



Welcome Back to AWS Cloud Practitioner

Your instructor:

Michael J Shannon

CISSP #42221 / #524169,
CCNP-Security, PCNSE7,
Security+, GIAC GSEC,
OpenFAIR, and
ITIL 4 Managing Professional

**Class will begin at
10:00 A.M. Central
Standard Time (CST)**

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

Add user

1 Details — 2 Permissions — 3 Review — 4 **Complete**

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://219258942154.signin.aws.amazon.com/console>

[Download .csv](#)

	User	Access key ID	Secret access key	Email login instructions
▶	✓ Administrator	AKIAIIBX4IGZMHPPV4XA	***** Show	Send email ↗

[Close](#)

Feedback English (US) © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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
```

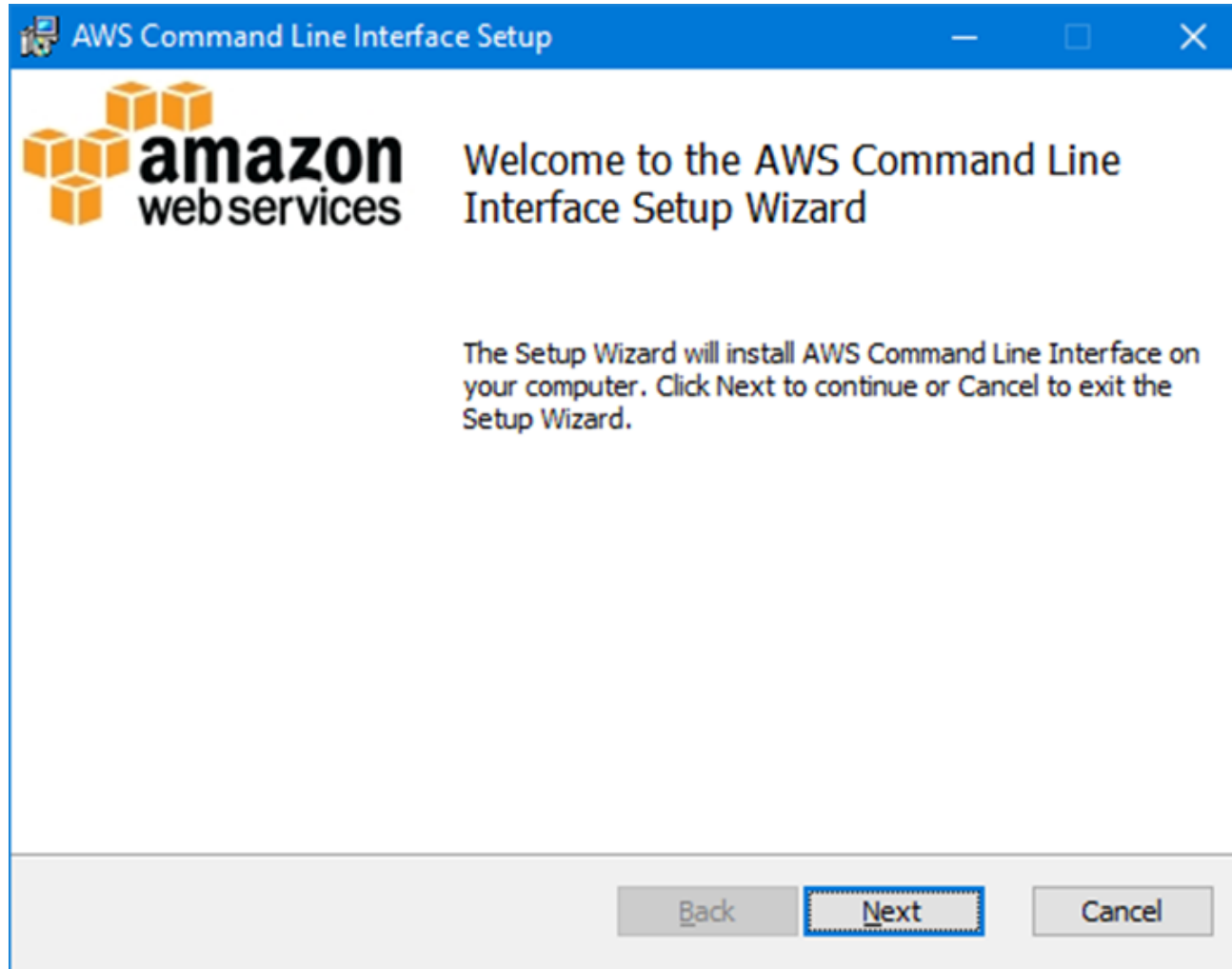
Amazon Linux

The AWS CLI comes pre-installed on [Amazon Linux AMI](#).

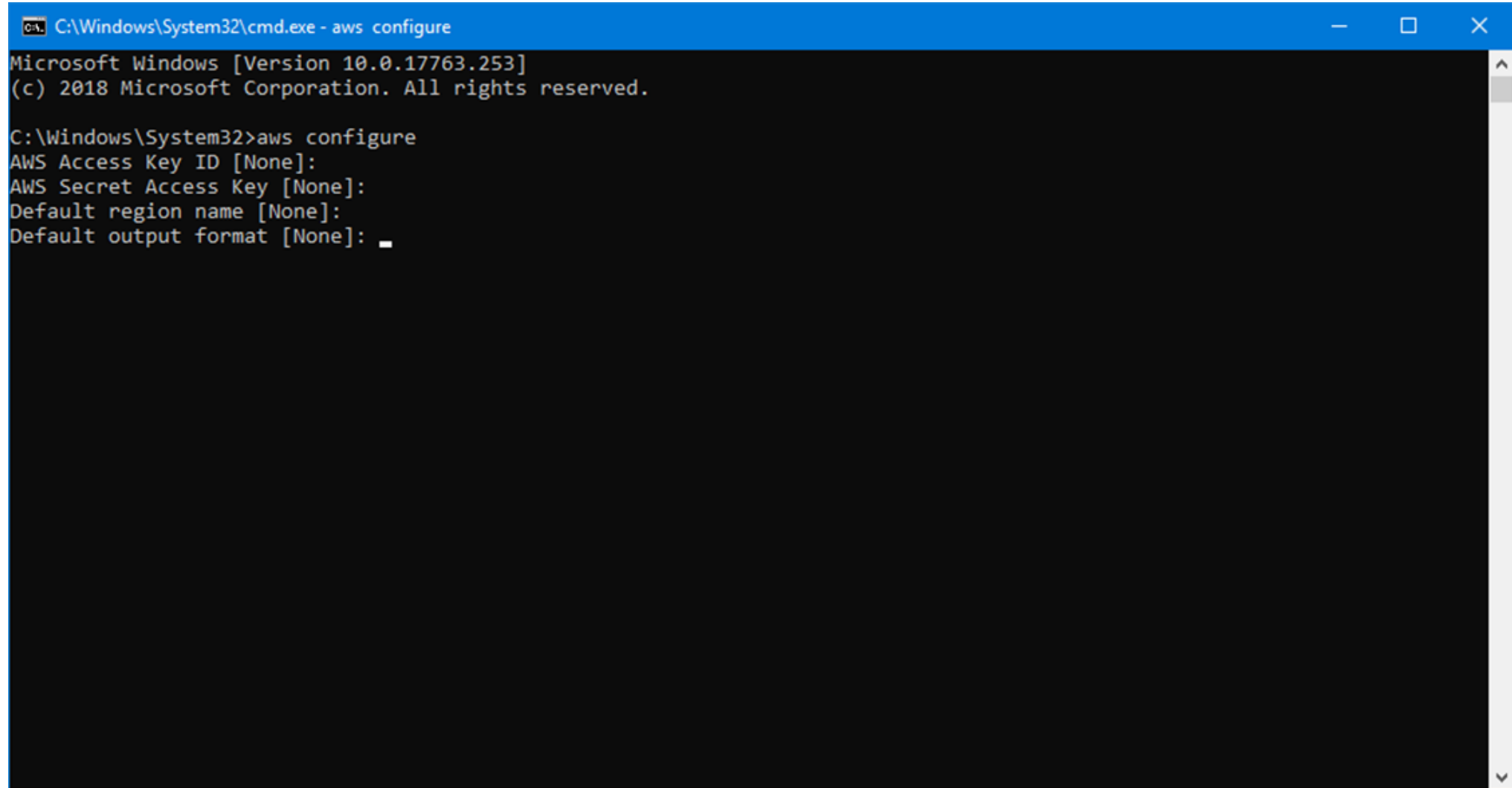
Release Notes

Check out the [Release Notes](#) for more information on the latest version.

Configuring CLI Access



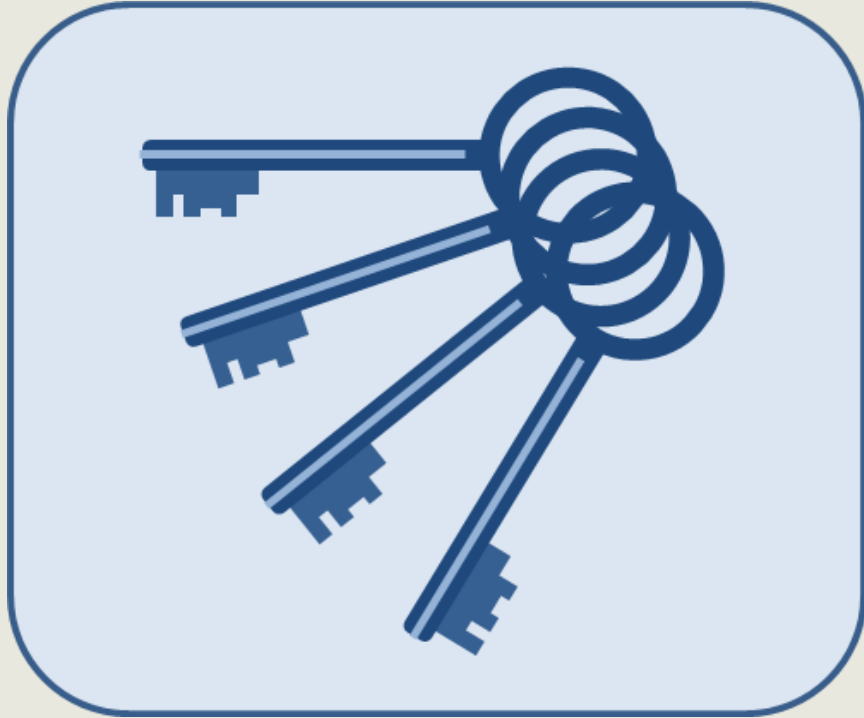
Configuring CLI Access



```
C:\Windows\System32\cmd.exe - aws configure
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\System32>aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]: _
```

Access Keys



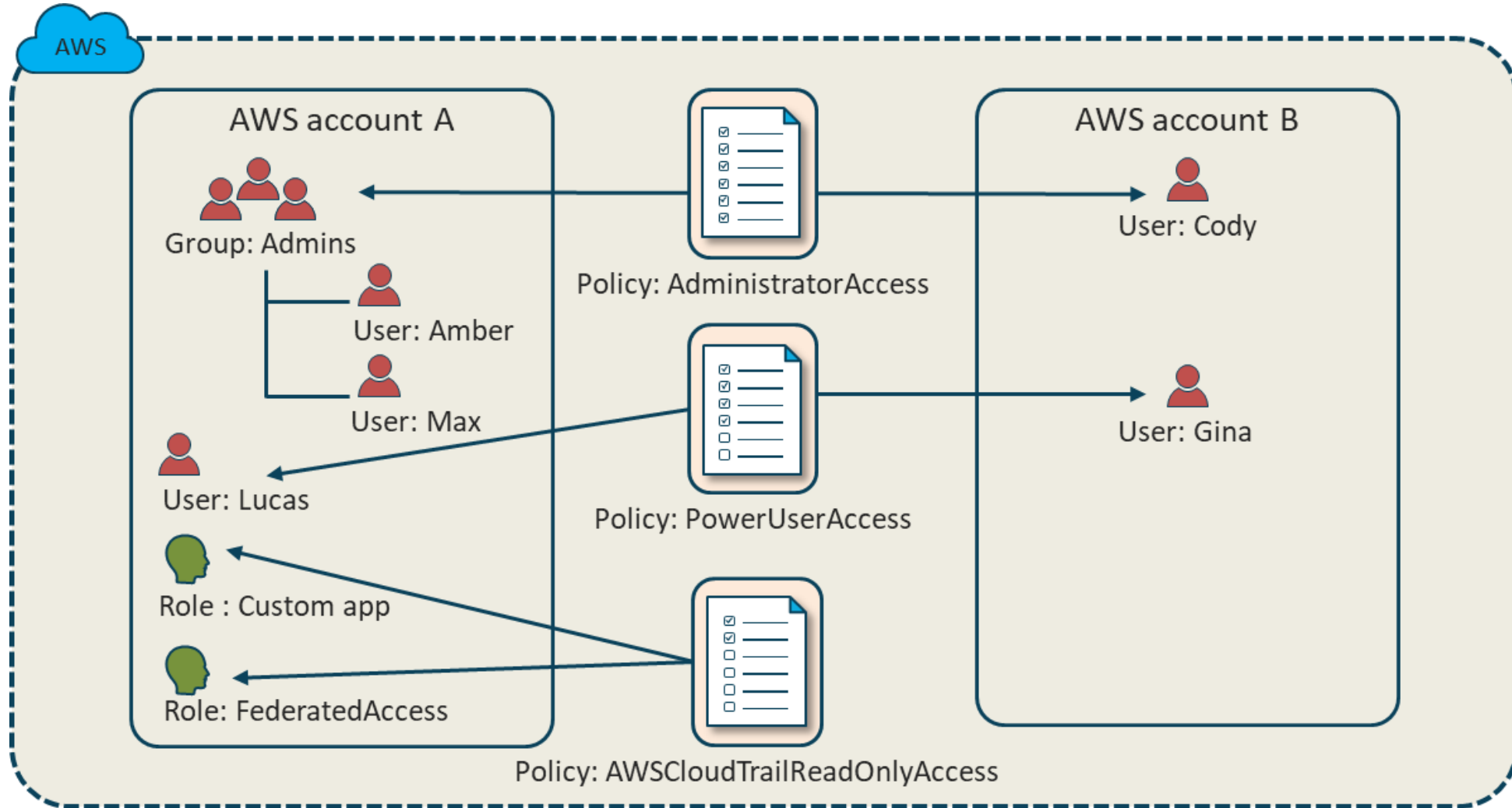
- Applications running outside of AWS will need access keys
- AWS SDKs will have digital signatures performed
- Signing protects message integrity by preventing tampering
- Requests must reach AWS within 15 minutes of the time stamp
- Version 4 also offers Forward Secrecy

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

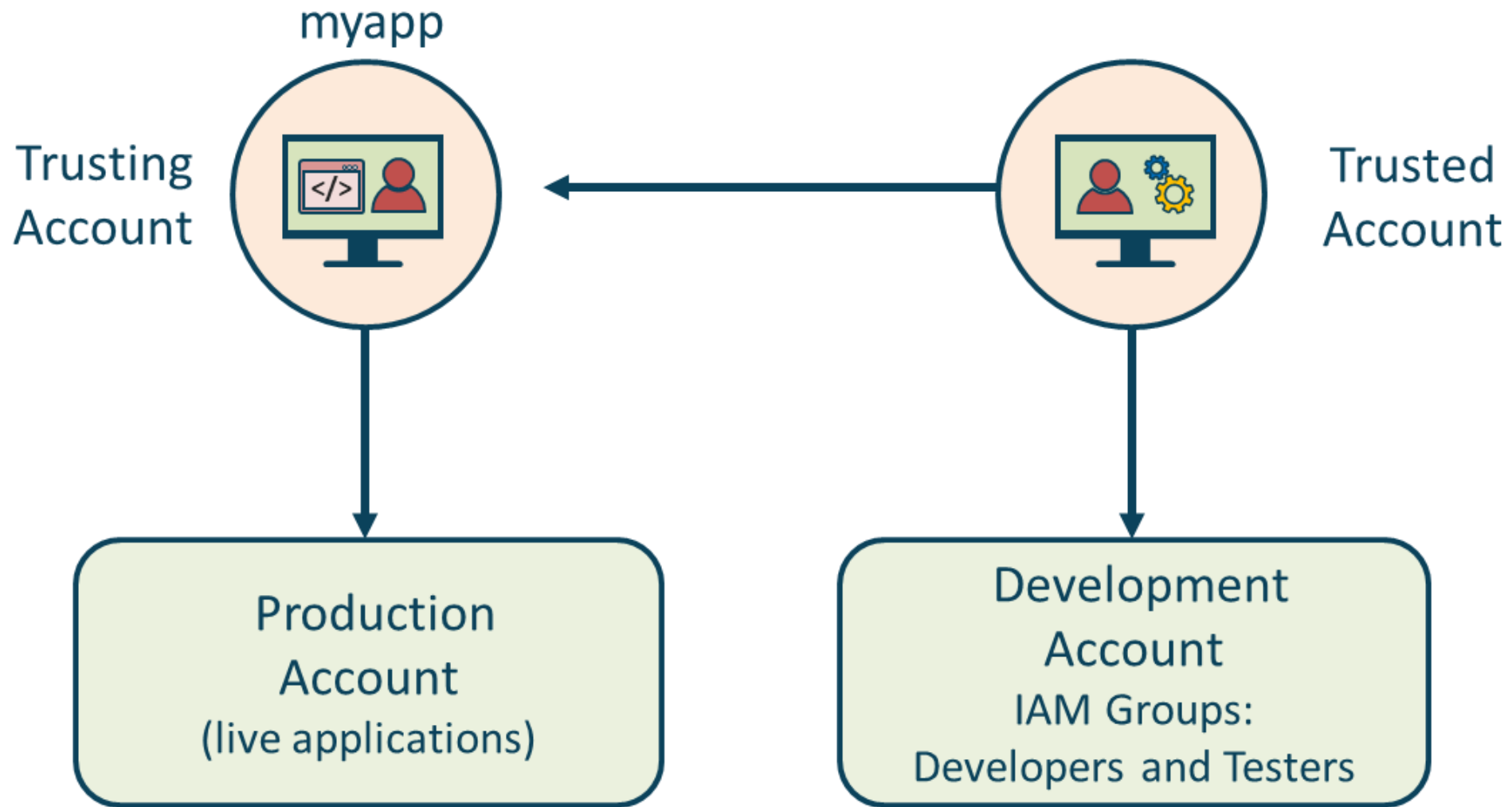


IAM Roles



- 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

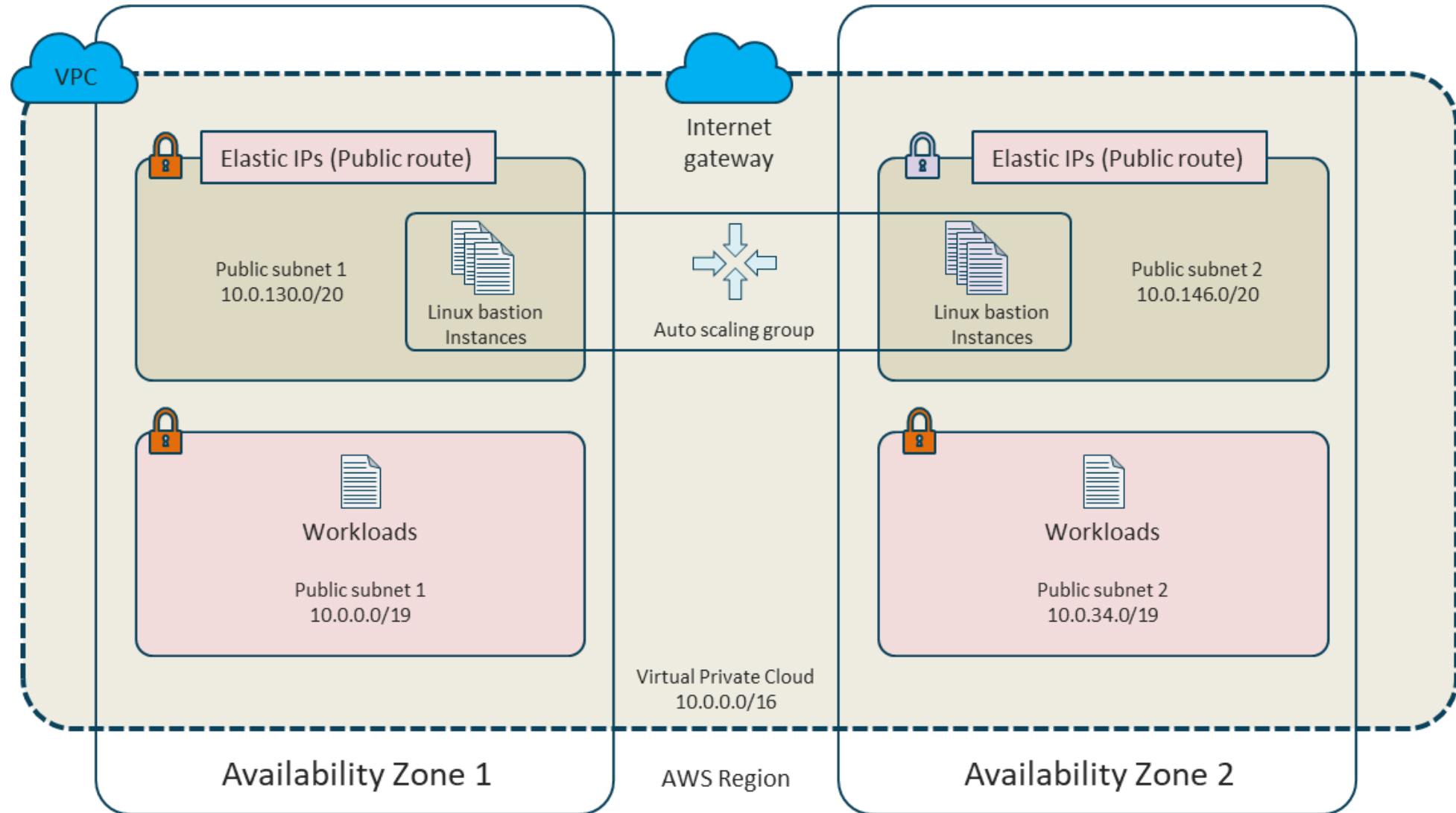
IAM Roles



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

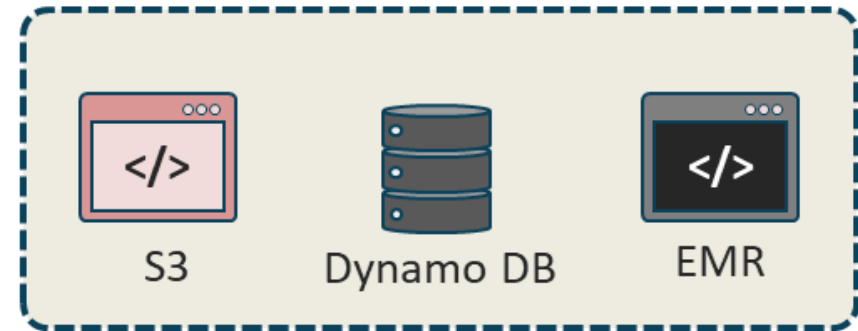
Bastion (Jump) Hosts



AWS Single-sign on (SSO)



AWS account resources



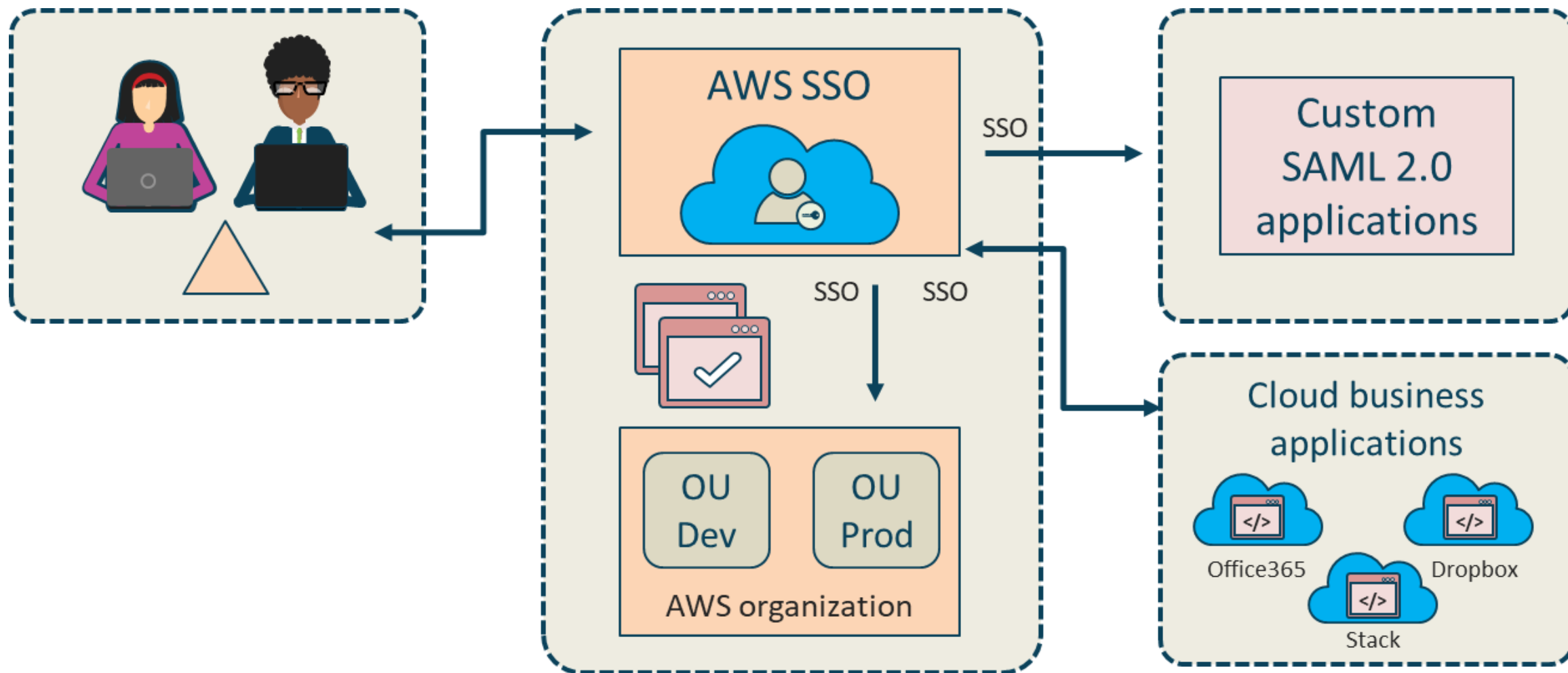
If users have many IAM accounts, consider SAML 2.0 federation to enable single-on (SSO)



SAML 2.0

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

AWS SSO




AWS SSO


Your applications

Hi John | [Sign out](#)


Search




AWS Management Console (3)




Dropbox





Office365



Slack


 650 (Account) >

 680 (Account) >

 903 (Account) v

SecurityAudit

Terms of Use

Powered by 

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_Ab129fa8b

✕

App client id

ex: 7lhlkkfbfb4q5kpp90urffao

Add Another Provider

* Required

Cancel

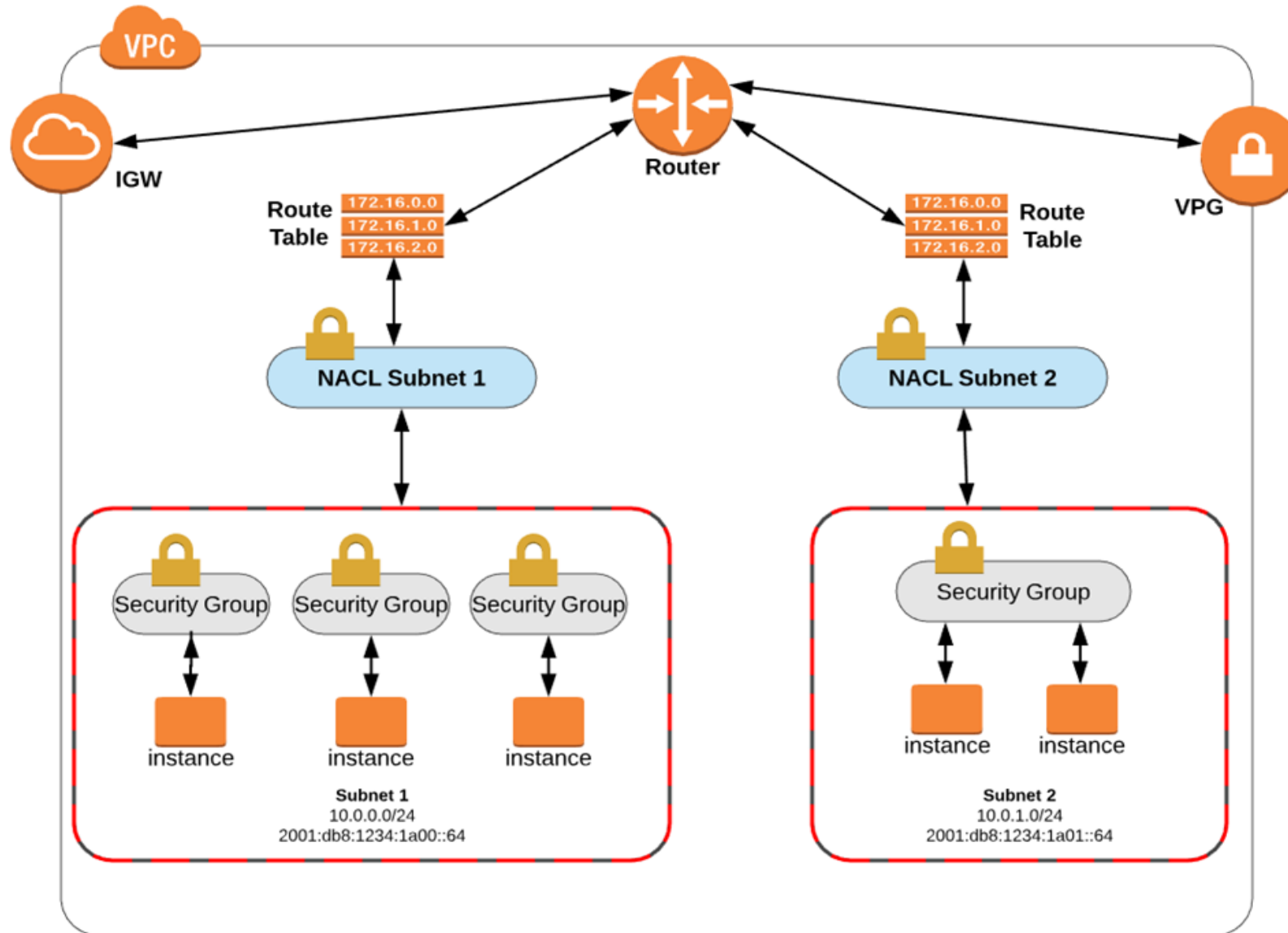
Create Pool

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

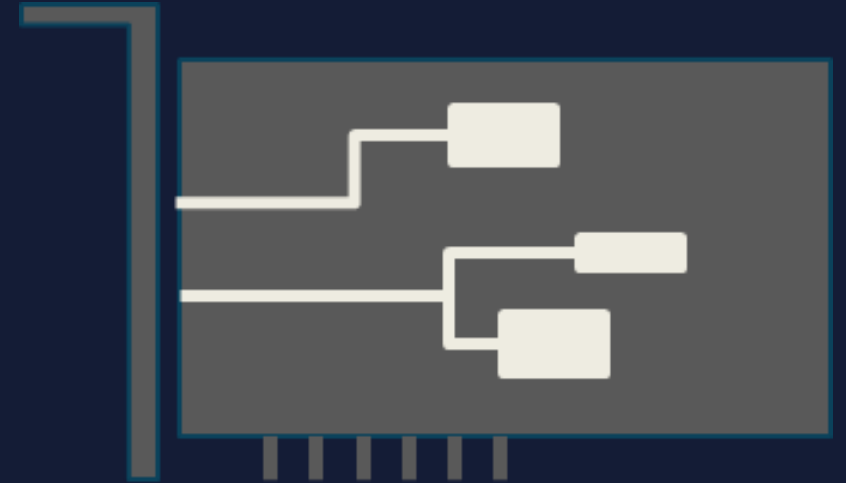


Network ACLs (NACLs)



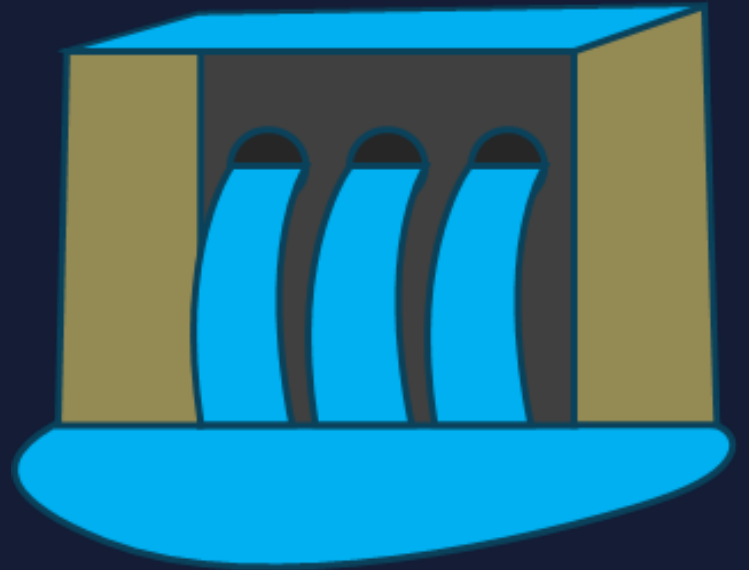
Security Groups

- 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

 Services ▾ Resource Groups ▾ 

 mjshannawstest ▾

[AWS WAF](#) > [Web ACLs](#) > Create web ACL

Step 1

Describe web ACL and associate it to AWS resources

Step 2

Add rules and rule groups: Add managed rule groups

Step 3

Set rule priority

Step 4

Configure metrics

Step 5

Review and create web ACL

Add managed rule groups [Info](#)

Close

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers.

▶ AWS managed rule groups

▶ Cyber Security Cloud Inc. managed rule groups

▶ Fortinet managed rule groups

▶ GeoGuard managed rule groups

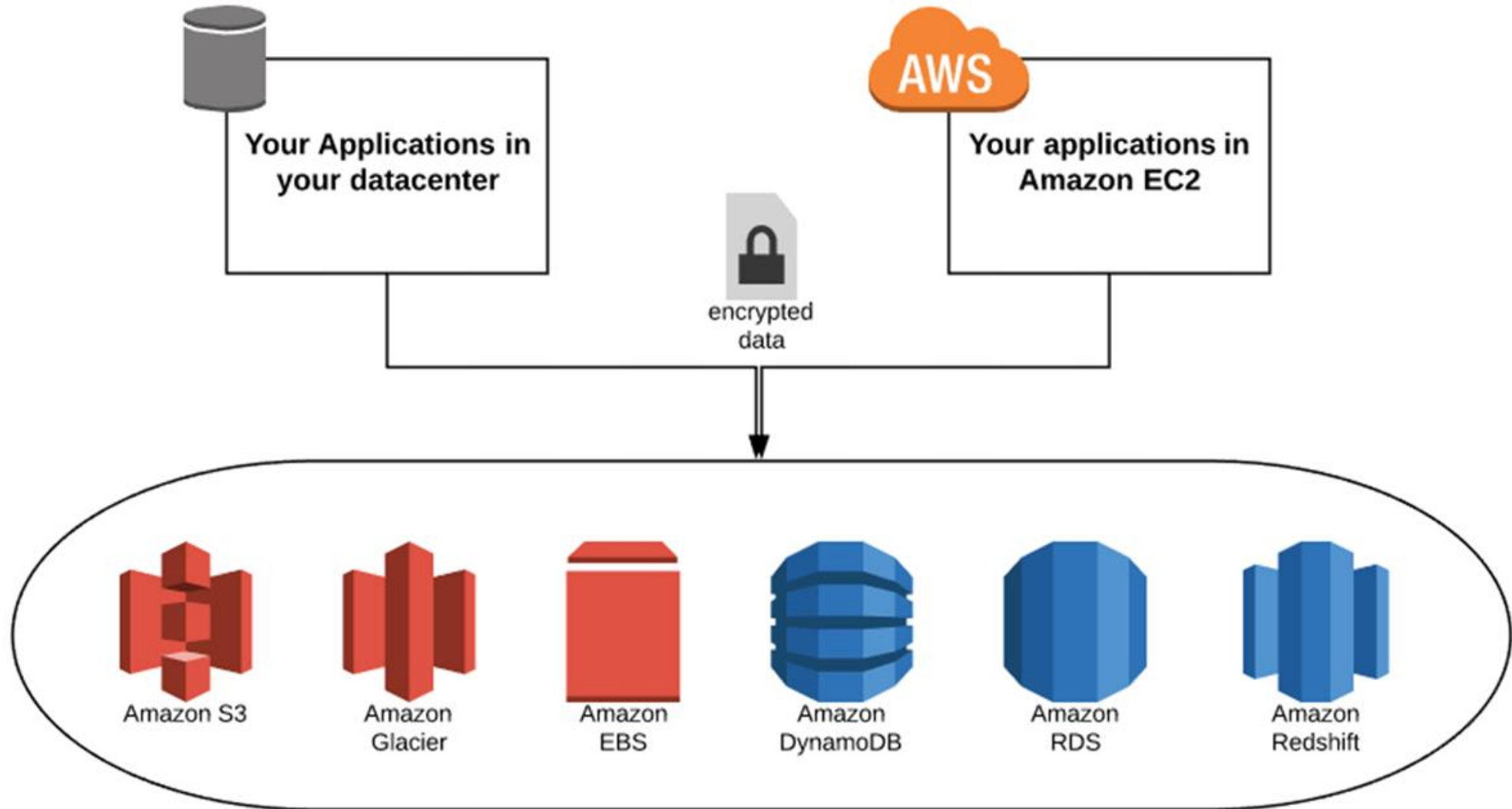
Cancel

Add rules

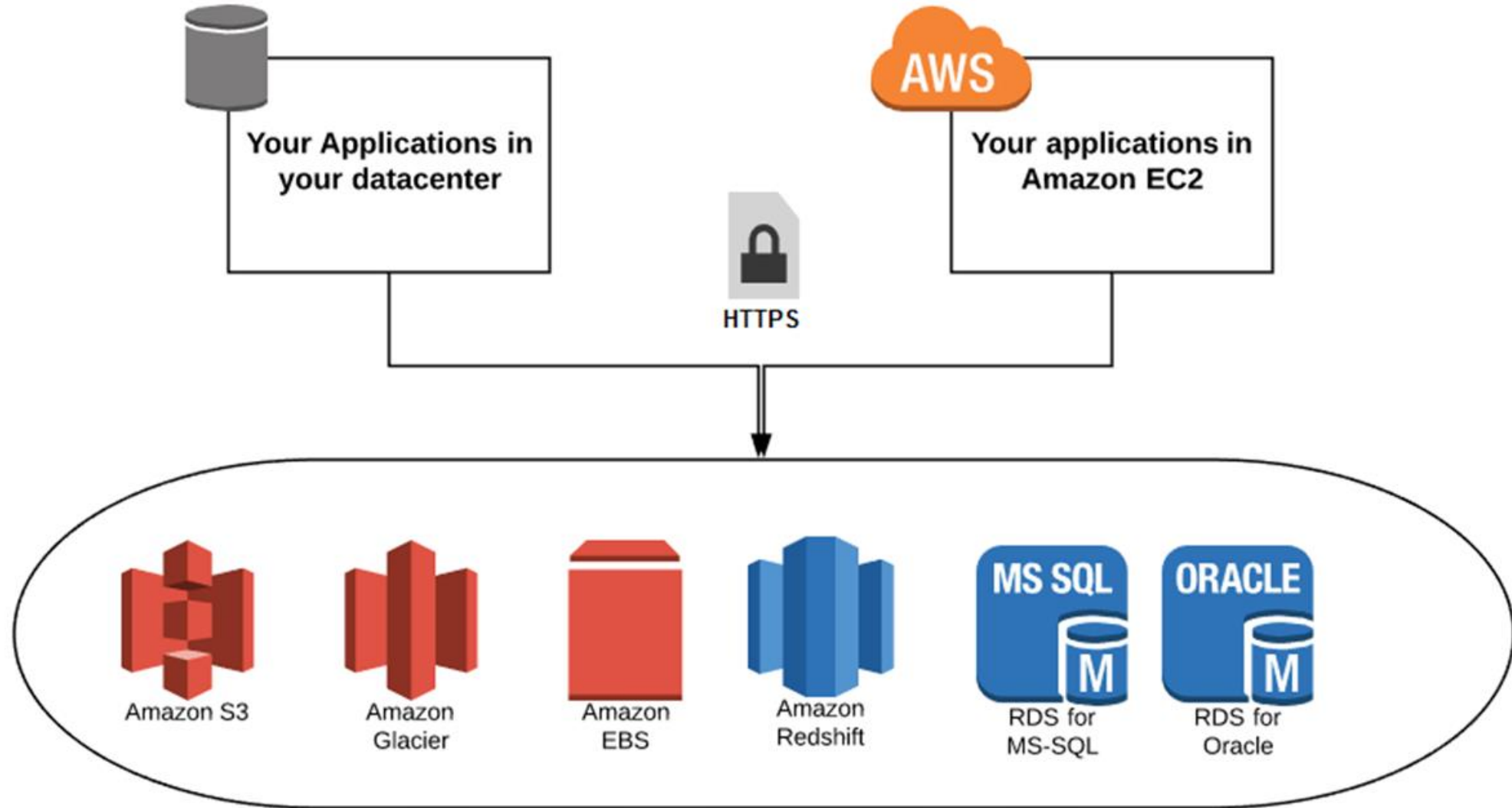
Web Application Firewall

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	<input type="radio"/> 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	<input type="radio"/> 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	<input type="radio"/> 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	<input type="radio"/> 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	<input type="radio"/> Add to web ACL
PHP application		

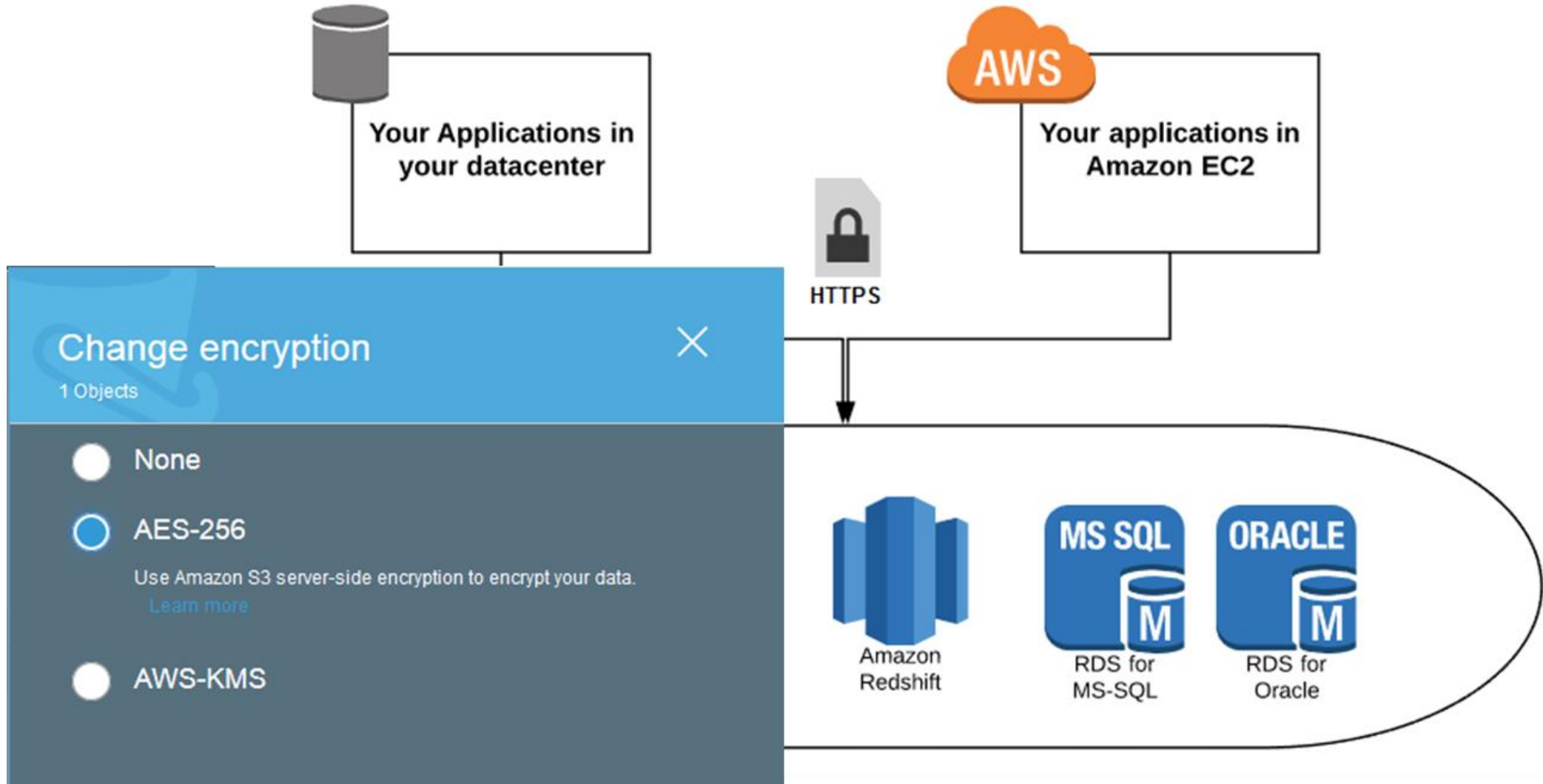
Client-side Encryption



Server-side Encryption



Server-side Encryption (i.e., S3 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 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

- 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



Amazon Inspector

- AWS discourages running assessment tools
- Includes knowledgebase of 100's of rules
- Produces a detailed list of security findings
- Results available through console or API
- Generates various meaningful reports

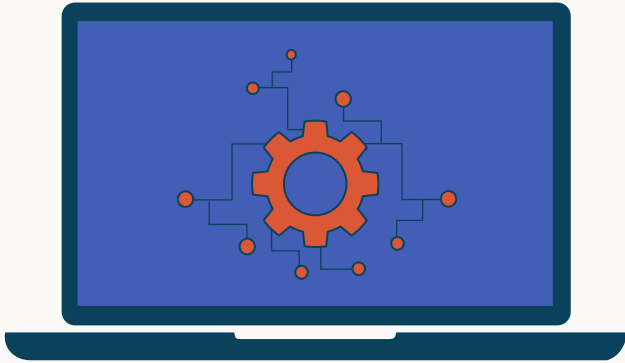


GuardDuty

- 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

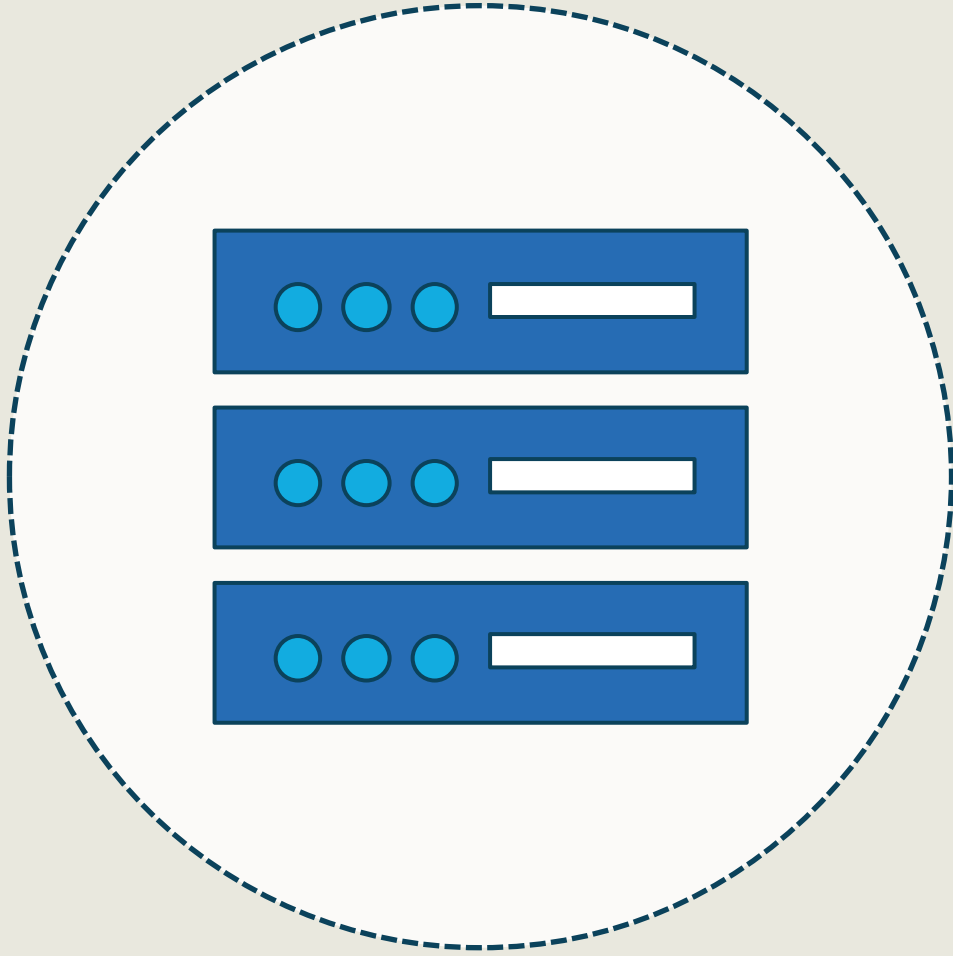


AWS Compute Services Survey



- 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

AWS Elastic Beanstalk



- 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

AWS Elastic Beanstalk

Application information

Application name

Up to 100 Unicode characters, not including forward slash (/).

Base configuration

Platform

Application code

-- Choose a platform --

Generic

Docker

Multi-container Docker

Preconfigured

Elastic Beanstalk Packer Builder

Go

.NET (Windows/IIS)

Java

Node.js

Ruby

PHP

Python

Tomcat

Preconfigured – Docker

GlassFish

Go

Python

... configuration options.

... or copy one from Amazon S3.

Cancel

Configure more options

Create application

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

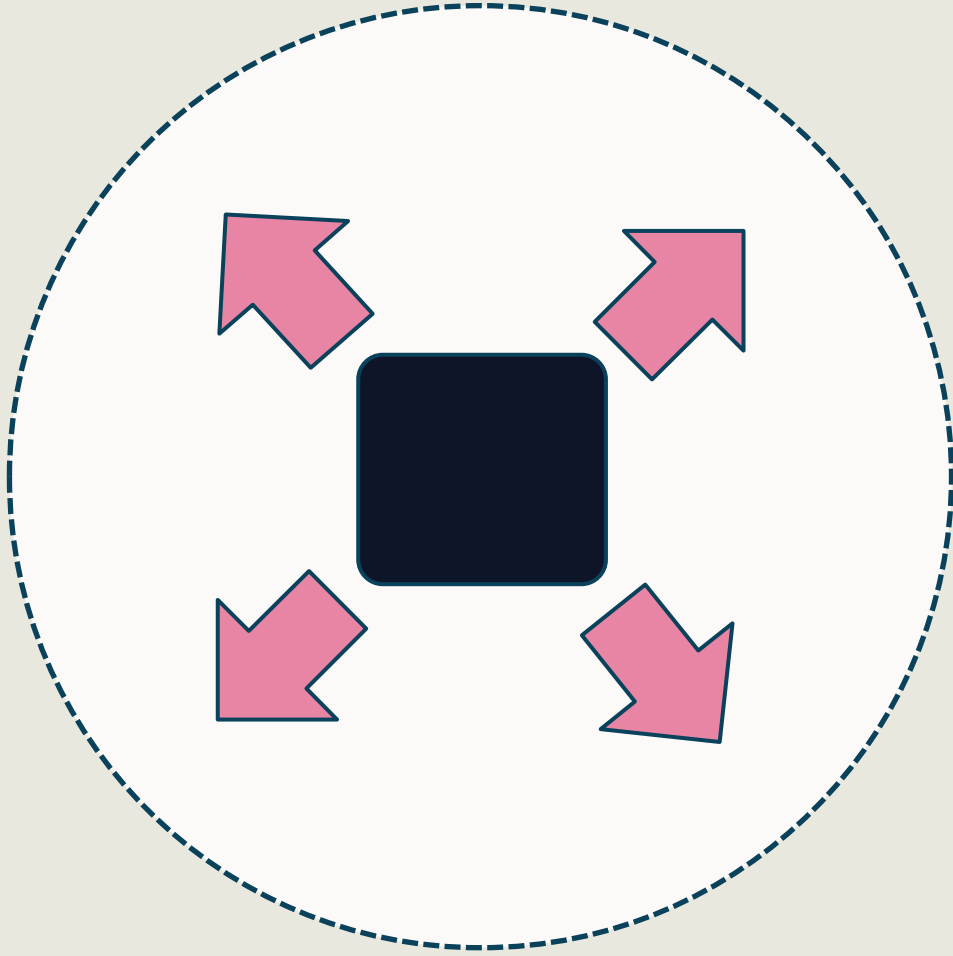
Containers



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

Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service

Auto Scaling

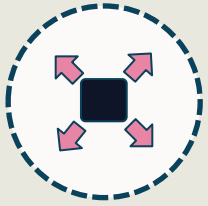


- Auto Scaling monitors applications and automatically modifies capacity to retain stable and predictable performance at the least possible cost
- You can build scaling plans for O/S instances, fleets, tasks, database tables, indexes, and replicas

Auto Scaling



Rapidly configure scaling feature with high visibility



Automate and optimize balance of availability and costs

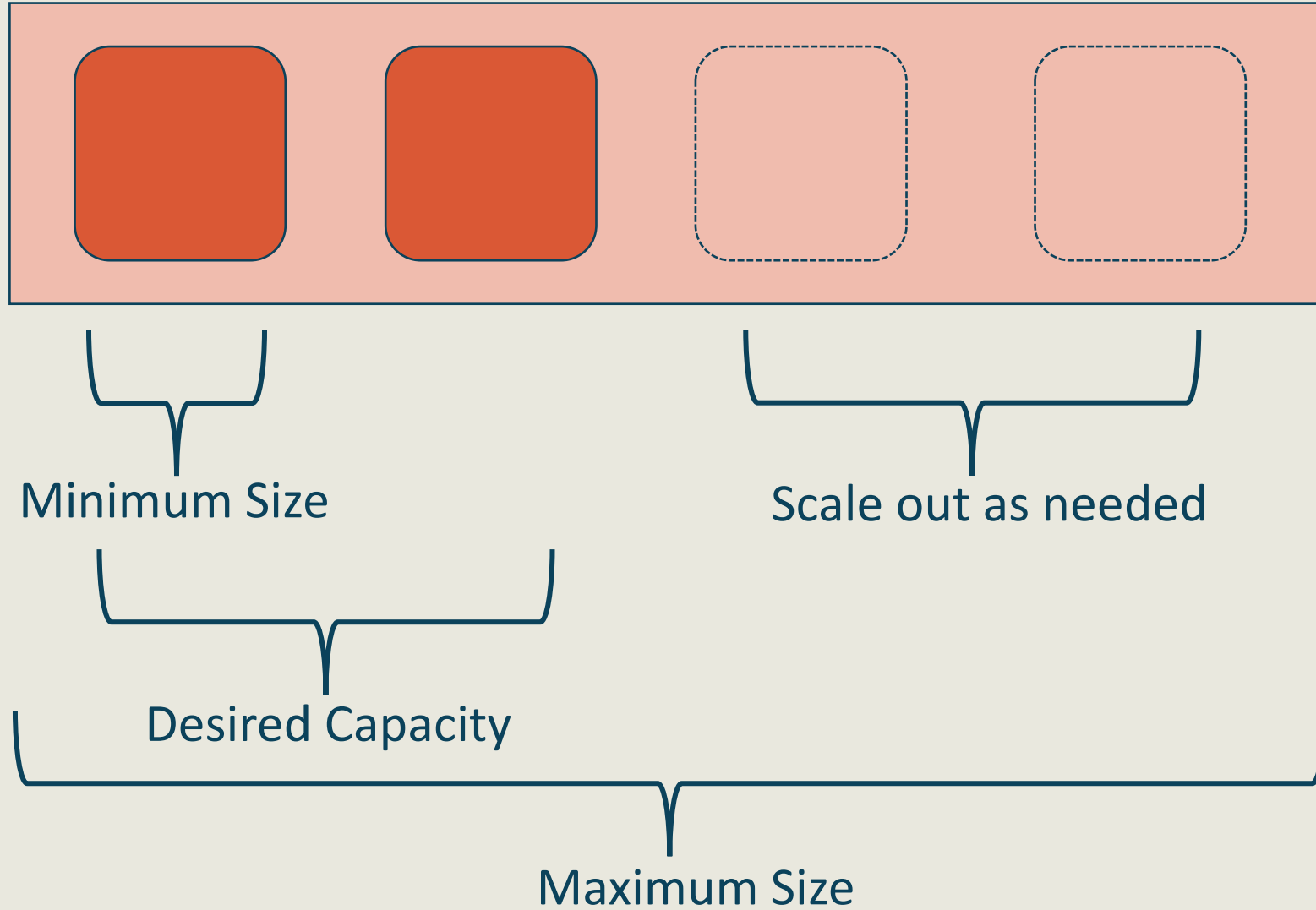


Constantly monitors to ensure desired performance levels



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 even Lambda functions.

AWS ELB

ELB Types



Application Load Balancer

For load balancing HTTP and HTTPS traffic for delivering modern application architectures

Network Load Balancer

For TCP,UDP, and TLS traffic routing traffic to VPCs optimized for high-speed, low-latency traffic

Classic Load Balancer

Legacy load balancing over multiple EC2 instances operating at both the request and connection level

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 CloudFormation

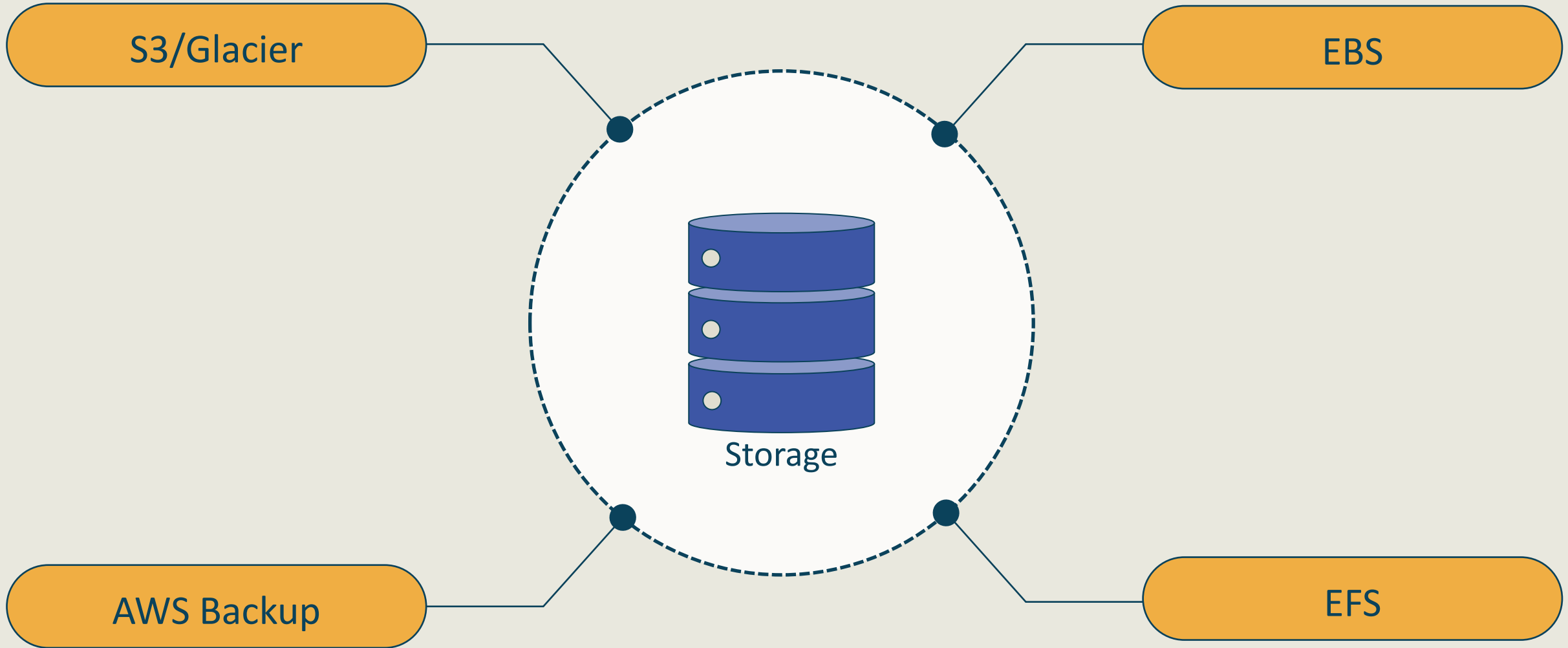
Template Name	Description	View	View in Designer	Launch
A single Amazon EC2 in an Amazon VPC	Creates a VPC and adds an Amazon EC2 instance with an Elastic IP address and a security group.	View	View in Designer	Launch Stack
Amazon VPC with static routing to an existing VPN	Creates a private subnet with 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 CloudFormation

The screenshot displays the AWS CloudFormation console interface. At the top, the navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a user profile 'mjshannawst'. Below the navigation bar, a toolbar contains icons for file operations and a 'Close' button. The main area is divided into two sections. The upper section shows a network diagram on a grid background, illustrating the relationships between various AWS resources. It includes two 'PublicSub...' (Public Subnets) represented by orange cube icons, a 'PublicLoa... SecurityGroup' (Public Load Balancing Security Group) represented by a red padlock icon, and other network components connected by lines. The lower section is a code editor for the CloudFormation template. It features a tab labeled 'temp...' and a 'Choose template language' dropdown set to 'JSON'. The JSON code is as follows:

```
1 {
2   "AWSTemplateFormatVersion": "2010-09-09",
3   "Description": "AWS CloudFormation Sample Template VPC_AutoScaling_With_Public_IPs.template: Sample template showing how to create a load
4   "Parameters": {
5     "KeyName": {
6       "Description": "Name of an existing EC2 KeyPair to enable SSH access to the instances",
7       "Type": "AWS::EC2::KeyPair::KeyName",
8       "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
9     },
10    "SSHLocation": {
11      "Description": "Lockdown SSH access to the bastion host (default can be accessed from anywhere)",
12      "Type": "String",
13      "ConstraintDescription": "must be a valid IP address or CIDR block"
14    }
```

AWS Storage Services Survey



Elastic Block Store (EBS)

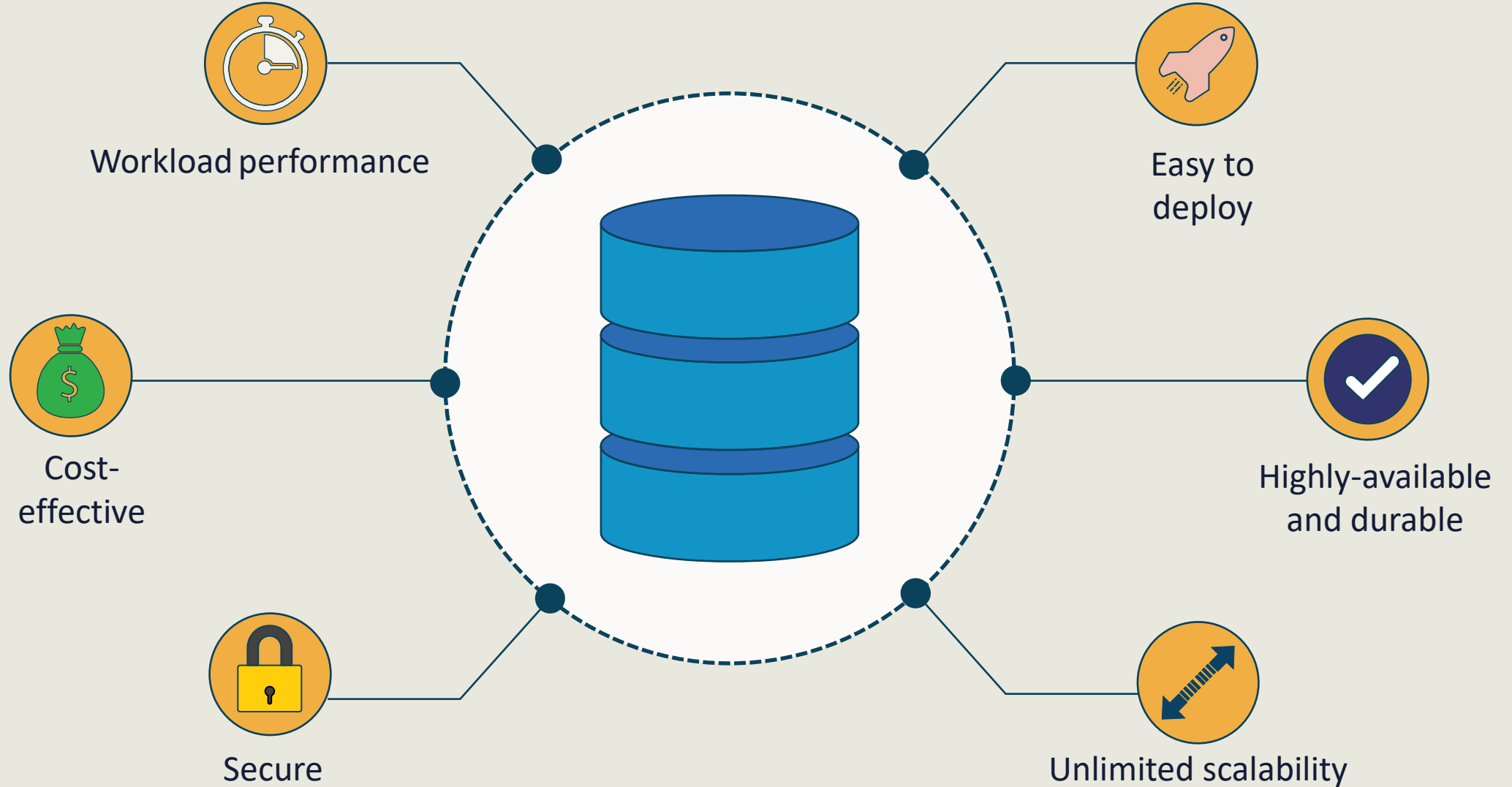


Amazon EBS offers persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud

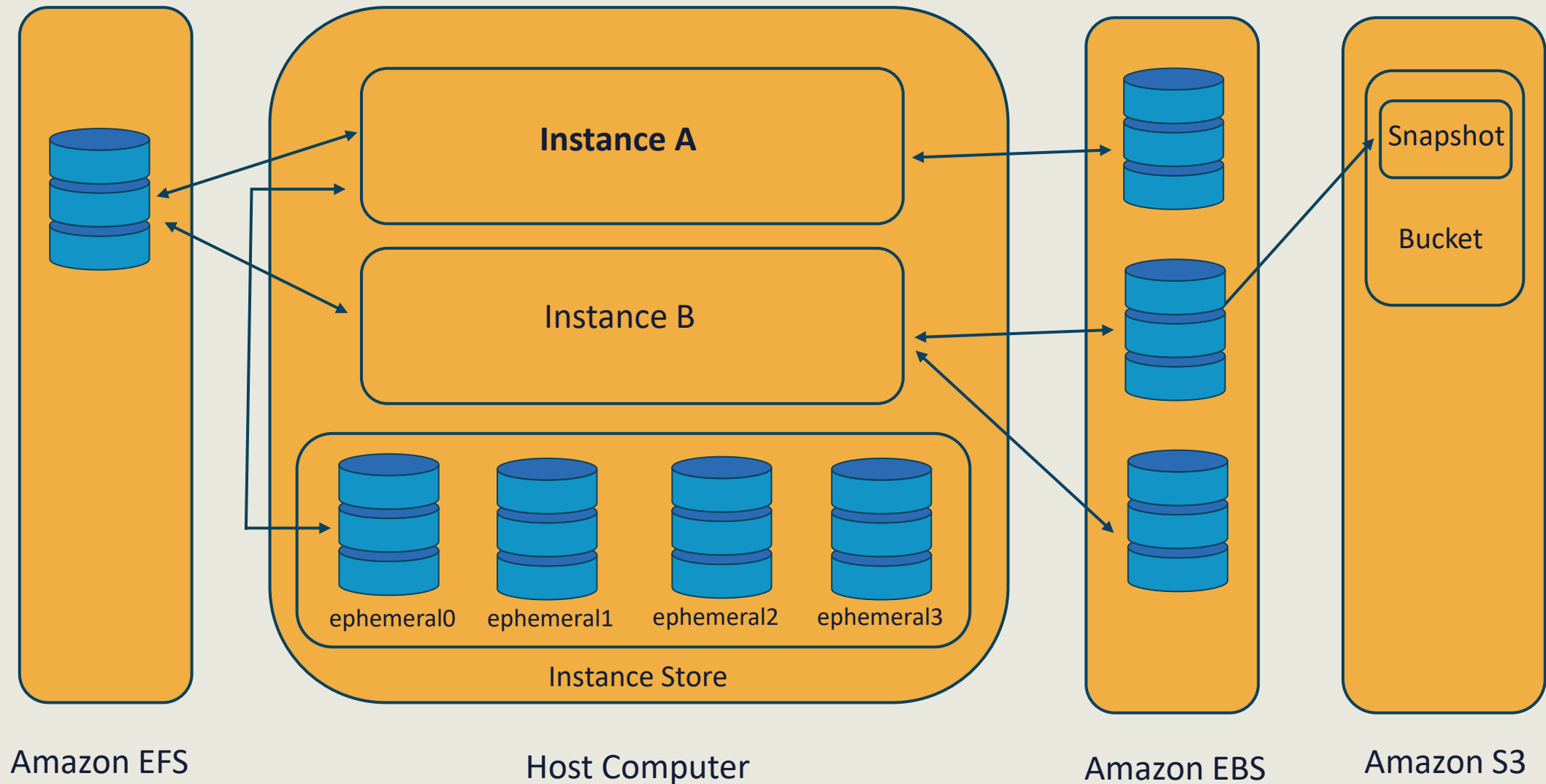
Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability

EBS volumes offer the consistent and low-latency performance needed to run your workloads

Elastic Block Storage (EBS)



Amazon EBS



EBS Encryption



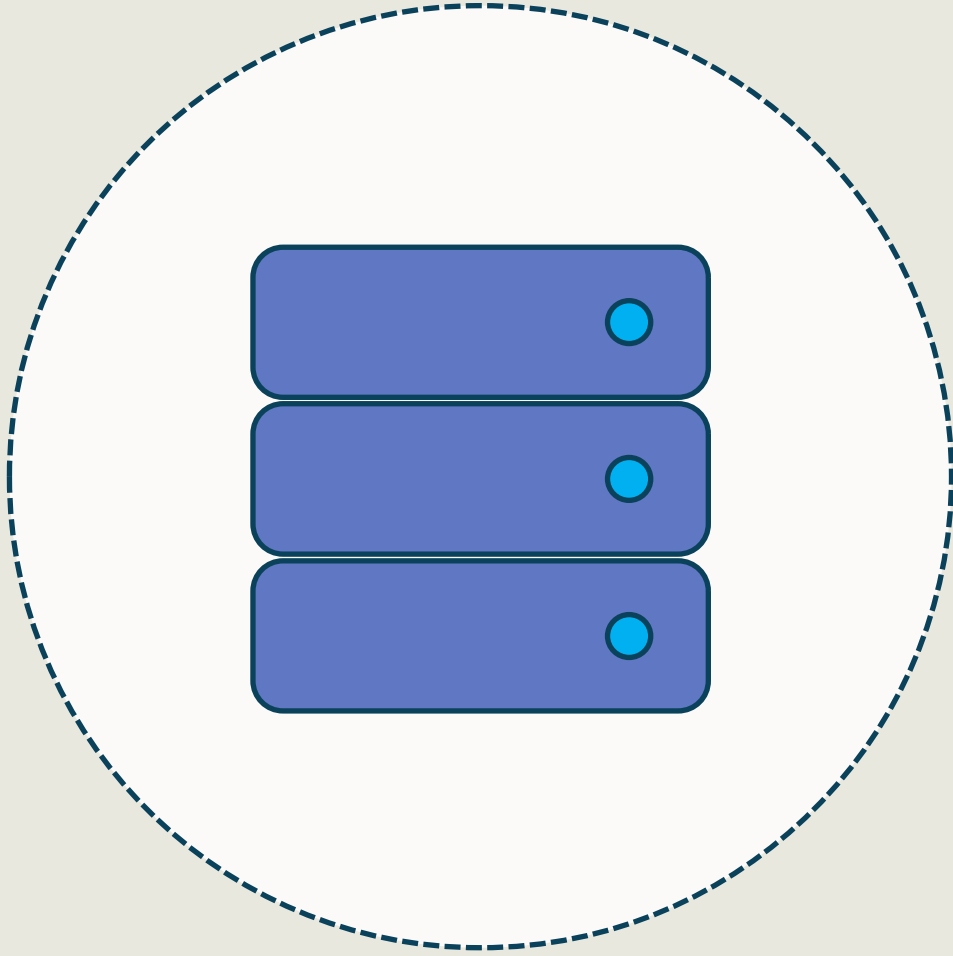
- When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:
 - Data at rest inside the volume
 - All data moving between the volume and the instance
 - All snapshots created from the volume
 - All volumes created from those snapshots
- You can encrypt both the boot and data volumes of an EC2 instance

EBS Encryption



- Amazon EBS encryption uses AWS KMS CMKs when creating encrypted volumes and any snapshots created from them
- You can enable the EBS Encryption by Default feature
- AWS encrypts new EBS volumes on launch
- AWS encrypts new copies of unencrypted snapshots
- Newly created EBS resources are encrypted to your account's default CMK unless you specify a custom CMK in the EC2 settings or at instance launch

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

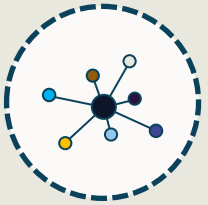
AWS Database Services Survey



Relational Database Service (RDS)



DynamoDB














Amazon Redshift

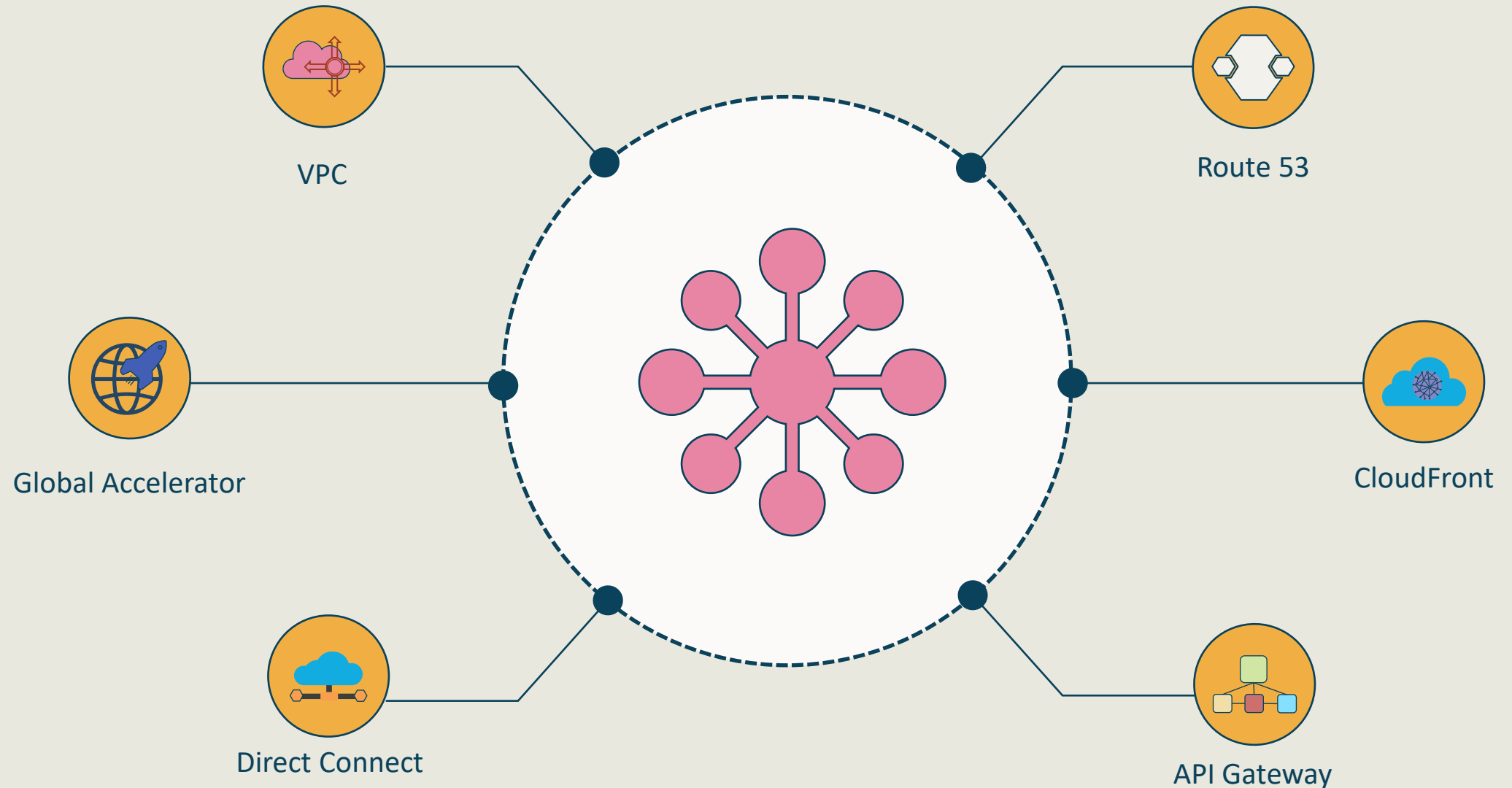


ElastiCache

Survey of 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 Networking and Content Distribution Survey



AWS Analytics Services Survey



- CloudWatch
- CloudTrail
- Elastic MapReduce (EMR)
- Kinesis
- Machine learning

AWS Support Plans



Basic



Developer

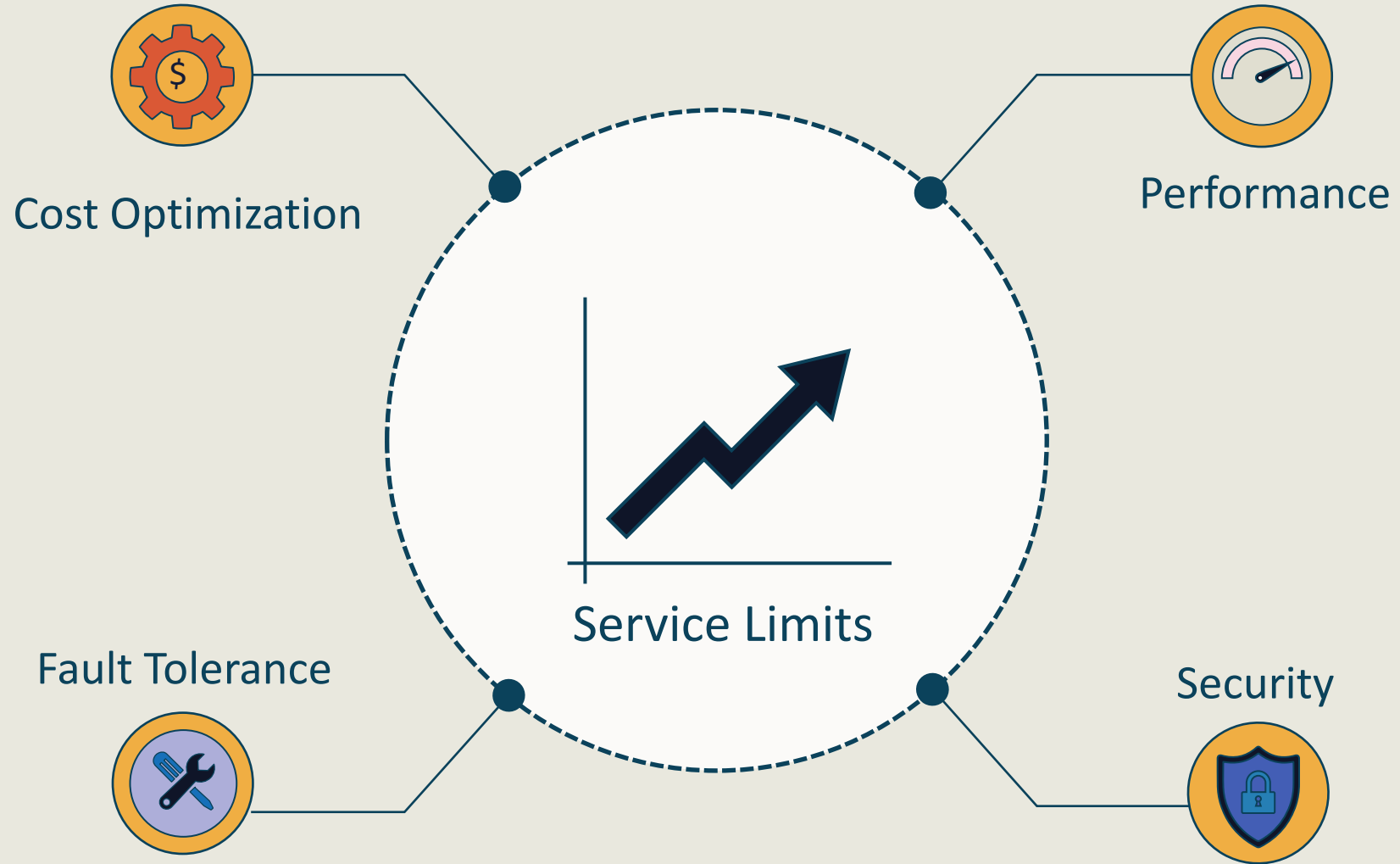


Business

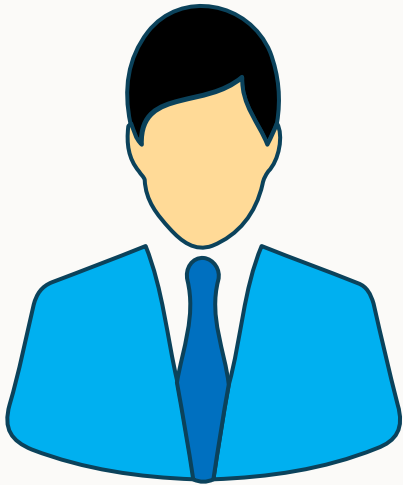


Enterprise

AWS Trusted Advisor

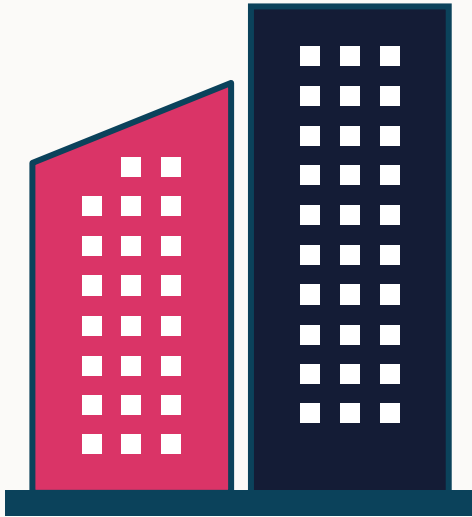


AWS Organizations



- AWS Organizations lets you centrally manage your environment as you scale and evolve your AWS workloads
- Helps you to centrally control billing, manage control access, compliance, and security
- Share resources across your AWS accounts

Organizations



Automate account creation and group accounts

Set up single payment for all AWS accounts

Define central configurations and resource sharing

No extra charge for AWS customers

Organizations

