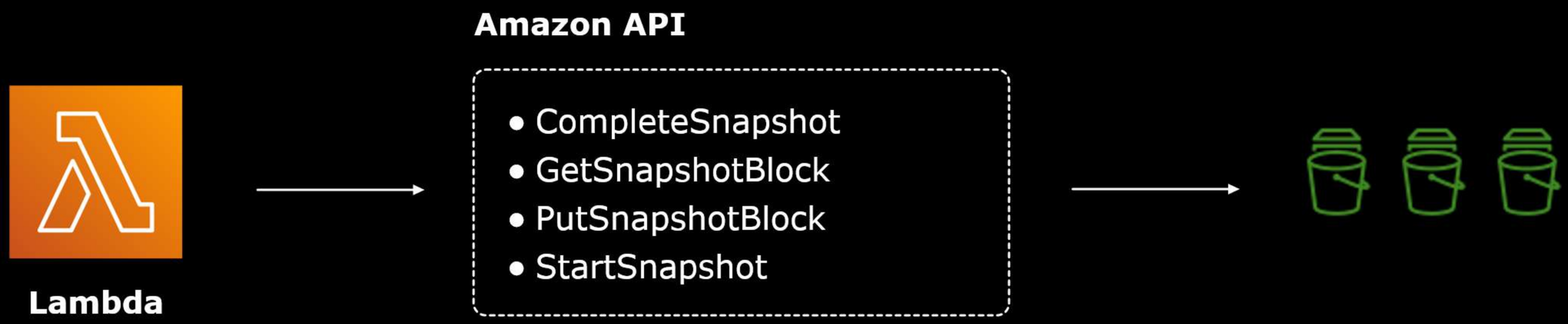
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



This serverless approach allows you to customize the steps and rules for managing your EBS snapshots

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Data Lifecycle Manager

- Automate the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs.
- protect your volumes by enforcing a regular backup schedule
- retain backups as required by your organization's internal policy
- reduce storage costs by deleting outdated backups
- implement disaster recovery backup policies that back up data to different AWS accounts

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Data Lifecycle Manager

How does it work?

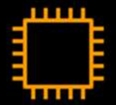
1. Create a policy in Data Lifecycle Manager

- EBS snapshot policy



when you want to create a policy for existing EBS volumes you have

- EBS-backed AMI policy



backups for AMIs that are backed with a single or multiple EBS volume

- Cross-account event policy



automatically copying shared snapshots across AWS accounts

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Data Lifecycle Manager

How does it work?

2. Define the tags of the EBS Volumes you want to backup

env: prod

env: uat

env: test

env: uat

3. Define the schedule and frequency to create your backups

4. Define retention period for your policy

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Data Lifecycle Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Backup

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Systems Manager

In this video, you will be able to:

- Understand how backups are generated in AWS Backup
- Create a vault, backup plan, and assign resources in AWS Backup

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Backup is a fully managed, centralized, and automated solution for backing up AWS resources.



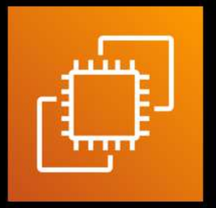
AWS Backup



EBS



EFS



EC2



RDS



DynamoDB



Storage Gateway



Aurora

Uses the default backup mechanism for each of these AWS services

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



How to create a backup?

- You need to create vaults

my-app


EBS


EFS


EC2


RDS

backup container

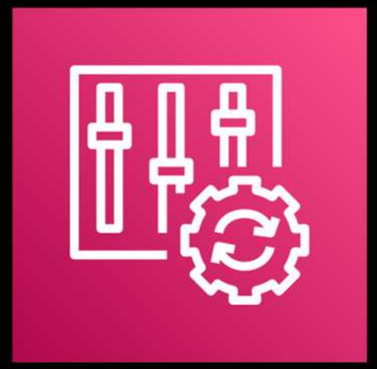
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



How to create a backup?

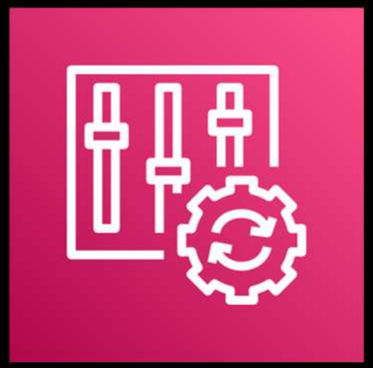
- You need to create vaults
- Create a backup plan
  - Schedule when to take your backups
  - Define the frequency of taking backups
  - Declare how long you want to store those backups

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Config

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

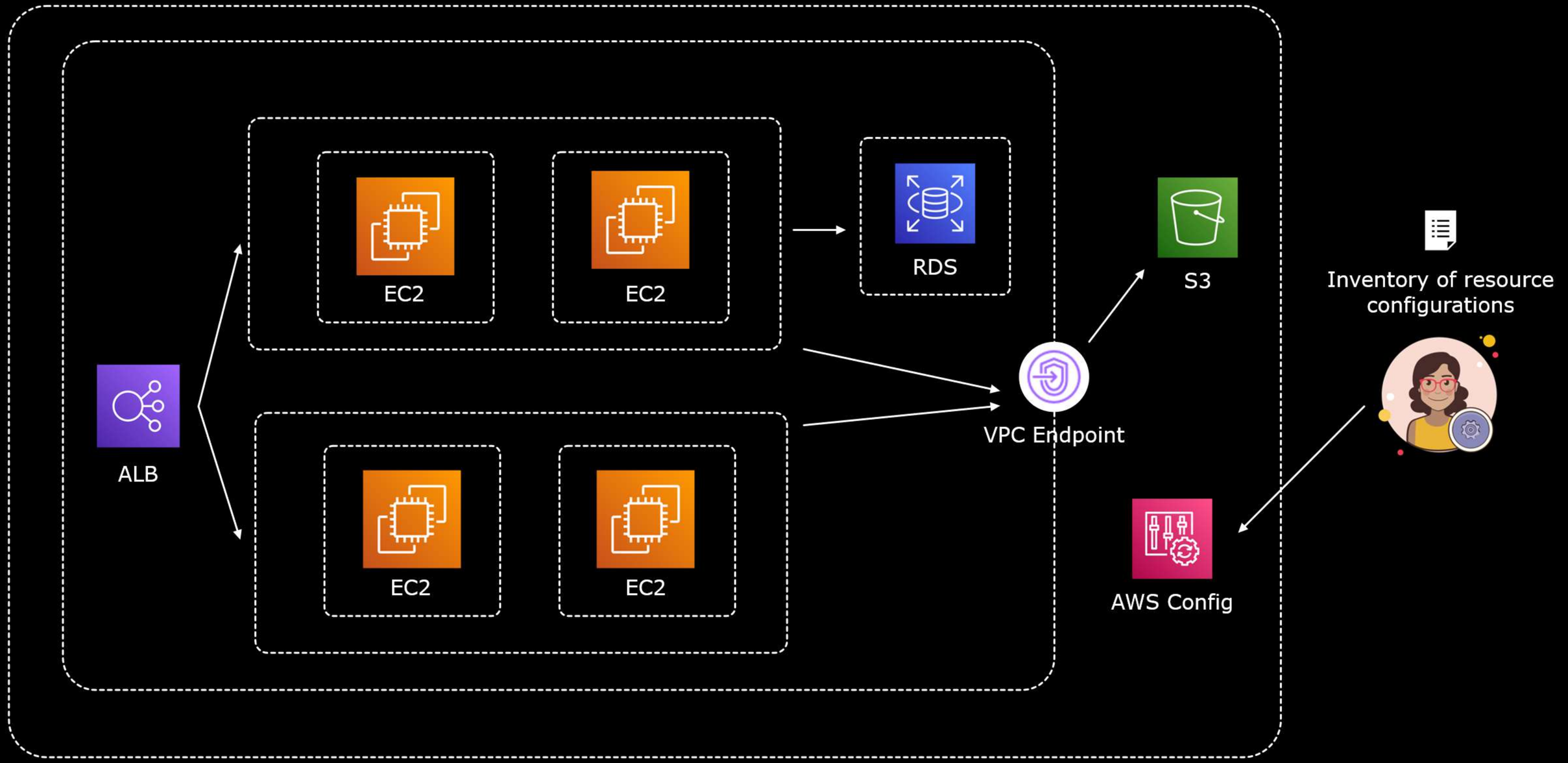


AWS Config

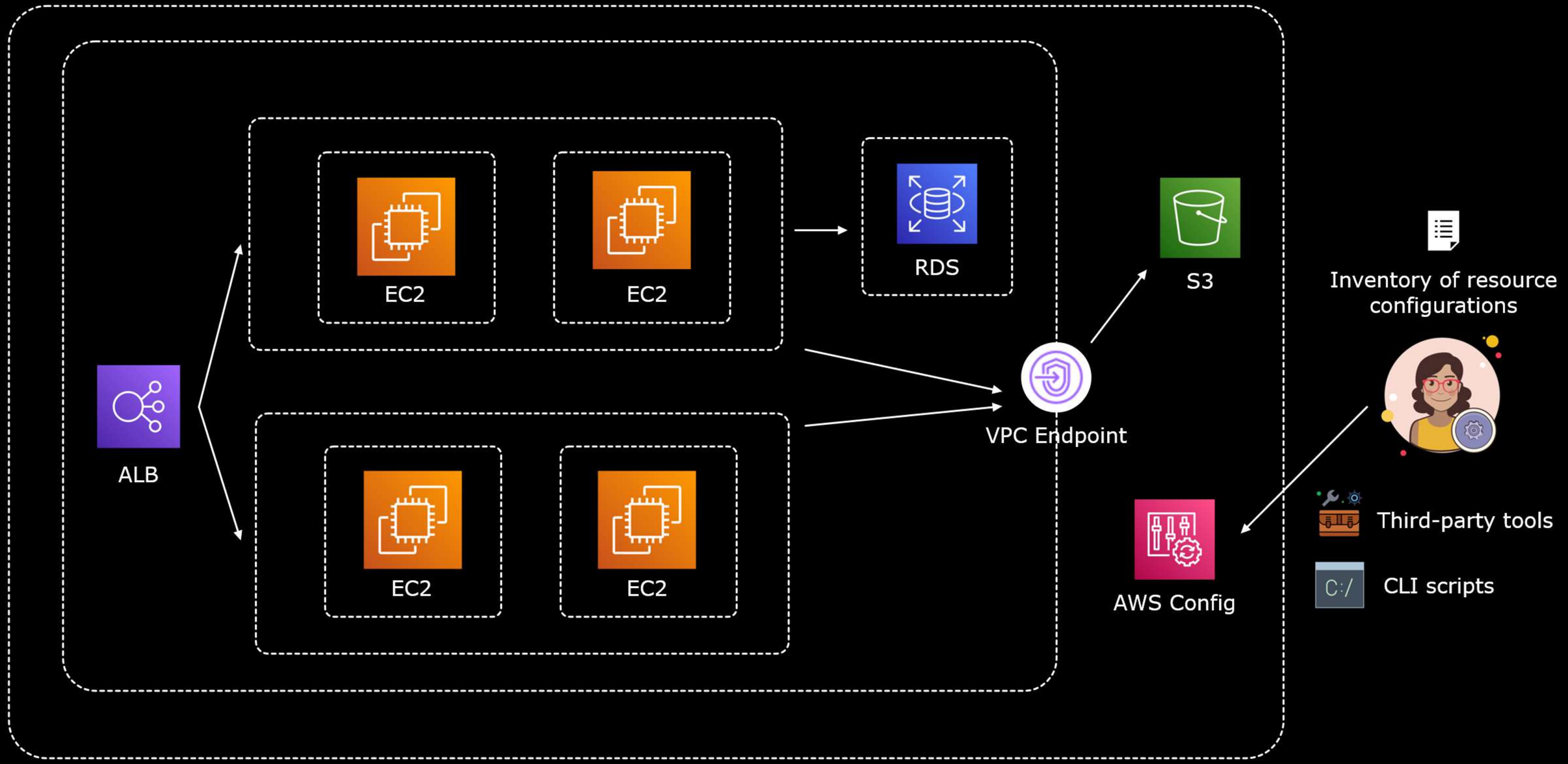
In this video, you will be able to:

- understand how AWS Config helps with the audit and governance of your AWS resources
- explain how the service works
- evaluate scenarios where AWS Config can be applicable

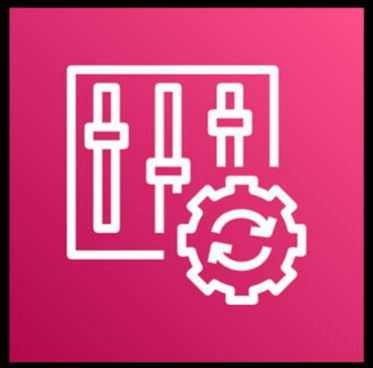
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

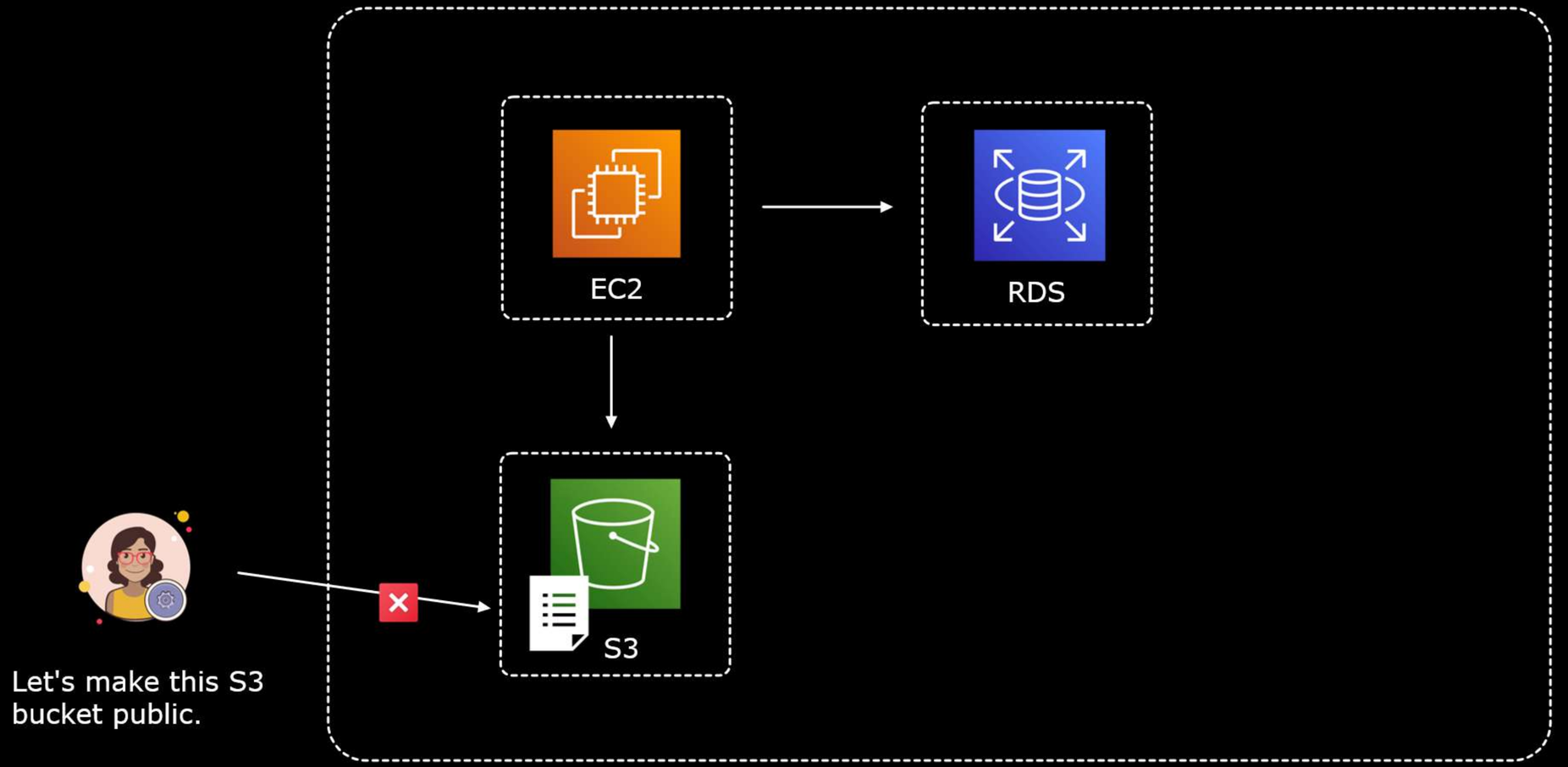


AWS Config

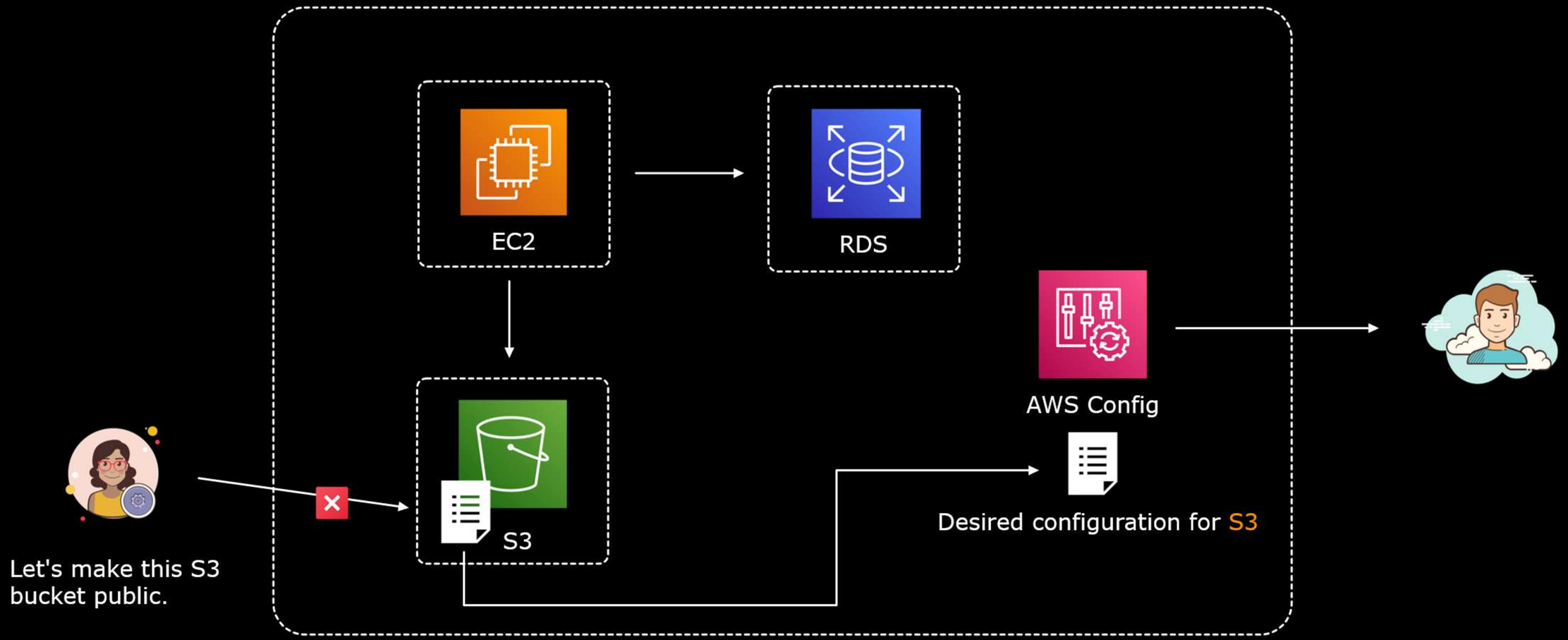
What is AWS Config?

- allows you to manage resource configurations collectively
- Two basic functions:
  - record all of the configuration data that runs on your resources
  - build configuration rules to ensure compliance in your infrastructure

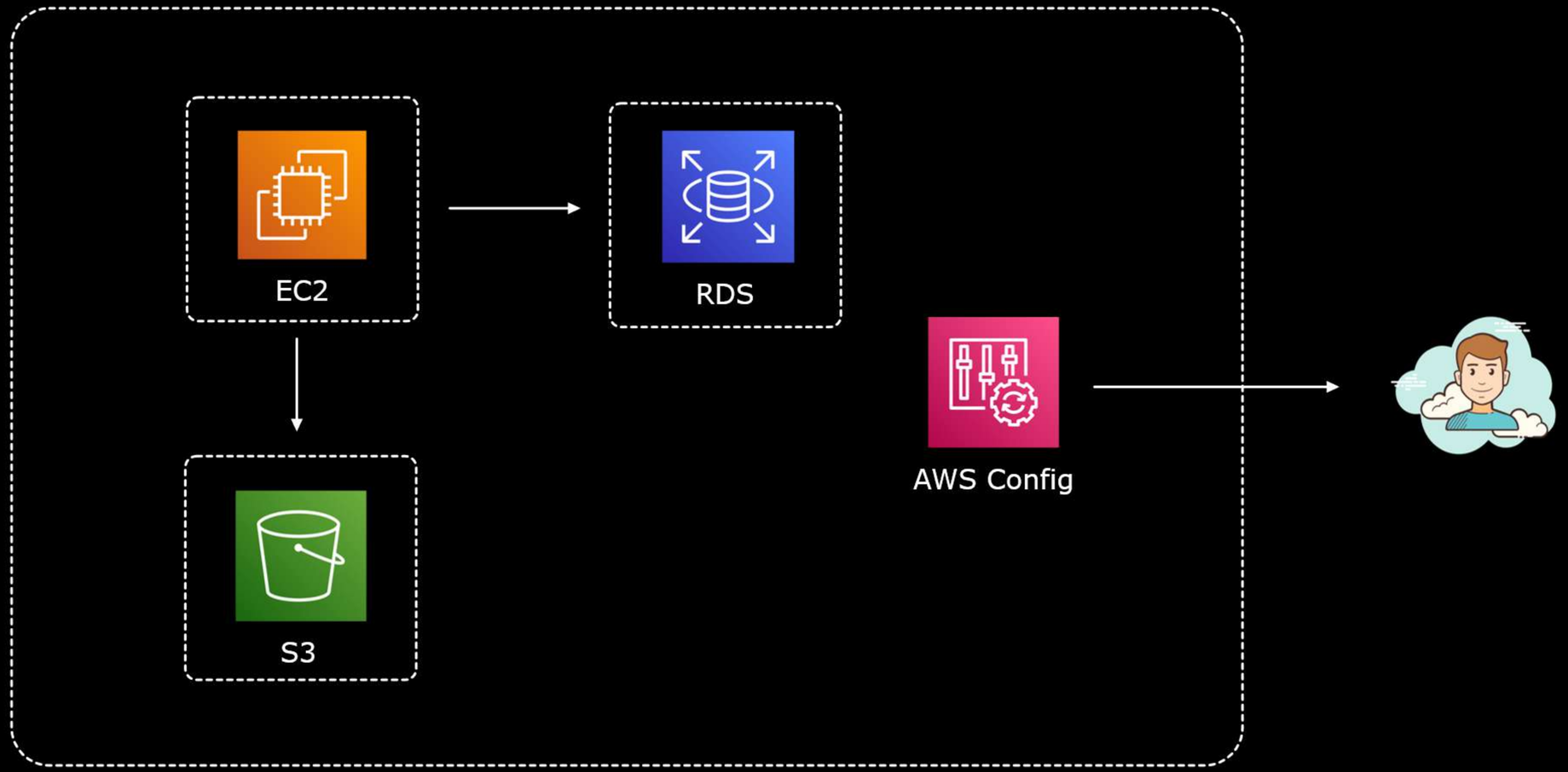
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



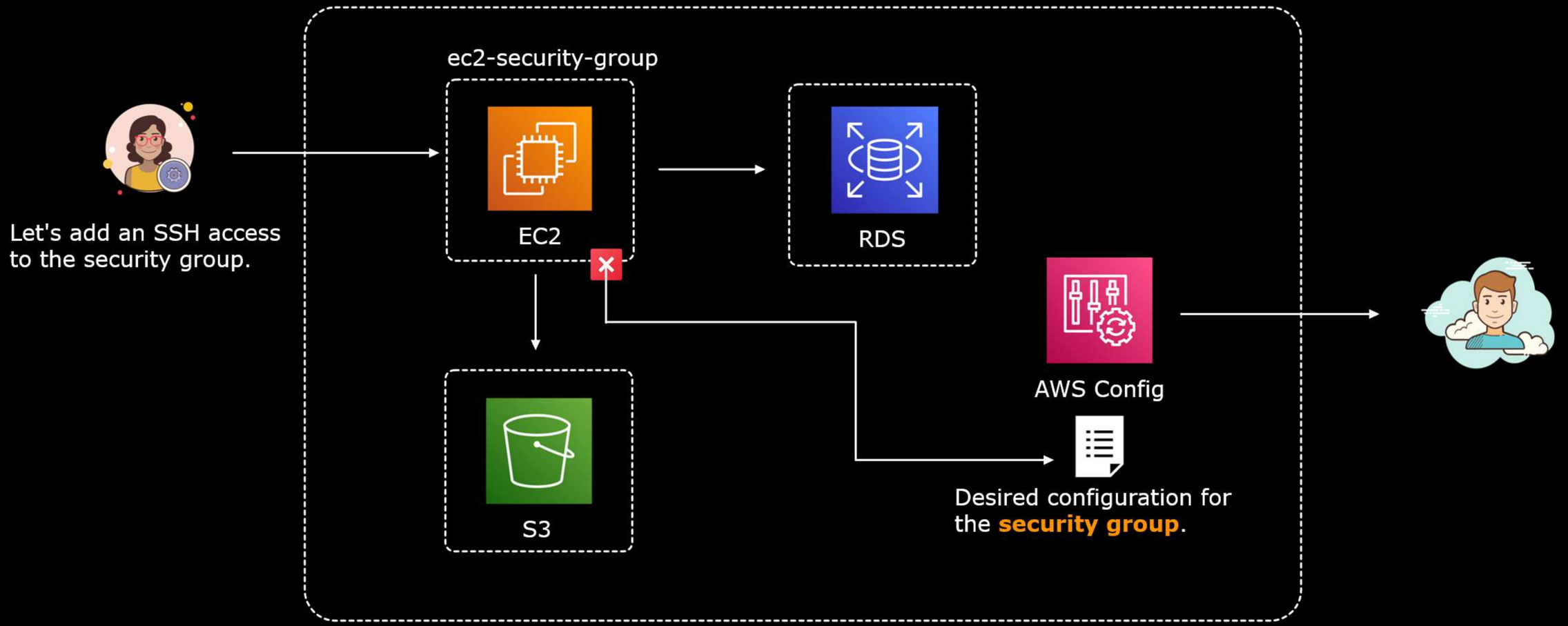
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



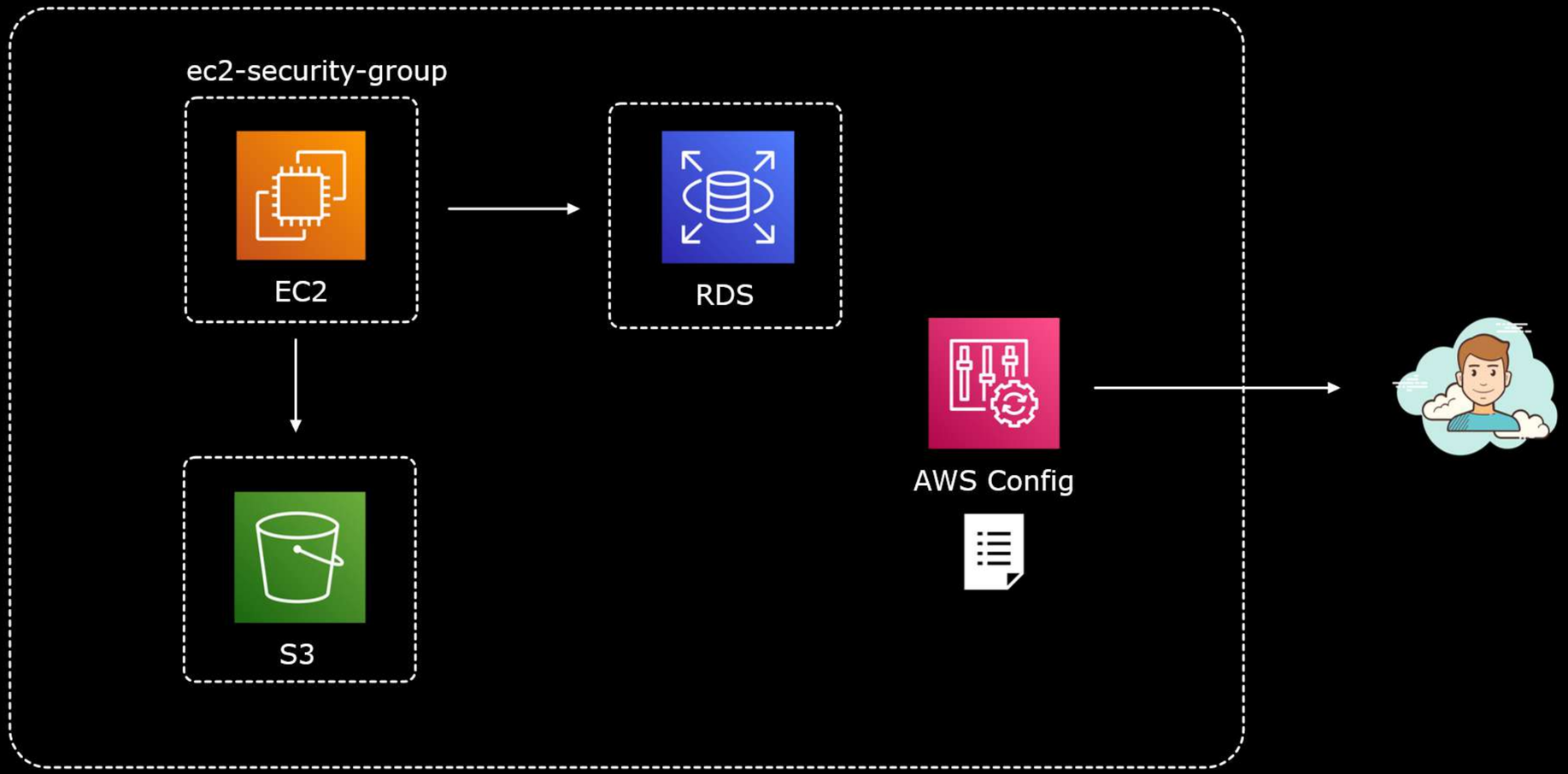
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



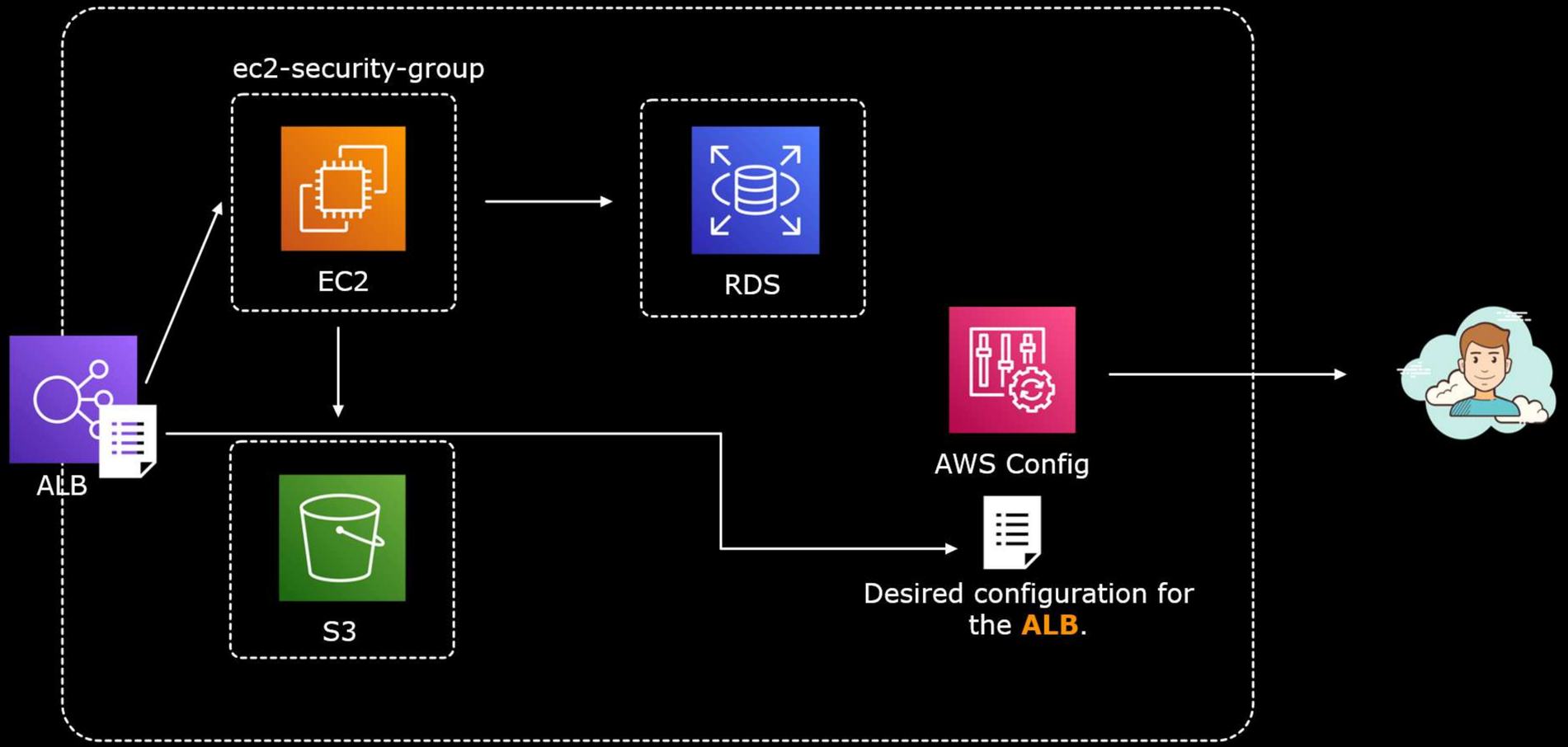
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



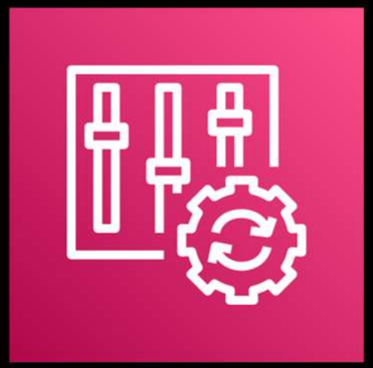
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Config

How does AWS Config work?

- First, you turn on AWS Config to let the service discover the supported AWS resources

> You can explicitly specify the resource types that you want to track.

- Then, you can start creating config rules

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

CONFIG RULES

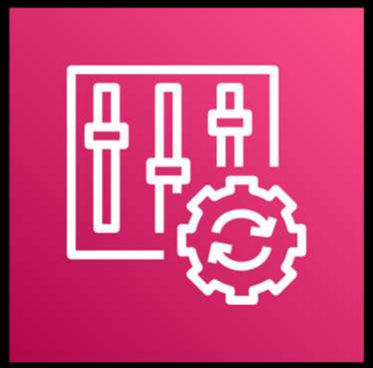
AWS Managed Rule

- are predefined but customizable rules that AWS provides to help you evaluate your AWS resources if they comply with desired configurations

Custom Rule

- a rule that is associated with a AWS Lambda function that you created which evaluates if your AWS resources comply with your desired configurations

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Config

When does AWS Config evaluate the rule you created?

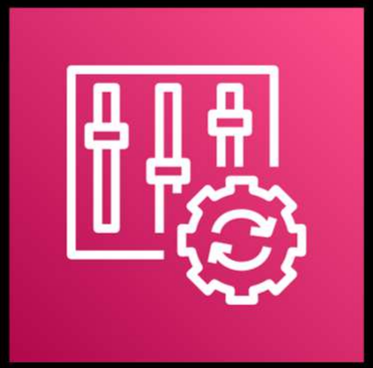
- AWS Config evaluates the config rules you create based on two triggers.

when there is a configuration change on your resource	based on a regular schedule you set

As long as you turn AWS Config on, you will still see the configuration changes of your resources.

- You can configure a config rule to publish a message to an SNS topic based on your requirement

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Config

- AWS Config is a regional service.
- But you can use the multi-account and multi-region data aggregation capability of AWS Config
  - You have to create an Aggregator in the region where you want to see the aggregated AWS Config configuration data

for an individual AWS account

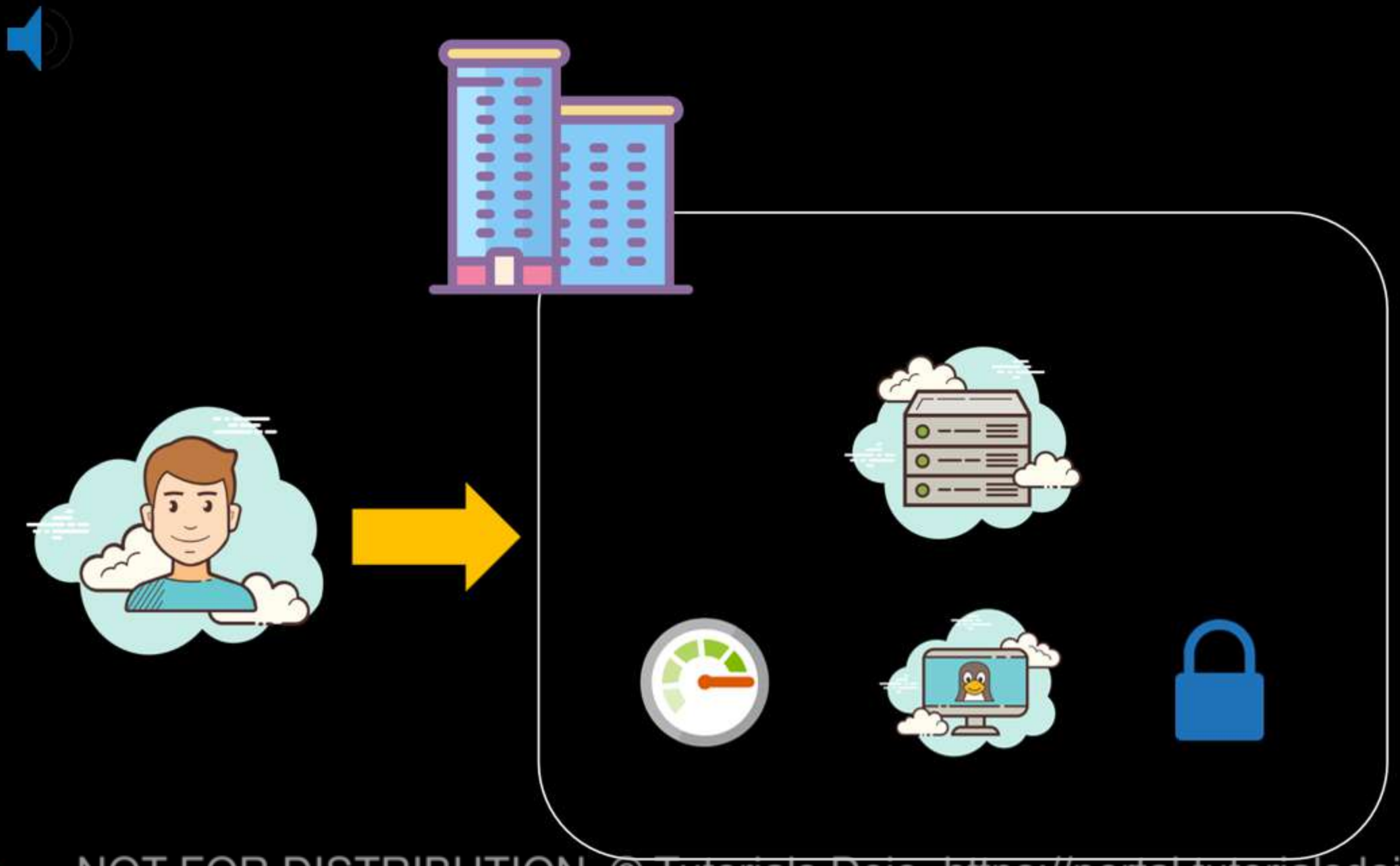
for an Organization

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Lambda

Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

No servers to manage!



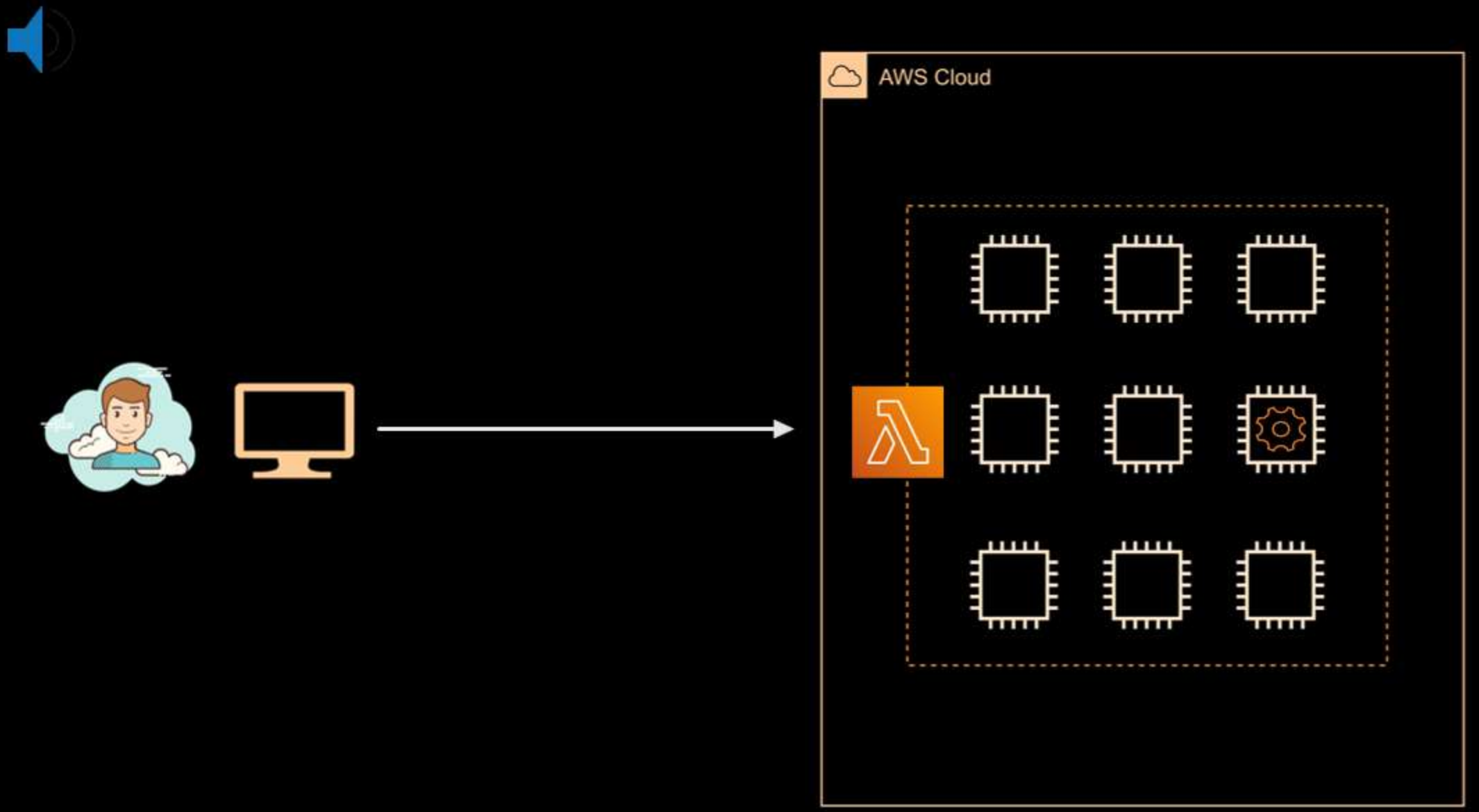
Create a Lambda function

Deploy your code

Run

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



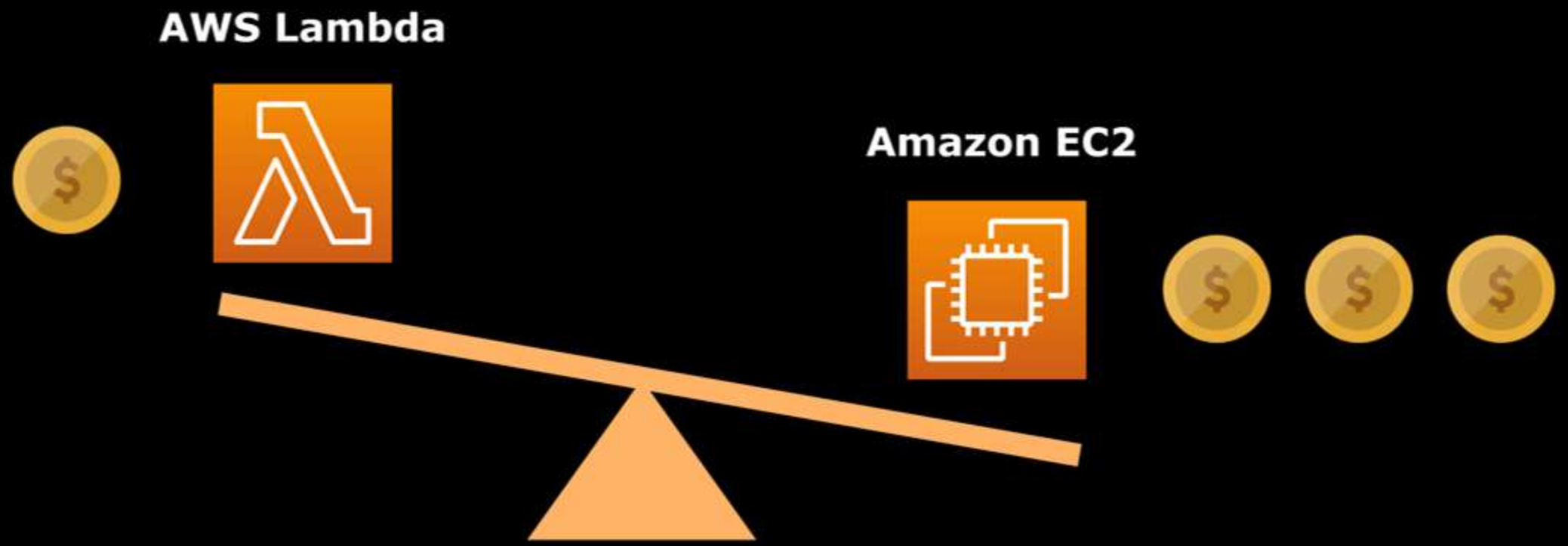
Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Faster development time

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Lambda is a lot cheaper than Amazon EC2

You only pay for invocation requests and the time your function executes

Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/













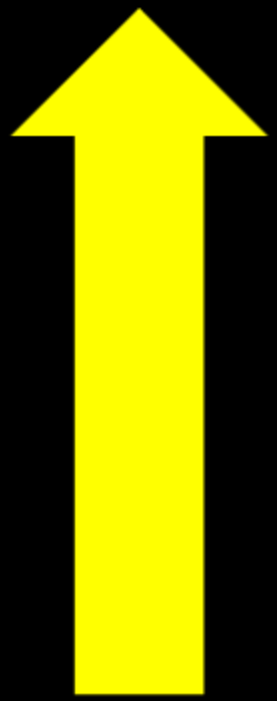




Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Instance	vCPU*	Mem (GiB)	Storage	Dedicated EBS Bandwidth (Mbps)	Network Performance
m4.large	2	8	EBS-only	450	Moderate
m4.xlarge	4	16	EBS-only	750	High
m4.2xlarge	8	32	EBS-only	1,000	High
m4.4xlarge	16	64	EBS-only	2,000	High
m4.10xlarge	40	160	EBS-only	4,000	10 Gigabit
m4.16xlarge	64	256	EBS-only	10,000	25 Gigabit

Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

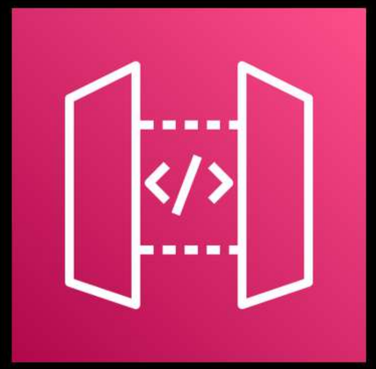


The higher the memory



The shorter the execution time of the Lambda function

Tutorials Dojo NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

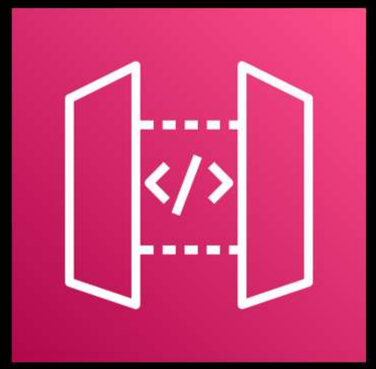


Amazon API Gateway

Tutorials Dojo

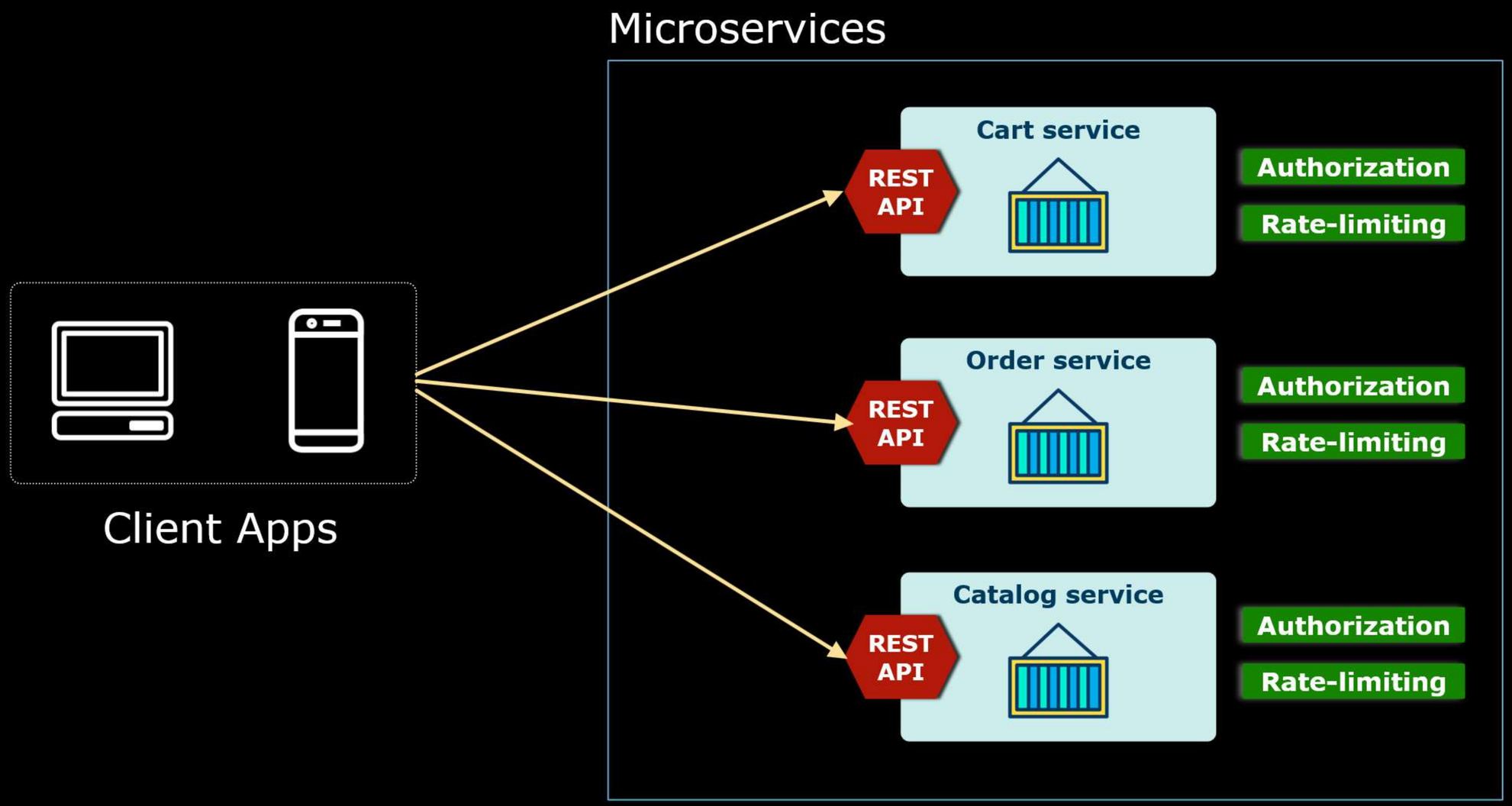
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

- API management service that lets you create, publish, maintain, monitor, and secure APIs at any scale



Amazon API Gateway

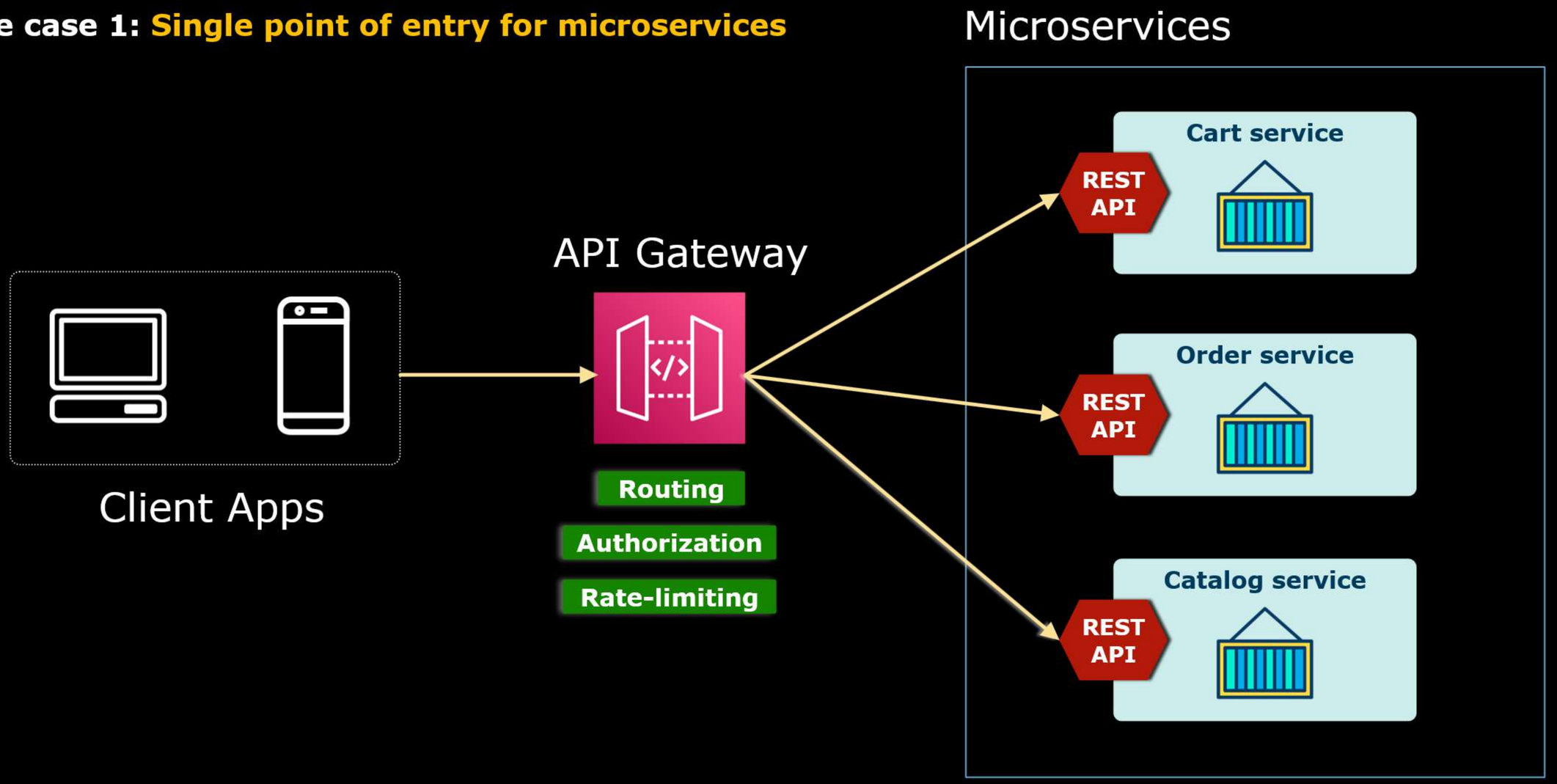
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

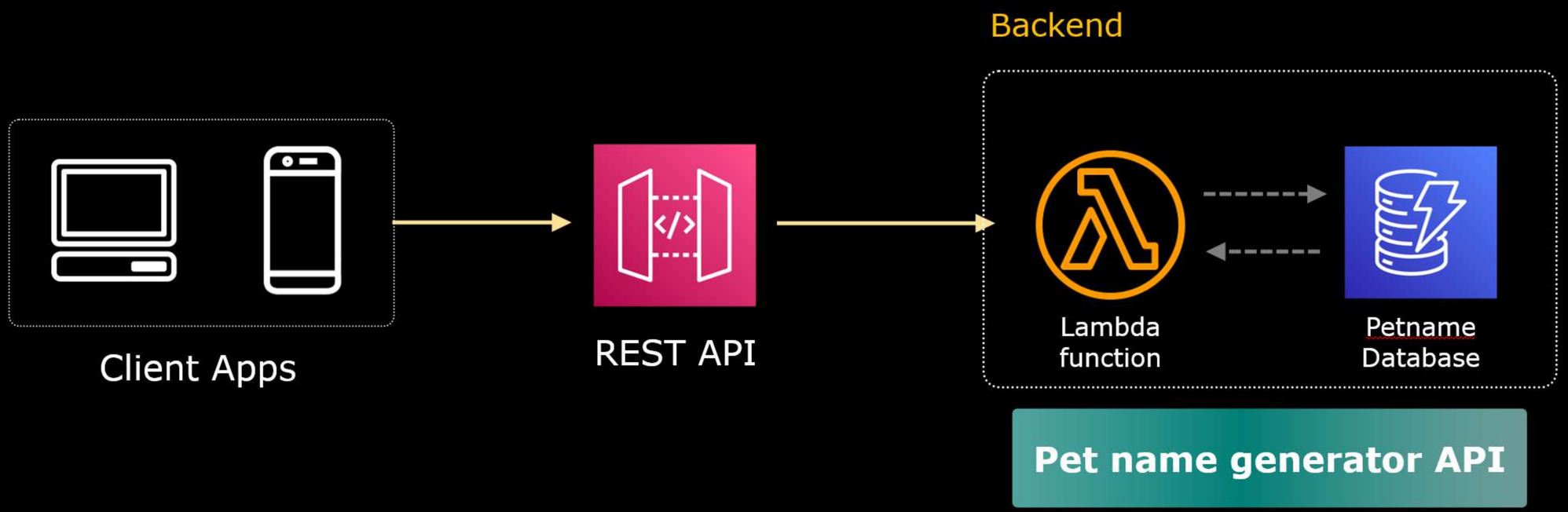
Use case 1: Single point of entry for microservices



Tutorials Dojo

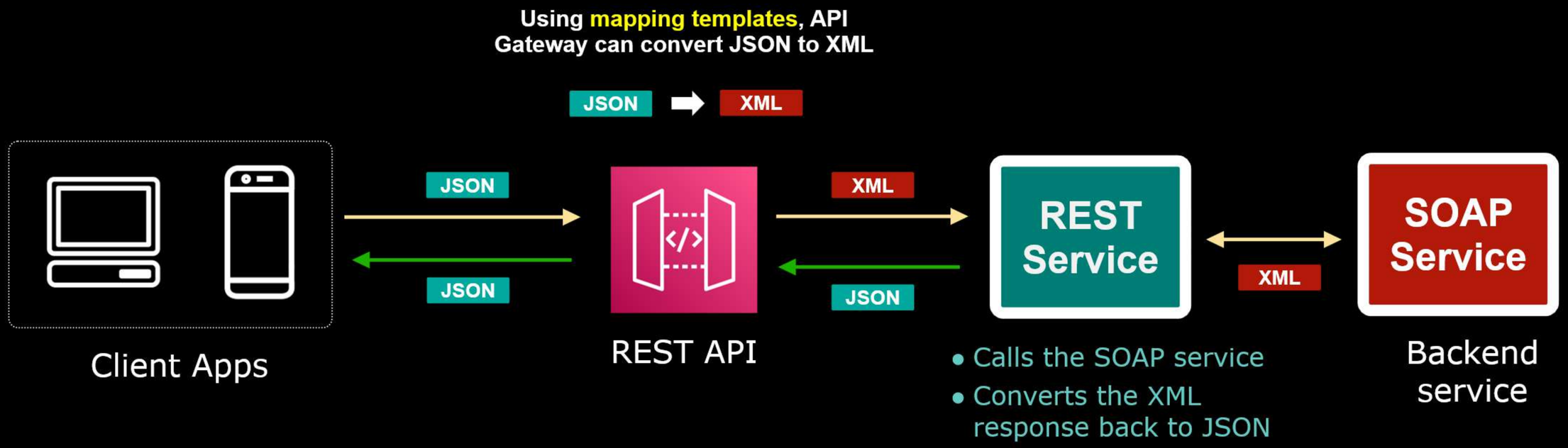
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Use case 2: Widely used in serverless applications



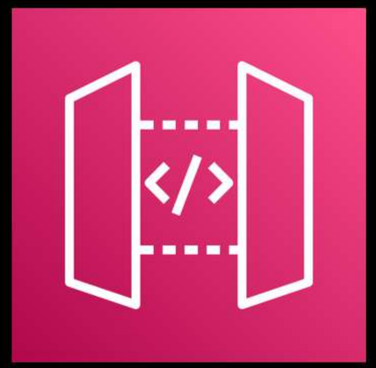
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Use case 3: Modernize legacy applications



Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon API Gateway

- You can choose between a REST API, HTTP API, and a WebSocket API endpoint

1. **REST API**

   - gives you full access to API Gateway features like caching, creating API keys, and usage plans

   - integration with other AWS services

2. **HTTP API**

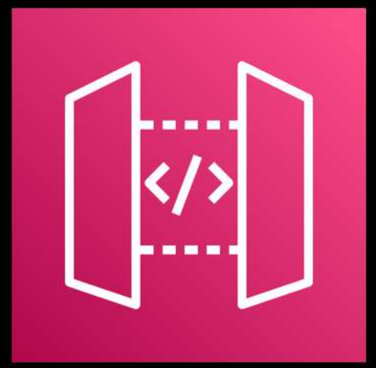
   - cheap and designed for low-latency applications

   - lacks other API Gateway features

3. **WebSocket API**

   - suitable for real-time applications such as chat applications

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



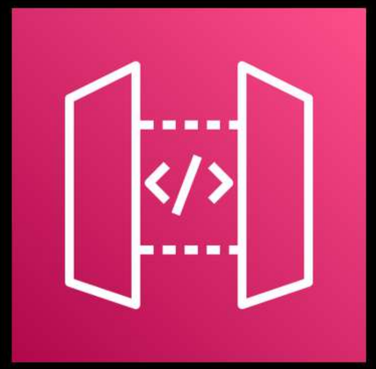
Amazon API Gateway

- Endpoint Types:

- API Gateway does not support unencrypted endpoints
- HTTPS for REST and HTTP API
- WSS for WebSocket API

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon API Gateway

- Endpoint Types:
  1. **Edge-optimized**
     - requests are routed to the nearest CloudFront Point of Presence
     - best for geographically distributed clients
  2. **Regional**
     - requests are routed in the same region where the API is deployed
     - intended for clients in the same region
  3. **Private**
     - APIs can only be accessed from a VPC using a VPC endpoint

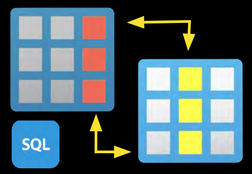
Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon DynamoDB
Overview

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Relational Database

- For applications with well-defined schema that **does NOT change too often**
- Has hundreds or **thousands of tables**
- Multiple **table joins**
- Tables having foreign keys
- Support **complex SQL queries**
- Tables having a **relationship** with other tables
- Has **ACID** properties



Atomicity
Consistency
I solation
Durability

- Perfect for **transactional** workloads



NoSQL Database

- For applications that require a **flexible schema** that changes too often
- **Does not have any related tables or table joins**
- Usually has **one table** only
- **Provides high throughput and performance** for your global applications
- **Can scale better** than relational databases
- Can be used if you are unsure of the database schema that you will implement
- Suitable if you expect to make a lot of database changes as your website or application grows
- Does not have ACID properties by default

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon DynamoDB

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon DynamoDB

- A fully managed NoSQL database
- **Highly scalable** storage and read/write capacity
- Provides **single-digit millisecond** performance
- **Serverless**
- Highly durable database
- Has built-in security, backup features as well as in-memory caching

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon DynamoDB

- Has the **least amount of operational overhead** than other types of databases
- Eliminates the manual database management tasks, provisioning and scaling activities
- **Capable of automatically scaling its read and write capacity** without the need for advanced capacity planning
- Can be queried using **simple key-value requests** via its APIs
- Can handle ~~**millions of requests per second**~~

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Dynamo

Dynamo: Amazon's Highly Available Key-value Store

Giuseppe DeCandia, Deniz Hastorun, Madan Jampani, Gunavardhan Kakulapati, Avinash Lakshman, Alex Pilchin, Swaminathan Sivasubramanian, Peter Vosshall and Werner Vogels

Amazon.com

ABSTRACT

Reliability at massive scale is one of the biggest challenges we face at Amazon.com, one of the largest e-commerce operations in the world; even the slightest outage has significant financial consequences and impacts customer trust. The Amazon.com platform, which provides services for many web sites worldwide, is implemented on top of an infrastructure of tens of thousands of servers and network components located in many datacenters around the world. At this scale, small and large components fail continuously and the way persistent state is managed in the face of these failures drives the reliability and scalability of the software systems.

This paper presents the design and implementation of Dynamo, a highly available key-value storage system that some of Amazon's core services use to provide an "always-on" experience. To achieve this level of availability, Dynamo sacrifices consistency under certain failure scenarios. It makes extensive use of object versioning and application-assisted conflict resolution in a manner that provides a novel interface for developers to use.

Categories and Subject Descriptors

D.4.2 [**Operating Systems**]: Storage Management; D.4.5 [**Operating Systems**]: Reliability; D.4.2 [**Operating Systems**]: Performance;

General Terms

Algorithms, Management, Measurement, Performance, Design, Reliability.

1. INTRODUCTION

Amazon runs a world-wide e-commerce platform that serves tens of millions customers at peak times using tens of thousands of servers located in many data centers around the world. There are strict operational requirements on Amazon's platform in terms of performance, reliability and efficiency, and to support continuous growth the platform needs to be highly scalable. Reliability is one of the most important requirements because even the slightest outage has significant financial consequences and impacts customer trust. In addition, to support continuous growth, the platform needs to be highly scalable.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
SOSP'07, October 14–17, 2007, Stevenson, Washington, USA.
Copyright 2007 ACM 978-1-59593-591-5/07/0010...$5.00.

One of the lessons our organization has learned from operating Amazon's platform is that the reliability and scalability of a system is dependent on how its application state is managed. Amazon uses a highly decentralized, loosely coupled, service oriented architecture consisting of hundreds of services. In this environment there is a particular need for storage technologies that are always available. For example, customers should be able to view and add items to their shopping cart even if disks are failing, network routes are flapping, or data centers are being destroyed by tornados. Therefore, the service responsible for managing shopping carts requires that it can always write to and read from its data store, and that its data needs to be available across multiple data centers.

Dealing with failures in an infrastructure comprised of millions of components is our standard mode of operation; there are always a small but significant number of server and network components that are failing at any given time. As such Amazon's software systems need to be constructed in a manner that treats failure handling as the normal case without impacting availability or performance.

To meet the reliability and scaling needs, Amazon has developed a number of storage technologies, of which the Amazon Simple Storage Service (also available outside of Amazon and known as Amazon S3), is probably the best known. This paper presents the design and implementation of Dynamo, another highly available and scalable distributed data store built for Amazon's platform. Dynamo is used to manage the state of services that have very high reliability requirements and need tight control over the tradeoffs between availability, consistency, cost-effectiveness and performance. Amazon's platform has a very diverse set of applications with different storage requirements. A select set of applications requires a storage technology that is flexible enough to let application designers configure their data store appropriately based on these tradeoffs to achieve high availability and guaranteed performance in the most cost effective manner.

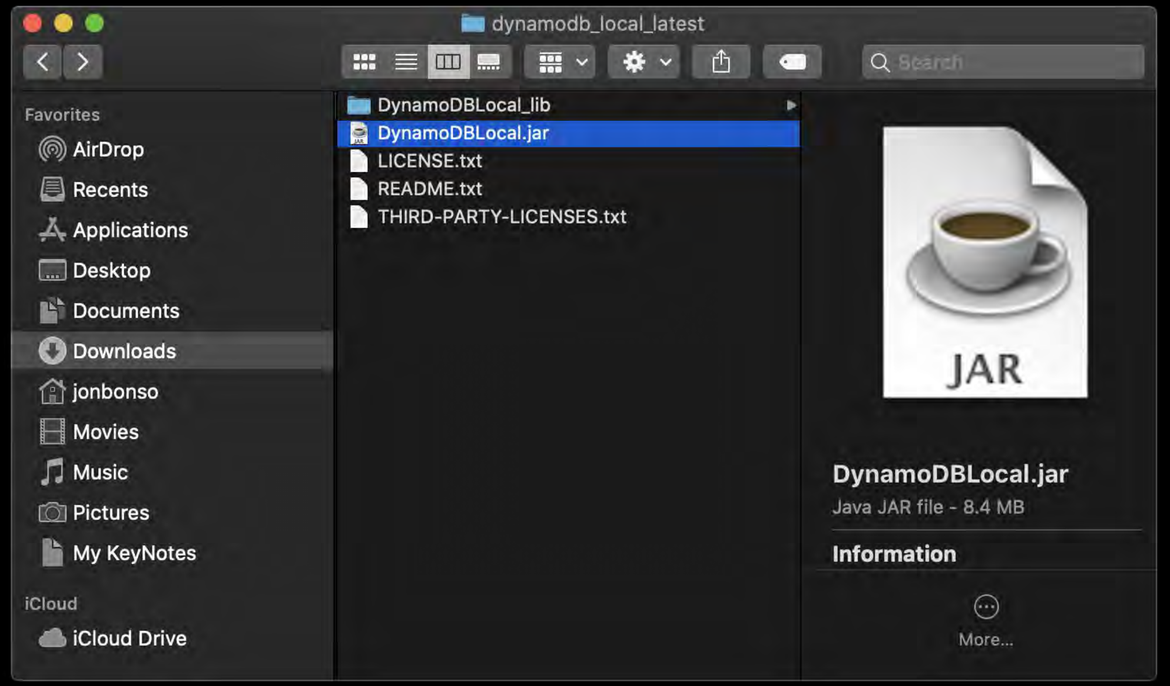
There are many services on Amazon's platform that only need primary-key access to a data store. For many services, such as those that provide best seller lists, shopping carts, customer preferences, session management, sales rank, and product catalog, the common pattern of using a relational database would lead to inefficiencies and limit scale and availability. Dynamo provides a simple primary-key only interface to meet the requirements of these applications.

Dynamo uses a synthesis of well known techniques to achieve scalability and availability: Data is partitioned and replicated using consistent hashing [10], and consistency is facilitated by object versioning [12]. The consistency among replicas during updates is maintained by a quorum-like technique and a decentralized replica synchronization protocol. Dynamo employs

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon DynamoDB



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon DynamoDB

HIGHLY SCALABLE

ULTRA-FAST PERFORMANCE



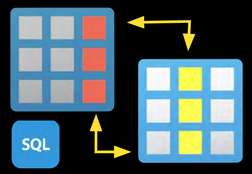
Response times in a matter of **milliseconds** or even in **microseconds!**

DynamoDB Table



- All data is stored in a **single table** only
- Capable of accepting millions of requests per second globally
- Faster and more scalable than traditional relational databases
- **Does not have a relationship** with other DynamoDB tables

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



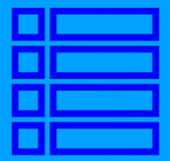
Relational Database



TABLE	TABLE
ROW	ITEM
COLUMN	ATTRIBUTE
PRIMARY KEY	PRIMARY KEY / PARTITION KEY
INDEX	SECONDARY INDEX
VIEW	GLOBAL SECONDARY INDEX
NESTED TABLE/OBJECT	MAP
ARRAY	LIST

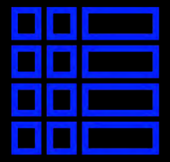
MAKES YOUR QUERIES RUN **FASTER**!

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



LOCAL SECONDARY INDEX

- Queries data over a **single partition** only (localized)
- Supports both eventual consistency or strong consistency
- Can only be added at the same time that you create the base table



GLOBAL SECONDARY INDEX

- Queries data across **all partitions** of the entire table
- Only supports eventual consistency
- Can be added or deleted at any time

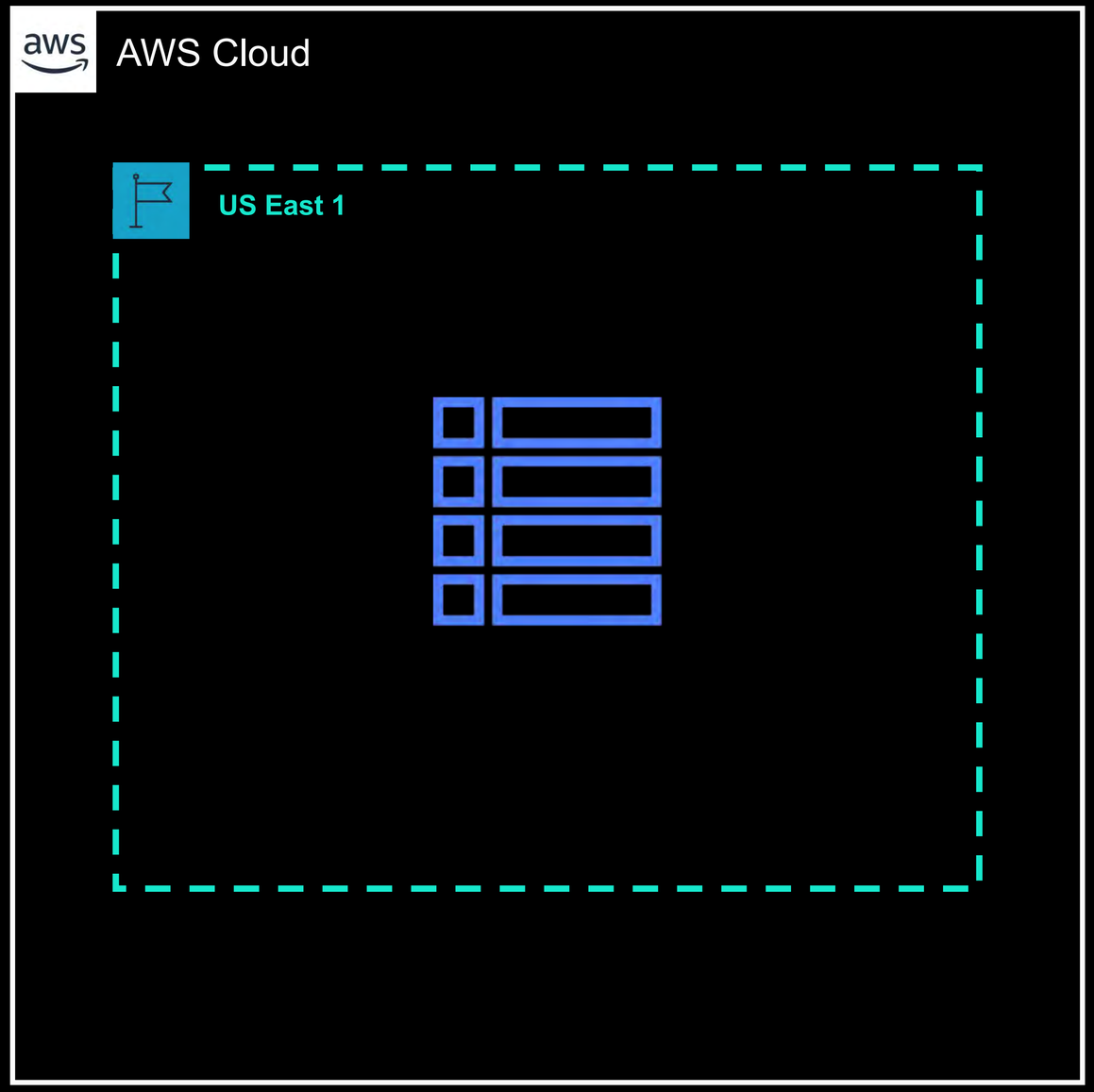
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



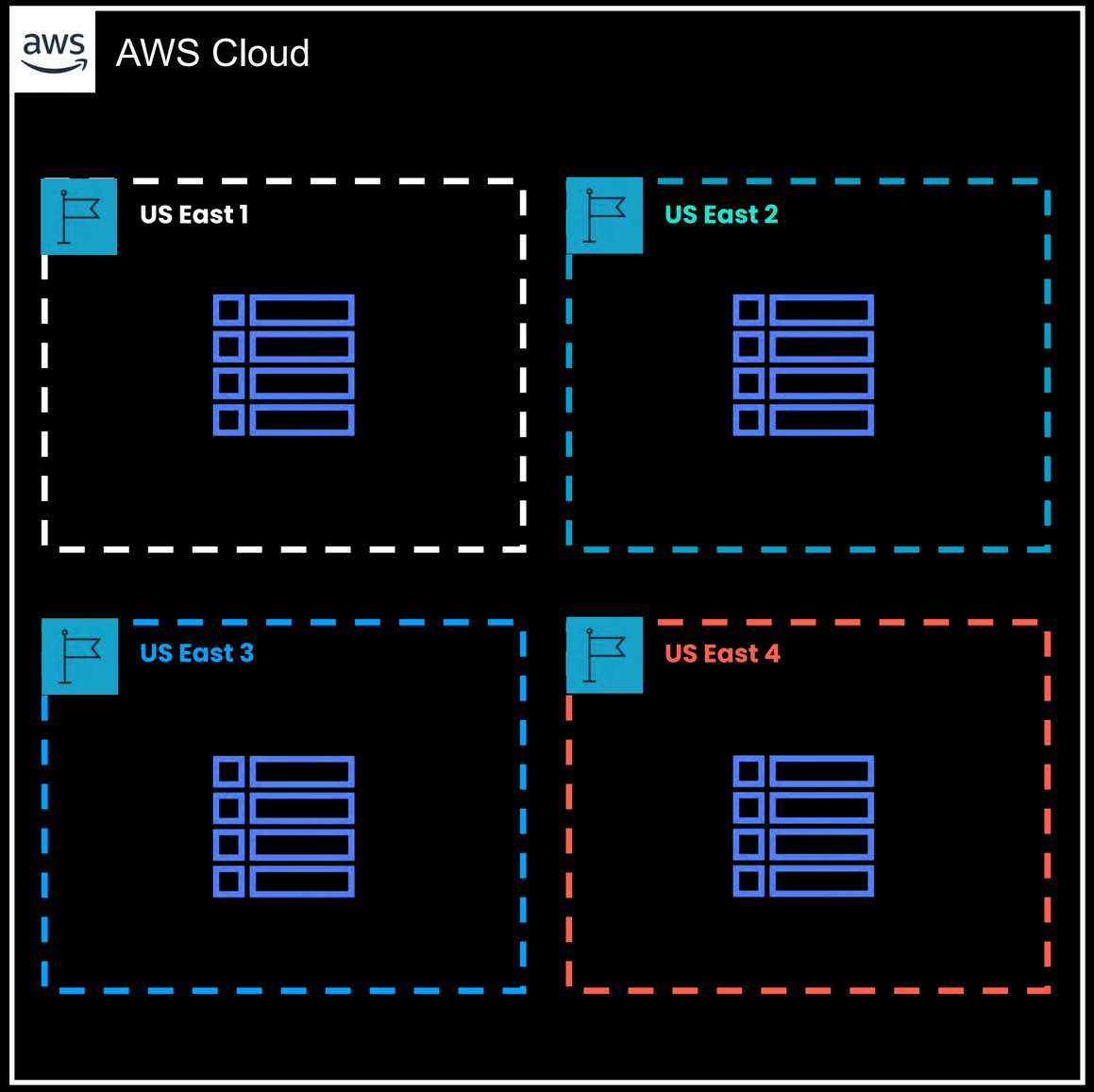
Amazon DynamoDB Features

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Single DynamoDB Table



DynamoDB Global Tables



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon DynamoDB Streams

- A data stream that **captures each and every data change made to the items**
- If an item was added, modified, or deleted, then that item will be included in the DynamoDB stream
- **Can be associated with AWS Lambda**. The function can poll the stream and execute a set of actions whenever it detects new stream records
- Can also be integrated with Kinesis Data Streams
- Important component that **needs to be enabled when using Amazon DynamoDB Global Tables**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon DynamoDB
TTL

- **Automatically expire the items** based on their timestamp and the TTL value that you specify
- TTL stands for **Time to Live**
- Allows you to define a timestamp per item
- Deletes the item from your table after the date and time of the specified timestamp
- **Reduces the number of obsolete data** in your table which can also **lower down your costs**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon DynamoDB
Transactions

- Provides **ACID properties** to your DynamoDB table for your **transactional** workloads
- Provides an **all-or-nothing change** to multiple items both within and across DynamoDB tables
- Consists of **DynamoDB transactional read and write APIs**
  - `TransactWriteItems`
  - `TransactGetItems`
- Empowers you to manage complex business workflows that require adding, updating, or deleting multiple items as an **atomic operation**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon DynamoDB Accelerator (DAX)

- An **in-memory cache** for Amazon DynamoDB that is fully managed and highly available
- Launches a **DAX cluster** that can be run in your default or custom **Amazon VPC**
- Provides response time in **microseconds** and not just in milliseconds
- Delivers fast response times for accessing eventually consistent data
- **Significantly reduces the response times** of your DynamoDB database

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon DynamoDB
Scaling

- **Measured in terms of:**
  - Read Capacity Unit or **RCU**
  - Write Capacity Unit or **WCU**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon DynamoDB Scaling

Provisioned Capacity Mode

- Suitable if your application has **predictable traffic** that doesn't vary over time
- Allows you to **manually set** or provision the RCU and WCU of your DynamoDB table
- **Has an Auto Scaling feature** that you can configure
- Can set the target utilization, minimum provisioned capacity, and maximum provisioned capacity values in the Auto Scaling settings
- At risk of over-provisioning and having unnecessary costs when the incoming traffic is way lower than expected

On-Demand Capacity Mode

- For applications with **inconsistent** traffic or has varying access patterns
- Suitable if you expect that there'll be more **traffic with sharp spikes** in the future
- **No manual Auto Scaling setting** that you can configure. The RCU & WCU are automatically scaled without any intervention
- Can be used if your application has a combination of predictable and **variable traffic**
- Suitable if you have clearly defined access patterns throughout the year but with variable amounts of traffic on certain days only

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon DynamoDB
Security

- Protects your data **both in transit and at rest**
- All data stored in Amazon DynamoDB is fully encrypted at rest by default
- The API calls from your private Amazon EC2 instances that go to DynamoDB can be configured to not traverse the public Internet by creating a **VPC Gateway Endpoint** and adding a new route table entry

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon DynamoDB
Identity & Access Management

```
{
    "Id": "TutorialsDojoPhilippineBooksPolicy1",
    "Version": "2012-10-17",

    "Statement": [
    {
      "Sid": "AllowAccessToBooksTable",
      "Effect": "Allow",

      "Action": [
                "dynamodb:Get*",
                "dynamodb:Query",
                "dynamodb:Scan",
                "dynamodb:BatchWrite*",
                "dynamodb:CreateTable",
                "dynamodb:Delete*",
                "dynamodb:Update*",
                “dynamodb:PutItem" ],

      "Resource": “arn:aws:dynamodb:us-west-2:12345:table/Books"

    }
  ]
}
```

Tutorials Dojo
www.tutorialsdojo.com

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Amazon DynamoDB
Backups

Point-in-time Recovery (PITR)

- **Automated** backup process
- Enables continuous backups to your table
- Allows you to restore your table at a point in time that you specify
- **Entails additional costs**

On-Demand Backup and Restore

- **Manual** backup process
- No continuous backups
- Can only restore to a particular backup that you've taken
- A **cost-effective** yet limited backup option feature for your data

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EBS

VS



Amazon EFS

VS



Amazon S3

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



BLOCK STORAGE



FILE STORAGE



OBJECT STORAGE

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon Elastic **Block** Store



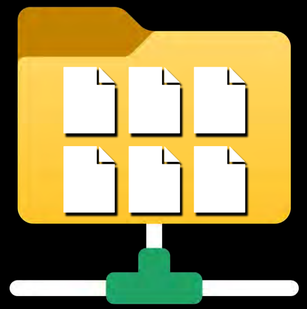
Amazon Elastic **File** System



Amazon Simple Storage Service



BLOCK STORAGE



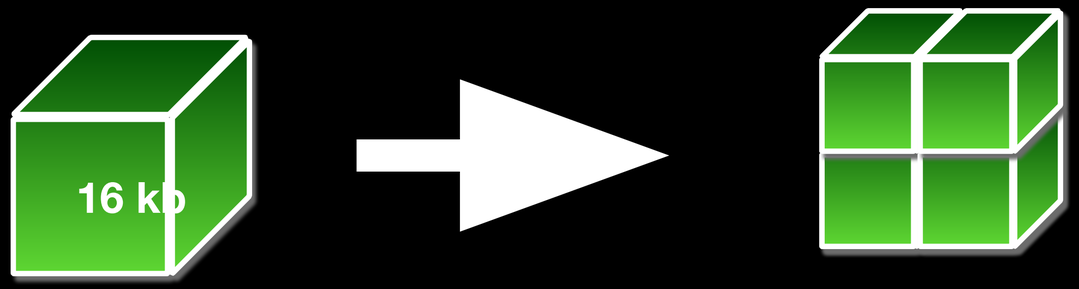
FILE STORAGE



OBJECT STORAGE

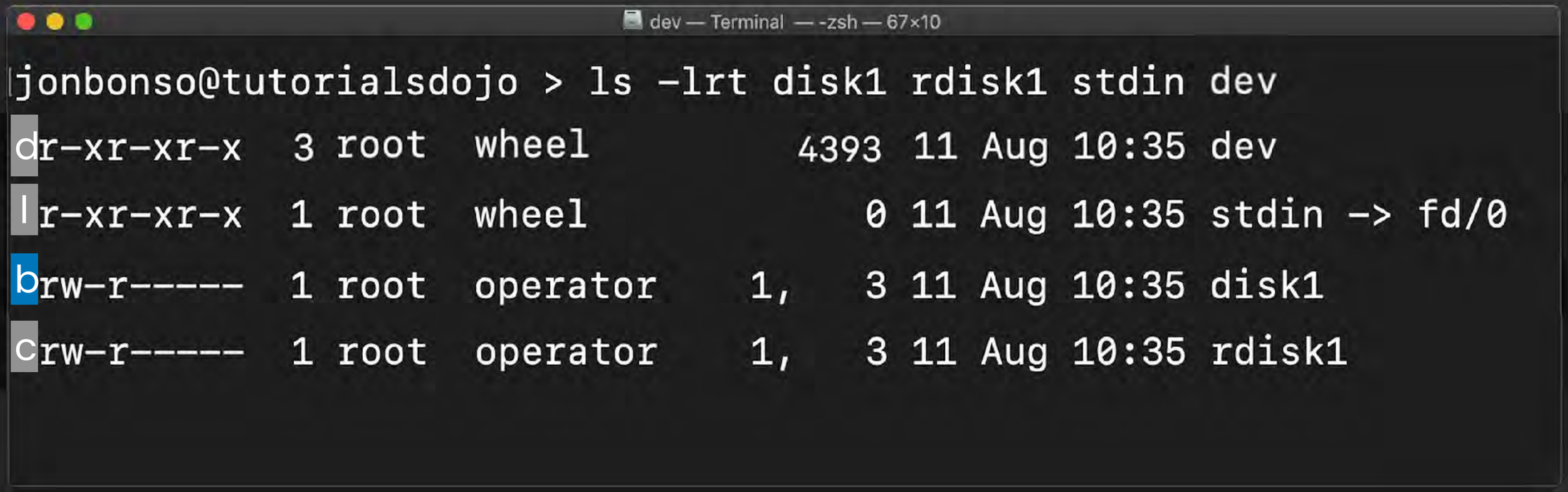
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Total File Size = 16 kb
Block Size = 4 kb

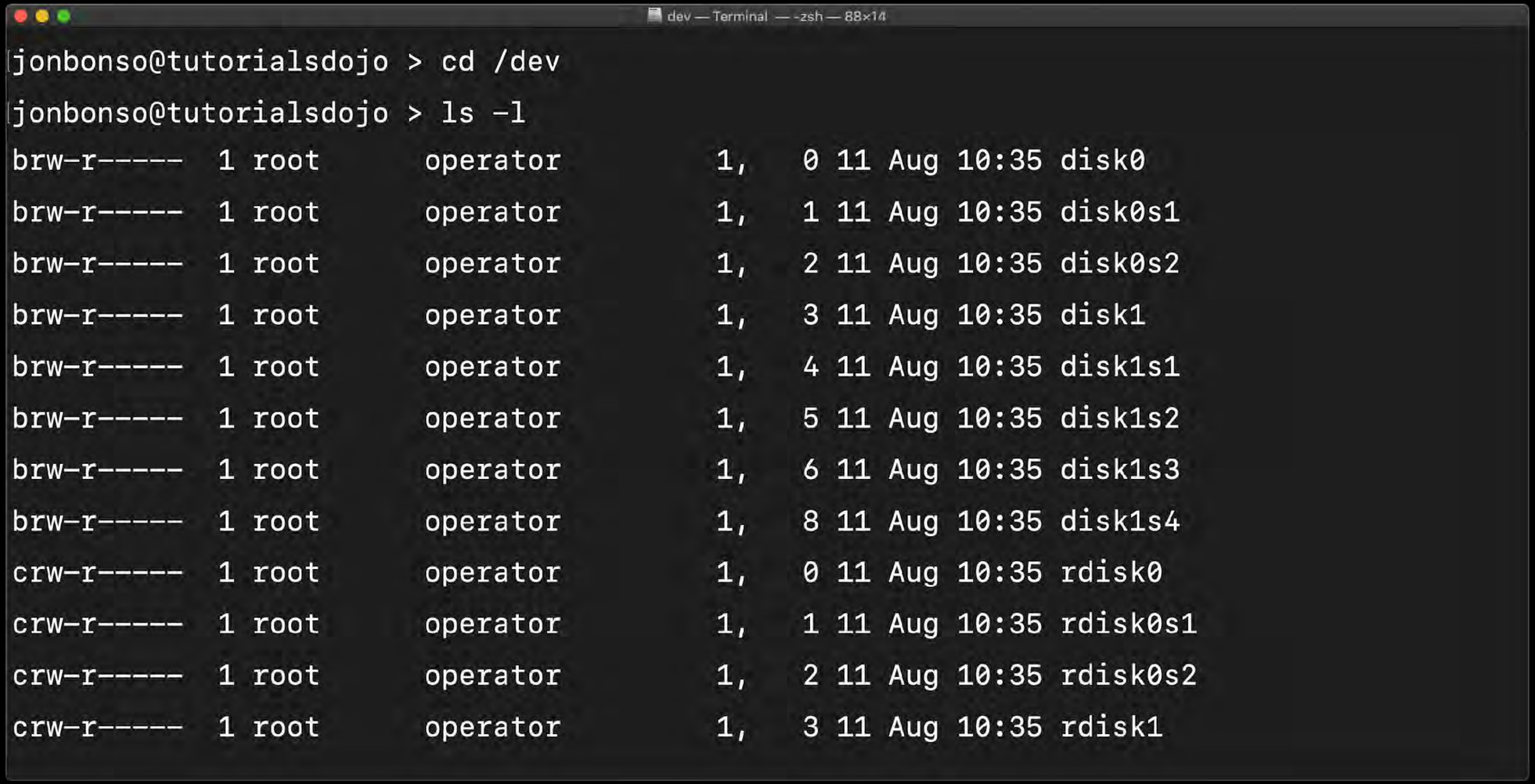


BLOCK STORAGE

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

portal — Terminal — ssh -i tutorialsdojo.pem andresbonifacio@portal.tutorialsdojo.com — 135×24

```
drwxr-xr-x 3 root root         140 Aug  3 05:20 input
brw-rw---- 1 root disk       7,   1 Aug  3 05:20 loop1
brw-rw---- 1 root disk       7,   5 Aug  3 05:20 loop5
brw-rw---- 1 root disk       7,   4 Aug  3 05:20 loop4
brw-rw---- 1 root disk       7,   2 Aug  3 05:20 loop2
brw-rw---- 1 root disk       7,   3 Aug  3 05:20 loop3
brw-rw---- 1 root disk     259,   1 Aug  3 05:21 nvme0n1p1
crw------- 1 root root       5,   1 Aug  3 05:21 console
crw--w---- 1 root tty        4,  64 Aug  3 05:21 ttyS0
crw--w---- 1 root tty        4,   1 Aug  3 05:21 tty1
brw-rw---- 1 root disk       7,   6 Aug 11 21:26 loop6
brw-rw---- 1 root disk       7,   0 Aug 11 21:26 loop0
crw-rw-rw- 1 root tty        5,   2 Aug 12 02:16 ptmx
root@ip-172-31-7-83:/dev#
```



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Lower latency than



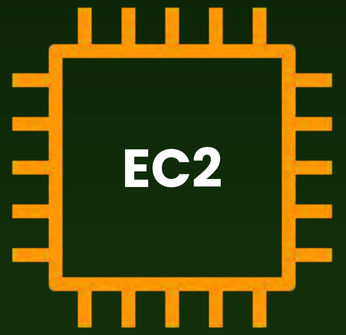
Amazon S3

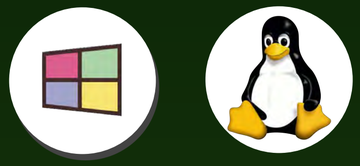


Amazon EBS



Amazon EFS



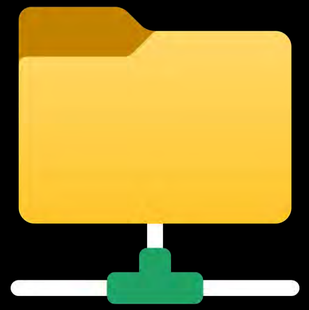


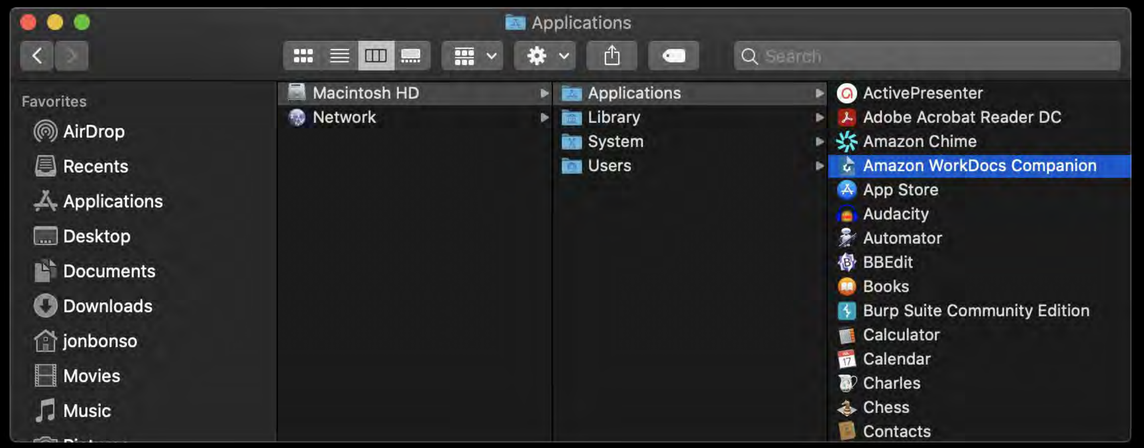
Attached/Mounted to the Amazon EC2 instance

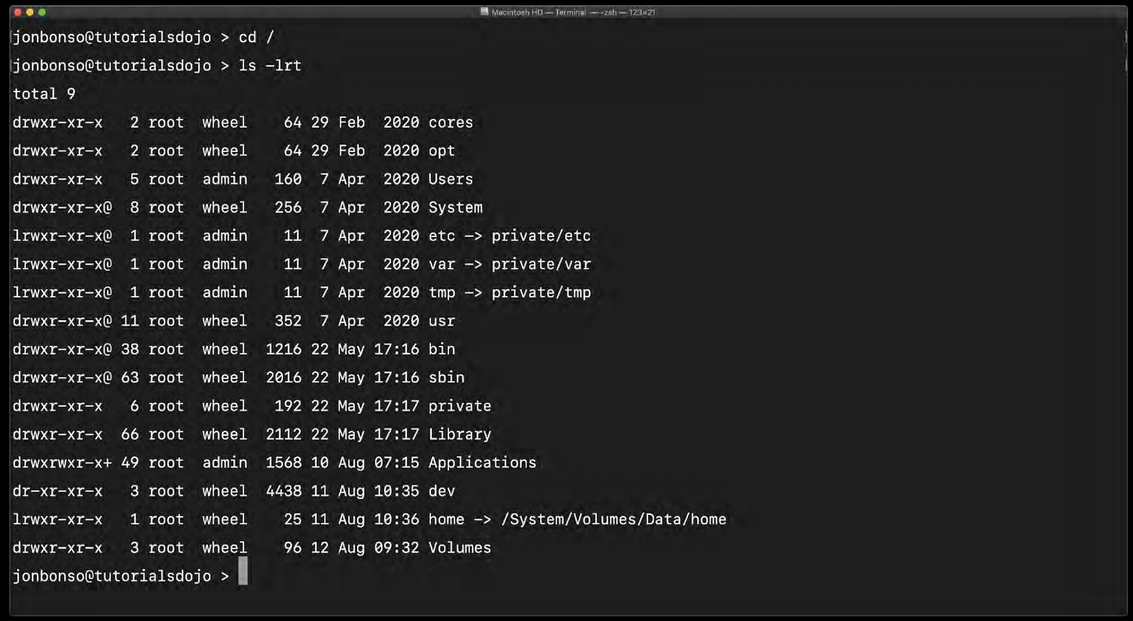
- The block storage or file storage is **physically attached** to the host/server or located in **close proximity**

- The **latency is low** when transferring data between 2 systems

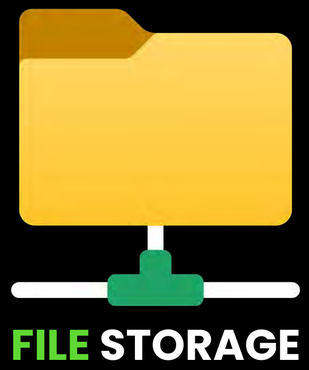
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/







NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Commonly used by multiple servers
- Uses the Portable Operating System Interface (POSIX)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



OBJECT STORAGE

- Every object usually includes a globally unique identifier, its **custom metadata** and the data itself
- Doesn't depend on the operating system of the host/ EC2 instance
- Upload or fetch objects using **RESTful web APIs** and **NOT by mounting it** to the host

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Amazon EBS



Amazon EFS



Amazon S3

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DURABILITY



Amazon EBS

Data is stored redundantly in a **single AZ only**



Amazon EFS



Amazon S3

Data is stored redundantly across multiple AZs

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ACCESS METHOD



Amazon EBS

Usually attached/mounted to a **single EC2 instance**

A single EBS volume can be attached to multiple EC2 instances by using the **Multi-Attach** feature

(available on certain EBS types only)

Two or more applications/ EC2 instances **can't access the exact same file concurrently**



Amazon EFS

Can be mounted to **thousands of EC2 instances or on-premises servers** across multiple AZs

Allows multiple applications or servers to **concurrently access the same files at the same time**



Amazon S3



Invoked via a **REST API** request call

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

SCALABILITY





Amazon EBS



Amazon EFS



Amazon S3

Not **highly scalable**

Both Amazon EFS and Amazon S3 are **highly scalable**

Need to manually resize the EBS Volume to increase storage capacity

Automatically grows and shrinks the file system as you add and remove files

Can store **virtually unlimited amounts of data**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

LATENCY



Amazon EBS



LOWEST



Amazon EFS

MODERATE



Amazon S3

HIGH — *if the request goes through the public Internet*

MODERATE — *if the request goes through the S3 Gateway Endpoint or S3 Interface Endpoint*

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

BACKUPS



Amazon EBS

Back up data using Amazon EBS Snapshots (incremental backups)

Allows you to copy your EBS snapshot to another AWS Region



Amazon EFS

Transfer your file system to another EFS file system using



AWS DataSync

Perform incremental backups of your EFS file system using



AWS Backup



Amazon S3

Cross-Region Replication (CRR)

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DATA ENCRYPTION



Amazon EBS

Encrypt your volume using Amazon EBS Encryption which is powered by



AWS KMS

Amazon EBS Encryption By Default
(Regional Setting)



Amazon EFS

Encryption in Transit

Encryption at Rest



Amazon S3

Client-side Encryption

Server-side Encryption

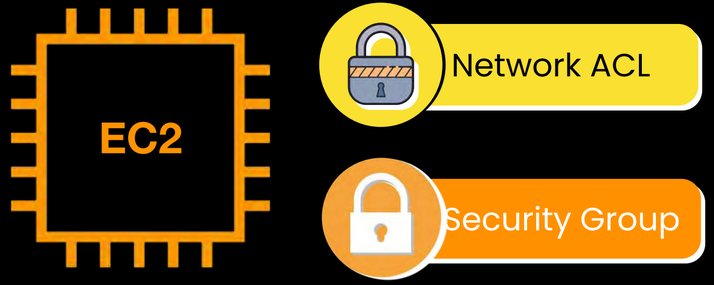
Enforce HTTPS connection by setting up the Bucket Policy

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ACCESS CONTROL

Amazon EBS

Controlled by the associated security groups and Network ACL of the EC2 instance that the volume is mounted to



Amazon EFS

Can associate a security group to the **file system mount target**



NFSv4 endpoint

Amazon S3



Access Control List (ACL)

Bucket Policy

S3 Access Points

S3 Object Lambda Access Points

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

NFSv4 Protocol Support



Amazon EBS



Amazon EFS



Amazon S3



NFSv4 Support

POSIX-compliant

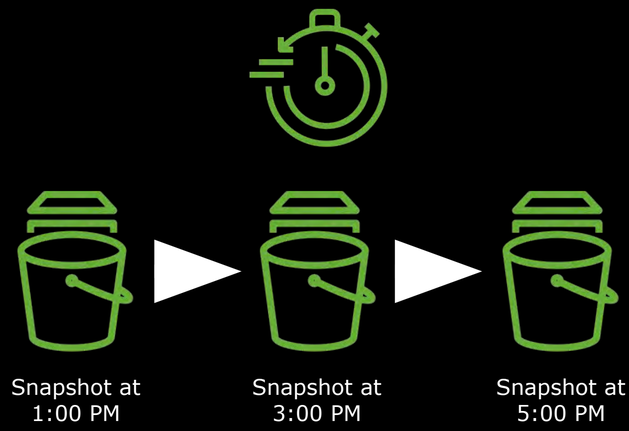


NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

DATA LIFECYCLE

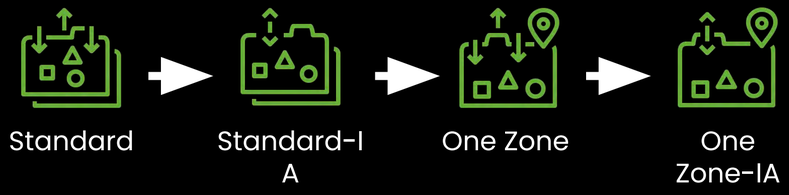
Amazon EBS

Amazon Data Lifecycle Manager (DLM)



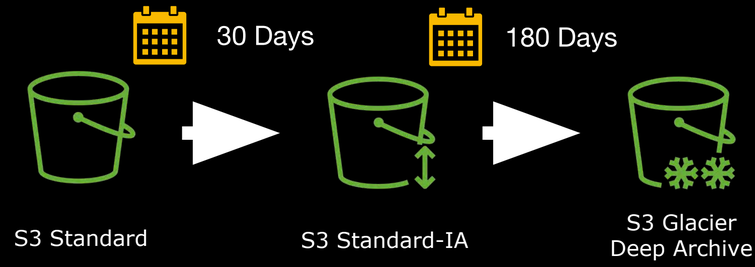
Amazon EFS

Amazon EFS lifecycle management



Amazon S3

Amazon S3 Lifecycle Policy



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

USE CASES



Amazon EBS



Amazon EFS



Amazon S3

For storing **dynamic** data that are **frequently accessed and updated**

For static data or for files that are NOT usually modified regularly

LOWEST Latency

A storage system accessed by multiple servers that **need concurrent access to the same set of files at the same time**

POSIX-compliant

For a cost-effective & serverless static web hosting that can be integrated with:



Amazon CloudFront

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Network Access Control List
(Network ACL)

VS



Security Group

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Network ACL



Security Group

- Created by default when you launch a new VPC and on your default VPC
- Acts as a virtual firewall that protects your AWS resources from unauthorized traffic
- Inbound & Outbound rules can be set to have one IP address or a CIDR range as a source
- Allows you to control the incoming and outgoing traffic to and from your network

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Network ACL



Security Group

Rule #	Type	Protocol	Port range	Source	Allow/Deny
10	HTTP	TCP	80	172.31.1.2/32	DENY
20	HTTPS	TCP	443	192.0.2.0/24	DENY
30	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
40	All IPv6 traffic	All	All	::/0	ALLOW

Ephemeral Ports

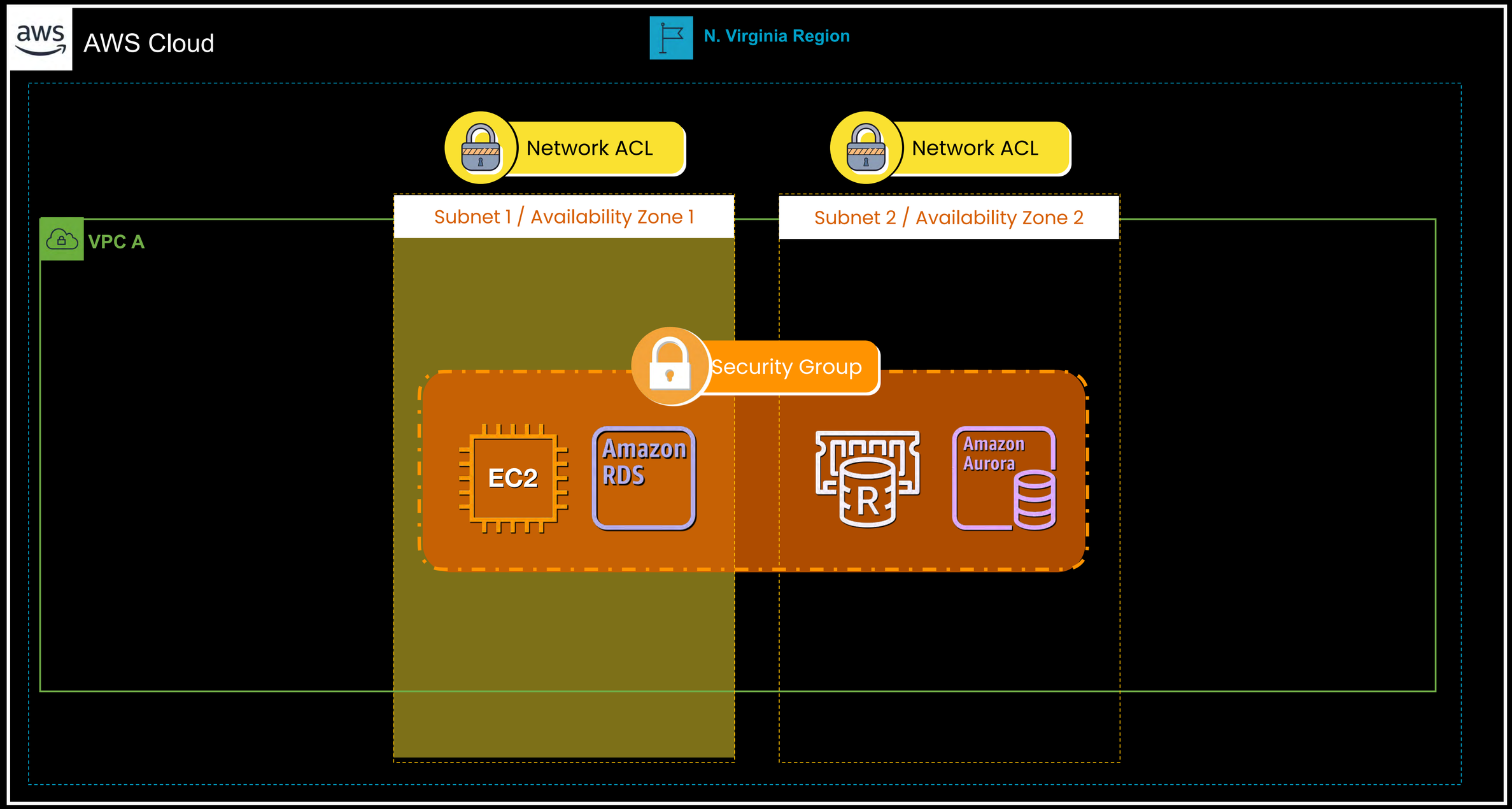


Outbound Rules

- 1024 – 65535
- 32768 – 61000
- 49152 – 65535



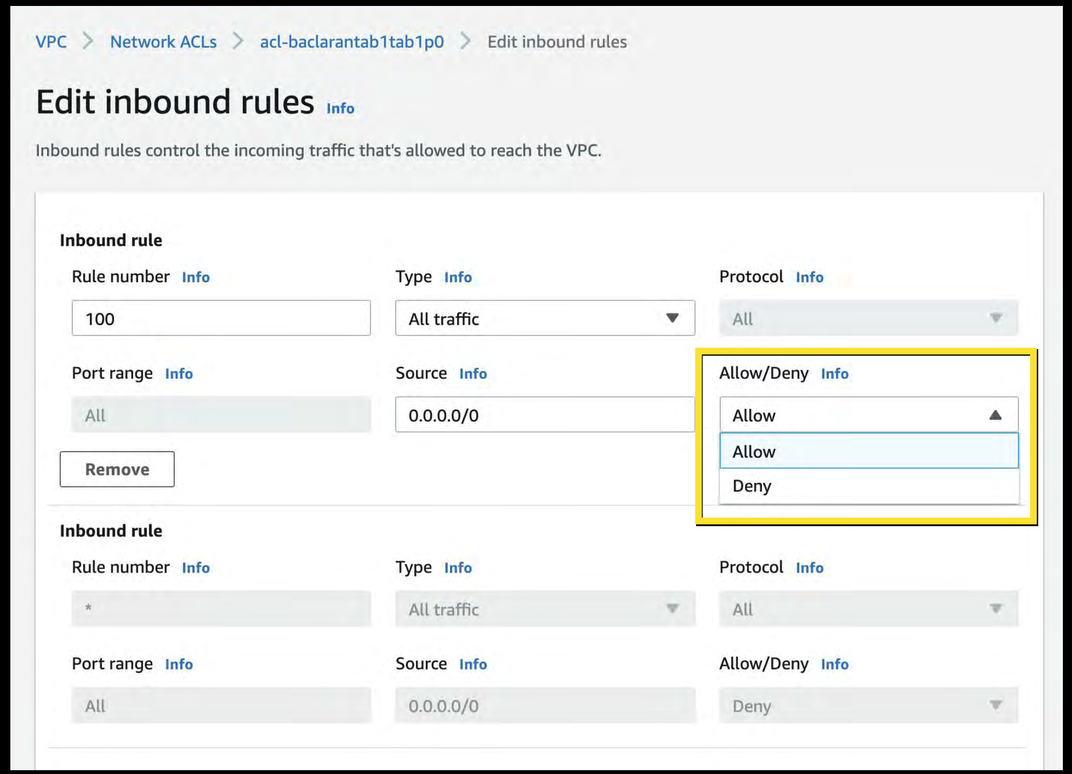
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

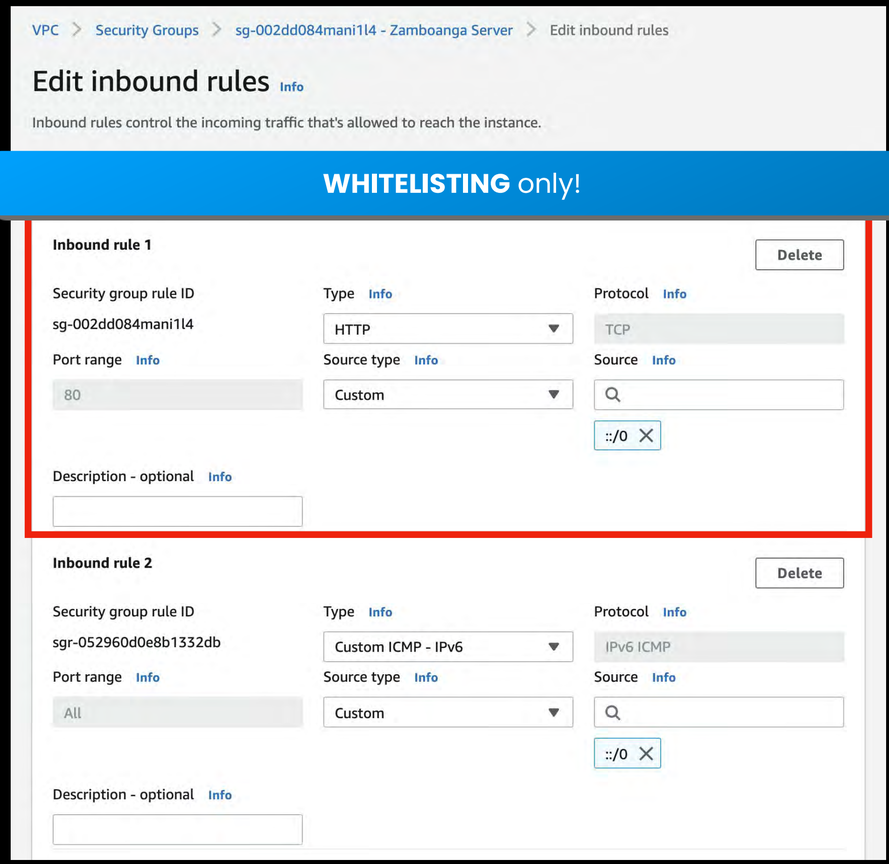
Network ACL

- Can explicitly DENY traffic



Security Group

- Cannot explicitly DENY traffic



Tutorials Dojo
www.tutorialsdojo.com

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Network ACL

STATELESS



Security Group

STATEFUL

STATE

STATEFUL

STATELESS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Network ACL

STATELESS

- Does not track the status of the request
- The inbound traffic that has already been permitted before is still subject to the rules for the outbound traffic, and vice versa
- Provides a more fine-grained control to configure both the inbound and outbound rules of your Network ACL



Security Group

STATEFUL

- Tracks all the status of the incoming requests
- If a traffic is a response to a particular request, then it will be allowed automatically regardless of any rules in your Outbound Rules
- It is aware if the outgoing traffic is:
  - Initiated from the EC2 instance itself
  - A response to the request that was initiated externally
- Its Outbound Rule can filter:
  - An API call initiated by an application hosted in the EC2 instance
  - A scheduled OS Patch that is initiated by the EC2 instance which automatically fetches updates from a designated repository

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Network ACL

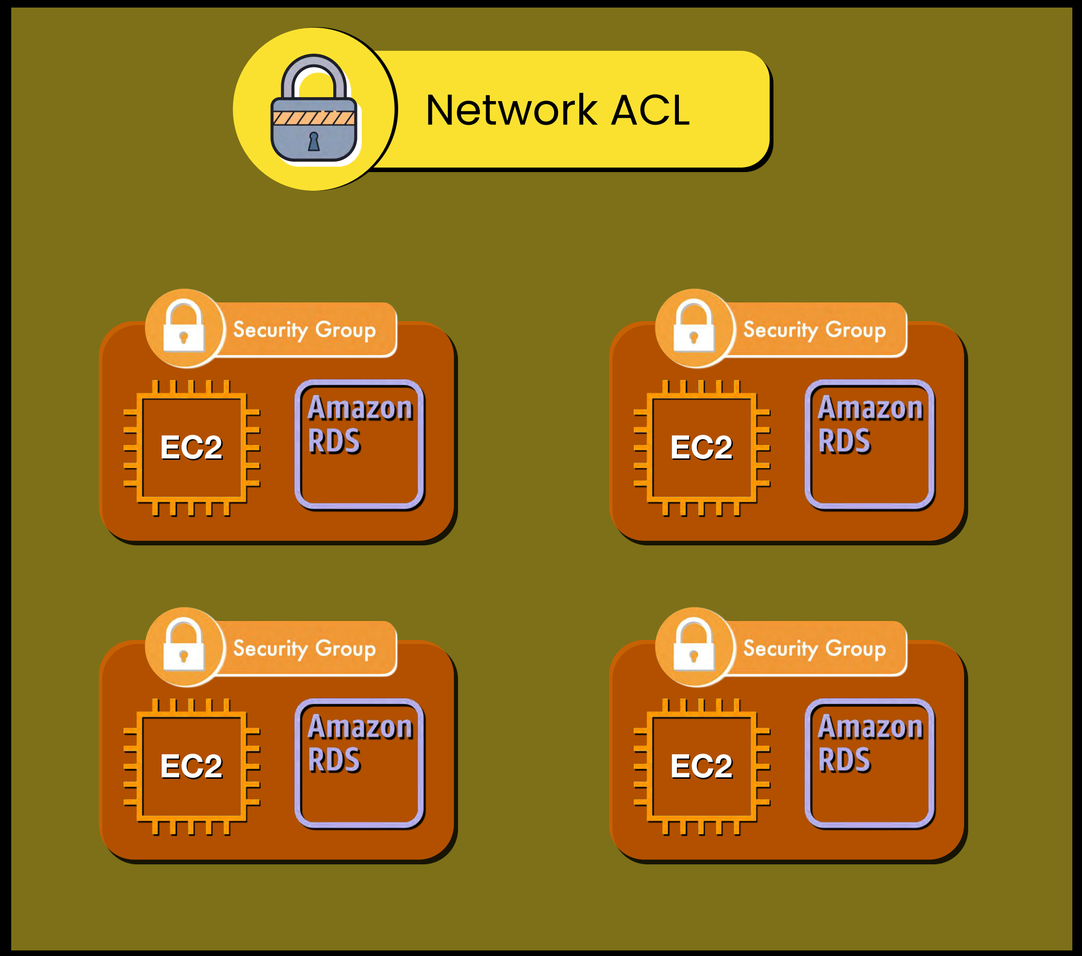
- Each rule has a corresponding rule number
- Evaluates the rules in order, starting with the lowest numbered rule



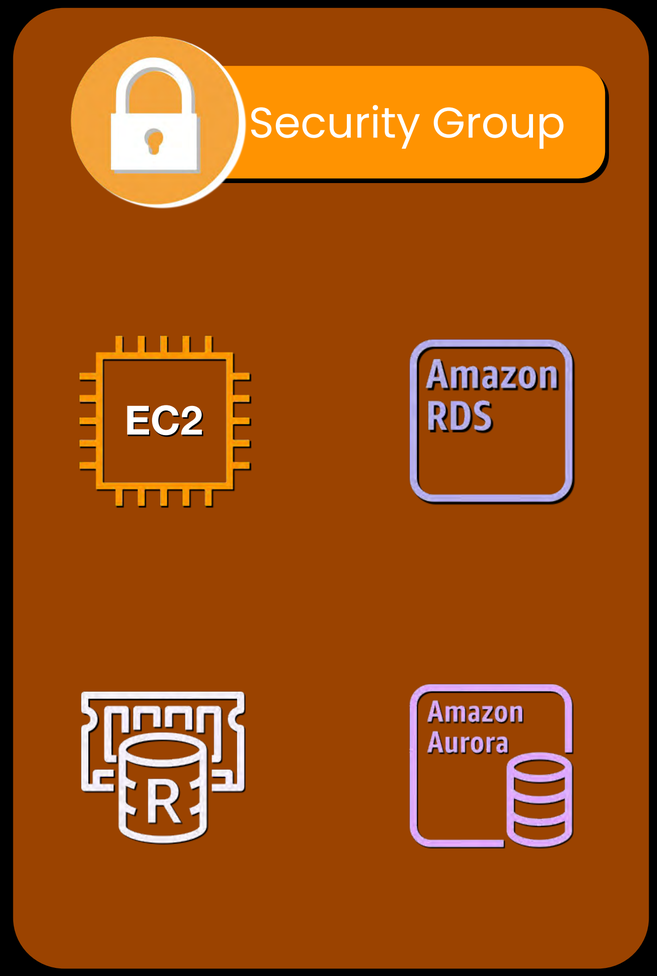
Security Group

- No rule number
- Evaluates ALL of the rules at the same time *(no order of precedence)*

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



- Applies the rules to all EC2 instances and other AWS resources in the subnets that it's associated with



- Applies the rules to a single EC2 instance only or to a group of AWS resources where it is associated with

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Network ACL

Ephemeral Ports



Outbound Rules

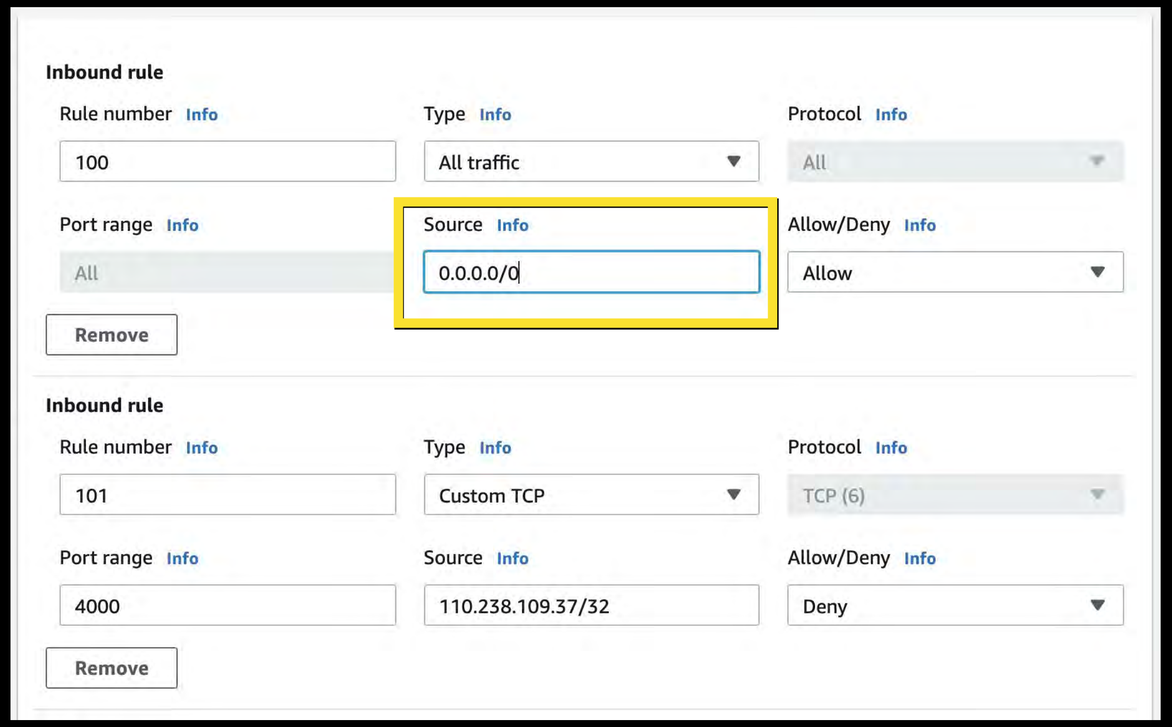
?	1024 - 65535
	32768 - 61000
	49152 - 65535

Security Group

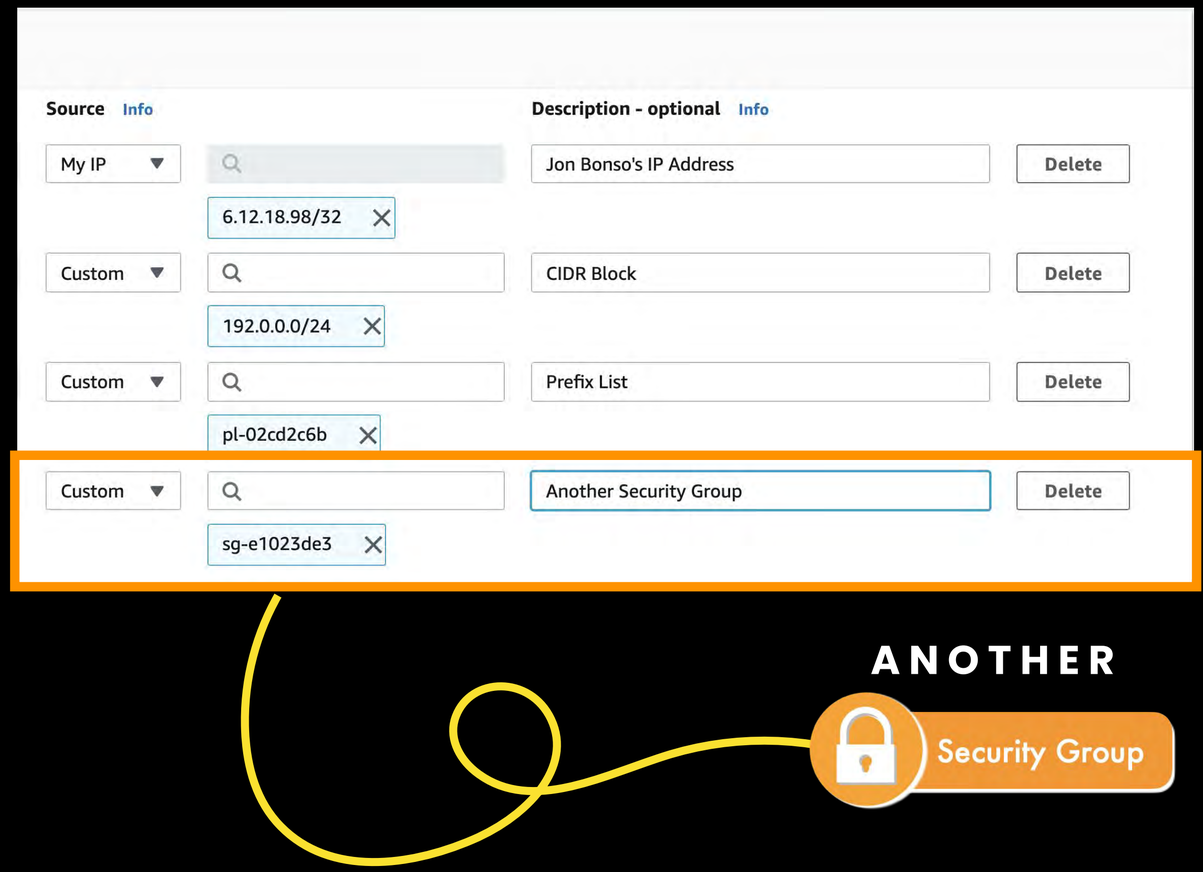
- Does NOT use Ephemeral Ports

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Network ACL



Security Group



ANOTHER

Security Group

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

INTEGRATION



AWS Storage Gateway

V

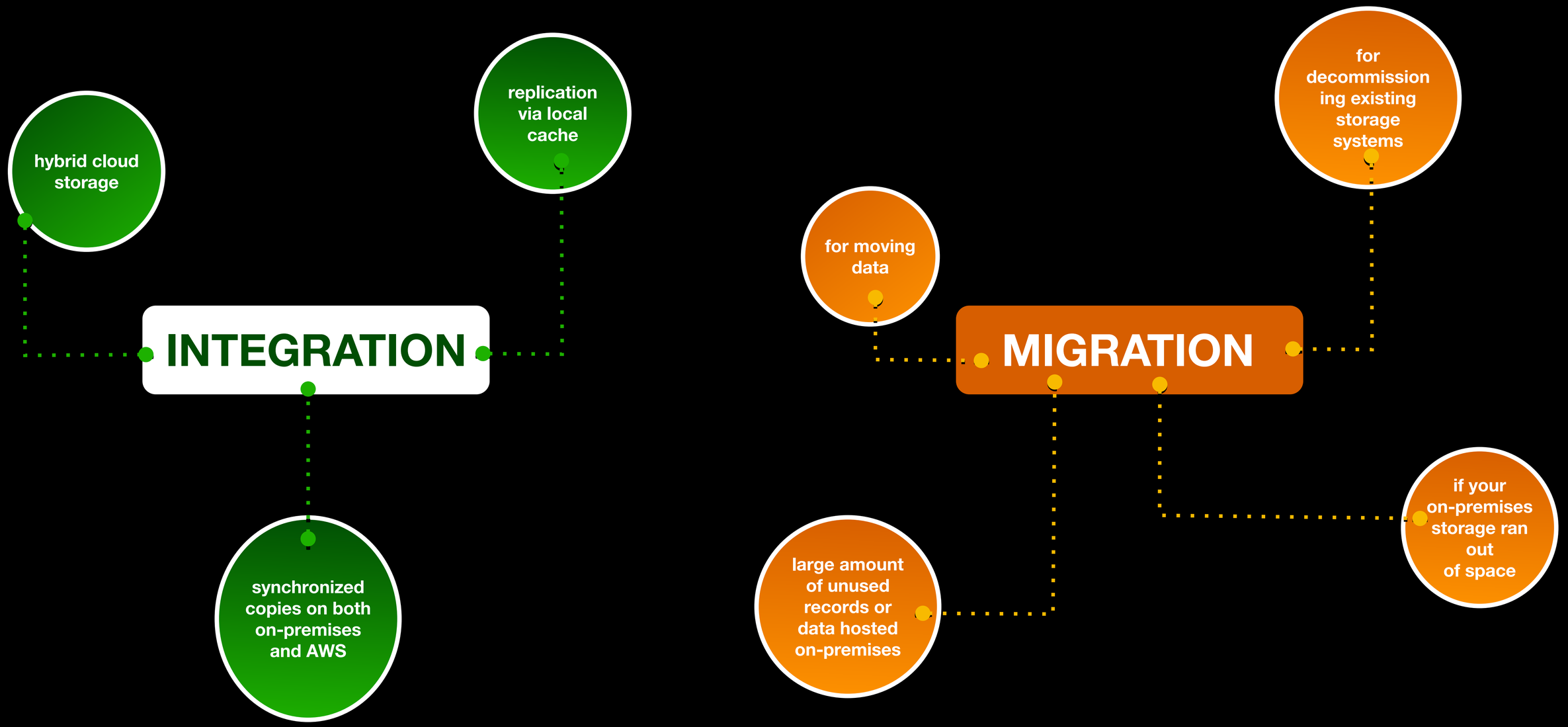
S

MIGRATION



AWS DataSync

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

REPLICATE DATA

INTEGRATION

MOVE DATA

MIGRATION



AWS Storage Gateway



AWS DataSync

On-premises data center

VM



DataSync Agent

Storage Area Network

On-premises data will still be actively used

On-premises data would not be utilized anymore*/will be decommissioned*

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



File Gateway

VS



Volume Gateway

VS

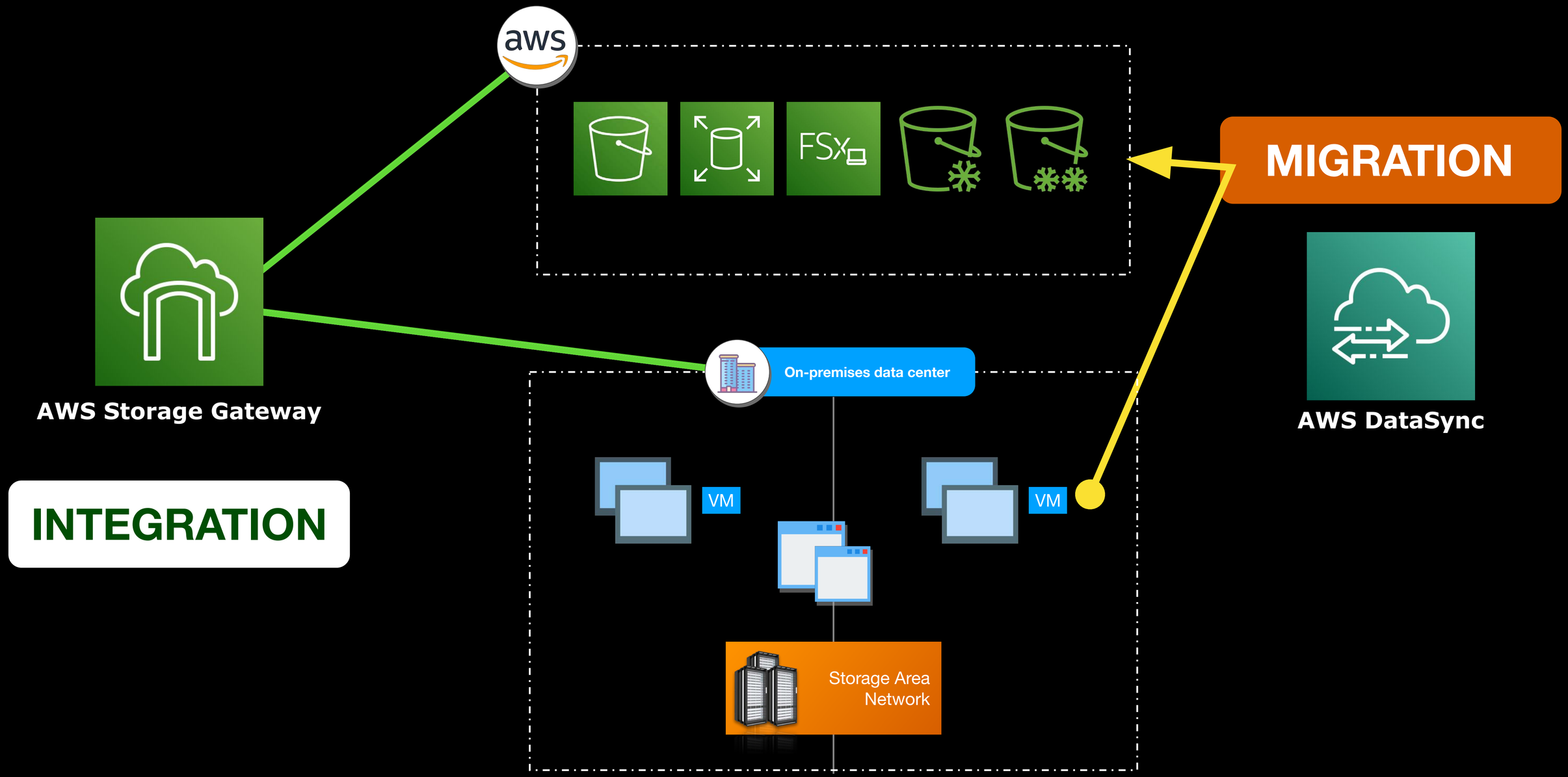


Tape Gateway



AWS Storage Gateway Types Comparison

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



AWS Storage Gateway Types



File Gateway



Volume Gateway



Tape Gateway

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

File Gateway

*File storage

NFS

- Also known as **Amazon S3 File Gateway**
- Stores data in: Amazon S3
- Provides a **local cache** for low-latency access to your most recently used data

SMB

- Also known as **Amazon FSx File Gateway**
- Stores data in: Amazon FSx for Windows File Server
- Provides a low-latency on-premises access to **Windows SMB file shares** of the Amazon FSx for Windows File Server service in AWS

Volume Gateway

*Block storage

CACHED

- Uses **Amazon S3** as the primary storage
- Stores a **subset** of frequently accessed data locally

STORED

- Retains the **entire** dataset in your on-premises data center
- Asynchronously backs up your data to Amazon S3

Tape Gateway

* Tape storage

GLACIER POOL

Amazon S3 Glacier

DEEP ARCHIVE POOL

Amazon S3 Glacier Deep Archive

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

File Gateway	Volume Gateway	Tape Gateway
FSx Can be integrated with: Microsoft **Active Directory** AWS Managed Microsoft AD	**No Active Directory Support**	**No Active Directory Support**

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



File Gateway



Volume Gateway



Tape Gateway

NFS

iSCSI

SMB

VTL

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

File Gateway

Volume Gateway

Tape Gateway



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

	Size value	Encryption	Versioning	Automatic Rotation	Cost
 AWS Systems Manager Parameter Store	**STANDARD** • Up to 4KB per entry **ADVANCED** • Up to 8KB per entry				
 AWS Secrets Manager	• **Up to 64KB per secret** • **Suitable for storing certificates**				

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

	Size value	Encryption	Versioning	Automatic Rotation	Cost
 AWS Systems Manager Parameter Store	**STANDARD** • Up to 4KB per entry **ADVANCED** • Up to 8KB per entry	• Uses **AWS KMS** for encryption • Encryption is **optional**			
 AWS Secrets Manager	• **Up to 64KB per secret** • **Suitable for storing certificates**	• Uses **AWS KMS** for encryption • Encryption is **enforced** • Storing plaintext data is not possible			

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

	Size value	Encryption	Versioning	Automatic Rotation	Cost
 AWS Systems Manager Parameter Store	**STANDARD** • Up to 4KB per entry **ADVANCED** • Up to 8KB per entry	• Uses **AWS KMS** for encryption • Encryption is **optional**	• One version can **only be** active at any given time		
 AWS Secrets Manager	• **Up to 64KB per secret** • **Suitable for storing certificates**	• Uses **AWS KMS** for encryption • Encryption is **enforced** • Storing plaintext data is not possible	• Multiple versions **can exist at the same time** when performing secret rotation		

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

	Size value	Encryption	Versioning	Automatic Rotation	Cost
AWS Systems Manager Parameter Store	**STANDARD** • Up to 4KB per entry **ADVANCED** • Up to 8KB per entry	• Uses **AWS KMS** for encryption • Encryption is **optional**	• One version can **only be** active at any given time	⊘	
AWS Secrets Manager	• **Up to 64KB per secret** • **Suitable for storing certificates**	• Uses **AWS KMS** for encryption • Encryption is **enforced** • Storing plaintext data is not possible	• Multiple versions **can exist at the same time** when performing secret rotation	• Can **rotate secrets automatically** • **Cross-account access** is supported • Can **generate random password**	

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

	Size value	Encryption	Versioning	Automatic Rotation	Cost
 AWS Systems Manager Parameter Store	**STANDARD** • Up to 4KB per entry **ADVANCED** • Up to 8KB per entry	• Uses **AWS KMS** for encryption • Encryption is **optional**	• One version can **only be** active at any given time		• It is **cheaper** Standard - FREE Advanced - $0.05/ parameter/month • $0.05 / 10,000 API calls
 AWS Secrets Manager	• **Up to 64KB per secret** • **Suitable for storing certificates**	• Uses **AWS KMS** for encryption • Encryption is **enforced** • Storing plaintext data is not possible	• Multiple versions **can exist at the same time** when performing secret rotation	• Can **rotate secrets automatically** • **Cross-account access** is supported • Can **generate random password**	• **More expensive** • $0.4/secret/month • $0.05 / 10,000 API calls

Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Exam Taking Strategies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Topics in SysOps Exam

- deploying and managing resources
- operating workloads
- security controls
- compliance requirements

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

?

?

?



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



Breakdown the question for better and faster decision-making process using:

K EYWORDS

E LIMINATION

E VALUATION

P ATTERNS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

KEYWORDS

keywords and keyphrases

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

PRIMARY SECONDARY

Question #01

The development team of a software company has just released the next version of their application in production. It is hosted in an Amazon ECS Cluster with RDS as its database and uses Route 53 as its DNS service. The new version of the application has undergone testing and now needs to be promoted to production from a separate environment. In order to have a smooth transition and avoid any unwanted outages, you need an initial set of traffic to be directed to the new version of the application for testing before doing the final cutover.

Which of the following will you implement on Route 53 to achieve this?

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

PRIMARY SECONDARY

Question #01

The development team of a software company has just released the next version of their application in production. It is hosted in an Amazon ECS Cluster with RDS as its database and uses Route 53 as its DNS service. The new version of the application has undergone testing and now needs to be promoted to production from a separate environment. In order to have a smooth transition and avoid any unwanted outages, you need an initial set of traffic to be directed to the new version of the application for testing before doing the final cutover.

Which of the following will you implement on Route 53 to achieve this?

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

PRIMARY SECONDARY

Question #01

The development team of a software company has just released the next version of their application in production. It is hosted in an Amazon ECS Cluster with RDS as its database and uses Route 53 as its DNS service. The new version of the application has undergone testing and now needs to be promoted to production from a separate environment. In order to have a smooth transition and avoid any unwanted outages, you need an initial set of traffic to be directed to the new version of the application for testing before doing the final cutover.

Which of the following will you implement on Route 53 to achieve this?

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

PRIMARY SECONDARY

Question #01

The development team of a software company has just released the next version of their application in production. It is hosted in an Amazon ECS Cluster with RDS as its database and uses Route 53 as its DNS service. The new version of the application has undergone testing and now needs to be promoted to production from a separate environment. In order to have a smooth transition and avoid any unwanted outages, you need an initial set of traffic to be directed to the new version of the application for testing before doing the final cutover.

Which of the following will you implement on Route 53 to achieve this?

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

ELIMINATION

eliminate irrelevant options

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Eliminating options help you:





save time



increase chances of getting the correct answer!



work with unfamiliar options

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Question #01

A leading advertising company is using Lambda to run a serverless application in AWS. The application processes transactions on an Amazon RDS database instance with MySQL support. As the company grows, the number of users has started to increase. As a result, your Lambda function is beginning to receive "too many connections" errors when attempting to connect to the RDS database. When the SysOps administrator checked the database settings, the max_connections parameter is already set to the maximum possible value.

What step should the Sysops administrator perform to resolve the issue?

maximum connection errors

- Increase the value of the max_connect_errors parameter to 10 to allow more errors.
- ~~Raise the Lambda function's provisioned concurrency setting to a higher value.~~
- Enable Multi-AZ setting for the RDS database instance.
- Provision an Amazon RDS Proxy and update the database connection string in your Lambda function.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Question #01

A leading advertising company is using Lambda to run a serverless application in AWS. The application processes transactions on an Amazon RDS database instance with MySQL support. As the company grows, the number of users has started to increase. As a result, your Lambda function is beginning to receive "too many connections" errors when attempting to connect to the RDS database. When the SysOps administrator checked the database settings, the max_connections parameter is already set to the maximum possible value.

What step should the Sysops administrator perform to resolve the issue?

maximum connection errors

- ~~Increase the value of the max_connect_errors parameter to 10 to allow more errors.~~
- ~~Raise the Lambda function's provisioned concurrency setting to a higher value.~~
- Enable Multi-AZ setting for the RDS database instance.
- Provision an Amazon RDS Proxy and update the database connection string in your Lambda function.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

EVALUATE

evaluate which among the remaining options makes sense

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

What do you need to evaluate?



Strong knowledge on fundamental concepts in SysOps is required.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Question #01

A leading advertising company is using Lambda to run a serverless application in AWS. The application processes transactions on an Amazon RDS database instance with MySQL support. As the company grows, the number of users has started to increase. As a result, your Lambda function is beginning to receive "too many connections" errors when attempting to connect to the RDS database. When the SysOps administrator checked the database settings, the max_connections parameter is already set to the maximum possible value.

What step should the Sysops administrator perform to resolve the issue?

maximum connection errors

- Increase the value of the max_connect_errors parameter to 10 to allow more errors.
- ~~Raise the Lambda function's provisioned concurrency setting to a higher value.~~
- Enable Multi-AZ setting for the RDS database instance.
- ✓ Provision an Amazon RDS Proxy and update the database connection string in your Lambda function.

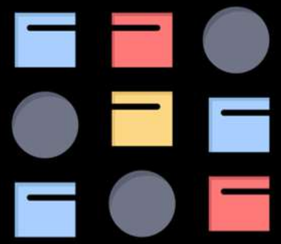
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

PATTERNS

patterns and anti-patterns

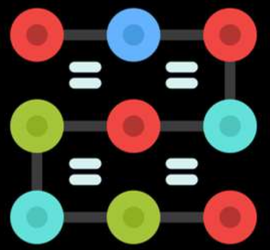
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

PATTERNS



recommended use case for AWS services

ANTI-PATTERNS



anything that goes against the recommended use case for AWS services

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Question #02

Due to the tight deadline of your project, your team needs to quickly update an RDS instance, deploy a new Application Load Balancer and launch multiple EC2 instances on your current CloudFormation stack. You want to be able to preview the proposed changes to your stack carefully to make sure the new infrastructure is correctly provisioned as you planned and to avoid any possible service disruptions.

Which of the following is the most suitable solution that you have to implement to meet the requirement?

anti-pattern

- ~~Update the CloudFormation stack directly. The proposed changes will be shown before provisioning the stack.~~
- ~~Use CloudFormation StackSets to review the proposed changes to be made on your stack.~~
- ✓ Use Change Sets when updating stacks to view the proposed changes.
- ~~Use Nested Stacks to create a side-by-side comparison of your current stack and the proposed changes.~~

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Question #03

A shoe company provisioned an Amazon Aurora database cluster with MySQL support. In addition, backtracking, point-in-time recovery, and automatic backup are enabled for the database cluster. However, a developer mistakenly performed a DELETE query without a WHERE clause on the database. The SysOps administrator needs to roll back the database cluster to a specific point in time within the last 72 hours and ensure that the database restore procedure will be done on the same DB instance and not by creating a new one.

What should the SysOps administrator do to restore the database?

- ~~Build an Aurora Replica and promote it to be the primary database instance.~~
- ~~Create a backup plan in AWS Backup that runs every 72 hours.~~
- ~~Utilize point-in-time recovery to restore the database instance to a specified point in time.~~

anti-pattern

- Rewind the Aurora database cluster to the desired recovery point by using backtracking.

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

K EYWORDS - kewords and phrases

E LIMINATION - eliminate unrelated options

E VALUATION - closely evaluate underlying concepts

P ATTERNS - look for patterns and anti-patterns



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Question #01

A leading advertising company is using Lambda to run a serverless application in AWS. The application processes transactions on an Amazon RDS database instance with MySQL support. As the company grows, the number of users has started to increase. As a result, your Lambda function is beginning to receive "too many connections" errors when attempting to connect to the RDS database. When the SysOps administrator checked the database settings, the max_connections parameter is already set to the maximum possible value.

What step should the Sysops administrator perform to resolve the issue?

- ~~Increase the value of the max_connect_errors parameter to 10 to allow more errors.~~
- ~~Raise the Lambda function's provisioned concurrency setting to a higher value.~~
- ✓ Enable Multi-AZ setting for the RDS database instance.
- ✓ Provision an Amazon RDS Proxy and update the database connection string in your Lambda function.

50% chance

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS Management Console

AWS services

Recently visited services

- EC2
- IAM
- Elastic Container Registry
- VPC
- Simple Notification Service
- Kinesis
- Launch Wizard
- S3
- CloudWatch
- Elastic Container Service
- Step Functions
- Billing
- CloudFormation
- Batch
- Simple Queue Service

All services

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
2-3 minutes



Build a web app
With Elastic Beanstalk
6 minutes



Build using virtual servers
With Lightsail
1-2 minutes



Register a domain
With Route 53
3 minutes



Connect an IoT device
With AWS IoT
5 minutes



Start migrating to AWS
With AWS MGN
1-2 minutes



Start a development project
With CodeStar
5 minutes



Deploy a serverless microservice
With Lambda, API Gateway
2 minutes



Stay connected to your AWS resources on-the-go



AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

Explore AWS

Introducing AWS Backup Audit Manager

Maintain and demonstrate your data backup and compliance posture at scale. Learn more »

Build Apps Faster with GraphQL

AWS AppSync uses GraphQL APIs to query data from multiple data sources in a single request. Get started »

AWS Free Digital Training

Learn the AWS Cloud today to create opportunities tomorrow: find out how. Learn more »

Free AWS Training

Advance your career with AWS Cloud Practitioner Essentials—a free, six-hour, foundational course. Learn more »

Have feedback?

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Management Console

https://us-west-1.console.aws.amazon.com/console/home?region=us-west-1

aws Services Search for services, features, marketplace products, and docs [Alt+S] td-lab-wayne @ 9141-2308-7266 N. California Support

AWS Management Console

AWS services

Recently visited services

- VPC
- S3
- AWS Backup
- CloudWatch
- Billing
- EFS
- Simple Notification Service
- Key Management Service
- Route 53
- EC2
- CloudTrail
- IAM
- CloudFormation
- AWS Cost Explorer
- Config

All services

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
2-3 minutes

Build a web app
With Elastic Beanstalk
6 minutes

Build using virtual servers
With Lightsail
1-2 minutes

Register a domain
With Route 53
3 minutes

Connect an IoT device
With AWS IoT
5 minutes

Start migrating to AWS
With AWS MGN
1-2 minutes

Stay connected to your AWS resources on-the-go

AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

Explore AWS

AWS Training
Free digital courses to help you develop your skills. Learn more »

AWS Certification
Propel your career forward with AWS Certification. Learn more »

Free AWS Training
Advance your career with AWS Cloud Practitioner Essentials—a free, six-hour, foundational course. Learn more »

AWS Certification
Explore the resources available to help you prepare for your AWS Certification. Learn more »

Waiting for us-west-1.console.aws.amazon.com...

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

INSTRUCTIONS

SCENARIO

You will create a non-default VPC with a public and private subnet located in us-west-1 using the VPC Wizard. Each subnet is assigned to a specific CIDR block in different availability zones. You have to ensure that a NAT gateway is in place to allow private resources to access the internet without exposing those resources to incoming internet connections. Lastly, you need to ensure that all the EC2 instances that will be provisioned in the VPC will be automatically associated with a DNS hostname.

GENERAL INSTRUCTION

Always use the default settings when implementing the instructions on the AWS Management Console unless stated otherwise.

1. Create a non-default VPC located in **us-west-1** that is configured to host resources with a CIDR block of **10.0.0.0/16** and name it **td-vpc-lab**.

2. Create a public subnet called **td-public-subnet** in **us-west-1a** and assign the **10.0.0.0/24** CIDR block. Then, create a private subnet called **td-private-subnet** in **us-west-1b** and assign the **10.0.1.0/24** CIDR block.

3. Create a NAT gateway and assign an Elastic IP address.

4. Ensure that all EC2 instances launched in the **td-vpc-lab** will always be associated with a DNS hostname.



Prepare to encounter exam labs on:

- Setting up CloudWatch monitoring
- Build ASG and load balancers
- Set up a VPC network
- Working with S3
- Creating backups using backup services and features in AWS

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

VPC Management Console

https://us-west-1.console.aws.amazon.com/vpc/home?region=us-west-1#wizardFullpagePublicAndPrivate:

aws Services Search for services, features, marketplace products, and docs [Alt+S] td-lab-wayne @ 9141-2308-7266 N. California Support

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block:
- (•) No IPv6 CIDR Block
- ( ) Amazon provided IPv6 CIDR block
- ( ) IPv6 CIDR block owned by me

VPC name:

Public subnet's IPv4 CIDR:* 10.0.0.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Public subnet name: Public subnet

Private subnet's IPv4 CIDR:* 10.0.1.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Private subnet name: Private subnet

You can add more subnets after Amazon Web Services creates the VPC.

Specify the details of your NAT gateway (NAT gateway rates apply).

Elastic IP Allocation ID:*

Service endpoints

Add Endpoint

Enable DNS hostnames:* (•) Yes ( ) No

Hardware tenancy:* Default

Cancel and Exit Back Create VPC

Feedback English (US)

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy Terms of Use Cookie preferences

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

INSTRUCTIONS

SCENARIO

You will create a non-default VPC with a public and private subnet located in us-west-1 using the VPC Wizard. Each subnet is assigned to a specific CIDR block in different availability zones. You have to ensure that a NAT gateway is in place to allow private resources to access the internet without exposing those resources to incoming internet connections. Lastly, you need to ensure that all the EC2 instances that will be provisioned in the VPC will be automatically associated with a DNS hostname.

GENERAL INSTRUCTION

Always use the default settings when implementing the instructions on the AWS Management Console unless stated otherwise.

1. Create a non-default VPC located in **us-west-1** that is configured to host resources with a CIDR block of **10.0.0.0/16** and name it **td-vpc-lab**.

2. Create a public subnet called **td-public-subnet** in **us-west-1a** and assign the **10.0.0.0/24** CIDR block. Then, create a private subnet called **td-private-subnet** in **us-west-1b** and assign the **10.0.1.0/24** CIDR block.

3. Create a NAT gateway and assign an Elastic IP address.

4. Ensure that all EC2 instances launched in the **td-vpc-lab** will always be associated with a DNS hostname.

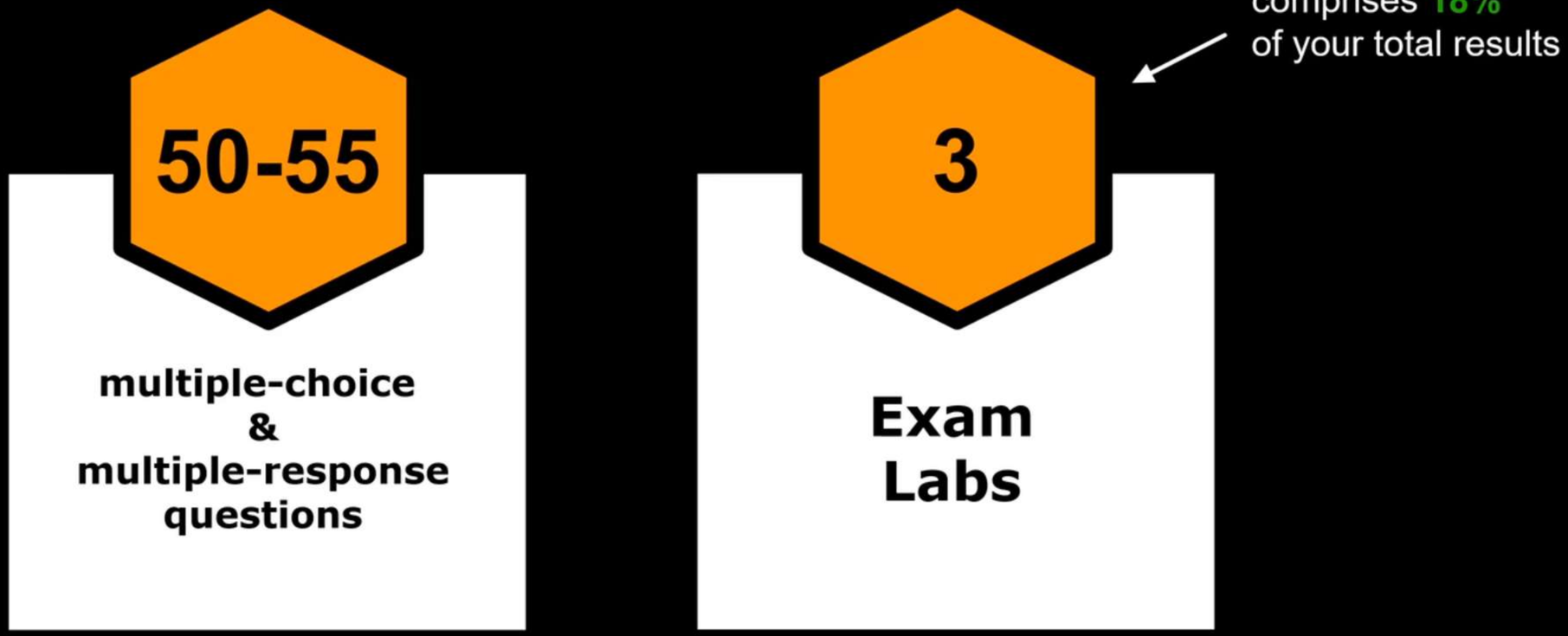
Press Esc to exit full screen



What to Expect in your SOA-C02 exam?

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

What items are included in the exam?



Tutorials Dojo
NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



720

passing score

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

AWS-Certified-SysOps-Administr
https://d1.awsstatic.com/training-and-certification/docs-sysops-associate/AWS-Certified-SysOps-Administrator-Associate_Exam-Guide.pdf
1 of 10
Page view
Read aloud
Draw
Highlight
Erase

aws training and certification

AWS Certified SysOps Administrator – Associate (SOA-C02) Exam Guide

Introduction

The AWS Certified SysOps Administrator – Associate (SOA-C02) exam is intended for system administrators in a cloud operations role. The exam validates a candidate's ability to deploy, manage, and operate workloads on AWS.

The exam also validates a candidate's ability to complete the following tasks:

- Support and maintain AWS workloads according to the AWS Well-Architected Framework
- Perform operations by using the AWS Management Console and the AWS CLI
- Implement security controls to meet compliance requirements
- Monitor, log, and troubleshoot systems
- Apply networking concepts (for example, DNS, TCP/IP, firewalls)
- Implement architectural requirements (for example, high availability, performance, capacity)
- Perform business continuity and disaster recovery procedures
- Identify, classify, and remediate incidents

Target candidate description

The target candidate should have 1 year of experience with deployment, management, networking, and security on AWS.

Recommended general IT knowledge

The target candidate should have the following knowledge:

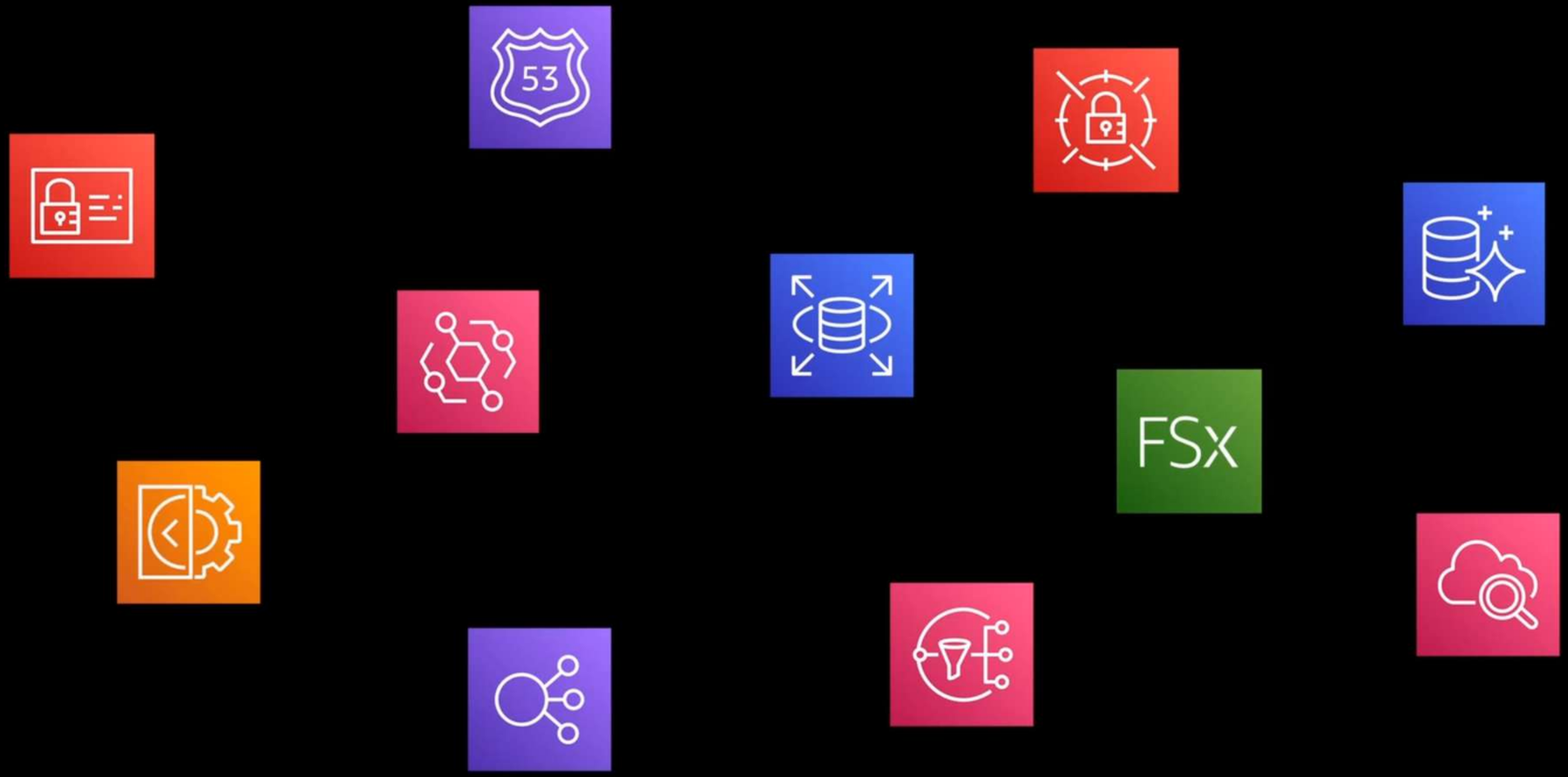
- 1–2 years of experience as a systems administrator in an operations role
- Experience in monitoring, logging, and troubleshooting
- Knowledge of networking concepts (for example, DNS, TCP/IP, firewalls)
- Ability to implement architectural requirements (for example, high availability, performance, capacity)

Recommended AWS knowledge

The target candidate should have the following knowledge:

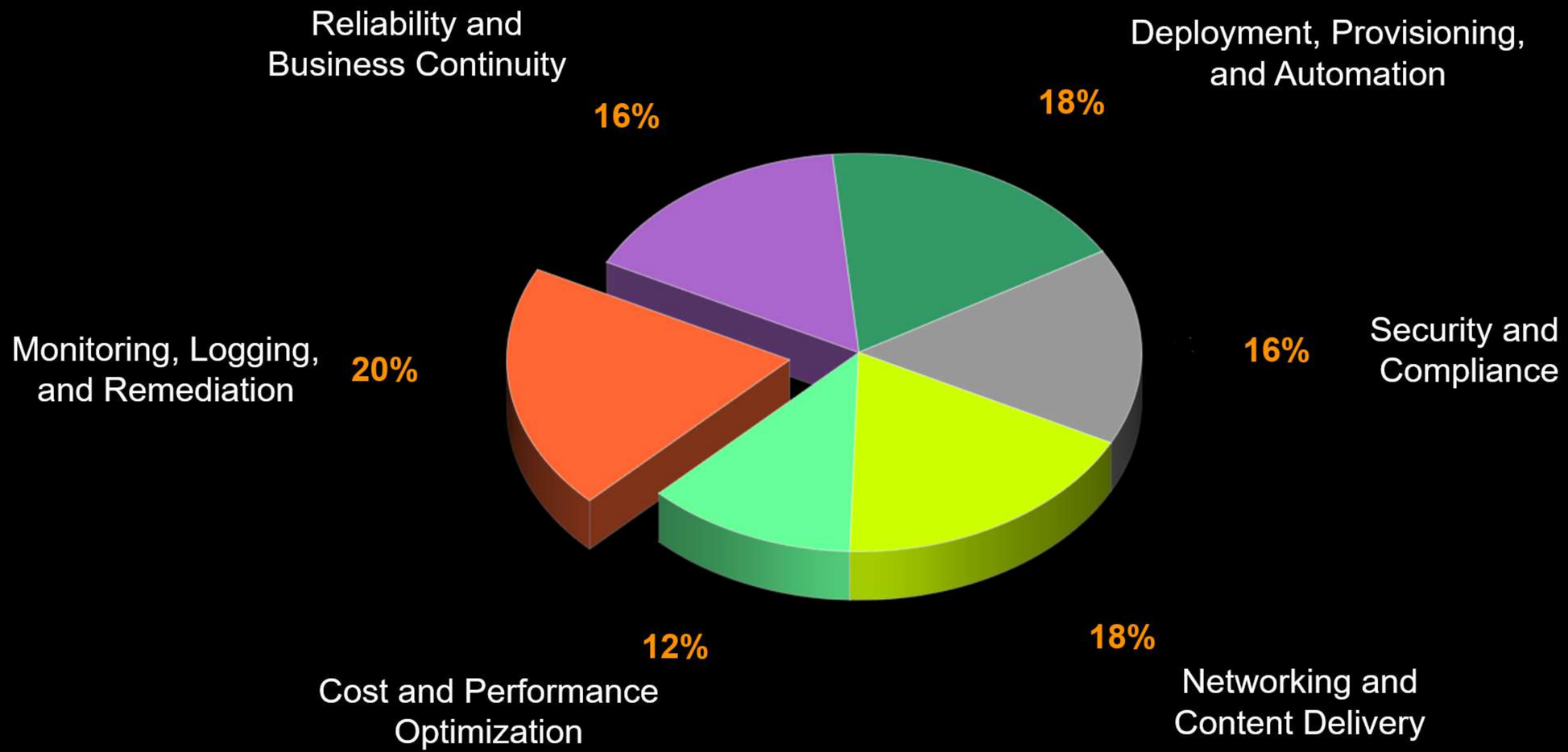
- Minimum of 1 year of hands-on experience with AWS technology
- Experience in deploying, managing, and operating workloads on AWS
- Understanding of the AWS Well-Architected Framework
- Hands-on experience with the AWS Management Console and the AWS CLI
- Understanding of AWS networking and security services
- Hands-on experience in implementing security controls and compliance requirements

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com



Tutorials Dojo

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

NEW: AWS Certified Solutions Architect Associate Video Course (Early Access) - $10.99 USD ONLY! LEARN MORE

AWS Certified SysOps Administrator Associate Practice Exams 2021

(5.0) ★★★★★ (30)

AWS Certified SysOps Administrator Associate Questions in TIMED mode, REVIEW mode, SECTION-BASED, and FINAL TEST mode with Explanations, Reference Links, Score Tracking, Plus BONUS Flashcards

View Course details

Jon-Bonso



Start Course

$14.99 USD

COURSE INCLUDES

- 6 Lessons
- 9 Topics
- 19 Quizzes
- Instructors: Jon Bonso, Chris Wayne Comendador

You are enrolled in this course

YOUR PROGRESS

AWS Certified SysOps Administrator Associate Practice Exams 2021

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Waiting for www.google-analytics.com...

Monitoring, Logging, and Remediation

1.1 Implement metrics, alarms, and filters by using AWS monitoring and logging service

1.2 Remediate issues based on monitoring and availability metrics

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization

Monitoring & Logging Services

Amazon CloudWatch Services



- Logs
- Events
- Alarms



Amazon EventBridge



CloudTrail



AWS Config

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization

Monitoring & Logging Services

AWS CloudWatch





Amazon SNS



- logs
- metric filters
- alarms
- dashboards

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1:
Monitoring, Logging, and Remediation

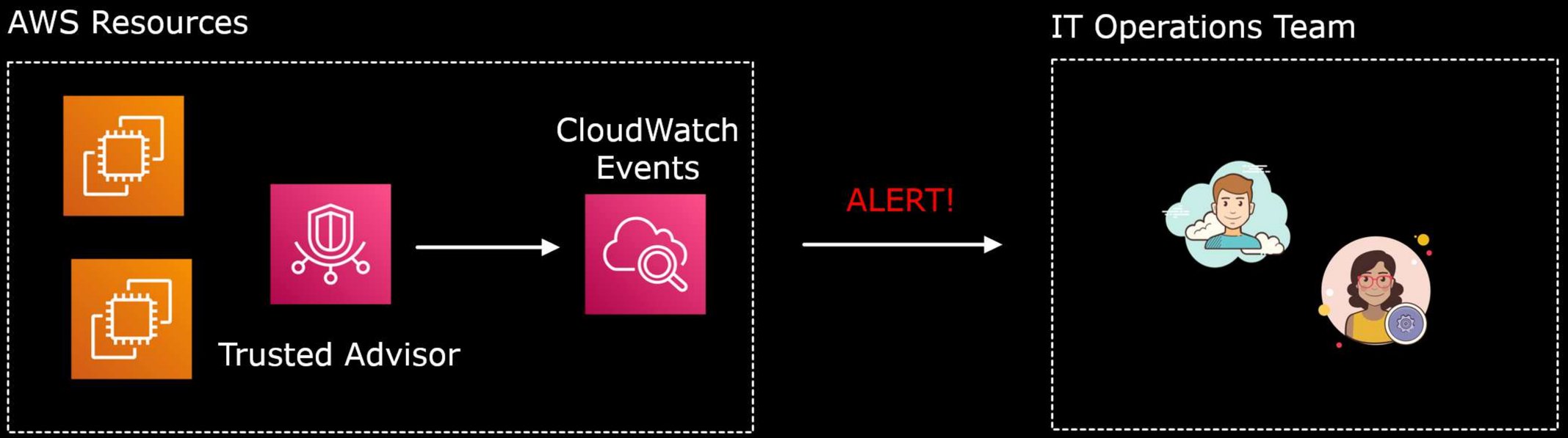
Domain 2:
Reliability and Business Continuity

Domain 3:
Deployment, Provisioning, and Automation

Domain 4:
Security and Compliance

Domain 5:
Networking and Content Delivery

Domain 6:
Cost and Performance Optimization



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

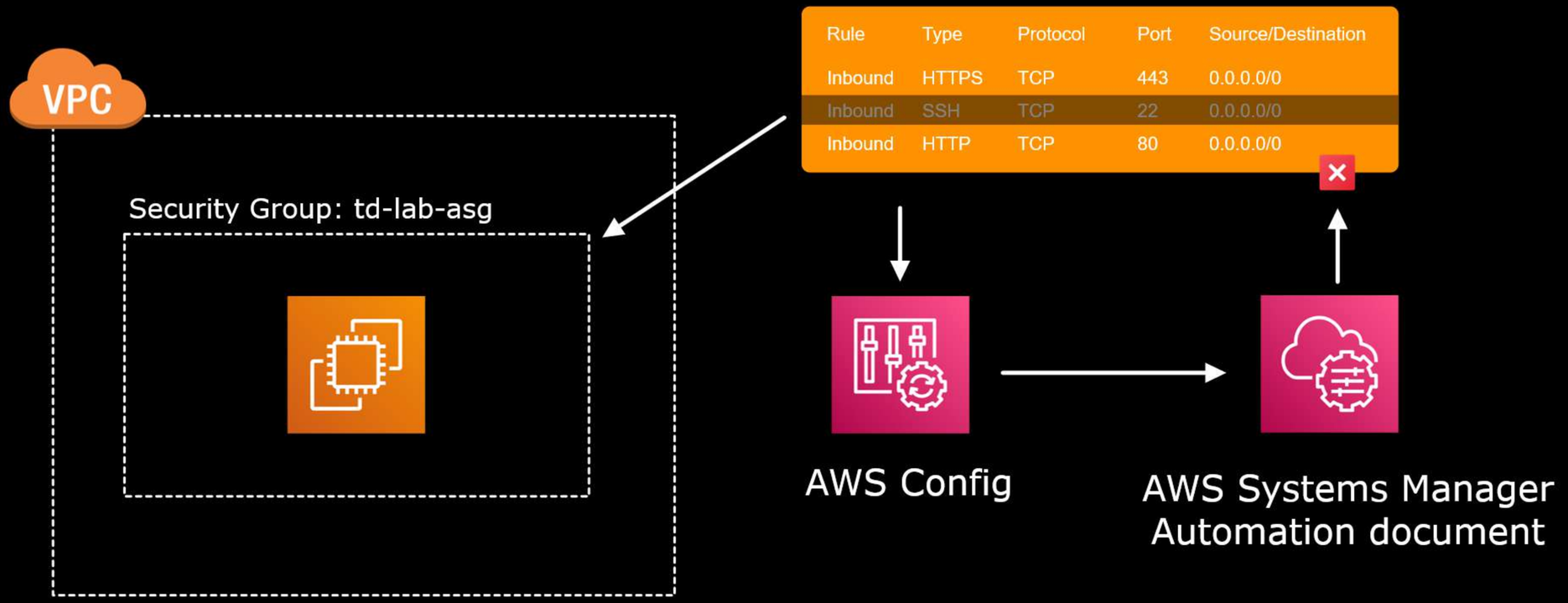
Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Reliability and Business Continuity

2.1 Implement scalability and elasticity

2.2 Implement high availability and resilient environments

2.3 Implement backup and restore strategies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization

Scalability

is the ability to quickly and easily increase or decrease your resources as needed

Services related to help create loosely coupled infrastructure:



ASG



RDS Replica



Aurora replica

Horizontal Scaling vs Vertical Scaling

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

High-availability

capability of your infrastructure to keep your business running without downtime

Services that help achieve high-availability in AWS



ELB



Route53



ASG

Differentiate Single AZ and Multi-AZ deployments for services like:



RDS



ELB



FSx



ASG

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Backup & Restore Strategies

cover topics on performing backup operations and being able to quickly restore your data

- S3 Lifecycle Rules
- S3 Versioning
- Amazon Data Lifecycle Manager
- RDS Snapshots
- EC2 AMI
- RDS point-in-time recovery
- Aurora backtracking
- AWS Backup

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization

Deployment, Provisioning, and Automation

3.1 Provision and maintain cloud resources

3.2 Automate manual or repeatable processes

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Automation

- refers to the use of tools to automatically control the installation, configuration, and management of cloud computing services.
- Buying resources is not enough. You need to implement deployments and provisioning actions in an automated approach.



EC2 Image Builder



CloudFormation

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization



AWS CloudFormation

Build strong foundation on the following concepts:

- Templates
- Stacks
- Stacksets
- Nested Stacks
- Custom Resources
- DependsOn and WaitConditions
- Helper scripts

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization

Automation

- refers to the use of tools to automatically control the installation, configuration, and management of cloud computing services.
- Buying resources is not enough. You need to be able to implement deployments and provisioning actions in an automated approach.



EC2 Image Builder



CloudFormation



AWS OpsWorks



EventBridge



AWS Config

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization

Security and Compliance

4.1 Implement and manage security and compliance policies

4.2 Implement data and infrastructure protection strategies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization



Identity Access Management

Build strong foundation on the following concepts:

- Evaluate and attach Policies
- Creating IAM Roles
- Implement MFA
- Implement Service-linked Roles

Evaluate IAM Policies and SCP Policies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization

Encryption & Key Management Services

Key Management

- key-rotations
- customer-managed keys
- custom key stores



KMS



CloudHSM

Encryption

- API Keys
- Passwords
- Certificates



Secrets Manager



Systems Manager Parameter Store

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization



Amazon S3

Build strong foundation on the following concepts:

- Pre-signed URLs
- Cross-account sharing
- Client-side and Server-side encryption
- MFA delete

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1:

Monitoring, Logging, and Remediation

Domain 2:

Reliability and Business Continuity

Domain 3:

Deployment, Provisioning, and Automation

Domain 4:

Security and Compliance

Domain 5:

Networking and Content Delivery

Domain 6:

Cost and Performance Optimization

Infrastructure Security Services



AWS WAF



AWS Shield



AWS Certificate Manager

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Networking and Content Delivery

5.1 Implement networking features and connectivity

5.2 Configure domains, DNS services, and content delivery

5.3 Troubleshoot network connectivity issues

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization



Networking

Broad range of networking topics like:

- Virtual Private Cloud
- Connecting an on-premises network to a VPC
- Network Protection
- DNS
- Caching and Content Delivery
- Remediation
- Troubleshooting network issues

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

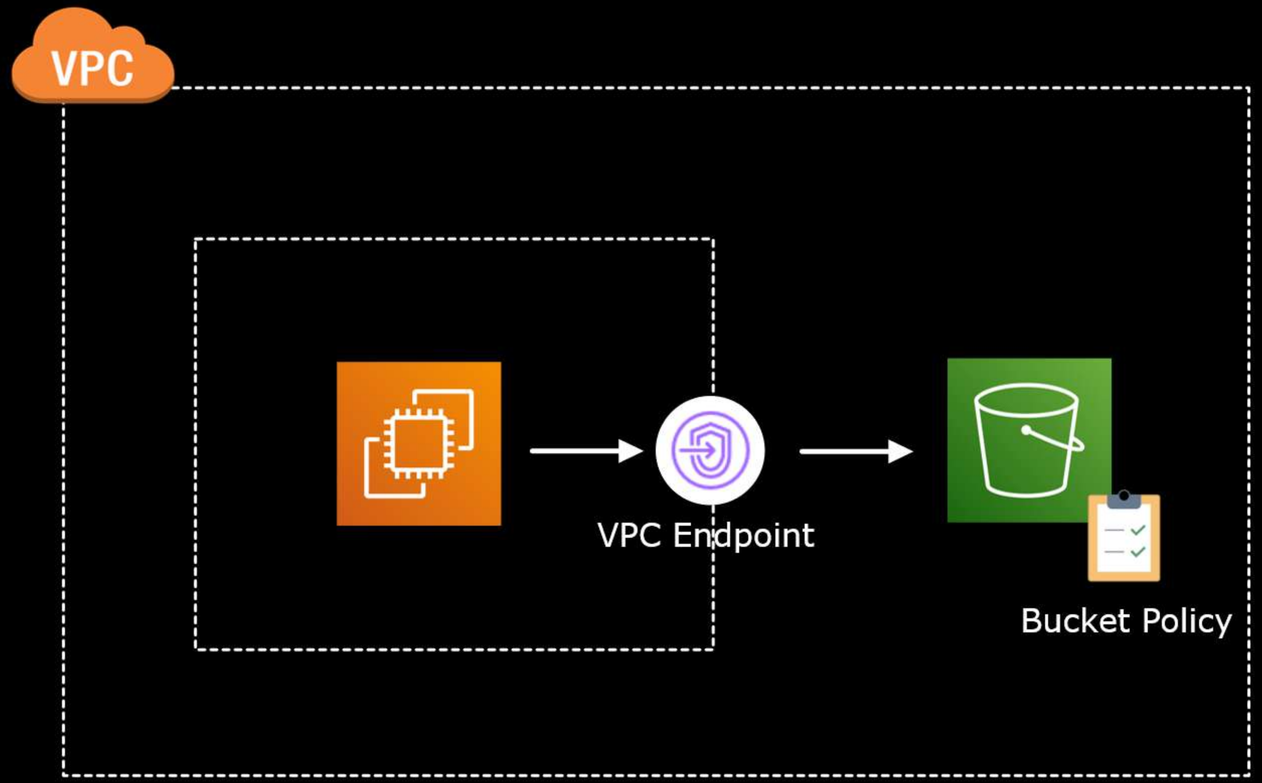
Domain 2: Reliability and Business Continuity

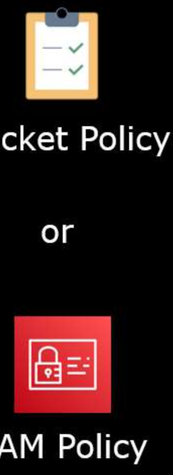
Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization





NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Cost and Performance Optimization

6.1 Implement cost optimization strategies

6.2 Implement performance optimization strategies

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1: Monitoring, Logging, and Remediation

Domain 2: Reliability and Business Continuity

Domain 3: Deployment, Provisioning, and Automation

Domain 4: Security and Compliance

Domain 5: Networking and Content Delivery

Domain 6: Cost and Performance Optimization

AWS Cost Optimization Tools



Trusted Advisor



AWS Compute Optimizer



Cost Explorer

- configuring billing alarms
- implementing cost monitoring procedures

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/

Domain 1:

Monitoring, Logging, and Remediation

Domain 2:

Reliability and Business Continuity

Domain 3:

Deployment, Provisioning, and Automation

Domain 4:

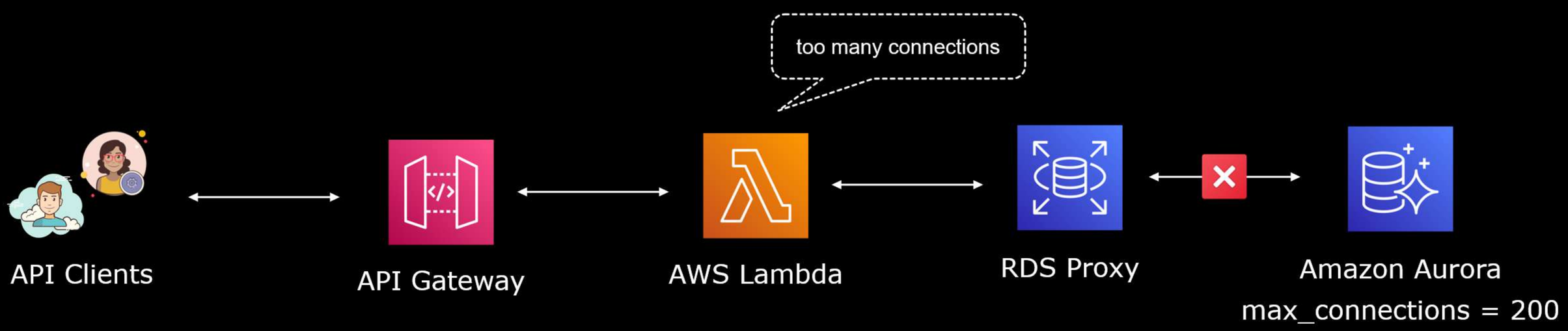
Security and Compliance

Domain 5:

Networking and Content Delivery

Domain 6:

Cost and Performance Optimization



NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/



SOA-C02 Exam Labs

NOT FOR DISTRIBUTION. © Tutorials Dojo. https://portal.tutorialsdojo.com/