Welcome Back to AWS Cloud Practitioner

Your instructor:

Michael J Shannon

Class will begin at 11:00 A.M. Eastern Standard Time (EST)

Choosing the Right Region

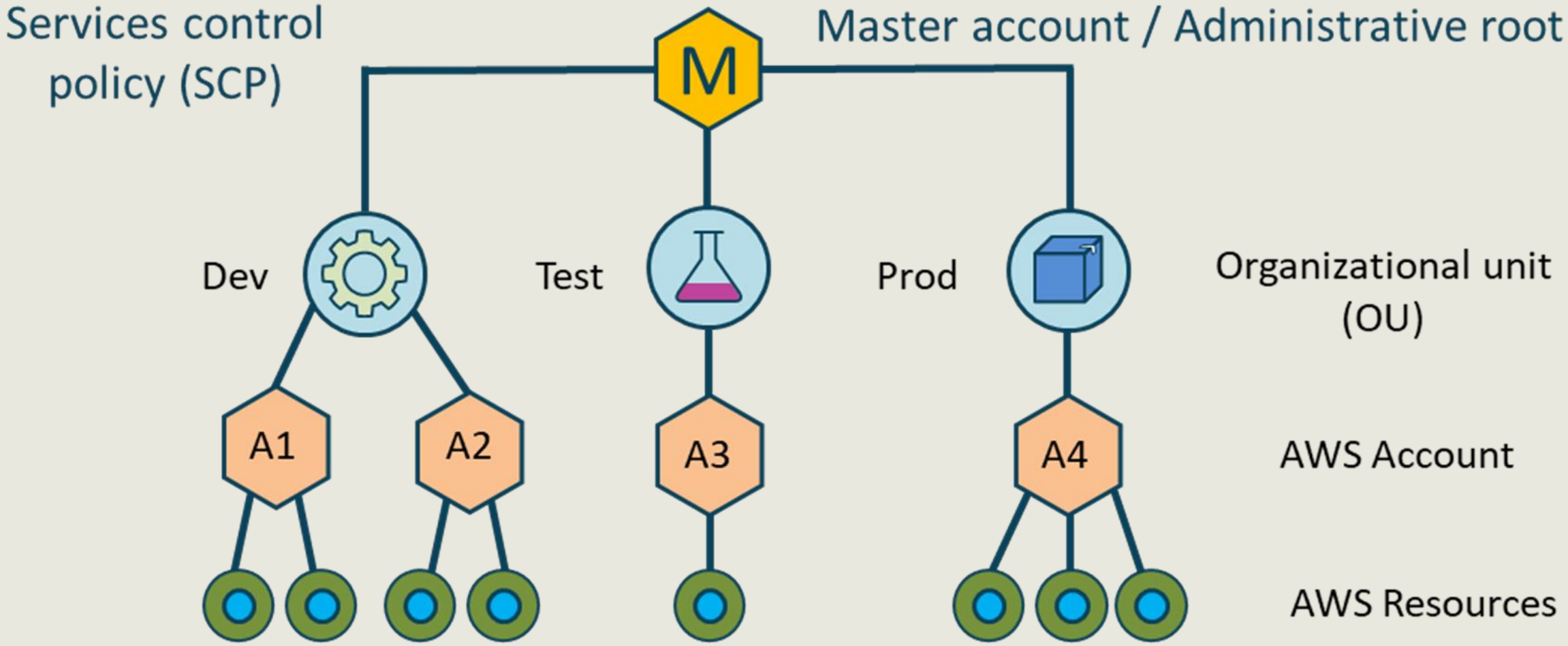
- When selecting the proper Region for your services, data, and applications, consider the following 4 business factors:
  - Compliance with data governance and legal requirements
  - Proximity to your customers
  - Available services within a Region
  - Pricing

Administer AWS from a Master Account

- AWS Organizations provide policy-based management for multiple AWS accounts
  - Create groups of accounts
  - Automate account creation using console and APIs
  - Apply and manage policies for account groups
- Enables you to simplify costs and take advantage of quantity discounts with a **single consolidated bill**
- Centrally manage **Service Control Policies (SCPs)** across multiple accounts without using custom scripts or manual processes

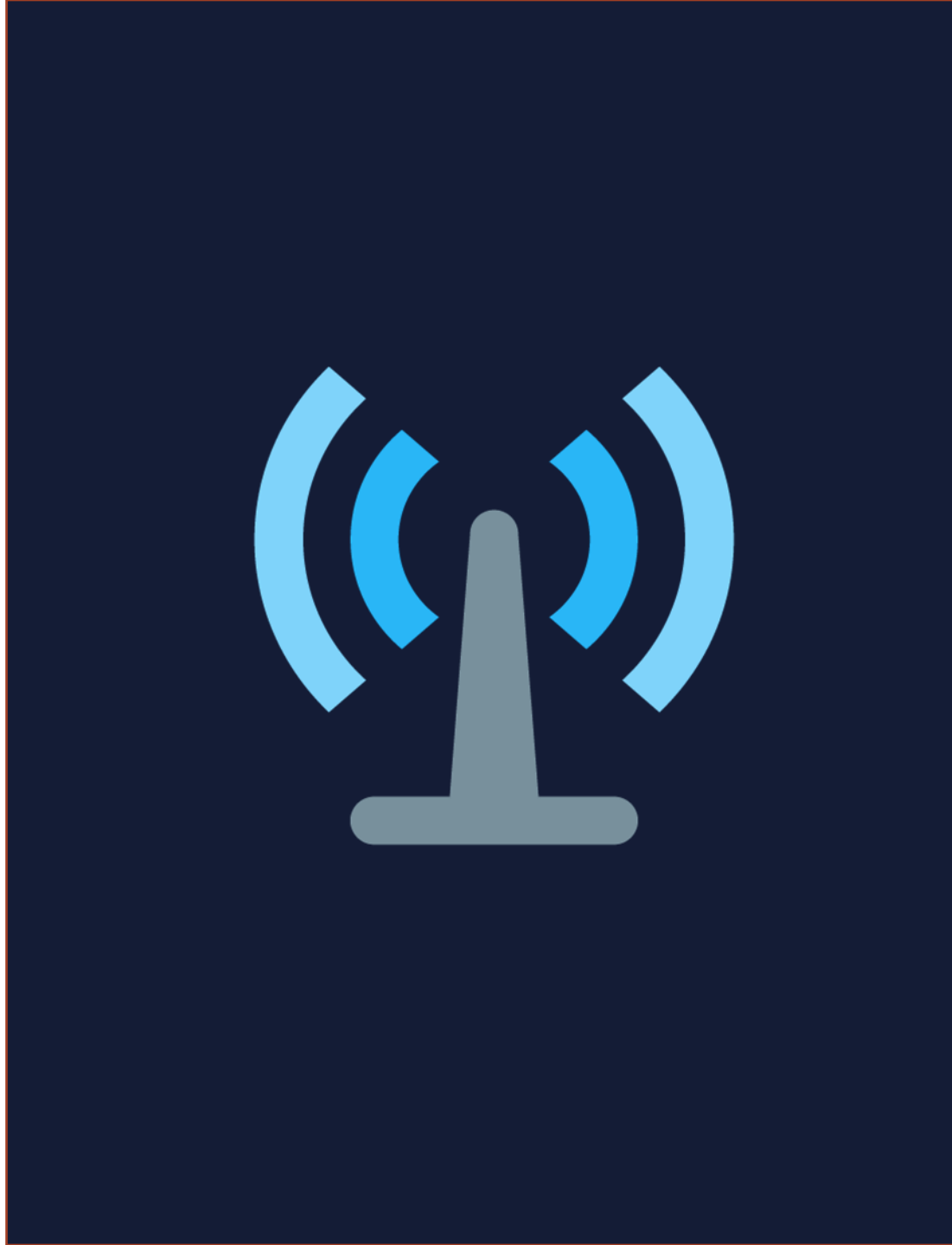
AWS Organizations

AWS Organizations



AWS Control Tower

- Enterprises with multiple AWS accounts can use Control Tower to easily set up and manage a secure, multi-account environment based on established best practices
- Operators can provision new AWS accounts with a few clicks and be confident that they conform to organizational governance and policies
- Excellent solution if you are:
  - Building a new AWS environment
  - Beginning a journey to AWS
  - Launching a new cloud initiative
  - Working with existing accounts



AWS Support Models

- Basic
- Developer
- Business
- Enterprise

Basic is the only free plan

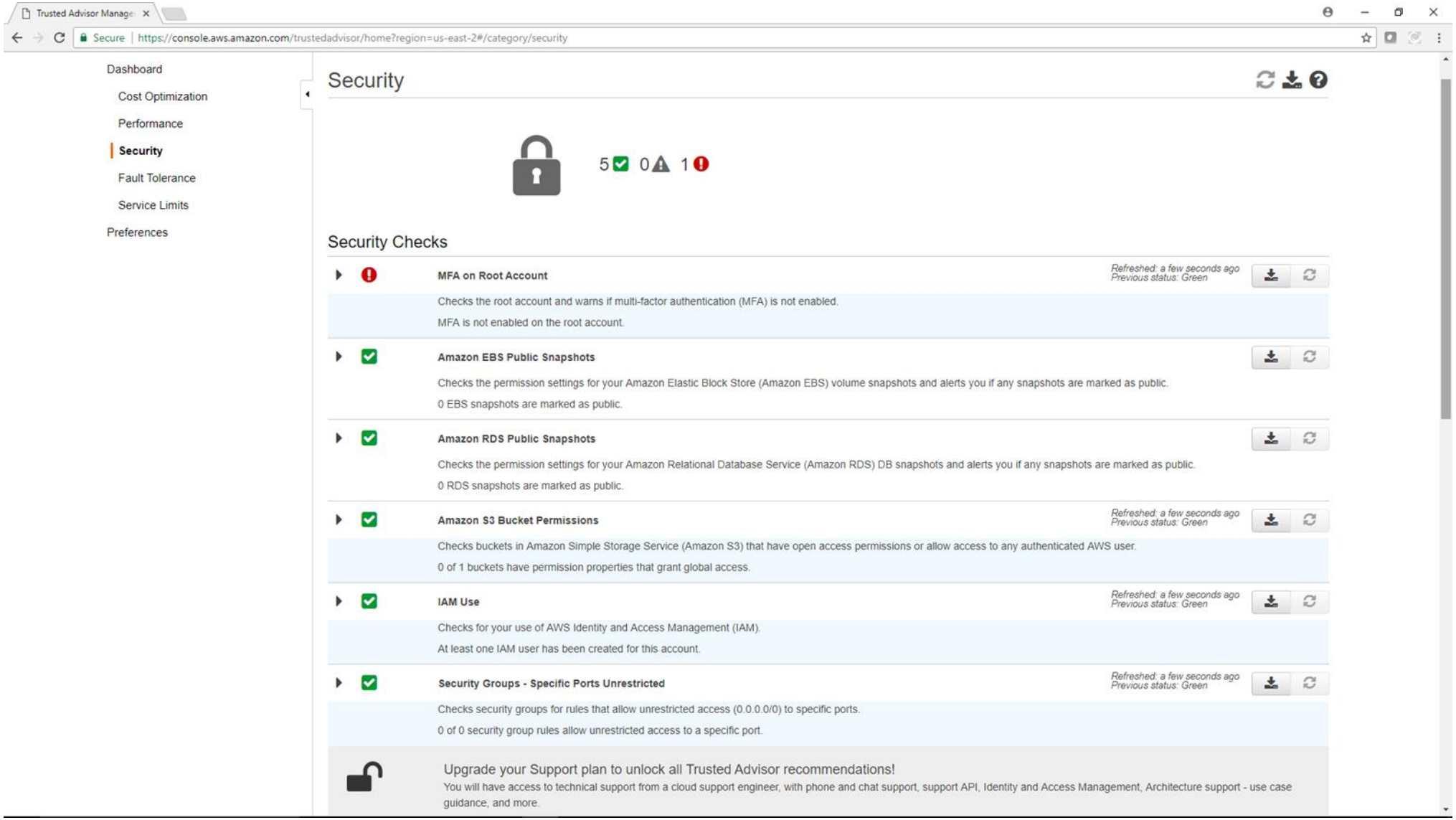
Business and Enterprise Plans

- Only these plans can use AWS Shield Advanced due to 24/7 support teams
- AWS Infrastructure Event Management (IEM) offers architecture and scaling guidance along with operational support for an additional fee
- AWS Support API provides programmatic access to some of the features of the AWS Service Catalog for support case management operations and Trusted Advisor operations (to access the checks)
- Enterprise plans only get the Concierge Support Team
- Get access to all 115 Trusted Advisor checks (14 cost optimization, 17 security, 24 fault tolerance, 10 performance, and 50 service limits) and associated recommendations

Trusted Advisor

- Online tool that offers real time guidance on provisioning resources using AWS best practices
- “Checks” help to optimize an AWS infrastructure, increase security, enhance performance, reduce total costs, and monitor service limits
- AWS Basic and Developer Support plan customers get 7 security checks and 50 service limit (quota) checks:
  - S3 Bucket Permissions
  - Security Groups - Specific Ports Unrestricted
  - IAM Use
  - MFA on Root Account
  - EBS and RDS Public Snapshots

AWS Trusted Advisor



Identity and Access Management (IAM)

- Identity and Access Management is a core AWS security service that enables the secure control of access to AWS resources
- IAM manages who is signed in (authenticated) and has permissions (authorized) to use resources

IAM and the Root User Account

- The AWS account root user is separate from IAM
- The Root user is a single standalone sign-in identity
- The root user has total access to all AWS services and resources in the account
- Do not use the root user account for common tasks
- Use the root user only to create your first IAM highest privilege administrative user

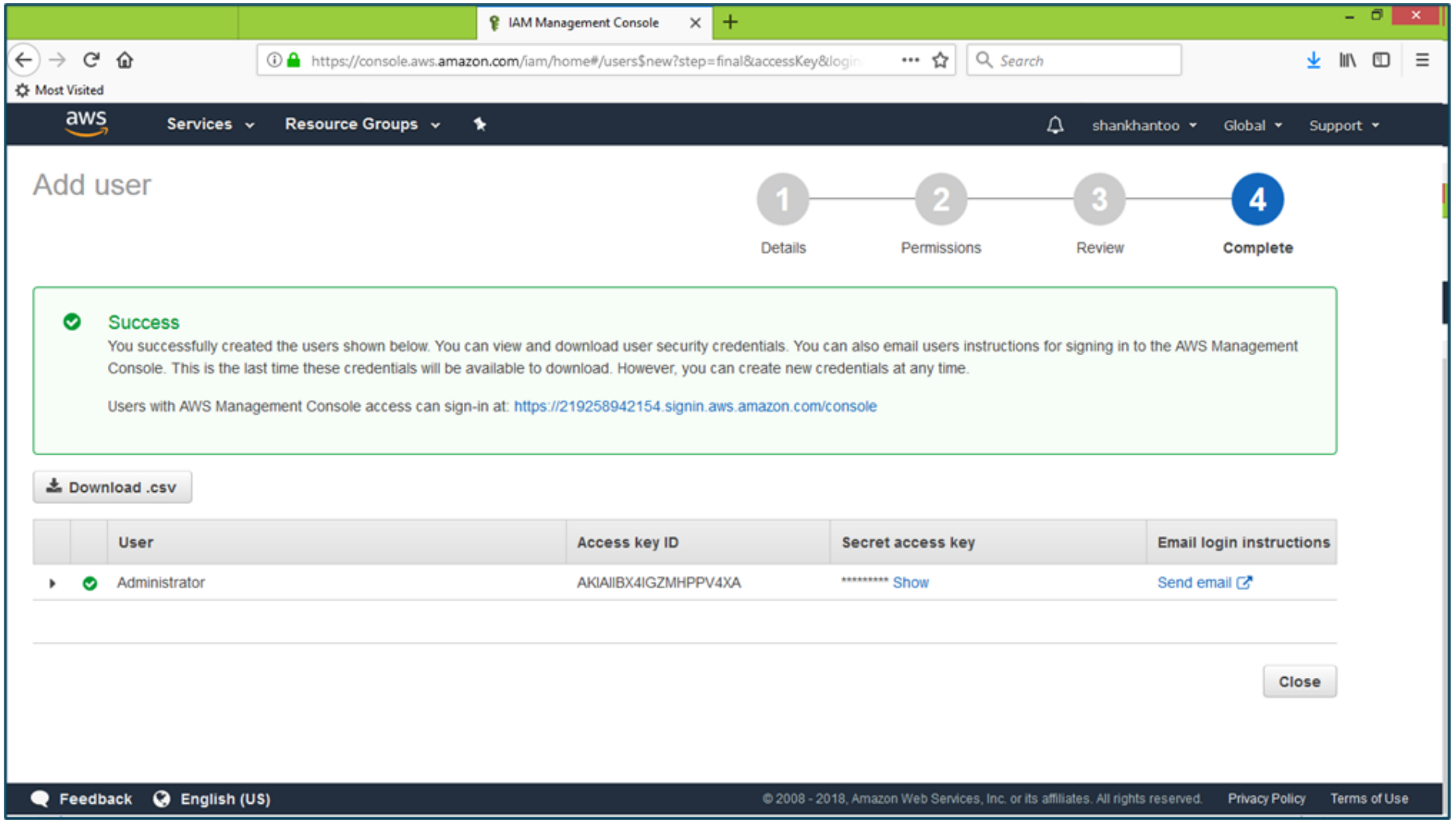
IAM Password Policies

- Password policies apply to all IAM users but not to the root account user
- Must have a minimum of 8 characters and a maximum of 128 characters
- Cannot be identical to your AWS account name or e-mail address

Accessing IAM

- AWS Management Console
- AWS command line tools
- AWS software development kits – SDKs
- IAM HTTPS API

Configuring CLI Access



Configuring CLI Access

AWS Command Line Interface

https://aws.amazon.com/cli/

The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

The AWS CLI introduces a new set of simple file commands for efficient file transfers to and from Amazon S3.

Getting Started »

CLI Reference »

GitHub Project »

Community Forum »

Windows

Download and run the 64-bit or 32-bit Windows installer.

Mac and Linux

Requires Python 2.6.5 or higher.
Install using pip.

```
pip install awscli
```

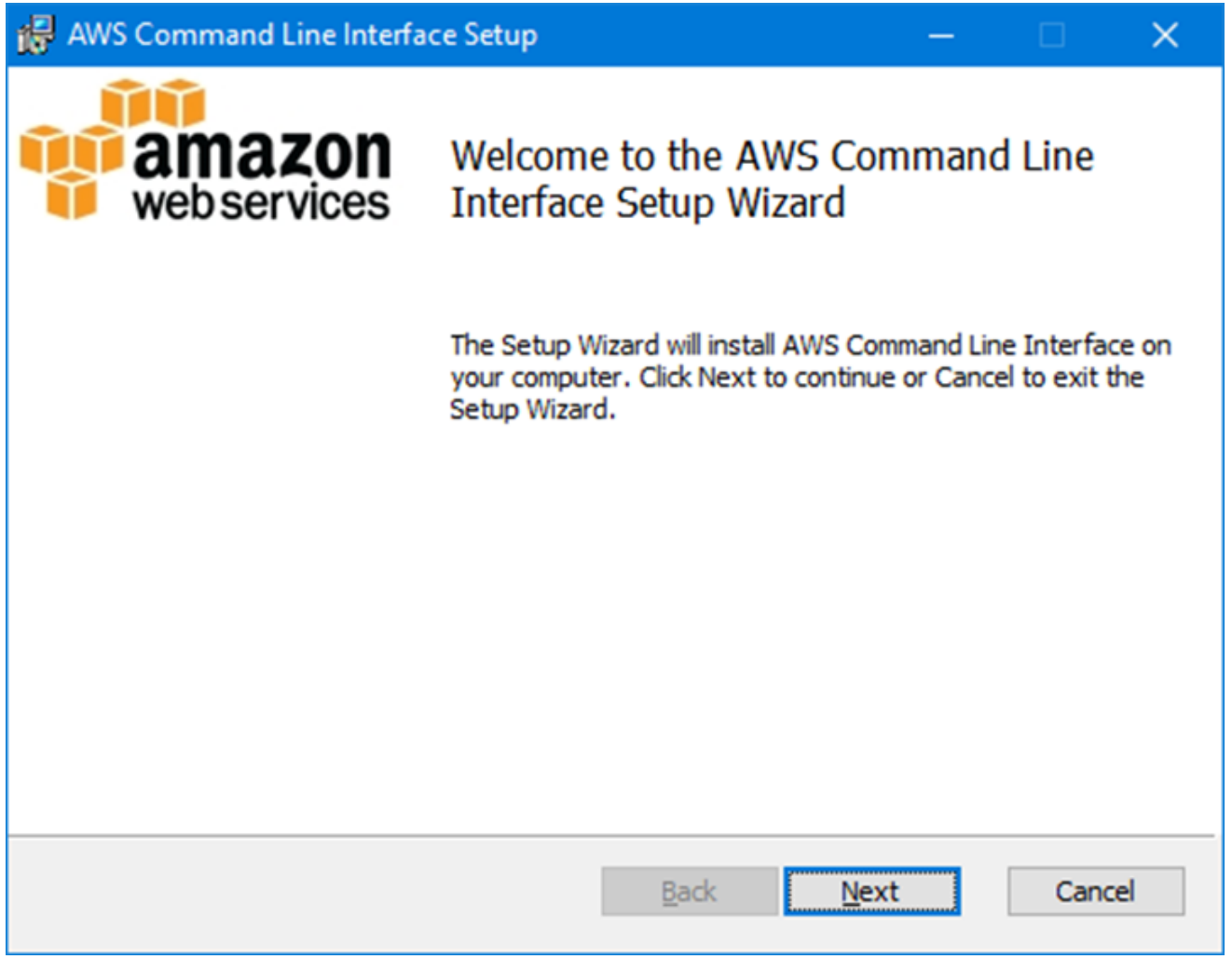
Amazon Linux

The AWS CLI comes pre-installed on Amazon Linux AMI.

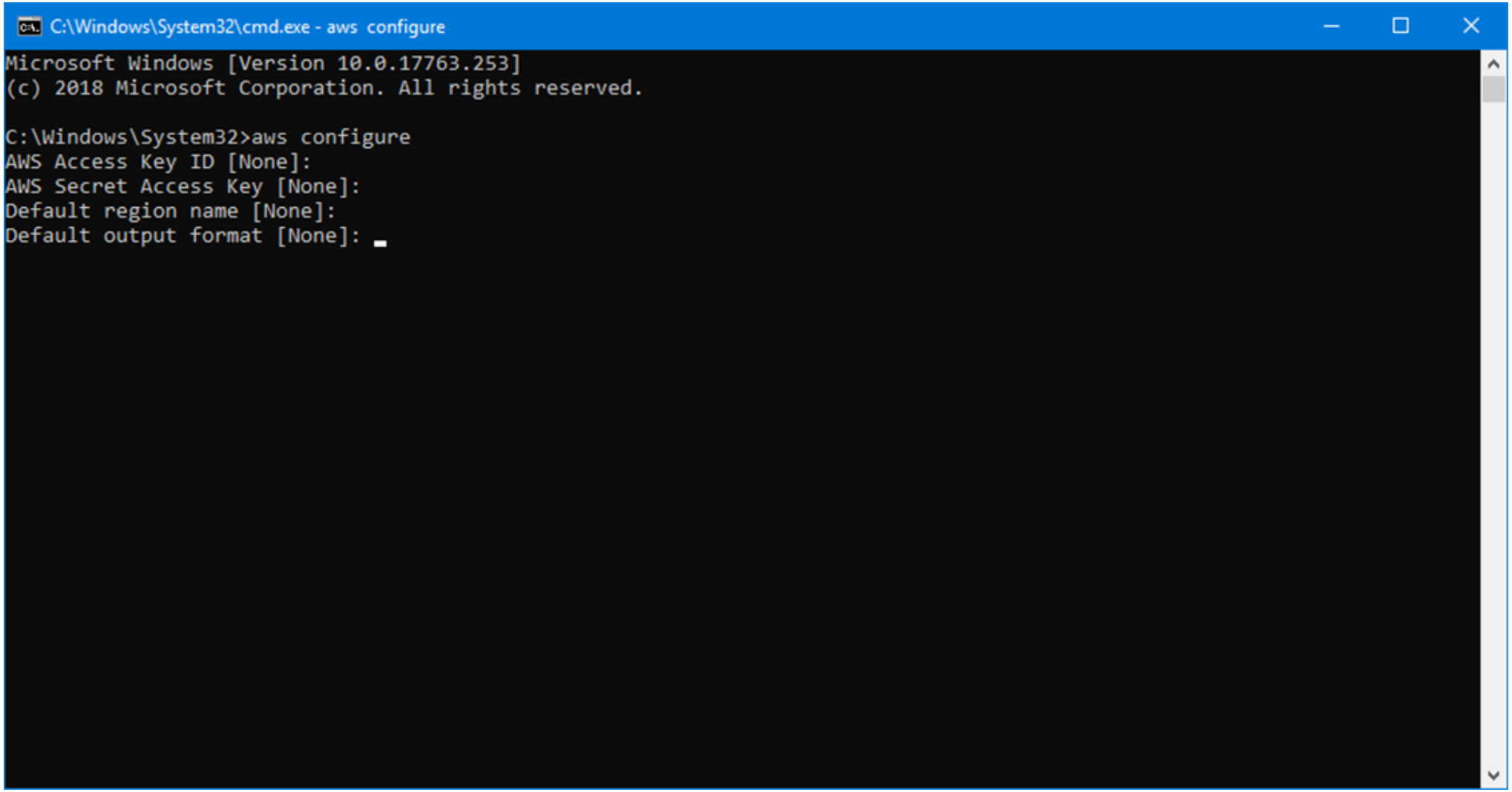
Release Notes

Check out the Release Notes for more information on the latest version.

Configuring CLI Access



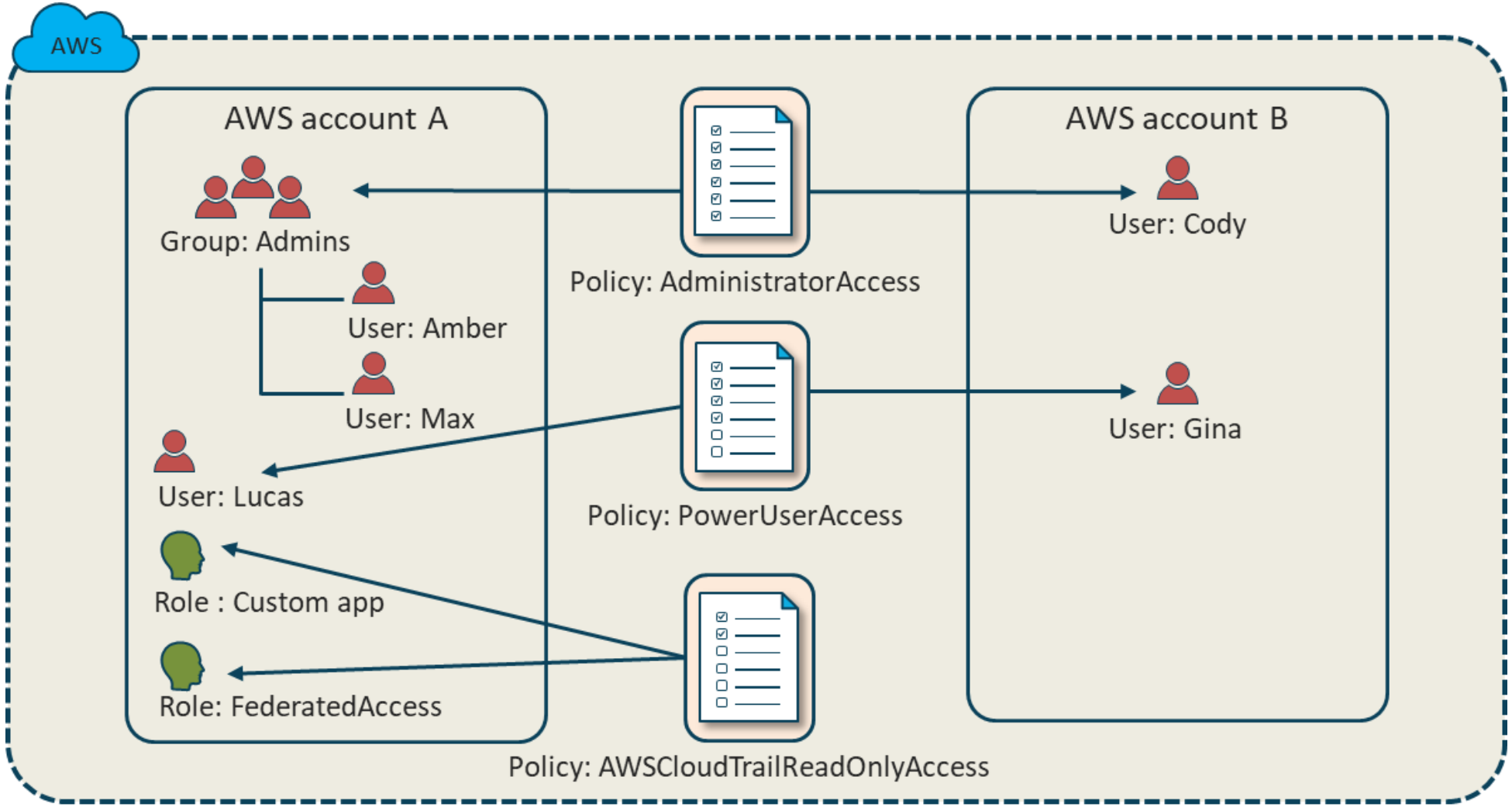
Configuring CLI Access



IAM Managed Policies

- A standalone permission set that is created and administered by AWS
- Standalone policies have their own Amazon Resource Name (ARN) that includes the policy name.
- For example: **arn:aws:iam::aws:policy/IAMReadOnlyAccess**
- They are intended to offer permissions for many common AWS use cases
  - Full-access
  - Power-user
  - Partial-access

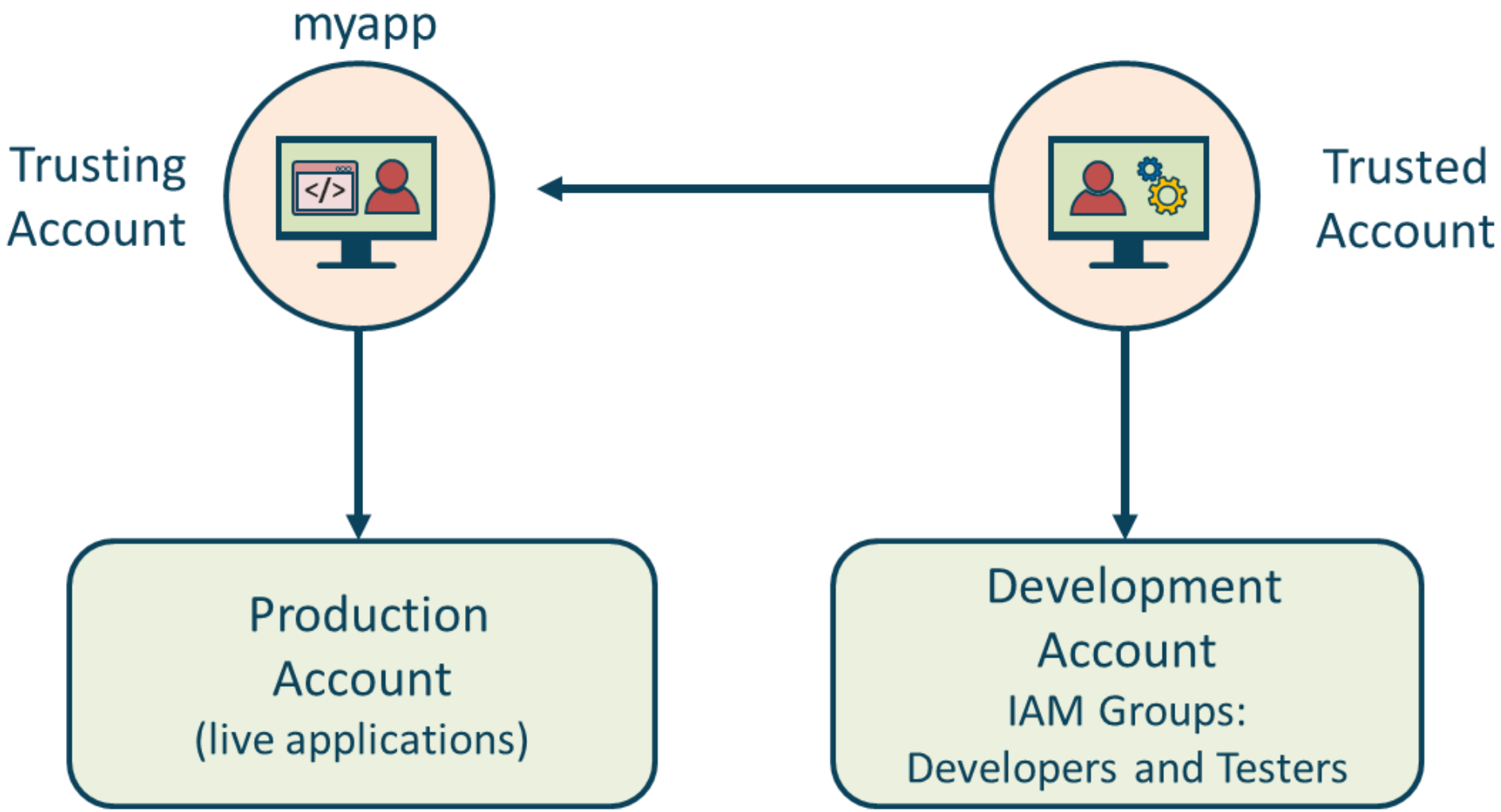
AWS Managed Policies



IAM Roles

- Identity that has permission assigned
- Intended to be assumed by a user, application, or service
- Does not have long-term credentials like passwords or keys
- AWS offers temporary credentials for the lifetime of session
- Often used to give access to identities outside of AWS

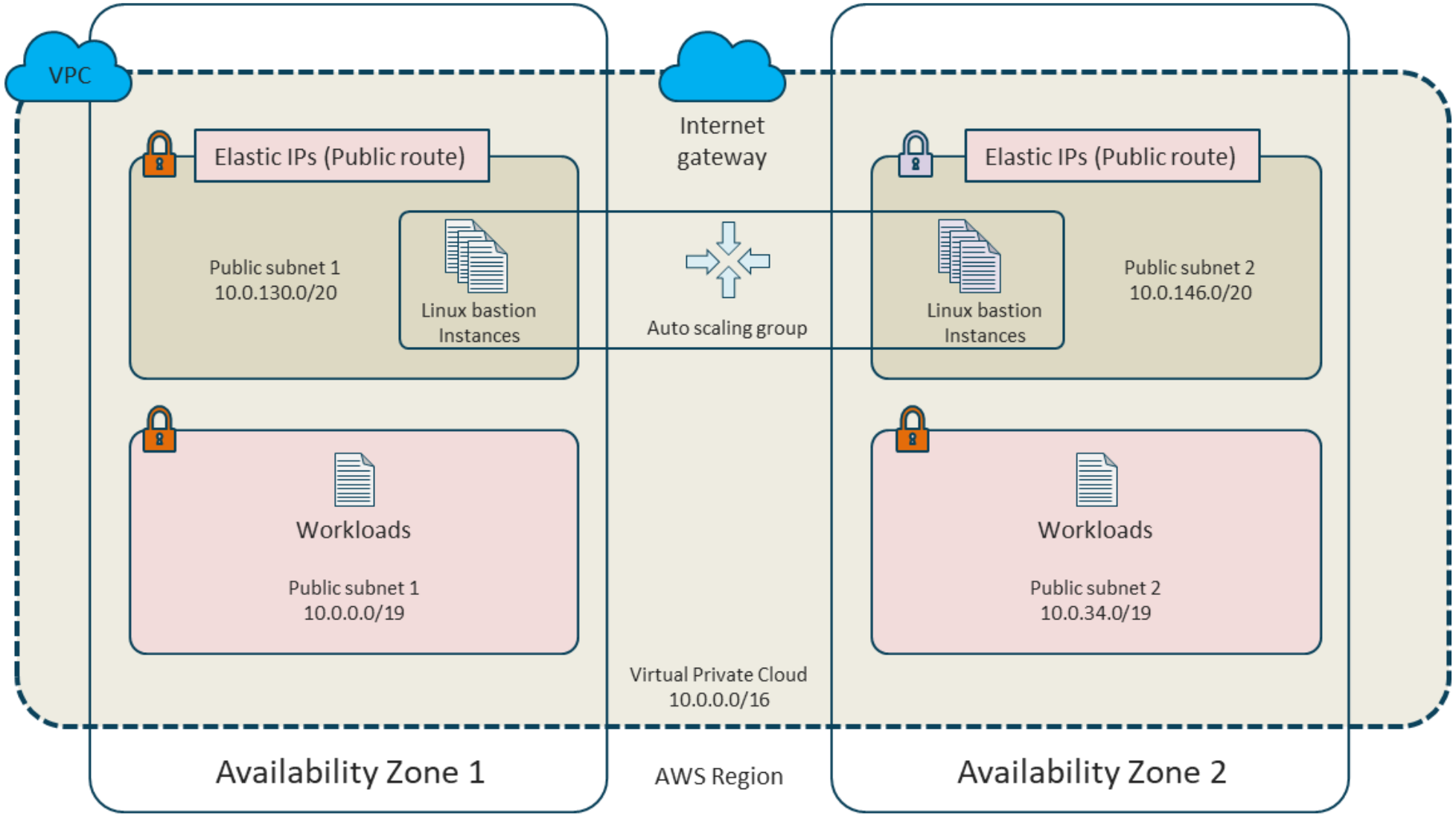
IAM Roles


myapp
Trusting Account
Trusted Account
Production Account
(live applications)
Development Account
IAM Groups:
Developers and Testers

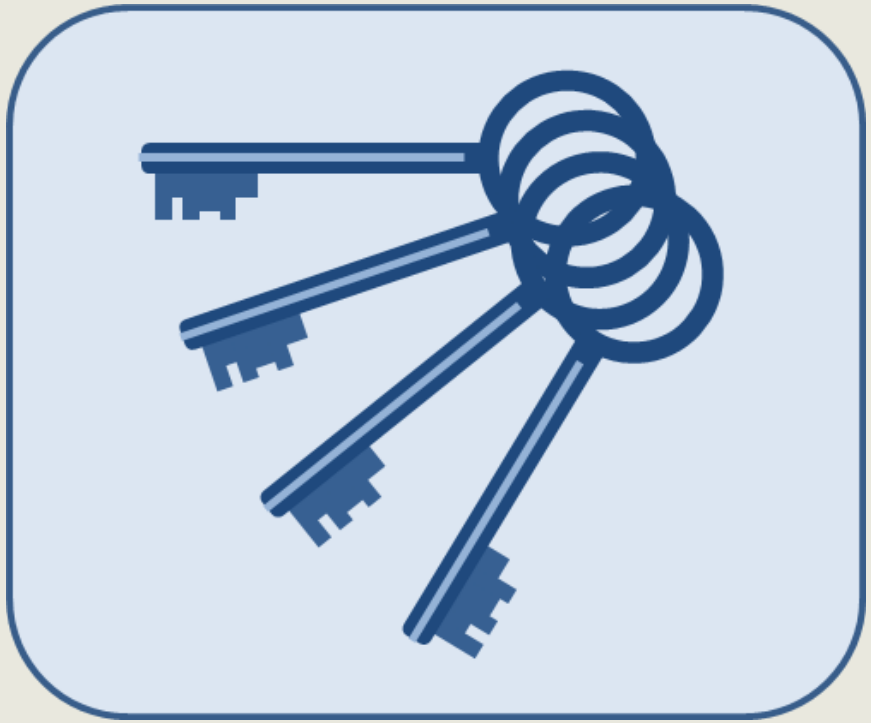
AWS STS Temporary Credentials

- A web service for creating temporary credentials
  - In your own code
  - Command-line-interface
  - Third-party tools
- Assumes necessary IAM roles with the trusted relationship
- Generates temporary, time-limited permission-based credentials only for a validity period
- Two ways to generate temporary credentials
  - Generate them with the CLI
  - Create from your code

Bastion (Jump) Hosts

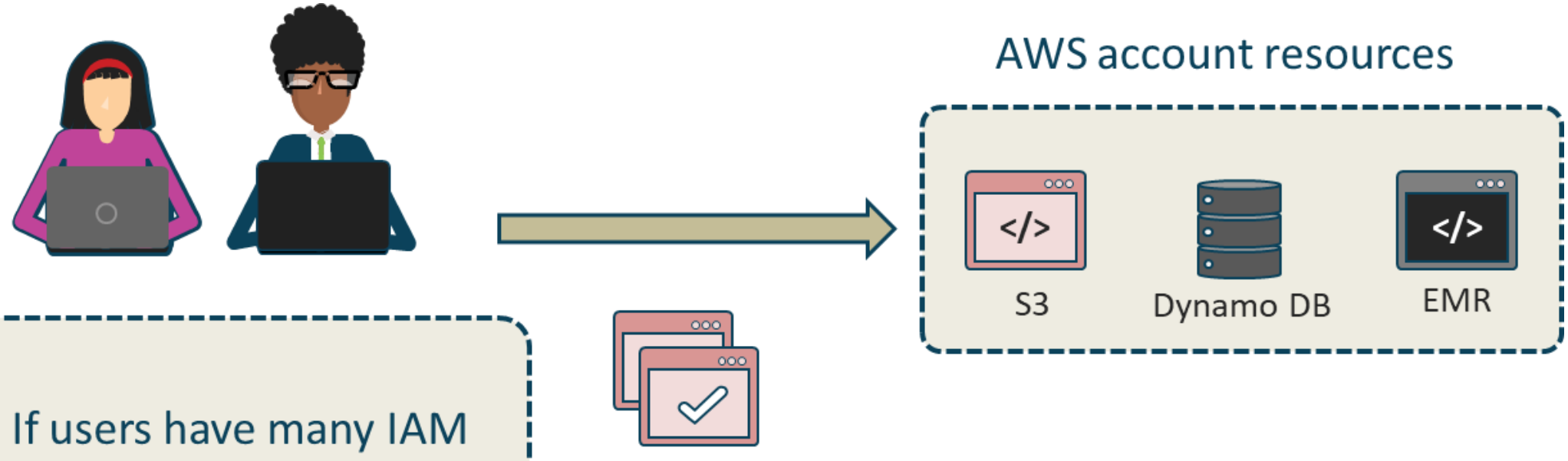


Access Keys



- Applications running outside of AWS will need access keys
- AWS SDKs will have digital signatures performed
- Signing protects message integrity by preventing tampering
- Requests must reach AWS within 15 minutes of the time stamp
- Version 4 also offers Forward Secrecy

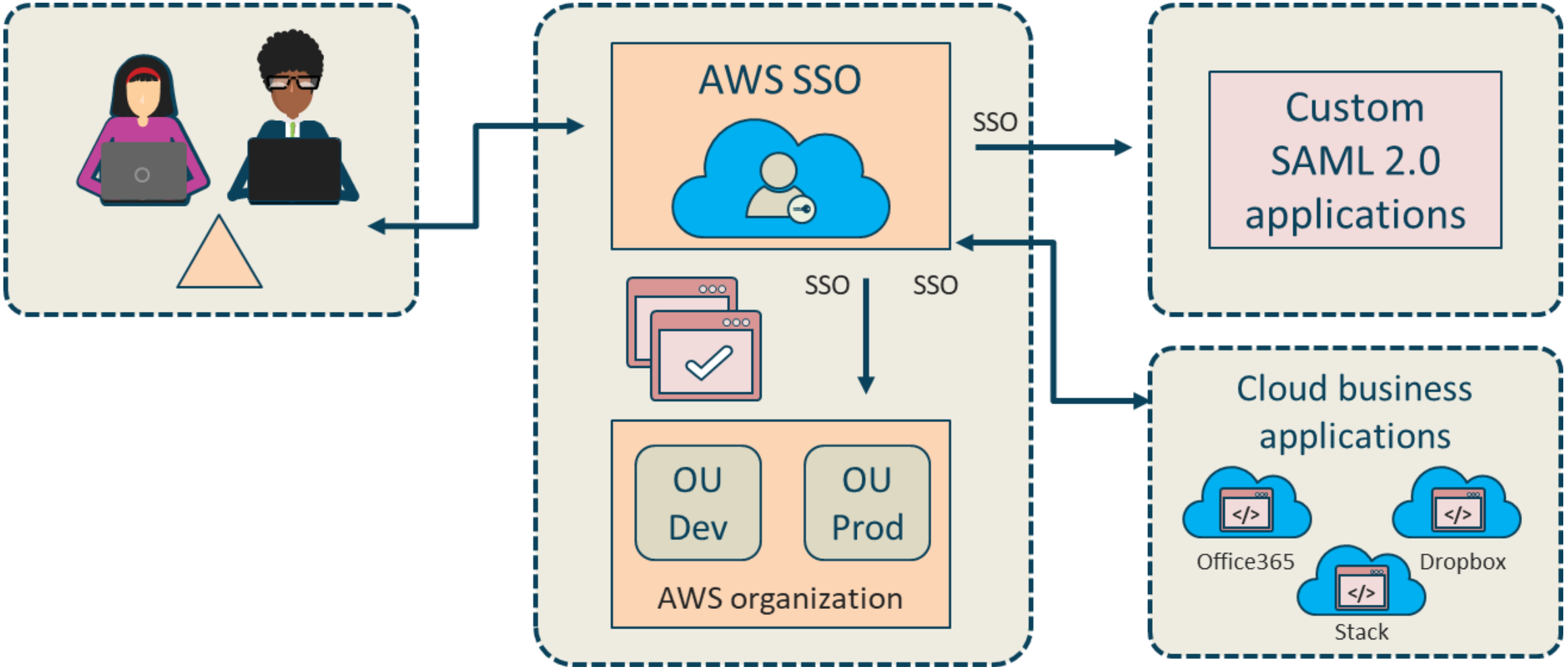
AWS Single-sign on (SSO)



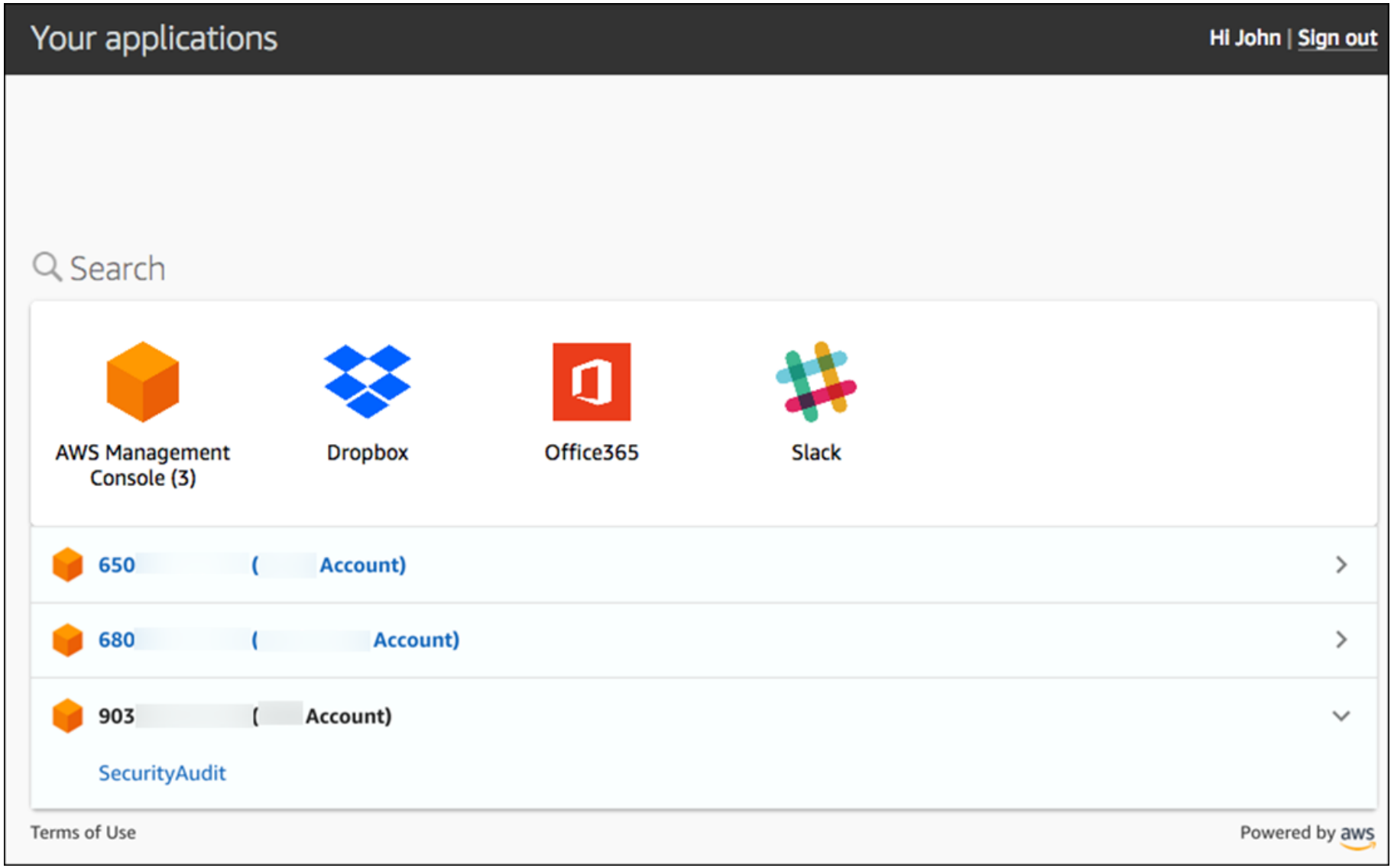
If users have many IAM accounts, consider SAML 2.0 federation to enable single-on (SSO)

Workshop: "Choose Your Own SAML Adventure: A Self-Directed Journey to AWS Federation Mastery" at AWS

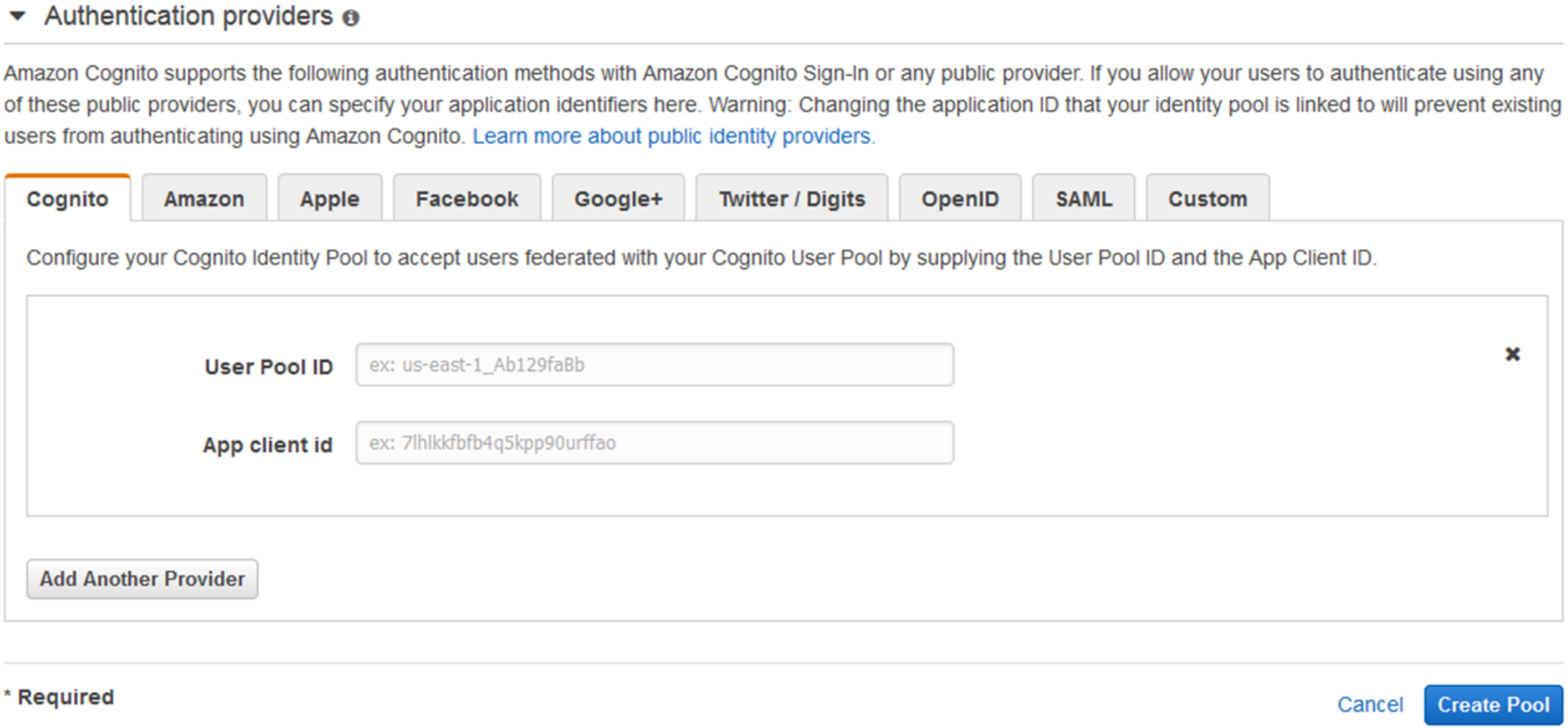
AWS SSO


AWS SSO
SSO
SSO
SSO
OU
Dev
OU
Prod
AWS organization
Custom
SAML 2.0
applications
Cloud business
applications
Office365
Dropbox
Stack

AWS SSO


Your applications
Hi John | Sign out
Search
AWS Management Console (3)
Dropbox
Office365
Slack
650 (Account)
680 (Account)
903 (Account)
SecurityAudit
Terms of Use
Powered by aws

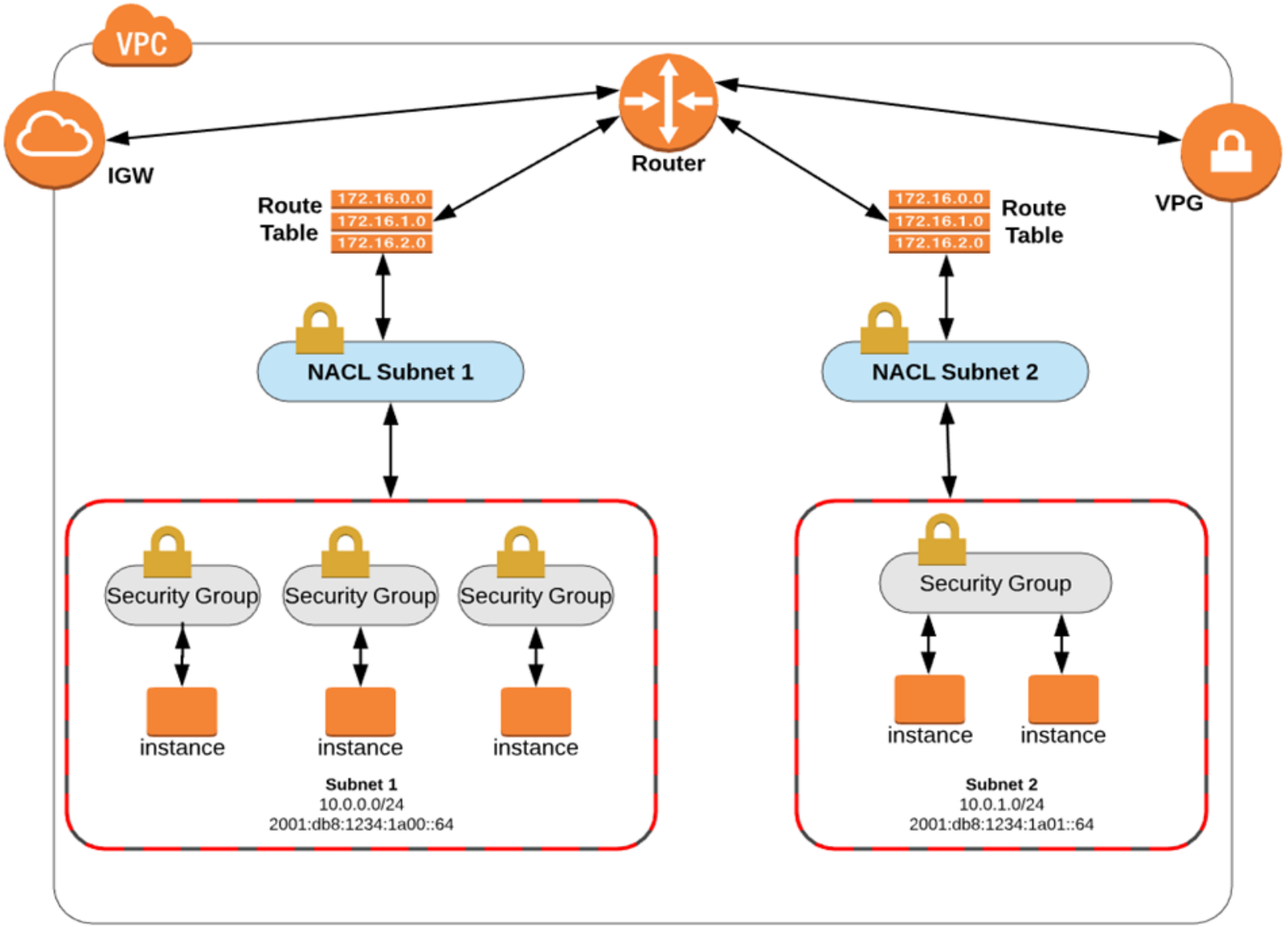
AWS Cognito


Authentication providers
Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.
Cognito
Amazon
Apple
Facebook
Google+
Twitter / Digits
OpenID
SAML
Custom
Configure your Cognito Identity Pool to accept users federated with your Cognito User Pool by supplying the User Pool ID and the App Client ID.
User Pool ID
ex: us-east-1_Ab129faBb
App client id
ex: 7lhlkkfbfb4q5kpp90urffao
Add Another Provider
* Required
Cancel
Create Pool

Network ACLs (NACLs)

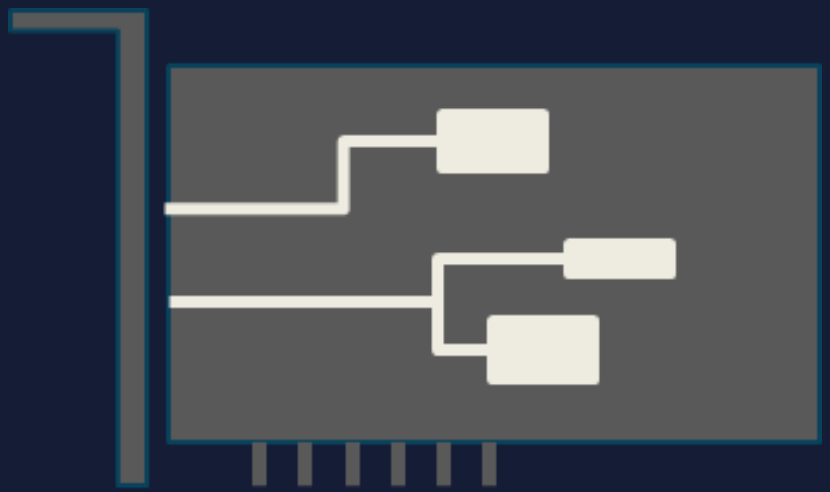
- Allow stateless traffic filtering to all inbound or outbound traffic on a VPC subnet
- Apply to all instances in the associated subnet
- Can contain ordered rules to permit or deny traffic (Rules are processed with a numbered order)
- Are agnostic of TCP sessions or UDP/ICMP flows
- Are stateless (static) in that the return traffic must be explicitly allowed in the other NACL
- Work together with security groups and can permit or deny traffic before it reaches the interfaces

Network ACLs (NACLs)



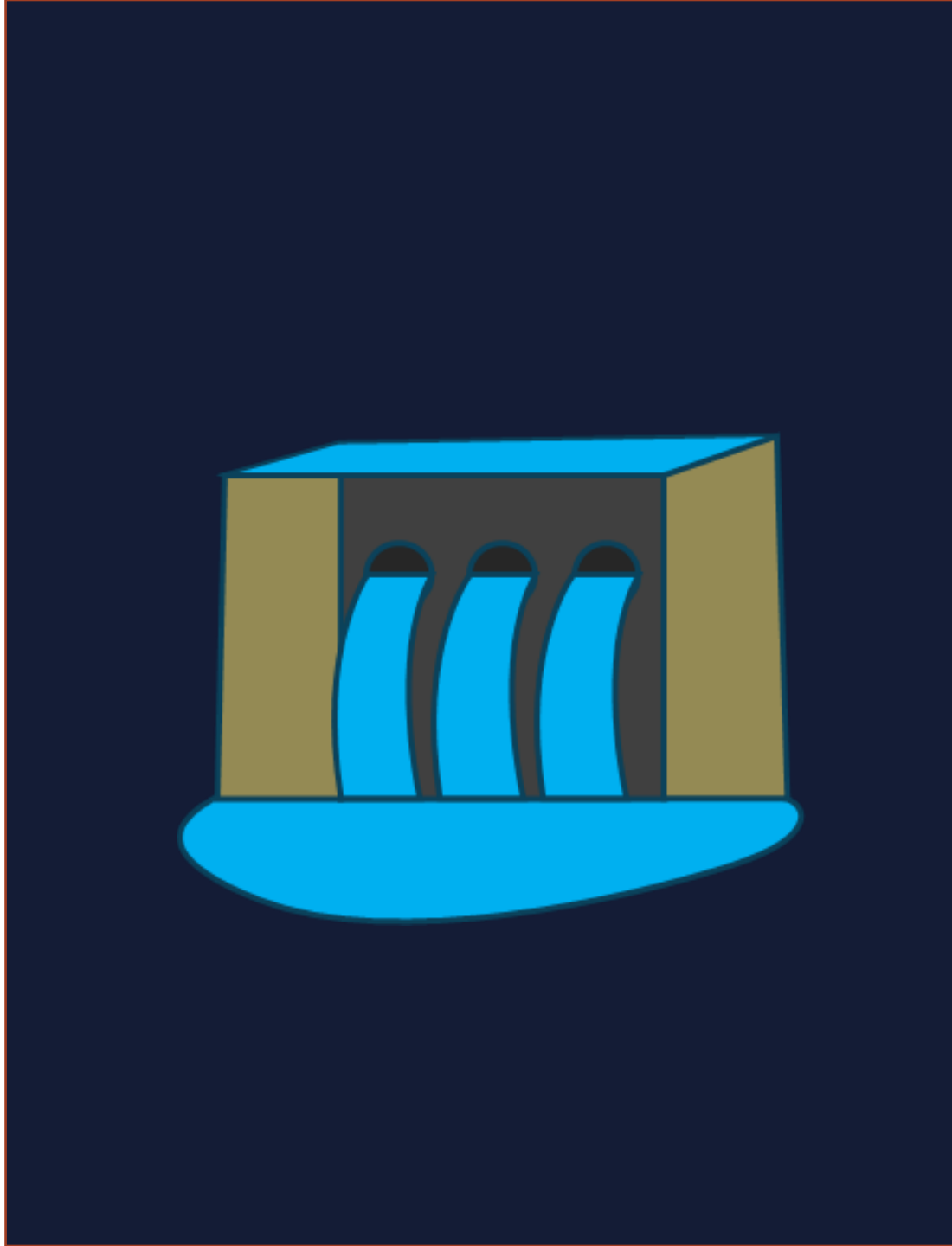
Security Groups

- Apply to individual EC2 instances in a subnet
- Layer 3/4 **stateful** virtual “Allow Only” firewalls – **no explicit deny rules**
- Operate at the hypervisor level attached to the virtual elastic network interfaces (eth0)
- ALL EC2 instances are launched with the default SG unless otherwise designated
- An unchanged Default SG will allow communication between **all** resources **within** the security group **AND** all outbound traffic - all other traffic is implicitly denied



Security Groups

- Return traffic is automatically allowed (with Shield Standard inspection)
- All rules **in all applied security groups** are evaluated before a decision is made
- You can only create a limited number of security groups on every VPC that you have
- There is also a limit on the number of rules you can add to one security group
- There is a limited number of security groups that you can use with a network interface



Web Application Firewall

Control and monitor HTTP/HTTPS requests forwarded to CloudFront (CDN), Application Elastic Load Balancer (ELB) or an API Gateway

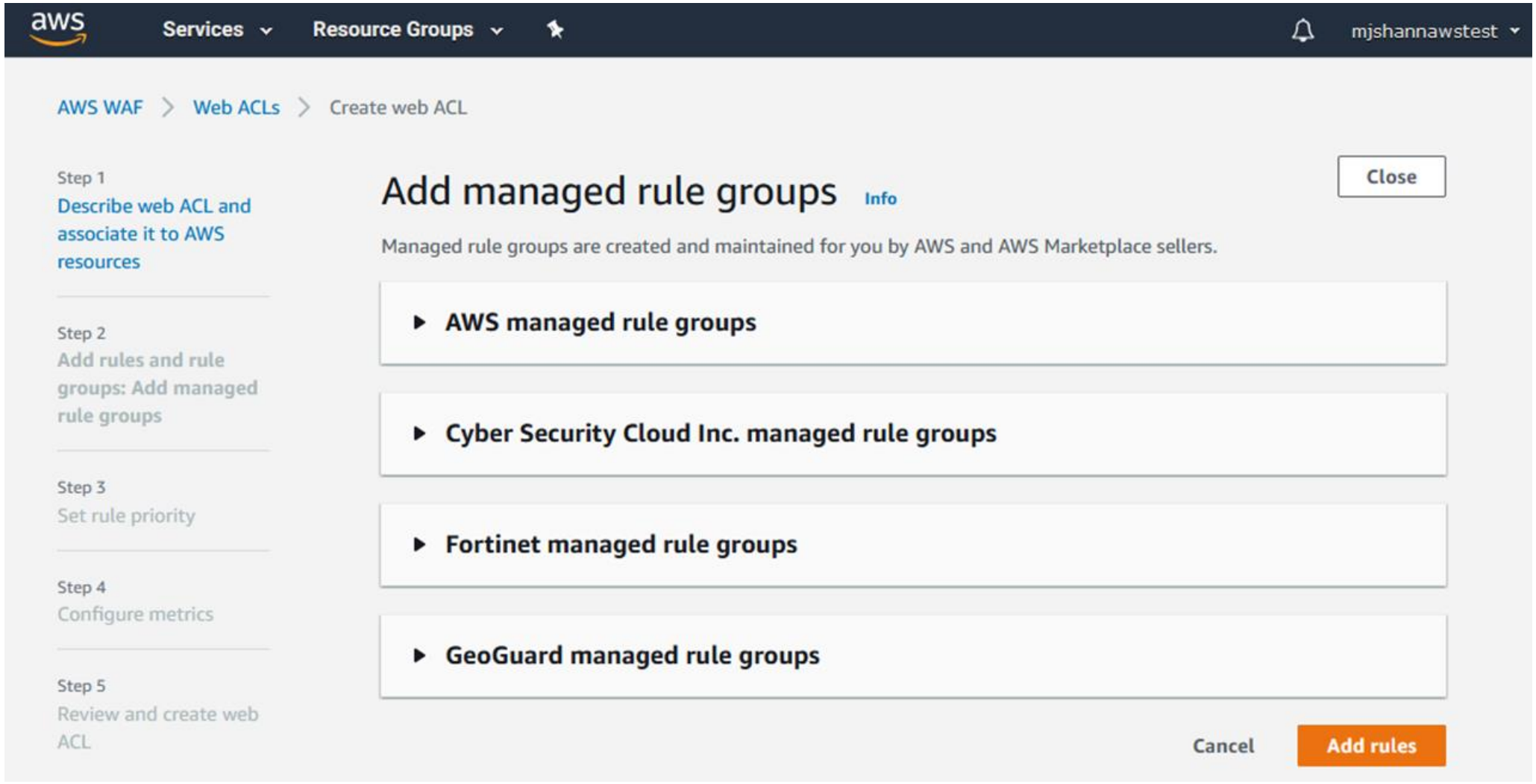
- Allow all requests except for ones you designate (permissive)
- Block all requests except for ones you designate (restrictive)
- Count the requests that match the properties that you specify

Web Application Firewall

Matching Condition Sets

- Country of request origin
- Originating IPv4 and IPv6 addresses
- Values in HTTP request headers
- Lengths of URIs, arguments, fields, field counts
- Literal or regex string patterns
- Presence of SQL injection (SQLi) code
- Presence of Cross-site Scripting (XSS) code
- Presence of Cross-site request forgery (XSRF) code

Web Application Firewall



Web Application Firewall

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	Add to web ACL
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	Add to web ACL
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications and common Common Vulnerabilities and Exposures (CVE).	700	Add to web ACL
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.	200	Add to web ACL
Linux operating system Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.	200	Add to web ACL
PHP application		

AWS Shield

Standard and Advanced Options

- DDoS protection provided at no extra cost
- Basic protection against common DoS floods and exploits
- Additional protection from known DDoS attacks
- Most common DDoS comes from botnet servers
- **Combined with NACLs, SGs, and WAF for layered defense**

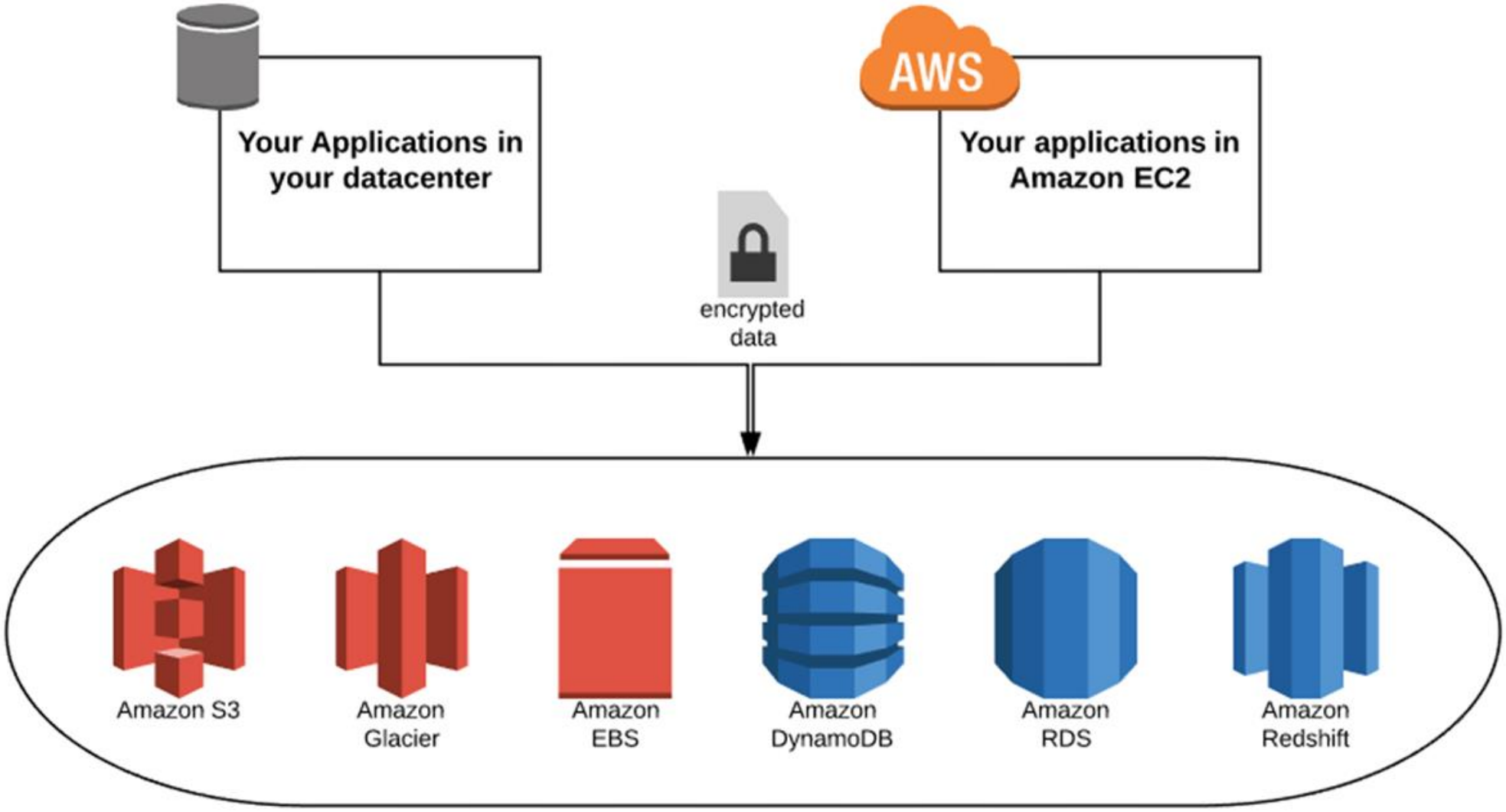
Amazon Inspector

- AWS discourages running assessment tool except in certain circumstances
- Amazon Inspector is an automated security assessment service that enhances security and compliance of applications running on AWS
- Inspector automatically evaluates applications for vulnerabilities and nonconformity with best practices and a knowledgebase of 100’s of rules
  - Produces a detailed list of security findings
  - Results available through console or API
  - Generates various meaningful reports

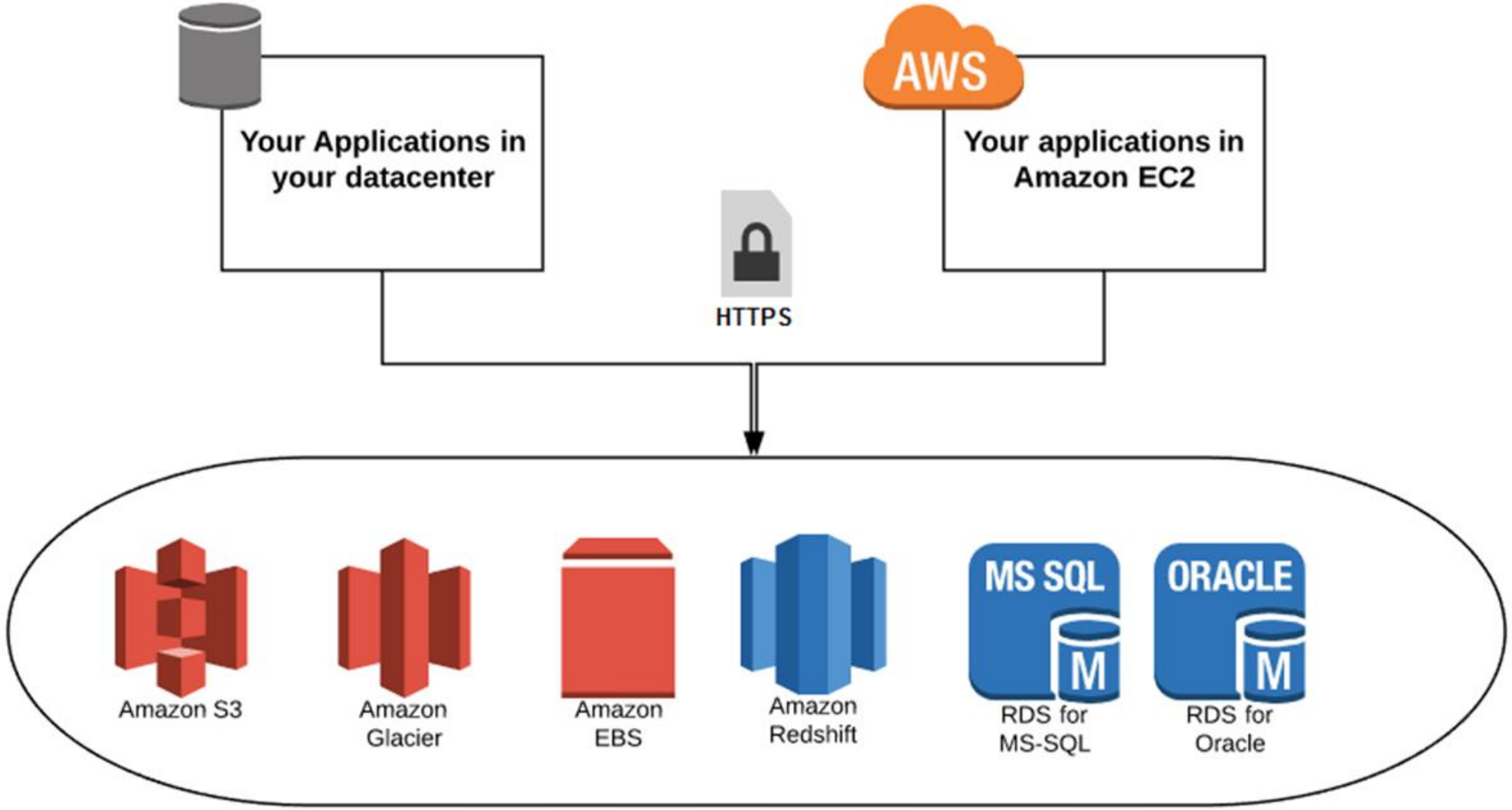
GuardDuty

- Fully-managed threat detection service
- Looks for anomalies and unauthorized actions
- Monitors for zero-day activities
- Produces well-defined "findings"
- Uses proprietary machine learning and AI algorithms
- Based on a partnership with several companies including Trend, Crowdstrike, and Rapid7

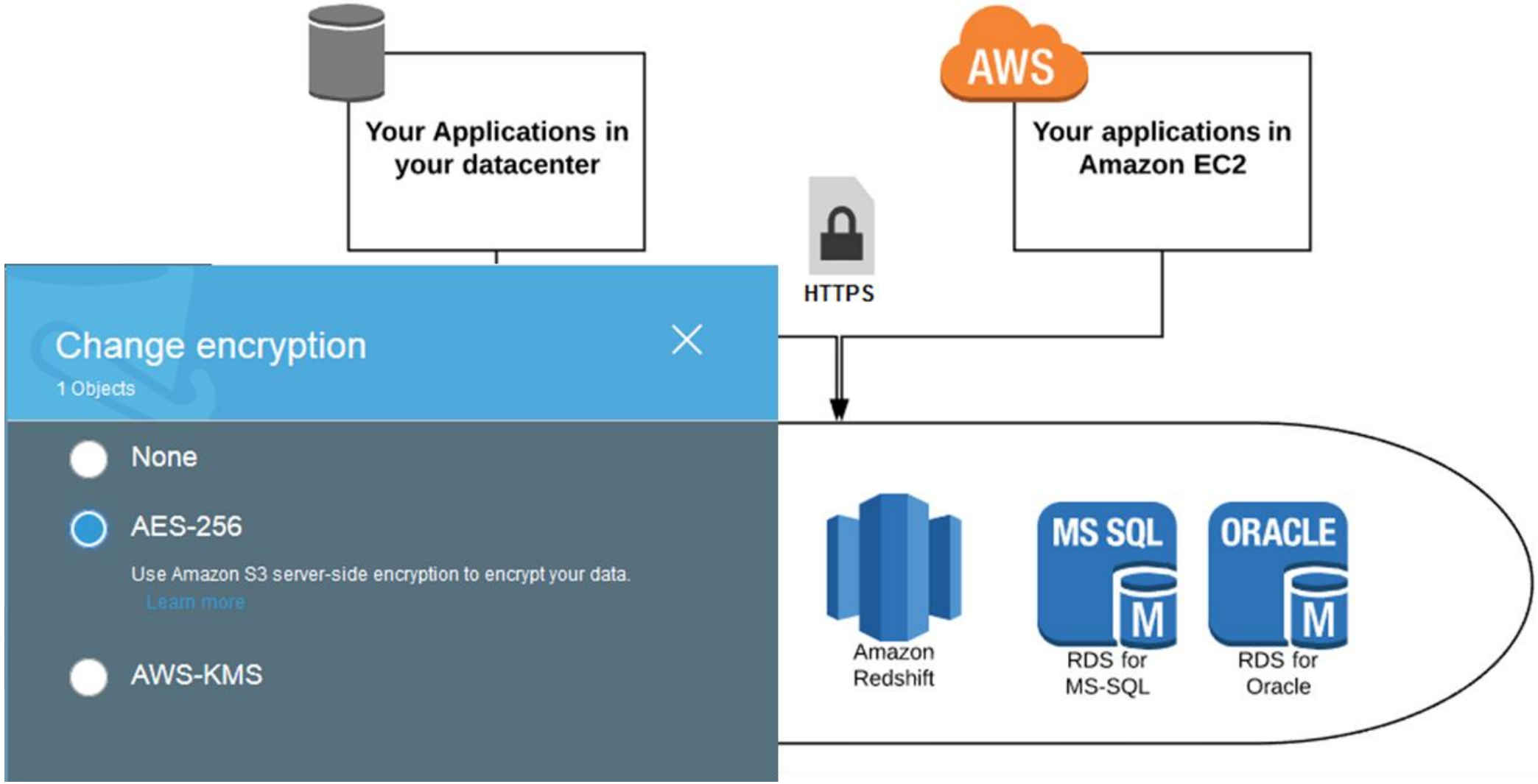
Client-side Encryption



Server-side Encryption



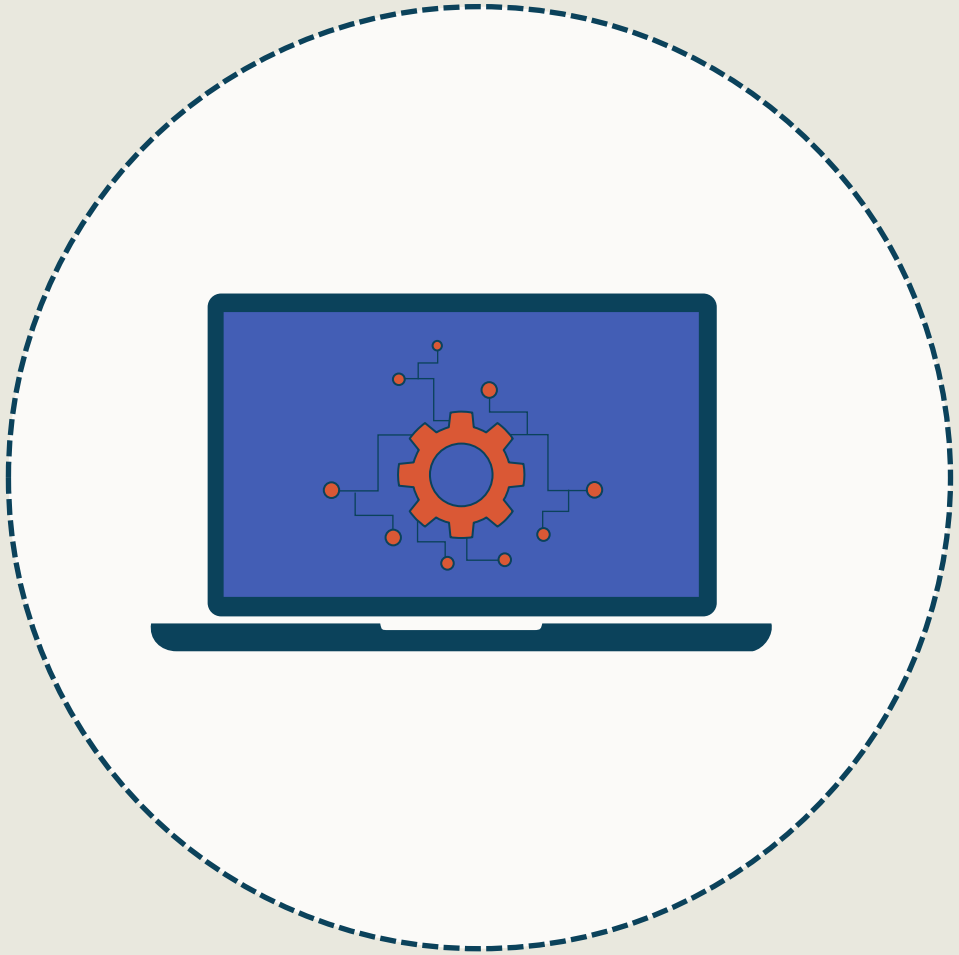
Server-side Encryption (i.e., SS3 SSE)



AWS KMS

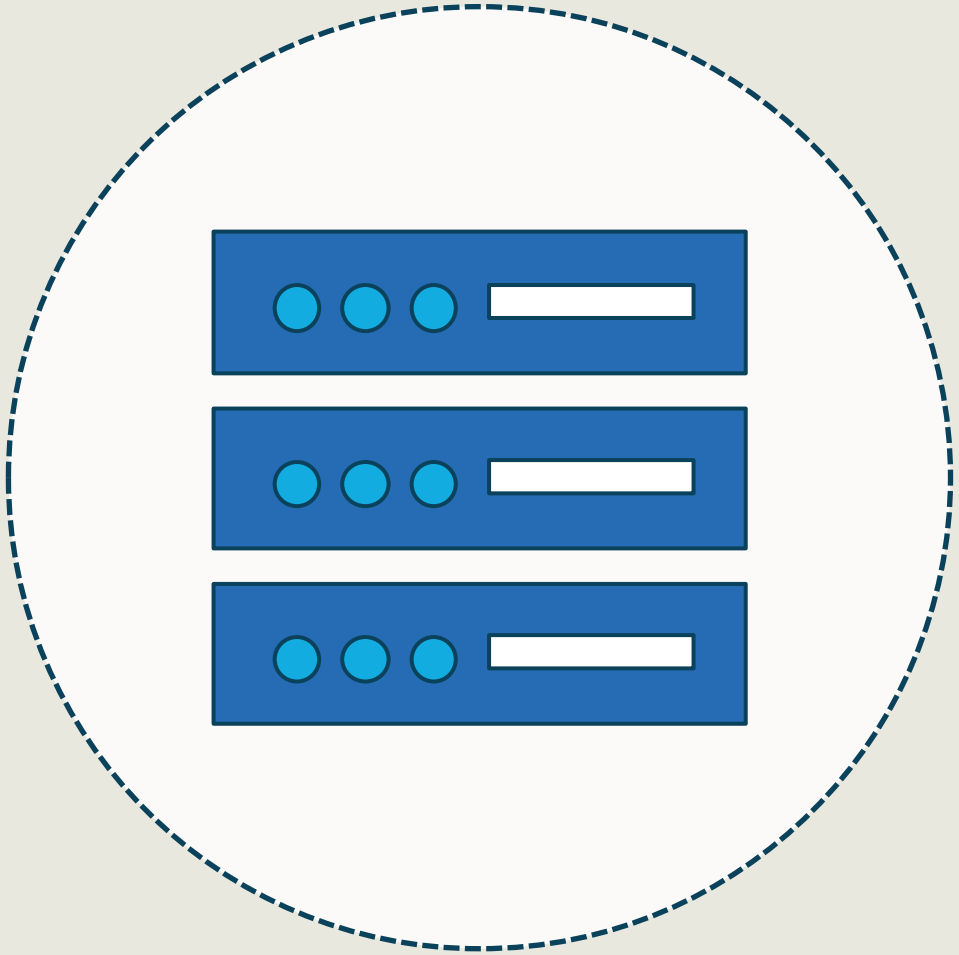
- Customer Master Keys (CMKs) are the main resource of the KMS service
- You can use a CMK to encrypt and decrypt up to 4 KB (4096 bytes) of data
- Typically, you use CMKs to generate, encrypt, and decrypt the data keys that you use outside of AWS KMS to encrypt your data
- There are three types of CMKs in AWS accounts:
  - Customer-managed
  - AWS-managed
  - AWS-owned

AWS Compute Services Survey



- EC2
- Lightsail
- Elastic Beanstalk
- Lambda
- Elastic Container Service (ECS)

Deploying EC2 Instances



- EC2 is a service that delivers resizable and secure compute capacity in the AWS cloud
- Makes rapid web-scale cloud computing easier by using a simple web service interface
- Provides control of your resources running on an established computing infrastructure

EC2 Instances

- Increase or decrease capacity within minutes
- EC2 allows you to select flexible configurations
- Securely integrated with most AWS services
- Highly available, reliable, and durable

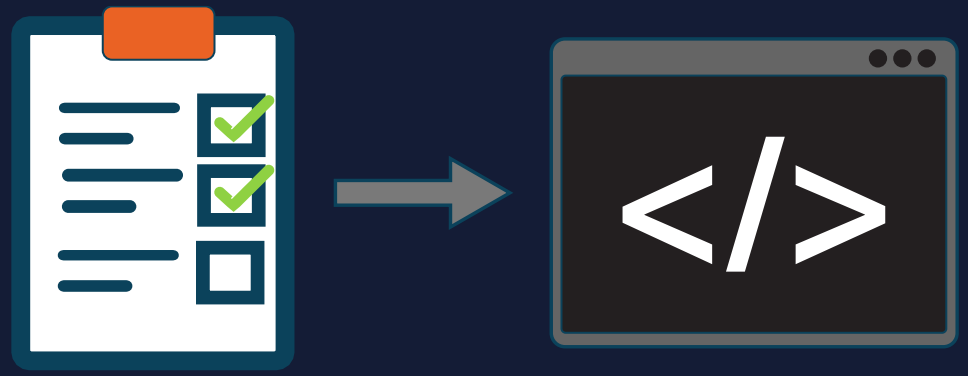
Convertible Reserved Instances

More flexible

- Convertible RIs give you even more flexibility
- Offers a significant discount (typically 45% compared to On-Demand)
- They allow you to change the instance family and other parameters associated with a Reserved Instance at any time

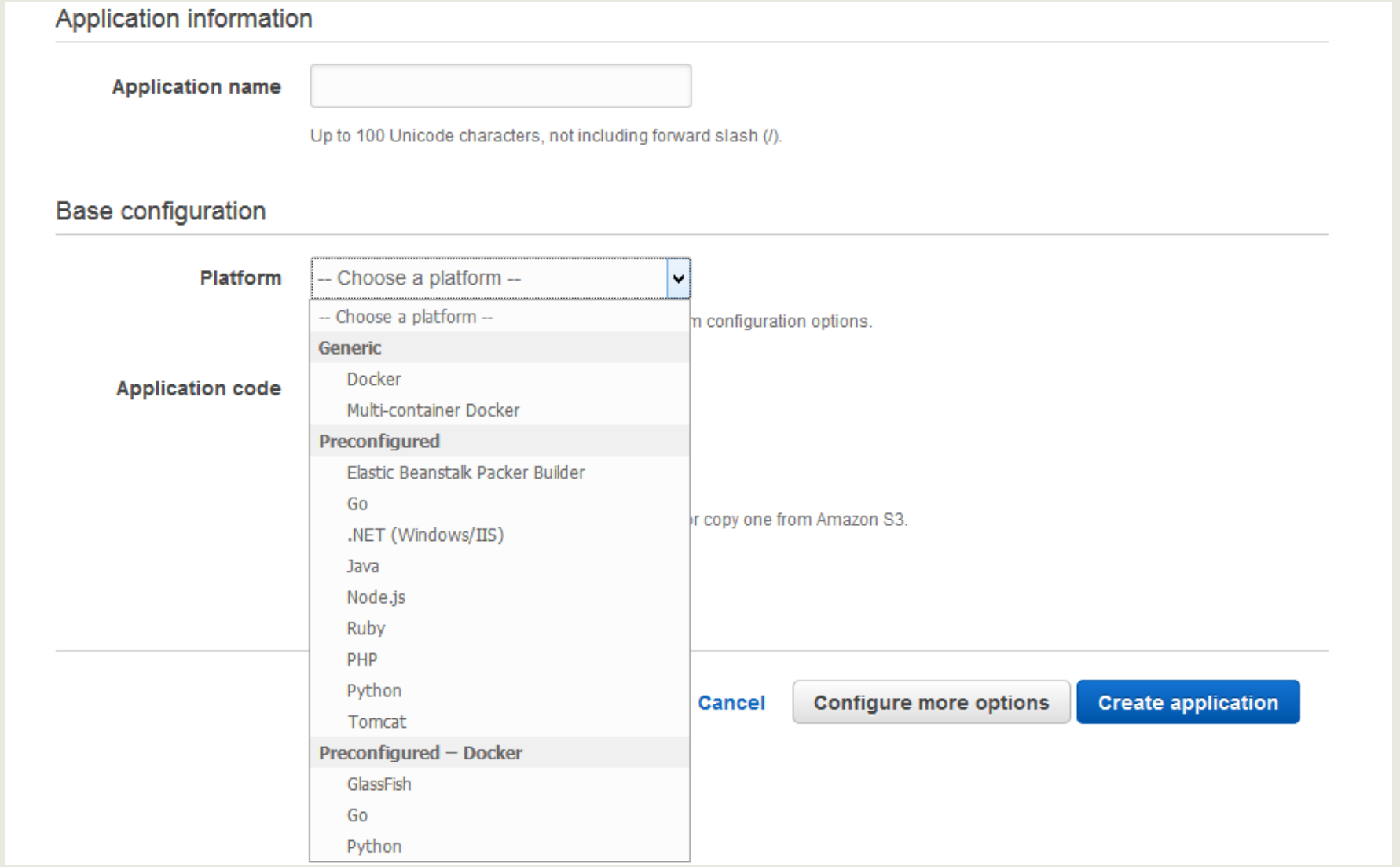
Elastic Beanstalk

The traditional Dev platform



- AWS Elastic Beanstalk is an easy-to-use service for deploying, monitoring and scaling web applications and services developed on several different platforms and applications
  - Choose your platform (Generic Docker, Preconfigured, Preconfigured Docker)
  - Upload an application or use a sample code from AWS
  - Run it

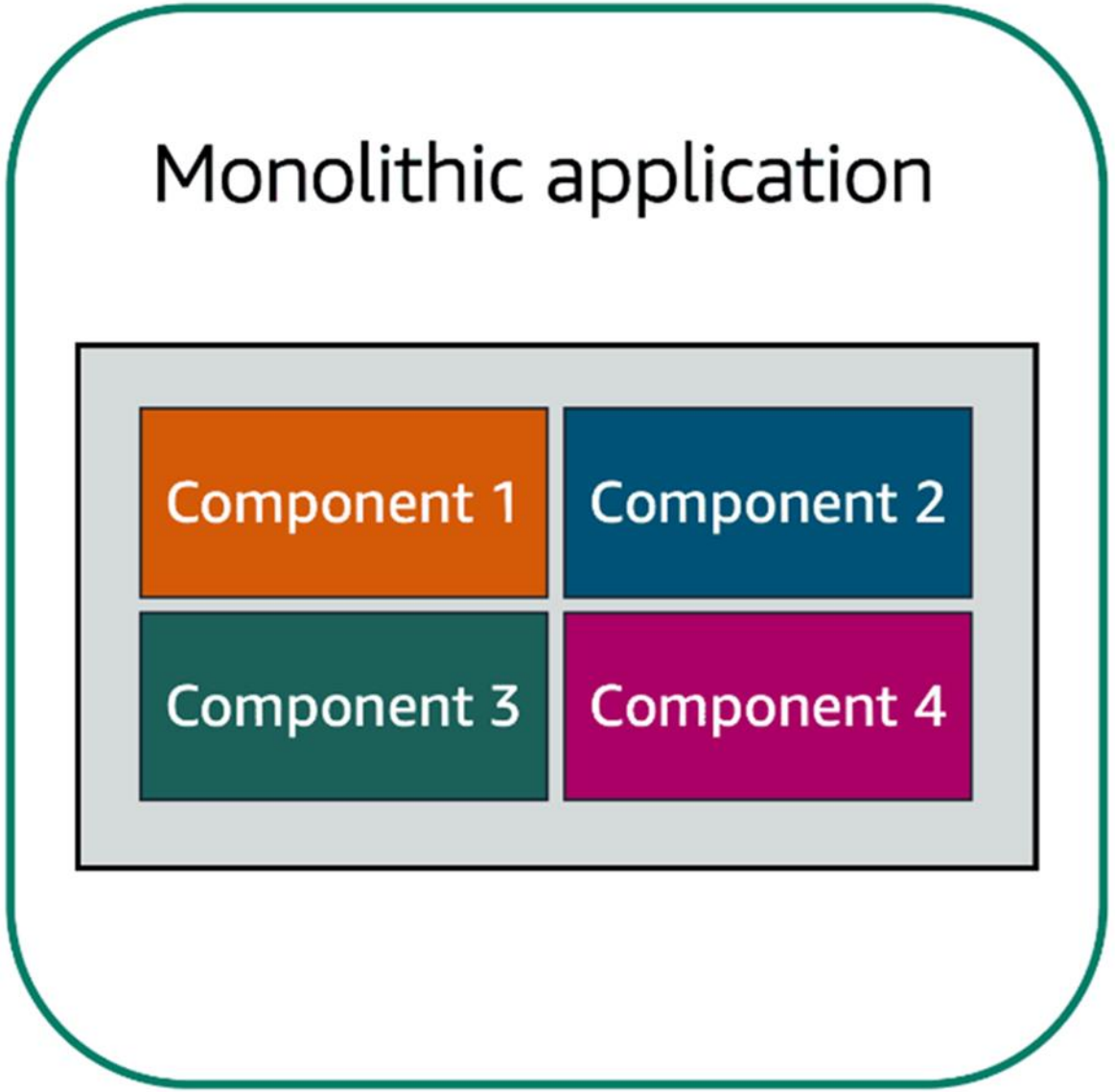
Elastic Beanstalk



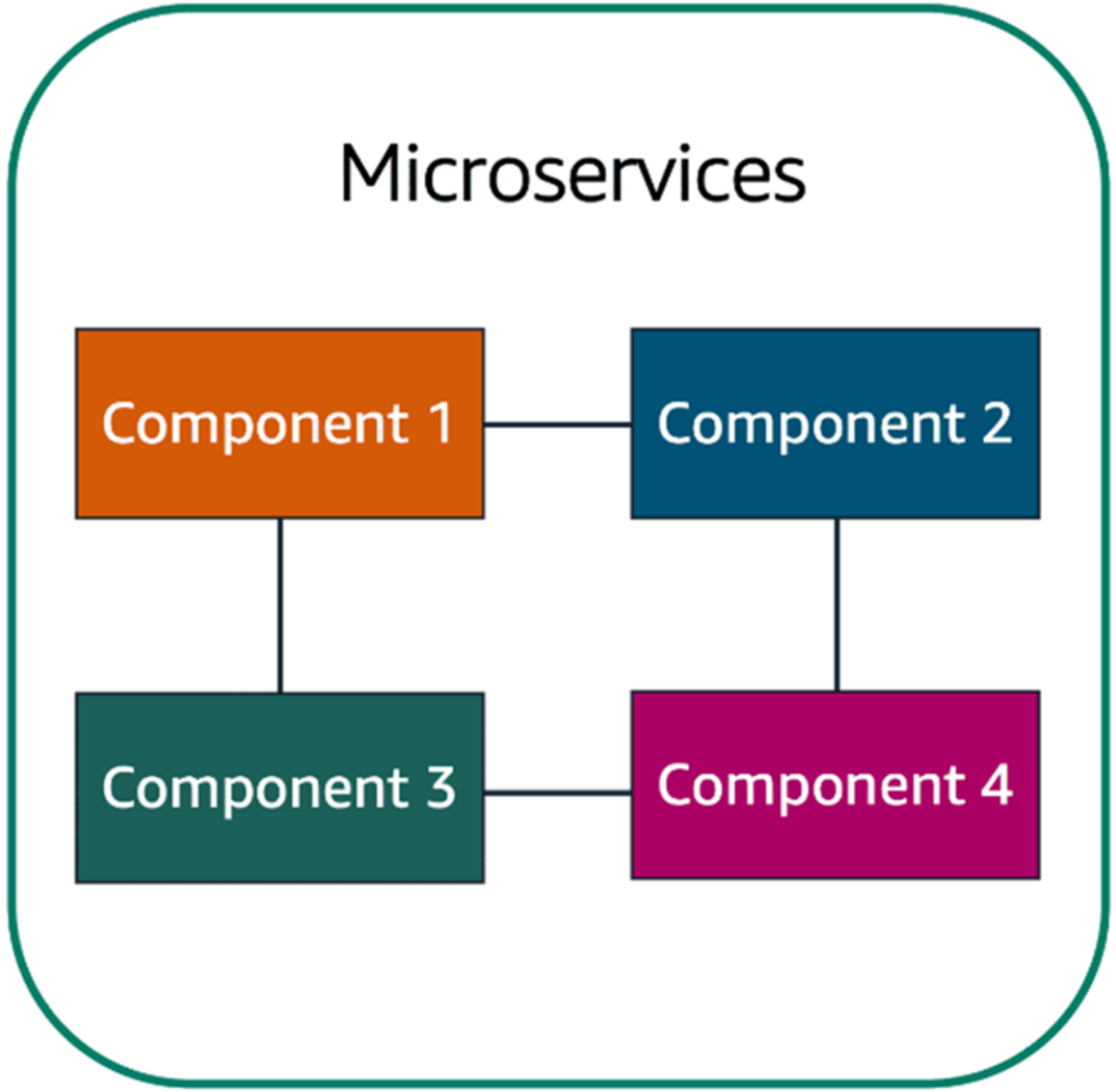
AWS Lambda

- AWS Lambda lets you run code without deploying or managing servers
- You pay only for the compute time you consume and there is no charge when your code is not running
- You can run code for virtually any type of application or backend service—all with zero administration

Monolithic Application Types



Microservices



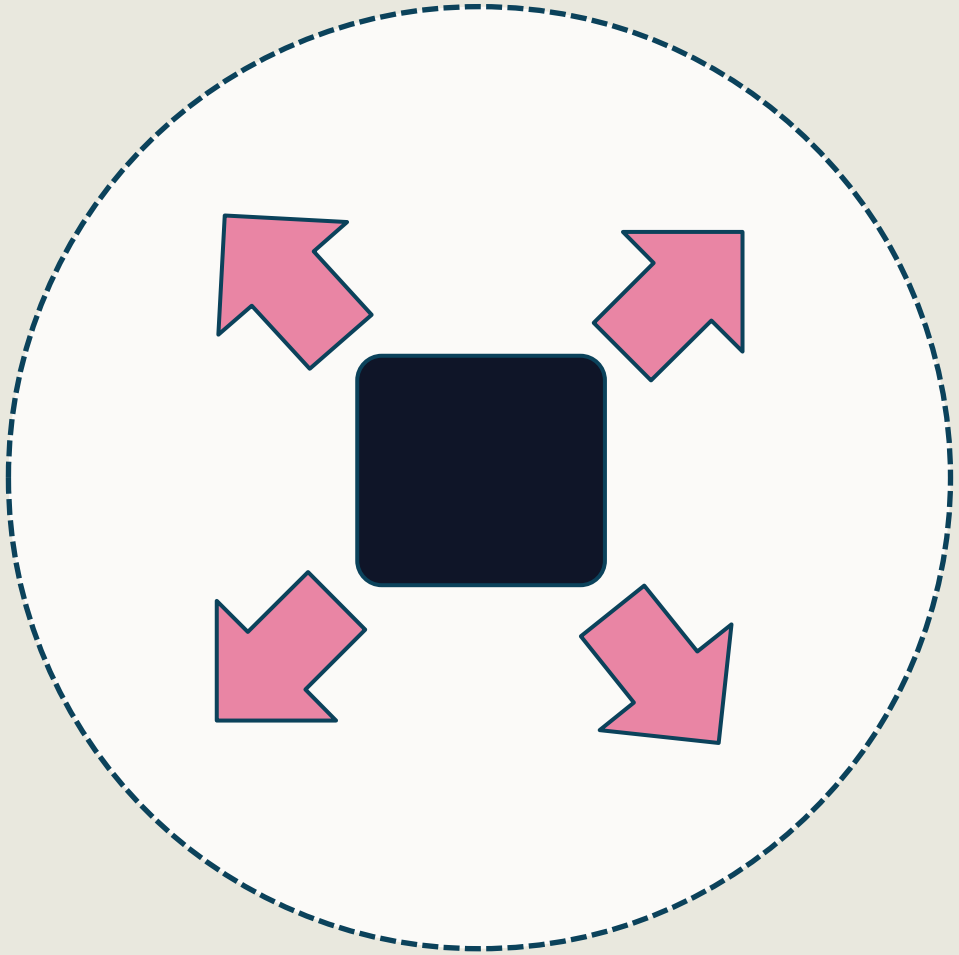
SNS and SQS

- Amazon **Simple Notification Service (SNS)** is a publish/subscribe service
- Using Amazon SNS topics, a publisher distributes messages to subscribers
  - Consider a coffee shop where the cashier provides coffee orders to the barista who makes the drinks
- Amazon **Simple Queue Service (SQS)** is a message queuing service that lets you send, store, and receive messages between software components, without losing messages or requiring other services to be available

Containers

- A container is a discrete environment within an operating system where one or more applications can run, typically assigned all the resources and dependencies needed to function properly
- Docker is the most common platform for developing “containerized” applications
- Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service
- AWS Fargate is the preferred way for customers to run containers on AWS across both ECS and EKS

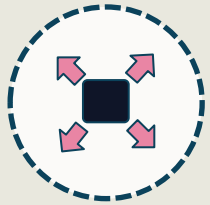
Auto Scaling



- Auto Scaling monitors applications and automatically modifies capacity to retain stable and predictable performance at the lowest cost
- You can build scaling plans for O/S instances, fleets, tasks, database tables, indexes, and replicas
- **Dynamic or Predictive scaling**

Auto Scaling

Rapidly configure scaling feature with high visibility

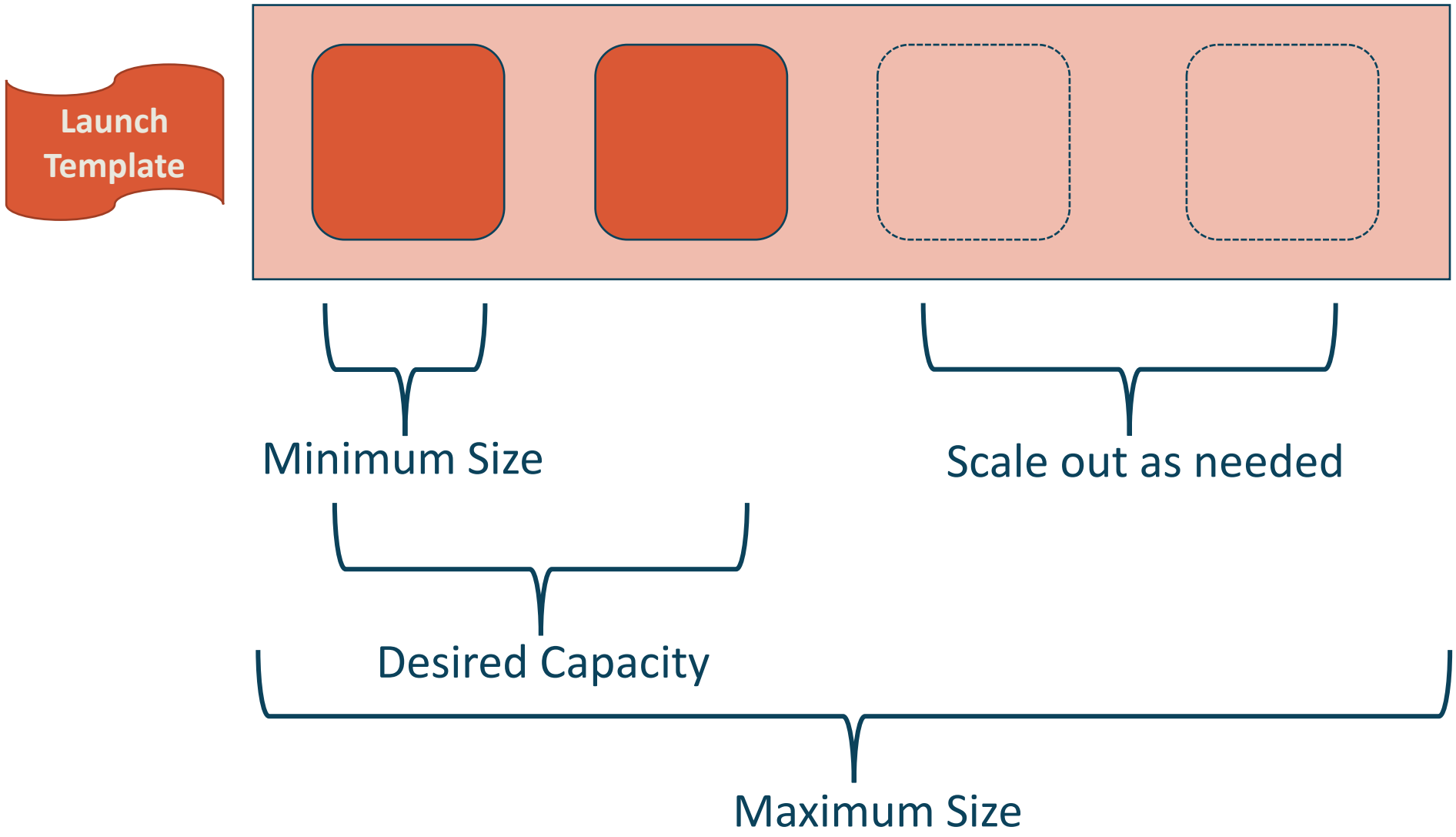


Automate and optimize balance of availability and costs

Constantly monitors to ensure desired performance levels

Automatically remove excess capacity to avoid overspending

Auto Scaling Group



Elastic Load Balancing (ELB)

- Elastic Load Balancing (ELB) automatically dispenses incoming traffic across several targets including **EC2 instances, IP addresses, containers, and Lambda functions**
- They can be public-facing or internal
- **Application** Load Balancer is for load balancing HTTP and HTTPS traffic for delivering modern application architectures
- **Network** Load Balancer is for TCP,UDP, and TLS traffic routing traffic to VPCs optimized for high-speed, low-latency traffic
- **Gateway** Load Balancer is used for virtual appliances and testing the marketplace

AWS CloudFormation

Offers common language to templatize the cloud environment

Infrastructure-as-code deployment with stacks

Configuration is in simple text file format

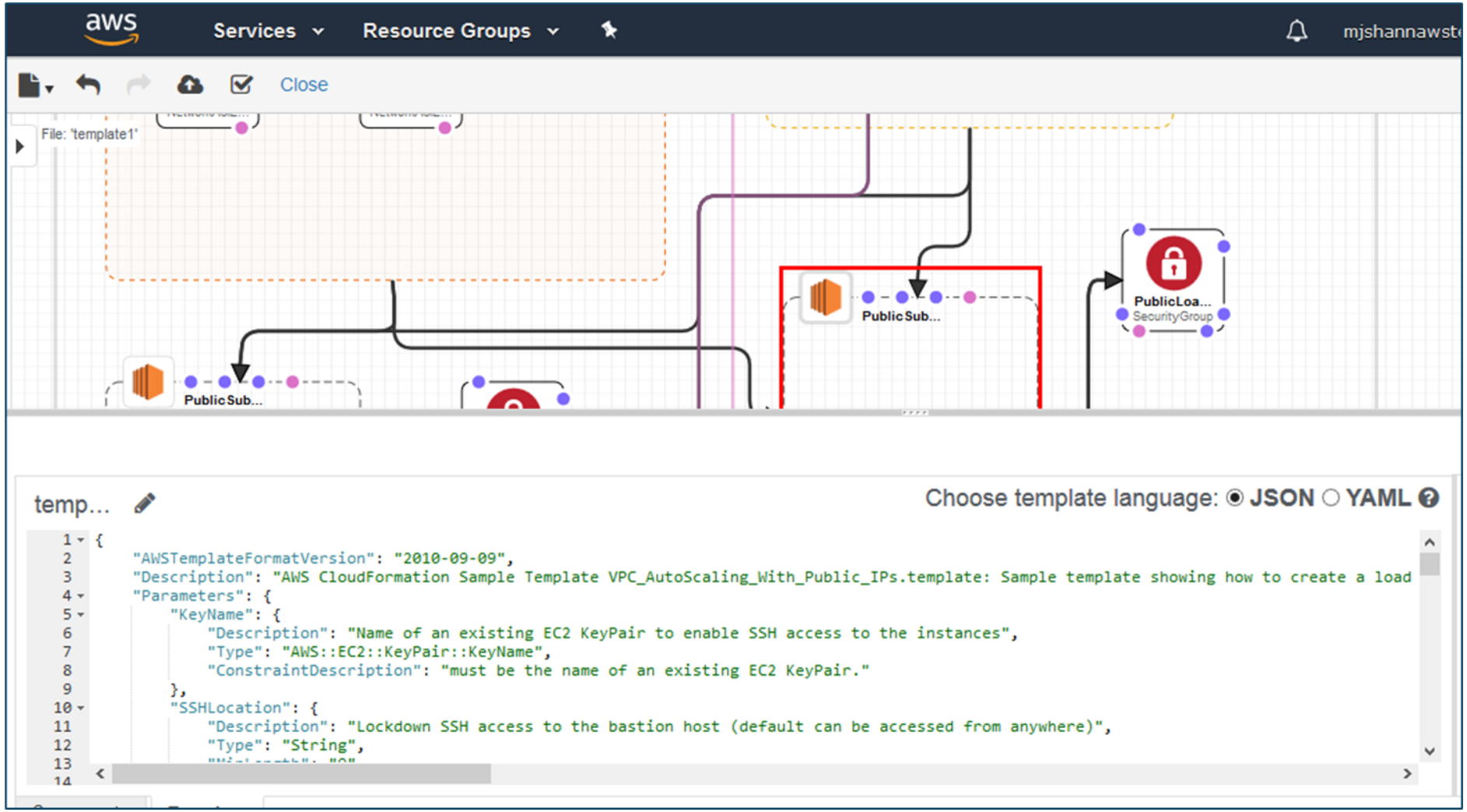
Serves as the “single source of truth” for environment

Safe, secure, and repeatable

AWS Cloud Formation

Template Name	Description	View	View in Designer	Launch
A single Amazon EC2 in an Amazon VPC	Creates a VPC and adds an Amazon EC2 instance with an Elastic IP address and a security group.	View	View in Designer	Launch Stack
Amazon VPC with static routing to an existing VPN	Creates a private subnet with a VPN connection that uses static routing to an existing VPN endpoint.	View	View in Designer	Launch Stack
Autoscaling and load-balancing website in an Amazon VPC	Creates a load balancing, auto scaling sample website in an existing VPC.	View	View in Designer	Launch Stack
Amazon VPC with DNS and public IP addresses	Creates a VPC with DNS support and public IP addresses enabled.	View	View in Designer	Launch Stack
Publicly accessible Amazon EC2 instances that are in an Auto Scaling group	Creates a load balancing, autoscaling group with instances that are directly accessible from the Internet.	View	View in Designer	Launch Stack
Amazon EC2 with multiple dynamic IP addresses in an Amazon VPC	Creates an Amazon EC2 instance with multiple dynamic IP addresses in a VPC.	View	View in Designer	Launch Stack

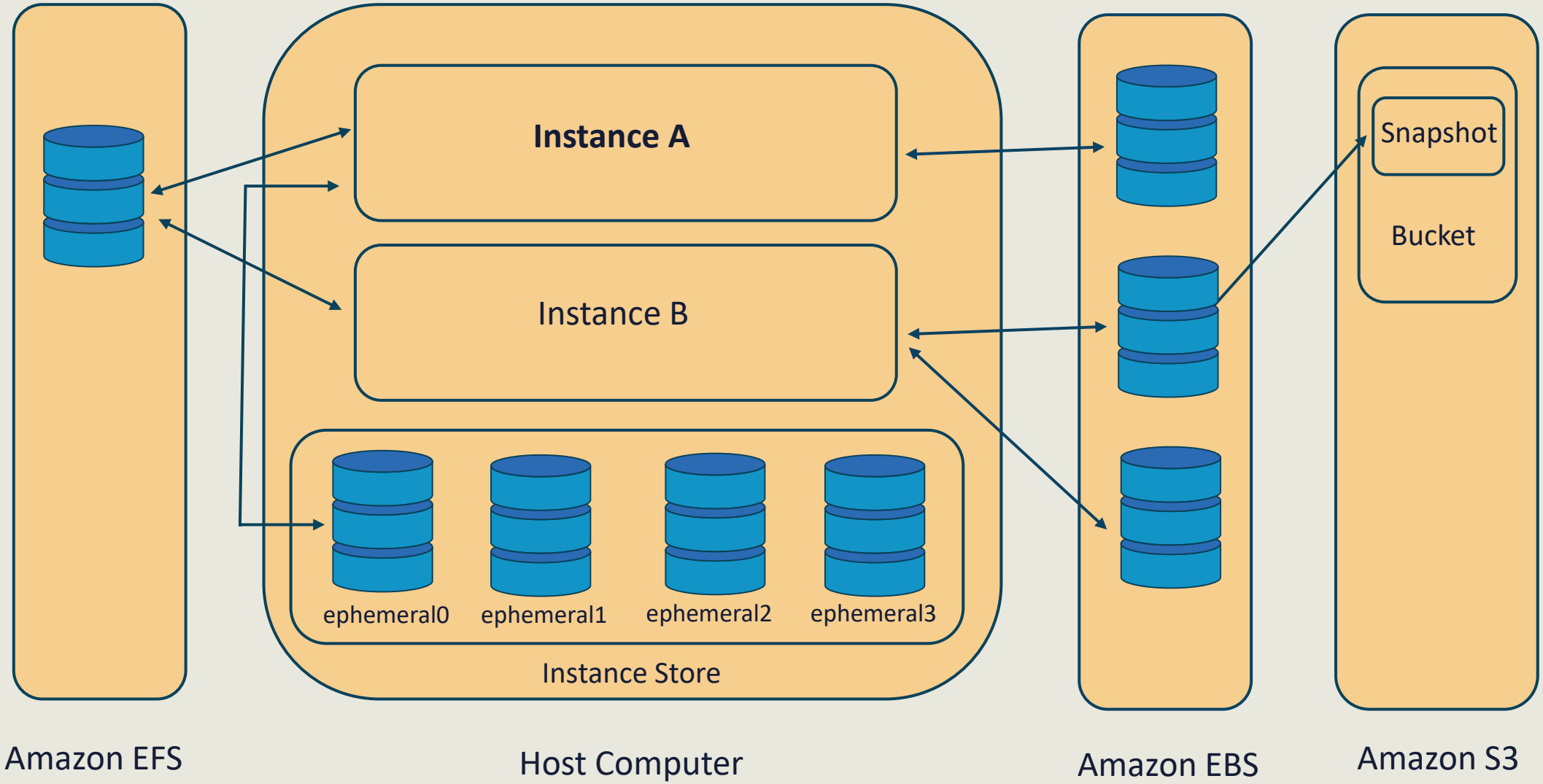
AWS Cloud Formation



Elastic Block Storage (EBS)

- Amazon EBS offers persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud
- Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability
- EBS volumes offer the consistent and low-latency performance needed to run your workloads

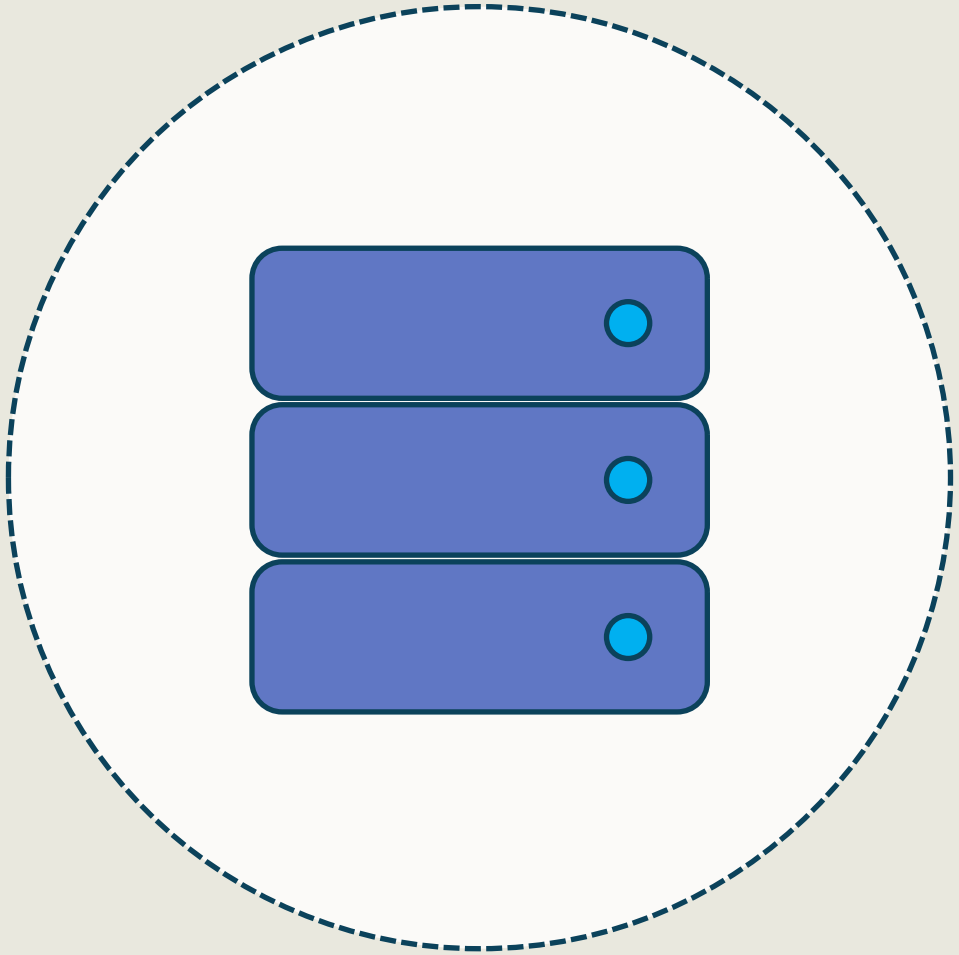
Amazon Block Storage (HDD and SDD)



Amazon Elastic File System (Amazon EFS)

- Amazon Elastic File System (Amazon EFS) provides a simple, scalable, elastic file system for Linux-based workloads for use with AWS Cloud services and on-premises resources
- It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files
- EFS is a fully managed service that requires no changes to your existing applications and tools, providing access through a standard file system interface for seamless integration

Working with Simple Storage Service (S3)



- S3 is object-based storage that is constructed to store and get unlimited volumes of data from anywhere on the Internet
- It provides a highly-available, extremely durable, and enormously scalable data storage infrastructure at very low cost

Overview of S3

Simple web service interface

Store and retrieve any amount of data at any time

Easily build applications that use Internet storage

Designed to be highly flexible and scalable

Makes the job easier for CDN developers

S3 Storage Plans (Tiers)

Standard	I-T	S-I A or 1 Z-I A	Glacier or Deep Archive
Eleven 9's durability	Three 9's of availability	Infrequent Access but rapid access when needed	Eleven 9's durability
Four 9's of availability	11 - 9's of durability	Lower per GB storage prices and retrieval fee	Data archiving with flexible access options
Low-cost throughput	Cheaper than Standard S3	Lower throughput	Can store data for as little as $0.004 per gigabyte per month

Storage Gateway

- AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage
- You can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration
- Can be appliance-based or in a hypervisor
- Often used in conjunction with Direct Connect 10 Gbps

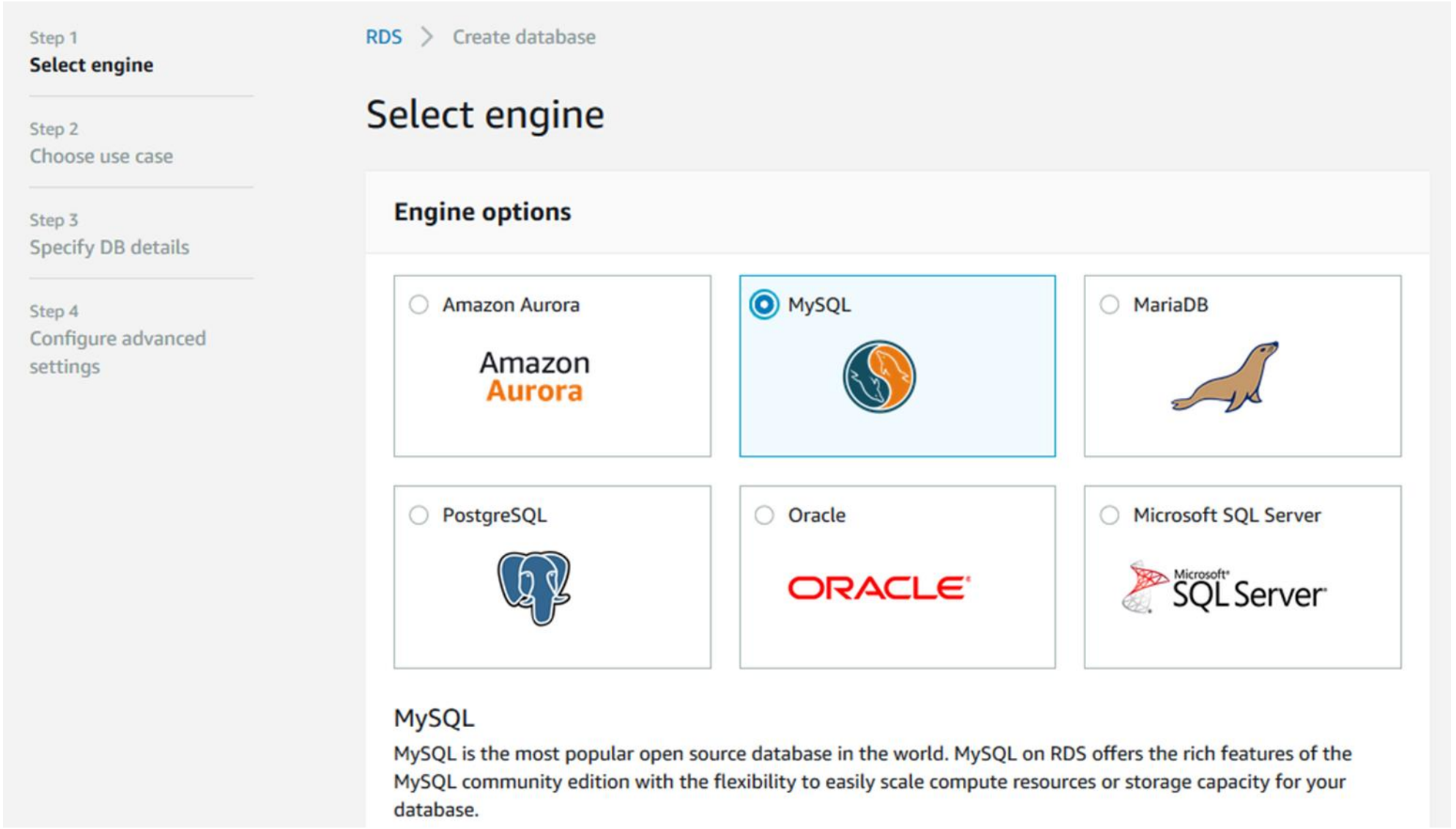
Survey of AWS Database Services

Database type	Use cases	AWS service
Relational	Traditional applications, ERP, CRM, e-commerce	Amazon Aurora, Amazon RDS, Amazon Redshift
Key-value	High-traffic web apps, e-commerce systems, gaming applications	Amazon DynamoDB
In-memory	Caching, session management, gaming leaderboards, geospatial applications	Amazon ElastiCache for Memcached Amazon ElastiCache for Redis
Document	Content management, catalogs, user profiles	Amazon DocumentDB
Wide column	High scale industrial apps for equipment maintenance, fleet management, and route optimization	Amazon Managed Apache Cassandra Service
Graph	Fraud detection, social networking, recommendation engines	Amazon Neptune
Time series	IoT applications, DevOps, industrial telemetry	Amazon Timestream
Ledger	Systems of record, supply chain, registrations, banking transactions	Amazon QLDB

AWS Relational Database Services (RDS)

- Amazon Relational Database Service (RDS) is a managed service for setting up, operating, and scaling a cloud-based relational database
- RDS is available on several database instance types that are optimized for memory, performance or I/O
- Can choose from Amazon Aurora, PostgreSQL, MySQL, MariaDB, **Oracle Database**, and SQL Server
- **Use the AWS Database Migration Service to migrate or replicate your existing databases to Amazon RDS**

AWS Relational Database Services (RDS)

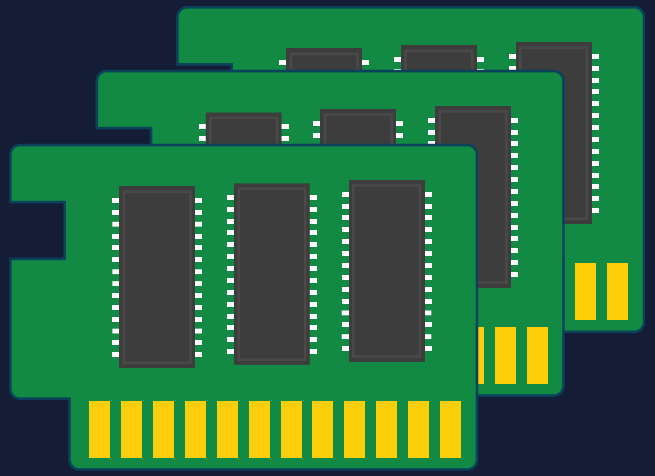


DynamoDB

- Amazon DynamoDB is a key-value and document database (NoSQL) that provides single-digit millisecond performance at any scale
- It is a fully managed, multi-region, multi-master database with built-in security, backup and restore, and in-memory caching for internet-scale applications
- It can handle more than 10 trillion requests per day and support peaks of more than 20 million requests per second
- Over 100,000 AWS clients use DynamoDB as their key-value and document database

Amazon ElastiCache

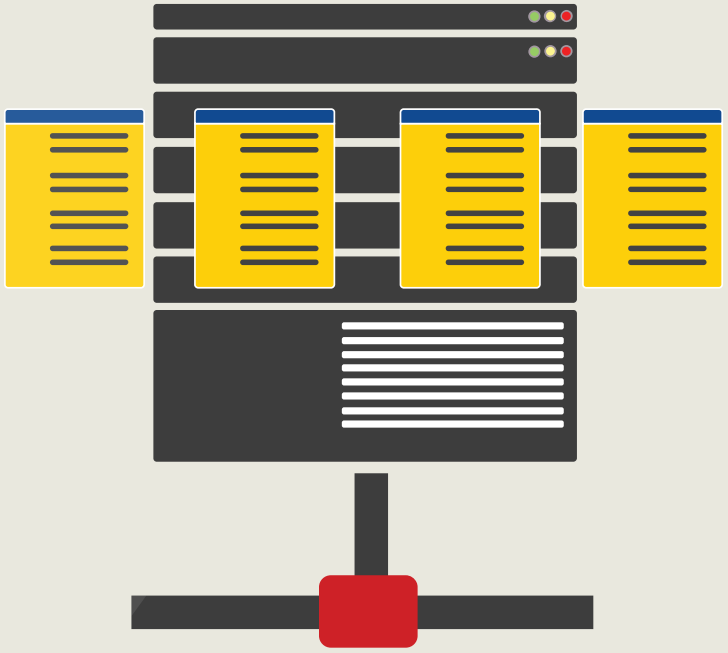
Redis or Memcached



- Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud
- The service improves the performance of web applications by empowering one to retrieve information from fast, managed, in-memory caches, instead of relying entirely on slower disk-based databases
- Amazon ElastiCache supports Redis and Memcached open-source in-memory caching engines

Amazon Redshift

Data Warehousing and Lakes



- Amazon Redshift clusters provide a fast, scalable data warehouse for cost-effective analysis of data across data warehouses and data lakes
- Uses machine learning, massively parallel query execution, and columnar storage on high-performance disks
- High security is provided using a 4-key nested encryption model

The Snow Family

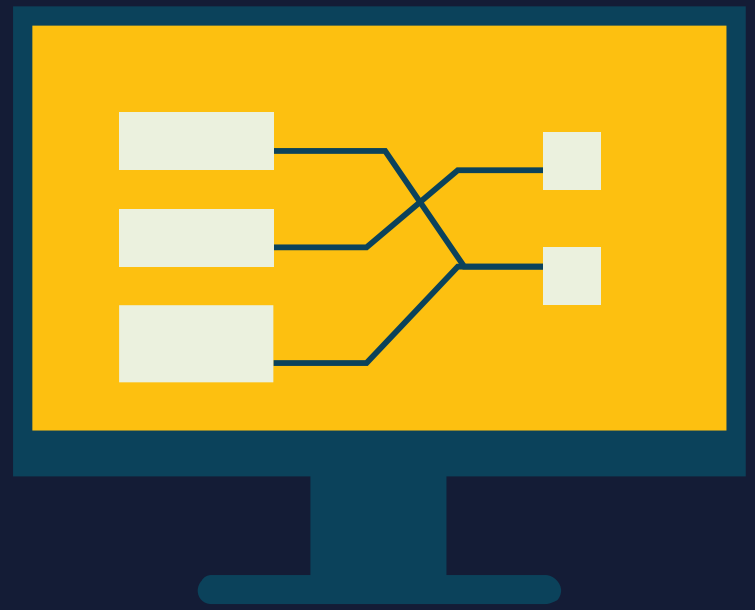
- **Snowcone** is a portable, rugged, and secure data box used to collect, process, and transfer up to 8 terabytes of data to AWS, either offline by shipping the device, or online with an AWS DataSync solution
- **Snowball** is a data migration and edge computing device that comes in two device options: Compute Optimized and Storage Optimized
  - Snowball Edge Storage Optimized devices offer 40 vCPUs of compute capacity combined with 80 terabytes of usable block or Amazon S3-compatible object storage
- **Snowmobile** moves up to 100 PB of data in a 45-foot-long rugged shipping container and is ideal for multi-petabyte or Exabyte-scale digital media migrations and data center shutdowns

CloudWatch

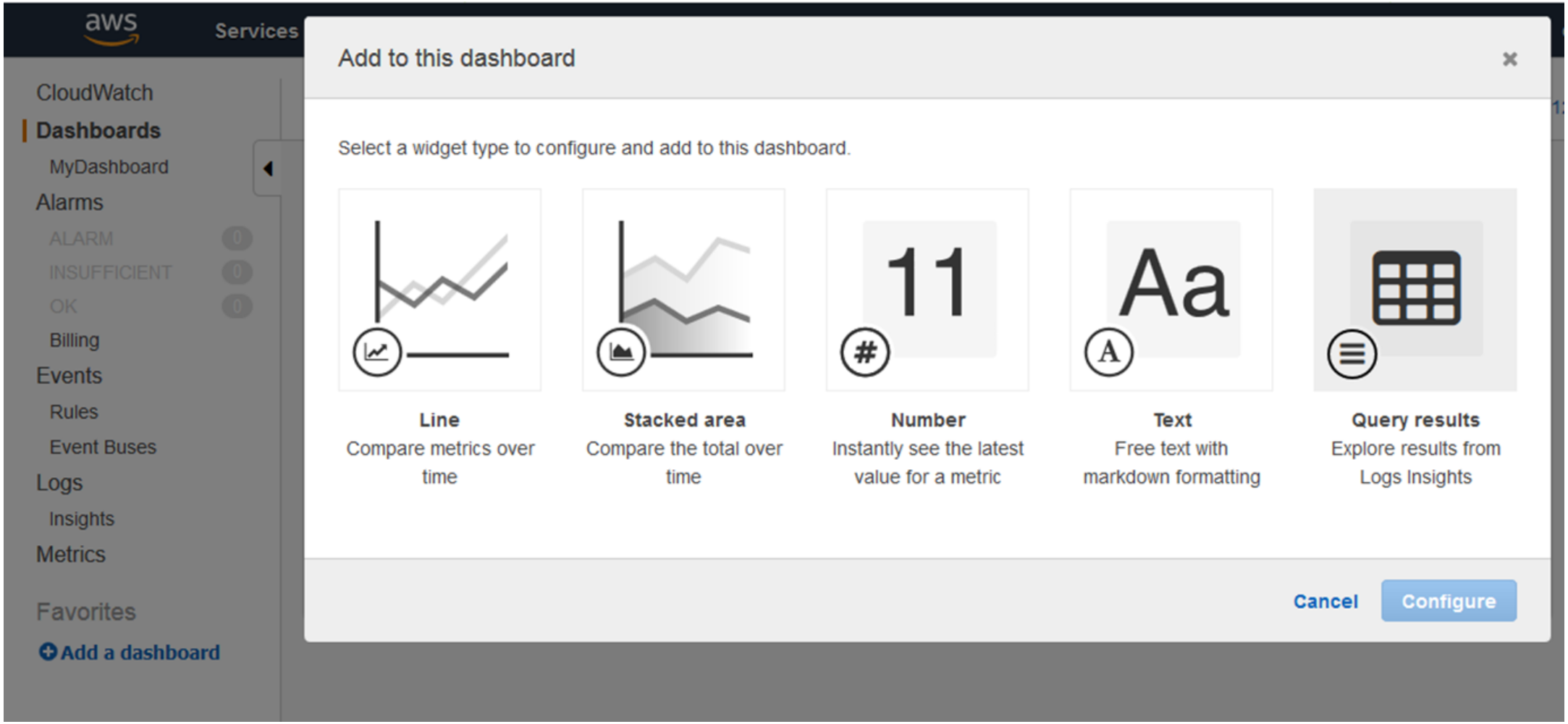
- Amazon CloudWatch is used for management and governance
- It is a monitoring and management service designed for developers, system operators, site reliability engineers (SRE), and managers
- CloudWatch offers data, meaningful metrics, and actionable insights to:
  - Monitor applications
  - Recognize and respond to system-wide performance changes
  - Optimize resource utilization
  - Gain a unified view of operational health

CloudWatch Use Cases

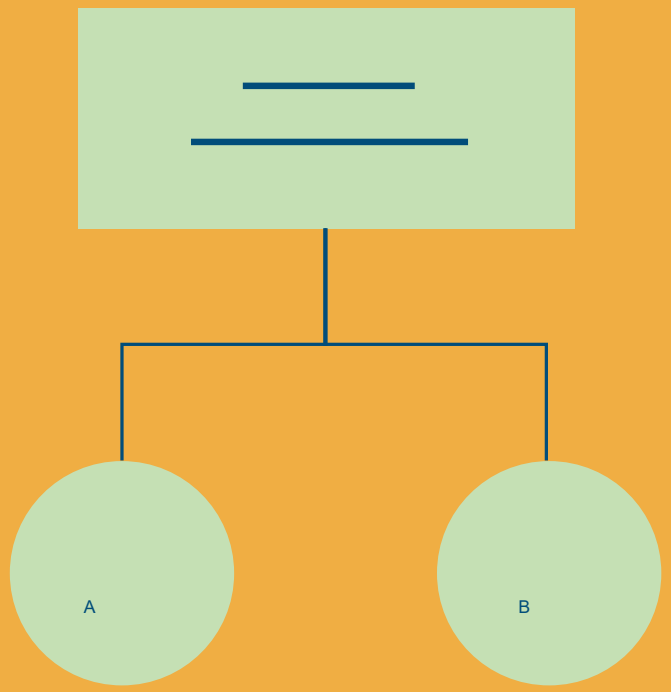
- Monitor critical metrics and logs, visualize application and infrastructure stacks, generate alarms, and correlate metrics and logs to recognize and resolve the root cause of performance issues
- Monitor applications and Trigger automated CloudWatch Alarms and Lambda workflows to enhance the customer experience
- Explore, analyze, and visualize logs instantly to optimize resources, leverage CloudWatch Alarms to automate capacity, and do resource planning for Auto Scaling



CloudWatch Dashboards



CloudTrail



- With CloudTrail, customers can log, continuously monitor, and retain account activity related to all API calls across the AWS infrastructure
- Within CloudTrail, CloudTrail Insights can be enabled where CloudTrail can automatically detect unusual API activities in AWS accounts
- **Example**: CloudTrail Insights could detect that a higher number of Amazon EC2 instances than usual have recently launched in an account or abnormal account activity has occurred then review the full event details to determine which actions need to be taken next

CloudTrail Use Cases

- **Exam: CloudTrail is one of the most common tools for getting insights into security events at AWS**
- Detect that a higher number of Amazon EC2 instances than usual have recently launched
- Identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred
- Create a workflow to add a specific policy to an Amazon S3 bucket when CloudTrail logs an API call that makes that bucket public
- Connect your VPC to CloudTrail by defining an interface VPC endpoint for CloudTrail

AWS X-Ray

- Assists developers in analyzing and debugging production, distributed applications (such as microservices)
- Better understand how your application and its underlying services are performing
- Identify and troubleshoot the root cause of performance issues and errors
- Get an end-to-end view of requests that traverse through the application and display a map of the application’s underlying components

Amazon Kinesis

- Makes it easy to gather, process, and analyze real-time, streaming data so you can get well-timed insights and react quickly to new data
- Offers abilities to cost-effectively process streaming data at any scale
- Provides flexibility to select the best tools for your application
- Allows you to consume real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications
- Enables you to process and analyze data as it arrives and respond rapidly instead of having to wait until all the data is collected

Cloud Endure

- Disaster Recovery is an automated IT resilience solution that assists in recovering your environment from unexpected outages, data corruption, ransomware, or other malicious attacks
- AWS Application Migration Service (CloudEndure Migration) simplifies, accelerates, and automates migrations from physical, virtual, and cloud-based infrastructure to AWS
- AWS Elastic Disaster Recovery (CloudEndure Disaster Recovery) reduces downtime and data loss by offering fast, dependable recovery of physical, virtual, and cloud-based servers into AWS in the event of IT disruptions