Introduction to Amazon Cloud, EC2 & IAM

Nayef M Khan
Solutions Architect

Agenda

- Introduction to AWS Cloud
- EC2 Overview
- Identity and Access Management
- AWS Organizations
- AWS SSO
- Sample Questions

1

Introduction to AWS

What is AWS?

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers millions of businesses in over 190 countries around the world.

Benefits

- Low Cost
- Elasticity & Agility
- Open & Flexible
- Secure
- Global Reach

The Most Extensive, Reliable and Secure Global Cloud Infrastructure Available

The Amazon Web Services (AWS) Global Infrastructure delivers a cloud infrastructure companies can depend on—no matter their size, changing needs, or challenges. The AWS Global Infrastructure is designed and built to deliver the most flexible, reliable, scalable, and secure cloud computing environment with the highest quality global

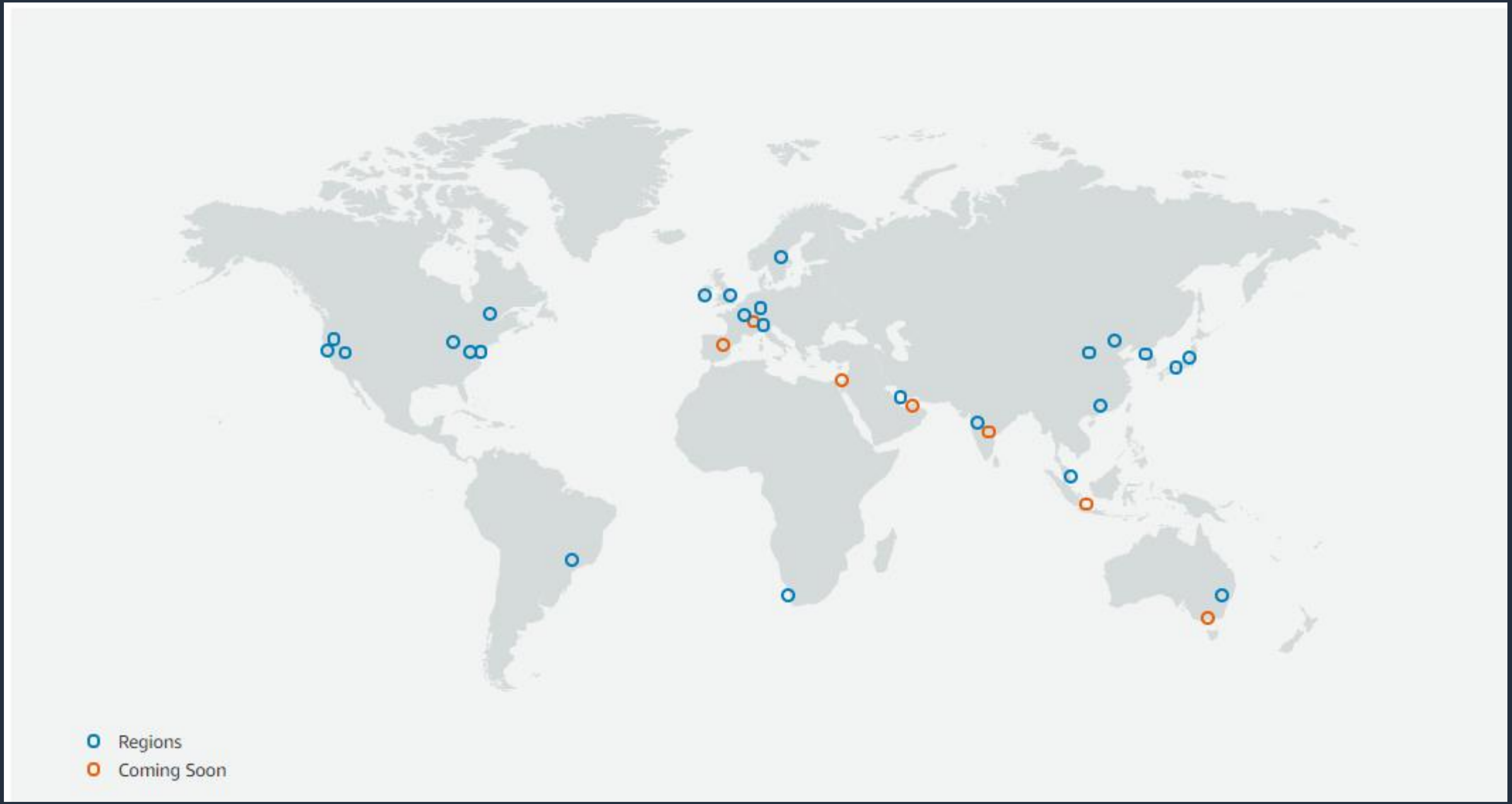
https://infrastructure.aws/

25

Regions

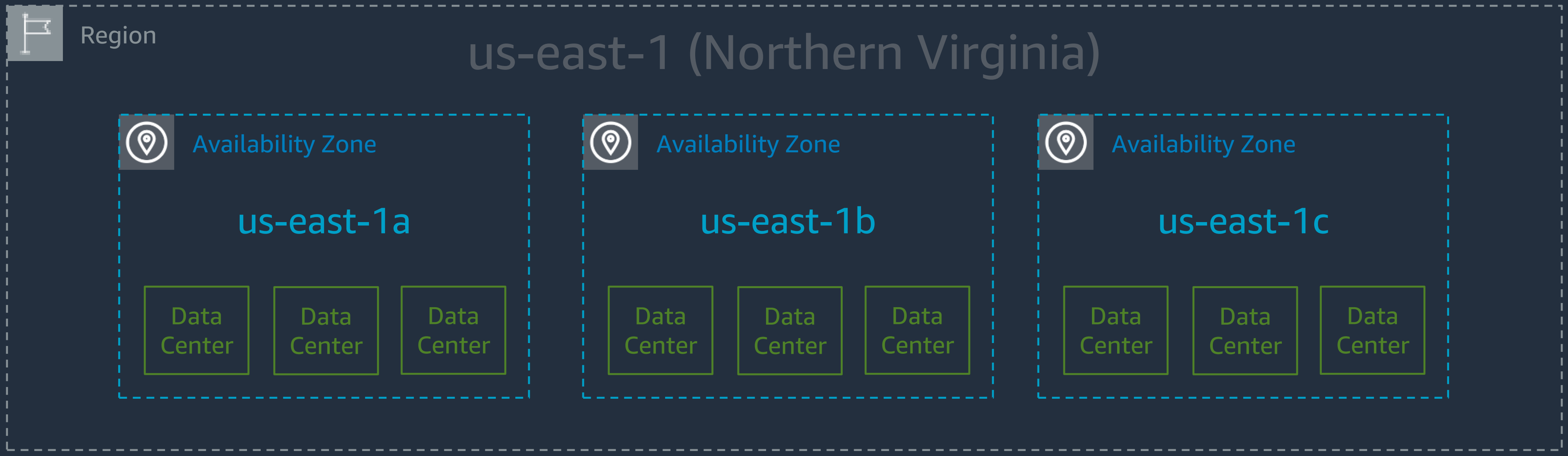
81

Availability Zones



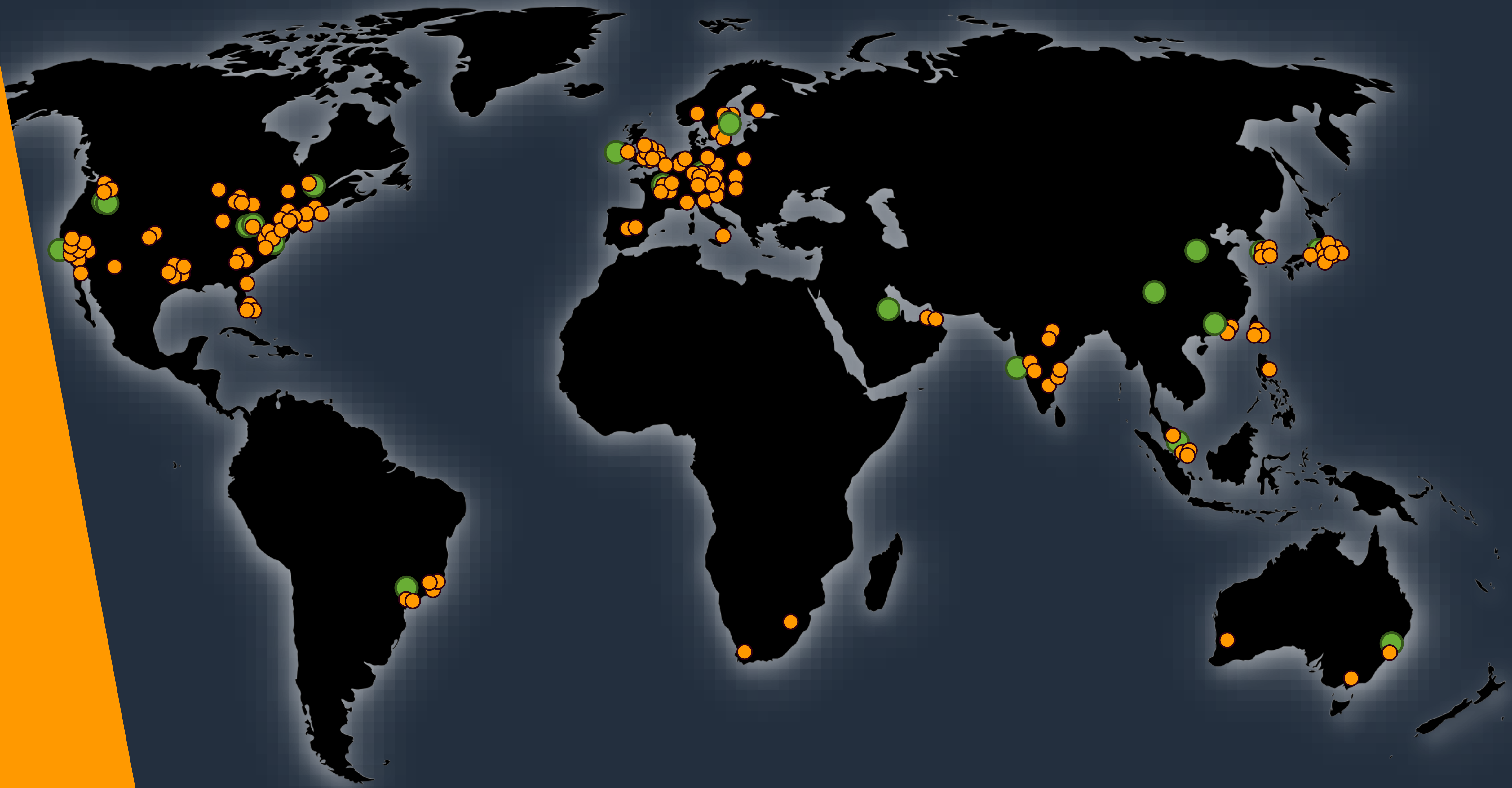
Availability Zones

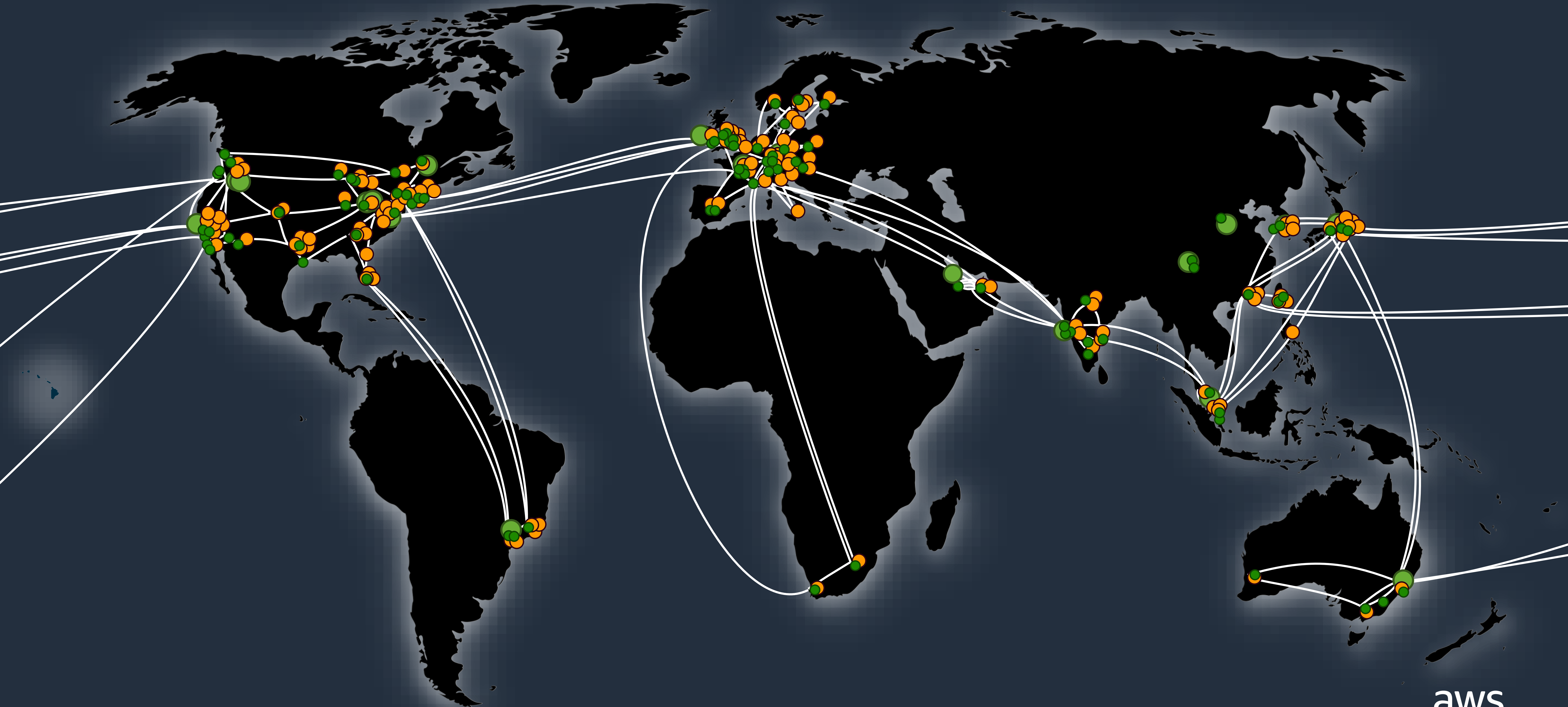
- A region is comprised of multiple Availability Zones (typically 3)
- Fully independent partitions on isolated fault lines, flood plains, and power grids
- Each AZ: redundant power and redundant dedicated network
- Each AZ: typically multiple data centers
- Between AZs: high throughput, low latency (<10ms) network
- Between AZs: physical separation < 100km (60mi)



230+

Amazon CloudFront Points of Presence

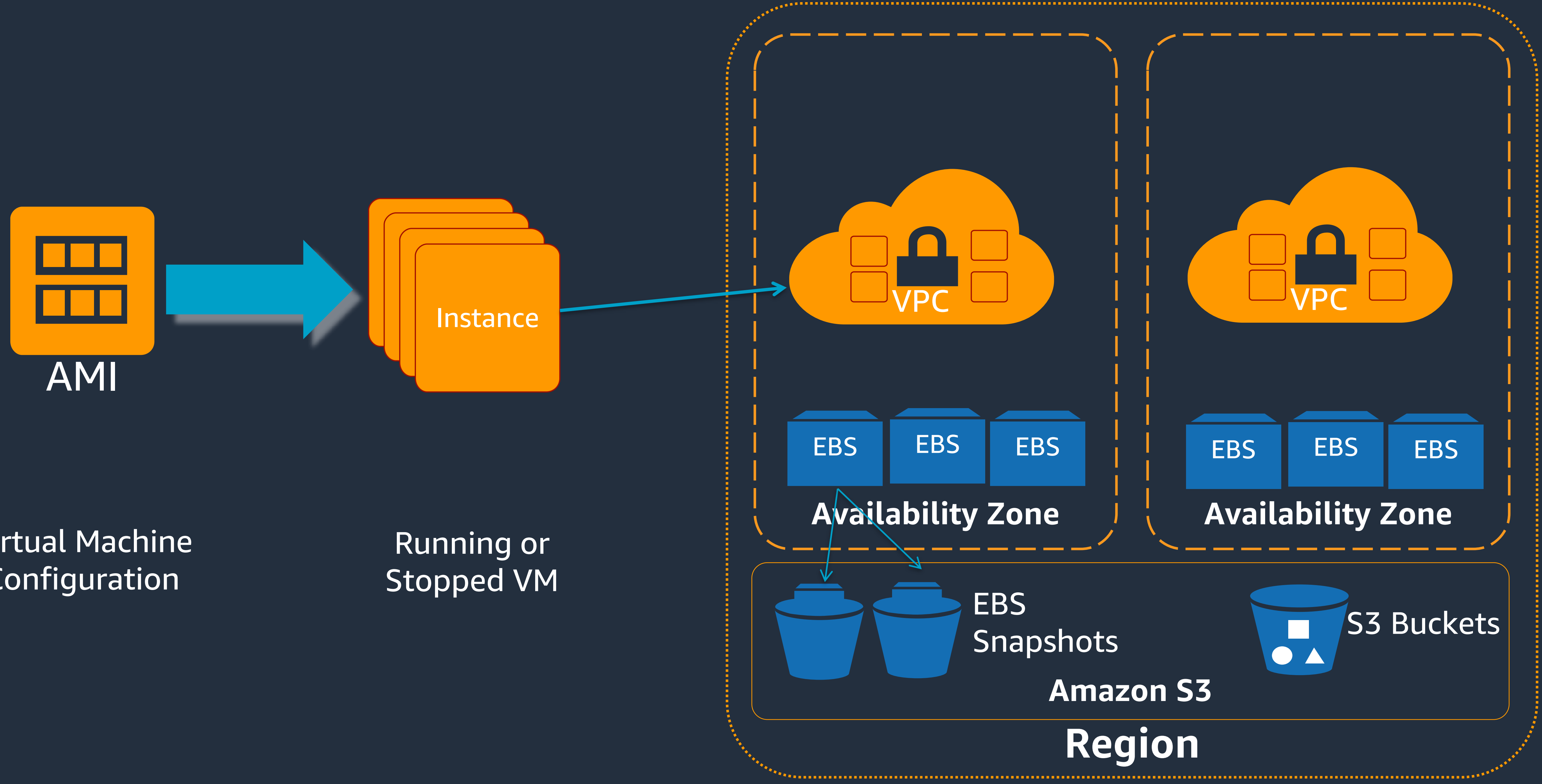




②

EC2 Overview

Amazon EC2 Terminology



Virtual Machine Configuration

Running or Stopped VM

What’s a virtual CPU? (vCPU)

- A vCPU is typically a hyper-threaded physical core*
- Divide vCPU count by 2 to get core count

- Cores by Amazon EC2 & RDS DB Instance type: https://aws.amazon.com/ec2/virtualcores/

** CPU Optimizing options allow disabling hyperthreading and reduce number of cores*

Memory and Storage

What's a GiB?

- Memory is presented as GibiBytes (GiB) and not Gigabytes (GB)
- 1 GB = 1000^3 bytes
- 1 GiB = 1024^3 bytes

What about storage?

- Storage is independent of compute
- You allocate drives known as EBS volumes
- Max 16 TiB per volume*
- Some instance types provide physically attached (ephemeral) storage

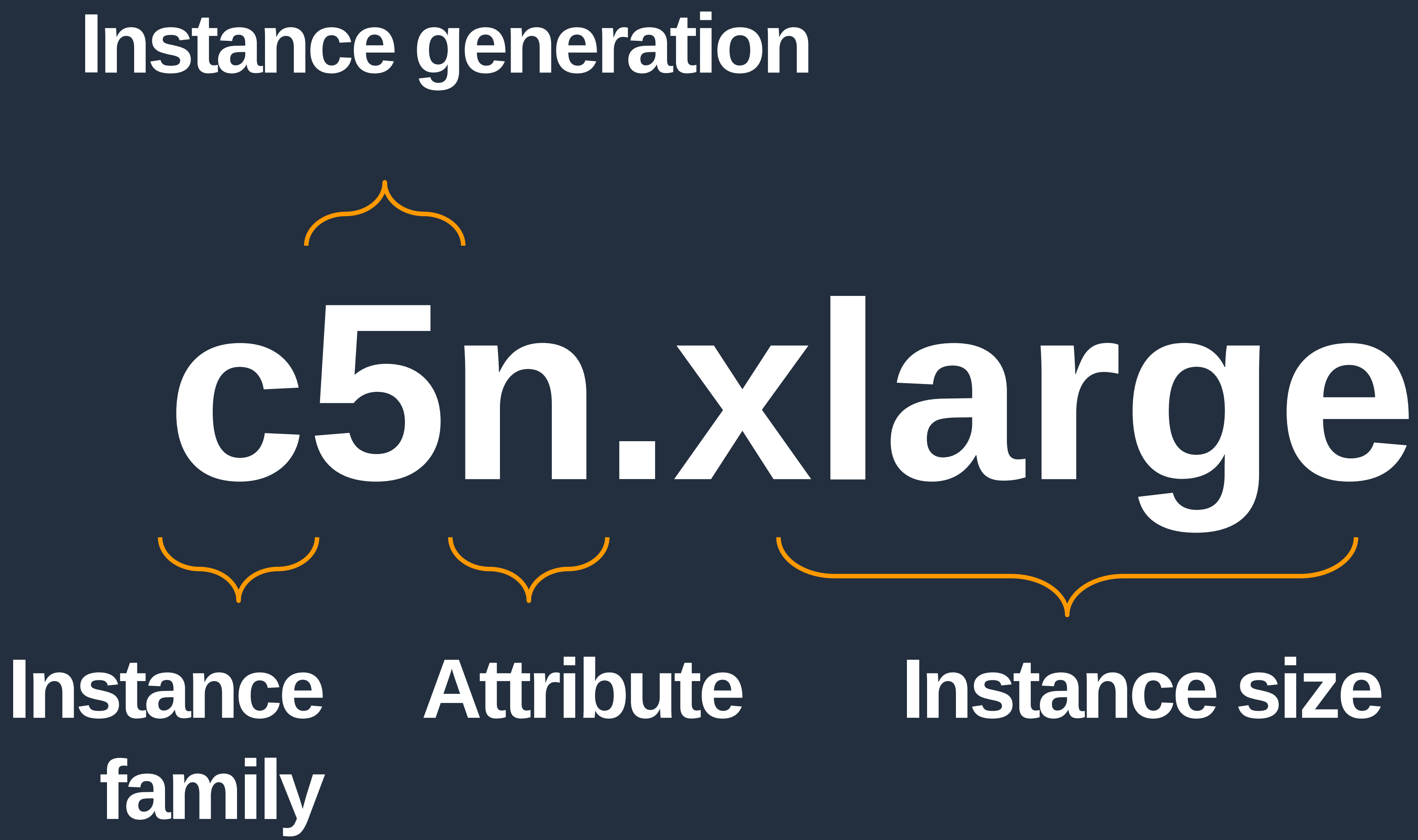
Resource allocation

- All resources assigned to you are dedicated to your instance with no over commitment*
    - All vCPUs are dedicated to you
    - Memory allocated is assigned only to your instance
    - Network resources are partitioned to avoid “noisy neighbors”

Instance Types

	General Purpose		Compute Optimized	Memory Optimized				Accelerated Computing			Storage Optimized		
	Burstable performance	General Purpose	Compute Intensive	Memory Optimized	In-memory	Memory Intensive	Compute and Memory Intensive	Graphics Intensive	General Purpose GPU	FPGA	High I/O	Dense Storage	Big Data Optimized
intel	T3	M5 M5n	C5 C5n	R5 R5n	X1	X1e	Z1d	G4 G3	P3 P2		I3 I3en	D2	H1
AMD	T3a	M5a	C5a	R5a									
arm	T4g	M6g	C6g	R6g									
others						u-12tb1			Inf1	F1			

EC2 Naming Explained



Instance generation

c5n.xlarge

Instance family

Attribute

Instance size

EC2 Operating Systems Supported

- Windows
- Amazon Linux
- Debian
- Suse
- CentOS
- Red Hat Enterprise Linux
- Ubuntu
- MacOS

for more OSes see: https://aws.amazon.com/marketplace/b/2649367011

Purchasing Options

On-Demand

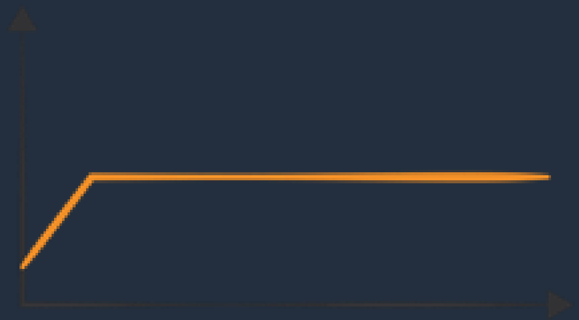
Pay for compute capacity by **the second** with no long-term commitments

For Spiky workloads or to define needs

Reserved Instances

Make a 1 or 3-year commitment and receive a **significant discount** off On-Demand prices

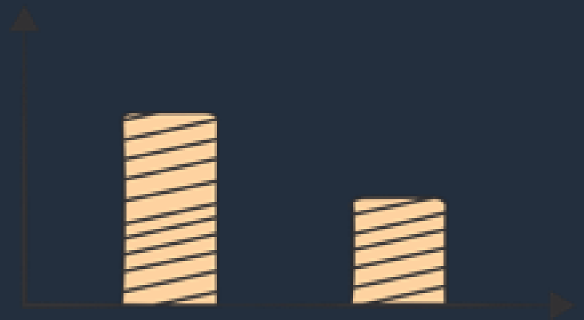
For committed utilization



Spot Instances

Spare EC2 capacity at **savings of up to 90%** off On-Demand prices

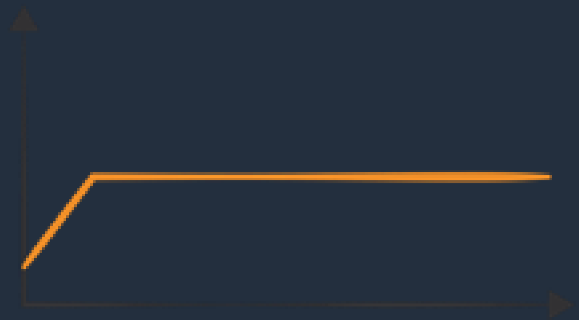
For time-insensitive or transient workloads Need to be Fault-tolerant, stateless



Savings Plans

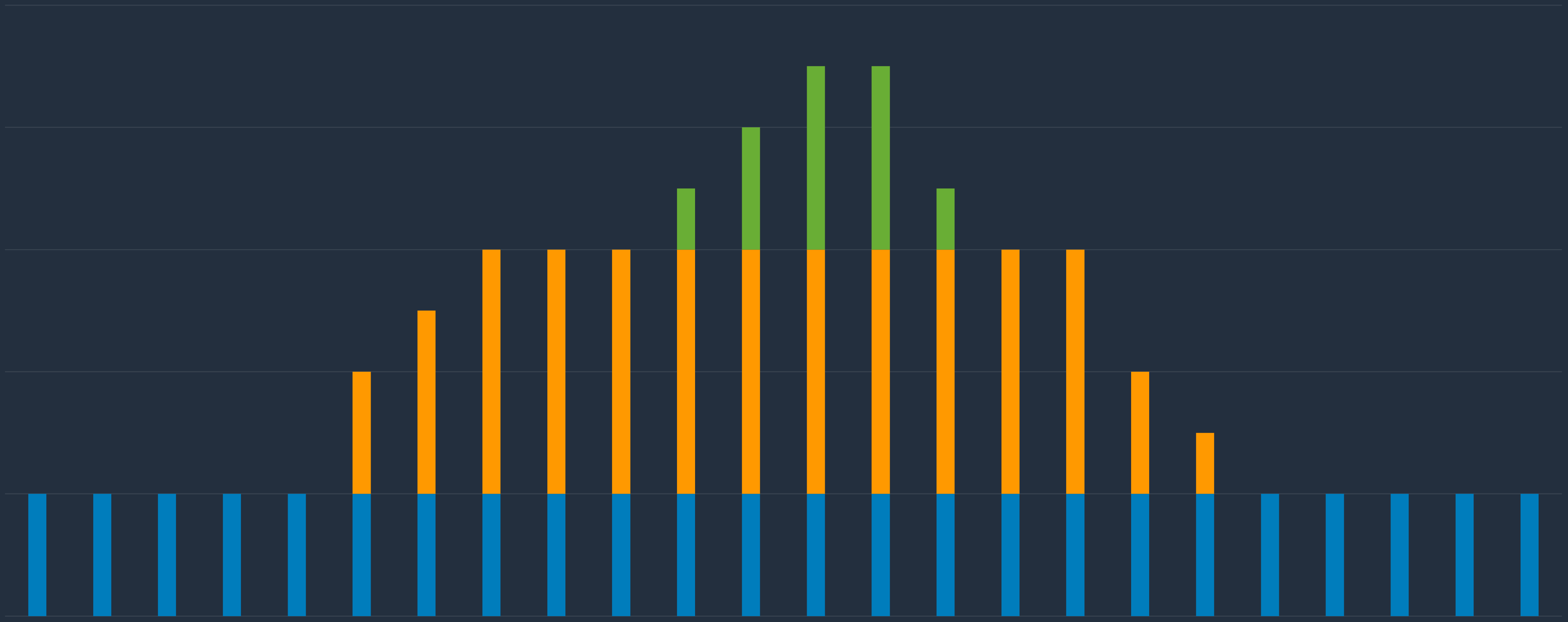
Commit to a $/h spend and **share discount** across compute options and regions

For committed utilization



To optimize EC2, combine multiple purchase options!

Simplify capacity and cost optimization



Now with hibernate

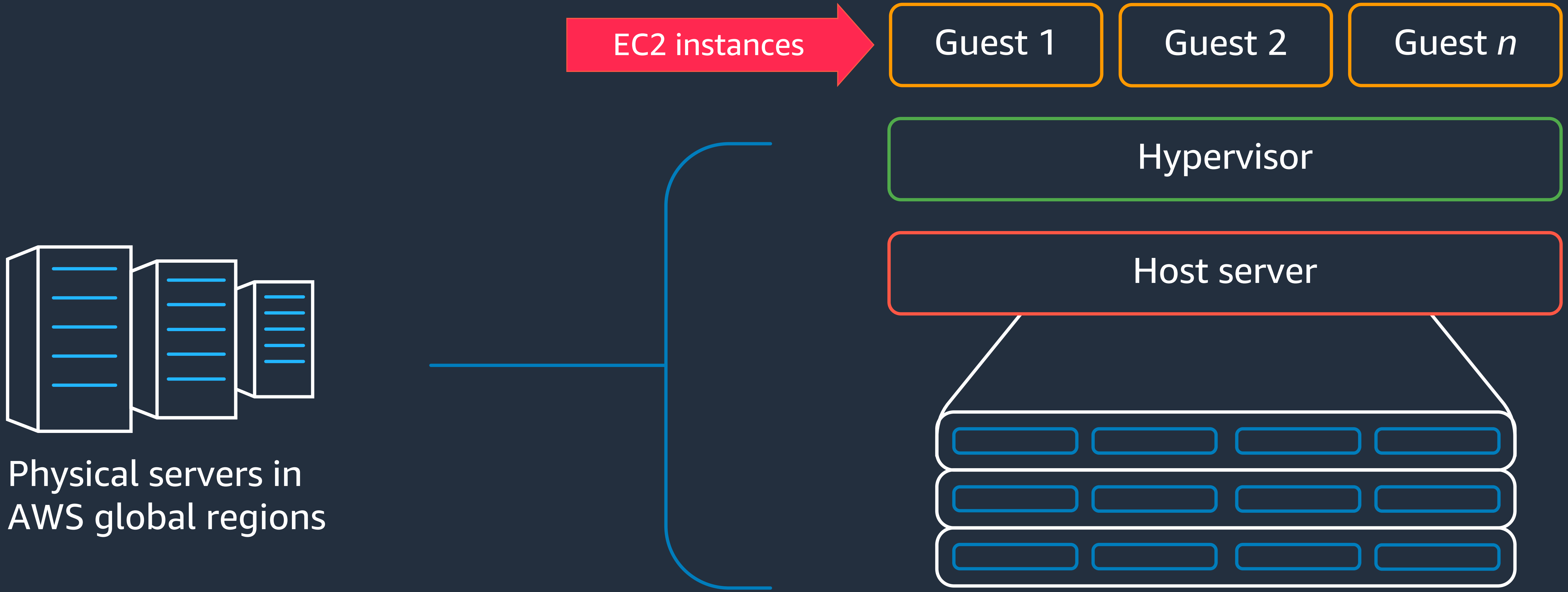
Scale using **Spot**, **On-Demand**, or both

Use **Reserved Instances** for known/steady-state workloads

AWS services make this easy and efficient

- Amazon EC2 Auto Scaling
- EC2 Fleet
- Amazon Elastic Container Service
- Amazon Elastic Container Service for Kubernetes
- AWS Thinkbox
- Amazon EMR
- AWS CloudFormation
- AWS Batch

EC2 Host Virtualization


EC2 instances

Guest 1

Guest 2

Guest *n*

Hypervisor

Host server

Physical servers in
AWS global regions

Which hypervisor do we use?

Original host architecture: Xen-based

- Hypervisor consumed resources from the underlying host
- Limited optimization

AWS Nitro Hypervisor: Custom KVM based hypervisor

- AWS Nitro System (launched on Nov 2017)
- Less server resources used, more resources for the customer
- AWS optimized

Bare metal: Direct access to processor and memory resources

- Built on the AWS Nitro system
- Enables custom hypervisors and micro-VM runtimes

AWS Nitro System

Nitro Card

Local NVMe storage

Elastic Block Storage

Networking, monitoring, and security

Nitro Security Chip

Integrated into motherboard

Protects hardware resources

Nitro Hypervisor

Lightweight hypervisor

Memory and CPU allocation

Bare metal-like performance

Modular building blocks for rapid design and delivery of EC2 instances

What is an Amazon Machine Image (AMI)?

- Provides the information required to launch an instance
- Launch multiple instances from a single AMI
- An AMI includes the following:
  - A template for the root volume (for example, operating system, applications)
  - Launch permissions that control which AWS accounts can use the AMI
  - Block device mapping that specifies volumes to attach to the instance

EC2 Placement Groups

Three Types of Placement Groups:

- Cluster Placement Group
  - Always in one availability zone
  - Low Network Latency / High Network Throughput
  - If on the exam it doesn’t specify then default to assuming its cluster.
- Spread Placement Group
  - Can be in multiple availability zones
  - Individual Critical EC2 Instances.
- Partition
  - Can be in multiple availability zones
  - Multiple EC2 Instances HDFS, HBase, and Cassandra.

Security Groups

- All Inbound traffic is blocked by default.
- All Outbound traffic is allowed.
- Changes to Security Groups take effect immediately.
- You can have any number of EC2 instances within a security group.
- You can have multiple security groups attached to EC2 Instances.
- Security Groups are STATEFUL.
- If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again.
- You cannot block specific IP addresses using Security Groups, instead use Network Access Control Lists (NACLs).

Instance Metadata

http://169.254.169.254/latest/meta-data/ contains a wealth of info

- ami-id
- ami-launch-index
- ami-manifest-path
- block-device-mapping/
- hostname
- instance-action
- ★ **instance-id**
- instance-type
- kernel-id
- local-hostname
- local-ipv4
- mac
- network/
- ★ **placement/availability-zone**
- profile
- public-hostname
- public-ipv4
- public-keys/

Quick Poll

What are the valid underlying hypervisors for EC2? (SELECT TWO)

1. ESX
2. Xen
3. OVM
4. Hyper-V
5. Nitro

Quick Poll

What are the valid underlying hypervisors for EC2? (SELECT TWO)

1. ~~ESX~~
2. Xen
3. ~~OVM~~
4. ~~Hyper-V~~
5. Nitro

Quick Poll

When creating a new security group, all inbound traffic is allowed by default.

1. True
2. False

Quick Poll

When creating a new security group, all inbound traffic is allowed by default.

1. ~~True~~
2. False

3

Identity and Access Management

What Is IAM

- IAM allows you to manage users and their level of access to the AWS console.
- It is important to understand IAM and how it works, both for the exam and for administrating a company’s AWS account in real life.

Key Features of IAM

Identity Access Management (IAM) offers the following features:

- Centralized control of your AWS account
- Shared Access to your AWS account
- Granular Permissions
- Identity Federation (including Active Directory, Facebook, Linkedin, etc)
- Multifactor Authentication
- Provides temporary access for users/devices and services where necessary
- Allows you to set up your own password rotation policy
- Integrates with many different AWS services
- Supports PCI DSS Compliance

Key Terminology For IAM

- Users – End Users such as people, employees of an organization, etc.
- Groups – A collection of users. Each user in the group will inherit the permissions of the group.
- Roles – You create roles and then assign them to AWS Resources.
- Policies – Policies are made up of documents, called Policy Documents. These documents are in a format called JSON and they give permissions as to what a User/Group/Role is able to do.

AWS Principal Entities

Account Owner ID (Root Account)

- Access to all subscribed services.
- Access to billing.
- Access to console and APIs.
- Access to Customer Support.

IAM Users, Groups and Roles

- Access to specific services.
- Access to console and/or APIs.
- Access to Customer Support (Business and Enterprise).

Temporary Security Credentials

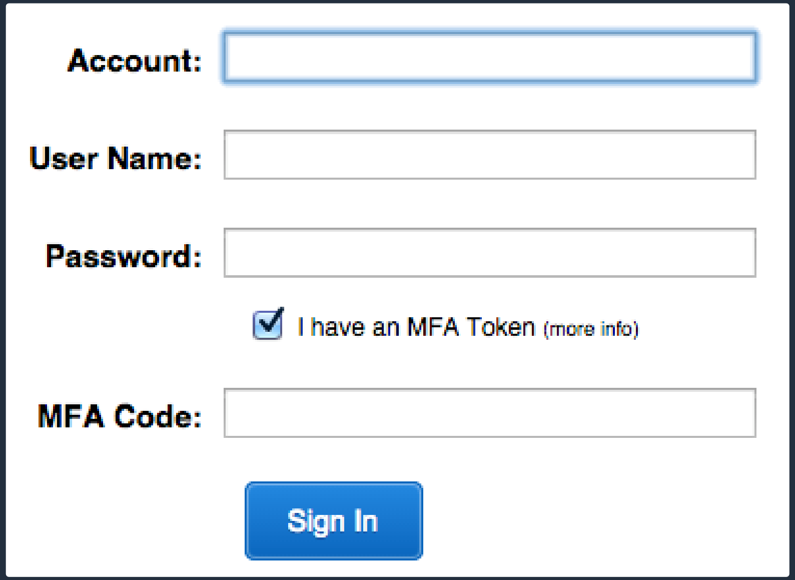
- Access to specific services.
- Access to console and/or APIs.

IAM User – Authentication

Authentication: *How do we know you are who you say you are?*

AWS Management Console

Login with **Username/Password** with optional **MFA** (recommended)



Account:

User Name:

Password:

☑ I have an MFA Token (more info)

MFA Code:

For time-limited access: **a Signed URL can** provide temporary access to the Console

API access

Access API using **Access Key + Secret Key**, with optional MFA

ACCESS KEY ID

Ex: `AKIAIOSFODNN7EXAMPLE`

SECRET KEY

Ex: `UtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

For time-limited access: Call the AWS Security Token Service (STS) to get a temporary AccessKey + SecretKey + session token

AWS Multi-factor Authentication (MFA)

Virtual MFA Device

- ○ Android & IPhone
  - ✓ Google Authenticator
  - ✓ Authy 2-Factor Authentication
- ○ Windows Phone
  - ✓ Authenticator

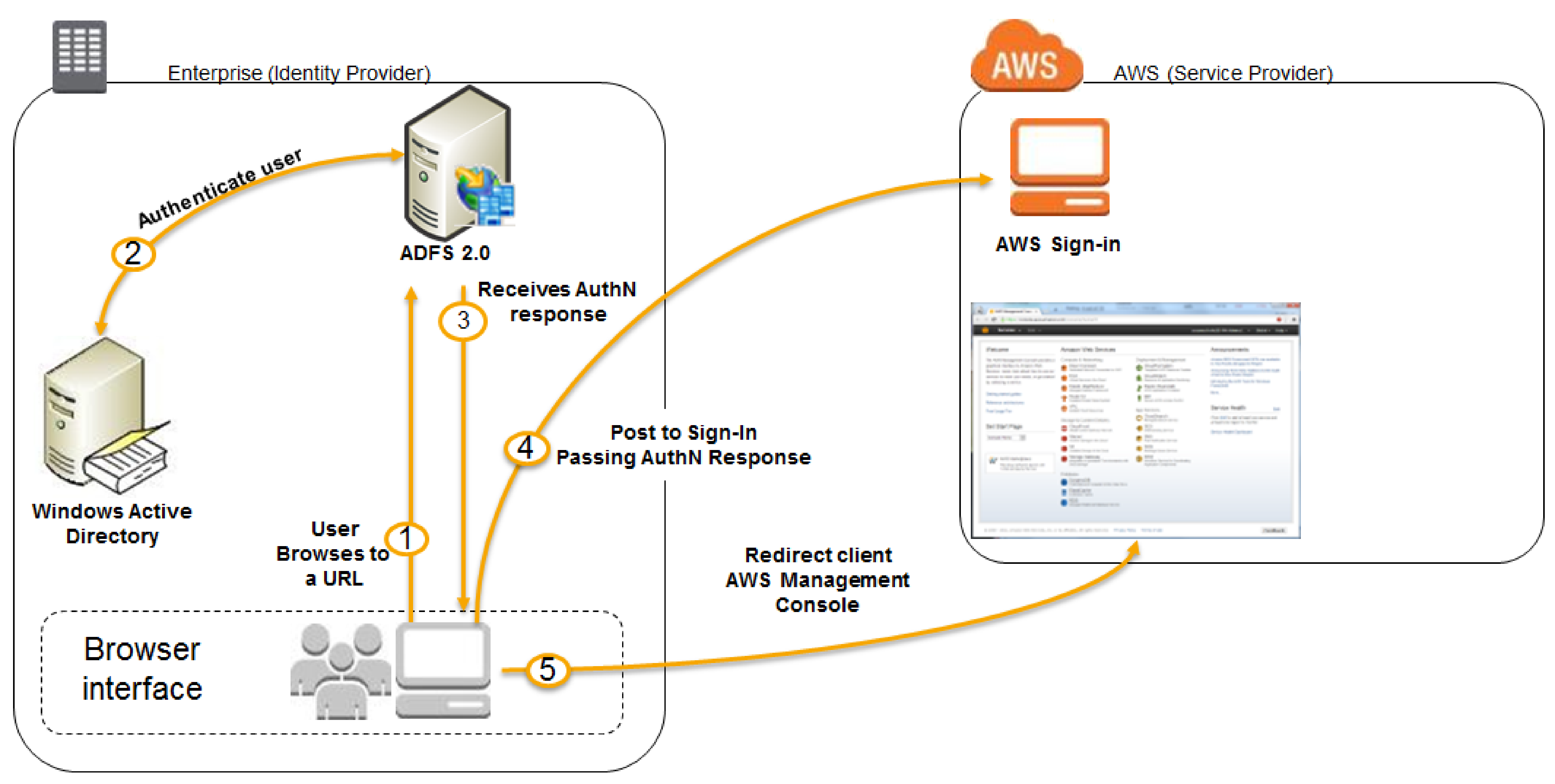
Hardware Key Fob

- ✓ SurePassID G-Pass Time-based 6-Digit Token

IAM Roles

- AWS identity object with an IAM Policy
- Can be used by persons, AWS services, and custom code
- Relies on short-lived one time usage credentials
- No usernames and passwords
- Preferred for federated access
- Allows one IAM role to assume other

Federation Support using IAM Roles



IAM Policy

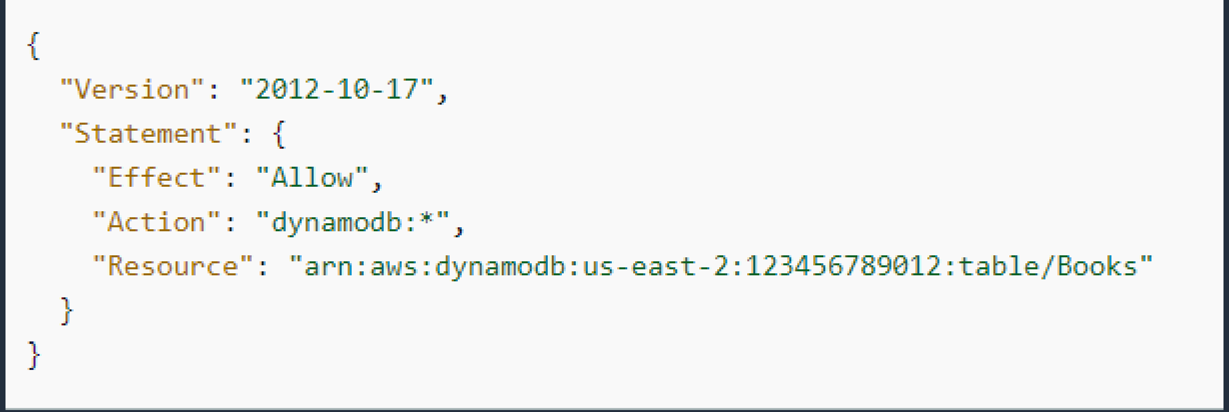
- JSON-formatted documents
- Contain statements (permissions) that specifies…

What level of access a principal (person or application) has and what actions it can perform against a particular AWS resource or list of resources.

```
{
 "Statement":[{
   "Effect":"effect",
   "Principal":"principal",
   "Action":"action",
   "Resource":"arn",
   "Condition":{
     "condition":{
       "key":"value" }
     }
   }
  ]
 }
```

Principal
Action
Resource
Condition

Supports multiple PARC statements.



```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-2:123456789012:table/Books"
  }
}
```

Identity-based IAM Policy Types

Managed Policies (Recommended)

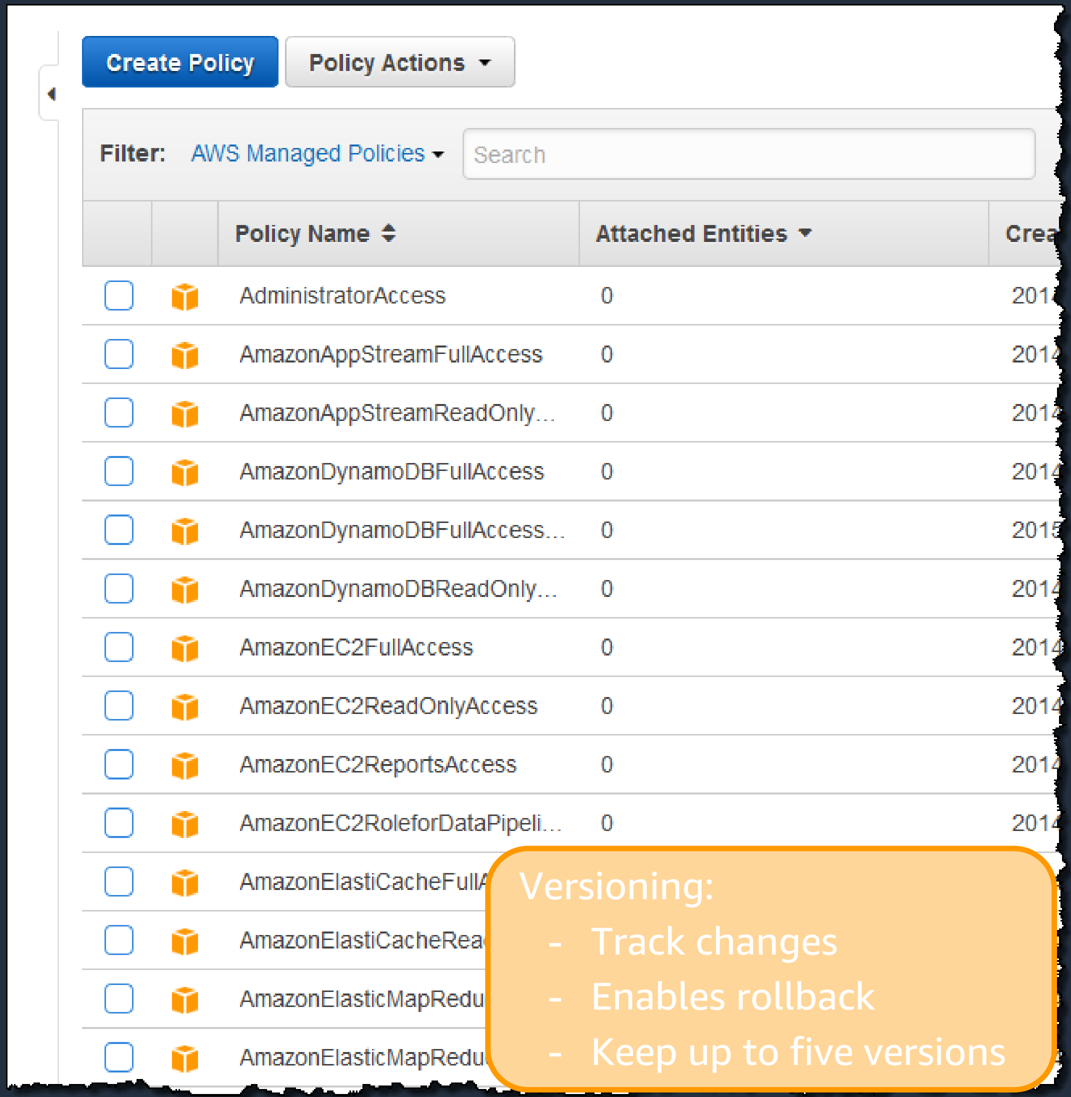
- Standalone object
- AWS managed policies
- Customer managed policies
- Reusable
- Versioning

<u>Limits:</u> 10 managed policies to a user, role, or group. Size of each managed policy cannot exceed 6,144 characters.

Inline Policies

- Embedded into a user, group or role
- Disposable / Temporary

<u>Limits:</u> Unlimited policies to a user, role, or group. Policy size cannot exceed the following. User policy - 2,048 characters; Role policy size - 10,240 characters; Group policy - 5,120 characters.



Filter: AWS Managed Policies ▾ Search

		Policy Name ⬍	Attached Entities ▾	Crea
□		AdministratorAccess	0	201
□		AmazonAppStreamFullAccess	0	2014
□		AmazonAppStreamReadOnly...	0	2014
□		AmazonDynamoDBFullAccess	0	2014
□		AmazonDynamoDBFullAccess...	0	2015
□		AmazonDynamoDBReadOnly...	0	2014
□		AmazonEC2FullAccess	0	2014
□		AmazonEC2ReadOnlyAccess	0	2014
□		AmazonEC2ReportsAccess	0	2014
□		AmazonEC2RoleforDataPipeli...	0	2014
□		AmazonElastiCacheFullA		
□		AmazonElastiCacheRea		
□		AmazonElasticMapRedu		
□		AmazonElasticMapRedu		

Versioning:

- Track changes
- Enables rollback
- Keep up to five versions

IAM Summary

- IAM consists of Users, Groups, Roles, and Policies.
- **IAM is universal**. It does not apply to regions at this time.
- The "**root account**" is simply the account created when first setup your AWS account. It has complete Admin access.
- New Users have **NO permissions** when first created.
- New Users are assigned **Access Key ID & Secret Access Keys** when first created
  - **These are not the same as password**, and you cannot use the Access Key ID & Secret Access Key to Login in to the console. You can use this to access AWS via the APIs and Command Line however.
  - **You only get to view these once.** If you lose them, you have to regenerate them; save them in secure location.
- **Always setup Multifactor Authentication on your root account.**
- **You can create and customize your own password rotation policies.**

Quick Poll

Which of the following is not a component of IAM?

1. Roles
2. Users
3. Organizational Units
4. Groups

Quick Poll

Which of the following is not a component of IAM?

1. ~~Roles~~
2. ~~Users~~
3. Organizational Units
4. ~~Groups~~

Quick Poll

When you create a new user, that user ______:

1. Will be able to interact with AWS using their access key ID and secret access key using the API, CLI, or SDK
2. Will be able to log in to the console only after MFA is enabled
3. Will only be able to log in to the console in the region in which that user was created
4. Will be able to log in to the console, using their access key ID and secret access key

Quick Poll

When you create a new user, that user _____:

1. Will be able to interact with AWS using their access key ID and secret access key using the API, CLI, or SDK
2. ~~Will be able to log in to the console only after MFA is enabled~~
3. ~~Will only be able to log in to the console in the region in which that user was created~~
4. ~~Will be able to log in to the console, using their access key ID and secret access key~~

④

AWS Organizations

As you increase usage within one account….

AWS Account

Everything

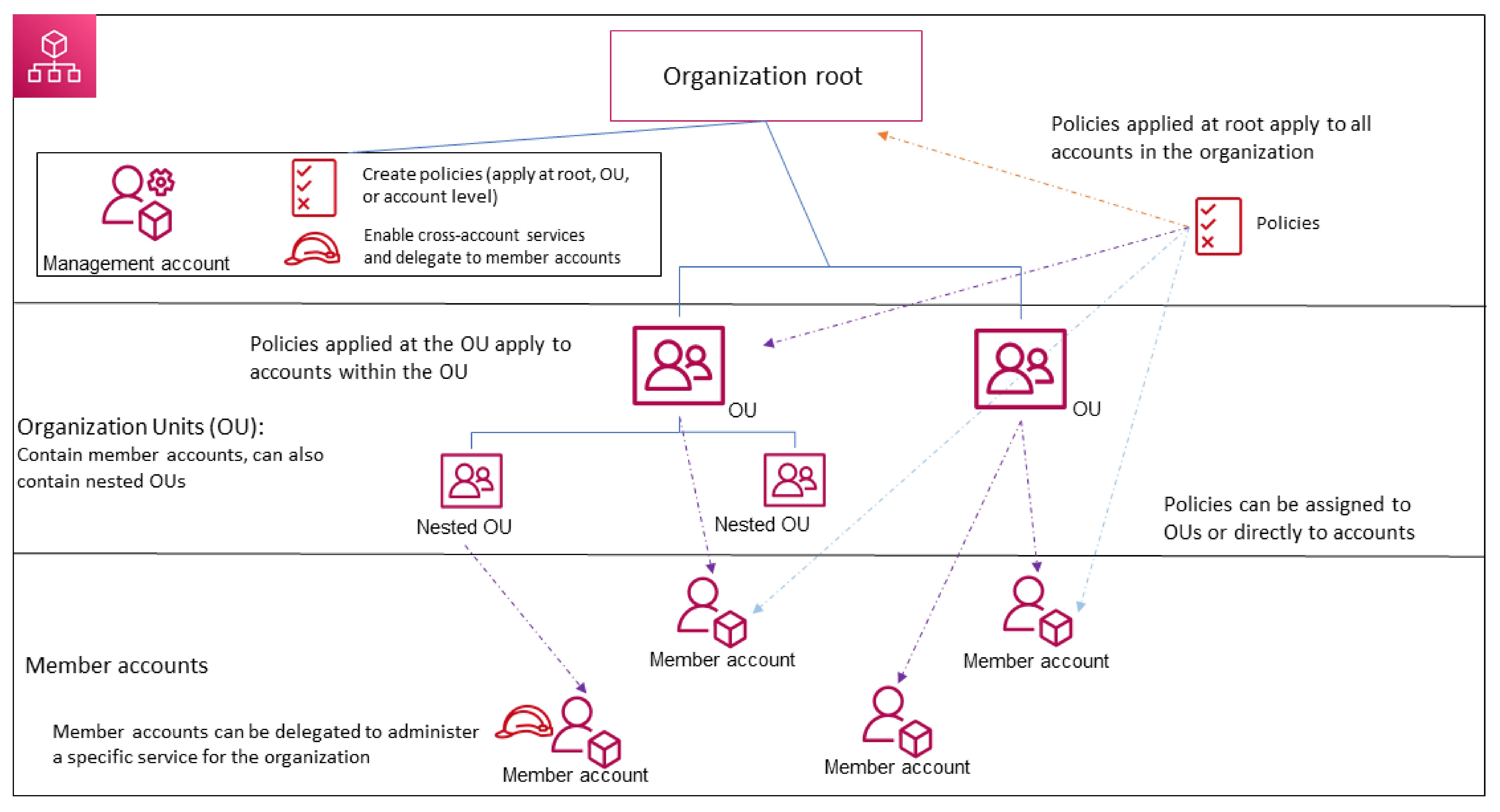
“Gray” boundaries

Complicated and messy over time

Difficult to track resources

People stepping on each other

AWS Organizations – Concepts and terms



Organization root

Management account

Create policies (apply at root, OU, or account level)

Enable cross-account services and delegate to member accounts

Policies applied at root apply to all accounts in the organization

Policies

Policies applied at the OU apply to accounts within the OU

Organization Units (OU):
Contain member accounts, can also contain nested OUs

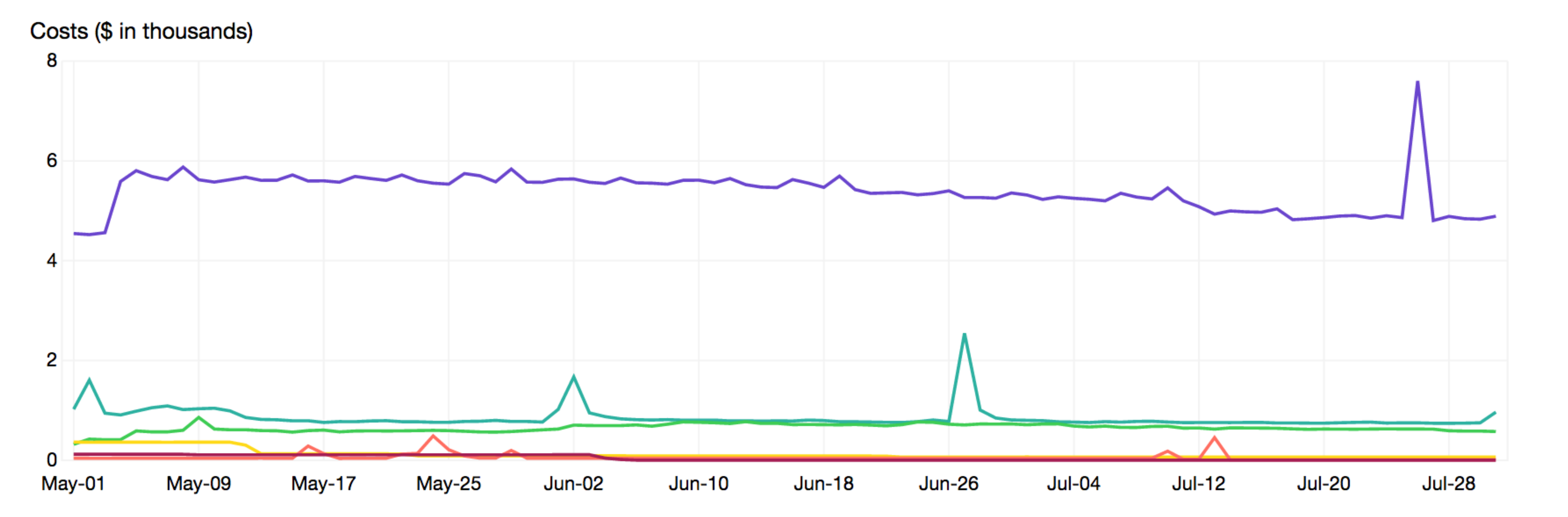
Policies can be assigned to OUs or directly to accounts

Member accounts

Member accounts can be delegated to administer a specific service for the organization

Centrally manage costs and billing

- Consolidate usage across all accounts into a single bill
- Manage your tax settings across accounts from a central Tax console
- Gain insights and manage spending across your organization (AWS Budgets and AWS Cost Explorer)

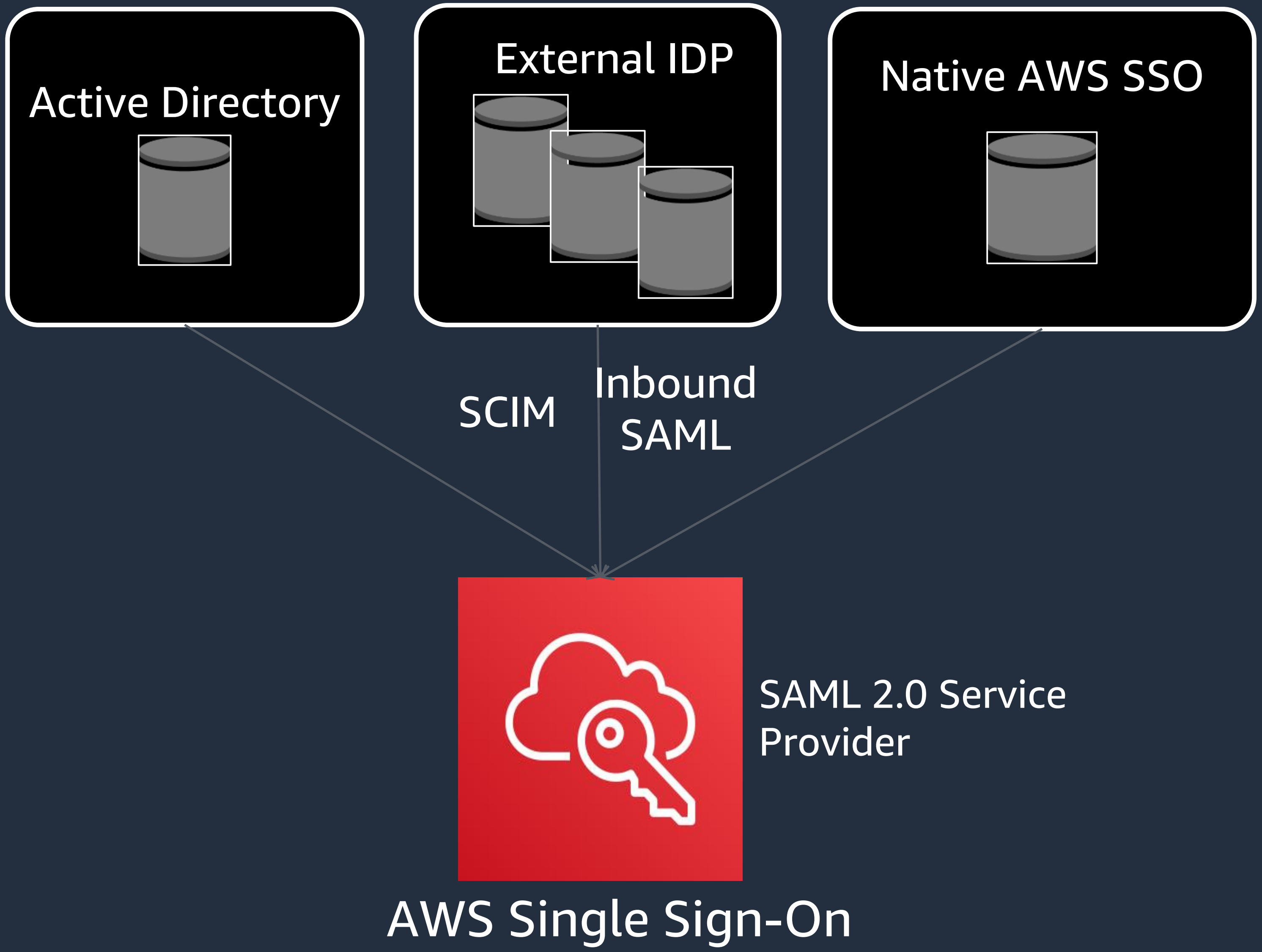


Monthly cost by member account

5

AWS SSO

Choose your identity store



Select your identity provider and centrally manage your users and groups

AWS Directory Service

Managed service for Active Directory

Use your existing Corporate Credentials for

- AWS-based applications
- AWS Management Console

Microsoft Managed AD

Based on Microsoft Active Directory in Windows Server 2012 R2. Supports adding trust relationships with on-premises domains. Extend your schema using MS AD

Simple AD

A Microsoft Active-Directory compatible directory powered by Samba 4.

AD Connector

Connect to your on-premises Active Directory. Integrates with existing RADIUS MFA solutions.

Quick Poll

You want to allow users of your company to login to AWS Console with their Active Directory credentials. Which of the following services will NOT meet your requirements? (Select TWO)

1. Simple AD
2. Cloud Active Directory
3. AD Connector
4. Cognito user pools

Quick Poll

Users of your company need to access AWS Console with their Active Directory credentials. Which of the following services will NOT meet your requirements? (Select TWO)

1. ~~Simple AD~~
2. Cloud Active Directory
3. ~~AD Connector~~
4. Cognito user pools

6

Sample Questions

Sample Question

Question: You need to run a production batch process quickly that will use several EC2 instances. The process cannot be interrupted and must be completed within a short time period.

What is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Reserved instances
2. Spot instances
3. On-demand instances
4. Flexible instances

Sample Question – breaking down the question

Question: You need to run a production **batch process quickly** that will use **several EC2 instances**. The process **cannot be interrupted** and **must be completed within a short time period**.

What is likely to be the **MOST cost-effective choice** of EC2 instance type to use for this requirement?

1. Reserved instances
2. Spot instances
3. On-demand instances
4. Flexible instances

Sample Question – eliminating options

Question: You need to run a production **batch process quickly** that will use **several EC2 instances**. The process **cannot be interrupted** and **must be completed within a short time period**.

What is likely to be the **MOST cost-effective choice** of EC2 instance type to use for this requirement?

1. Reserved instances
2. Spot instances
3. On-demand instances
4. ~~Flexible instances~~

Sample Question – final answer

Question: You need to run a production **batch process quickly** that will use **several EC2 instances**. The process **cannot be interrupted** and **must be completed within a short time period**.

What is likely to be the **MOST cost-effective choice** of EC2 instance type to use for this requirement?

~~1. Reserved instances~~

~~2. Spot instances~~

3. On-demand instances

~~4. Flexible instances~~

Sample Question

Question: You have been asked to come up with a solution for providing single sign-on to existing staff in your company who manage on-premises web applications and now need access to the AWS management console to manage resources in the AWS cloud.

Which product combinations provide the best solution to achieve this requirement?

1. Use your on-premises LDAP directory with IAM
2. Use IAM and MFA
3. Use the AWS Secure Token Service (STS) and SAML
4. Use IAM and Amazon Cognito

Sample Question – breaking down the question

Question: You have been asked to come up with a solution for providing single sign-on to existing staff in your company who manage **<u>on-premises</u>** web applications and now **<u>need access to the AWS management console</u>** to manage resources in the AWS cloud.

Which **<u>product combinations</u>** provide the best solution to achieve this requirement?

1. Use your on-premises LDAP directory with IAM
2. Use IAM and MFA
3. Use the AWS Secure Token Service (STS) and SAML
4. Use IAM and Amazon Cognito

Sample Question – eliminating options

Question: You have been asked to come up with a solution for providing single sign-on to existing staff in your company who manage **on-premises** web applications and now **need access to the AWS management console** to manage resources in the AWS cloud.

Which **product combinations** provide the best solution to achieve this requirement?

1. Use your on-premises LDAP directory with IAM
2. ~~Use IAM and MFA~~
3. Use the AWS Secure Token Service (STS) and SAML
4. ~~Use IAM and Amazon Cognito~~

Sample Question – final answer

Question: You have been asked to come up with a solution for providing single sign-on to existing staff in your company who manage **on-premises** web applications and now **need access to the AWS management console** to manage resources in the AWS cloud.

Which **product combinations** provide the best solution to achieve this requirement?

1. ~~Use your on-premises LDAP directory with IAM~~
2. ~~Use IAM and MFA~~
3. Use the AWS Secure Token Service (STS) and SAML
4. ~~Use IAM and Amazon Cognito~~

Session 1 Additional Materials

1. AWS Well Architected Framework - https://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf
2. EC2 FAQ

   https://aws.amazon.com/ec2/faqs/
3. IAM FAQ

   https://aws.amazon.com/iam/faqs/
4. AWS Organizations FAQ

   https://aws.amazon.com/organizations/faqs/

Session 1 Additional Materials

5. EC2 Instance Types

https://aws.amazon.com/ec2/instance-types/

6. EC2 Pricing

https://aws.amazon.com/ec2/pricing/

7. Exam Readiness

https://aws.amazon.com/training/course-descriptions/exam-workshop-solutions-architect-associate/

8. AWS SSO FAQ

https://aws.amazon.com/single-sign-on/faqs/

9. Placement Groups

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Hands-on Demo

Q&A

Nayef M Khan

Solutions Architect

Thank You!