AWS Cloud Practitioner Course

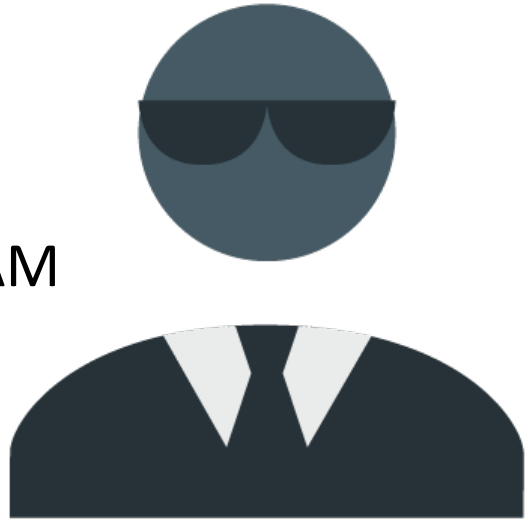
Michael J. Shannon

IT/Security Consultant, Instructor, and Author

Welcome back to AWS Cloud Practitioner!

DAY TWO

- Segment 1: Storage, Database, and Other Services
- Segment 2: AWS Security Basics and IAM
- Segment 3: Infrastructure Security
- Segment 4: Billing and Pricing

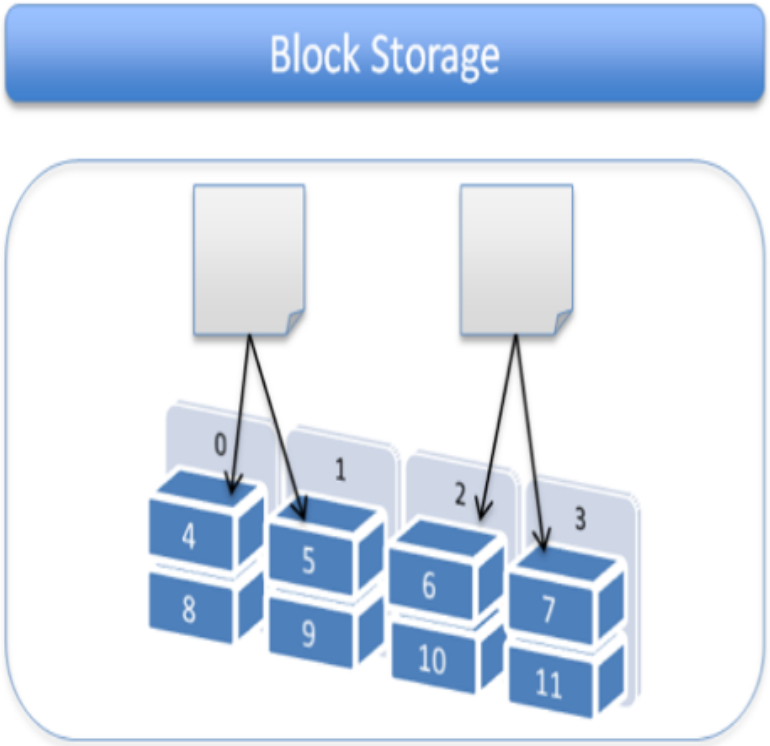


@iconshock.com

Segment 1: Database and Other Advanced Services

Block Storage at CSPs

- Files are split up and stored in fixed-sized blocks
- Host databases, supporting random read/write operations, and keeping system files of the running virtual machines
- Capacity increased by adding more nodes
- Suitable for apps that need high IOPS, database, and transactional data



@lifehacker.com

Elastic Block Storage (EBS)

- **Amazon Elastic Block Store (Amazon EBS)** provides 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

Some Object Storage Concepts

- Data is stored as discrete objects
- Data is not placed in a hierarchy of directories and instead resides in a flat address space
- Applications identify the discrete data objects by a unique address
- Designed for access at the application level using an API rather than at the user level
- Each object may also have metadata that is retrieved with it to better define or classify relationships with other objects

Core Storage Services

- **Amazon Simple Storage Service (Amazon S3)** is an object storage service that offers industry-leading scalability, data availability, security, and performance
- Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements
- S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world

Core Storage Services

- **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

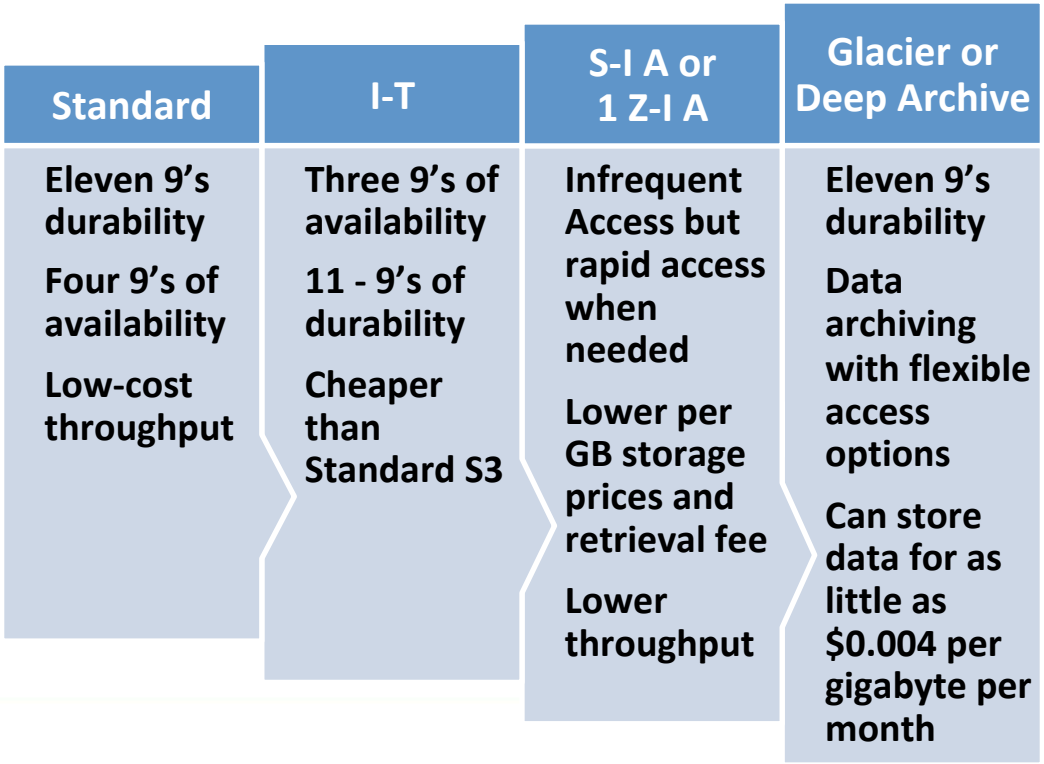
Core Storage Services

- **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.

@iconshock.com

Object Storage Tiering Strategy

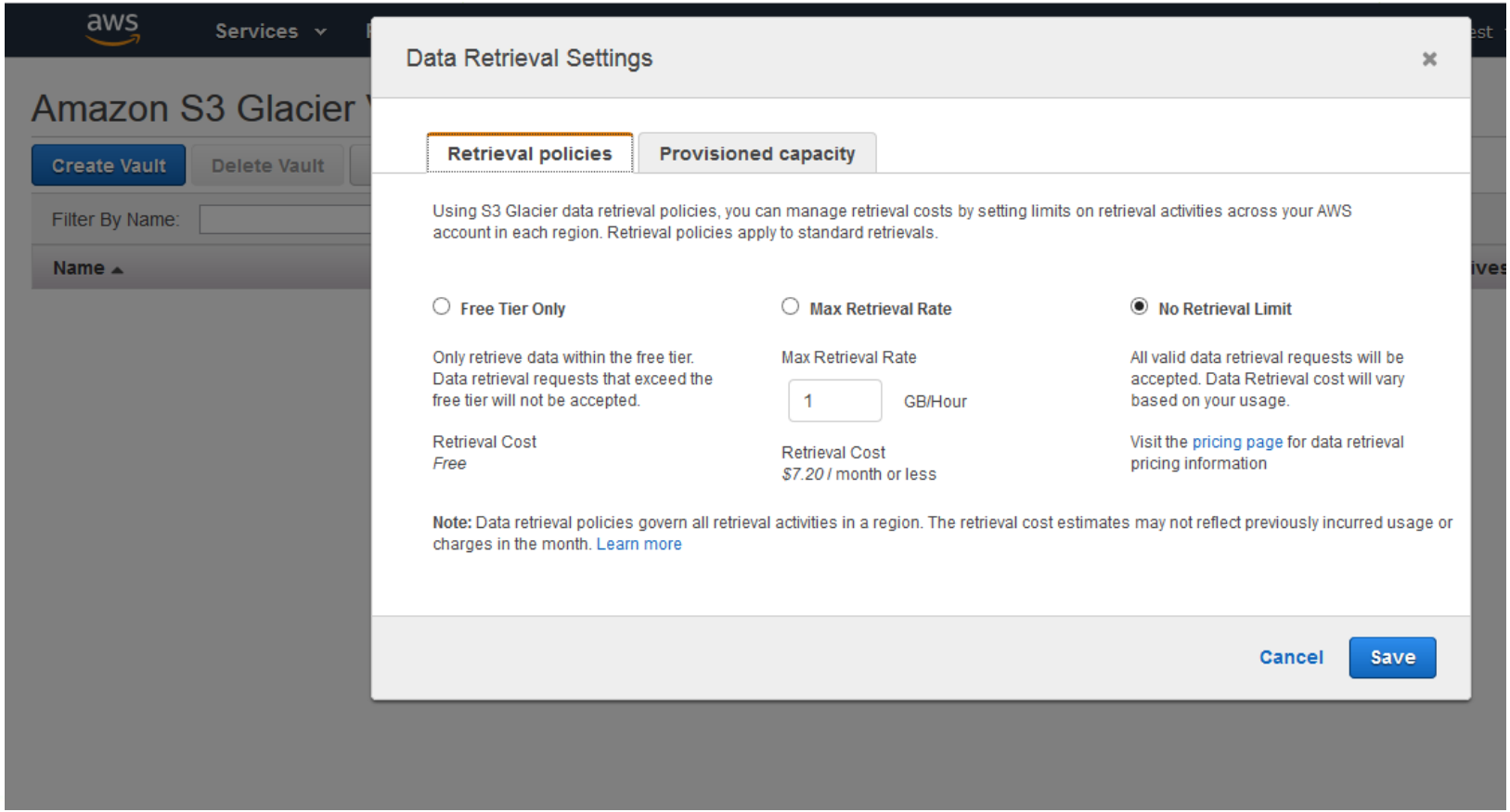
- **aws.amazon.com/s3/storage-classes/**



Amazon S3 Glacier

- Glacier is a low-cost, highly-durable (99.999999999%), and secure long-term backup and archiving solution
- Also offers query-in-place functionality to perform powerful analytics directly on the archived data at rest
- Data storage for as little as $0.004 per gigabyte a month
- Amazon S3 Glacier provides three retrieval options:
  - Expedited retrievals
  - Standard retrievals
  - Bulk retrievals

Amazon S3 Glacier



Core Database Services

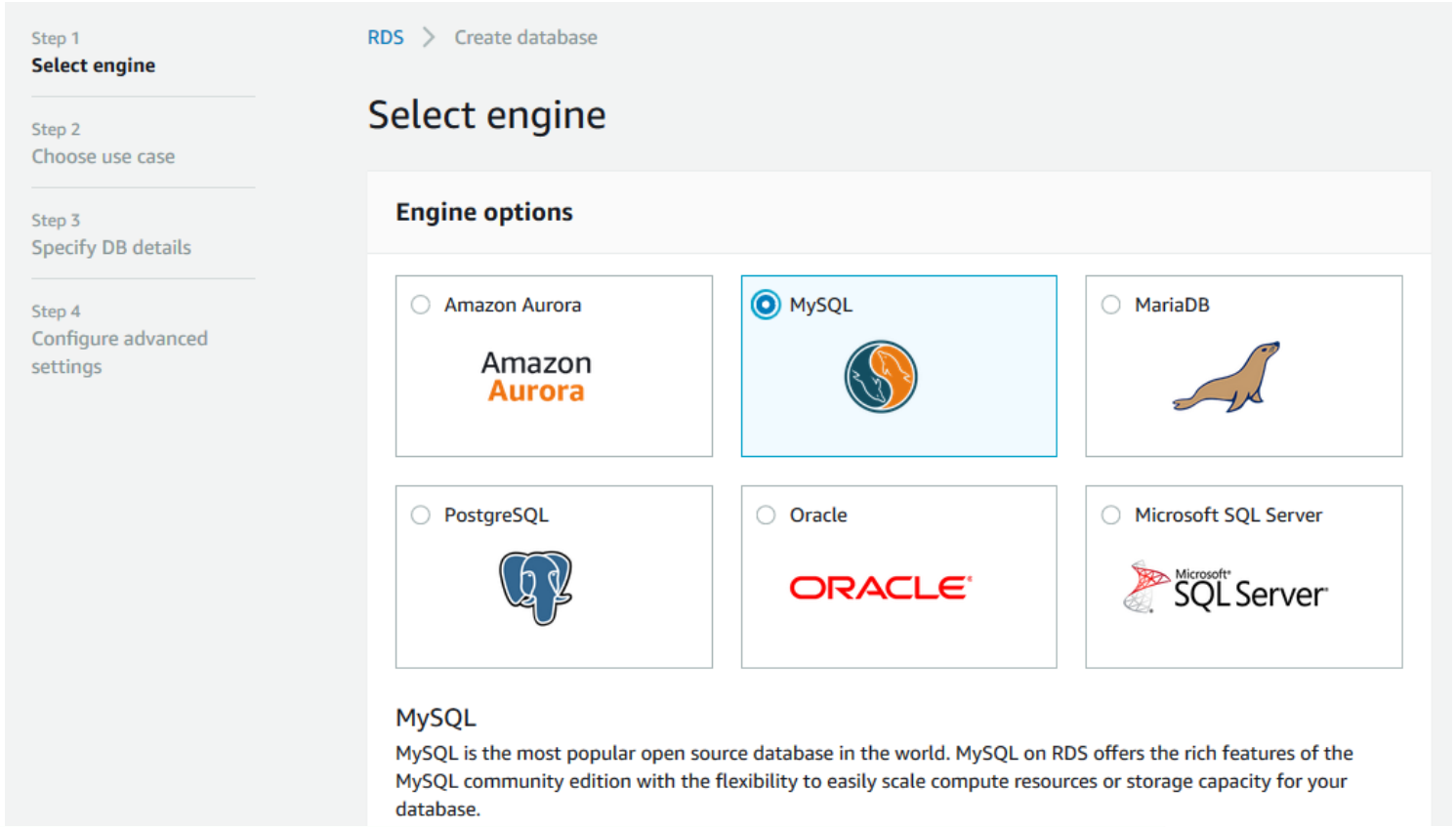
- **Amazon Relational Database Service (RDS)** is a managed service for setting up, operating, and scaling a cloud-based relational database
- RDS is available on several database instance types that are optimized for memory, performance or I/O
- Can choose from Amazon Aurora, PostgreSQL, MySQL, MariaDB,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

Core Database Services

- **Amazon Aurora** is a fully-managed MySQL and PostgreSQL compatible relational database engine
  - Aurora supports up to 64TB of auto-scaling storage capacity, 6-way replication across three availability zones, and 15 low-latency read replicas
  - Costs start at less than $1/day

@iconshock.com

AWS Relational Database Service (RDS)



Core Database Services

- **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

Core Database Services

- **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

@iconshock.com

Core Database Services

- **Amazon Neptune** is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets
- **Amazon Quantum Ledger Database (QLDB)** is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log owned by a central trusted authority
- **Amazon Timestream** is a fast, scalable, fully managed time series database service for IoT and operational applications to store and analyze trillions of events per day at 1/10th the cost of relational databases

Amazon Redshift

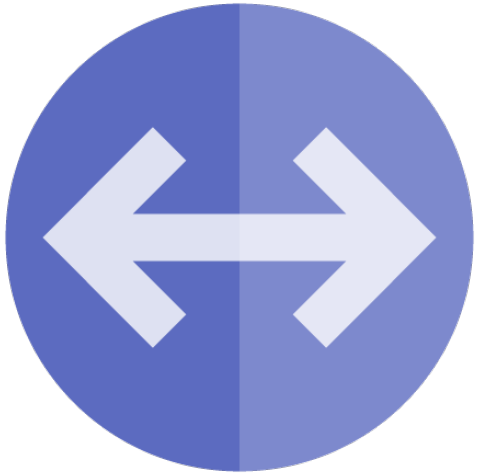
- **Amazon Redshift** clusters provide a fast, scalable data warehouse for cost-effective analysis of data across data warehouses and data lakes
- Uses machine learning, massively parallel query execution, and columnar storage on high-performance disks
- High security is provided using a 4-key nested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

Virtual Resource Migrations

- Migration to an on-premise virtual or cloud solution is one of the first steps in the cloud adoption model
- Virtual machine templates are invaluable streamlined and standardized installation policies/profiles
- Templates offer repeatable processes that reduce error and costs while offering faster deployment times
- A Master VM template is a master image to be used as a baseline implementation which can be easily patched and updated as needed (AWS CloudFormation)

Virtual Resource Migrations

- Physical to Virtual (P2V)
  - Convert physical server to virtual
  - Manual, Semi-automated, or Fully automated
- Virtual to Virtual (V2V)
  - Example: Open Virtualization Format (OVF)
- Virtual to Physical (V2P)
  - More complex involving several tools – rarely done



@iconshock.com

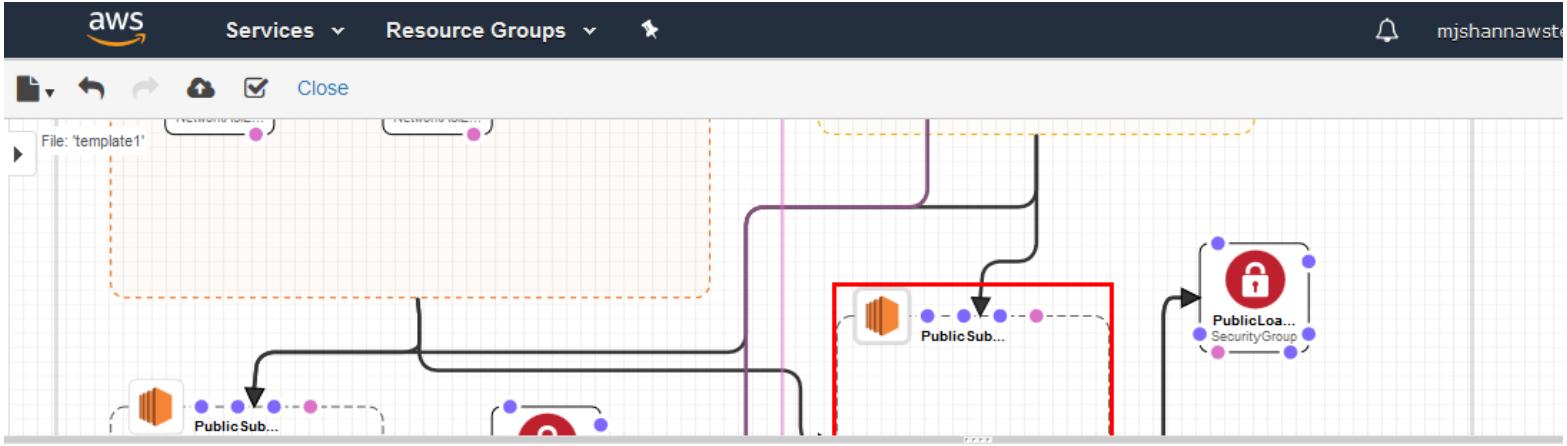
AWS CloudFormation

- AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment – Infrastructure-As-Code
- CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts
- This file serves as the single source of truth for your cloud environment in a safe, repeatable manner

Example: AWS CloudFormation Template

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 Templates



temp...

Choose template language: JSON YAML

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Description": "AWS CloudFormation Sample Template VPC_AutoScaling_With_Public_IPs.template: Sample template showing how to create a load
    "Parameters": {
        "KeyName": {
            "Description": "Name of an existing EC2 KeyPair to enable SSH access to the instances",
            "Type": "AWS::EC2::KeyPair::KeyName",
            "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
        },
        "SSHLocation": {
            "Description": "Lockdown SSH access to the bastion host (default can be accessed from anywhere)",
            "Type": "String",
```

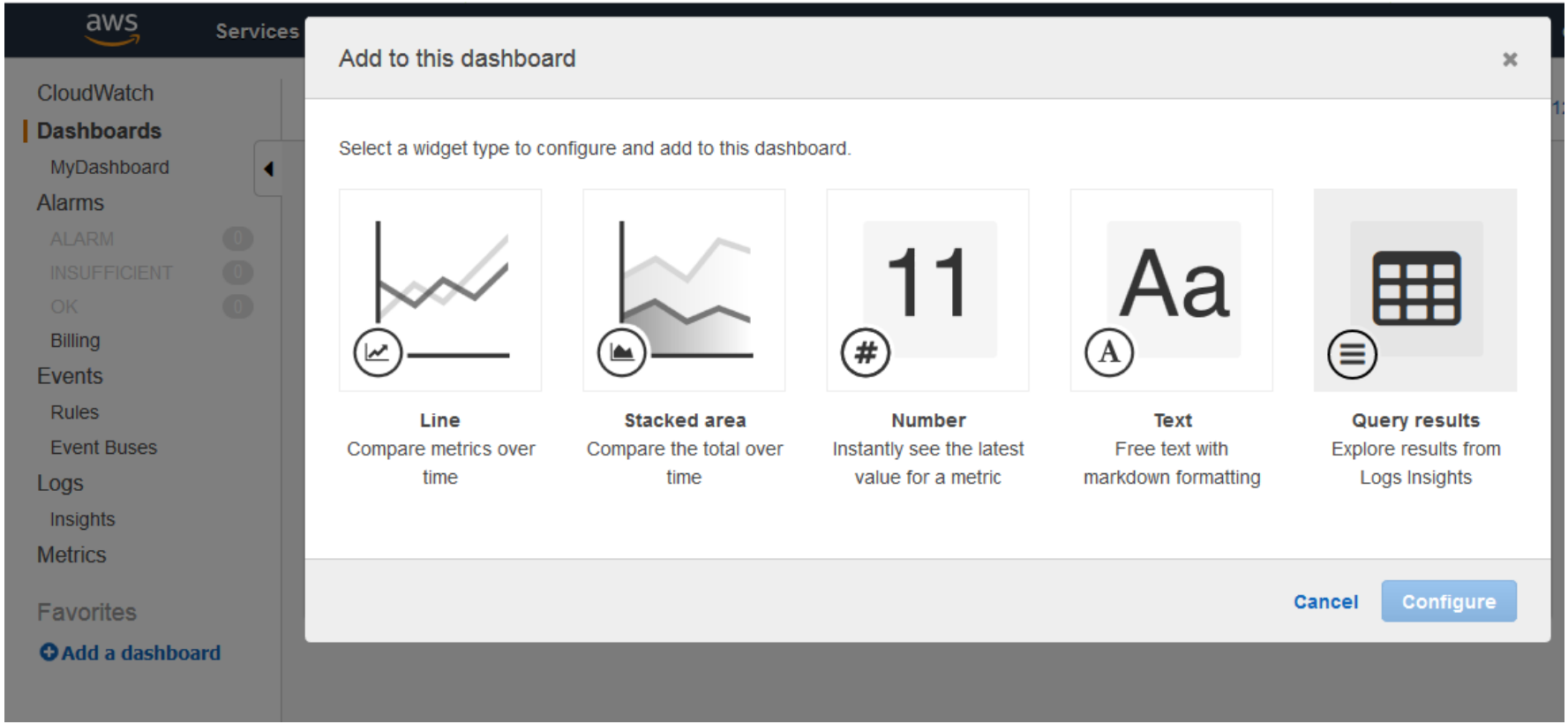
Amazon CloudWatch

- **Amazon CloudWatch** is used for management and governance
- CloudWatch is a monitoring and management service designed for developers, system operators, site reliability engineers (SRE), and IT 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 and troubleshoot the infrastructure
  - 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
  - Trigger automated CloudWatch Alarms and Lambda workflows to enhance the customer experience
  - Explore, analyze, and visualize logs instantly to address operational issues and improve applications performance
- Optimize resources
  - Leverage CloudWatch Alarms to automate capacity and resource planning with Auto Scaling

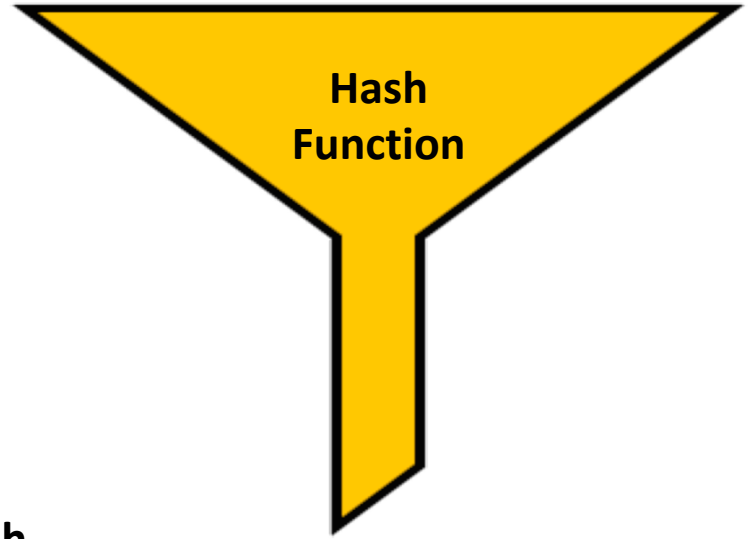
CloudWatch Dashboards



Segment 2: AWS Security Survey and IAM

Hashing

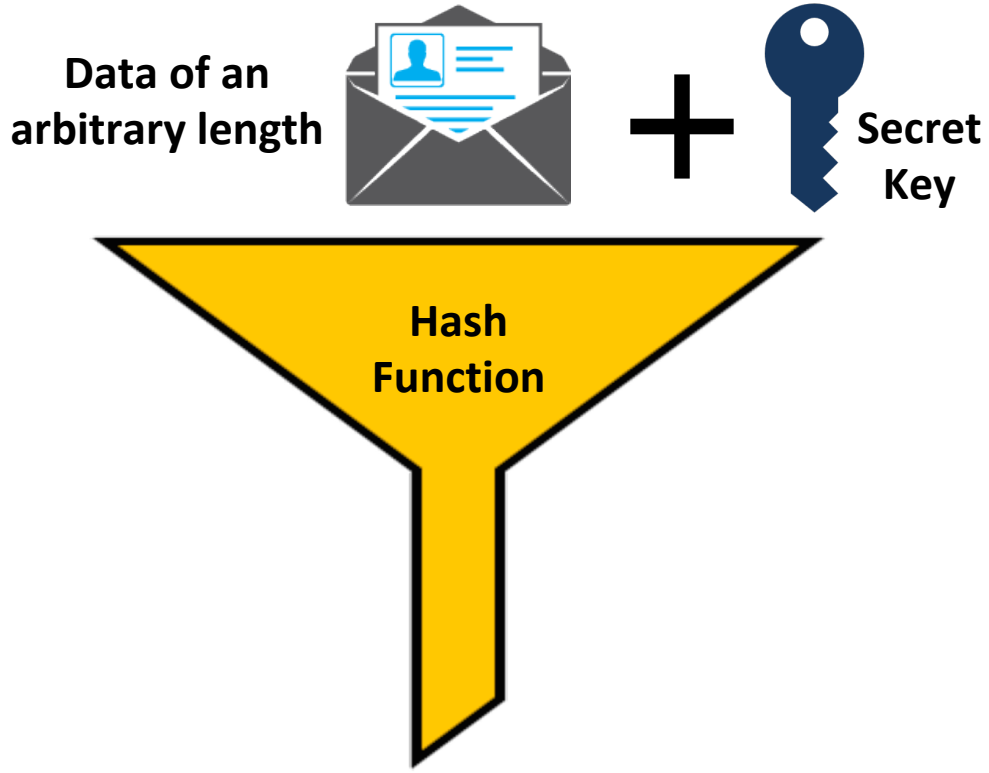
Data of an arbitrary length



Fixed-length Hash (fingerprint)

2@#D67Yc9p01Qz$gBj&kP

Hashed MAC for Integrity



Encryption

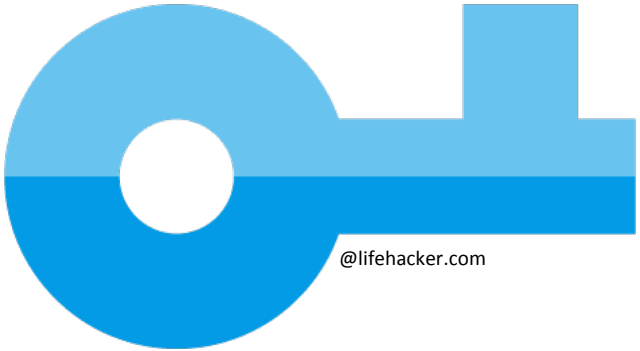
- Encryption hides the original data or message content by scrambling the clear text into a random appearing string of characters called ciphertext
- Decryption reverses the process of encryption when an entity has the proper decryption key
- Many applications store and send information in clear text
- Two ways to implement encryption:
  - Link encryption
  - Packet payload encryption

Symmetric Key Systems

- Symmetric key cryptosystems use the same key to encrypt and decrypt data
- Also called secret-key or private-key encryption
- Sender and receiver must share the same secret key before achieving secure communication so protecting this key is tantamount
- Often used to protect bulk data, data in storage, and with Virtual Private Networks
- Key management can be a challenge

Symmetric Key Systems

- They work fast and are often used for bulk encryption when data privacy is needed using 40 to 256-bit keys (1.5×10^{77} possible keys)
- Common algorithms:
  - DES (obsolete)
  - RC4 (obsolete)
  - 3DES-EDE
  - AES-CBC-128/256
  - AES-GCM-128/256



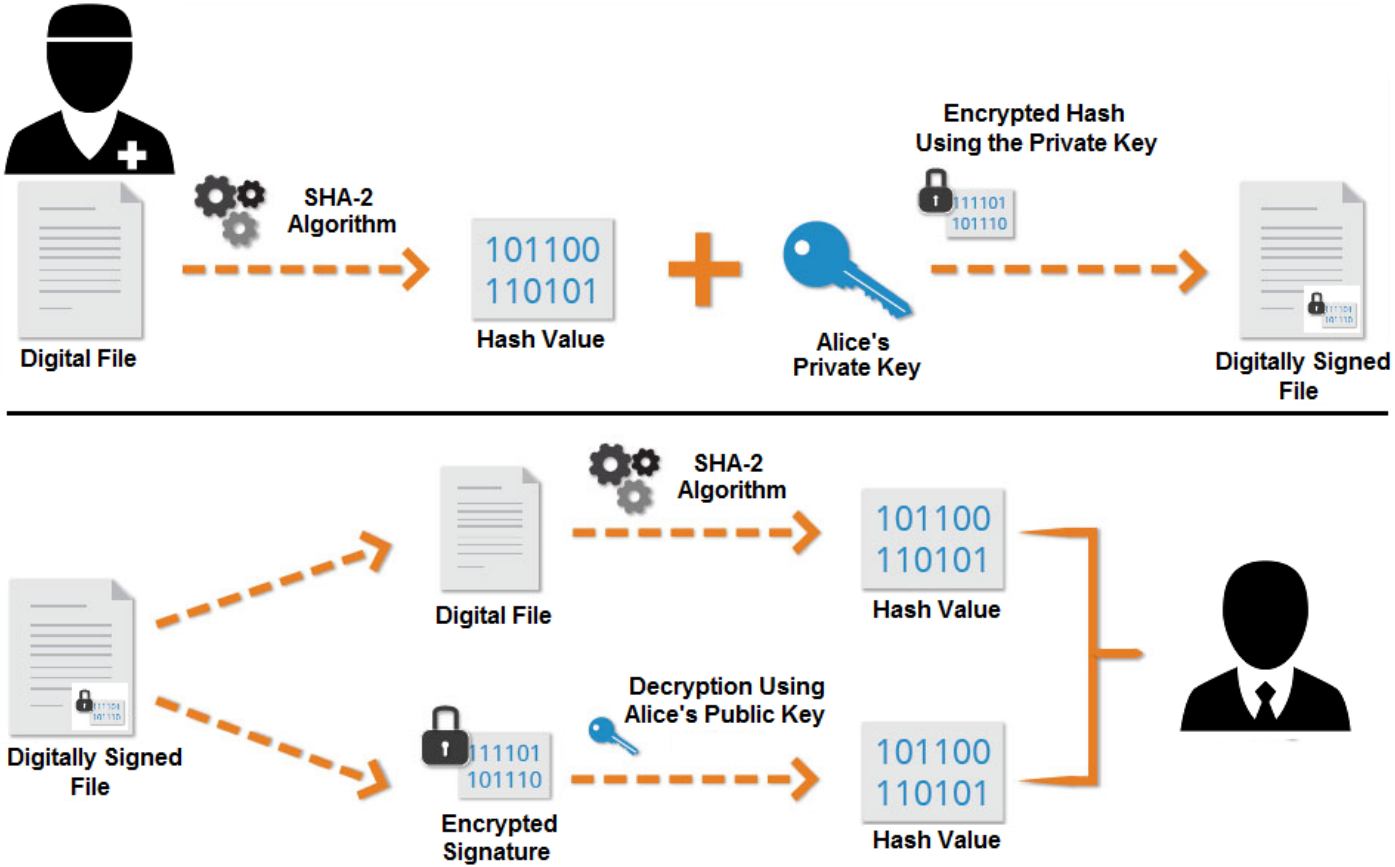
Asymmetric Key Systems

- The system uses a pair of mathematically related keys.
- Entities generate the key pair and share the public key while keeping the private key secret.
- Data that is encrypted with the private key requires the public key to decrypt and vice versa.
- Asymmetric encryption is also known as public key encryption.
- Common asymmetric protocols are RSA, DSA, ElGamal, Diffie-Hellman, ECDH (elliptic curve) and EC-DSA.

Digital Signatures

- Digital signatures offer service similar to handwritten signatures but over the Internet
- Uses hashing algorithm to append a fingerprint to the original data or message
- The fingerprint encrypted with the sender's (signer) private key becomes the digital signature
- The original message/data and signature are sent together to the recipient

Digital Signatures



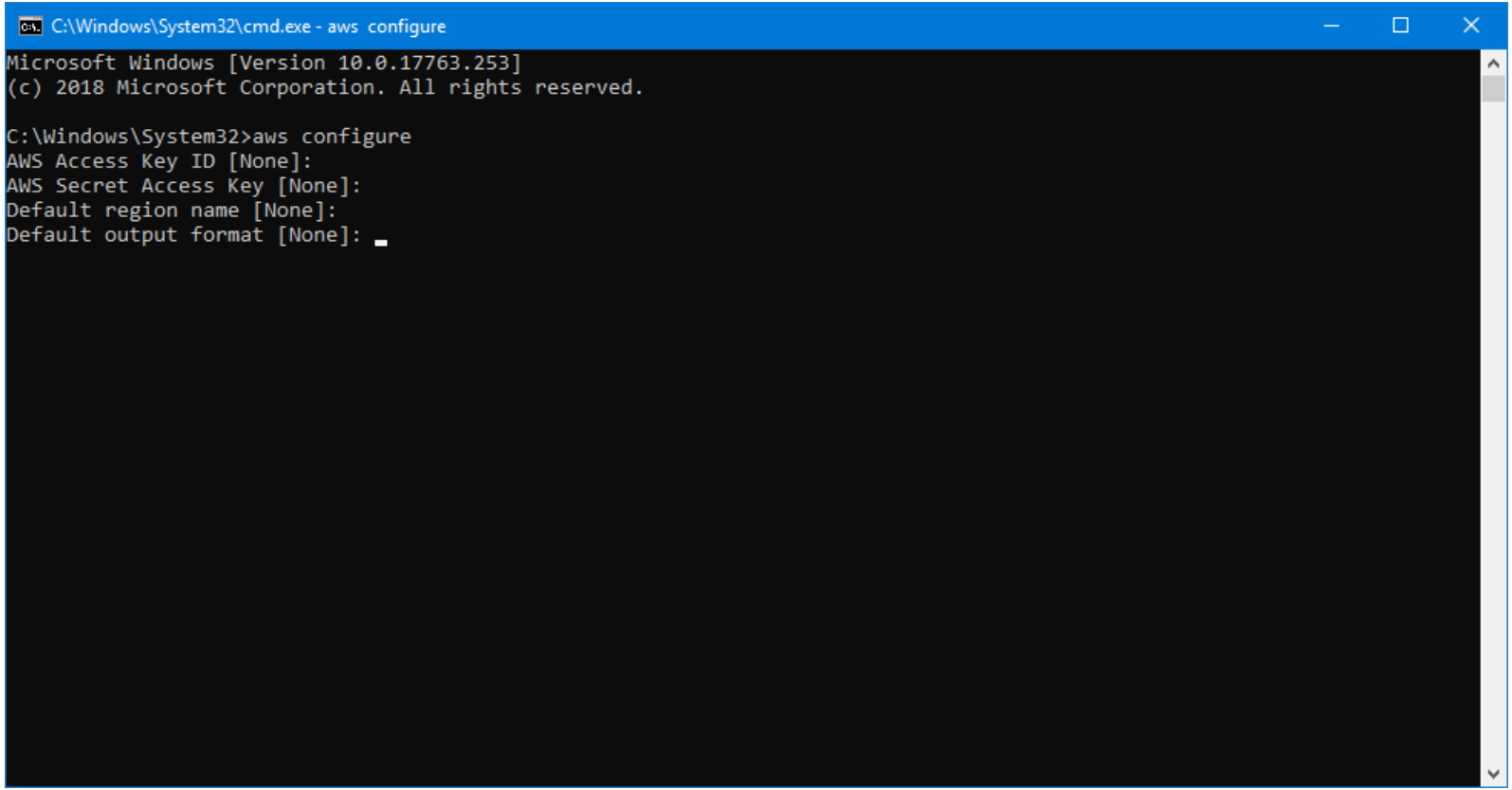
Protecting Cloud Data in Transit

- The **AWS Management Console** uses SSL/TLS between the client browser and console service endpoints to protect AWS service management traffic
- Traffic is encrypted, data integrity is authenticated, and the client browser authenticates the identity of the console service endpoint by using an X.509v3 certificate
- After an SSL/TLS session is established between the client browser and the console service endpoint, all subsequent HTTP traffic is protected within the SSL/TLS session

Protecting Cloud Data in Transit

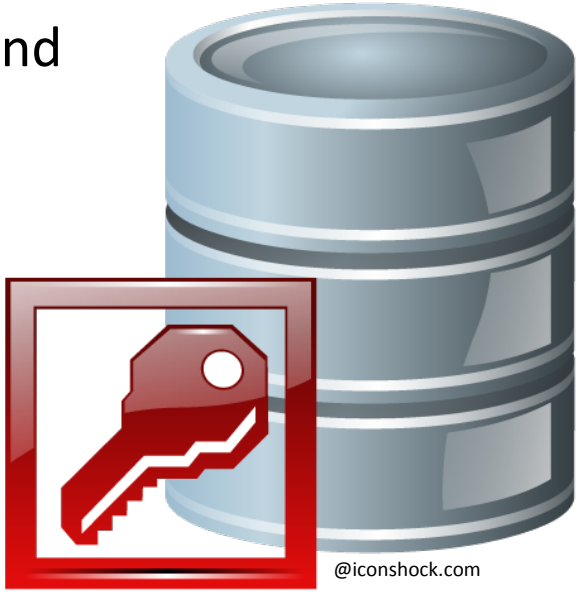
- You can also use APIs to manage cloud services
  - Directly from applications
  - Third-party tools
  - Via SDKs
  - Via AWS command line tools
- APIs are RESTful web services over HTTPS
  - SSL/TLS sessions are established between the client and the specific AWS service endpoint
  - All subsequent traffic, including the REST envelope and user payload, is protected in the SSL/TLS session

AWS Command Line Interface

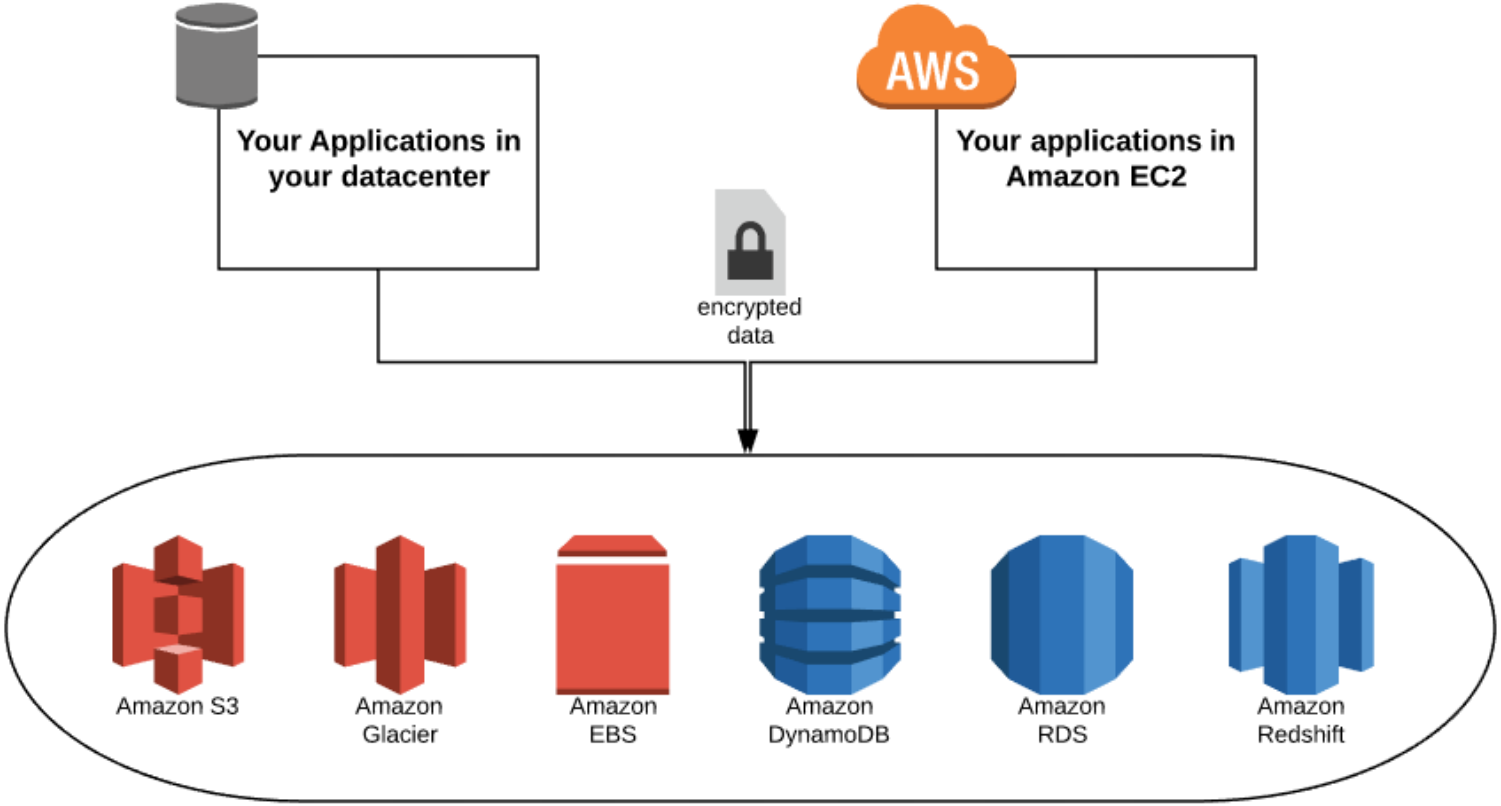


Encryption and Key Management in AWS

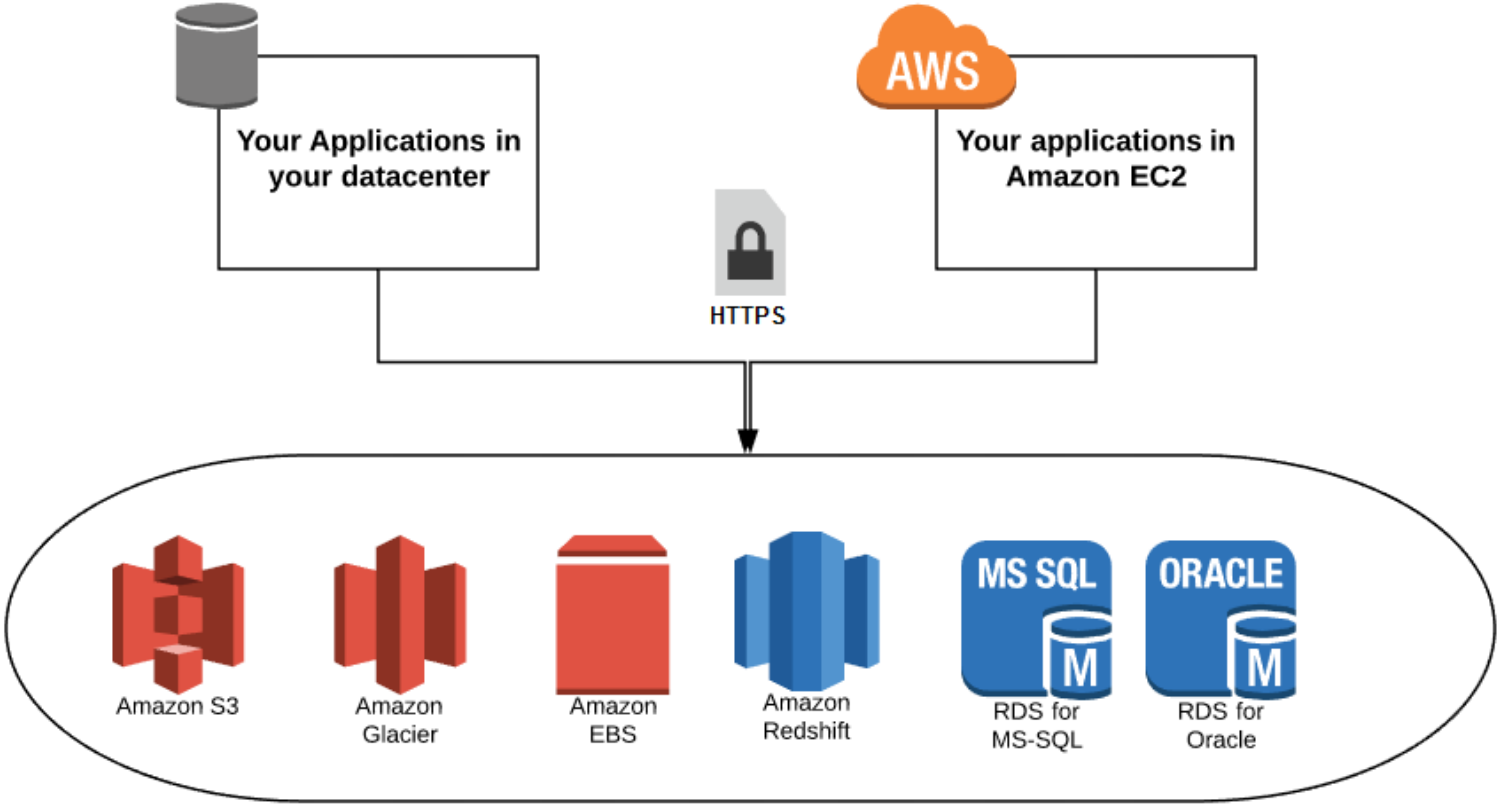
- Client-side encryption: You encrypt your data and manage your own keys
- Server-side encryption: AWS encrypts data and manages the keys for you
- Key Management
  - On your own
  - AWS Management Key Service (KMS)
  - AWS Partner Solutions (Sophos, Trend, etc.)
  - AWS Cloud HSM



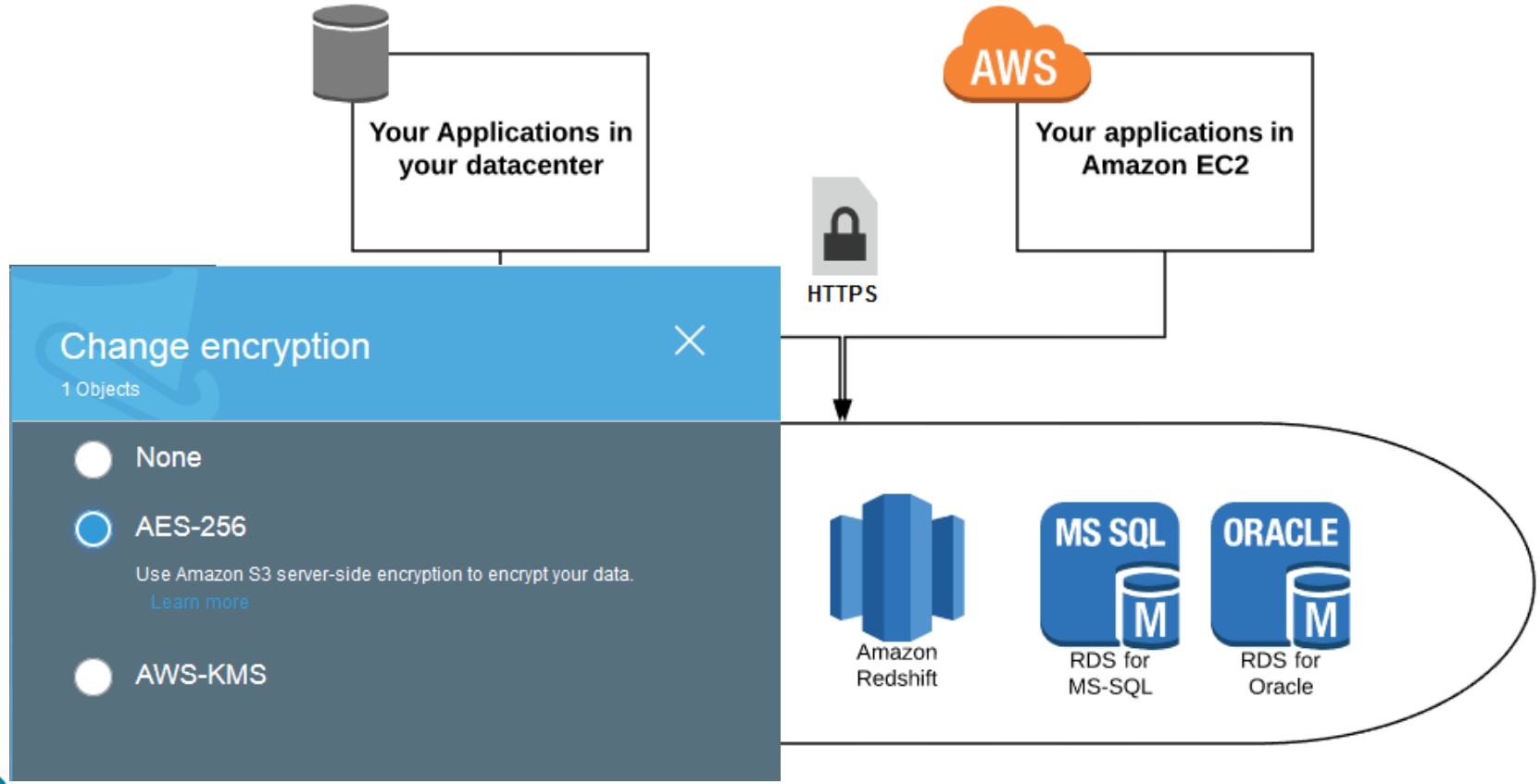
Client-side Encryption



Server-side Encryption



Server-side Encryption

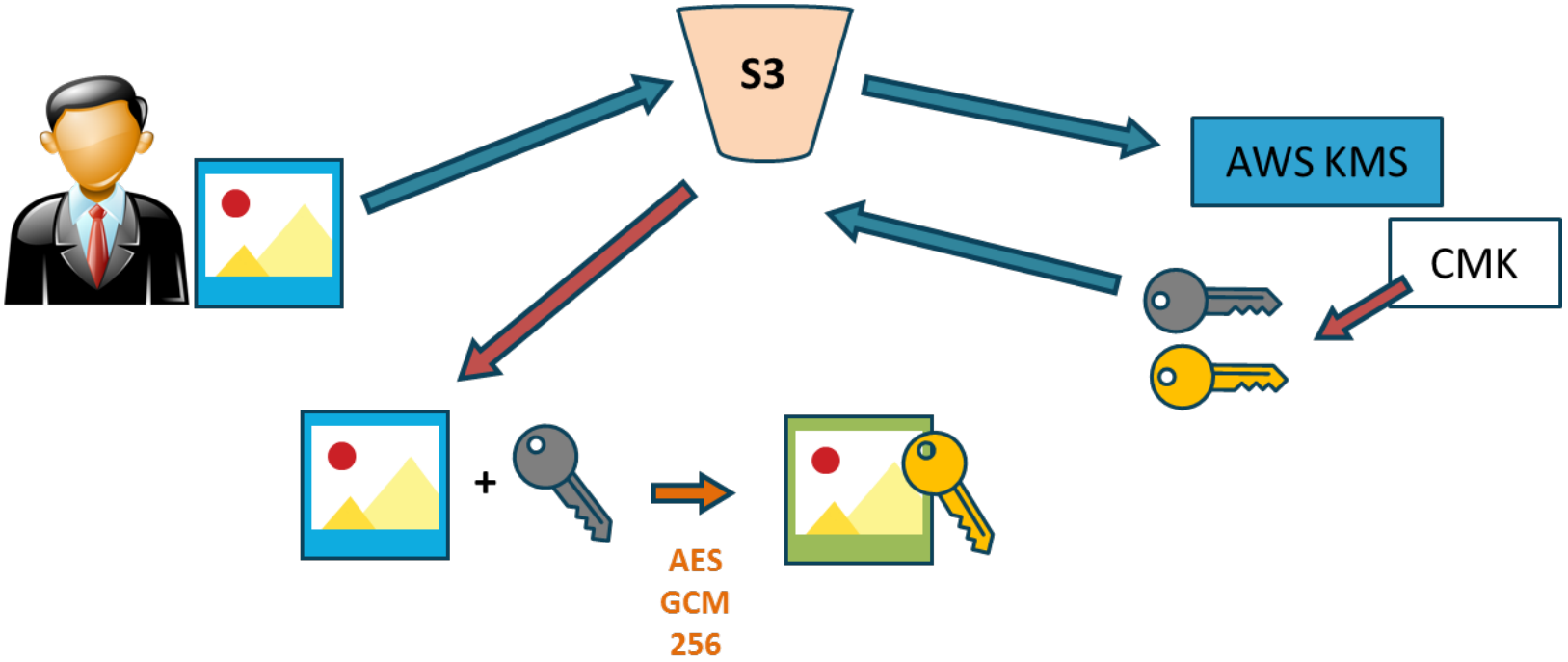


AWS Key Management Service (KMS)

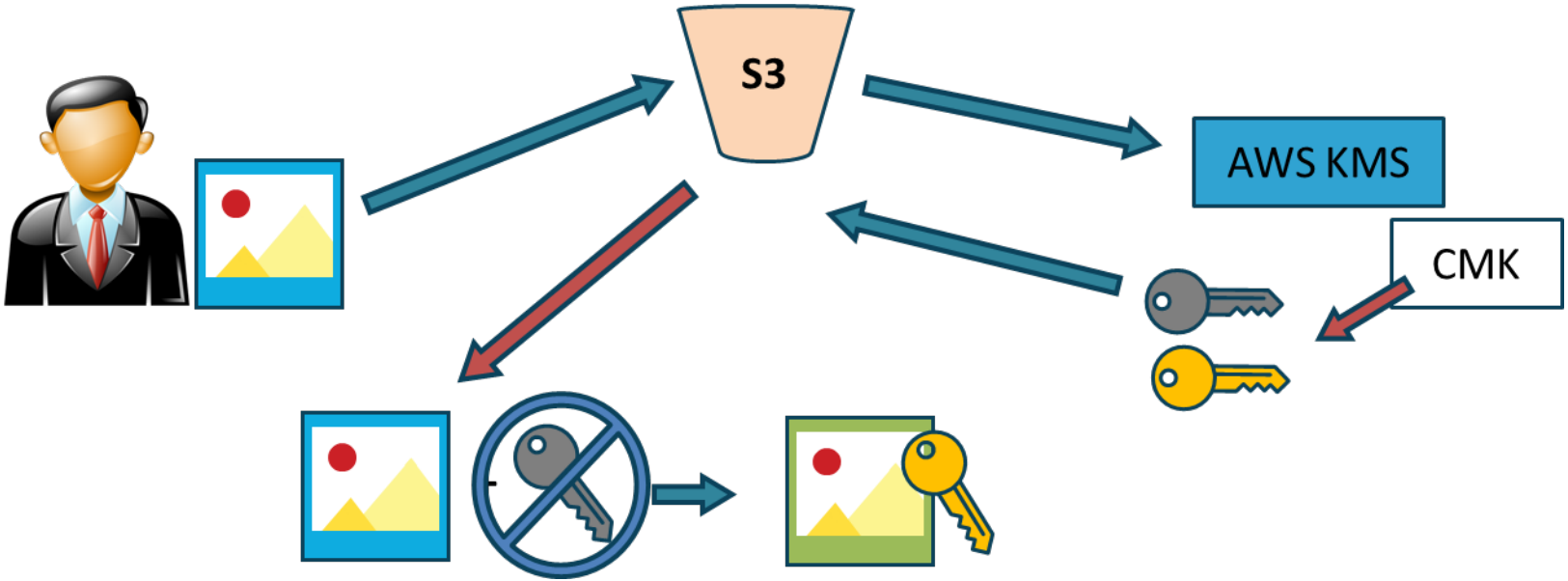
- Customer Master Keys (CMKs) are the main resource of the KMS service
- You can use a CMK to encrypt and decrypt up to 4 KB (4096 bytes) of data
- Typically, you use CMKs to generate, encrypt, and decrypt the data keys that you use outside of AWS KMS to encrypt your data
- There are three types of CMKs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

AWS Key Management Service (KMS)

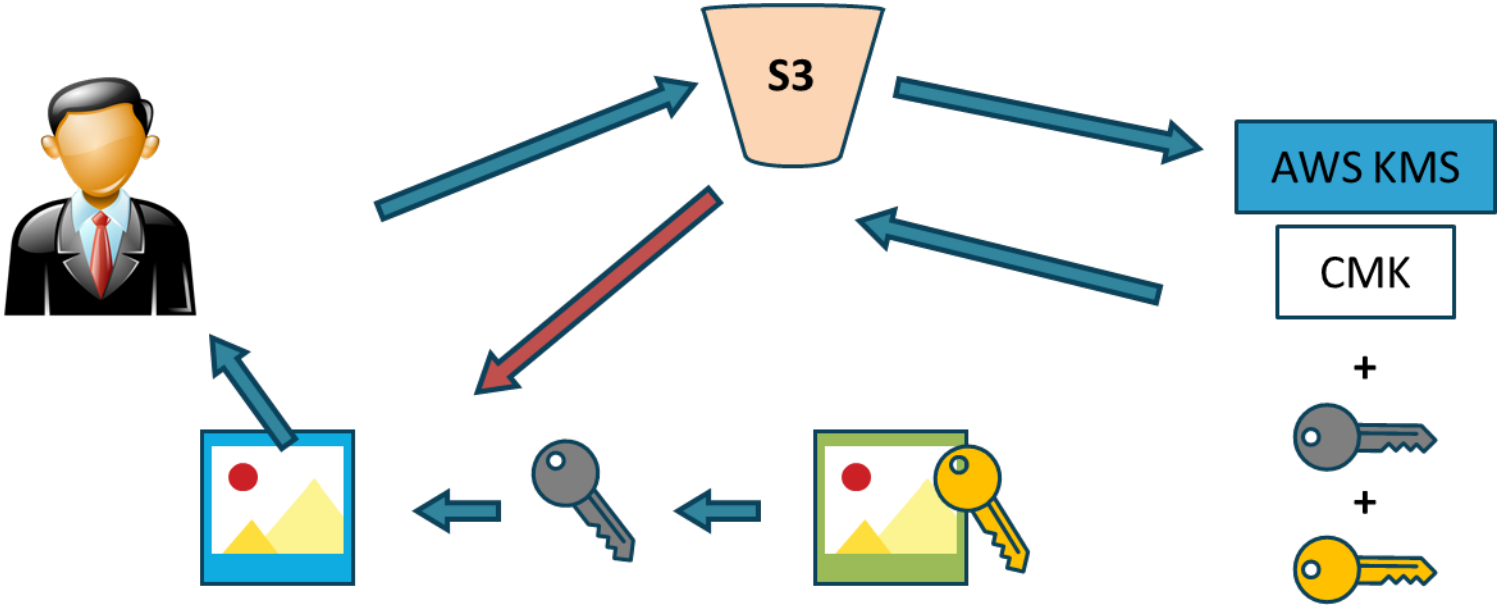
AWS Key Management Service (KMS)



AWS Key Management Service (KMS)



AWS Key Management Service (KMS)



AWS EBS Encryption

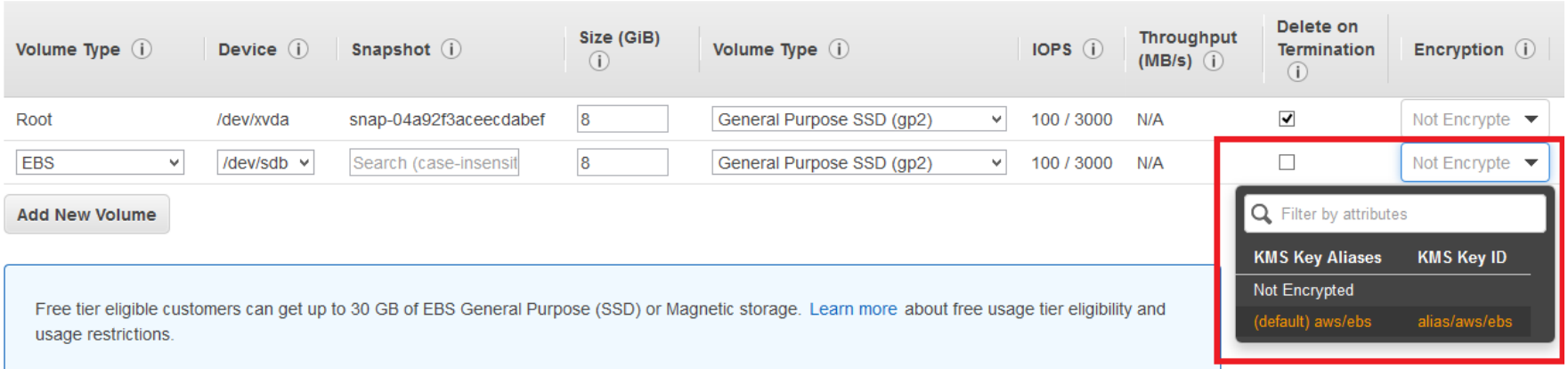
- When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:
  - Data at rest inside the volume
  - All data moving between the volume and the instance
  - All snapshots created from the volume
  - All volumes created from those snapshots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

@iconshock.com

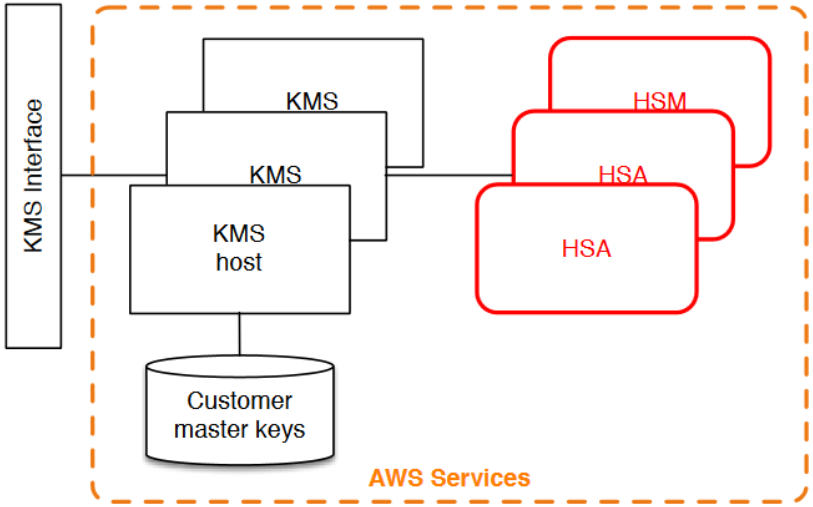
AWS EBS Encryption

- 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

AWS EBS Encryption



AWS Hardware Security Module (HSM)

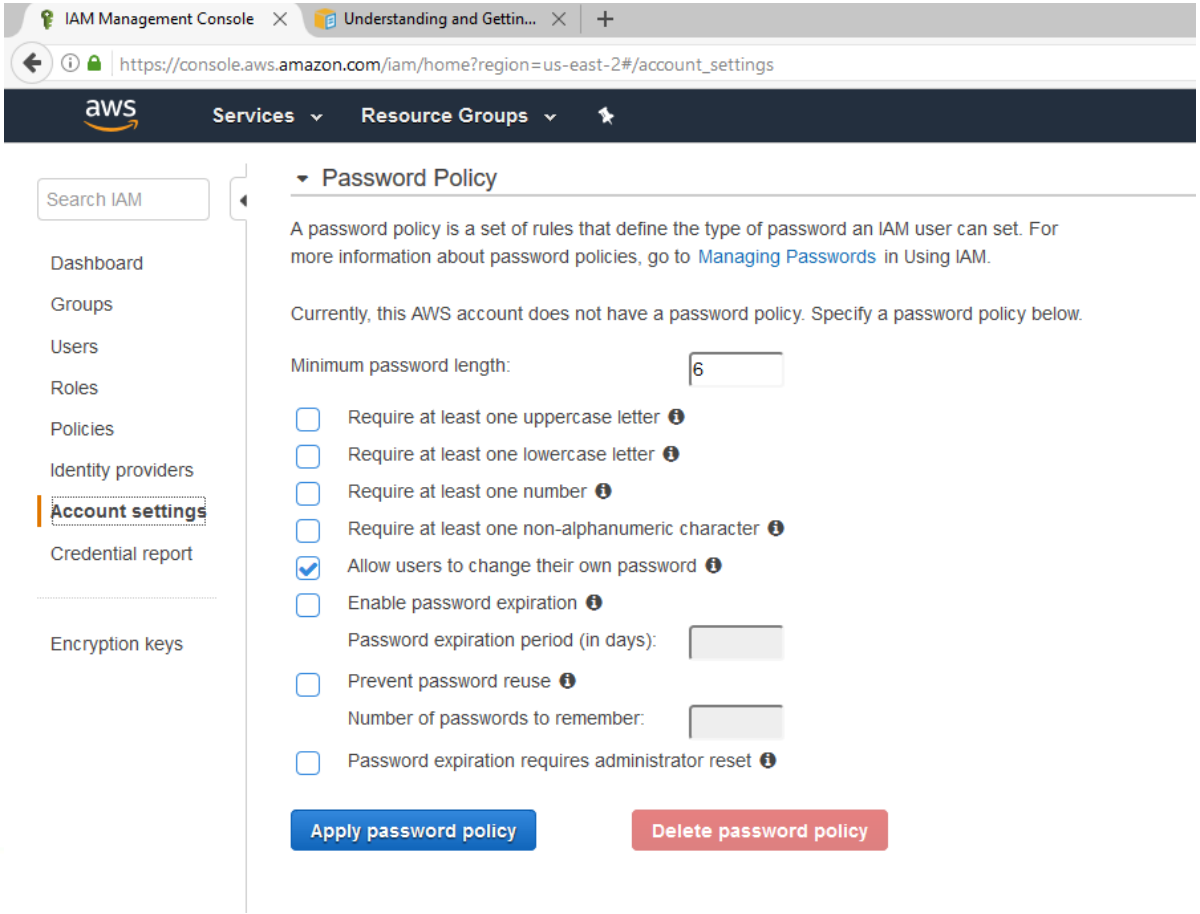


- Generate and use encryption keys on highly secure HSMs
- FIPS 140-2 Level 3 compliant
- Offload the SSL processing for web servers
- Protect private keys for CA
- Enable Transparent Data Encryption (TDE) for Oracle databases

Identity and Access Management (IAM)

- A user can be any individual, system, or application that interacts with cloud resources, either programmatically or through the a management Console or CLI
- Use your account root user email address and password to sign in to the management console
- Create IAM Groups, Users, and Roles starting with a full Administrative Group/User to avoid signing in with root
- Immediately implement multifactor authentication (MFA) hardware and/or software (TOTP) solutions

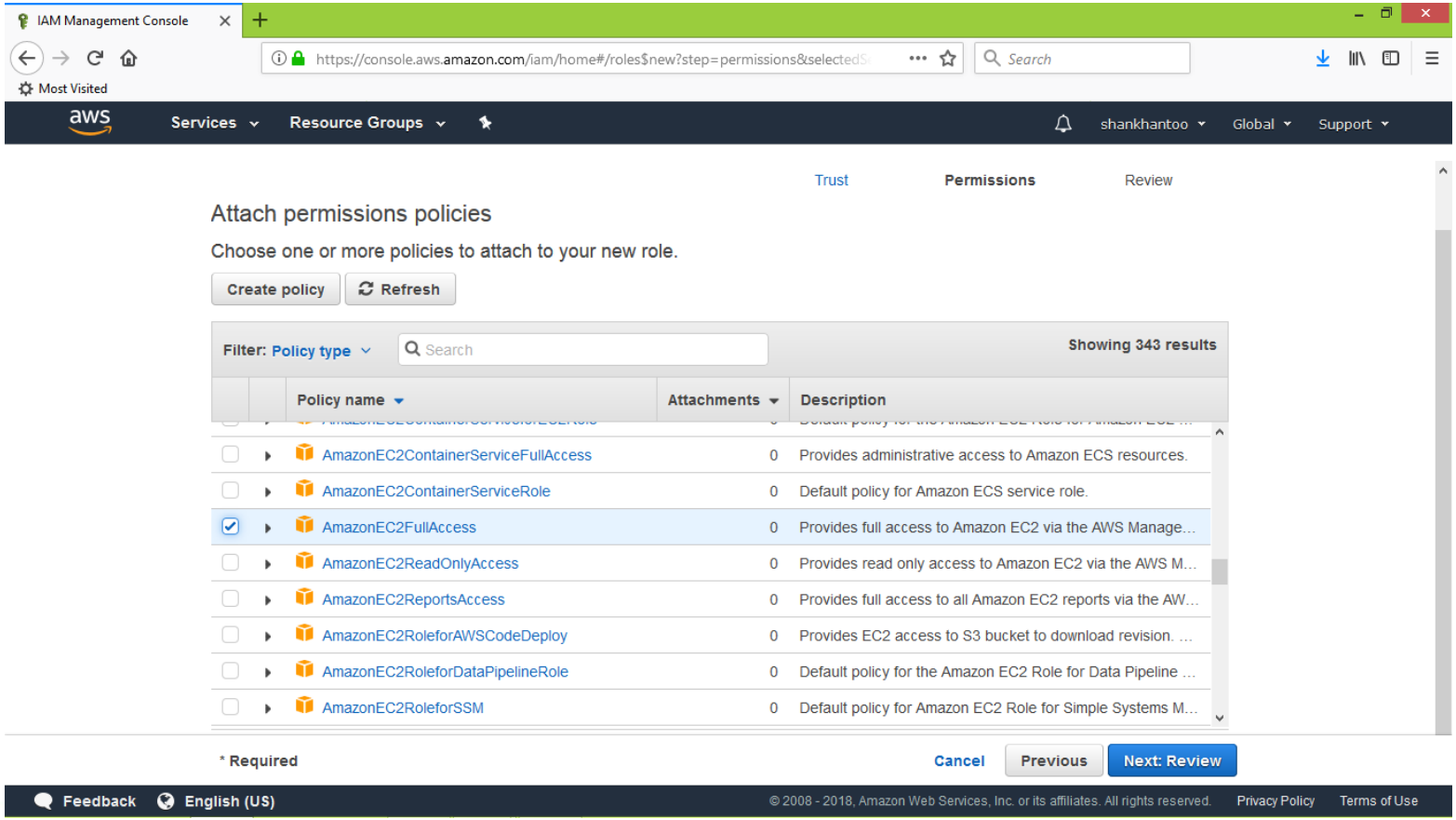
IAM Password Policies



Managed Policies

- A standalone policy that is created and administered by AWS
- Makes it easier to assign suitable permissions to users, groups, and roles without manual configuration
- Job function policies align closely to commonly used job duties in the IT industry
- You can still create standalone “customer managed” policies
- It is recommended to begin by copying an existing AWS managed policy and then making changes

Managed Policies

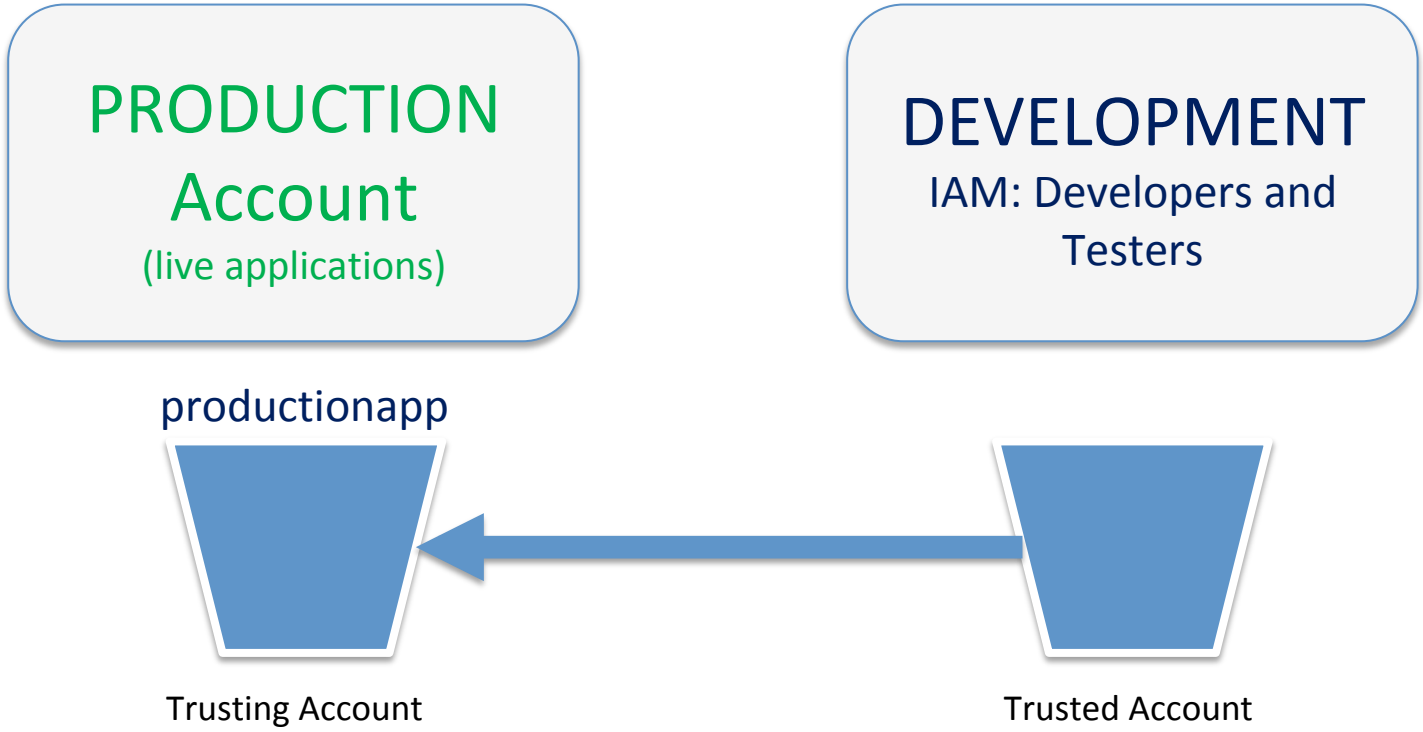


IAM Roles

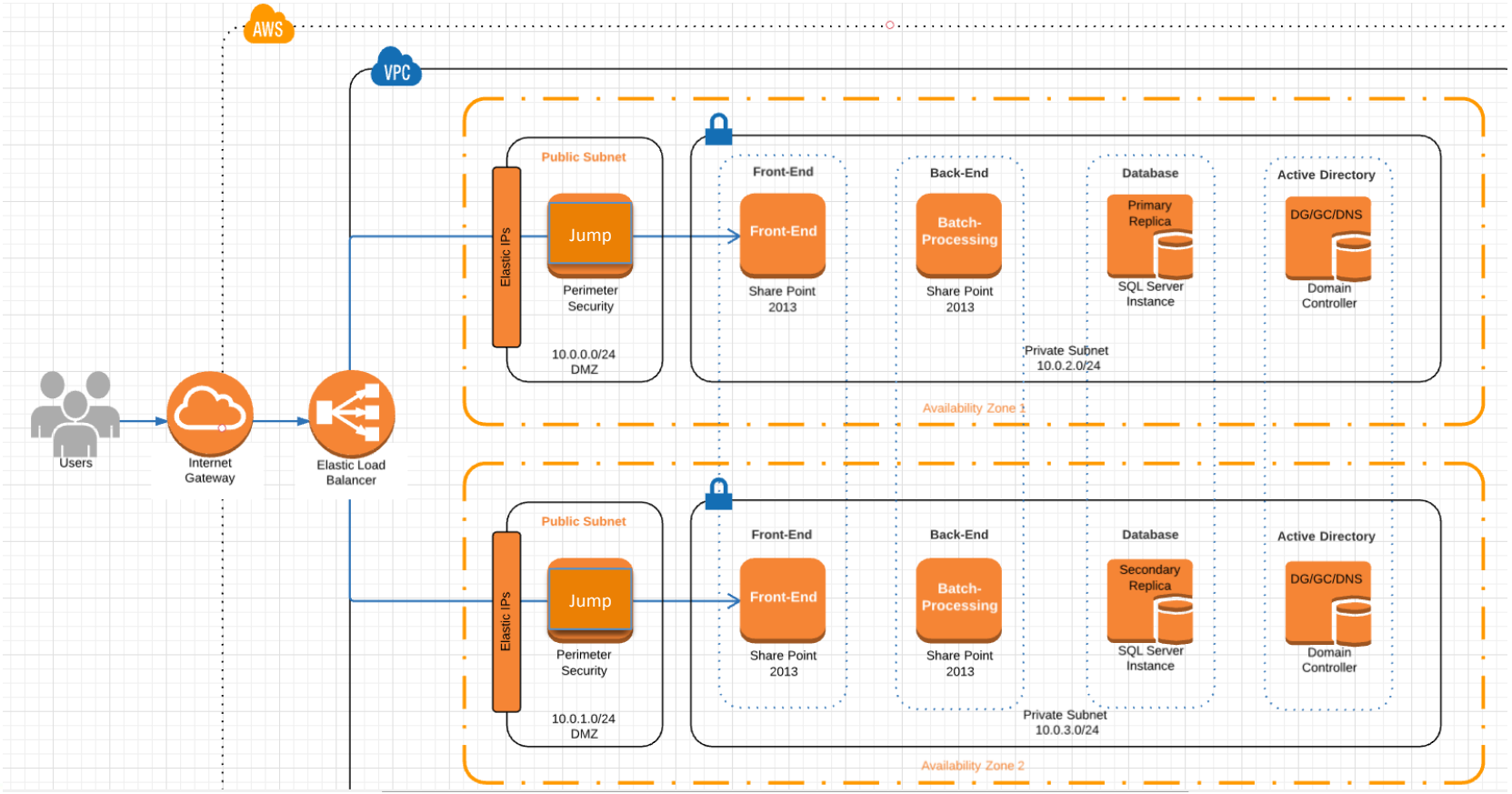
- An AWS IAM entity that has a set of permissions that can be assumed by another entity
- Use roles to allow applications running on your Amazon EC2 instances to securely access your AWS resources
- You can share resources in one account with users in a different account
- If you deploy large fleets of elastically scaling EC2 instances, IAM roles can provide a more secure and convenient way to manage the distribution of access keys

PRODUCTION
Account
(live applications)

DEVELOPMENT
Account
(application sandbox)



Demo: Assigning a Role to a Bastion



Assigning a Role to GCP Stackdriver

Monitor AWS accounts (optional)

Add AWS accounts to monitor as part of this Workspace. You can edit this selection later in workspace settings. Learn more

Authorize AWS for Stackdriver

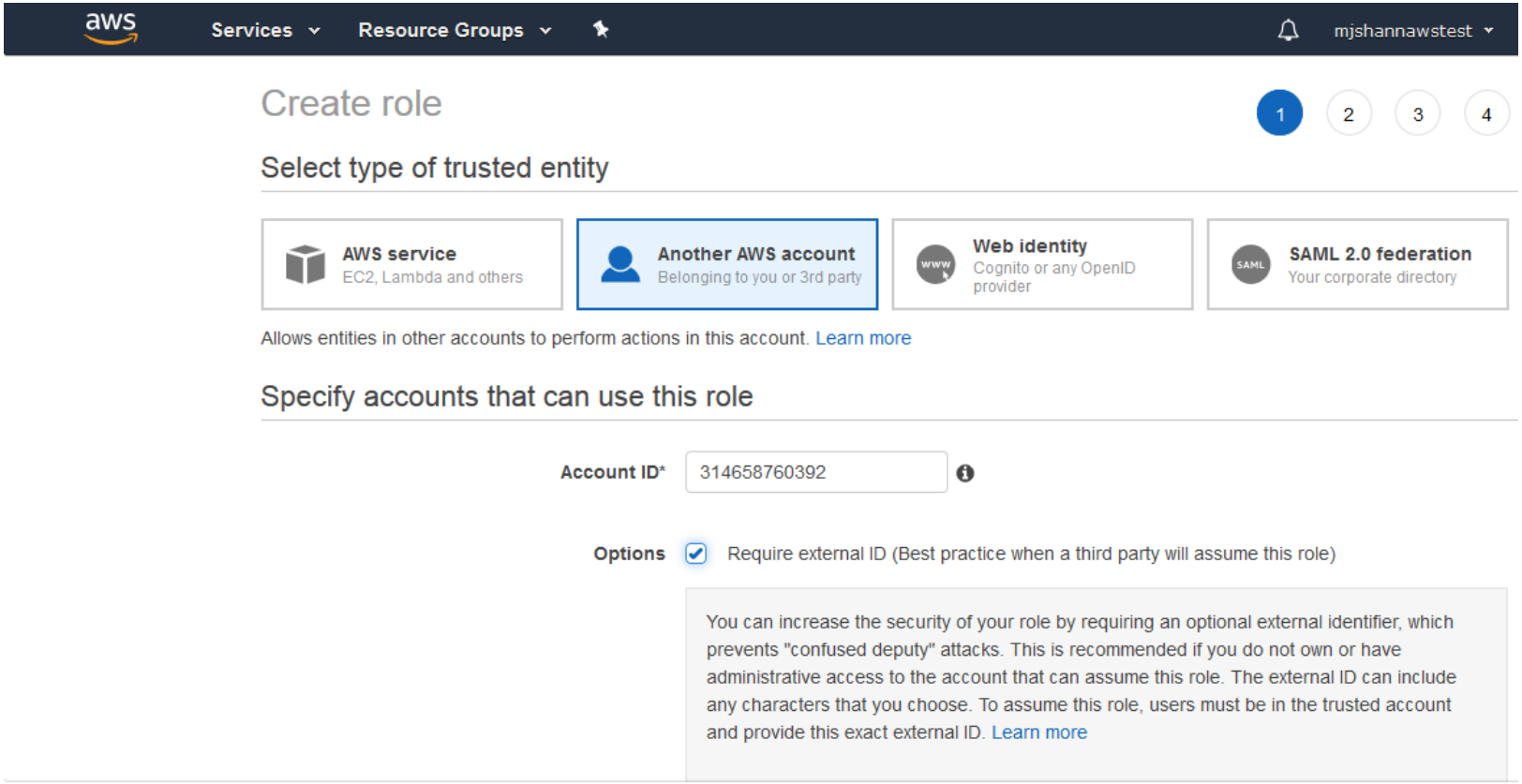
1. Log in to your Amazon IAM console and click Roles.
2. Click "Create New Role"
3. Select the role type "Another AWS account"
4. Check the box "Require external ID"
5. Enter the following:

   Account ID **314658760392**

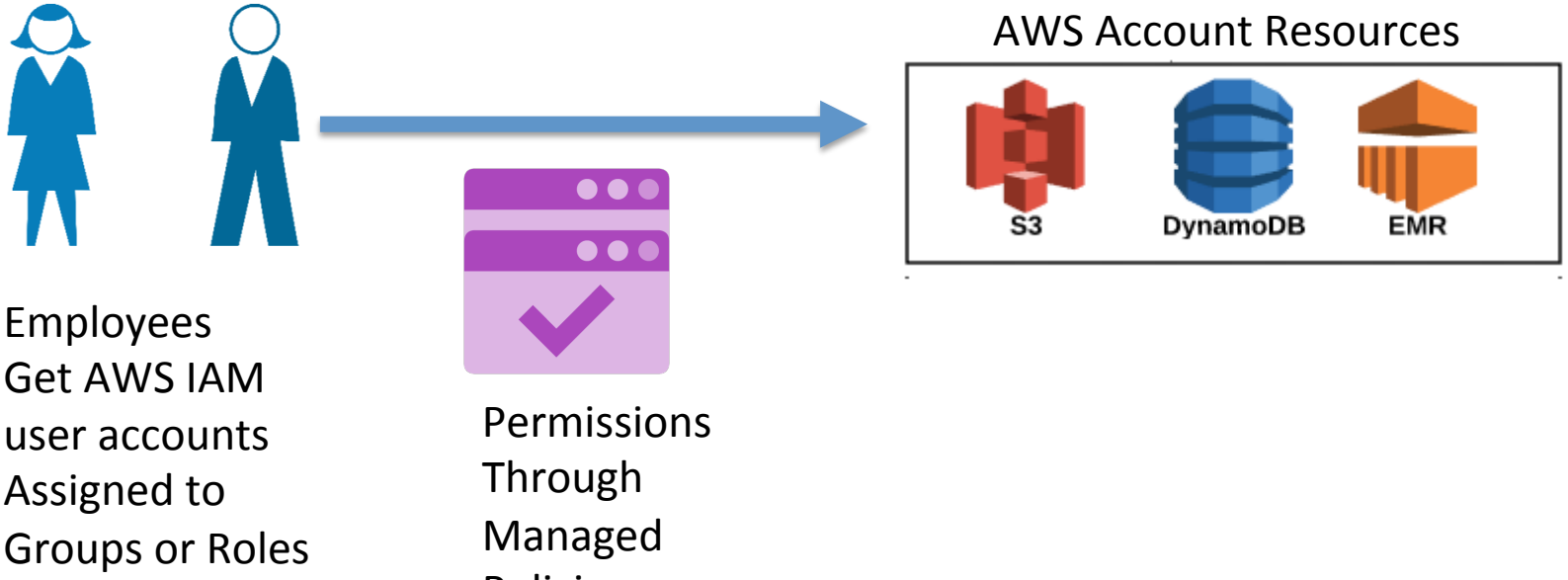
   External ID **sd6644334**

   Require MFA **unchecked**
6. Click "Next: Permissions"
7. Select "ReadOnlyAccess" from the policy template list and click "Next: Review".
8. Enter a "Role Name" such as **Stackdriver** and click "Create Role"
9. Select the "Role Name" you just entered from the role list to see the summary page.
10. Copy the "Role ARN" value and paste it in the AWS Role ARN field below.

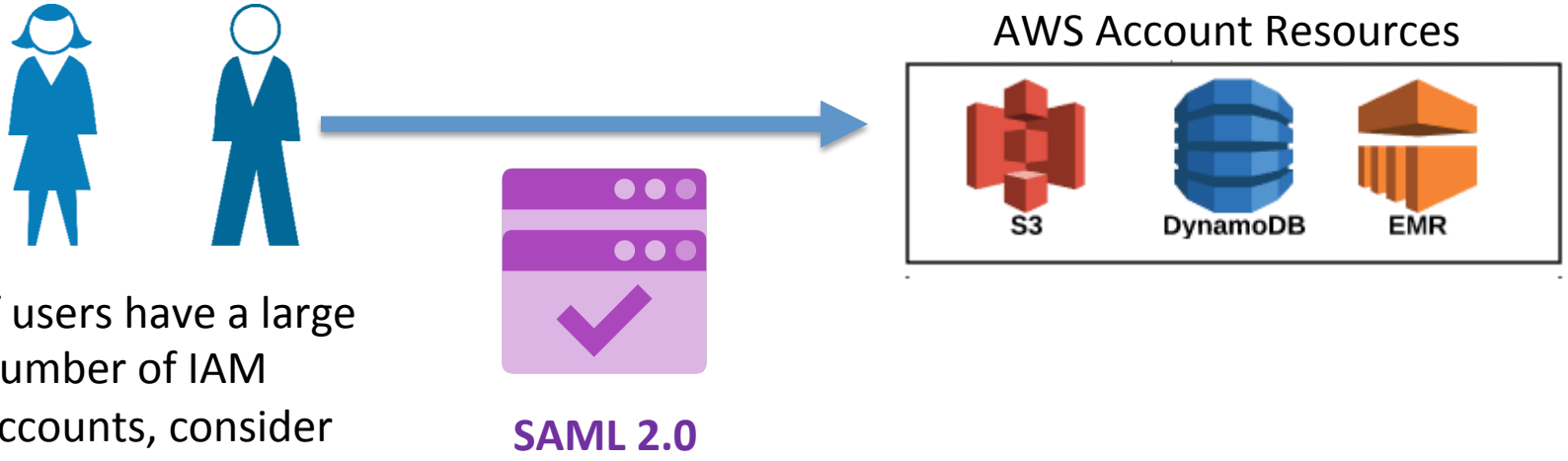
Assigning a Role to GCP Stackdriver



Default Access to AWS Resources



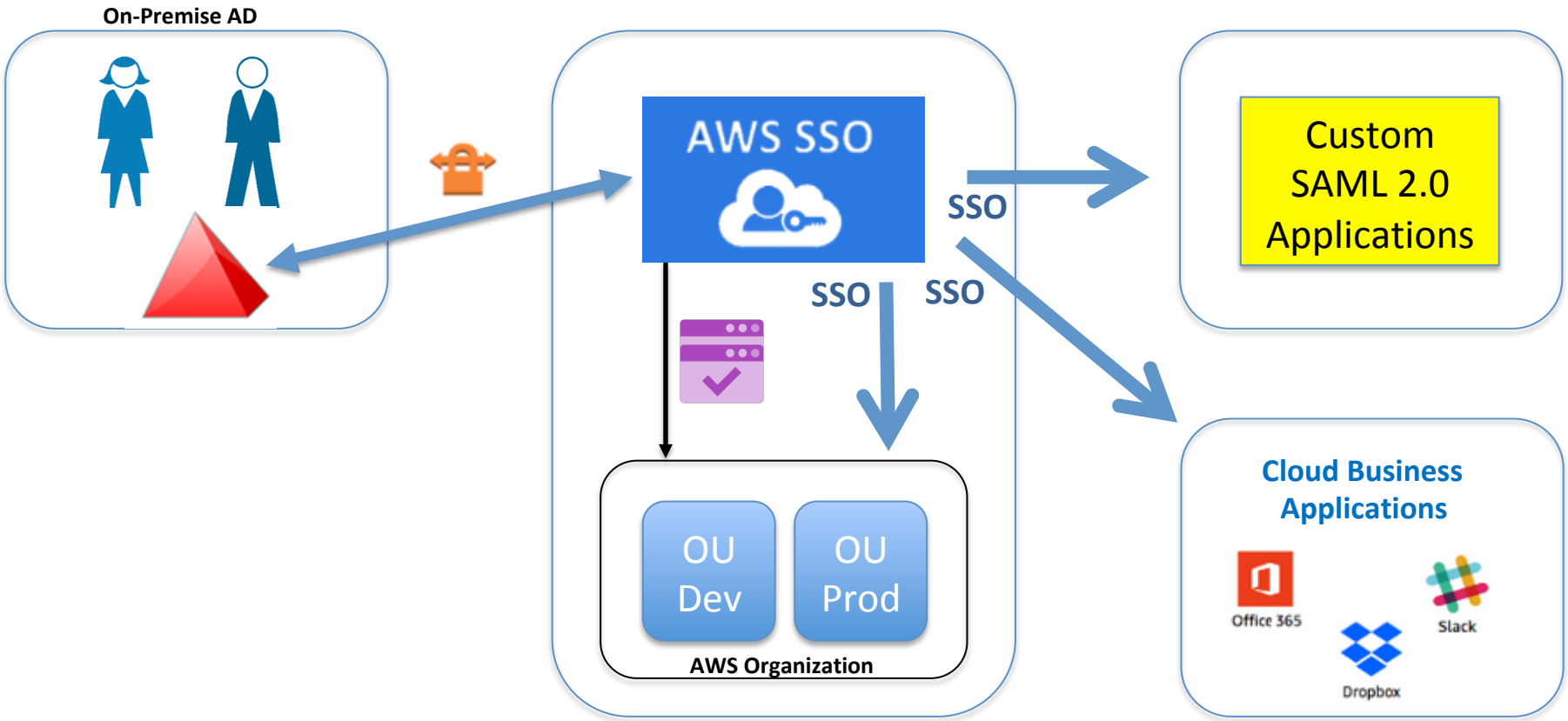
Single-Sign-On Access to AWS



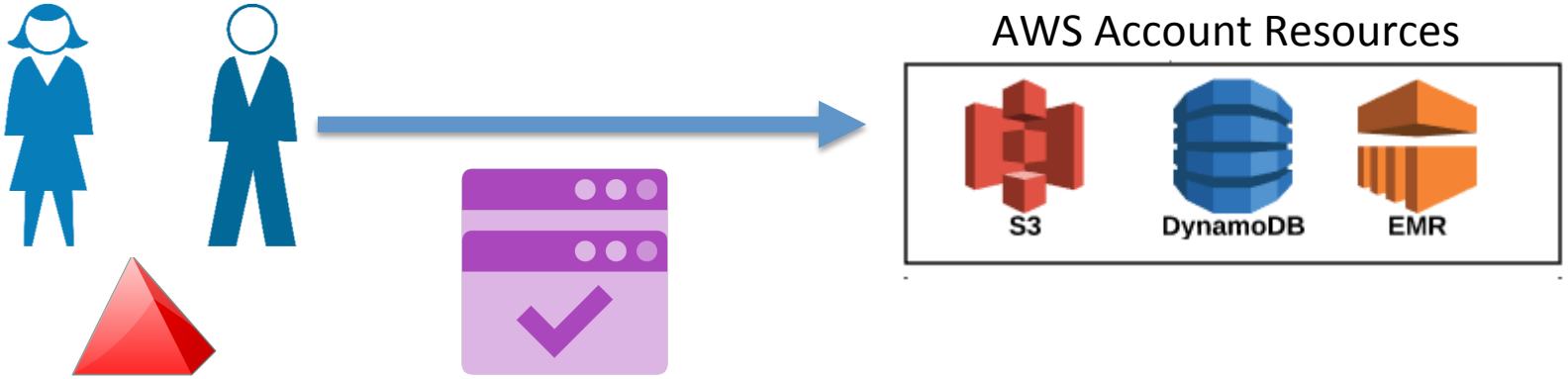
If users have a large number of IAM accounts, consider SAML 2.0 federation to enable single sign-on (SSO)

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

AWS Single Sign-On (SSO)



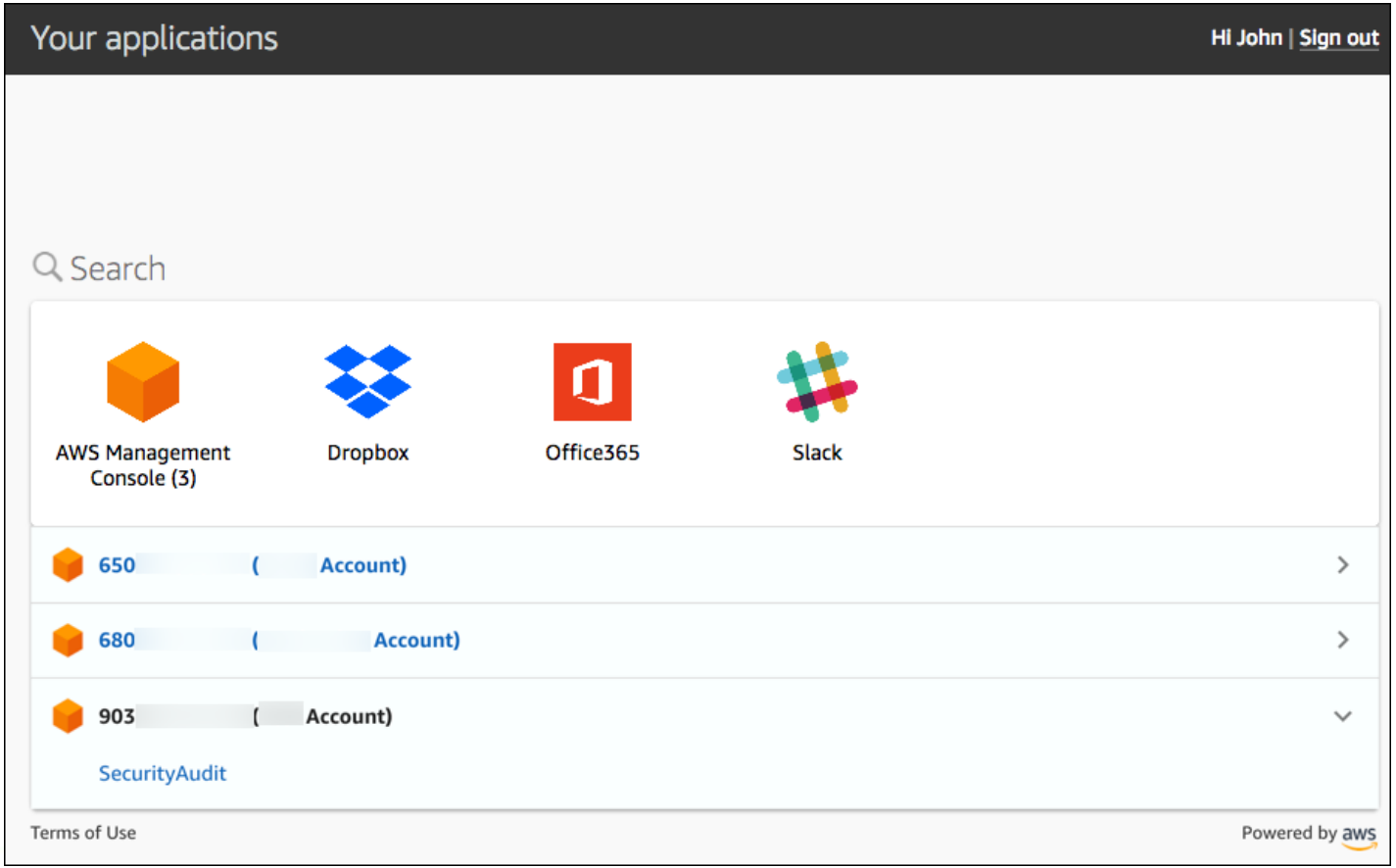
Single-Sign-On Access to AWS



Corporate Microsoft Active Directory

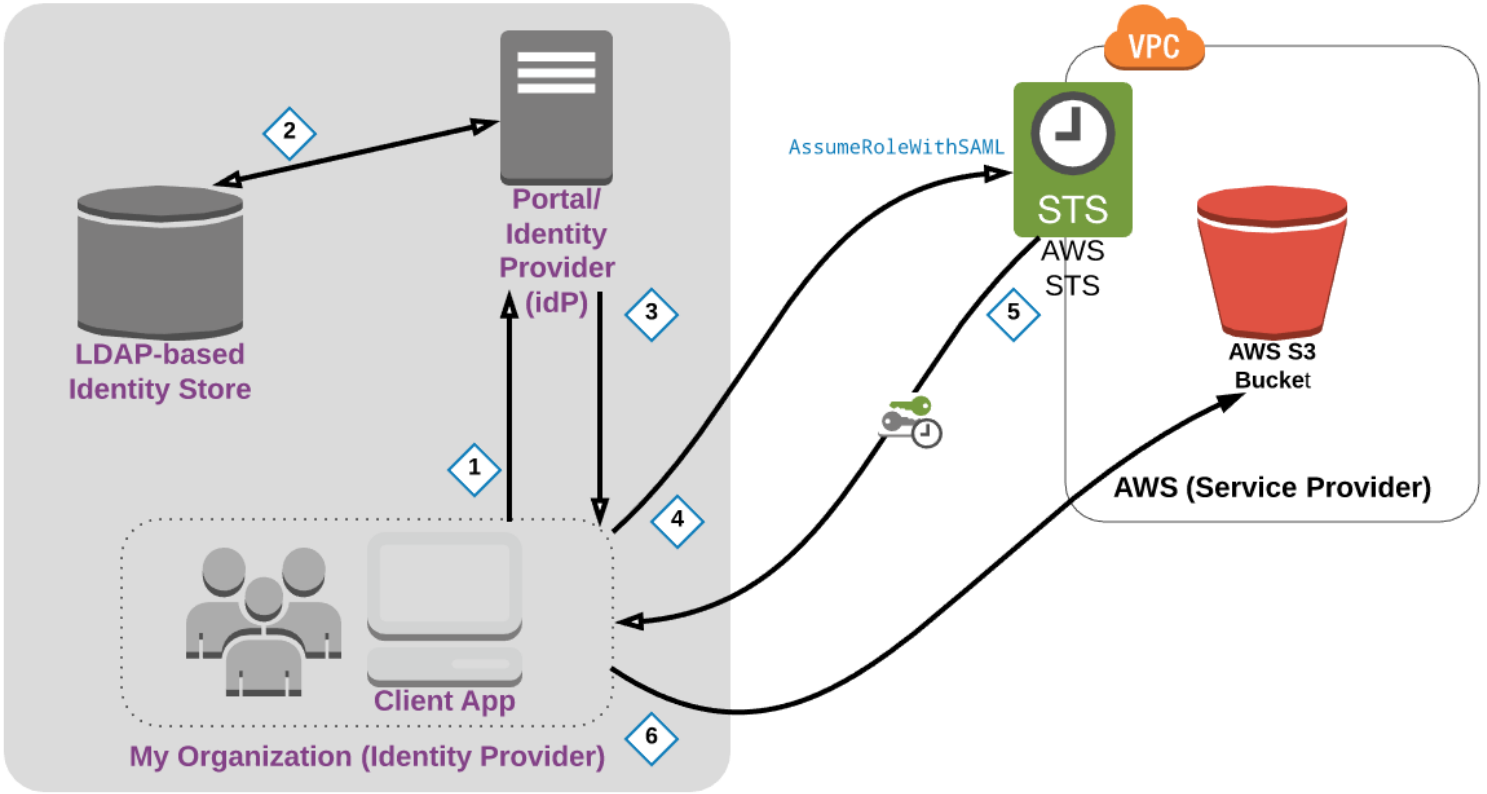
AWS SSO also integrates with Microsoft Active Directory (AD) through AWS Directory Service

AWS SSO Access to Resources

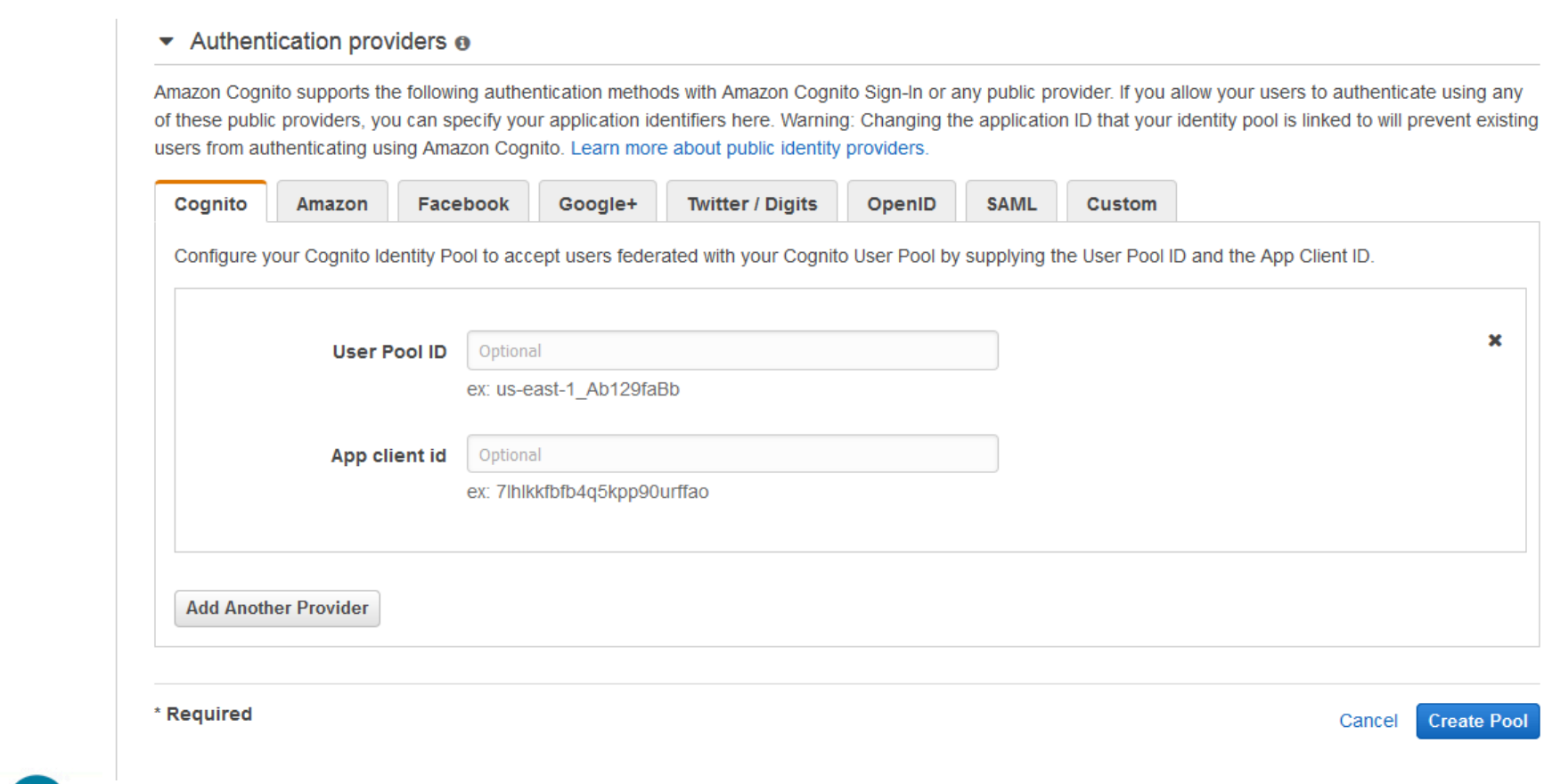


Pearson

Amazon Cognito



AWS Cognito

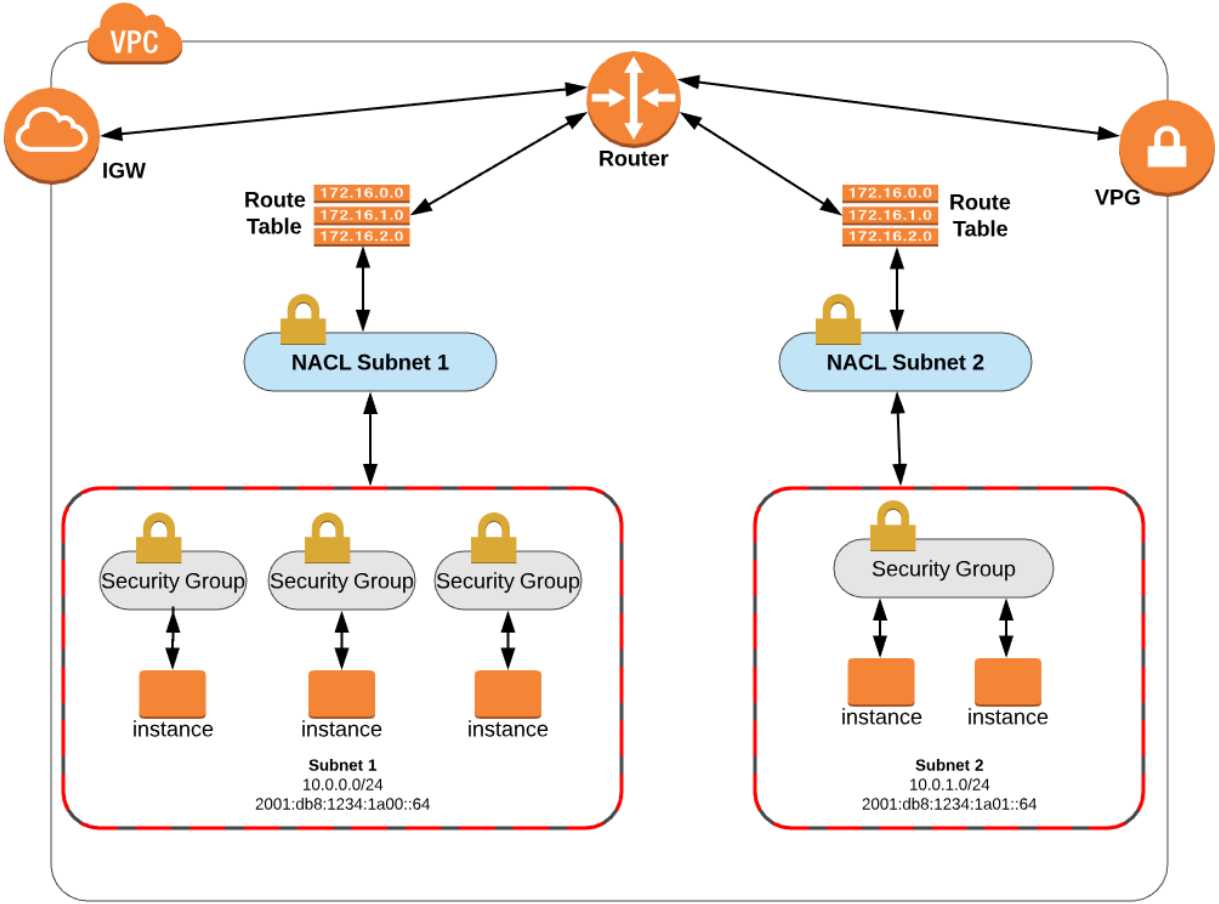


Segment 3: Infrastructure Security

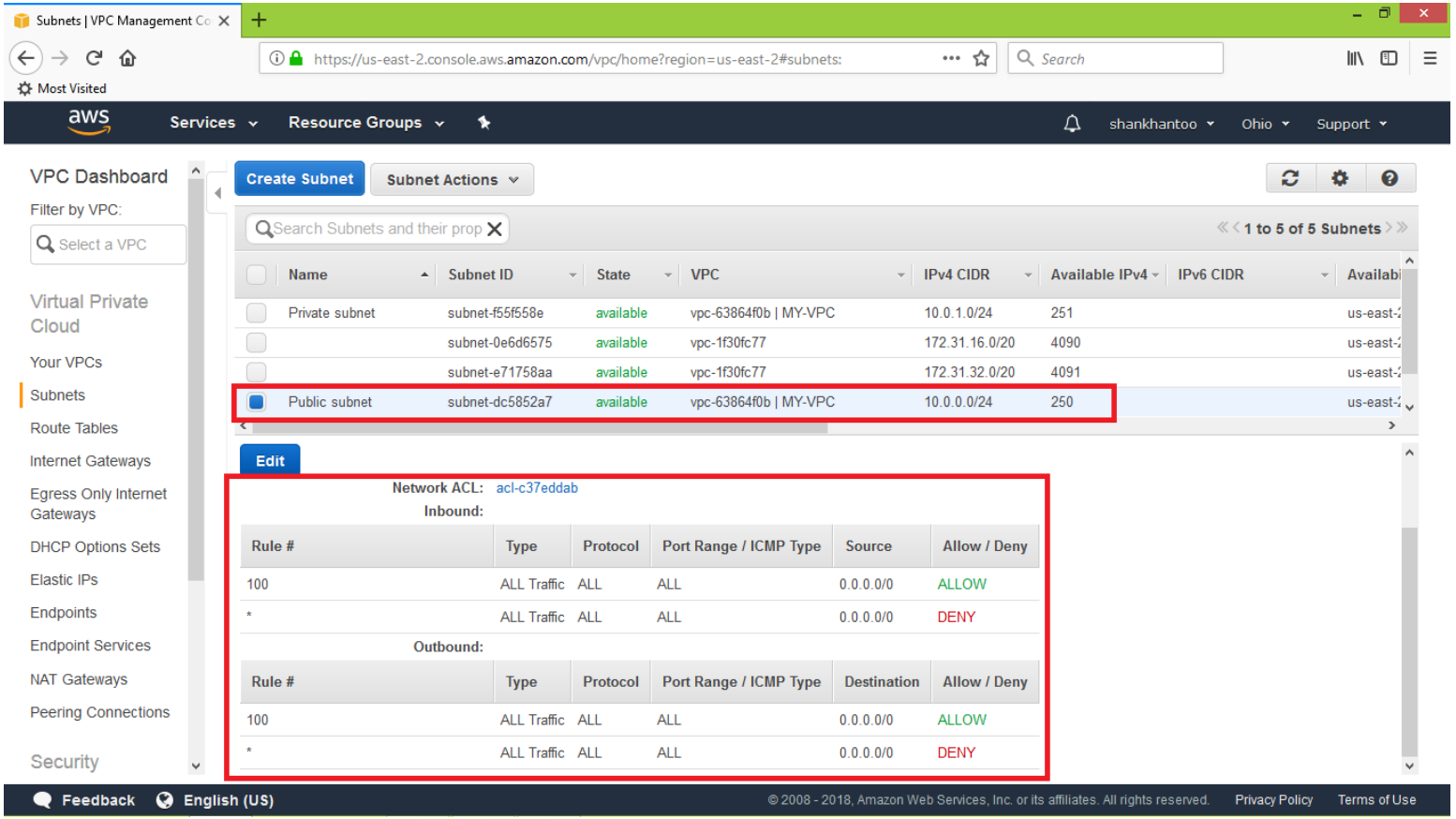
Network ACLs

- NACLs allow stateless traffic filtering and management of IPv4 and IPv6 traffic
- Applies to all inbound OR outbound traffic from a subnet within a VPC
- Can contain ordered rules (ACE's) to permit or deny based on IP protocol (for example GRE, IPSec ESP, ICMP), service port, and source/destination IP address
- NACLs are agnostic of TCP and UDP sessions
- NACLs work in conjunction with security groups and can permit or deny traffic before it reaches the security group

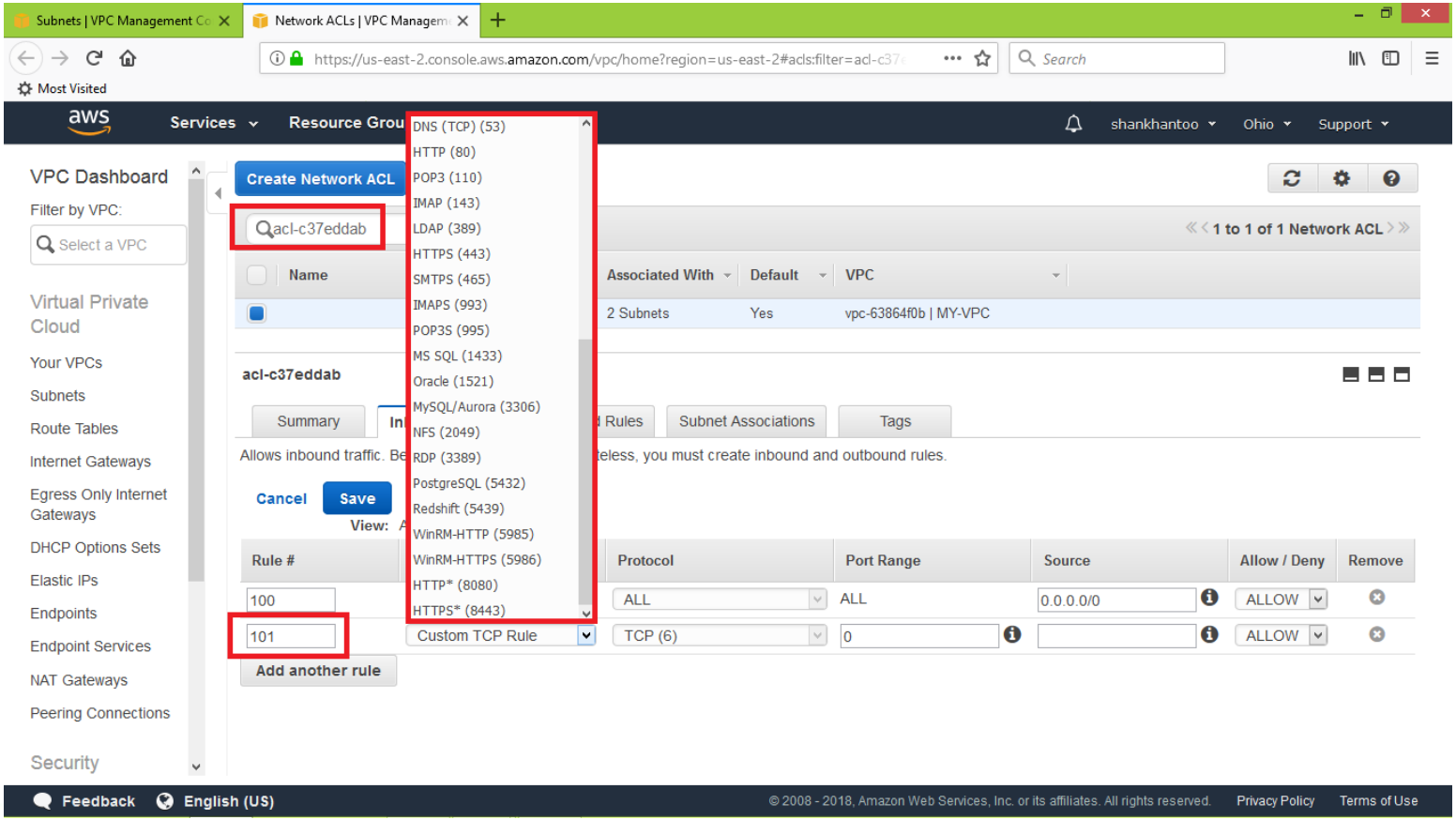
NACLs and Security Groups



NACLs


Subnets | VPC Management Co
https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#subnets:
Search
Most Visited
aws
Services
Resource Groups
shankhantoo
Ohio
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Create Subnet
Subnet Actions
Search Subnets and their prop
1 to 5 of 5 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Private subnet subnet-f55f558e available vpc-63864f0b | MY-VPC 10.0.1.0/24 251
subnet-0e6d6575 available vpc-1f30fc77 172.31.16.0/20 4090
subnet-e71758aa available vpc-1f30fc77 172.31.32.0/20 4091
Public subnet subnet-dc5852a7 available vpc-63864f0b | MY-VPC 10.0.0.0/24 250
Edit
Network ACL: acl-c37eddab
Inbound:
Rule # Type Protocol Port Range / ICMP Type Source Allow / Deny
100 ALL Traffic ALL ALL 0.0.0.0/0 ALLOW
* ALL Traffic ALL ALL 0.0.0.0/0 DENY
Outbound:
Rule # Type Protocol Port Range / ICMP Type Destination Allow / Deny
100 ALL Traffic ALL ALL 0.0.0.0/0 ALLOW
* ALL Traffic ALL ALL 0.0.0.0/0 DENY
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

NACLs



NACL Recommendations

- AWS Documentation » **Amazon Virtual Private Cloud » User Guide** » Security » Recommended Network ACL Rules for Your VPC

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

ACL Rules for the Public Subnet

Inbound					
Rule #	**Source IP**	**Protocol**	**Port**	**Allow/Deny**	**Comments**
100	0.0.0.0/0	TCP	80	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	0.0.0.0/0	TCP	443	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	Public IP address range of your home network	TCP	22	ALLOW	Allows inbound SSH traffic from your home network (over the Internet gateway).
130	Public IP address range of your home network	TCP	3389	ALLOW	Allows inbound RDP traffic from your home network (over the Internet gateway).
140	0.0.0.0/0	TCP	1024-65535	ALLOW	Allows inbound return traffic from hosts on the Internet that are responding to requests originating in the subnet. This range is an example only. For information about choosing the correct ephemeral ports for your configuration, see Ephemeral Ports.
*	0.0.0.0/0	all	all	DENY	Denies all inbound IPv4 traffic not already handled by a preceding rule (not modifiable).

Security Groups

- A security group is a virtual layer 3/4 **stateful** firewall that controls the (whitelisted only) traffic flow for its associated instances
- SGs operate at the hypervisor level for all EC2 instances and other VPC objects
- All EC2 instances are launched with the default SG unless a user-defined SG is specified when spun up
- An unchanged default SG will **permit** communication between all resources within the security group AND allows all outbound traffic
- All other traffic is implicitly denied

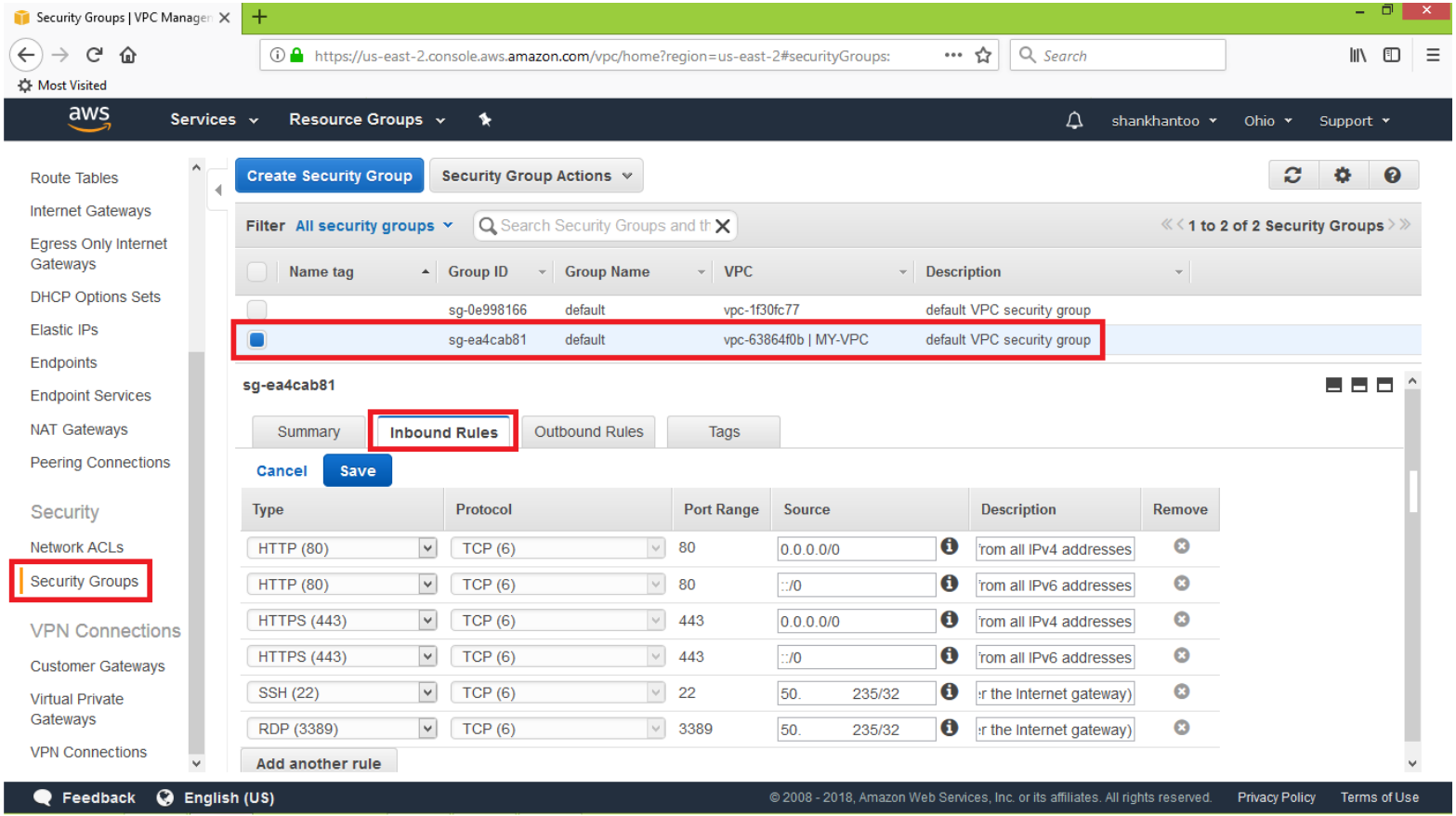
Security Groups

- Security groups are stateful—if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules
- IOW, Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules
- You add the inbound rules to control incoming traffic to the instance and outbound rules to control the outgoing traffic from your instance
- Remember: You can specify allow rules, but not deny rules

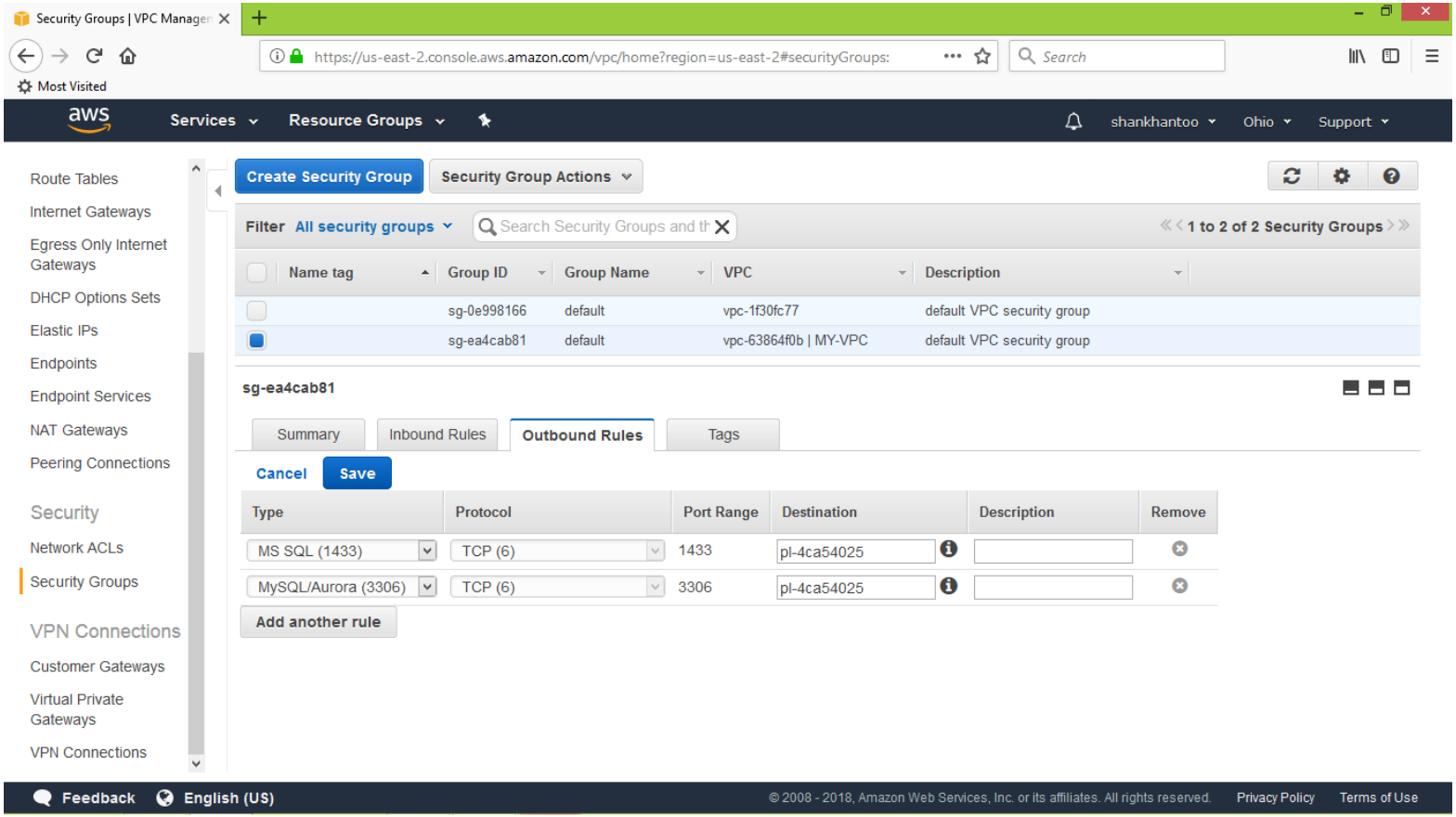
Comparing Security Groups and NACLs

Network ACL	Security Group
Functions at the network level	Functions at the instance level
Supports allow and deny rules	Supports allow rules only (whitelisting)
Stateless so return traffic must be explicitly allowed	Stateful so that return traffic is automatically allowed
Rules are processed in a numbered order	All rules are evaluated before deciding to allow traffic
Applies automatically to all of the instances in the associated subnet	Applies to the instance only

Inbound Rules to Web Servers



Outbound Rules to Web Servers



AWS Web Application Firewall (WAF)

- AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests forwarded to Amazon CloudFront or an ELB Application Load Balancer

- At a basic level WAF can:
  - 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 (monitor mode before deployment)

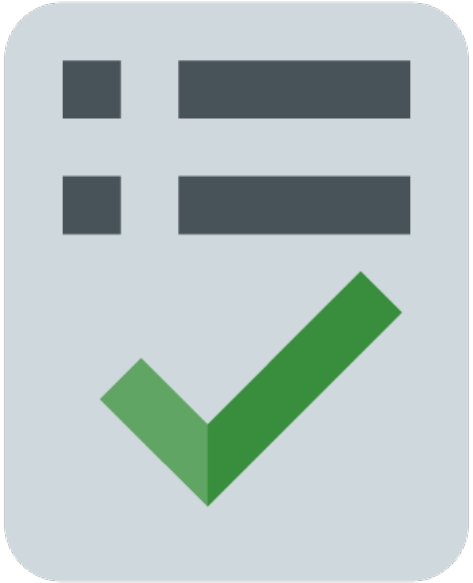
WAF Matching Attributes

- IP addresses of originating requests
- Country that requests originate from
- Values in request headers
  (e.g. User-Agent, Content-Type)
- Literal or regex string patterns that appear in requests (e.g. [cC][mM][dD].[eE][xX][eE])
- Length of requests (buffer overflows)
- Presence of SQL injection code that is likely to be malicious
- Presence of a malicious cross-site scripting attack

@iconshock.com

Web ACLs

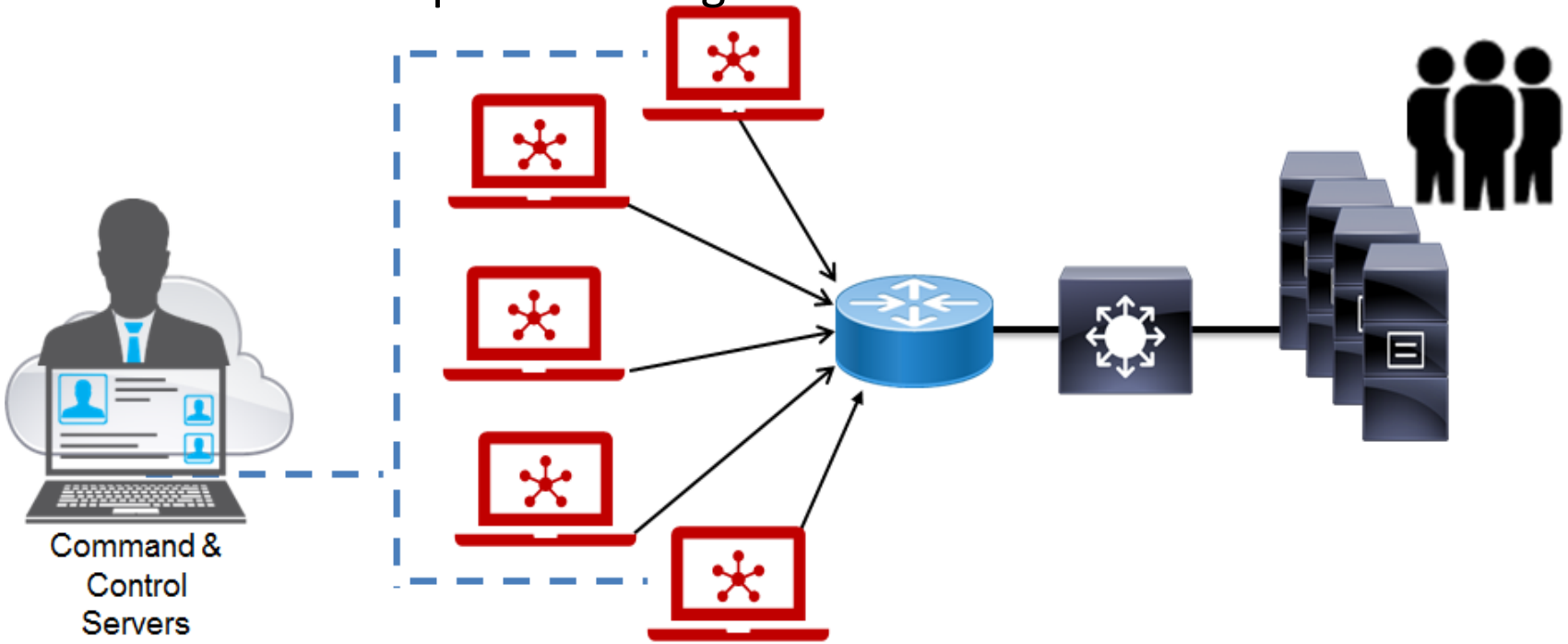
- After you combine your conditions into rules, you combine the rules into a web ACL
- This is where you define an action for each rule—allow, block, or count—**and a default action**



@iconshock.com

Anti-DDoS

- AWS provides AWS Shield Standard and AWS Shield Advanced for protection against DDoS attacks



AWS Shield Advanced

- Provides expanded DDoS attack protection for your Elastic Load Balancing load balancers, CloudFront distributions, and Amazon Route 53 hosted zones
- Includes intelligent DDoS attack detection and mitigation for OSI layers 3 through 7
- You get 24x7 DDoS response team (DRT) assistance during a DDoS attack
- You have exclusive access to advanced, real-time metrics and reports for deep visibility into attacks on your AWS resources

Amazon Inspector

- Automated security assessment service that helps security and compliance of applications deployed on AWS
- Automatically assesses applications for vulnerabilities or deviations from best practices
- Produces a detailed list of security findings prioritized by severity level
- Inspector includes a knowledge base of hundreds of rules mapped to common security best practices and vulnerability definitions

AWS Guard Duty

- Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior
- It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise (Zero Days)
- GuardDuty also detects potentially compromised instances or reconnaissance by attackers.
- Uses proprietary ML and AI along with strategic partners

AWS Guard Duty

- When GuardDuty detects suspicious or unexpected behavior it generates a finding - a notification that has the details about a impending security issue
- The finding details include information about what occurred, what AWS resources were involved in the suspicious activity, when this activity took place, and other data
- The finding type provides a description of the potential security issue: ***Recon:EC2/PortProbeUnprotectedPort***
- docs.aws.amazon.com: “Amazon GuardDuty Finding Types”

Segment 4: Billing and Pricing

AWS Organizations

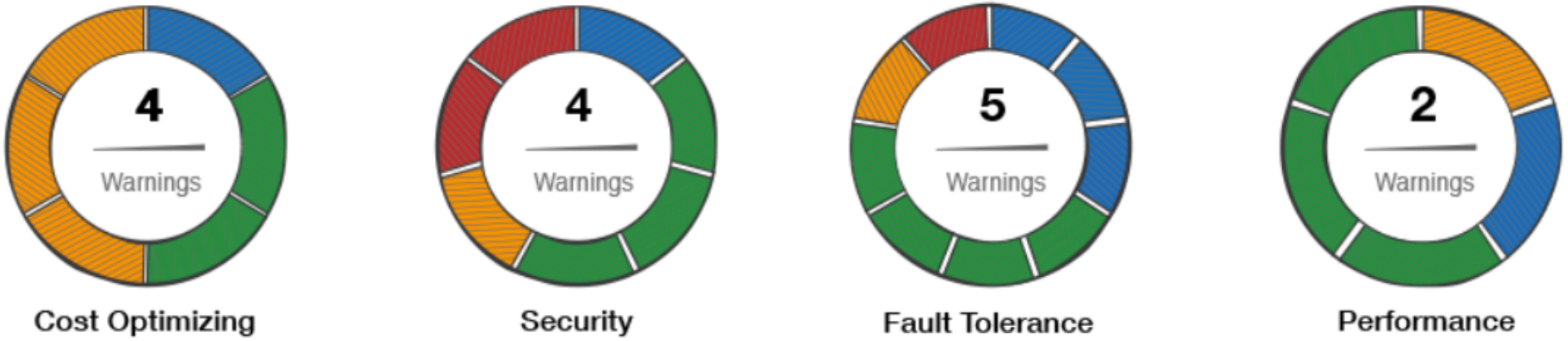
- AWS Organizations provide policy-based management for multiple AWS accounts
  - Create groups of accounts
  - Automate account creation
  - Apply and manage policies for account groups
- Organizations centrally manage Service Control Policies (SCPs) across multiple accounts without using custom scripts or manual processes
- Can also use Organizations to automate the creation of new accounts through APIs

Service Pricing

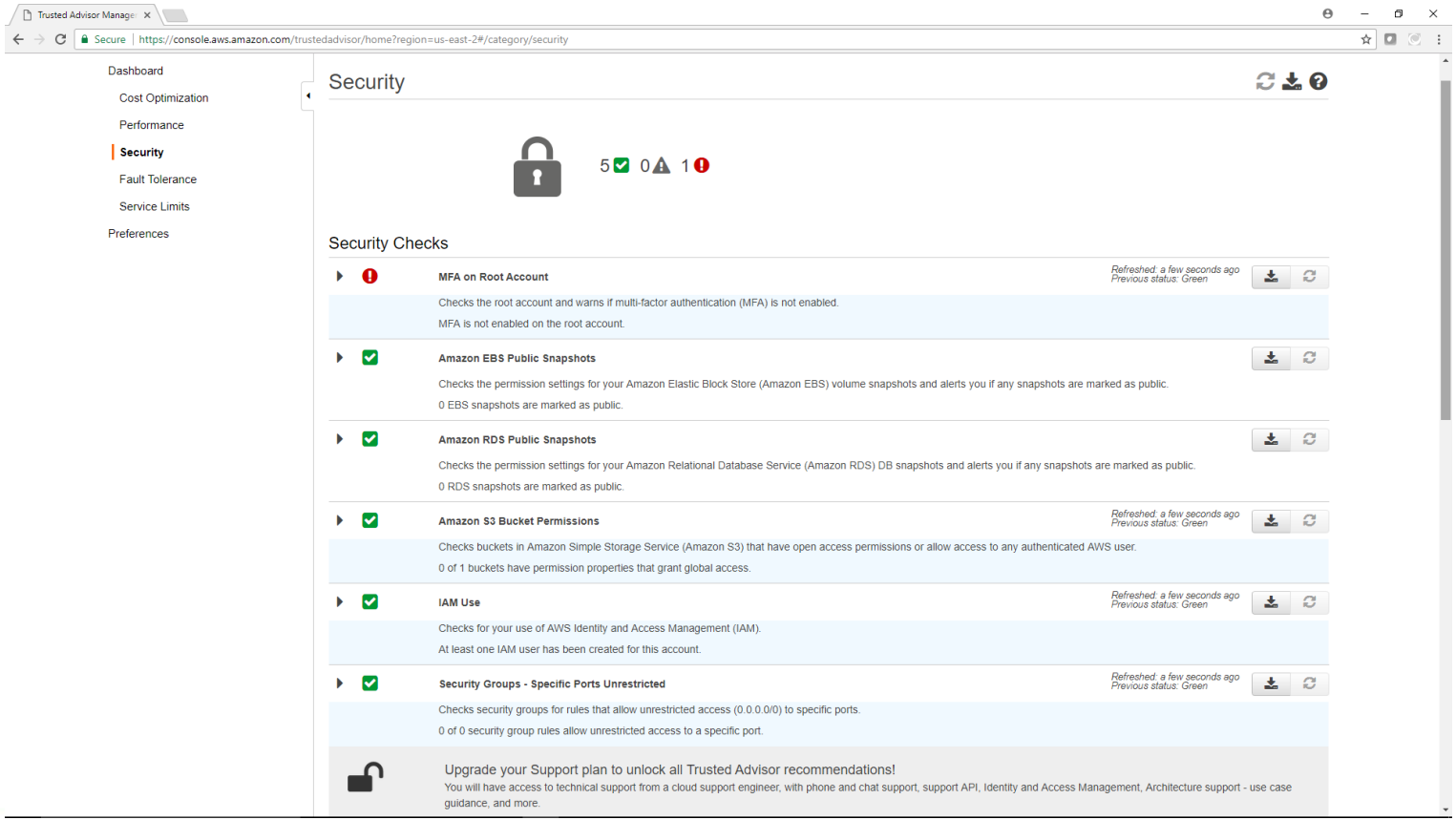
- AWS offers you a pay-as-you-go approach for pricing for over 120 cloud services
- With AWS you pay only for the individual services you need, for as long as you use them, and without requiring long-term contracts or complex licensing
- AWS pricing is similar to how you pay for utilities like water and electricity - you only pay for the services you consume, and once you stop using them, there are no additional costs or termination fees

AWS Trusted Advisor

- Uses best practices derived from history of serving thousands of AWS customers
- Also Personal Health Dashboard
- Includes 27 individual checks within 4 categories:



AWS Trusted Advisor



AWS Support Models

- **Basic**
- **Developer**
- **Business**
- **Enterprise**

@iconshock.com

AWS Cloud Practitioner Course

Michael J. Shannon

THANK YOU FOR ATTENDING!