

# AWS Security Crash Course



## **Michael J. Shannon**

CISSP  
Cisco CCNP - Security  
Palo Alto Networks Certified  
Network Security Engineer (PNCSE7)  
Security+  
ITIL 4 Managing Professional (MP)  
OpenFAIR Foundation  
AWS SysOps Administrator: Associate



# Welcome to the AWS Security Crash Course

- **Segment 1:** AWS Security Triad, AWS Security Pillar, Shared Security Responsibility Model and Credential Management
- **Segment 2:** Identity and Access Management (IAM)
- **Segment 3:** Infrastructure Security
- **Segment 4:** AWS WAF, Shield Advanced, and GuardDuty, and Security Hub
- **Segment 5:** Key Management Service (KMS), Service-Specific Security (S3 and EBS), and Organizational Service Control Policies (SCP) and more



## Segment 1: AWS Security Triad, Security Pillar Shared Security Responsibility Model and Credential Management

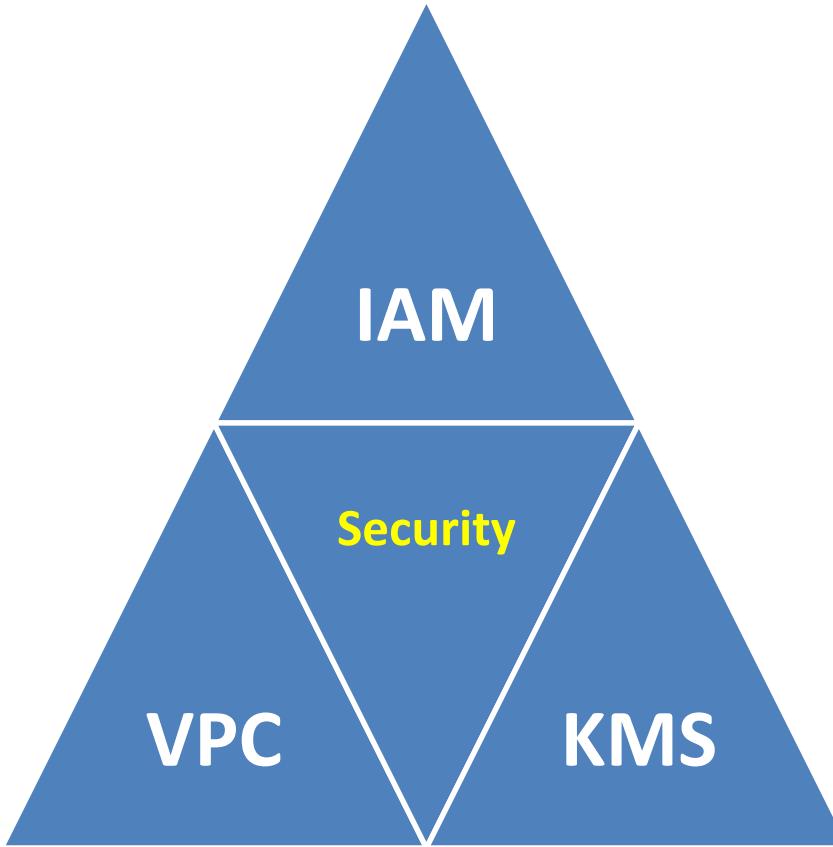
# AWS Well-Architected Security Pillar

- 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

# The AWS Security Triad



# Well-Architected 5 Security Areas

Identity and  
Access  
Management

Detective  
Controls

Infrastructure  
Protection

Data  
Protection

Incident  
Response

# 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

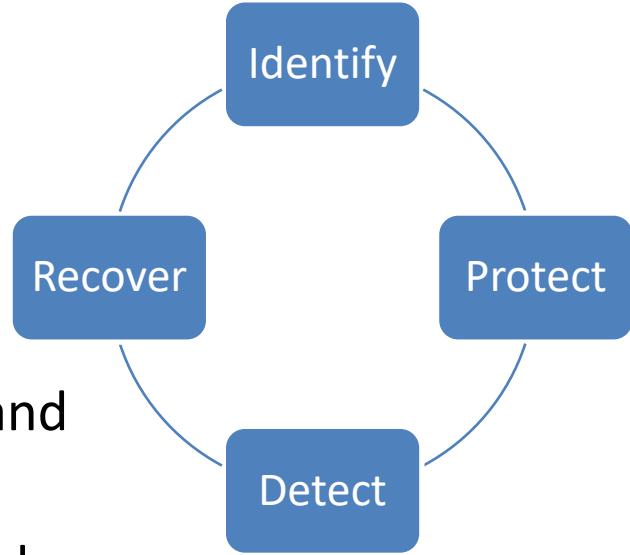


# The Parkerian Hexad



# AWS Foundational Best Practices

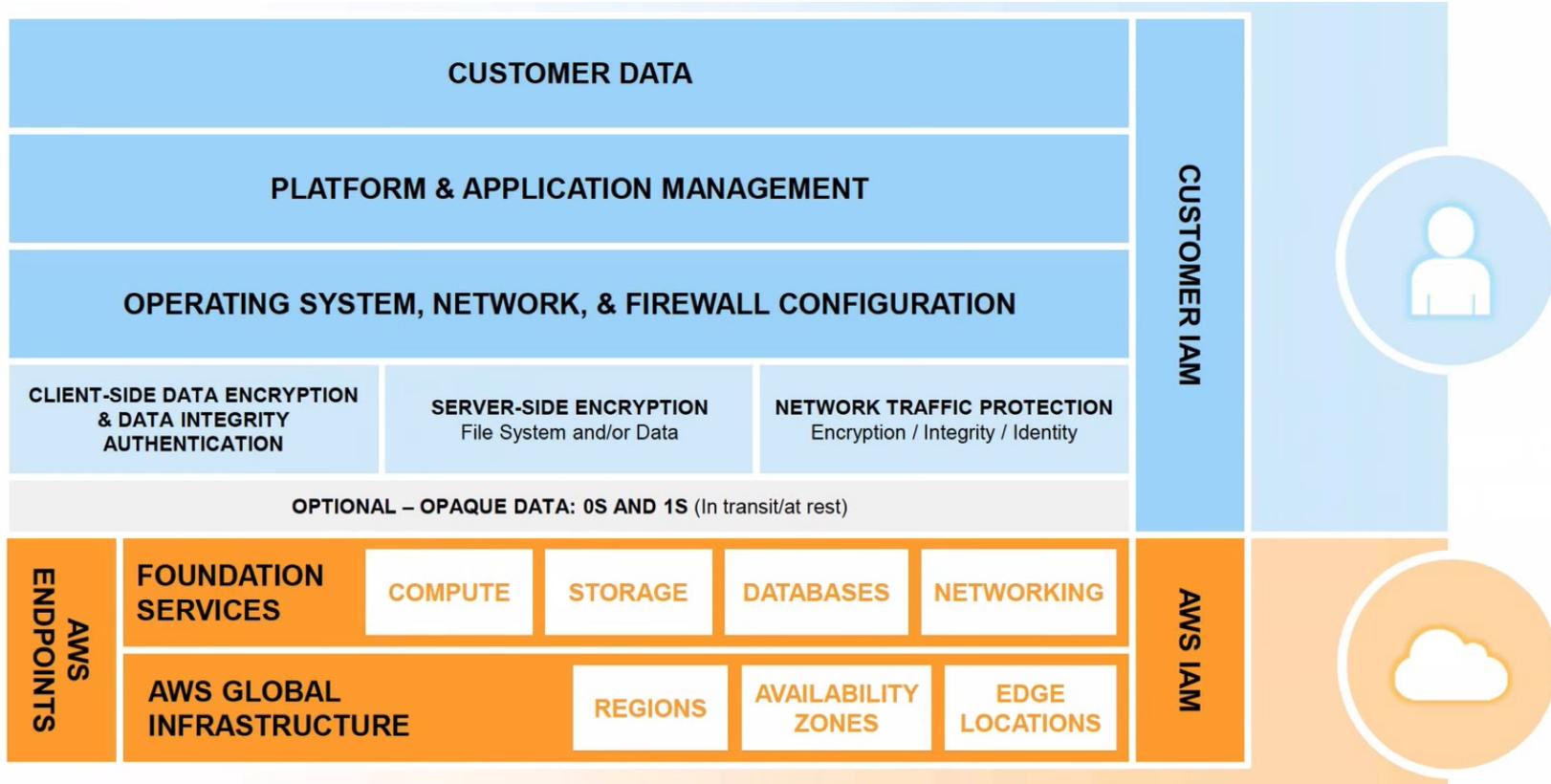
- The AWS Foundational Security Best Practices standard is a set of controls that detect deviations from security best practices
- It allows you to continuously appraise all accounts and workloads to rapidly detect and analyze gaps
- Based on the NIST Cybersecurity Framework



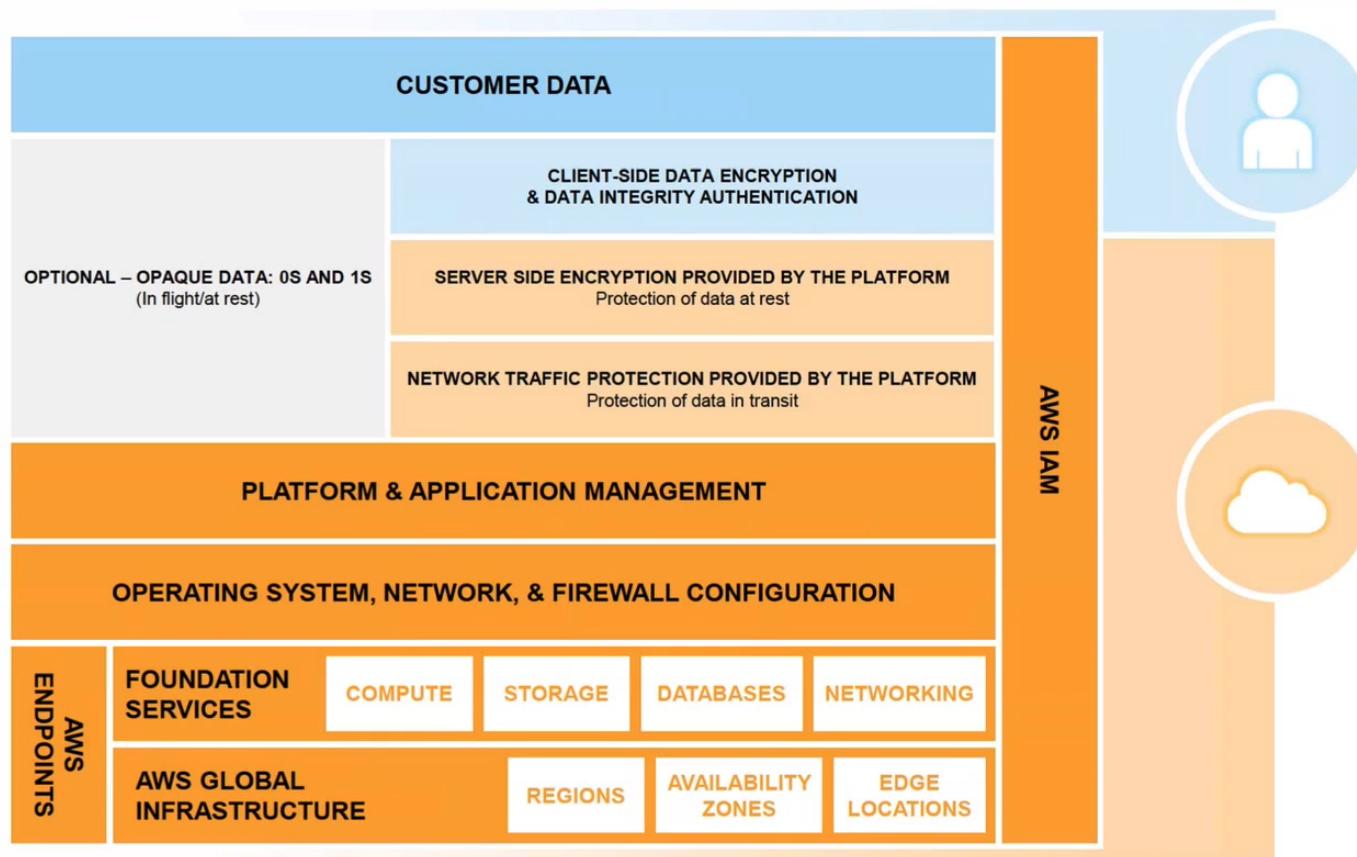
# AWS Responsibilities

- 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 Security Model (EC2/VPC/EBS)



# Shared Security Model (S3/DynamoDB)



# Credentials: AWS Root Account

The screenshot shows a web browser window with two tabs: "Mail - Brio Insurance Group" and "AWS Console - Signup". The "AWS Console - Signup" tab is active, displaying the "Create an AWS account" form. The form includes fields for Email address, Password, Confirm password, and AWS account name, each with a corresponding input box. A large yellow "Continue" button is positioned below the password fields. To the left of the form, there is promotional text about AWS Accounts including 12 months of free tier access and links to EC2, S3, and DynamoDB. At the bottom of the page, there is copyright information for Amazon Web Services and links to Privacy Policy and Terms of Use.

Mail - Brio Insurance Group X AWS Console - Signup X +

https://portal.aws.amazon.com/billing/signup?redirect\_url=https%3A%2F%2Faws.amazon.com%2Fsignups%2Froot%2Fcreate%2F

Search

Most Visited

aws English ▾

Create an AWS account

AWS Accounts Include  
12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB  
Visit [aws.amazon.com/free](http://aws.amazon.com/free) for full offer terms

Email address

Password

Confirm password

AWS account name ⓘ

Continue

Sign in to an existing AWS account

© 2018 Amazon Web Services, Inc. or its affiliates.  
All rights reserved.  
[Privacy Policy](#) | [Terms of Use](#)

# Credentials: AWS Root Account



## 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](#)

The advertisement features a dark blue background with several orange hexagonal icons containing symbols like a speech bubble, a rocket, a dollar sign, a handshake, and a lock. A large white outline of a user profile is positioned in the center, with a checkmark icon below it. The AWS logo is in the top right corner. The text "AWS IQ" is prominently displayed in large white letters at the bottom left, followed by the tagline "Find AWS Certified experts for on-demand project work". A "LEARN MORE" button is located at the bottom right.

AWS IQ

Find AWS Certified experts  
for on-demand project work

LEARN MORE



Pearson

# Credentials: AWS Root Account

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



@iconshock.com

# Credentials: AWS Root Account

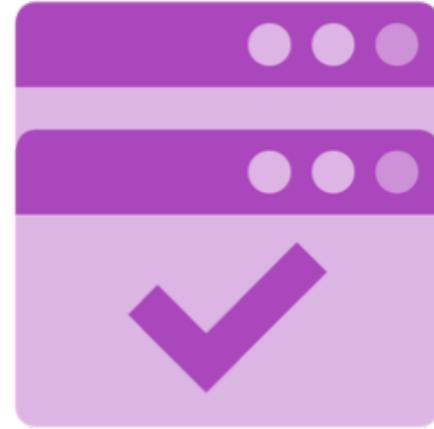
- If you must keep your access key, rotate (change) it regularly
- To delete or rotate your AWS account access keys, go to the Security Credentials page in the AWS Management Console
- Never share your AWS account password or access keys with anyone



@iconshock.com

# 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 AWS-created X.509v3 signing certificate
- Transfer Route 53 domain to another account



@iconshock.com

# 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

The screenshot shows the AWS IAM console interface. At the top, there is a link to the IAM users sign-in page: [https://\[REDACTED\].signin.aws.amazon.com/console](https://[REDACTED].signin.aws.amazon.com/console). To the right of the link is a blue button labeled "Customize" with a red rectangular box drawn around it. Below the link, the "IAM Resources" section is visible, showing "Users: 1", "Groups: 1", "Roles: 3", and "Identity Providers: 0". Under "Customer Managed Policies", it says "0". The "Security Status" section contains several items with checkboxes:

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

A modal dialog box titled "Create Account Alias" is displayed in the center. It has two input fields: "Account" and "Alias". The "Account" field is empty. The "Alias" field is also empty. At the bottom of the dialog are two buttons: "Cancel" and "Yes, Create", with "Yes, Create" being blue.

# My Security Credentials

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.

mjshannawstest ▾ N. Virginia ▾

My Account  
My Organization  
My Billing Dashboard  
**My Security Credentials**  
Access reso  
Sign Out

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

The screenshot shows the AWS IAM Security Credentials page. A modal window is displayed in the center, providing instructions and best practices for managing security credentials.

**Modal Content:**

- You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.
- To help secure your account, follow an [AWS best practice](#) by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

**Buttons:**

- [Continue to Security Credentials](#)
- [Get Started with IAM Users](#)

Don't show me this message again

**Page Navigation:**

- Search IAM
- Dashboard
- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report
- Encryption keys

**Collapsed Side Navigation:**

- Multi-factor authentication (MFA)
- Access keys (access key ID and secret access key)
- CloudFront key pairs
- X.509 certificate
- Account identifiers

# 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.

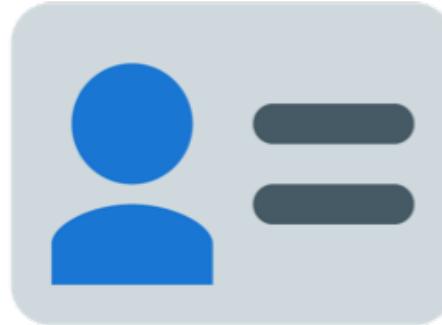
- ▲ CloudFront key pairs
- ▲ X.509 certificate
- ▲ Account identifiers

# Credential Usage Options

Credential Type	Use	Description
Passwords	AWS root account or IAM user account login to the AWS Management Console	A string of characters used to log into your AWS account or IAM account. AWS passwords must be a minimum of 6 characters and may be up to 128 characters.
Multi-Factor Authentication (MFA)	AWS root account or IAM user account login to the AWS Management Console	A six-digit single-use code that is required in addition to your password to log in to your AWS Account or IAM user account.
Access Keys	Digitally signed requests to AWS APIs (using the AWSSDK, CLI, or REST/Query APIs)	Includes an access key ID and a secret access key. You use access keys to digitally sign programmatic requests that you make to AWS.

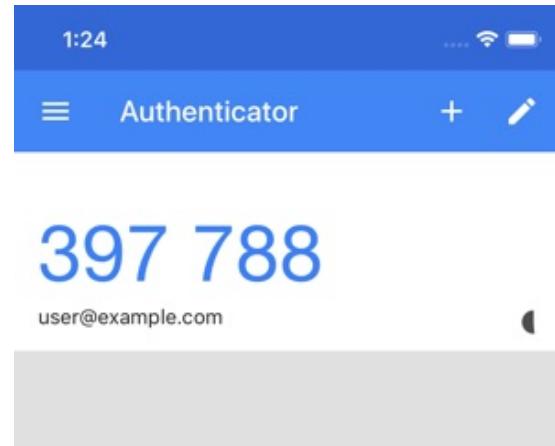
# Passwords

- AWS Account
  - Individual IAM user accounts
  - AWS Discussion Forums
  - AWS Support Center
- 
- AWS passwords can be up to 128 characters long and contain special characters
  - You are encouraged to create long and strong passwords that cannot be easily guessed



# 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



# Access Keys

- AWS requires that all API requests must include a digital signature that is used to verify the requestor identity
- Digital signature is calculated using a cryptographic hash (HMAC-SHA256) where the input to the function in this case includes the text of your request and your secret access key
- Offers message integrity and anti-replay protection
- Required to sign message using a key derived from your secret access key instead of using the secret access key itself

# 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](#).

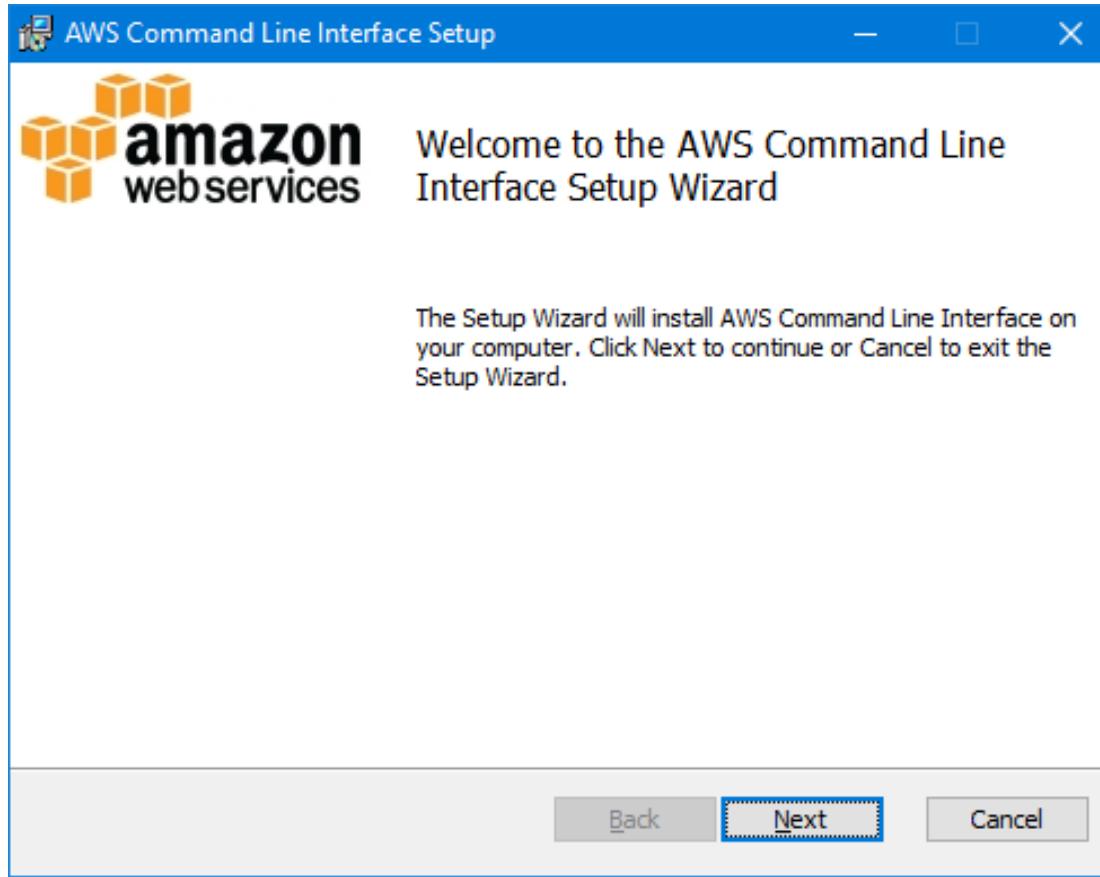
### Release Notes

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

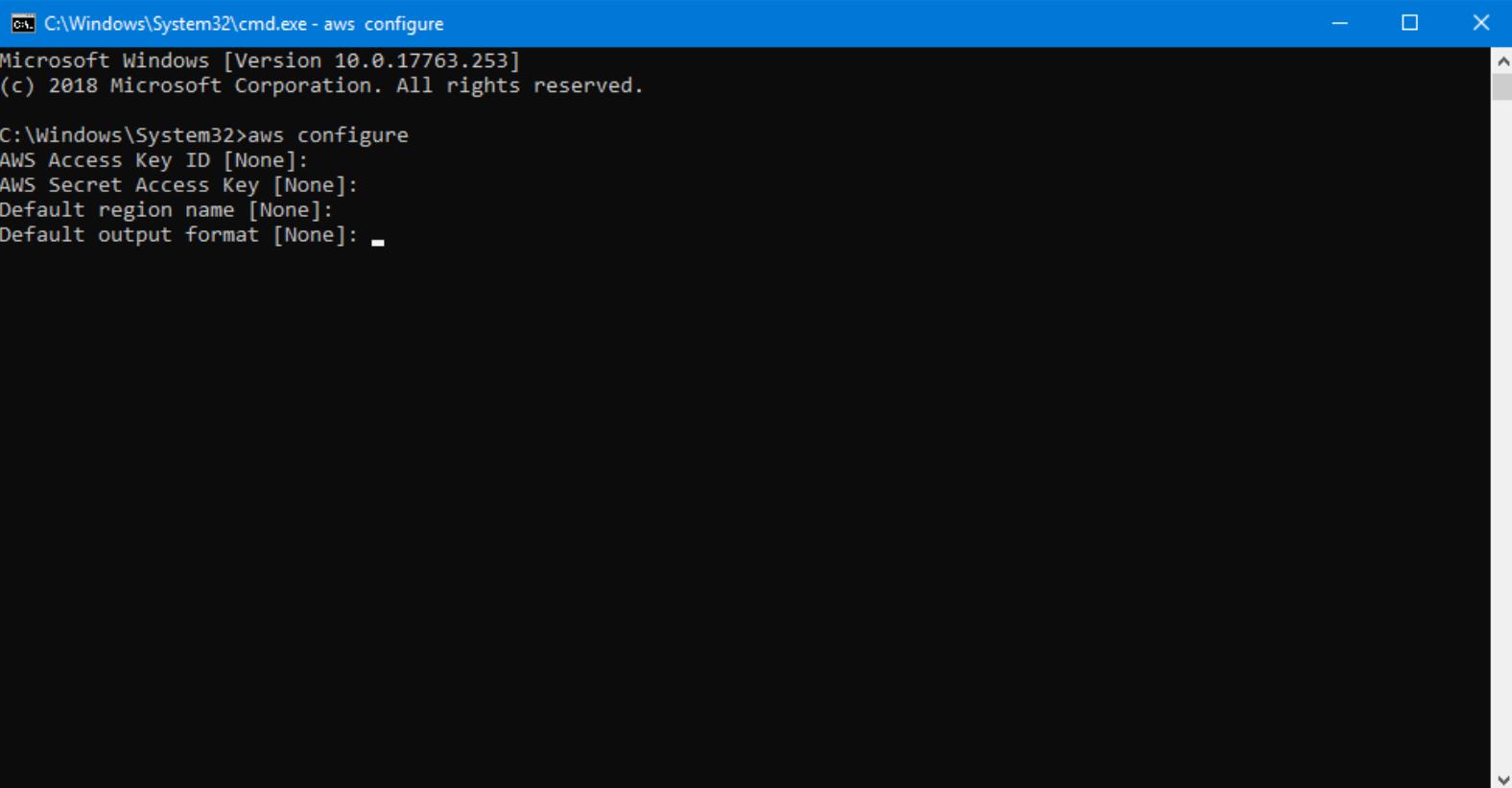


Pearson

# AWS Command Line Interface



# AWS Command Line Interface



The screenshot shows a Windows Command Prompt window titled "C:\Windows\System32\cmd.exe - aws configure". The window displays the following text:

```
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

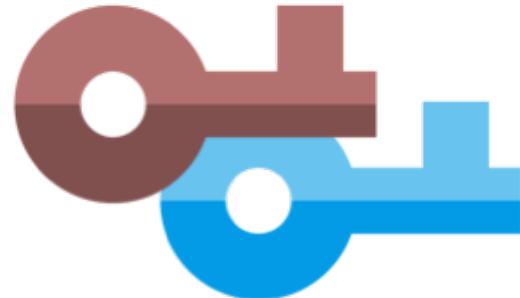
C:\Windows\System32>aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]: -
```

# Credential Usage Options

Credential Type	Use	Description
Key Pairs	<ul style="list-style-type: none"><li>· SSH login to EC2 instances</li><li>· CloudFront signed URLs</li><li>· Windows instances</li></ul>	<p>To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. Linux instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.</p>
X.509 Certificates	<ul style="list-style-type: none"><li>· Digitally signed SOAP requests to AWS APIs</li><li>· SSL server certificates for HTTPS</li></ul>	<p>X.509 certificates are only used to sign SOAP-based requests (currently used only with Amazon S3). You can have AWS create an X.509 certificate and private key that you can download, or you can upload your own certificate by using the <a href="#">Credential Report</a>.</p>

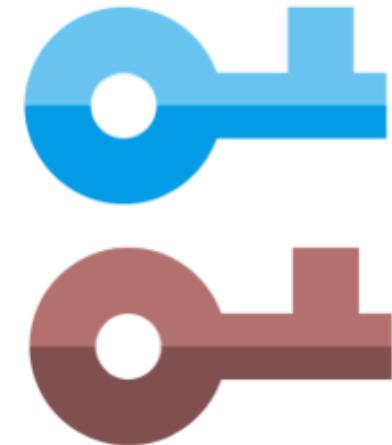
# Key Pairs

- Amazon EC2 uses public–key cryptography to encrypt and decrypt login information
- Public–key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data
- The public and private keys are known as a key pair



# 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
- Asymmetric 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



Pearson

# AWS Secrets Manager

- Protect secrets used across all of your 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

# Secrets Manager

Step 1 AWS Secrets Manager > Secrets > Store a new secret

Step 2 Secret type

Step 3 Name and description

Step 4 Configure rotation

Step 5 Review

## Store a new secret

### Select secret type Info

Credentials for RDS database

Credentials for Redshift cluster

Credentials for DocumentDB database

Credentials for other database

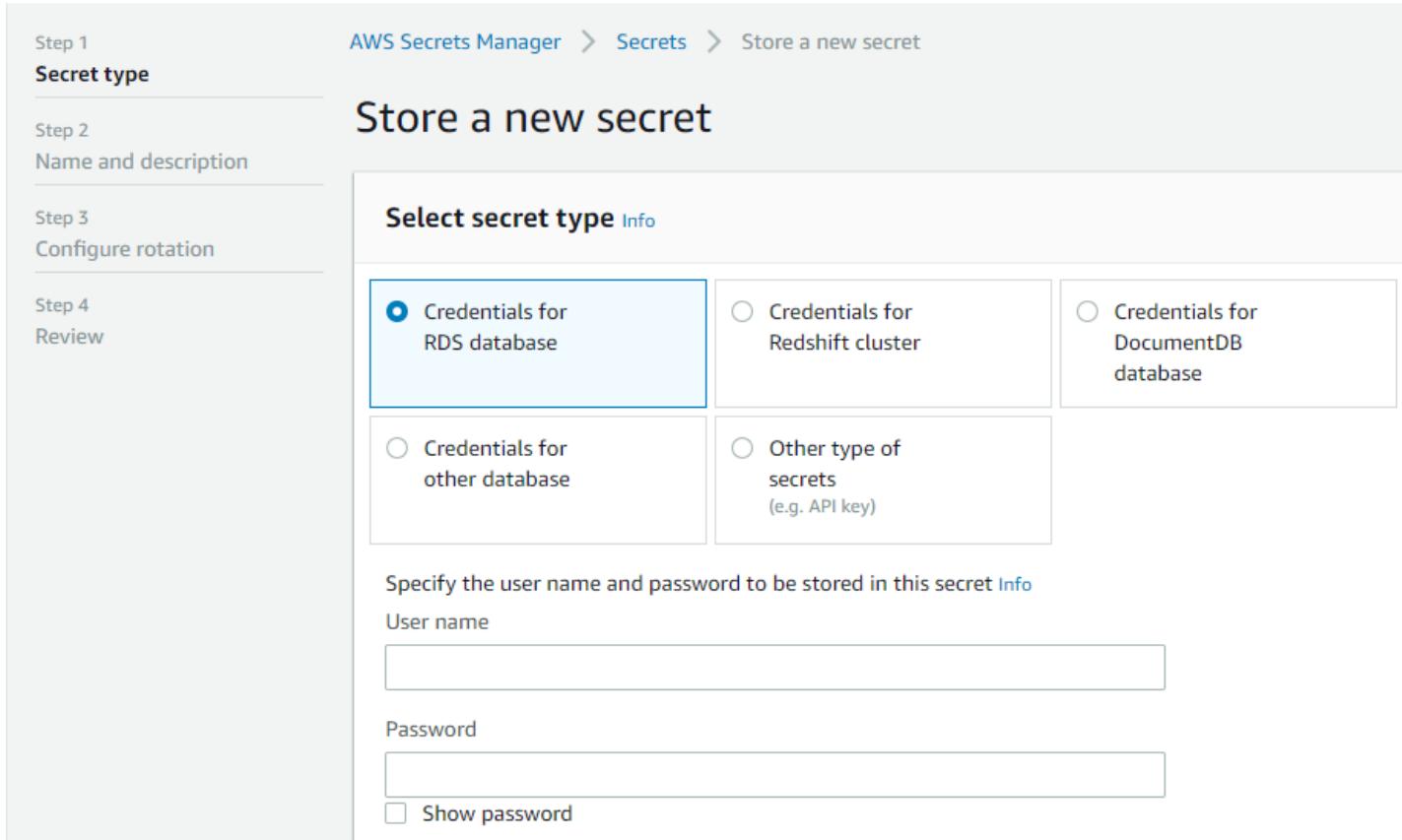
Other type of secrets (e.g. API key)

Specify the user name and password to be stored in this secret Info

User name

Password

Show password



# Secrets Manager

## Select the encryption key [Info](#)

Select the AWS KMS key to use to encrypt your secret information. You can encrypt using the default service encryption key that AWS Secrets Manager creates on your behalf or a customer master key (CMK) that you have stored in AWS KMS.

[Add new key](#) 

## Select which RDS database this secret will access [Info](#)

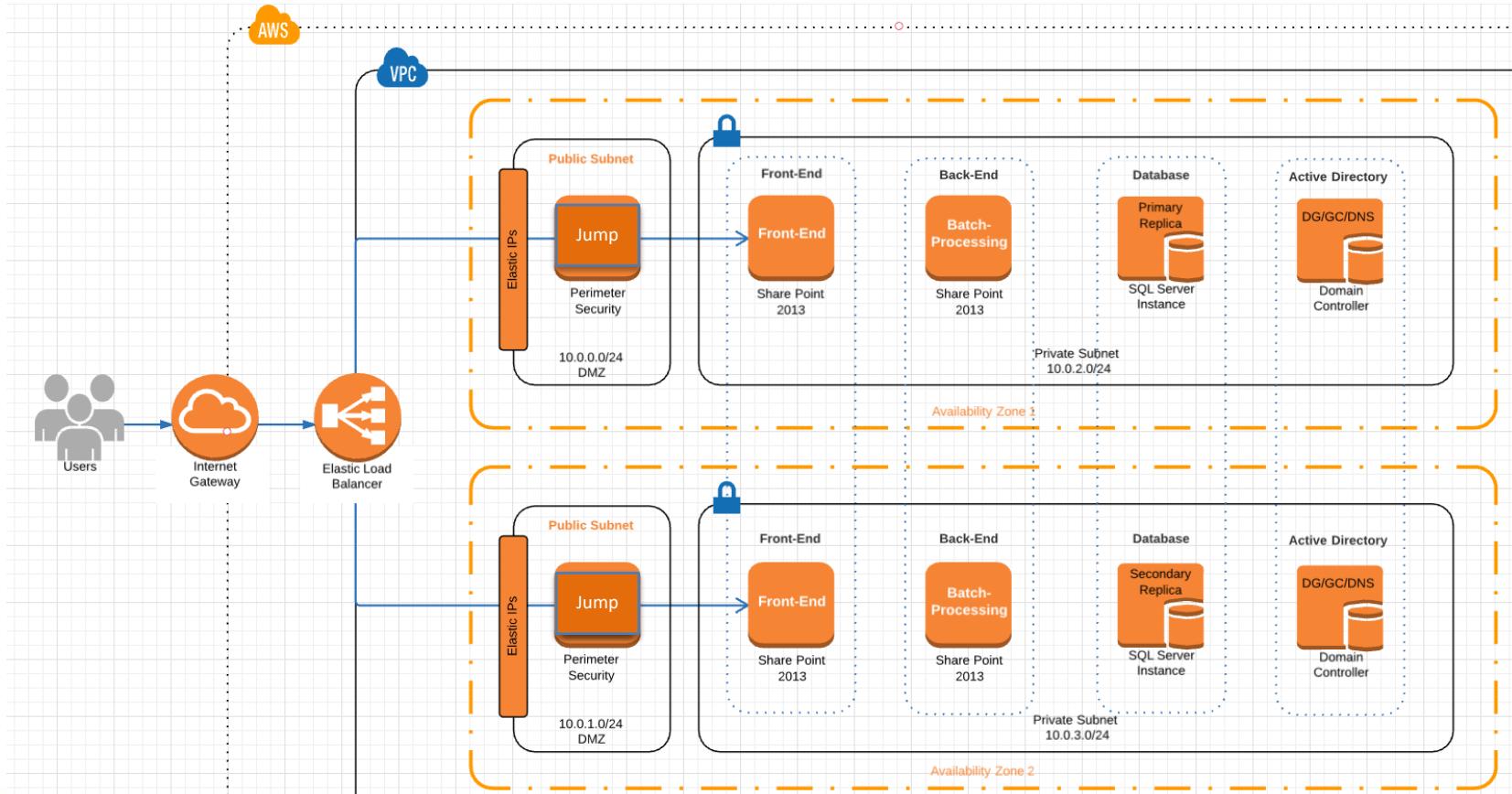
< 1 >

DB instance	DB engine	Status	Creation date
-------------	-----------	--------	---------------



No databases

# Using a Bastion (Jump) Host



# 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

- 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



@iconshock.com

# 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

**Compliance dashboard filtering**

Group dashboard results based on

- Compliance type
- Patch group
- Resource group

Filter further  Resources  Rules

**Compliance resources summary**

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

Compliance Overall



Pearson

# Session Manager Makes it Easy

1) Configure your instances to use Session Manager

2) Assign user IAM policies to control instance access

3) Specify account options for session logs

4) Start a session on your instances by launching bash or shell terminal

# 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
- **<https://aws.amazon.com/blogs/security/>**



@iconshock.com

# AppStream 2.0 Process

1. Using an HTML5 desktop browser the user logs on to a Single Sign-On URL, authenticating the user against the corporate directory using SAML 2.0 federation
2. After successful authentication the user will see a list of provisioned applications such as RDP and Putty
3. The applications are only visible within the browser and with its underlying OS hidden
4. The user then connects to the backend systems over the ports opened through security groups
5. The user logs off and AppStream 2.0 destroys the instance used for the session.



## Segment 2: Identity and Access Management (IAM)

# 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

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=us-east-2#/account\\_settings](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), Credential report, and Encryption keys. The main content area is titled 'Password Policy'. It explains what a password policy is and states that the account does not have one. It includes fields for minimum password length (set to 6) and several checkboxes for password requirements. The 'Allow users to change their own password' checkbox is checked. Buttons at the bottom are 'Apply password policy' (blue) and 'Delete password policy' (red).

IAM Management Console | Understanding and Gettin... | +

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

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:

Require at least one uppercase letter ⓘ

Require at least one lowercase letter ⓘ

Require at least one number ⓘ

Require at least one non-alphanumeric character ⓘ

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)

Screenshot of the AWS IAM Management Console home page.

The left sidebar shows the navigation menu:

- Search IAM
- Dashboard**
- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report
- Encryption keys

The main content area includes:

- Welcome to Identity and Access Management**
- IAM users sign-in link:** <https://1234567890.signin.aws.amazon.com/console> (Customize | Copy Link)
- IAM Resources**
  - Users: 0
  - Groups: 0
  - Customer Managed Policies: 0
  - Roles: 0
  - Identity Providers: 0
- Security Status**: 1 out of 5 complete.
  - Completed:** Delete your root access keys
  - Pending:** Activate MFA on your root account
  - Pending:** Create individual IAM users
  - Pending:** Use groups to assign permissions
  - Pending:** Apply an IAM password policy
- Feature Spotlight**: Introduction to AWS IAM (Video thumbnail)
- Additional Information**
  - IAM best practices
  - IAM documentation
  - Web Identity Federation Playground
  - Policy Simulator
  - Videos, IAM release history and additional resources

# IAM (continued)

The screenshot shows the AWS IAM Management Console interface. The top navigation bar includes the IAM Management Console logo, a search bar with the URL <https://console.aws.amazon.com/iam/home#/users>, and various browser controls. Below the navigation bar is the AWS header with links for Services, Resource Groups, and Support, along with user information for shankantoo.

The left sidebar contains a navigation menu with the following items:

- Dashboard
- Groups
- Users** (highlighted with a red box)
- Roles
- Policies
- Identity providers
- Account settings
- Credential report
- Encryption keys

The main content area has two primary buttons at the top: "Add user" (highlighted with a red box) and "Delete user". Below these buttons is a search bar labeled "Find users by username or access key" and a message stating "Showing 0 results". A table follows, with columns: "User name" (with a dropdown arrow), "Groups", "Access key age", "Password age", "Last activity", and "MFA". A note at the bottom of the table says "There are no IAM users. [Learn more](#)".

# IAM (continued)

IAM Management Console

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

Services Resource Groups

shankantoo Global Support

User name\* Administrator

Add another user

Select AWS access type

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



Pearson

Feedback

English (US)

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

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](#)

# IAM (continued)

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
<input checked="" type="checkbox"/> AdministratorAccess	Job function	0	Provides full access to AWS services and resources.
<input type="checkbox"/> AlexaForBusinessDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services.
<input type="checkbox"/> AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to relate...
<input type="checkbox"/> AlexaForBusinessGatewayExe...	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/> AlexaForBusinessReadOnlyAc...	AWS managed	0	Provide read only access to AlexaForBusiness services
<input type="checkbox"/> AmazonAPIGatewayAdministra...	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gateway v...

Cancel Create group



# IAM (continued)

The screenshot shows the AWS IAM Management Console with a red box highlighting the 'Review' section of a user creation wizard. The URL in the browser is https://console.aws.amazon.com/iam/home#/users\$new?step=review&accessKey&logins.

**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)

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home#/users\\$new?step=final&accessKey&login](https://console.aws.amazon.com/iam/home#/users$new?step=final&accessKey&login). The page title is "Add user". A progress bar at the top indicates four steps: 1. Details (gray), 2. Permissions (gray), 3. Review (gray), and 4. Complete (blue). A success message box is displayed, stating: "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." It includes a link to sign-in: "Users with AWS Management Console access can sign-in at: <https://4.signin.aws.amazon.com/console>". Below this is a table showing the newly created user "Administrator". The table has columns: User, Access key ID, Secret access key, and Email login instructions. The "Access key ID" column shows "AKIAIIBX4IGZMHPPV4XA" and a "Show" link. The "Email login instructions" column has a "Send email" link. A "Download .csv" button is also present. A "Close" button is located at the bottom right of the message box.

User	Access key ID	Secret access key	Email login instructions
Administrator	AKIAIIBX4IGZMHPPV4XA ***** Show		<a href="#">Send email</a>



# IAM (continued)

IAM Management Console + Close

https://console.aws.amazon.com/iam/home#/users Search

Most Visited Services Resource Groups shankhtoo Global Support

Add user Delete user

Search IAM

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

Find users by username or access key Showing 1 result

User name	Groups	Access key age	Password age	Last activity	MFA
Administrator	Admins	None	Today	None	Not enabled

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

# 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 AWS resources
- Provide access for externally authenticated users
- **Tutorial: <https://docs.aws.amazon.com/IAM/>**

# 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



**PRODUCTION**  
**Account**  
(live applications)

**DEVELOPMENT**  
**Account**  
(application sandbox)

**PRODUCTION**  
**Account**  
(live applications)

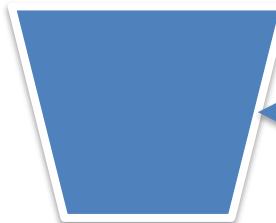
**DEVELOPMENT**  
**Account**  
(application sandbox)



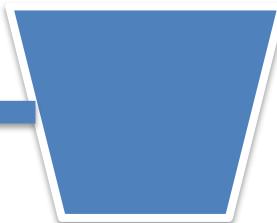
**PRODUCTION**  
**Account**  
(live applications)

**DEVELOPMENT**  
IAM: Developers and  
Testers

productionapp



Trusting Account



Trusted Account



# IAM Roles

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-east-2#/roles>. The left sidebar has a red box around the 'Roles' link under the 'AWS Services' section. The main content area has a red box around the 'Create role' button at the top of the role list table.

**What are IAM roles?**

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

**Additional resources:**

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

Create role		Delete role
<input type="text"/> Search		
	Role name ▾	Description
<input type="checkbox"/>	Bastion	Allows EC2 instances to call AWS services on your behalf.

# IAM Roles

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=us-east-2#/roles\\$new?step=type](https://console.aws.amazon.com/iam/home?region=us-east-2#/roles$new?step=type). The page is titled "Create role" and displays the first step: "Select type of trusted entity". There are four options: "AWS service" (selected), "Another AWS account", "Web identity", and "SAML 2.0 federation". Below this, a note states "Allows AWS services to perform actions on your behalf." A link to "Learn more" is provided. The next section, "Choose the service that will use this role", lists various AWS services. The "EC2" option is selected and highlighted with a red box, with the sub-note "Allows EC2 instances to call AWS services on your behalf.". Other listed services include Lambda, API Gateway, AWS Support, AppSync, Application Auto Scaling, Auto Scaling, Batch, CloudFormation, CloudHSM, CloudWatch Events, CodeBuild, CodeDeploy, Config, DMS, Data Pipeline, DeepLens, Directory Service, DynamoDB, ElastiCache, Elastic Beanstalk, Elastic Container Service, Elastic Transcoder, Elastic Load Balancing, Glue, GuardDuty, Inspector, IoT, Kinesis, Lambda, Lex, Machine Learning, MediaConvert, OpsWorks, Redshift, SageMaker, SNS, SWF, Service Catalog, Step Functions, Storage Gateway, Trusted Advisor, and Rekognition.

Create role

Select type of trusted entity

1 2 3

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 AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

**EC2**  
Allows EC2 instances to call AWS services on your behalf.

**Lambda**  
Allows Lambda functions to call AWS services on your behalf.

API Gateway	CodeDeploy	EMR	IoT	S3
AWS Support	Config	ElastiCache	Kinesis	SMS
AppSync	DMS	Elastic Beanstalk	Lambda	SNS
Application Auto Scaling	Data Pipeline	Elastic Container Service	Lex	SWF
Auto Scaling	DeepLens	Elastic Transcoder	Machine Learning	SageMaker
Batch	Directory Service	Elastic Load Balancing	MediaConvert	Service Catalog
CloudFormation	DynamoDB	Glue	OpsWorks	Step Functions
CloudHSM	EC2	Greengrass	RDS	Storage Gateway
CloudWatch Events	EC2 - Fleet	GuardDuty	Redshift	Trusted Advisor
CodeBuild	EKS	Inspector	Rekognition	

# IAM Roles

## Create role

1 2 3

### Attach permissions policies

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

[Create policy](#)

Refresh

Filter: Policy type	Policy name	Attachments	Description
<input type="checkbox"/>	AmazonEC2SpotFleetAutoscaleRole	0	Policy to enable Autoscaling for Amazon EC2 Spot Fleet
<input type="checkbox"/>	AmazonEC2SpotFleetRole	0	Allows EC2 Spot Fleet to request and terminate Spot Inst...
<input type="checkbox"/>	AmazonEC2SpotFleetTaggingRole	0	Allows EC2 Spot Fleet to request, terminate and tag Spot ...
<input checked="" type="checkbox"/>	AmazonECS_FullAccess	0	Provides administrative access to Amazon ECS resources...
<input type="checkbox"/>	AmazonECSServiceRolePolicy	0	Policy to enable Amazon ECS to manage your cluster.
<input type="checkbox"/>	AmazonECSTaskExecutionRolePolicy	0	Provides access to other AWS service resources that are ...
<input type="checkbox"/>	AmazonEKS_CNI_Policy	0	This policy provides the Amazon VPC CNI Plugin (amazon...
<input type="checkbox"/>	AmazonEKSClusterPolicy	0	This policy provides Kubernetes the permissions it requir...
<input type="checkbox"/>	AmazonEKSServicePolicy	0	This policy allows Amazon Elastic Container Service for K...
<input type="checkbox"/>	AmazonEKSWorkerNodePolicy	0	This policy allows Amazon EKS worker nodes to connect t...
<input type="checkbox"/>	AmazonElastiCacheFullAccess	0	Provides full access to Amazon ElastiCache via the AWS ...
<input type="checkbox"/>	AmazonElastiCacheReadOnlyAccess	0	Provides read only access to Amazon ElastiCache via the...

# IAM Roles

## Create role

1 2 3

### Attach permissions policies

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

[Create policy](#)

Refresh

Policy name		Attachments	Description
<input type="checkbox"/>	AWSLambdaENIManagementAccess	0	Provides minimum permissions for a Lambda function to ...
<input type="checkbox"/>	AWSLambdaExecute	0	Provides Put, Get access to S3 and full access to CloudW...
<input checked="" type="checkbox"/>	AWSLambdaFullAccess	0	Provides full access to Lambda, S3, DynamoDB, CloudW...
<input type="checkbox"/>	AWSLambdaInvocation-DynamoDB	0	Provides read access to DynamoDB Streams.
<input type="checkbox"/>	AWSLambdaKinesisExecutionRole	0	Provides list and read access to Kinesis streams and writ...
<input type="checkbox"/>	AWSLambdaReadOnlyAccess	0	Provides read only access to Lambda, S3, DynamoDB, Cl...
<input type="checkbox"/>	AWSLambdaReplicator	0	Grants Lambda Replicator necessary permissions to repli...
<input type="checkbox"/>	AWSLambdaRole	0	Default policy for AWS Lambda service role.
<input type="checkbox"/>	AWSLambdaSQSExecutionRole	0	Provides receive message, delete message, and read attr...
<input type="checkbox"/>	AWSLambdaVPCAccessExecutionRole	0	Provides minimum permissions for a Lambda function to e...
<input type="checkbox"/>	AWSMarketplaceFullAccess	0	Provides the ability to subscribe and unsubscribe to AWS ...
<input type="checkbox"/>	AWSMarketplaceGetEntitlements	0	Provides read access to AWS Marketplace Entitlements

# IAM Roles

The screenshot shows the AWS IAM Management Console interface. The URL in the browser is <https://console.aws.amazon.com/iam/home?region=us-east-2#roles/JumpHost>. The left sidebar has a 'Roles' section highlighted with an orange border. The main content area shows the 'JumpHost' role summary. The role ARN is arn:aws:iam::219258942154:role/JumpHost. The role description allows EC2 instances to call AWS services on your behalf. The instance profile ARNs are arn:aws:iam::219258942154:instance-profile/JumpHost. The path is /. The creation time is 2018-06-13 13:46 CDT. The maximum CLI/API session duration is 1 hour (3,600 seconds). Below the summary, there are tabs for 'Permissions', 'Trust relationships', 'Access Advisor', and 'Revoke sessions'. The 'Permissions' tab is selected, showing an 'Attach policy' button and a list of attached policies: 'AWSLambdaFullAccess' and 'AmazonECS\_FullAccess'. A red box highlights the 'JumpHost' link in the breadcrumb navigation.

IAM Management Console

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

Services Resource Groups

Search IAM

Dashboard

Groups

Users

**Roles**

Policies

Identity providers

Account settings

Credential report

Encryption keys

Roles > **JumpHost**

## Summary

Role ARN: arn:aws:iam::219258942154:role/JumpHost

Role description: Allows EC2 instances to call AWS services on your behalf. | Edit

Instance Profile ARNs: arn:aws:iam::219258942154:instance-profile/JumpHost

Path: /

Creation time: 2018-06-13 13:46 CDT

Maximum CLI/API session duration: 1 hour (3,600 seconds) | Edit

**Permissions** **Attached policies: 2**

Policy name ▾

- ▶ AWSLambdaFullAccess
- ▶ AmazonECS\_FullAccess

# IAM Roles

EC2 Management Console +

[https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:](#)

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign

Number of instances 1 Launch into Auto Scaling Group i

Purchasing option  Request Spot instances

Network vpc-1f30fc77 (default) C Create new VPC

Subnet No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP Use subnet setting (Enable)

Placement group  Add instance to placement group.

**IAM role** None C Create new IAM role

**Shutdown behavior** JumpHost

Enable termination protection  Protect against accidental termination

Monitoring  Enable CloudWatch detailed monitoring  
Additional charges apply.

Tenancy Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

T2 Unlimited  Enable  
Additional charges may apply

# 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.

# 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

# 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.

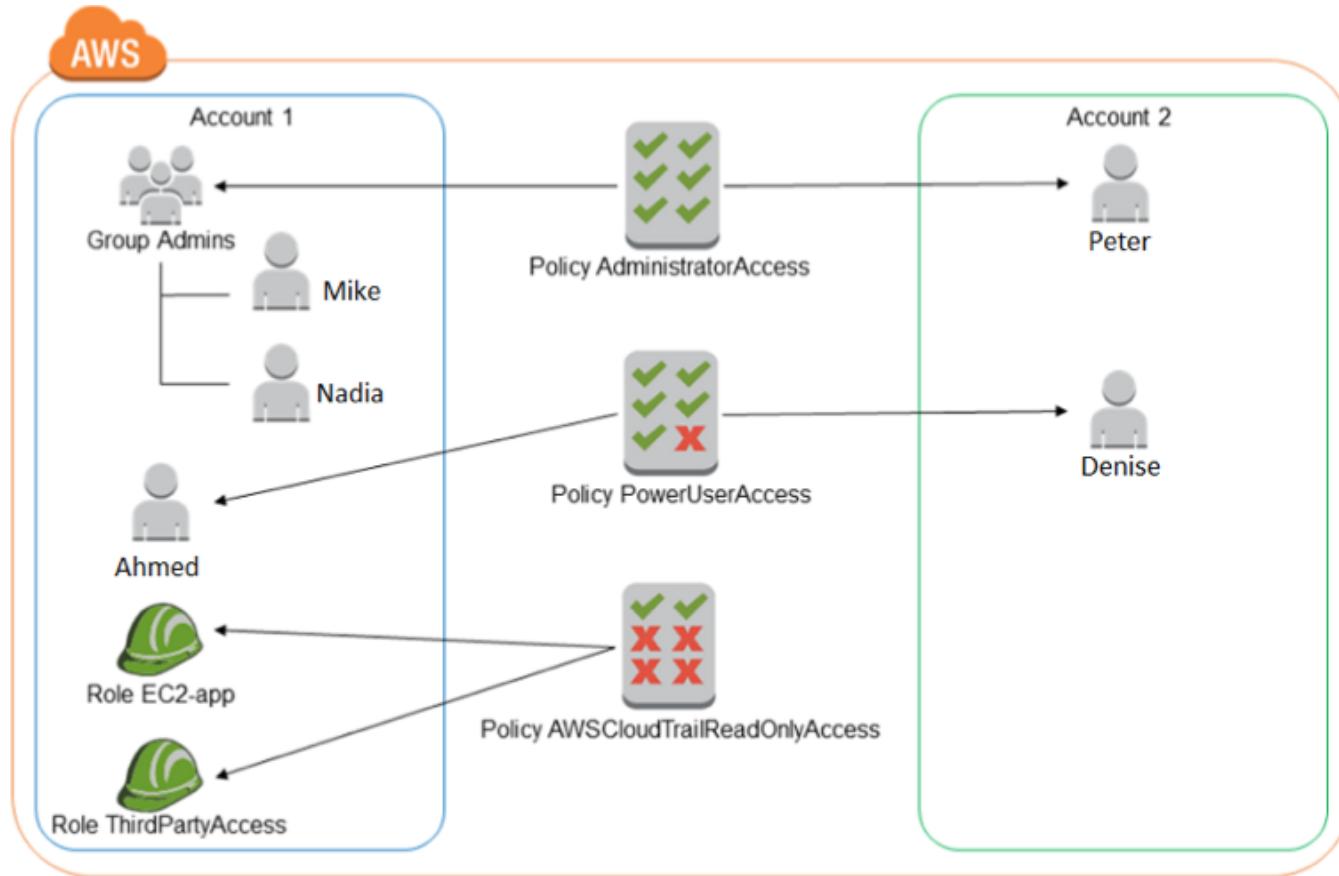
Create policy Refresh

Filter: Policy type ▾ Search Showing 343 results

	Policy name	Attachments	Description
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	0	Default policy for the Amazon EC2 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

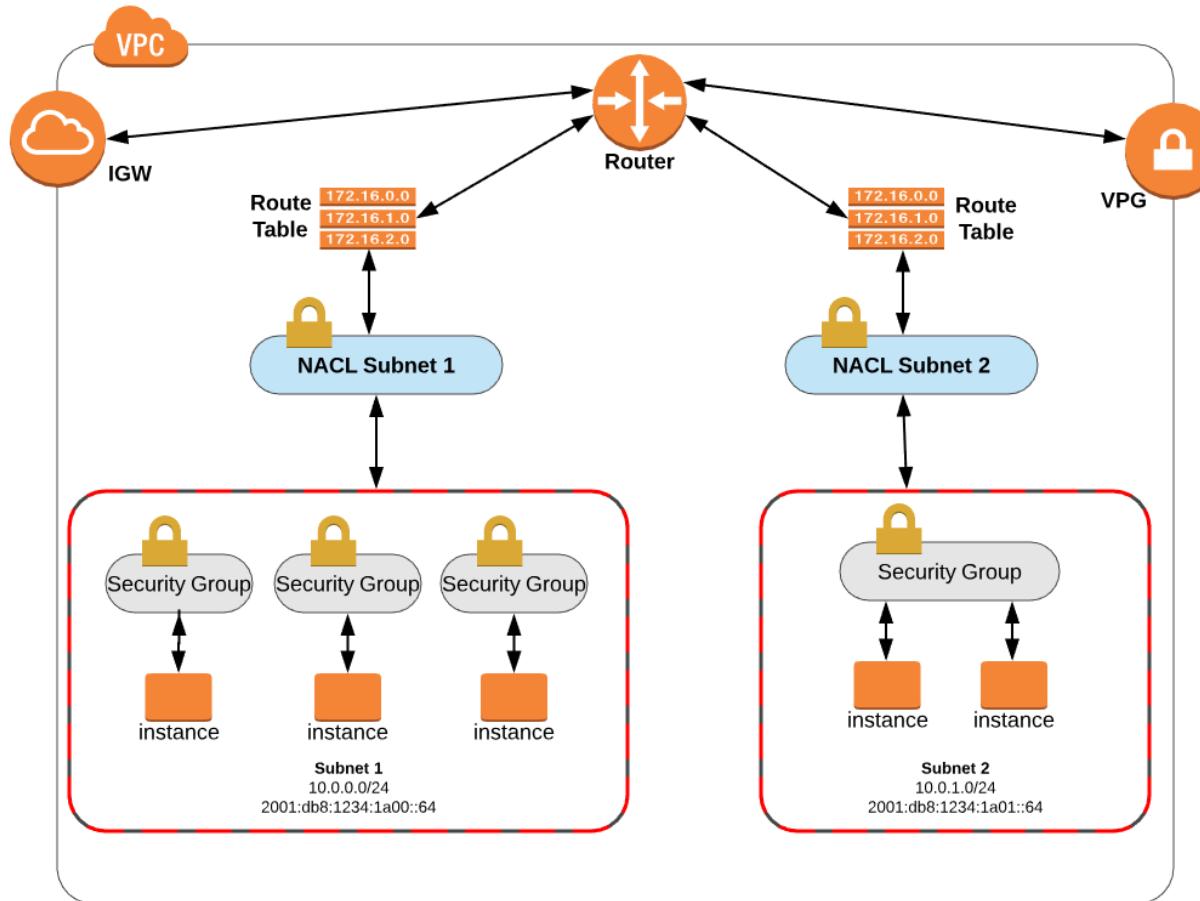
# AWS Managed Policies



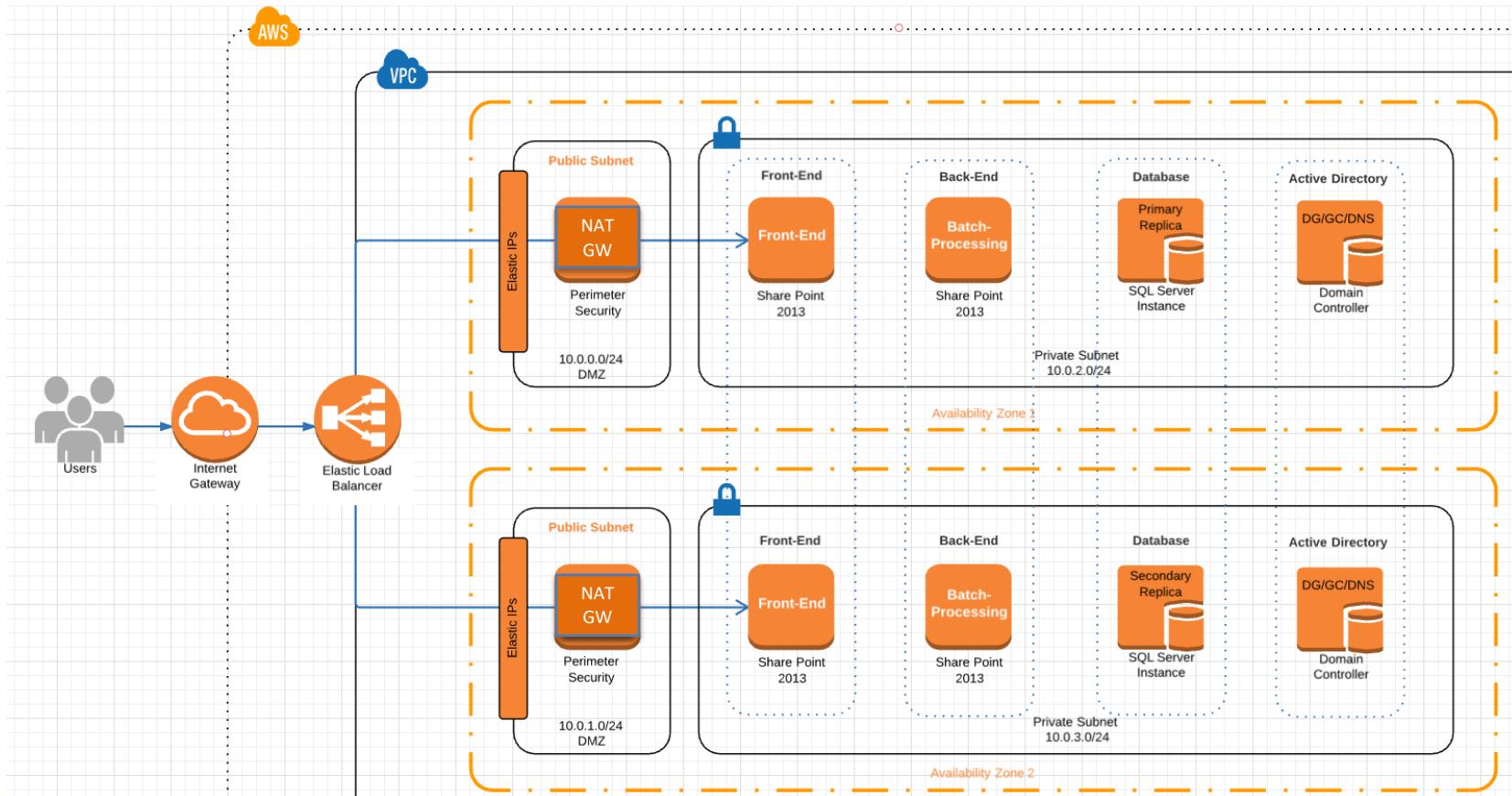


## Segment 3: Infrastructure Security

# Infrastructure Security Begins with Design



# Infrastructure Security Begins with Design



# VPC with Public & Private Subnets

VPC Management Console X + https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#wizardSelector: Search

Most Visited

aws Services Resource Groups shankhantoo

## Step 1: Select a VPC Configuration

**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**

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

**Creates:**

A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via Network Address Translation (NAT). (Hourly charges for NAT devices apply.)

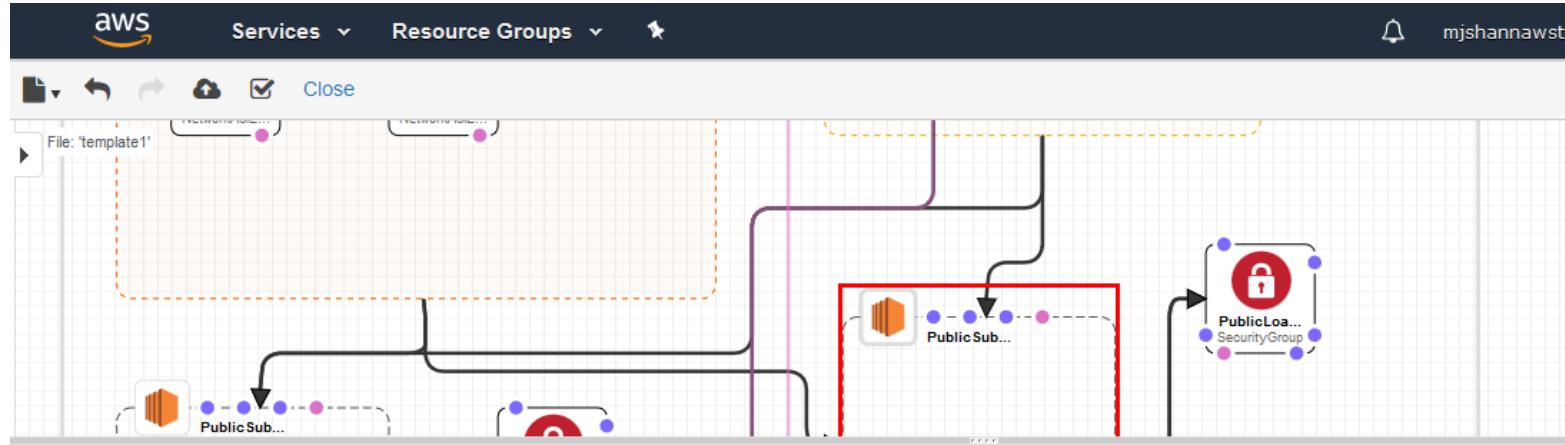
Select

```
graph TD; Internet["Internet, S3, DynamoDB, SNS, SQS, etc."] --- VPC[Amazon Virtual Private Cloud]; VPC --- PublicSubnet[Public Subnet]; VPC --- PrivateSubnet[Private Subnet]; PublicSubnet --- NAT[NAT]; PrivateSubnet --- NAT
```

# AWS CloudFormation Templates

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.	<a href="#">View</a>	<a href="#">View in Designer</a>	<a href="#">Launch Stack</a> 
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.	<a href="#">View</a>	<a href="#">View in Designer</a>	<a href="#">Launch Stack</a> 
Autoscaling and load-balancing website in an Amazon VPC	Creates a load balancing, auto scaling sample website in an existing VPC.	<a href="#">View</a>	<a href="#">View in Designer</a>	<a href="#">Launch Stack</a> 
Amazon VPC with DNS and public IP addresses	Creates a VPC with DNS support and public IP addresses enabled.	<a href="#">View</a>	<a href="#">View in Designer</a>	<a href="#">Launch Stack</a> 
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.	<a href="#">View</a>	<a href="#">View in Designer</a>	<a href="#">Launch Stack</a> 
Amazon EC2 with multiple dynamic IP addresses in an Amazon VPC	Creates an Amazon EC2 instance with multiple dynamic IP addresses in a VPC.	<a href="#">View</a>	<a href="#">View in Designer</a>	<a href="#">Launch Stack</a> 

# AWS CloudFormation Templates



Choose template language:  **JSON**  **YAML** [?](#)

```
temp... 
```

```
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": "22<br/>0.0.0.0/0"  
14    }  
15  }  
16 }<
```

# 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  
  
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.

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

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

# 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

### 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.

### CloudTrailCWLogsRetentionTime

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

### CloudTrailS3RetentionTime

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

### CloudTrailEncryptS3Logs

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

# 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

**i** 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

# Options for Protecting VPC

- **Internet-only**
  - Carefully plan routing and server placement in public and private subnets
  - Encrypt application and administrative traffic using SSL/TLS, or build custom user VPN solutions
  - Use security groups and NACLs
- **IPSec over the Internet**
  - Establish a private IPSec connection using IKEv1 and IPSec using standard AWS VPN facilities
  - Or establish customer- specific VPN software infrastructure in the cloud, and on-premises

# Options for Protecting VPC

- **AWS Direct Connect without IPSec**
  - Depending on your data protection requirements, you might not need additional protection over private peering.
- **AWS Direct Connect with IPSec**
  - Establish a private IPSec connection using IKEv1 and IPSec using standard AWS VPN facilities
  - Or establish customer- specific VPN software infrastructure in the cloud, and on-premises
- **PrivateLink** – leverages VPC endpoints and EINs
- **Hybrid** - Using a combination of these approaches

# AWS Site-to-Site VPN

The screenshot shows the AWS VPC Management Console interface. The left sidebar lists various VPC resources: Your VPCs, Subnets, 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 main content area is titled 'Resources' and displays statistics for the US East (Ohio) region. A red box highlights the 'VPN Connections' section, which contains a brief description of AWS VPC and a 'Create VPN Connection' button.

VPC Dashboard

Filter by 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

Network ACLs

Security Groups

**Resources**

**Start VPC Wizard** **Launch EC2 Instances**

Note: Your Instances will launch in the US East (Ohio) region.

You are using the following Amazon VPC resources in the US East (Ohio) region:

1 VPC	2 Internet Gateways
0 Egress-only Internet Gateways	3 Subnets
1 Route Table	1 Network ACL
0 Elastic IPs	0 VPC Peering Connections
0 Endpoints	0 Nat Gateways
1 Security Group	0 Running Instances
0 VPN Connections	0 Virtual Private Gateways
0 Customer Gateways	1 DHCP Options Set

**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**

**Service Health**

Current Status	Details
<span style="color: green;">✓</span> Amazon VPC - US East (Ohio)	Service is operating normally
<span style="color: green;">✓</span> Amazon EC2 - US East (Ohio)	Service is operating normally

[View complete service health details](#)

**Additional Information**

[VPC Documentation](#)

[All VPC Resources](#)

[Forums](#)

[Report an Issue](#)

# AWS Site-to-Site VPN

VPN Connections > Create VPN Connection

## Create VPN Connection

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.

Name tag  ⓘ

Virtual Private Gateway\*  ⚒

Customer Gateway  Existing  
 New

Customer Gateway ID  ⚒

Routing Options  Dynamic (requires BGP)  
 Static

### Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1  Generated by Amazon ⓘ

Pre-Shared Key for Tunnel 1  Generated by Amazon ⓘ

Inside IP CIDR for Tunnel 2  Generated by Amazon ⓘ

Pre-shared key for Tunnel 2  Generated by Amazon ⓘ

VPN connection charges apply once this step is complete. [View Rates](#)

# AWS Site-to-Site VPN

The screenshot shows the AWS Management Console with the 'AWS' logo and 'Most Visited' link in the top left. The top navigation bar includes 'Services' (with a dropdown arrow), 'Resource Groups' (with a dropdown arrow), and a star icon. On the right, there is a bell icon, 'Administrator @ 2', and 'Support' links. The main content area is titled 'VPN Connections > Create VPN Connection'. Below it, the section 'Create VPN Connection' is displayed. A note says: 'Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.' It also mentions 'VPN connection charges apply once this step is complete.' with a 'View Rates' link. The form fields include 'Name tag' (input field with an info icon), 'Virtual Private Gateway\*' (dropdown menu with a 'C' icon), 'Customer Gateway' (radio buttons for 'Existing' and 'New'), 'Customer Gateway ID' (dropdown menu with a 'C' icon), and 'Routing Options' (radio buttons for 'Dynamic (requires BGP)' and 'Static').

# Create Virtual Private Gateway

The screenshot shows the AWS VPC console interface for creating a new Virtual Private Gateway. The top navigation bar includes tabs for 'Create Virtual Private Gateway' and a '+' button. The URL in the address bar is <https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#CreateVirtualPrivateGateway>. The main content area is titled 'Create Virtual Private Gateway' and contains fields for 'Name tag' (empty), 'ASN' (set to 'Custom ASN' with value '64512'), and a 'Create Virtual Private Gateway' button.

Virtual Private Gateways > Create Virtual Private Gateway

## Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag

ASN  Amazon default ASN i  Custom ASN i

64512 i

[Cancel](#) [Create Virtual Private Gateway](#)

# 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

The screenshot shows the AWS Certificate Manager interface in a web browser. The title bar says "AWS Certificate Manager". The address bar shows the URL: <https://us-east-2.console.aws.amazon.com/acm/home?region=us-east-2#/wizard?firstrun=true>. The main content area is titled "Request a certificate". A sidebar on the left lists steps: "Step 1: Add domain names" (highlighted in orange), "Step 2: Select validation method", "Step 3: Review", and "Step 4: Validation".

**Step 1: Add domain names**

You can use AWS Certificate Manager certificates with other [AWS Services](#).

Choose **Import a certificate** to import an existing certificate instead of requesting a new one. [Learn more.](#) [\*\*Import a certificate\*\*](#)

**Add domain names**

Type the fully qualified domain name of the site you want to secure with an SSL/TLS certificate (for example, www.example.com). Use an asterisk (\*) to request a wildcard certificate to protect several sites in the same domain. For example: \*.example.com protects www.example.com, site.example.com and images.example.com.

**Domain name\***

Domain name*	Remove
www.trainologie.com	X
trainologie.com	X
*.trainologie.com	X

[\*\*Add another name to this certificate\*\*](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name. [Learn more.](#)

**\*At least one domain name is required**

[Cancel](#) [\*\*Next\*\*](#)

# Create Virtual Private Gateway

**Customer Gateway**

Existing

New

**Customer Gateway ID**



**Routing Options**

Dynamic (requires BGP)

Static

## Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

**Inside IP CIDR for Tunnel 1**

Generated by Amazon



**Pre-Shared Key for Tunnel 1**

Generated by Amazon



**Inside IP CIDR for Tunnel 2**

Generated by Amazon



**Pre-shared key for Tunnel 2**

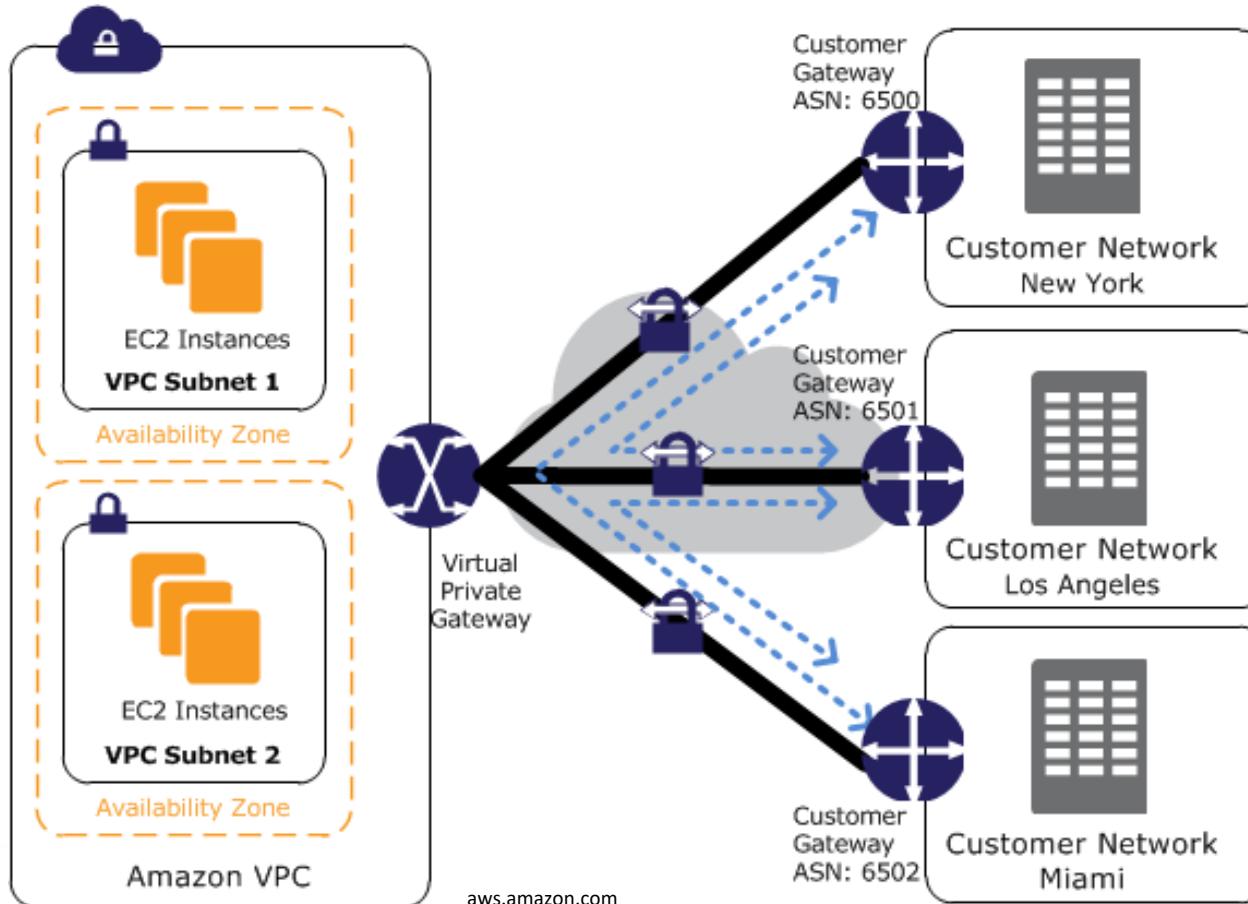
Generated by Amazon



[Cancel](#)

[Create VPN Connection](#)

# AWS CloudHub VPN



# AWS Client VPN Endpoints



## Create Client VPN Endpoint

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

Name Tag  i

Description  i

Client IPv4 CIDR\*  i

### Authentication Information

Server certificate ARN\*  C i

Authentication Options Choose one or more authentication methods from below i

Use mutual authentication

Use user-based authentication

Active Directory authentication

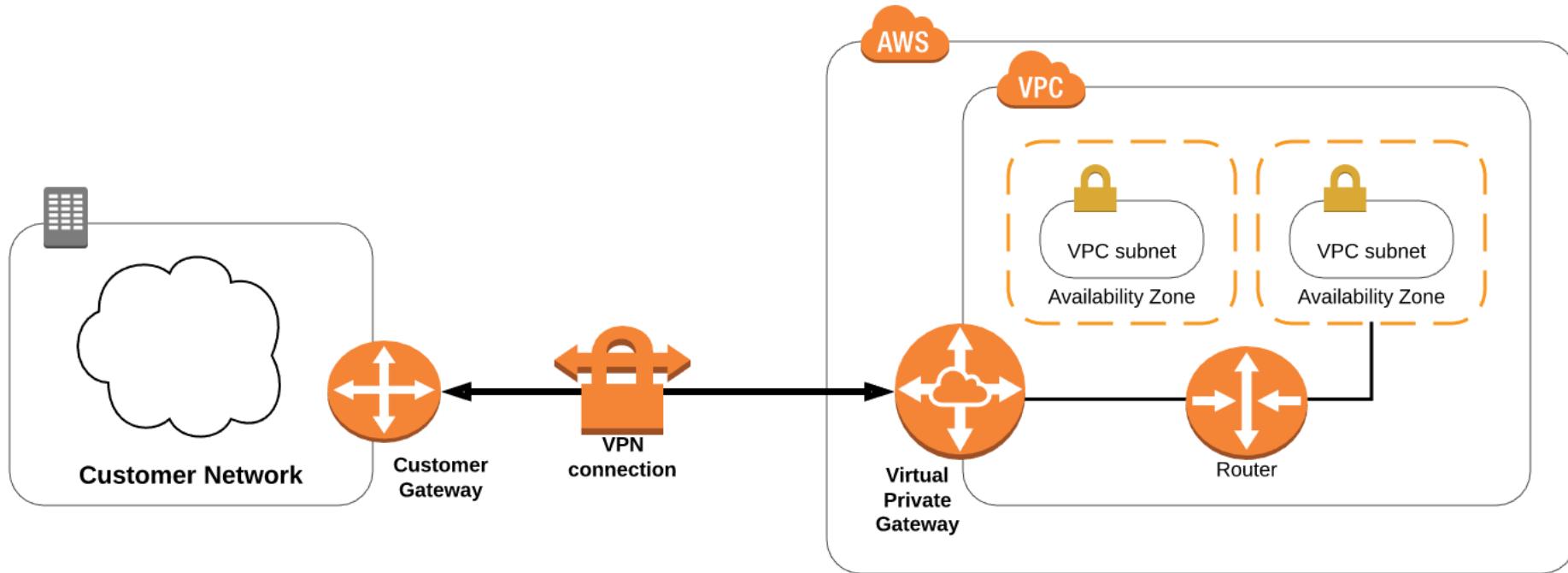
Client certificate ARN\*  C i

Directory ID\*  C i

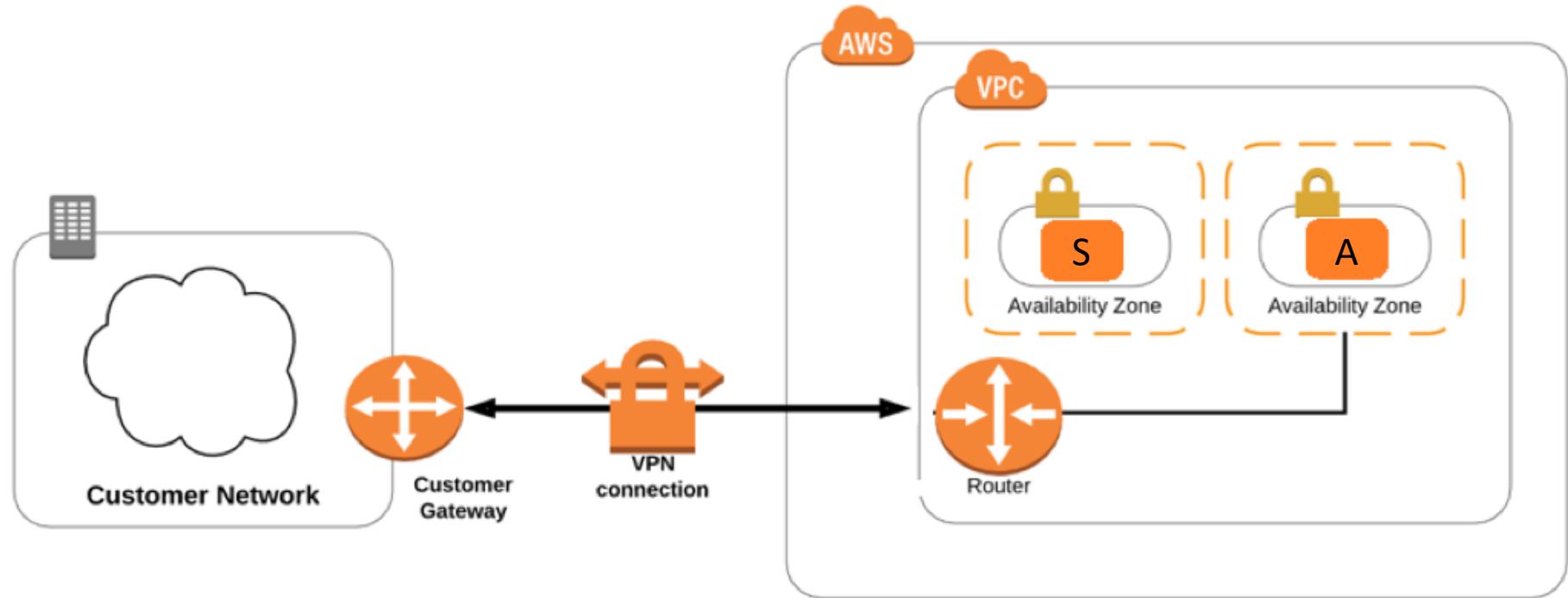
# AWS Site-to-Site (Managed) VPNs

- 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



# EC2 Instance to Terminate VPN



# AWS Marketplace

aws marketplace

View Categories ▾ Your Saved List

AMI & SaaS ▾

Fortinet Inc. (20)

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)

 **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)

 **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)

 **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 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