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

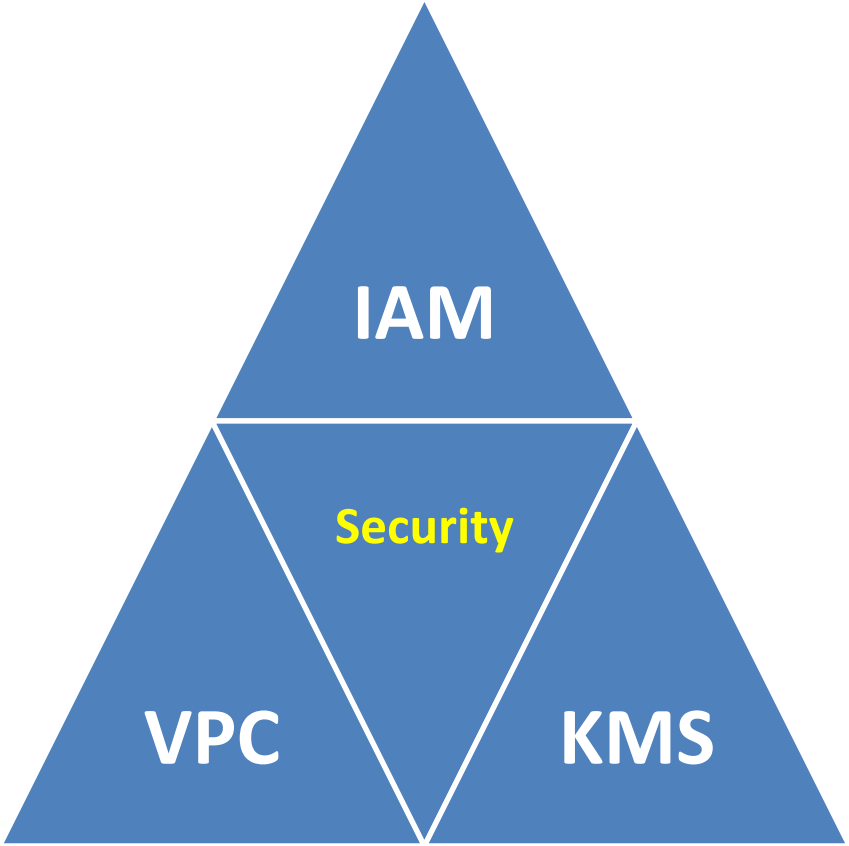
Segment 1: AWS Security Triad, Security Pillar Shared Security Responsibility Model and Credential Management

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

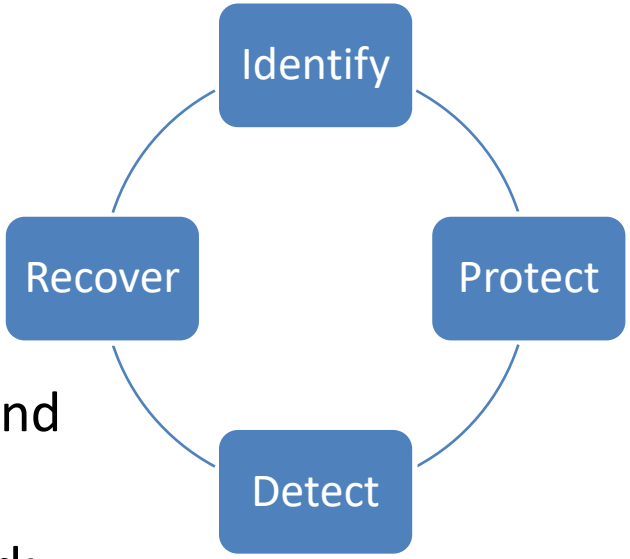
Design Principles in the Cloud

- 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

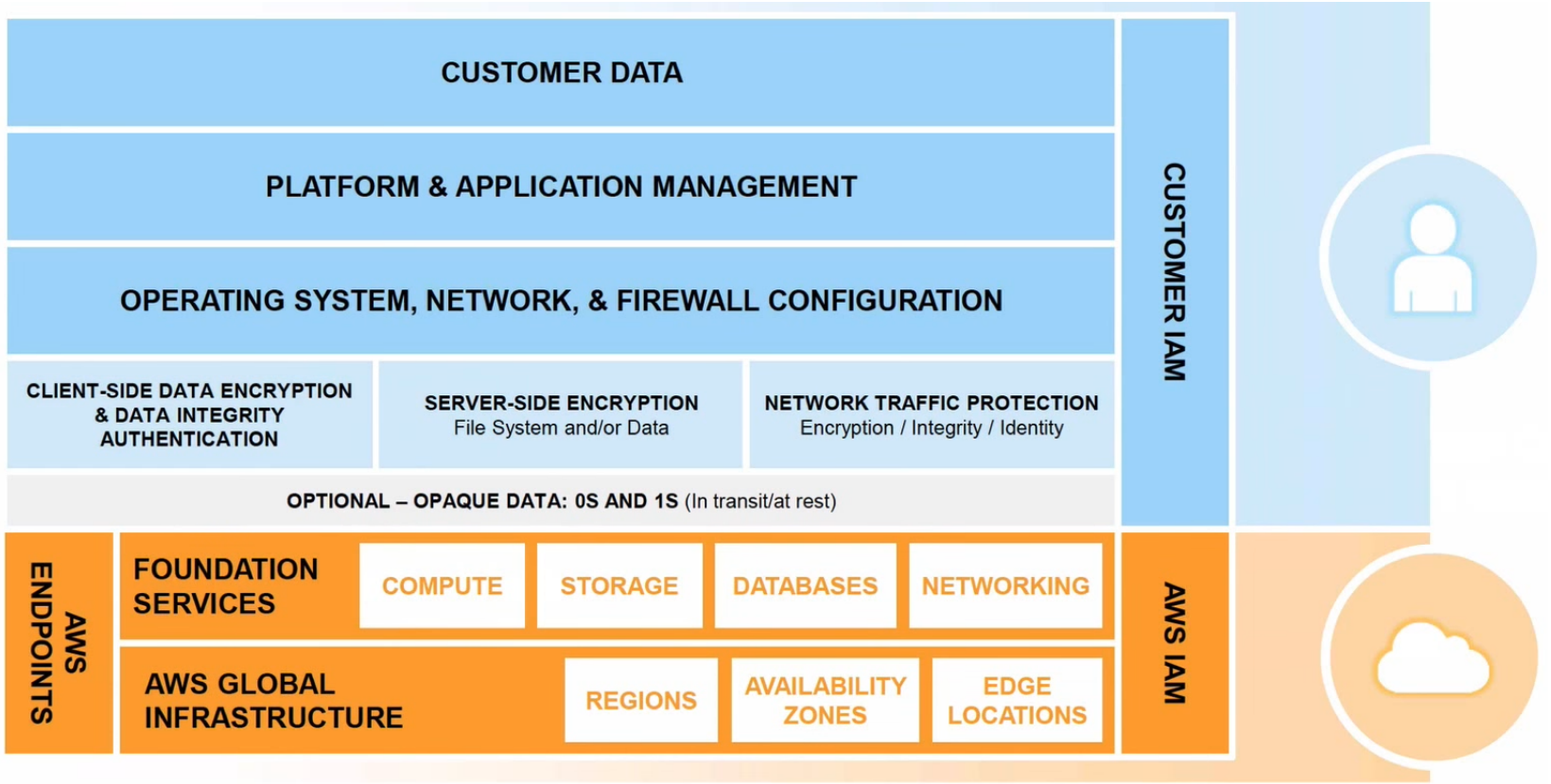
- The AWS Foundational Security Best Practices standard is a set of controls that detect deviations from security best practices
- It allows you to continuously appraise all accounts and workloads to rapidly detect and analyze gaps
- Based on the NIST Cybersecurity Framework



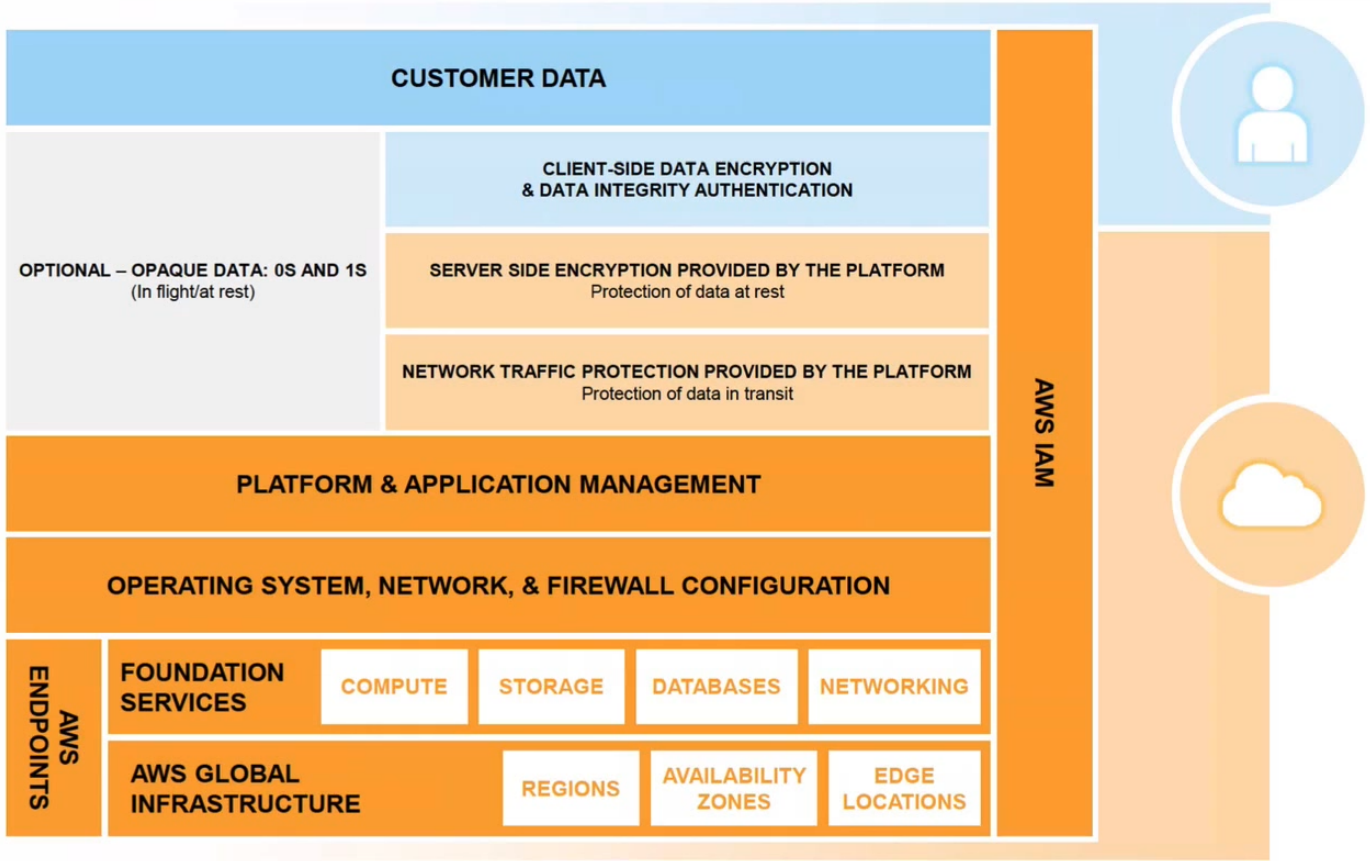
AWS Responsibilities

- 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.

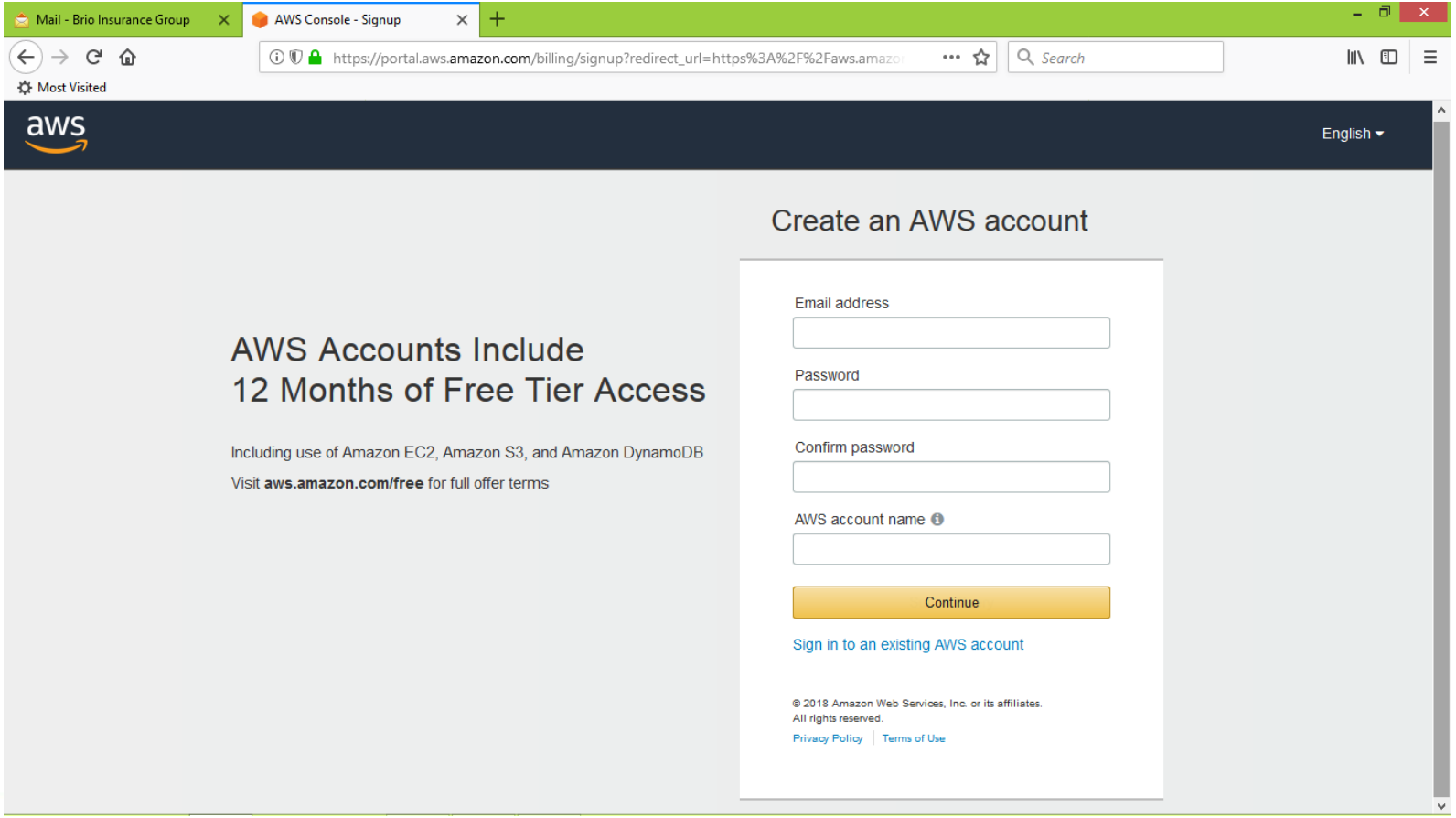
Shared Security Model (EC2/VPC/EBS)



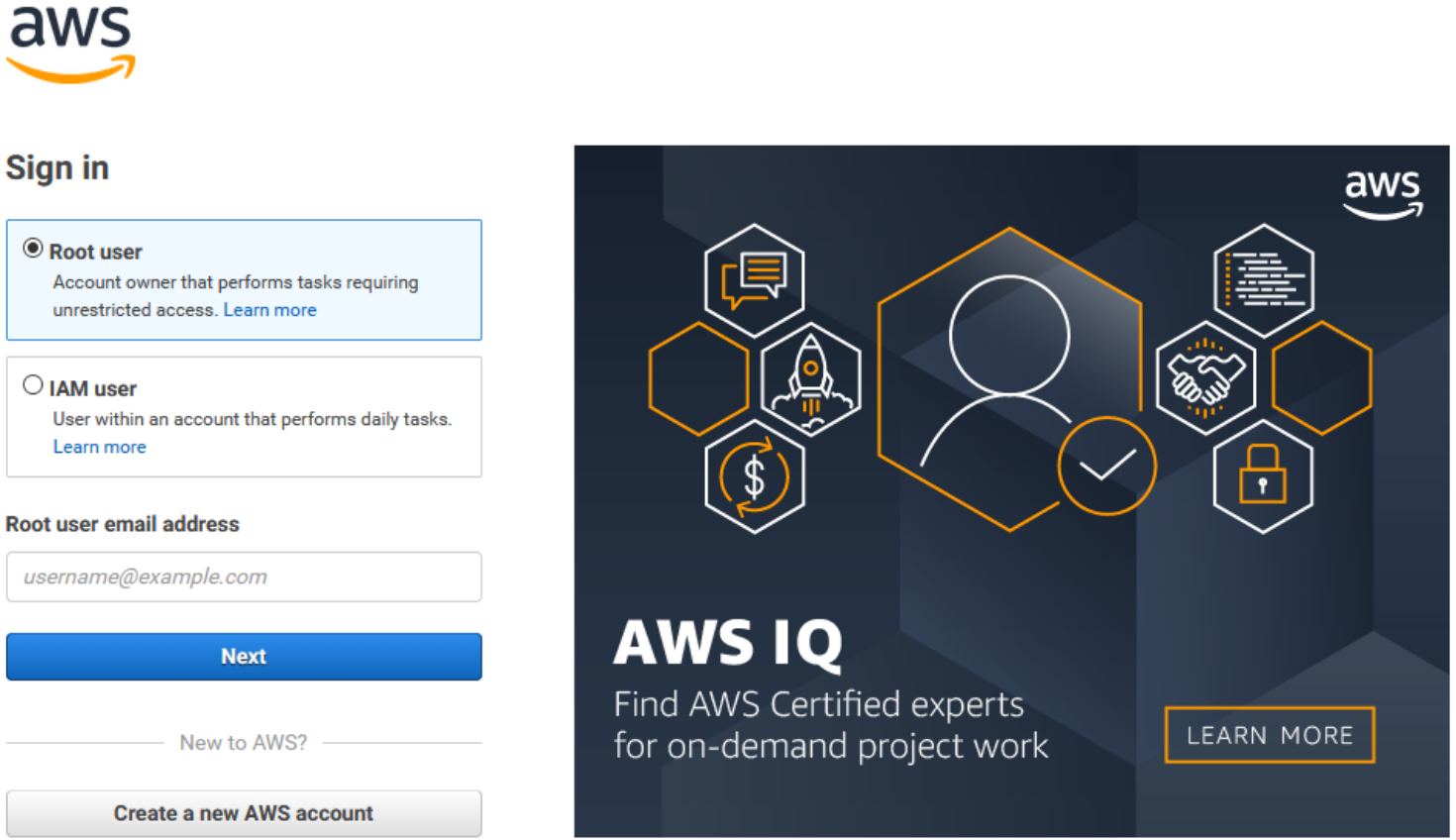
Shared Security Model (S3/DynamoDB)



Credentials: AWS Root Account



Credentials: AWS Root Account



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

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

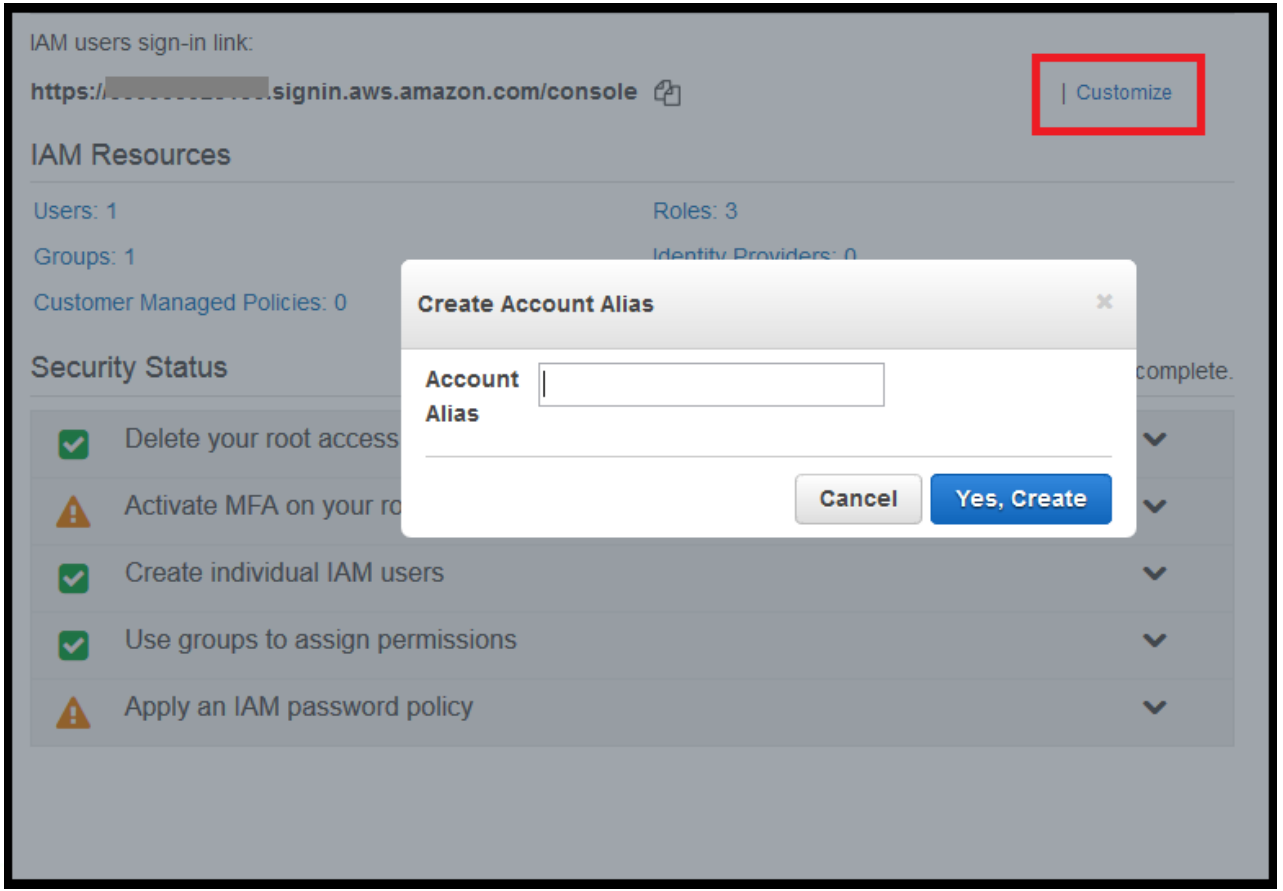
Your sign-in page URL has the following format, by default.

```
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.

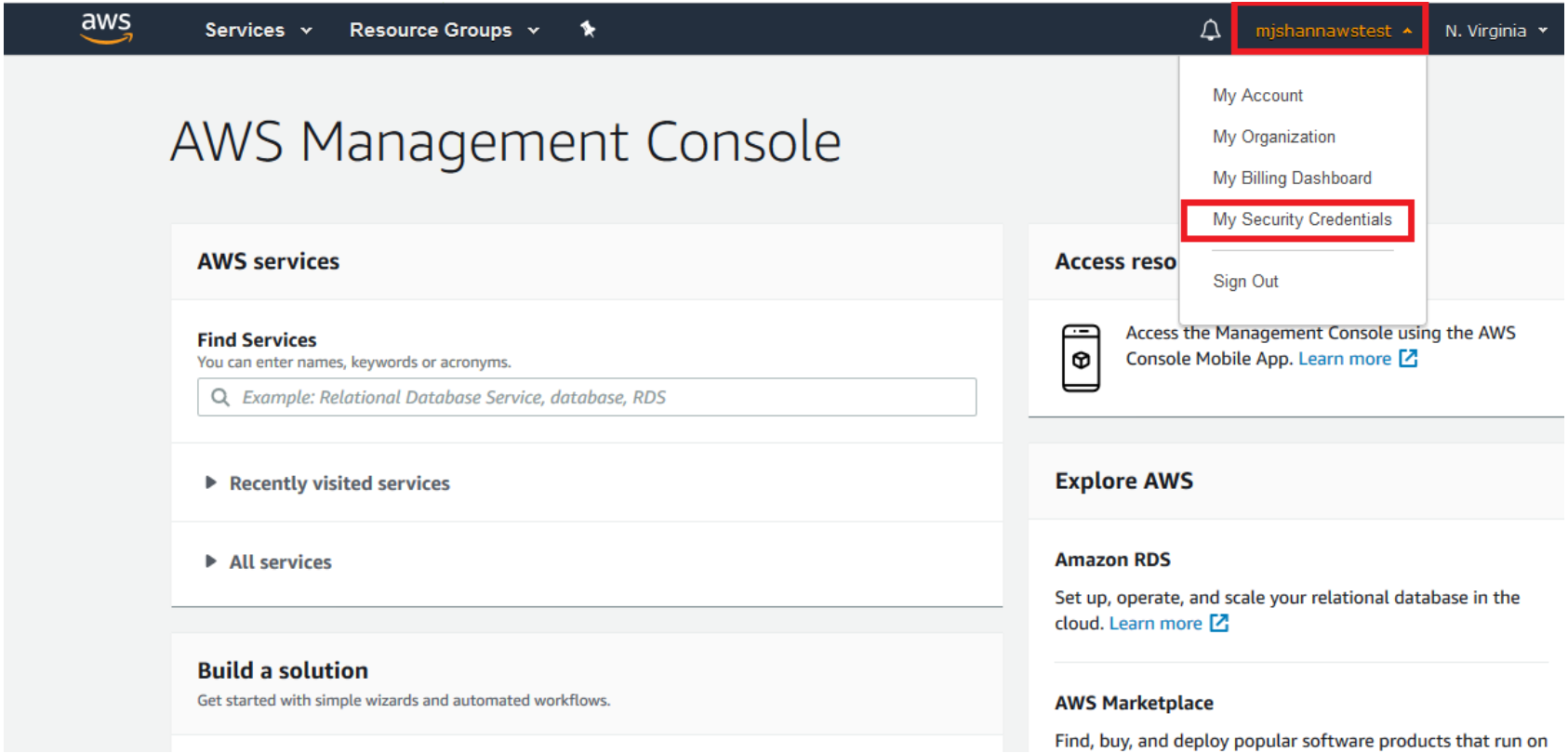
```
https://Your_Alias.signin.aws.amazon.com/console/
```

Creating an Alias

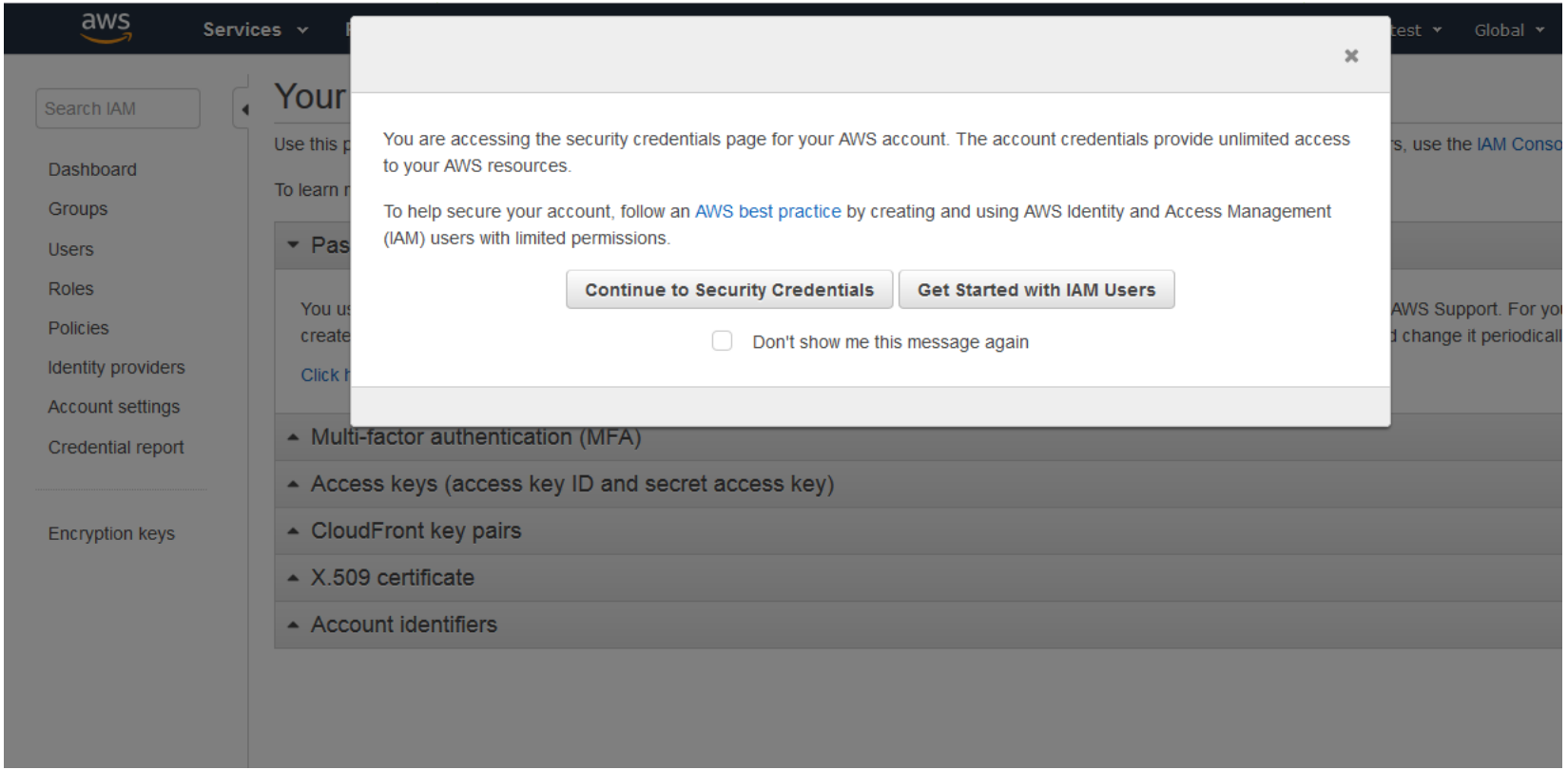


Pearson

My Security Credentials



My Security Credentials



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.

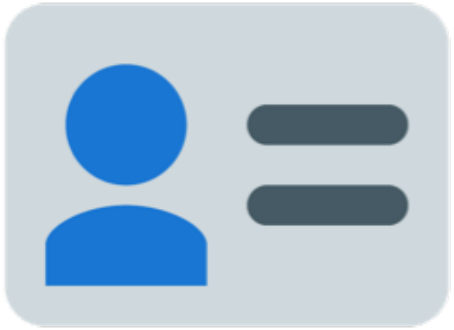
- CloudFront key pairs
- X.509 certificate
- Account identifiers

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 AWS SDK, 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

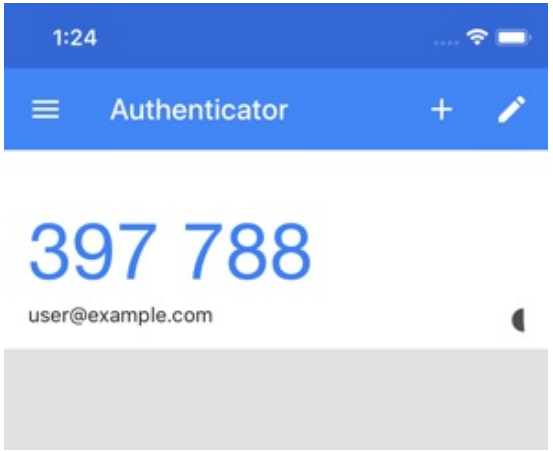
- AWS Account
- Individual IAM user accounts
- AWS Discussion Forums
- AWS Support Center



- 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.

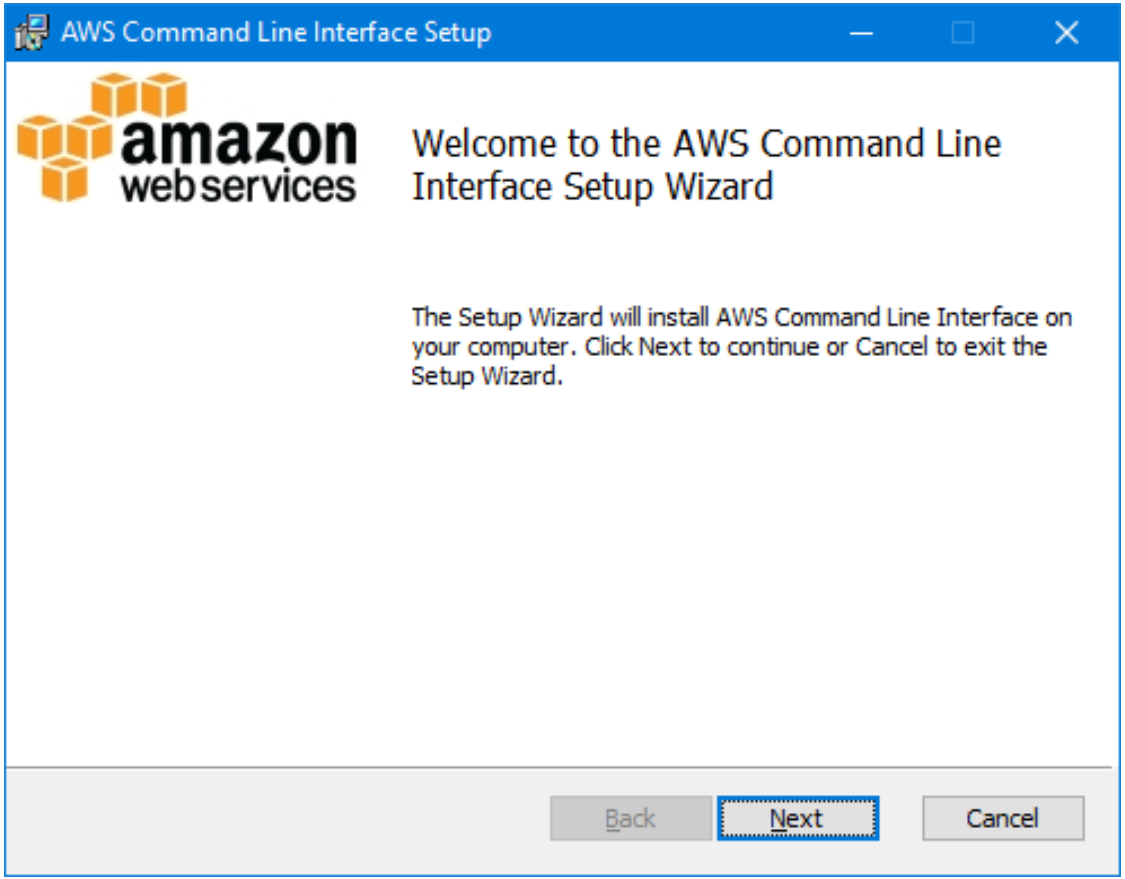
Mac and Linux
Requires Python 2.6.5 or higher.
Install using pip.

```
pip install awscli
```

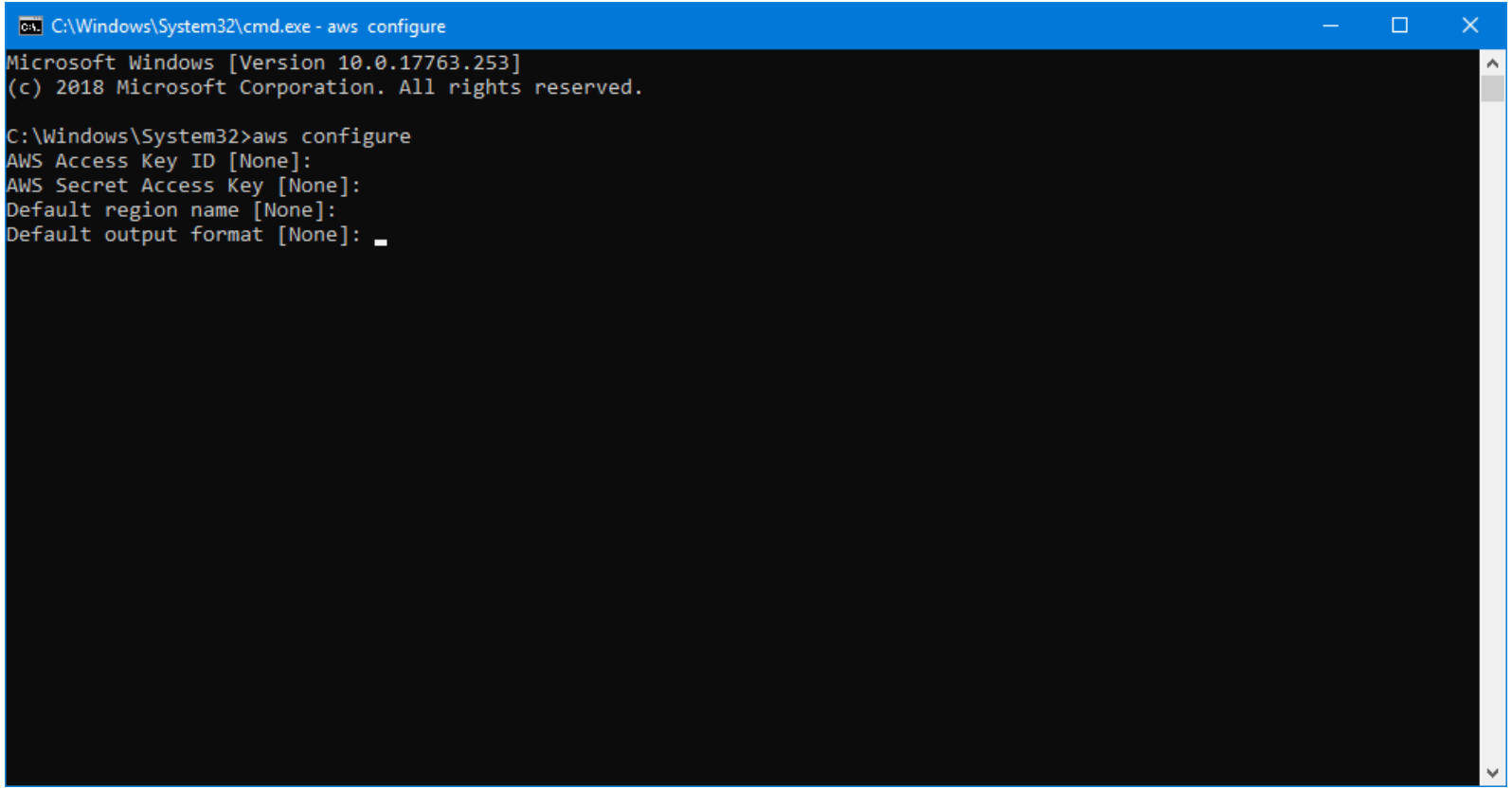
Amazon Linux
The AWS CLI comes pre-installed on Amazon Linux AMI.

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

AWS Command Line Interface



AWS Command Line Interface

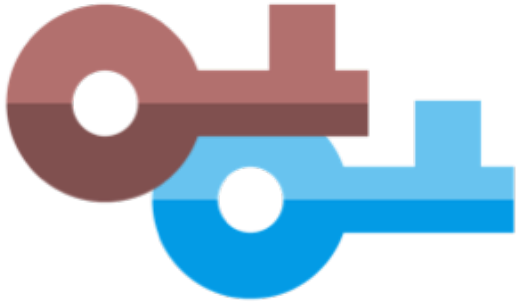


Credential Usage Options

Credential Type	Use	Description
Key Pairs	• SSH login to EC2 instances • CloudFront signed URLs • Windows instances	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.
X.509 Certificates	• Digitally signed SOAP requests to AWS APIs • SSL server certificates for HTTPS	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 Credential Report.

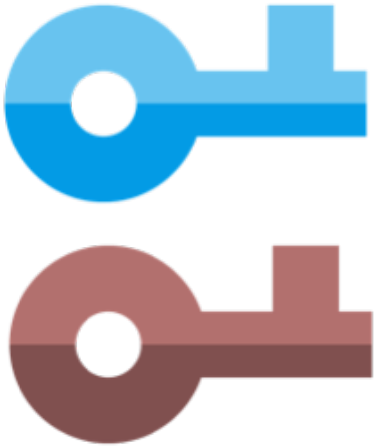
Key Pairs

- 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

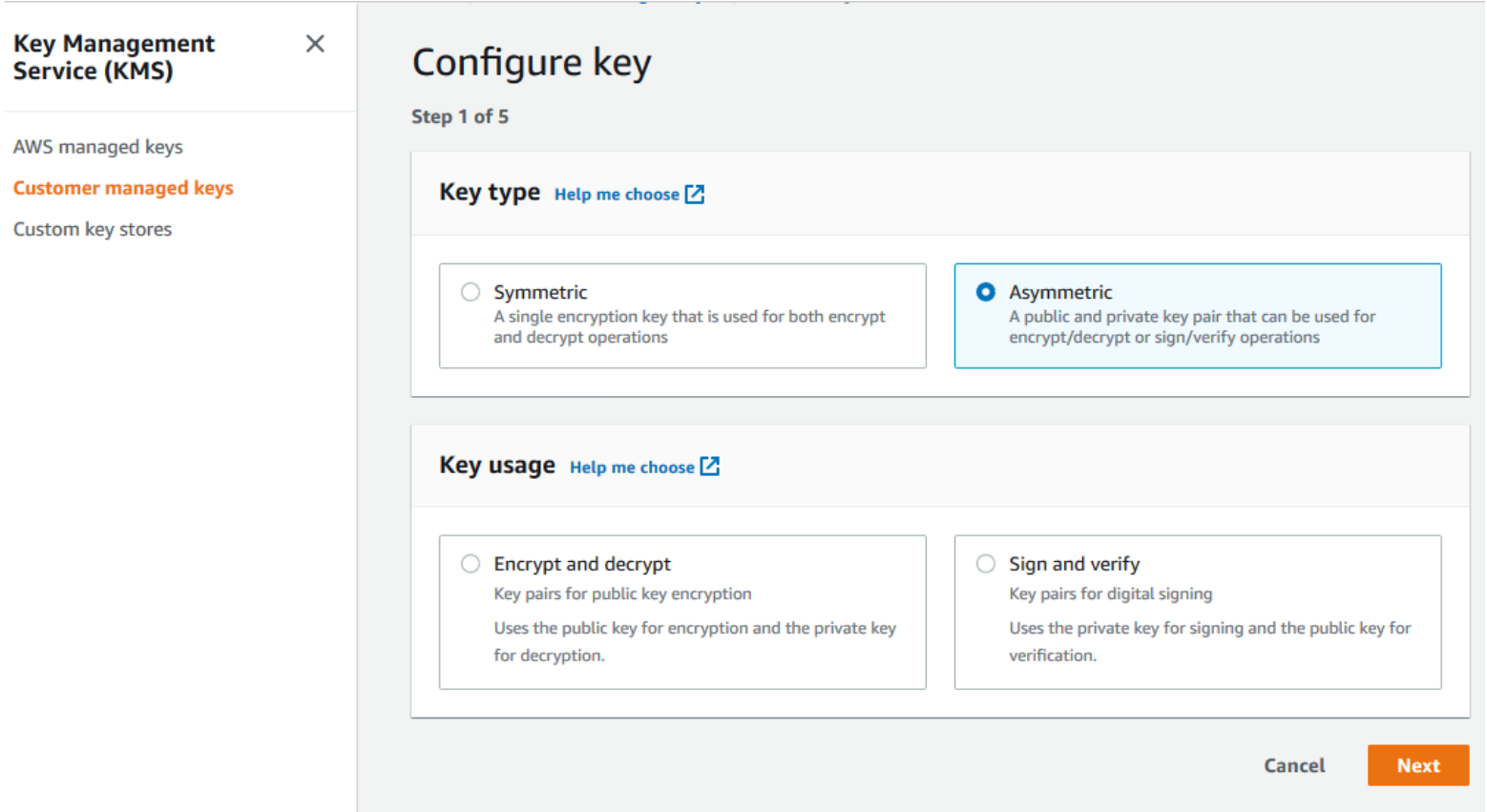


Key Pairs in KMS

- 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.



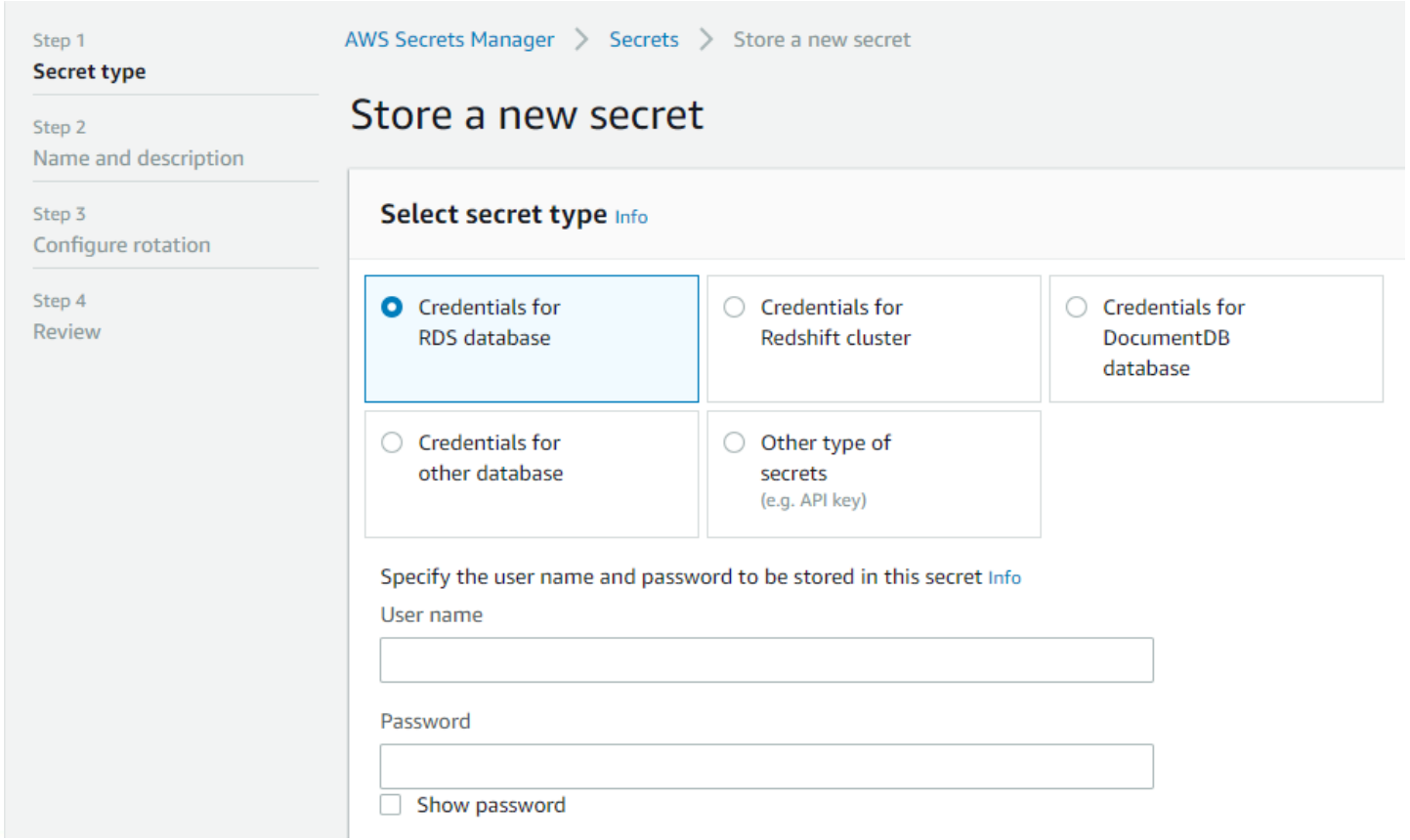
Key Pairs in KMS



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



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.

DefaultEncryptionKey

Add new key

Select which RDS database this secret will access Info

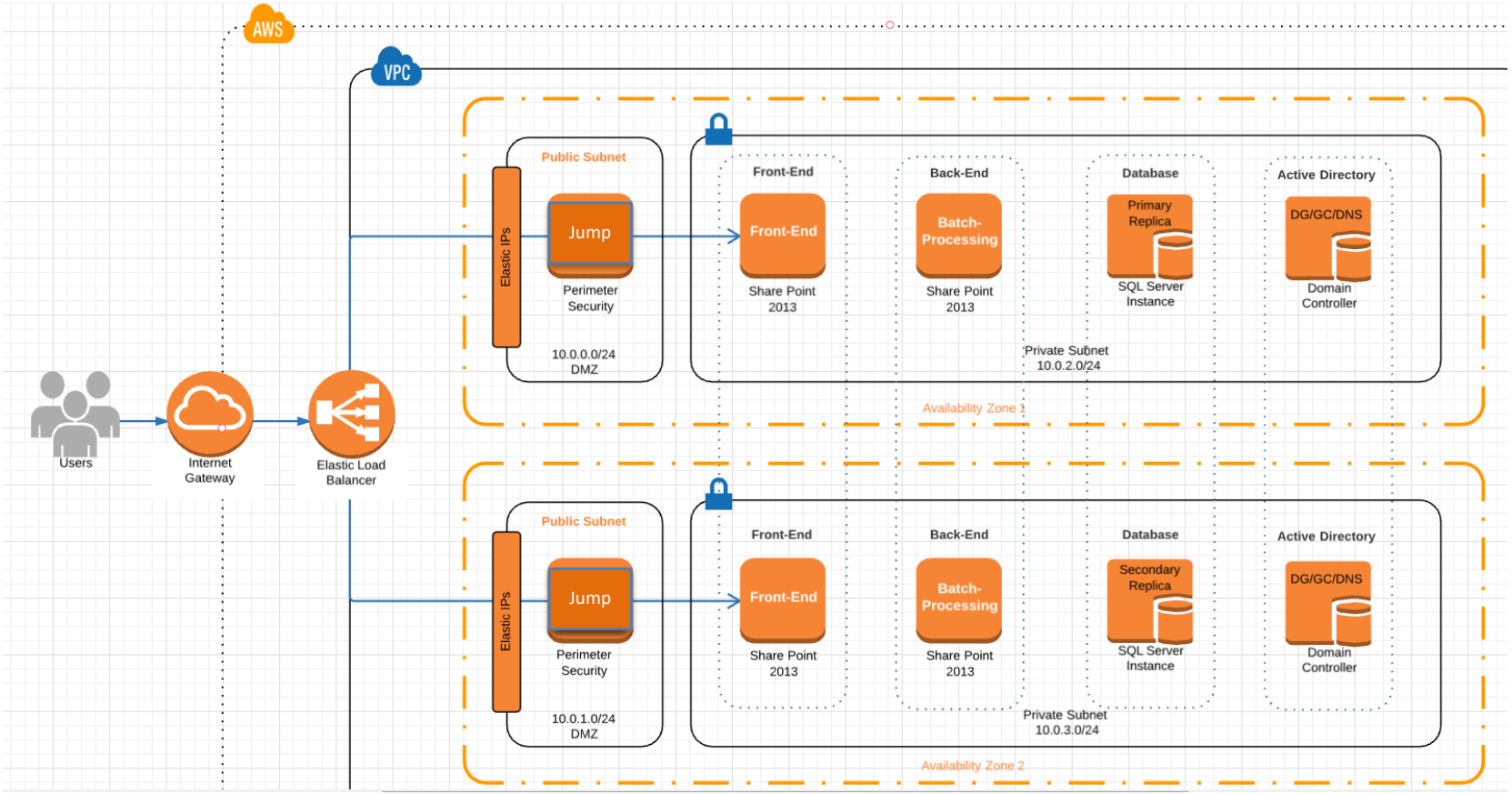
Search instances

1

DB instance	DB engine	Status	Creation date

No databases

Using a Bastion (Jump) Host



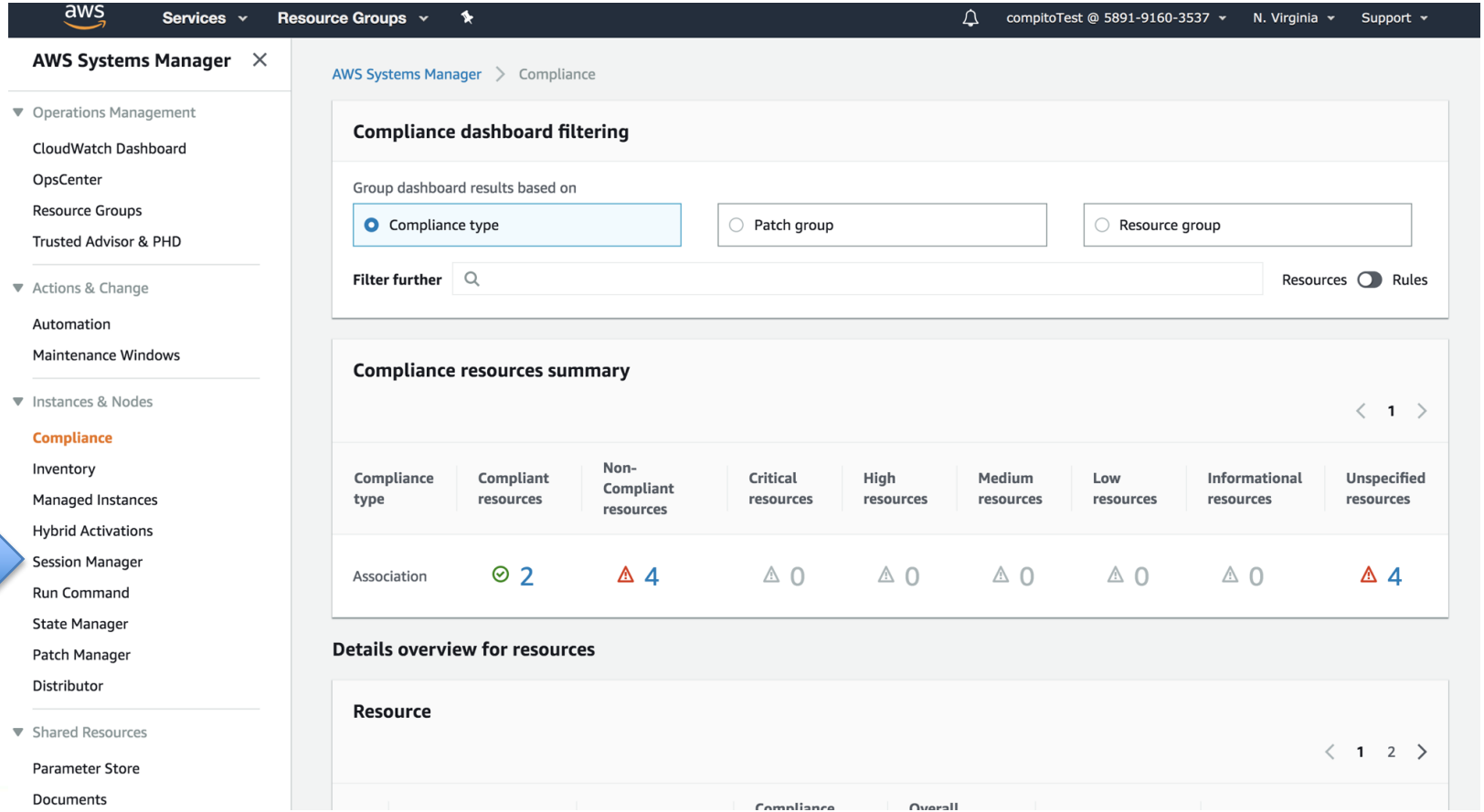
AWS Systems Manager

- 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

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

AWS Systems Manager



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/**

AppStream 2.0 Process

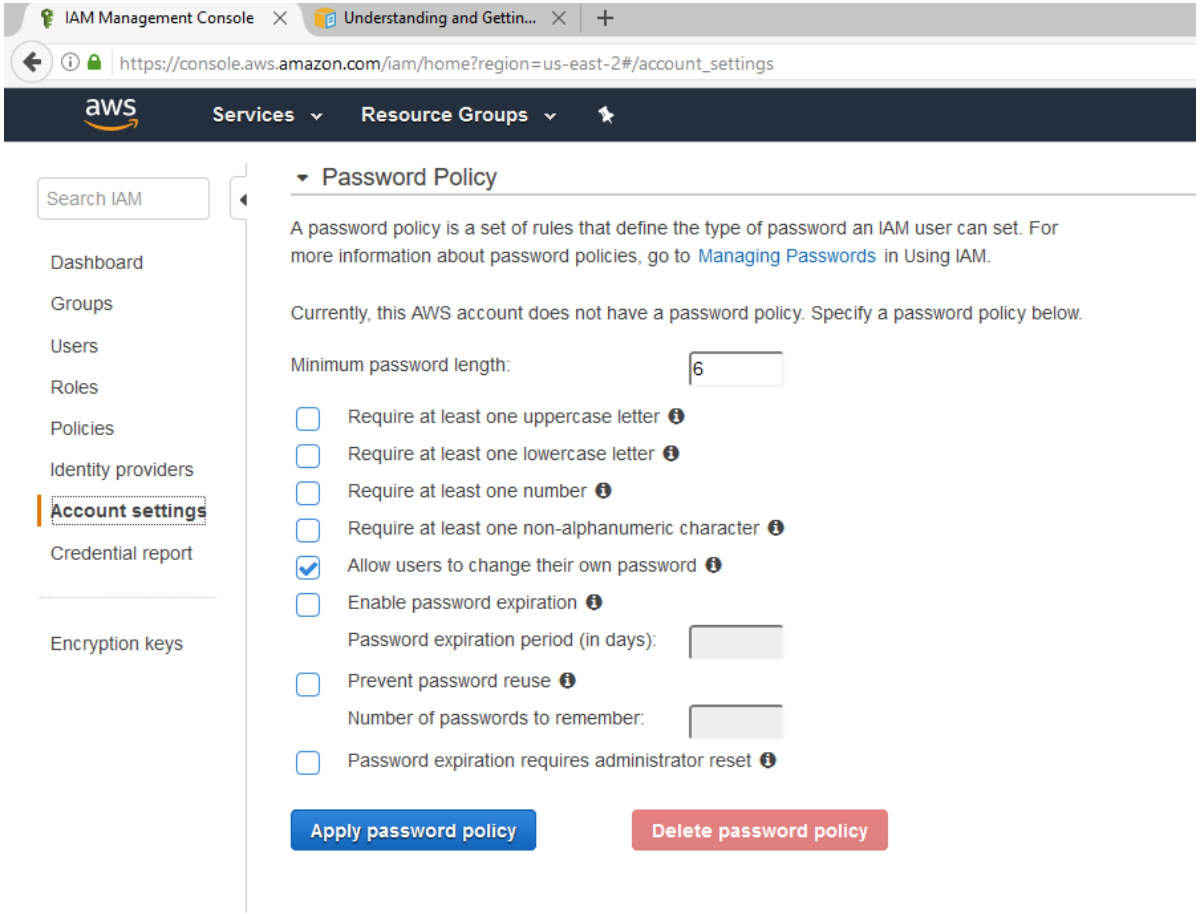
1. Using an HTML5 desktop browser the user logs on to a Single Sign-On URL, authenticating the user against the corporate directory using SAML 2.0 federation
2. After successful authentication the user will see a list of provisioned applications such as RDP and Putty
3. The applications are only visible 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)

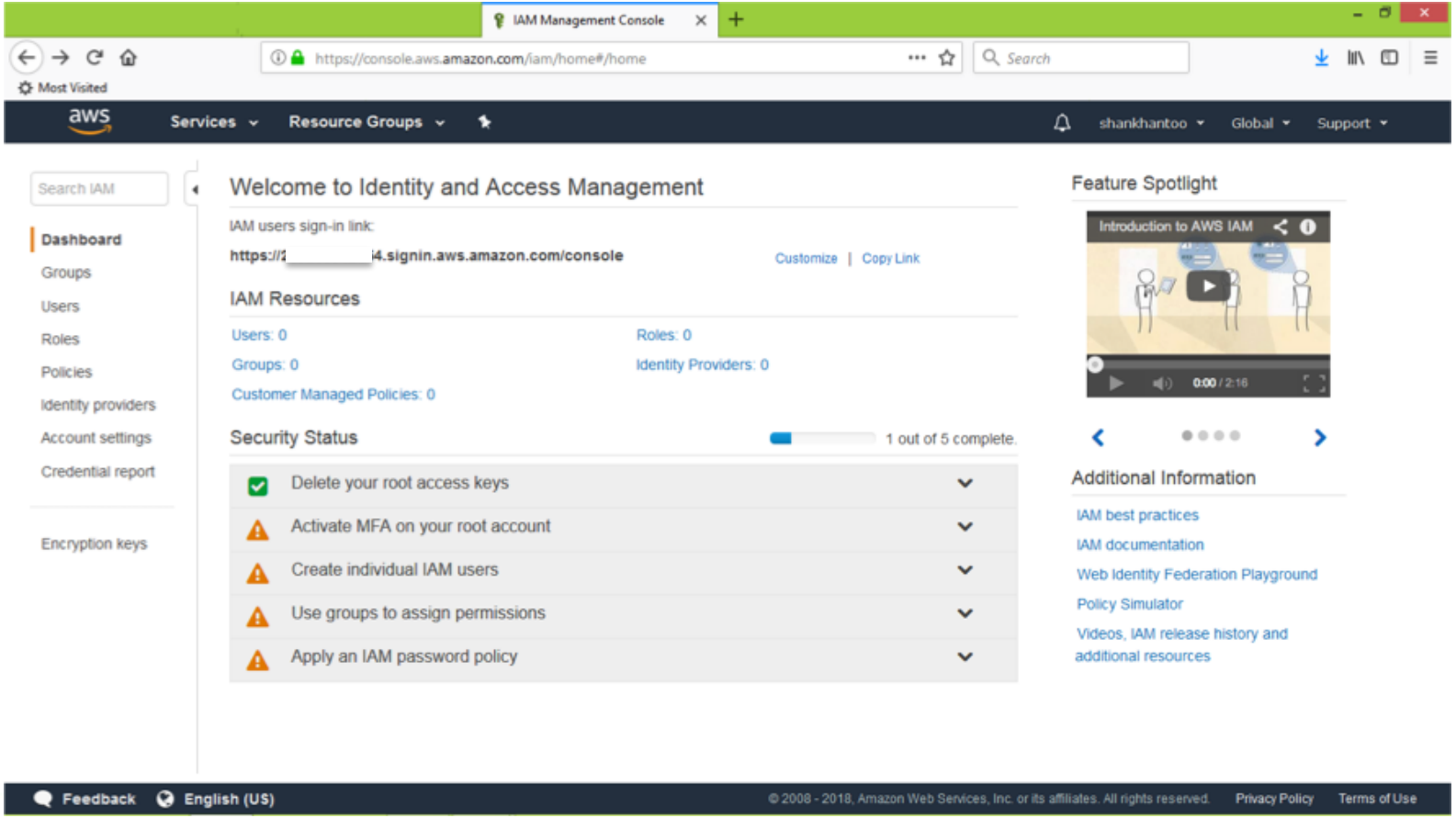
Identity and Access Management (IAM)

- 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**.

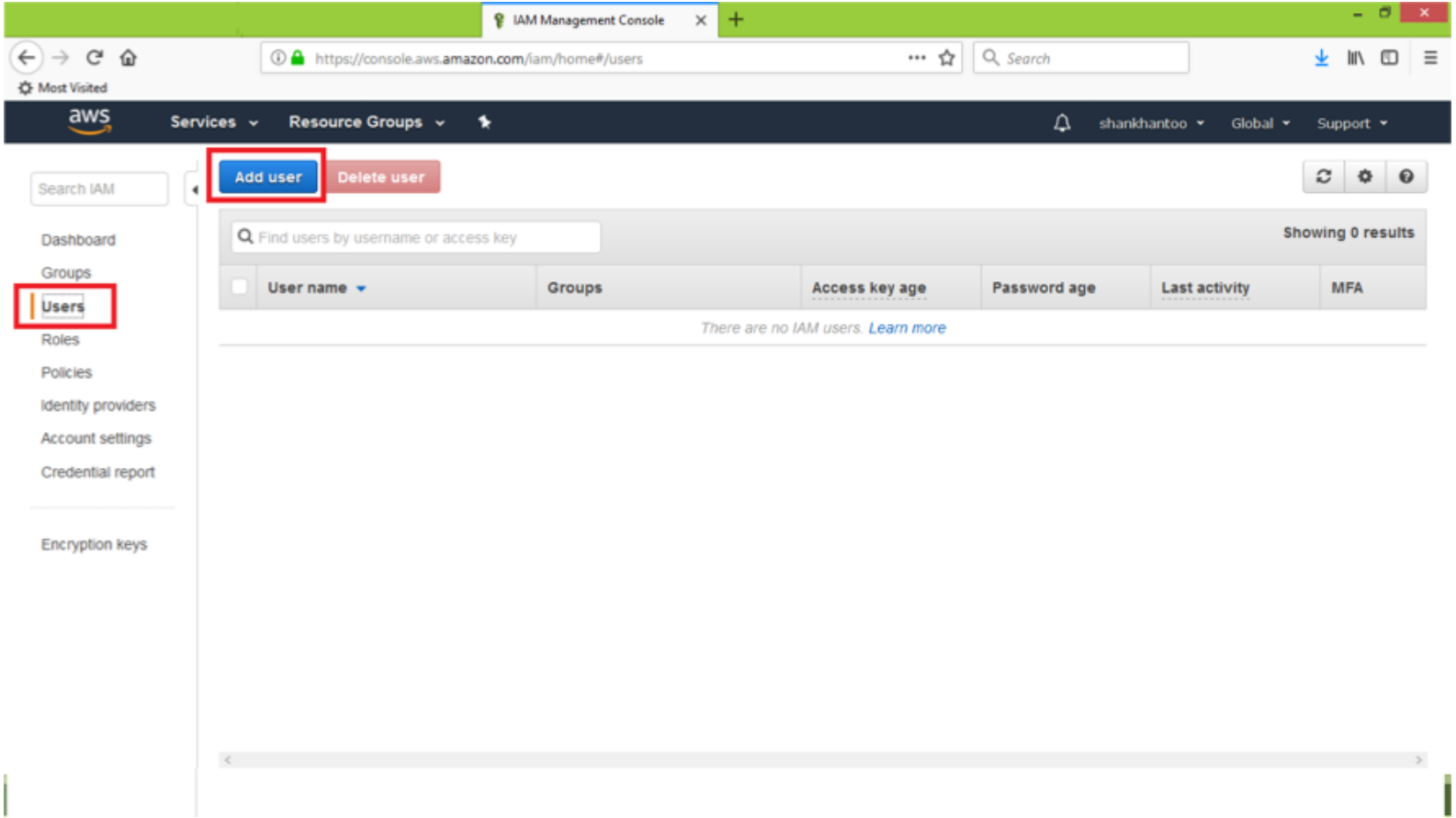
IAM Password Policies



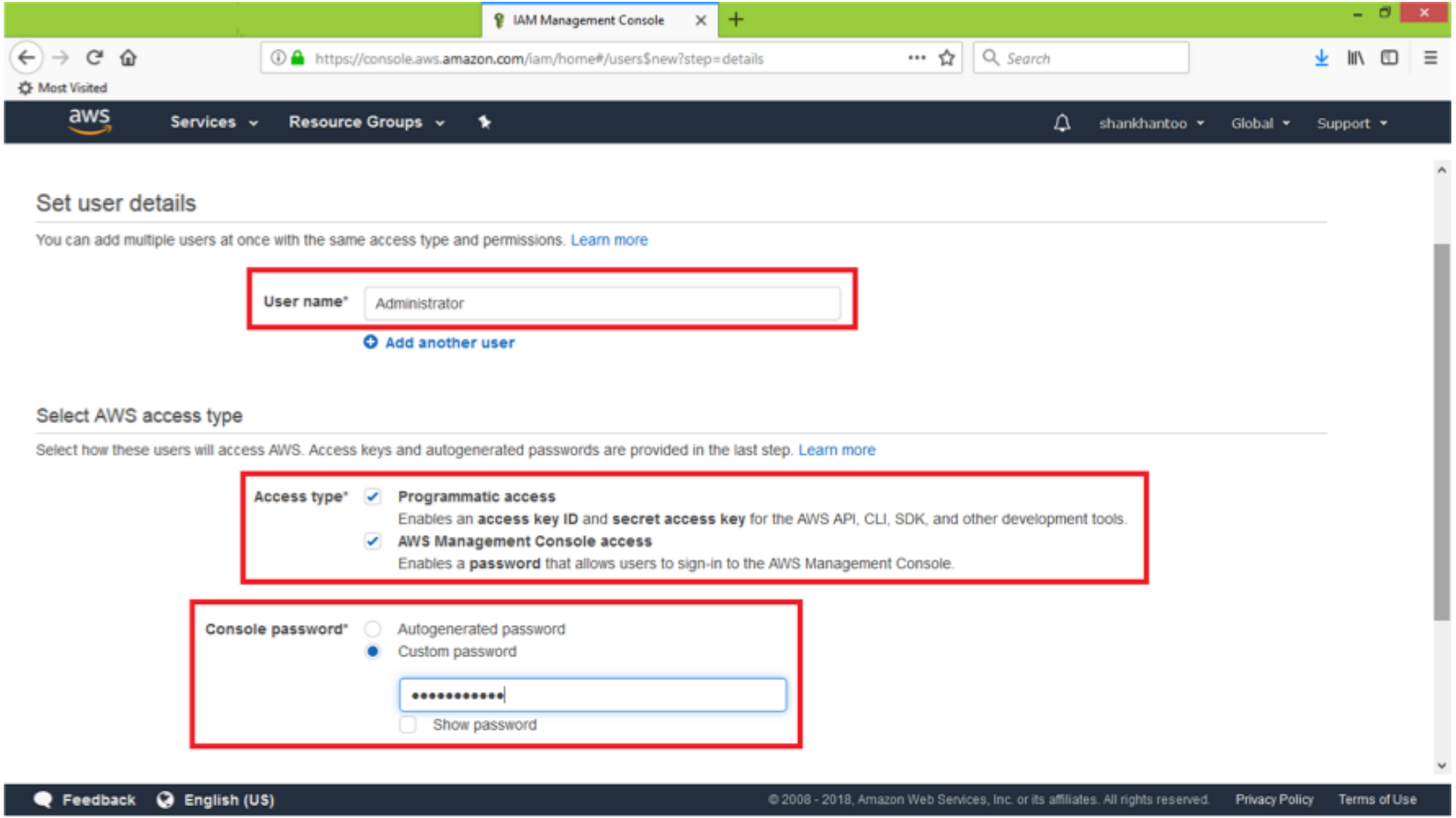
IAM (continued)



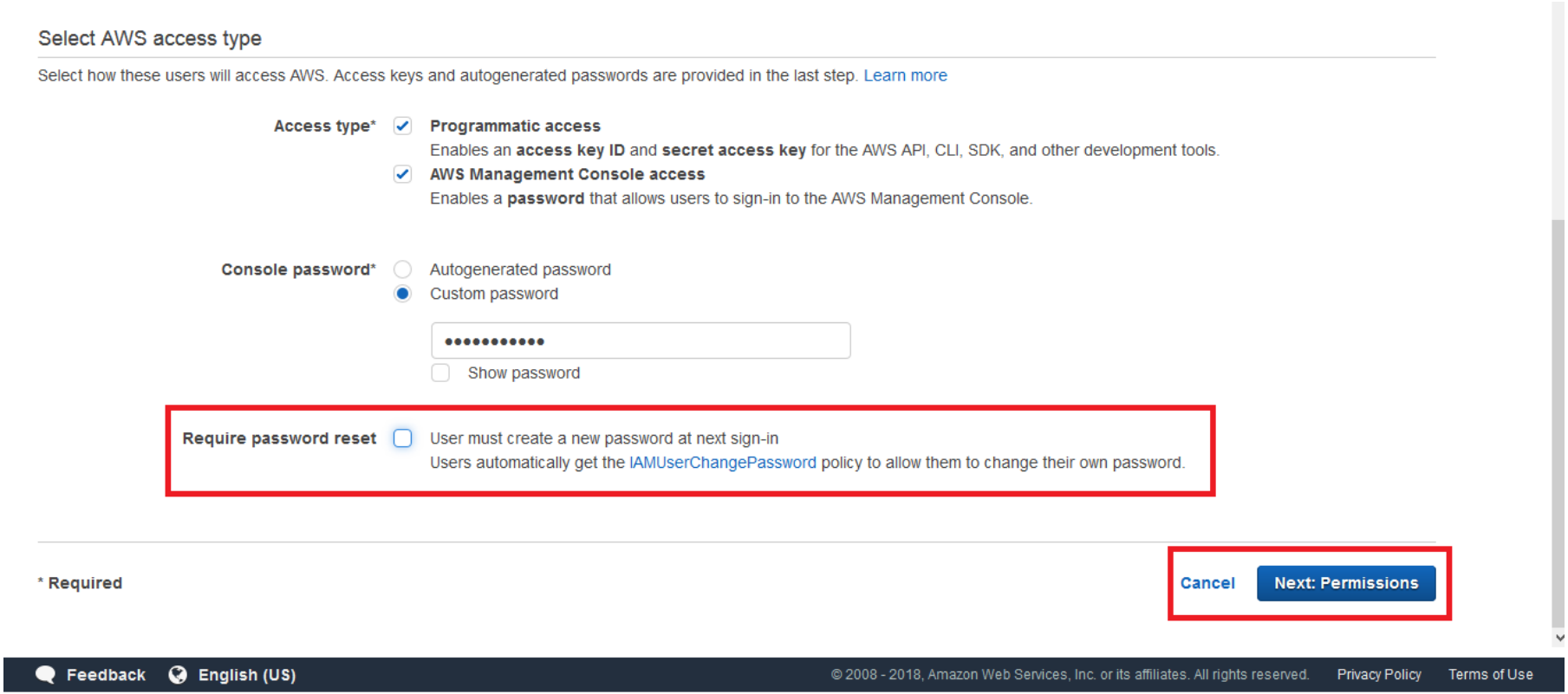
IAM (continued)



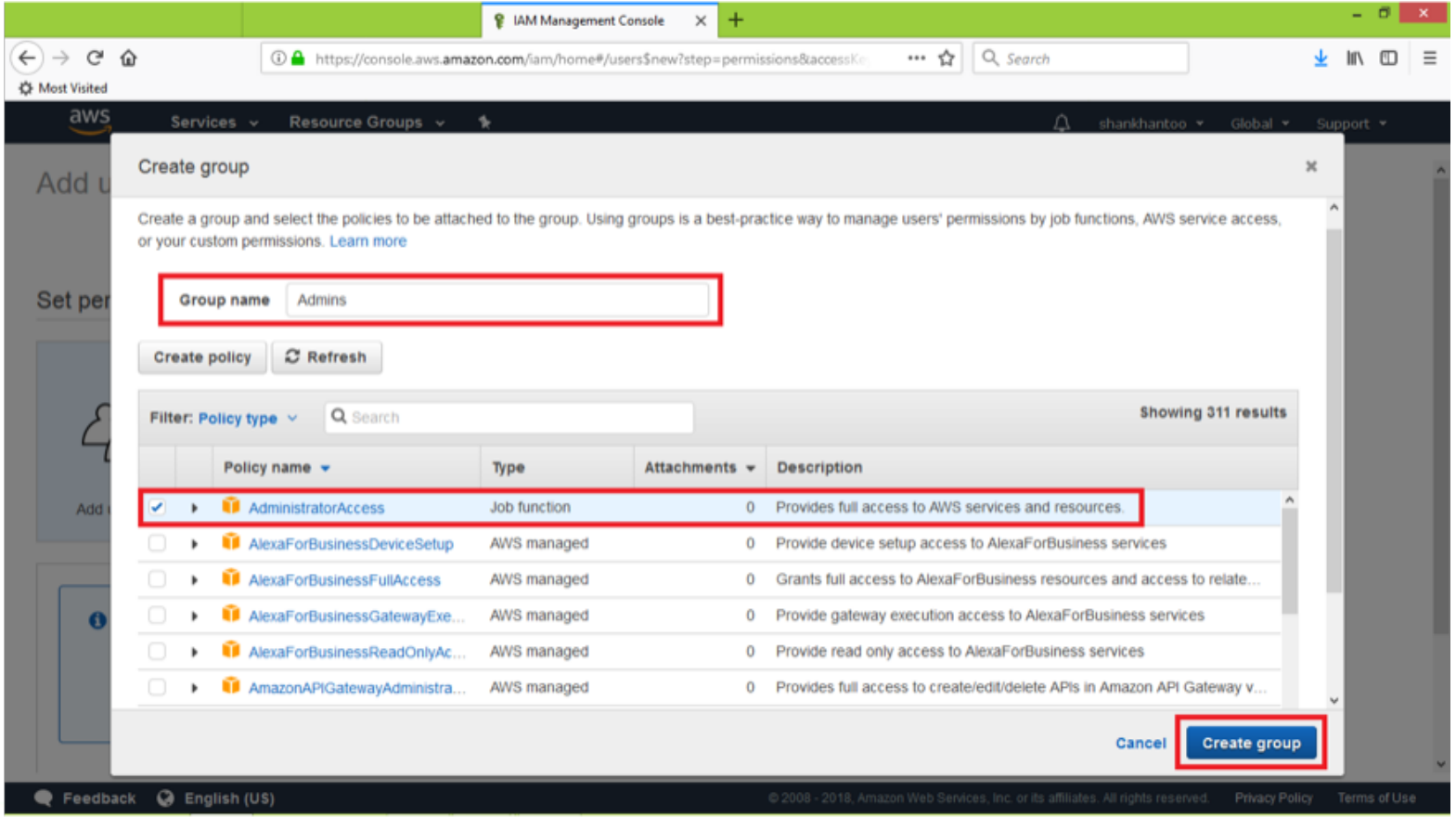
IAM (continued)



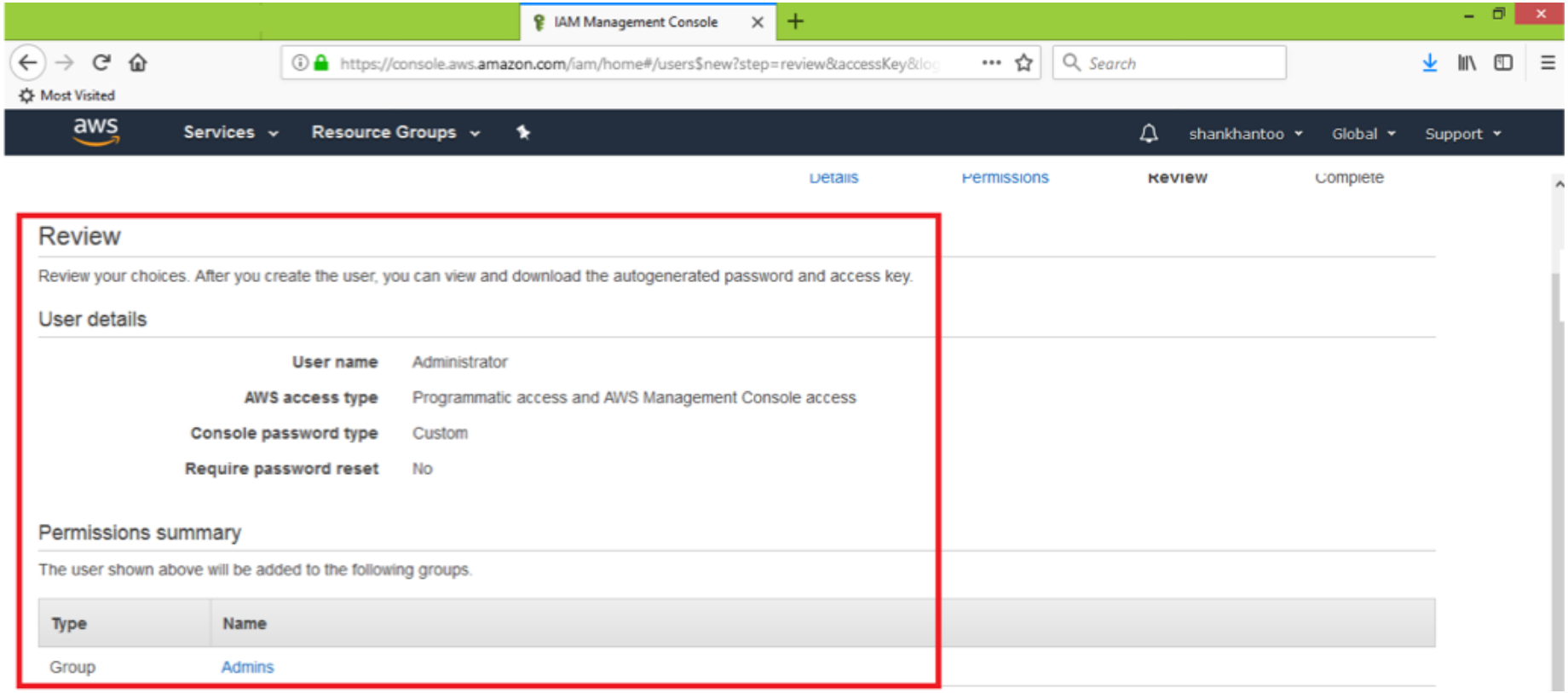
IAM (continued)



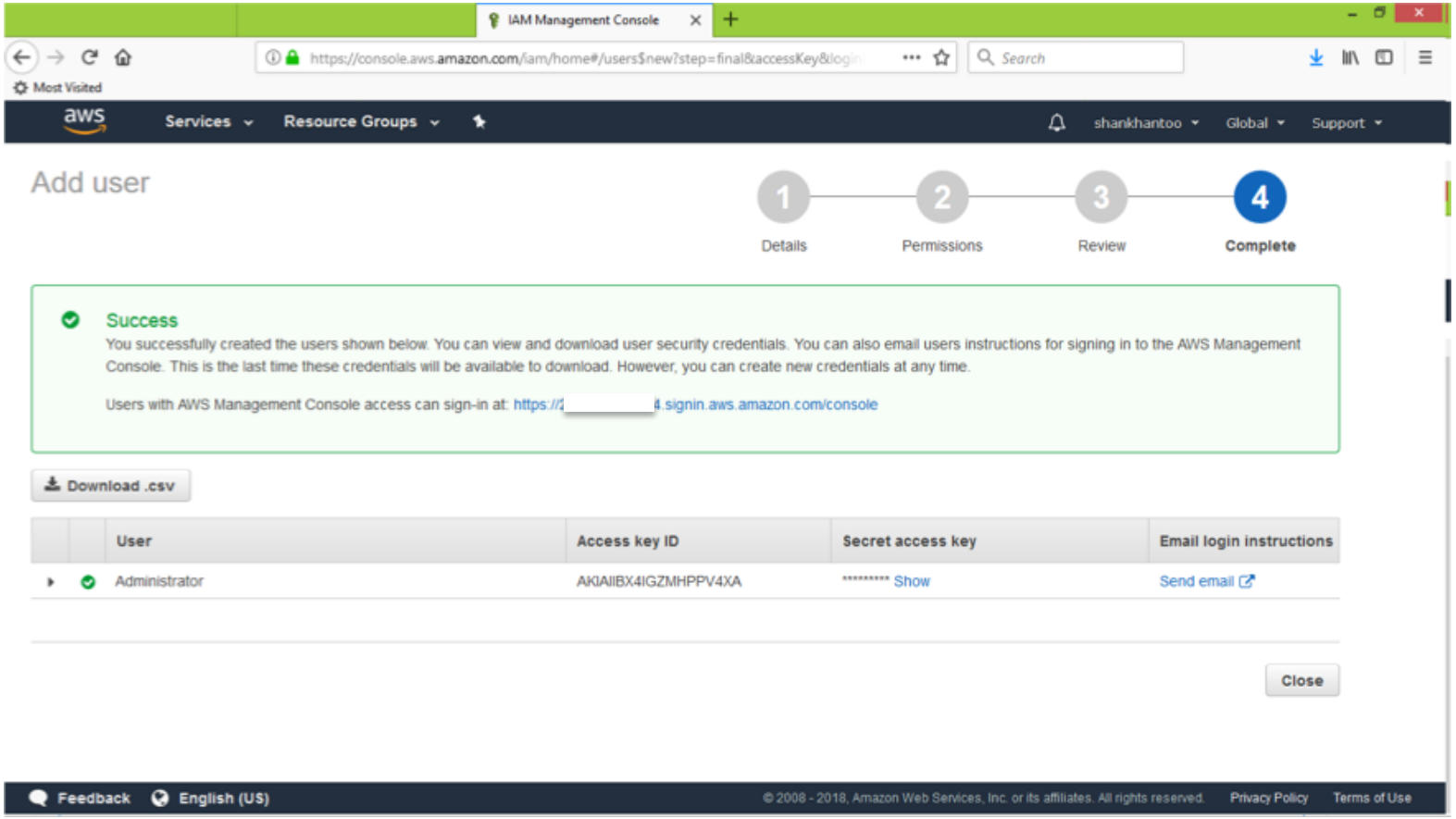
IAM (continued)



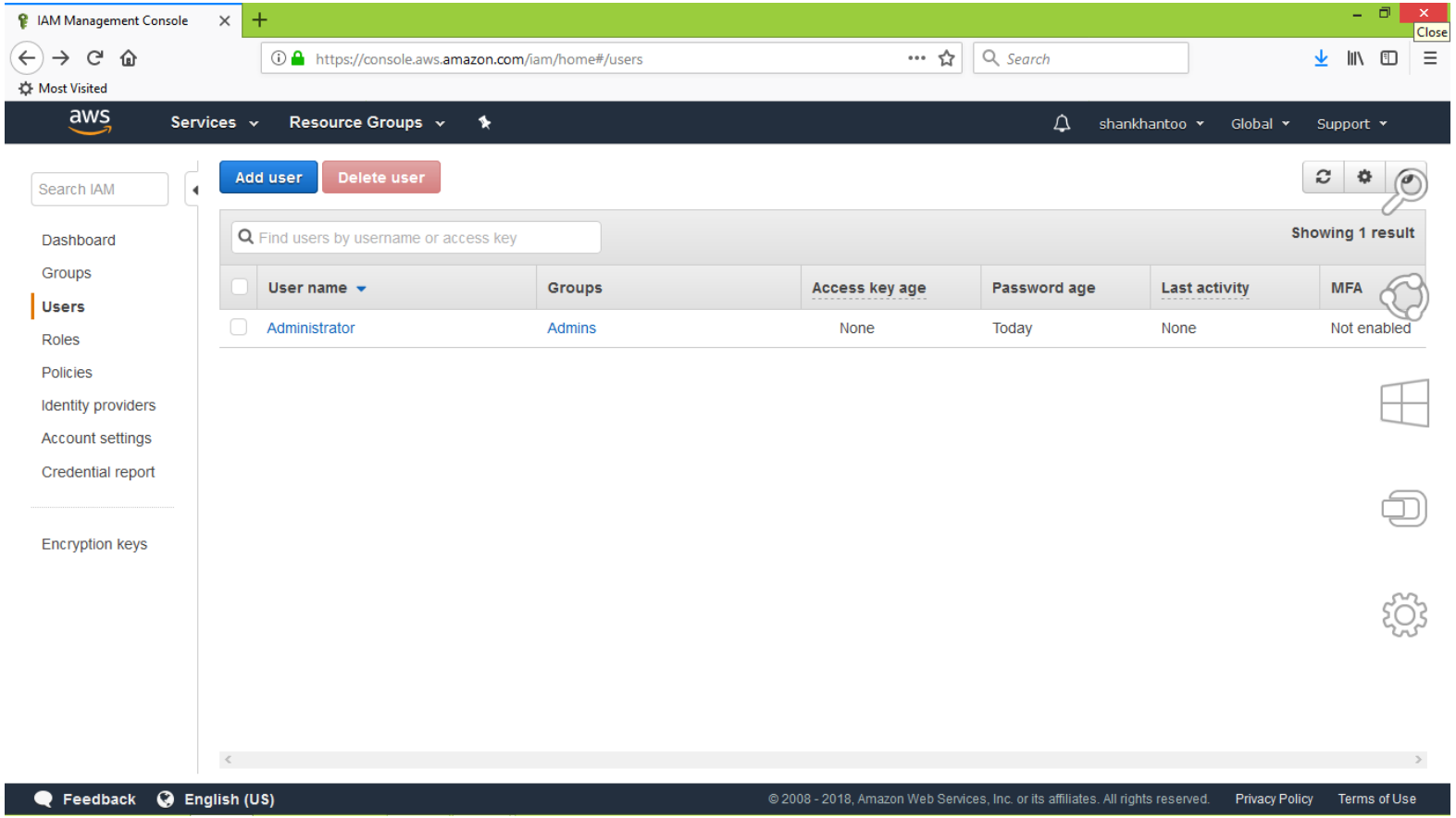
IAM (continued)



IAM (continued)



IAM (continued)



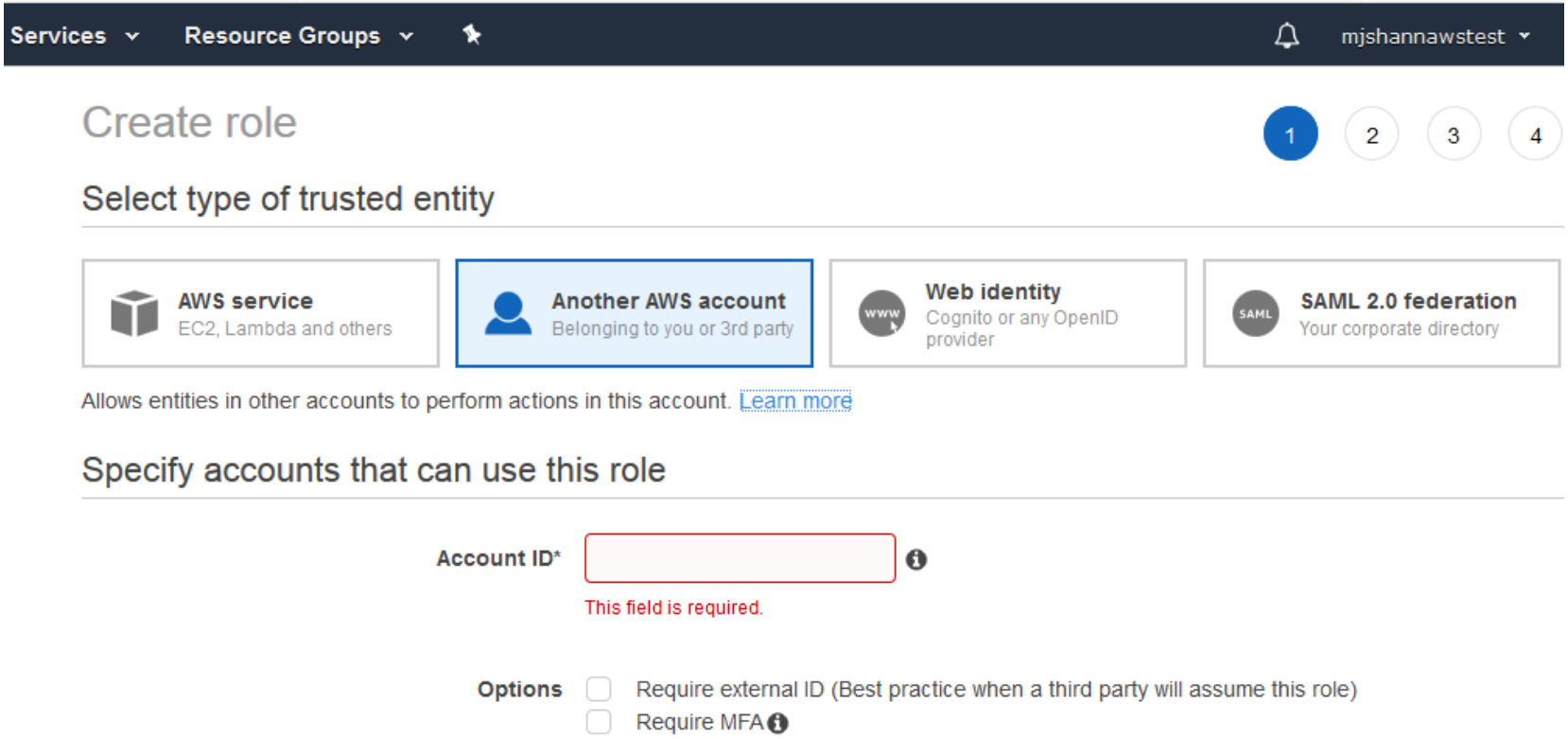
IAM Roles

- 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

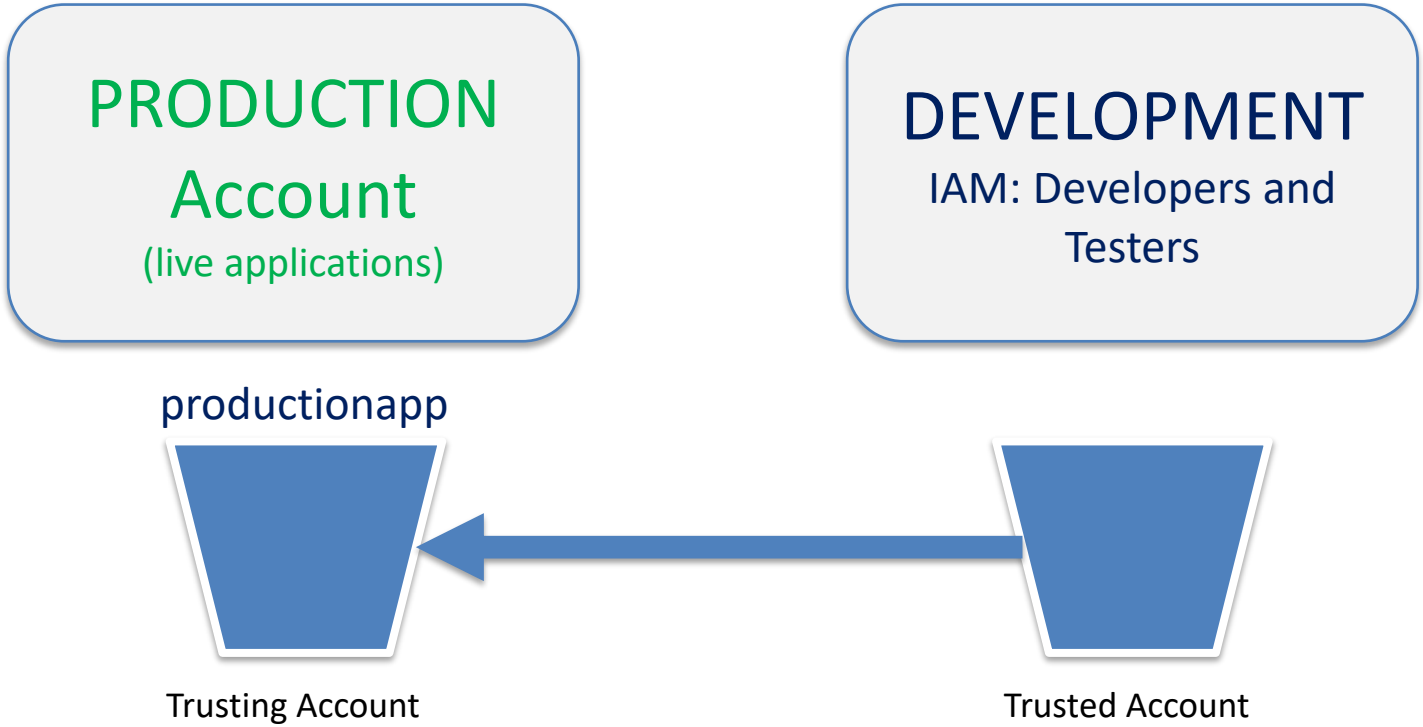


PRODUCTION
Account
(live applications)

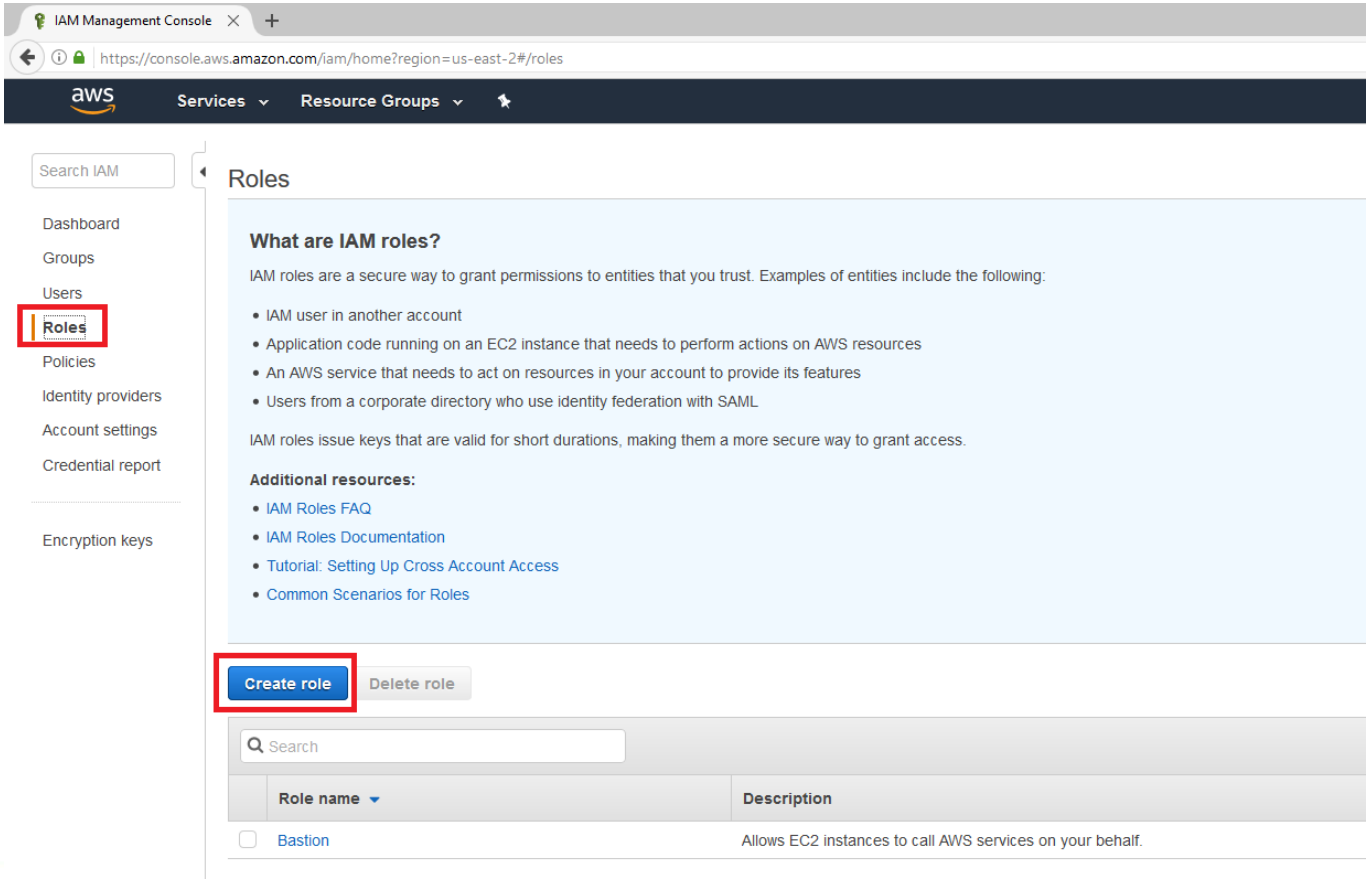
DEVELOPMENT
Account
(application sandbox)

PRODUCTION
Account
(live applications)

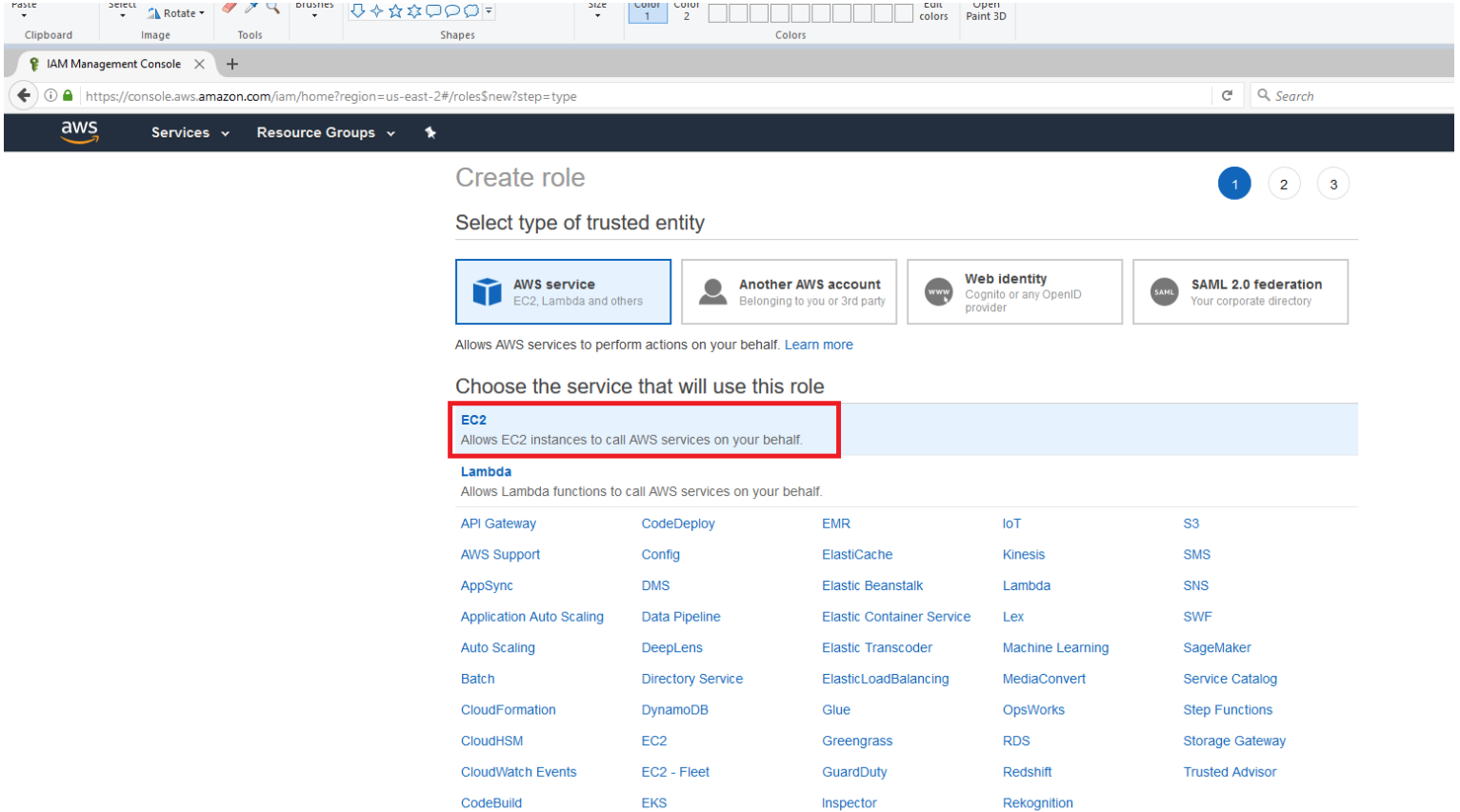
DEVELOPMENT
Account
(application sandbox)



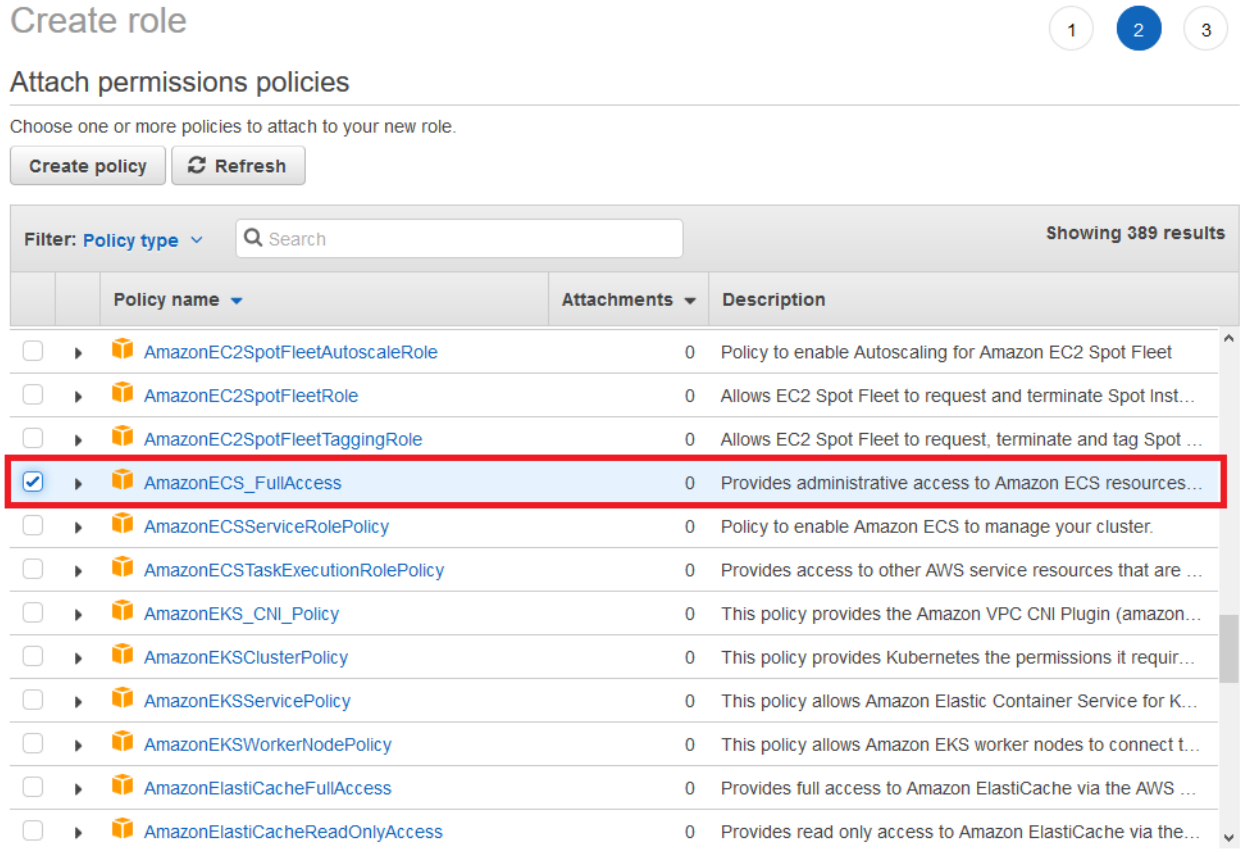
IAM Roles



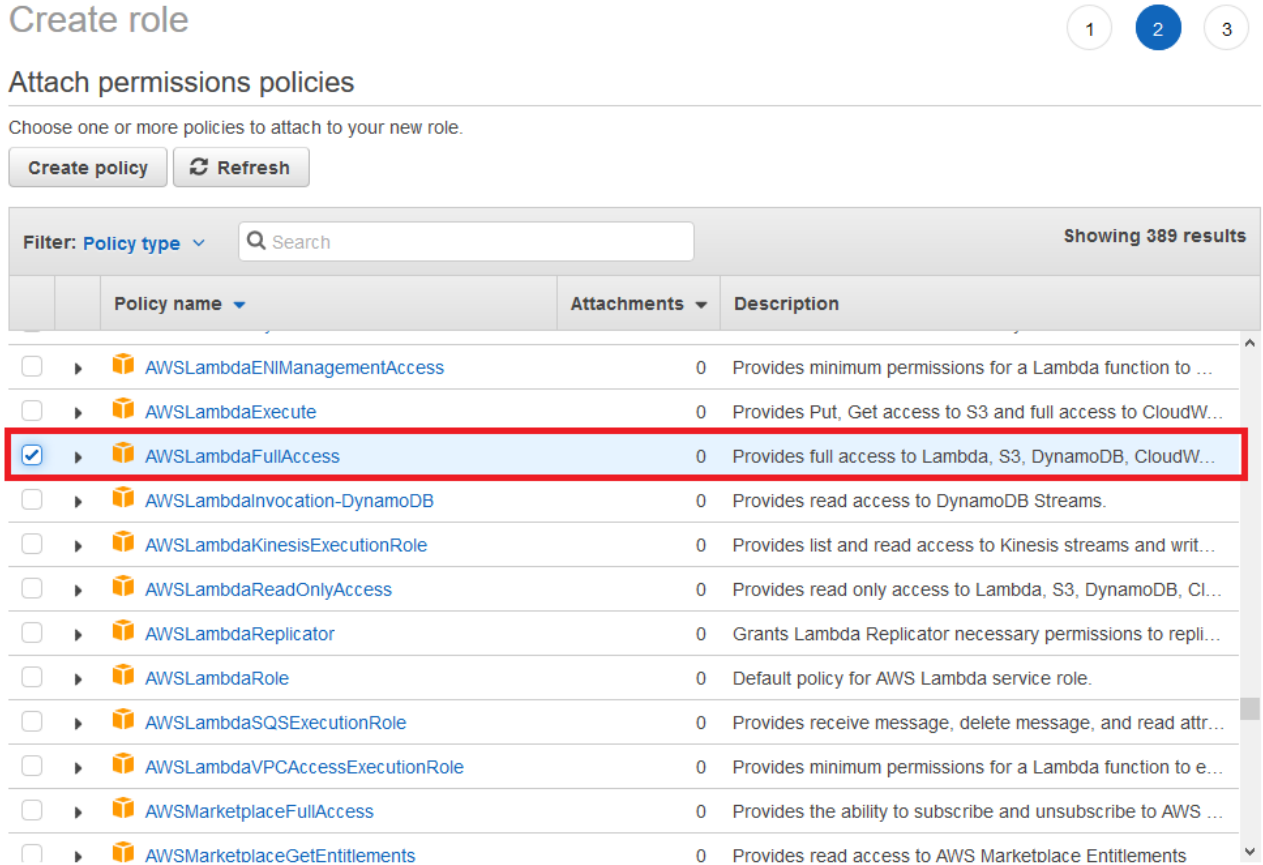
IAM Roles


IAM Management Console
https://console.aws.amazon.com/iam/home?region=us-east-2#/roles$new?step=type
Search
aws
Services
Resource Groups
Create role
1
2
3
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 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
AWS Support
AppSync
Application Auto Scaling
Auto Scaling
Batch
CloudFormation
CloudHSM
CloudWatch Events
CodeBuild
CodeDeploy
Config
DMS
Data Pipeline
DeepLens
Directory Service
DynamoDB
EC2
EC2 - Fleet
EKS
EMR
ElastiCache
Elastic Beanstalk
Elastic Container Service
Elastic Transcoder
ElasticLoadBalancing
Glue
Greengrass
GuardDuty
Inspector
IoT
Kinesis
Lambda
Lex
Machine Learning
MediaConvert
OpsWorks
RDS
Redshift
Rekognition
S3
SMS
SNS
SWF
SageMaker
Service Catalog
Step Functions
Storage Gateway
Trusted Advisor

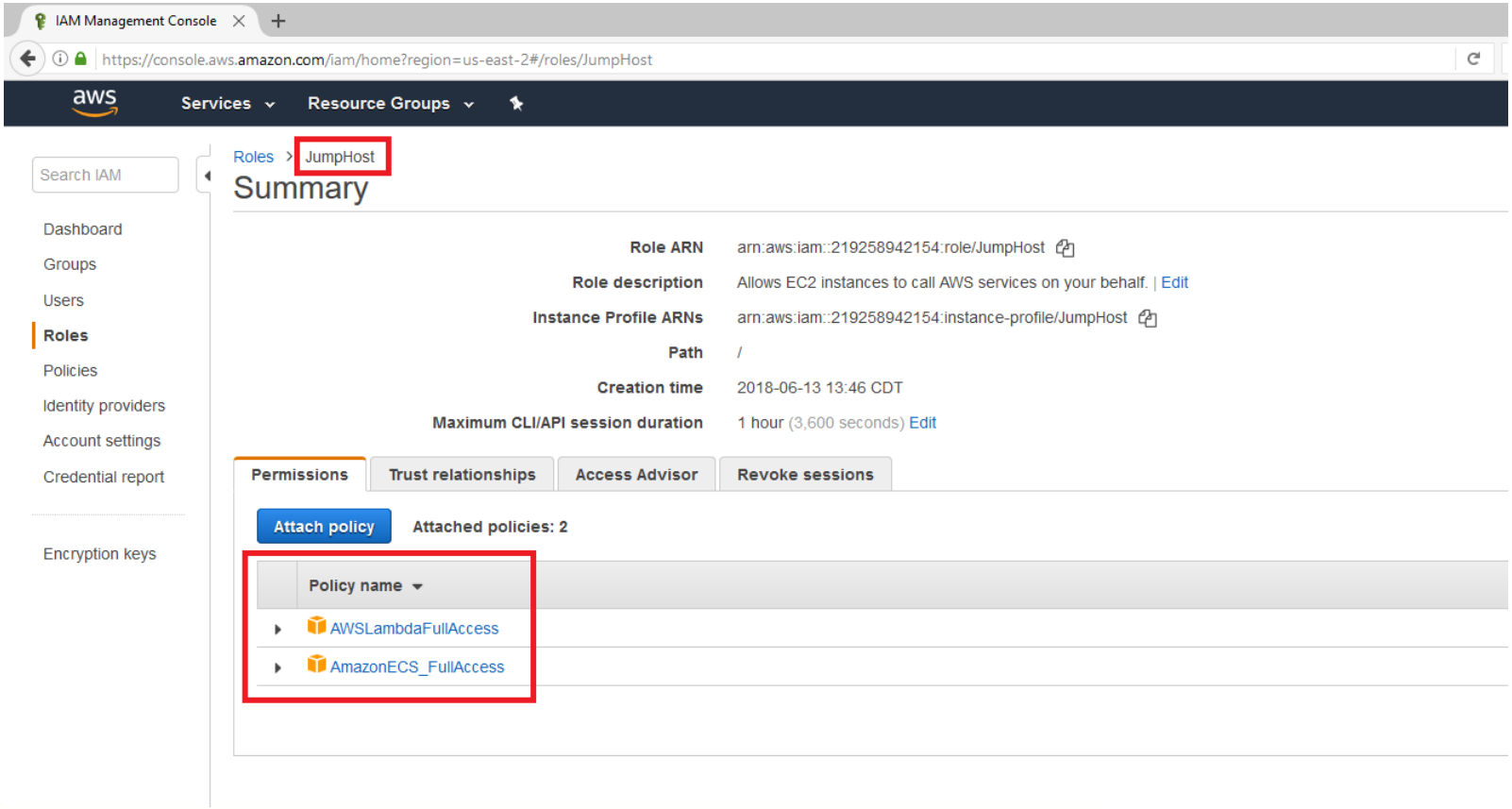
IAM Roles



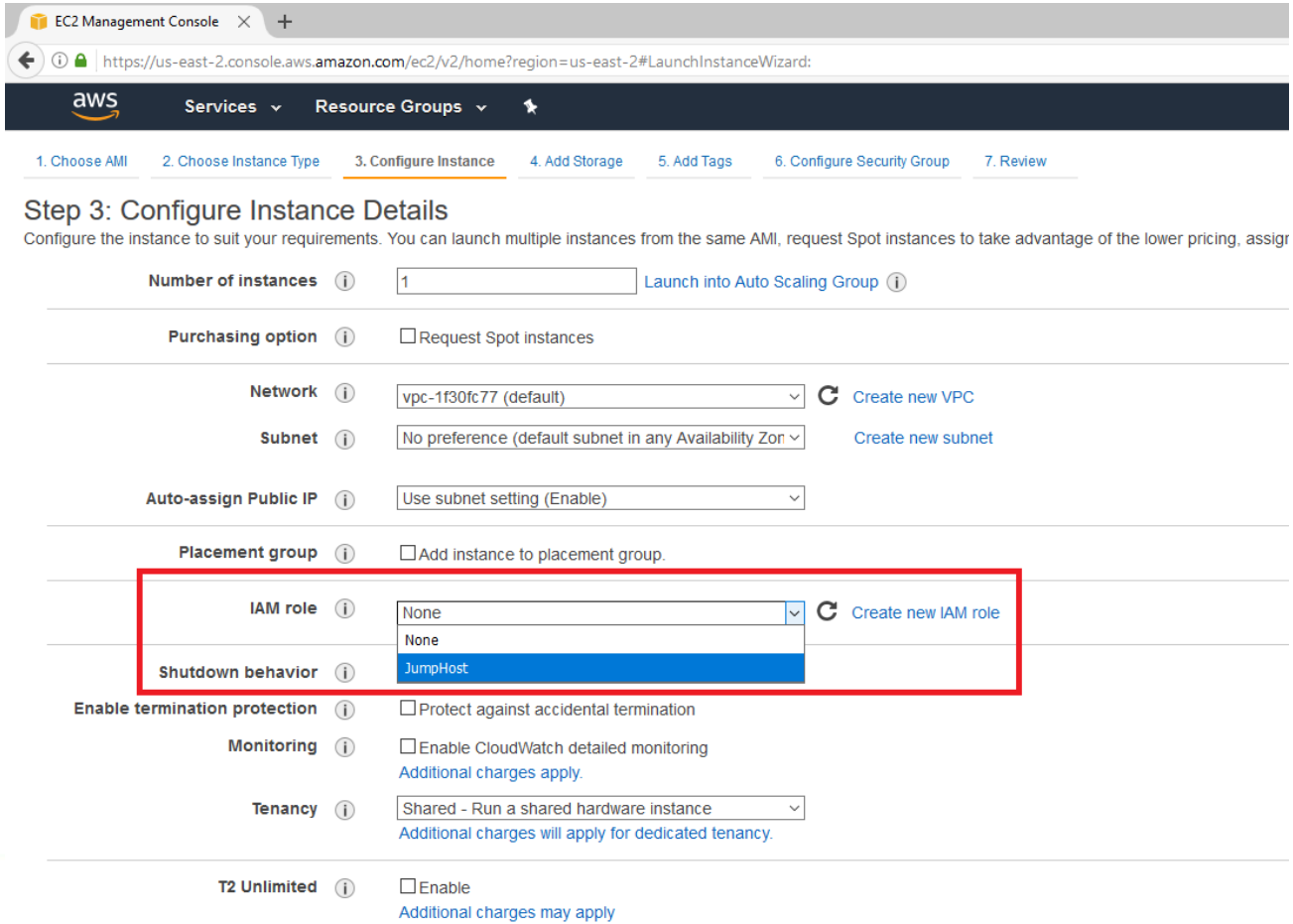
IAM Roles



IAM Roles



IAM Roles



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

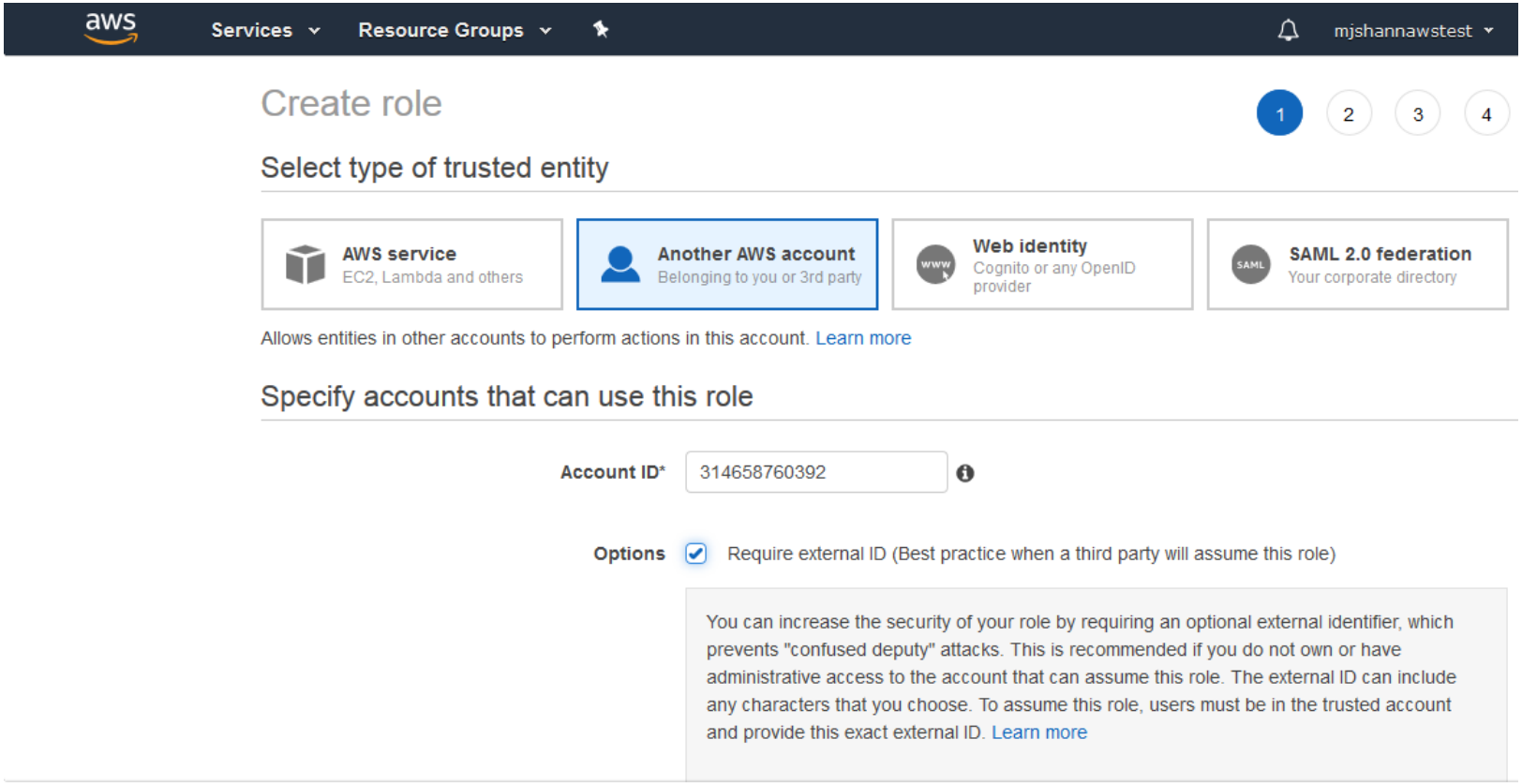
1. Log in to your Amazon IAM console and click Roles.
2. Click "Create New Role"
3. Select the role type "Another AWS account"
4. Check the box "Require external ID"
5. Enter the following:

   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.

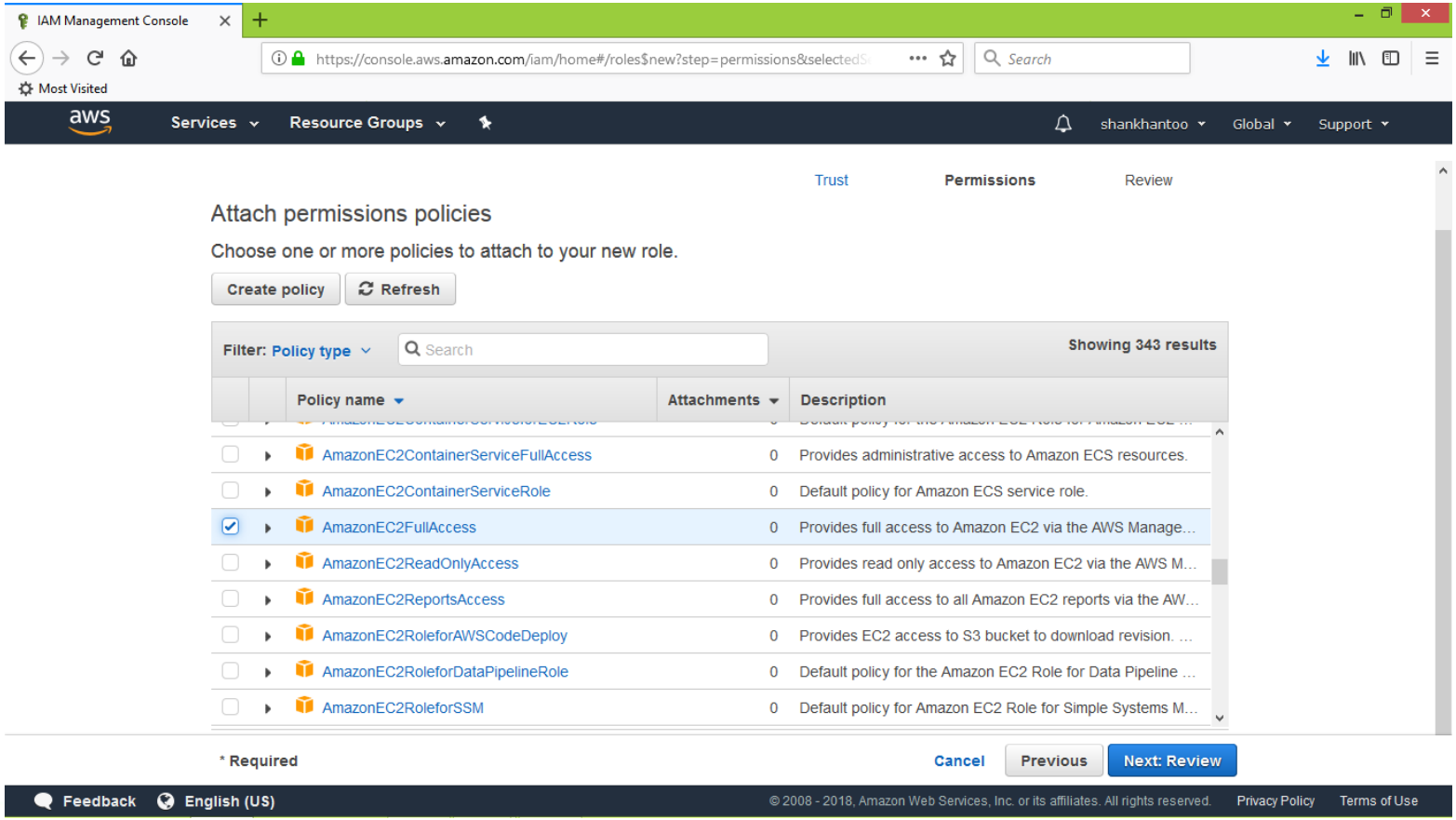
Assigning a Role to GCP Stackdriver



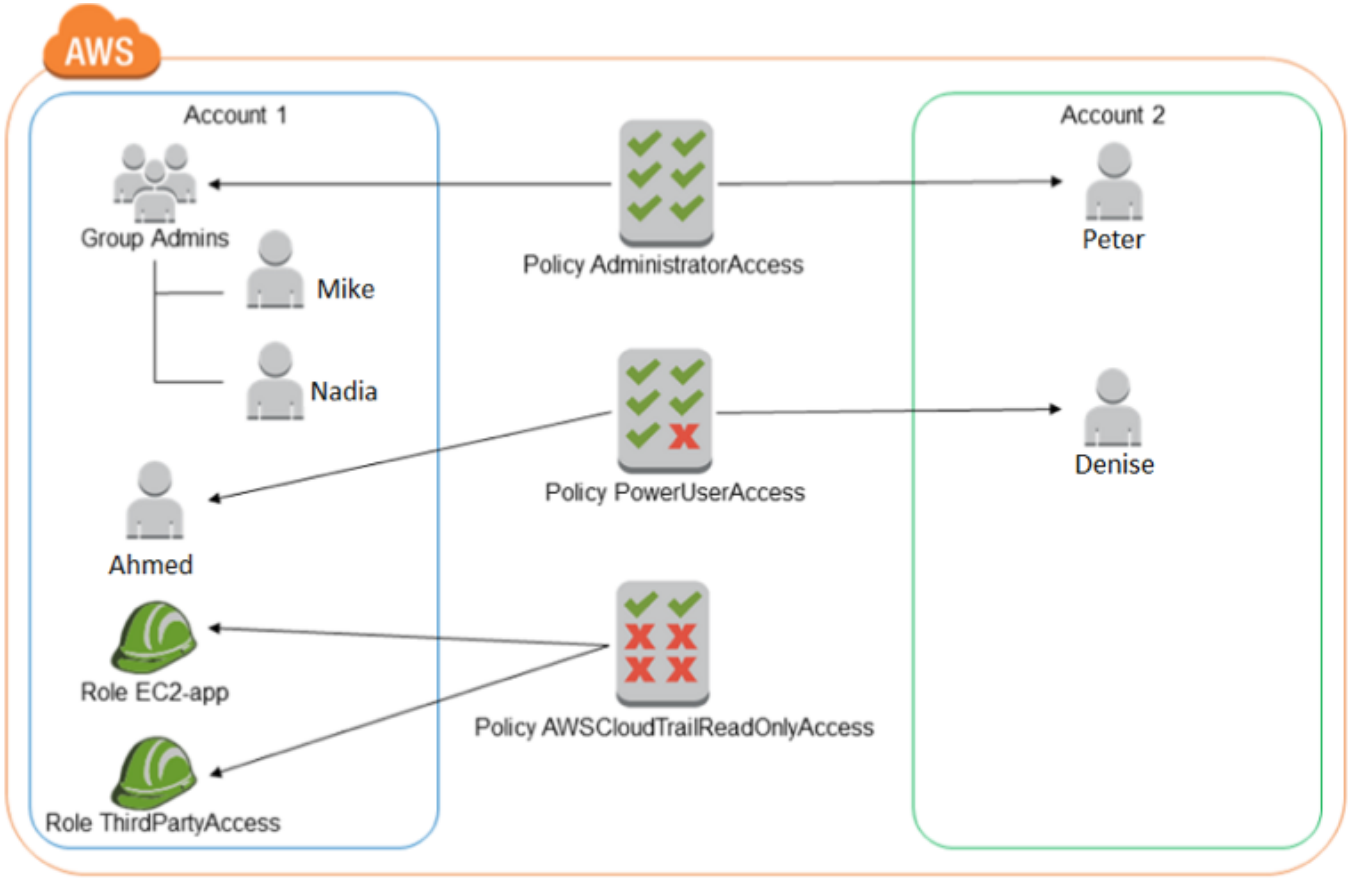
AWS Managed Policies

- 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

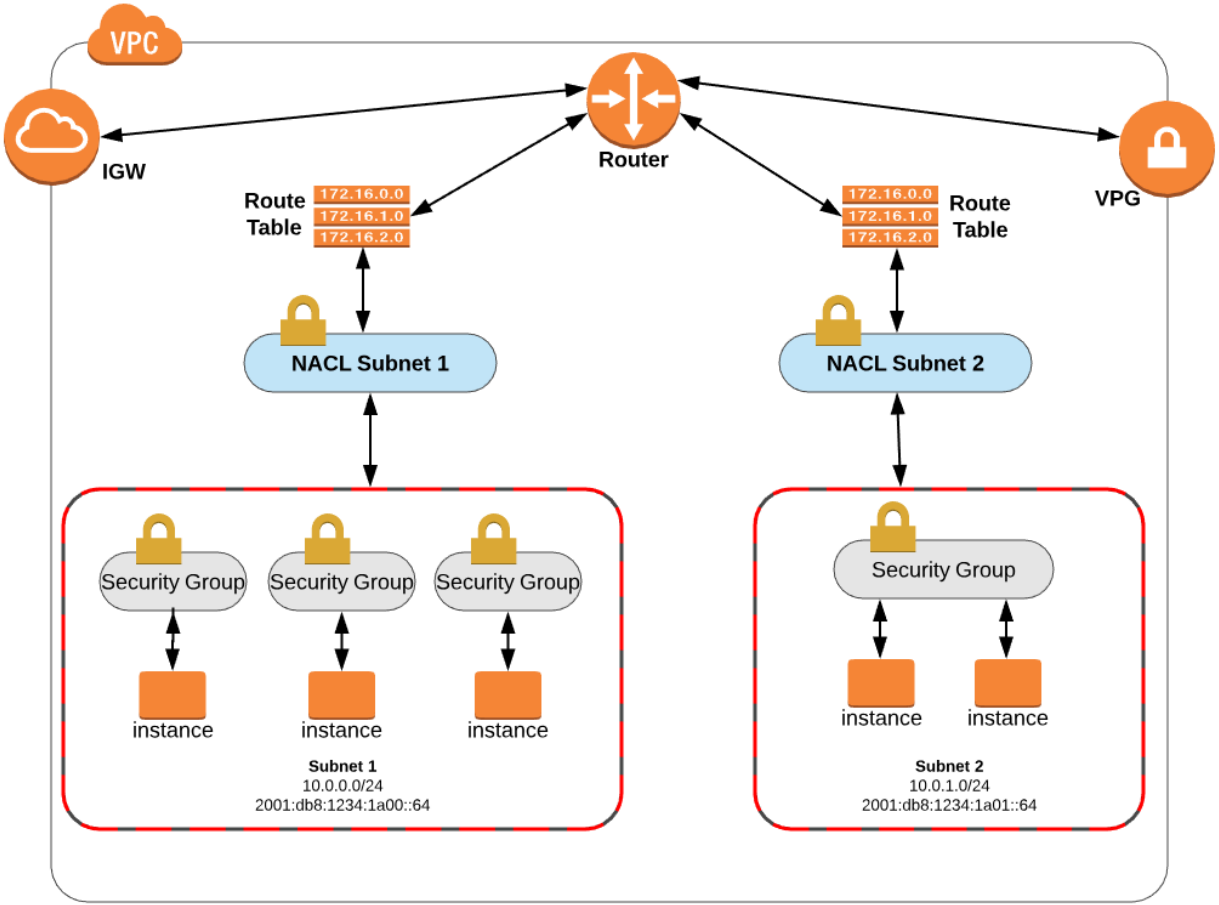


AWS Managed Policies

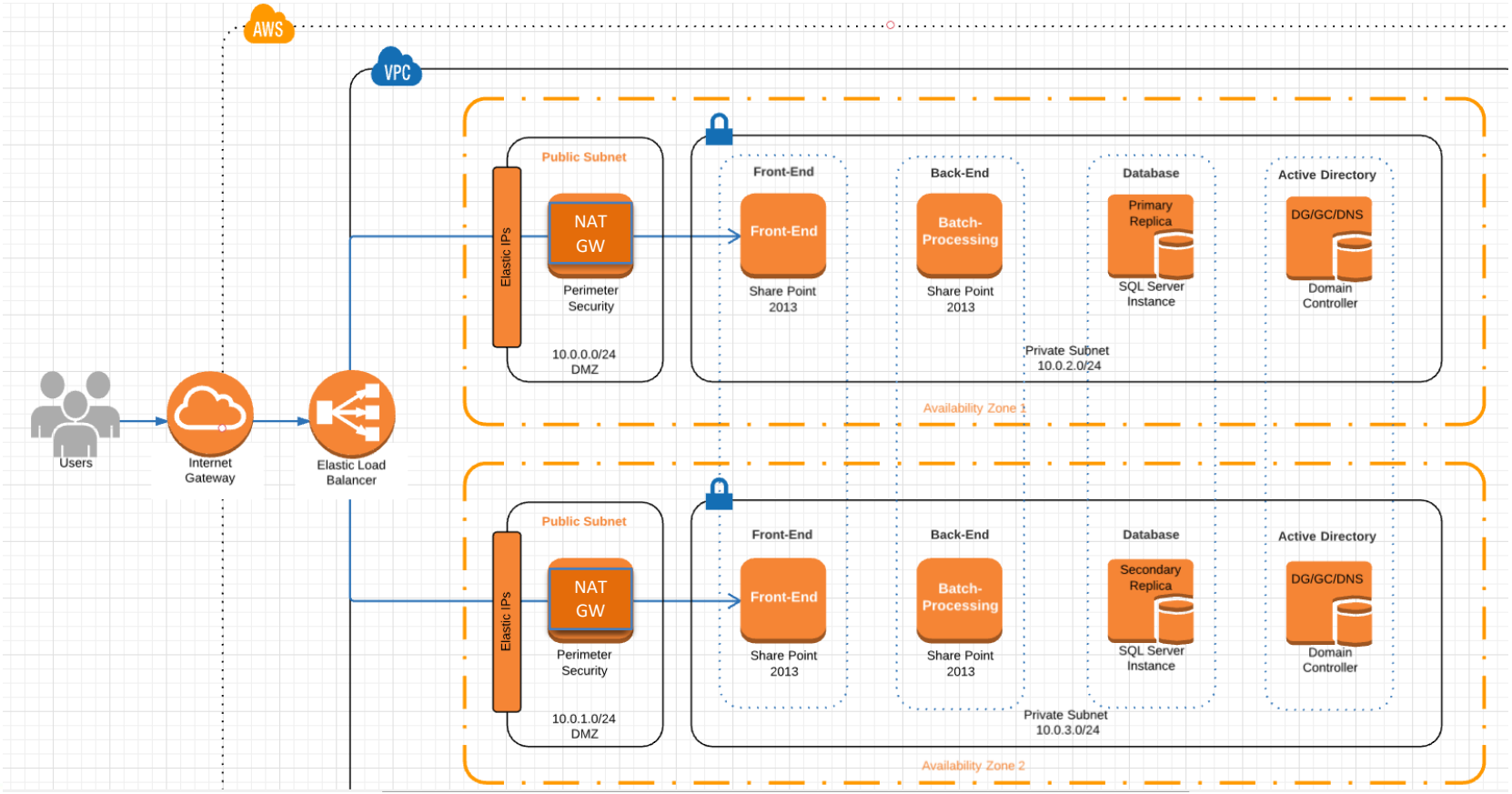


Segment 3: Infrastructure Security

Infrastructure Security Begins with Design



Infrastructure Security Begins with Design



Pearson

VPC with Public & Private Subnets

VPC Management Console

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

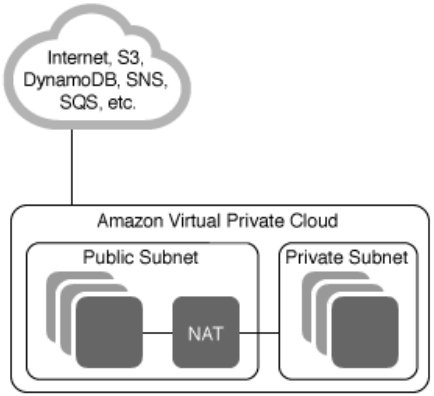
- VPC with a Single Public Subnet
- **VPC with Public and Private Subnets**
- VPC with Public and Private Subnets and Hardware VPN Access
- VPC with a Private Subnet Only and Hardware VPN Access

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

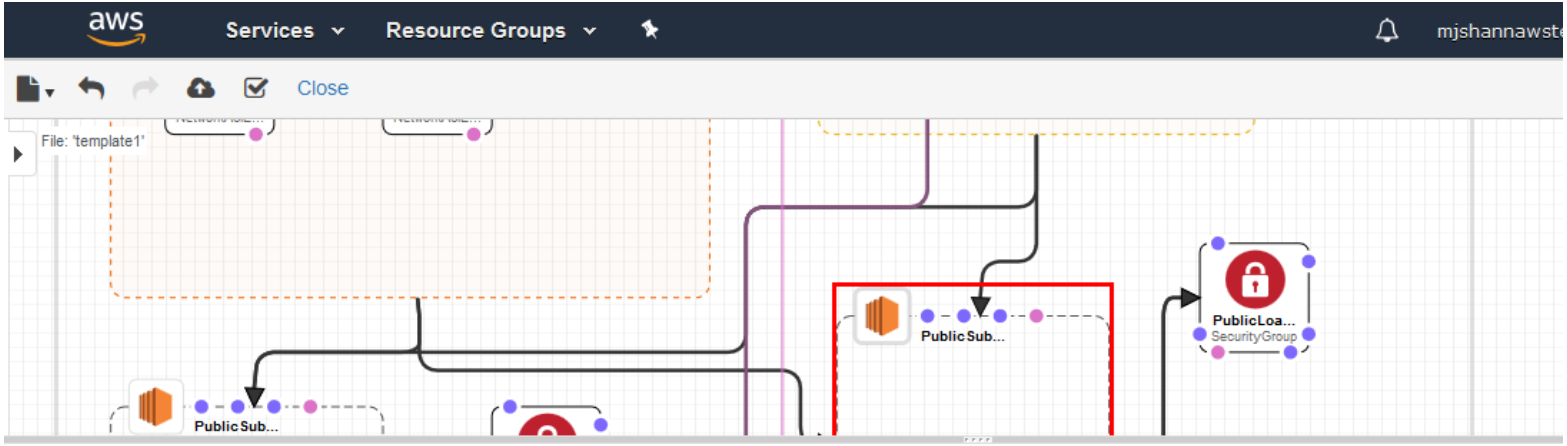


Pearson

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.	View	View in Designer	Launch Stack
Amazon VPC with static routing to an existing VPN	Creates a private subnet with a VPN connection that uses static routing to an existing VPN endpoint.	View	View in Designer	Launch Stack
Autoscaling and load-balancing website in an Amazon VPC	Creates a load balancing, auto scaling sample website in an existing VPC.	View	View in Designer	Launch Stack
Amazon VPC with DNS and public IP addresses	Creates a VPC with DNS support and public IP addresses enabled.	View	View in Designer	Launch Stack
Publicly accessible Amazon EC2 instances that are in an Auto Scaling group	Creates a load balancing, autoscaling group with instances that are directly accessible from the Internet.	View	View in Designer	Launch Stack
Amazon EC2 with multiple dynamic IP addresses in an Amazon VPC	Creates an Amazon EC2 instance with multiple dynamic IP addresses in a VPC.	View	View in Designer	Launch Stack

AWS CloudFormation Templates



temp...

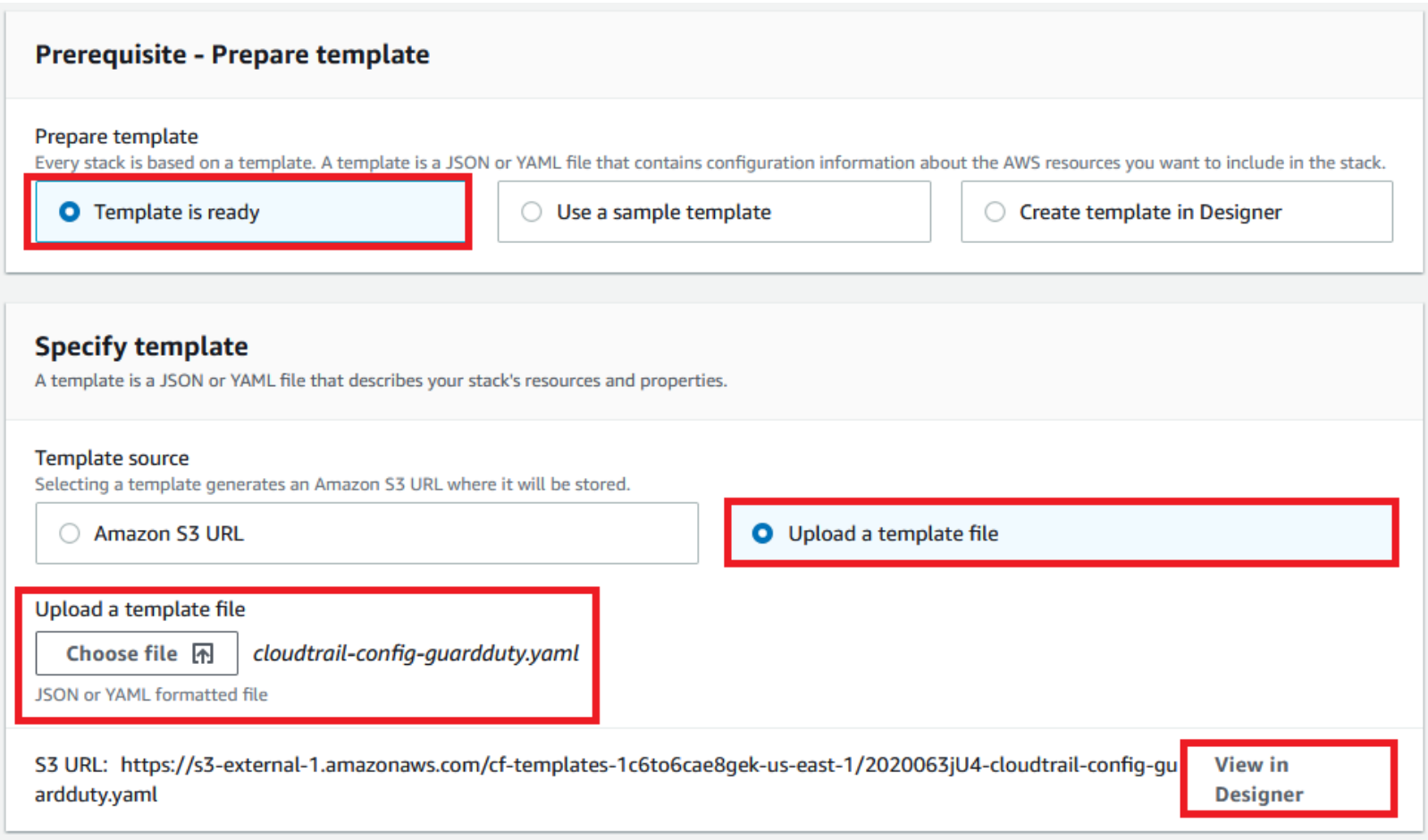
Choose template language: JSON YAML

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

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



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

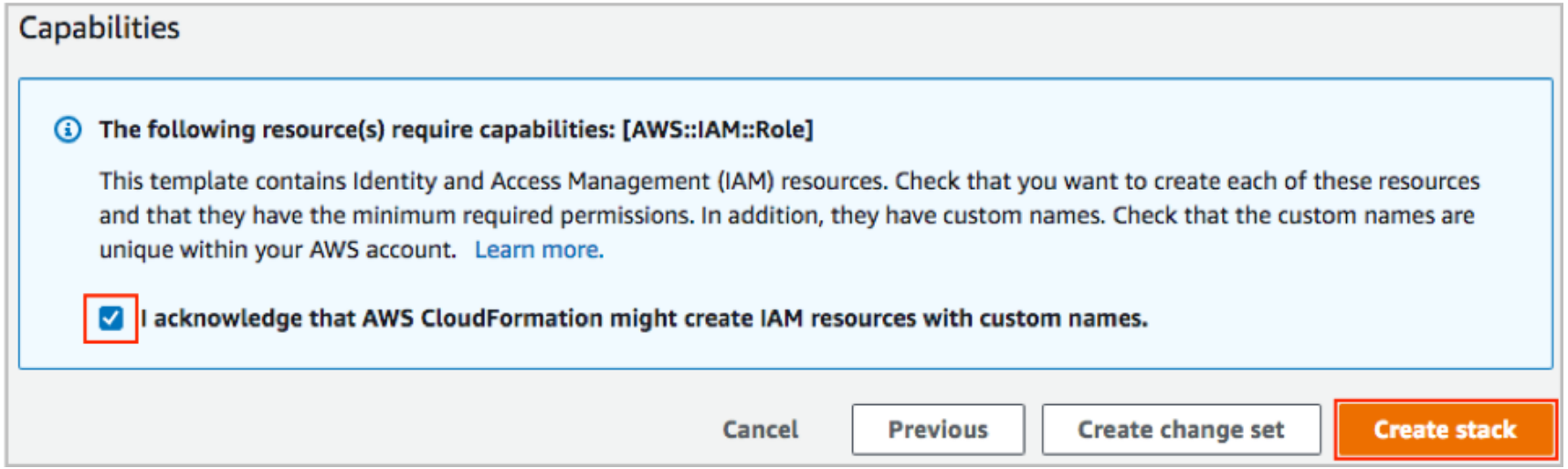
GuardDuty

GuardDutyEmailAddress

Enter the email address that will receive the alerts

someone@example.com

Automating with CloudFormation



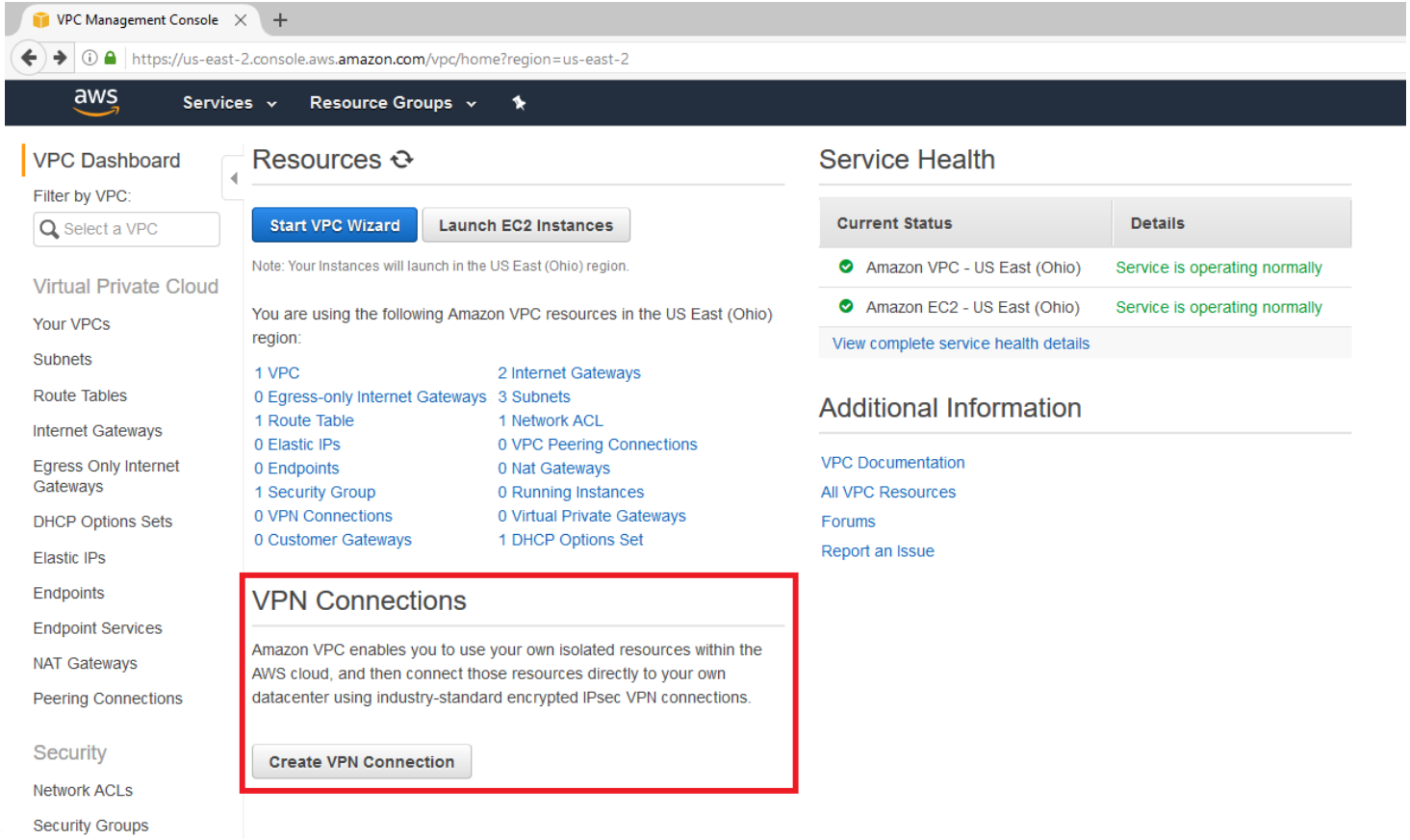
Options for Protecting VPC

- **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

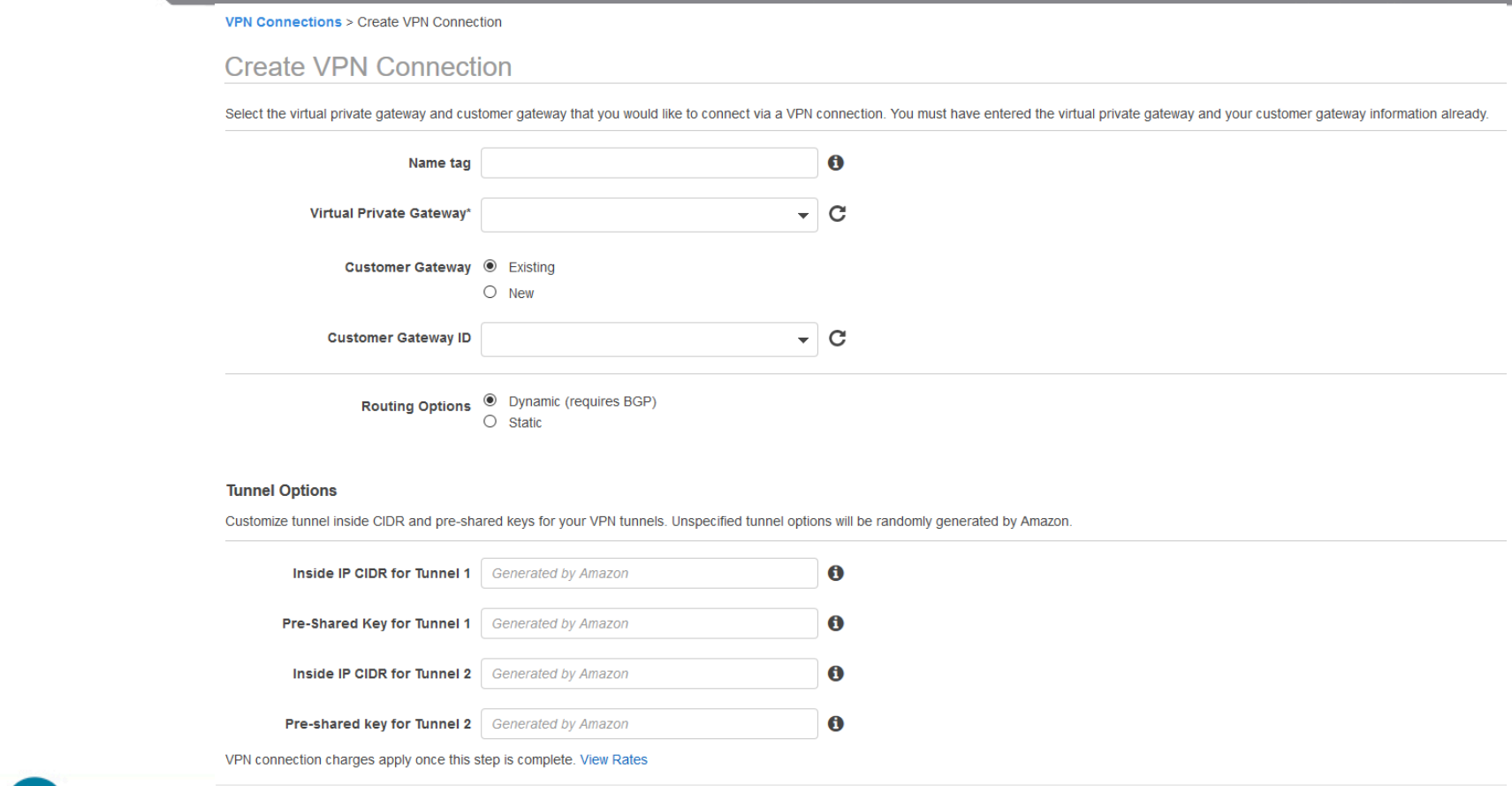
Options for Protecting VPC

- **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

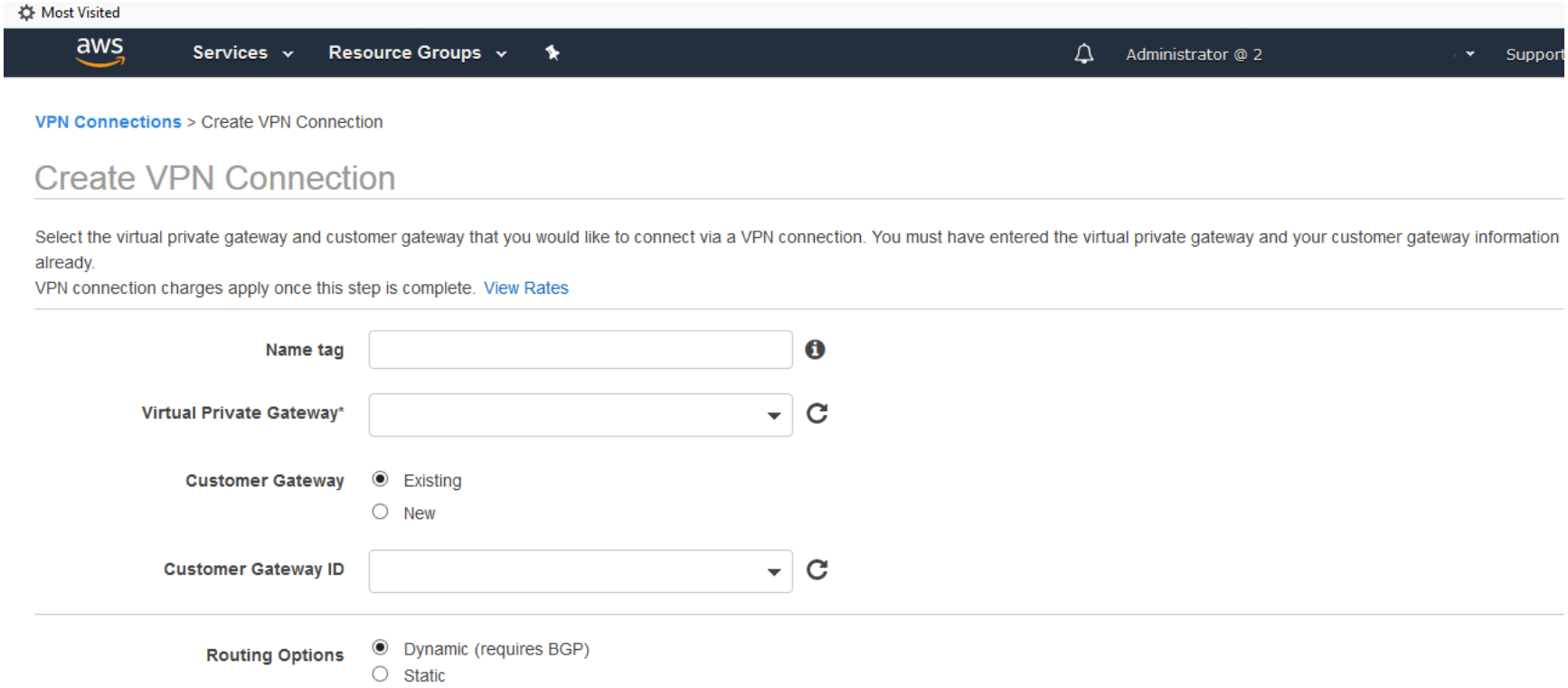
AWS Site-to-Site VPN



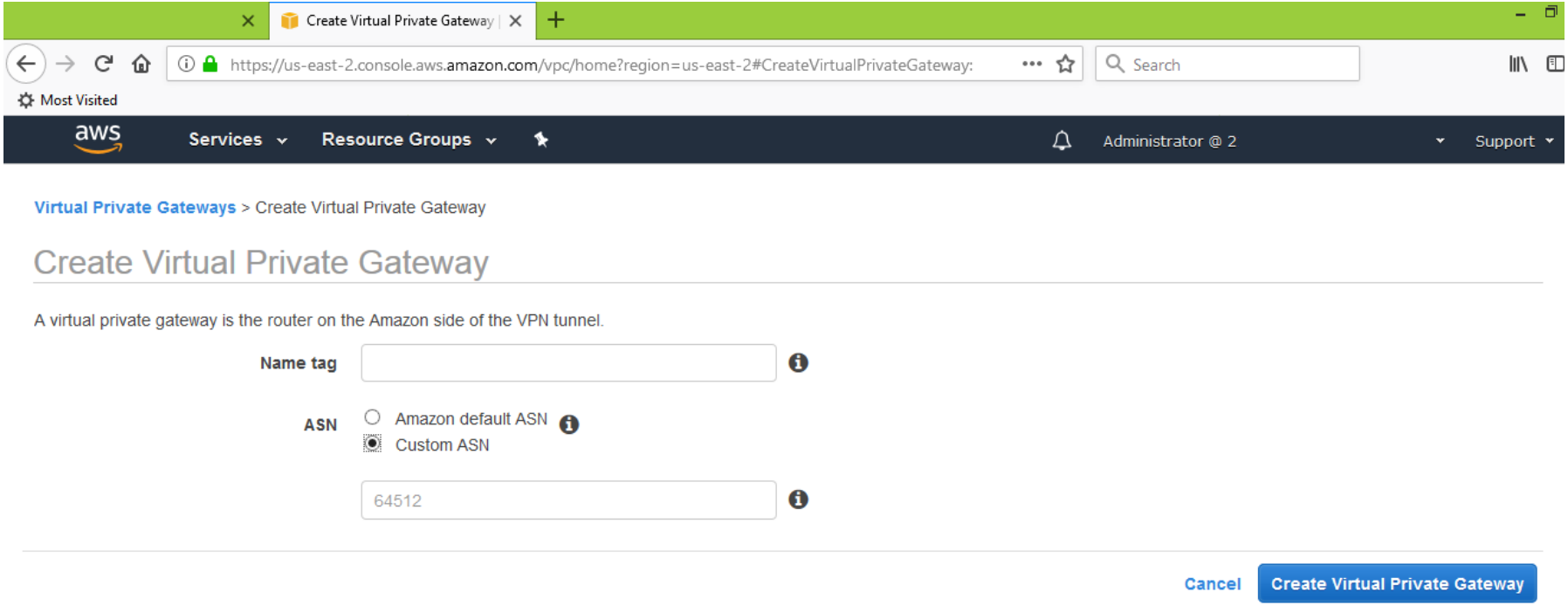
AWS Site-to-Site VPN



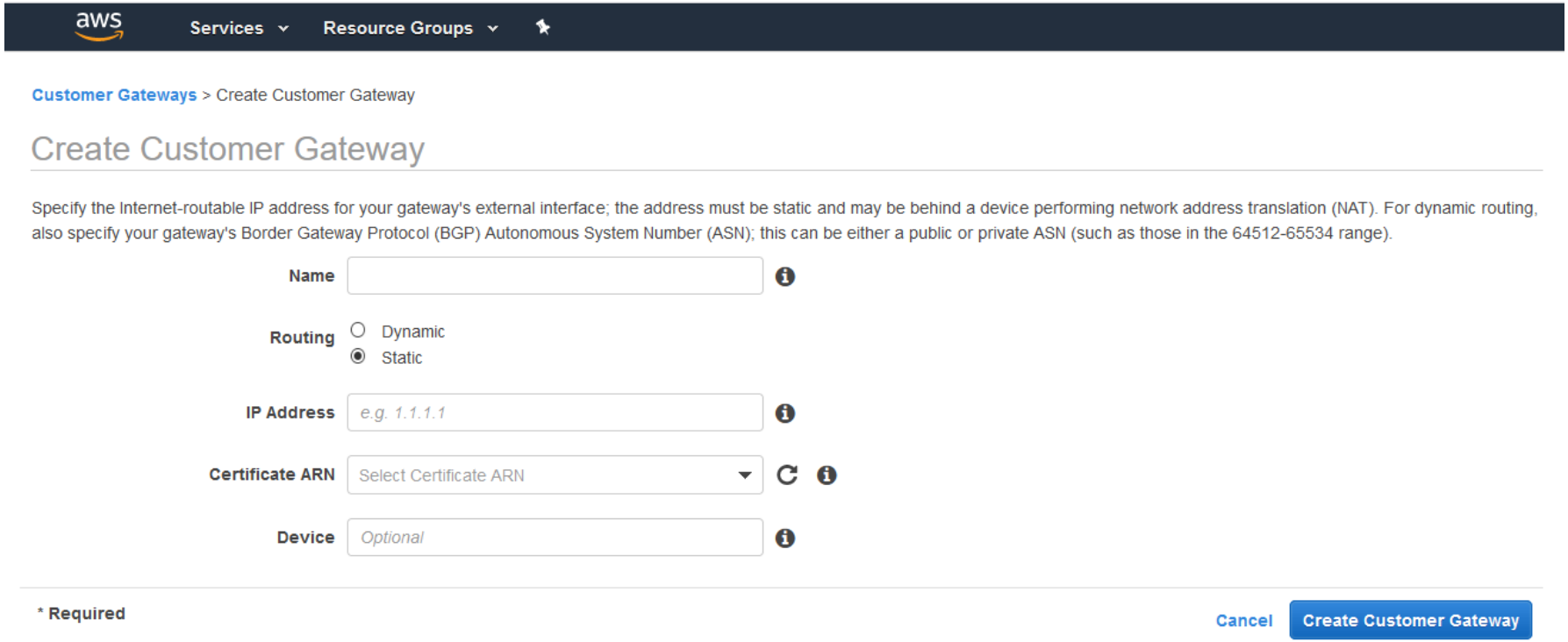
AWS Site-to-Site VPN



Create Virtual Private Gateway

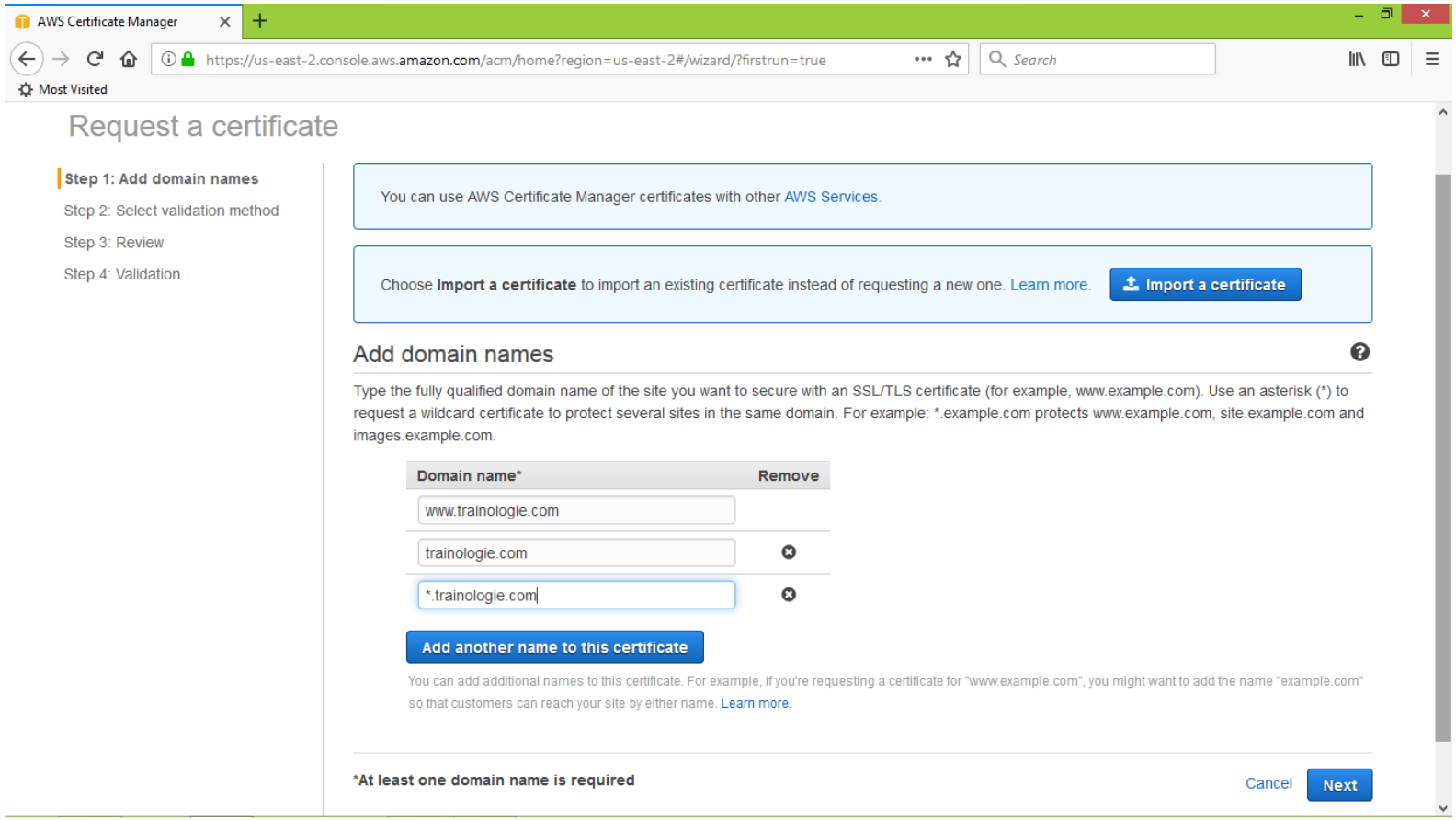


Create Customer Gateway



Pearson

Using AWS Certificate Manager



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* ⓘ

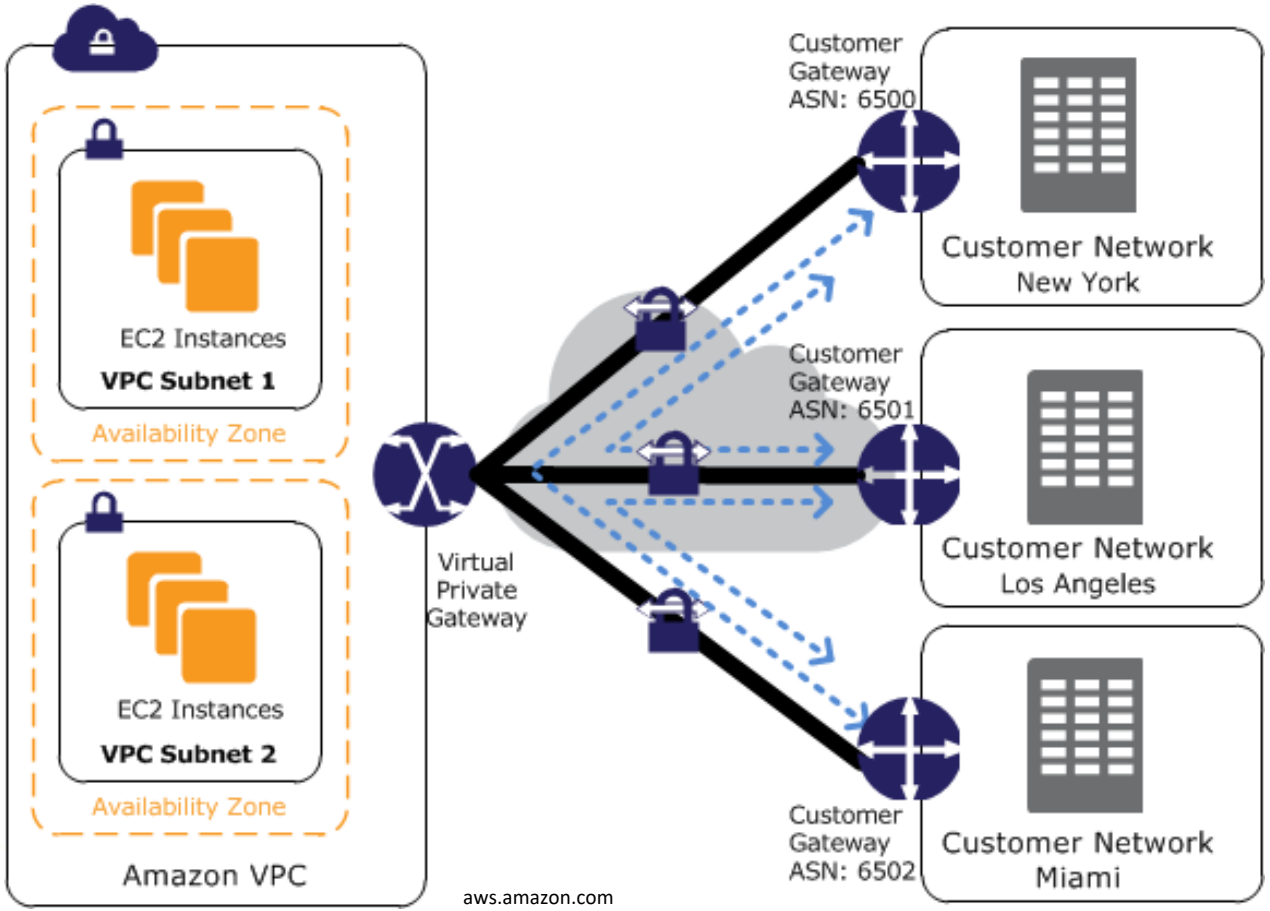
Pre-Shared Key for Tunnel 1 *Generated by Amazon* ⓘ

Inside IP CIDR for Tunnel 2 *Generated by Amazon* ⓘ

Pre-shared key for Tunnel 2 *Generated by Amazon* ⓘ

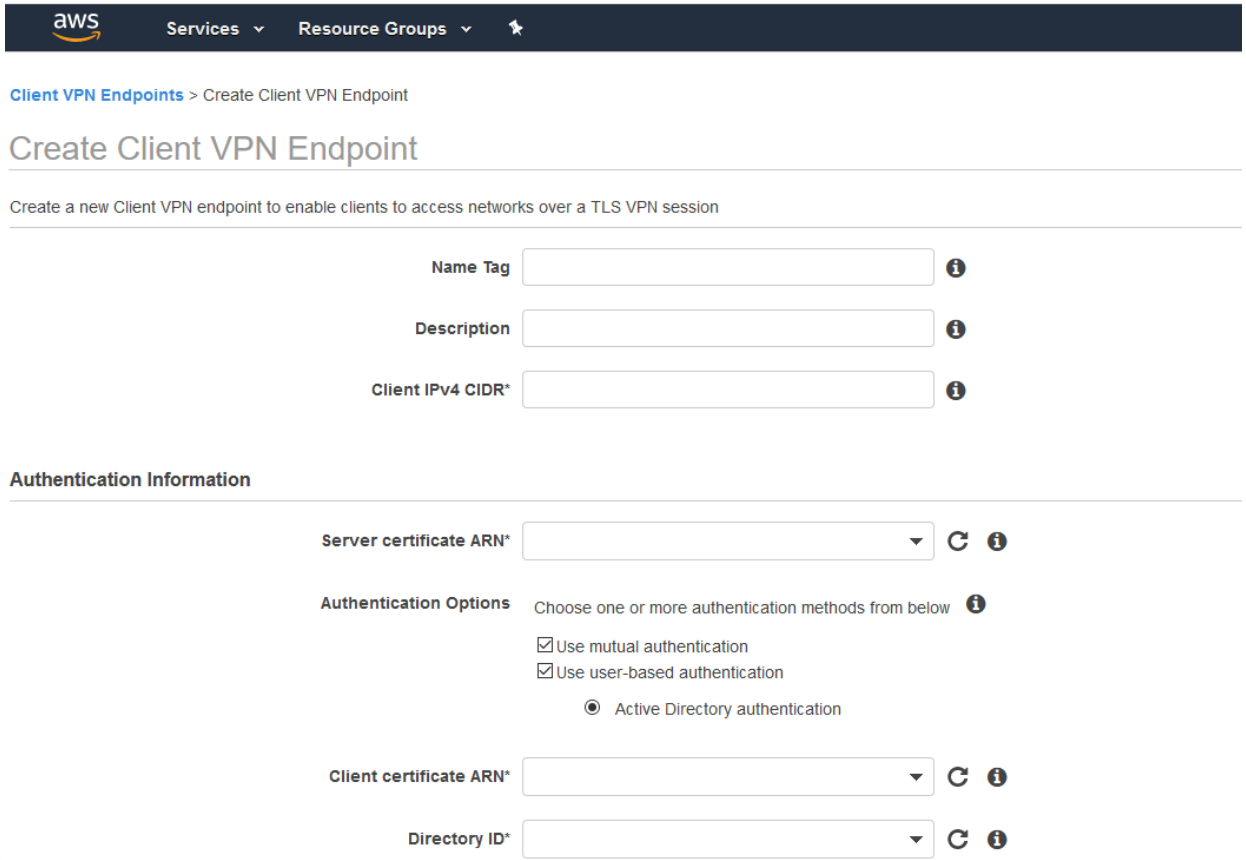
Cancel **Create VPN Connection**

AWS CloudHub VPN



aws.amazon.com

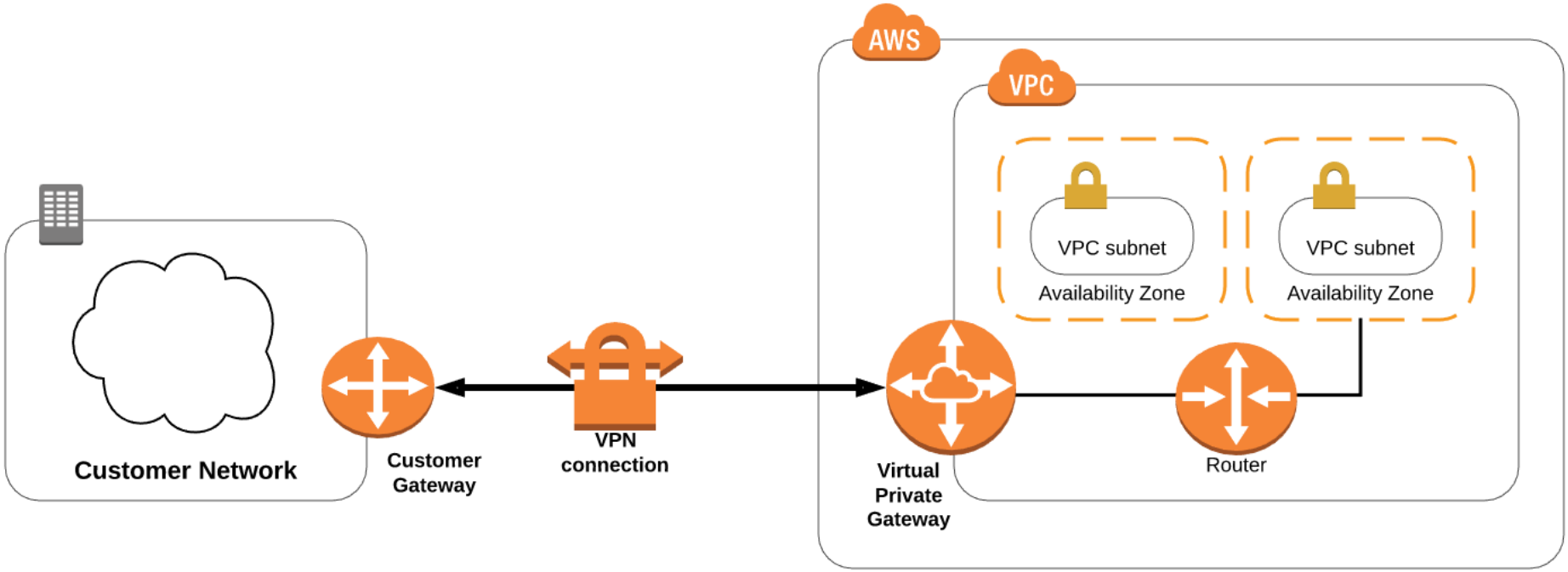
AWS Client VPN Endpoints



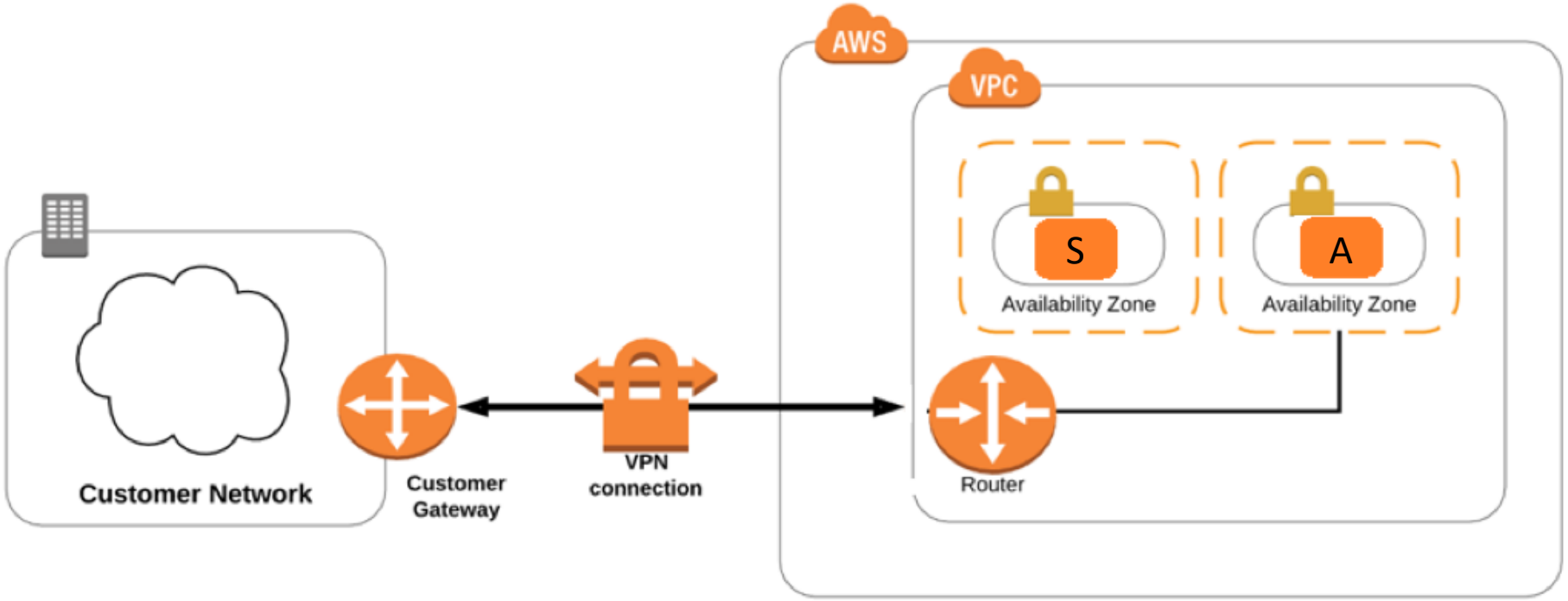
AWS Site-to-Site (Managed) VPNs

- 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

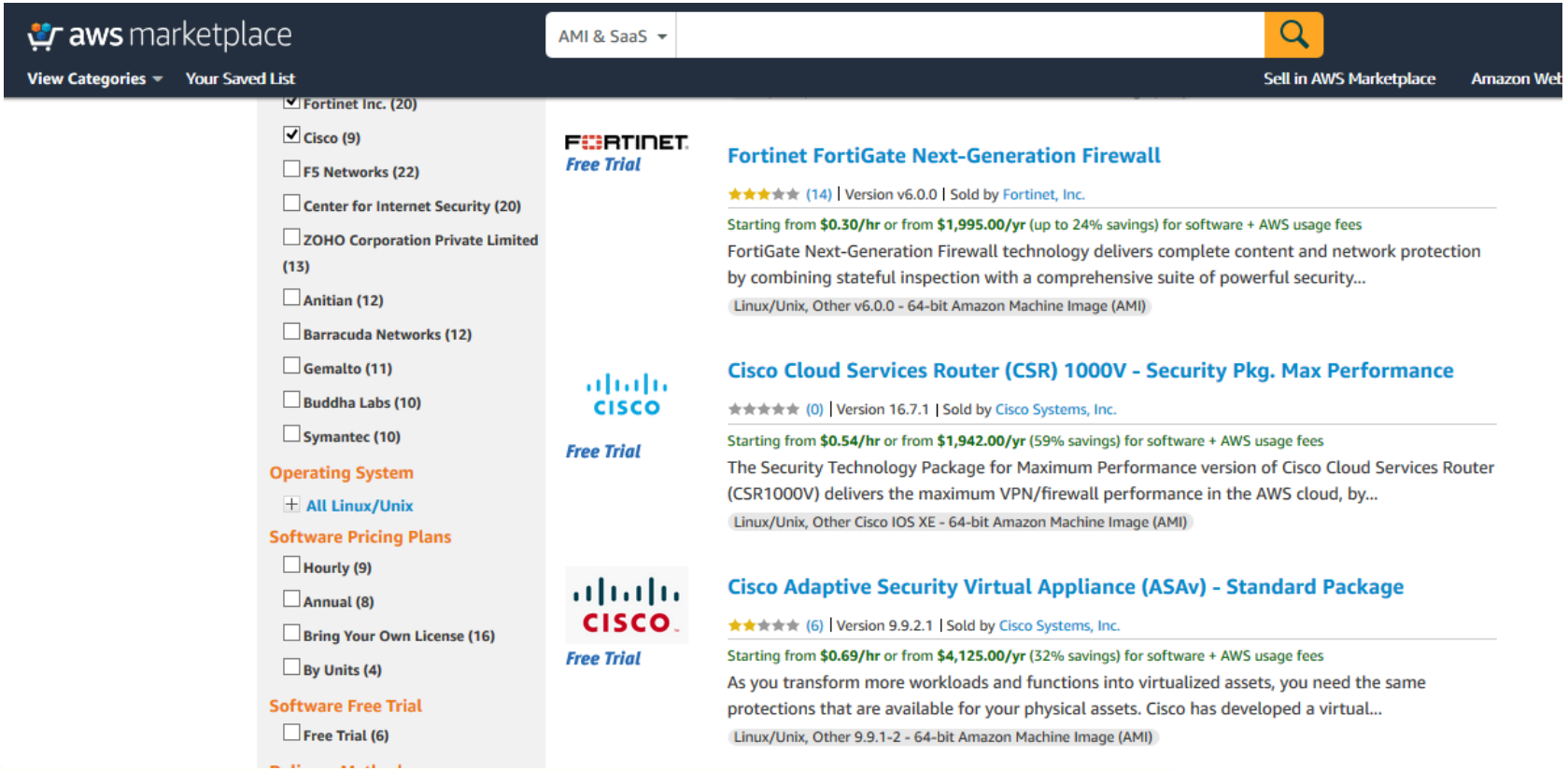
Single VPN Connection



EC2 Instance to Terminate VPN



AWS Marketplace



AWS 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