

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button or a video thumbnail.

AWS Cloud Practitioner Course

Michael J.
Shannon

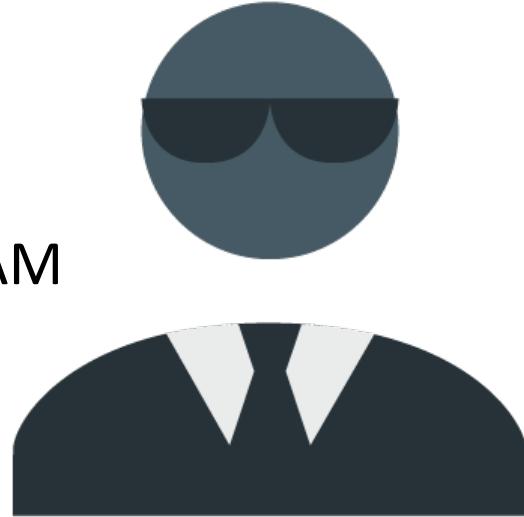
IT/Security Consultant,
Instructor, and
Author



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



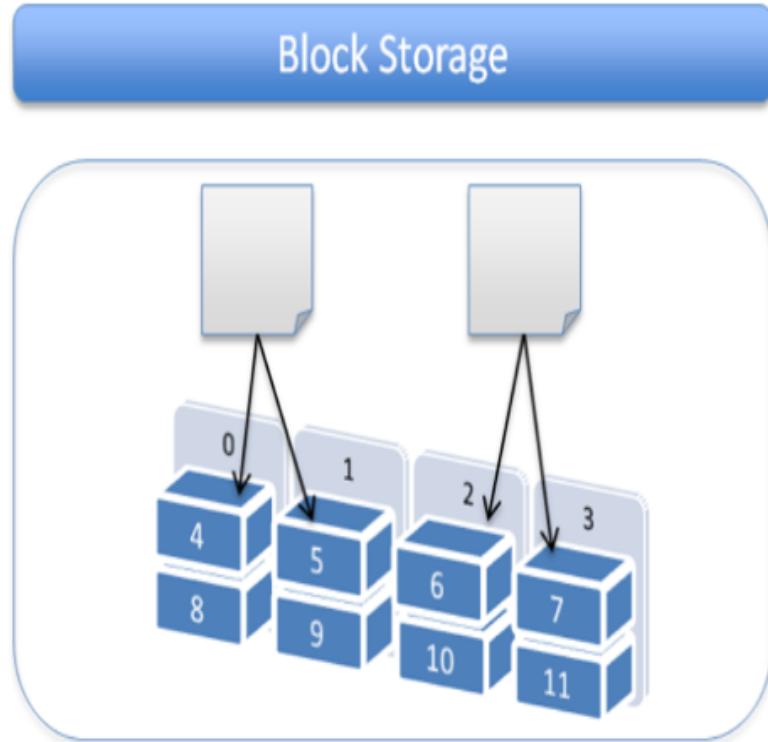
@iconshock.com



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

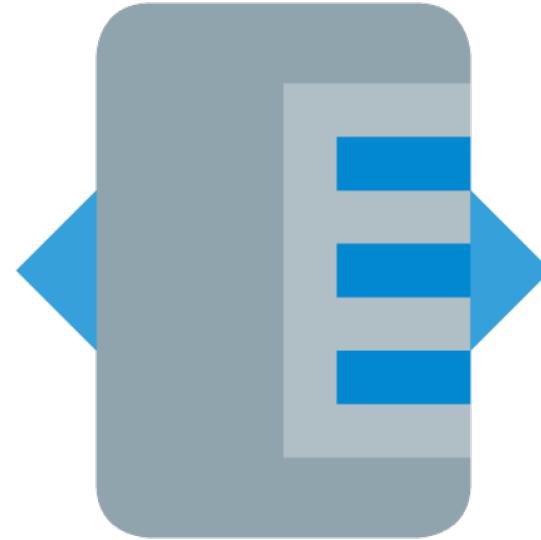
- **Amazon Simple Storage Service (Amazon S3)** is an object storage service that offers industry-leading scalability, data availability, security, and performance
- Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your 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/

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

Amazon S3 Glacier

- Glacier is a low-cost, highly-durable (99.99999999%), 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

The screenshot shows the 'Data Retrieval Settings' dialog box from the AWS S3 Glacier interface. The dialog has two tabs: 'Retrieval policies' (selected) and 'Provisioned capacity'. A note at the top states: 'Using S3 Glacier data retrieval policies, you can manage retrieval costs by setting limits on retrieval activities across your AWS account in each region. Retrieval policies apply to standard retrievals.' Three options are available for retrieval policies:

- Free Tier Only: Only retrieve data within the free tier. Data retrieval requests that exceed the free tier will not be accepted. Retrieval Cost: Free.
- Max Retrieval Rate: Set the maximum retrieval rate to 1 GB/Hour. Retrieval Cost: \$7.20 / month or less.
- No Retrieval Limit: All valid data retrieval requests will be accepted. Data Retrieval cost will vary based on your usage. Visit the [pricing page](#) for data retrieval pricing information.

A note at the bottom states: 'Note: Data retrieval policies govern all retrieval activities in a region. The retrieval cost estimates may not reflect previously incurred usage or charges in the month. [Learn more](#)'

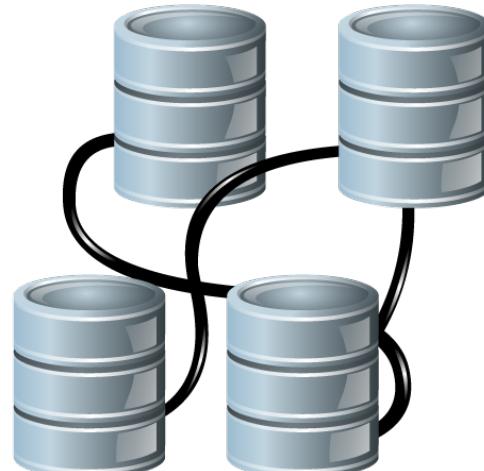
At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

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)

Step 1
Select engine

Step 2
Choose use case

Step 3
Specify DB details

Step 4
Configure advanced settings

RDS > Create database

Select engine

Engine options

- Amazon Aurora
Amazon Aurora
- MySQL

- MariaDB

- PostgreSQL

- Oracle
ORACLE®
- Microsoft SQL Server


MySQL

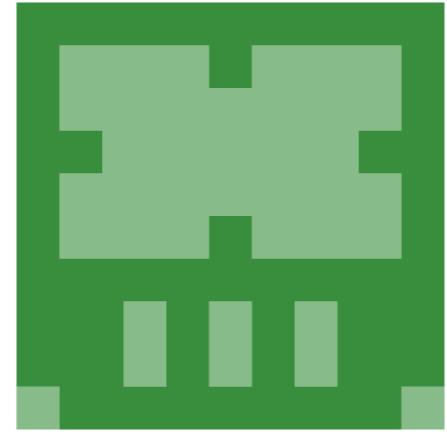
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.

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



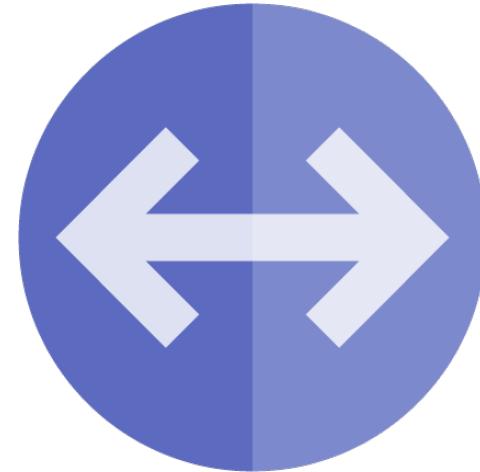
@iconshock.com

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

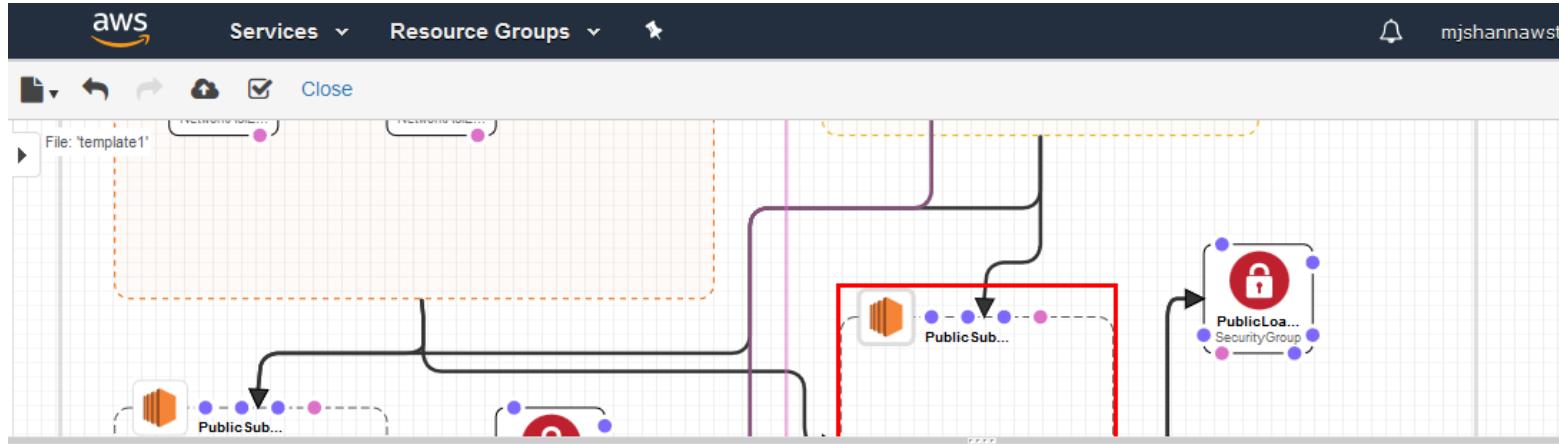
AWS CloudFormation

- 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   
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      "Default": ""  
14    }  
}
```

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

AWS Services

CloudWatch

Dashboards

MyDashboard

Alarms

ALARM 0

INSUFFICIENT 0

OK 0

Billing

Events

Rules

Event Buses

Logs

Insights

Metrics

Favorites

Add a dashboard

Add to this dashboard

Select a widget type to configure and add to this dashboard.

Line
Compare metrics over time

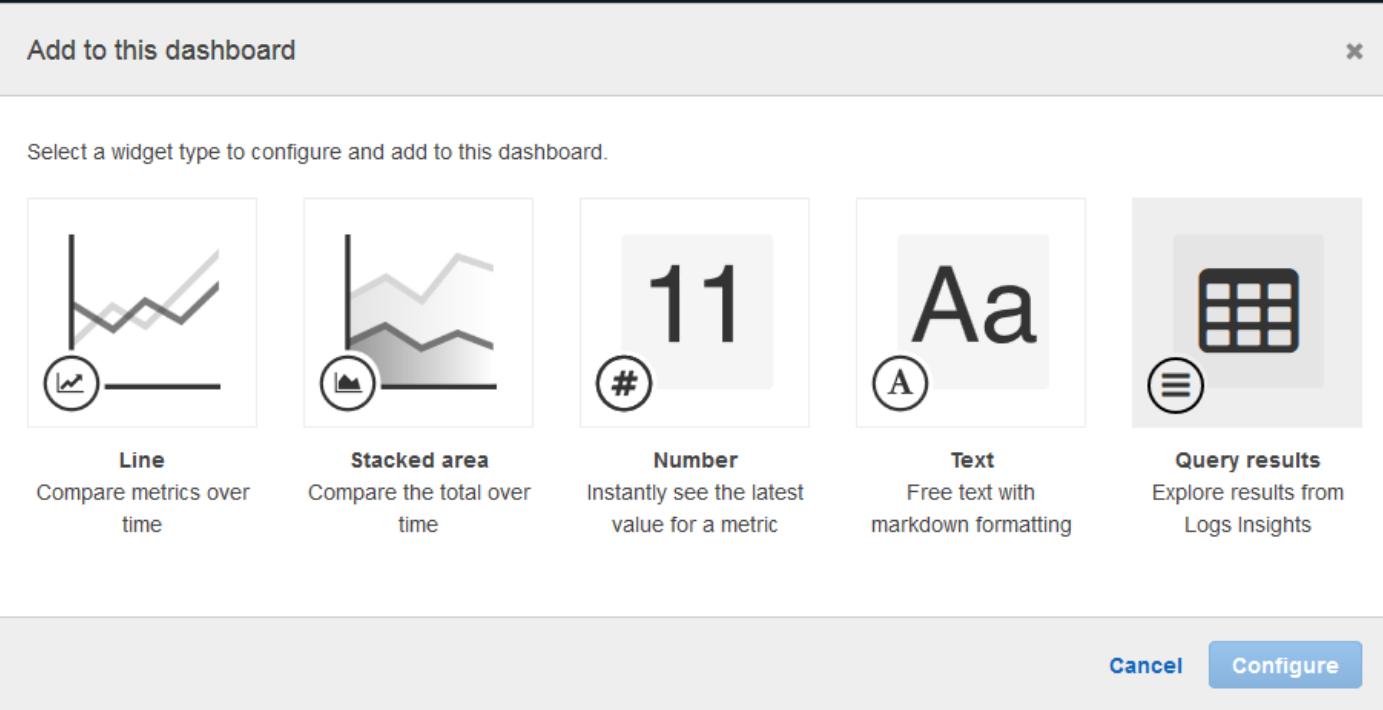
Stacked area
Compare the total over time

Number
Instantly see the latest value for a metric

Text
Free text with markdown formatting

Query results
Explore results from Logs Insights

Cancel Configure





Segment 2: AWS Security Survey and IAM

Hashing

Data of an arbitrary length



Hash Function

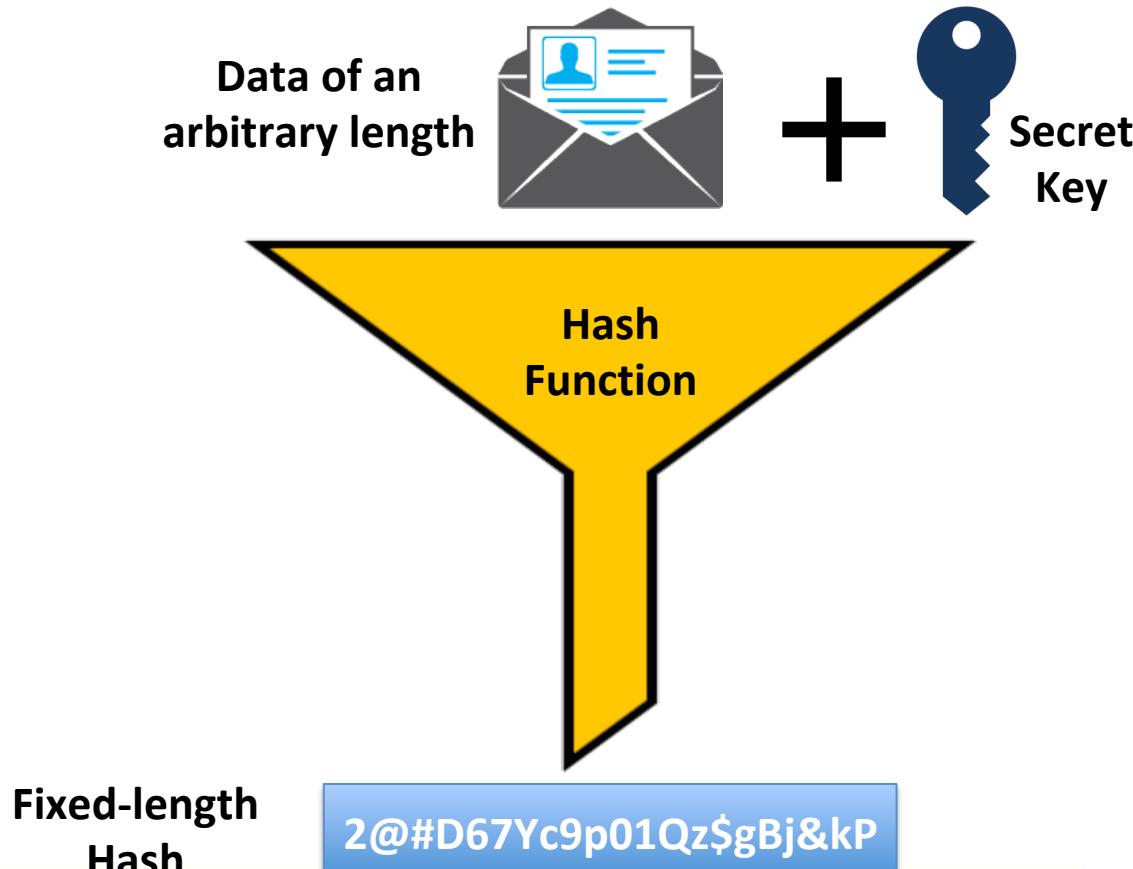
Fixed-length
Hash
(fingerprint)

2@#D67Yc9p01Qz\$gBj&kP



Pearson

Hashed MAC for Integrity



Encryption

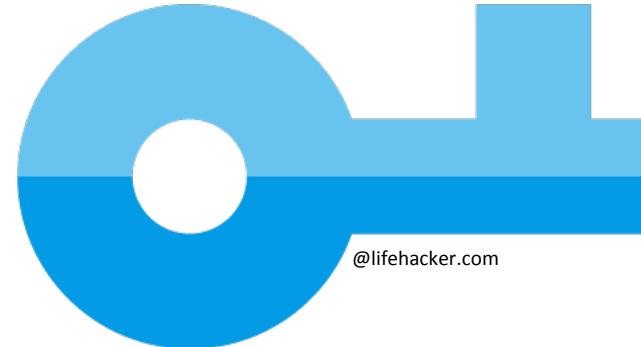
- Encryption hides the original data or message content by scrambling the clear text into a random appearing string of characters called ciphertext
- Decryption reverses the process of encryption when an entity has the proper decryption key
- Many applications store and send information in clear text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



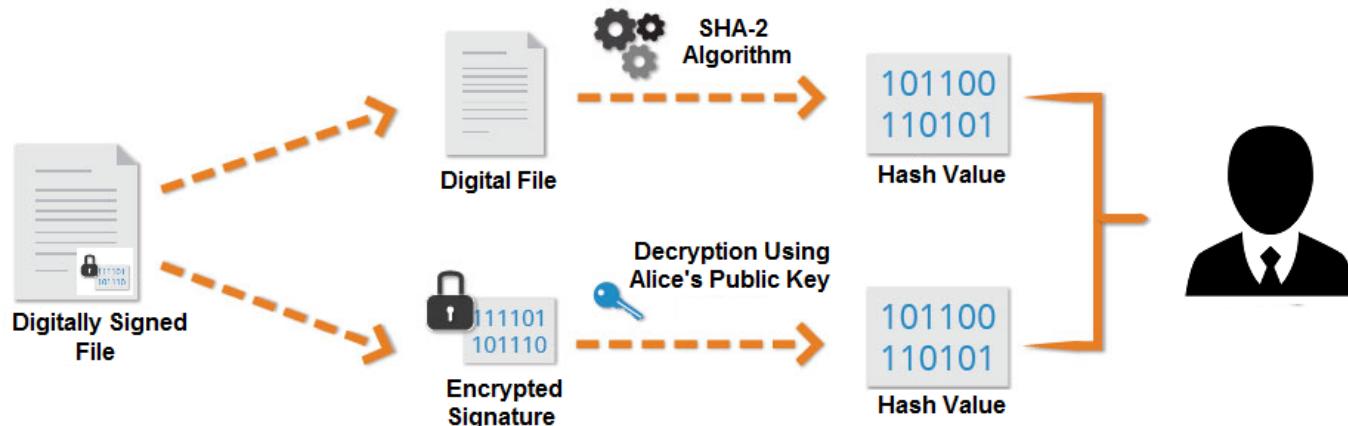
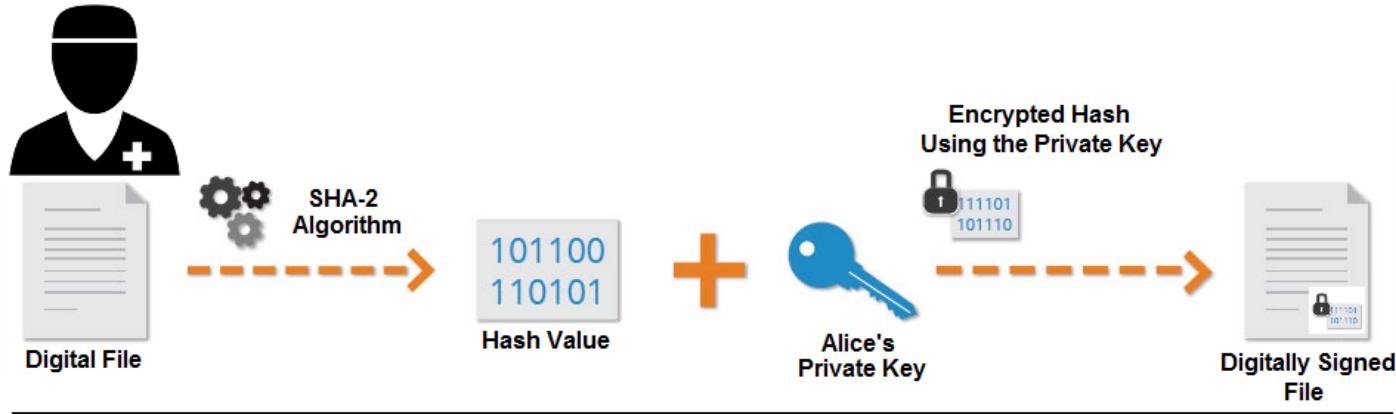
Asymmetric Key Systems

- 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



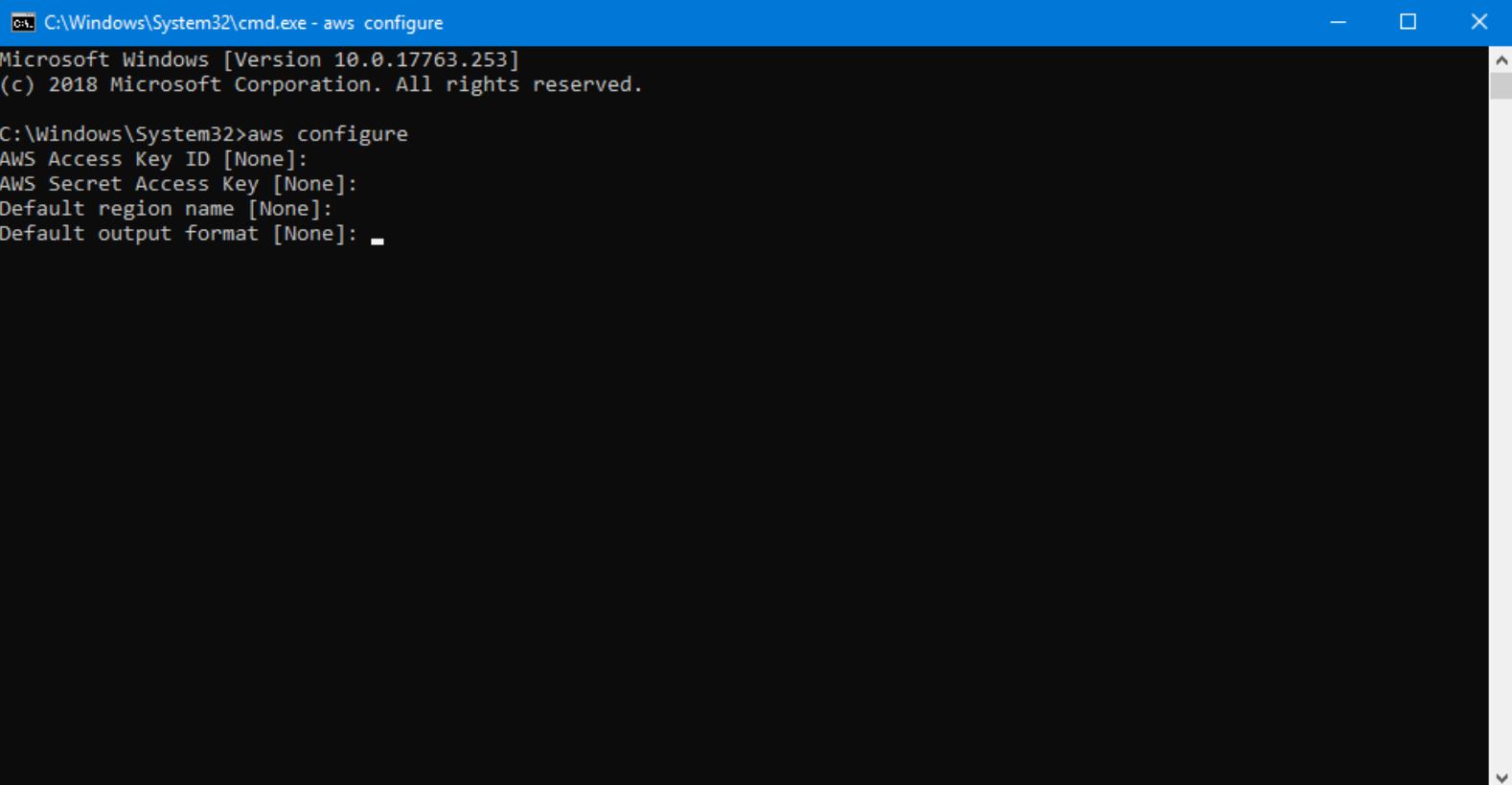
Protecting Cloud Data in Transit

- 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



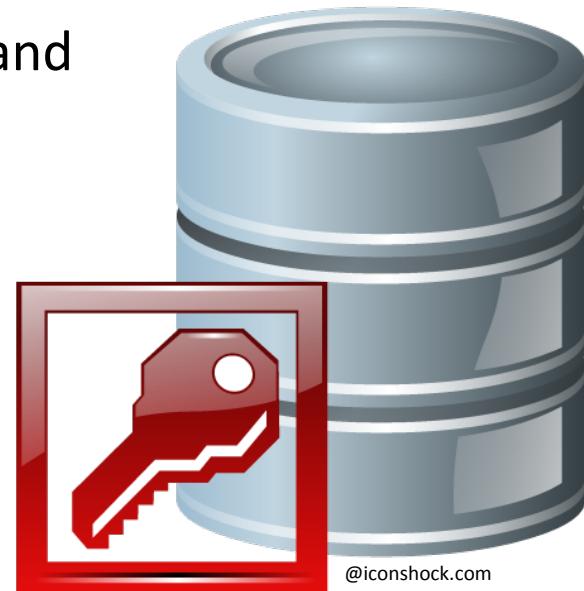
C:\Windows\System32\cmd.exe - aws configure

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]: -
```

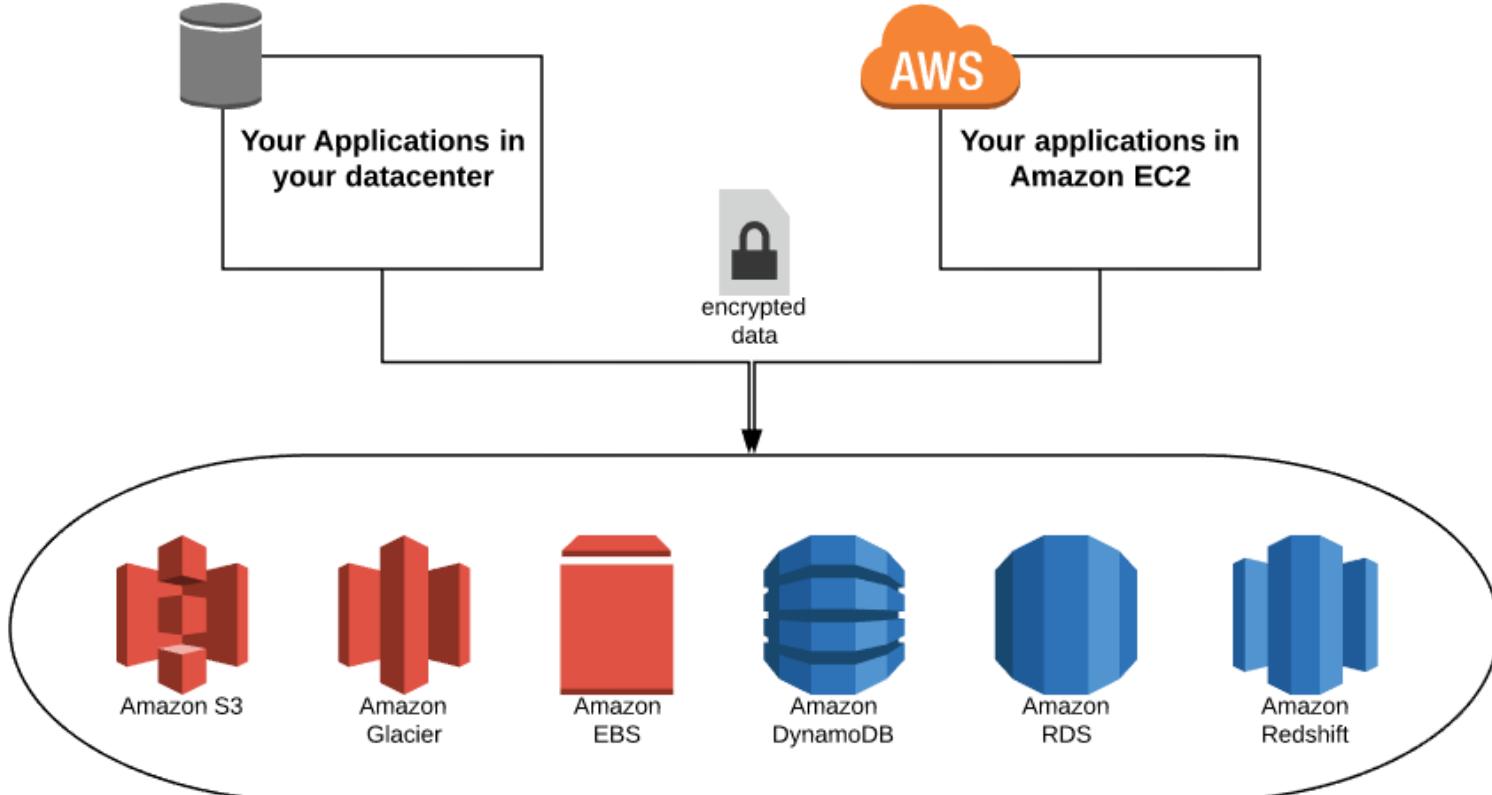
Encryption and Key Management in AWS

- 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

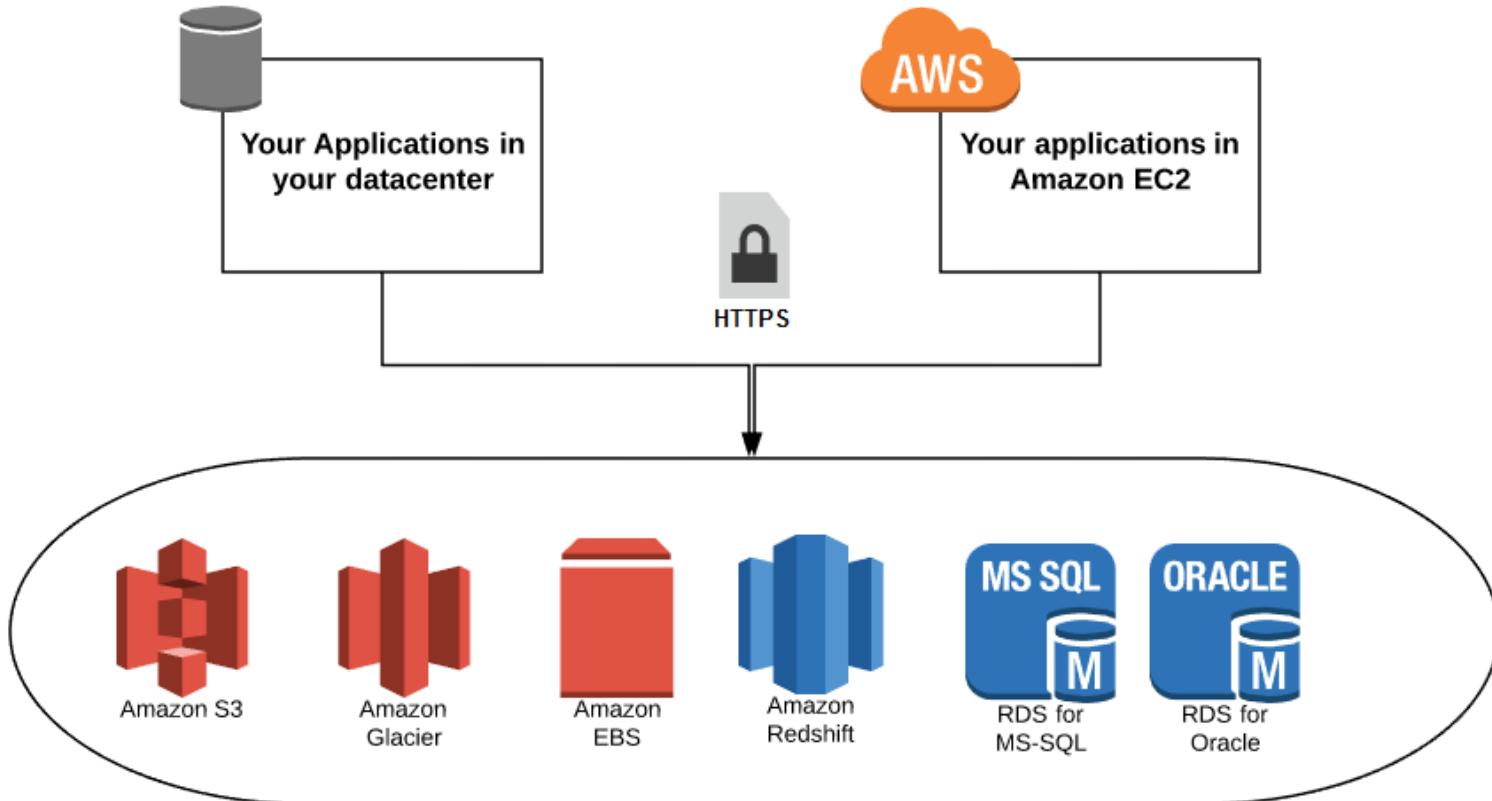


@iconshock.com

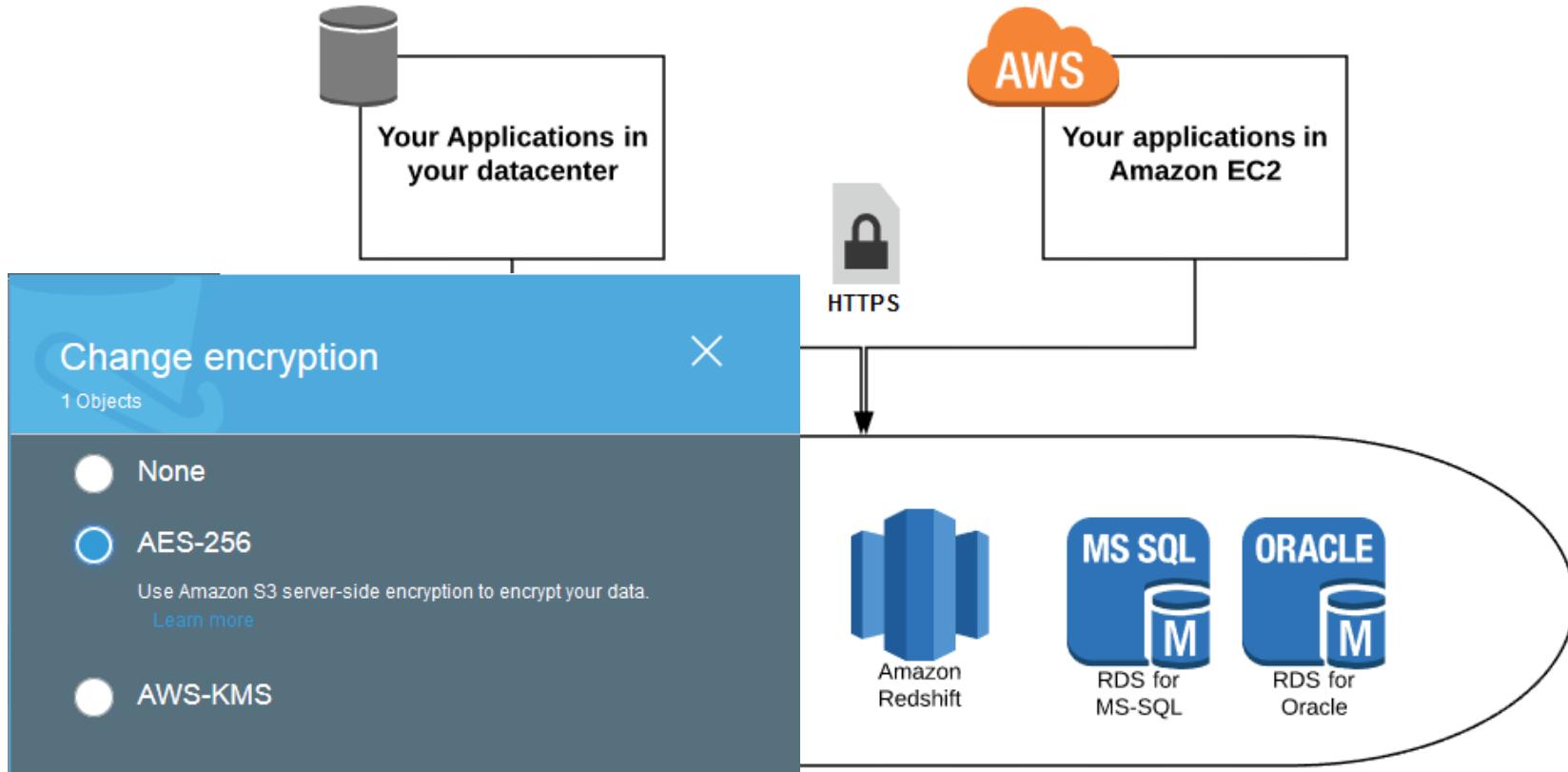
Client-side Encryption



Server-side Encryption



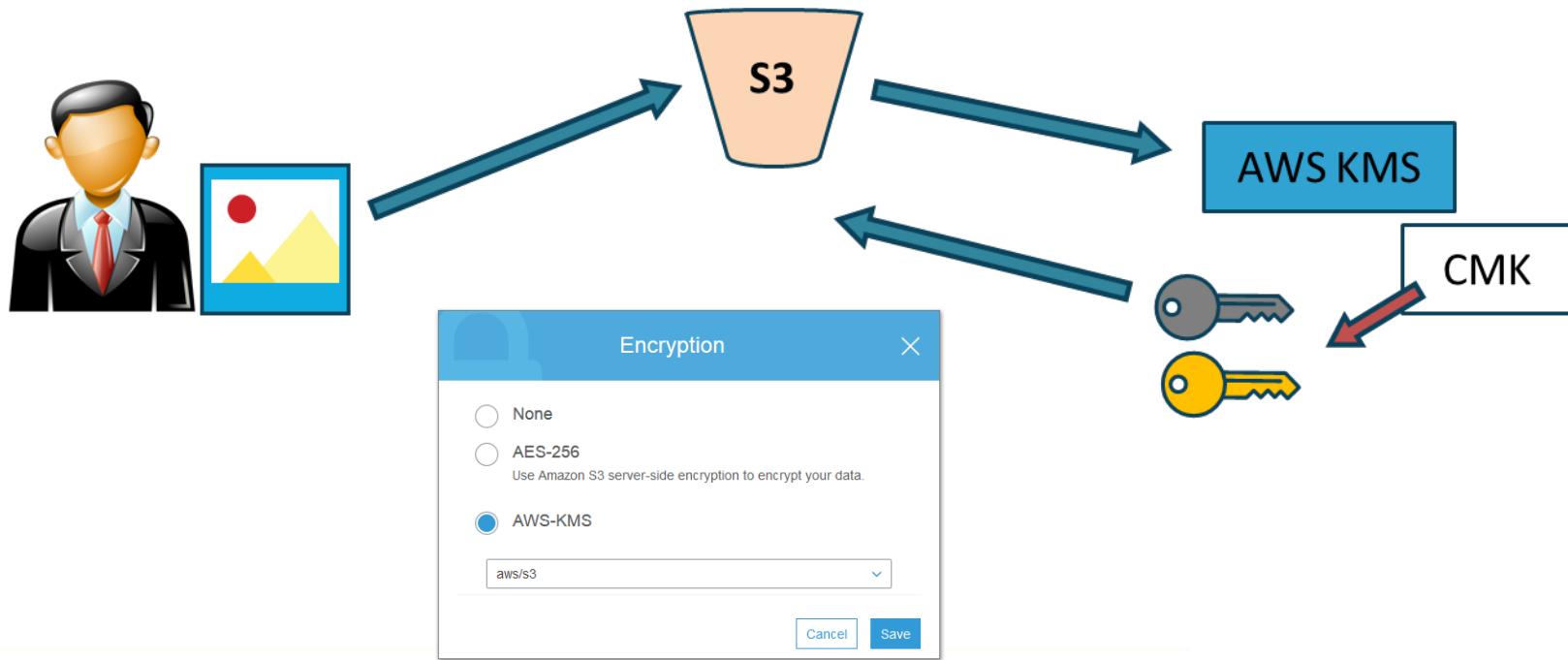
Server-side Encryption



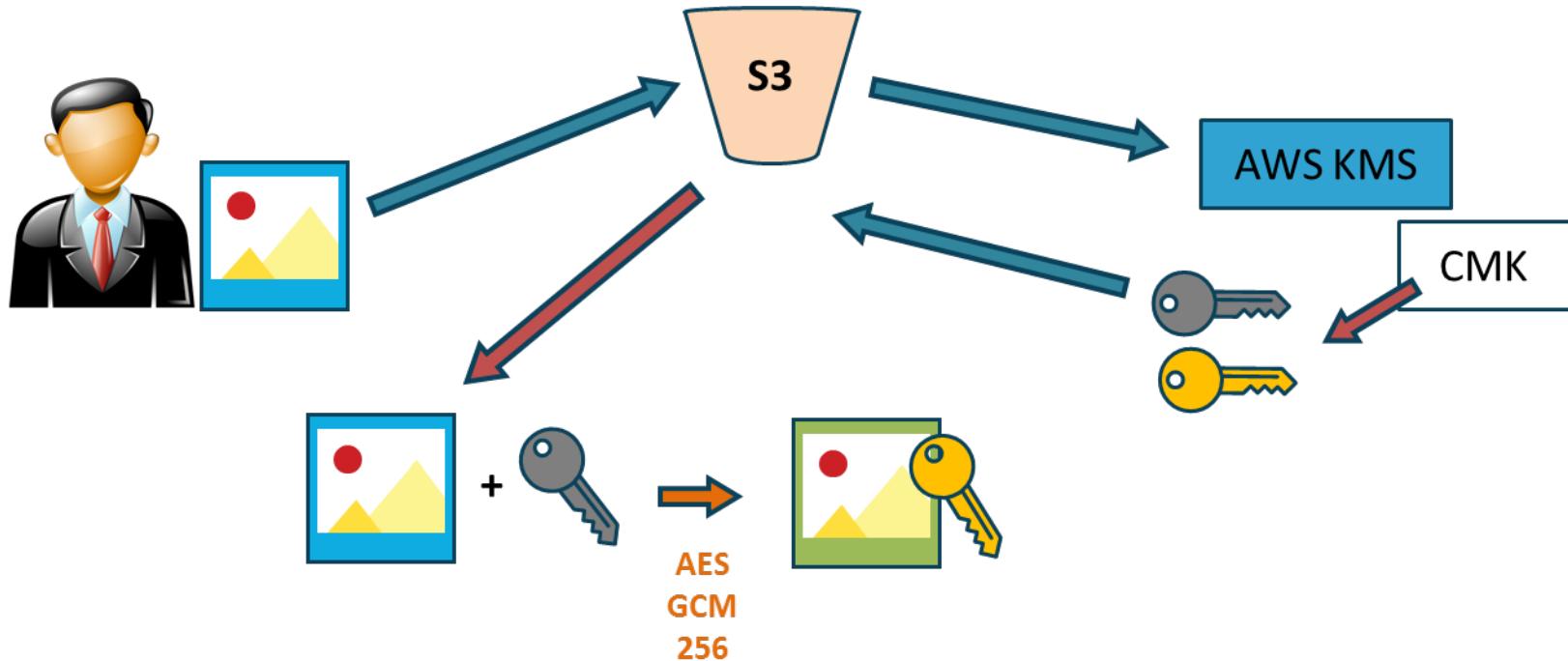
AWS Key Management Service (KMS)

- 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

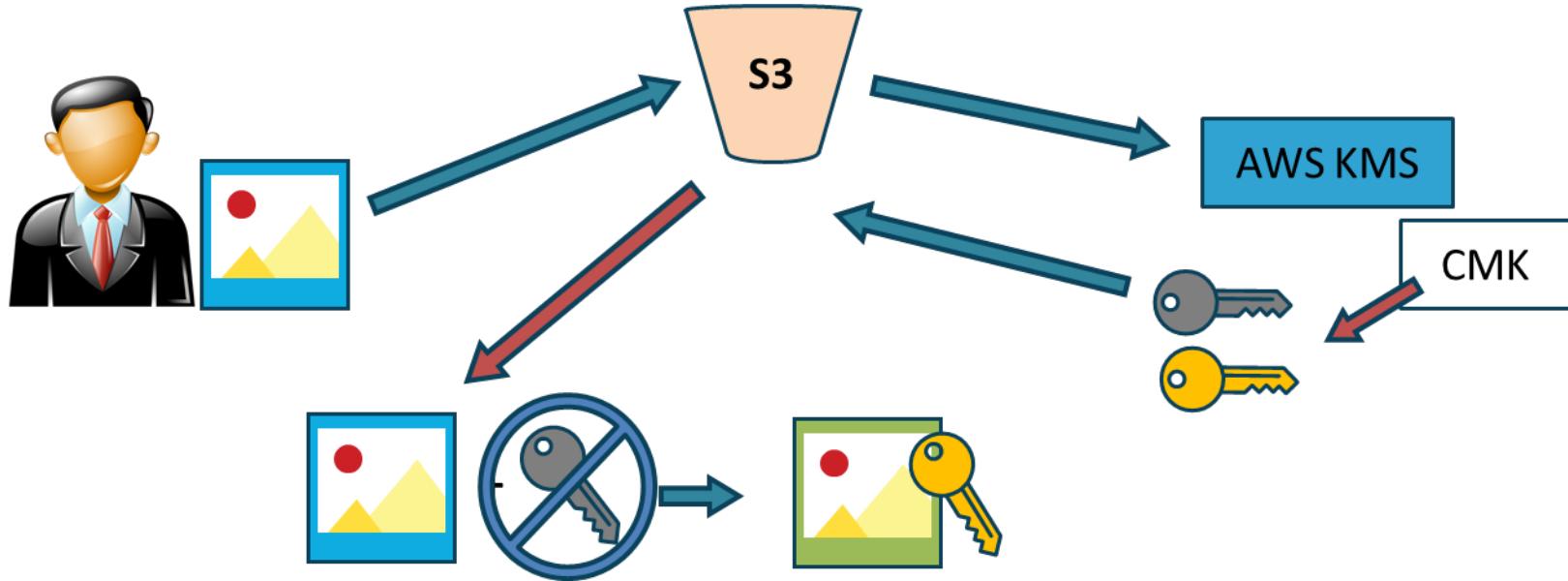
AWS Key Management Service (KMS)



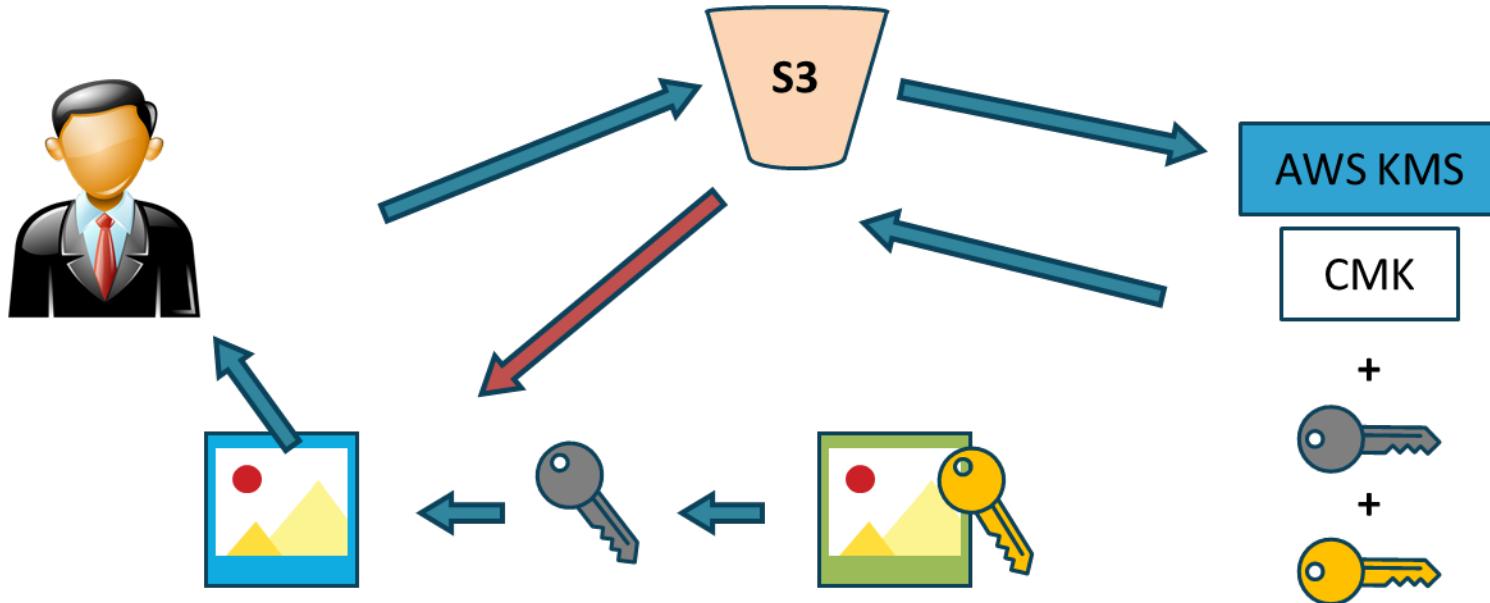
AWS Key Management Service (KMS)



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

Volume Type <i>(i)</i>	Device <i>(i)</i>	Snapshot <i>(i)</i>	Size (GiB) <i>(i)</i>	Volume Type <i>(i)</i>	IOPS <i>(i)</i>	Throughput (MB/s) <i>(i)</i>	Delete on Termination <i>(i)</i>	Encryption <i>(i)</i>
Root	/dev/xvda	snap-04a92f3aceecdabef	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensit	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input type="checkbox"/>	Not Encrypted

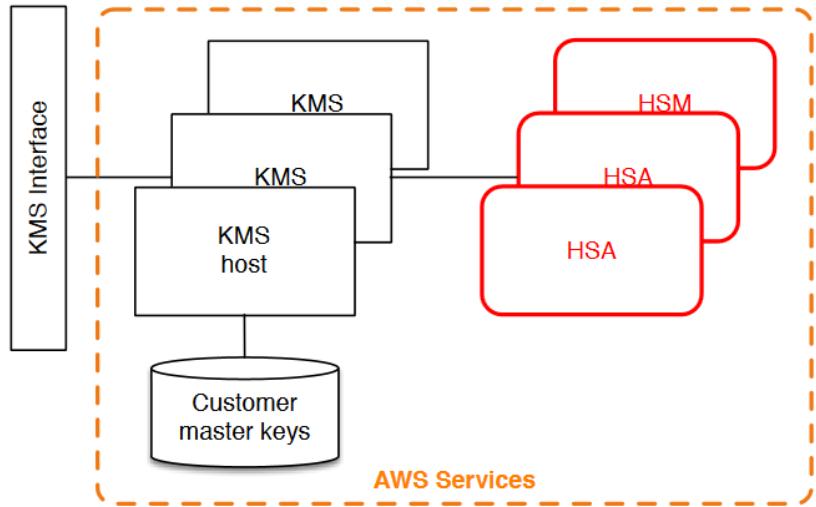
Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Filter by attributes

KMS Key Aliases	KMS Key ID
Not Encrypted	
(default) aws/ebs	alias/aws/ebs

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

The screenshot shows the AWS IAM Management Console with the URL https://console.aws.amazon.com/iam/home?region=us-east-2#/account_settings. The left sidebar has a 'Search IAM' field and links for Dashboard, Groups, Users, Roles, Policies, Identity providers, **Account settings** (which is selected and highlighted in orange), Credential report, and Encryption keys. The main content area is titled 'Password Policy'. It defines a password policy as a set of rules for IAM users. A note says the account does not have a password policy yet. It includes fields for minimum password length (set to 6), checkboxes for various requirements (uppercase, lowercase, numbers, non-alphanumeric), and options for password expiration, reuse prevention, and administrator reset. Buttons at the bottom are 'Apply password policy' (blue) and 'Delete password policy' (red).

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

Require at least one uppercase letter i

Require at least one lowercase letter i

Require at least one number i

Require at least one non-alphanumeric character i

Allow users to change their own password i

Enable password expiration i

Password expiration period (in days):

Prevent password reuse i

Number of passwords to remember:

Password expiration requires administrator reset i

Apply password policy **Delete password policy**

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 Management Console + https://console.aws.amazon.com/iam/home#/roles\$new?step=permissions&selectedS... Search shankantoo Global Support

Services Resource Groups

Trust Permissions Review

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy Refresh

Filter: Policy type ▾ Search Showing 343 results

	Policy name	Attachments	Description
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	0	Default policy for the Amazon ECS Role for Amazon ECS ...
<input type="checkbox"/>	AmazonEC2ContainerServiceFullAccess	0	Provides administrative access to Amazon ECS resources.
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	0	Default policy for Amazon ECS service role.
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	0	Provides full access to Amazon EC2 via the AWS Manage...
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	0	Provides read only access to Amazon EC2 via the AWS M...
<input type="checkbox"/>	AmazonEC2ReportsAccess	0	Provides full access to all Amazon EC2 reports via the AW...
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeploy	0	Provides EC2 access to S3 bucket to download revision. ...
<input type="checkbox"/>	AmazonEC2RoleforDataPipelineRole	0	Default policy for the Amazon EC2 Role for Data Pipeline ...
<input type="checkbox"/>	AmazonEC2RoleforSSM	0	Default policy for Amazon EC2 Role for Simple Systems M...

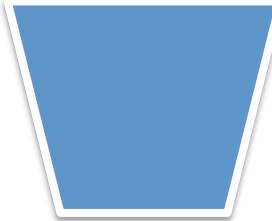
* Required Cancel Previous Next: Review

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)

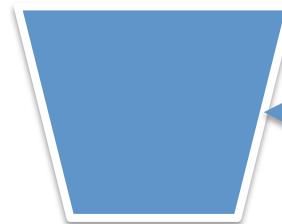
DEVELOPMENT
Account
(application sandbox)



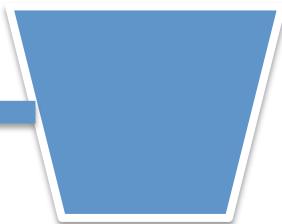
PRODUCTION
Account
(live applications)

DEVELOPMENT
IAM: Developers and
Testers

productionapp

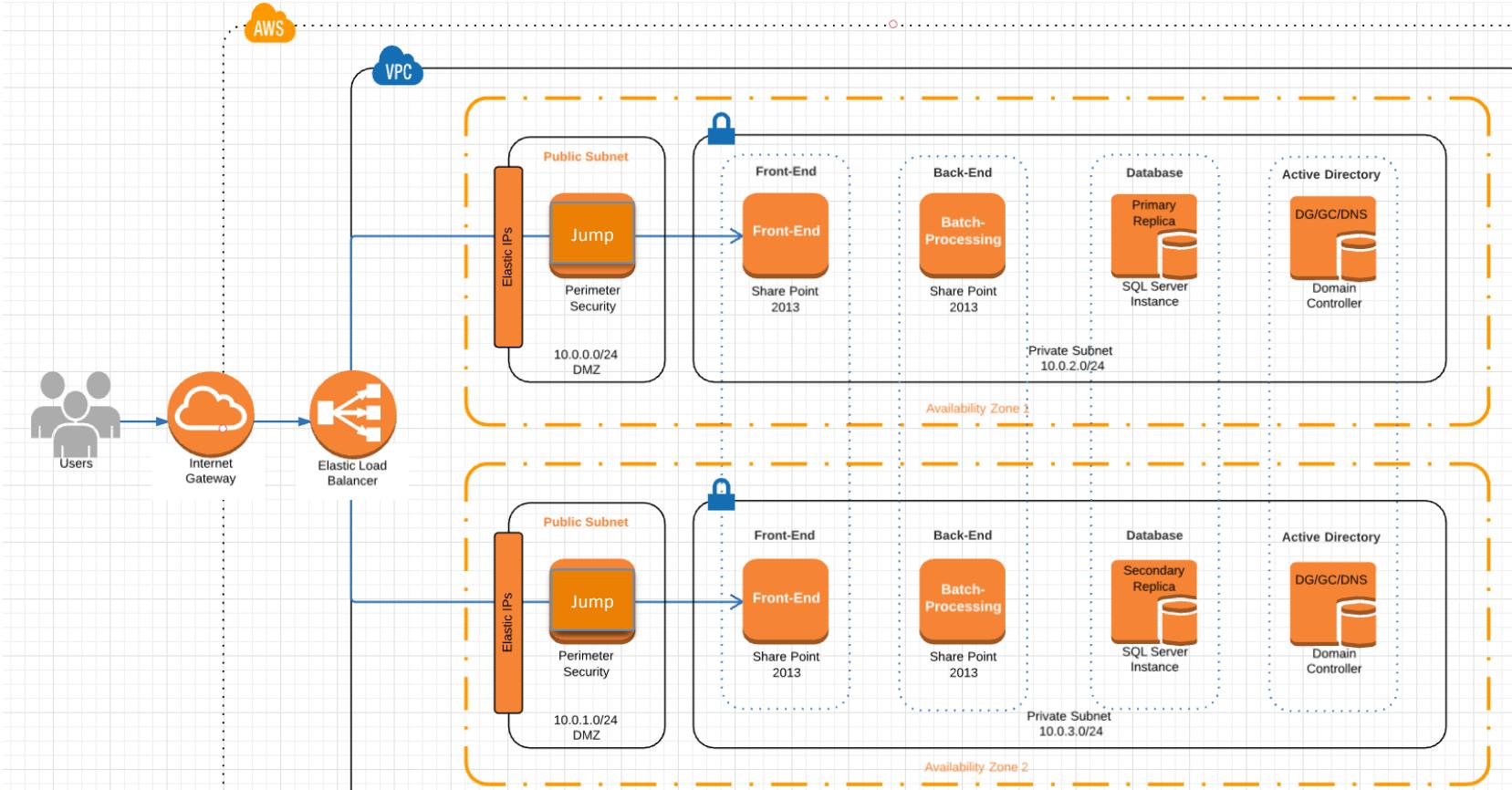


Trusting Account



Trusted Account

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

Screenshot of the AWS IAM "Create role" wizard, step 1: Select type of trusted entity.

The "Another AWS account" option is selected.

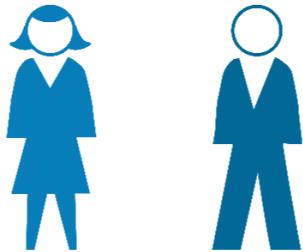
Below the selection, it says: "Allows entities in other accounts to perform actions in this account." with a "Learn more" link.

The next step, "Specify accounts that can use this role," shows an Account ID input field containing "314658760392".

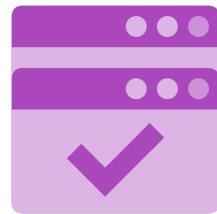
An "Options" section includes a checked checkbox for "Require external ID (Best practice when a third party will assume this role)".

A tooltip explains: "You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID." with a "Learn more" link.

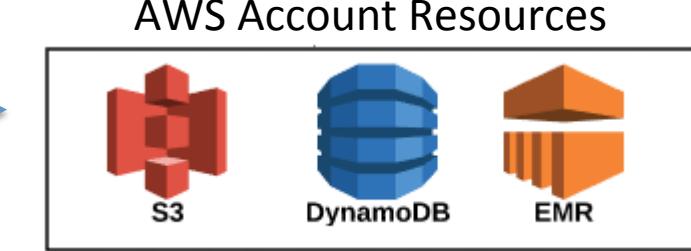
Default Access to AWS Resources



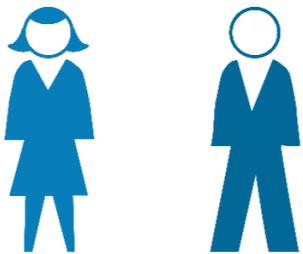
Employees
Get AWS IAM
user accounts
Assigned to
Groups or Roles



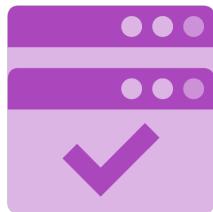
Permissions
Through
Managed
Policies



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)



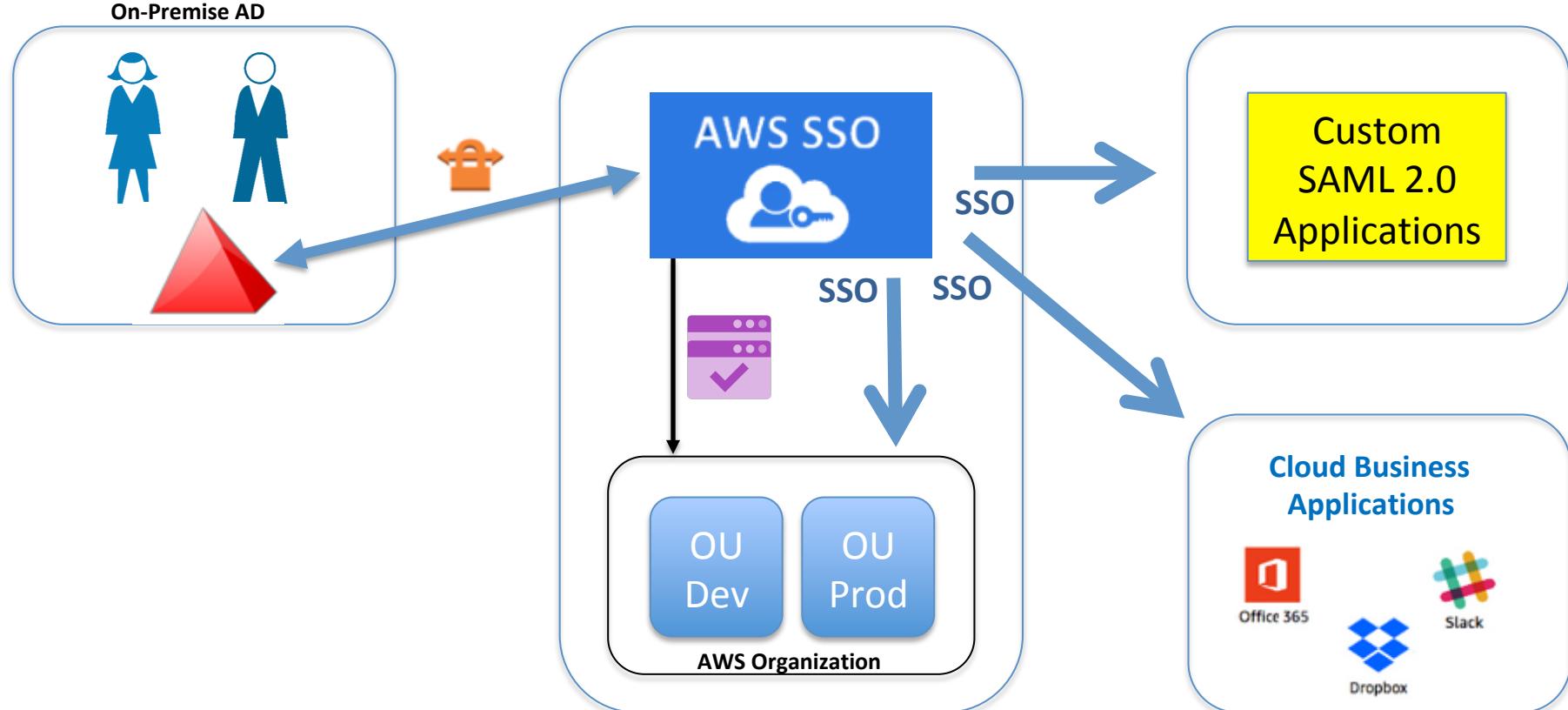
SAML 2.0

AWS Account Resources

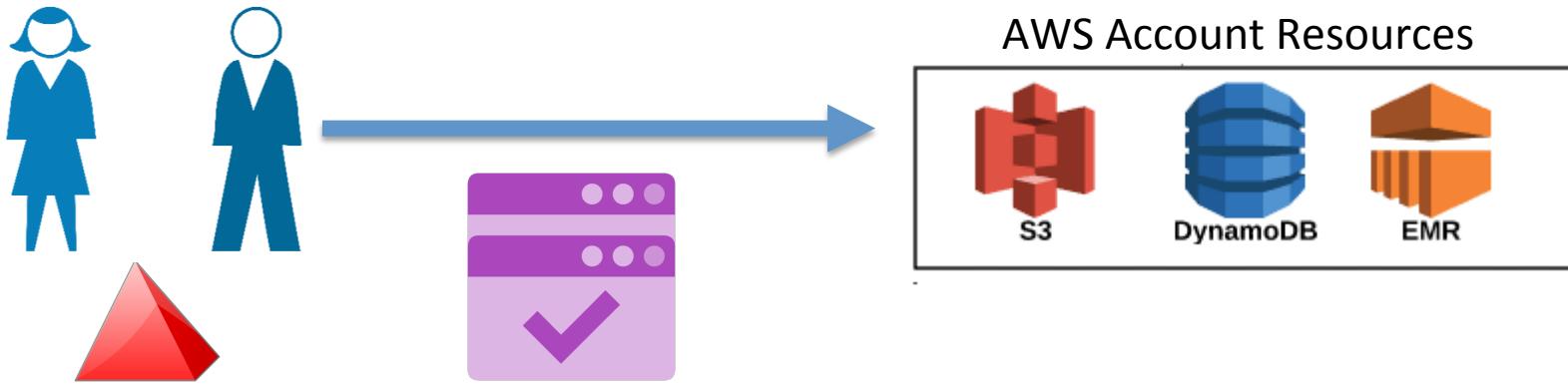


“Choose Your Own SAML Adventure: A Self-Directed Journey to AWS Identity Federation Mastery” at AWS

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

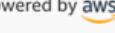
Your applications

Hi John | [Sign out](#)

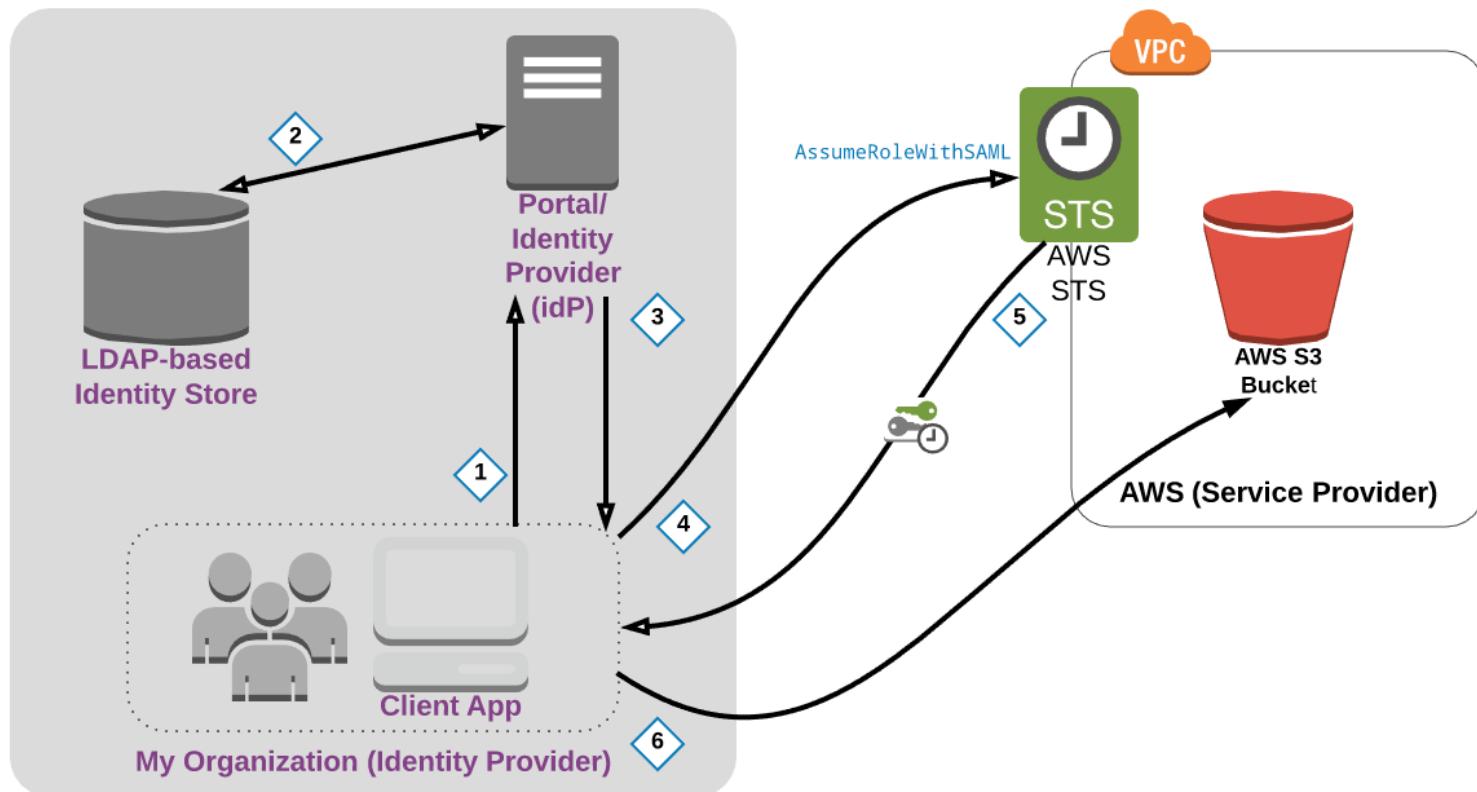
Search

 AWS Management Console (3)	 Dropbox	 Office365	 Slack
 650 (Account)			>
 680 (Account)			>
 903 (Account)			>
SecurityAudit			

[Terms of Use](#)

Powered by 

Amazon Cognito



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

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

Optional



ex: us-east-1_Ab129faBb

App client id

Optional

ex: 7ihlkkfbfb4q5kpp90urffao

Add Another Provider

* Required

Cancel

Create Pool



Pearson

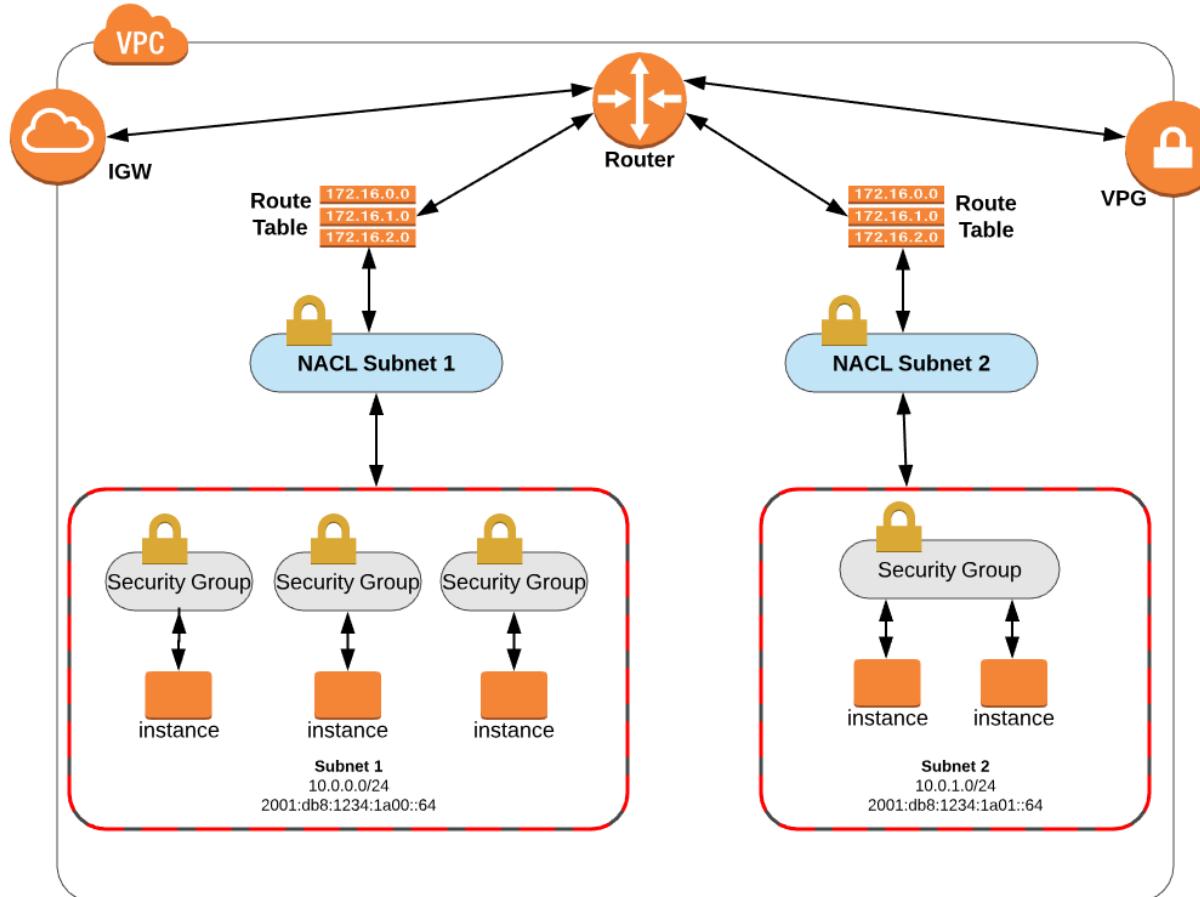


Segment 3: Infrastructure Security

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

The screenshot shows the AWS VPC Management Console with the Subnets page open. The left sidebar lists various VPC components: Virtual Private Cloud, Your VPCs, Subnets (selected), Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, and Security. The main content area displays a table of subnets, with the "Public subnet" highlighted by a red box. Below the table, the "Edit" tab is selected for the Network ACL (acl-c37eddab). The ACL configuration is shown in two sections: Inbound and Outbound. Both sections contain two rules: one allowing all traffic (Rule #100) and one denying all traffic (Rule *). The "Allow / Deny" column uses green for ALLOW and red for DENY.

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Available IPv6
Private subnet	subnet-f5ff558e	available	vpc-63864f0b MY-VPC	10.0.1.0/24	251		us-east-2
	subnet-0e6d6575	available	vpc-1f30fc77	172.31.16.0/20	4090		us-east-2
	subnet-e71758aa	available	vpc-1f30fc77	172.31.32.0/20	4091		us-east-2
Public subnet	subnet-dc5852a7	available	vpc-63864f0b MY-VPC	10.0.0.0/24	250		us-east-2

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



NACLs

The screenshot shows the AWS VPC Management Console with the Network ACLs page open. A search bar at the top has 'acl-c37eddb' entered. On the left, the VPC Dashboard sidebar lists various VPC components. In the center, a modal window titled 'Create Network ACL' is displayed, showing a list of port protocols and numbers. Two input fields at the bottom of this list are highlighted with red boxes: 'Rule #' containing '100' and '101'. A 'Save' button is visible. To the right, the main Network ACL details page shows it is associated with a VPC and two subnets, with a note about creating rules. A table below lists existing rules.

Protocol	Port Range	Source	Allow / Deny	Remove
ALL	ALL	0.0.0.0/0	ALLOW	X
TCP (6)	0		ALLOW	X

Feedback

English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy Terms of Use



Pearson

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

The screenshot shows the AWS VPC Manager interface. The left sidebar has a red box around the 'Security Groups' link under the 'Security' section. The main content area shows a list of security groups with one selected, also highlighted by a red box. The selected security group is 'sg-ea4cab81'. The 'Inbound Rules' tab is active, highlighted with a red box. Below it is a table listing inbound rules:

Type	Protocol	Port Range	Source	Description	Remove
HTTP (80)	TCP (6)	80	0.0.0.0/0	From all IPv4 addresses	X
HTTP (80)	TCP (6)	80	::/0	From all IPv6 addresses	X
HTTPS (443)	TCP (6)	443	0.0.0.0/0	From all IPv4 addresses	X
HTTPS (443)	TCP (6)	443	::/0	From all IPv6 addresses	X
SSH (22)	TCP (6)	22	50. 235/32	(From the Internet gateway)	X
RDP (3389)	TCP (6)	3389	50. 235/32	(From the Internet gateway)	X

Add another rule

Outbound Rules to Web Servers

The screenshot shows the AWS VPC Manager interface. The left sidebar navigation bar includes options like Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, and Security Groups. The Security Groups option is currently selected, indicated by an orange vertical bar.

The main content area displays a list of security groups. Two security groups are listed:

Name tag	Group ID	Group Name	VPC	Description
	sg-0e998166	default	vpc-1f30fc77	default VPC security group
	sg-ea4cab81	default	vpc-63864f0b MY-VPC	default VPC security group

The details for the security group 'sg-ea4cab81' are shown. The 'Outbound Rules' tab is selected. There are two rules listed:

Type	Protocol	Port Range	Destination	Description	Remove
MS SQL (1433)	TCP (6)	1433	pl-4ca54025	i	x
MySQL/Aurora (3306)	TCP (6)	3306	pl-4ca54025	i	x

An 'Add another rule' button is visible at the bottom of the rule table.



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

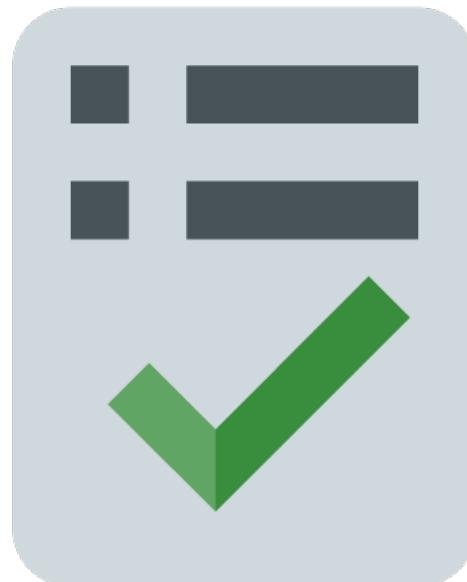
- IP addresses of originating requests
- Country that requests originate from
- Values in request headers
(e.g. User-Agent, Content-Type)
- Literal or regex string patterns that appear in requests (e.g. [cC][mM][dD].[eE][xX][eE])
- Length of requests (buffer overflows)
- Presence of SQL injection code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



@iconshock.com

Web ACLs

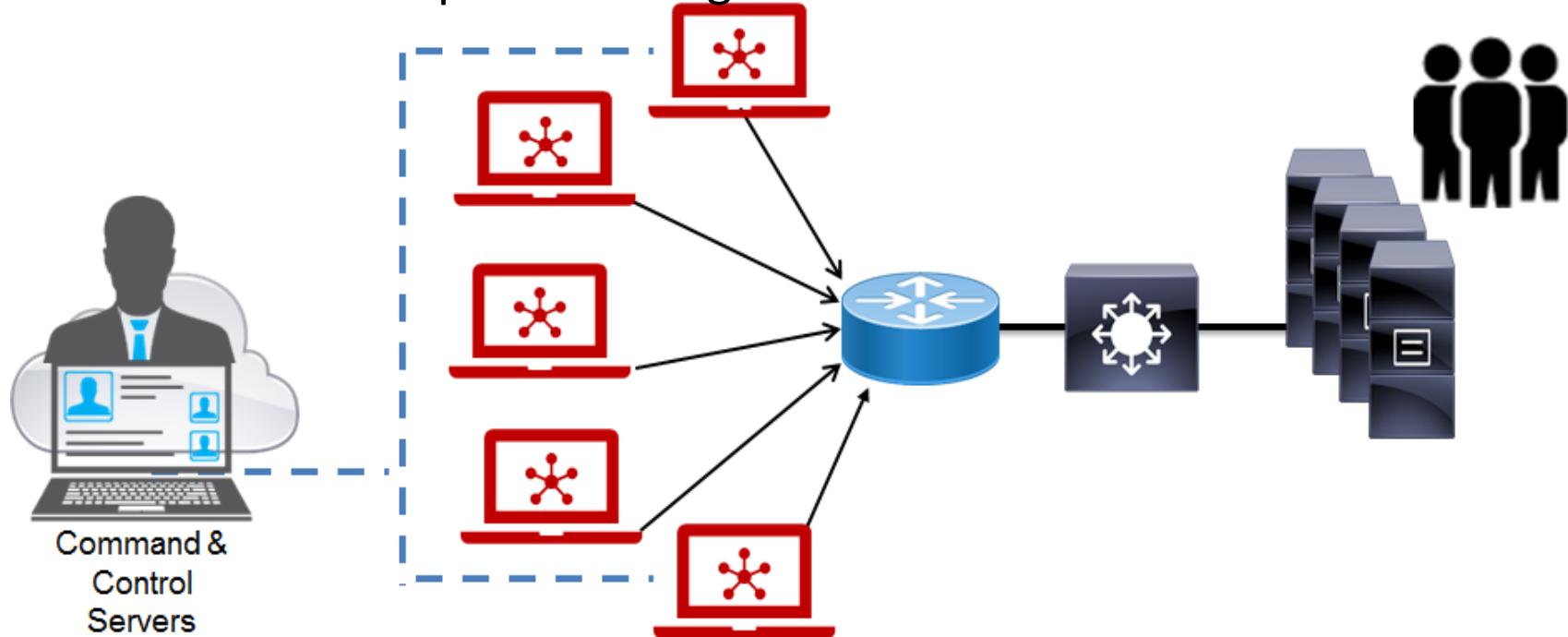
- After you combine your conditions into rules, you combine the rules into a web ACL
- This is where you define an action for each rule—allow, block, or count—**and a default action**



@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

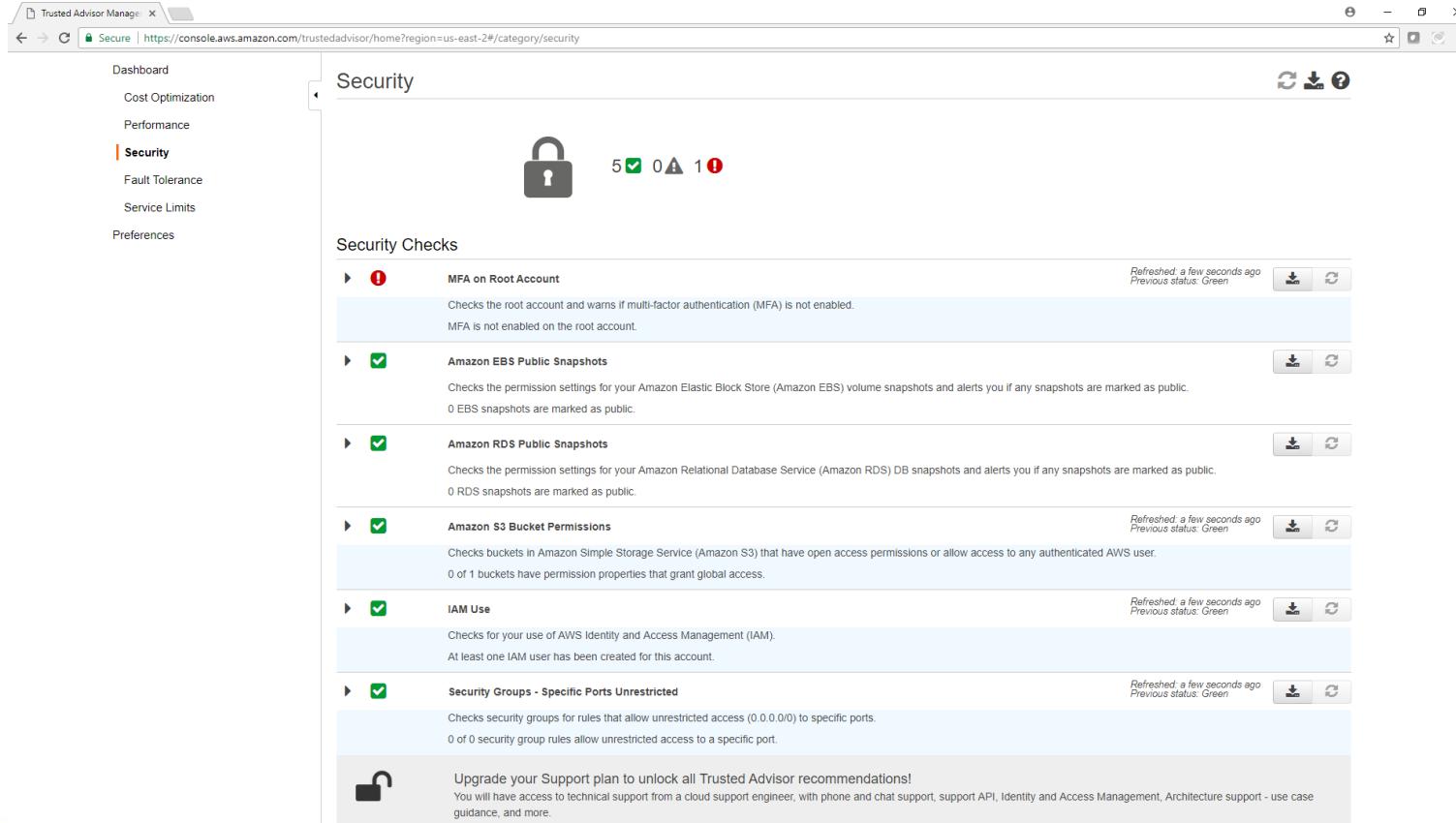
- AWS offers you a pay-as-you-go approach for pricing for over 120 cloud services
- With AWS you pay only for the individual services you need, for as long as you use them, and without requiring long-term contracts or complex licensing
- AWS pricing is similar to how you pay for utilities like water 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



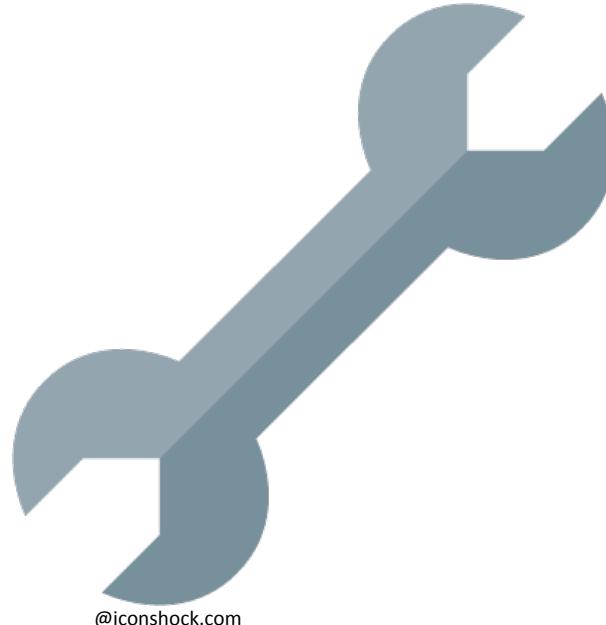
The screenshot shows the AWS Trusted Advisor Security dashboard. On the left, a sidebar menu includes Dashboard, Cost Optimization, Performance, Security (selected), Fault Tolerance, Service Limits, and Preferences. The main content area is titled "Security" and features a large lock icon with the status "5 ✓ 0 ⚠ 1 ⚠". Below this, the "Security Checks" section lists the following items:

- MFA on Root Account**: Checks if multi-factor authentication is enabled on the root account. Status: MFA is not enabled on the root account.
- Amazon EBS Public Snapshots**: Checks permission settings for Amazon EBS volume snapshots. Status: 0 EBS snapshots are marked as public.
- Amazon RDS Public Snapshots**: Checks permission settings for Amazon RDS DB snapshots. Status: 0 RDS snapshots are marked as public.
- Amazon S3 Bucket Permissions**: Checks buckets in Amazon S3 for open access permissions. Status: 0 of 1 buckets have permission properties that grant global access.
- IAM Use**: Checks for IAM users. Status: At least one IAM user has been created for this account.
- Security Groups - Specific Ports Unrestricted**: Checks security groups for unrestricted access rules. Status: 0 of 0 security group rules allow unrestricted access to a specific port.

At the bottom, a note states: "Upgrade your Support plan to unlock all Trusted Advisor recommendations! You will have access to technical support from a cloud support engineer, with phone and chat support, support API, Identity and Access Management, Architecture support - use case guidance, and more."

AWS Support Models

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



@iconshock.com

AWS Cloud Practitioner Course



Michael J.
Shannon

THANK YOU FOR
ATTENDING!

