

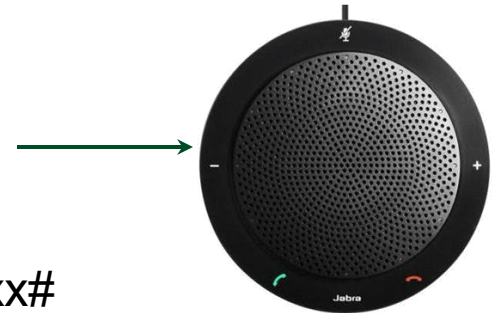
AWS Security Essentials

Instructor: Philip Matusiak

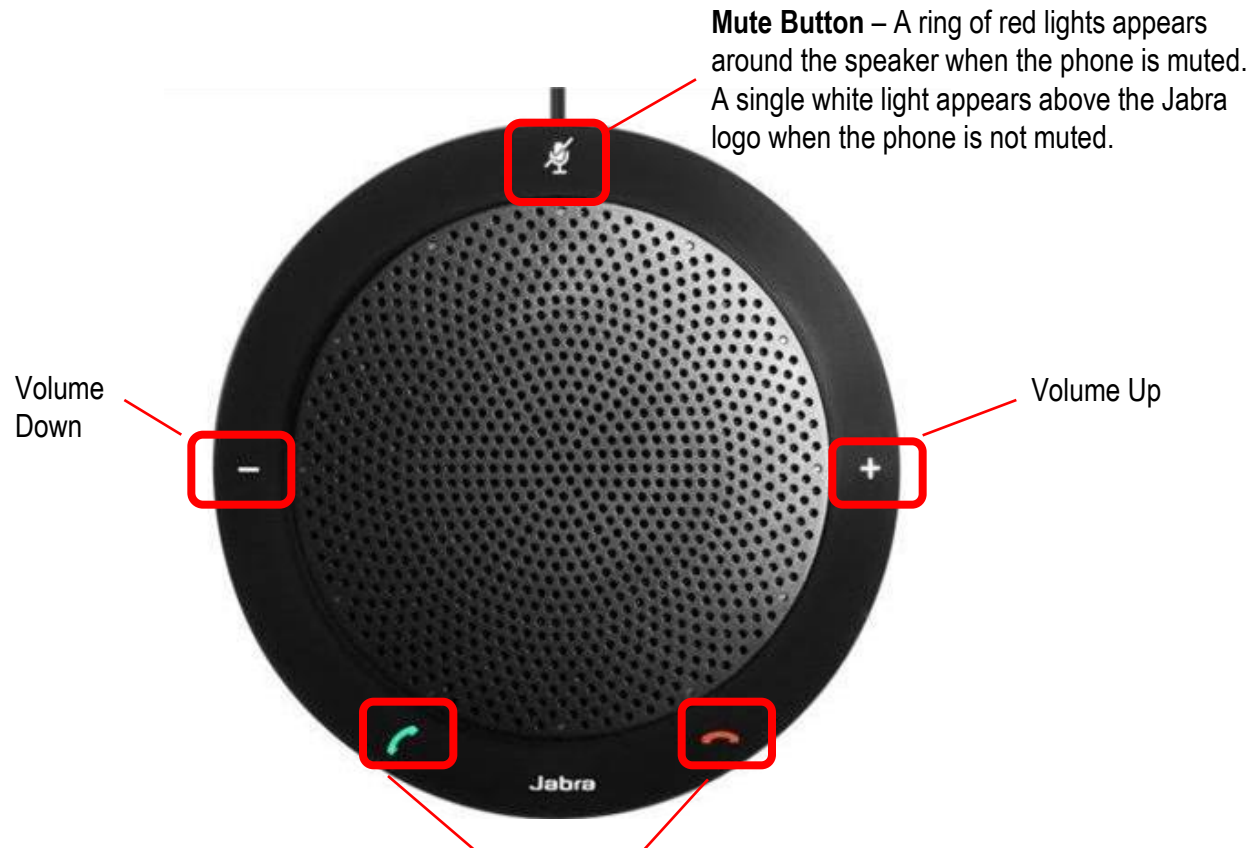
Email: philmatusiak@gmail.com



- 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



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.

Volume Down

Volume Up

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



Mastering AWS Security

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

By Albert Anthony

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

Customer

Accounts and Credentials



Amazon S3

VPC



Amazon EC2



Amazon RDS



Amazon Workspaces

AWS

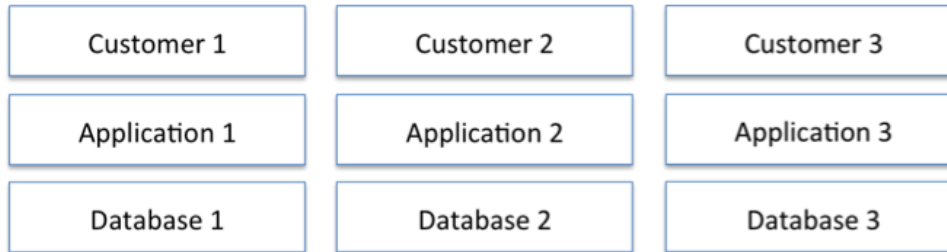
AWS Global Infrastructure

Cloud service models – IaaS, PaaS, and SaaS

User Application	IaaS Model	PaaS Model	SaaS Model
Application	Application	Application	Application
Data	Data	Data	Data
Runtime (Libraries)	Runtime (Libraries)	Runtime (Libraries)	Runtime (Libraries)
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Server	Server	Server	Server
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Multi-tenancy models

(A) Shared Nothing



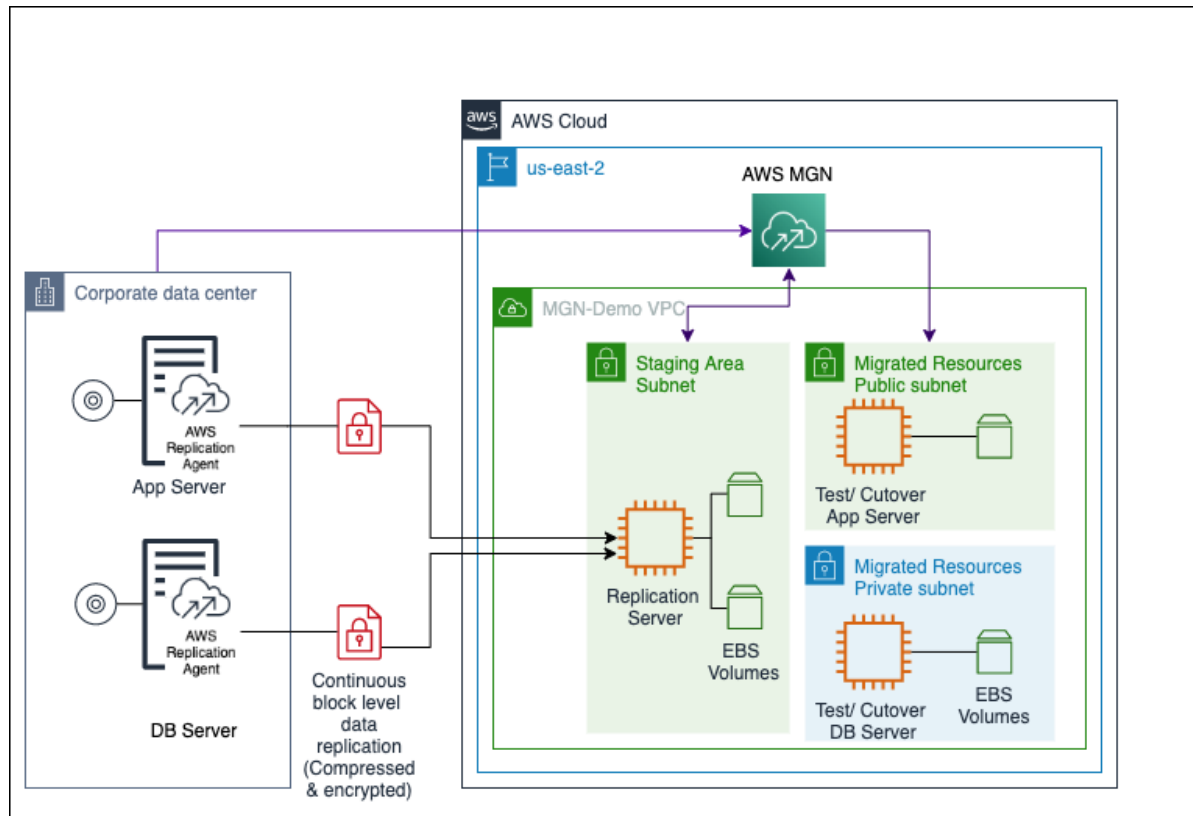
(B) Shared Application



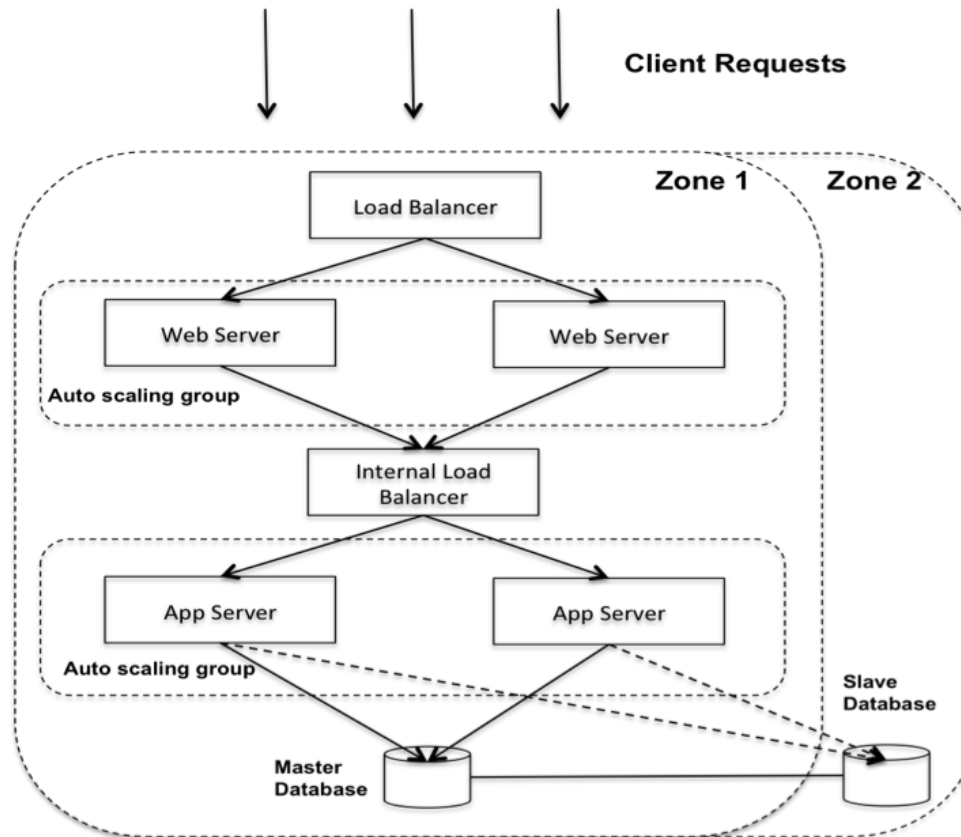
(C) Shared Everything



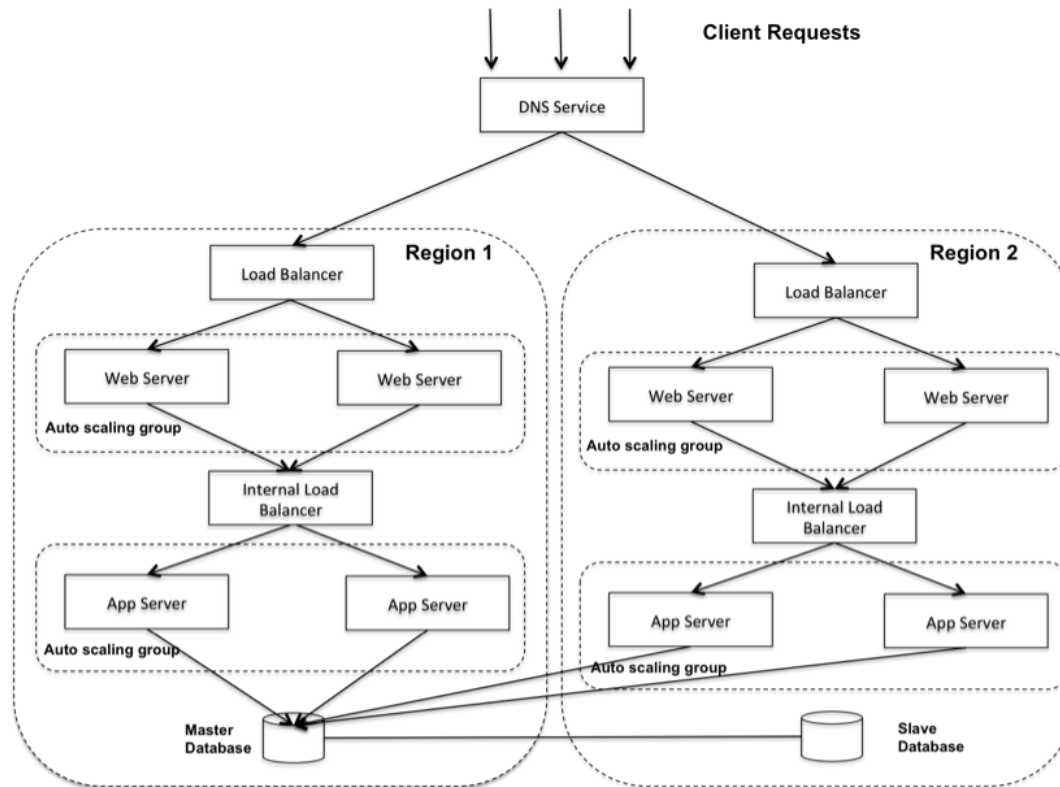
Migrating on-premise applications to the cloud



Cloud-based single tier architecture



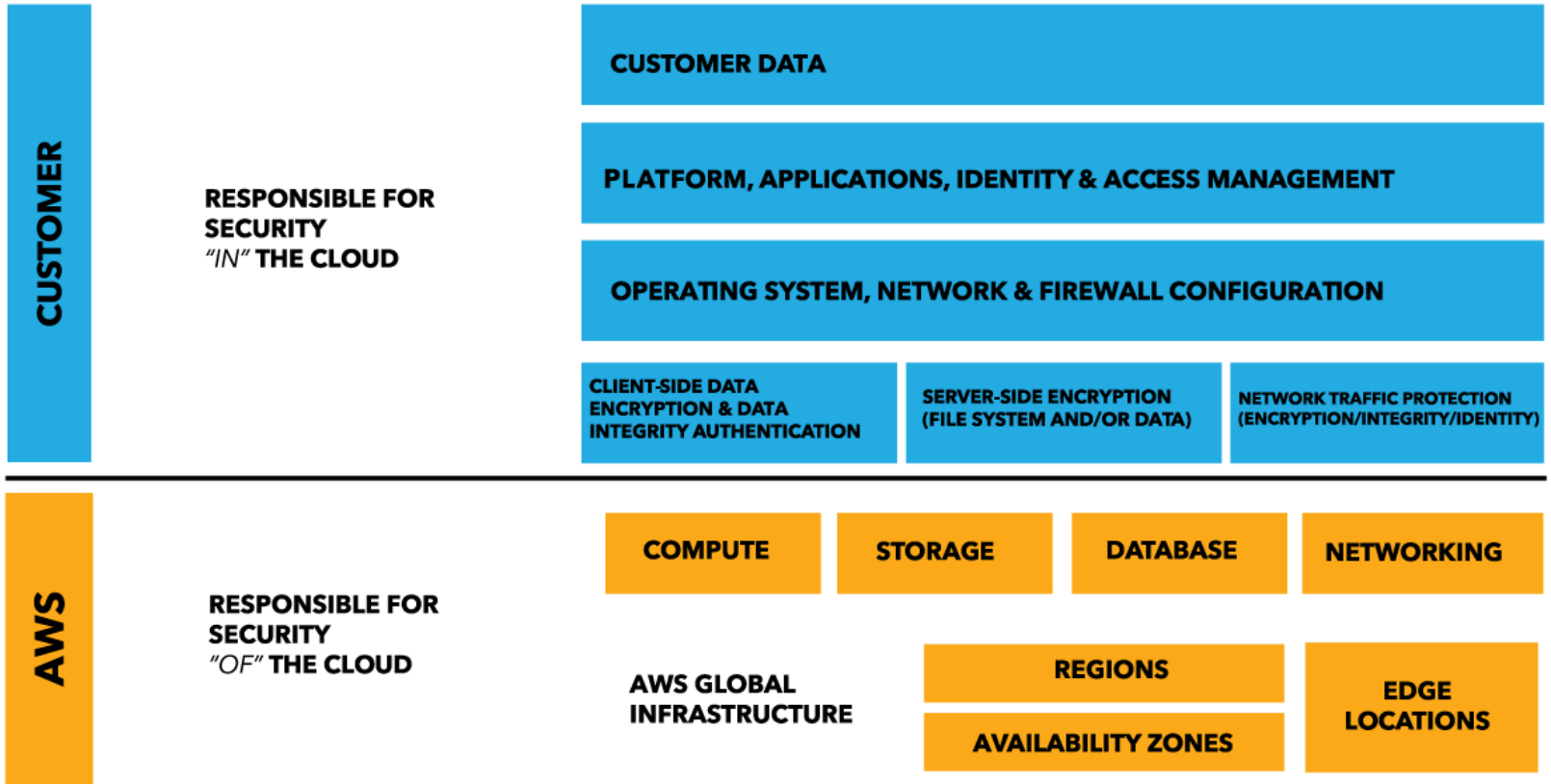
Cloud-based multitier architecture (high availability)



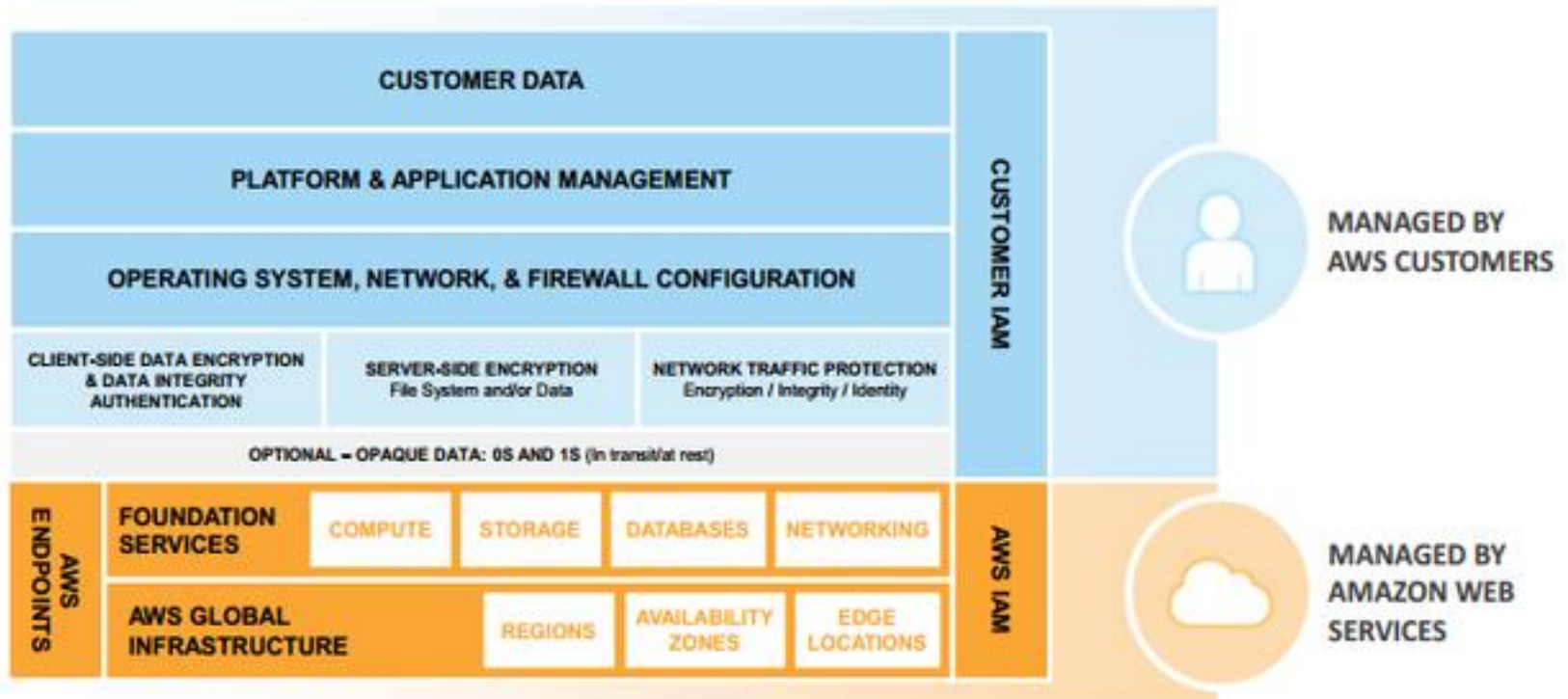
AWS Security Essentials - 1



1.1 AWS shared security responsibility model



1.2 Shared responsibility model for infrastructure services



1.3 AWS key pairs

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair
Choose an existing key pair
Create a new key pair
Proceed without a key pair

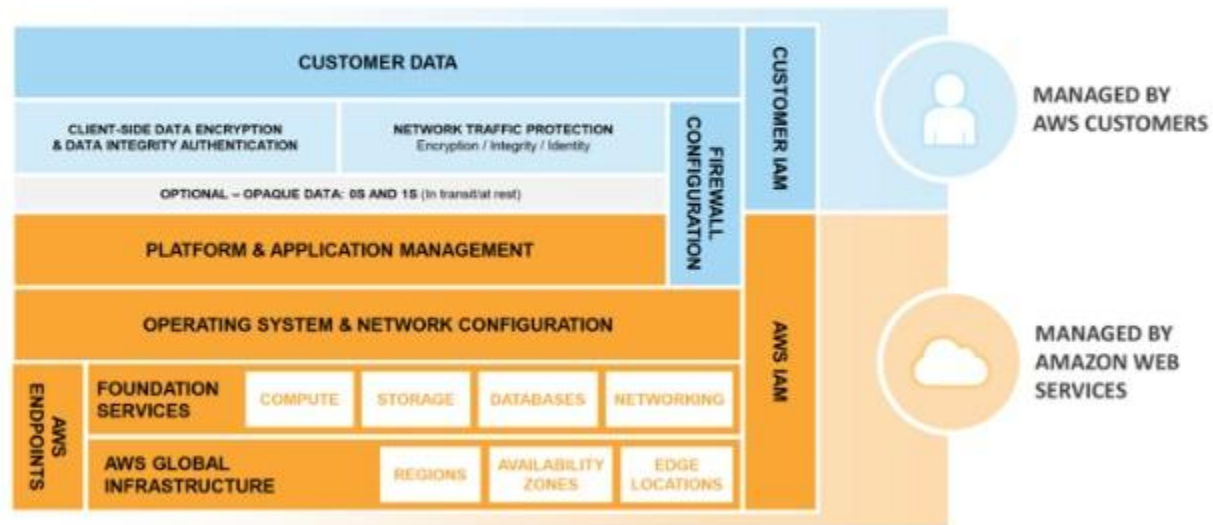
I acknowledge that I have access to the selected private key file (AppServer-KeyPair.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

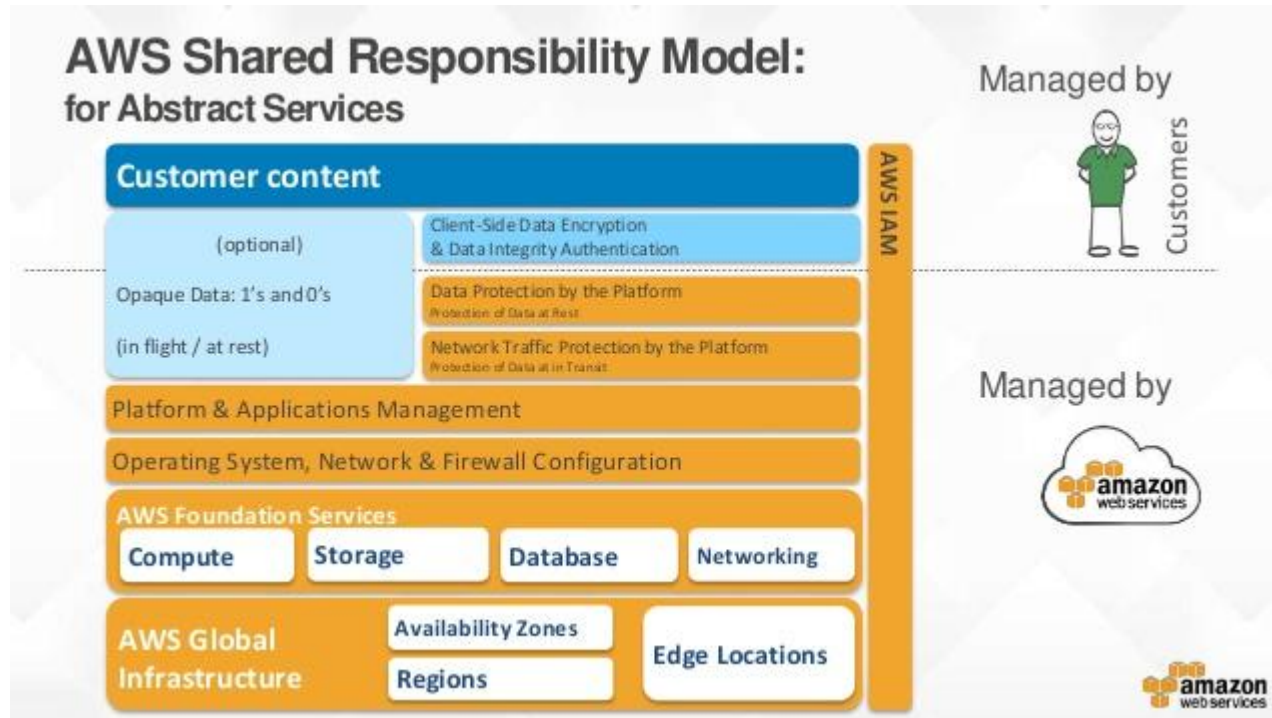
1.4 Shared responsibility model for container services

Shared Security Model: Container Services

Such as Amazon RDS and Amazon EMR



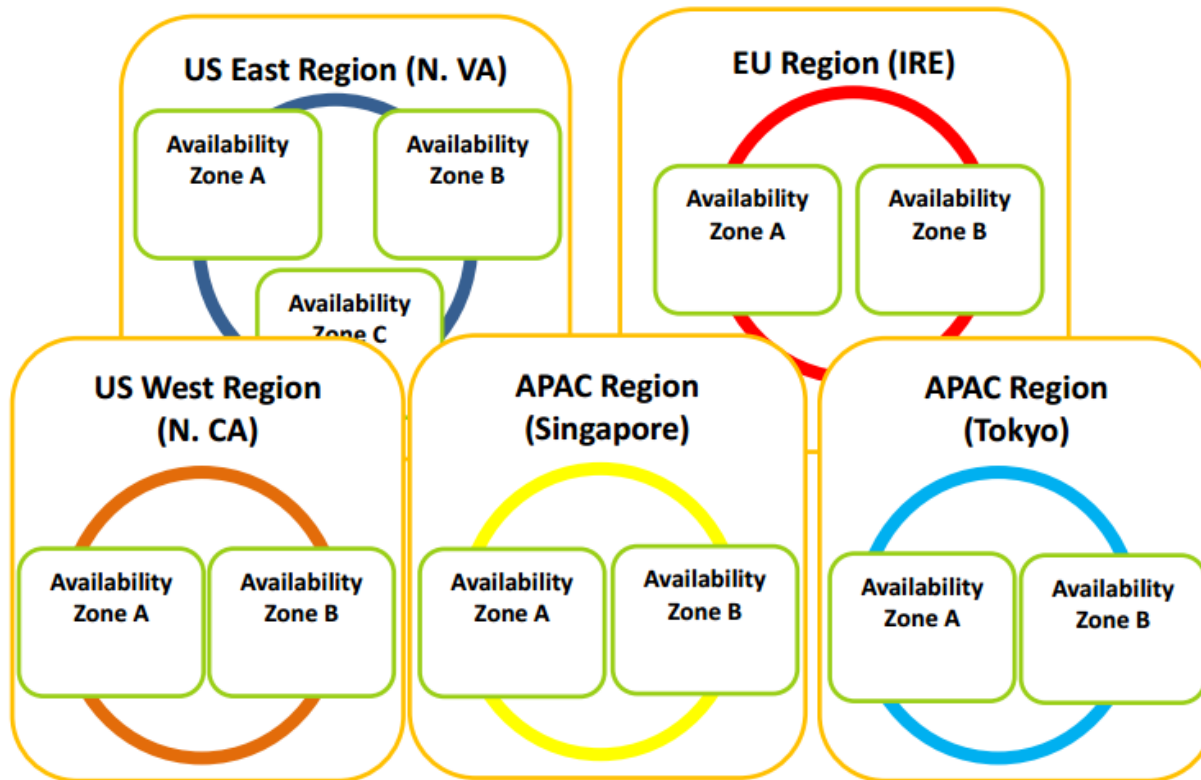
1.5 - Shared responsibility model for abstracted services



1.6 - AWS shared security model - AWS responsibilities



1.7 - AWS regions and availability zones



1.8 - AWS Service Health Dashboard



[Amazon Web Services](#) » Service Health Dashboard

Get a personalized view of AWS service health

Open the Personal Health Dashboard

Current Status - Oct 18, 2017 PDT

Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time, operational issue with one of our services that is not described below, please inform us by clicking on the "Contact Us" link to submit a service issue report. All dates and times are Pacific Time (PST/PDT).

North America			South America	Europe	Asia Pacific	Contact Us
Recent Events		Details				RSS
✓	AWS Direct Connect (Oregon)	[RESOLVED] Network Connectivity more ▾				
✓	AWS Internet Connectivity (Oregon)	[RESOLVED] Network Connectivity more ▾				
Remaining Services		Details				RSS
✓	Amazon API Gateway (Montreal)	Service is operating normally				

1.9 AWS shared security model - customer responsibilities



1.10 - AWS Trusted Advisor checks

Trusted Advisor Dashboard



Cost Optimization



0 ✓ 0 ⚠ 0 ❗

Performance



1 ✓ 0 ⚠ 0 ❗

Security



4 ✓ 0 ⚠ 1 ❗

Fault Tolerance



0 ✓ 0 ⚠ 0 ❗

Recommended Actions

▶ **Security Groups - Specific Ports Unrestricted**

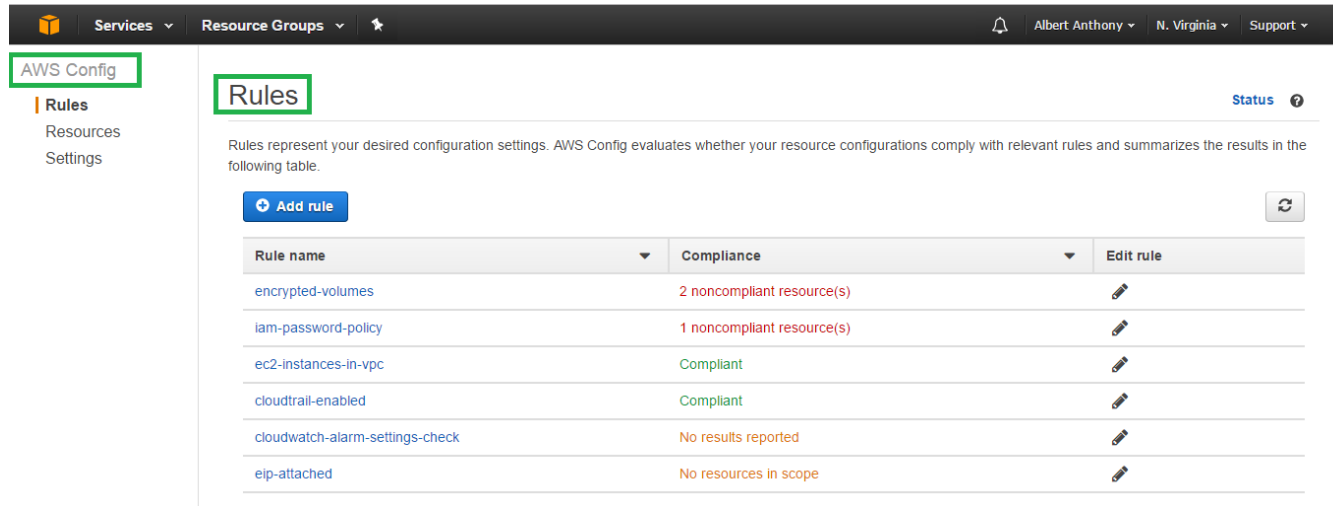
Refreshed: a few seconds ago



Checks security groups for rules that allow unrestricted access (0.0.0.0) to specific ports.

11 of 33 security group rules allow unrestricted access to a specific port.

1.11 - AWS Config Rules



The screenshot shows the AWS Config console interface. The top navigation bar includes 'Services', 'Resource Groups', and user information for 'Albert Anthony' in 'N. Virginia'. The left sidebar shows 'AWS Config' with sub-items 'Rules', 'Resources', and 'Settings'. The main content area is titled 'Rules' and contains a table of configuration rules. A blue 'Add rule' button and a refresh icon are visible above the table. The table lists six rules with their respective compliance statuses.

Rule name	Compliance	Edit rule
encrypted-volumes	2 noncompliant resource(s)	
iam-password-policy	1 noncompliant resource(s)	
ec2-instances-in-vpc	Compliant	
cloudtrail-enabled	Compliant	
cloudwatch-alarm-settings-check	No results reported	
eip-attached	No resources in scope	

AWS Security Essentials - 2



2.1 - AWS console login

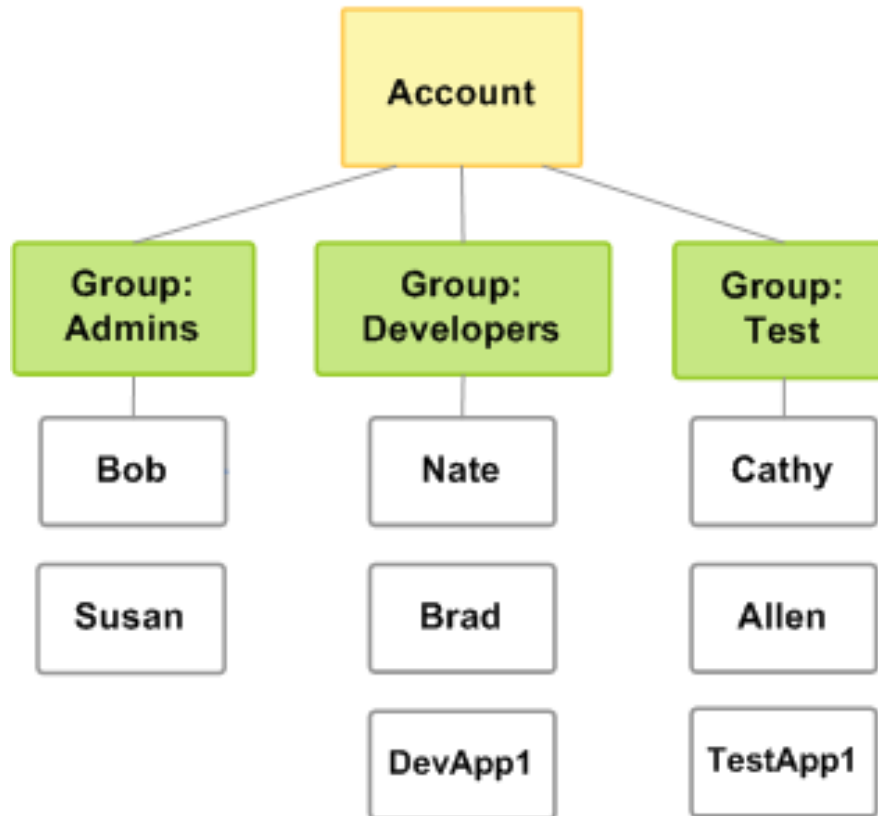
The screenshot shows the AWS console login page. At the top left is the Amazon Web Services logo. The main content area is split into two sections. On the left is the login form with three input fields: 'Account:', 'User Name:', and 'Password:'. Below these fields is a blue 'Sign In' button and a link for 'Sign in using root account credentials'. A note states 'MFA users, enter your code on the next screen.' On the right is a promotional banner for the 'AWS SUMMIT San Francisco'. The banner features the text 'View the latest product announcements from the AWS Summit – San Francisco' and a 'LEARN MORE >' button. At the bottom of the page, there is a language dropdown menu set to 'English' and a footer with the text 'Terms of Use Privacy Policy © 1998-2017, Amazon Web Services, Inc. or its affiliates.'

2.2 - AWS IAM users

The screenshot displays the AWS IAM console interface. At the top, the AWS logo is on the left, and the user profile 'Albert' and region 'Global' are on the right. The left-hand navigation menu includes 'Dashboard', 'Groups', 'Users' (highlighted), 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Credential report', and 'Encryption keys'. The main content area features a search bar for users and a table of user details.

<input type="checkbox"/>	User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/>	WWUser1	WWInternational	None	44 days	None
<input type="checkbox"/>	Test-Allen	WWInternational	None	44 days	None
<input type="checkbox"/>	sliamuser	IAM-View-Only-Users	⚠ 150 days	150 days	130 days
<input type="checkbox"/>	SL-S3-EC2-...	S3-ReadOnly-Users	✅ 53 days	None	53 days
<input type="checkbox"/>	SL-IAM-Us...	AdminGroup	✅ 45 days	None	39 days
<input type="checkbox"/>	SL-IAM-LAB	None	✅ 3 days	3 days	None
<input type="checkbox"/>	SL-CLI-User	None	✅ 3 days	None	None

2.3 - AWS IAM groups



2.4 - AWS Service Role types

Create role



Select type of trusted entity

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

Choose the service that will use this role

API Gateway	Data Pipeline	IoT	Service Catalog
Auto Scaling	Directory Service	Lambda	Storage Gateway
Batch	DynamoDB	Lex	

* Required

Cancel

Next: Permissions

2.5 - AWS SAML Role

Create role

1 Trust 2 Permissions 3 Review

AWS service

Another AWS account

Web identity

SAML
Saml 2.0 federation

Allows users that are federated with SAML 2.0 to assume this role to perform actions in your account. [Learn more](#)

Choose a SAML 2.0 provider

If you're creating a role for API access, choose an Attribute and then type a Value to include in the role. This restricts access to users with the specified attributes.

SAML provider [Create new provider](#) [Refresh](#)

Allow programmatic access only

Allow programmatic and AWS Management Console access

* Required

Cancel [Next: Permissions](#)

2.6 - AWS cross-account access roles

Create role

1 Trust 2 Permissions 3 Review

AWS service Another AWS account Web identity SAML
Saml 2.0 federation

Allows entities in other accounts to perform actions in this account. [Learn more](#)
Specify accounts that can use this role

Account ID* ⓘ

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

* Required Cancel Next: Permissions

2.7 - AWS identity provider access roles

Create role



Select type of trusted entity

Allows users federated by the specified external web identity or OpenID Connect (OIDC) provider to assume this role to perform actions in your account. [Learn more](#)

Choose a web identity provider

Identity provider: [Create new provider](#) | [Refresh](#)

* Required

Cancel

Next: Permissions

2.8 - AWS account root user recommendations

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

IAM Resources

Users: 26

Roles: 44

Groups: 12

Identity Providers: 0









Customer Managed Policies: 32

Security Status

5 out of 5 complete.

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions

2.9 - AWS job functions policies

<input type="checkbox"/>	Policy name ▾	Type	Attachments ▾	Description
<input type="checkbox"/>	▶  AdministratorAccess	Job function	4	Provides full access to AWS services and resources.
<input type="checkbox"/>	▶  Billing	Job function	2	Grants permissions for billing and cost management. This includ
<input type="checkbox"/>	▶  DatabaseAdministrator	Job function	0	Grants full access permissions to AWS services and actions req
<input type="checkbox"/>	▶  DataScientist	Job function	0	Grants permissions to AWS data analytics services.
<input type="checkbox"/>	▶  NetworkAdministrator	Job function	0	Grants full access permissions to AWS services and actions req
<input type="checkbox"/>	▶  PowerUserAccess	Job function	0	Provides full access to AWS services and resources, but does n
<input type="checkbox"/>	▶  SecurityAudit	Job function	0	The security audit template grants access to read security config
<input type="checkbox"/>	▶  SupportUser	Job function	0	This policy grants permissions to troubleshoot and resolve issue

2.10 - AWS Create Policy options

Create Policy

Step 1 : Create Policy

Step 2 : Set Permissions

Step 3 : Review Policy

Create Policy

A policy is a document that formally states one or more permissions. Create a policy by copying an AWS Managed Policy, using the Policy Generator, or typing your own custom policy.

Copy an AWS Managed Policy

Start with an AWS Managed Policy, then customize it to fit your needs.

Select

Policy Generator

Use the policy generator to select services and actions from a list. The policy generator uses your selections to create a policy.

Select

Create Your Own Policy

Use the policy editor to type or paste in your own policy.

Select



2.11 - AWS IAM Policy Simulator

IAM Policy Simulator Mode : Existing Policies Albert Anthony

Policies [Back](#)

Selected group **IAMAdministrator**

IAM Policies

Filter

IAMFullAccess

Policy Simulator

AWS Identity a... 2 Action(s) sele... [Select All](#) [Deselect All](#) [Reset Contexts](#) [Clear Results](#) [Run Simulation](#)

▶ **Global Settings**

Action Settings and Results [5 actions selected. 0 actions not simulated. 2 actions allowed. 3 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
▶ Amazon SQS	DeleteMessage	not required	*	denied Implicitly denied (no matchi...
▶ Amazon SQS	AddPermission	not required	*	denied Implicitly denied (no matchi...
▶ Amazon SQS	CreateQueue	not required	*	denied Implicitly denied (no matchi...
▶ AWS Identity and Acces...	CreateGroup	group	*	allowed 1 matching statements.
▶ AWS Identity and Acces...	CreatePolicy	policy	group	allowed 1 matching statements.

Resource Policies

2.12 - AWS IAM Access Advisor

Services ▾ Resource Groups ▾ ☆

Albert Anthony ▾ Global ▾ Support ▾

Search IAM

Users > Albert

Summary

User ARN `arn:aws:iam::902891488394:user/Albert`

Path `/`

Creation time 2016-08-25 10:45 UTC+0530

Permissions Groups (1) Security credentials **Access Advisor**

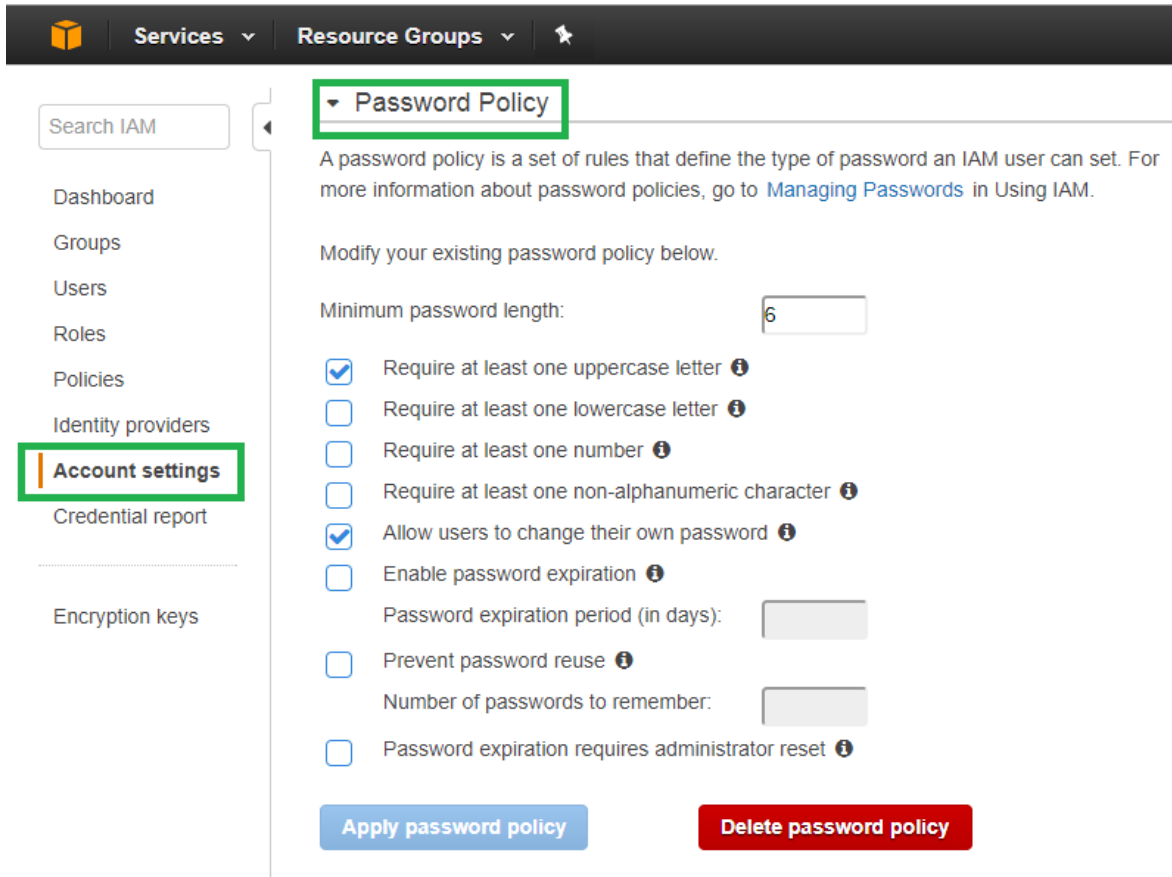
Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. [Learn more](#)

Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015 [Learn more](#)

Filter: No filter ▾ Search Showing 73 results

Service Name ↕	Policies Granting Permissions	Last Accessed ▾
AWS Identity and Access Management	AdministratorAccess	144 days ago
Amazon S3	AdministratorAccess	145 days ago
Amazon EC2	AdministratorAccess	162 days ago
Elastic Load Balancing	AdministratorAccess	314 days ago

2.13 - AWS IAM Password Policy



The screenshot shows the AWS IAM console interface. At the top, there is a navigation bar with 'Services' and 'Resource Groups' dropdown menus. On the left, a sidebar contains navigation links: 'Search IAM', 'Dashboard', 'Groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings' (highlighted with a green box), 'Credential report', and 'Encryption keys'. The main content area is titled 'Password Policy' (also highlighted with a green box). Below the title, there is a descriptive paragraph: '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.' Below this, it says 'Modify your existing password policy below.' The configuration options include: 'Minimum password length:' with a text input field containing '6'; a list of checkboxes for password requirements: 'Require at least one uppercase letter' (checked), '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' (checked), 'Enable password expiration', 'Prevent password reuse', and 'Password expiration requires administrator reset'. There are also two text input fields for 'Password expiration period (in days):' and 'Number of passwords to remember:'. At the bottom, there are two buttons: 'Apply password policy' (blue) and 'Delete password policy' (red).

2.14 - AWS Security Credentials

Services ▾ Resource Groups ▾

Albert Anthony ▾ Global ▾ Support ▾

Search IAM

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

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management, see [AWS Security Credentials](#) in AWS General Reference.

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- + Password
- + Multi-Factor Authentication (MFA)
- + Access Keys (Access Key ID and Secret Access Key)
- + CloudFront Key Pairs
- + X.509 Certificates
- Account Identifiers

You use your 12-digit account ID to reference your account programmatically and in other contexts. You use your canonical user ID to configure [Amazon S3 access control lists \(ACLs\)](#).

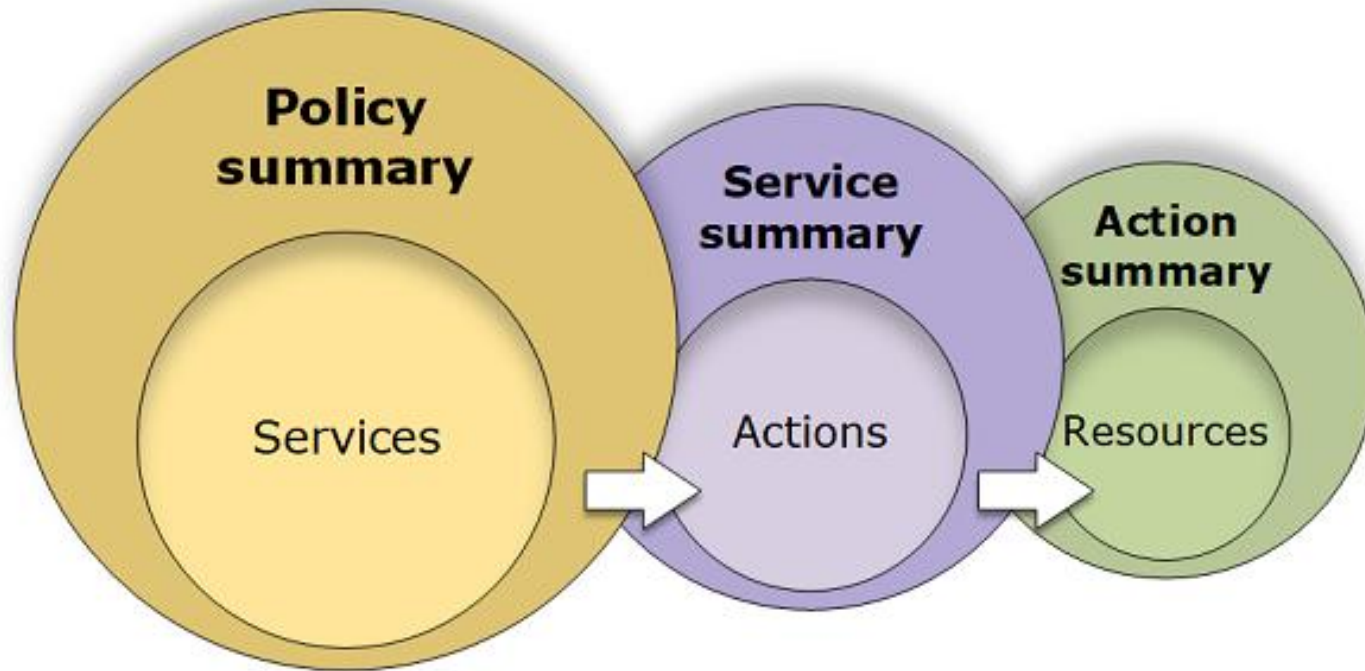
AWS Account ID:

Canonical User ID:

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

Console

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

AWS Security Essentials - 3



3. Figure 1 - AWS VPC components

The screenshot displays the AWS VPC Dashboard interface. At the top, there is a navigation bar with 'Services', 'Resource Groups', and user information 'Albert Anthony' in the 'Mumbai' region. The left sidebar contains a 'VPC Dashboard' menu with categories like 'Virtual Private Cloud', 'Your VPCs', 'Subnets', 'Route Tables', 'Internet Gateways', 'Egress Only Internet Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Endpoints', 'NAT Gateways', 'Peering Connections', 'Security', and 'Network ACLs'. The main content area is titled 'Resources' and includes buttons for 'Start VPC Wizard' and 'Launch EC2 Instances'. A note states: 'Note: Your Instances will launch in the region.' Below this, a section titled 'You are using the following Amazon VPC resources in the region:' lists various resources, with a green box highlighting the following items:

2 VPCs	2 Internet Gateways
0 Egress-only Internet Gateways	4 Subnets
4 Route Tables	2 Network ACLs
1 Elastic IP	0 VPC Peering Connections
0 Endpoints	0 Nat Gateways
4 Security Groups	1 Running Instance
0 VPN Connections	0 Virtual Private Gateways
0 Customer Gateways	

Below the resources list is a 'VPN Connections' section with a description: '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.' and a 'Create VPN Connection' button. To the right, the 'Service Health' section shows a table with two entries:

Current Status	Details
✔ Amazon VPC - Asia Pacific (Mumbai)	Service is operating normally
✔ Amazon EC2 - Asia Pacific (Mumbai)	Service is operating normally

Below the service health table is a link to 'View complete service health details'. Further down, the 'Additional Information' section includes links for 'VPC Documentation', 'All VPC Resources', 'Forums', and 'Report an Issue'.

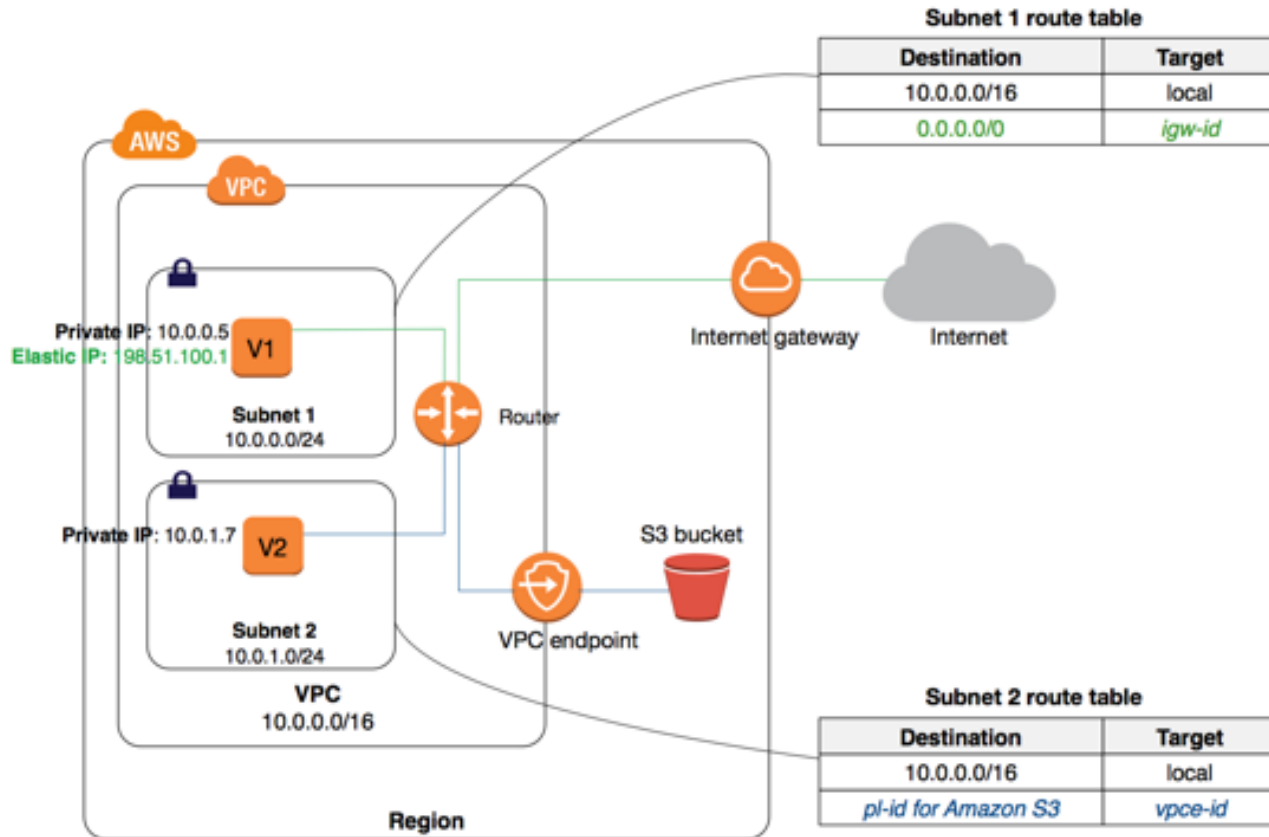
3. Figure 2 - AWS VPC route tables

The screenshot displays the AWS Management Console interface for VPC Route Tables. The left sidebar shows navigation options like 'Virtual Private Cloud', 'Route Tables', and 'Internet Gateways'. The main content area shows a list of route tables, with the selected route table 'rtb-59331530' expanded to show its routes. The 'Routes' tab is highlighted with a green box, and the route table 'rtb-59331530' is also highlighted with a green box in the list above.

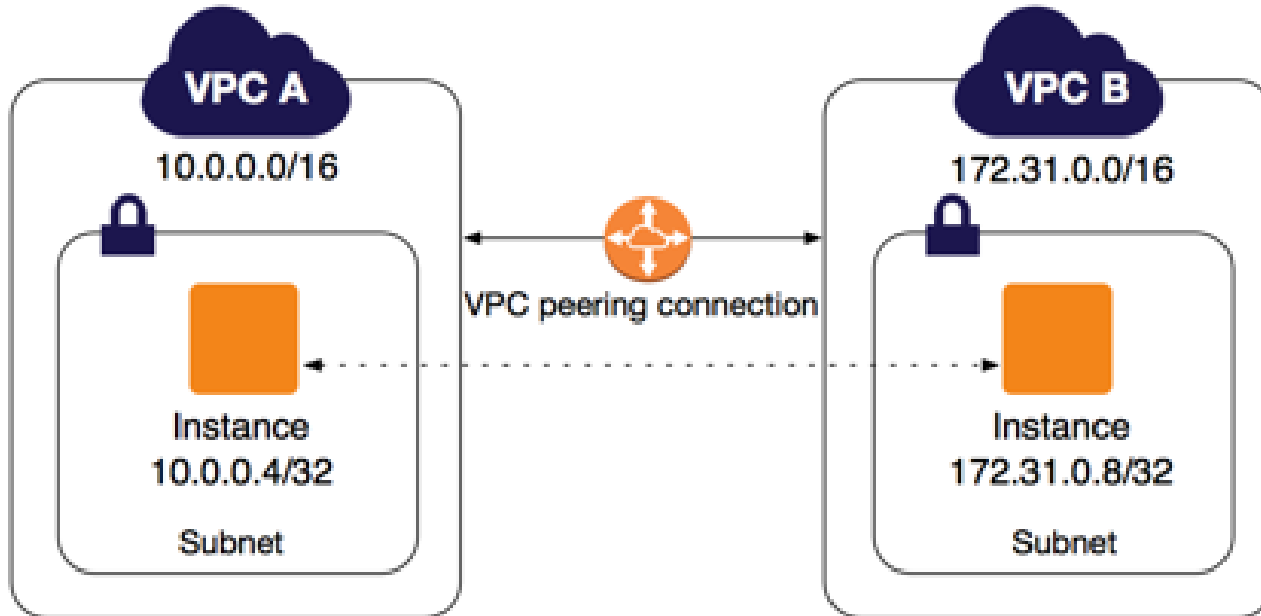
Name	Route Table ID	Explicitly Associat	Main	VPC
NAT Route Table	rtb-0b311762	0 Subnets	No	vpc-0466956d Default VPC
Custom Route Table	rtb-063e186f	1 Subnet	No	vpc-3cd49d55 My-Lab-VPC
	rtb-9e50a2f7	0 Subnets	Yes	vpc-0466956d Default VPC
	rtb-59331530	1 Subnet	Yes	vpc-3cd49d55 My-Lab-VPC

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-a50e9ecc	Active	No

3. Figure 3 - AWS VPC endpoints



3. Figure 4 - AWS VPC peering



3. Figure 5 - AWS VPC wizard

Services ▾ Resource Groups ▾

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

This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your data center - effectively extending your data center to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.

Creates:

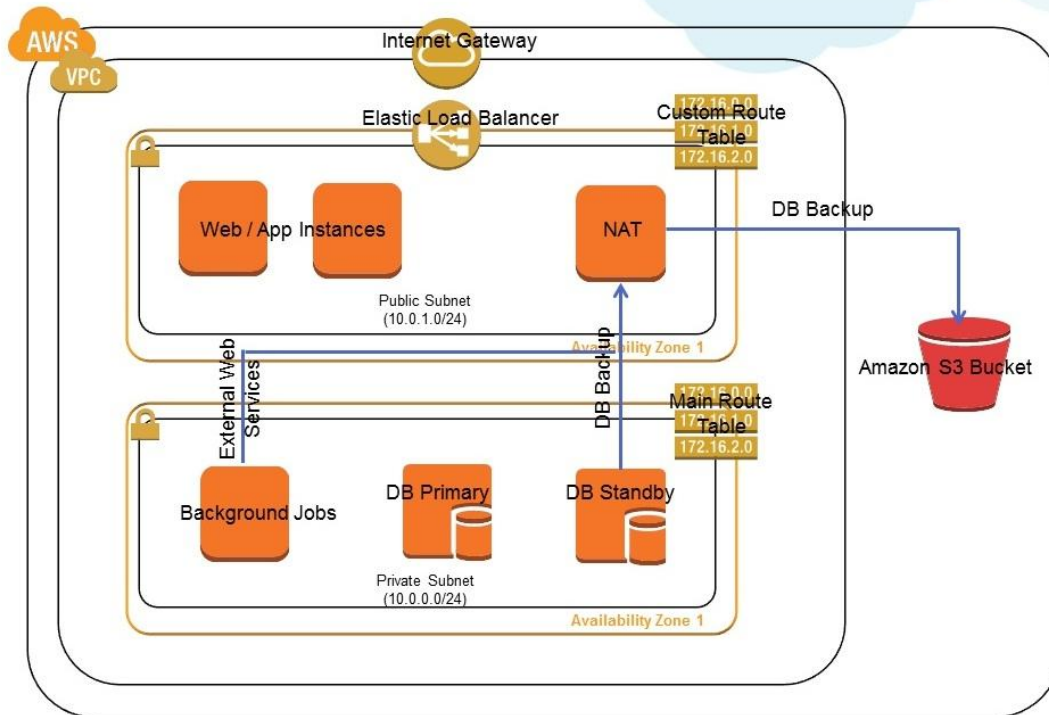
A /16 network with two /24 subnets. One subnet is directly connected to the Internet while the other subnet is connected to your corporate network via IPsec VPN tunnel. (VPN charges apply.)

Select

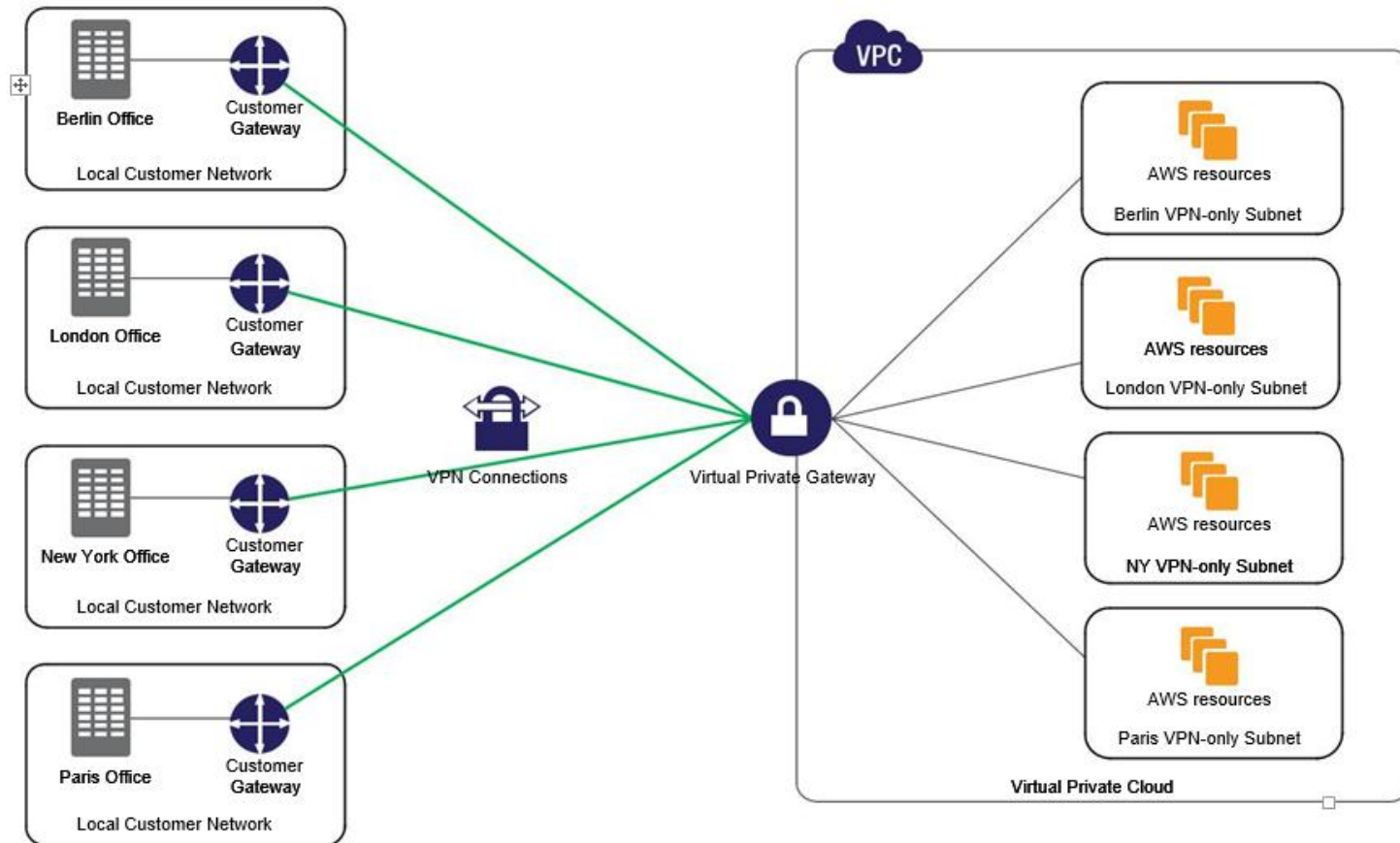
The diagram illustrates the network architecture. At the top, a cloud icon represents the Internet, with services like S3, DynamoDB, SNS, and SQS listed. Below it is the Amazon Virtual Private Cloud (VPC), which contains two subnets: a Public Subnet and a Private Subnet. The Public Subnet is connected to the Internet. The Private Subnet is connected to a Corporate Data Center via a VPN tunnel. The Corporate Data Center is represented by a server rack icon.

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

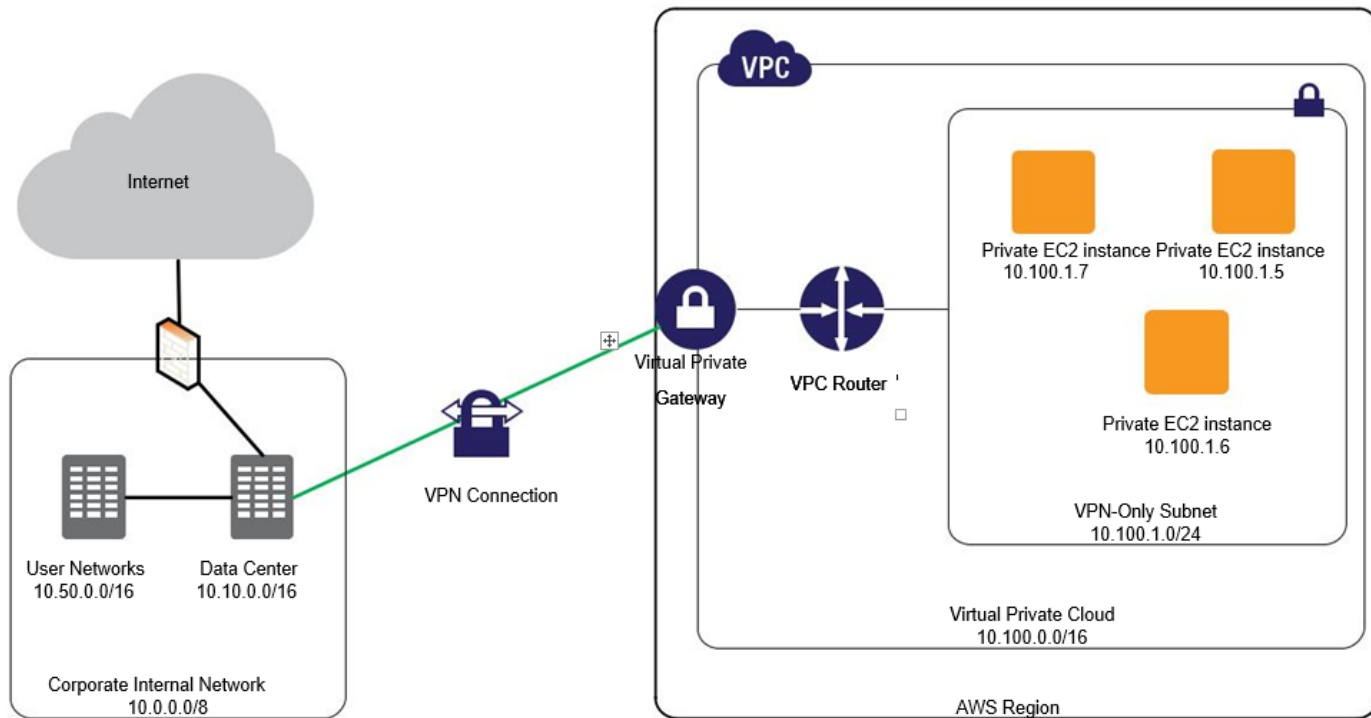
Public and Private Subnets in a VPC



3. Figure 7 - AWS VPC for connecting branch offices



3. Figure 8 - AWS VPC extend corporate data center



3. Figure 9 - AWS VPC security groups

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

Create Security Group Security Group Actions

Filter All security groups Search Security Groups and t X

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input checked="" type="checkbox"/>	WebServer-SG	sg-9ce83cec	WebServer-SG	vpc-1f88c166 SL-VPC-Lab	Security Group for Web Servers
<input type="checkbox"/>	DBServer-SG	sg-0dee3a7d	DBServer-SG	vpc-1f88c166 SL-VPC-Lab	Database Server Security Group
<input type="checkbox"/>	Albert-SG	sg-631cc813	Albert-SG	vpc-1f88c166 SL-VPC-Lab	Albert-SG
<input type="checkbox"/>		sg-5337d422	default	vpc-ac13b4d5 My-SL-Lab-...	default VPC security group

sg-9ce83cec | WebServer-SG

Summary Inbound Rules Outbound Rules Tags

Edit

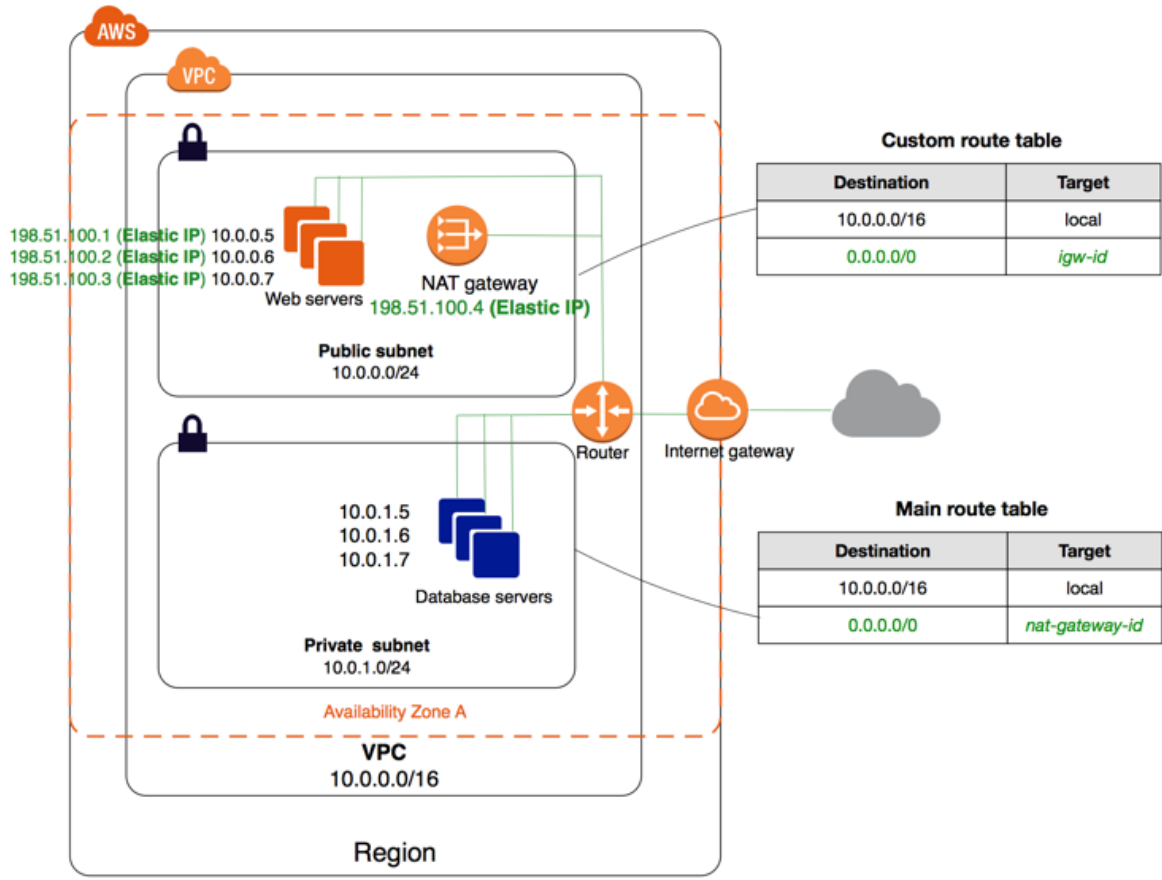
Type	Protocol	Port Range	Source
HTTP (80)	TCP (6)	80	0.0.0.0/0
SSH (22)	TCP (6)	22	0.0.0.0/0
HTTPS (443)	TCP (6)	443	0.0.0.0/0

3. Figure 10 - AWS VPC NACL

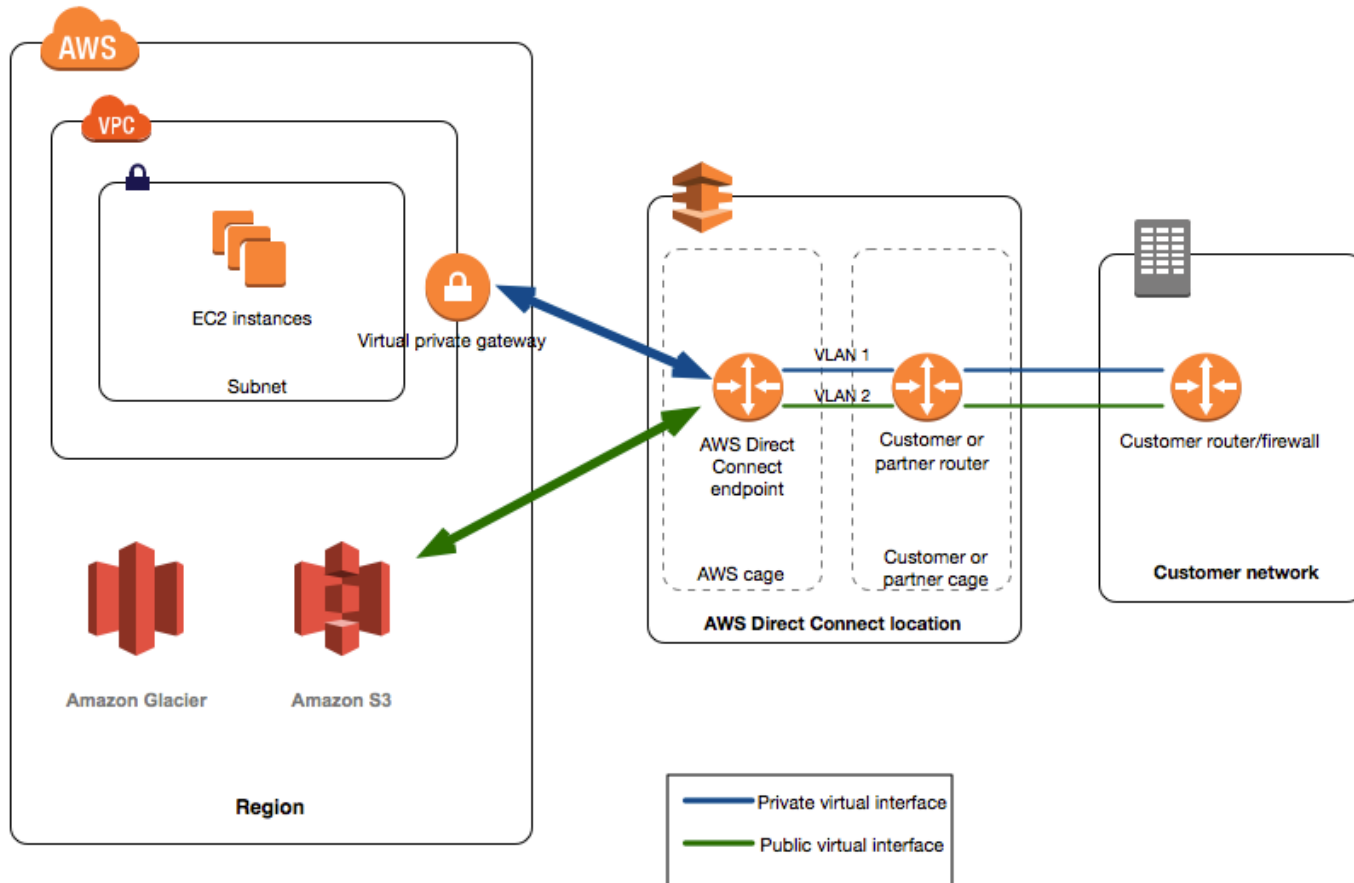
The screenshot shows the AWS VPC console interface. On the left sidebar, the 'Security' section is expanded, and 'Network ACLs' is highlighted. The main content area displays a list of Network ACLs. The 'SL-Public-NACL' (ID: ac1-4bbf4133) is selected and highlighted with a green box. Below the list, the configuration for 'ac1-4bbf4133 | SL-Public-NACL' is shown, with the 'Inbound Rules' tab selected and highlighted. A note states: 'Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.' Below this note is an 'Edit' button and a 'View: All rules' dropdown. A table lists the inbound rules:

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

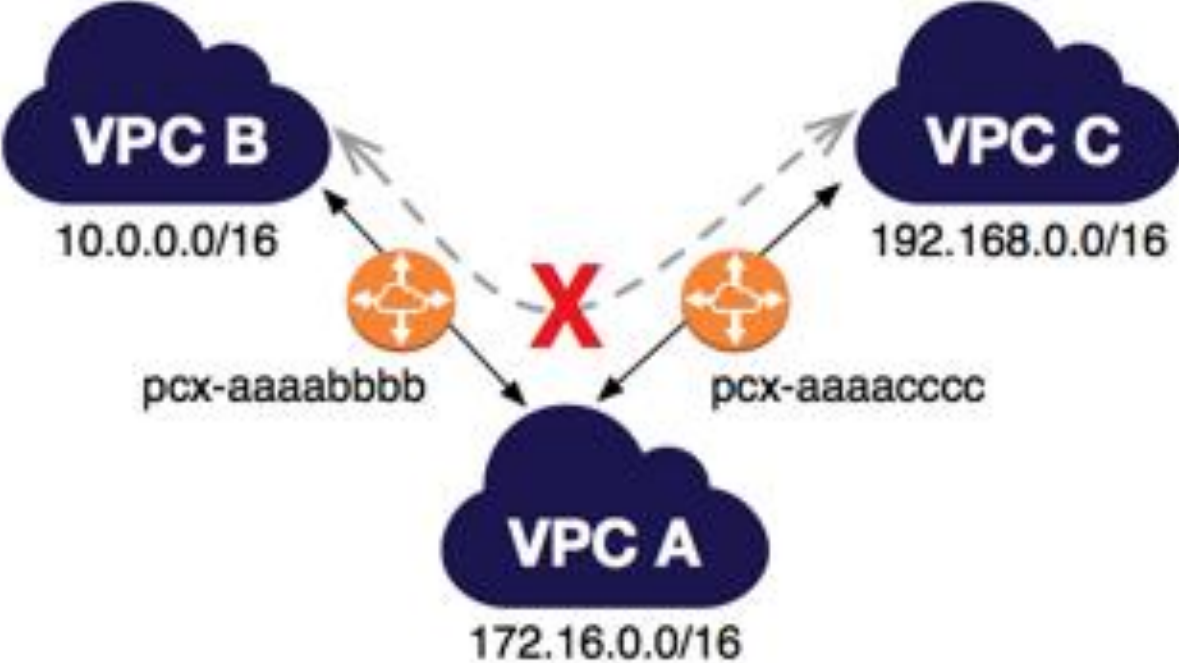
3. Figure 11 - AWS custom VPC



3. Figure 12 - AWS direct connect



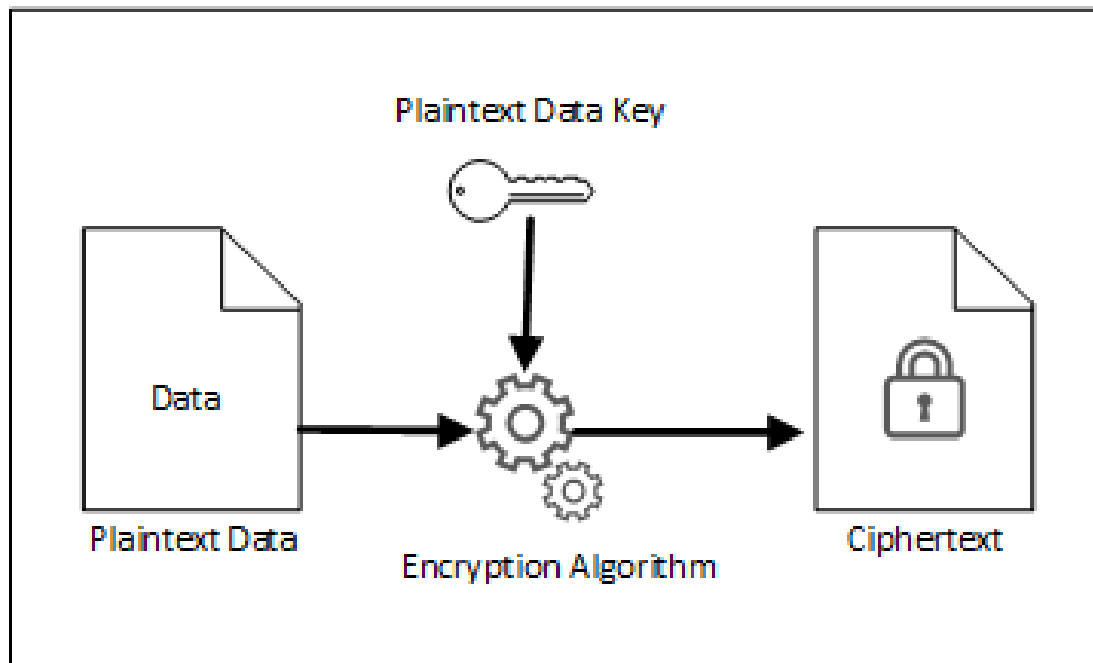
3. Figure 13 - AWS VPC Transitive Peering



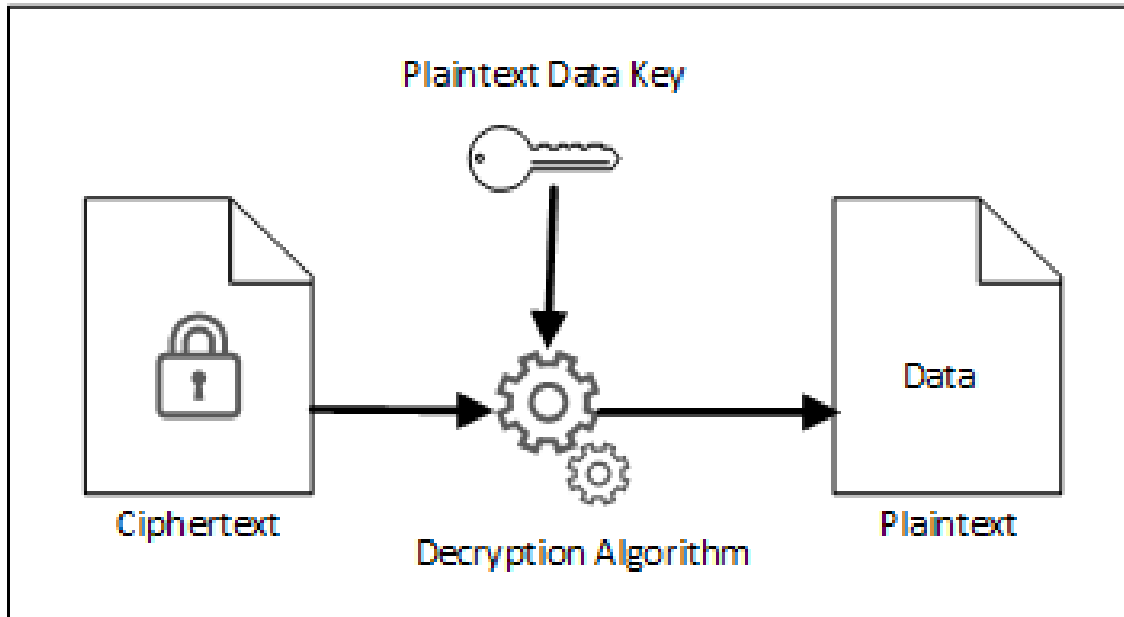
AWS Security Essentials - 4



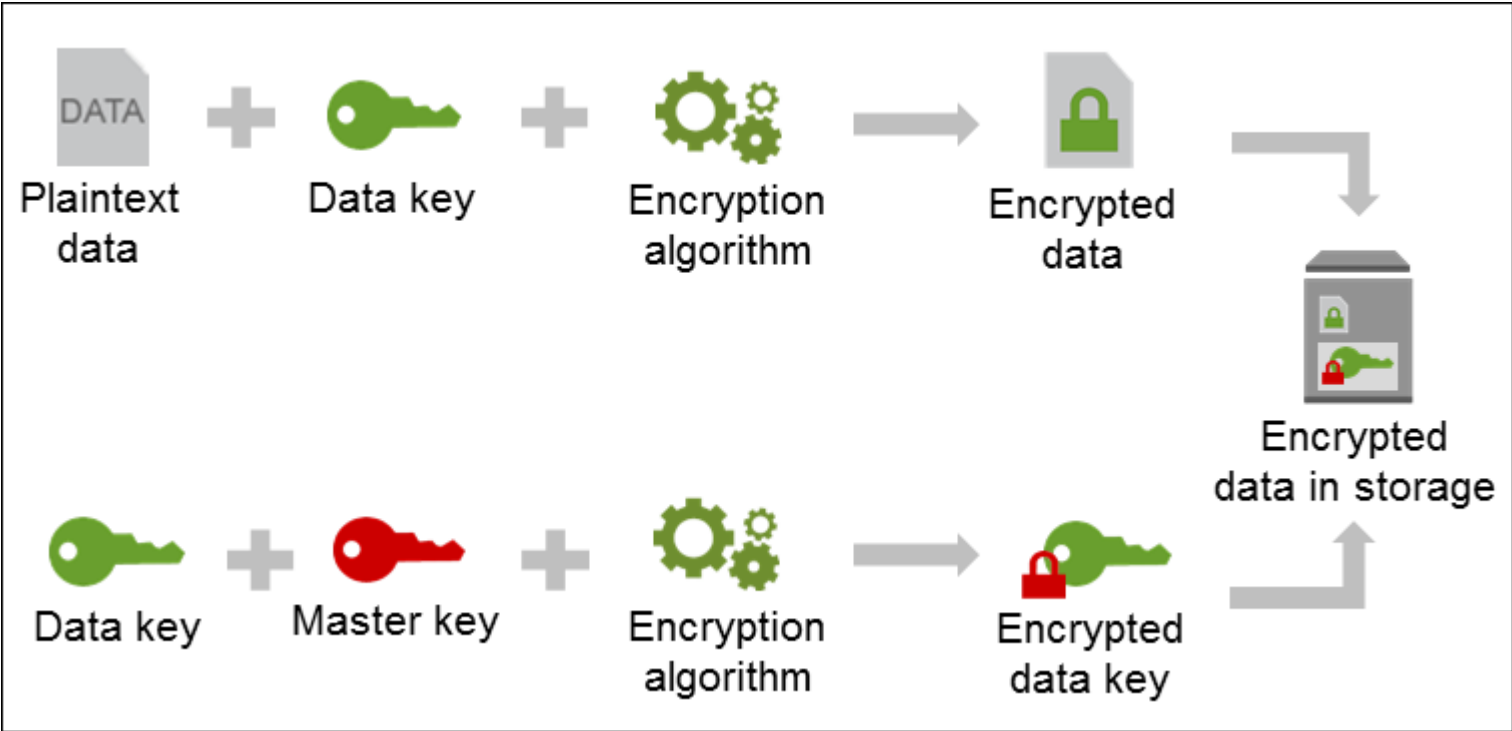
4. Figure 1 - AWS encryption workflow



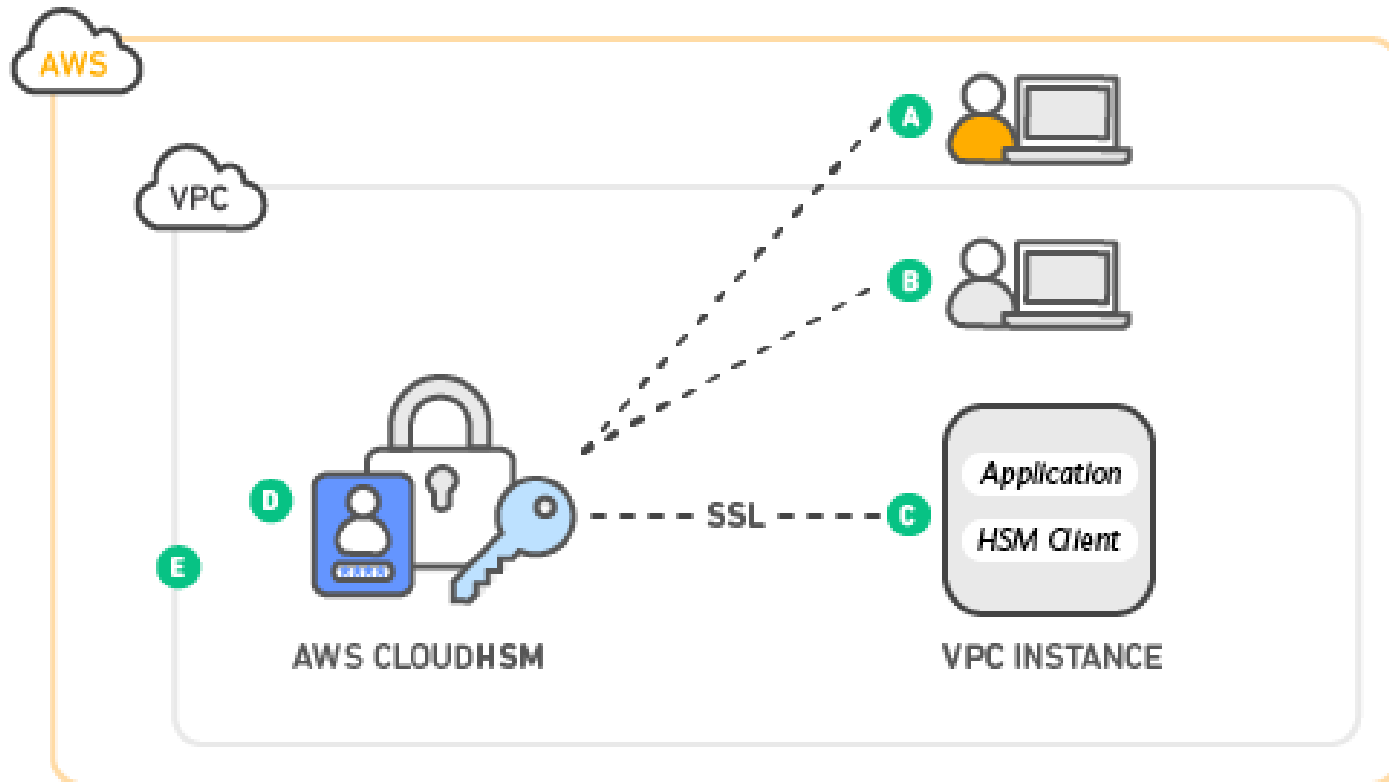
4. Figure 2 - AWS decryption workflow



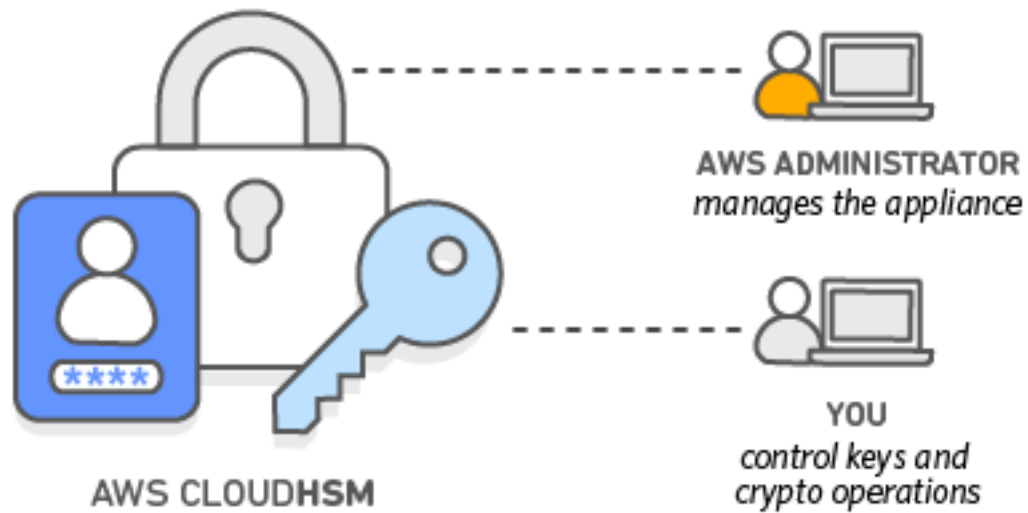
4. Figure 3 - AWS envelope encryption



4. Figure 4 - AWS CloudHSM



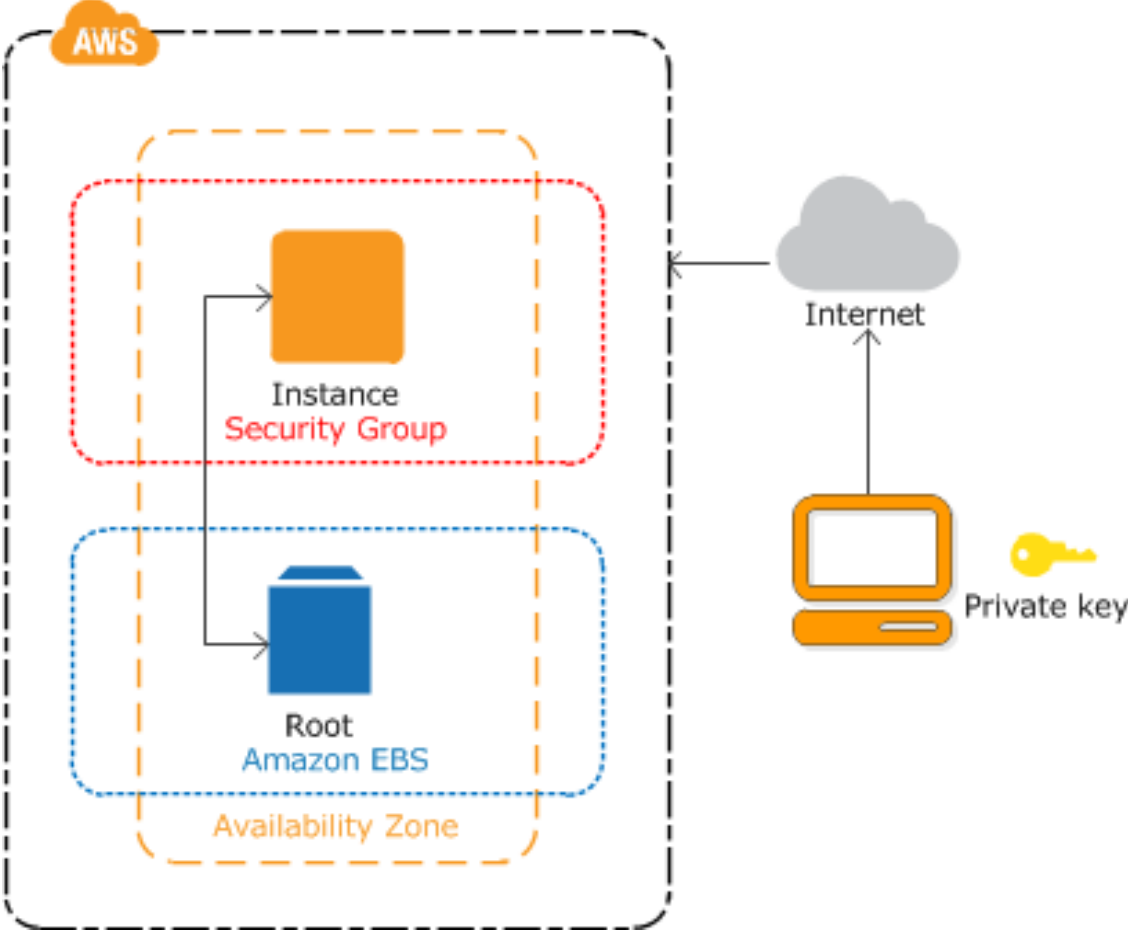
4. Figure 5 - AWS CloudHSM separation of duties



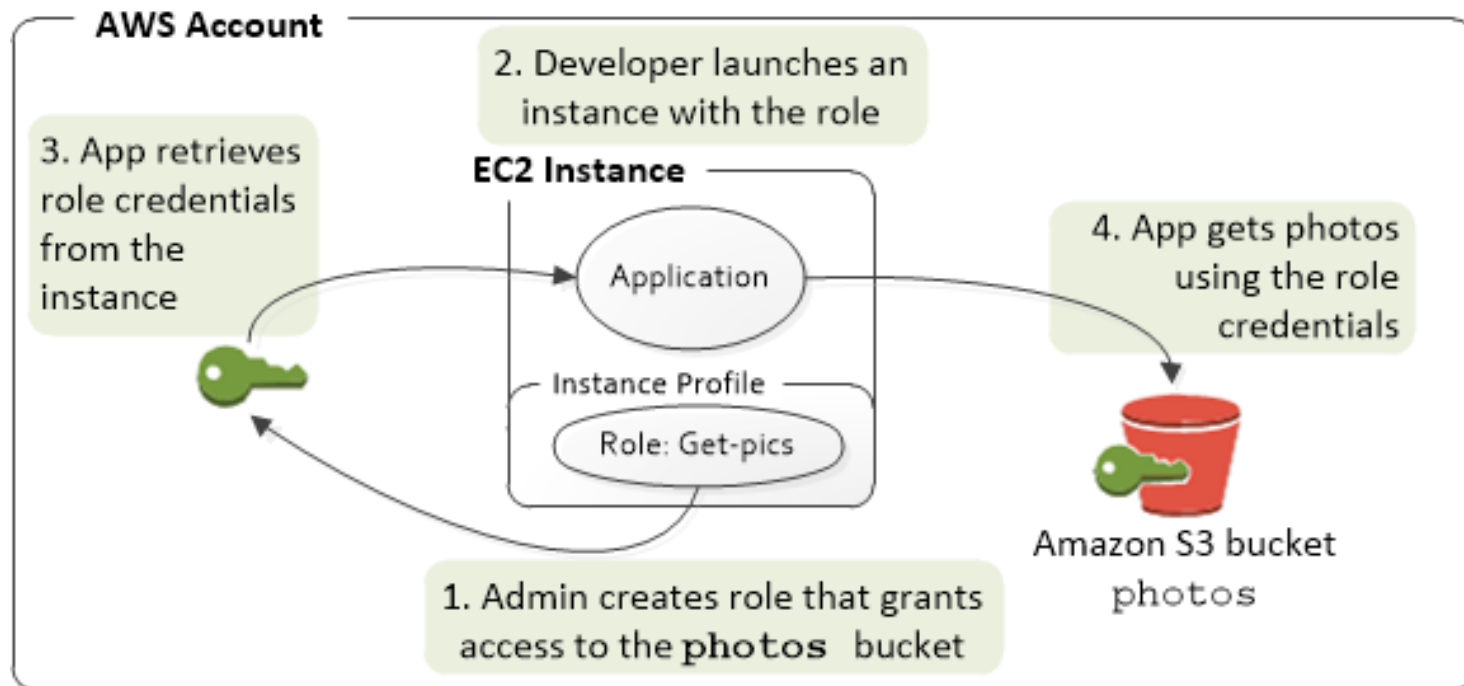
AWS Security Essentials - 5



5. Figure 1 - AWS EC2 security



5. Figure 2 - IAM role for EC2 instance



5. Figure 3 - AWS security groups

The screenshot displays the AWS Management Console interface for configuring a security group. The top navigation bar includes 'Services', 'Resource Groups', and user information. The left sidebar shows navigation options for VPC, Subnets, Route Tables, Internet Gateways, and more. The main content area shows the 'Web Servers Security Group' configuration page, with the 'Inbound Rules' tab selected. The 'Inbound Rules' table lists three rules: HTTP (80), SSH (22), and HTTPS (443), all using TCP protocol and allowing traffic from 0.0.0.0/0. A 'Cancel' button and a 'Save' button are visible above the table. Below the table is an 'Add another rule' button.

Type	Protocol	Port Range	Source	Description	Remove
HTTP (80)	TCP (6)	80	0.0.0.0/0		✕
SSH (22)	TCP (6)	22	118.185.136.34/32		✕
HTTPS (443)	TCP (6)	443	0.0.0.0/0		✕

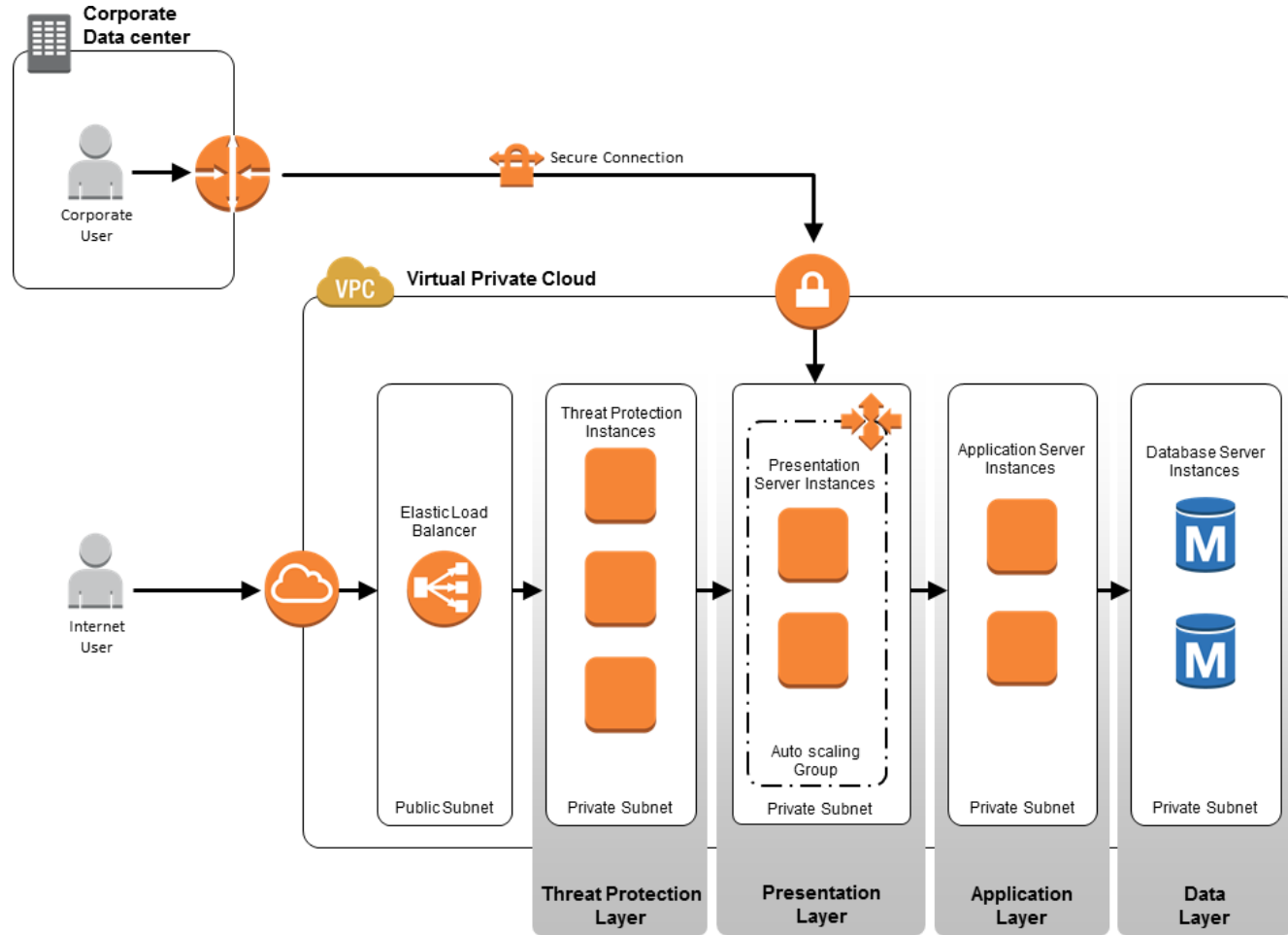
5. Figure 4 - AWS security groups object reference

The screenshot displays the AWS Management Console interface for configuring a security group. The main content area shows the 'Inbound Rules' tab for the security group 'sg-5940cf2a | Database Security Group'. A dropdown menu is open, listing several security groups, with 'sg-36153c46 | Web Servers Security Group' highlighted. The console header shows 'Services' and 'Resource Groups' menus, and the left sidebar lists various VPC-related services.

Name tag	Group ID	Group Name	VPC
	sg-21aaaf51	SecurityGroup-Allen	vpc-57...
	sg-2e00055e	launch-wizard-1	vpc-57...
	sg-36153c46	SL-Web-SG	vpc-57...
	sg-5940cf2a	Database Security Gr...	vpc-57...
	sg-5705e024		
	sg-5940cf2a	Database Security Group	vpc-57...
	sg-700d0800		vpc-57...
	sg-7455c308		
	sg-8f0306ff		
	sg-920306e2		
	sg-e5090c95		
	sg-e70c0997		
	sg-e885659b		

Type	Protocol	Port Range	Remove
ALL Traffic	ALL	ALL	

5. Figure 5 - AWS layered network defense



5. Figure 6 - Amazon Inspector splash screen



Install



Run



Analyze

5. Figure 7 - Amazon Inspector CloudTrail events

The screenshot shows the Amazon CloudTrail console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information (Albert, N. Virginia, Support). The left sidebar shows 'CloudTrail' with sub-items 'Dashboard', 'Event history' (highlighted), and 'Trails'. A 'Create a trail' banner is visible at the top right of the main content area.

Event history

Your event history contains the create, modify, and delete activities for supported services taken by people, groups, or AWS services in your AWS account. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs.

You can view the last 7 days of events. Choose an event to view more information about it. [Learn more](#)

Filter: **Event source** | inspector.amazonaws.com | Time range: Select time range

	Event time	User name	Event name	Resource type	Resource name
▶	2017-09-23, 07:09:52...	root	StartAssessmentRun		
▶	2017-09-23, 08:13:54...	root	CreateAssessmentTe...		
▶	2017-09-23, 08:13:53...	root	CreateAssessmentTa...		
▶	2017-09-23, 08:13:52...	root	CreateResourceGroup		
▶	2017-09-23, 07:56:42...	root	RegisterCrossAccou...		
▶	2017-09-23, 07:56:39...	root	RegisterCrossAccou...		

5. Figure 8 - Amazon Inspector CloudWatch metrics

The screenshot shows the AWS console interface for Amazon Inspector. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information (Albert, N. Virginia, Support). The left sidebar lists various AWS services, with 'Metrics' highlighted. The main content area is titled 'Amazon Inspector' and shows a graph area with a search bar and a table of metrics.

<input checked="" type="checkbox"/>	AssessmentTargetName (4)	AssessmentTargetArn	Metric Name
<input checked="" type="checkbox"/>	Web-Server	arn:aws:inspector:us-east-1:100122829558	TotalAssessmentRuns
<input checked="" type="checkbox"/>	Web-Server	arn:aws:inspector:us-east-1:100122829558	TotalMatchingAgents
<input checked="" type="checkbox"/>	Web-Server	arn:aws:inspector:us-east-1:100122829558	TotalHealthyAgents
<input checked="" type="checkbox"/>	Web-Server	arn:aws:inspector:us-east-1:100122829558	TotalFindings



5. Figure 9 - Amazon Inspector dashboard

The screenshot displays the Amazon Inspector dashboard. At the top, the AWS logo is on the left, and navigation links for 'Services', 'Resource Groups', and a star icon are in the center. On the right, there are notification and user location indicators: a bell icon, 'Albert', 'N. Virginia', and 'Support'. A left-hand navigation menu includes 'Dashboard' (highlighted), 'Assessment targets', 'Assessment templates', 'Assessment runs', and 'Findings'. The main content area is titled 'Amazon Inspector' with a help icon. Below the title, a brief description states: 'Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues. [Learn more.](#)'

The dashboard is divided into three main sections:

- Notable findings:** Shows 0 important findings and 1 recent finding.
- Assessment status:** Shows 0 assessments running, 1 assessment run completed, and 0 assessment runs failed.
- Account settings:** Includes a link to 'Manage Amazon Inspector service role'.

The 'Recent Assessment Runs (Last 10)' section contains a table with the following data:

Name	Date Run	Status
Run - WebServer - 2017-09-23T13:39:50.208Z	Today at 7:09 PM (GMT+5)	Analysis complete

5. Figure 10 - Amazon Inspector rules package

The screenshot shows the Amazon Inspector console interface. At the top, the navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information for 'Albert' in 'N. Virginia'. The main heading is 'Get started with Amazon Inspector'. On the left, a sidebar lists four steps: 'Step 1: Prerequisites', 'Step 2: Define an assessment target', 'Step 3: Define an assessment template' (which is highlighted with an orange bar), and 'Step 4: Review'. The main content area is titled 'Define an assessment template' with a help icon. Below the title, a descriptive paragraph explains that an assessment template allows specifying properties like rules packages, duration, and SNS notifications. The form contains three fields: 'Name*' with the value 'WebServer', 'Rules packages*' with a dropdown menu open showing 'Security Best Practices-1.0' selected, and 'Duration*' with a dropdown menu open showing 'Runtime Behavior Analysis-1.0', 'Common Vulnerabilities and Exposures-1.1', and 'CIS Operating System Security Configuration Benchmarks-1.0'. A note below the duration dropdown states: 'You can modify the duration, but note that assessment templates with longer durations can deliver fuller sets of findings.' At the bottom, there is a '*Required' label and three buttons: 'Cancel', 'Previous', and 'Next'.

aws Services Resource Groups Albert N. Virginia Support

Get started with Amazon Inspector

Step 1: Prerequisites
Step 2: Define an assessment target
Step 3: Define an assessment template
Step 4: Review

Define an assessment template ?

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. [Learn more.](#)

Name* WebServer

Rules packages* Select an Inspector rules package

- Security Best Practices-1.0

Duration* Runtime Behavior Analysis-1.0
Common Vulnerabilities and Exposures-1.1
CIS Operating System Security Configuration Benchmarks-1.0

You can modify the duration, but note that assessment templates with longer durations can deliver fuller sets of findings.

*Required Cancel Previous Next

5. Figure 11 - Amazon Inspector assessment template

<input type="checkbox"/>	Name	Duration	Target name	Last run	All runs
<input type="checkbox"/>	Web Servers	na	Web-Server		

Assessment Template - Web Servers

Name*

Target name*

Rules packages* Security Best Practices-1.0 ✕

Duration*

Tags

Key	Value	<input type="button" value="↻"/>
<input type="text" value="Add a new key"/>	<input type="text"/>	

Attributes added to findings

Key	Value
<input type="text" value="Add a new key"/>	<input type="text" value="Add a new value"/>

5. Figure 12 - AWS shield tiers

AWS Shield

Standard Protection



*Available to ALL AWS customers at
No Additional Cost*

Advanced Protection



*Paid service that provides additional,
comprehensive protections from large
and sophisticated attacks*

AWS Security Essentials – End Day 2



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

AWS Security Essentials - 6



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

Rules example

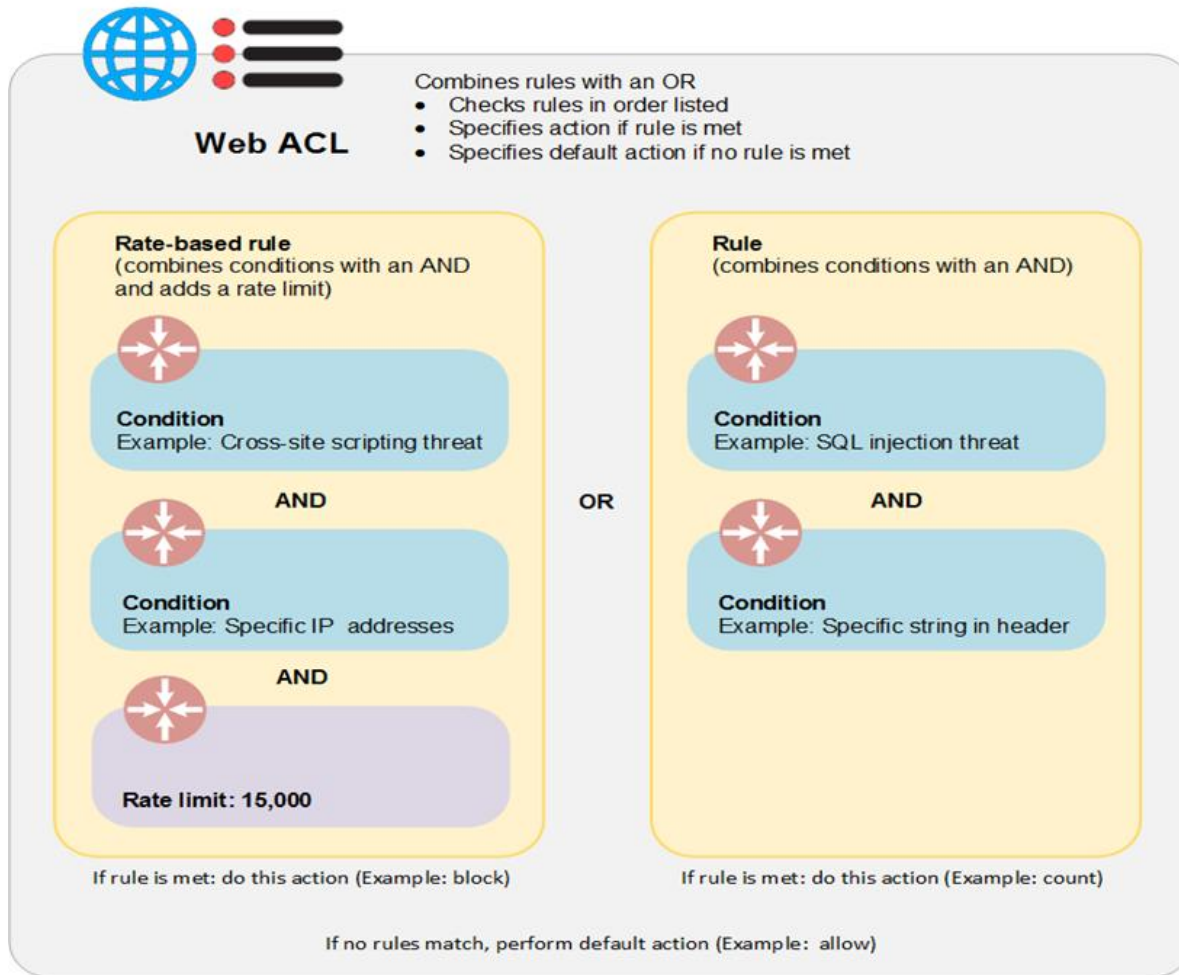
Bad User-Agents

IP match condition
Suspicious IPs

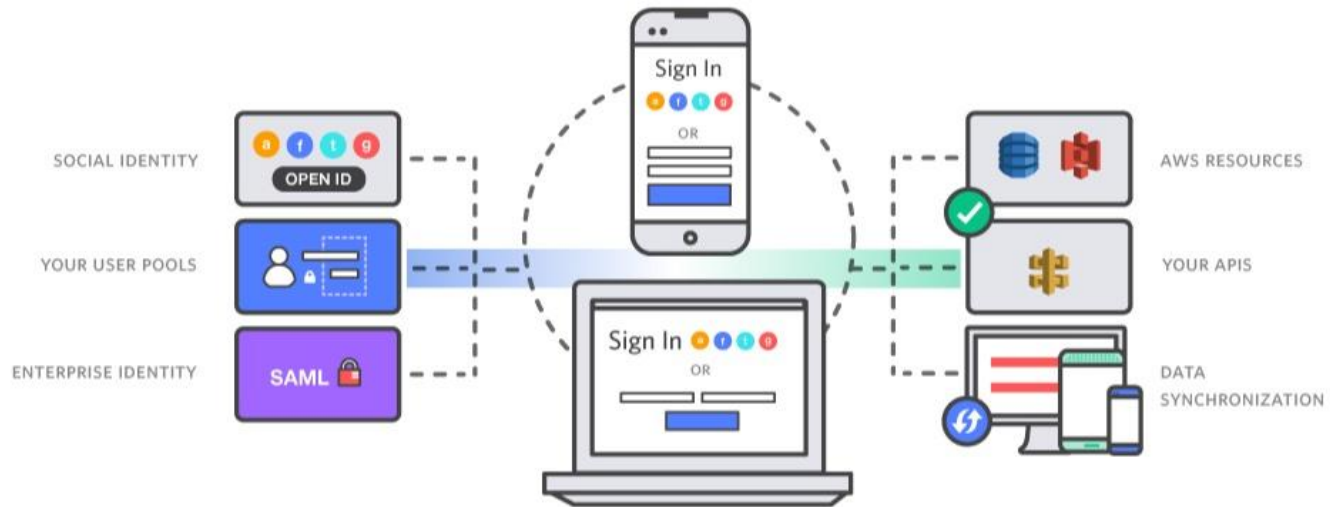
and

String match condition
Bad bots

6. Figure 4 AWS WAF Web ACL



6. Figure 5 - AWS Cognito overview



AWS Security Essentials - 7



7.AWS CloudWatch Alert

AWS Free Tier limit alert



no-reply-aws@amazon.com
To: aws@drmddev.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.

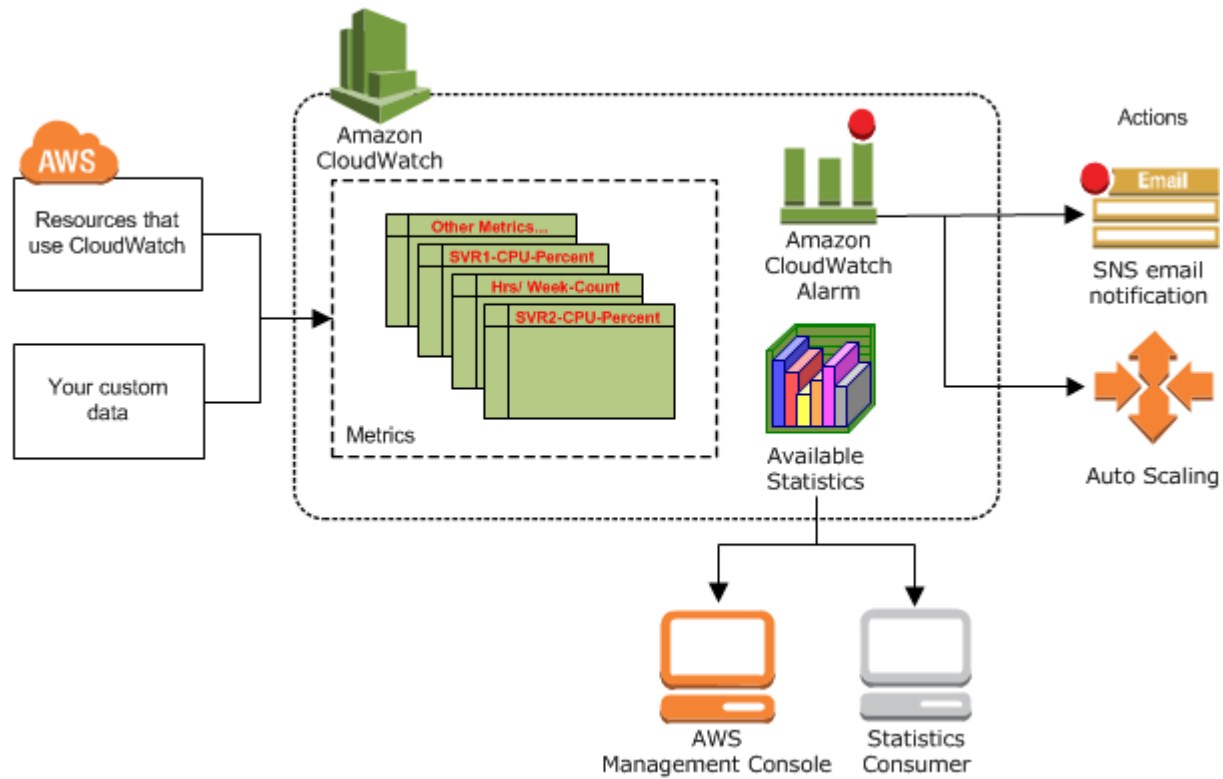
Product	AWS Free Tier Usage as of 10/18/2021	Usage Limit	AWS Free Tier Usage Limit
AmazonEC2	26.12903265 GB-Mo	30.0 GB-Mo	30 GB of Amazon Elastic Block Storage in any combination of General Purpose (SSD) or Magnetic

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



7. Figure 1 - AWS CloudWatch architecture



7. Figure 2 - AWS CloudWatch Create Alarm

Create Alarm

1. Select Metric 2. Define Alarm

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name: Billing-Alarm

Description: Billing Alarm

Whenever charges for: EstimatedCharges

is: >= USD \$ 100

Additional settings

Provide additional configuration for your alarm.

Treat missing data as: bad (breaching threshold) ⓘ

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line

EstimatedCharges >= 100

Time	EstimatedCharges
9/24 00:00	~10
9/26 00:00	~10
9/28 00:00	~10

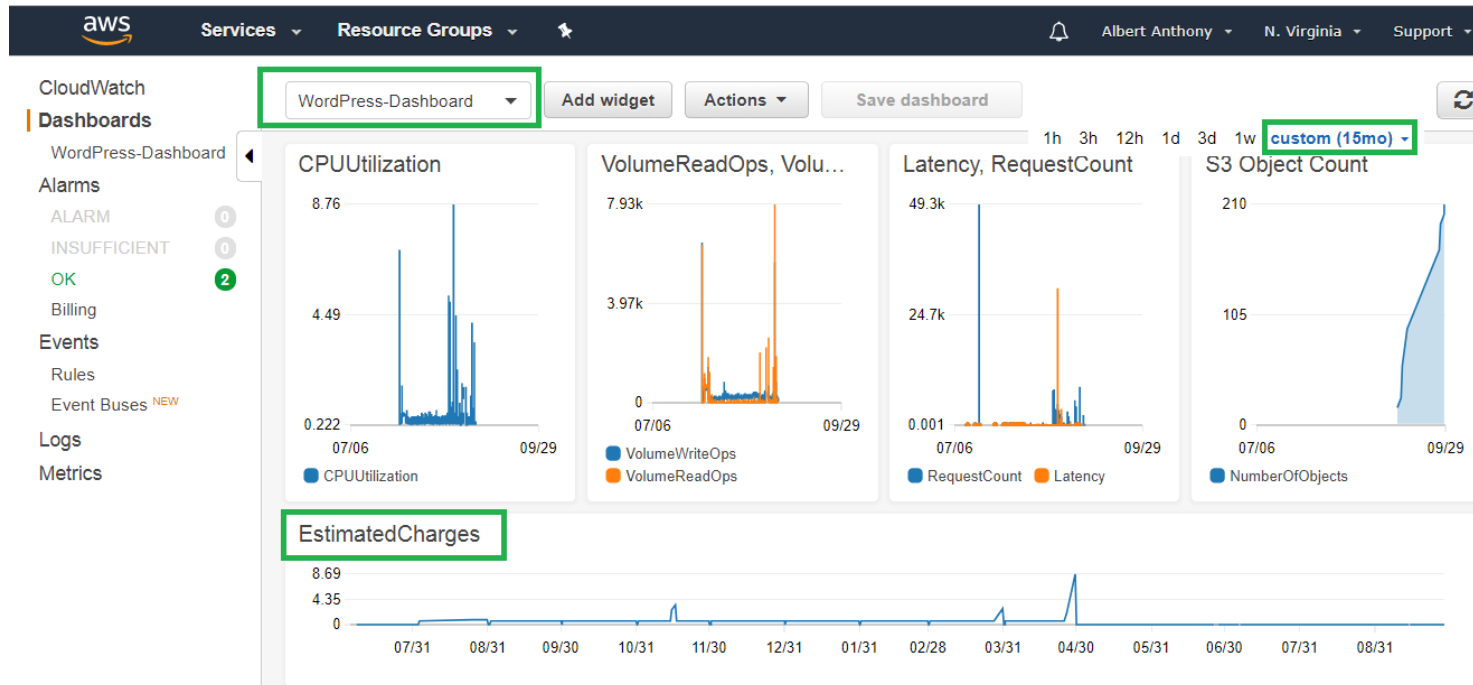
Namespace: AWS/Billing

Currency: USD

Metric Name: EstimatedCharges

Cancel Previous Next **Create Alarm**

7. Figure 3 - AWS CloudWatch dashboard



7. Figure 4 - AWS CloudWatch Metrics





























All metrics | Graphed metrics (13) | Graph options

Q Search for any metric, dimension or resource id

338 Metrics

Billing 14 Metrics	DynamoDB 14 Metrics	EBS 81 Metrics
EC2 136 Metrics	RDS 72 Metrics	S3 8 Metrics
SNS 4 Metrics	SQS 9 Metrics	




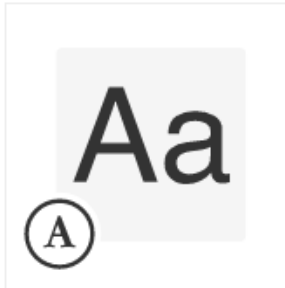
7. Figure 5 - AWS CloudWatch Metric details

All metrics		Graphed metrics (9)		Graph options			
Label	Namespace	Dimensions	Metric Name	Statistic	Period	Y Axis	Actions
 AmazonCloudWatch	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	  
 AmazonEC2	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	  
 AmazonRDS	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	  
 AmazonS3	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	  
 AmazonSNS	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	  
 AWSDataTransfer	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	  
 awskms	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	  

7. Figure 6 - AWS CloudWatch dashboard options

Add to this dashboard ×

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

			
Line Compare metrics over time	Stacked area Compare the total over time	Number Instantly see the latest value for a metric	Text Free text with markdown formatting

Cancel Configure

7. Figure 7 - AWS CloudWatch Events

Start Responding to CloudWatch Events



Determine events of interest in the CloudWatch Events stream



Create rules to select events of interest



Specify actions to take when a rule matches an event

7. Figure 8 - AWS CloudWatch alarm

Create Alarm

1. **Select Metric** 2. Define Alarm

EC2 Search Metrics 1 to 50 of 68 Metrics

Per-Instance Metrics By Auto Scaling Group By Image (AMI) Id Aggregated by Instance Type Across All Instances

EC2 > Per-Instance Metrics

InstanceId	InstanceName	Metric Name
<input type="checkbox"/> i-0332c3c79f97a3e63		CPUCreditBalance
<input type="checkbox"/> i-0332c3c79f97a3e63		CPUCreditUsage
<input checked="" type="checkbox"/> i-0332c3c79f97a3e63		CPUUtilization
<input type="checkbox"/> i-0332c3c79f97a3e63		DiskReadBytes
<input type="checkbox"/> i-0332c3c79f97a3e63		DiskReadOps

Title: CPUUtilization Average 5 Minutes

Update Graph

Time Range: Relative Absolute UTC (GMT)

From: 3 days ago

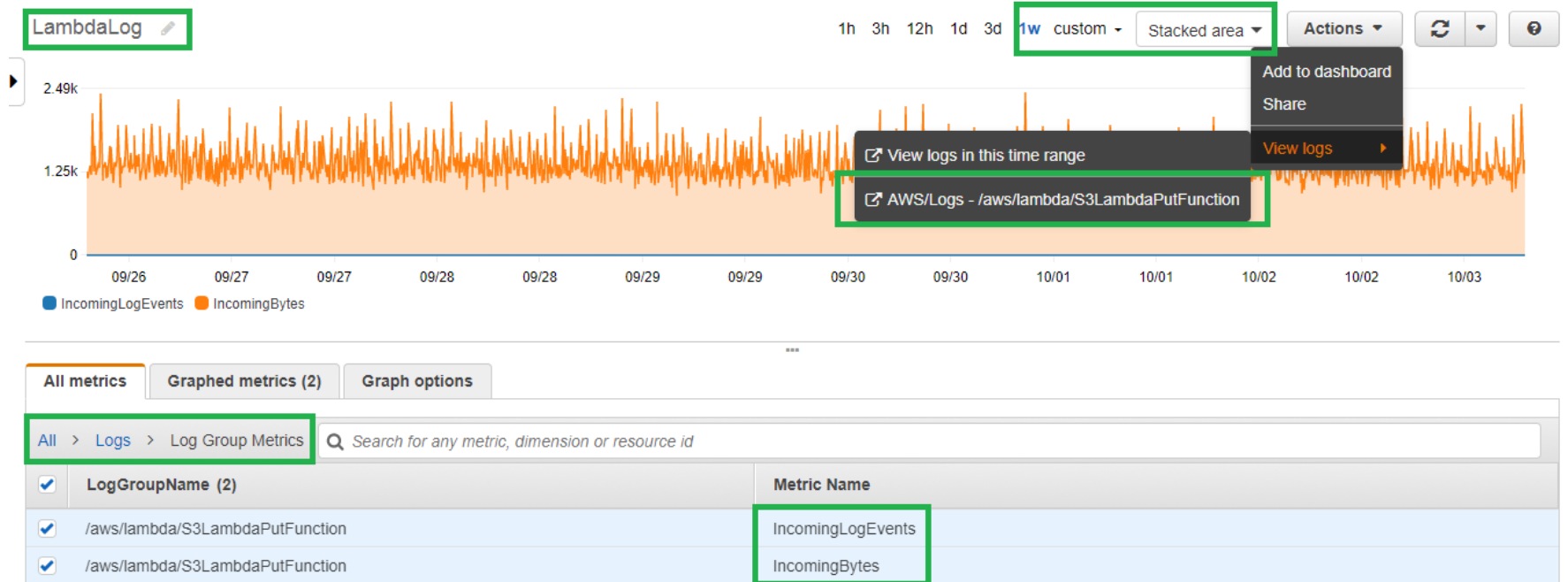
To: 0 hours ago

Zoom: 1h | 3h | 6h | 12h | 1d | 3d | 1w | 2w

Left Y-axis: Limits Min 0 Max Auto Auto

Cancel Previous Next Create Alarm

7. Figure 9 - AWS CloudWatch log monitoring



7. Figure 10 - AWS CloudWatch Create Logs Metric

Define Logs Metric Filter

Filter for Log Group: /aws/lambda/S3LambdaPutFunction

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax.](#)

Filter Pattern
Error ⓘ

[Show examples](#)

Select Log Data to Test

2017/07/14/[\$LATEST]406fdc6d58964b02a467ca7e1b98b5e3 ⓘ **Test Pattern**

[Clear](#)

```
Loading function

START RequestId: 3d2a2042-689b-11e7-ac85-158ea65b4e01 Version: $LATEST

An error occurred (AccessDenied) when calling the GetObject operation: Access Denied
```

Results

Please paste logs lines above and click **Test Pattern**.

[Cancel](#) [Assign Metric](#)

7. Figure 11 - AWS system and instance checks

<input type="checkbox"/>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
<input type="checkbox"/>	wordpress in...	i-0a8b6f46708f94aaf	t2.micro	ap-south-1a	● running	✓ 2/2 checks passed	None	ec2-13-126-201-229.ap..
<input checked="" type="checkbox"/>	Test Wordpr...	i-0bdebf80221ef3d07	t2.micro	ap-south-1a	● running	✓ 2/2 checks passed	None	ec2-52-66-170-35.ap-s..

Instance: **i-0bdebf80221ef3d07 (Test Wordpress Instance)** Public DNS: **ec2-52-66-170-35.ap-south-1.compute.amazonaws.com**

Description **Status Checks** Monitoring Tags Usage Instructions

Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks.

[Create Status Check Alarm](#)

System Status Checks ⓘ

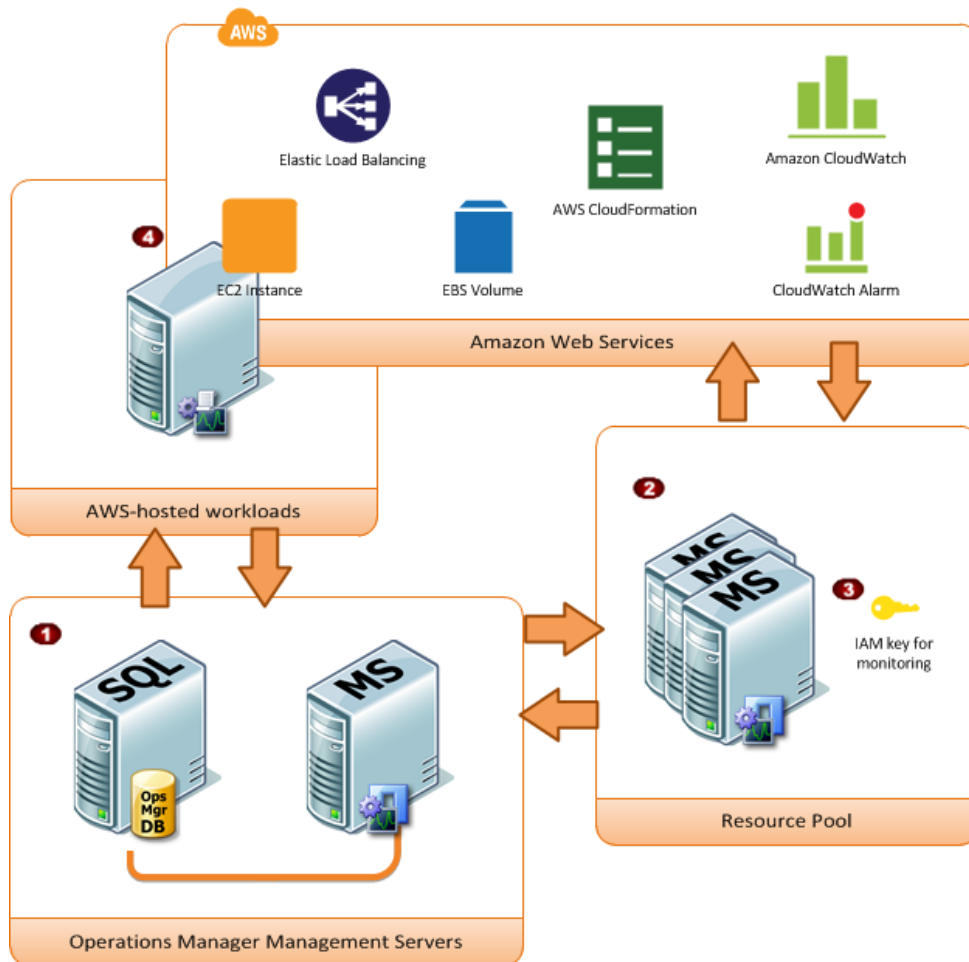
These checks monitor the AWS systems required to use this instance and ensure they are functioning properly.
System reachability check passed

Instance Status Checks ⓘ

These checks monitor your software and network configuration for this instance.
Instance reachability check passed

This check verifies that your instance's operating system is accepting traffic.
If this check fails, you may need to reboot your instance or make modifications to your operating system configuration.

7. Figure 12 - AWS Management Pack



AWS Security Essentials - 8

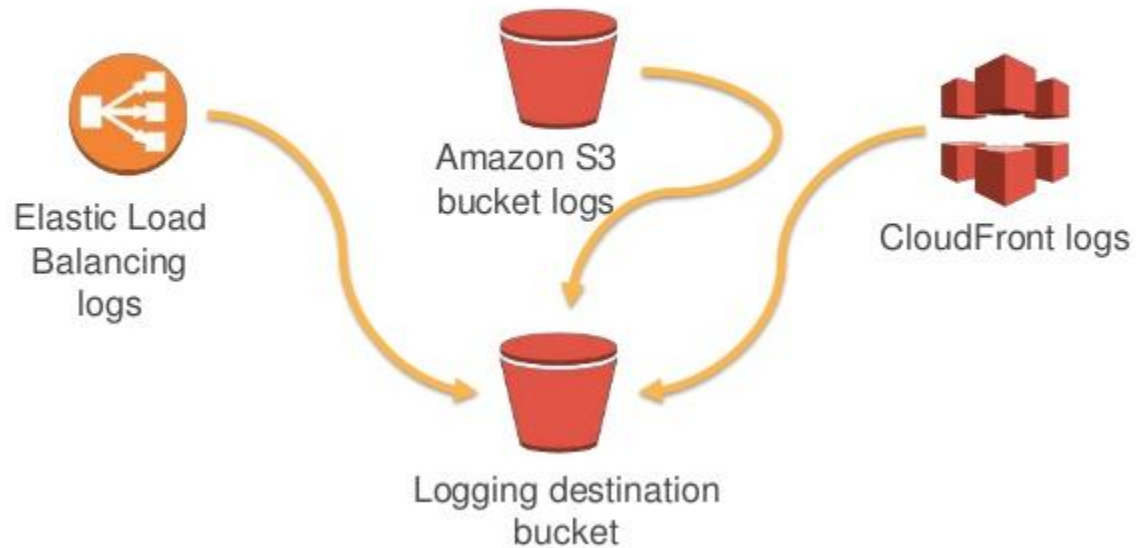


8. Table 1 - AWS logs classification

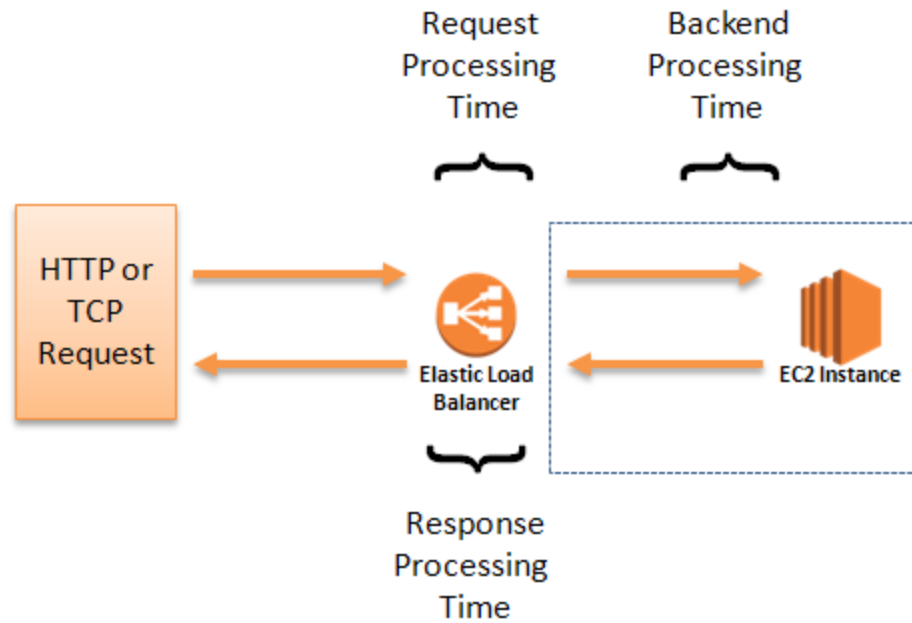
AWS Infrastructure logs	AWS service logs	Host-based logs
AWS CloudTrail	Amazon S3	Messages
AWS VPC flow logs	AWS ELB	IIS/Apache
	Amazon CloudFront	Windows Event logs
	AWS Lambda	Custom logs

8. Figure 1 - AWS access logging S3

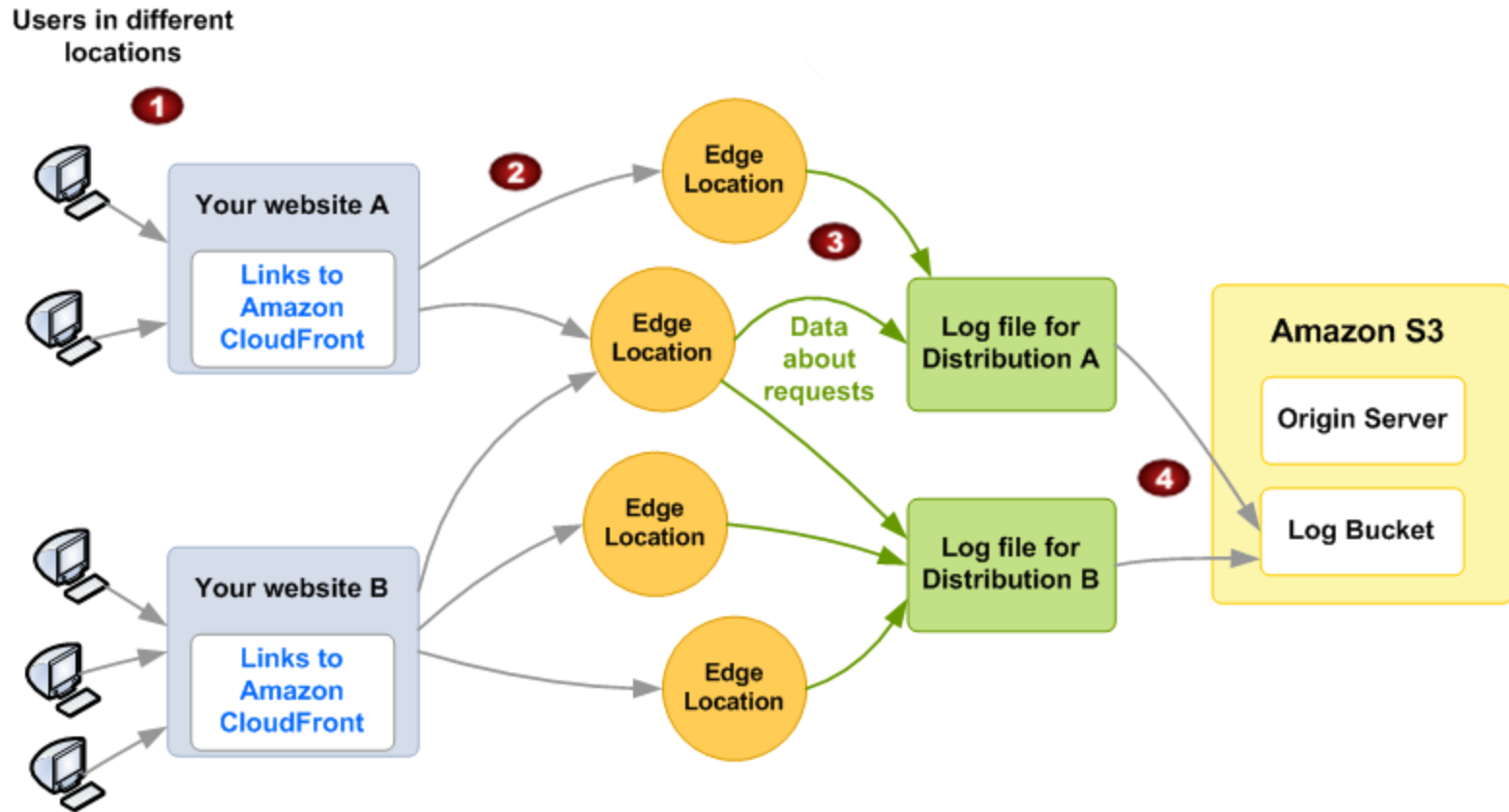
Logging—Elastic Load Balancing, CloudFront, Amazon S3 access logs



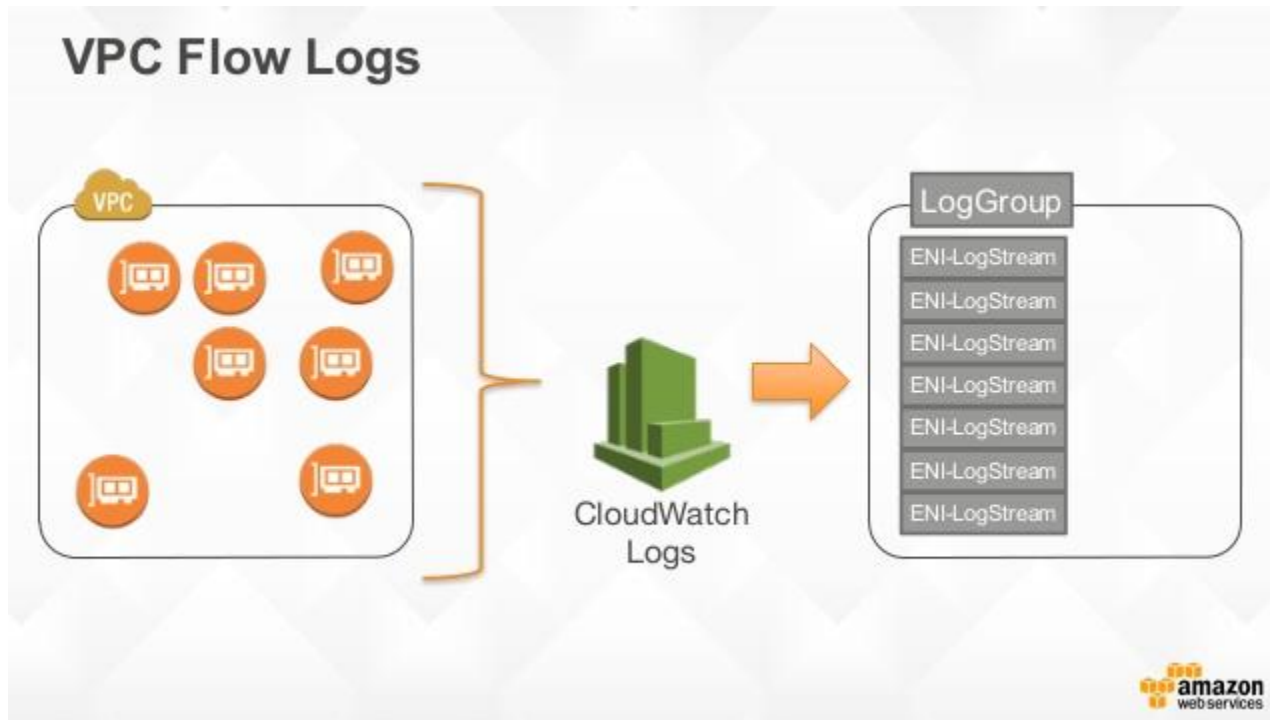
8. Figure 2 - Amazon ELB logging



8. Figure 3 - Amazon CloudFront logging



8. Figure 4 - Amazon VPC flow logs



8. Figure 5 - AWS CloudWatch Logs

CloudWatch > Log Groups

Create Metric Filter Actions ▾



Filter: Log Group Name Prefix ×




⏪ ⏩ Log Groups 1-4

Log Groups	Expire Events After	Metric Filters	Subscriptions
<input checked="" type="radio"/> /aws/lambda/S3LambdaPutFunction	Never Expire	2 filters	None
<input type="radio"/> /aws/lambda/SNSLambdaFunction	Never Expire	0 filters	None
<input type="radio"/> /aws/lambda/myFunction	Never Expire	0 filters	None
<input type="radio"/> /aws/lambda/myfunction	Never Expire	0 filters	None

8. Figure 6 - AWS CloudWatch Log streams

CloudWatch > Log Groups > Streams for /aws/lambda/S3LambdaPutFunction




Search Log Group Create Log Stream Delete Log Stream  

Filter: Log Stream Name Prefix x   Log Streams 1-50 

<input type="checkbox"/> Log Streams	Last Event Time
<input type="checkbox"/> 2017/10/07/[\$LATEST]e03d91ab00d84158b3f7e423c0396b7a	2017-10-07 21:30 UTC+5:30
<input type="checkbox"/> 2017/10/07/[\$LATEST]6a945f8450c44ab2877b3731293f9060	2017-10-07 21:23 UTC+5:30
<input type="checkbox"/> 2017/10/07/[\$LATEST]93e60de3239f45ceb0b6b939c77610f9	2017-10-07 21:20 UTC+5:30
<input type="checkbox"/> 2017/10/07/[\$LATEST]8047709d14504d0f8511e2f37d9438b7	2017-10-07 20:11 UTC+5:30
<input type="checkbox"/> 2017/10/07/[\$LATEST]a8b8b02652bb444aabf83dbf0936acc4	2017-10-07 20:07 UTC+5:30

8. Figure 7 - AWS CloudWatch events log

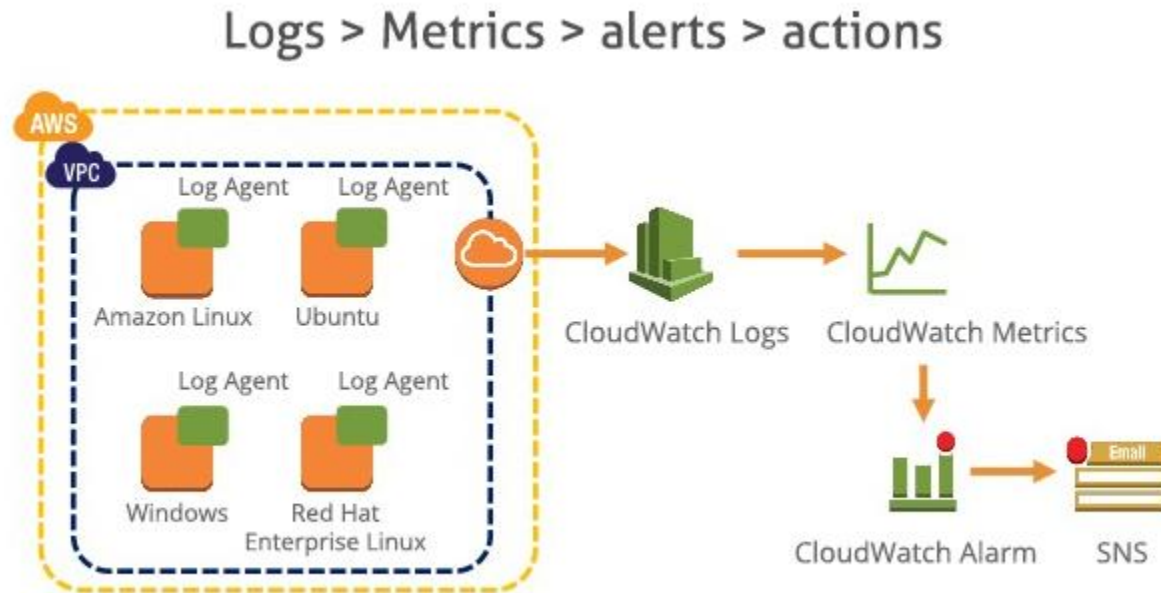
CloudWatch > Log Groups > /aws/lambda/S3LambdaPutFunction > 2017/10/07/[\$LATEST]6a945f8450c44ab2877b3731293f9060

Expand all Row Text   

Filter events all 30s 5m 1h 6h 1d 1w custom ▾

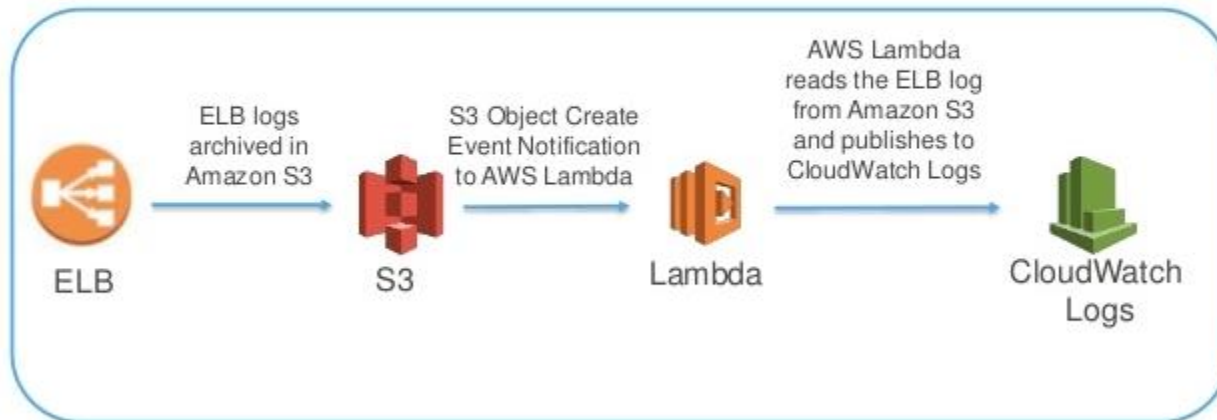
Time (UTC +00:00)	Message
2017-10-07	
An error occurred (AccessDenied) when calling the GetObject operation: Access Denied	
▼ 15:53:06	Error getting object AWSLogs/902891488394/CloudTrail/us-east-2/2017/10/07/902891488394_CloudTrail_us-east-2_20171007T1545Z
Error getting object AWSLogs/902891488394/CloudTrail/us-east-2/2017/10/07/902891488394_CloudTrail_us-east-2_20171007T1545Z_w0nojtB6lRmmnx5N.json.gz from bucket albertanthony. Make sure they exist and your bucket is in the same region as this function.	
▶ 15:53:06	An error occurred (AccessDenied) when calling the GetObject operation: Access Denied: ClientError Traceback (most recent call last):
▶ 15:53:06	END RequestId: 9bb64113-ab77-11e7-854b-cd5426b48afd
▶ 15:53:06	REPORT RequestId: 9bb64113-ab77-11e7-854b-cd5426b48afd Duration: 21.48 ms Billed Duration: 100 ms Memory Size: 128 MB Max
▶ 15:53:06	START RequestId: 791ea986-ab77-11e7-85b3-bfe3ee4a8df1 Version: \$LATEST
▶ 15:53:06	An error occurred (AccessDenied) when calling the GetObject operation: Access Denied
▶ 15:53:06	Error getting object AWSLogs/902891488394/CloudTrail/ap-northeast-1/2017/10/07/902891488394_CloudTrail_ap-northeast-1_20171007T1545Z

8. Figure 8 - AWS CloudWatch Log agent lifecycle

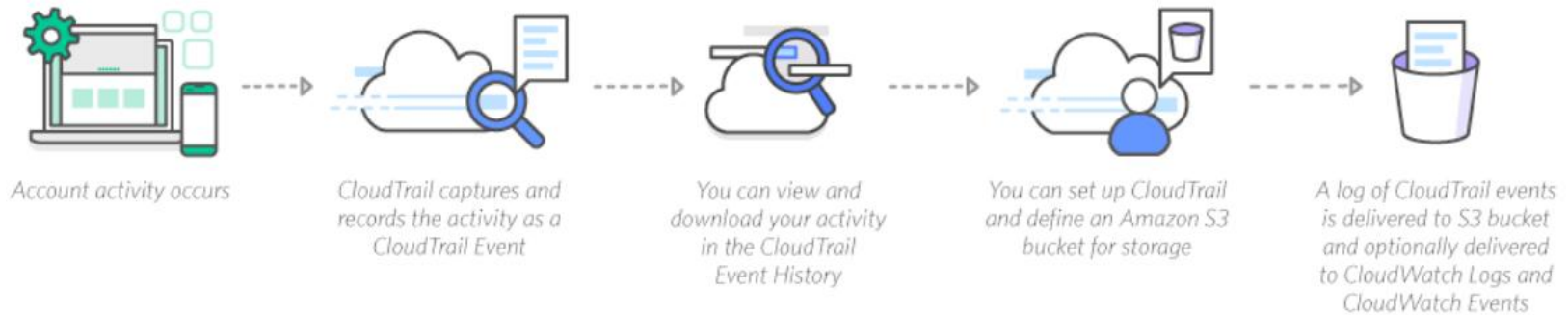


8. Figure 9 - AWS CloudWatch Logs lifecycle

Flow of events



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	Event source	logs.amazonaws.com
AWS region	ap-south-1	Event time	2017-10-08, 04:31:42 PM
Error code		Request ID	11232d98-ac18-11e7-bdb0-d356217574b0
Event ID	9c7d0d4e-cfb5-4bac-b5bb-6b108f6720a8	Source IP address	52.66.68.156
Event name	CreateLogStream	User name	S3LambdaPutFunction

Resources Referenced (0)

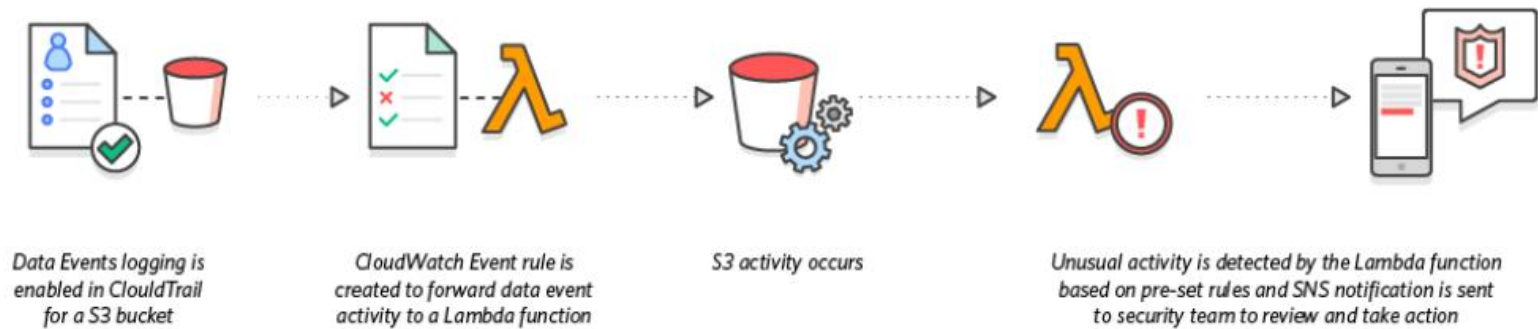
8. Figure 12 - AWS CloudTrail compliance audit workflow



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

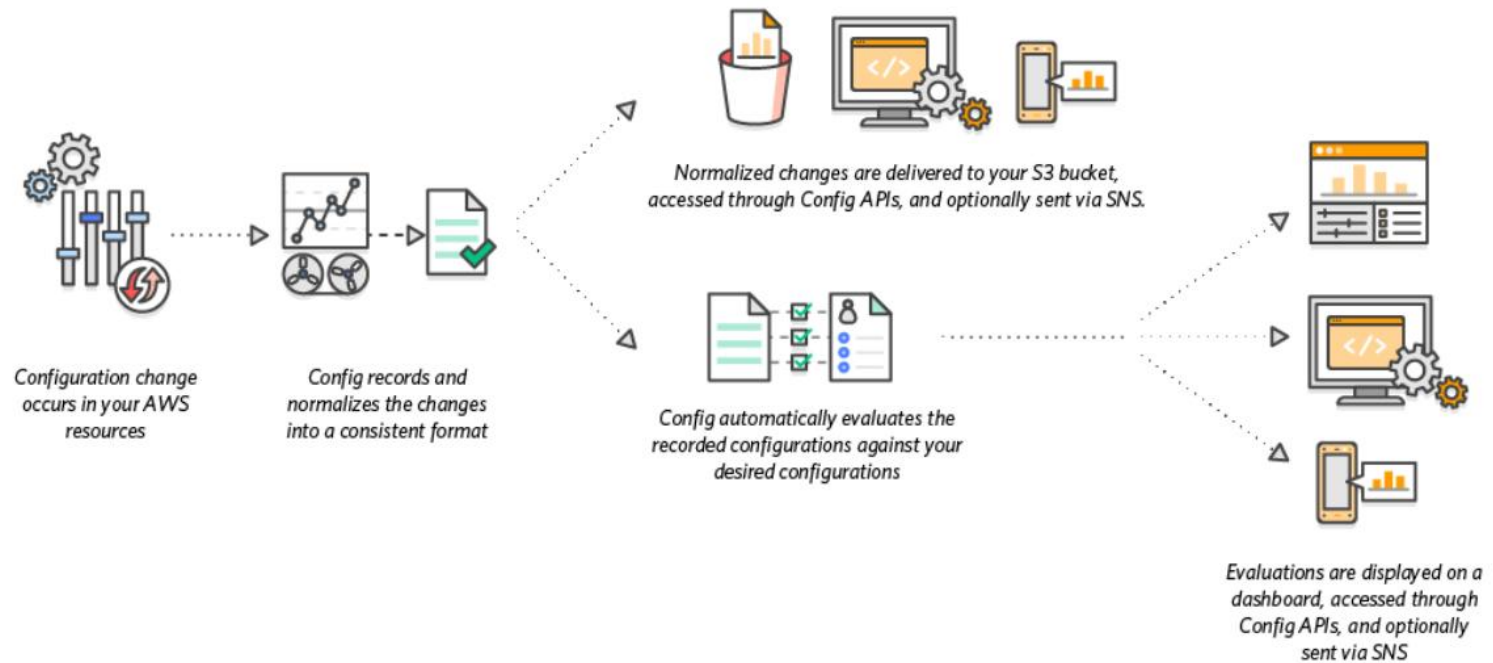


8. Figure 16 - AWS certifications and assurance programs

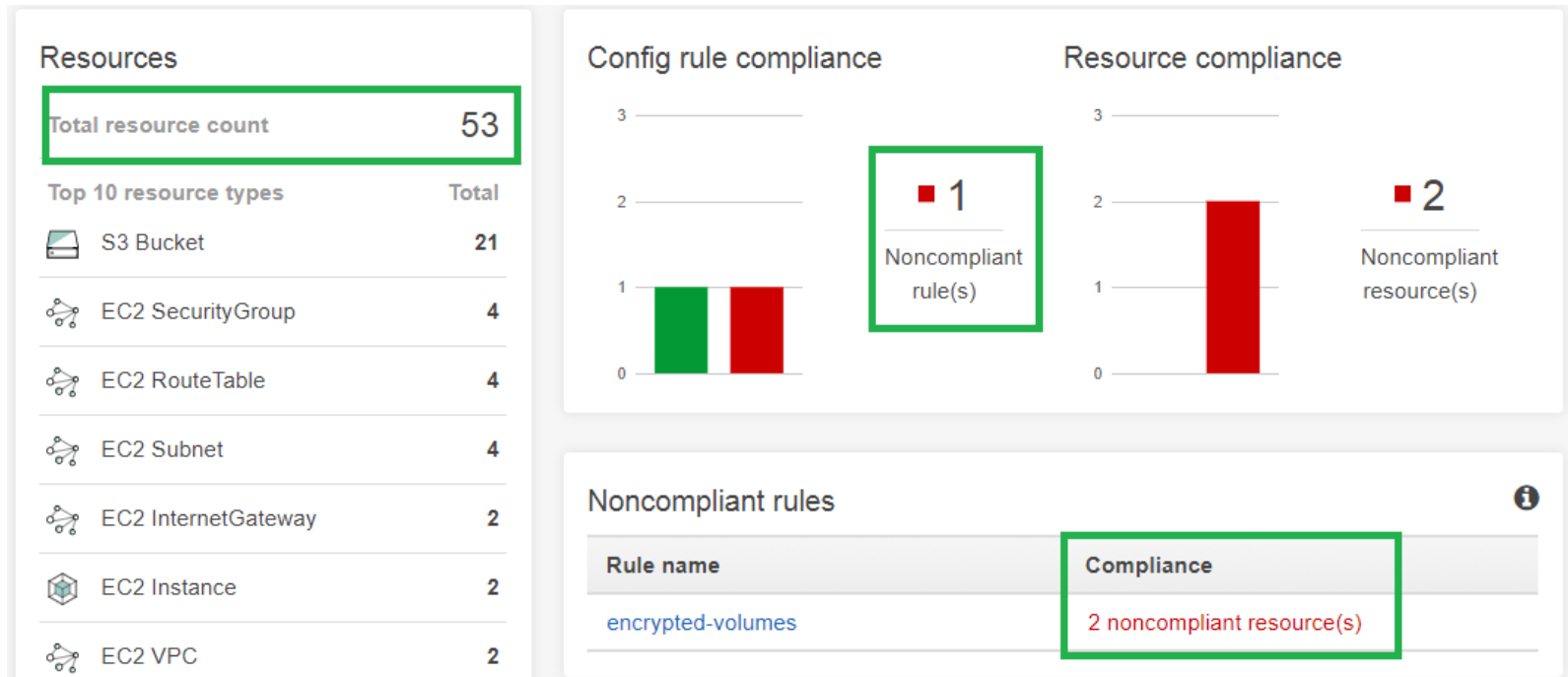
Key AWS Certifications and Assurance Programs



8. Figure 17 - AWS Config workflow



8. Figure 18 - AWS Config dashboard



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