AWS Security Essentials Course

Michael J. Shannon

CISSP and Certified Cloud Security Professional (CCSP)

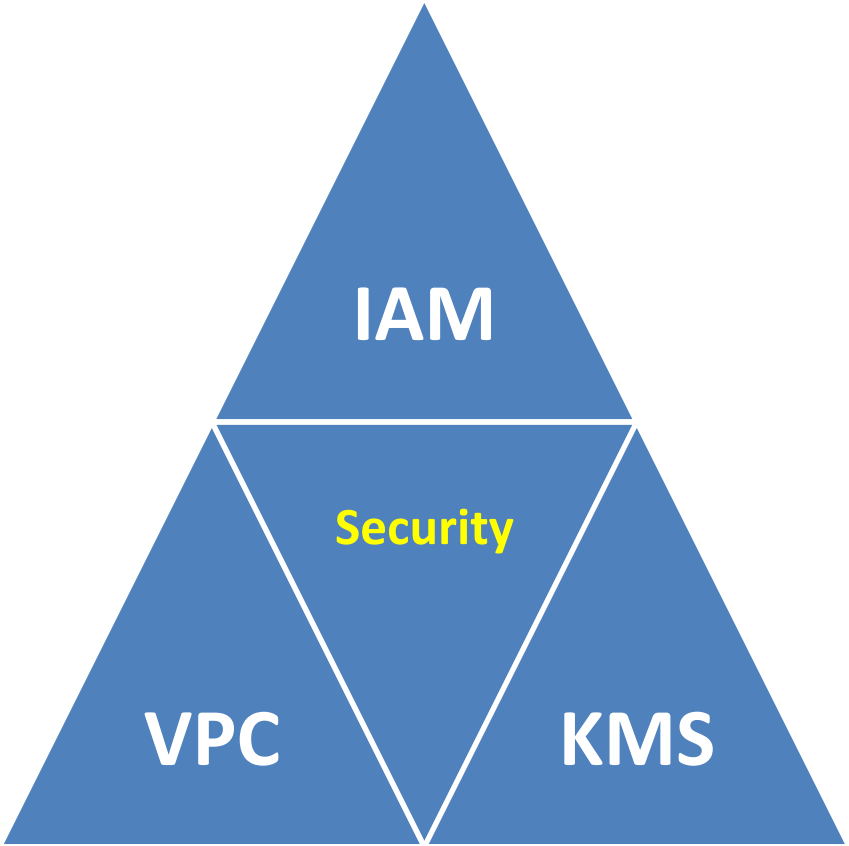
AWS Certified Security - Specialty

Cisco CCNP - Security

Palo Alto PNCSE7

ITIL 4 Managing Professional (MP)

The AWS Security Triad



key
management

AWS Well-Architected Security Pillar

- Encompasses the ability to protect information, systems, and assets
- Provides business value using solid risk assessment and mitigation strategies and techniques
- Implements several cloud design principles to strengthen system security

@iconshock.com

Well-Architected 5 Security Areas

- Identity and Access Management
- Detective Controls
- Infrastructure Protection
- Data Protection
- Incident Response

Security Design Principles in the Cloud

- Implement a strong security foundation
- Enable traceability
- Apply security at every layer
- Automate security best practices
- Protect data in transit and at rest
- Separate people from direct data access
- Prepare for security events and incidents

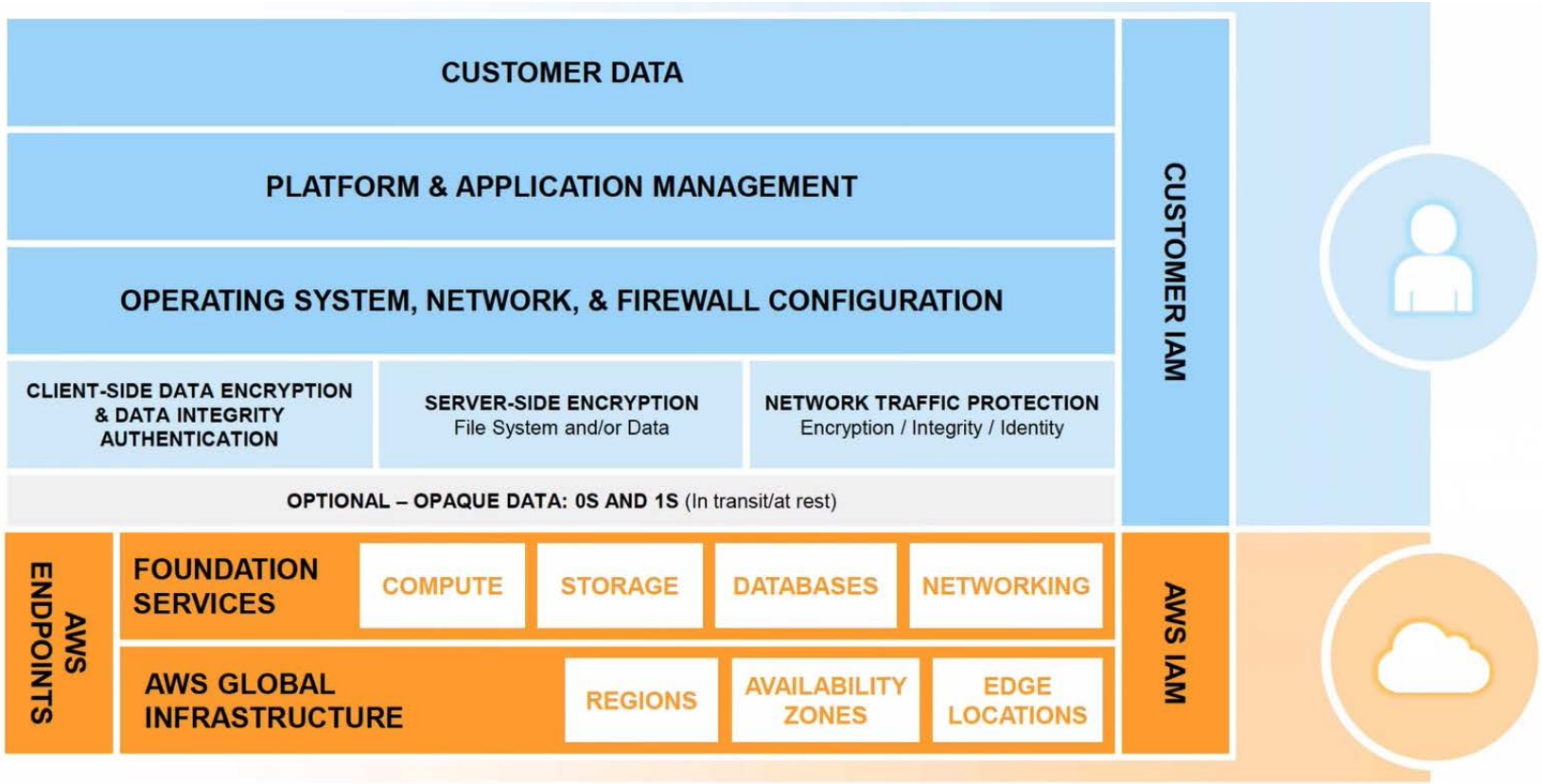
AWS Security Reference Architecture

- The AWS Security Reference Architecture (AWS SRA) is a holistic set of guidelines for deploying the full complement of AWS security services in a multi-account environment
- It can be used to help design, implement, and manage AWS security services so that they align with AWS best practices
- The overall architectural guidance complements detailed, service-specific recommendations such as those found on the AWS security website

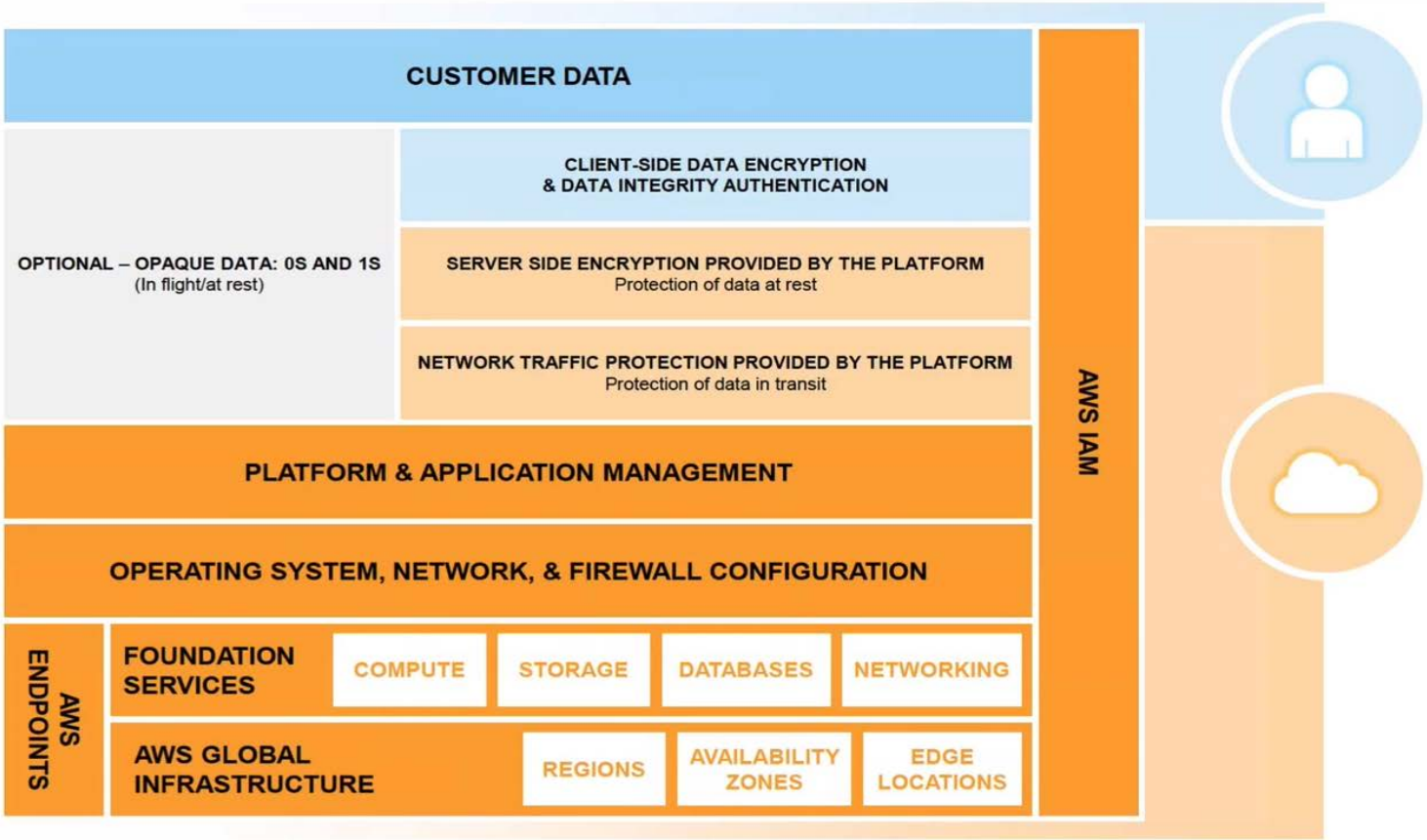
AWS Responsibilities

- AWS operates and manages the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.
- The AWS global infrastructure is designed to security best practices and security compliance standards on top of some of the most secure computing infrastructure in the world.
- AWS provides tools and information to assist customers in their efforts to account for and validate that controls are operating effectively in their extended IT environment.

Shared Responsibility with IaaS



Shared Responsibility with PaaS



Credentials: AWS Root Account

Mail - Brio Insurance Group | AWS Console - Signup

https://portal.aws.amazon.com/billing/signup?redirect_url=https%3A%2F%2Faws.amazo

Most Visited

aws

English

AWS Accounts Include 12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB

Visit **aws.amazon.com/free** for full offer terms

Create an AWS account

Email address

Password

Confirm password

AWS account name

Continue

Sign in to an existing AWS account

Privacy Policy | Terms of Use

Credentials: AWS Root Account

aws

Sign in

◉ **Root user**
Account owner that performs tasks requiring unrestricted access. Learn more

○ **IAM user**
User within an account that performs daily tasks. Learn more

Root user email address

username@example.com

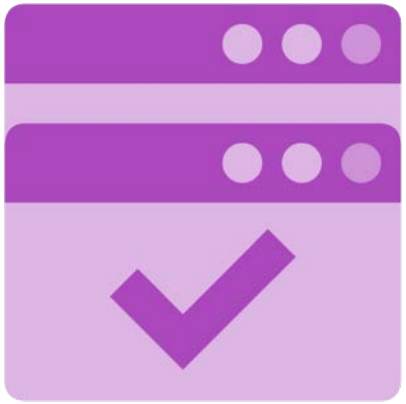
Next

New to AWS?

Create a new AWS account

AWS Root Account Distinctives

- Change root user details (password)
- Change Support Plan
- Payment options and billing
- Close an AWS account
- Sign up for GovCloud
- Create an Organization and Master Account
- Transfer Route 53 domain to another account



@iconshock.com

Credentials: AWS Root Account

- If you have generated an access key for your AWS root account, **strongly consider deleting it**
- Instead, use your account email address and password to sign into the AWS Management Console and create an IAM user for yourself that has administrative privileges

@iconshock.com

Credentials: AWS Root Account

- Rotate root account password regularly
- To **delete** (or rotate) your AWS account access keys, go to the Security Credentials page in the AWS Management Console
- Never share your AWS account password or access keys with anyone
- **Configure root account challenge questions** at https://console.aws.amazon.com/billing/home?#/account/

Signing Into Your Accounts

Your sign-in page URL has the following format, by default.

```
https://Your_AWS_Account_ID.signin.aws.amazon.com/console/
```

If you create an AWS account alias for your AWS account ID, your sign-in page URL will look like the following example.

```
https://Your_Alias.signin.aws.amazon.com/console/
```

Creating an Alias

IAM users sign-in link:

https://[redacted].signin.aws.amazon.com/console

| Customize

IAM Resources

Users: 1

Roles: 3

Groups: 1

Identity Providers: 0

Customer Managed Policies: 0

Create Account Alias

Account Alias

Cancel **Yes, Create**

Security Status

complete.

- Delete your root access
- Activate MFA on your ro
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy

My Security Credentials

aws Services Resource Groups mjshannawstest N. Virginia

My Account
My Organization
My Billing Dashboard
My Security Credentials
Sign Out

AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.

Example: Relational Database Service, database, RDS

Recently visited services

All services

Build a solution

Get started with simple wizards and automated workflows.

Access reso

Access the Management Console using the AWS Console Mobile App. Learn more

Explore AWS

Amazon RDS

Set up, operate, and scale your relational database in the cloud. Learn more

AWS Marketplace

Find, buy, and deploy popular software products that run on

My Security Credentials

- Password
- Multi-factor authentication (MFA)
- Access keys (access key ID and secret access key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the signing documentation . For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions

Create New Access Key

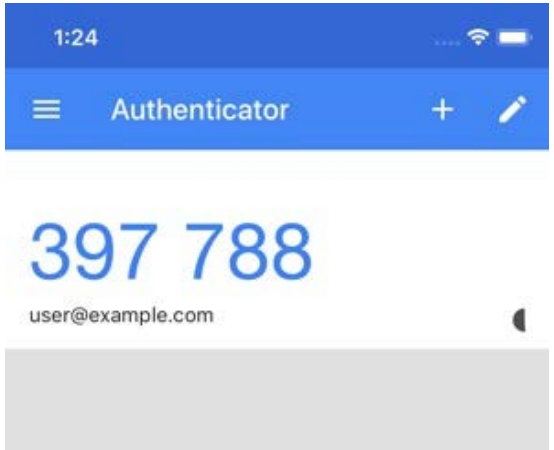
Important Change - Managing Your AWS Secret Access Keys

As described in a previous announcement, you cannot retrieve the existing secret access keys for your AWS root account, though you can still create a new root access key at any time. As a best practice, we recommend creating an IAM user that has access keys rather than relying on root access keys.

- CloudFront key pairs
- X.509 certificate
- Account identifiers

AWS Multi-Factor Authentication (MFA)

- Provide a six-digit single-use code in addition to your standard credentials before given access to the AWS Account settings or AWS services and resources
- AWS MFA supports the use of both hardware tokens and virtual MFA devices



TOTP Virtual authenticator apps

Android	Twilio Authy Authenticator, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator, Symantec VIP
iOS	Twilio Authy Authenticator, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator, Symantec VIP

Access Keys

- AWS requires that all API requests must include a digital signature to verify the requestor identity
- Offers message integrity and anti-replay protection
- Digital signature is calculated using a SHA256 cryptographic hash where the input includes the text of your request and you're a key derived from your secret access key (forward secrecy)
- With AWS SDKs to generate requests, the digital signature calculation is done for you

AWS Command Line Interface

AWS Command Line Interface

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

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

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

Getting Started »

CLI Reference »

GitHub Project »

Community Forum »

Windows

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

Mac and Linux

Requires Python 2.6.5 or higher.
Install using pip.

```
pip install awscli
```

Amazon Linux

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

Release Notes

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

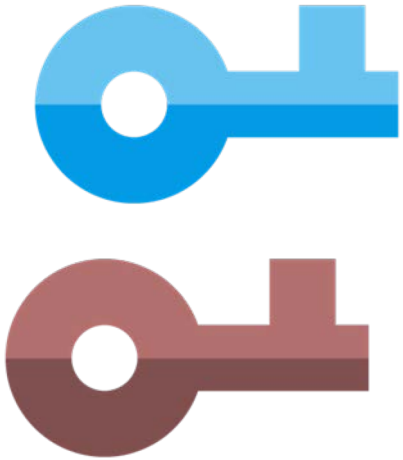
AWS Command Line Interface

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]:
```

Key Pairs in KMS



- AWS KMS has provided support for asymmetric keys
- You can generate, manage, and use public/private key pairs to protect your application data using the new APIs through the AWS SDK
- Keys can be generated as CMKs where the private piece never leaves the service, or as a data key where the private portion is returned to your calling application encrypted under a CMK.
- RSA 2048, RSA 3072, RSA 4096, ECC NIST P-256, ECC NIST P-384, ECC NIST-521, and ECC SECG P-256k1.

Key Pairs in KMS

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

Configure key

Step 1 of 5

Key type Help me choose

- Symmetric
  A single encryption key that is used for both encrypt and decrypt operations
- Asymmetric
  A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

Key usage Help me choose

- Encrypt and decrypt
  Key pairs for public key encryption
  Uses the public key for encryption and the private key for decryption.
- Sign and verify
  Key pairs for digital signing
  Uses the private key for signing and the public key for verification.

Cancel Next

AWS Secrets Manager

- Protect secrets used across all supported AWS services
- Allows you to rotate, manage, and retrieve:
  - Database credentials
  - API keys
  - Secrets throughout lifecycles
- Rotation schemes integrates with:
  - Amazon RDS for MySQL
  - Amazon RDS for PostgreSQL
  - Amazon Aurora

AWS Secrets Manager

- In March 2021 **multi-Region secrets** were introduced to replicate secrets for multi-region workloads
- Three new rules were added to **AWS Config** to help admins verify that secrets are configured based on organizational requirements
- There is now a higher secrets hard limit of 500,000 per account

Secrets Manager

- (selected) Credentials for Amazon RDS database
- Credentials for Amazon DocumentDB database
- Credentials for Amazon Redshift cluster
- Credentials for other database
- Other type of secret
  API key, OAuth token, other.

Credentials Info

User name

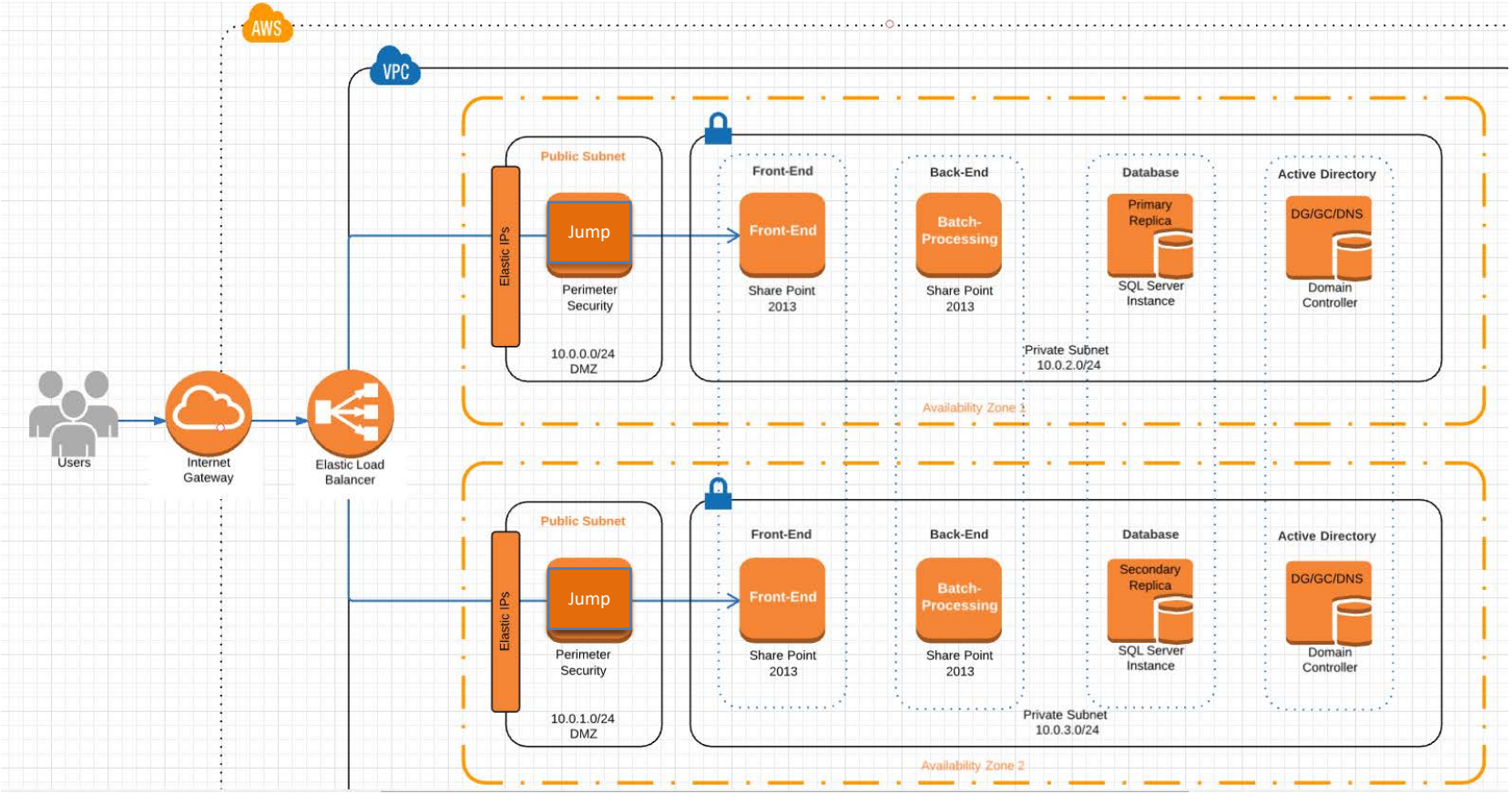
Password

Show password

Encryption key Info

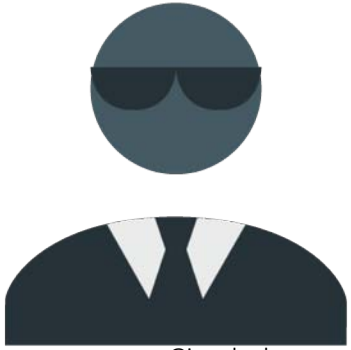
You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

Using a Bastion Host (Jump Box)



AWS Systems Manager

- Systems Manager enables you to manage servers running on AWS and in your on-premises data center through a single interface
- It securely communicates with a lightweight agent installed on your servers to execute management tasks
- This helps you manage resources for Windows and Linux operating systems running on Amazon EC2 or on-premises



@iconshock.com

AWS Session Manager

@iconshock.com

- You can easily and securely access your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS CLI without having to open inbound ports, maintain bastion hosts, or manage SSH keys
- You can find this service in AWS Systems Manager

AWS Systems Manager

aws | Services | Resource Groups | compitoTest @ 5891-9160-3537 | N. Virginia | Support

AWS Systems Manager

- Operations Management
  - CloudWatch Dashboard
  - OpsCenter
  - Resource Groups
  - Trusted Advisor & PHD
- Actions & Change
  - Automation
  - Maintenance Windows
- Instances & Nodes
  - Compliance
  - Inventory
  - Managed Instances
  - Hybrid Activations
  - Session Manager
  - Run Command
  - State Manager
  - Patch Manager
  - Distributor
- Shared Resources
  - Parameter Store
  - Documents

AWS Systems Manager > Compliance

Compliance dashboard filtering

Group dashboard results based on

- (●) Compliance type
- ( ) Patch group
- ( ) Resource group

Filter further [ ] Resources ◯ Rules

Compliance resources summary

1

Compliance type	Compliant resources	Non-Compliant resources	Critical resources	High resources	Medium resources	Low resources	Informational resources	Unspecified resources
Association	2	4	0	0	0	0	0	4

Details overview for resources

Resource

1 2

Compliance | Overall

Systems Manager Incident Manager

- Offers powerful techniques for managing all kinds of security incidents including operational and availability issues
- Can automatically act upon CloudWatch alarms
- Runs pre-configured response plans and engages with first responders through SMS and phone calls
- Can enable chat commands and notifications using AWS Chatbot
- Runs automation workflows with Systems Manager Automation runbooks

Systems Manager Incident Manager

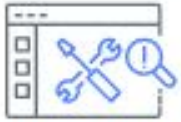
AWS Chatbot
Enable teams to use chat to monitor and respond.

Escalation plans + Contacts
Multi-stage plans to define when people get engaged.

Runbooks
Create blueprints for incident mitigation.

Amazon CloudWatch
Use monitoring to start an incident the moment they are triggered.

Response plans
Be prepared by defining templates that engage responders and activate a runbook at the time of detection.



Incident + Analysis
Collect information to diagnose, remediate, and learn from incidents.

AppStream 2.0

- An SSO dynamic bastion solution
- AppStream spins-up fresh instances each time a user requests access
- As soon as the session closes and the Disconnect Timeout period is reached, AppStream terminates the instance

Segment 2: Identity and Access Management (IAM) & AWS SSO

AWS Recommends Single Sign-On!

There is a better way to connect your existing directory and give your users access across AWS
AWS IAM Identity Center (successor to AWS Single Sign-On) offers a better way to connect or create a workforce directory, and to manage users' access to multiple AWS accounts, AWS applications, and SAML 2.0-based cloud applications. Learn more

Go to IAM Identity Center

IAM dashboard

Security recommendations

Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

AWS Account

Account ID

Account Alias

shan-can-do-aws Edit | Delete

Sign-in URL for IAM users in this account

Identity and Access Management (IAM)

- A user can be any individual, system, or application that interacts with AWS resources, either programmatically or through the AWS Management Console or AWS CLI
- Use your AWS account root user email address and password to sign in to the IAM console at: https://console.aws.amazon.com/iam/
- In the navigation pane, choose Users and then Add user.
- For User name, type a user name, such as **Administrator**.

IAM Password Policies

IAM Management Console | Understanding and Gettin...

https://console.aws.amazon.com/iam/home?region=us-east-2#/account_settings

aws | Services | Resource Groups

Search IAM

- Dashboard
- Groups
- Users
- Roles
- Policies
- Identity providers
- **Account settings**
- Credential report

- Encryption keys

Password Policy

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: 6

- [ ] Require at least one uppercase letter
- [ ] Require at least one lowercase letter
- [ ] Require at least one number
- [ ] Require at least one non-alphanumeric character
- [x] Allow users to change their own password
- [ ] Enable password expiration

  Password expiration period (in days):
- [ ] Prevent password reuse

  Number of passwords to remember:
- [ ] Password expiration requires administrator reset

Apply password policy | Delete password policy

IAM (continued)

IAM Management Console

https://console.aws.amazon.com/iam/home#/users$new?step=details

Most Visited

aws Services Resource Groups shankhantoo Global Support

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* Administrator

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type*
- Programmatic access
  Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- AWS Management Console access
  Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*
- Autogenerated password
- Custom password

••••••••••••

Show password

Feedback English (US)

 Privacy Policy Terms of Use

IAM (continued)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ○ Autogenerated password
◉ Custom password

••••••••••••

☐ Show password

Require password reset ☐ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required

Cancel | Next: Permissions

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

IAM (continued)

IAM Management Console

https://console.aws.amazon.com/iam/home#/users$new?step=permissions&accessK

Most Visited

Search

aws Services Resource Groups shankhantoo Global Support

Add u

Set per

Add

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name: Admins

Create policy | Refresh

Filter: Policy type | Search | Showing 311 results

	Policy name	Type	Attachments	Description
✓	AdministratorAccess	Job function	0	Provides full access to AWS services and resources.
	AlexaForBusinessDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services
	AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to relate...
	AlexaForBusinessGatewayExe...	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
	AlexaForBusinessReadOnlyAc...	AWS managed	0	Provide read only access to AlexaForBusiness services
	AmazonAPIGatewayAdministra...	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gateway v...

Cancel | Create group

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

IAM (continued)

IAM Management Console

https://console.aws.amazon.com/iam/home#/users$new?step=review&accessKey&log

Most Visited

Search

aws Services Resource Groups shankhantoo Global Support

Details Permissions Review Complete

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	Administrator
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	Admins

IAM (continued)

IAM Management Console

https://console.aws.amazon.com/iam/home#/users$new?step=final&accessKey&log

Most Visited

aws Services Resource Groups shankhantoo Global Support

Add user

1 Details 2 Permissions 3 Review 4 Complete

Success

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

Users with AWS Management Console access can sign-in at: https://[redacted]4.signin.aws.amazon.com/console

Download .csv

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

Close

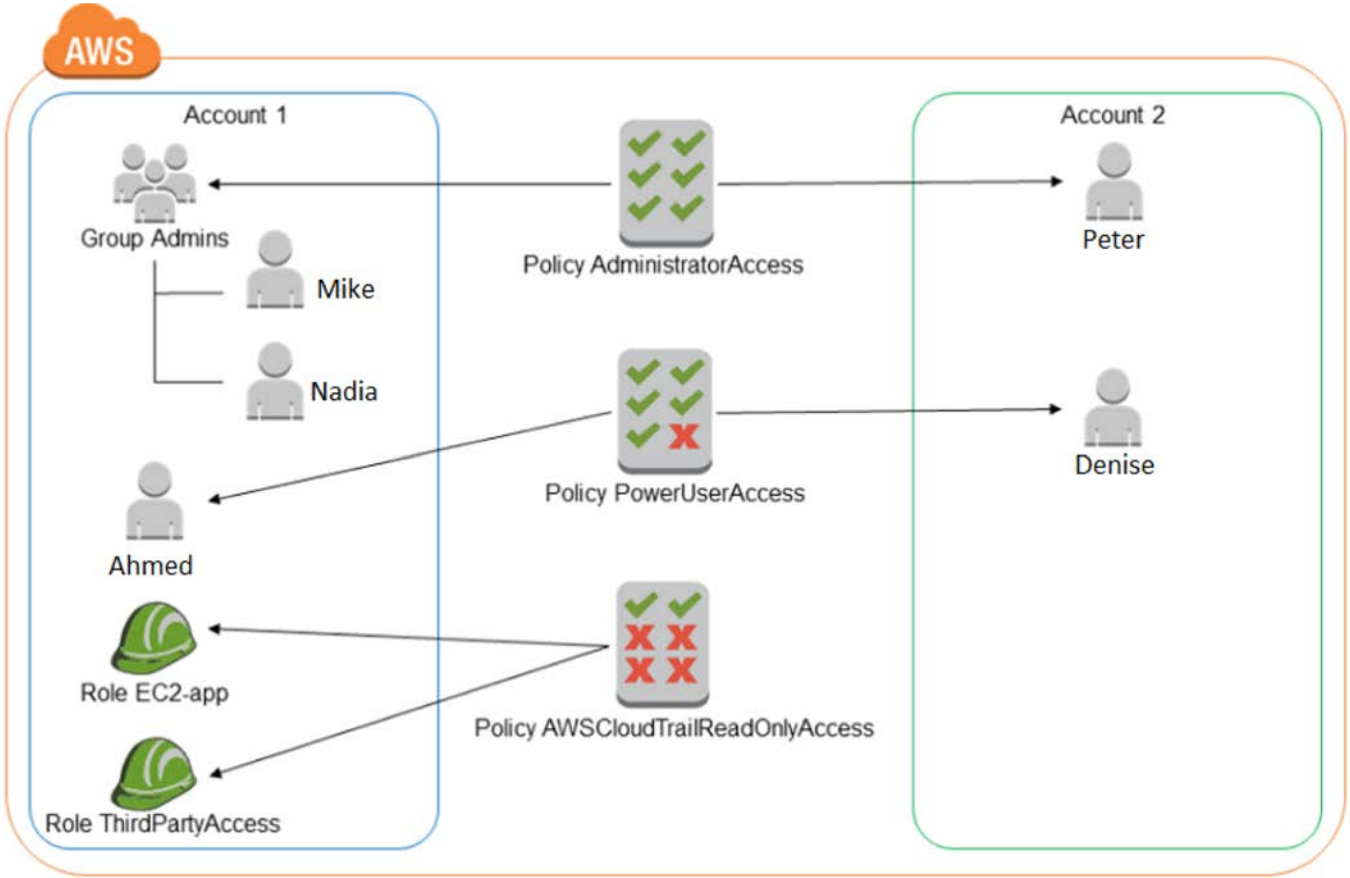
Feedback English (US)

 Privacy Policy Terms of Use

AWS 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

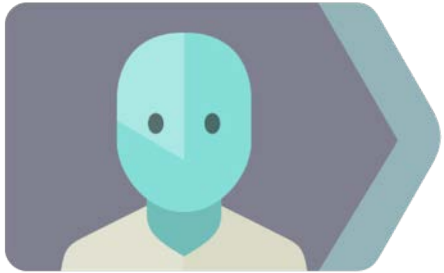
AWS Managed Policies



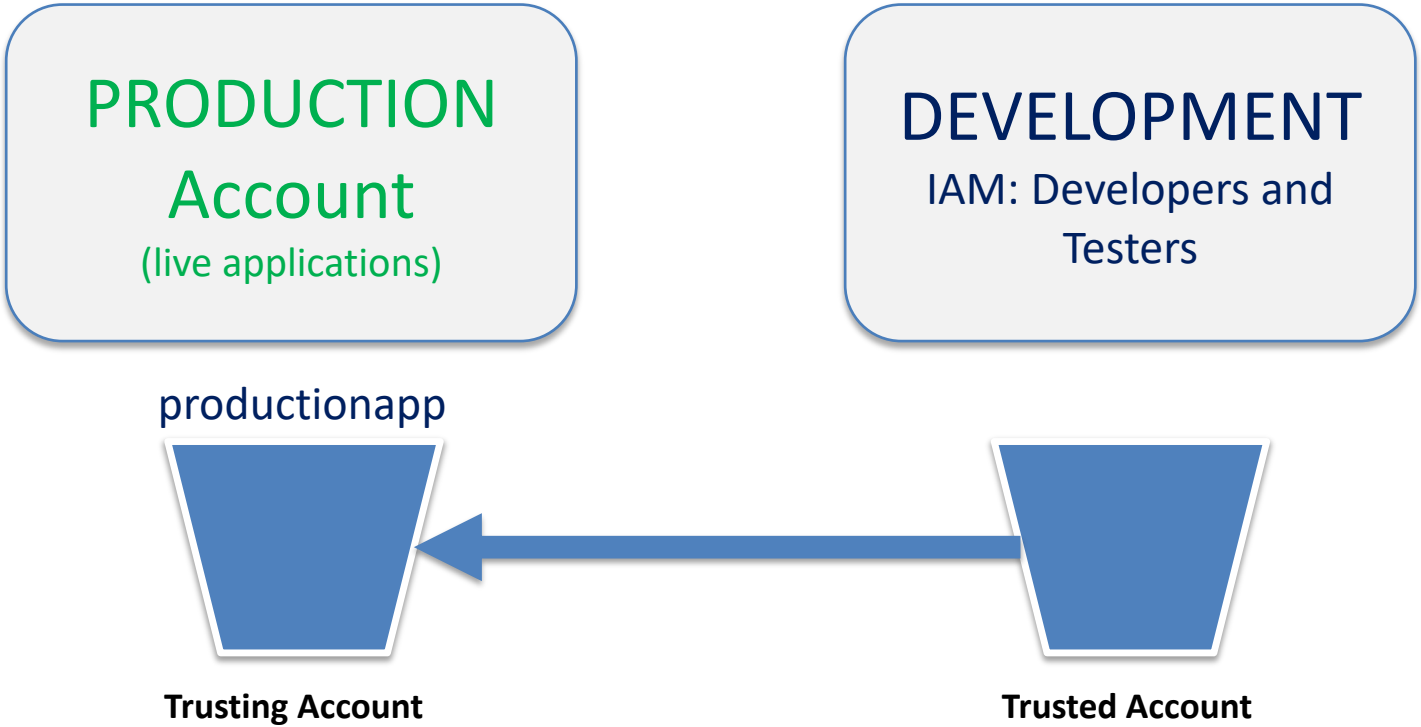
IAM Roles

- 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

Role Use Cases



- Provide access for an IAM user in one AWS account that you own to access resources in another account that you own
- Provide access to IAM users in AWS accounts owned by 3rd parties
- Provide access for services offered by AWS to other AWS cloud resources
- Provide access for externally authenticated users



Assigning a Role to GCP Operations

Stackdriver Select workspace

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.

Roles with Another AWS Account

Services Resource Groups mjshannawstest

Create role

1 2 3 4

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows entities in other accounts to perform actions in this account. Learn more

Specify accounts that can use this role

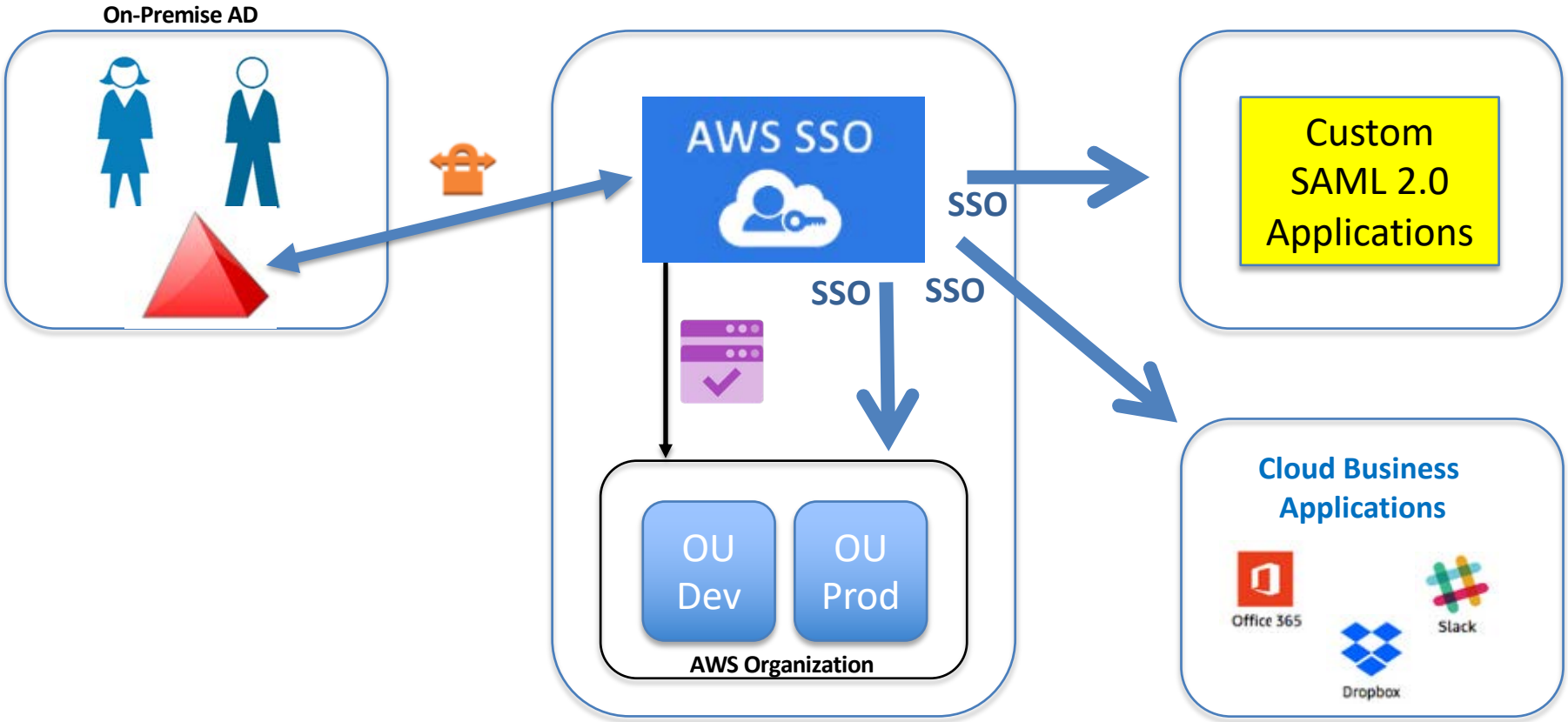
Account ID*

This field is required.

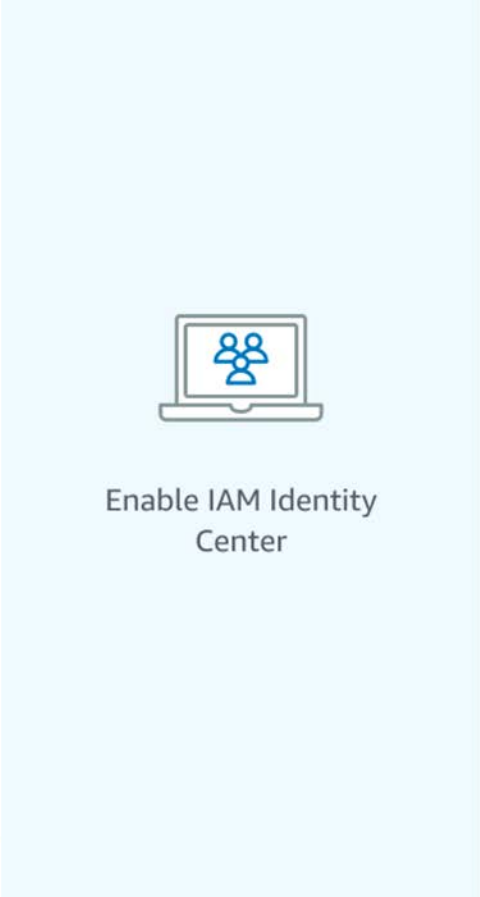
Options

- Require external ID (Best practice when a third party will assume this role)
- Require MFA

AWS IAM Identity Center



IAM Identity Center



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)

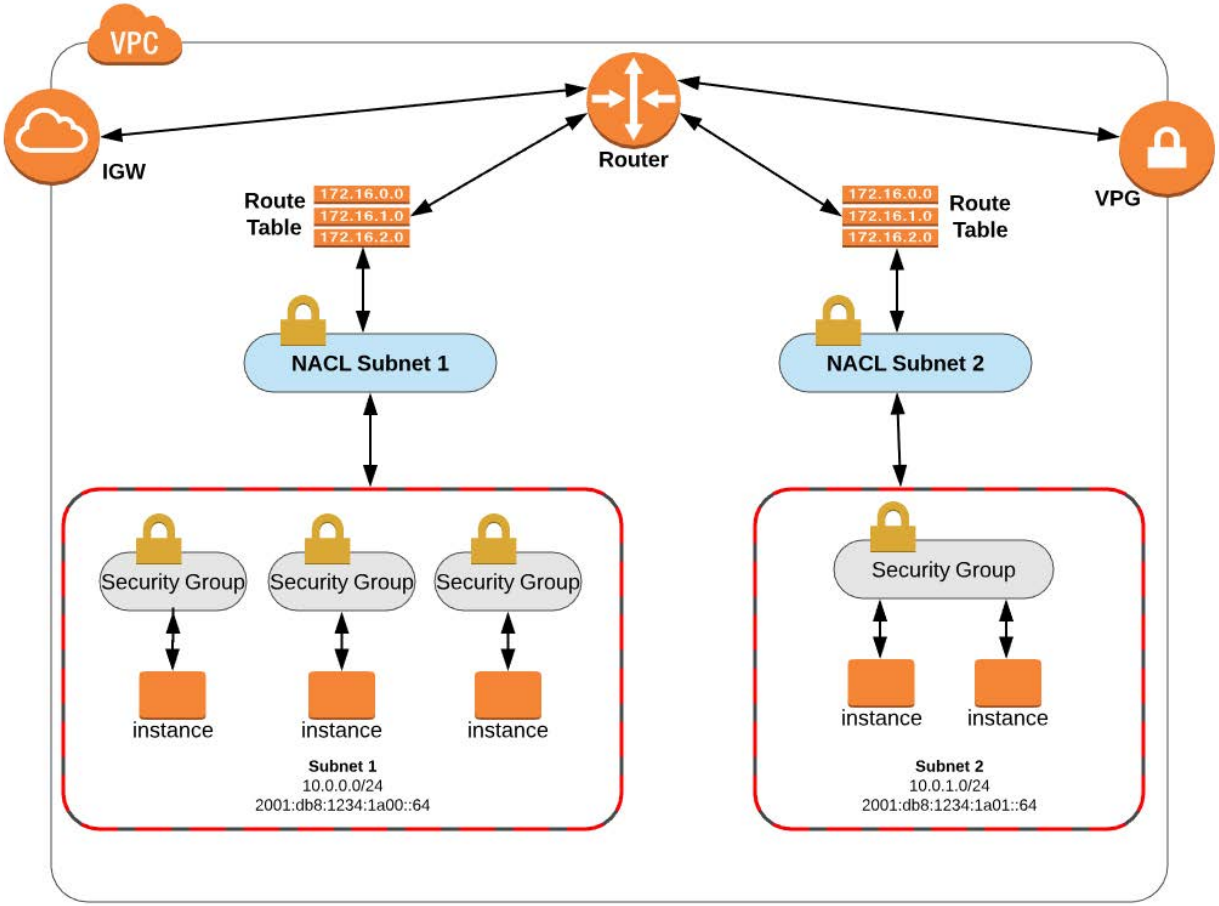
SecurityAudit

Terms of Use

Powered by aws

Segment 3: Infrastructure Security

Security Begins with Subnet Design



The New VPC Wizard

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

- ○ VPC only
- ◉ VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

project

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

IPv6 CIDR block Info

- ◉ No IPv6 CIDR block
- ○ Amazon-provided IPv6 CIDR block

Preview

VPC Show details

Your AWS virtual network

project-vpc

Subnets (4)

Subnets within this VPC

us-east-1a

project-subnet-public1-us-east-1a

project-subnet-private1-us-east-1a

us-east-1b

project-subnet-public2-us-east-1b

project-subnet-private2-us-east-1b

The New VPC Wizard

Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1	2	3

▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0	2

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0	2	4

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ

Preview

VPC Show details

Your AWS virtual network

project-vpc

Subnets (4)

Subnets within this VPC

us-east-1a

project-subnet-public1-us-east-1a

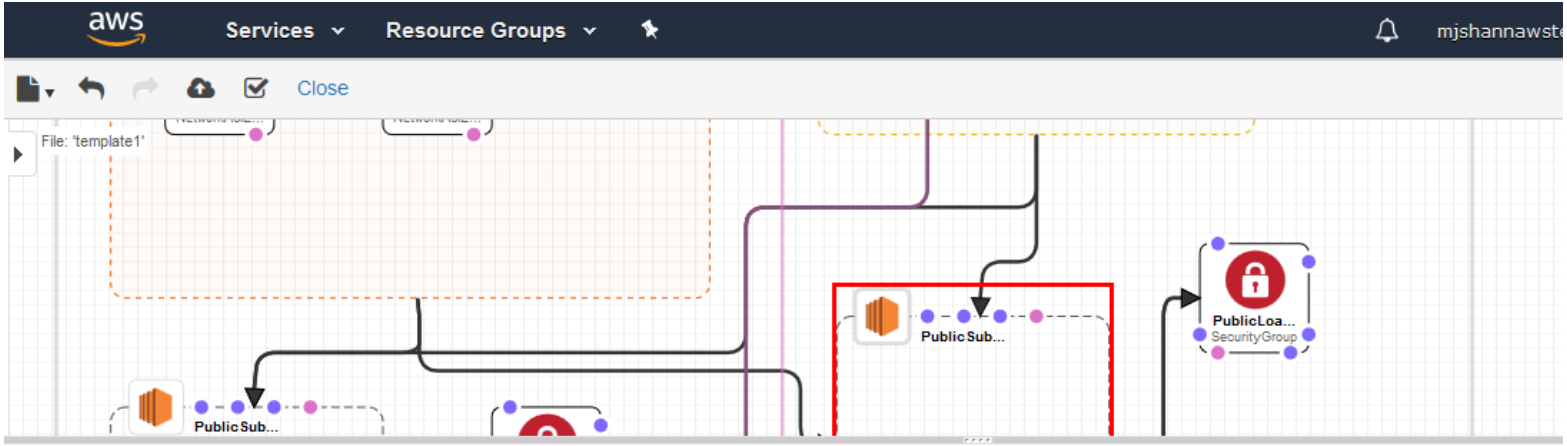
project-subnet-private1-us-east-1a

us-east-1b

project-subnet-public2-us-east-1b

project-subnet-private2-us-east-1b

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             "MinLength": "9",
14
```

Automate Detective Controls with CloudFormation

- The Well-Architected initiative recommends automating the deployment of detective controls using CloudFormation
- This involves several key services including:
  - **AWS CloudTrail** – an API monitoring service that allows for governance, compliance, operational auditing, and risk auditing of your AWS account
  - **Amazon GuardDuty** - a threat detection service that continuously monitors for malicious or unauthorized behavior
  - **AWS Config** - a service that lets you assess, audit, and evaluate the configurations of your AWS resources

Automating with CloudFormation

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

- (●) Template is ready
- ( ) Use a sample template
- ( ) Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

- ( ) Amazon S3 URL
- (●) Upload a template file

Upload a template file

Choose file *cloudtrail-config-guardduty.yaml*

JSON or YAML formatted file

S3 URL: https://s3-external-1.amazonaws.com/cf-templates-1c6to6cae8gek-us-east-1/2020063jU4-cloudtrail-config-guardduty.yaml

View in Designer

Automating with CloudFormation

Stack name

DetectiveControls

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

General

CloudTrail

Configure AWS CloudTrail. If you have previously enabled CloudTrail select No.

Yes

Config

Configure AWS Config. If you have previously enabled Config select No.

Yes

GuardDuty

Configure Amazon GuardDuty. If you have previously enabled GuardDuty select No.

Yes

Automating with CloudFormation

S3AccessLogsBucketName

Optional: The name of an existing S3 bucket for storing S3 Access Logs. Leave blank for no S3 access logs.

Cloudtrail

CloudTrail

CloudTrailBucketName

The name of the new S3 bucket to create for CloudTrail to send logs to. Can contain only lower-case characters, numbers, periods, and dashes.Each label in the bucket name must start with a lowercase letter or number.

mjshannCWtestbucket

CloudTrailCWLogsRetentionTime

Number of days to retain logs in CloudWatch Logs. 0=Forever. Default 1 year, note logs are stored in S3 default 10 years

365

CloudTrailS3RetentionTime

Number of days to retain logs in the S3 Bucket before they are automatically deleted. Default is ~ 10 years

3650

CloudTrailEncryptS3Logs

OPTIONAL: Use KMS to enrypt logs stored in S3. A new key will be created

Yes

Automating with CloudFormation

CloudTrailLogS3DataEvents

OPTIONAL: These events provide insight into the resource operations performed on or within S3

No

Config

ConfigBucketName

The name of the S3 bucket Config Service will store configuration snapshots in. Each label in the bucket name must start with a lowercase letter or number.

mjshannCWtestbucketSnapshots

ConfigSnapshotFrequency

AWS Config configuration snapshot frequency

One_Hour

ConfigS3RetentionTime

Number of days to retain logs in the S3 Bucket before they are automatically deleted. Default is ~ 10 years

3650

GuardDuty

GuardDutyEmailAddress

Enter the email address that will receive the alerts

someone@example.com

Automating with CloudFormation

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more.

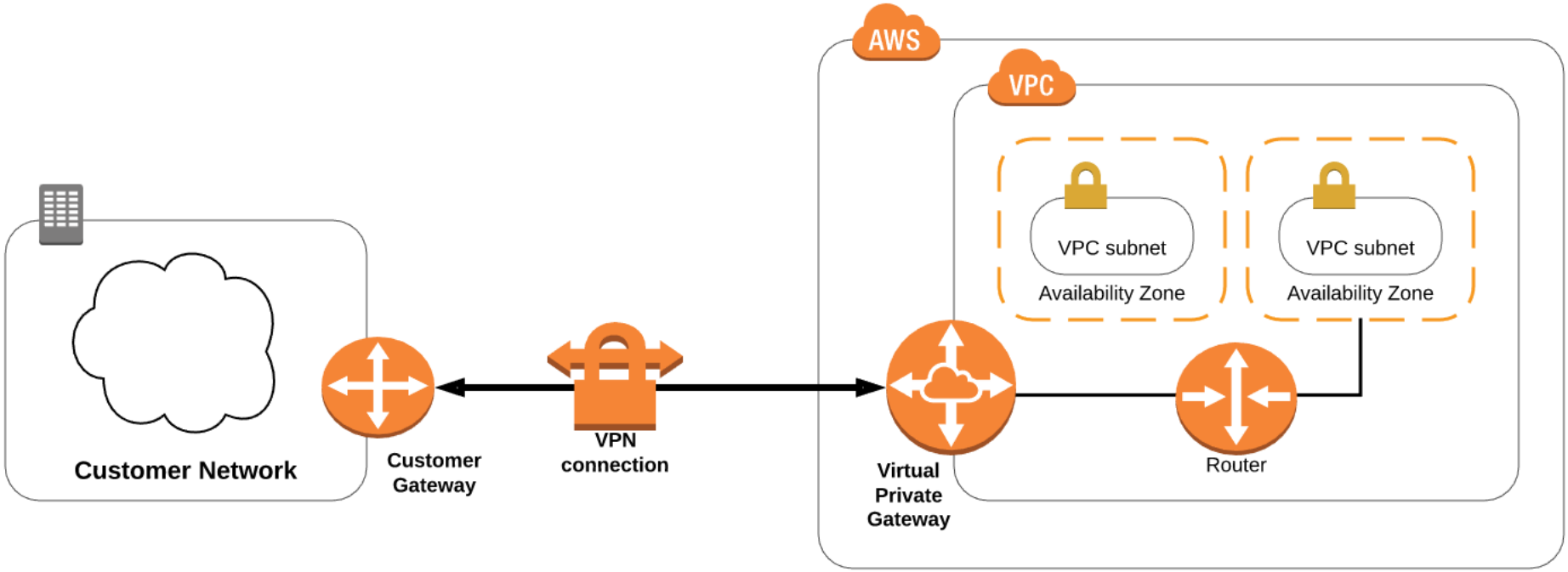
☑ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

Cancel | Previous | Create change set | **Create stack**

AWS Site-to-Site (Managed) VPNs

- Instances that you launch into a VPC can't communicate with your own (remote) network by default.
- In a VPC, a VPN connection refers to the connection between your VPC and your own network.
  1. Attach a virtual private gateway to the VPC
  2. Create a custom route table
  3. Update the security group rules
  4. Create an AWS managed VPN connection

Single VPN Connection



AWS Site-to-Site VPN

Route Tables See all regions	US East 1	Network ACLs See all regions	US East 2
Internet Gateways See all regions	US East 1	Security Groups See all regions	US East 2
Egress-only Internet Gateways See all regions	US East 0	Customer Gateways See all regions	US East 0
DHCP option sets See all regions	US East 1	Virtual Private Gateways See all regions	US East 0
Elastic IPs See all regions	US East 2	Site-to-Site VPN Connections See all regions	US East 0
Endpoints See all regions	US East 3	Running Instances See all regions	US East 0
Endpoint Services See all regions	US East 0		

Additional Information

VPC Documentation

All VPC Resources

Forums

Report an Issue

AWS Network Manager

AWS Network Manager centrally manages your Cloud WAN core network and your Transit Gateway network across AWS and on-premises locations. Learn more

Get started with Network Manager

Site-to-Site VPN Connections

Amazon VPC enables you to use your own isolated resources within the AWS Cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

Create VPN Connection

Create Customer Gateway

aws Services Resource Groups

Customer Gateways > Create Customer Gateway

Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

Name

Routing
- ○ Dynamic
- ◉ Static

IP Address e.g. 1.1.1.1

Certificate ARN Select Certificate ARN

Device Optional

* Required

Cancel | Create Customer Gateway

Using AWS Certificate Manager

AWS Certificate Manager > Certificates > Request certificate

Request certificate

Certificate type Info

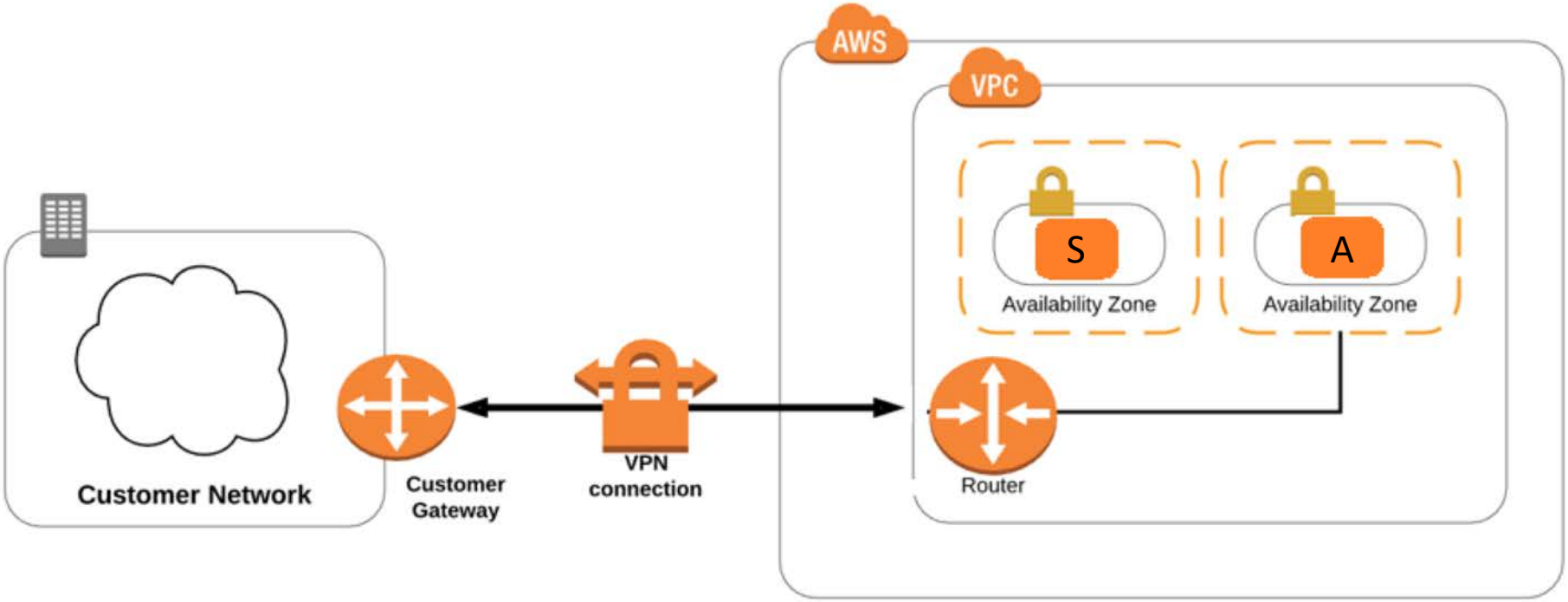
ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for acm to provide.

- (●) Request a public certificate
  Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.
- ( ) Request a private certificate
  No private CAs available for issuance.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit AWS Private Certificate Authority

Cancel Next

EC2 Instance to Terminate VPN



AWS Marketplace

aws marketplace

AMI & SaaS

View Categories | Your Saved List | Sell in AWS Marketplace | Amazon Web

- [x] Fortinet Inc. (20)
- [x] Cisco (9)
- [ ] F5 Networks (22)
- [ ] Center for Internet Security (20)
- [ ] ZOHO Corporation Private Limited (13)
- [ ] Anitian (12)
- [ ] Barracuda Networks (12)
- [ ] Gemalto (11)
- [ ] Buddha Labs (10)
- [ ] Symantec (10)

Operating System

+ All Linux/Unix

Software Pricing Plans

- [ ] Hourly (9)
- [ ] Annual (8)
- [ ] Bring Your Own License (16)
- [ ] By Units (4)

Software Free Trial

- [ ] Free Trial (6)

FORTINET

Free Trial

Fortinet FortiGate Next-Generation Firewall

★★★★★ (14) | Version v6.0.0 | Sold by Fortinet, Inc.

Starting from **$0.30/hr** or from **$1,995.00/yr** (up to 24% savings) for software + AWS usage fees

FortiGate Next-Generation Firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security...

Linux/Unix, Other v6.0.0 - 64-bit Amazon Machine Image (AMI)

CISCO

Free Trial

Cisco Cloud Services Router (CSR) 1000V - Security Pkg. Max Performance

★★★★★ (0) | Version 16.7.1 | Sold by Cisco Systems, Inc.

Starting from **$0.54/hr** or from **$1,942.00/yr** (59% savings) for software + AWS usage fees

The Security Technology Package for Maximum Performance version of Cisco Cloud Services Router (CSR1000V) delivers the maximum VPN/firewall performance in the AWS cloud, by...

Linux/Unix, Other Cisco IOS XE - 64-bit Amazon Machine Image (AMI)

CISCO

Free Trial

Cisco Adaptive Security Virtual Appliance (ASAv) - Standard Package

★★★★★ (6) | Version 9.9.2.1 | Sold by Cisco Systems, Inc.

Starting from **$0.69/hr** or from **$4,125.00/yr** (32% savings) for software + AWS usage fees

As you transform more workloads and functions into virtualized assets, you need the same protections that are available for your physical assets. Cisco has developed a virtual...

Linux/Unix, Other 9.9.1-2 - 64-bit Amazon Machine Image (AMI)

AWS Client VPN Endpoints

aws Services Resource Groups

Client VPN Endpoints > Create Client VPN Endpoint

Create Client VPN Endpoint

Create a new Client VPN endpoint to enable clients to access networks over a TLS VPN session

Name Tag

Description

Client IPv4 CIDR*

Authentication Information

Server certificate ARN*

Authentication Options Choose one or more authentication methods from below

- [x] Use mutual authentication
- [x] Use user-based authentication
  - (•) Active Directory authentication

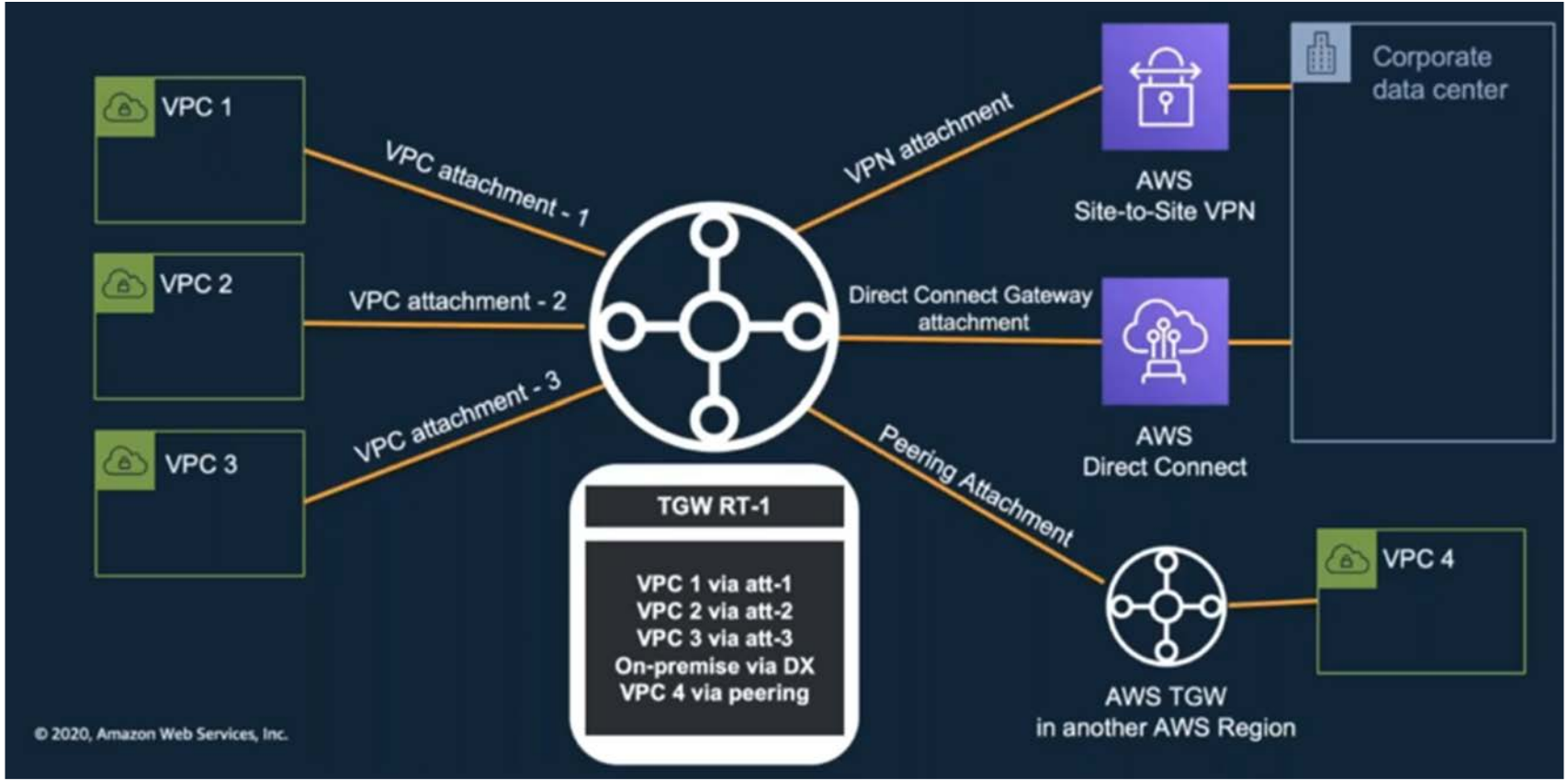
Client certificate ARN*

Directory ID*

AWS Transit Gateway

- **AWS Transit Gateway** allows customers to connect their VPCs and their on-premises networks to a single gateway
- You can easily to scale your networks across multiple accounts and Amazon VPCs to keep up with growth
- You only need to create and manage a single connection (hub) from the central gateway to each VPC, on-premises data center, or remote office across your network
- Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other network that is connected to the Gateway

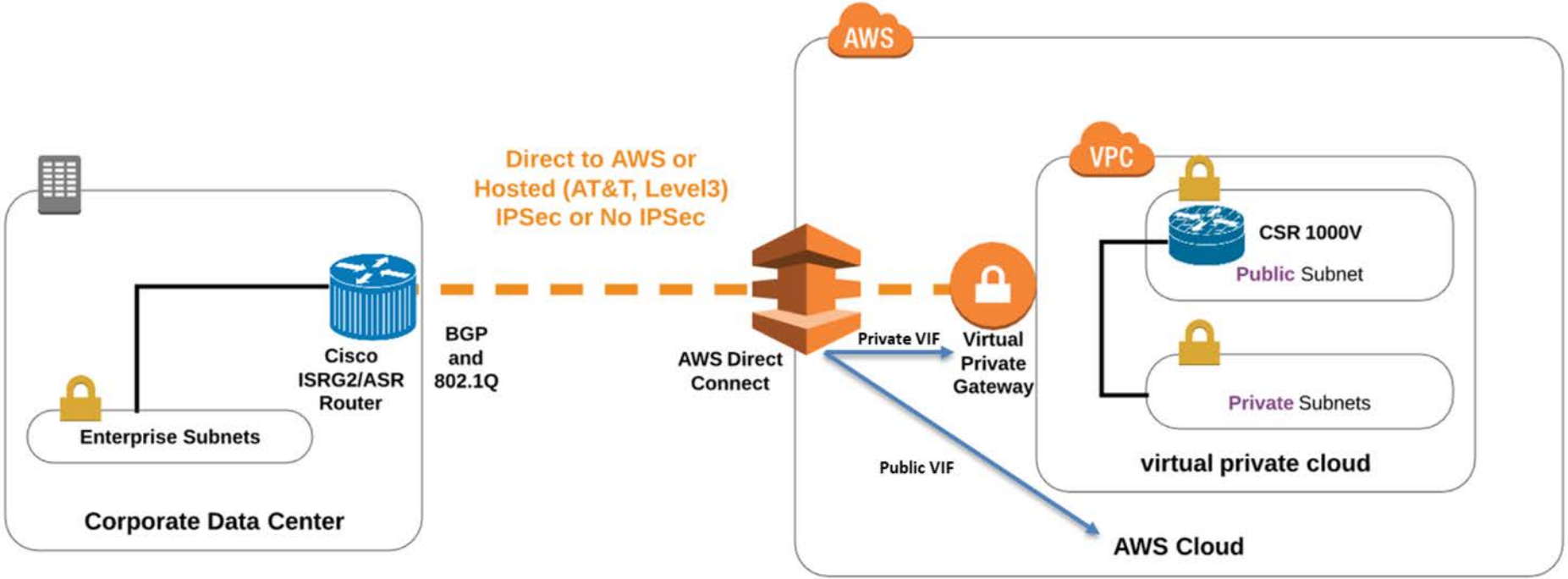
AWS Transit Gateway



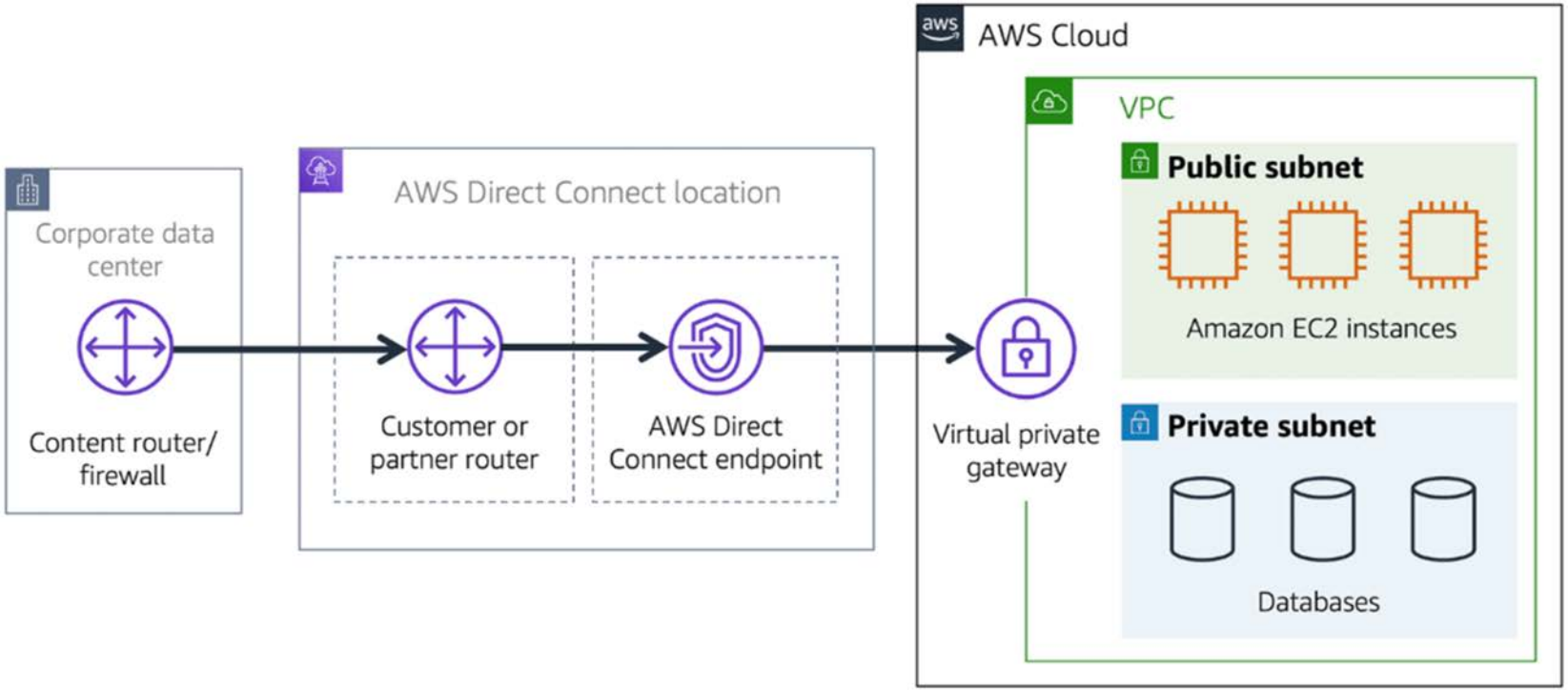
AWS Direct Connect

- AWS Direct Connect provides an alternative to using the Internet to utilize AWS cloud services
- Establishes private connectivity between AWS and your datacenter, office, or colocation environment
- Private network connections may reduce costs, increase bandwidth, and provide a more consistent network experience than Internet-based connections
- All AWS services (e.g. Amazon EC2/VPC, S3, and DynamoDB) can be used with Direct Connect

AWS Direct Connect



AWS Direct Connect



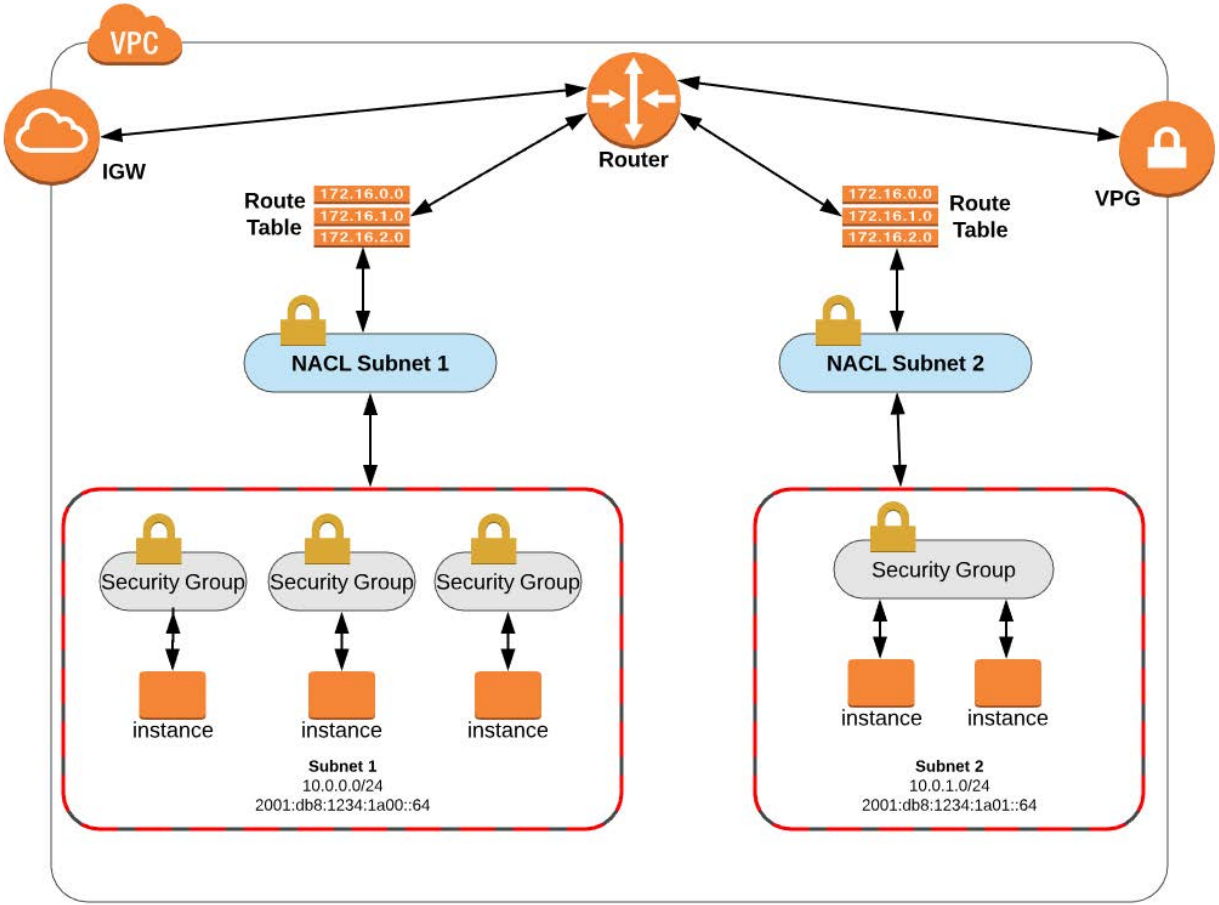
AWS Direct Connect

AWS Direct Connect Location	Campus Location also accessible from	Associated AWS Region	Location-specific features
Cologix COL2, Columbus, OH****		US East (Ohio)	100 Gbps available 100 Gbps MACsec supported 10 Gbps MACsec supported
Cologix MIN3, Minneapolis, MN		US East (Ohio)	
CyrusOne West III, Houston, TX	CyrusOne West I - III, Houston	US East (Ohio)	100 Gbps available
Equinix CH2, Chicago, IL	Equinix CH1 - CH2 & CH4, Chicago	US East (Ohio)	100 Gbps supported 100 Gbps MACsec supported
Netrality Properties 1102 Grand, Kansas City, MO		US East (Ohio)	
QTS, Chicago, IL		US East (Ohio)	10 Gbps MACsec supported
165 Halsey Street, Newark, NJ		US East (Virginia)	100 Gbps available 100 Gbps MACsec supported 10 Gbps MACsec supported

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:

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	Availabi
Private subnet	subnet-f55f558e	available	vpc-63864f0b | MY-VPC	10.0.1.0/24	251		us-east-
	subnet-0e6d6575	available	vpc-1f30fc77	172.31.16.0/20	4090		us-east-
	subnet-e71758aa	available	vpc-1f30fc77	172.31.32.0/20	4091		us-east-
Public subnet	subnet-dc5852a7	available	vpc-63864f0b | MY-VPC	10.0.0.0/24	250		us-east-

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)

Privacy Policy Terms of Use

NACLs

Subnets | VPC Management Co | Network ACLs | VPC Managem

https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#acls:filter=acl-c37

Most Visited

aws | Services | Resource Grou | 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 Network ACL

acl-c37eddab

1 to 1 of 1 Network ACL

Name	Associated With	Default	VPC
	2 Subnets	Yes	vpc-63864f0b | MY-VPC

acl-c37eddab

Summary | Inbound Rules | Subnet Associations | Tags

Allows inbound traffic. Be... stateless, you must create inbound and outbound rules.

Cancel | Save

View: A...

Rule #		Protocol	Port Range	Source	Allow / Deny	Remove
100		ALL	ALL	0.0.0.0/0	ALLOW	
101	Custom TCP Rule	TCP (6)	0		ALLOW	

Add another rule

DNS (TCP) (53)
HTTP (80)
POP3 (110)
IMAP (143)
LDAP (389)
HTTPS (443)
SMTPS (465)
IMAPS (993)
POP3S (995)
MS SQL (1433)
Oracle (1521)
MySQL/Aurora (3306)
NFS (2049)
RDP (3389)
PostgreSQL (5432)
Redshift (5439)
WinRM-HTTP (5985)
WinRM-HTTPS (5986)
HTTP* (8080)
HTTPS* (8443)

Feedback | English (US)

 Privacy Policy | Terms of Use

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

Security Groups

- To associate a security group with an instance, it is best practice to specify the security group when you launch the instance
- When **you** create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group
- By default, an SG includes an outbound rule that allows all outbound traffic but no inbound traffic is allowed until you add inbound rules to the security group

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

Default Security Group

Security Groups | VPC Manager

https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#securityGroups:

Most Visited

aws | Services | Resource Groups | shankhantoo | Ohio | Support

- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

Security

- Network ACLs
- Security Groups

VPN Connections

- Customer Gateways
- Virtual Private Gateways
- VPN Connections

Create Security Group | Security Group Actions

Filter: All security groups | Search Security Groups and th

1 to 2 of 2 Security Groups

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

sg-0e998166

Summary | Inbound Rules | Outbound Rules | Tags

Edit

Type	Protocol	Port Range	Destination	Description
ALL Traffic	ALL	ALL	0.0.0.0/0	

Feedback | English (US)

 Privacy Policy | Terms of Use

Default Security Group

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from instances assigned to the same security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic. This rule is added by default if you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC.

Inbound Rules to Web Servers

Security Groups | VPC Manager

https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#securityGroups:

Most Visited

aws Services Resource Groups shankhantoo Ohio Support

Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections

Security
Network ACLs
Security Groups

VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections

Create Security Group | Security Group Actions

Filter All security groups | Search Security Groups and th | 1 to 2 of 2 Security Groups

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

sg-ea4cab81

Summary | Inbound Rules | Outbound Rules | Tags

Cancel | Save

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

Add another rule

Feedback English (US)

 Privacy Policy Terms of Use

Outbound Rules to Web Servers

Security Groups | VPC Manager

https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#securityGroups:

Most Visited

aws | Services | Resource Groups | shankhantoo | Ohio | Support

- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

Security

- Network ACLs
- Security Groups

VPN Connections

- Customer Gateways
- Virtual Private Gateways
- VPN Connections

Create Security Group | Security Group Actions

Filter All security groups | Search Security Groups and th

1 to 2 of 2 Security Groups

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

sg-ea4cab81

Summary | Inbound Rules | Outbound Rules | Tags

Cancel | Save

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

Add another rule

Feedback | English (US)

 Privacy Policy | Terms of Use

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

Using Managed Rule Groups

Step 4
Configure metrics

Step 5
Review and create web ACL

- Cloudbric Corp. managed rule groups
- Cyber Security Cloud Inc. managed rule groups
- F5 managed rule groups
- Fortinet managed rule groups
- GeoGuard managed rule groups
- Imperva managed rule groups
- ThreatSTOP managed rule groups

Using Managed Rule Groups

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

Firewall Manager

- Centrally configure and manage firewall rules across all accounts and applications in AWS Organizations
- Quick rollout of WAF rules for your Application Load Balancers, API Gateways, and Amazon CloudFront distributions
- AWS Firewall Manager integrates with Managed Rules for AWS WAF
- Configure new VPC Security Groups and audit any existing security groups for EC2, and Application ELBs
- Deploy Network Firewalls across accounts and VPCs in your organization

Segment 4: Additional Security Services

AWS Shield Standard

- Included with AWS WAF at no additional cost beyond what you are paying for AWS WAF and your other AWS services
- AWS technologies that are built from the ground up to provide resilience in the face of network and transport layer DDoS attacks
- For web application attacks, you also can use AWS WAF to configure web access control lists (web ACLs) that target network layer DDoS regex request patterns and help to minimize the effects of a DDoS attack

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 must have a Business or Enterprise Support Plan**
- You have exclusive access to advanced, real-time metrics and reports for deep visibility into attacks on your AWS resources

AWS Shield Threat Landscape Report

- The AWS Shield Threat Landscape Report (TLR) offers a summary of threats detected by AWS Shield
- The report is produced by the AWS Threat Research Team (TRT) that persistently monitors and evaluates the threat landscape to formulate security controls for AWS customers

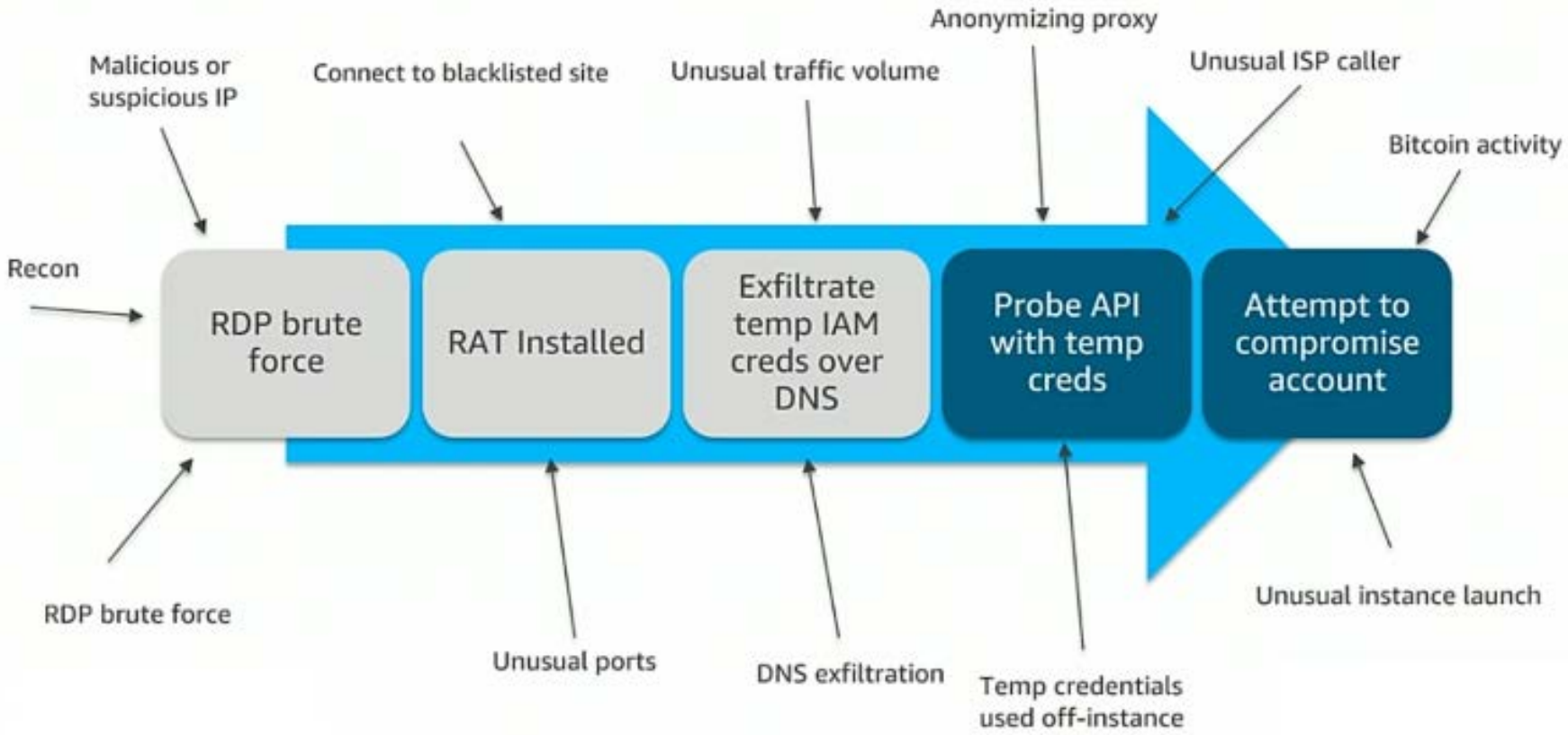
AWS Guard Duty

- GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior
- It monitors for 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
- In 2021 AWS launched domain reputation modeling which can identify malicious domain 7-14 days before commercial threat feeds

AWS Guard Duty

- When GuardDuty detects suspicious or unexpected behavior it generates a **finding** - a notification that has the details about an 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
- Another newer feature is GuardDuty for EKS Protection

AWS Guard Duty

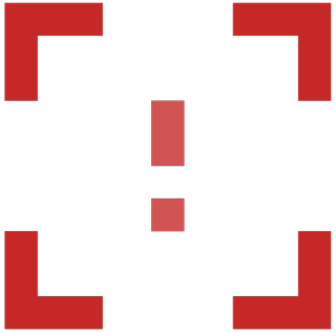


Amazon Detective

- Analyzes and visualizes security findings from the GuardDuty console to a Detective console
- IP Address Drill Down feature is useful for forensic teams performing investigations to determine events taking place from an EC2 instance
- Supports AWS Organizations to simplify security operations and investigations across all accounts
- It leverages the Detective Graph Database

Enabling Security Hub

- Security Hub is a cloud security posture management service that offers a consolidated view of your security status in AWS
- You can automate security checks, manage security findings, and classify the highest priority security issues across your AWS environment using:
  - Amazon GuardDuty
  - Amazon Inspector
  - S3 bucket policy findings from Amazon Macie
  - Also integrated partner solutions like Forcepoint Cloud Security Gateway (CSG)



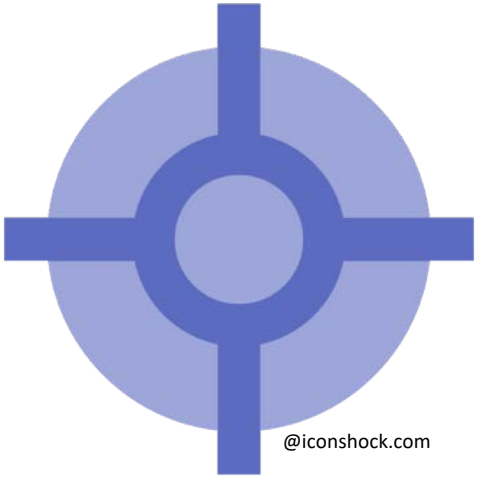
@iconshock.com

Security Hub Use Cases

- Continuously scan AWS accounts for configuration errors using:
  - **Center for Internet Security (CIS) AWS Foundations benchmarks**
  - **PCI DSS v3.2.1 benchmarks**
  - **AWS Foundational Best Practices Standards**
- Report on security check results at the account and multi-account level to recognize your global security posture
- Use the Hub's summary dashboards and filtering rules to identify and prioritize which findings

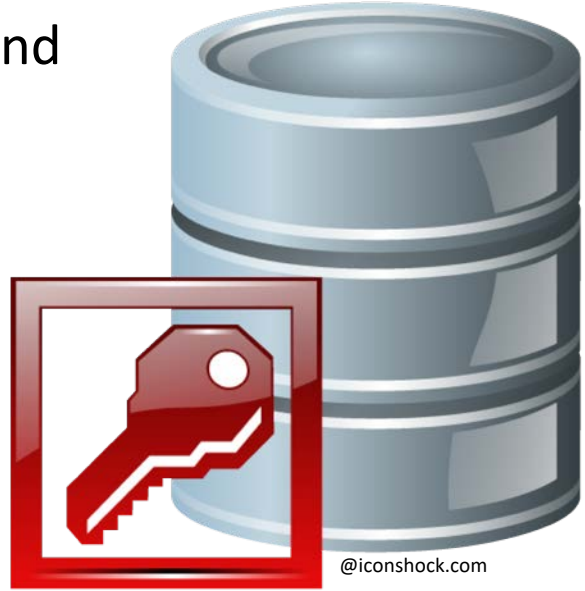
Enabling Security Hub

- Enabling Security Hub grants it permissions to import findings from:
  - Amazon GuardDuty
  - Amazon Inspector
  - Amazon Macie
  - AWS IAM Access Analyzer
  - AWS Firewall Manager
- **AWS offers a 30-day free trial**

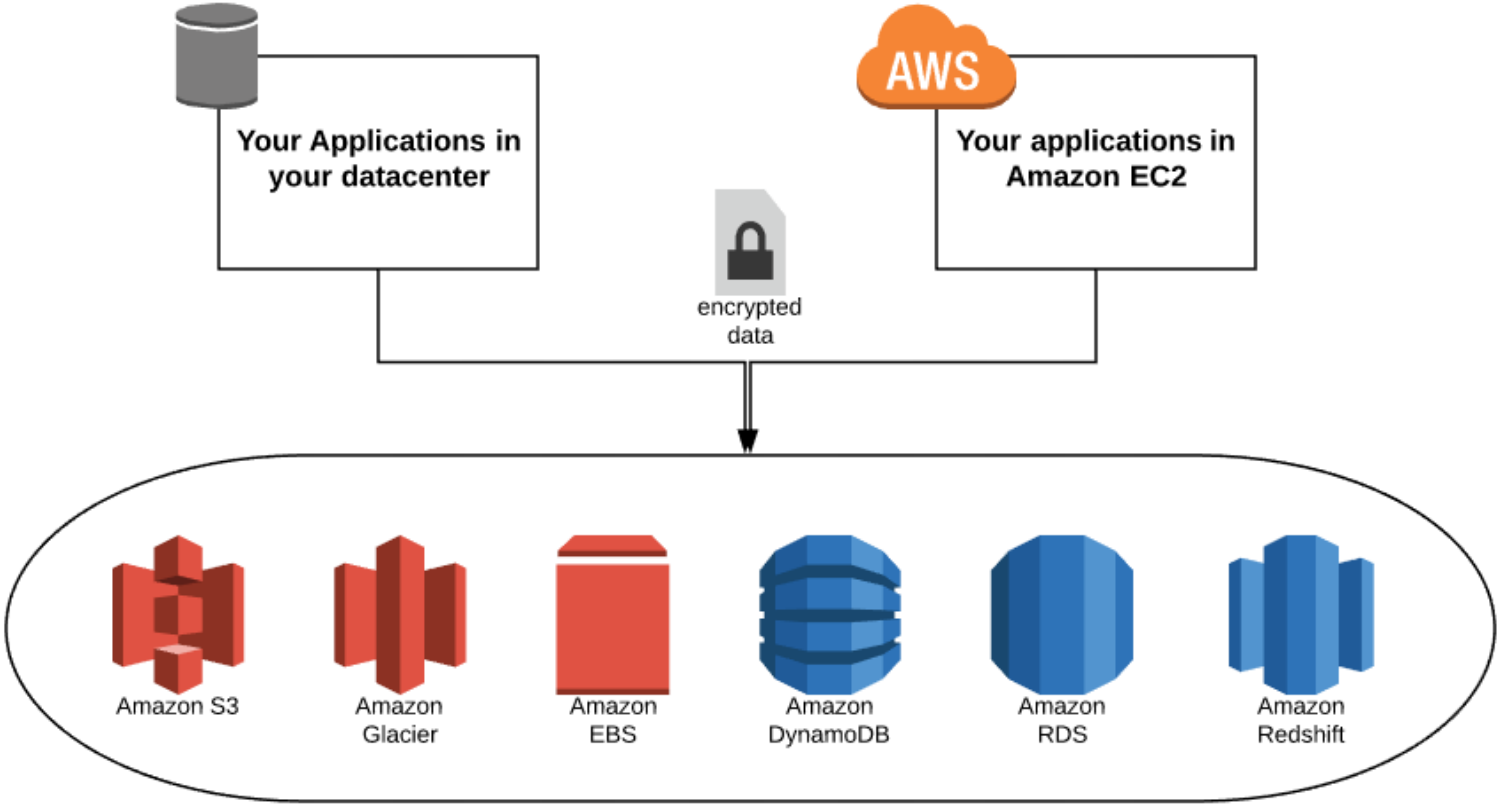


Encryption and Key Management in AWS

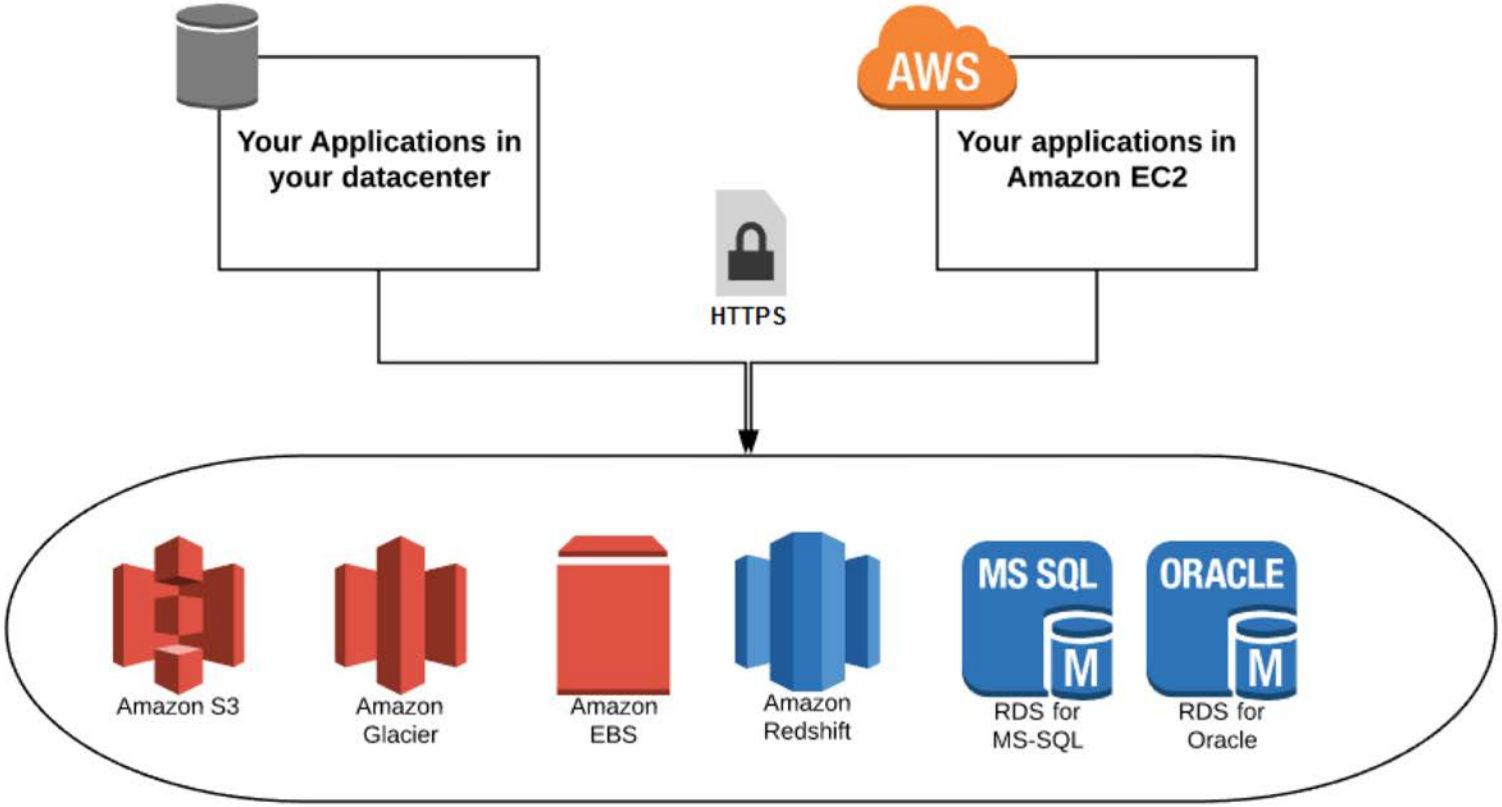
- Client-side encryption: You encrypt you data and manage your own keys
- Server-side encryption: AWS encrypts data and manages the keys for you
- Key Management
  - On your own
  - AWS Management Key Service (KMS)
  - AWS Partner Solutions (Sophos, Trend, etc.)
  - AWS Cloud HSM



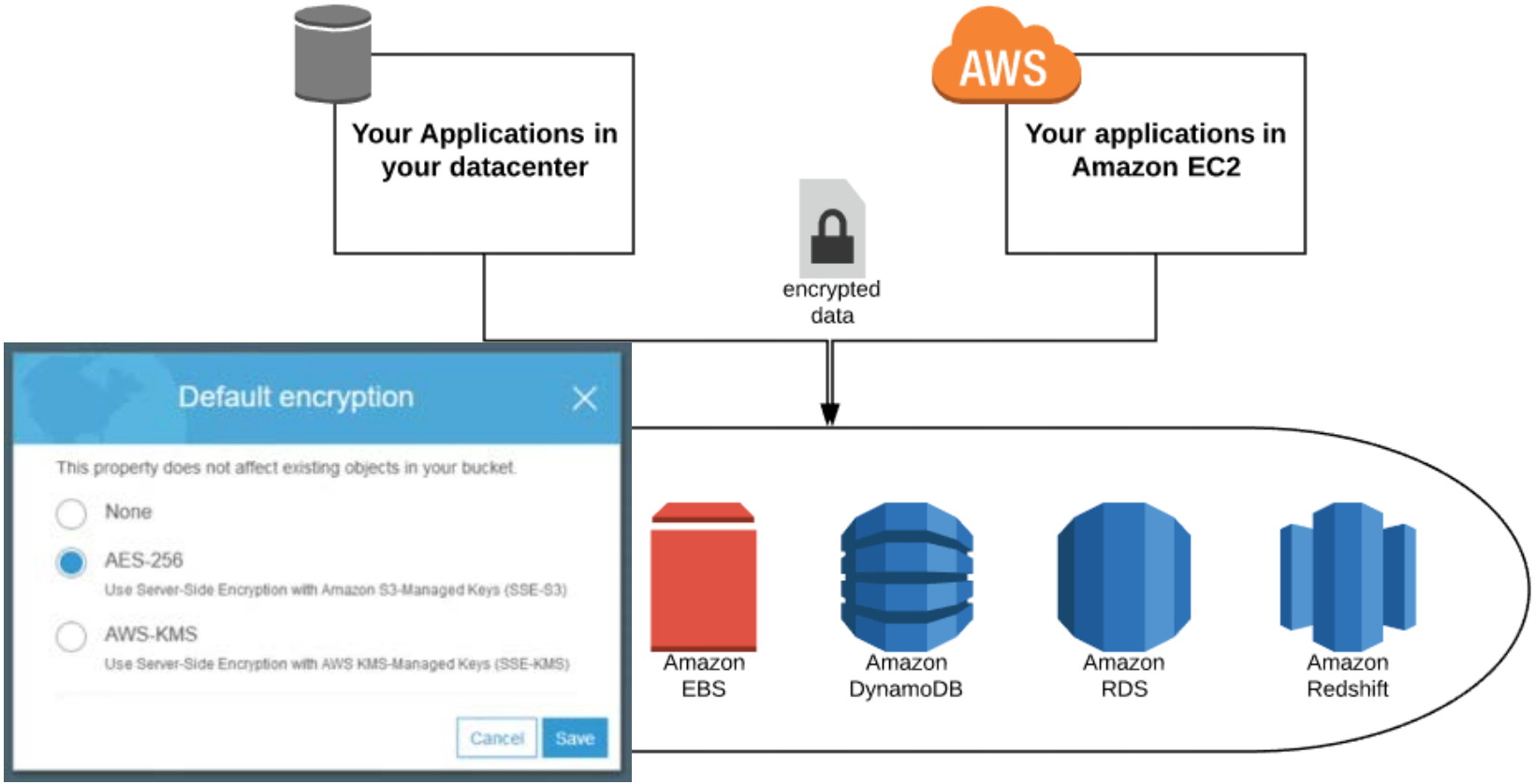
Client-side Encryption



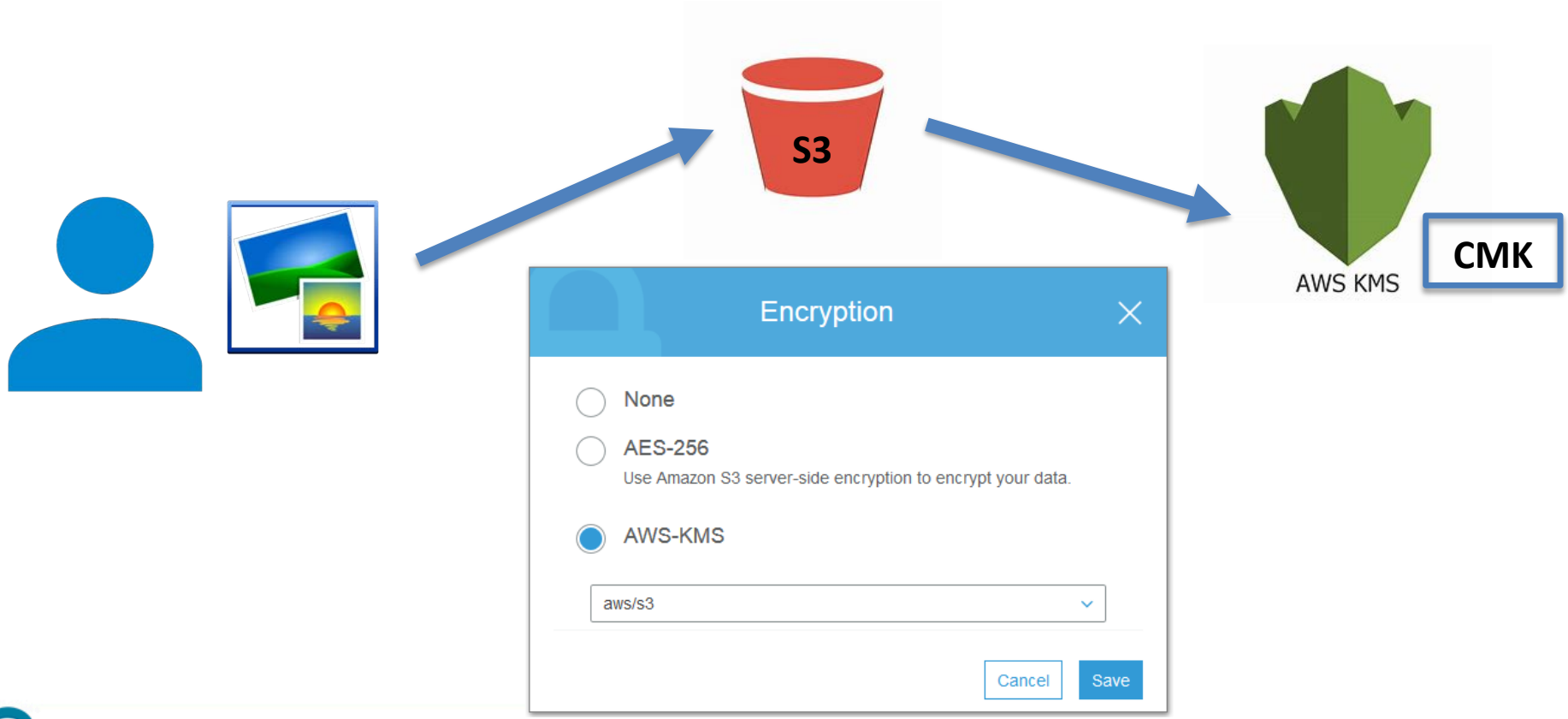
Server-side Encryption



AWS S3 Server-side Encryption



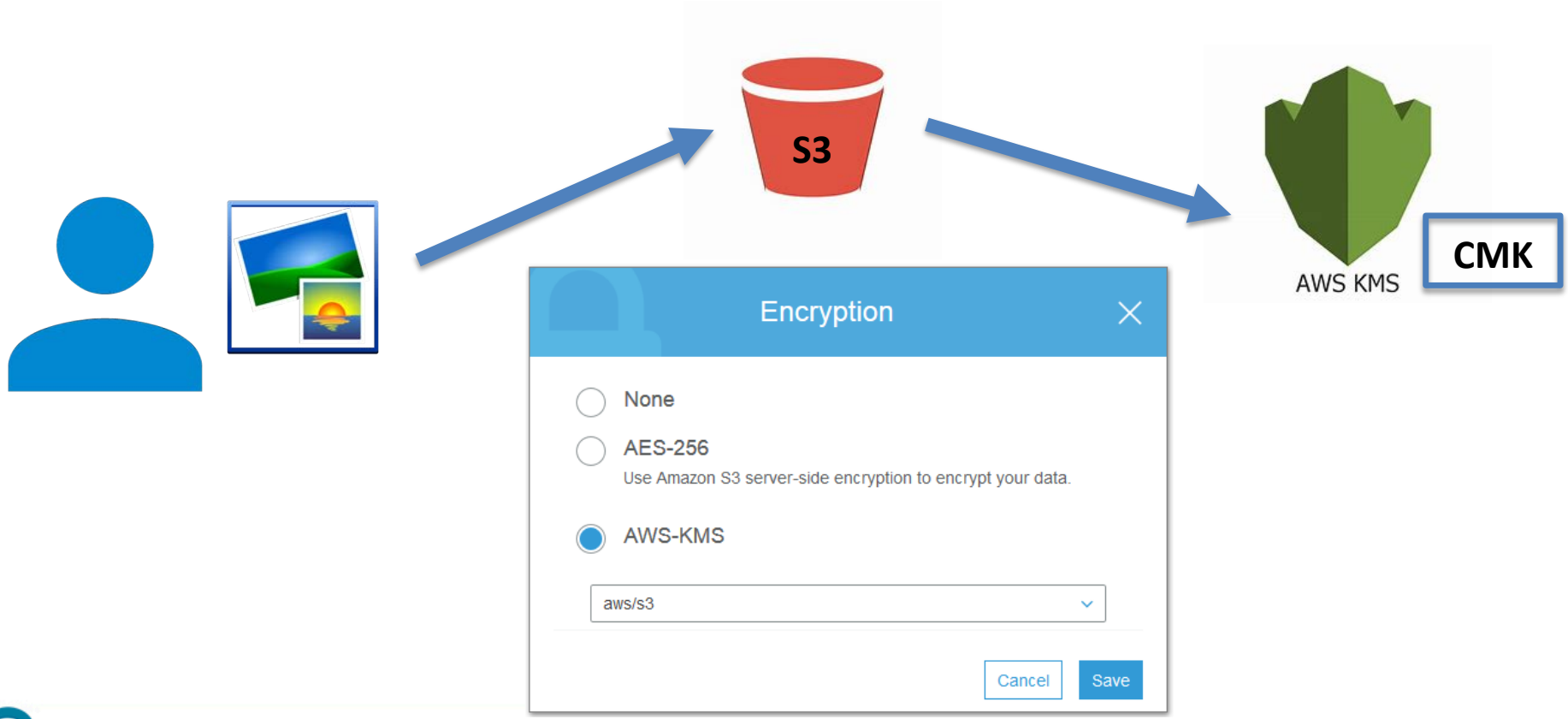
S3 SSE-KMS Encryption



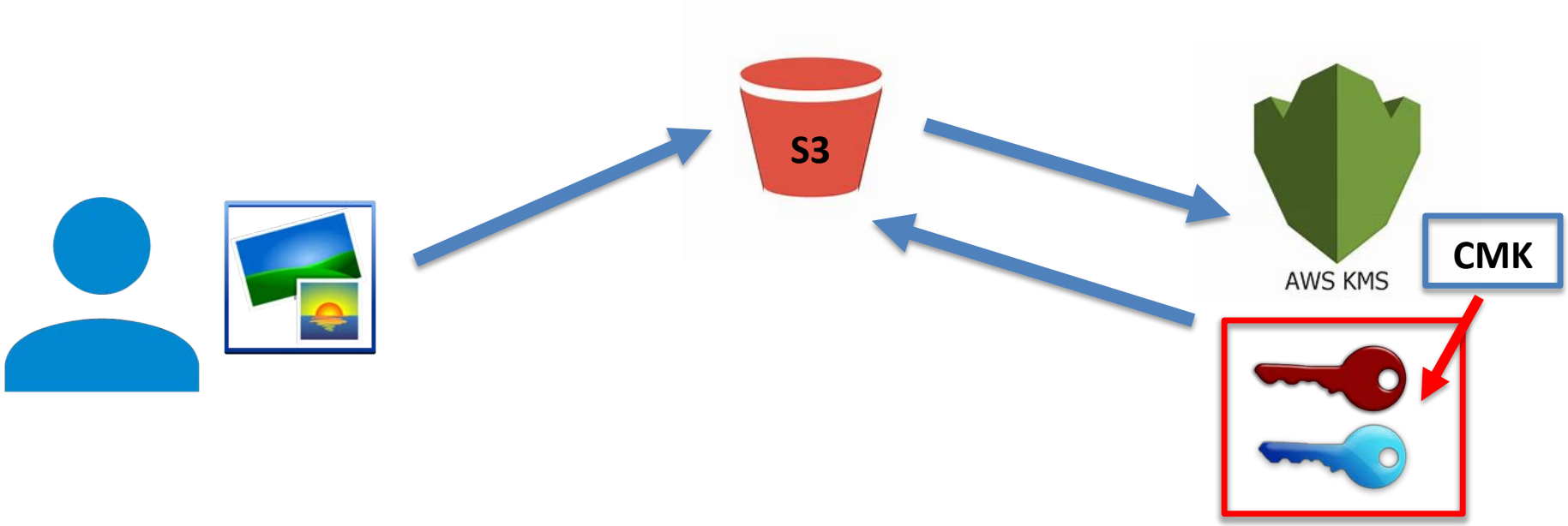
Types of CMKs

- There are three types of CMKs in AWS accounts: customer managed CMKs, AWS managed CMKs, and AWS owned CMKs
  - Customer managed CMKs are CMKs in your AWS account that you create, own, and manage
  - AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that integrates with AWS KMS
  - AWS owned CMKs are not in your AWS account. They are part of a collection of CMKs that AWS owns and manages for use in multiple AWS accounts - AWS services can use AWS owned CMKs to protect your data

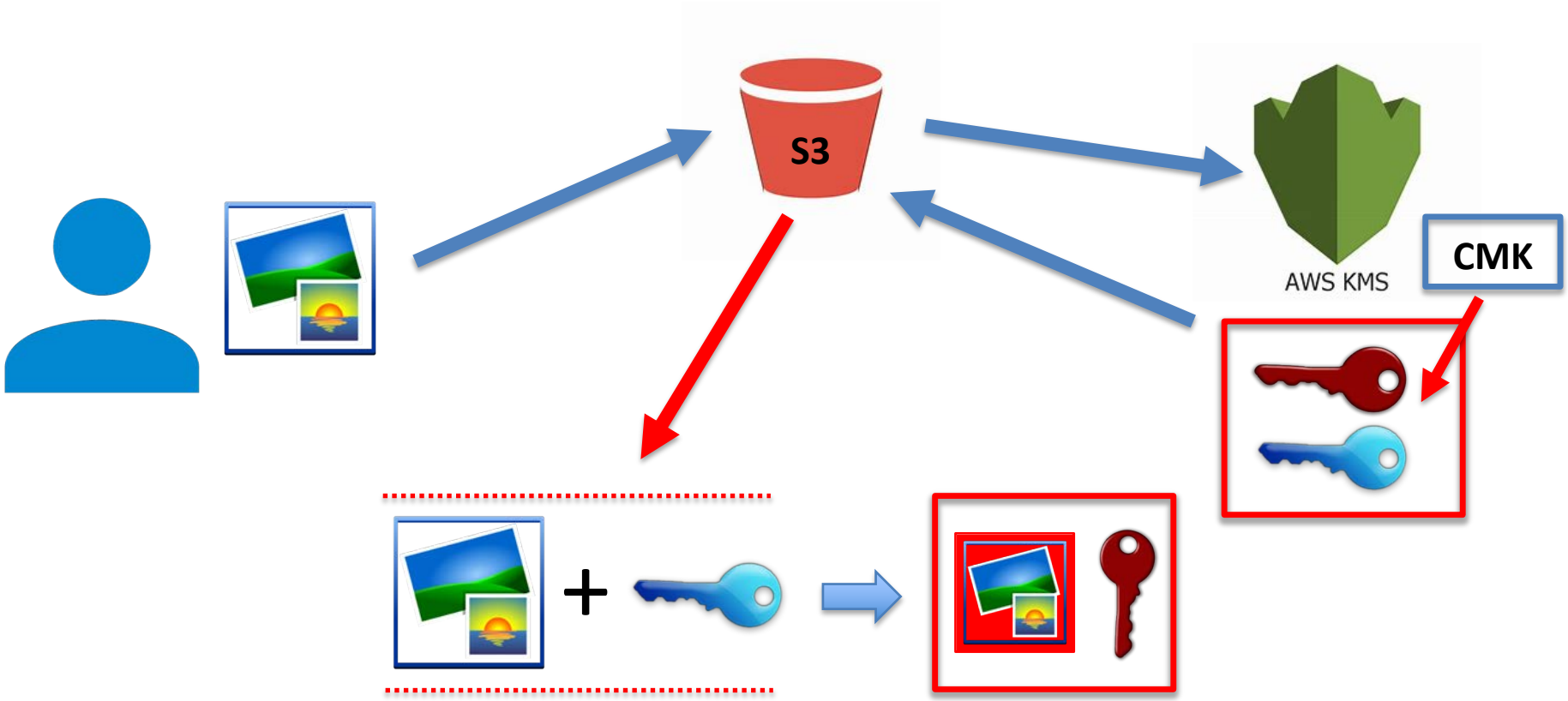
S3 SSE-KMS Encryption



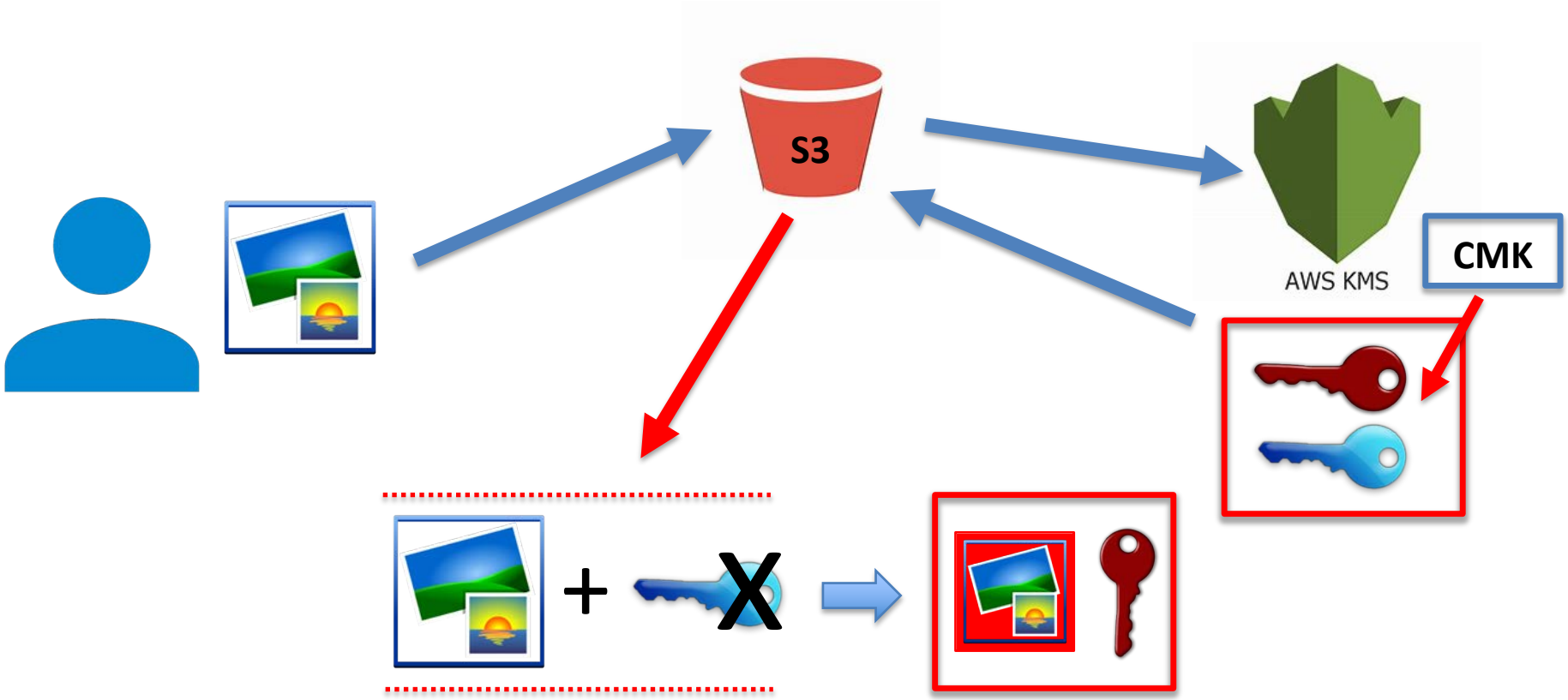
S3 SSE-KMS Encryption



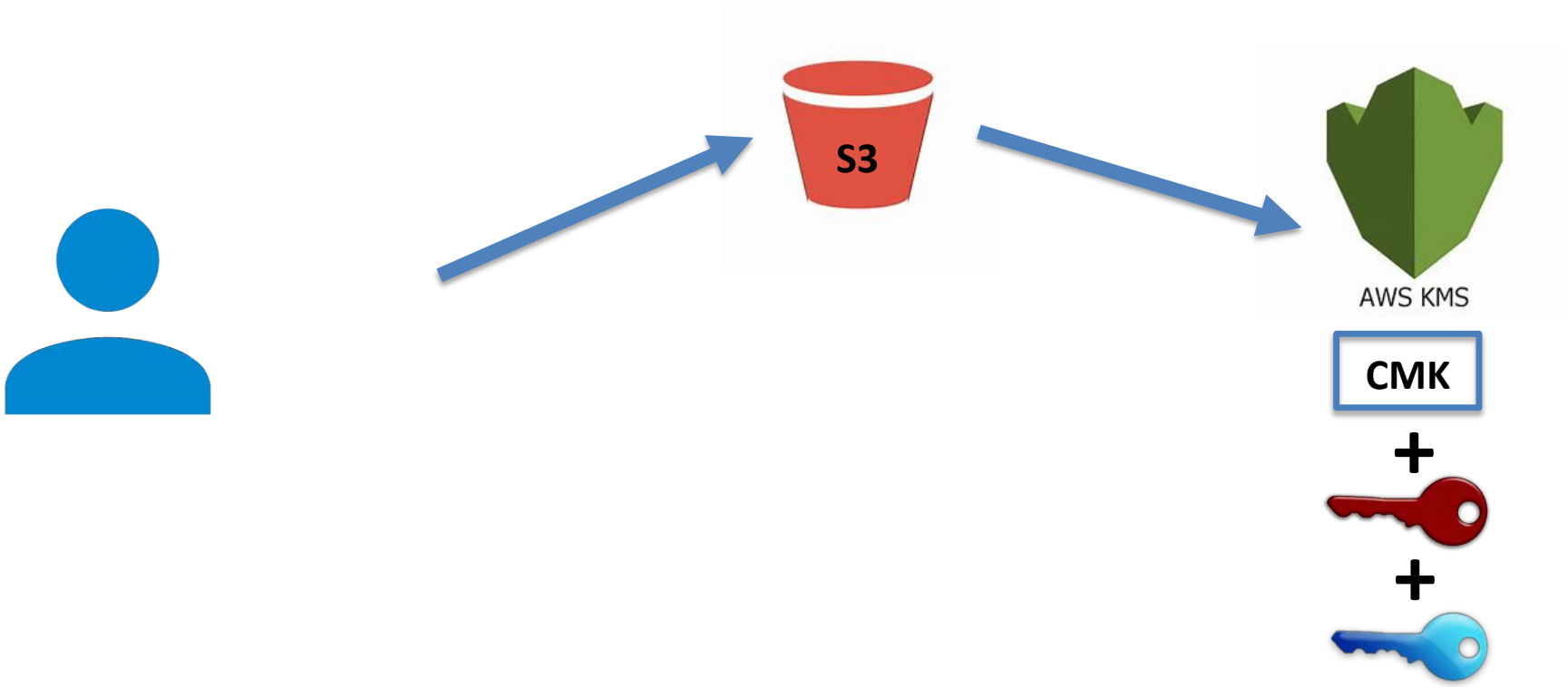
S3 SSE-KMS Encryption



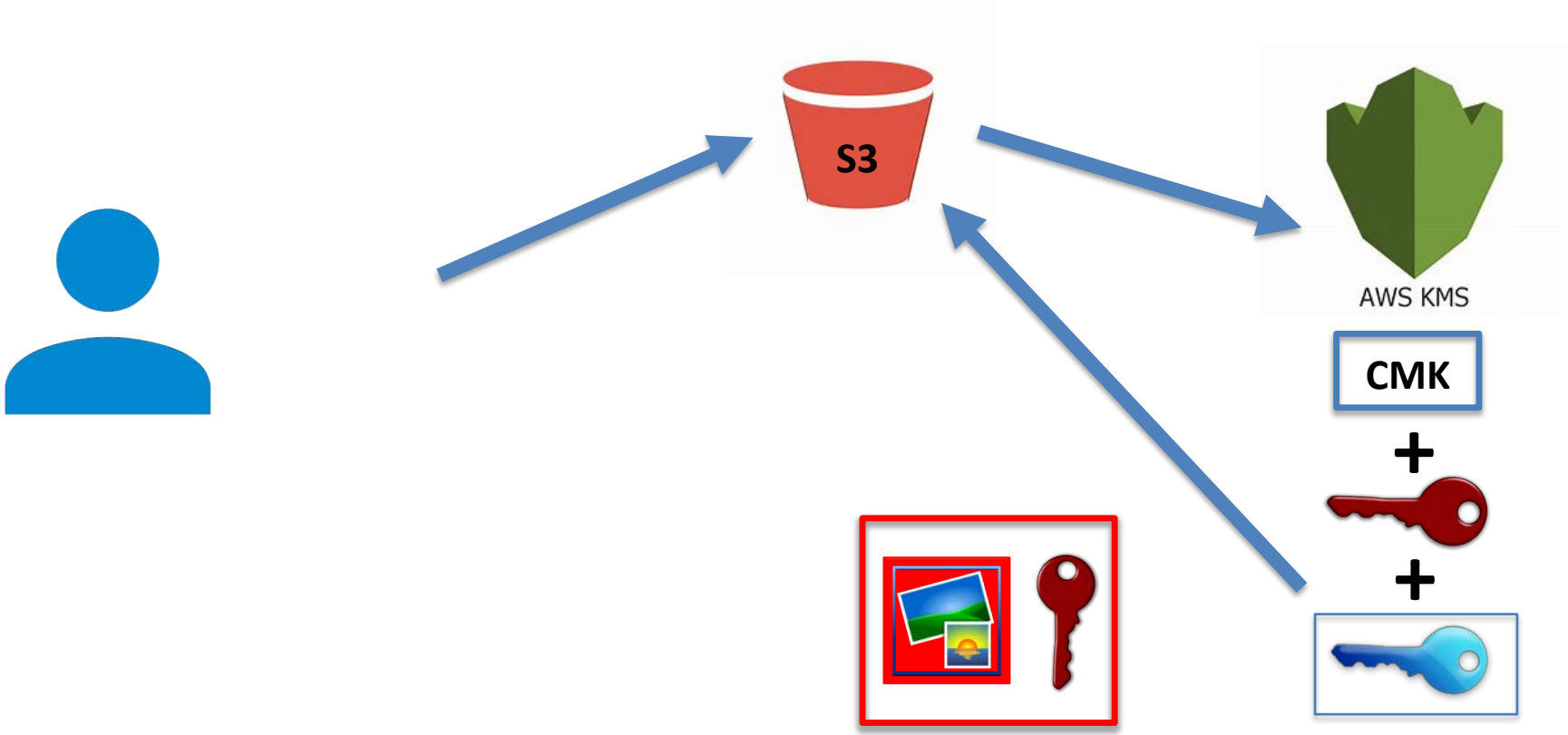
S3 SSE-KMS Encryption



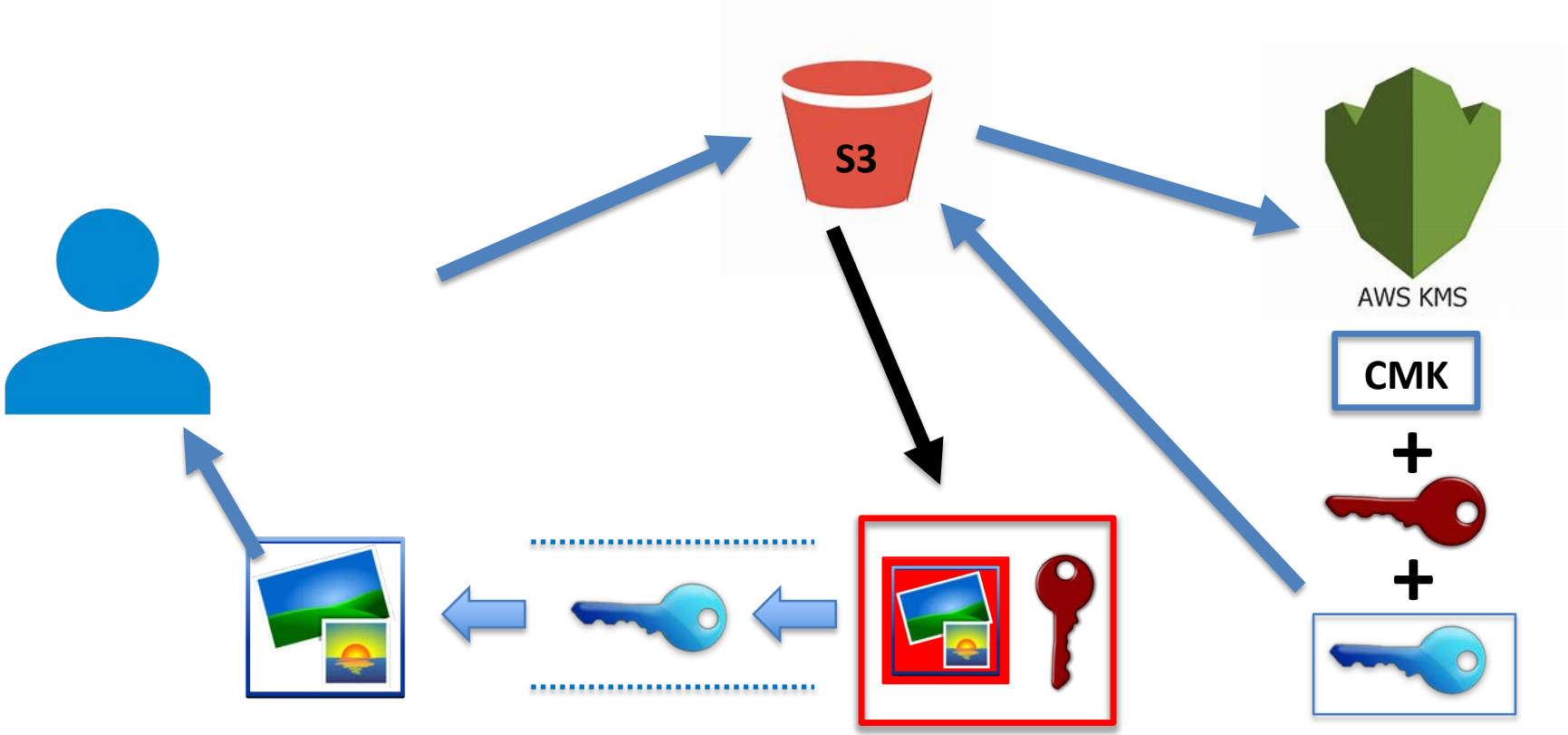
S3 SSE-KMS Decryption



S3 SSE-KMS Decryption



S3 SSE-KMS Decryption



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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-04a92f3aceecdabef	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypte
EBS	/dev/sdb	Search (case-insensit	8	General Purpose SSD (gp2)	100 / 3000	N/A	☐	Not Encrypte

Add New Volume

Filter by attributes

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

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.

AWS EBS Encryption by Default

- 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 ec2 enable-ebs-encryption-by-default
```

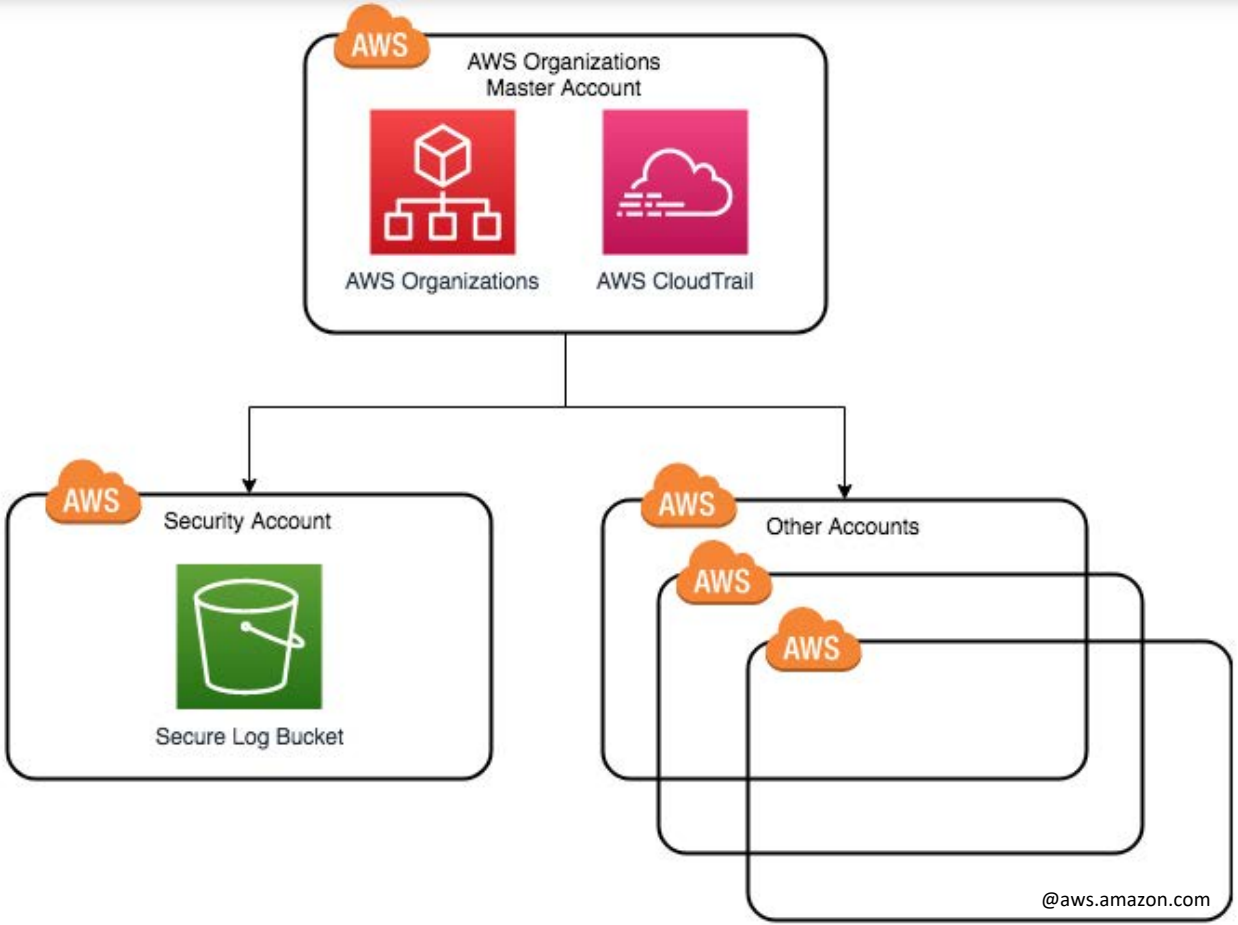
S3 Security Distinctives

- Backed with the Amazon S3 Service Level Agreement
- Designed to provide 99.999999999% durability and 99.99% availability of objects over a given year
- Designed to sustain the concurrent loss of data in two facilities
- Amazon S3 further protects your data using versioning
- Deploy VPC endpoints for accessing Amazon S3
- Use Bucket Policies instead of ACLs (only use ACLs sparingly for controlling object-level access)

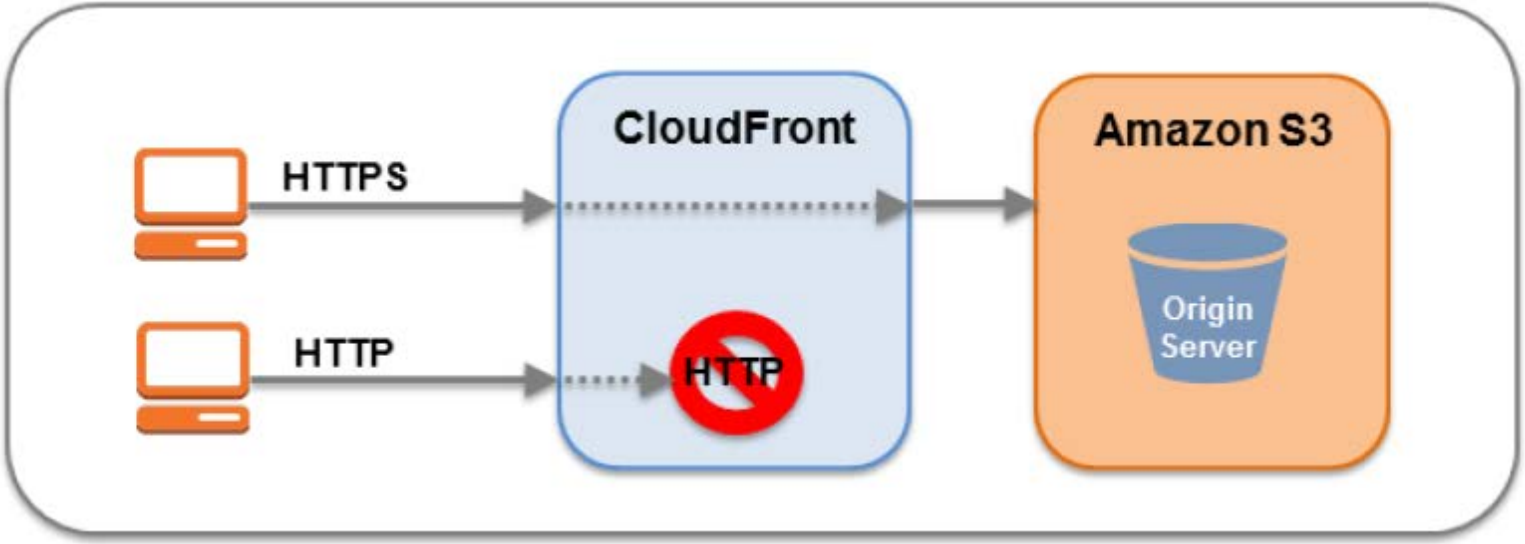
Create a Data Bunker

- A data bunker is a secure account which stores critical security data in a secure location
- Only select members of your security team should have access to this account
- Security teams should:
  - Create a new security account in a multi-account organization
  - Create a secure S3 bucket in that account
  - Turn on CloudTrail for the organization and send the logs to this bucket in the secure data account
- You may want to also consider what other data you need to store there (i.e., secure backups)

Create a Data Bunker



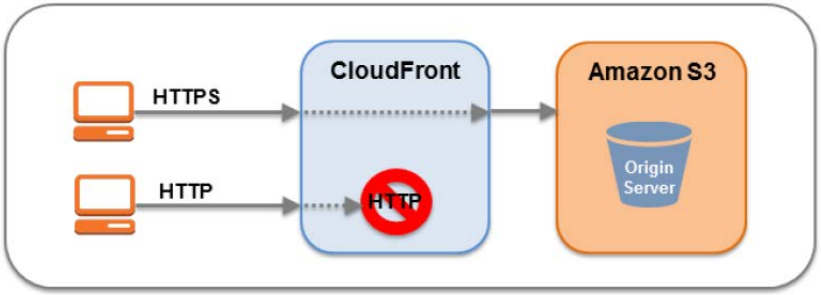
Amazon CloudFront Security



- Every request made to its control API must be authenticated – signed with an HMAC-SHA signature only accessible through TLS-enabled endpoints
- Private Content Feature controls who can download content from CloudFront
- Origin Access Identities can control access to original copies of objects

Amazon CloudFront Security

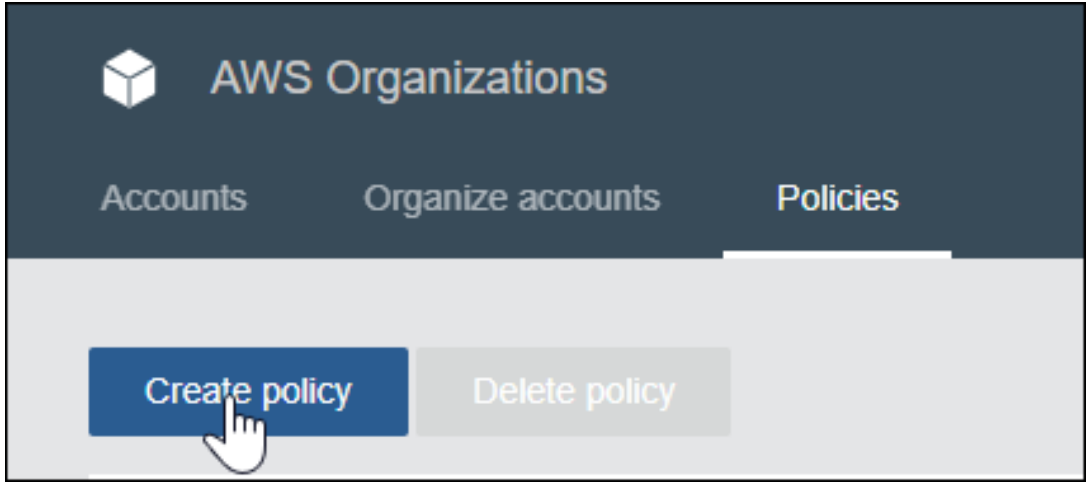
- Amazon CloudFront supports the TLSv1.1 and TLSv1.2 protocols for HTTPS connections between CloudFront and your custom origin webserver
- Selection of cipher suites includes ECDHE protocol on connections to both viewers and the origin



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
- Can also use Organizations to automate the creation of new accounts through APIs
- Organizations centrally manage Service Control Policies (SCPs) across multiple accounts without using custom scripts or manual processes

SCP Guardrails



SCP Guardrails

Create new policy

A service control policy (SCP) defines the maximum permissions for account users and roles. An SCP doesn't grant permissions. Learn more

Policy name *

DenyChangesToAdminRole

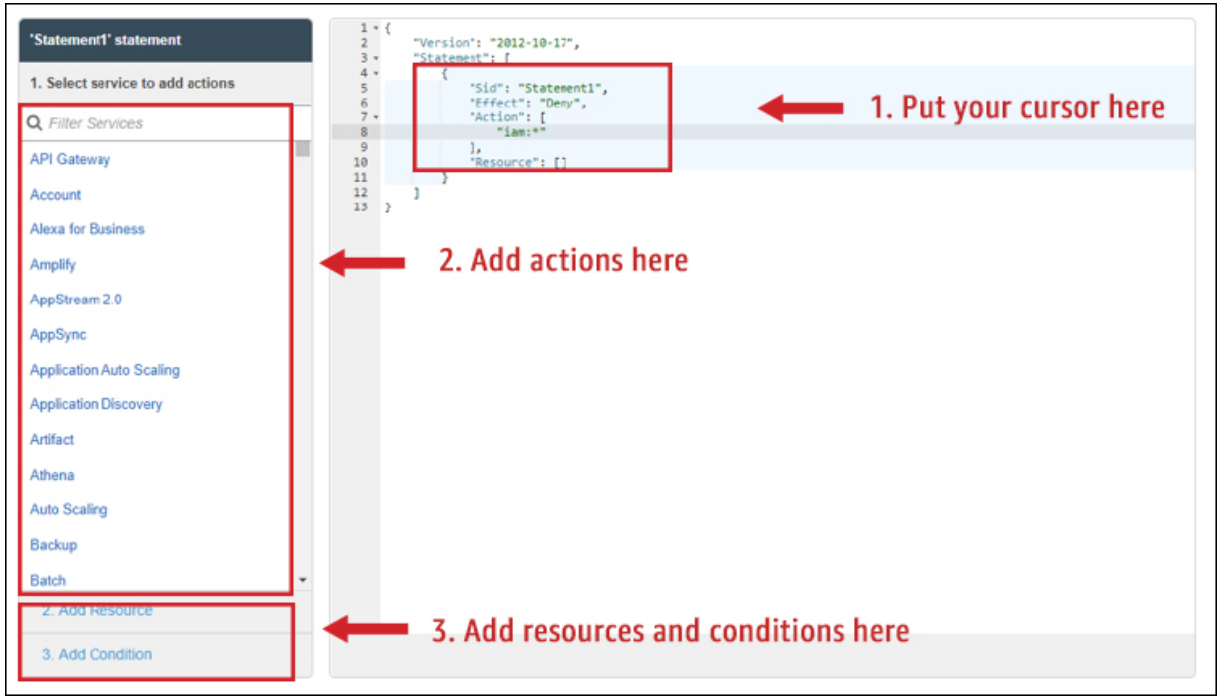
The policy name can have up to 128 characters.

Description

Prevents all IAM principals from making changes to AdminRole.

The description can have up to 512 characters. You can't edit the description later.

SCP Guardrails



SCP Guardrails

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "DenyChangesToAdminRole",
6              "Effect": "Deny",
7              "Action": [],
8              "Resource": []
9          }
10     ]
11 }
```

SCP Guardrails

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "Statement1",
6              "Effect": "Deny",
7              "NotAction": [
8                  "iam:GetContextKeysForPrincipalPolicy",
9                  "iam:GetRole",
10                 "iam:GetRolePolicy",
11                 "iam:ListAttachedRolePolicies",
12                 "iam:ListInstanceProfilesForRole",
13                 "iam:ListRolePolicies",
14                 "iam:ListRoleTags"
15             ],
16             "Resource": []
17         }
18     ]
19 }
```

SCP Guardrails

DenyChangesToAdminRole was created.

Create policy | Delete policy

	Policy name	Policy type	Description
	FullAWSAcc…	Service control	Allows access to every operation
	DenyChang…	Service control	Prevents all IAM principals from making changes to AdminRole.

AWS Security Crash Course

Michael J. Shannon

THANK YOU FOR ATTENDING!