AWS Security Essentials

Instructor: Philip Matusiak
Email: philmatusiak@gmail.com

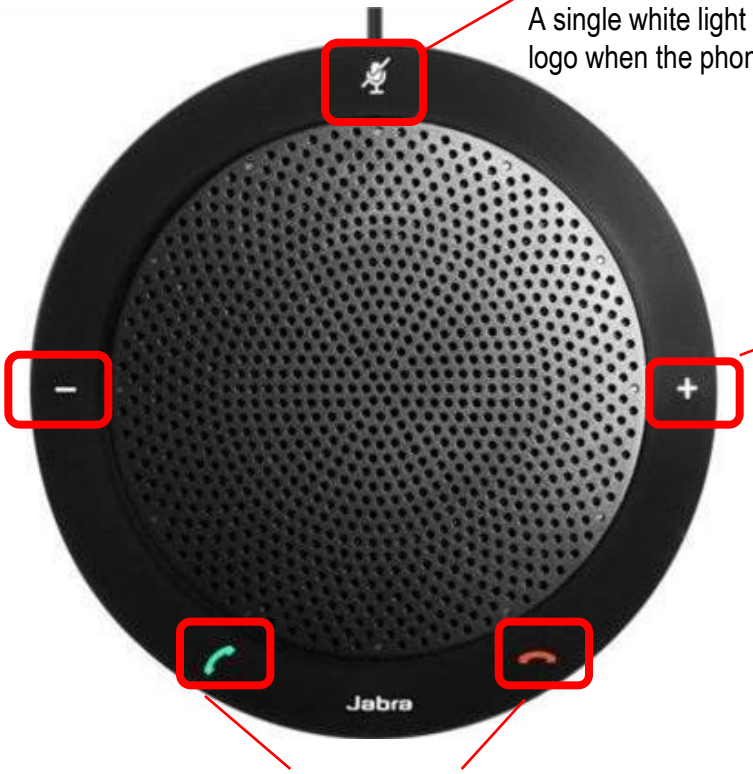
- Class begins at 10 Eastern time
- For Class Audio Connection:
  - ONLC Office Locations –
    Audio is connected over Jabra™ speaker

  - Home or Office –
    Call: xxx-xxx-xxxx Access Code: xxx xxx xxx#
    Enter the audio pin shown in the GoToMeeting panel
- If you need assistance, call 800-288-8221

onlc Training Centers

The Jabra Speaker

Mute Button – A ring of red lights appears around the speaker when the phone is muted. A single white light appears above the Jabra logo when the phone is not muted.



The On/Off Hook buttons have no function when connected to GoToMeeting audio.

RCI
REMOTE CLASSROOM INSTRUCTION

Mastering AWS Security

Mastering AWS Security starts with a deep dive into the fundamentals of the shared security responsibility model. T...

By Albert Anthony

REMOTE CLASSROOM INSTRUCTION

- Overview of Security in AWS
- AWS Identity and Access Management
- AWS Virtual Private Cloud
- Data Security in AWS
- Securing Servers in AWS
- Securing Applications in AWS
- Monitoring in AWS
- Logging and Auditing in AWS
- AWS Security Best Practices

Overview of Security in AWS

- Overview of Security in AWS
- Chapter overview
- AWS shared security responsibility model
- AWS Security responsibilities
- Customer security responsibilities
- AWS account security features
- AWS Security services
- AWS Security resources
- Summary

AWS Identity and Access Management

- AWS Identity and Access Management
- Chapter overview
- IAM features and tools
- IAM Authentication
- IAM Authorization
- Passwords Policy
- AWS credentials
- IAM limitations
- IAM best practices
- Summary

AWS Virtual Private Cloud

- AWS Virtual Private Cloud
- Chapter overview
- VPC components
- VPC features and benefits
- VPC use cases
- VPC security
- Creating VPC
- VPC limits
- VPC best practices
- Summary

Data Security in AWS

- Data Security in AWS
- Chapter overview
- Encryption and decryption fundamentals
- Securing data at rest
- Securing data in transit
- AWS KMS
- AWS CloudHSM
- Amazon Macie
- Summary

Securing Servers in AWS

- Securing Servers in AWS
- EC2 Security best practices
- EC2 Security
- Amazon Inspector
- AWS Shield
- Summary

Securing Applications in AWS

- Securing Applications in AWS
- AWS Web Application Firewall (WAF)
- Signing AWS API requests
- Amazon Cognito
- Amazon API Gateway
- Summary

Monitoring in AWS

- Monitoring in AWS
- AWS CloudWatch
- Monitoring Amazon EC2
- Summary

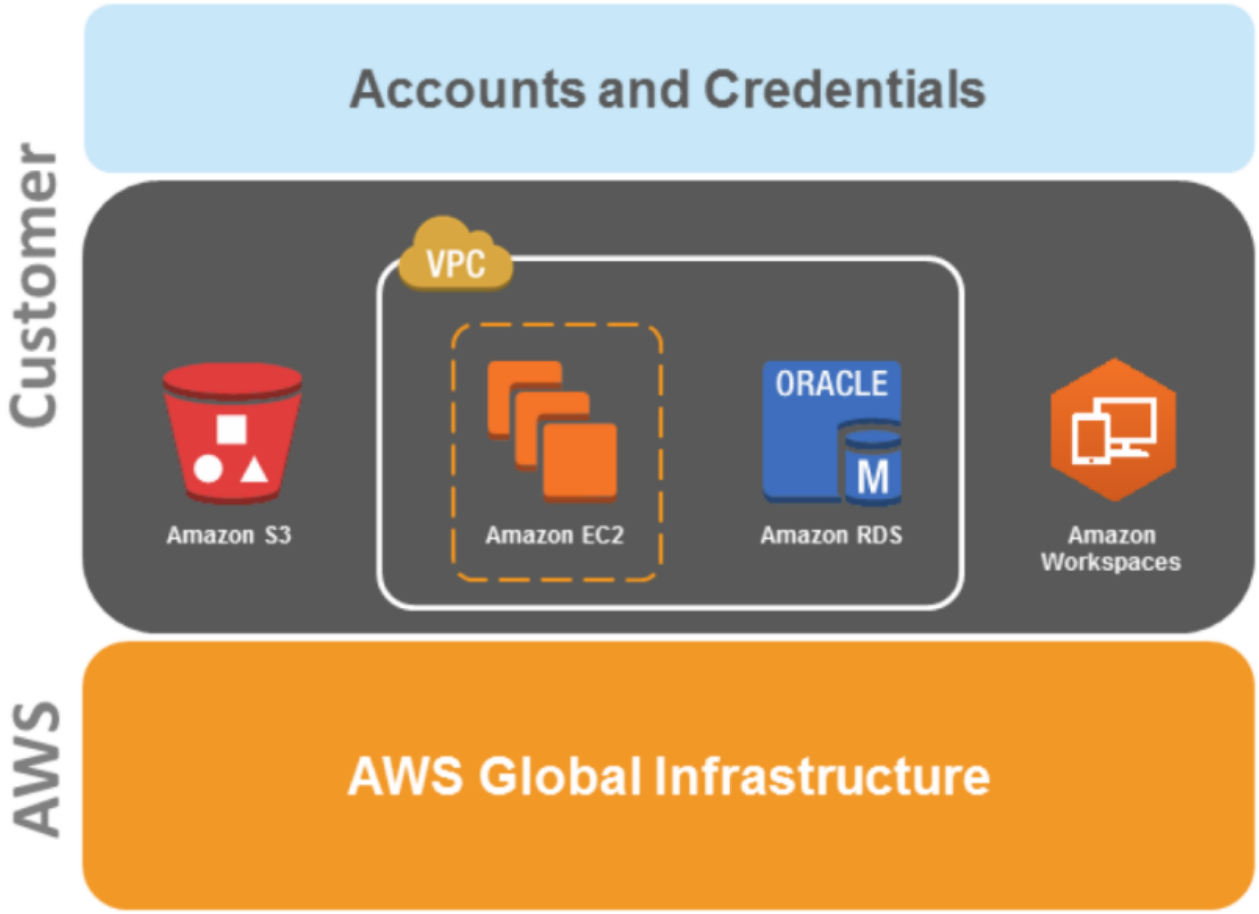
Logging and Auditing in AWS

- Logging and Auditing in AWS
- Logging in AWS
- AWS CloudWatch Logs
- AWS CloudTrail
- Auditing in AWS

- AWS Artifact
- AWS Config
- AWS Trusted Advisor
- AWS Service Catalog
- AWS Security Audit Checklist

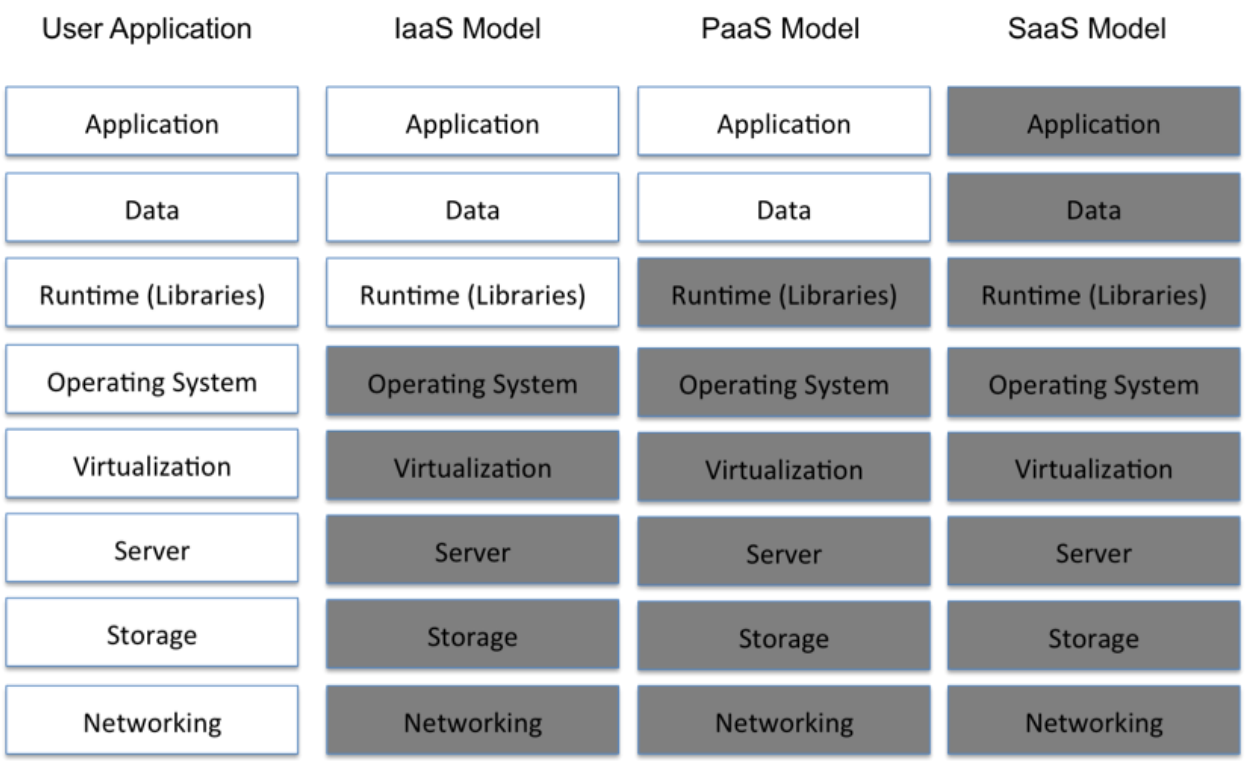
AWS Security Best Practices

- AWS Security Best Practices
- Shared security responsibility model
- IAM security best practices
- VPC
- Data security
- Security of servers
- Application security
- Monitoring, logging, and auditing
- AWS CAF
- Summary



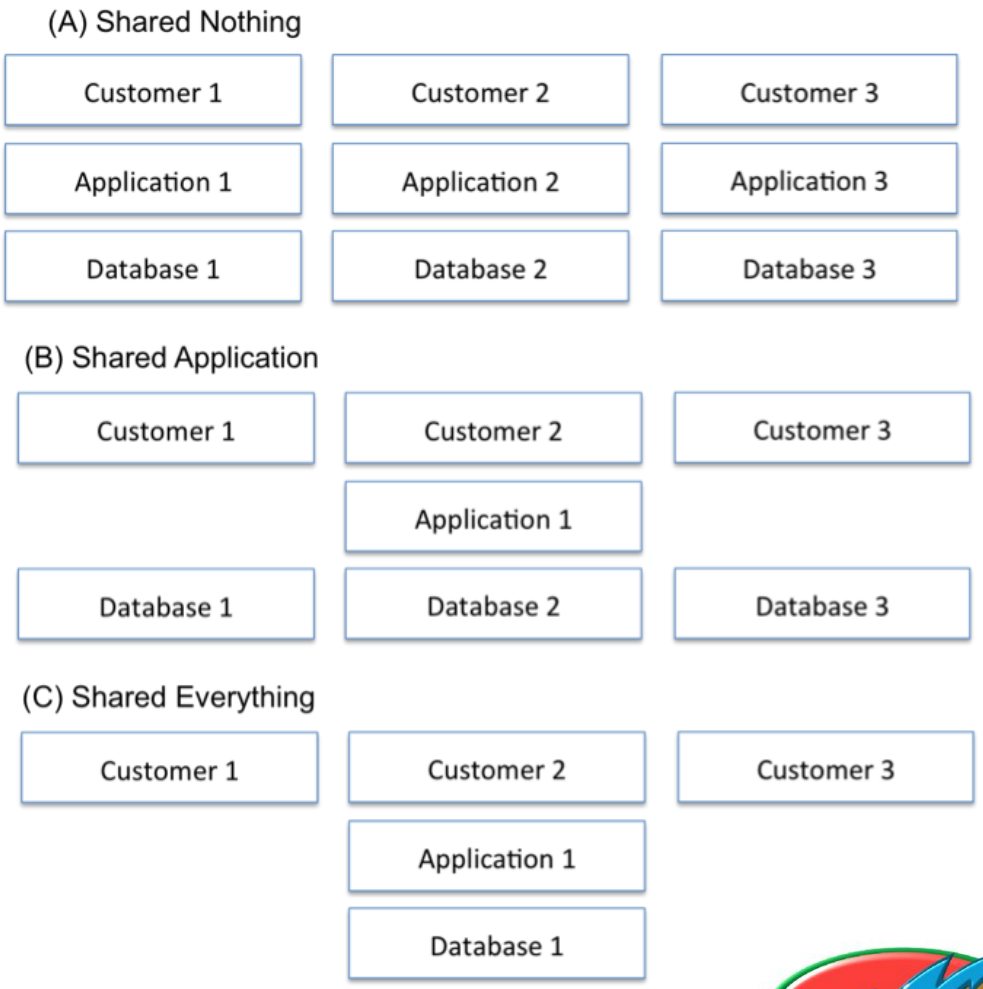
RCI
REMOTE CLASSROOM INSTRUCTION

Cloud service models – IaaS, PaaS, and SaaS

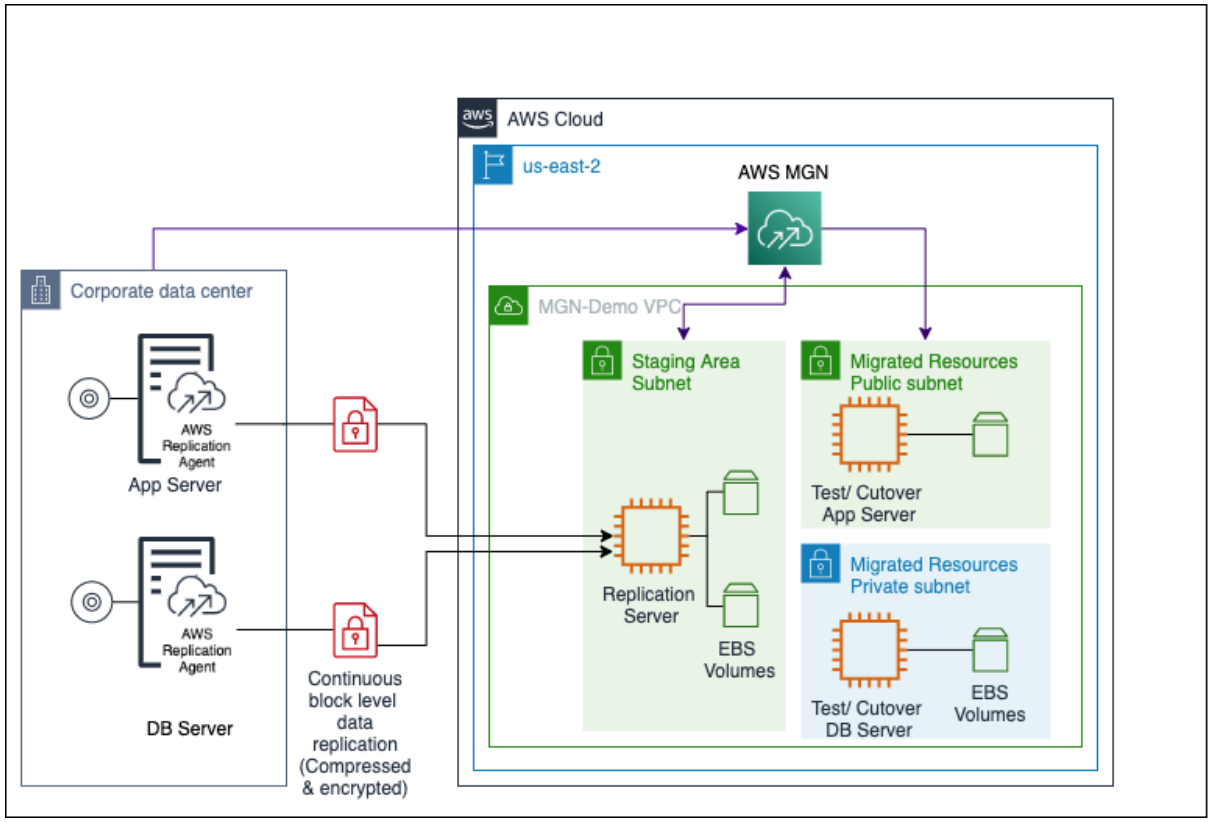


RCI
REMOTE CLASSROOM INSTRUCTION

Multi-tenancy models

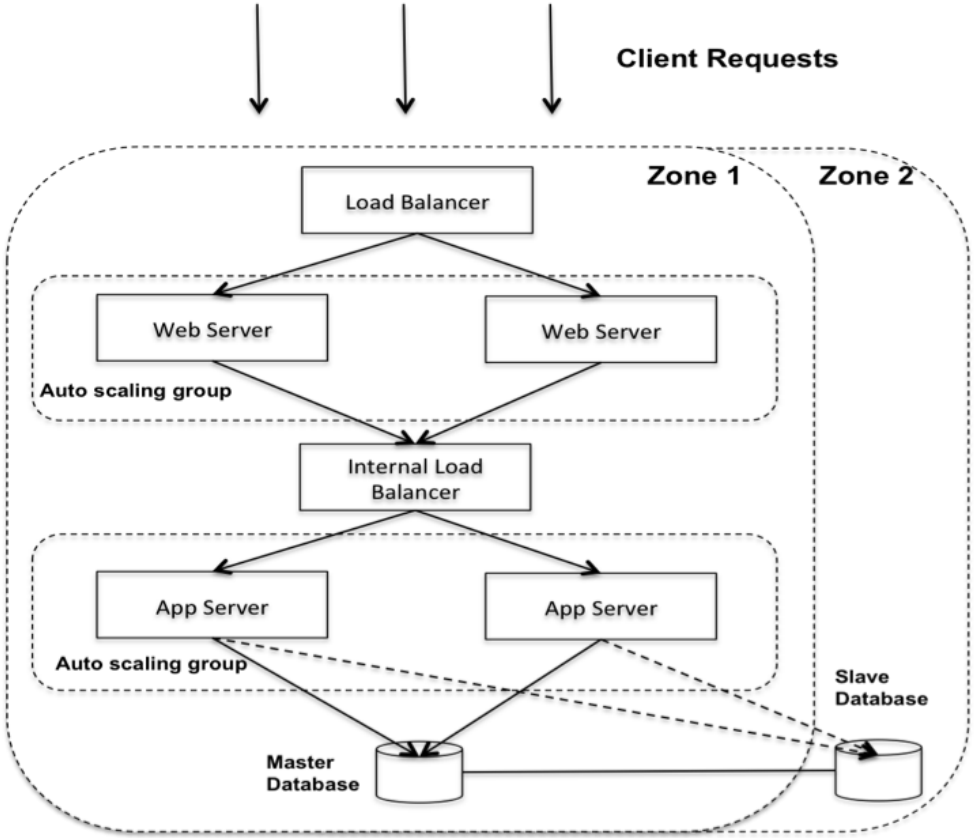


Migrating on-premise applications to the cloud



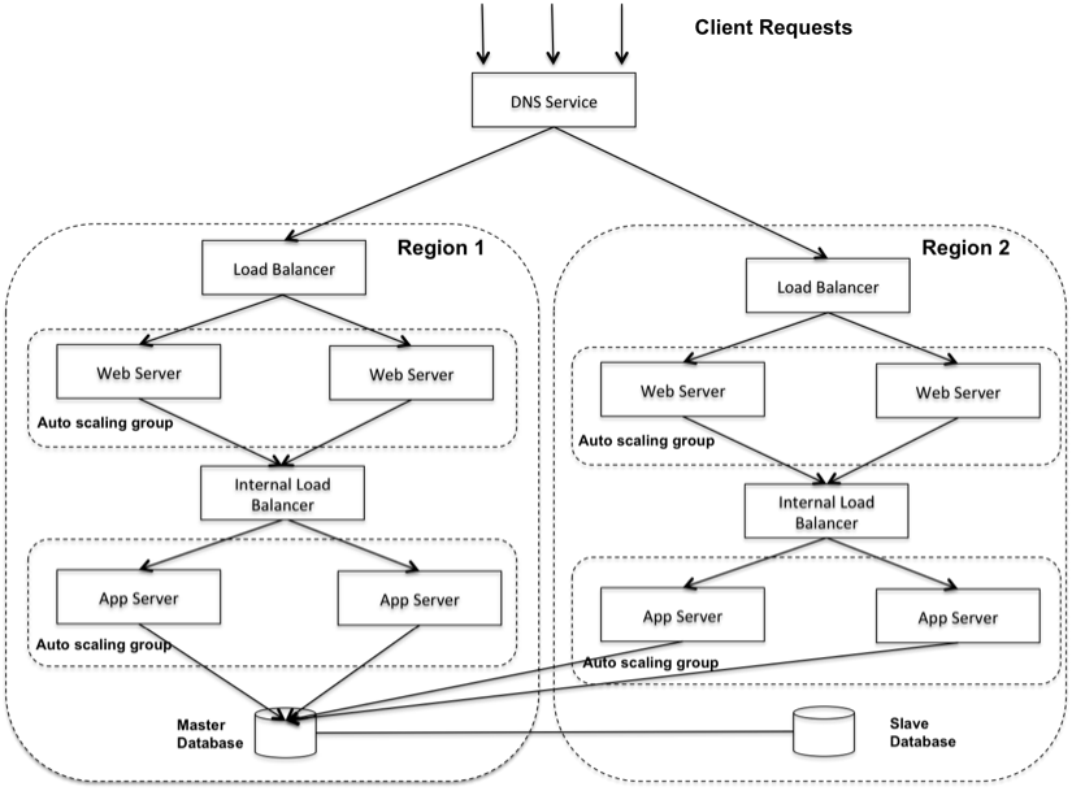
REMOTE CLASSROOM INSTRUCTION

Cloud-based single tier architecture



REMOTE CLASSROOM INSTRUCTION

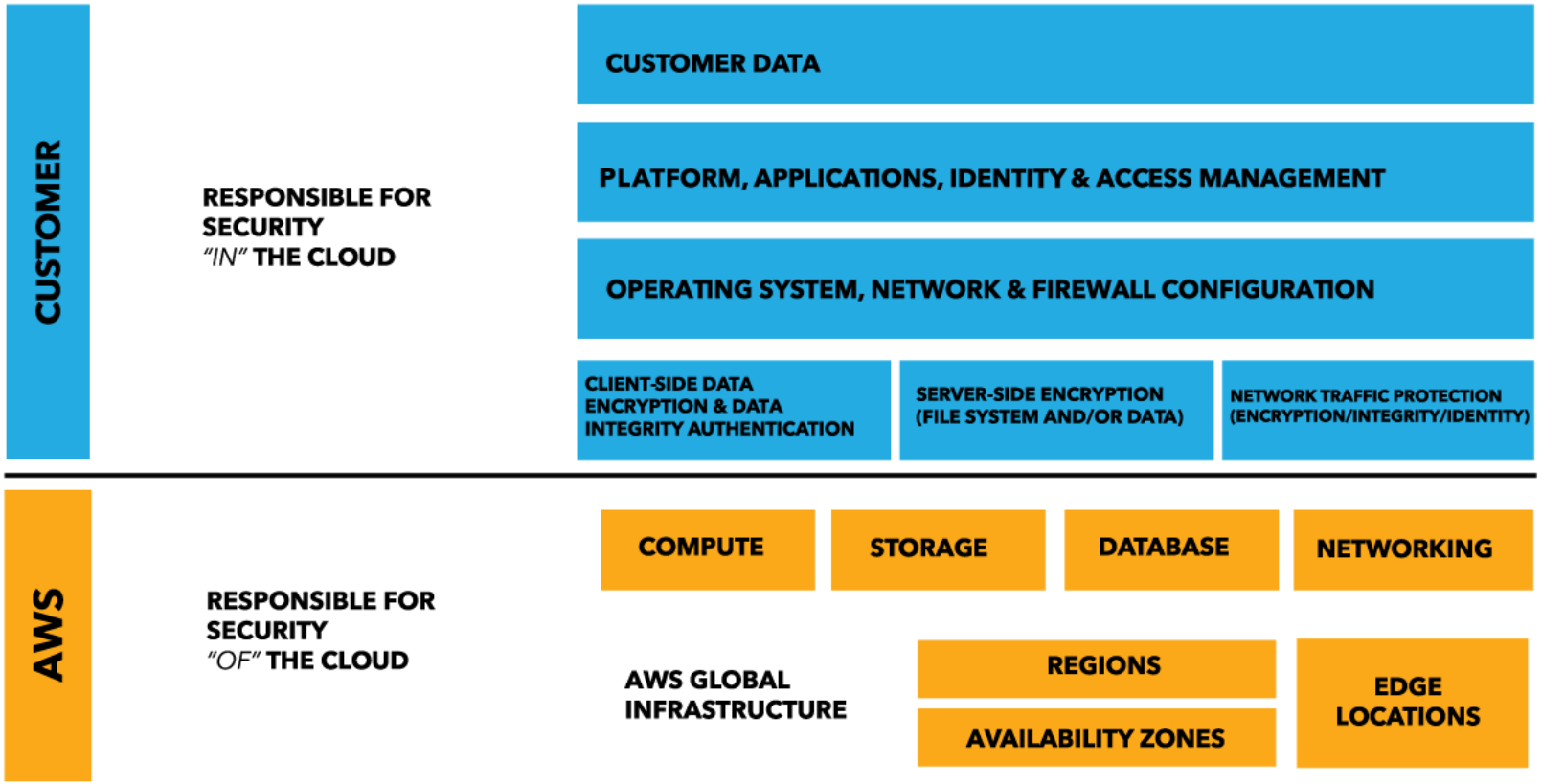
Cloud-based multitier architecture (high availability)



AWS Security Essentials - 1

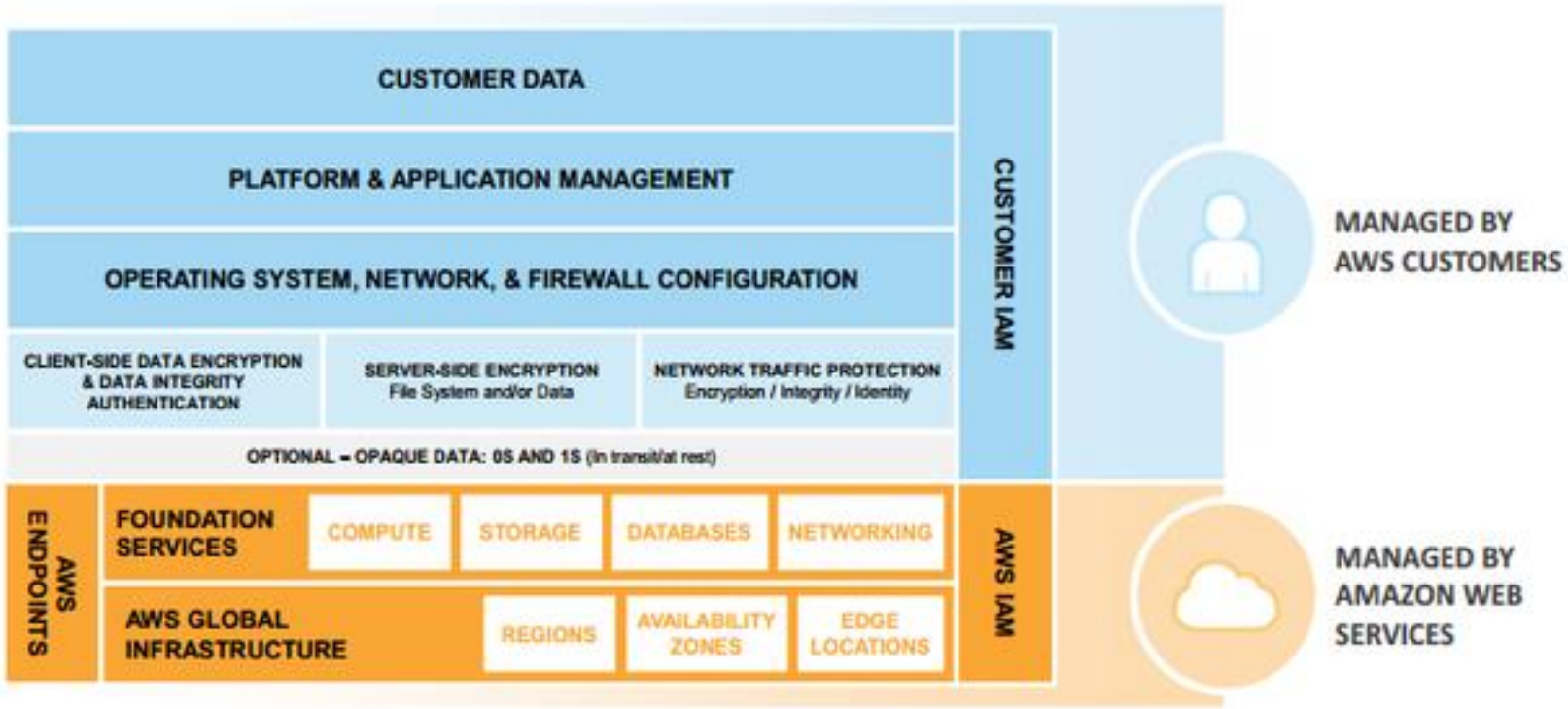
onlc
Training Centers

1.1 AWS shared security responsibility model



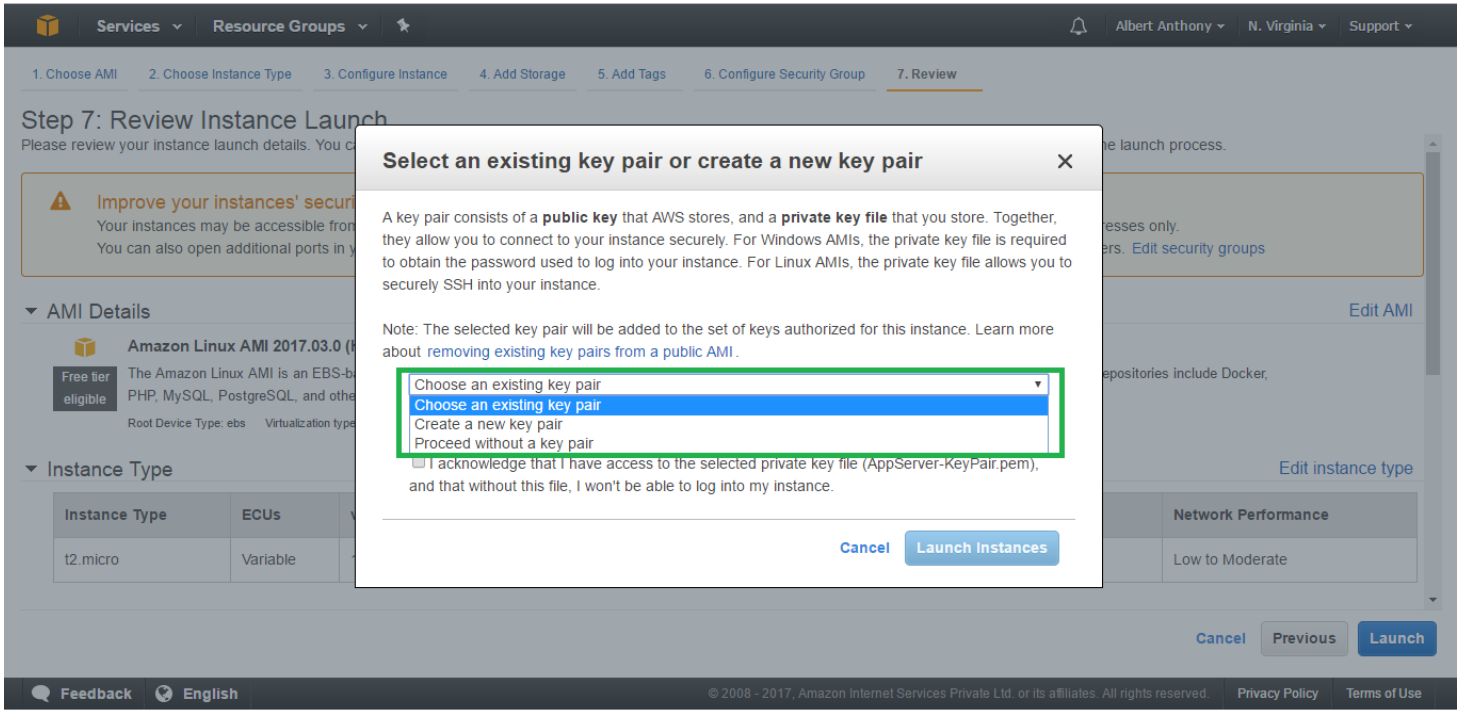
RCI
REMOTE CLASSROOM INSTRUCTION

1.2 Shared responsibility model for infrastructure services



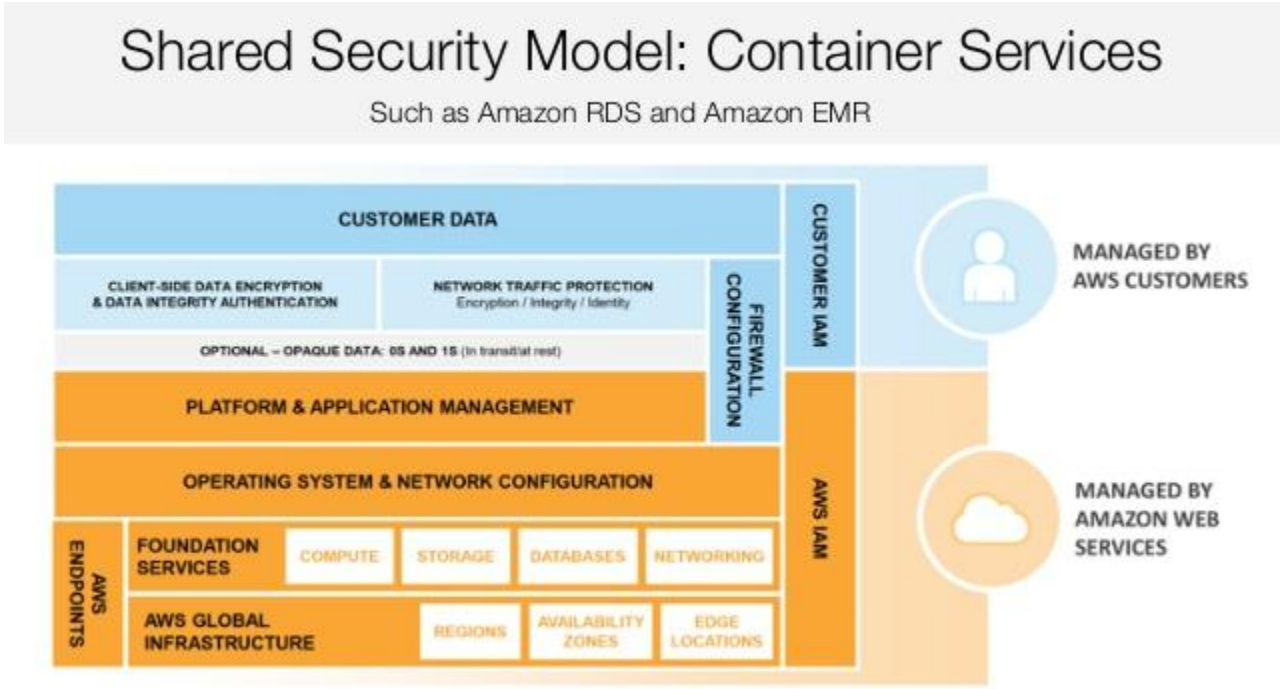
REMOTE CLASSROOM INSTRUCTION

1.3 AWS key pairs



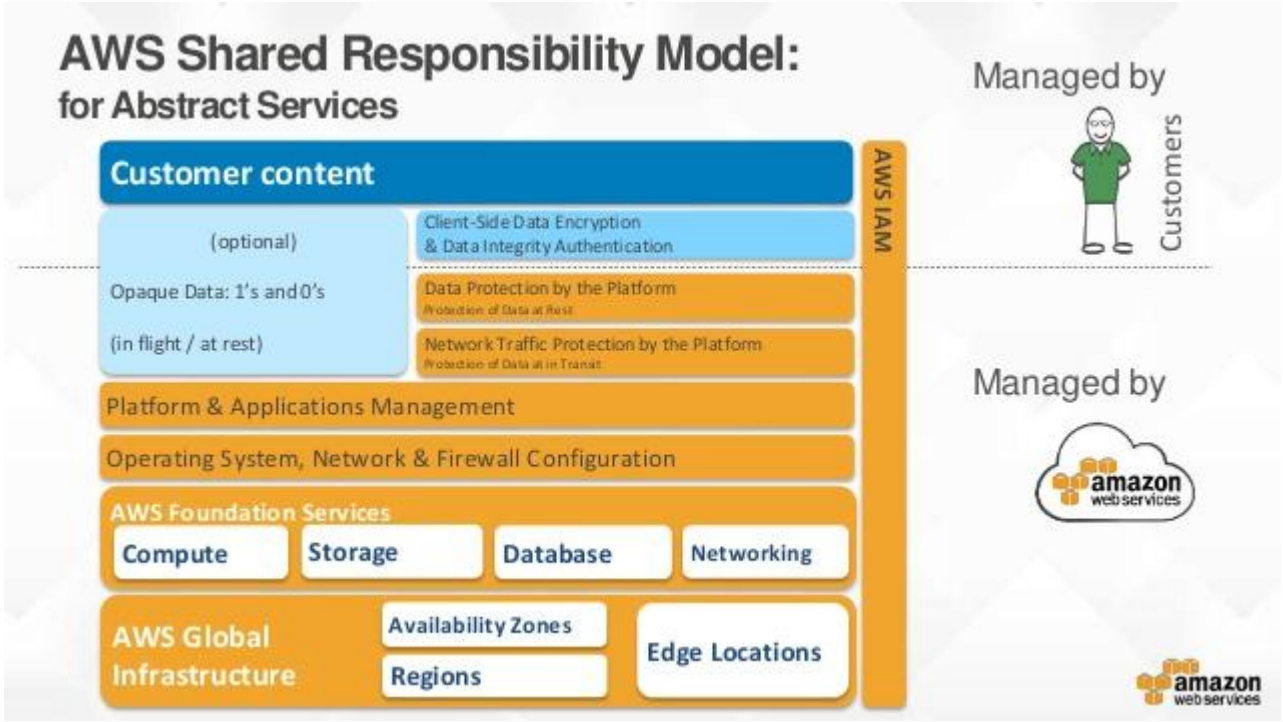
REMOTE CLASSROOM INSTRUCTION

1.4 Shared responsibility model for container services



REMOTE CLASSROOM INSTRUCTION

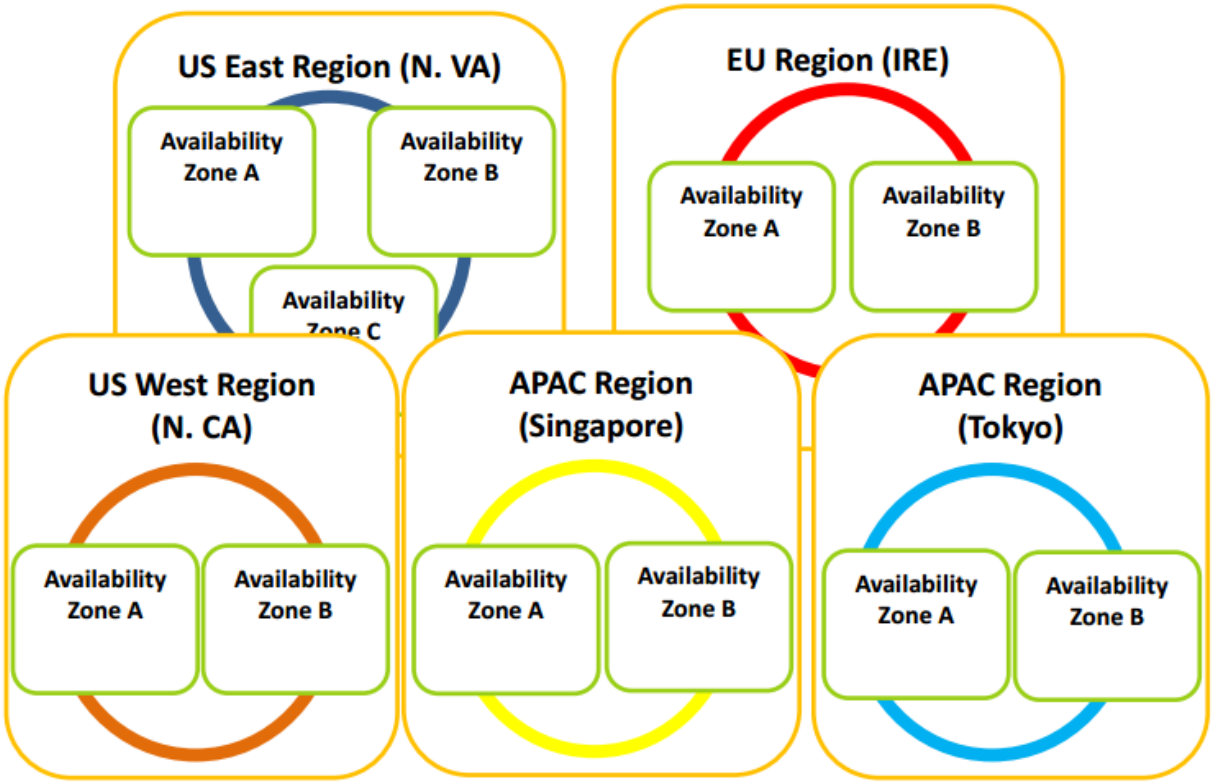
1.5 - Shared responsibility model for abstracted services



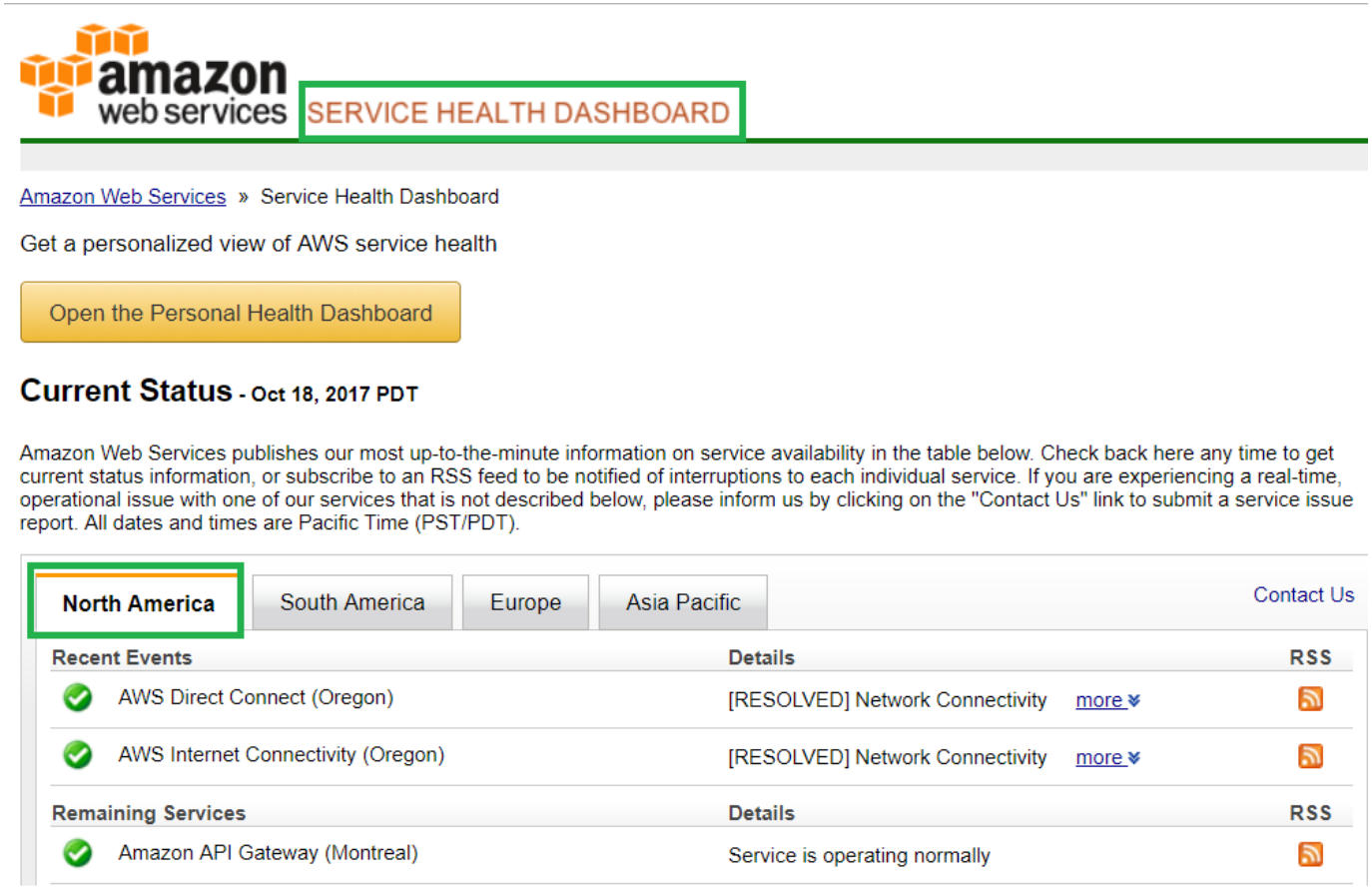
REMOTE CLASSROOM INSTRUCTION

1.6 - AWS shared security model - AWS responsibilities

1.7 - AWS regions and availability zones



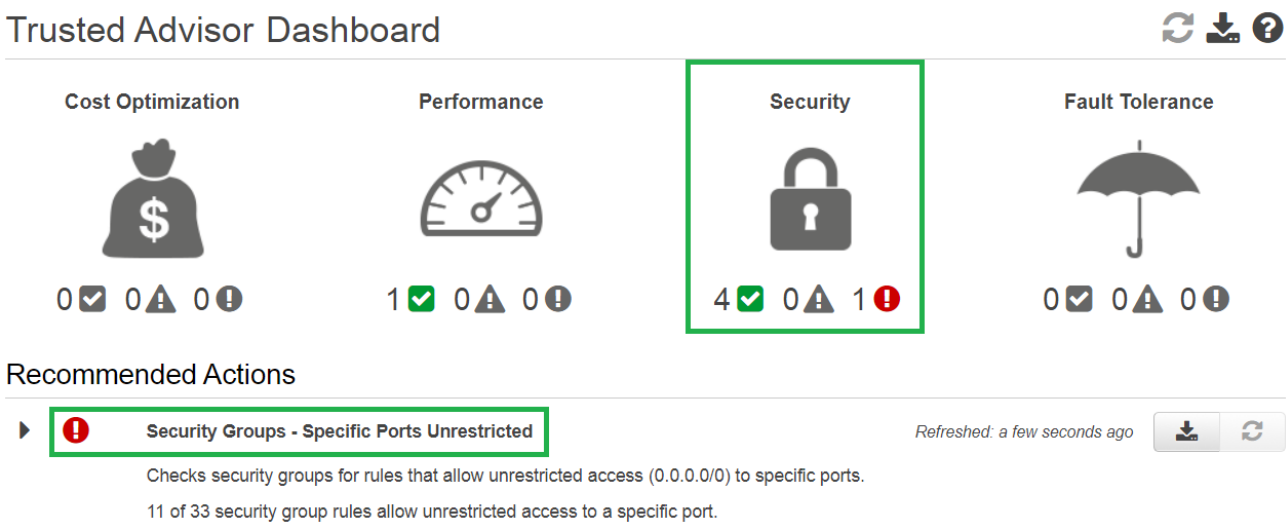
1.8 - AWS Service Health Dashboard



RCI
REMOTE CLASSROOM INSTRUCTION

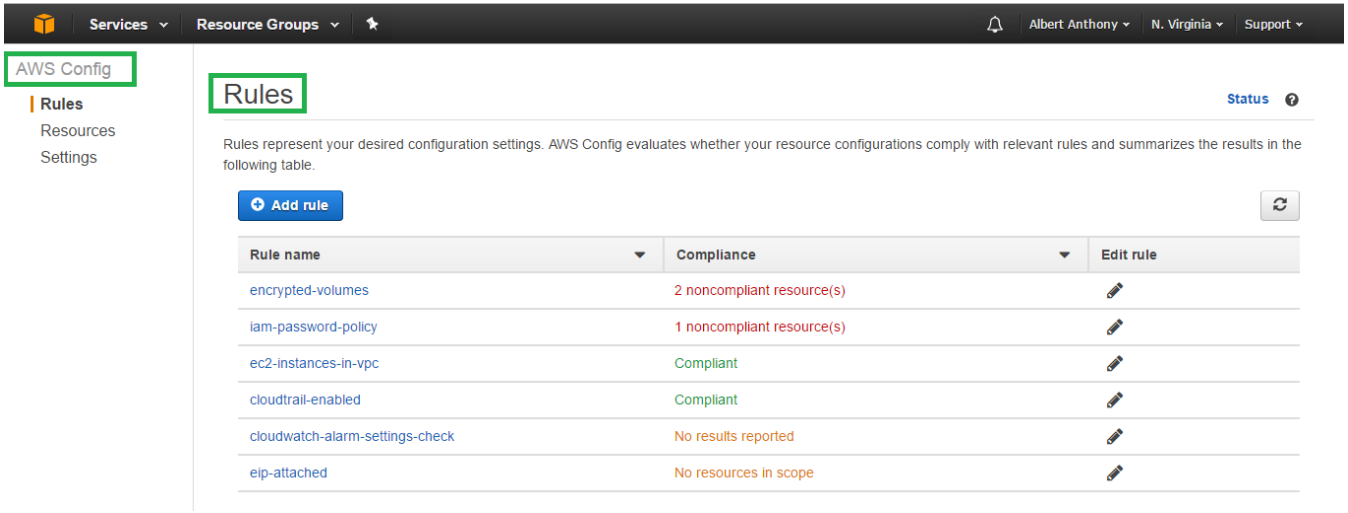
1.9 AWS shared security model - customer responsibilities

1.10 - AWS Trusted Advisor checks



REMOTE CLASSROOM INSTRUCTION

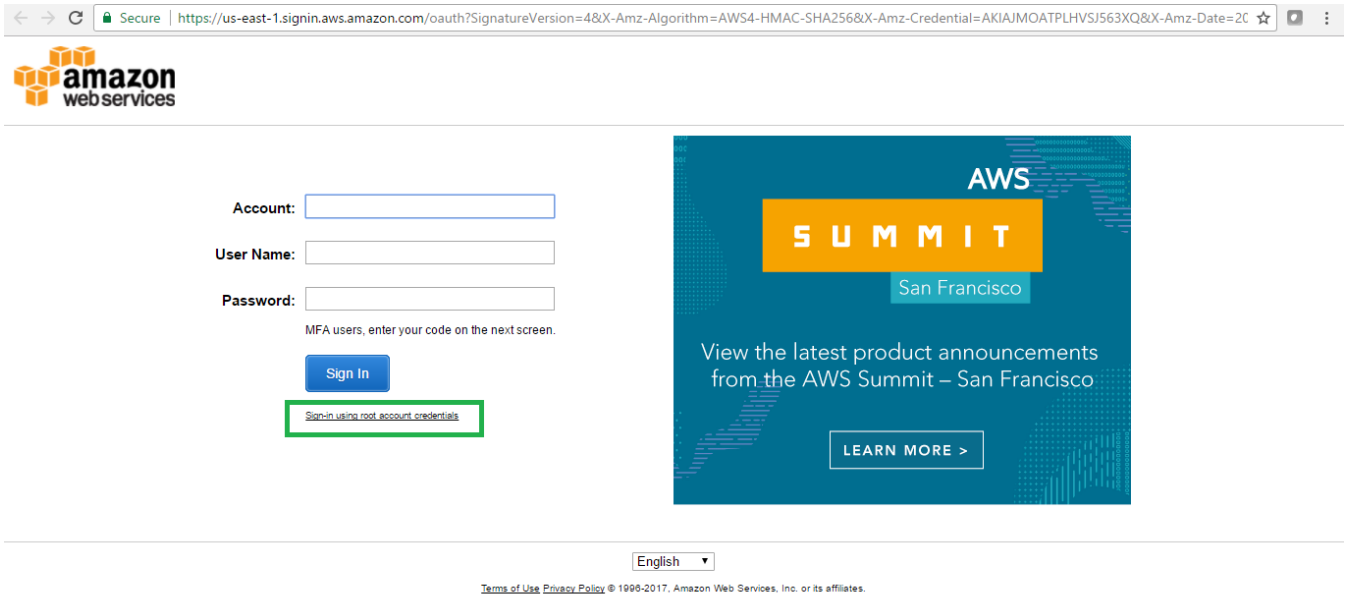
1.11 - AWS Config Rules



AWS Security Essentials - 2

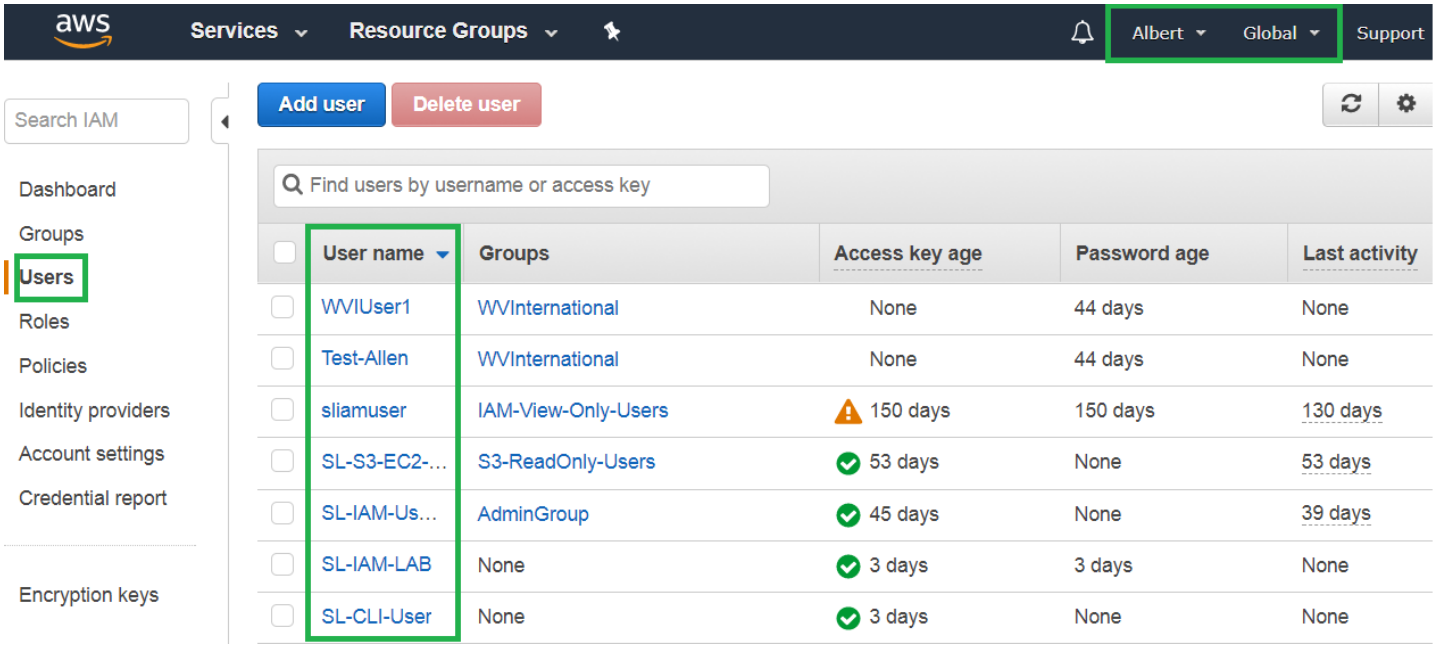
onlc
Training Centers

2.1 - AWS console login



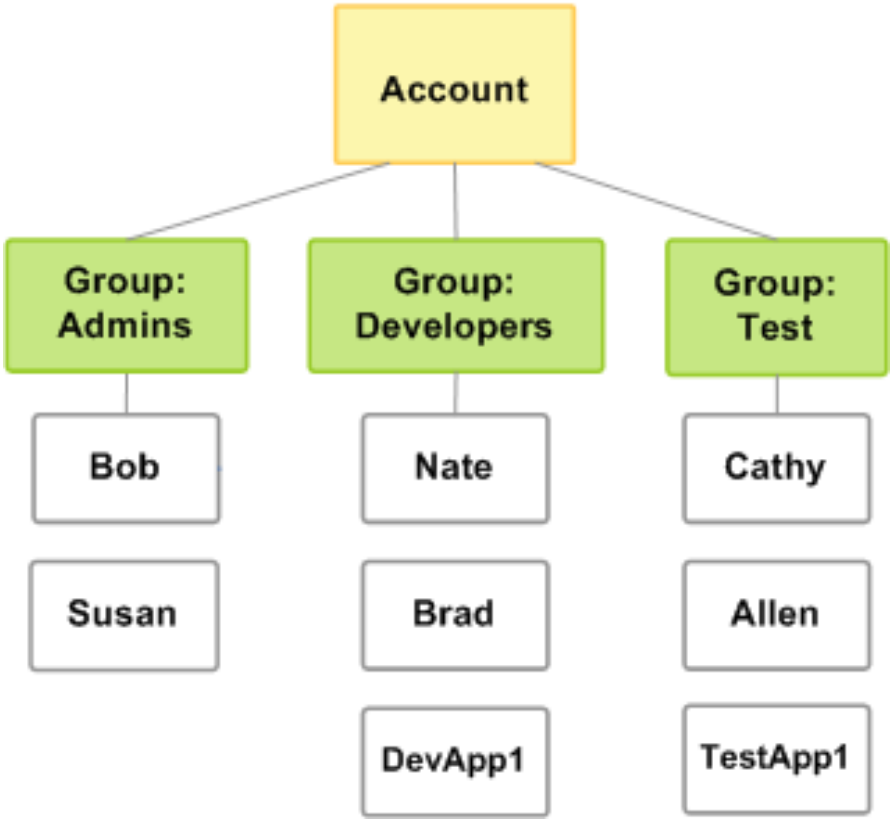
REMOTE CLASSROOM INSTRUCTION

2.2 - AWS IAM users

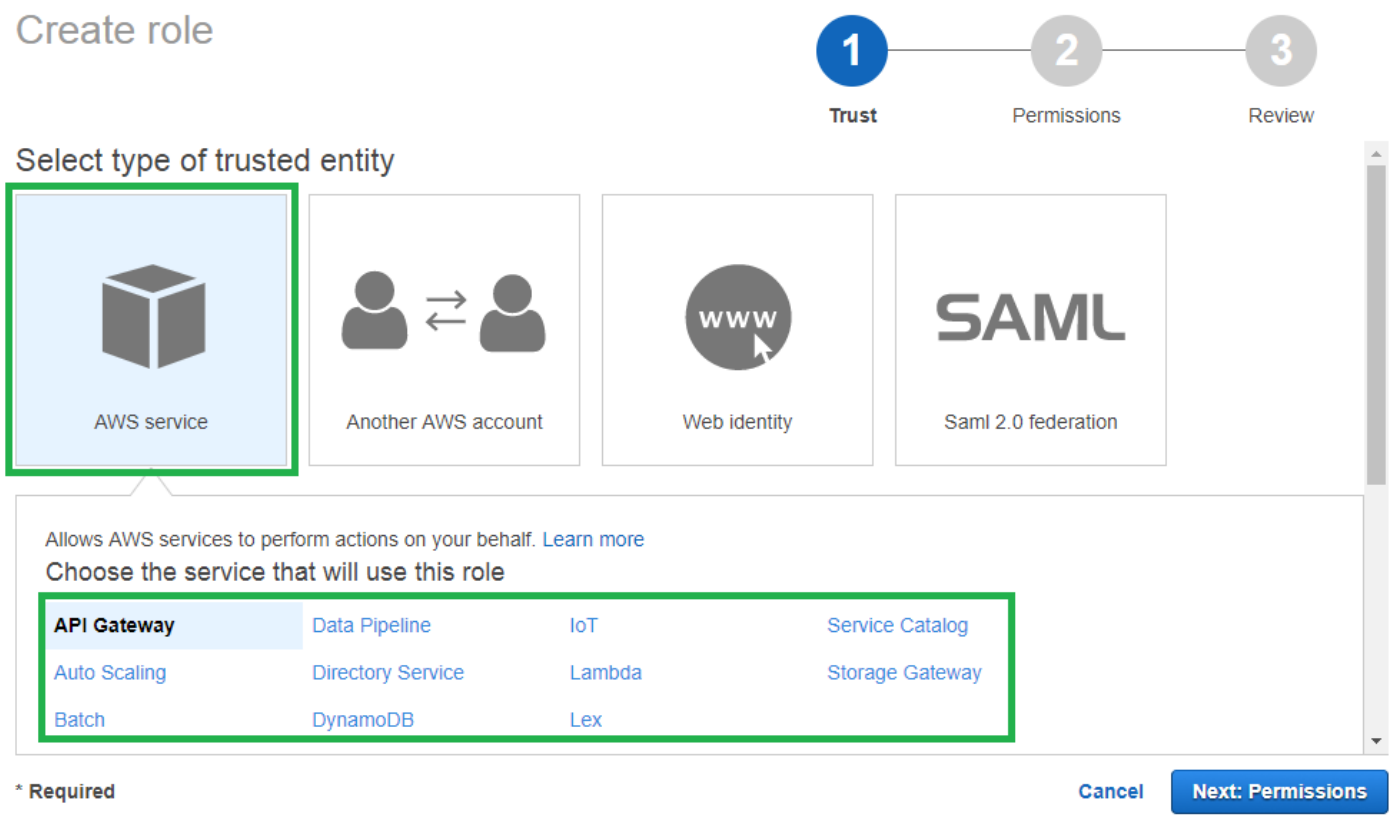


REMOTE CLASSROOM INSTRUCTION

2.3 - AWS IAM groups

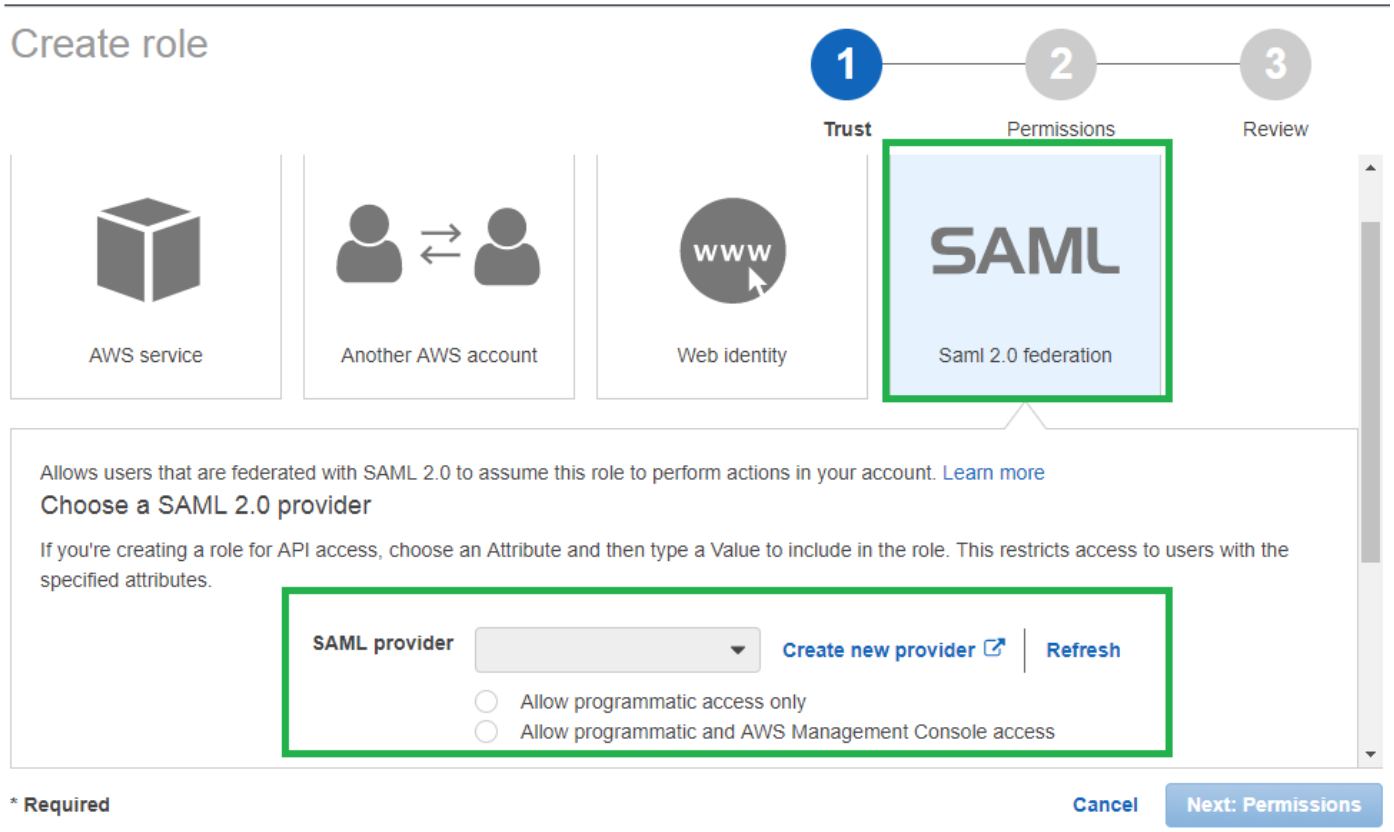


2.4 - AWS Service Role types



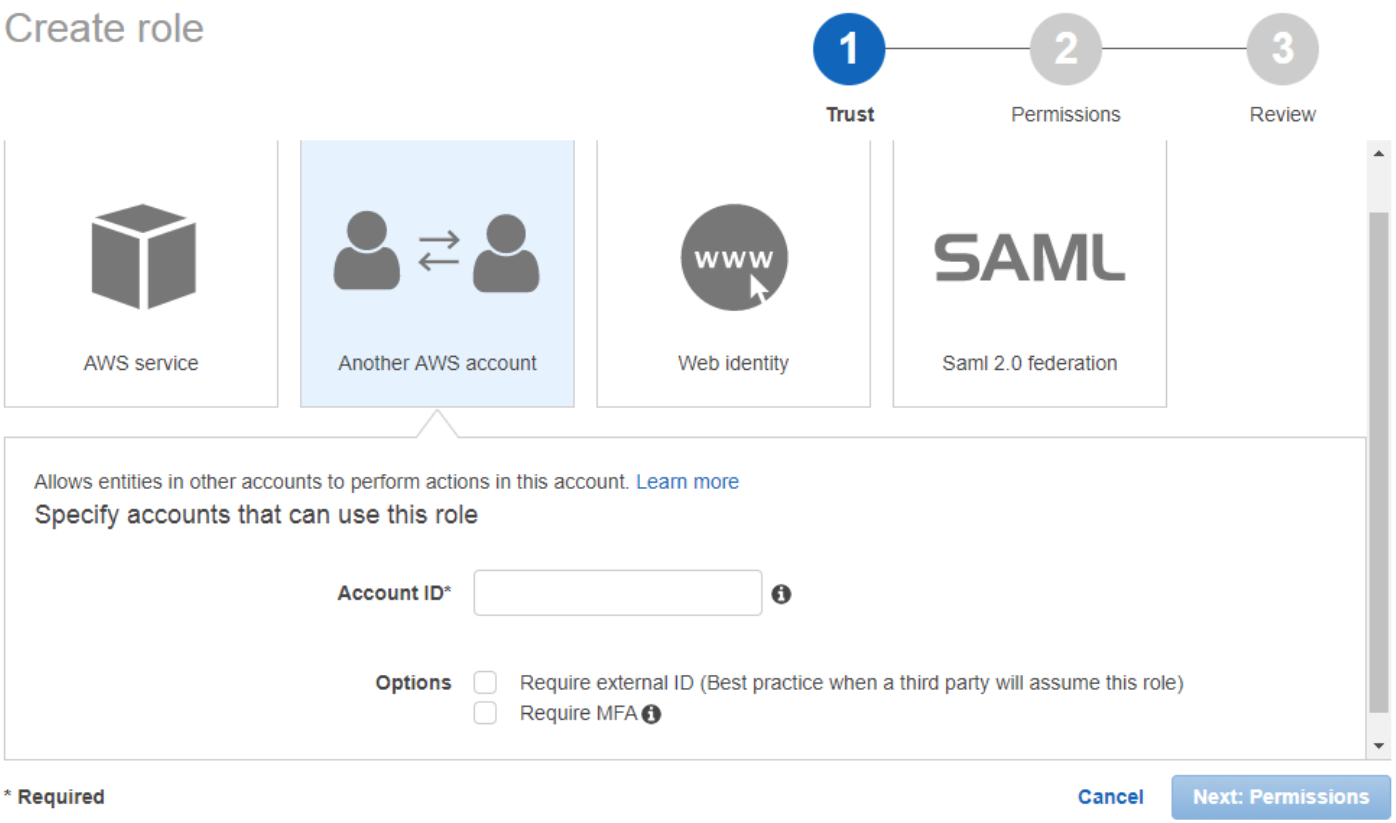
REMOTE CLASSROOM INSTRUCTION

2.5 - AWS SAML Role



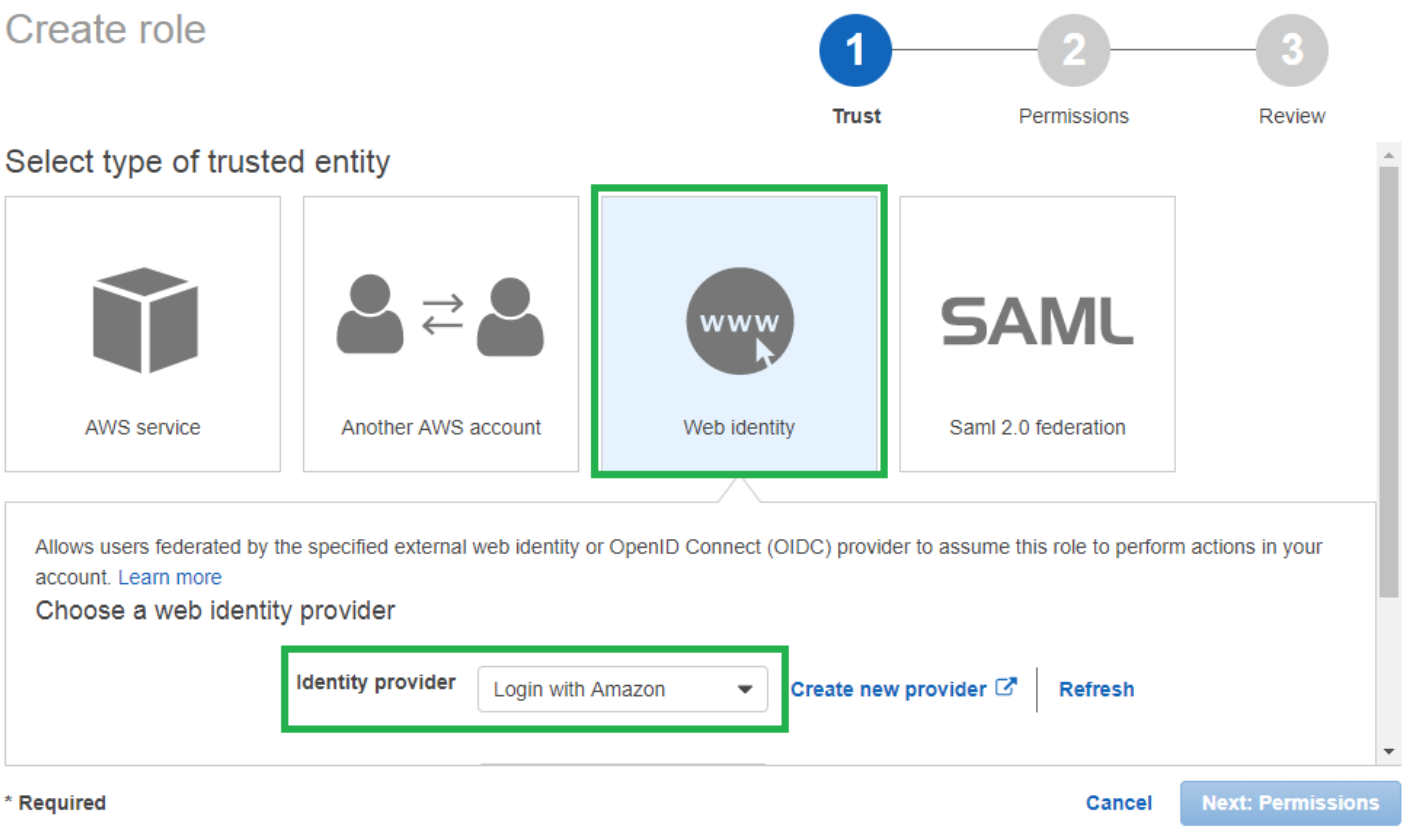
REMOTE CLASSROOM INSTRUCTION

2.6 - AWS cross-account access roles



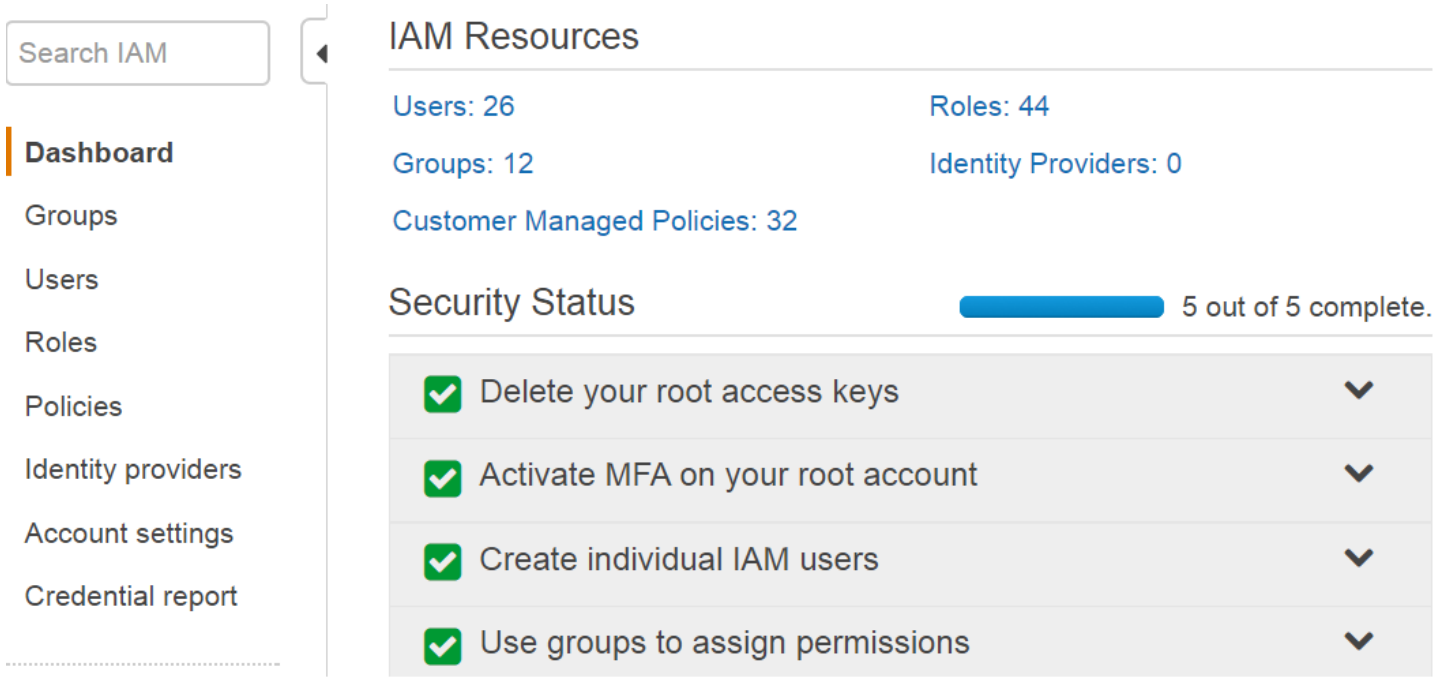
REMOTE CLASSROOM INSTRUCTION

2.7 - AWS identity provider access roles



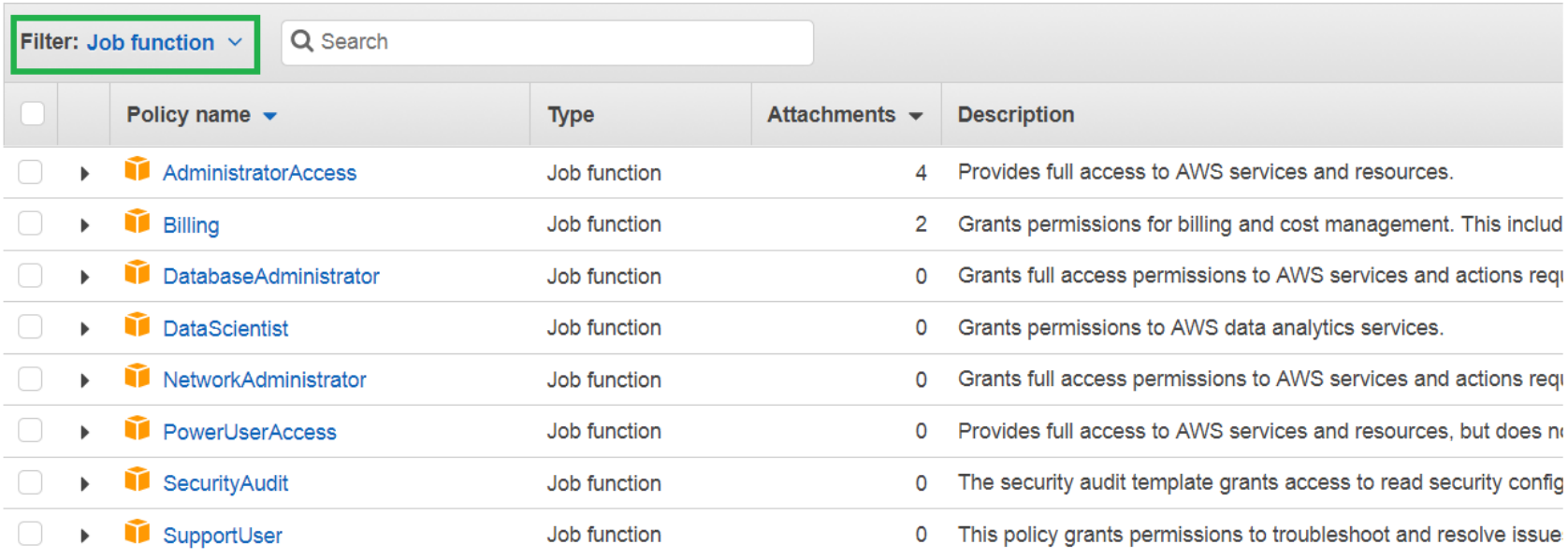
REMOTE CLASSROOM INSTRUCTION

2.8 - AWS account root user recommendations

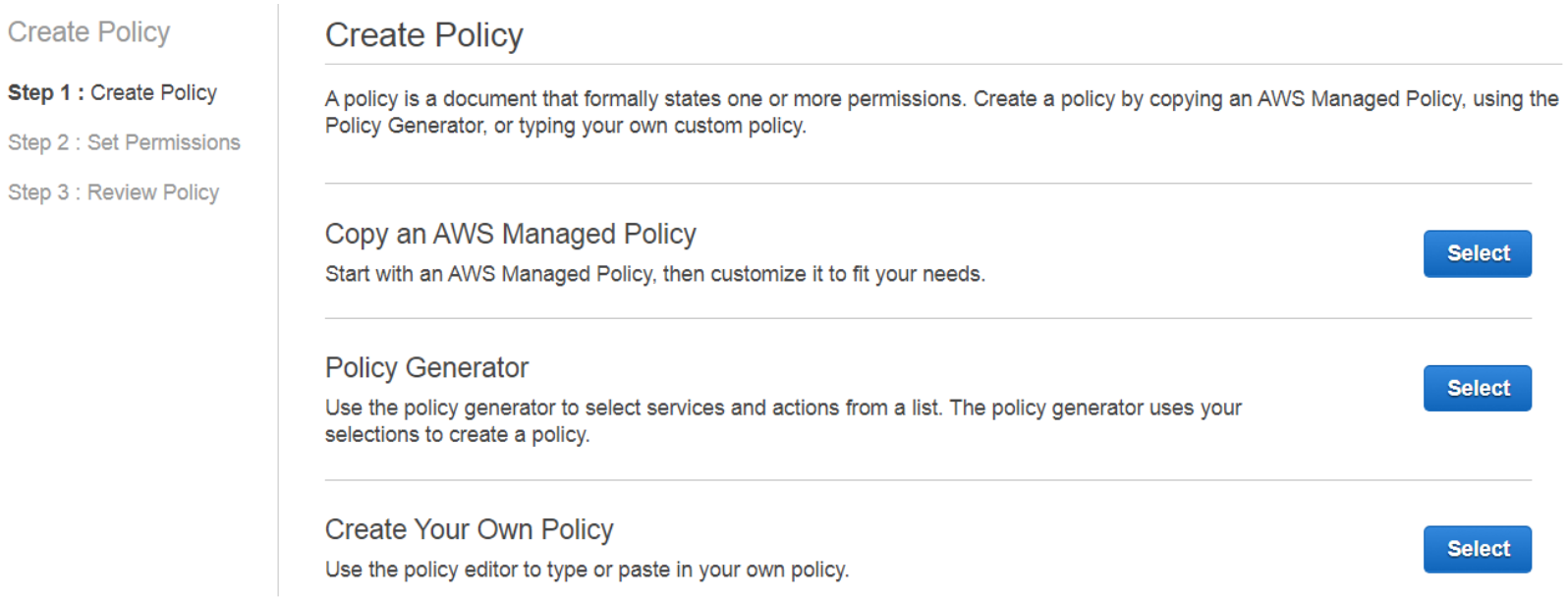


REMOTE CLASSROOM INSTRUCTION

2.9 - AWS job functions policies

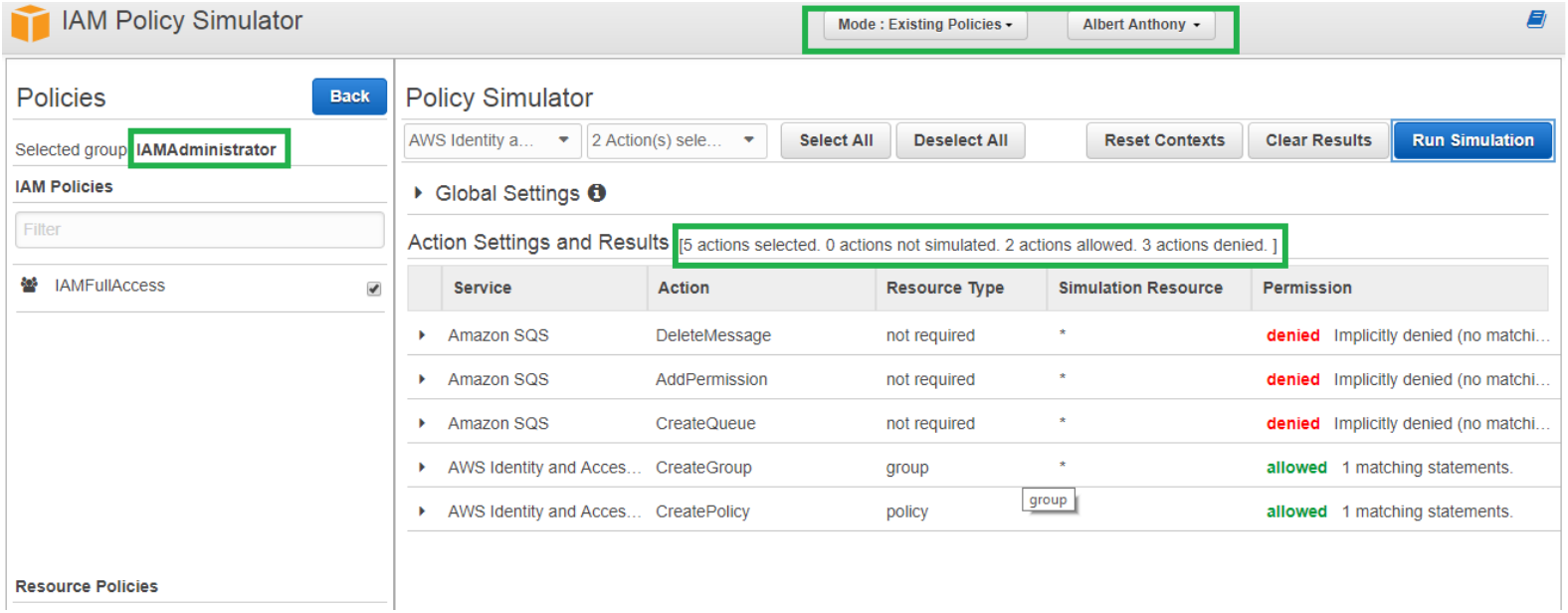


2.10 - AWS Create Policy options



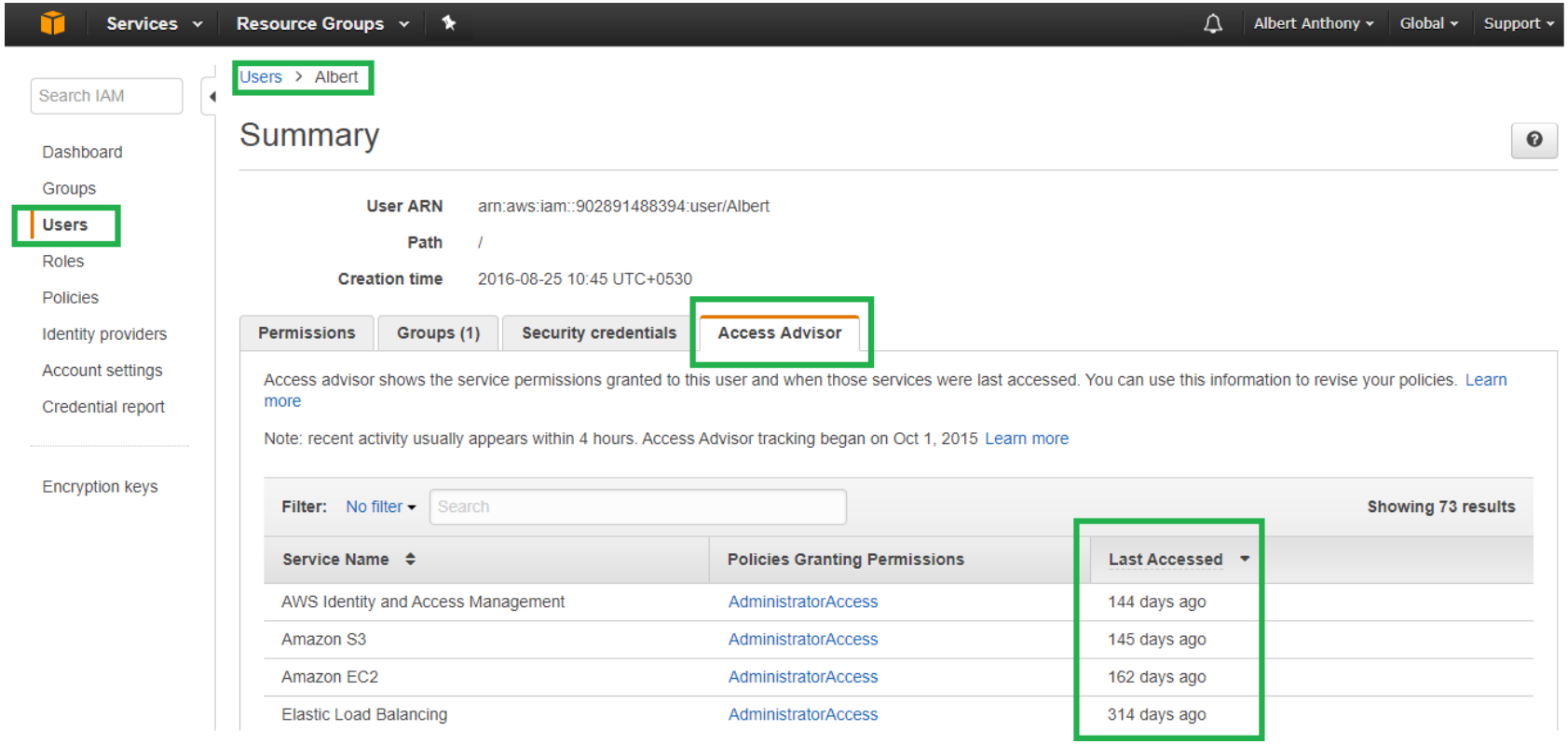
REMOTE CLASSROOM INSTRUCTION

2.11 - AWS IAM Policy Simulator

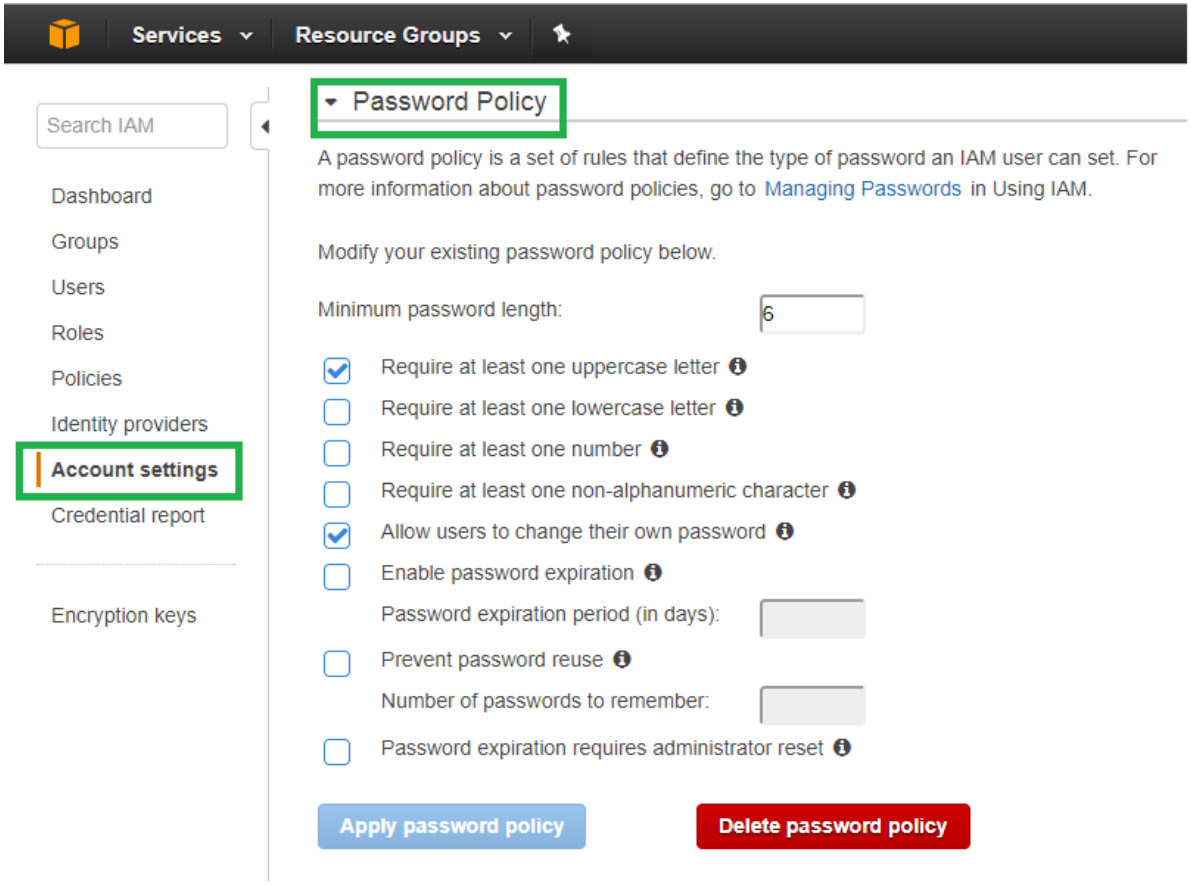


REMOTE CLASSROOM INSTRUCTION

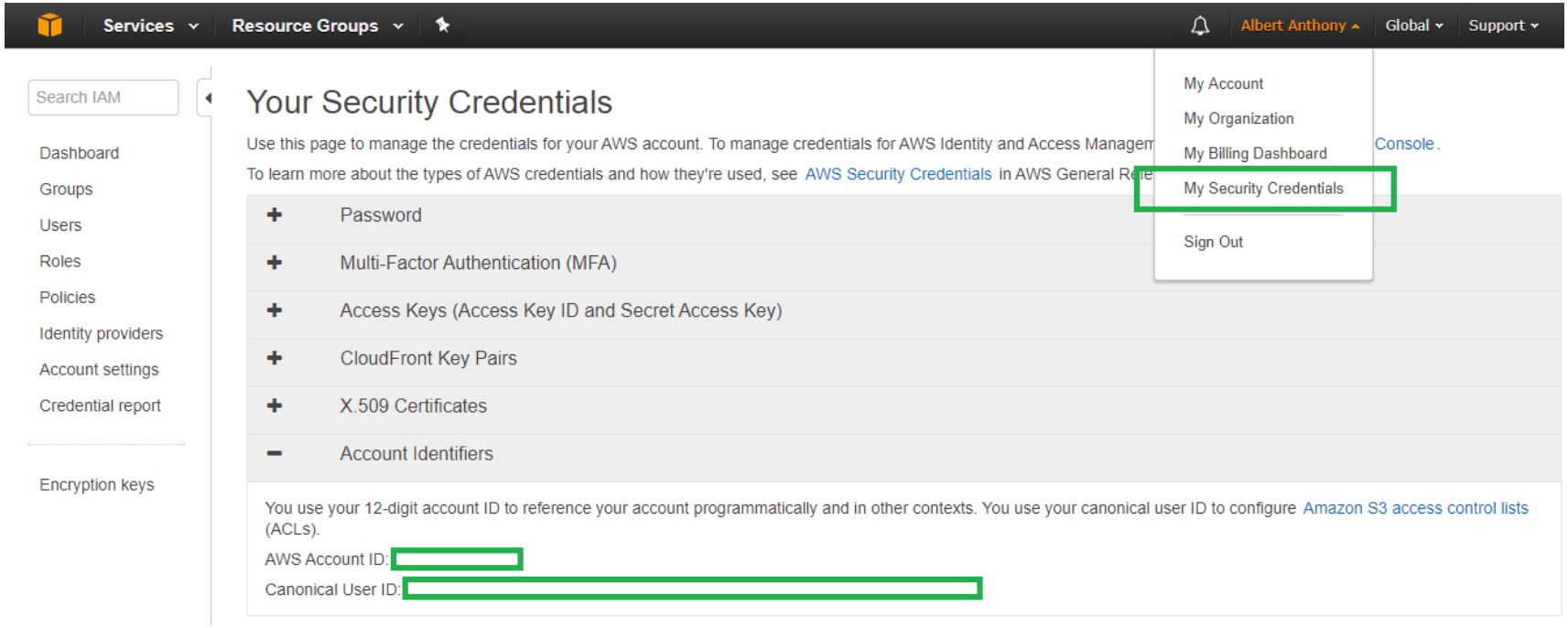
2.12 - AWS IAM Access Advisor



2.13 - AWS IAM Password Policy

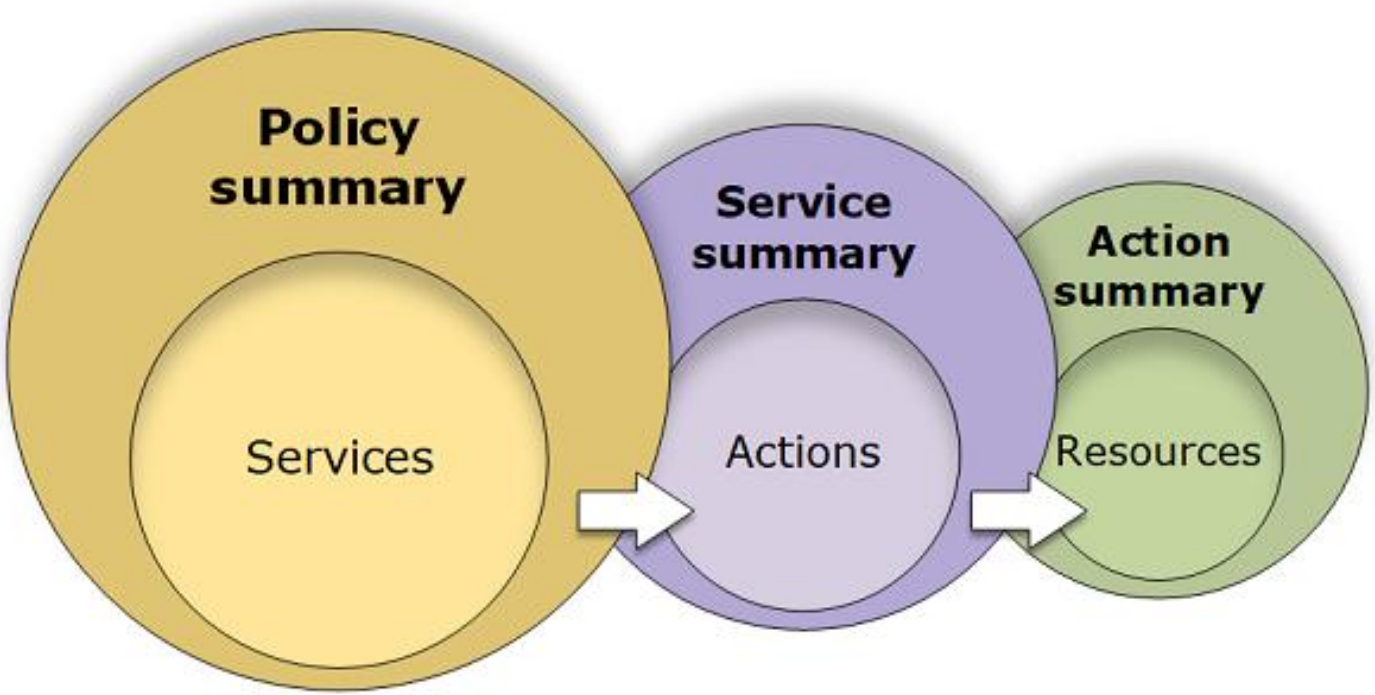


2.14 - AWS Security Credentials



REMOTE CLASSROOM INSTRUCTION

2.15 - AWS IAM policy summaries



AWS Security Essentials - Lab

- Login into AWS Dashboard
- Review the Dashboard
- Setup IAM Administrator Account
- Setup IAM Service Role for EC2 Admin
- Generate a Key Pair
- Create a Security Group (Port 809 and 3389)
- Launch an EC2 Instance
- RDP to Windows Server
- Install IIS
- Test Web and Application Server
- Generate a Snapshot

AWS Security Essentials – End Day 1

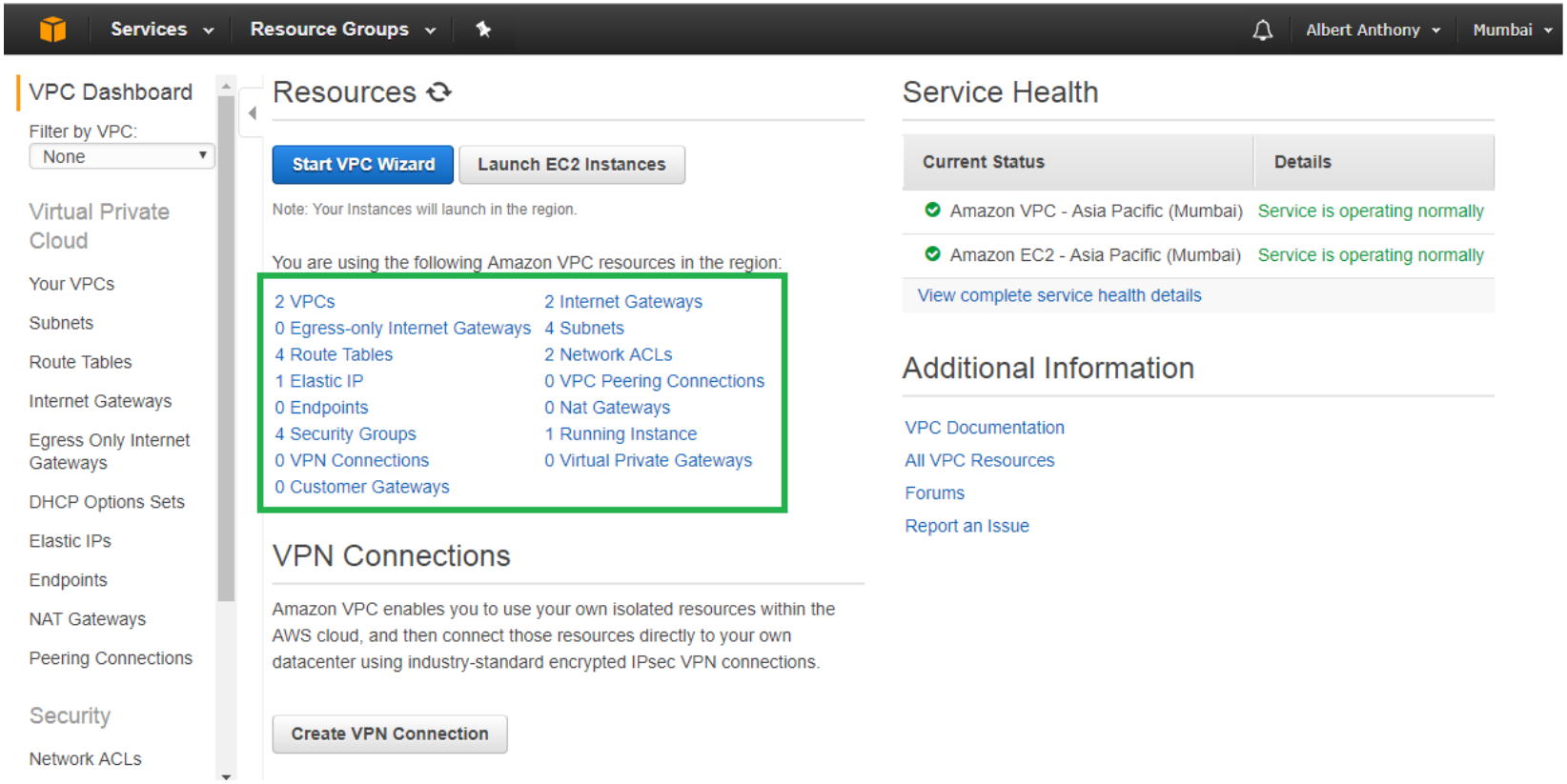
- **Day 2**
- **Chapter 3**
- **Chapter 4**
- **Chapter 5**

onlc
Training Centers

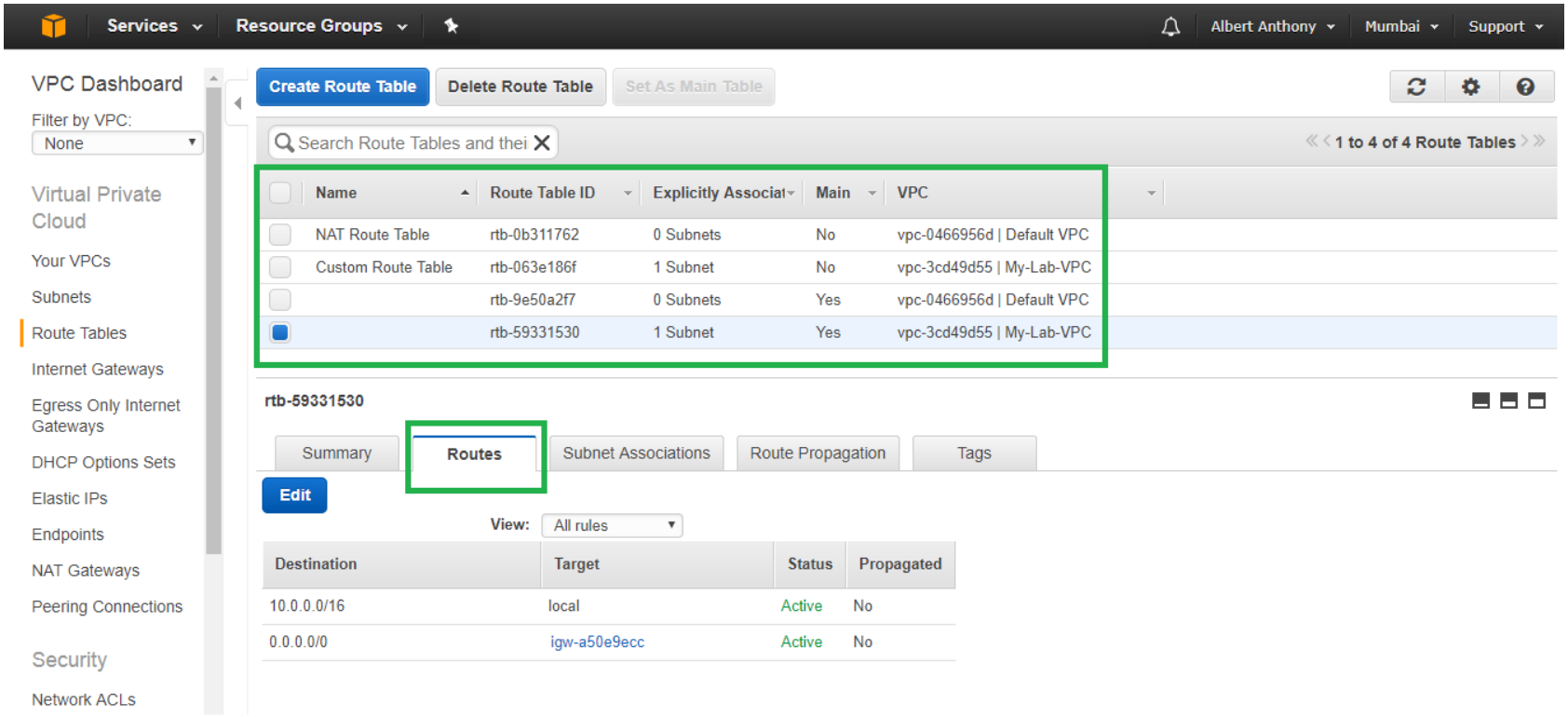
AWS Security Essentials - 3

onlc
Training Centers

3.Figure 1 - AWS VPC components

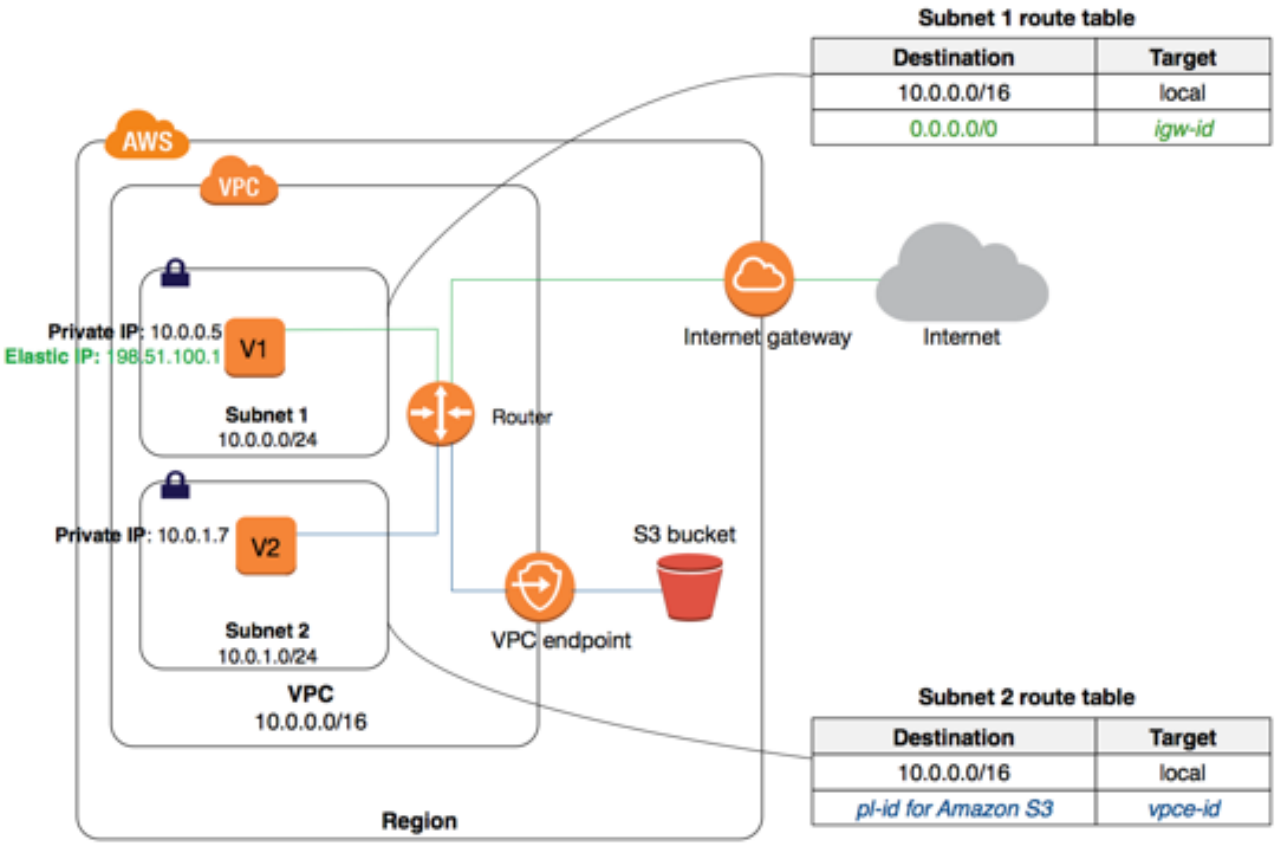


3.Figure 2 - AWS VPC route tables

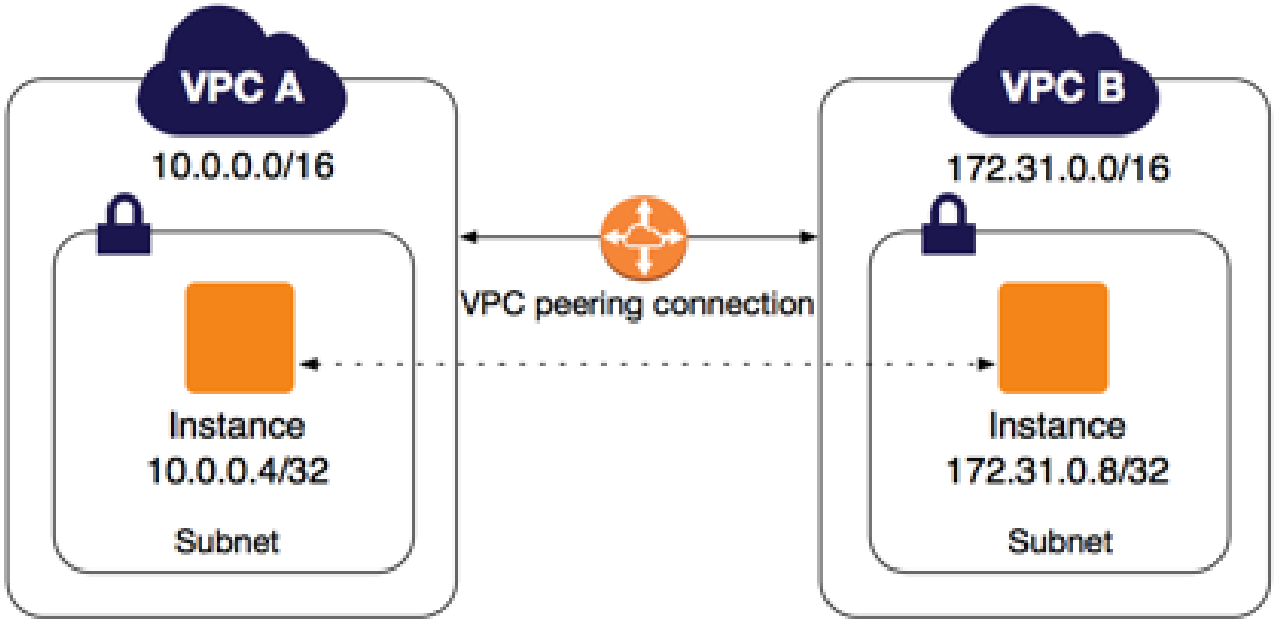


REMOTE CLASSROOM INSTRUCTION

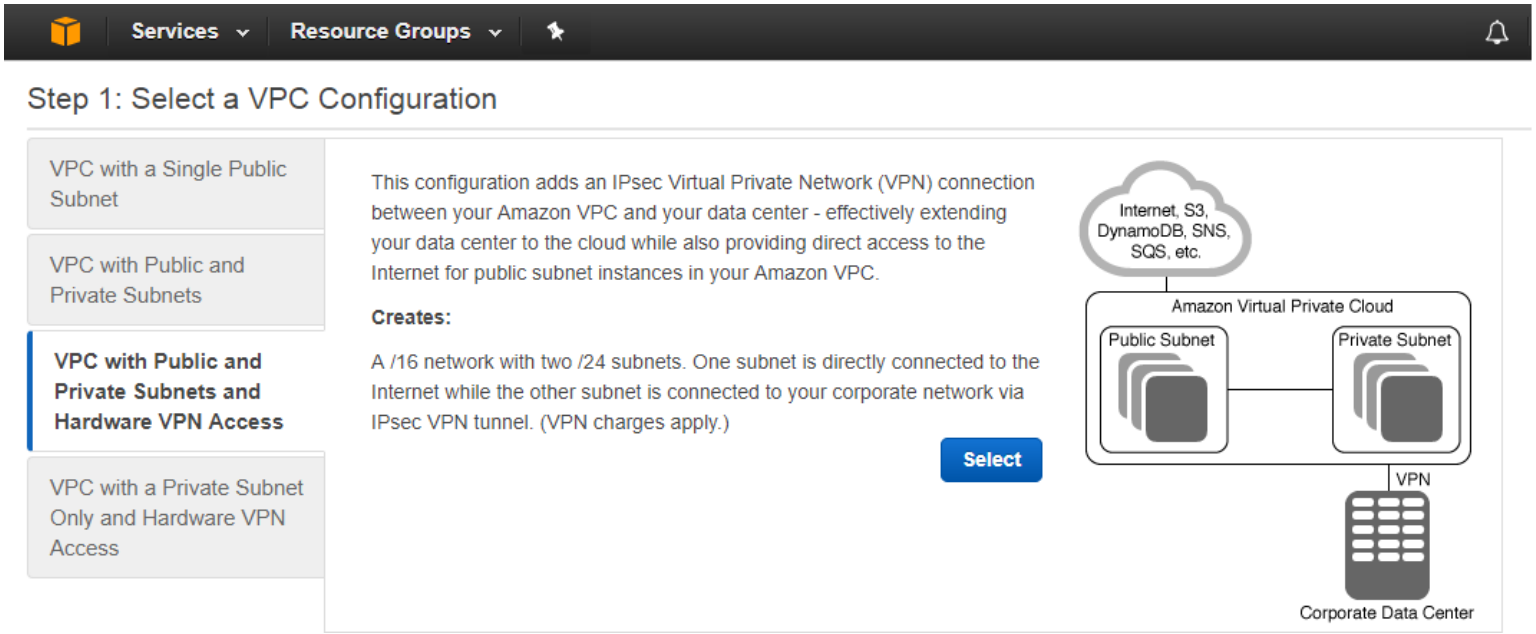
3.Figure 3 - AWS VPC endpoints



3.Figure 4 - AWS VPC peering

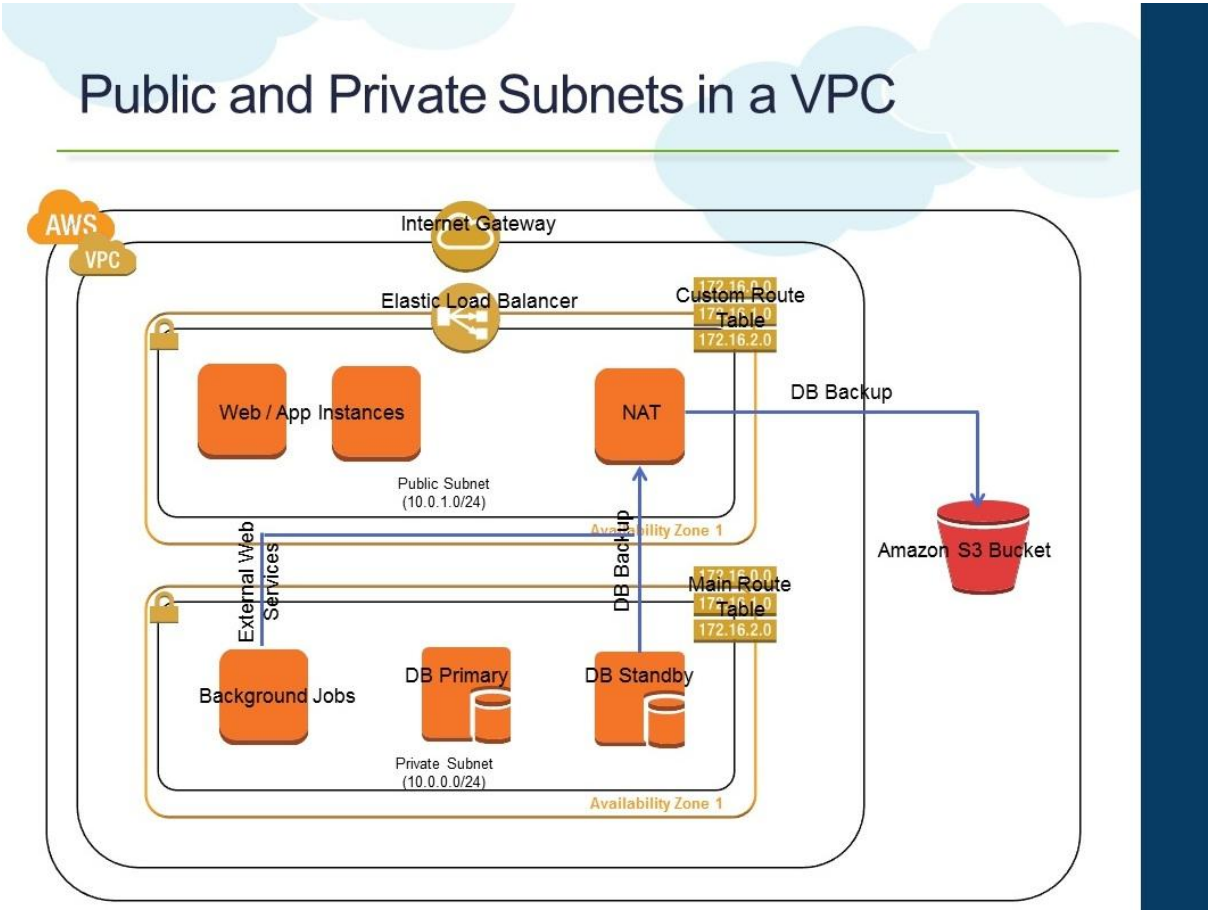


3.Figure 5 - AWS VPC wizard

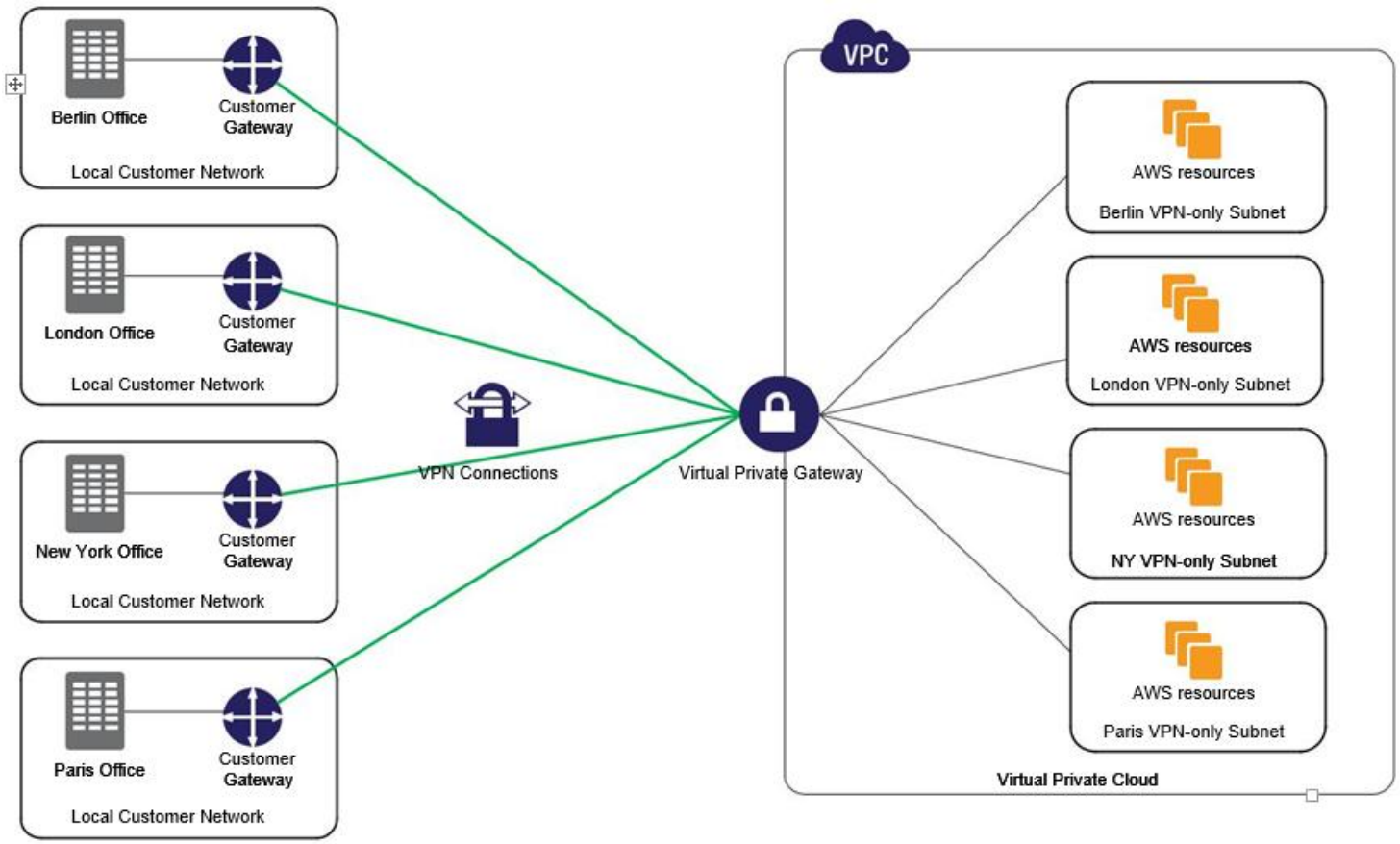


REMOTE CLASSROOM INSTRUCTION

3.Figure 6 - AWS VPC for a multi-tier web application

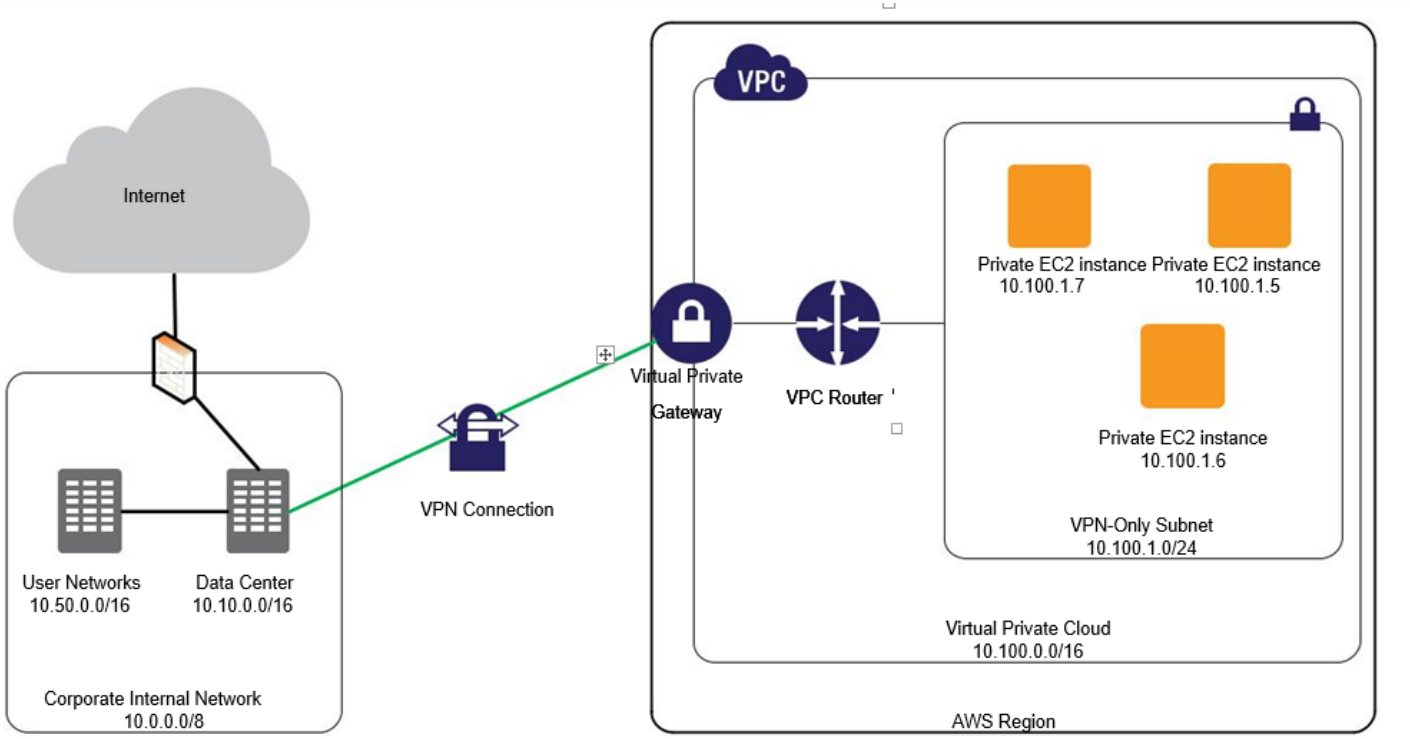


3.Figure 7 - AWS VPC for connecting branch offices



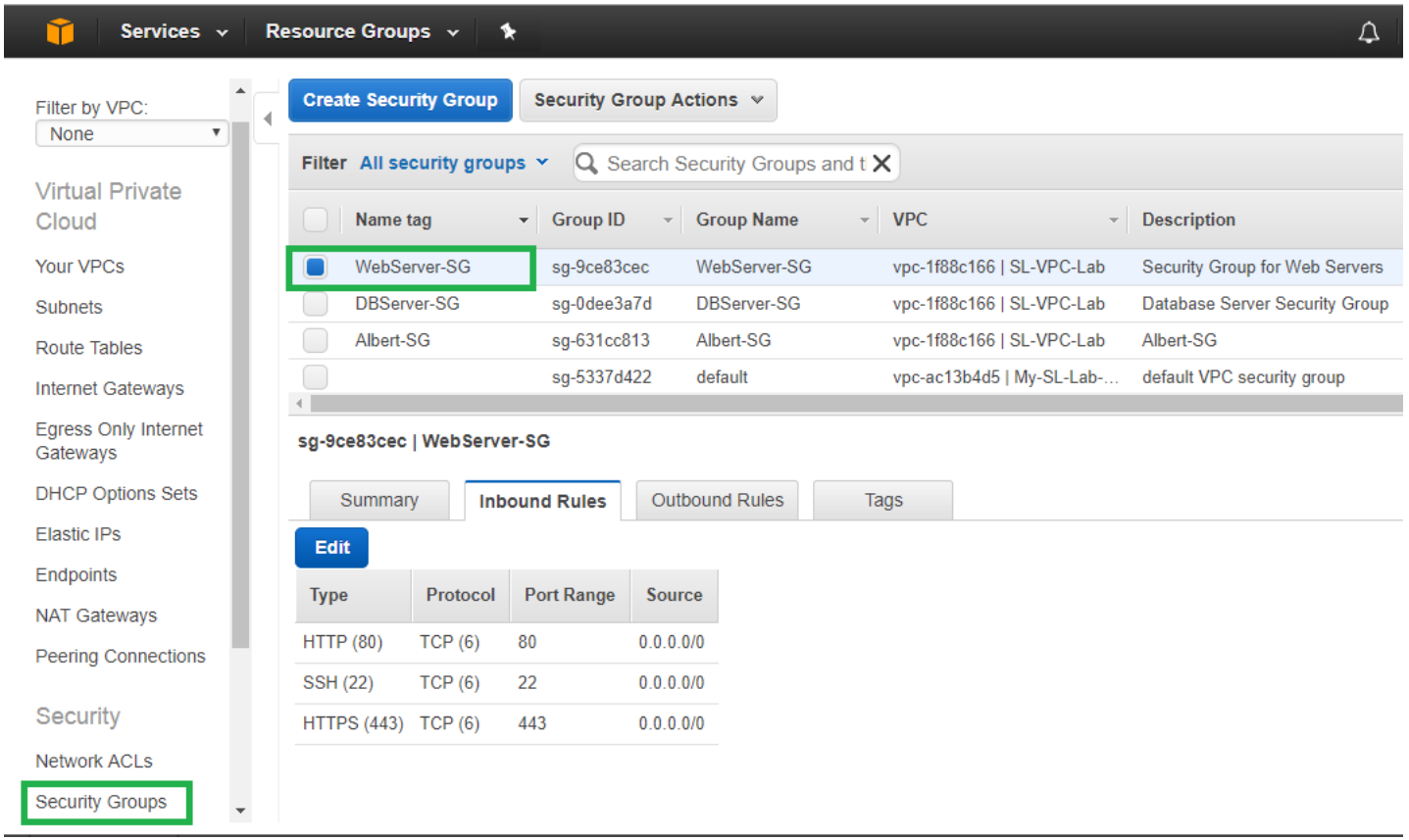
REMOTE CLASSROOM INSTRUCTION

3.Figure 8 - AWS VPC extend corporate data center

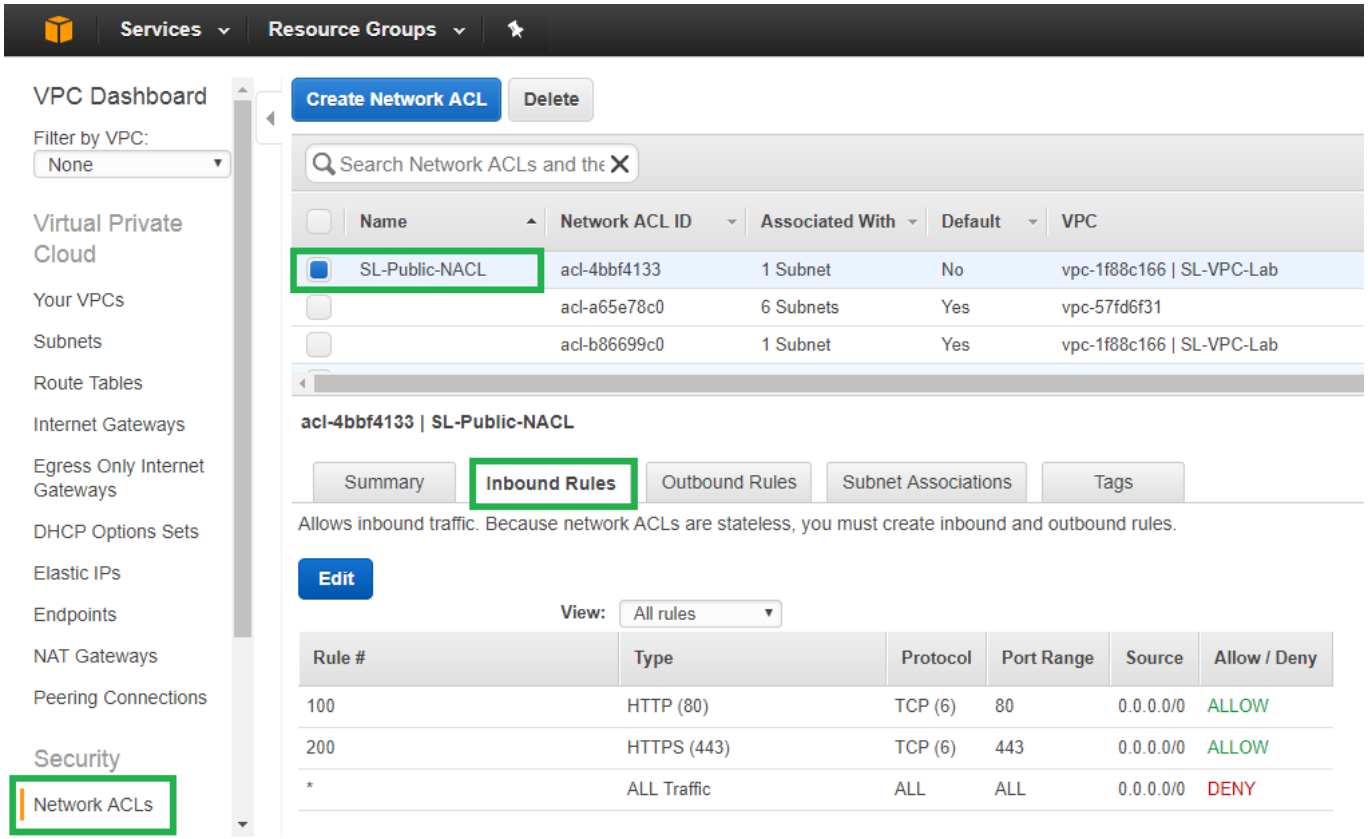


REMOTE CLASSROOM INSTRUCTION

3.Figure 9 - AWS VPC security groups

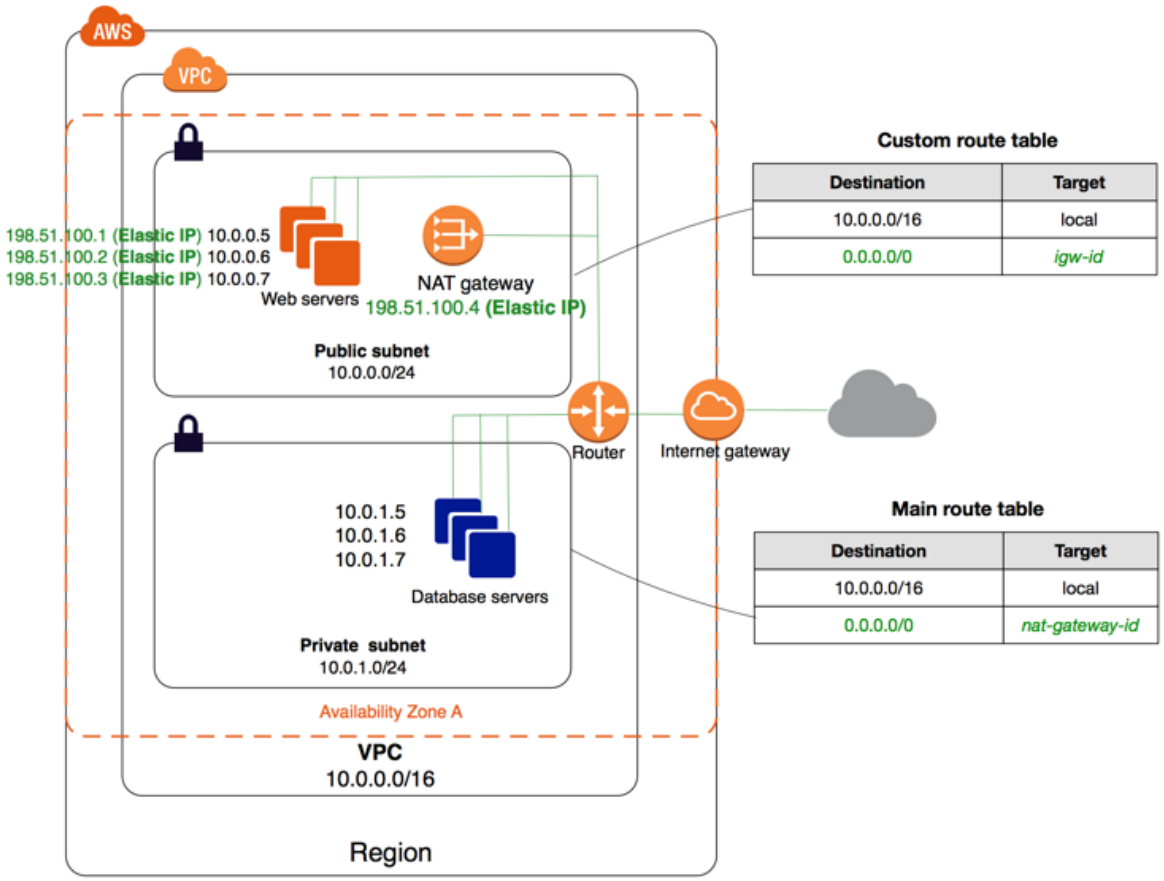


3.Figure 10 - AWS VPC NACL



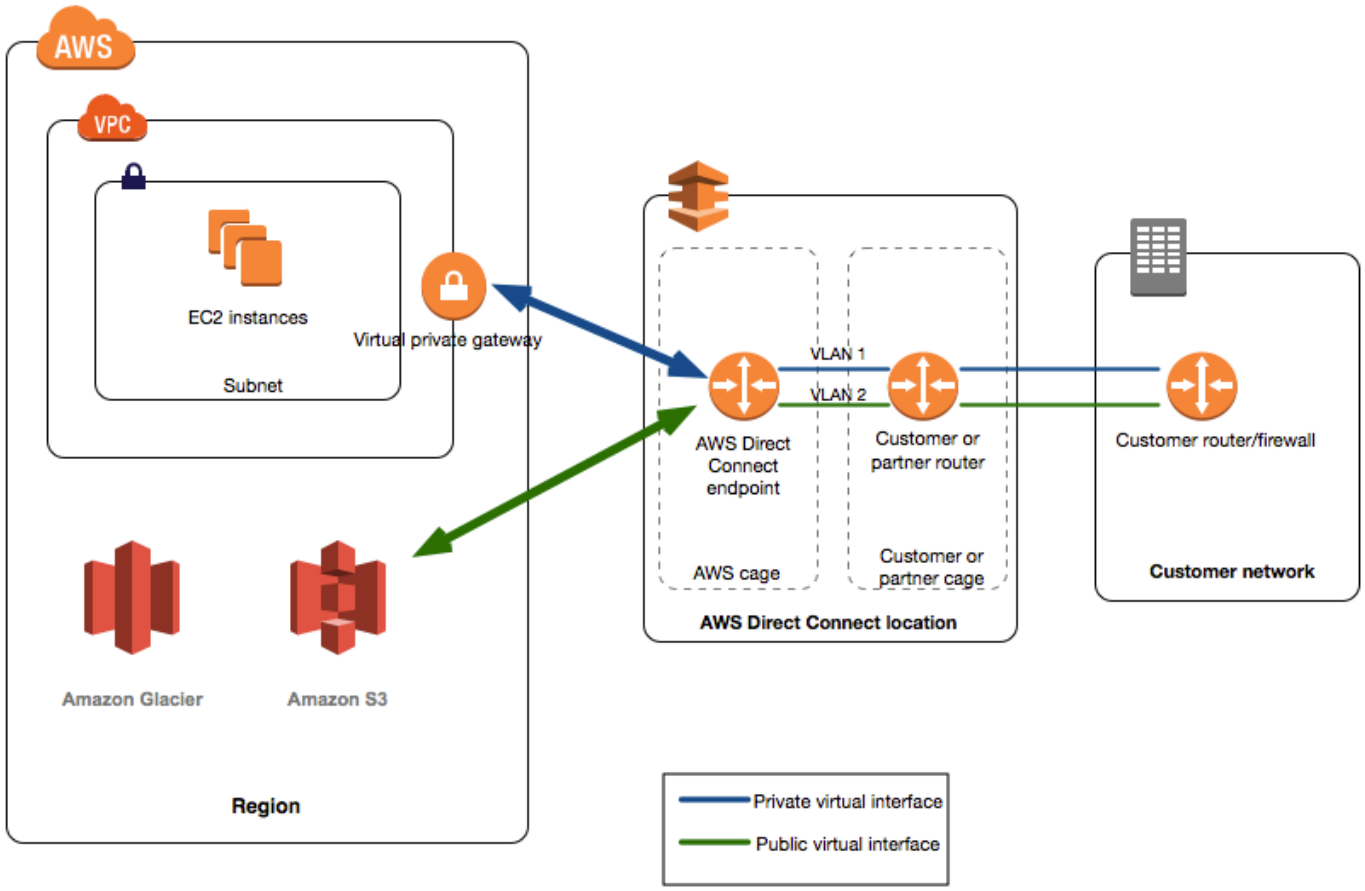
REMOTE CLASSROOM INSTRUCTION

3.Figure 11 - AWS custom VPC



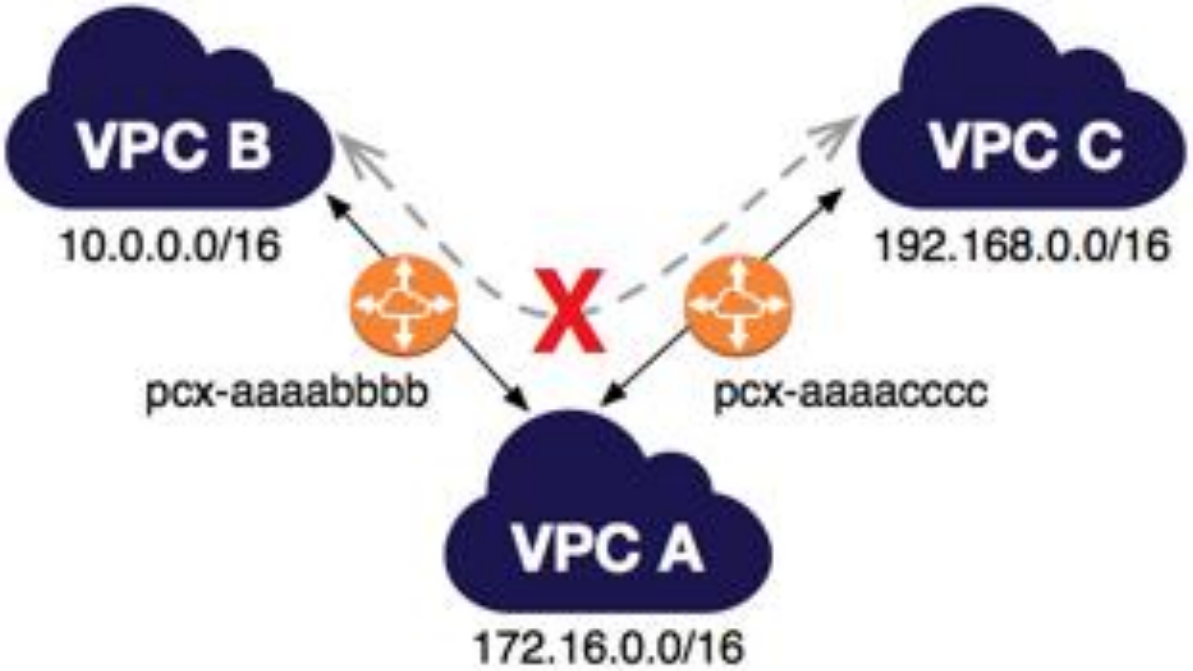
REMOTE CLASSROOM INSTRUCTION

3.Figure 12 - AWS direct connect



REMOTE CLASSROOM INSTRUCTION

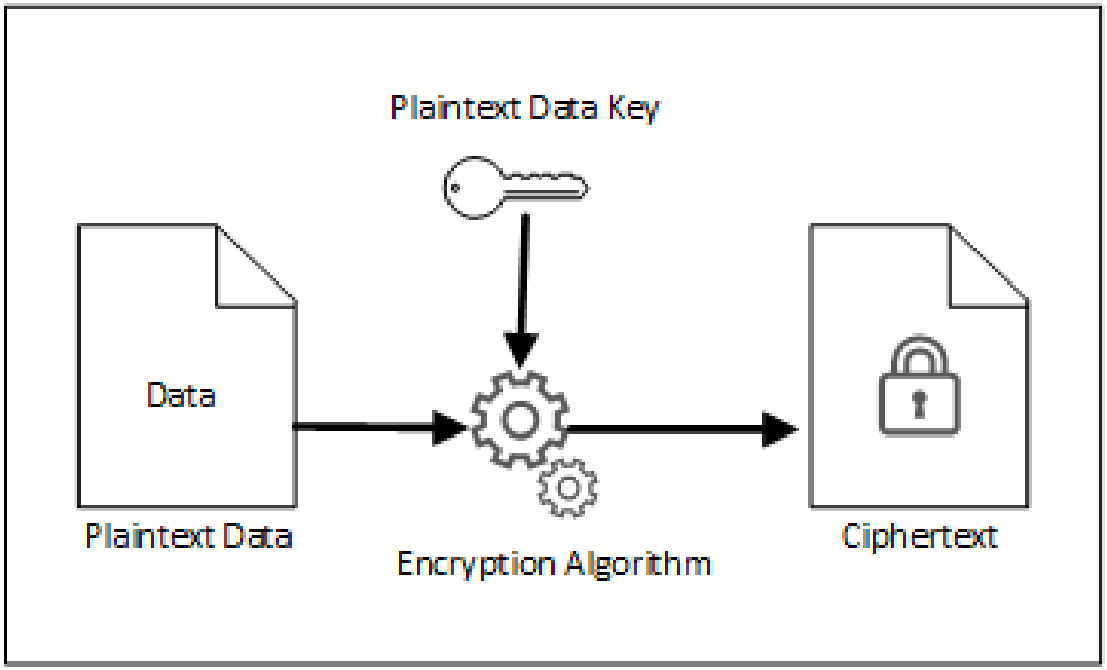
3.Figure 13 - AWS VPC Transitive Peering



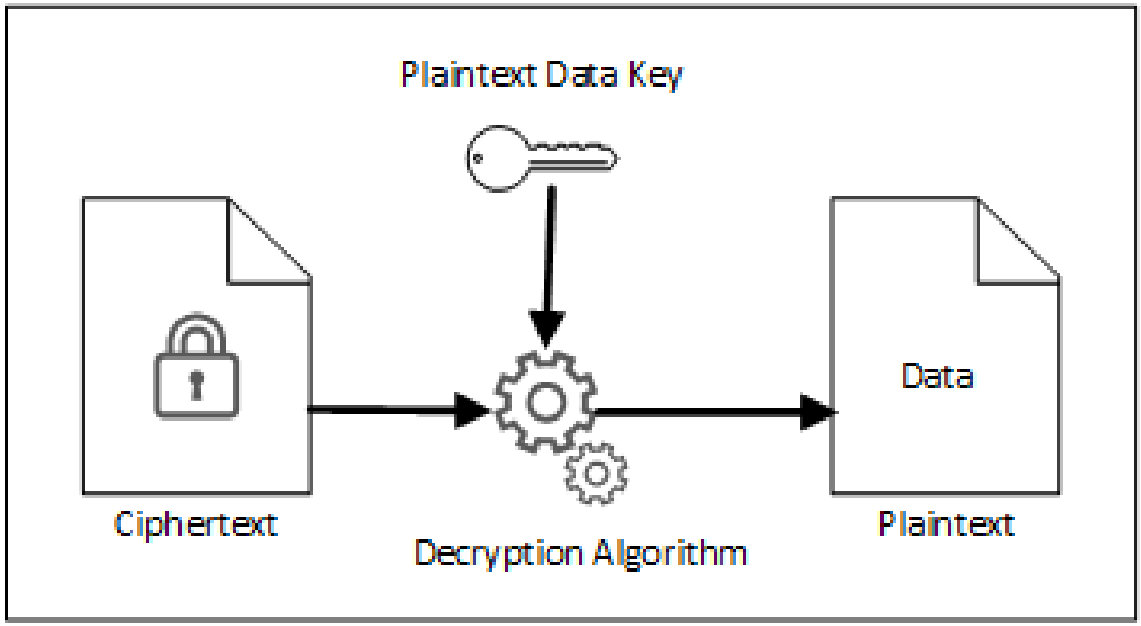
AWS Security Essentials - 4

onlc
Training Centers

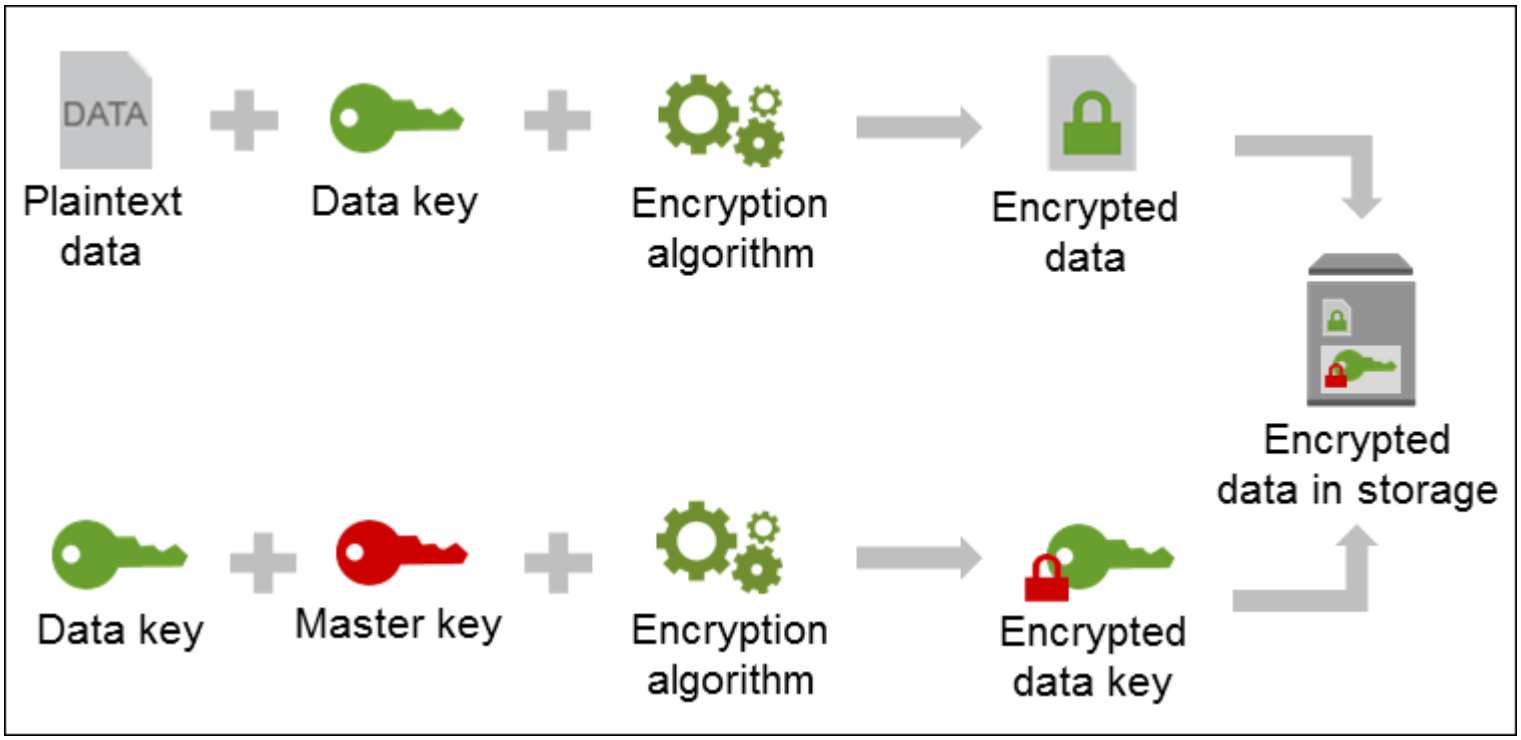
4.Figure 1 - AWS encryption workflow



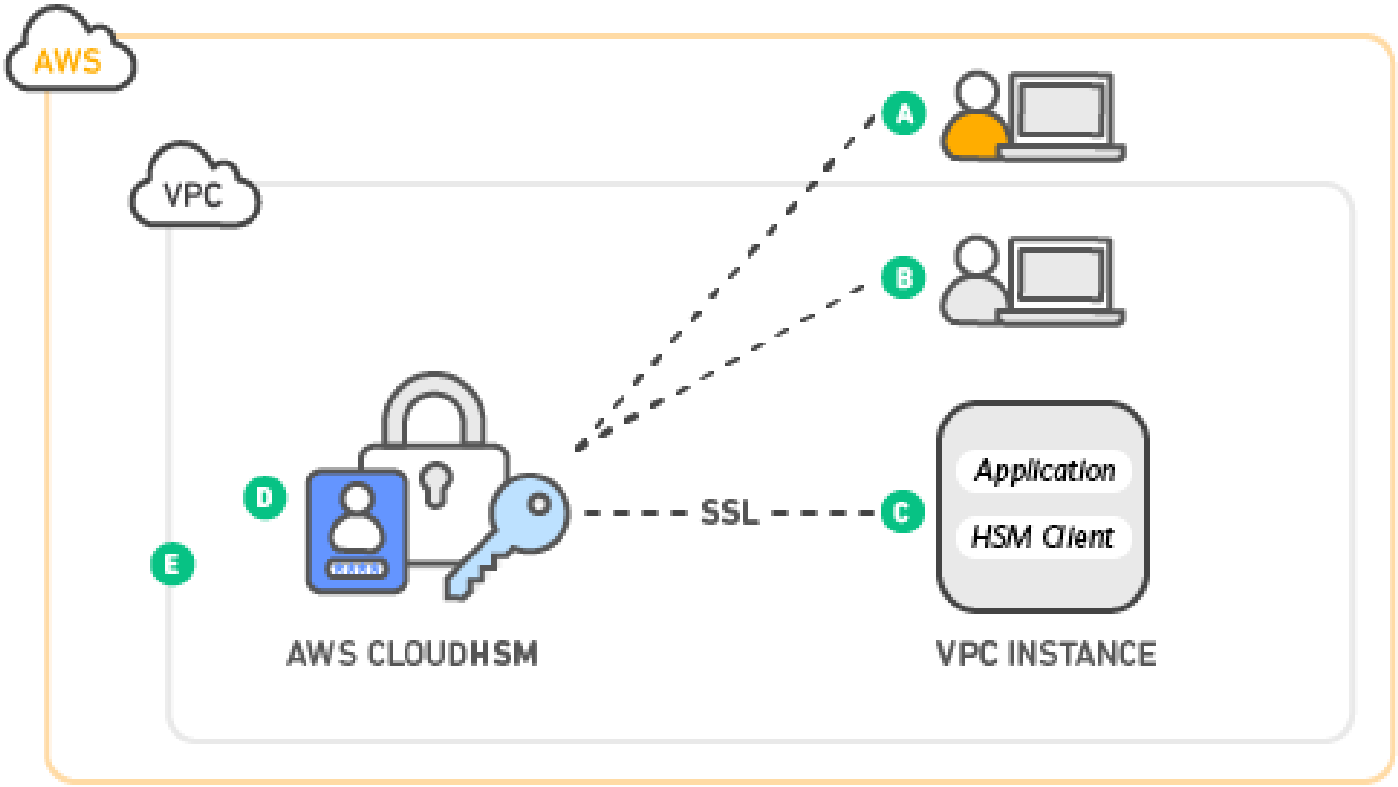
4.Figure 2 - AWS decryption workflow



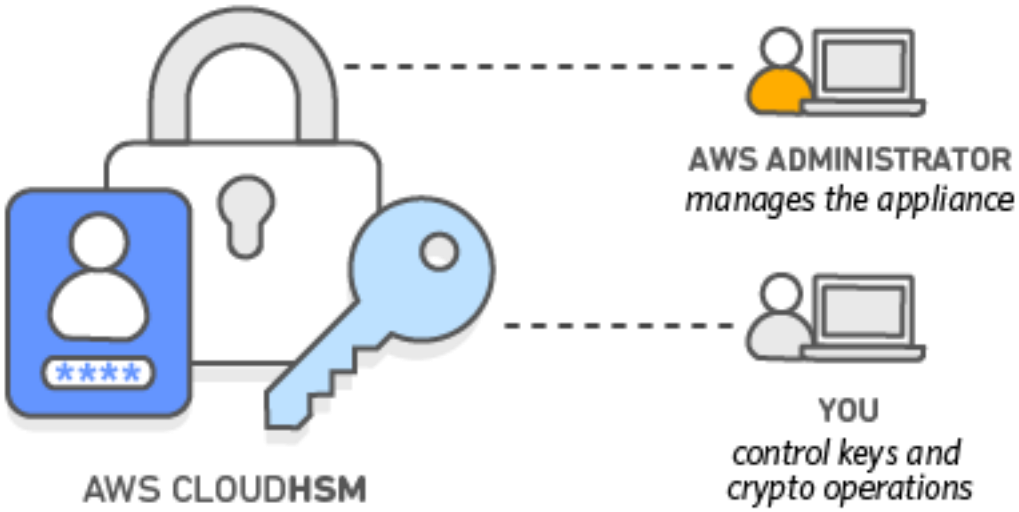
4.Figure 3 - AWS envelope encryption



4.Figure 4 - AWS CloudHSM



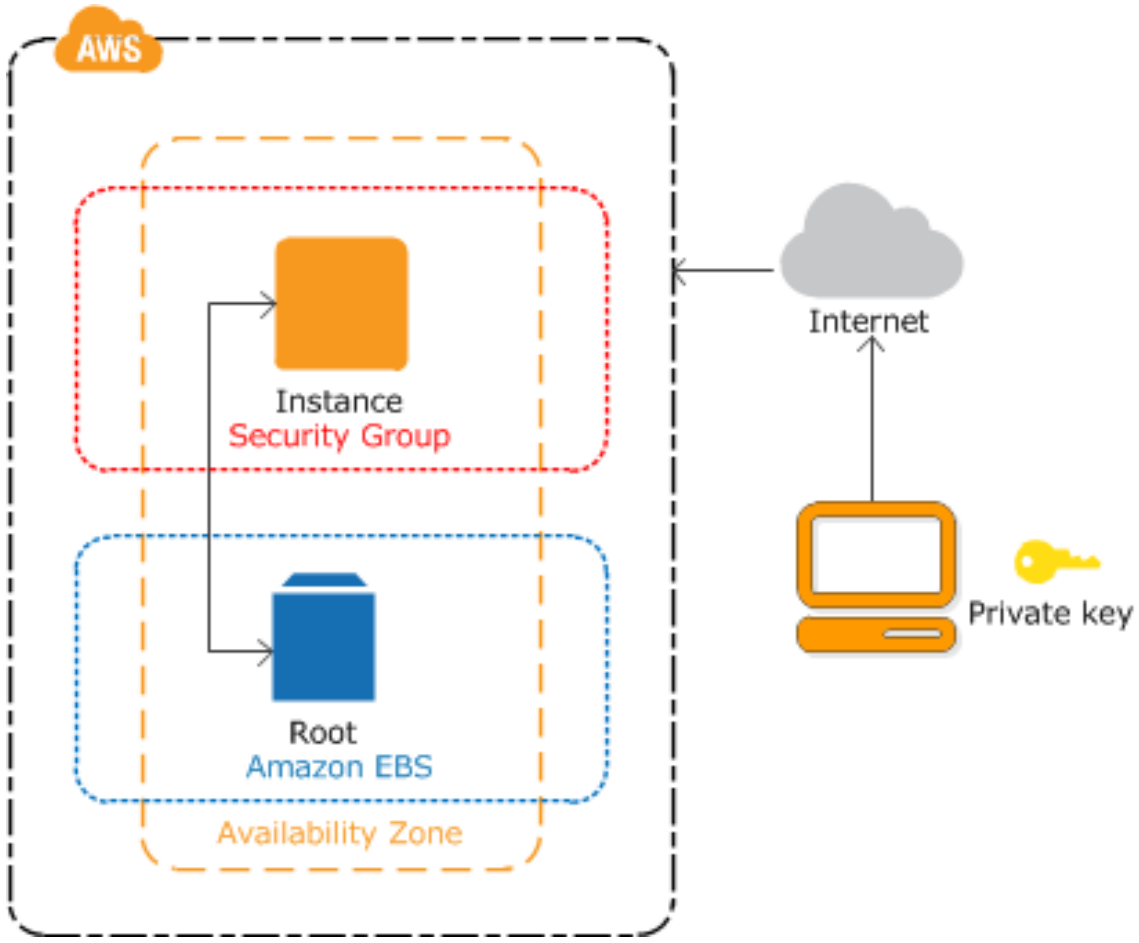
4.Figure 5 - AWS CloudHSM separation of duties



AWS Security Essentials - 5

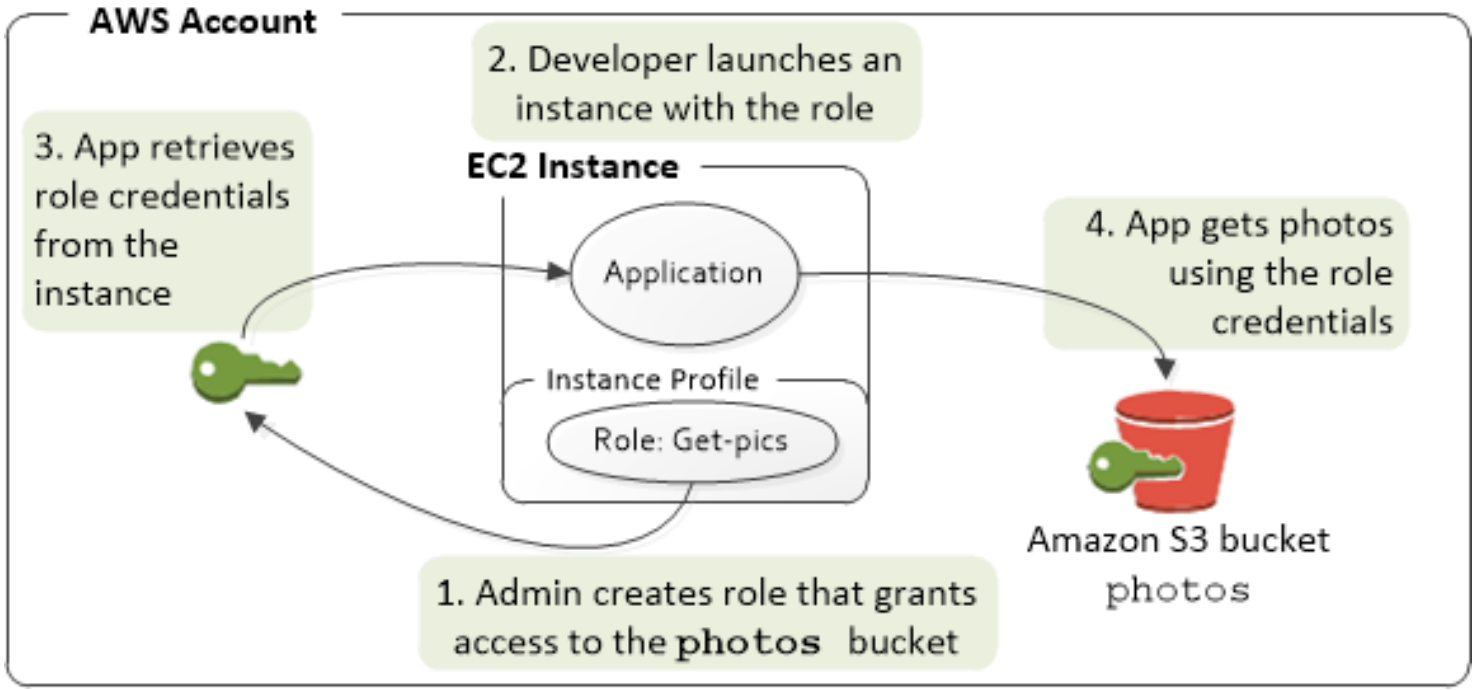
onlc
Training Centers

5.Figure 1 - AWS EC2 security

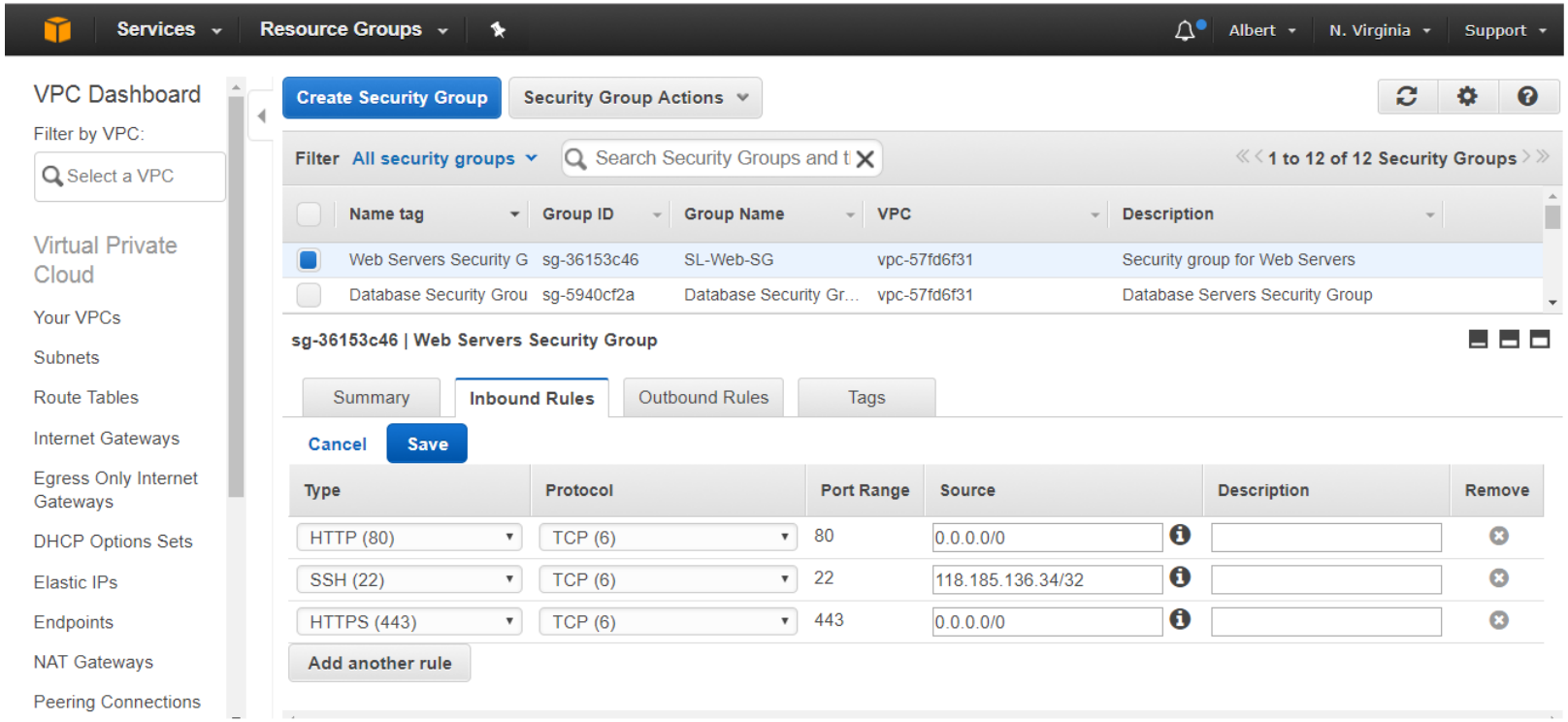


REMOTE CLASSROOM INSTRUCTION

5.Figure 2 - IAM role for EC2 instance

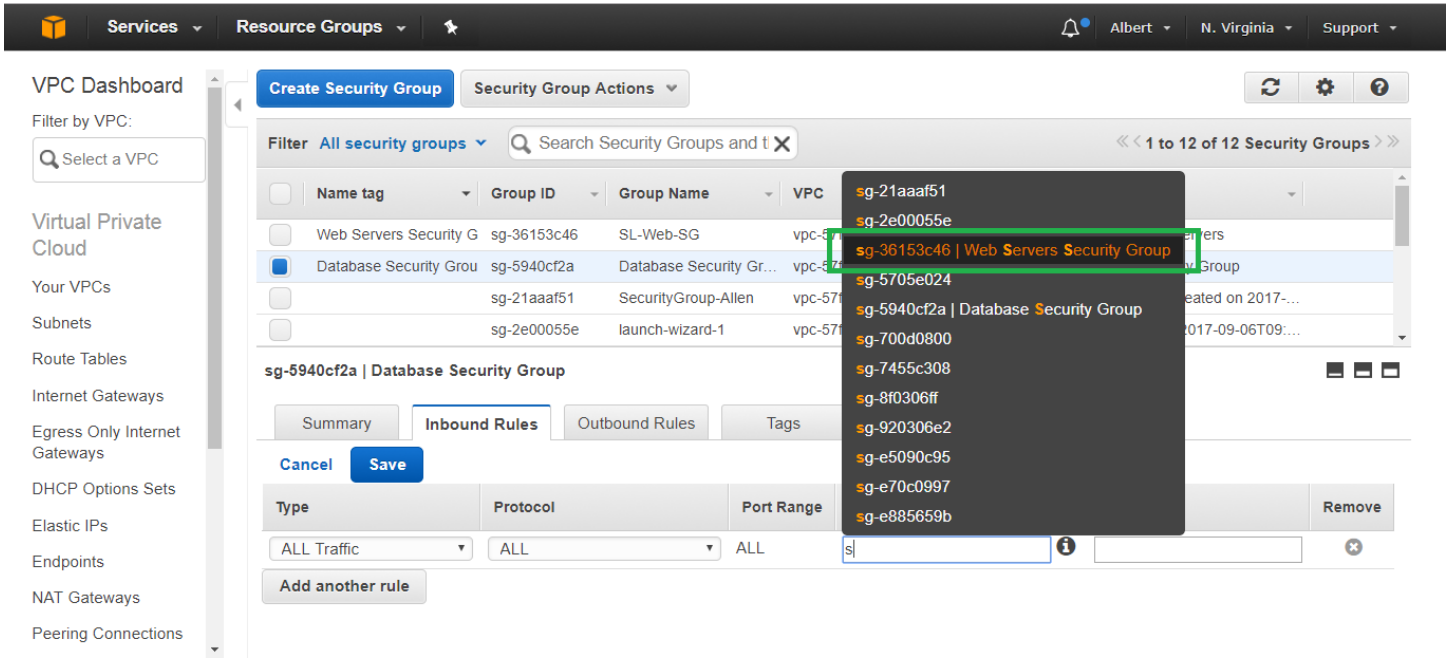


5.Figure 3 - AWS security groups



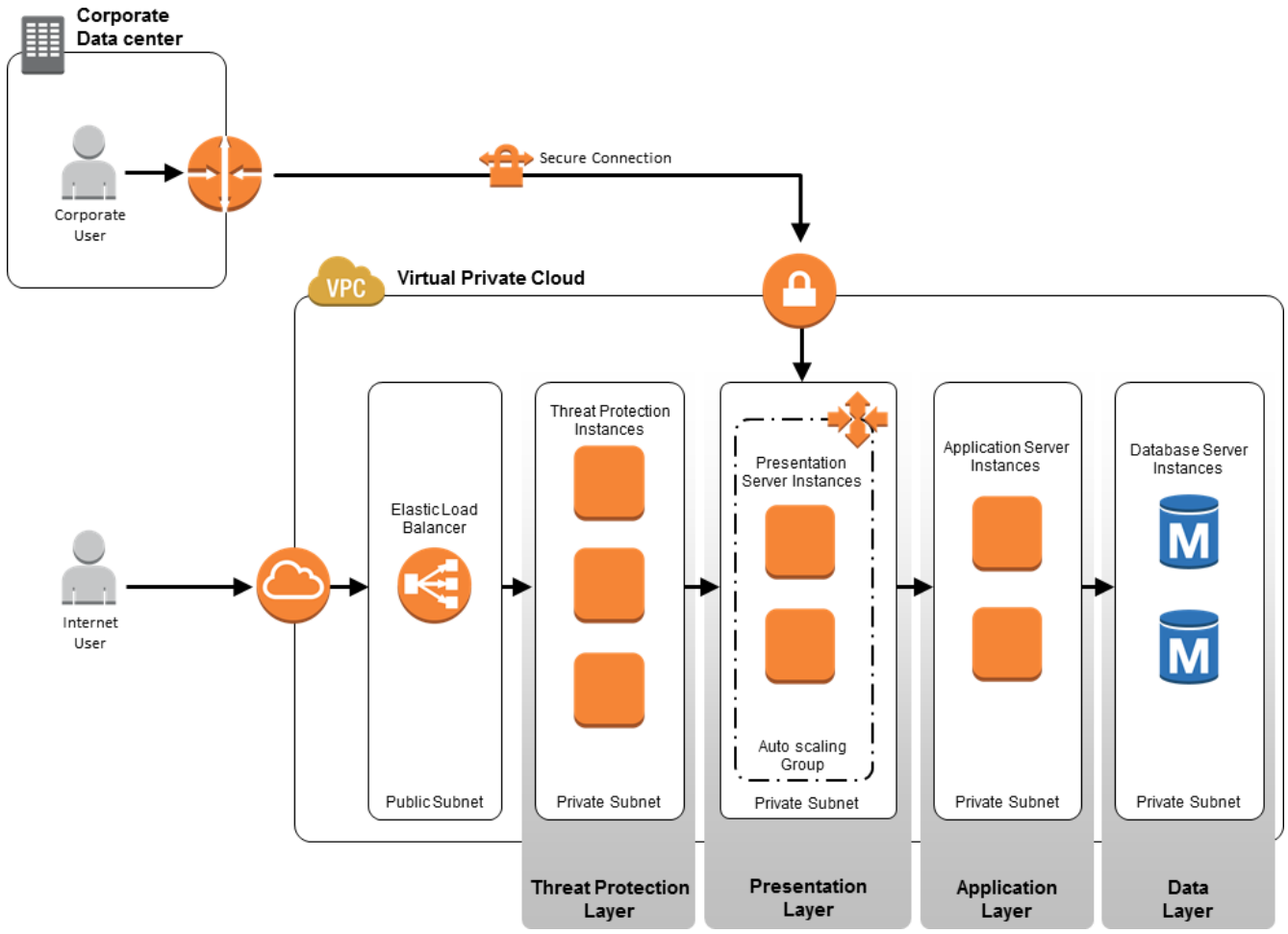
REMOTE CLASSROOM INSTRUCTION

5.Figure 4 - AWS security groups object reference



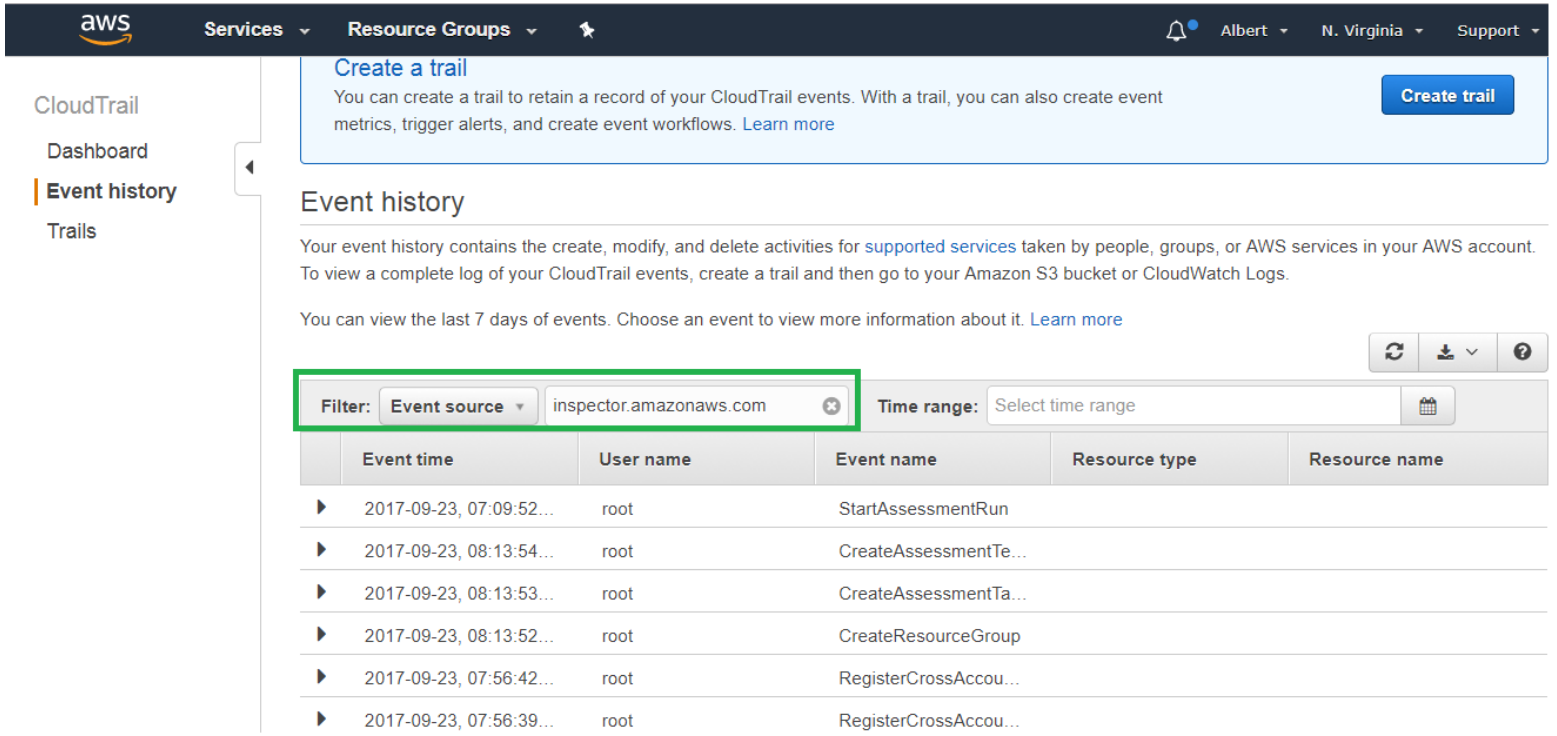
REMOTE CLASSROOM INSTRUCTION

5.Figure 5 - AWS layered network defense

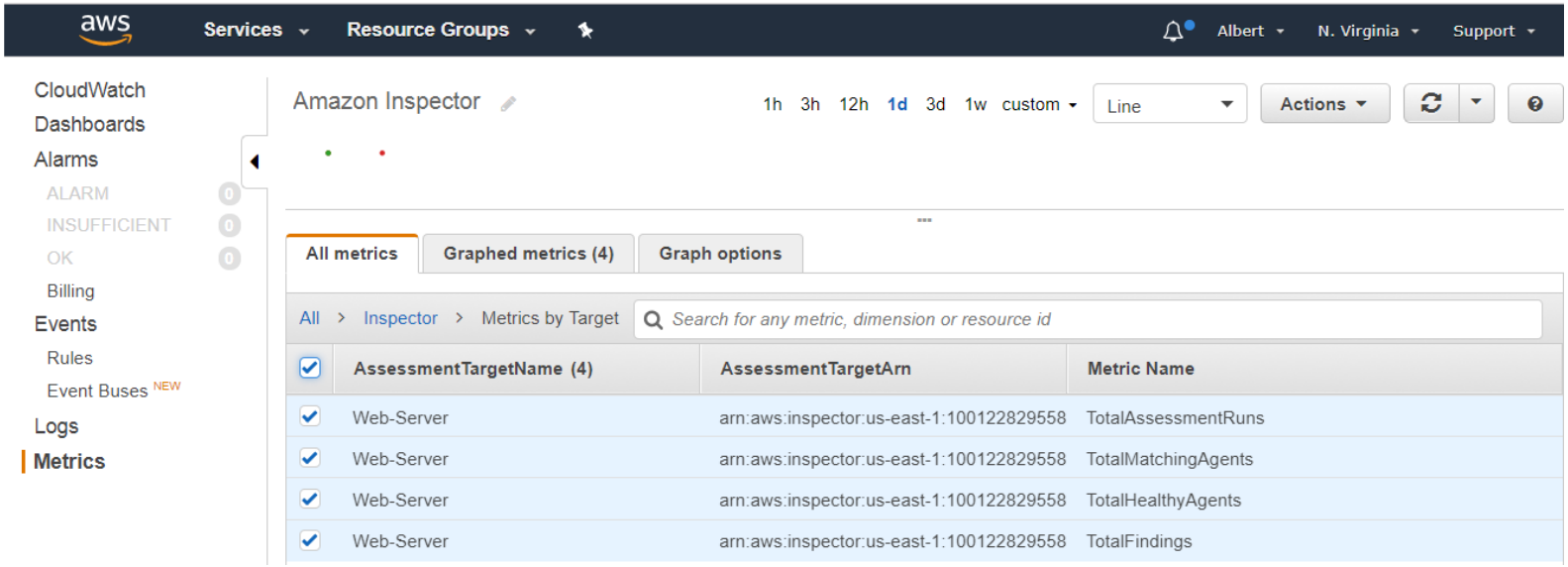


5.Figure 6 - Amazon Inspector splash screen

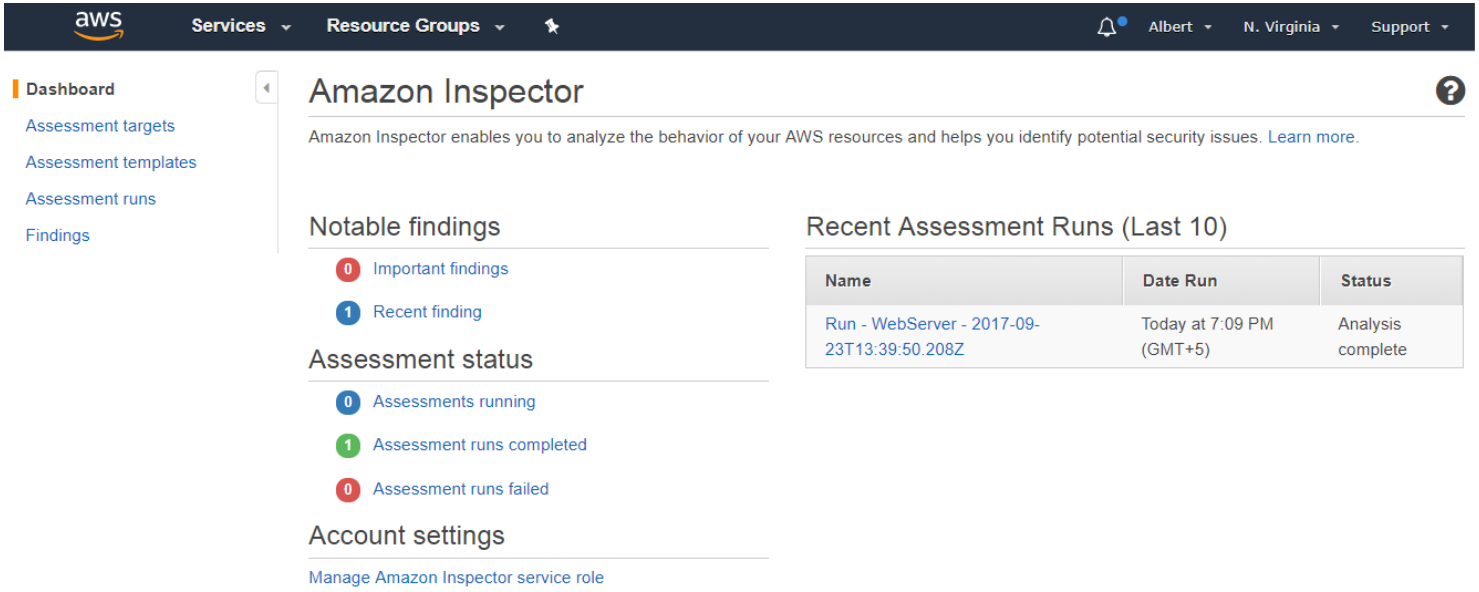
5.Figure 7 - Amazon Inspector CloudTrail events



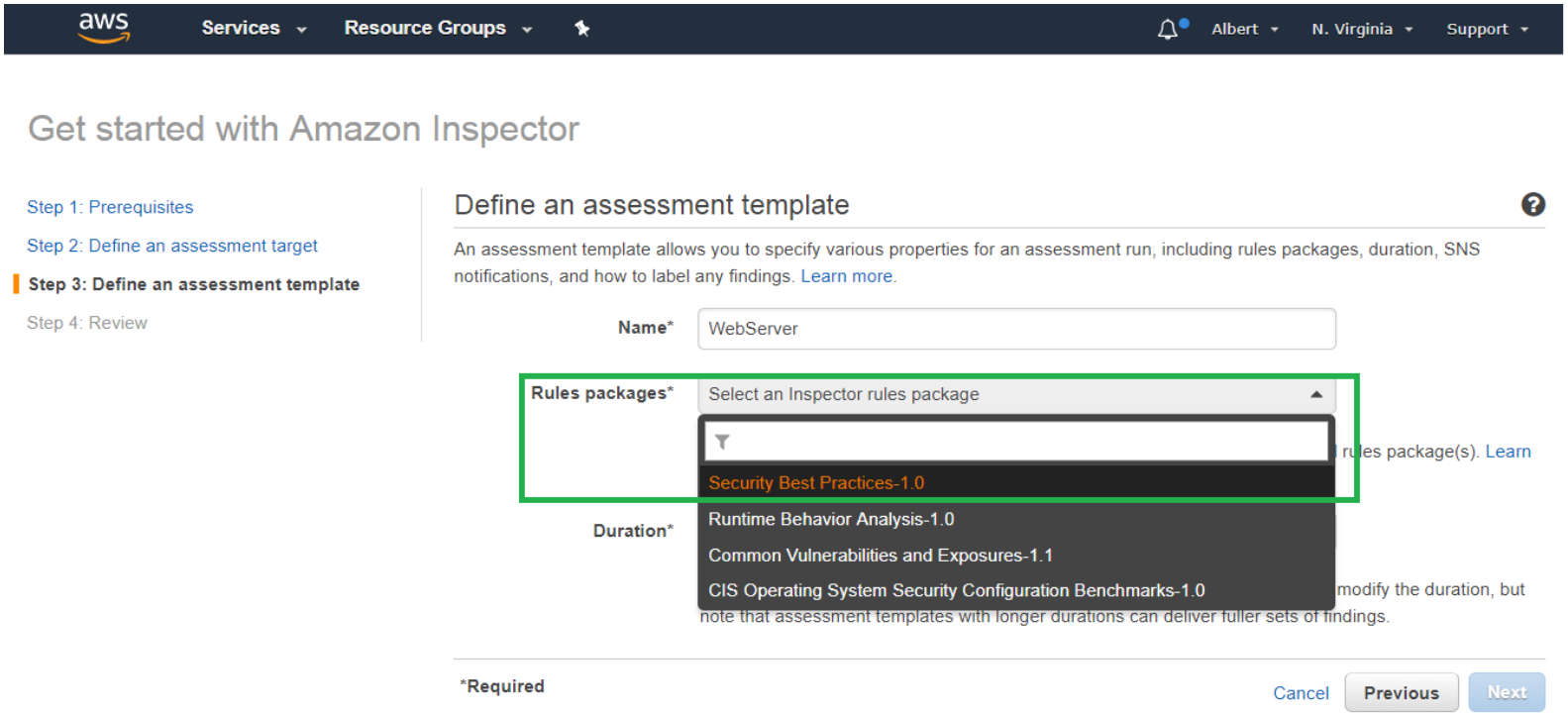
5.Figure 8 - Amazon Inspector CloudWatch metrics



5.Figure 9 - Amazon Inspector dashboard

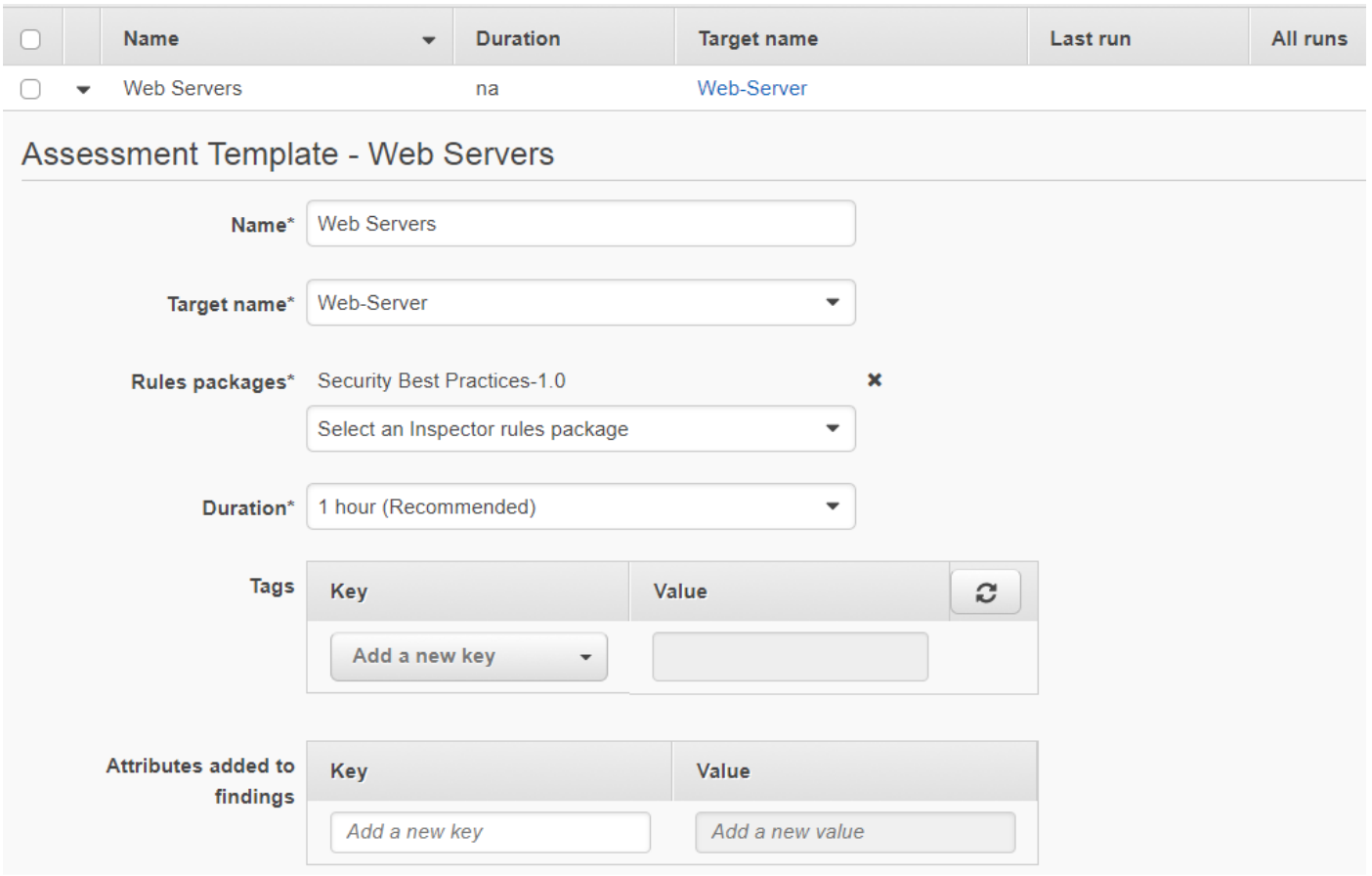


5.Figure 10 - Amazon Inspector rules package



REMOTE CLASSROOM INSTRUCTION

5.Figure 11 - Amazon Inspector assessment template



REMOTE CLASSROOM INSTRUCTION

5.Figure 12 - AWS shield tiers

AWS Security Essentials – End Day 2

- **Day 3**
- **Chapter 6**
- **Chapter 7**
- **Chapter 8**

onlc
Training Centers

AWS Security Essentials - 6

onlc
Training Centers

6.Figure 1 - AWS Web Application Firewall

Web traffic filtering with custom rules

Create custom rules that can allow, block, or count web requests based on originating IP addresses or strings that appear

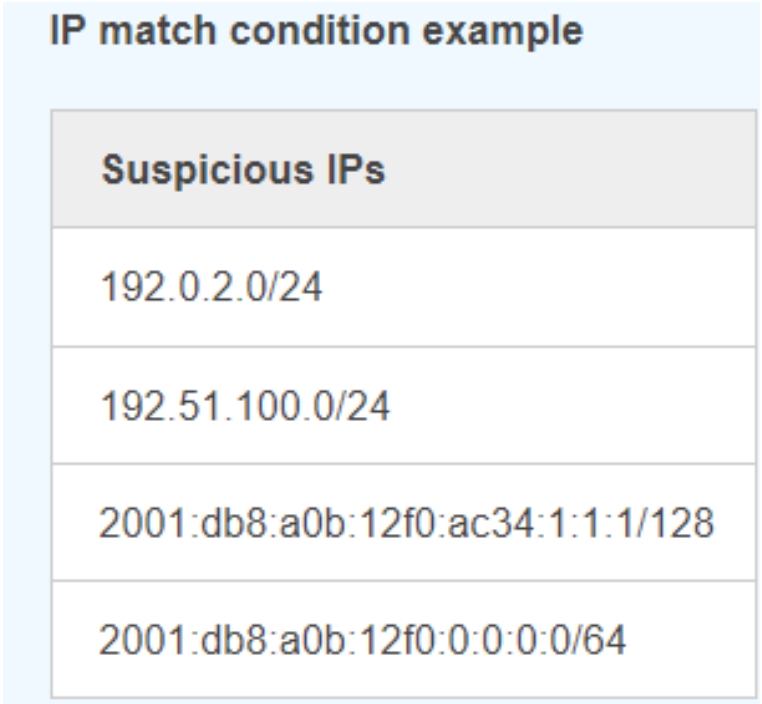
Block malicious requests

Configure AWS WAF to recognize and block common web application security risks like SQL injection (SQLi) and cross-site scripting (XSS).

Tune your rules and monitor traffic

Review details about the web requests that AWS WAF allows, blocks, or counts, and update rules to thwart new attacks.

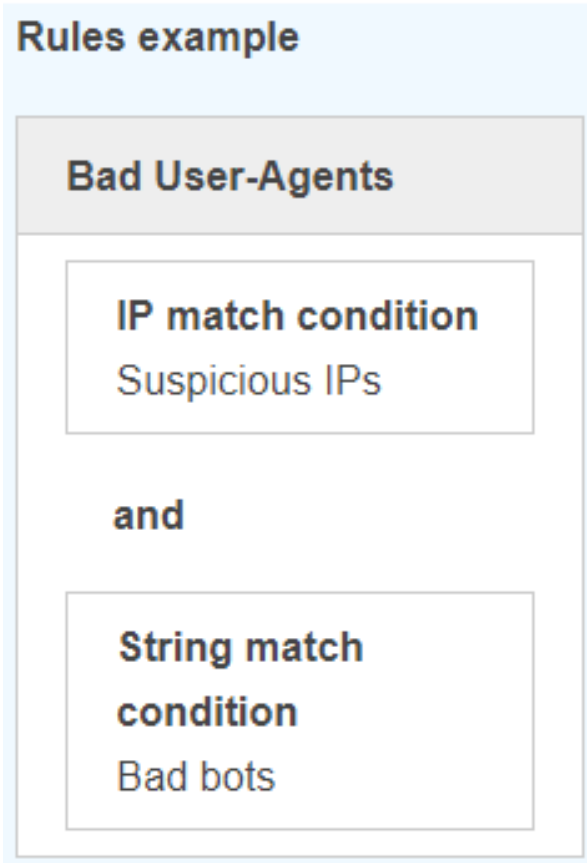
6.Figure 2 - AWS WAF condition



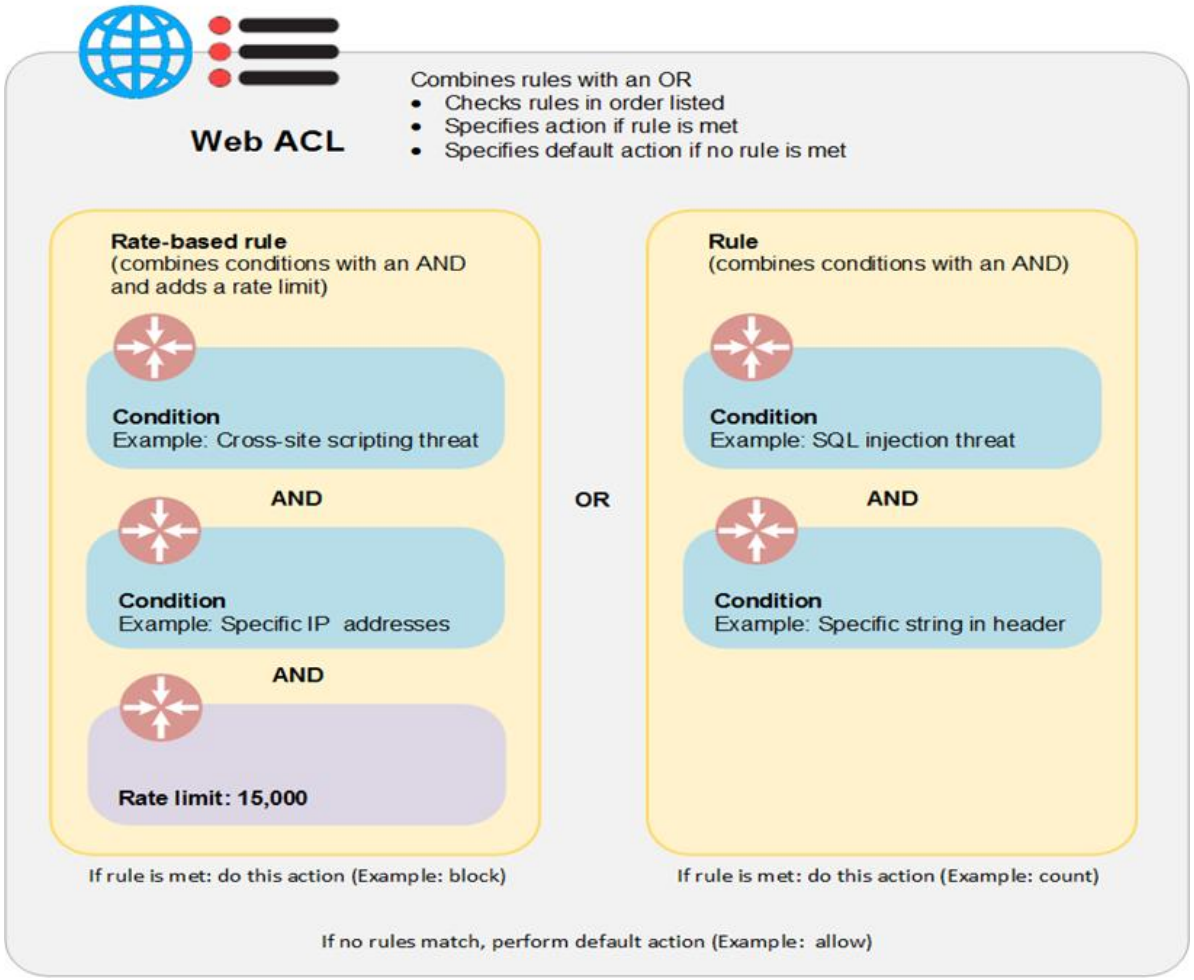
IP match condition example

Suspicious IPs
192.0.2.0/24
192.51.100.0/24
2001:db8:a0b:12f0:ac34:1:1:1/128
2001:db8:a0b:12f0:0:0:0:0/64

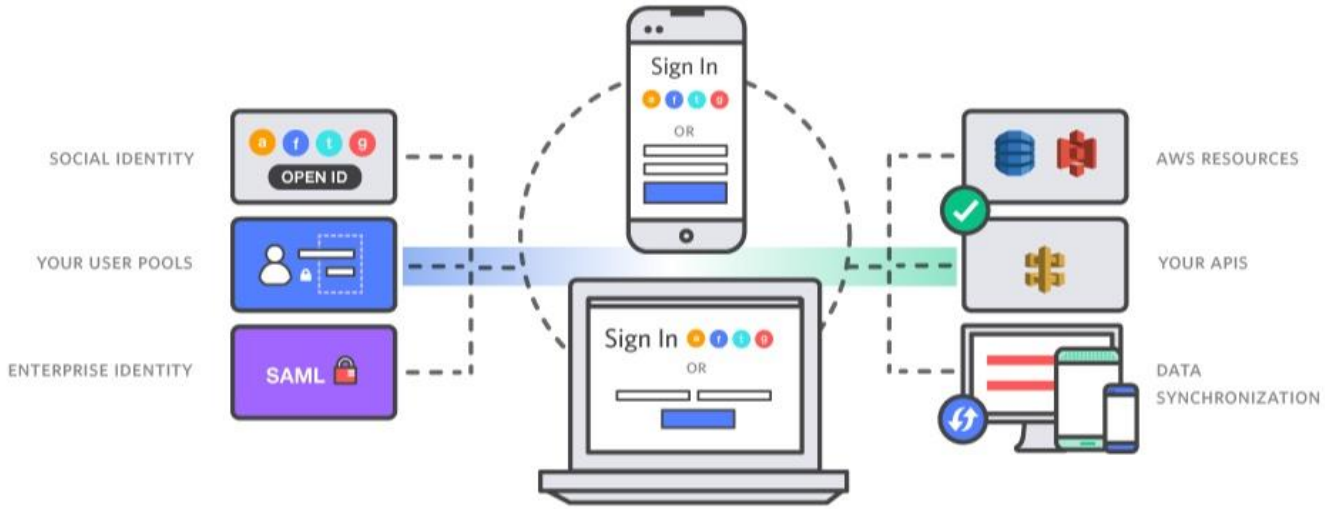
6.Figure 3 - AWS WAF rules



6.Figure 4 AWS WAF Web ACL



6.Figure 5 - AWS Cognito overview

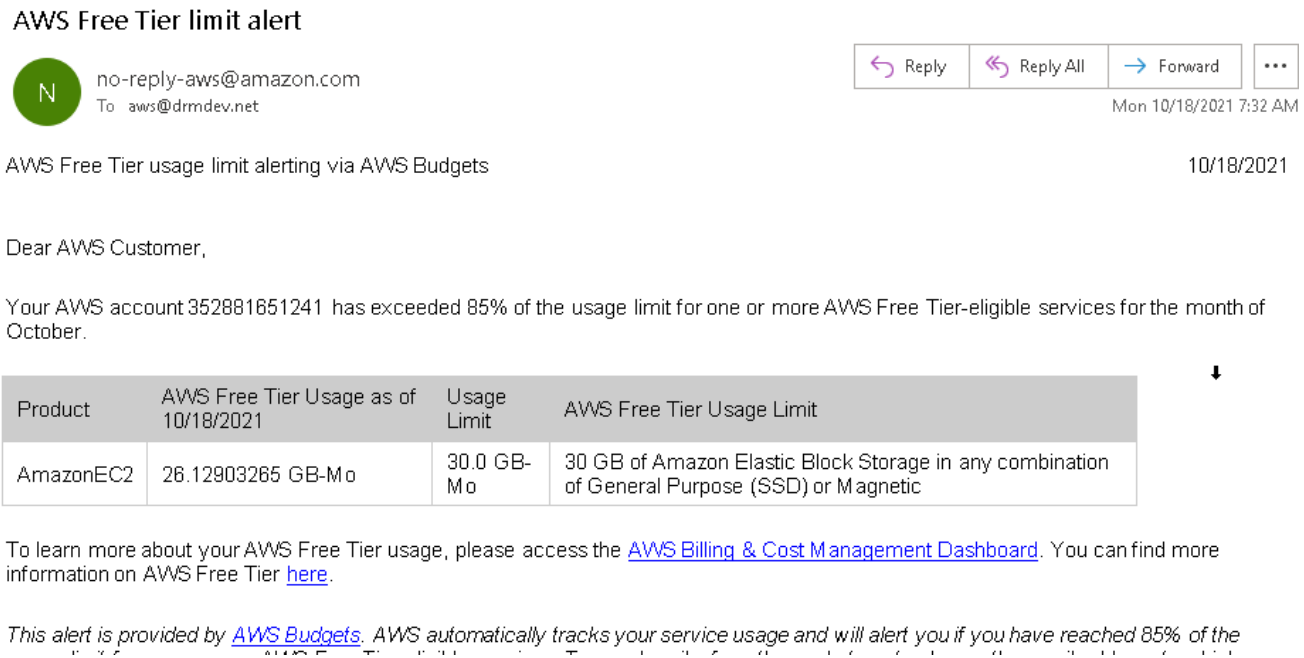


REMOTE CLASSROOM INSTRUCTION

AWS Security Essentials - 7

onlc
Training Centers

7.AWS CloudWatch Alert



AWS Free Tier limit alert

N no-reply-aws@amazon.com
To aws@drmdev.net

Reply | Reply All | Forward | ...
Mon 10/18/2021 7:32 AM

AWS Free Tier usage limit alerting via AWS Budgets 10/18/2021

Dear AWS Customer,

Your AWS account 352881651241 has exceeded 85% of the usage limit for one or more AWS Free Tier-eligible services for the month of October.

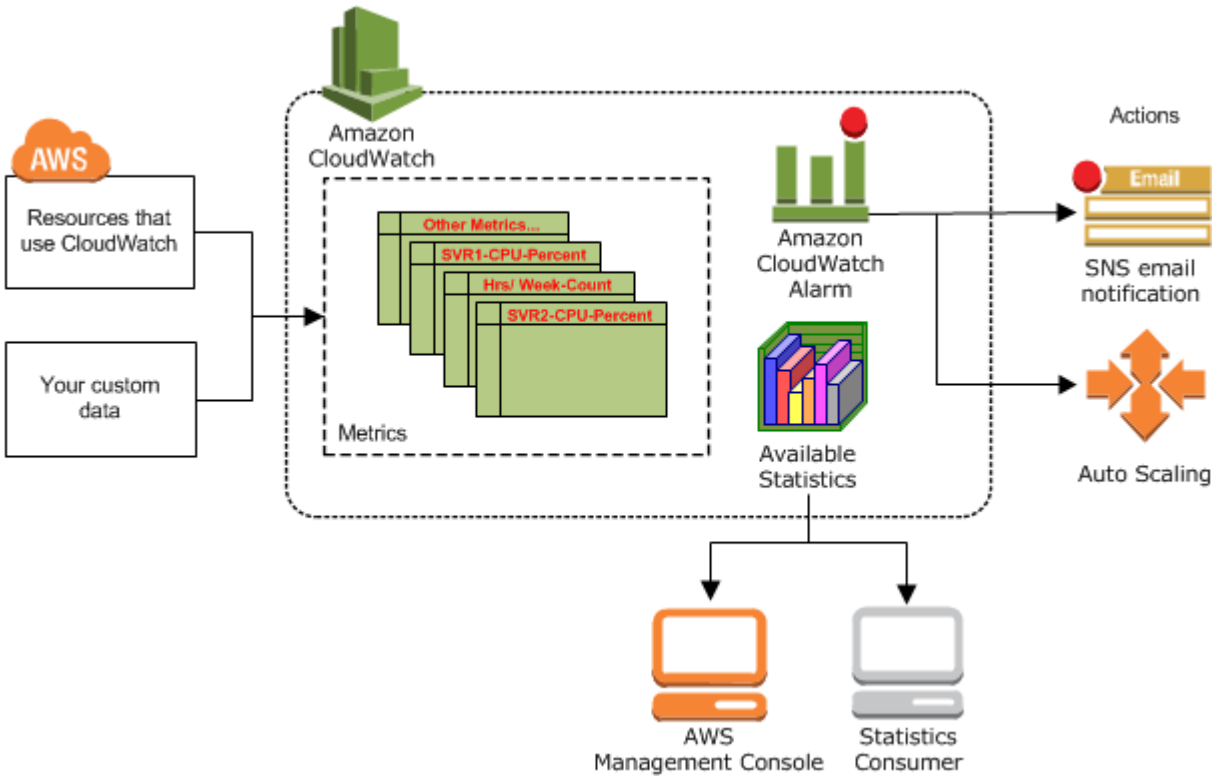
Product	AWS Free Tier Usage as of 10/18/2021	Usage Limit	AWS Free Tier Usage Limit
AmazonEC2	26.12903265 GB-Mo	30.0 GB-Mo	30 GB of Amazon Elastic Block Storage in any combination of General Purpose (SSD) or Magnetic

To learn more about your AWS Free Tier usage, please access the AWS Billing & Cost Management Dashboard. You can find more information on AWS Free Tier here.

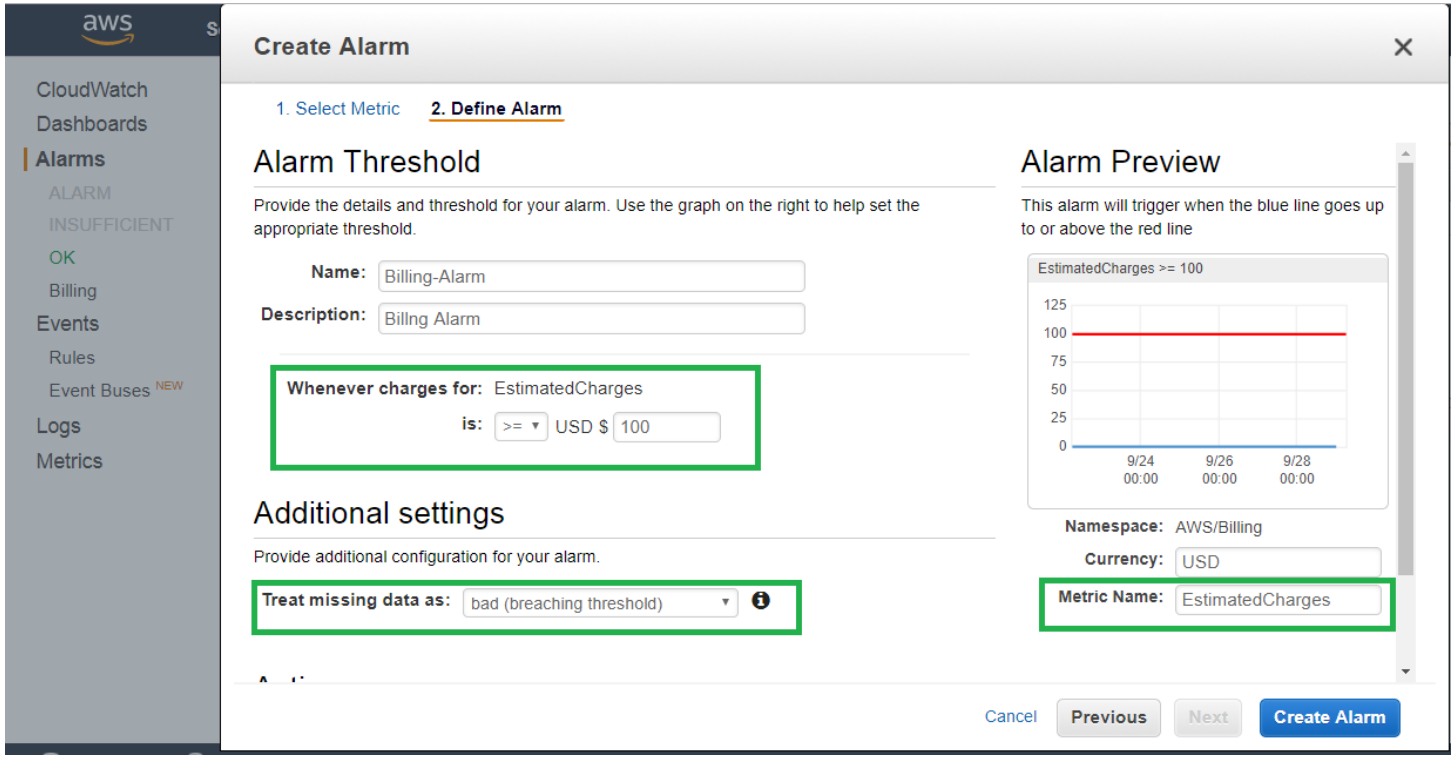
This alert is provided by AWS Budgets. AWS automatically tracks your service usage and will alert you if you have reached 85% of the

REMOTE CLASSROOM INSTRUCTION

7.Figure 1 - AWS CloudWatch architecture

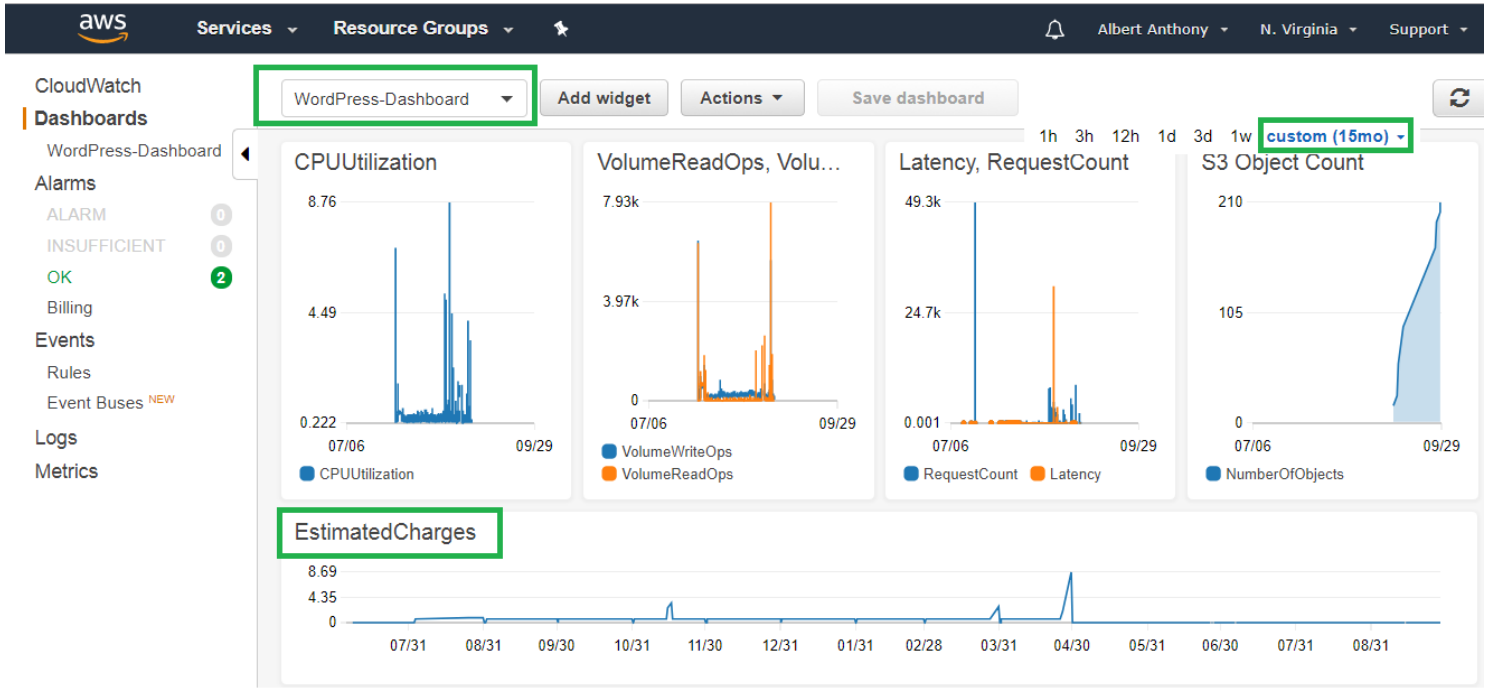


7.Figure 2 - AWS CloudWatch Create Alarm



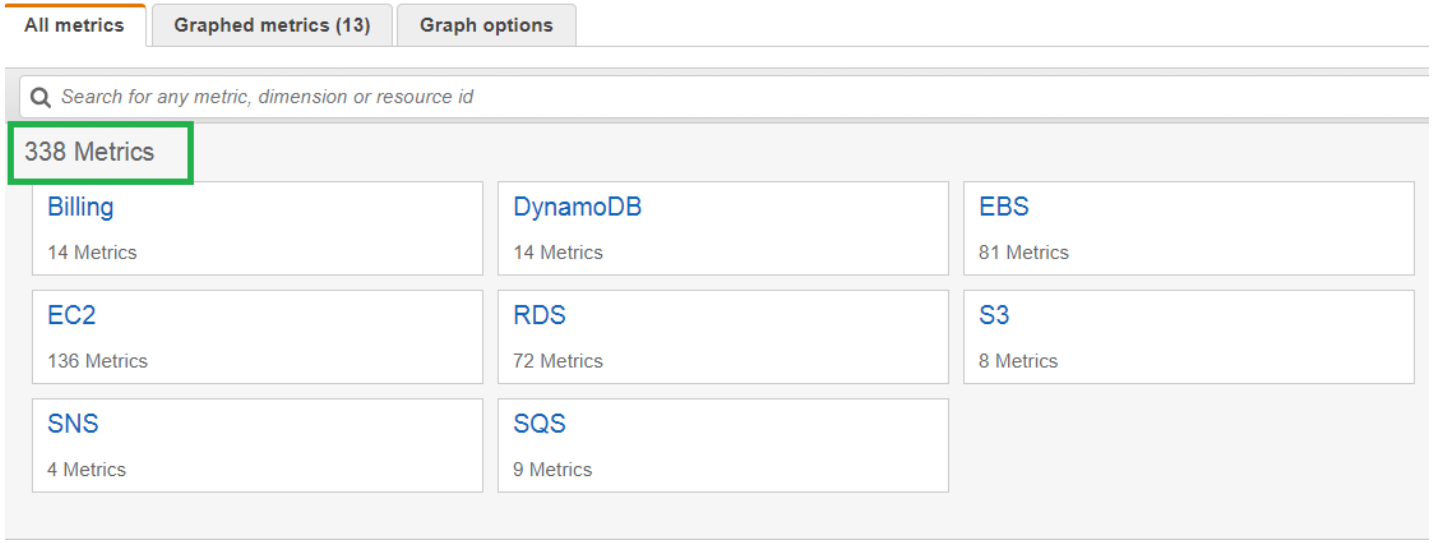
REMOTE CLASSROOM INSTRUCTION

7.Figure 3 - AWS CloudWatch dashboard



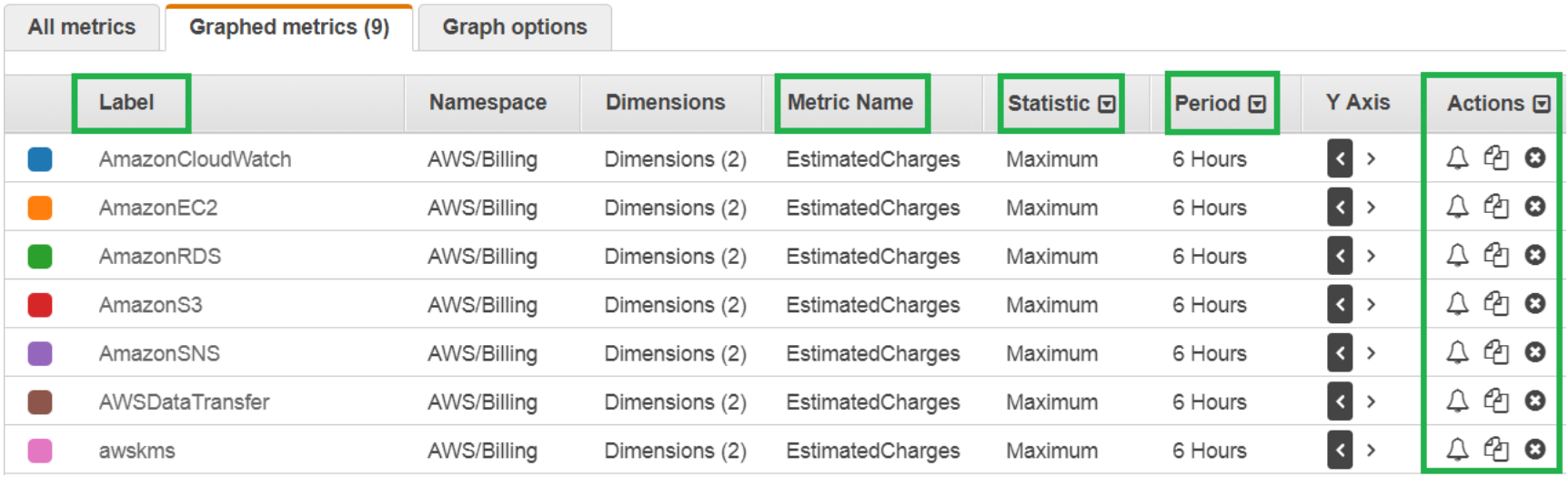
REMOTE CLASSROOM INSTRUCTION

7.Figure 4 - AWS CloudWatch Metrics



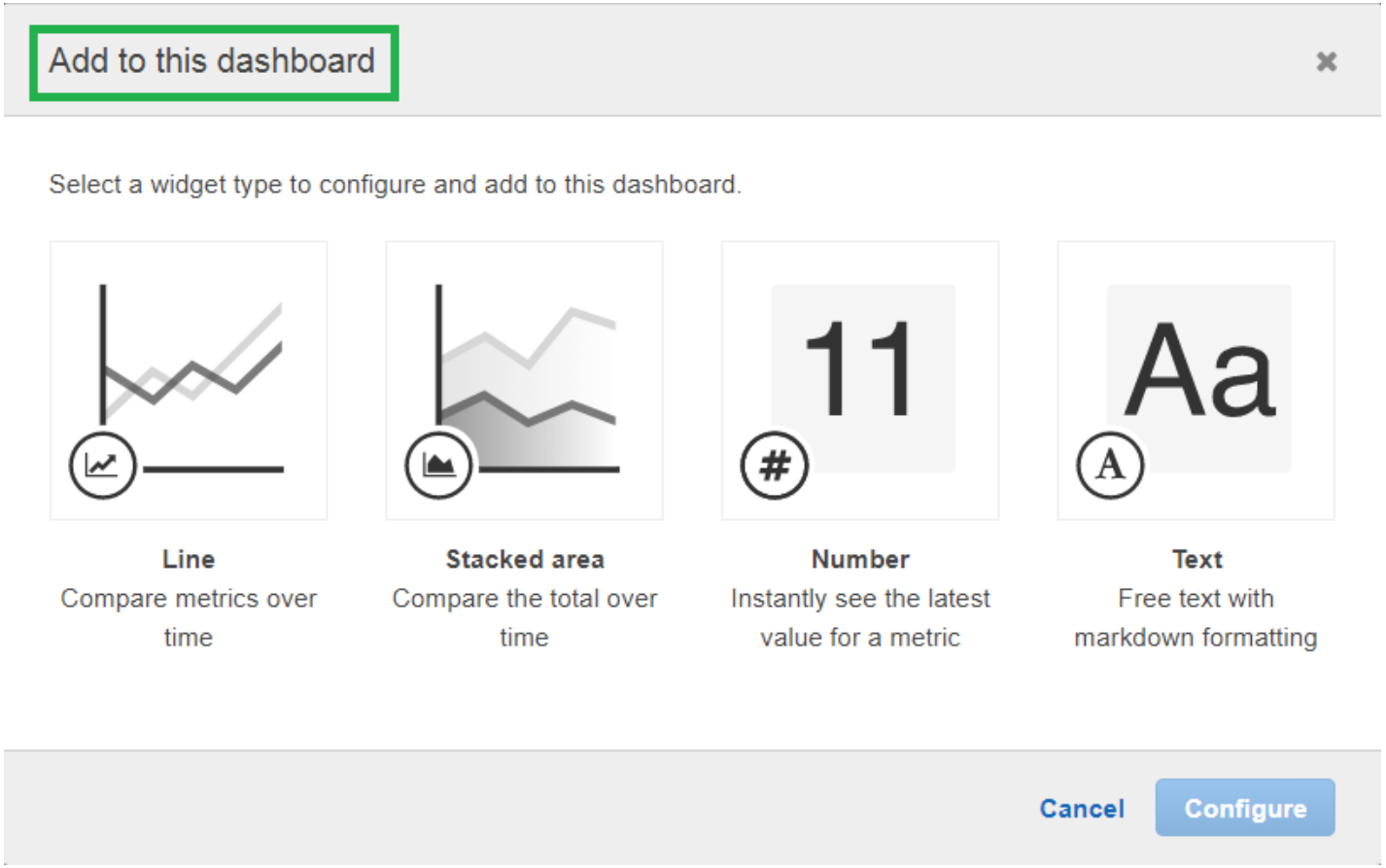
REMOTE CLASSROOM INSTRUCTION

7.Figure 5 - AWS CloudWatch Metric details

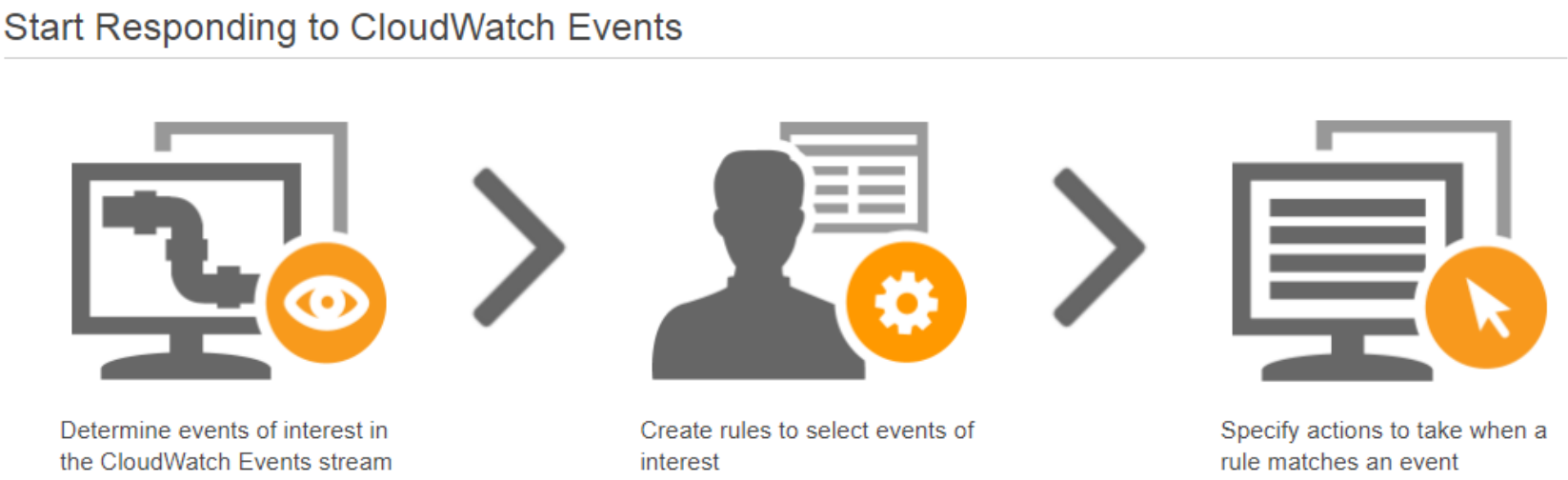


RCI
REMOTE CLASSROOM INSTRUCTION

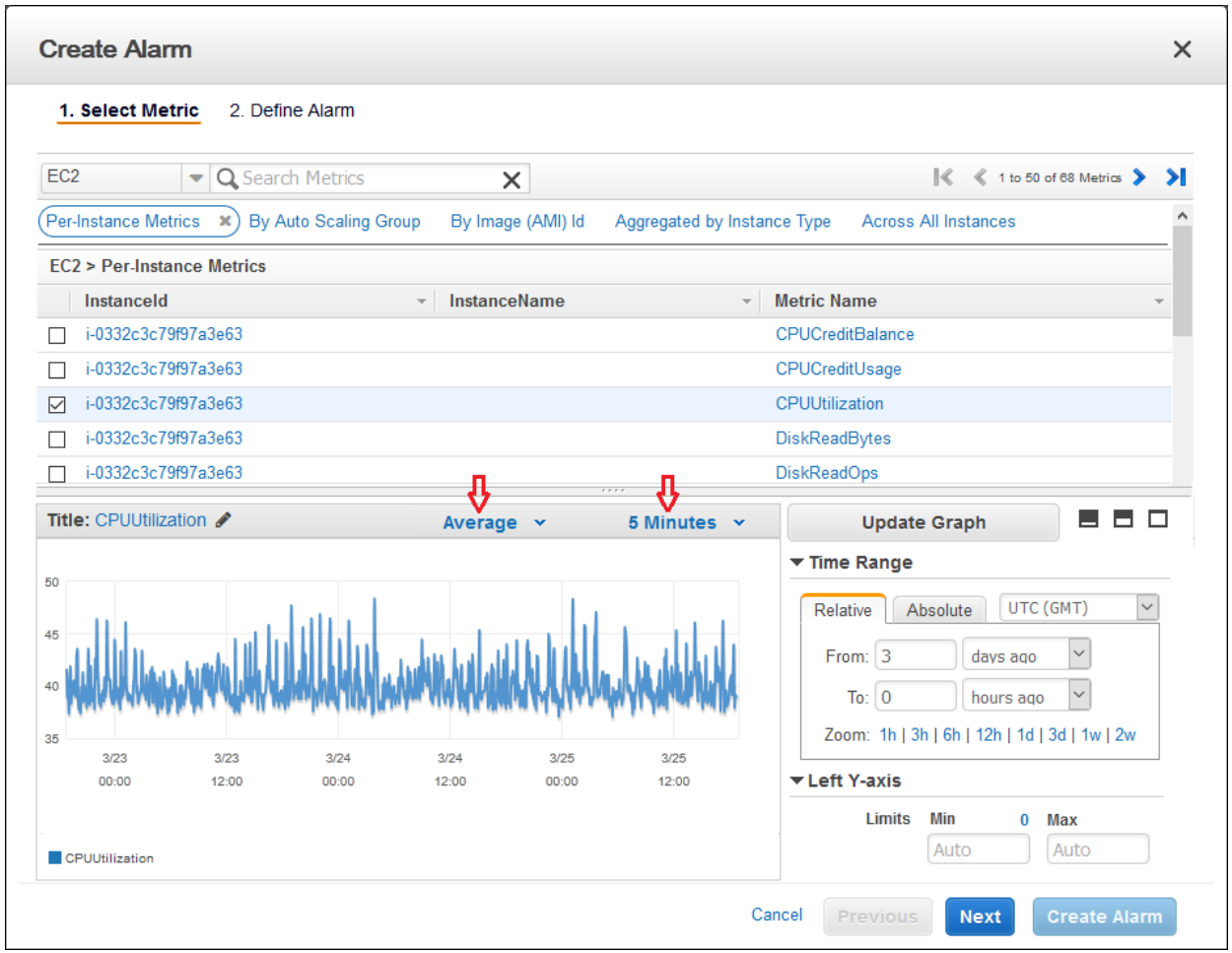
7.Figure 6 - AWS CloudWatch dashboard options



7.Figure 7 - AWS CloudWatch Events

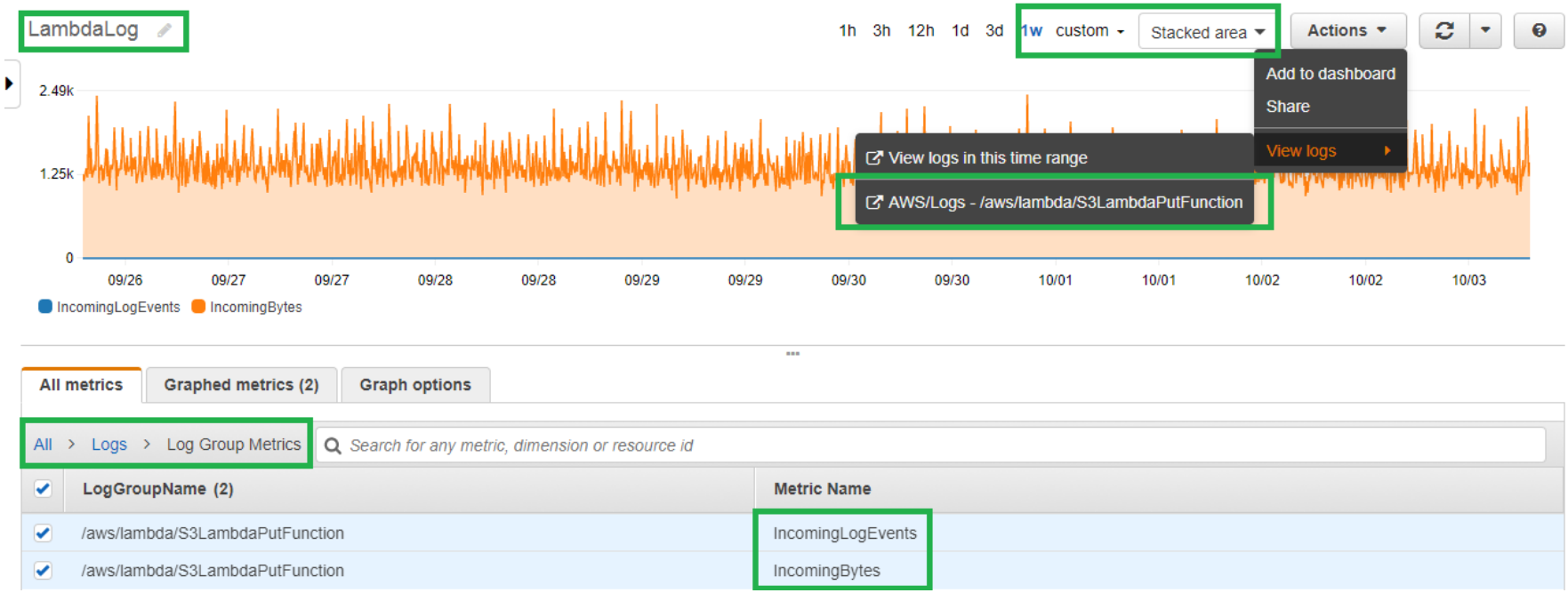


7.Figure 8 - AWS CloudWatch alarm



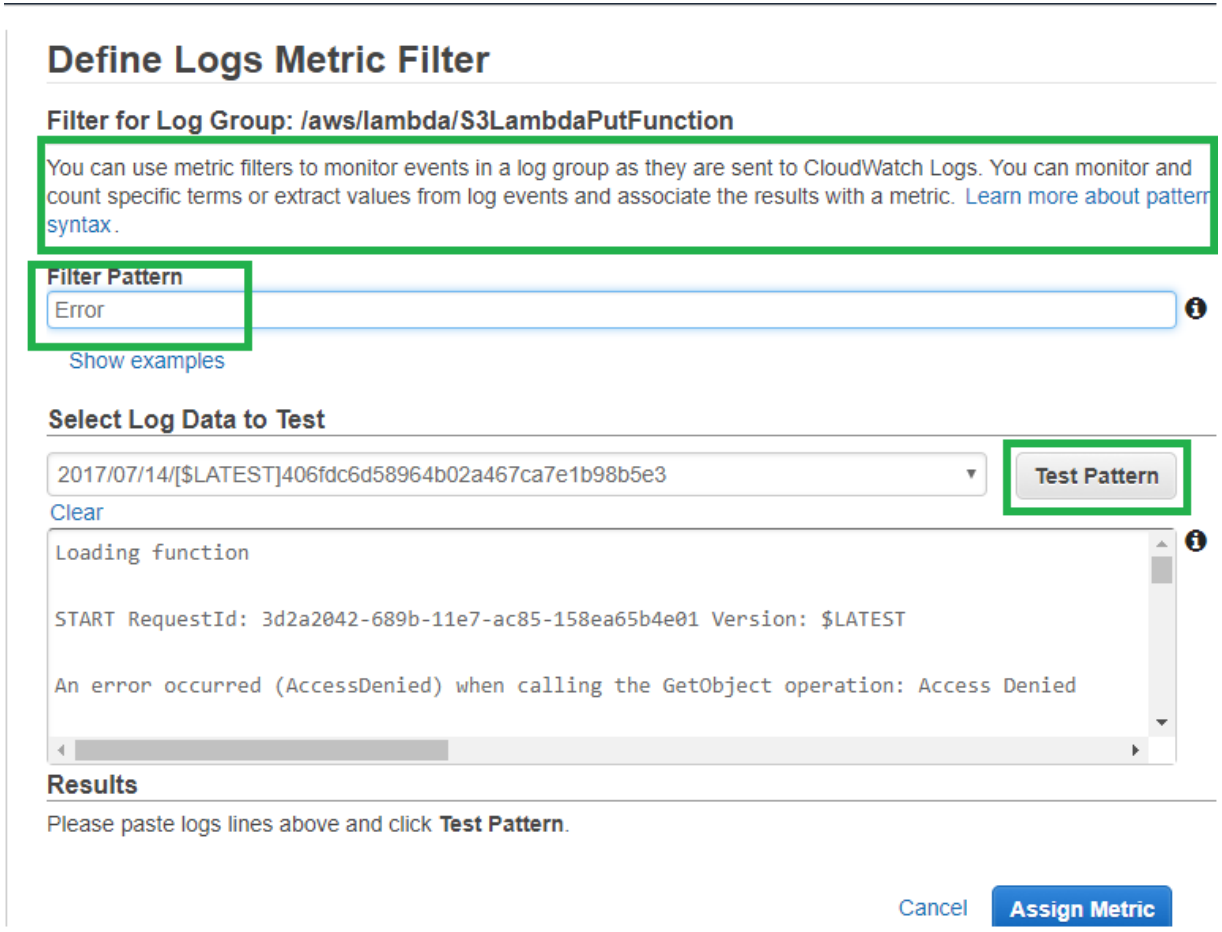
REMOTE CLASSROOM INSTRUCTION

7.Figure 9 - AWS CloudWatch log monitoring



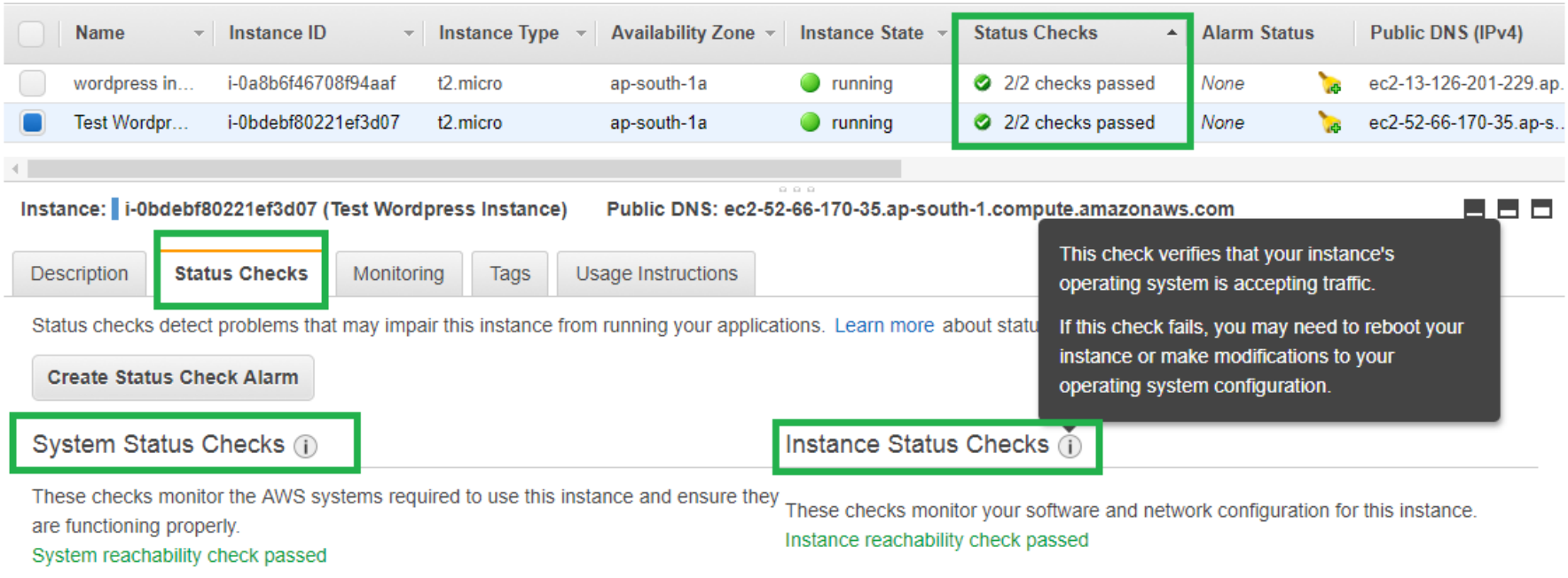
REMOTE CLASSROOM INSTRUCTION

7.Figure 10 - AWS CloudWatch Create Logs Metric



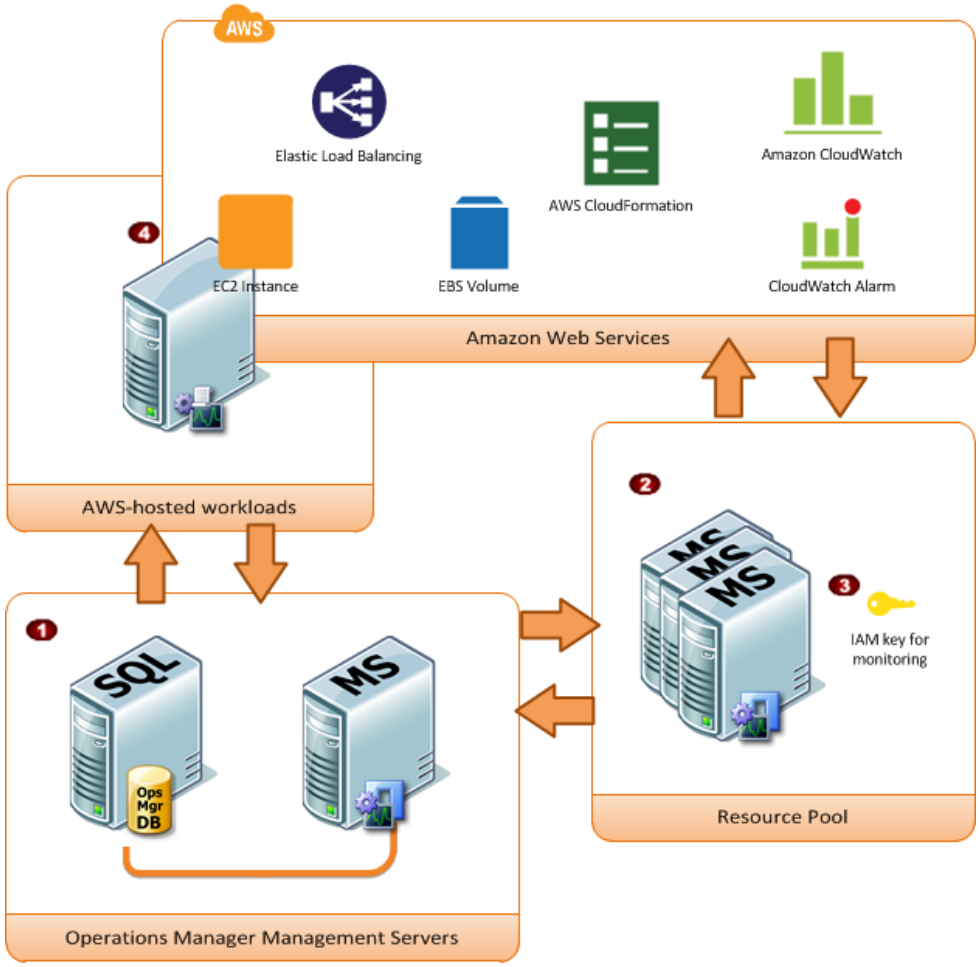
REMOTE CLASSROOM INSTRUCTION

7.Figure 11 - AWS system and instance checks



REMOTE CLASSROOM INSTRUCTION

7.Figure 12 - AWS Management Pack



REMOTE CLASSROOM INSTRUCTION

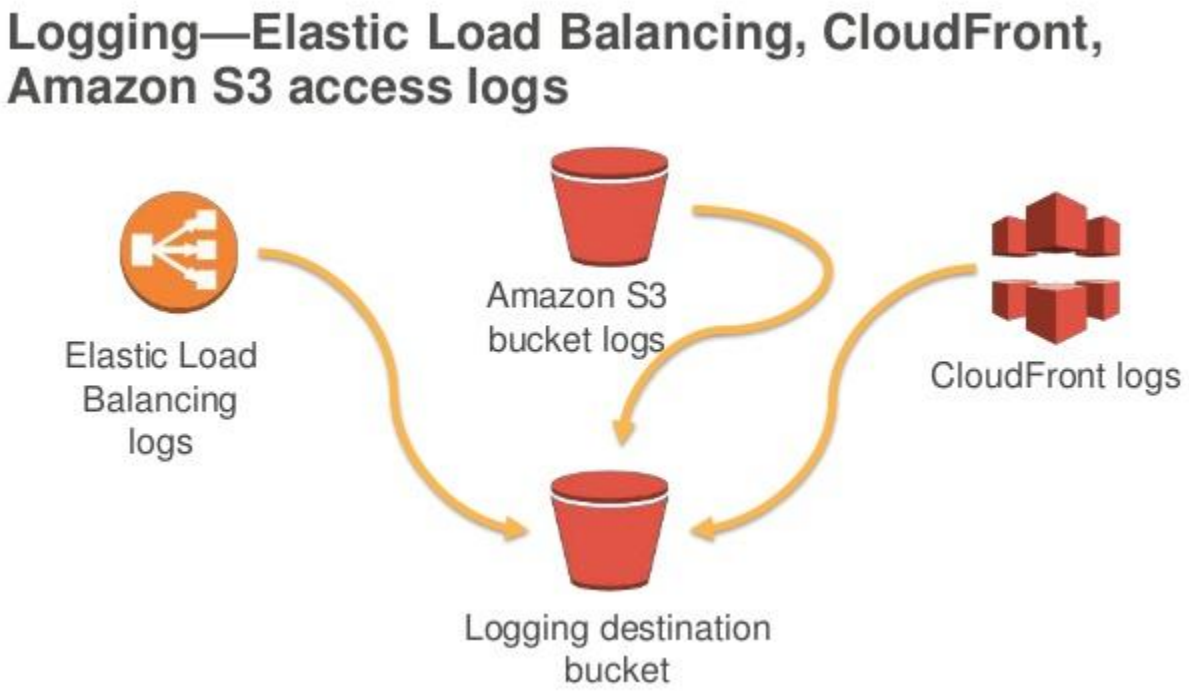
AWS Security Essentials - 8

onlc
Training Centers

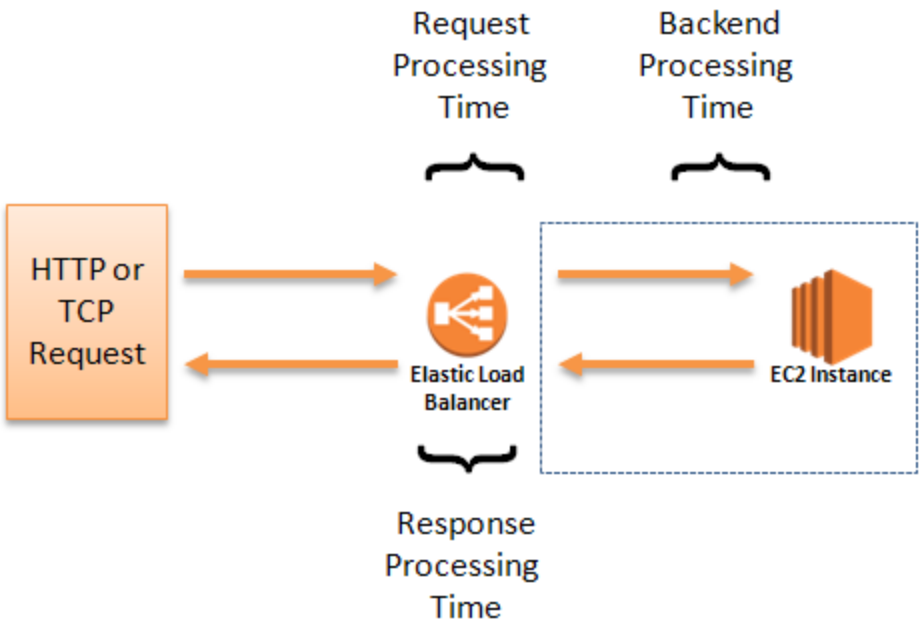
8. Table 1 - AWS logs classification

AWS infrastructure logs	AWS service logs	Host-based logs
AWS CloudTrail	Amazon S3	Messages
AWS VPC flow logs	AWS ELB	IIS/Apache
	Amazon CloudFront	Windows Event logs
	AWS Lambda	Custom logs

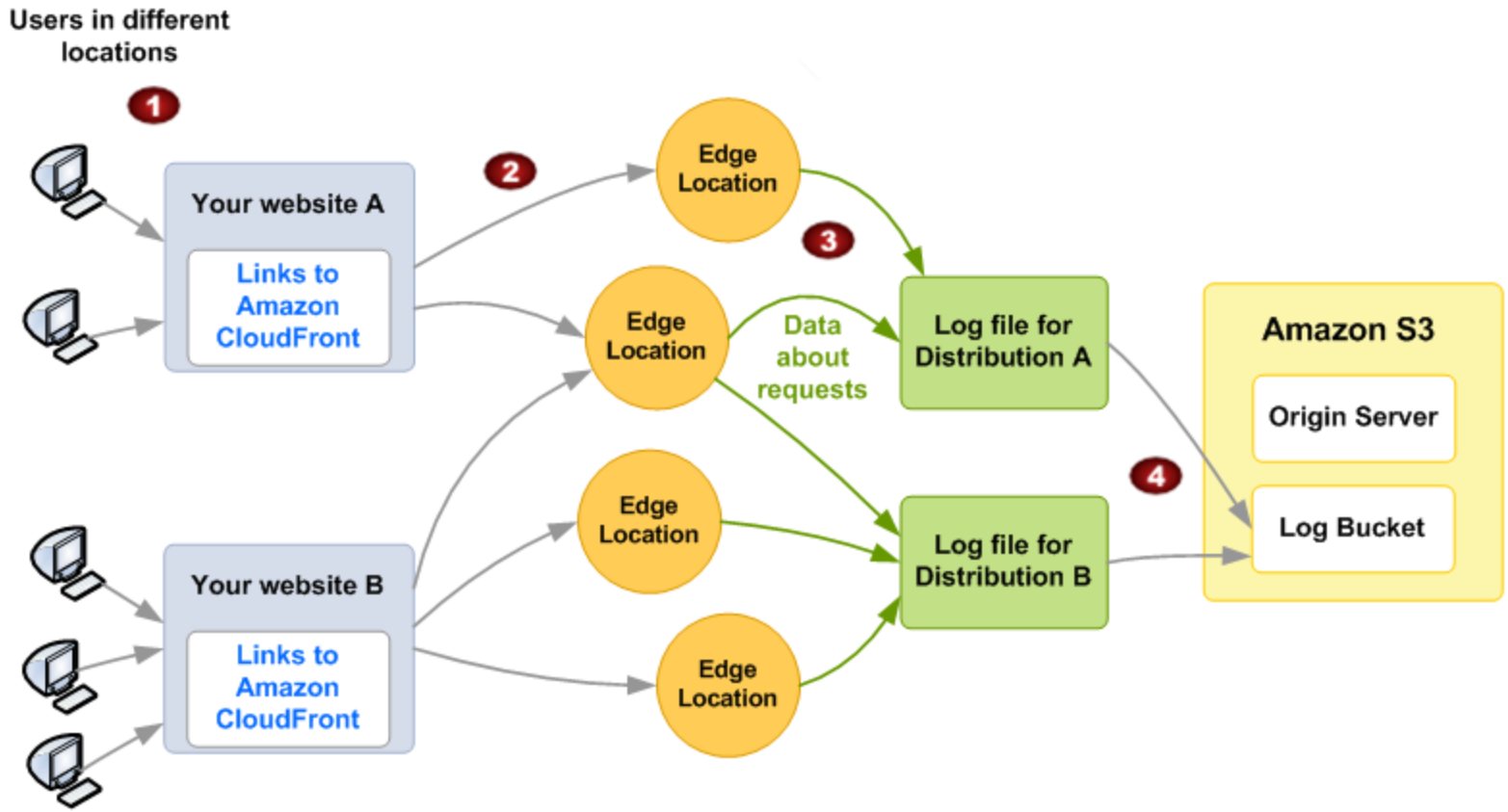
8.Figure 1 - AWS access logging S3



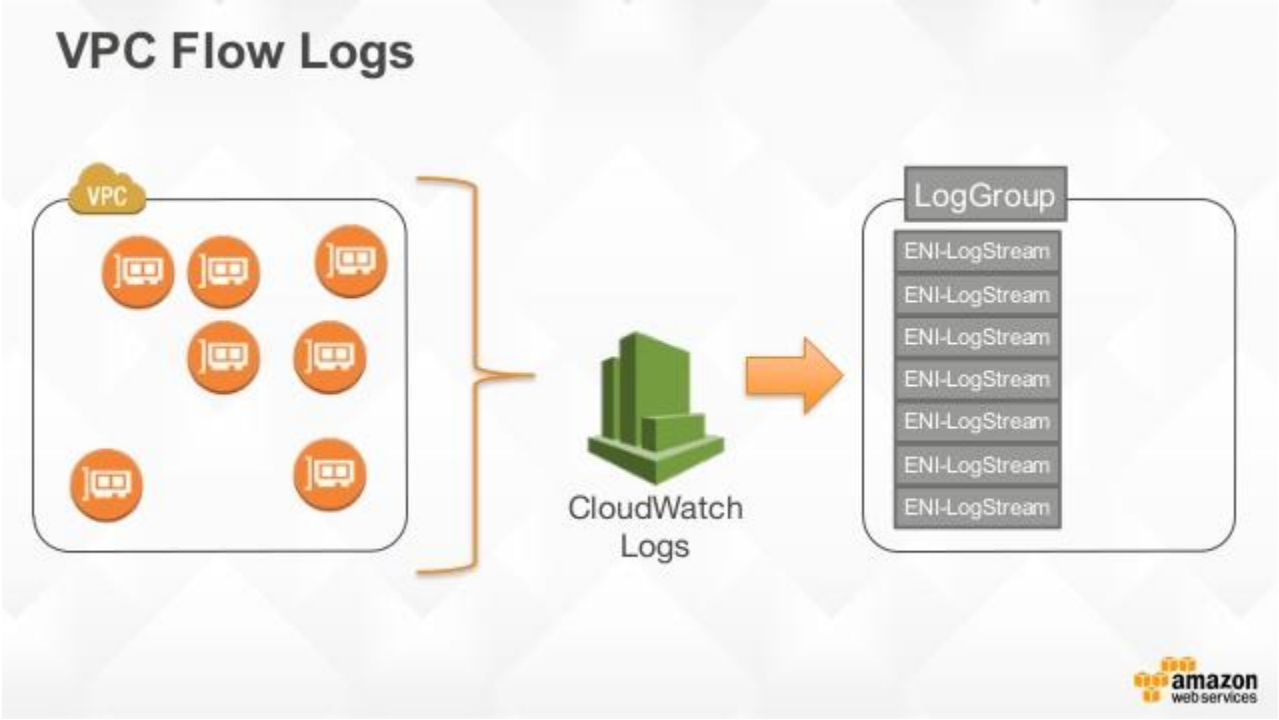
8.Figure 2 - Amazon ELB logging



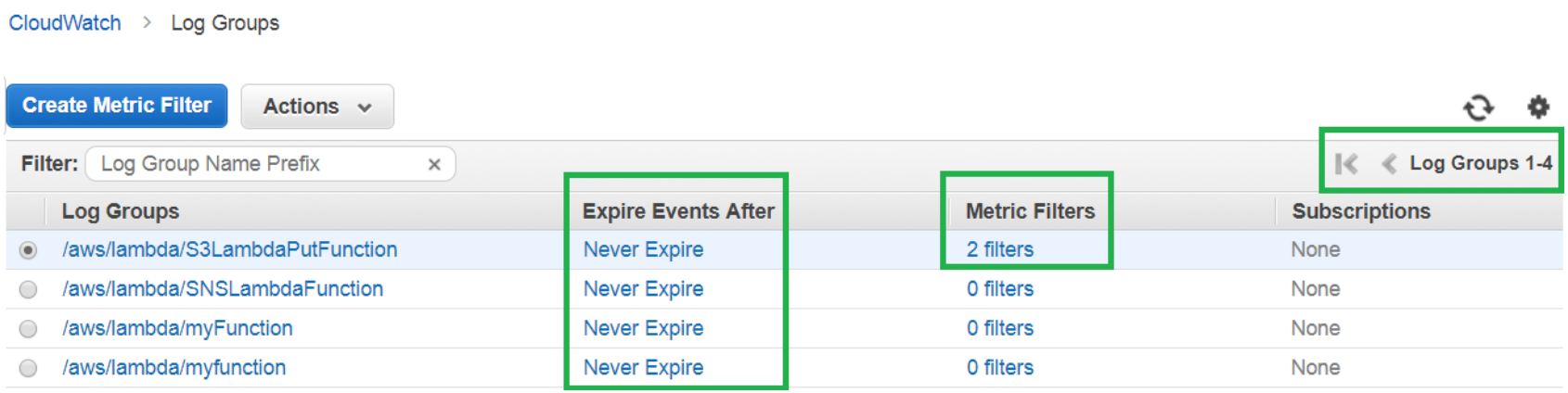
8.Figure 3 - Amazon CloudFront logging



8.Figure 4 - Amazon VPC flow logs

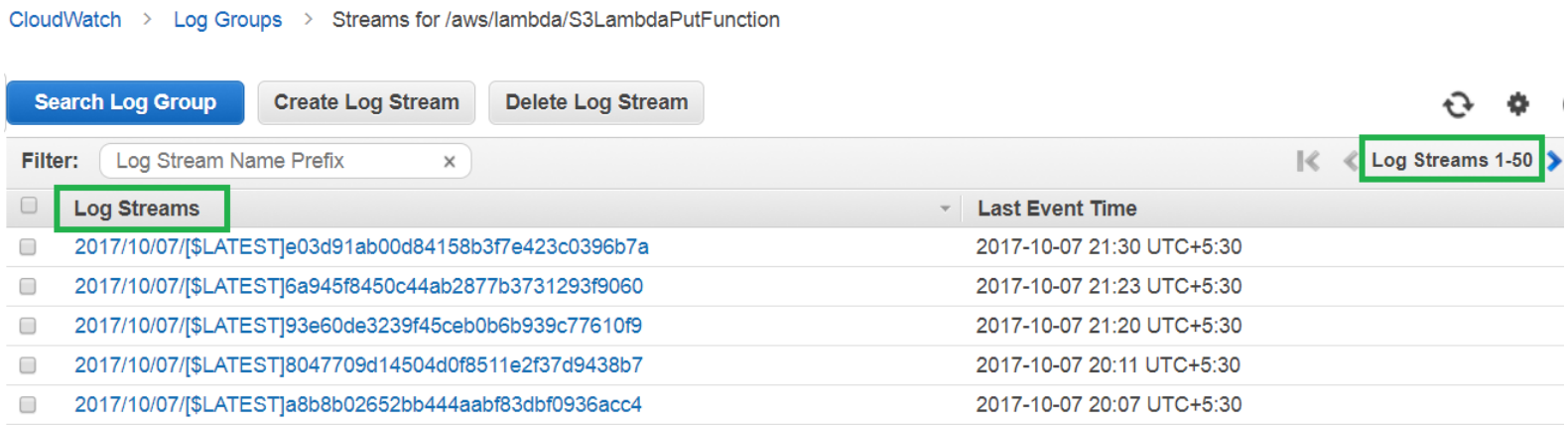


8.Figure 5 - AWS CloudWatch Logs

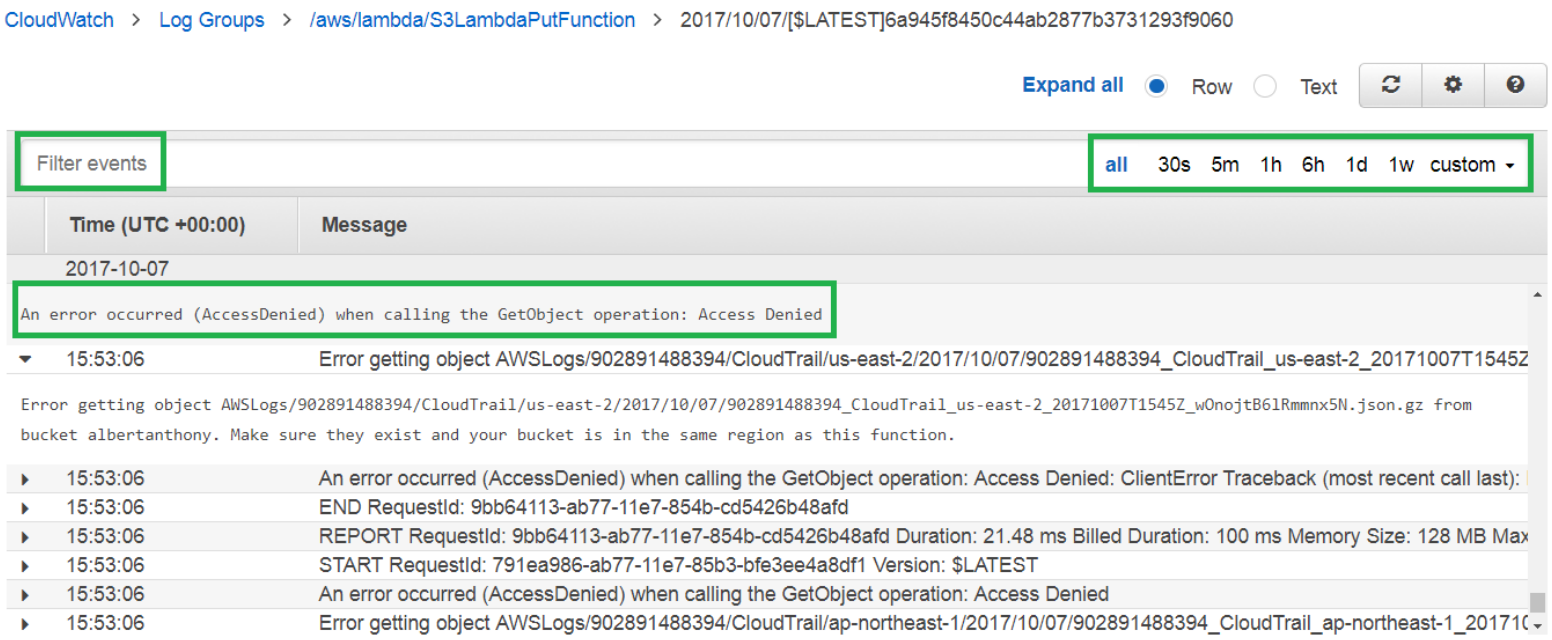


REMOTE CLASSROOM INSTRUCTION

8.Figure 6 - AWS CloudWatch Log streams

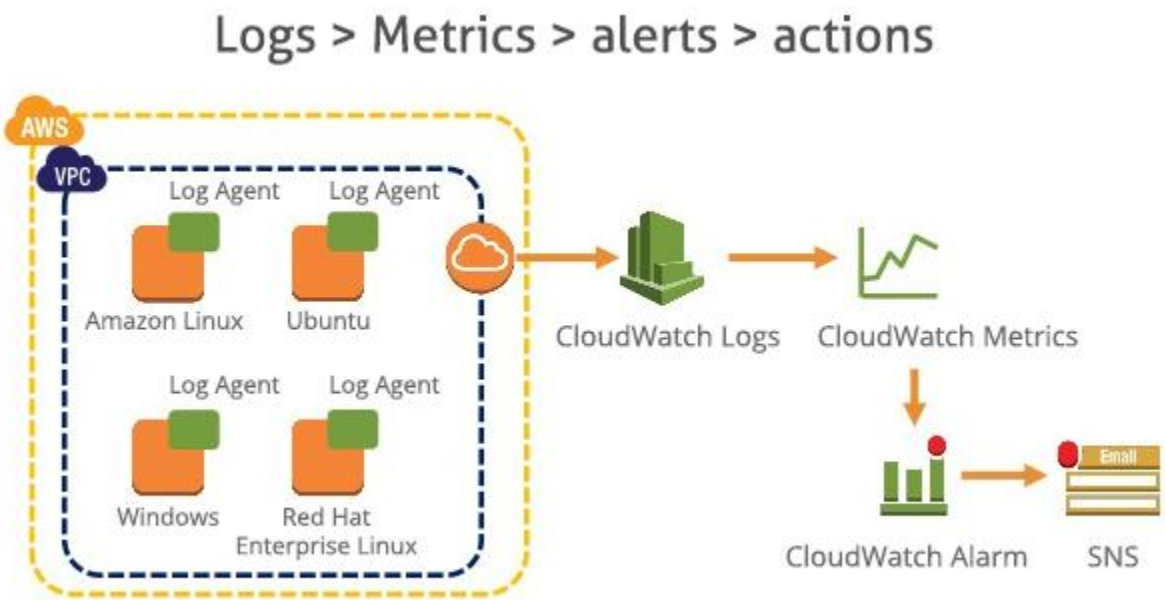


8.Figure 7 - AWS CloudWatch events log



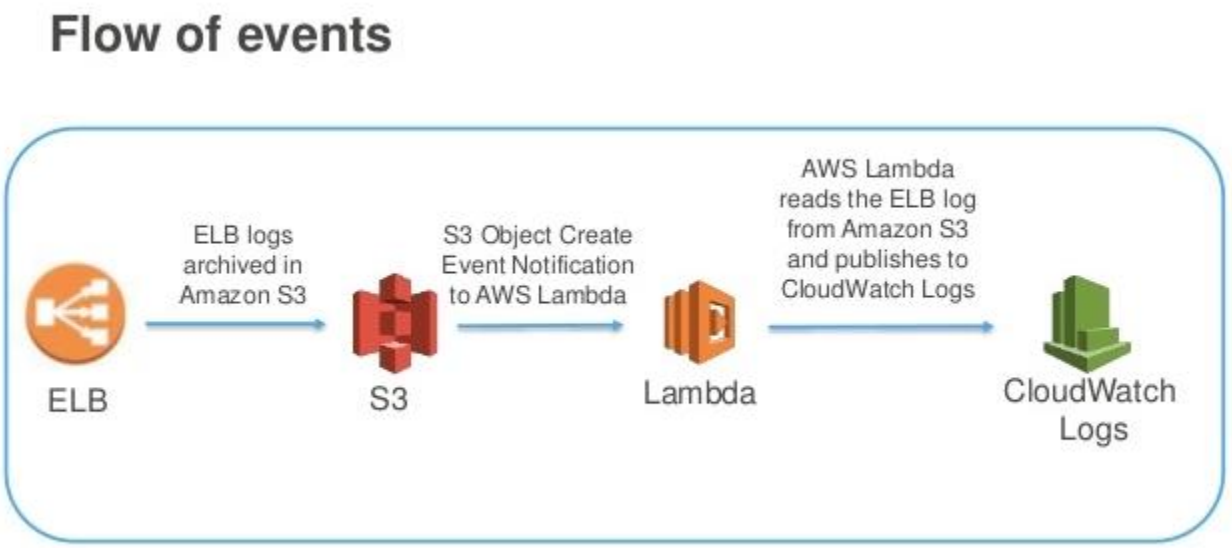
REMOTE CLASSROOM INSTRUCTION

8.Figure 8 - AWS CloudWatch Log agent lifecycle

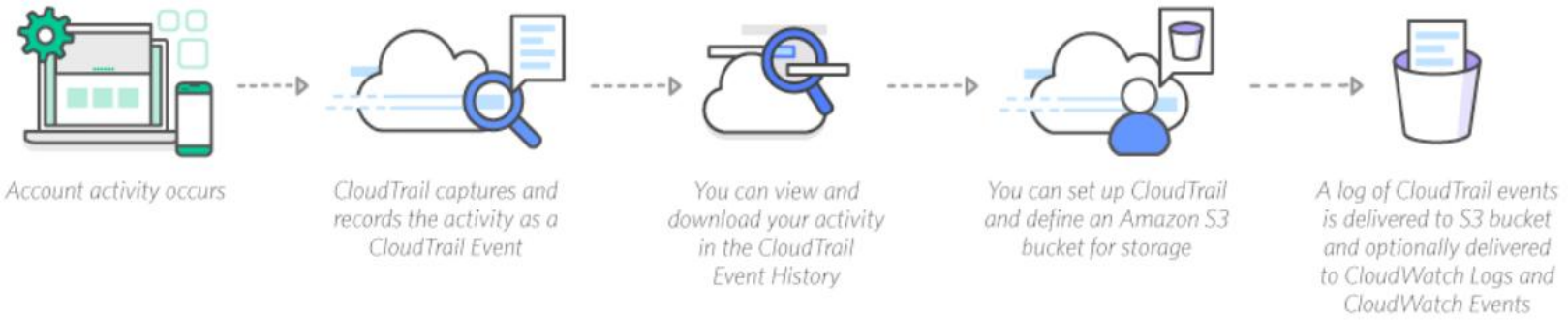


REMOTE CLASSROOM INSTRUCTION

8.Figure 9 - AWS CloudWatch Logs lifecycle



8.Figure 10 - AWS CloudTrail lifecycle



8.Figure 11 - AWS CloudTrail events

	Event time	User name	Event name	Resource type
▶	2017-10-08, 08:56:01 …	root	ConsoleLogin	
▼	2017-10-08, 04:31:42 …	S3LambdaPutFunction	CreateLogStream	

AWS access key ASIAJRGSLRIJL2TUS5SQ

AWS region ap-south-1

Error code

Event ID 9c7d0d4e-cfb5-4bac-b5bb-6b108f6720a8

Event name CreateLogStream

Event source logs.amazonaws.com

Event time 2017-10-08, 04:31:42 PM

Request ID 11232d98-ac18-11e7-bdb0-d356217574b0

Source IP address 52.66.68.156

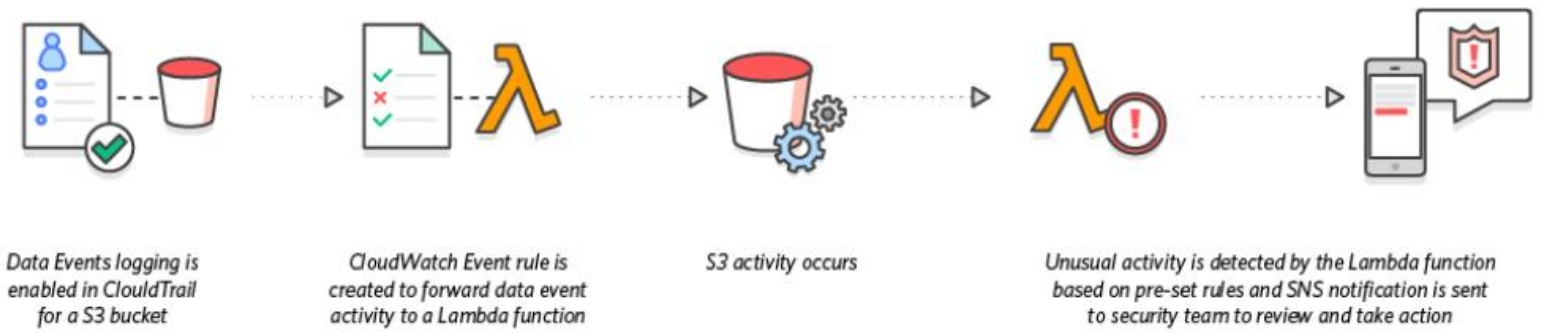
User name S3LambdaPutFunction

Resources Referenced (0)

8.Figure 12 - AWS CloudTrail compliance audit workflow

8.Figure 13 - AWS CloudTrail security analysis workflow

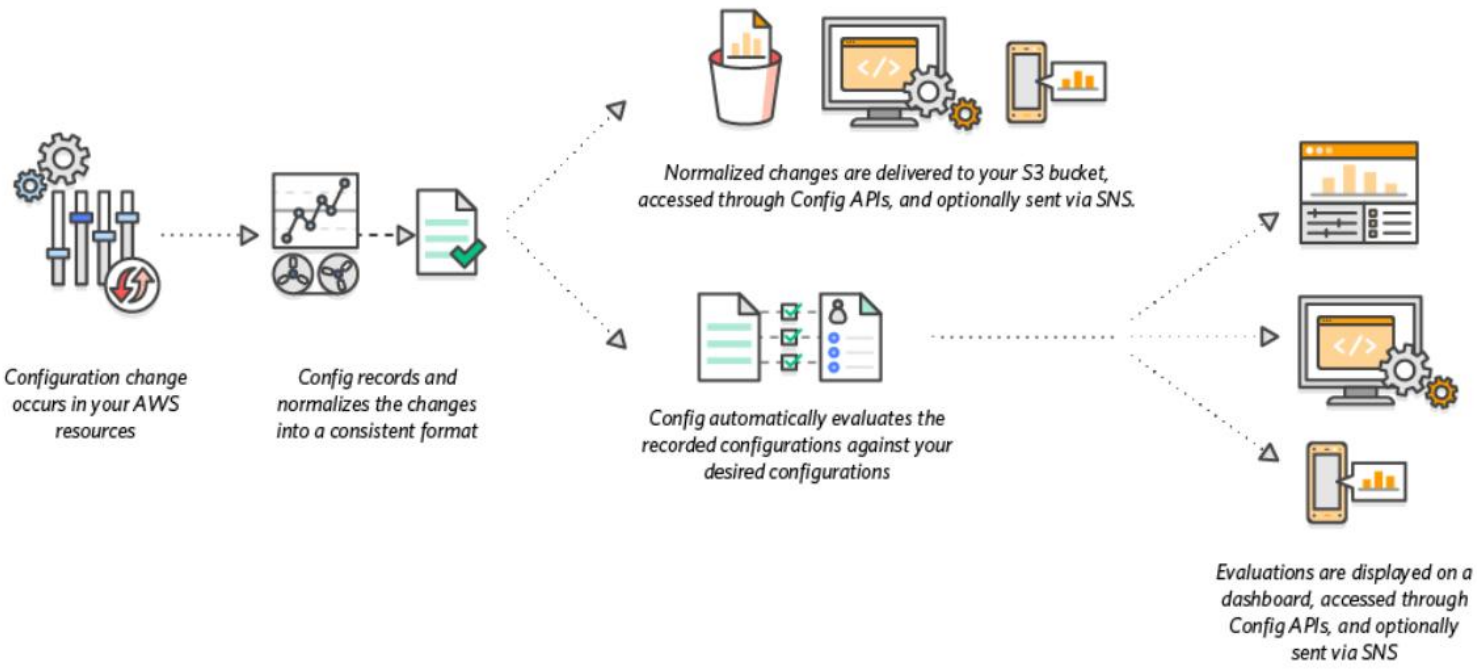
8.Figure 14 - AWS CloudTrail data exfiltration workflow



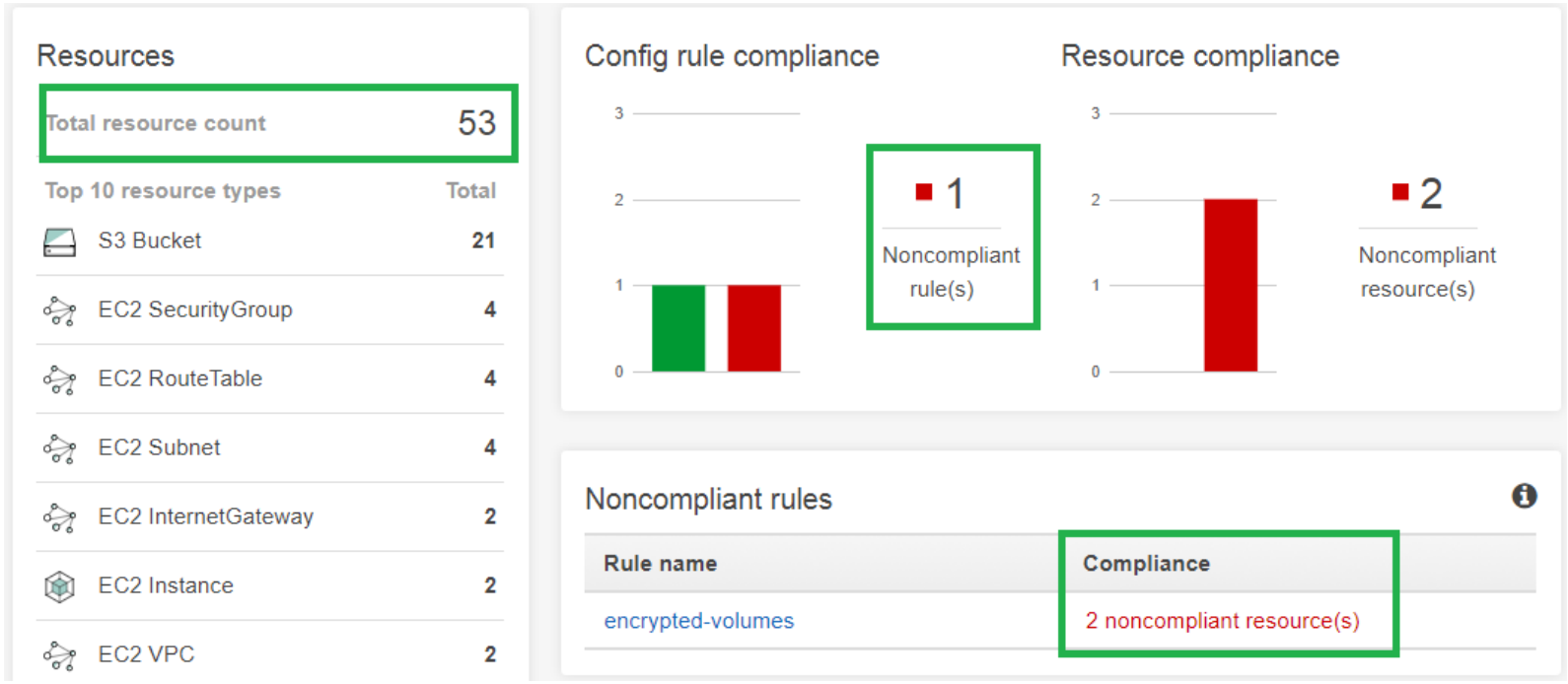
8.Figure 15 - AWS CloudTrail operational issue troubleshooting workflow

8.Figure 16 - AWS certifications and assurance programs

8.Figure 17 - AWS Config workflow



8.Figure 18 - AWS Config dashboard



REMOTE CLASSROOM INSTRUCTION

8.Figure 19 - AWS Service Catalog

Create and manage portfolios

Use portfolios to organize your products and distribute them to end users.

Add products

You can upload your line of business products or products you already own licenses to.

Manage user access

Decide who can access products and set policies on where and how users can launch them.

AWS Security Essentials – End Day 3

- **Wrap Up**
- **Tear Down AWS Resources**
- **Evaluations**
- **Email: philmatusiak@gmail.com**

onlc
Training Centers