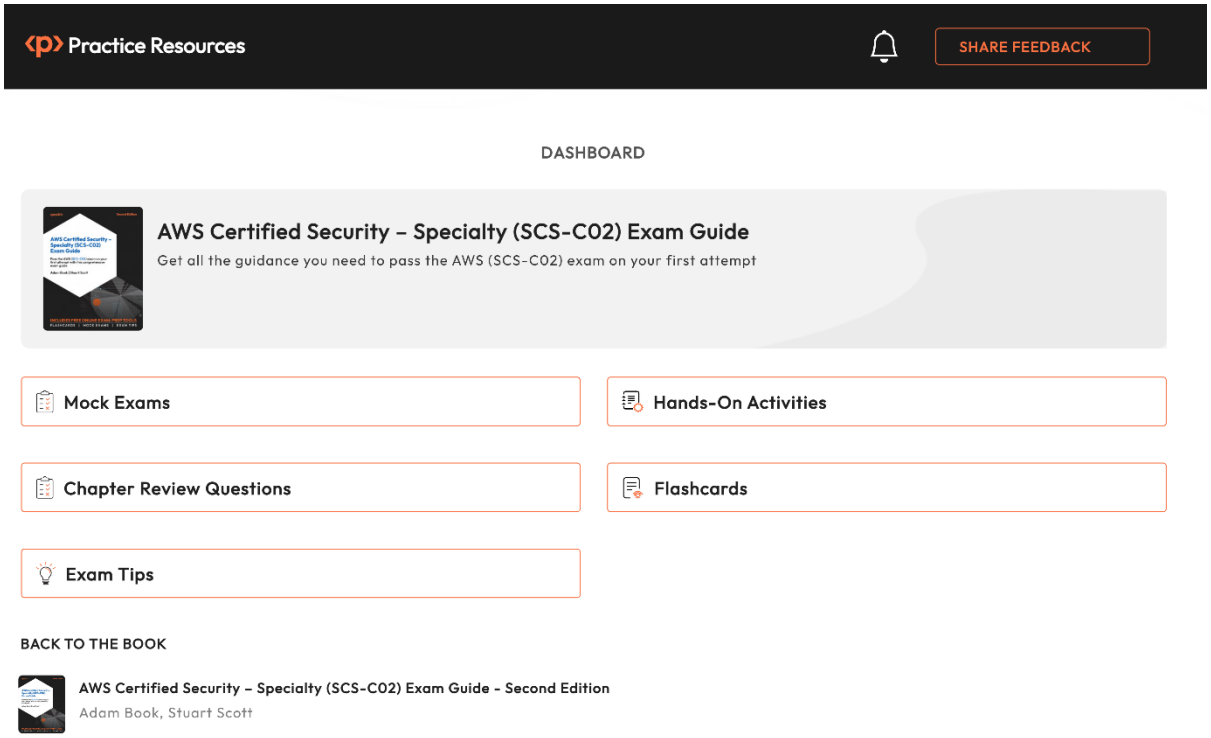
AWS Certified Security – Specialty (SCS-C02) Exam Guide

Preface:



Chapter 1:

Practice Resources

SHARE FEEDBACK

DASHBOARD

AWS Certified Security – Specialty (SCS-C02) Exam Guide

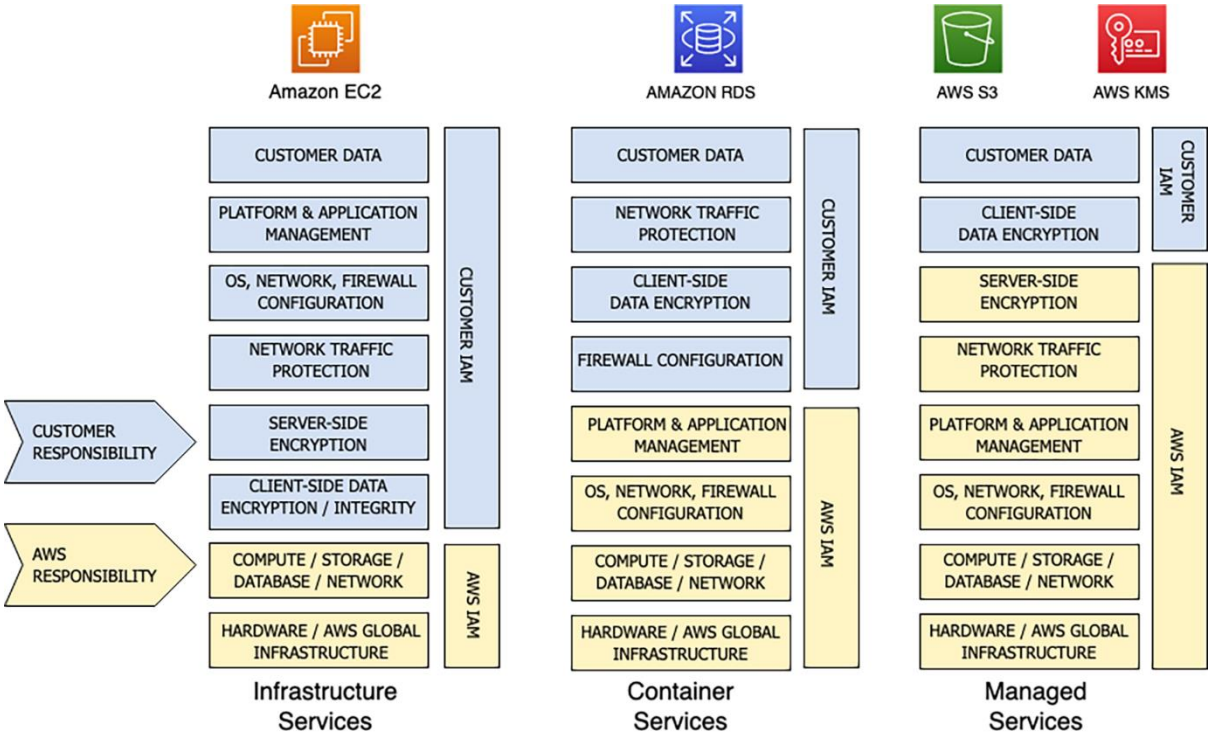
Get all the guidance you need to pass the AWS (SCS-C02) exam on your first attempt

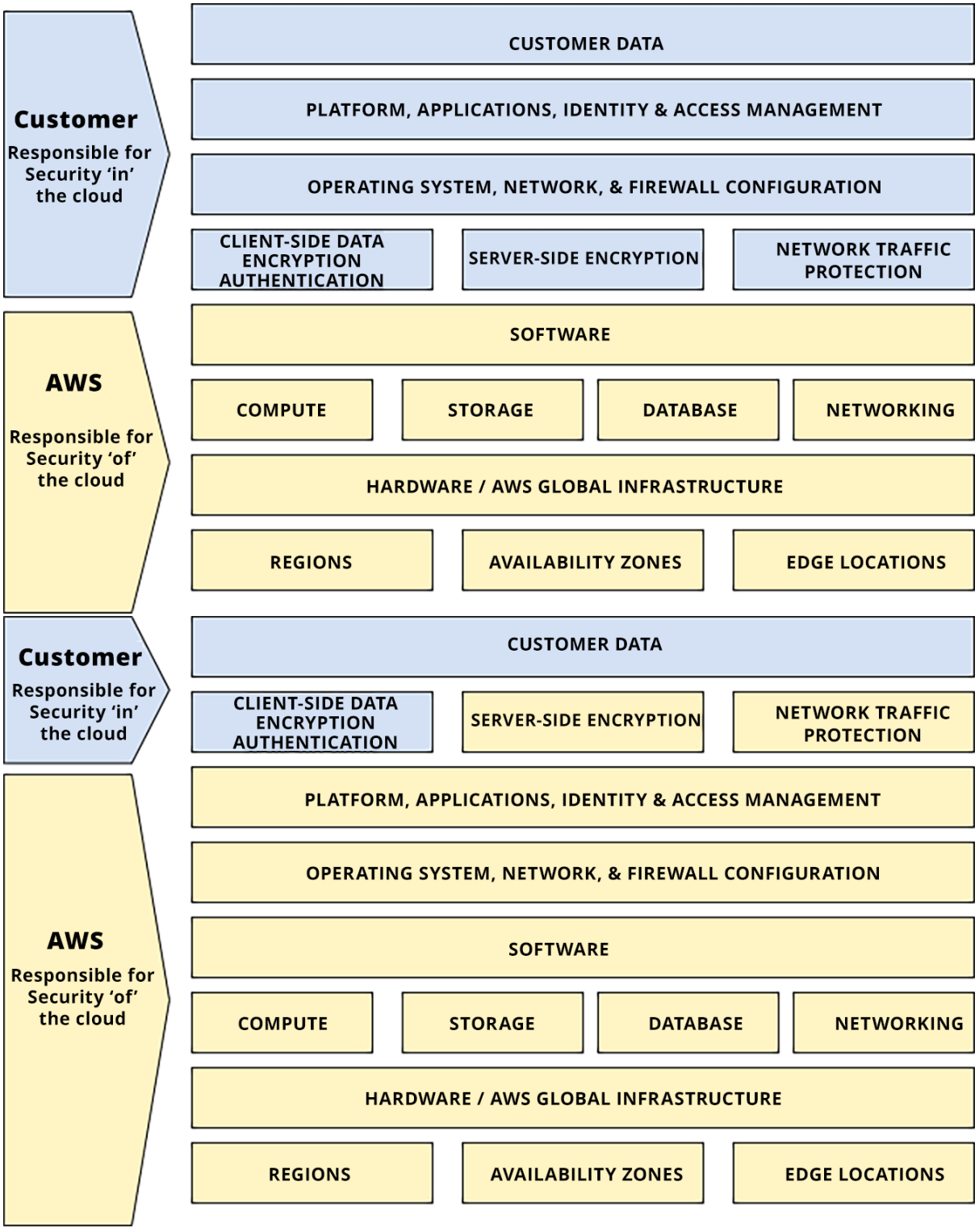
- Mock Exams
- Hands-On Activities
- Chapter Review Questions
- Flashcards
- Exam Tips

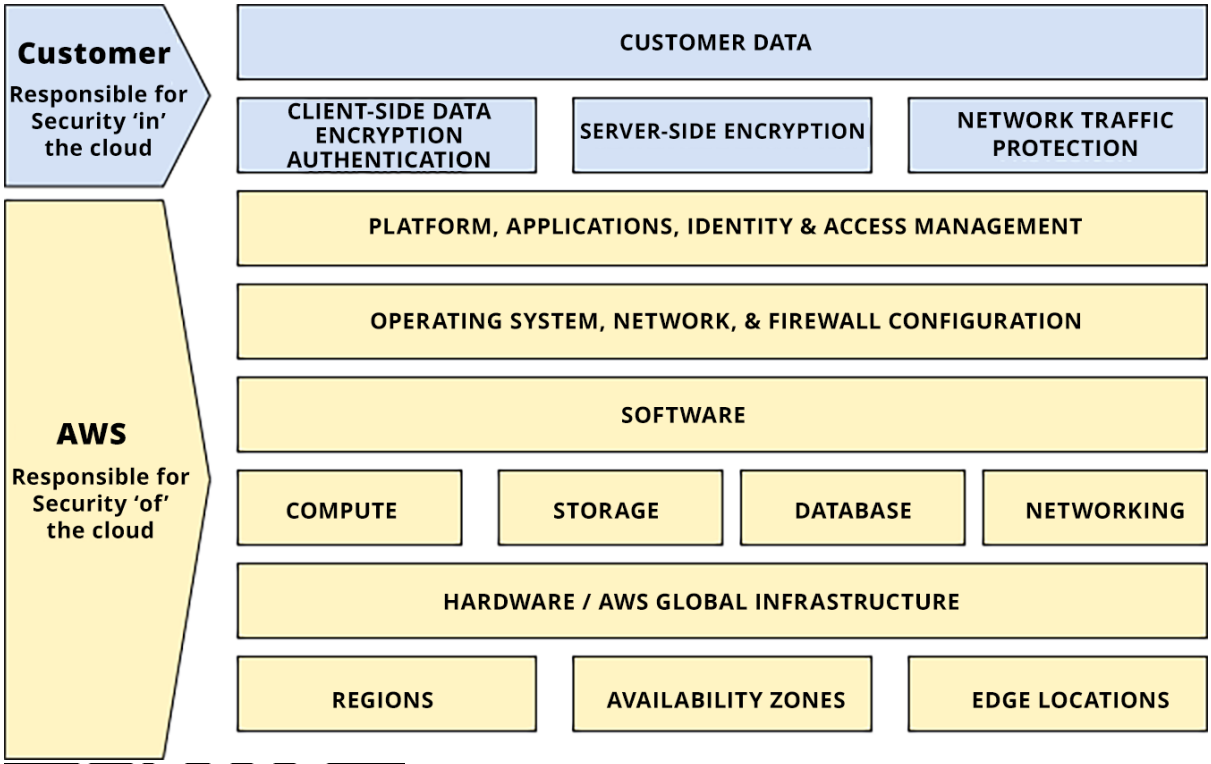
BACK TO THE BOOK

AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition

Adam Book, Stuart Scott




Customer
Responsible for Security 'in' the cloud
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK, & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION AUTHENTICATION
SERVER-SIDE ENCRYPTION
NETWORK TRAFFIC PROTECTION
AWS
Responsible for Security 'of' the cloud
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE / AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS
Customer
Responsible for Security 'in' the cloud
CUSTOMER DATA
CLIENT-SIDE DATA ENCRYPTION AUTHENTICATION
SERVER-SIDE ENCRYPTION
NETWORK TRAFFIC PROTECTION
AWS
Responsible for Security 'of' the cloud
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK, & FIREWALL CONFIGURATION
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE / AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS



DASHBOARD > CHAPTER 1

AWS Shared Responsibility Model

Summary

This chapter discussed the three shared security models used for AWS services: infrastructure, container, and abstract services. You learned that, from a security perspective and depending on the service you are using, your responsibility as a customer and that of AWS as the cloud provider can change.

Understanding these models and being able to differentiate between them will be beneficial when you implement your security strategies across your solutions as it means you will clearly understand where your responsibility ends and AWS's responsibility begins. This will help ensure that you do not leave any vulnerabilities across your AWS infrastructure within your accounts.

You also examined how the shared security model can help you by clarifying which items you and your organization are responsible for when it comes to compliance and audits for your business.

Chapter 2, Fundamental AWS Services, will provide a brief overview of many of the services used in the AWS ecosystem that are not particularly focused on security. Even the services that do not have a specific security focus often play a significant role in the solutions we build for our systems and customers. The AWS Security Competency exam expects you to have a base knowledge of the services offered and how you can fortify them as a security engineer or professional.

Chapter Review Questions

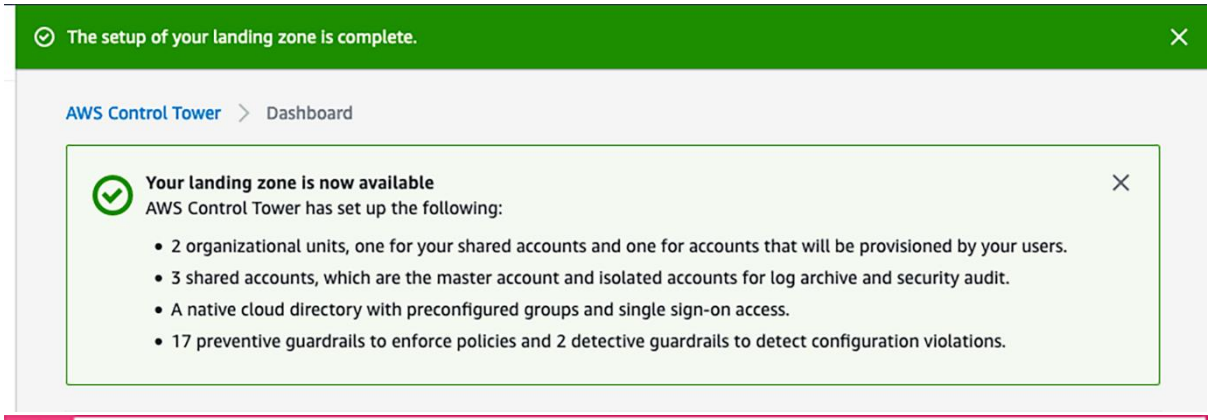
The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

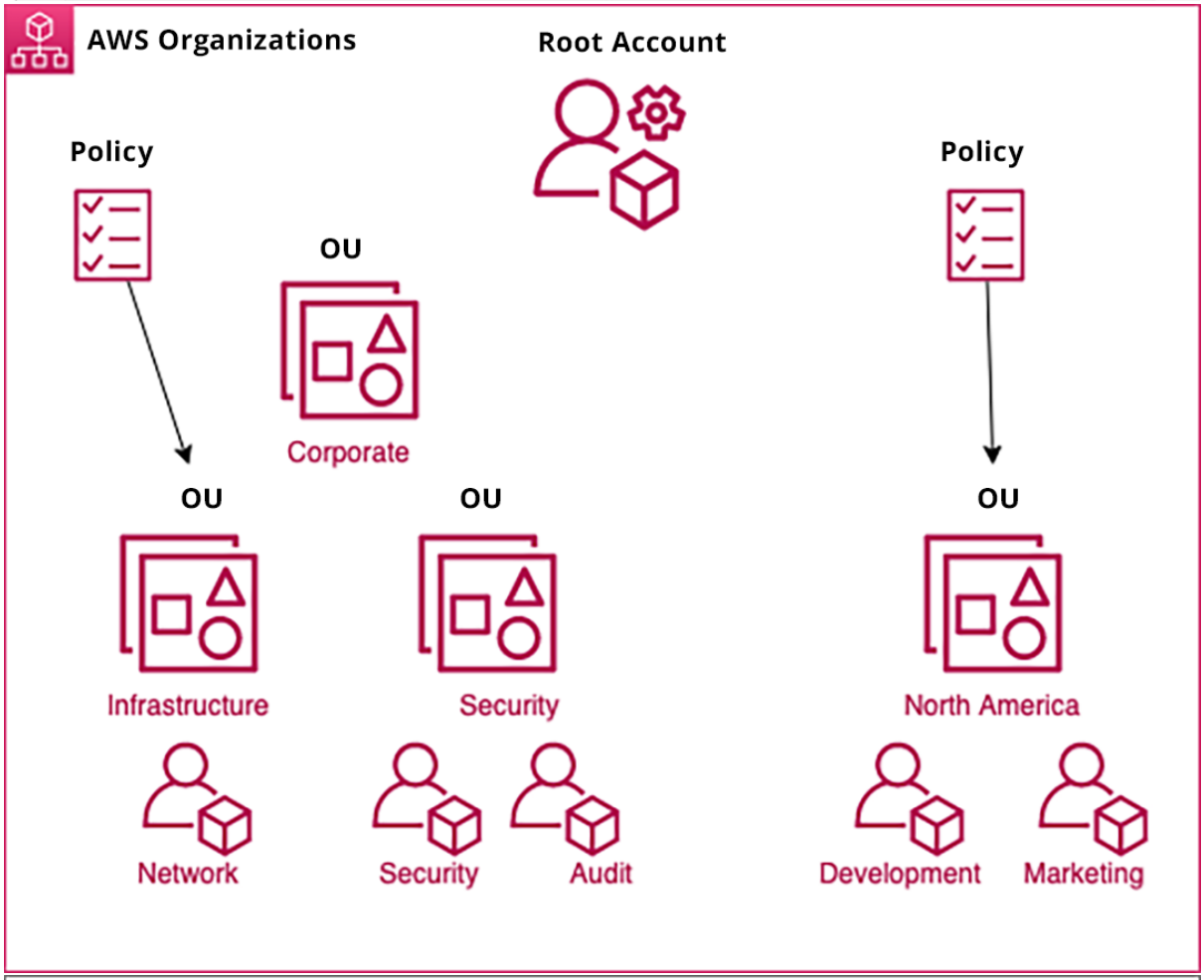
Select Quiz

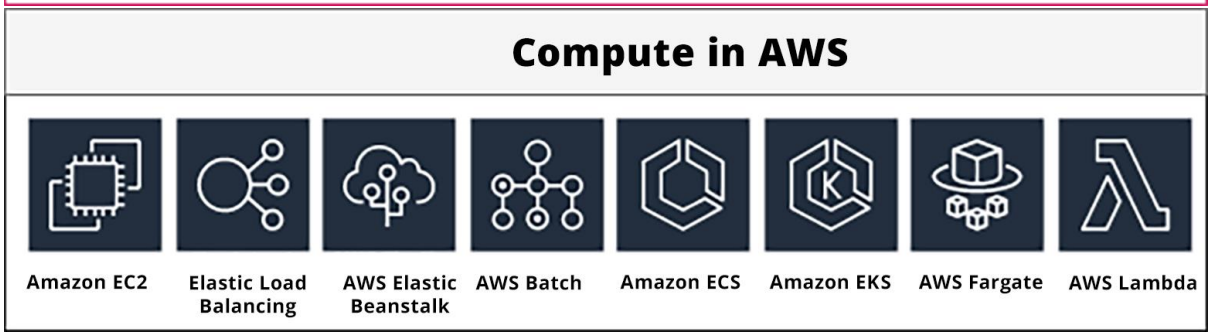
Quiz 1 START

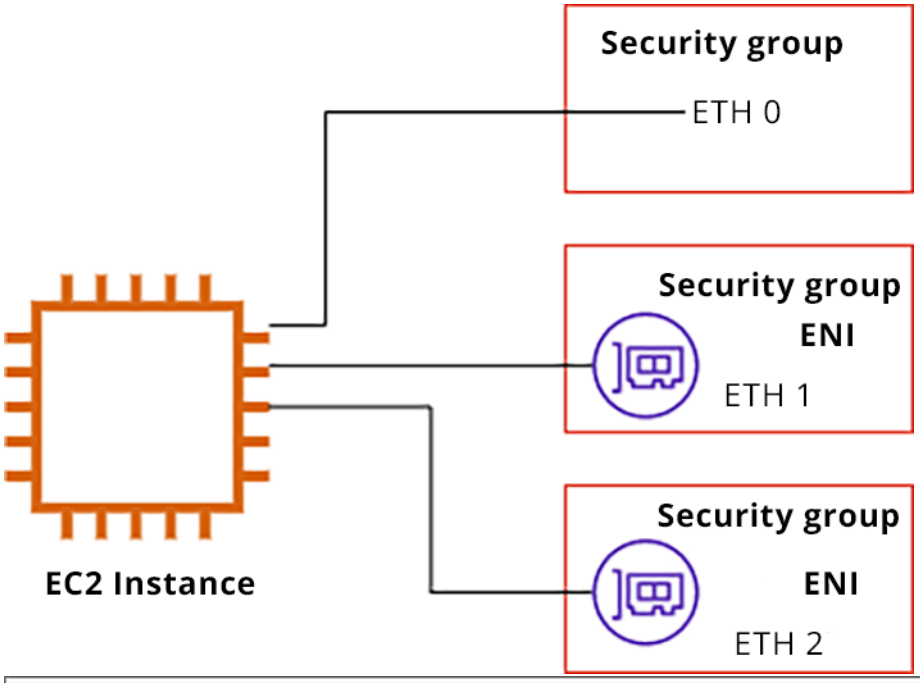
SHOW QUIZ DETAILS

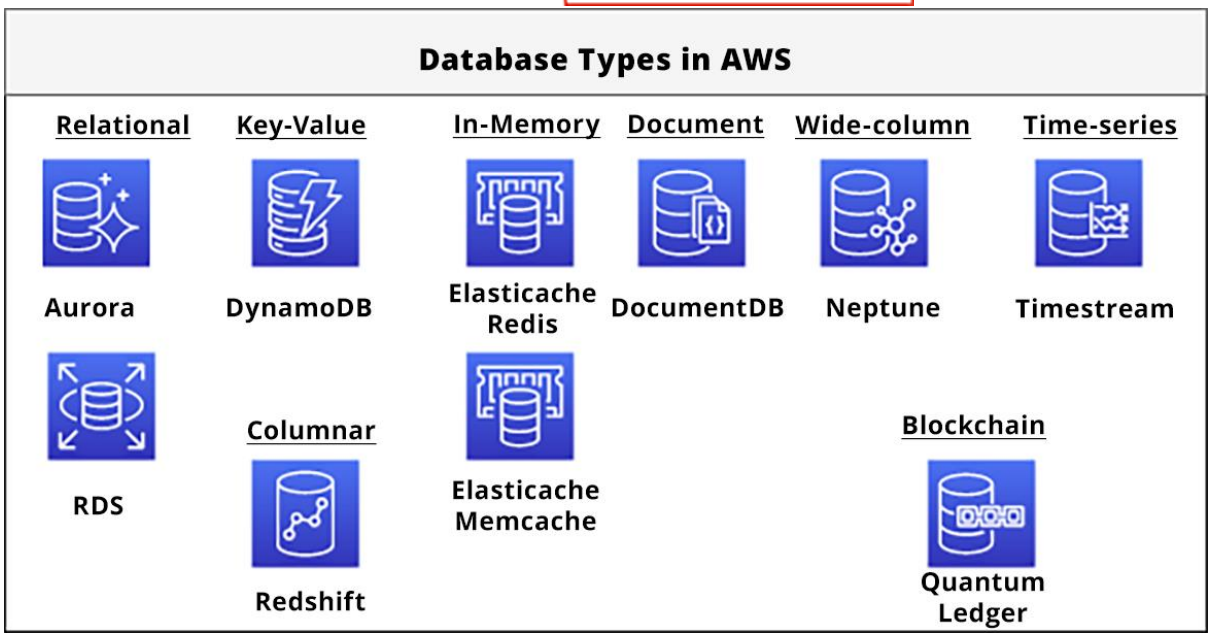
Chapter 2:

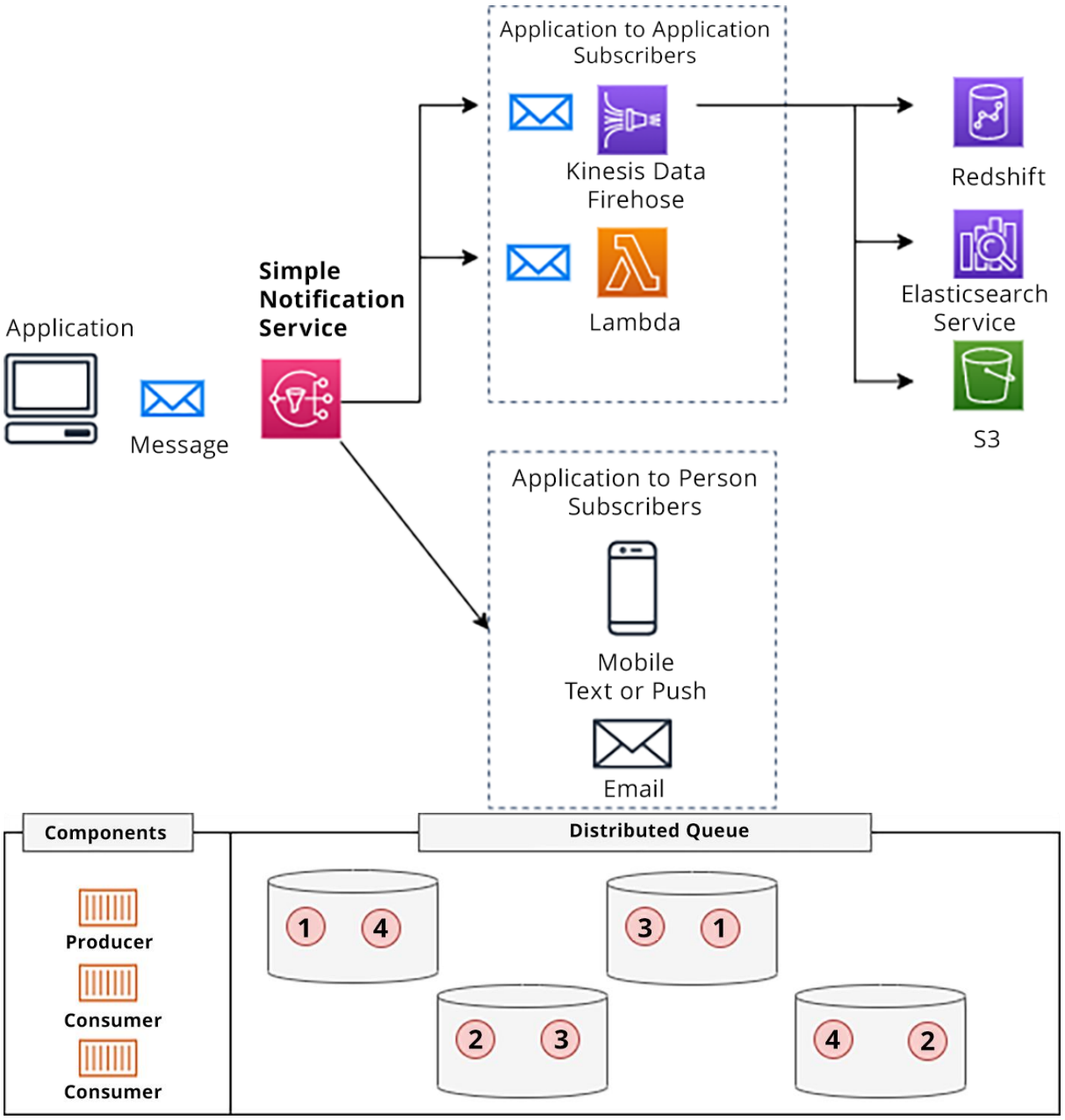

The setup of your landing zone is complete.
AWS Control Tower
Dashboard
Your landing zone is now available
AWS Control Tower has set up the following:
• 2 organizational units, one for your shared accounts and one for accounts that will be provisioned by your users.
• 3 shared accounts, which are the master account and isolated accounts for log archive and security audit.
• A native cloud directory with preconfigured groups and single sign-on access.
• 17 preventive guardrails to enforce policies and 2 detective guardrails to detect configuration violations.


AWS Organizations
Root Account
Policy
Policy
OU
Corporate
OU
OU
OU
Infrastructure
Security
North America
Network
Security
Audit
Development
Marketing


Compute in AWS
Amazon EC2
Elastic Load Balancing
AWS Elastic Beanstalk
AWS Batch
Amazon ECS
Amazon EKS
AWS Fargate
AWS Lambda


Security group
ETH 0
Security group
ENI
ETH 1
Security group
ENI
ETH 2
EC2 Instance


Database Types in AWS
Relational
Key-Value
In-Memory
Document
Wide-column
Time-series
Aurora
DynamoDB
Elasticache Redis
DocumentDB
Neptune
Timestream
RDS
Columnar
Elasticache Memcache
Blockchain
Redshift
Quantum Ledger


Application to Application
Subscribers
Kinesis Data
Firehose
Lambda
Redshift
Elasticsearch
Service
S3
Application
Message
Simple
Notification
Service
Application to Person
Subscribers
Mobile
Text or Push
Email
Components
Producer
Consumer
Consumer
Distributed Queue
1
4
3
1
2
3
4
2

Checks summary

0

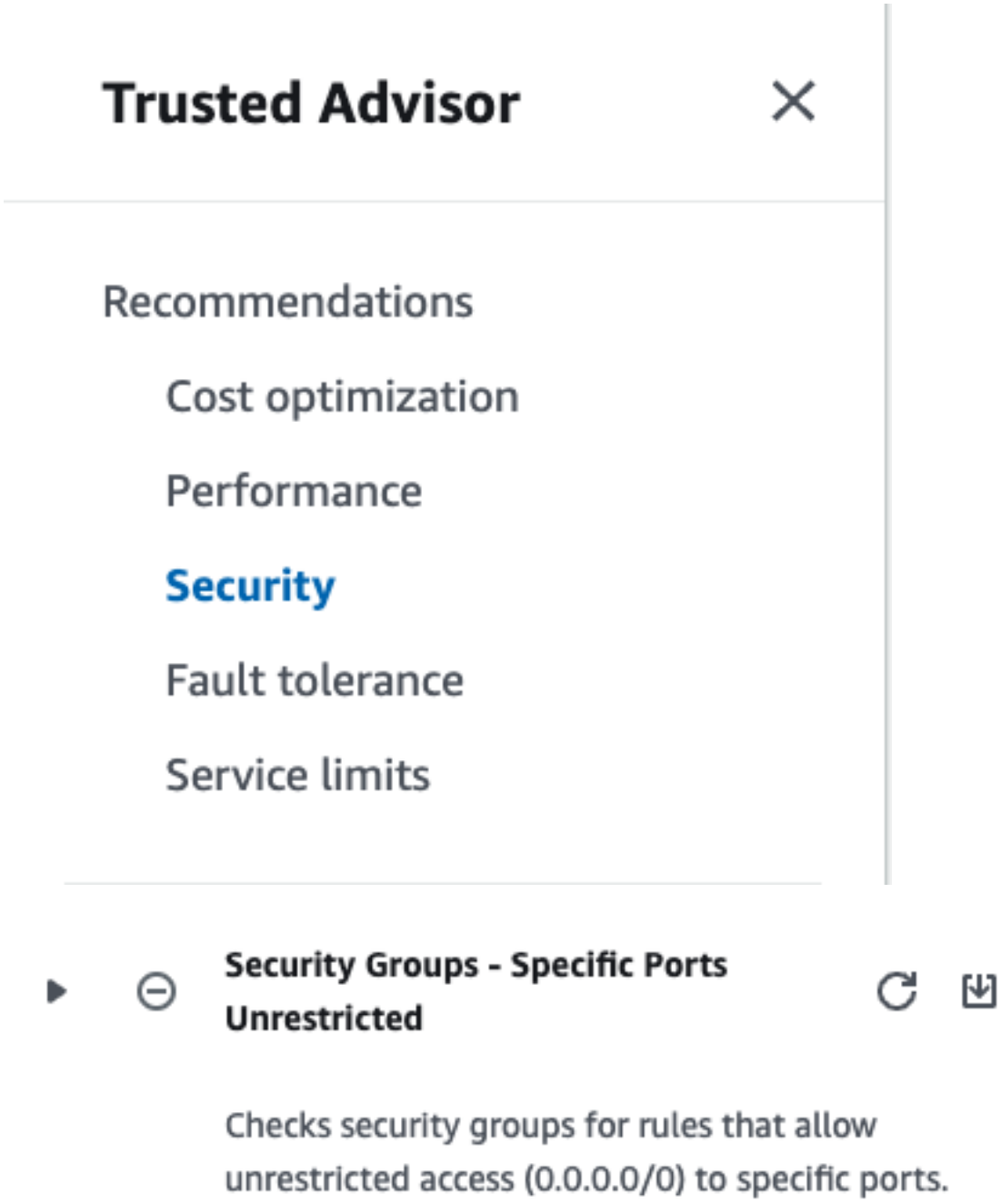
Action recommended Info

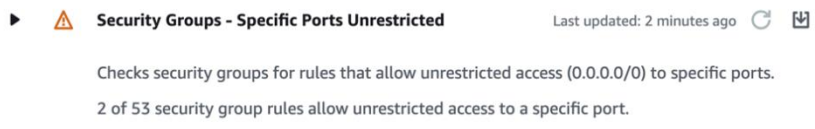
0

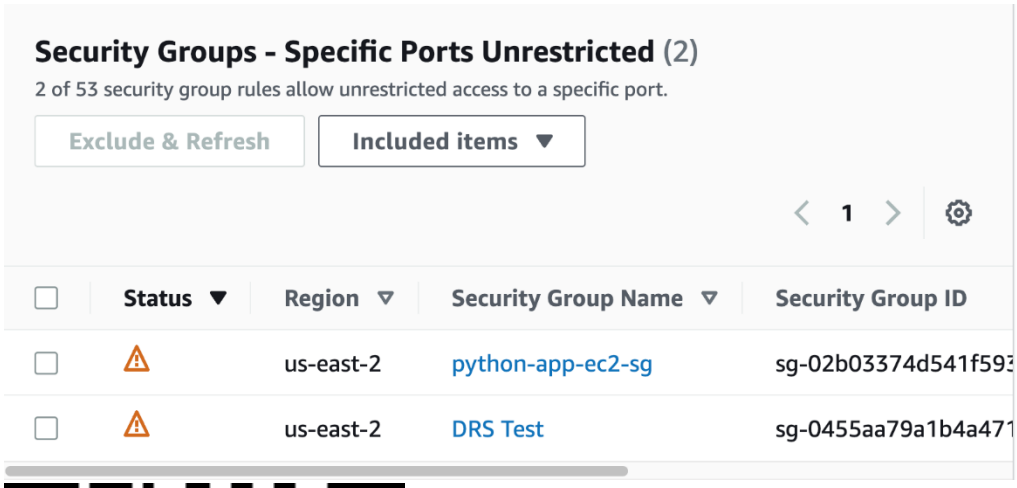
Investigation recommended Info

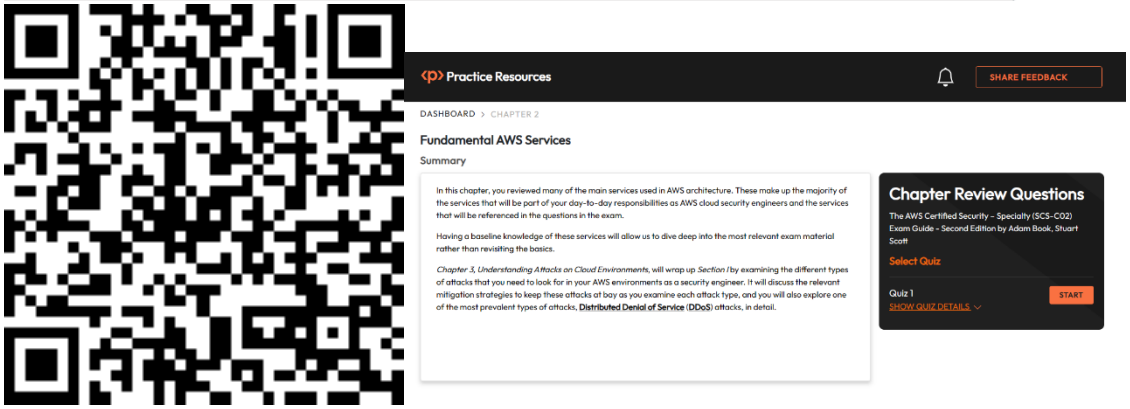
0

Checks with excluded items Info

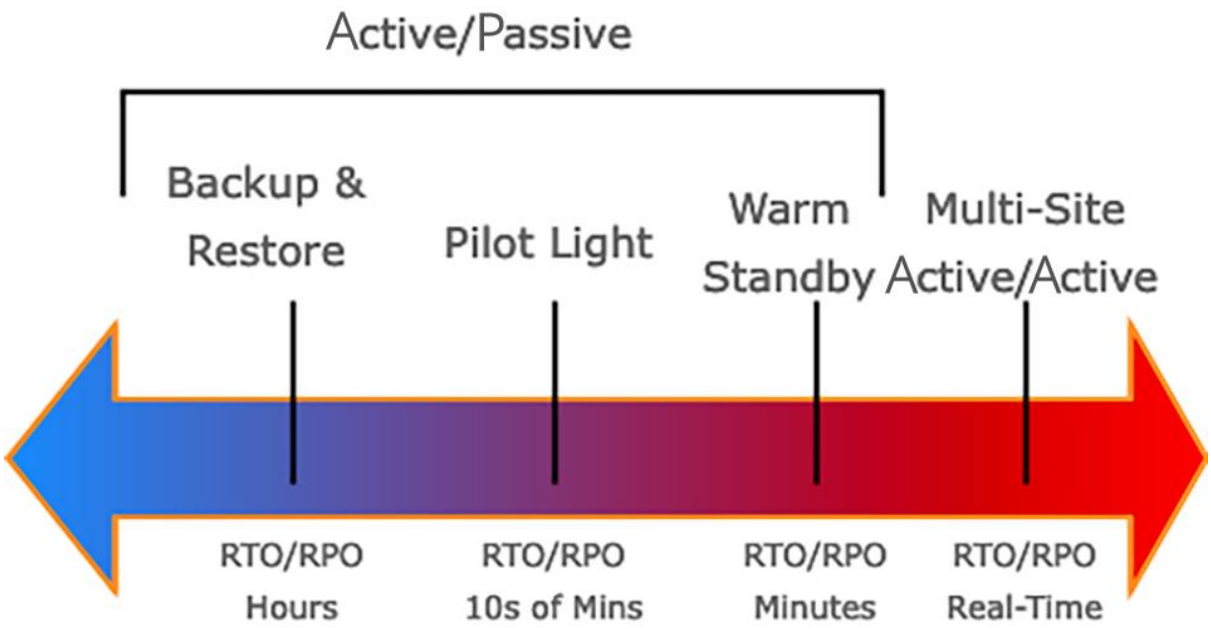

Trusted Advisor
Recommendations
Cost optimization
Performance
Security
Fault tolerance
Service limits
Security Groups - Specific Ports Unrestricted
Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

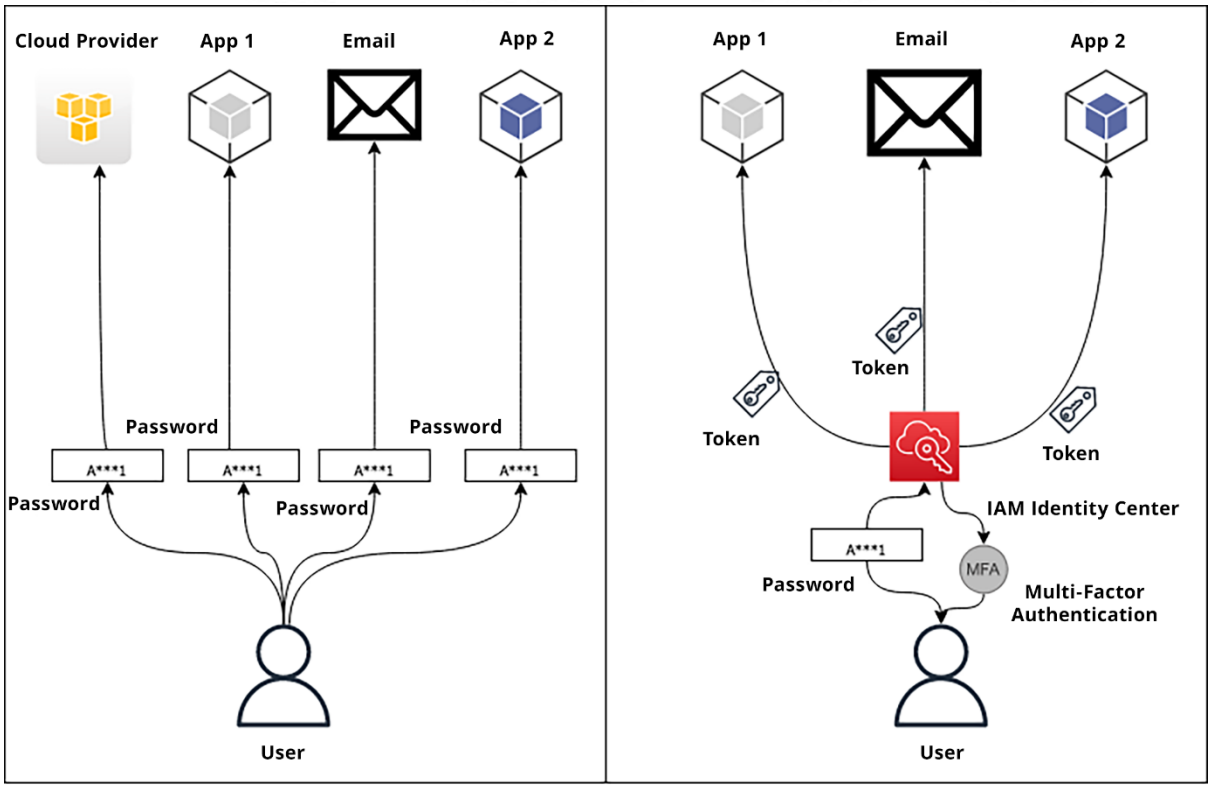

Security Groups - Specific Ports Unrestricted
Last updated: 2 minutes ago
Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.
2 of 53 security group rules allow unrestricted access to a specific port.


Security Groups - Specific Ports Unrestricted (2)
2 of 53 security group rules allow unrestricted access to a specific port.
Exclude & Refresh
Included items
1
Status
Region
Security Group Name
Security Group ID
us-east-2
python-app-ec2-sg
sg-02b03374d541f593
us-east-2
DRS Test
sg-0455aa79a1b4a471

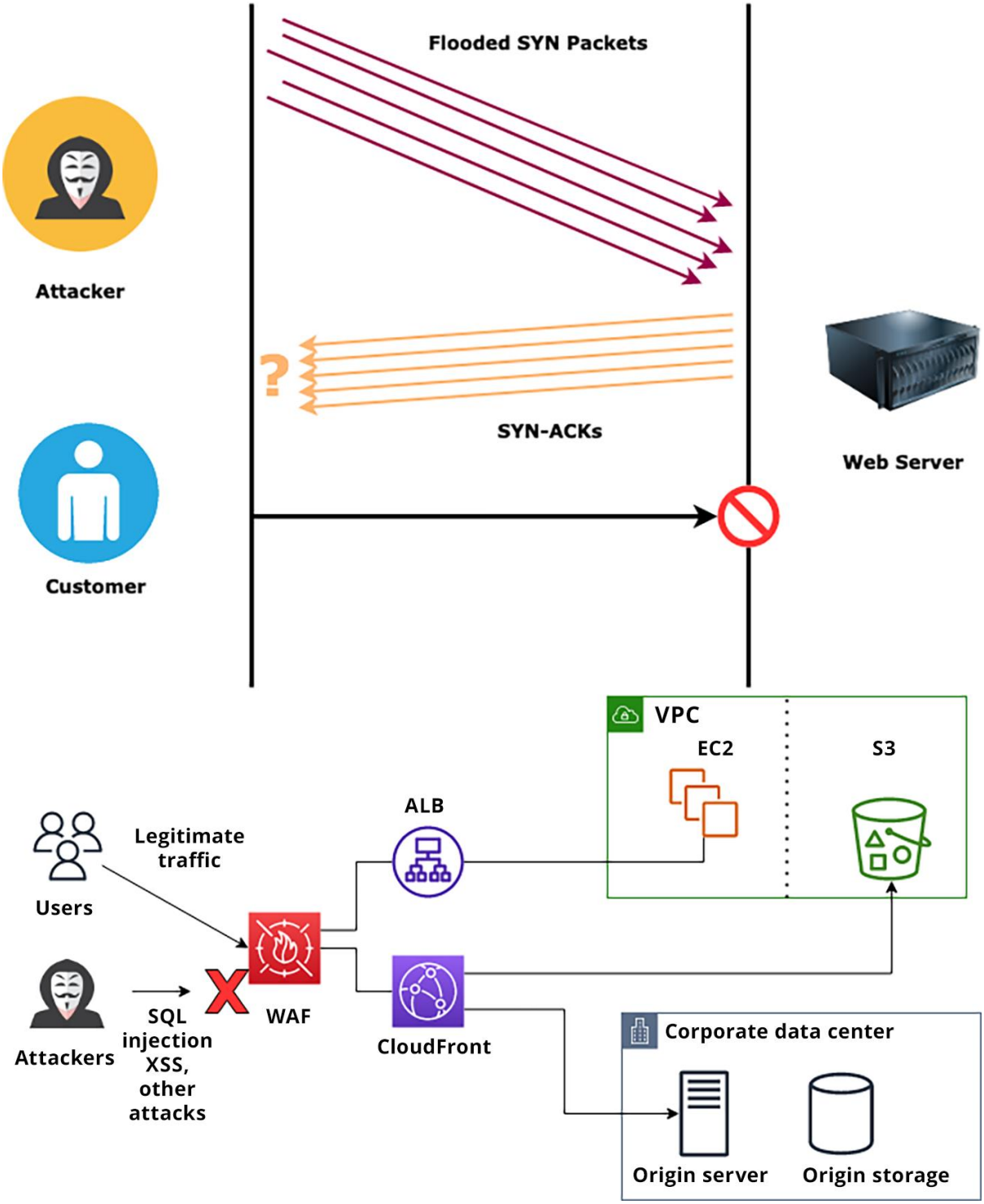

Practice Resources
SHARE FEEDBACK
DASHBOARD > CHAPTER 2
Fundamental AWS Services
Summary
In this chapter, you reviewed many of the main services used in AWS architecture. These make up the majority of the services that will be part of your day-to-day responsibilities as AWS cloud security engineers and the services that will be referenced in the questions in the exam.
Having a baseline knowledge of these services will allow us to dive deep into the most relevant exam material rather than revisiting the basics.
Chapter 3, Understanding Attacks on Cloud Environments, will wrap up Section I by examining the different types of attacks that you need to look for in your AWS environments as a security engineer. It will discuss the relevant mitigation strategies to keep these attacks at bay as you examine each attack type, and you will also explore one of the most prevalent types of attacks, Distributed Denial of Service (DDoS) attacks, in detail.
Chapter Review Questions
The AWS Certified Security - Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott
Select Quiz
Quiz 1
START
SHOW QUIZ DETAILS

Chapter 3:

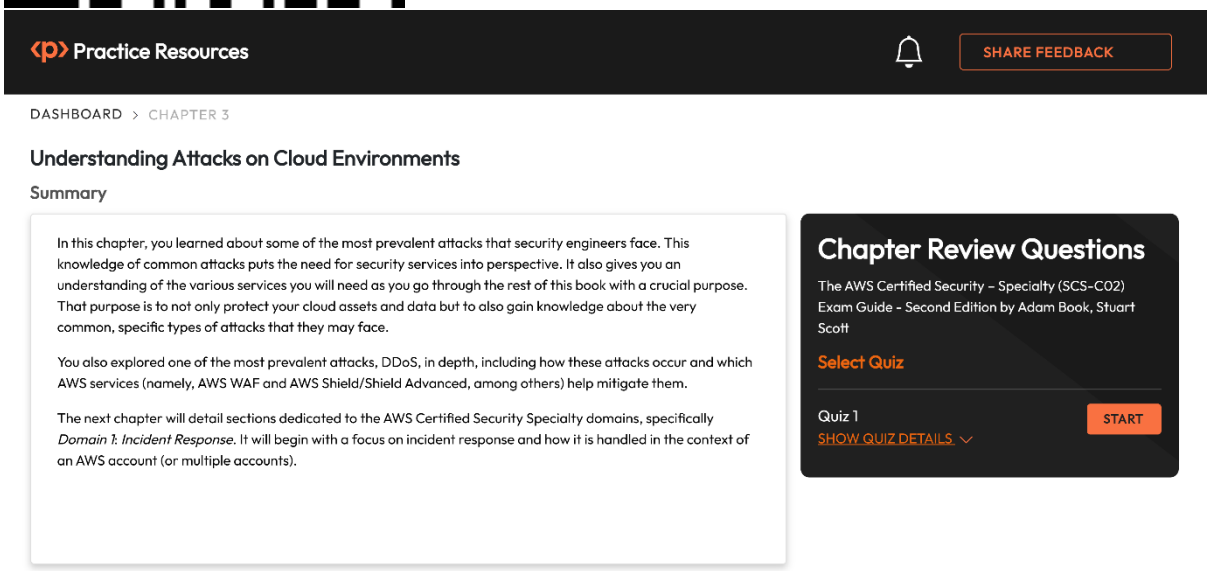




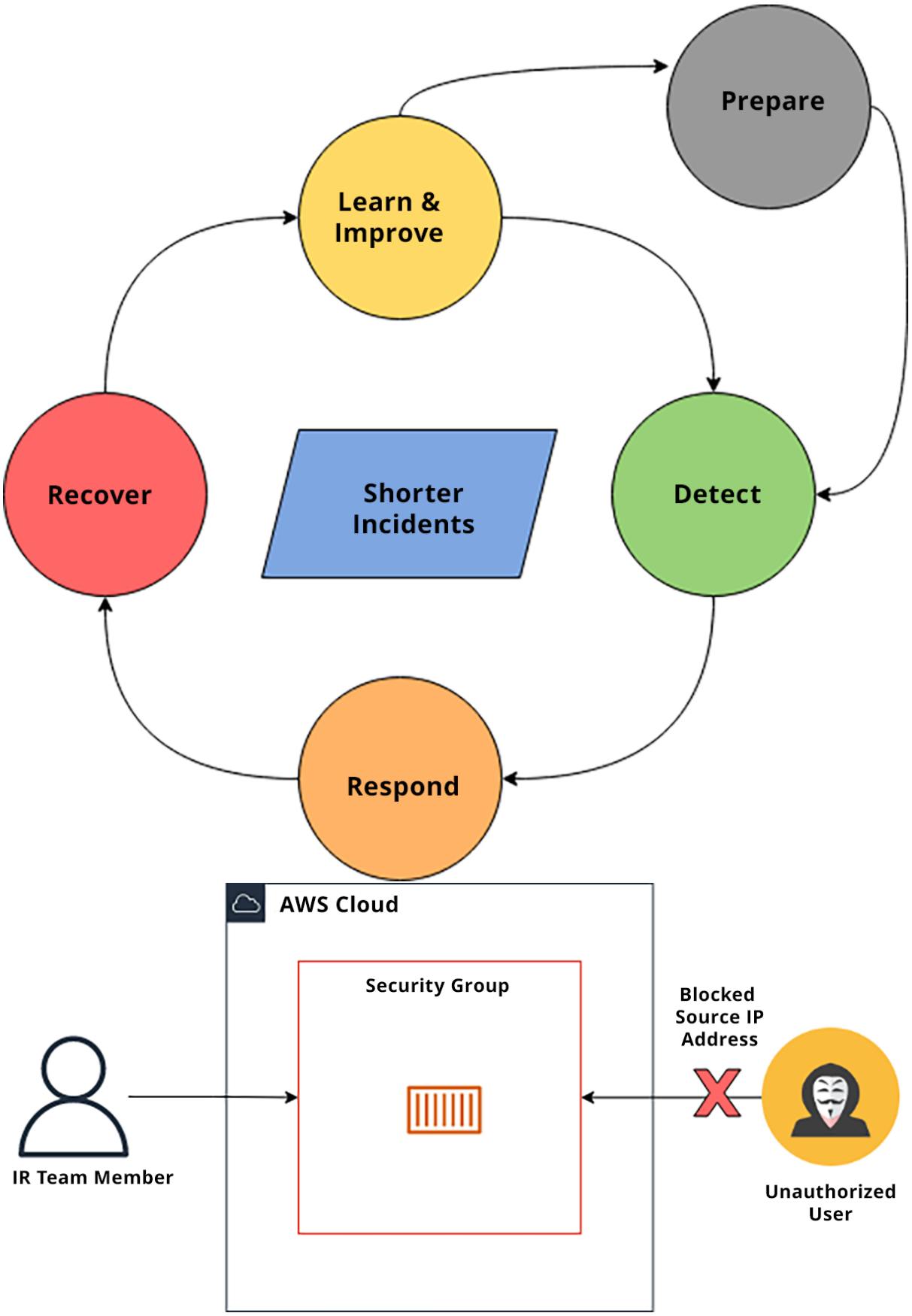
Multiple Identities **Identity Federation**

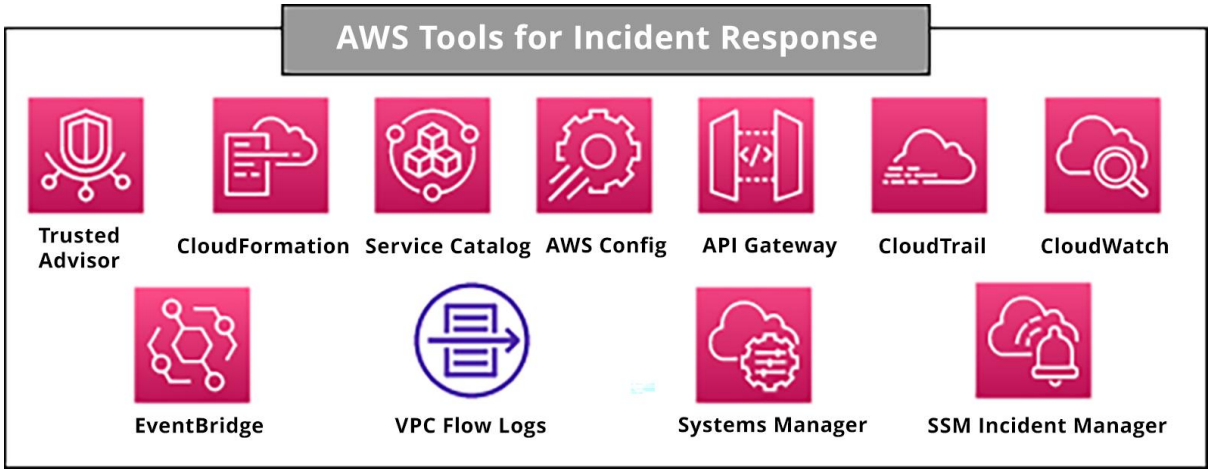

Flooded SYN Packets
Attacker
?
SYN-ACKs
Web Server
Customer
VPC
EC2
S3
ALB
Legitimate traffic
Users
WAF
CloudFront
Attackers
SQL injection XSS, other attacks
Corporate data center
Origin server
Origin storage

	AWS Shield	AWS Shield Advanced
Basic protection against DDoS attacks		
No additional cost		
custom mitigation rules		
Access to the DDoS response team		
Pricing based on number of resources protected		

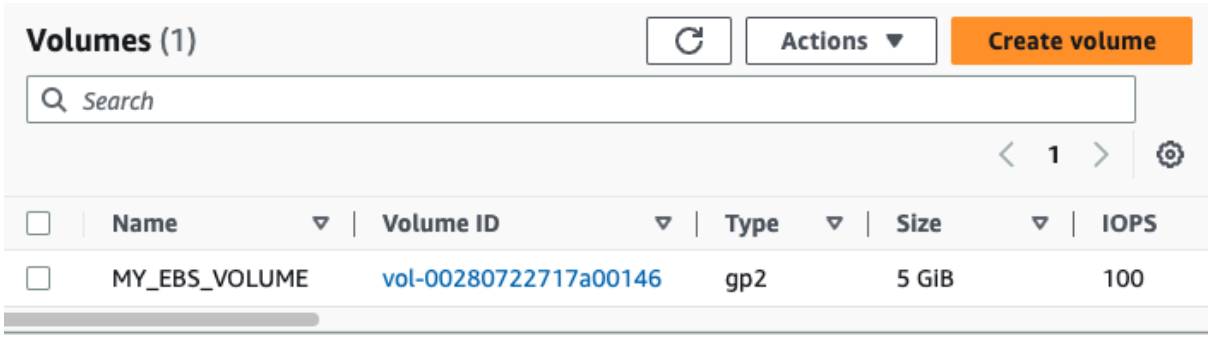


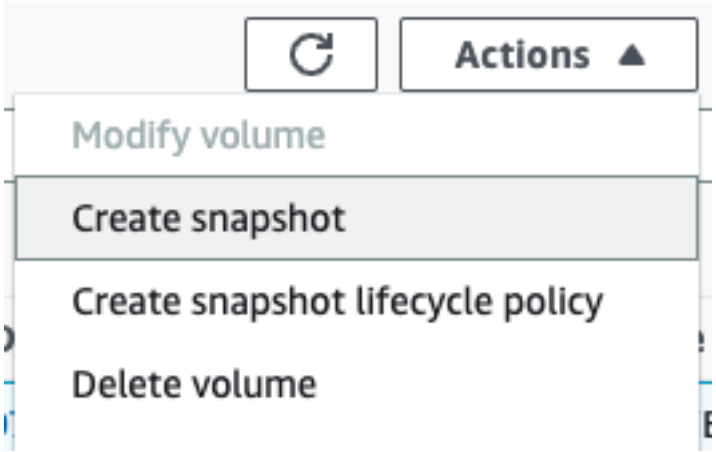
Chapter 4:


Prepare
Learn & Improve
Recover
Shorter Incidents
Detect
Respond
AWS Cloud
Security Group
Blocked Source IP Address
IR Team Member
Unauthorized User


AWS Tools for Incident Response
Trusted Advisor
CloudFormation
Service Catalog
AWS Config
API Gateway
CloudTrail
CloudWatch
EventBridge
VPC Flow Logs
Systems Manager
SSM Incident Manager


Elastic Block Store
Volumes
Snapshots
Lifecycle Manager


Volumes (1)
Actions
Create volume
Search
1
Name
Volume ID
Type
Size
IOPS
MY_EBS_VOLUME
vol-00280722717a00146
gp2
5 GiB
100


Actions
Modify volume
Create snapshot
Create snapshot lifecycle policy
Delete volume

Create snapshot Info

Create a point-in-time snapshot to back up the data on an Amazon EBS volume to Amazon S3.

Details

Volume ID

vol-00280722717a00146 (MY_EBS_VOLUME)

Description

Add a description for your snapshot

IR Snapshot

255 characters maximum.

Encryption Info

Not encrypted

Successfully created snapshot snap-06dcb1580d269b892 from volume vol-00280722717a00146.
If you need your snapshot to be immediately available consider using Fast Snapshot Restore.

Manage fast snapshot restore

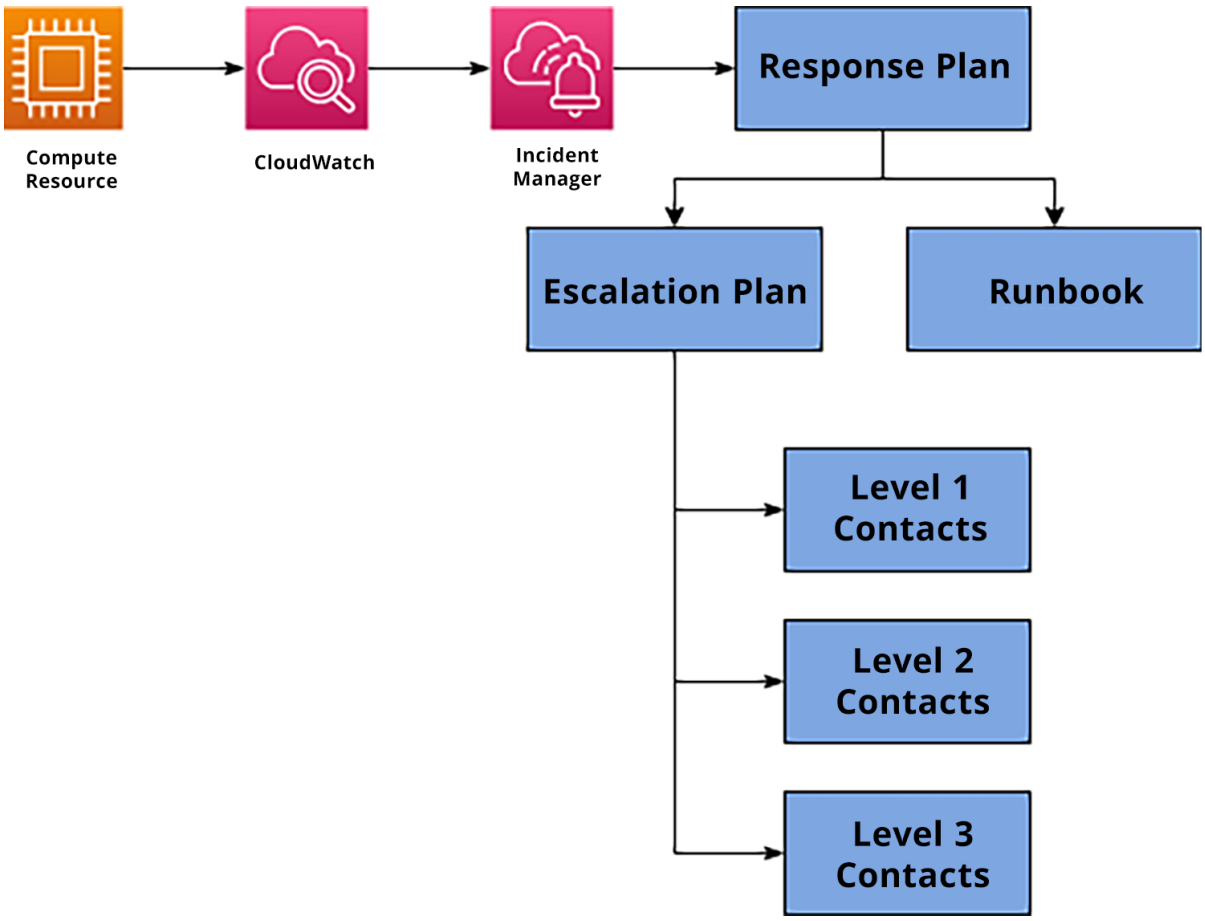
Snapshots (3)

Recycle Bin | Actions | Create snapshot

Owned by me | Search

1

Name	Snapshot ID	Size	Description
IR_snapshot	snap-024fa1245efc875ec	5 GiB	IR Snapshot



Select trusted entity Info

Trusted entity type

- **AWS service** — Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- **AWS account** — Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- **Web identity** — Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

Use cases for other AWS services:

Incident Manager

- **Incident Manager Service Role** — Allows Incident Manager to manage incident records and related resources on your behalf.
- **Incident Manager** — Allows Incident Manager to call AWS services on your behalf

How it works

Respond faster to incidents by preparing an incident response plan. Let us help you create one.

General settings

In general settings you configure which AWS Regions Incident Manager will replicate

Set up

Contact details - *optional*

their contact channels to engage them quickly and efficiently during an incident.

Create contact

Escalation plans - *optional*

Escalation plans engage your contacts in timed stages to ensure the correct contacts are

Create escalation plan

Response plan

Respond quickly and automatically using response plans. Response plans bring

Create response plan

Regions

Choose the Regions you want to replicate data to.

Select Regions

US East (Ohio) ×
us-east-2

This key will be used to encrypt and decrypt your resources. Learn more about KMS

(•) Use AWS owned key

( ) Choose an existing AWS KMS key

Contact details

Name

The name appears in response plans and escalation plans.

JoeJones

The contact name must have 1-255 characters. Valid characters: Alphanumeric characters, _ (underscore), - (hyphen), and spaces.

Unique alias

The unique alias appears in escalation plans, response plans, and incidents. It can help you quickly find the correct contact.

jjones

The contact unique alias must have 1-50 characters. Valid characters a-z, 0-9, _ (underscore), and - (hyphen).

Contact channel

Contact channels are the methods Incident Manager can use to engage a contact. Use contact channels to define an engagement plan and engage the contact.

Type	Channel name	Detail	
SMS	Tier1	+1234567890	Remove

Add contact channel

Response plan details

Name

The response plan name must be unique and can't be changed after creation. The name is used to create the response plan ARN or in response plans with no display name.

EC2-Shutdown-US-EAST-2

The response plan name must be between 1-200 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Display name - *optional*

The display name helps you identify the response plan when creating incidents.

EC2-Shutdown-US-EAST_2

Incident defaults

Title

The incident title must be unique, identifiable, and relatable to the incident. The incident title appears in the incidents list followed by the incident ARN.

Shutdown EC2 Instance

Impact

The impact defines the impact to customers and scope of the incident.

High

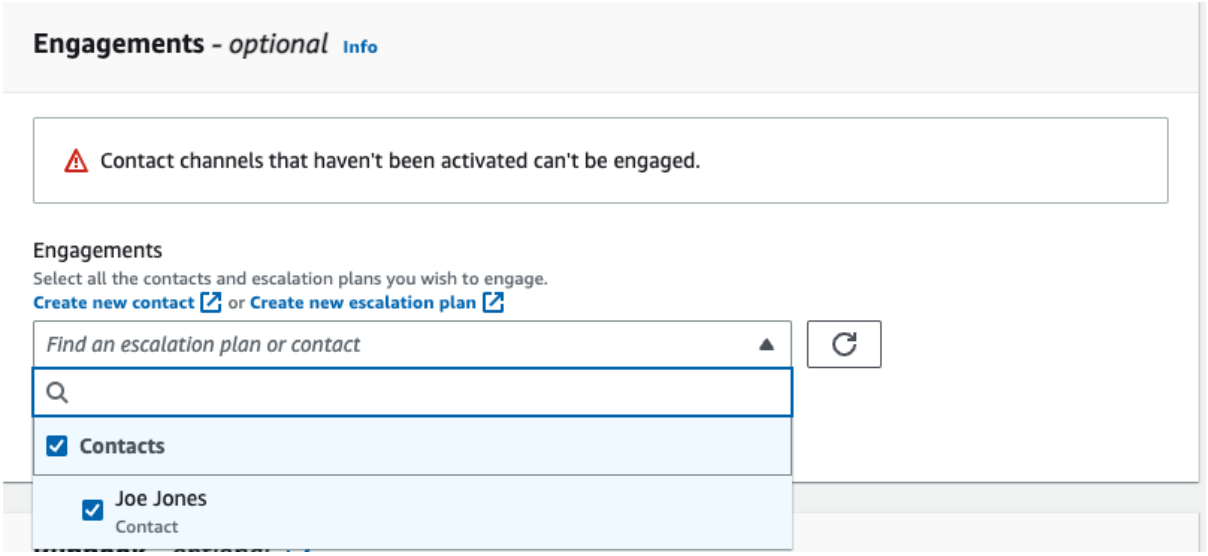
Summary - *optional*

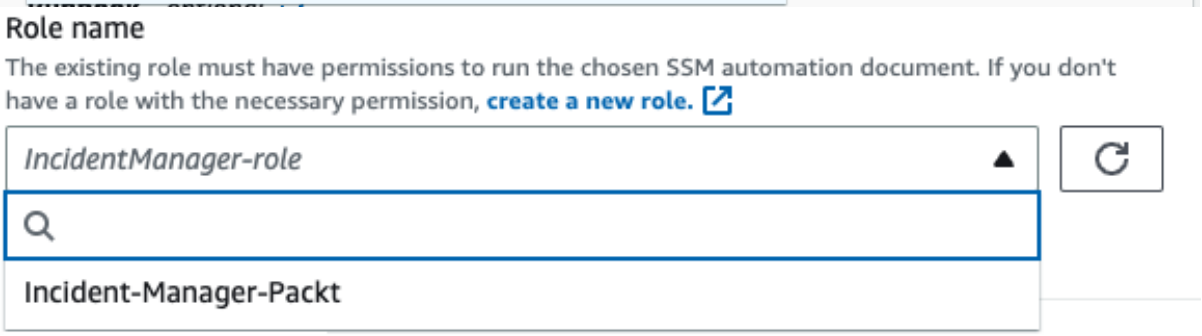
The summary is a brief description that is used to provide an overview of the incident. Use Markdown to format the content.

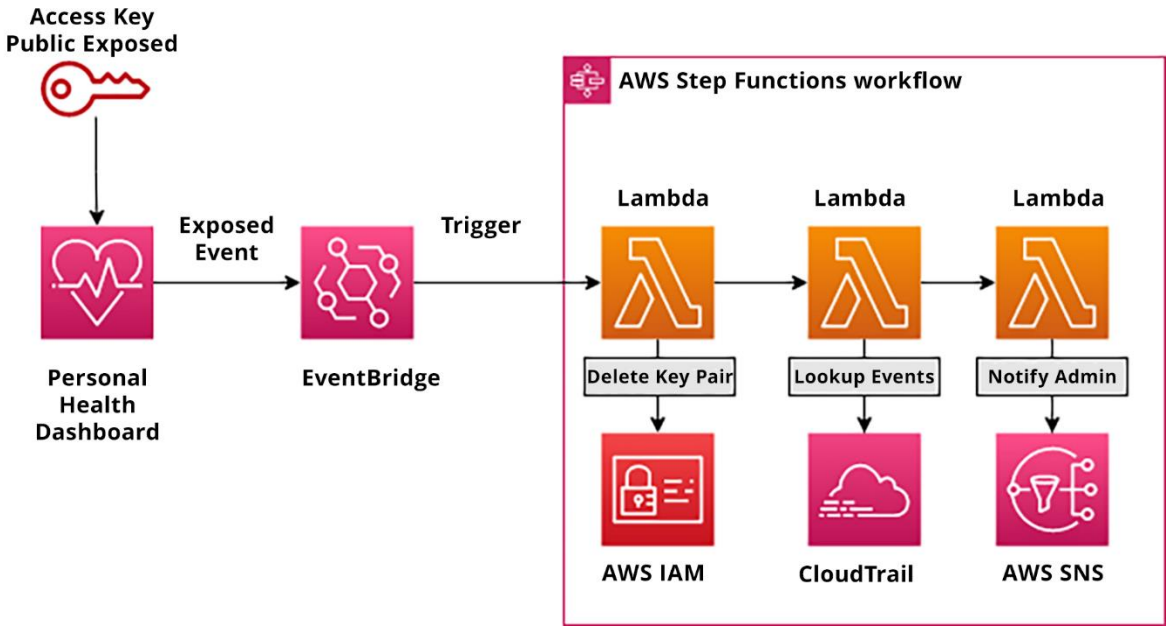
Learn more

This will set the state of the EC2 instance to Shutdown - turning the instance off

This will set the state of the EC2 instance to Shutdown - turning the instance off


Engagements - optional Info
Contact channels that haven't been activated can't be engaged.
Engagements
Select all the contacts and escalation plans you wish to engage.
Create new contact or Create new escalation plan
Find an escalation plan or contact
Contacts
Joe Jones
Contact


Role name
The existing role must have permissions to run the chosen SSM automation document. If you don't have a role with the necessary permission, create a new role.
IncidentManager-role
Incident-Manager-Packt


Access Key
Public Exposed
Personal
Health
Dashboard
Exposed
Event
EventBridge
Trigger
AWS Step Functions workflow
Lambda
Lambda
Lambda
Delete Key Pair
Lookup Events
Notify Admin
AWS IAM
CloudTrail
AWS SNS

Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 4

Incident Response

Summary

This chapter examined the first domain of the AWS Certified Security – Specialty certification: IR. You were given a brief overview of two significant articles published on this topic: *Security Pillar - Well-Architected Framework* and *AWS Incident Response* whitepaper.

You learned how to detect events that may need to be addressed by your IR team, both from a logging and an alerting perspective.

You also looked at how using native tools such as AWS System Manager can help automate the response when an incident has been detected and can contact pre-defined personnel and track the progress of the incident. Finally, you saw how different IR operation procedures could be implemented from either a human intervention standpoint or using automation.

In the next chapter, you will look at another tool used in IR, AWS Config. It can help you become more proactive and show what changes are made to a specific resource.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

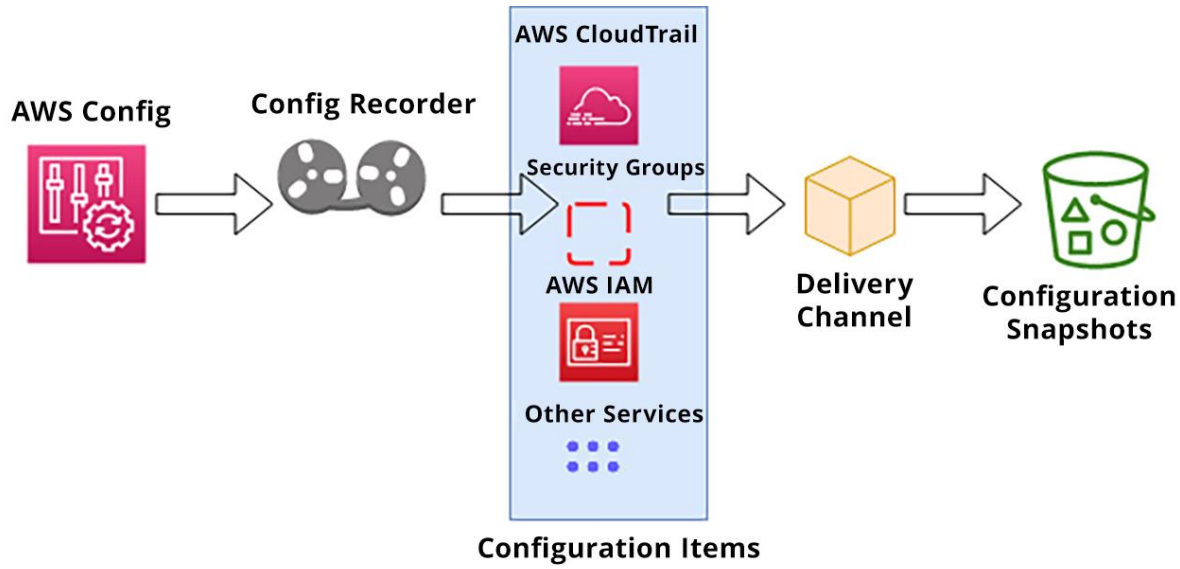
Select Quiz

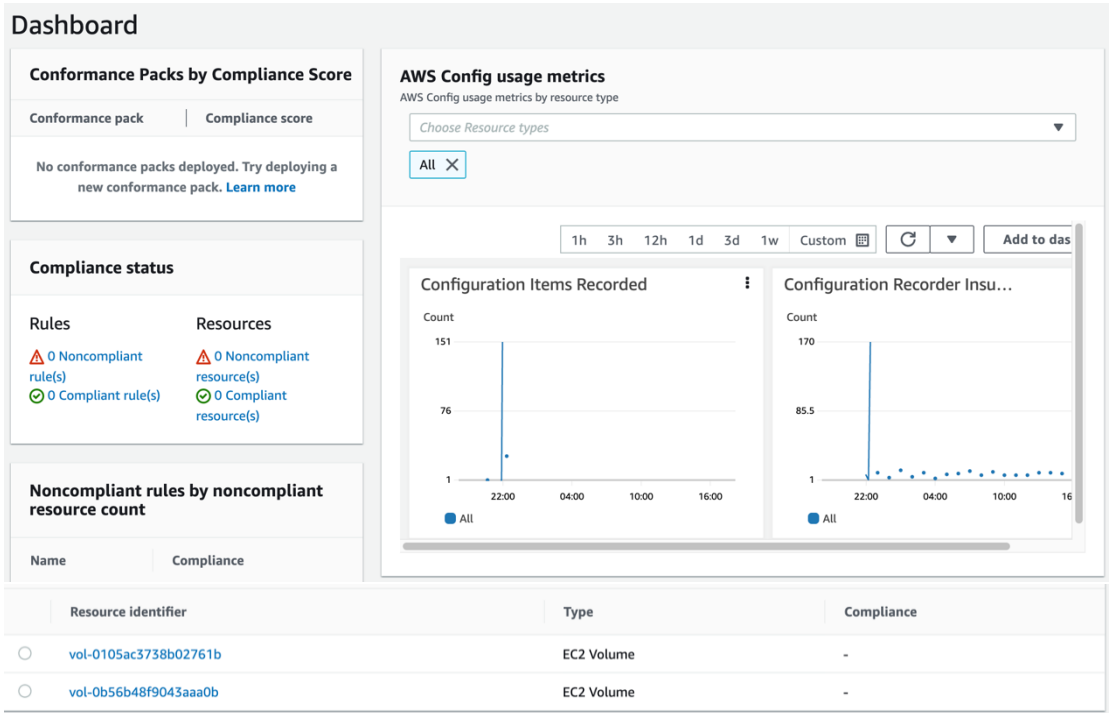
Quiz 1

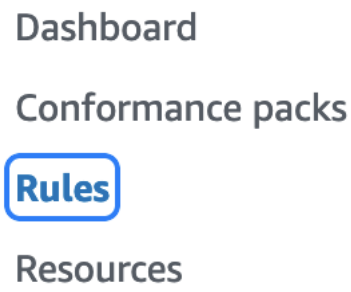
SHOW QUIZ DETAILS

START

Chapter 5:


AWS Config
Config Recorder
AWS CloudTrail
Security Groups
AWS IAM
Other Services
Configuration Items
Delivery Channel
Configuration Snapshots

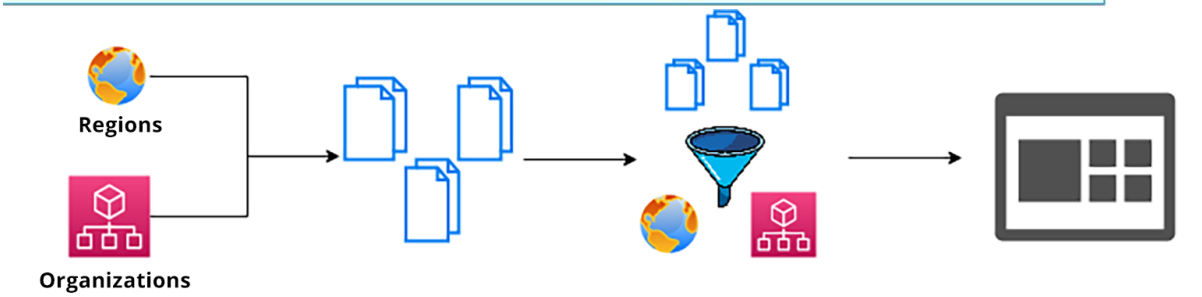

Dashboard
Conformance Packs by Compliance Score
Conformance pack
Compliance score
No conformance packs deployed. Try deploying a new conformance pack. Learn more
Compliance status
Rules
0 Noncompliant rule(s)
0 Compliant rule(s)
Resources
0 Noncompliant resource(s)
0 Compliant resource(s)
Noncompliant rules by noncompliant resource count
Name
Compliance
AWS Config usage metrics
AWS Config usage metrics by resource type
Choose Resource types
All
1h 3h 12h 1d 3d 1w Custom
Add to das
Configuration Items Recorded
Configuration Recorder Insu…
Count
151
76
1
170
85.5
22:00 04:00 10:00 16:00
All
Resource identifier
Type
Compliance
vol-0105ac3738b02761b
EC2 Volume
-
vol-0b56b48f9043aaa0b
EC2 Volume
-


Dashboard
Conformance packs
Rules
Resources

AWS Managed Rules (2)

restricted-ssh

	Name	Labels	Supported evaluation mode	Description
○	nacl-no-unrestricted-ssh-rdp	NACL, SSH, RDP, RESTRICTED, NETWORK, ACL, TCP	DETECTIVE	Checks if default ports for SSH tcp/22 or RDP tcp/3389 ingress traffic for network access control lists (NACLs) is unrestricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source CIDR block of '0.0.0.0/0' or '::/0' for ports 22 or 3389.
◉	restricted-ssh	EC2	DETECTIVE	Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.



Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 5

Managing Your Environment with AWS Config

Summary

In this chapter, you examined the AWS Config service in detail. You saw how to start the configuration recorder to begin inventorying the resources in our AWS account, and reviewed the different types of rules available for AWS Config and how the rules get triggered inside an account.

You also learned how to use AWS Config in a multi-account or multi-Region setup and the differences between using a single-account setup. The chapter concluded with a list of the key points on the AWS Config service you will need to know for the AWS exam.

Chapter 6, Event Management with Security Hub and GuardDuty, will discuss the Incident Response pillar, diving deep into the services of AWS Security Hub and AWS GuardDuty. You will see how these two services can work hand in hand and provide visibility into your accounts while simultaneously detecting abnormalities that need to be remediated.

Chapter Review Questions

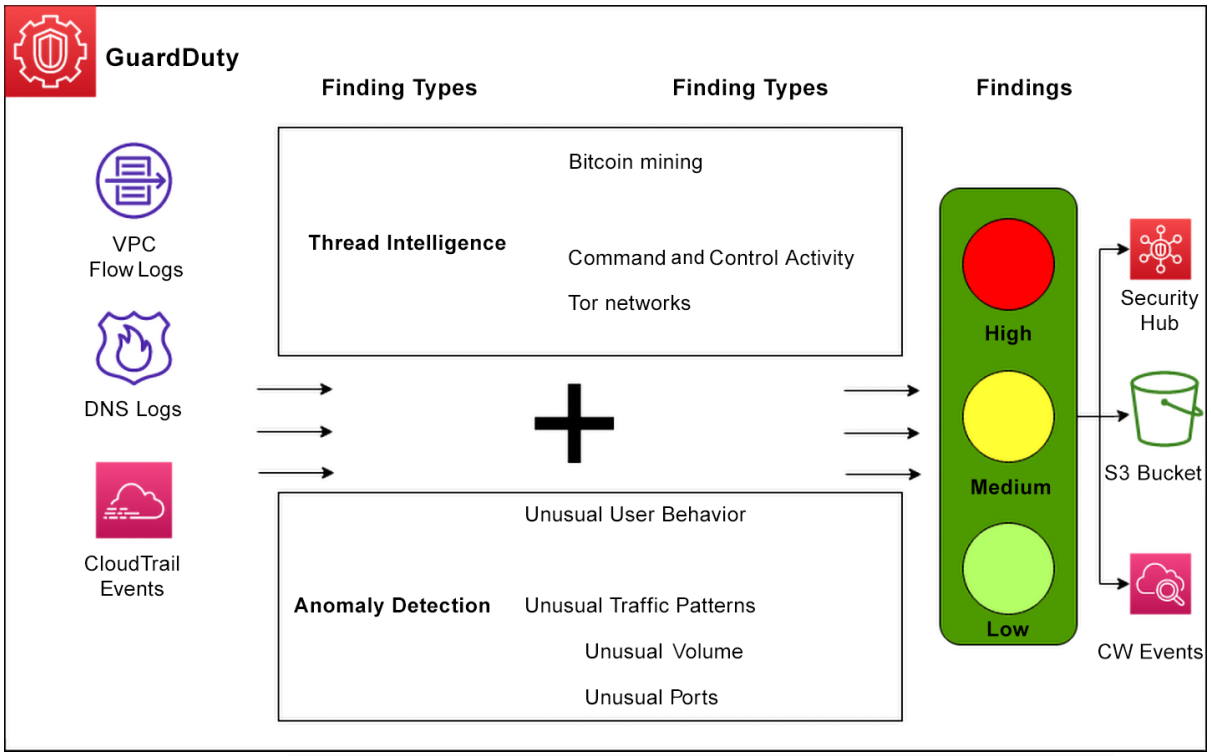
The AWS Certified Security – Specialty (SCS-C02) Exam Guide – Second Edition by Adam Book, Stuart Scott

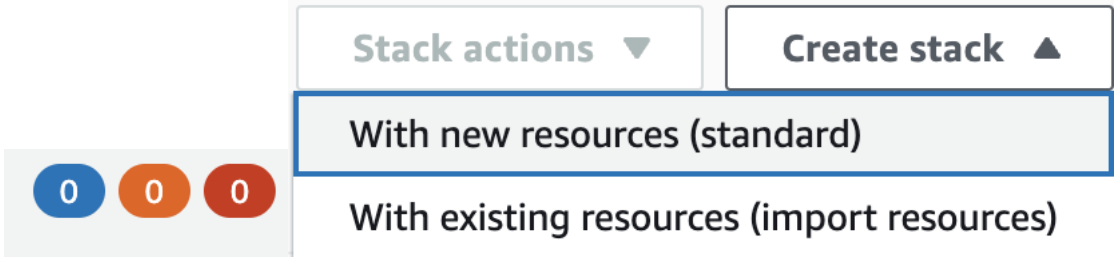
Select Quiz

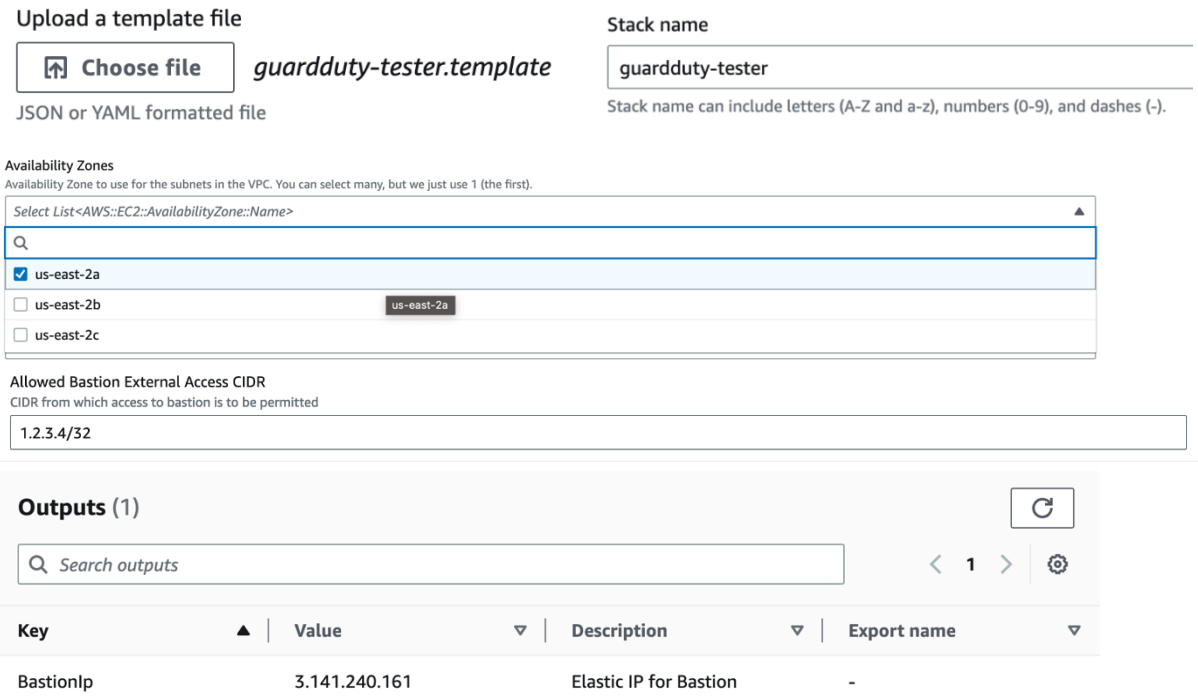
Quiz 1 START

SHOW QUIZ DETAILS

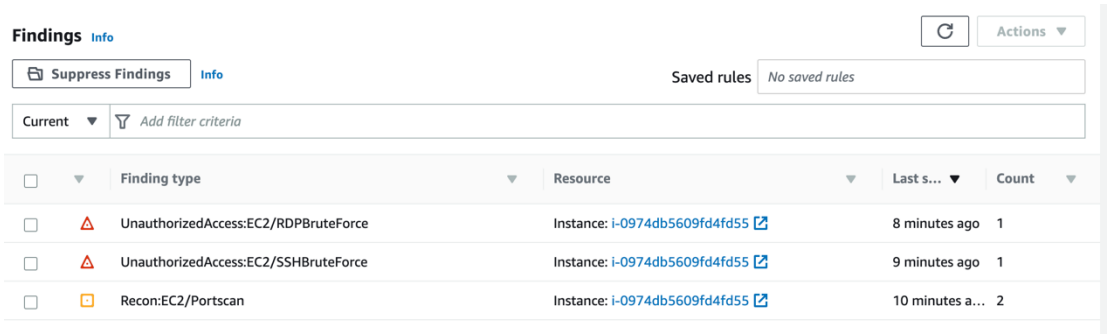
Chapter 6:

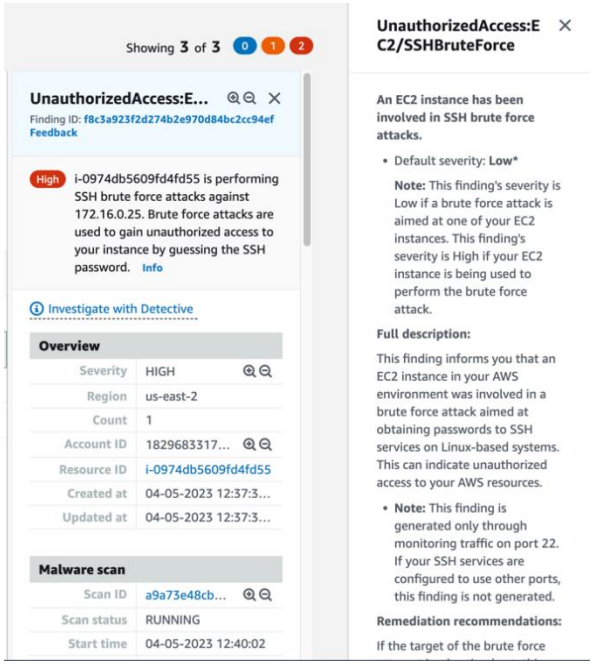

GuardDuty
Finding Types
Finding Types
Findings
VPC Flow Logs
DNS Logs
CloudTrail Events
Thread Intelligence
Bitcoin mining
Command and Control Activity
Tor networks
Anomaly Detection
Unusual User Behavior
Unusual Traffic Patterns
Unusual Volume
Unusual Ports
High
Medium
Low
Security Hub
S3 Bucket
CW Events

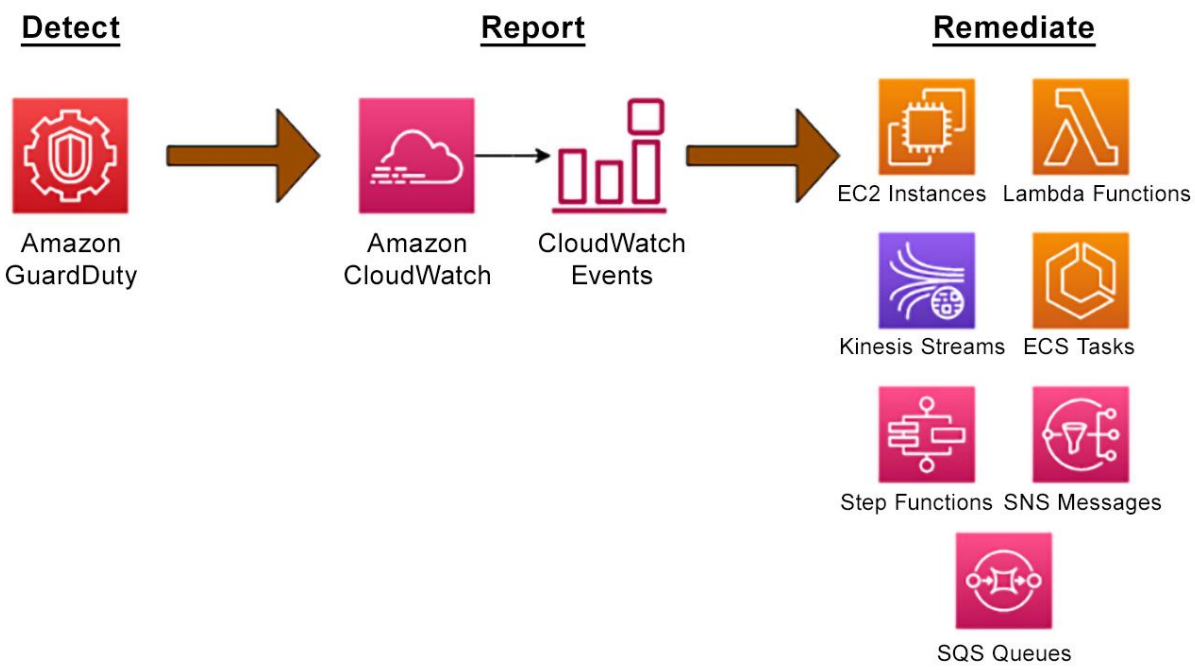

Stack actions
Create stack
With new resources (standard)
With existing resources (import resources)
0
0
0

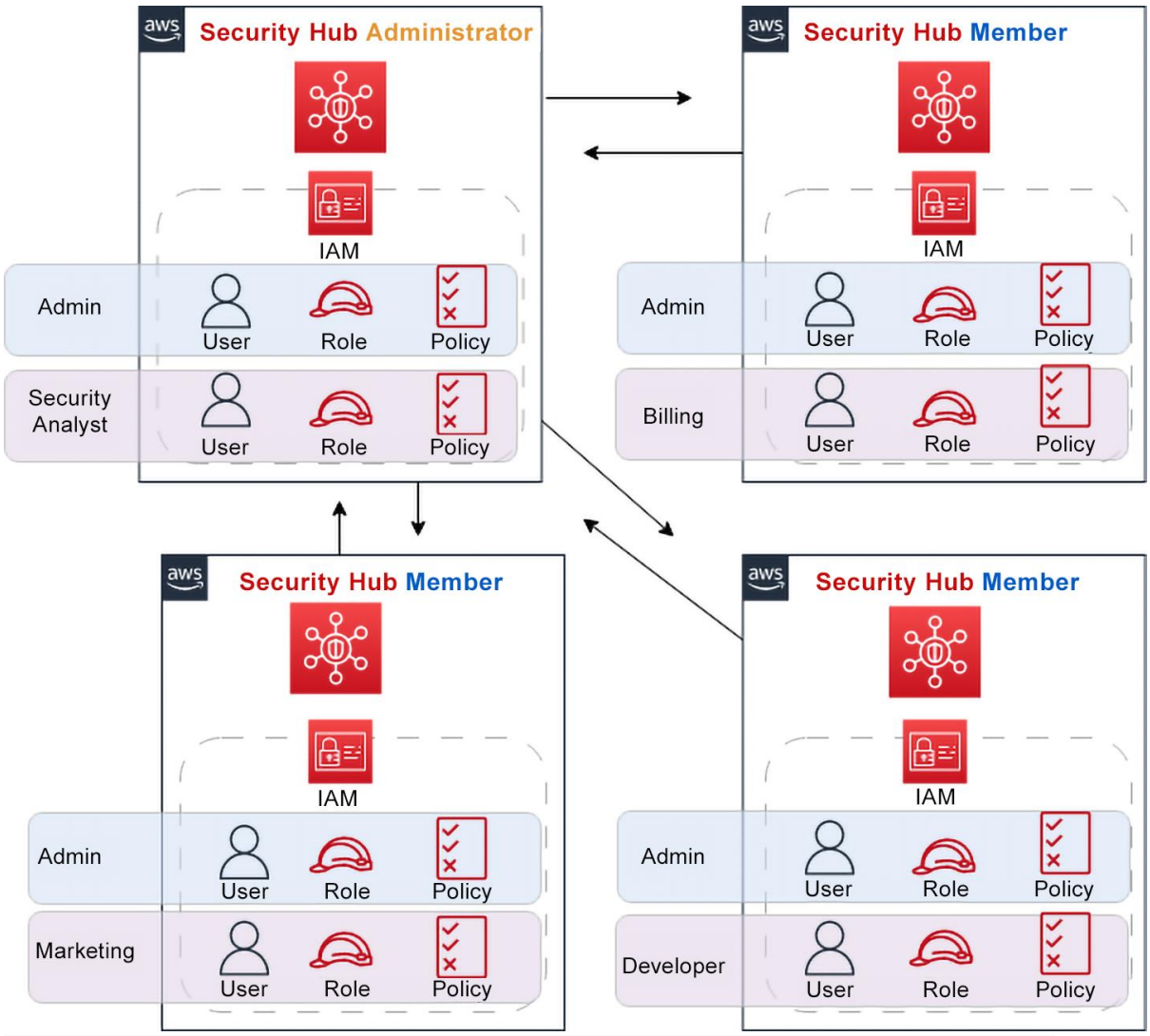

Upload a template file
Choose file
guardduty-tester.template
JSON or YAML formatted file
Stack name
guardduty-tester
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Availability Zones
Availability Zone to use for the subnets in the VPC. You can select many, but we just use 1 (the first).
Select List<AWS::EC2::AvailabilityZone::Name>
us-east-2a
us-east-2b
us-east-2c
us-east-2a
Allowed Bastion External Access CIDR
CIDR from which access to bastion is to be permitted
1.2.3.4/32

Outputs (1)
Search outputs
1
Key
Value
Description
Export name
BastionIp
3.141.240.161
Elastic IP for Bastion
-


Findings Info
Actions
Suppress Findings Info
Saved rules No saved rules
Current Add filter criteria
Finding type
Resource
Last s...
Count
UnauthorizedAccess:EC2/RDPBruteForce
Instance: i-0974db5609fd4fd55
8 minutes ago
1
UnauthorizedAccess:EC2/SSHBruteForce
Instance: i-0974db5609fd4fd55
9 minutes ago
1
Recon:EC2/Portscan
Instance: i-0974db5609fd4fd55
10 minutes a...
2


Showing 3 of 3
UnauthorizedAccess:E...
Finding ID: f8c3a923f2d274b2e970d84bc2cc94ef
Feedback
High
i-0974db5609fd4fd55 is performing SSH brute force attacks against 172.16.0.25. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password. Info
Investigate with Detective
Overview
Severity HIGH
Region us-east-2
Count 1
Account ID 1829683317...
Resource ID i-0974db5609fd4fd55
Created at 04-05-2023 12:37:3...
Updated at 04-05-2023 12:37:3...
Malware scan
Scan ID a9a73e48cb...
Scan status RUNNING
Start time 04-05-2023 12:40:02
UnauthorizedAccess:EC2/SSHBruteForce
An EC2 instance has been involved in SSH brute force attacks.
Default severity: Low*
Note: This finding's severity is Low if a brute force attack is aimed at one of your EC2 instances. This finding's severity is High if your EC2 instance is being used to perform the brute force attack.
Full description:
This finding informs you that an EC2 instance in your AWS environment was involved in a brute force attack aimed at obtaining passwords to SSH services on Linux-based systems. This can indicate unauthorized access to your AWS resources.
Note: This finding is generated only through monitoring traffic on port 22. If your SSH services are configured to use other ports, this finding is not generated.
Remediation recommendations:
If the target of the brute force


Detect
Report
Remediate
Amazon GuardDuty
Amazon CloudWatch
CloudWatch Events
EC2 Instances
Lambda Functions
Kinesis Streams
ECS Tasks
Step Functions
SNS Messages
SQS Queues



Specify template

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

Template source

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

- ○ Amazon S3 URL
- ◉ Upload a template file

Upload a template file

Choose file *No file chosen*

JSON or YAML formatted file

Stack name

Stack name

enable-config1

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

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

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more

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

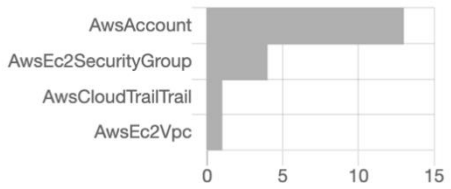
Create change set | Cancel | Previous | Submit

Security standards

Enabling AWS Security Hub grants it permissions to conduct security checks. **Service Linked Roles (SLRs)** with the following services are used to conduct security checks: Amazon CloudWatch, Amazon SNS, AWS Config, and AWS CloudTrail.

- ☑ Enable AWS Foundational Security Best Practices v1.0.0
- ☐ Enable CIS AWS Foundations Benchmark v1.2.0
- ☑ Enable CIS AWS Foundations Benchmark v1.4.0
- ☑ Enable NIST Special Publication 800-53 Revision 5
- ☐ Enable PCI DSS v3.2.1

Resource type



aws

Amazon: Inspector

Description

An automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Type of integration

Sends findings to Security Hub

Categories

Vulnerability Assessment and Management

How to receive findings from this integration

The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. Go to service homepage

Status

Accepting findings. See findings | Stop accepting findings

aws

AWS: IoT Device Defender - Audit

Description

AWS IoT Device Defender Audit is a security service that allows you to audit the configuration of devices, and mitigation security risks.

Type of integration

Sends findings to Security Hub

Categories

IoT Security

How to receive findings from this integration

The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. Go to service homepage

Status

Not accepting findings | Accept findings

Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 6

Event Management with Security Hub and GuardDuty

Summary

This chapter concludes *Section 2* on incident response, with a review of the AWS services Security Hub and GuardDuty. You explored how the GuardDuty service works and how it presents its findings. You also walked through setting up the GuardDuty service from the Amazon Management Console.

You then took a look at the Amazon Security Hub service and examined how it can present security findings from AWS security services, such as GuardDuty, Amazon Macie, Amazon Inspector, AWS Firewall Manager, and third-party services in a unified view, thereby making tracking your security posture much easier on yourself as a security professional.

Chapter 7, Logs Generated by AWS Services, will begin the next domain in the AWS Security Specialty exam, *logging and monitoring*. This domain concerns the different types of logs you can capture, how to do so, and what they tell you.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

Select Quiz

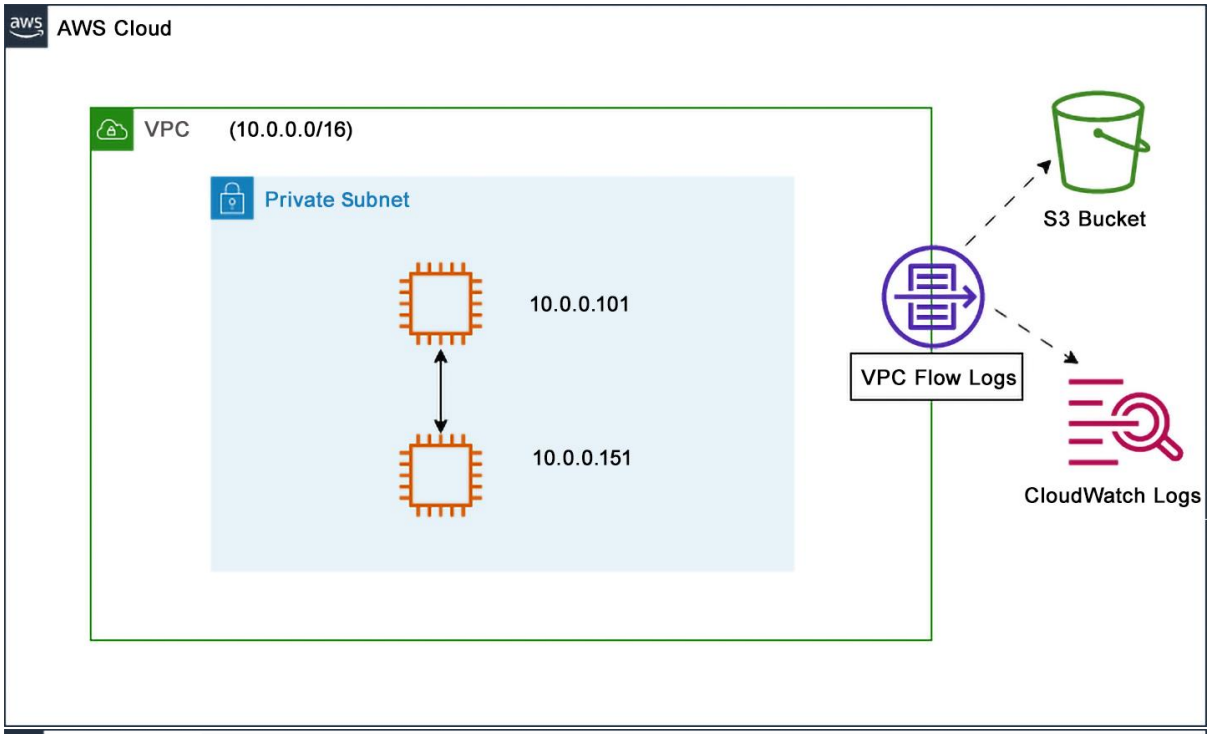
Quiz 1

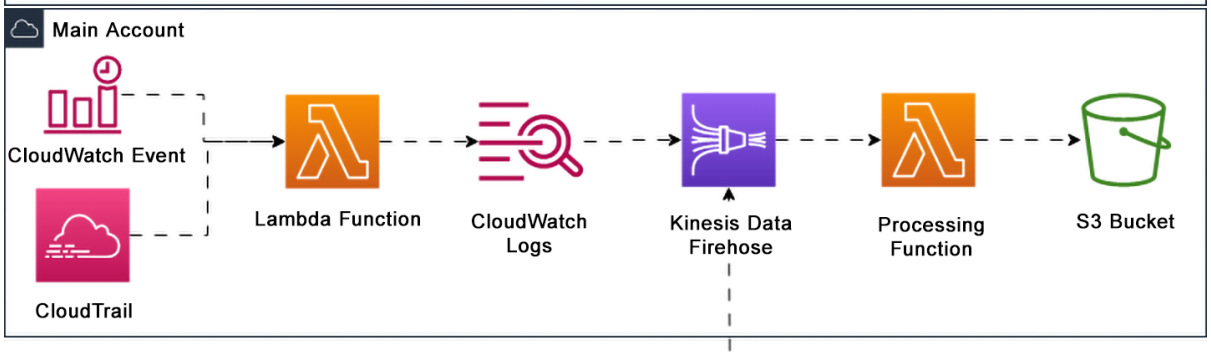
SHOW QUIZ DETAILS

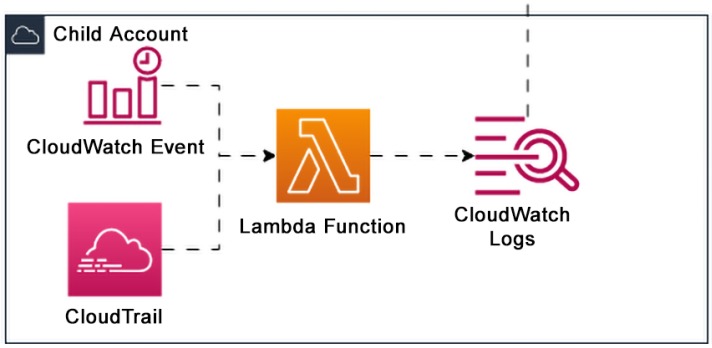
START

Chapter 7:

Name	Type	Last modified	Size	Storage class
packt-security-logsLogs/	Folder	-	-	-





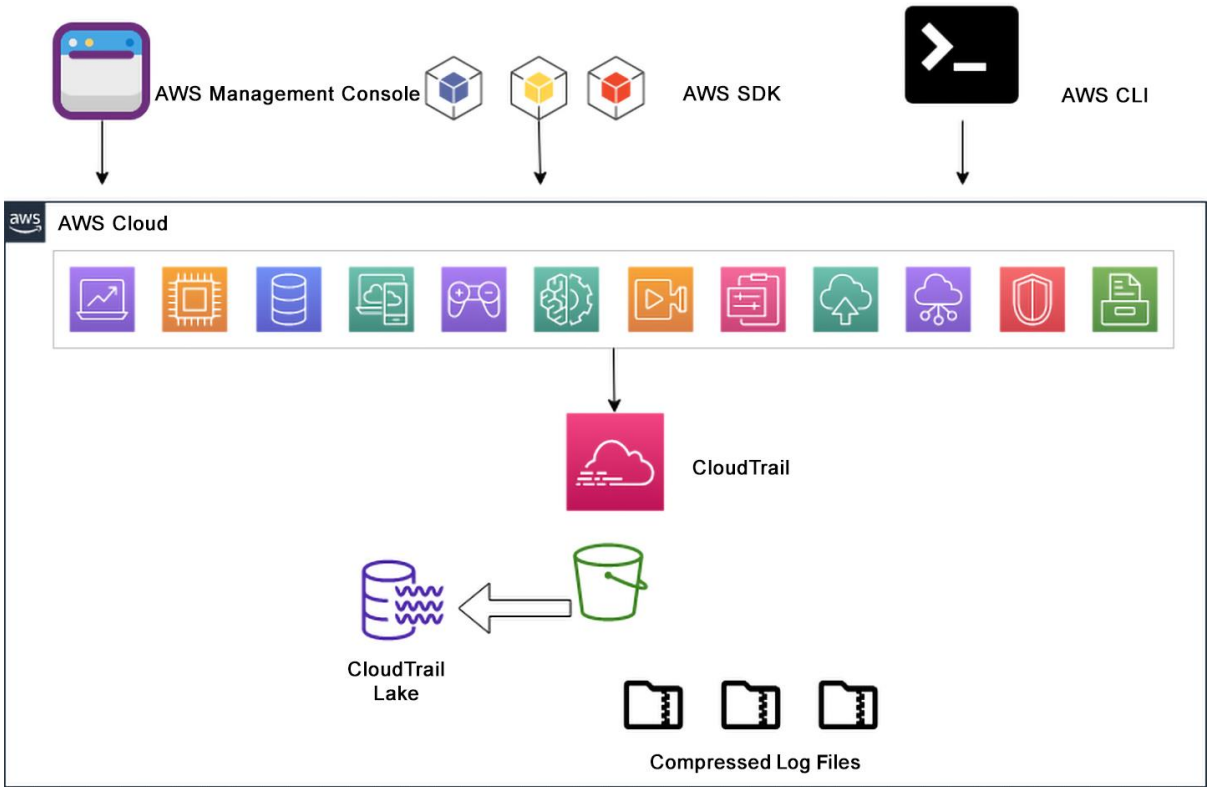


Name	Type
packt-security-logsLogs/	Folder

Amazon S3 > Buckets > packt-security-logs > packt-security-logsLogs/ > 2023-04-15-04-13-40-A52C111EBB5A6D2F

2023-04-15-04-13-40-A52C111EBB5A6D2F Info

Copy S3 URI | Download | Open | Object actions



Trail name

Enter a display name for your trail.

security-cert

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

packt-security-cert-ctrail-logs

Logs will be stored in packt-security-cert-ctrail-logs/AWSLogs/182968331794

Log file SSE-KMS encryption Info

☑ Enabled

Customer managed AWS KMS key

◉ New

○ Existing

AWS KMS alias

packt-cloudtrail

KMS key and S3 bucket must be in the same region.

▼ Additional settings

Log file validation Info

☐ Enabled

Events Info

Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply

Event type

Choose the type of events that you want to log.

☑ Management events
Capture management operations performed on your AWS resources.

☑ Data events
Log the resource operations performed on or within a resource.

☐ Insights events
Identify unusual activity, errors, or user behavior in your account.

Management events Info

Management events show information about management operations performed on resources in your AWS account.

ⓘ Charges apply to log management events on this trail because you are logging at least one other copy of management events in your account.

API activity

Choose the activities you want to log.

☑ Read ☑ Write

☐ Exclude AWS KMS events

☐ Exclude Amazon RDS Data API events

Data events Info

Additional charges apply Data events show information about the resource operations performed on or within a resource.

ⓘ **Advanced event selectors are enabled**
Use the following fields for fine-grained control over the data events captured by your trail.

Switch to basic event selectors

▼ Data event: S3 Remove

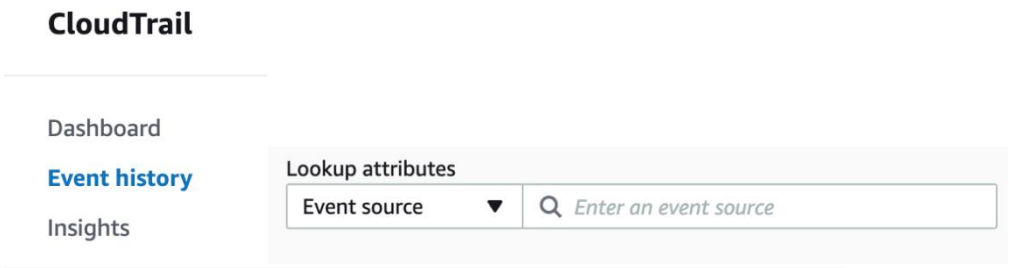
Data event type

Choose the source of data events to log.

S3 ▼

Log selector template

Log all events ▼



DASHBOARD > CHAPTER 7

Logs Generated by AWS Services

Summary

This chapter covered the different types of logs produced by various AWS services and how they can be stored for later use and consumption or, if needed, for an audit.

You saw how S3 can record access to its objects and folders using S3 access logging. You also explored how to troubleshoot and record network activity using VPC Flow Logs. In reviewing another way to capture network traffic, you saw the capabilities of both ELB logging and WAF logs.

You also learned about the service that records all API calls, CloudTrail. You examined how to turn on a new trail for a specific purpose and how to look up events in that trail. In case using the legacy trail becomes limiting, you looked at how to expand the capabilities of CloudTrail using CloudTrail Lake.

Chapter 8, CloudWatch and CloudWatch Metrics, will discuss the CloudWatch service and how it consumes logs. You will also see how CloudWatch can gather and publish predefined and custom metrics from our services.

Chapter Review Questions

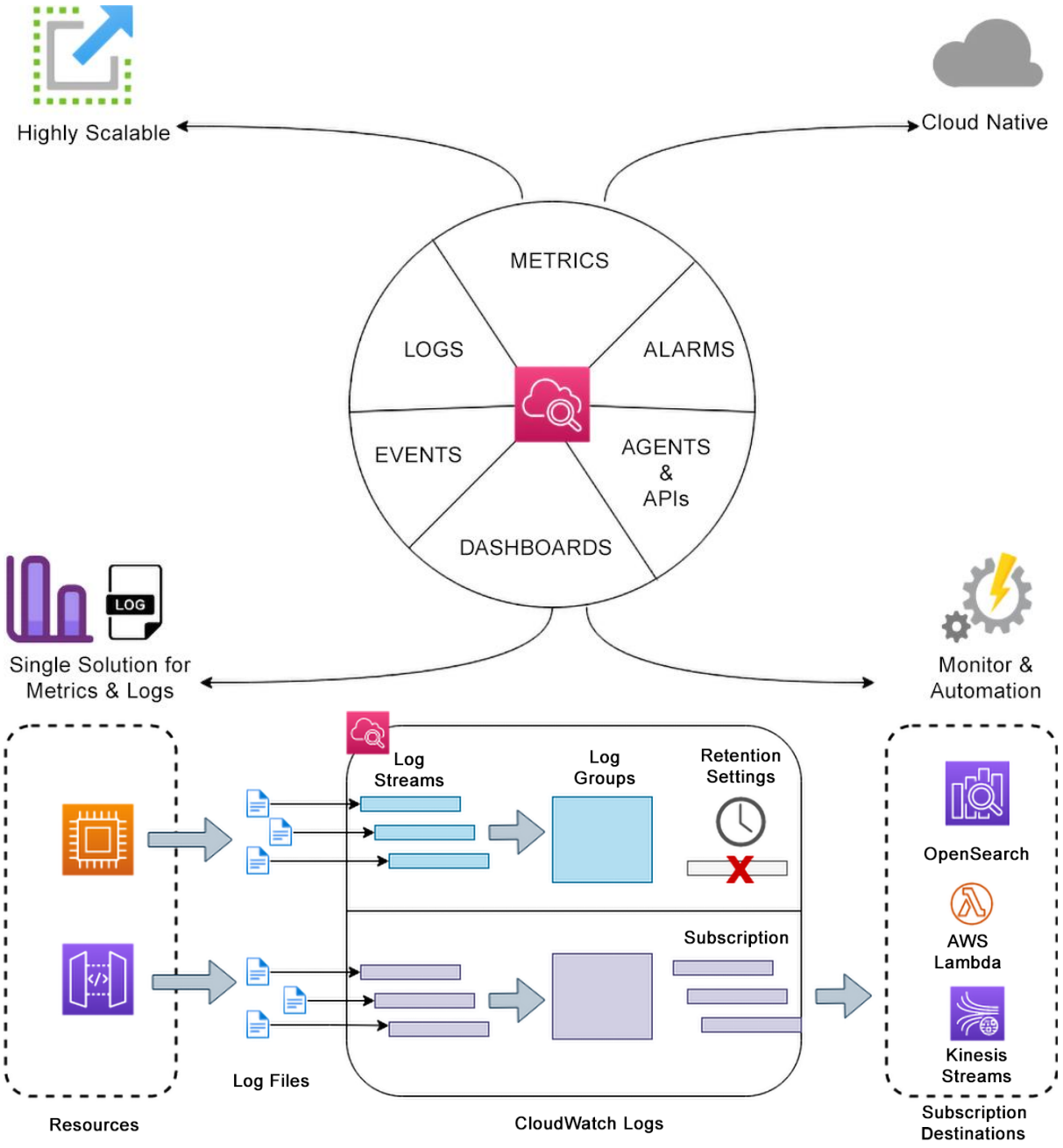
The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

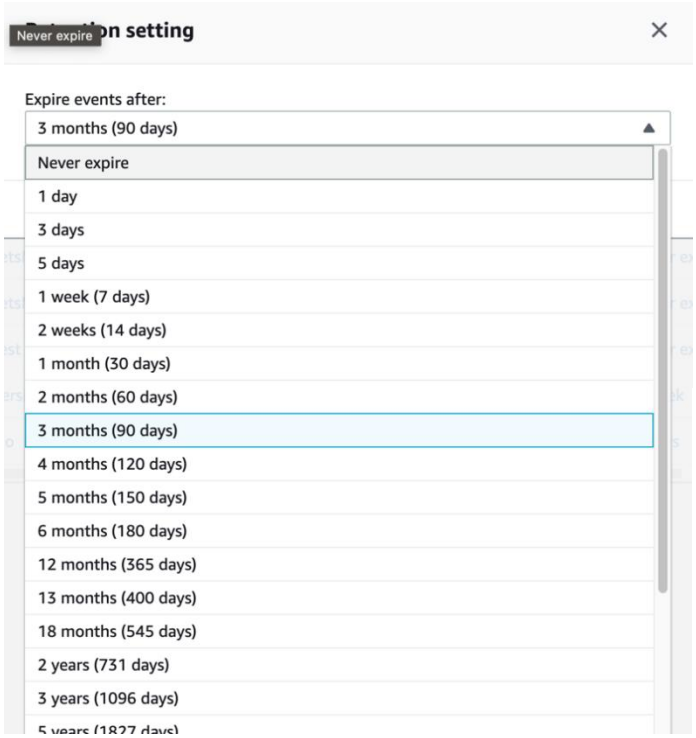
Select Quiz

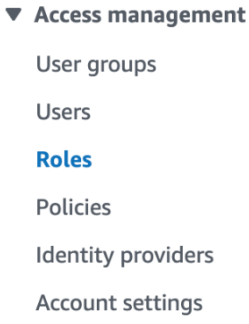
Quiz 1 START

SHOW QUIZ DETAILS

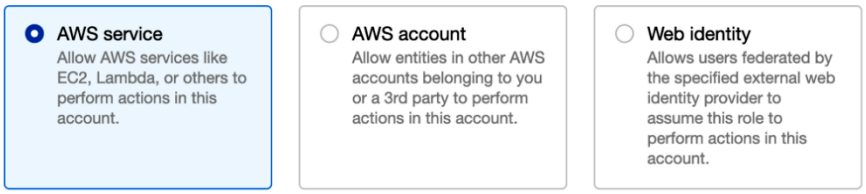
Chapter 8:


Highly Scalable
Cloud Native
METRICS
LOGS
ALARMS
EVENTS
AGENTS & APIs
DASHBOARDS
LOG
Single Solution for Metrics & Logs
Monitor & Automation
Log Streams
Log Groups
Retention Settings
Subscription
Log Files
Resources
CloudWatch Logs
OpenSearch
AWS Lambda
Kinesis Streams
Subscription Destinations





Trusted entity type



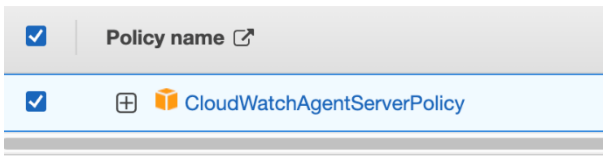
Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

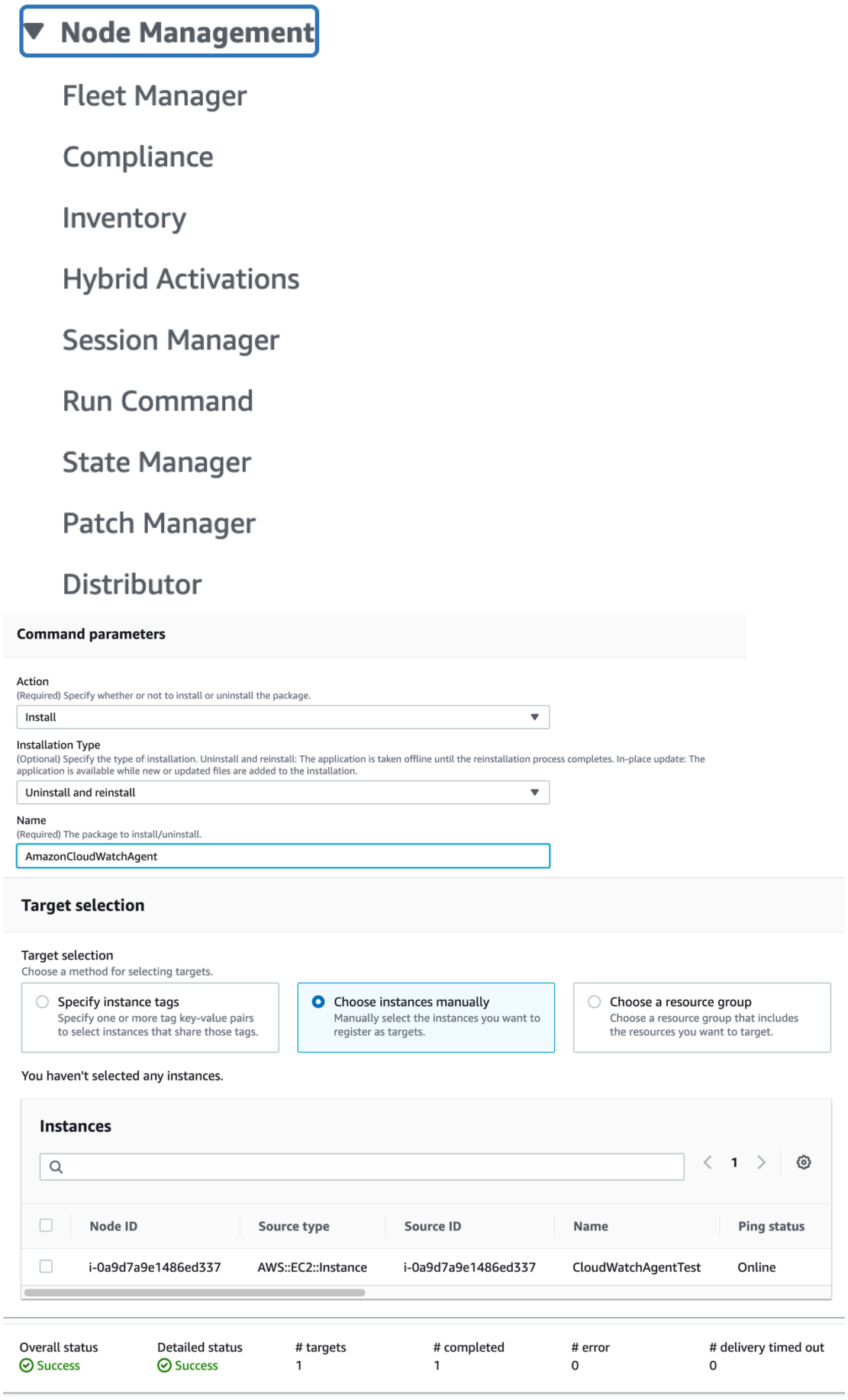
EC2

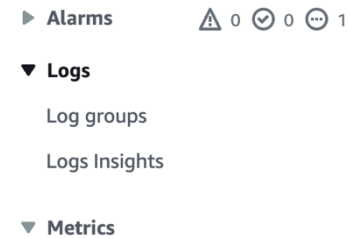
Allows EC2 instances to call AWS services on your behalf.



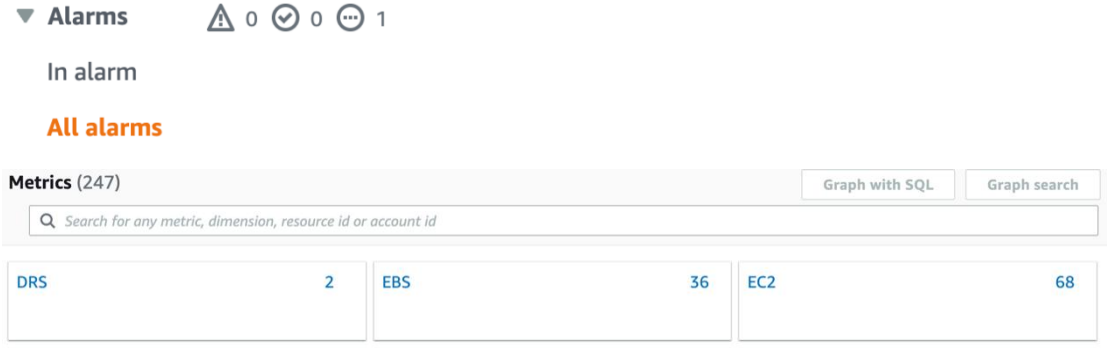
Key pair name - *required*

Proceed without a key pair (Not recommended) Default value


Node Management
Fleet Manager
Compliance
Inventory
Hybrid Activations
Session Manager
Run Command
State Manager
Patch Manager
Distributor
Command parameters
Action
(Required) Specify whether or not to install or uninstall the package.
Install
Installation Type
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.
Uninstall and reinstall
Name
(Required) The package to install/uninstall.
AmazonCloudWatchAgent
Target selection
Target selection
Choose a method for selecting targets.
Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.
Choose instances manually
Manually select the instances you want to register as targets.
Choose a resource group
Choose a resource group that includes the resources you want to target.
You haven't selected any instances.
Instances
1
Node ID
Source type
Source ID
Name
Ping status
i-0a9d7a9e1486ed337
AWS::EC2::Instance
i-0a9d7a9e1486ed337
CloudWatchAgentTest
Online
Overall status
Success
Detailed status
Success
targets
1
completed
1
error
0
delivery timed out
0



Log group	Data prot...	Sensitive ...	Retention	Metric filt...
/aws/guardduty/malware-scan-events	Inactive	-	3 months	-



Conditions

Threshold type

- (●) Static — Use a value as a threshold
- ( ) Anomaly detection — Use a band as a threshold

Whenever CallCount is...

Define the alarm condition.

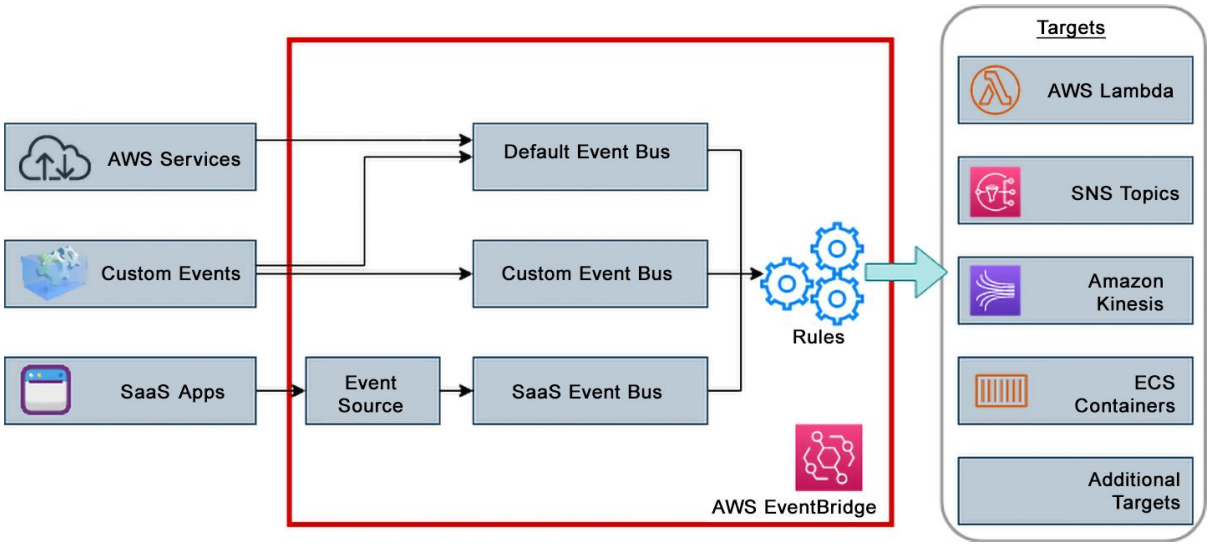
- (●) Greater — > threshold
- ( ) Greater/Equal — >= threshold
- ( ) Lower/Equal — <= threshold
- ( ) Lower — < threshold

than...

Define the threshold value.

0.05

Must be a number



Buses

Event buses

Rules

Global endpoints

Archives

Replays

Event pattern Info

Event source
AWS service or EventBridge partner as source
AWS services

AWS service
The name of the AWS service as the event source
EC2

Event type
The type of events as the source of the matching pattern
EC2 Instance State-change Notification

- Any state
- Specific state(s)

terminated

- Any instance
- Specific instance Id(s)

Event pattern
Event pattern, or filter to match the events

```
: ["aws.ec2"],
type": ["EC2 Instance State-change Notification"],
: {
": ["terminated"]
```

Copy | Test pattern | Edit pattern

Target 1

Target types

Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.

- ○ EventBridge event bus
- ○ EventBridge API destination
- ◉ AWS service

Select a target | Info

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

SNS topic ▼

Topic

config-demo-topic ▼ ↻

Practice Resources 🔔 SHARE FEEDBACK

DASHBOARD > CHAPTER 8

CloudWatch and CloudWatch Metrics

Summary

In this chapter, you looked at AWS's CloudWatch service and its multiple functionalities. You saw how it can gather logs for many of the other services running in AWS and store them for the specified period. You also saw how the CloudWatch service provides monitoring and metrics for the different services running in AWS. You looked at both predefined metrics and custom ones.

With the metric capabilities of CloudWatch, you can track your resources and create alarms and dashboards to monitor and keep track of services within your purview.

The chapter concluded with a discussion of Amazon EventBridge, the event bus service. You saw how EventBridge can take events from multiple sources, both internal to AWS and external, and use rules to process the events and then send the events to one or more specified targets for proper processing. You also learned how EventBridge can help you build a decoupled EDA in AWS.

In *Chapter 9, Parsing Logs and Events with AWS Native Tools*, you will look at using cloud-native services to sort through a mountain of log files when looking for a particular item. This can be done using services such as **Kinesis Data Firehose** and **Amazon Athena**.

Chapter Review Questions

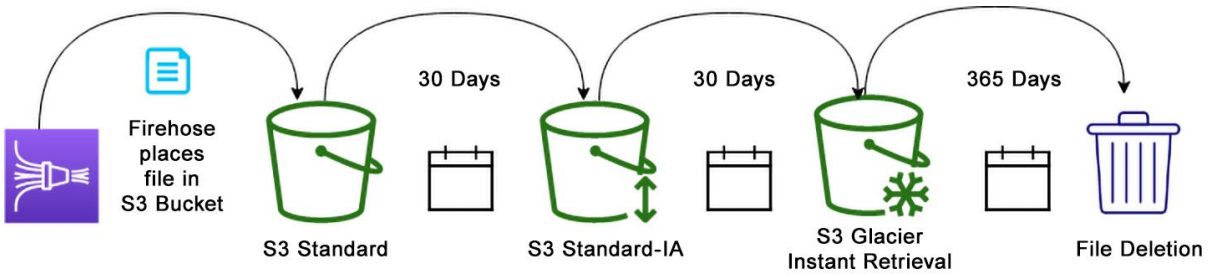
The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

Select Quiz

Quiz 1 START

SHOW QUIZ DETAILS

Chapter 9:



General configuration

AWS Region

US East (Ohio) us-east-2

Bucket name Info

packt-security-chapter9

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

packt-security-chapter9

Objects | Properties | Permissions | Metrics | Management | Access Points

Lifecycle rules (0)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. Learn more

View details | Edit | Delete | Actions | Create lifecycle rule

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers

No lifecycle rules

There are no lifecycle rules for this bucket.

Create lifecycle rule

Lifecycle rule name

security-cert-delete-24hours

Up to 255 characters

Choose a rule scope

- Limit the scope of this rule using one or more filters
- Apply to all objects in the bucket

Apply to all objects in the bucket

If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". Learn more

- [x] I acknowledge that this rule will apply to all objects in the bucket.

Lifecycle rule actions

Choose the actions you want this rule to perform. Per-request fees apply. Learn more or see Amazon S3 pricing

- [ ] Move current versions of objects between storage classes
- [ ] Move noncurrent versions of objects between storage classes
- [x] Expire current versions of objects
- [ ] Permanently delete noncurrent versions of objects
- [ ] Delete expired object delete markers or incomplete multipart uploads

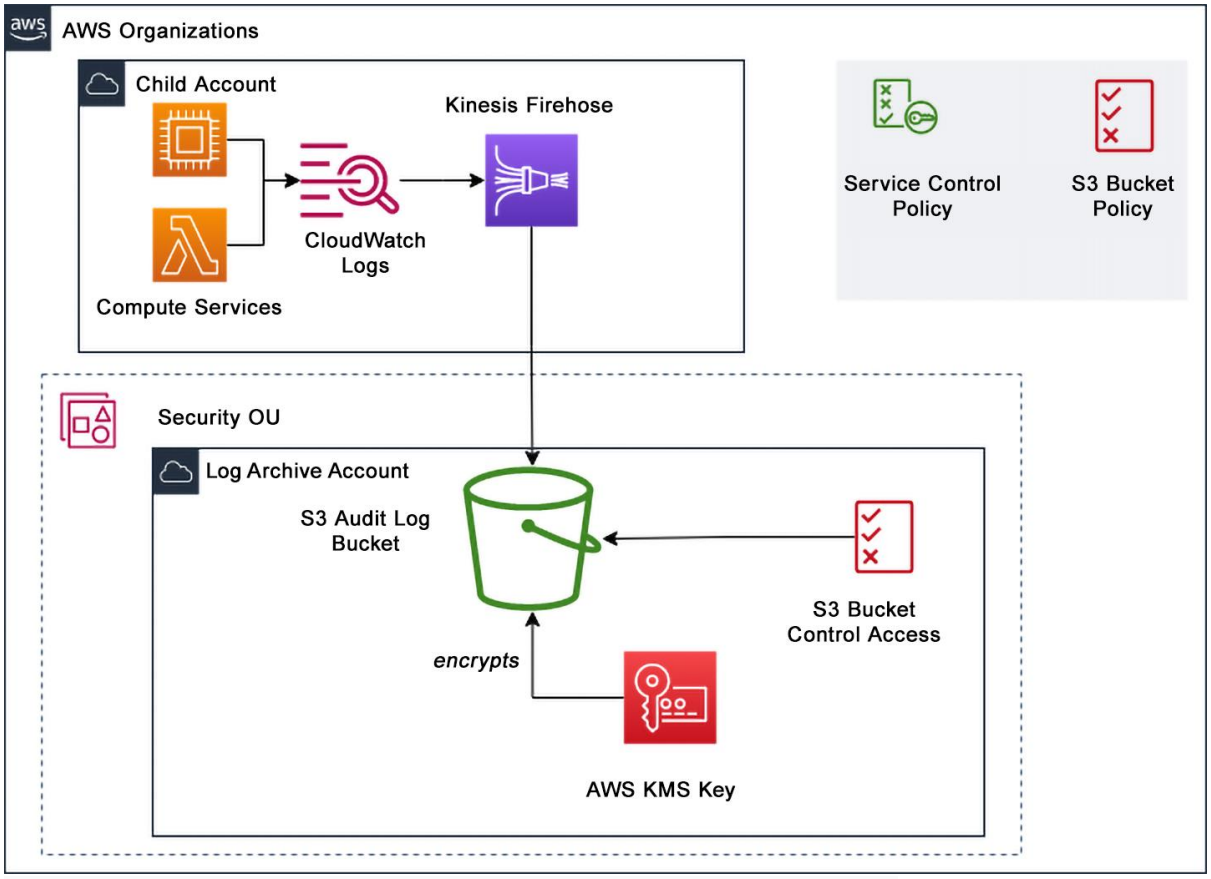
These actions are not supported when filtering by object tags or object size.

Expire current versions of objects

For version-enabled buckets, Amazon S3 adds a delete marker and the current version of an object is retained as a noncurrent version. For non-versioned buckets, Amazon S3 permanently removes the object. Learn more

Days after object creation

1



Choose source and destination

Specify the source and the destination for your delivery stream. You cannot change the source and destination of your delivery stream once it has been created.

Source Info

Direct PUT

Destination Info

Amazon S3

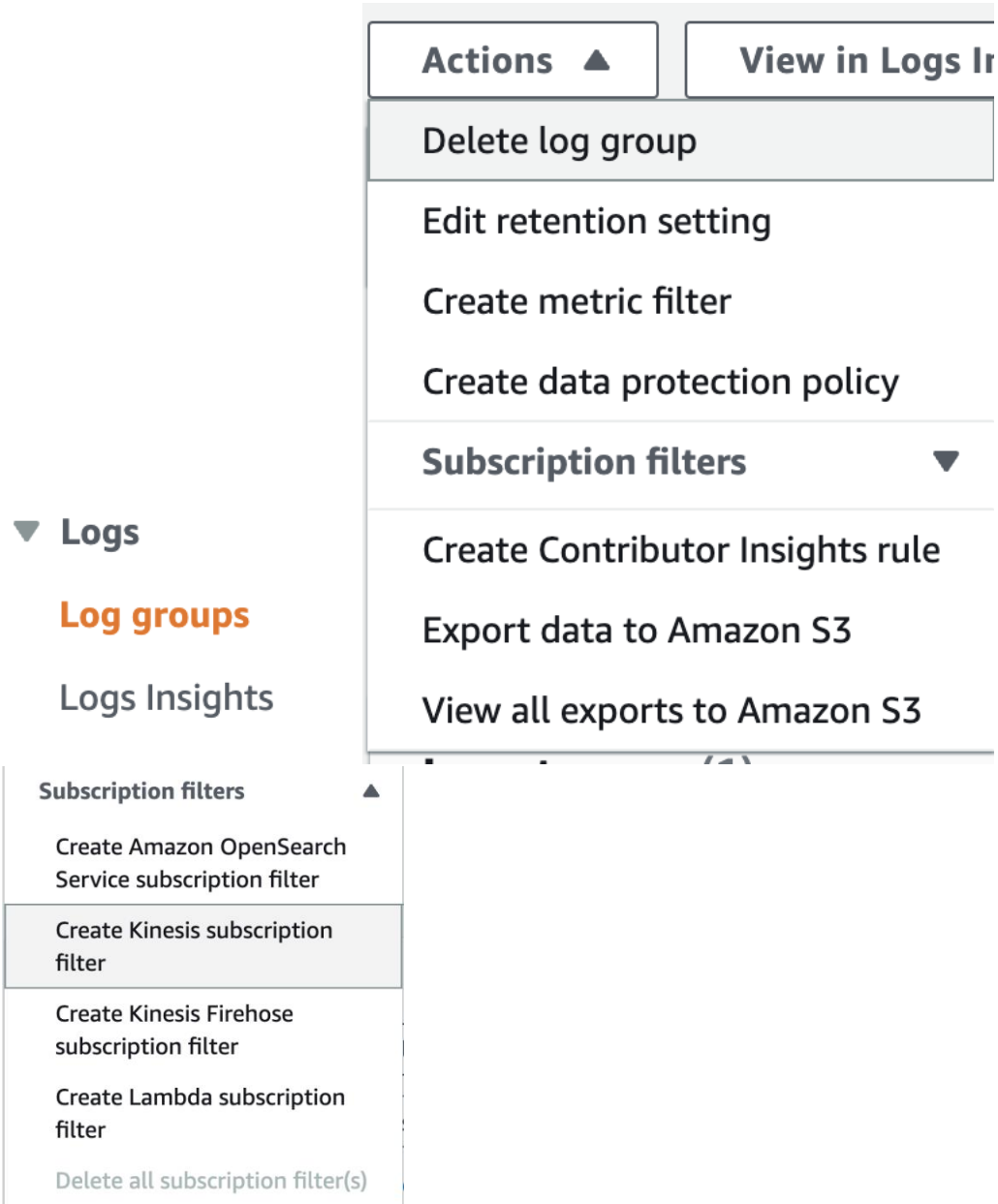
Destination settings Info

Specify the destination settings for your Firehose stream.

S3 bucket

s3://packt-security-chapter9 Browse Create

Format: s3://bucket



Choose destination

Choose the account and delivery stream to execute when a log event matches the filter you are going to specify.

Destination account

- (•) Current account
  Send log data to a Kinesis Firehose delivery stream in the current account.
- ( ) Cross-account
  Send log data to a specified Kinesis Firehose delivery stream in another account. **Learn more about cross-account set up**

Kinesis Firehose delivery stream

Select an existing delivery stream you want to deliver matching log events to, or **create a new Kinesis Firehose data stream**.

packt-chapter9-firehose

Grant permission

To grant CloudWatch Logs permission to put data into your delivery stream, select an existing role below or **create a new role**.

Select an existing role

If your newly created role is not showing up in the dropdown list, please try the refresh button to the right.

FireHoseTrustRole

Configure log format and filters

Choose your log format to get a recommended filter pattern for your log data, or select "Other" to enter a custom filter pattern. An empty filter pattern matches all log events.

Log format

Other

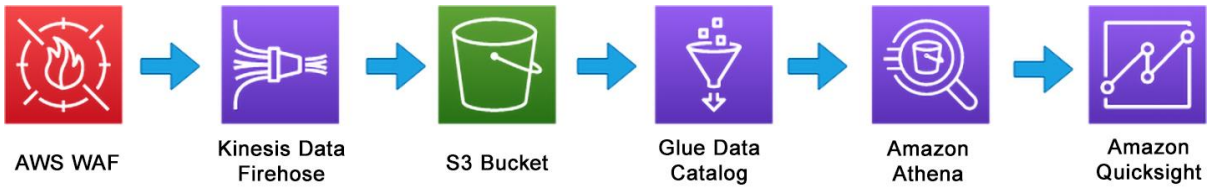
Subscription filter pattern

Specify the log event structure and any filter conditions to apply on your log data as it gets streamed to the Amazon Kinesis Firehose service.

Subcription filter pattern

Subscription filter name

Chapter9-Firehose



Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 9

Parsing Logs and Events with AWS Native Tools

Summary

In this chapter, you learned how to review and analyze many log files using native tools found in AWS.

You also had a brief overview of how costs can affect your decisions when choosing the correct storage solution for your long-term log storage for your account and your organization. This overview was presented through the different tiers of storage available in the S3 service and their durability and reliability ratings.

Next, you explored how to move logs out of CloudWatch Logs using subscription filters. You learned that combining CloudWatch subscription filters with the Kinesis Data Firehose service allows you to take incoming logs to CloudWatch Logs and push them into an S3 bucket where they could be stored at lower costs and then be queried by the Amazon Athena service.

You also examined how you could use Kinesis Data Firehose to stream the logs to Amazon OpenSearch, the fast search engine with custom visualizations based on Elasticsearch.

The next chapter marks the beginning of the next section on *Infrastructure Security*. In *Chapter 10*, *Configuring Infrastructure Security*, you will start with configuring infrastructure security. This includes the steps to set up a **Virtual Private Cloud** (**VPC**), security groups, and **Network Access Control Lists** (**NACLs**).

Chapter Review Questions

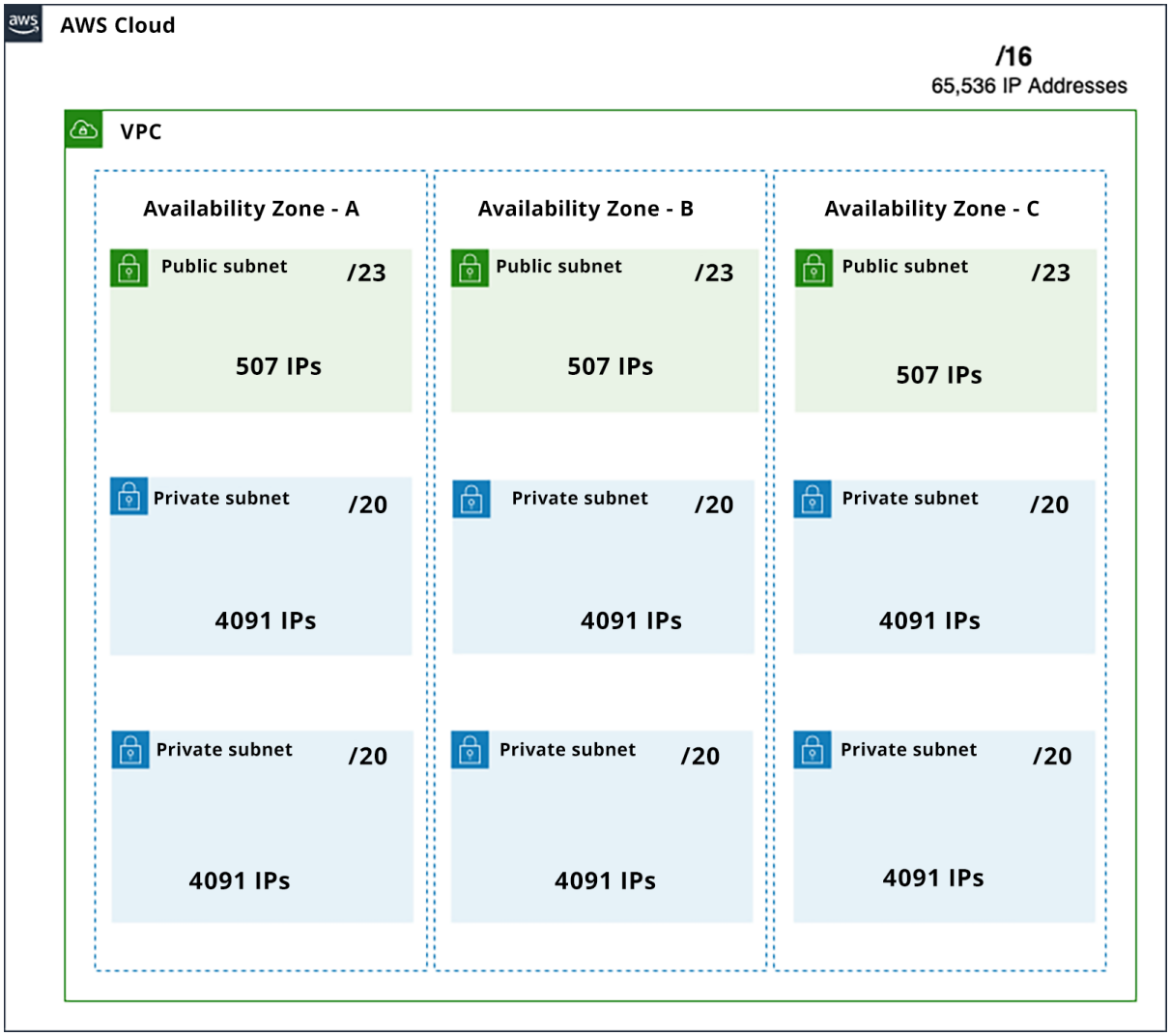
The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

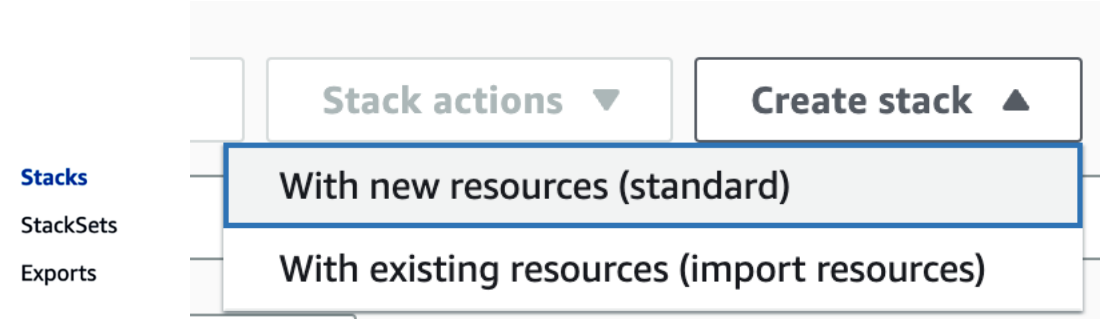
Select Quiz

Quiz 1 START

SHOW QUIZ DETAILS

Chapter 10:





Template source

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

Amazon S3 URL | Upload a template file

Upload a template file

Choose file *No file chosen*

JSON or YAML formatted file

Stack name

Stack name

chapt10-vpc

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

Stack info | Events | Resources | Outputs | Parameters | Template | Change sets

Filter by VPC:

Select a VPC

vpc-00a2bccb3bc9ce9ed
MyVPC
Owner: 182968331794

Subnets (2) Info

Actions | Create subnet

Filter subnets

search: vpc-00a2bccb3bc9ce9ed | Clear filters

1

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6
MyPublicSubnet	subnet-008e1f8337cabe33b	Available	vpc-00a2bccb3bc9ce9ed | MyVPC	10.0.1.0/24	–
MyPrivateSubnet	subnet-060e9b168c531919d	Available	vpc-00a2bccb3bc9ce9ed | MyVPC	10.0.2.0/24	–

subnet-060e9b168c531919d / MyPrivateSubnet

Actions

Details

Subnet ID
subnet-060e9b168c531919d

Available IPv4 addresses
251

VPC
vpc-00a2bccb3bc9ce9ed | MyVPC

Auto-assign public IPv4 address
No

Outpost ID
–

Hostname type
IP name

Owner
182968331794

Subnet ARN
arn:aws:ec2:us-east-2:182968331794:subnet/subnet-060e9b168c531919d

IPv6 CIDR
–

Route table
rtb-0a4c3d6a9ee5efe8e | MyPrivateRouteTable

Auto-assign IPv6 address
No

IPv4 CIDR reservations
–

Resource name DNS A record
Disabled

State
Available

Availability Zone
us-east-2c

Network ACL
acl-07104d0abbb81d306

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations
–

Resource name DNS AAAA record
Disabled

IPv4 CIDR
10.0.2.0/24

Availability Zone ID
use2-az3

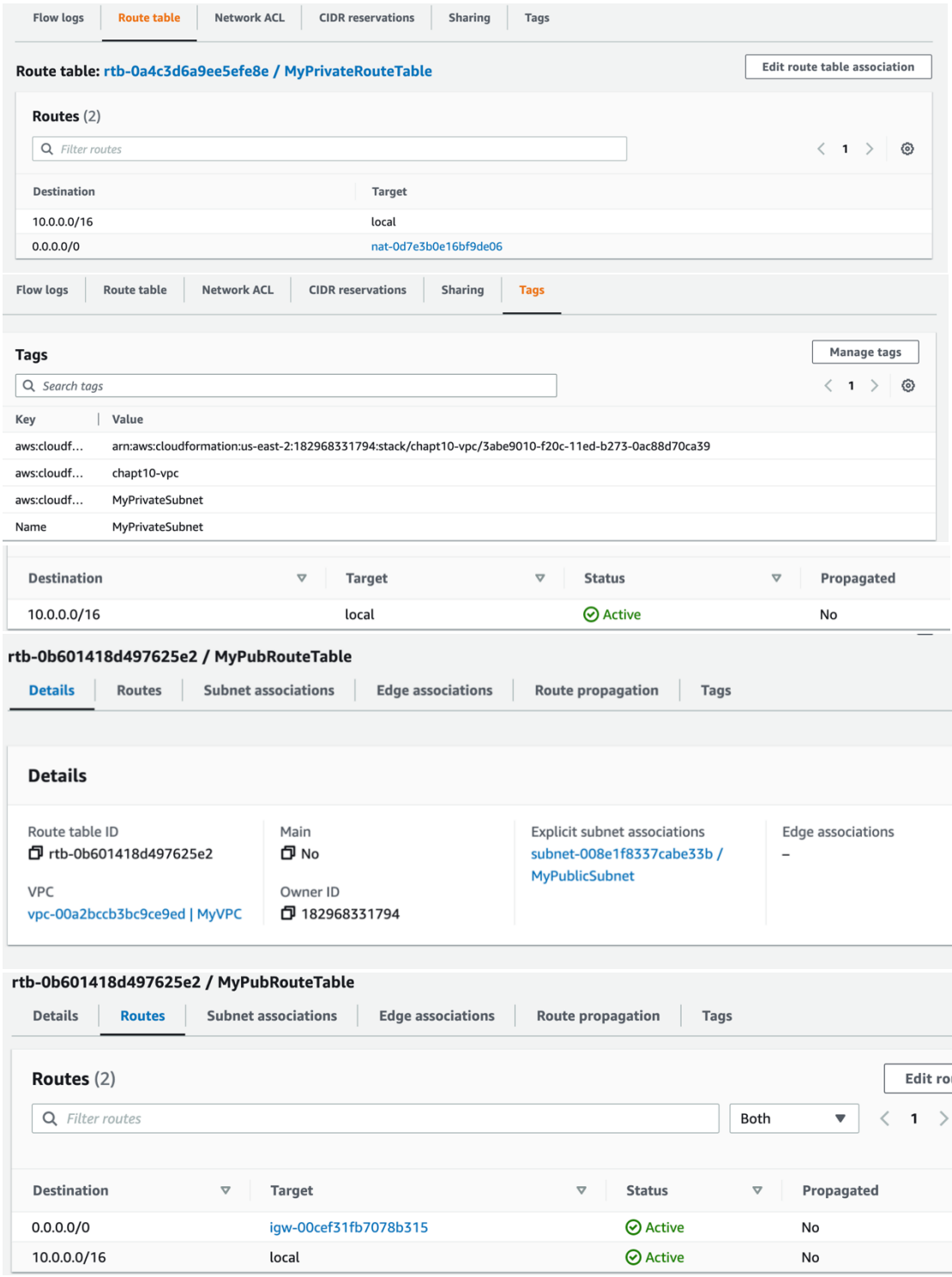
Default subnet
No

Customer-owned IPv4 pool
–

IPv6-only
No

DNS64
Disabled

Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags


Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Route table: rtb-0a4c3d6a9ee5efe8e / MyPrivateRouteTable
Edit route table association
Routes (2)
Filter routes
1
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
nat-0d7e3b0e16bf9de06
Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Tags
Manage tags
Search tags
1
Key
Value
aws:cloudf...
arn:aws:cloudformation:us-east-2:182968331794:stack/chapt10-vpc/3abe9010-f20c-11ed-b273-0ac88d70ca39
aws:cloudf...
chapt10-vpc
aws:cloudf...
MyPrivateSubnet
Name
MyPrivateSubnet
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
rtb-0b601418d497625e2 / MyPubRouteTable
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Details
Route table ID
rtb-0b601418d497625e2
Main
No
Explicit subnet associations
subnet-008e1f8337cabe33b / MyPublicSubnet
Edge associations
–
VPC
vpc-00a2bccb3bc9ce9ed | MyVPC
Owner ID
182968331794
rtb-0b601418d497625e2 / MyPubRouteTable
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Edit routes
Filter routes
Both
1
Destination
Target
Status
Propagated
0.0.0.0/0
igw-00cef31fb7078b315
Active
No
10.0.0.0/16
local
Active
No

rtb-0b601418d497625e2 / MyPubRouteTable

Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
MyPublicSubnet	subnet-008e1f8337cabe33b	10.0.1.0/24	–

Subnets without explicit associations (0)

Edit subnet associations

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR

No subnets without explicit associations

All your subnets are associated with a route table.

rtb-0b601418d497625e2 / MyPubRouteTable

Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

Route Propagation (0)

Edit route propagation

Find virtual private gateway

Virtual Private Gateway	Propagation

No virtual private gateways

No virtual private gateways which are allowed to update this route table.

Details Info

Network ACL ID	Associated with	Default	VPC ID
acl-07104d0abbb81d306	2 Subnets	Yes	vpc-00a2bccb3bc9ce9ed / MyVPC

Owner: 182968331794

Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (2)

Edit inbound rules

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

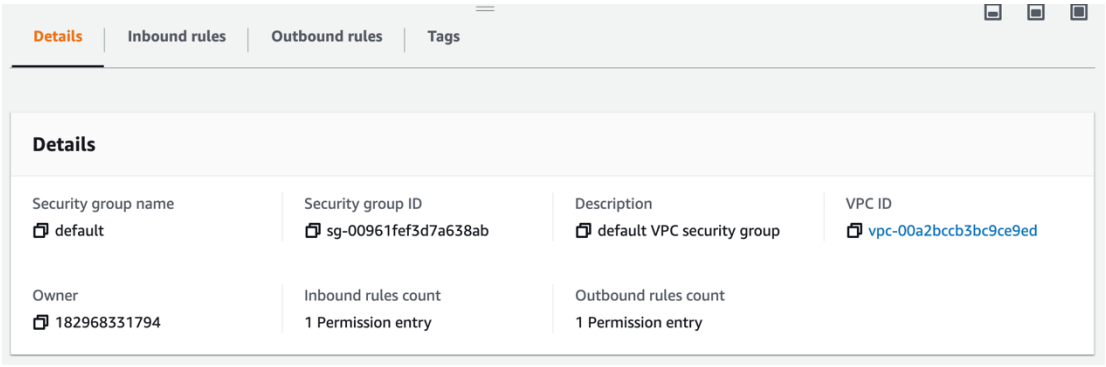
Inbound rules | Outbound rules | Subnet associations | Tags

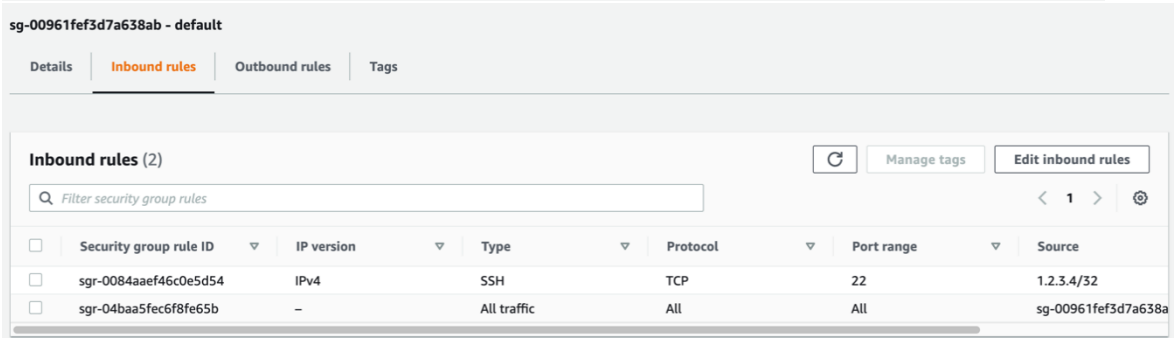
Subnet associations (2)

Edit subnet associations

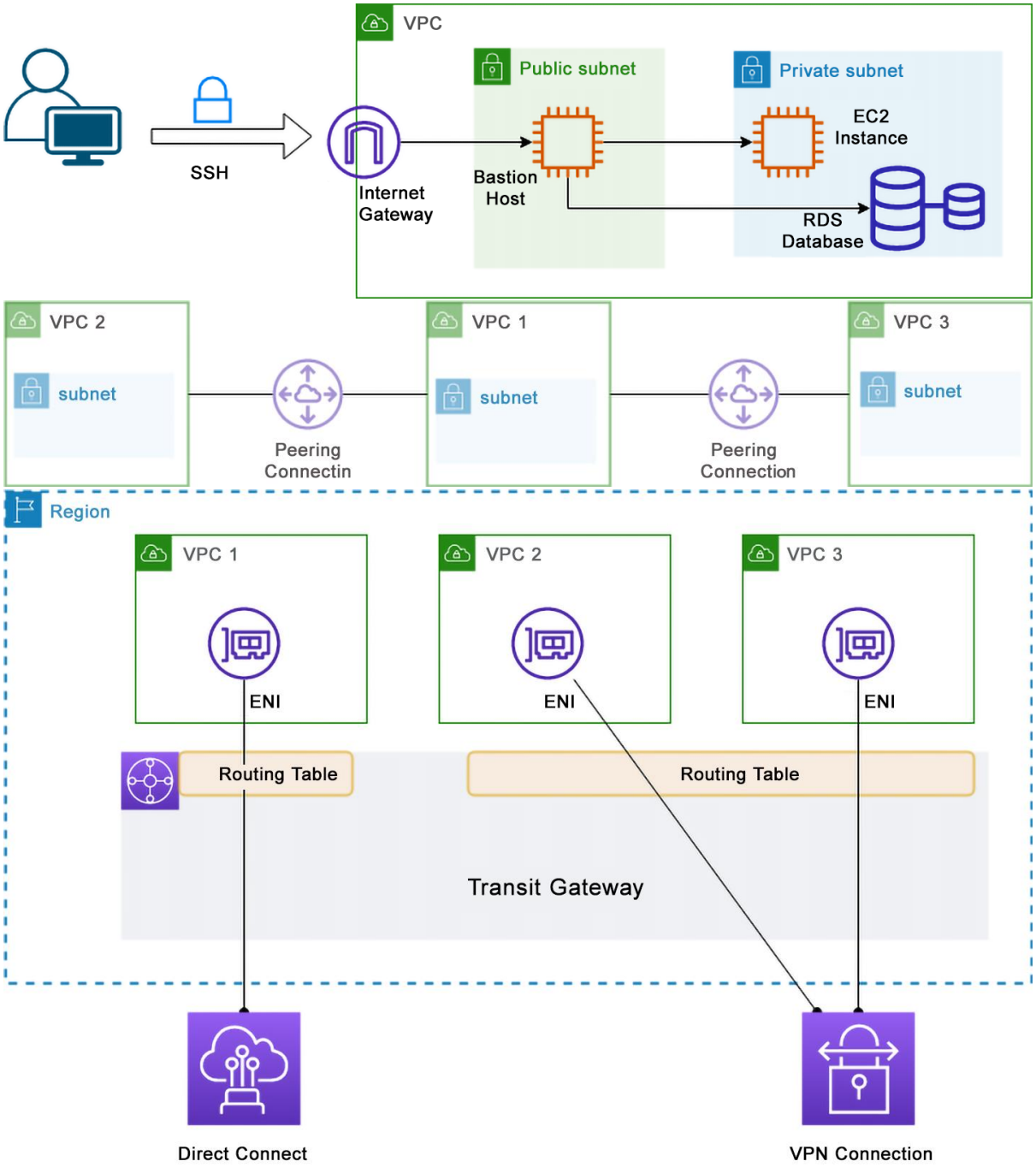
Filter subnet associations

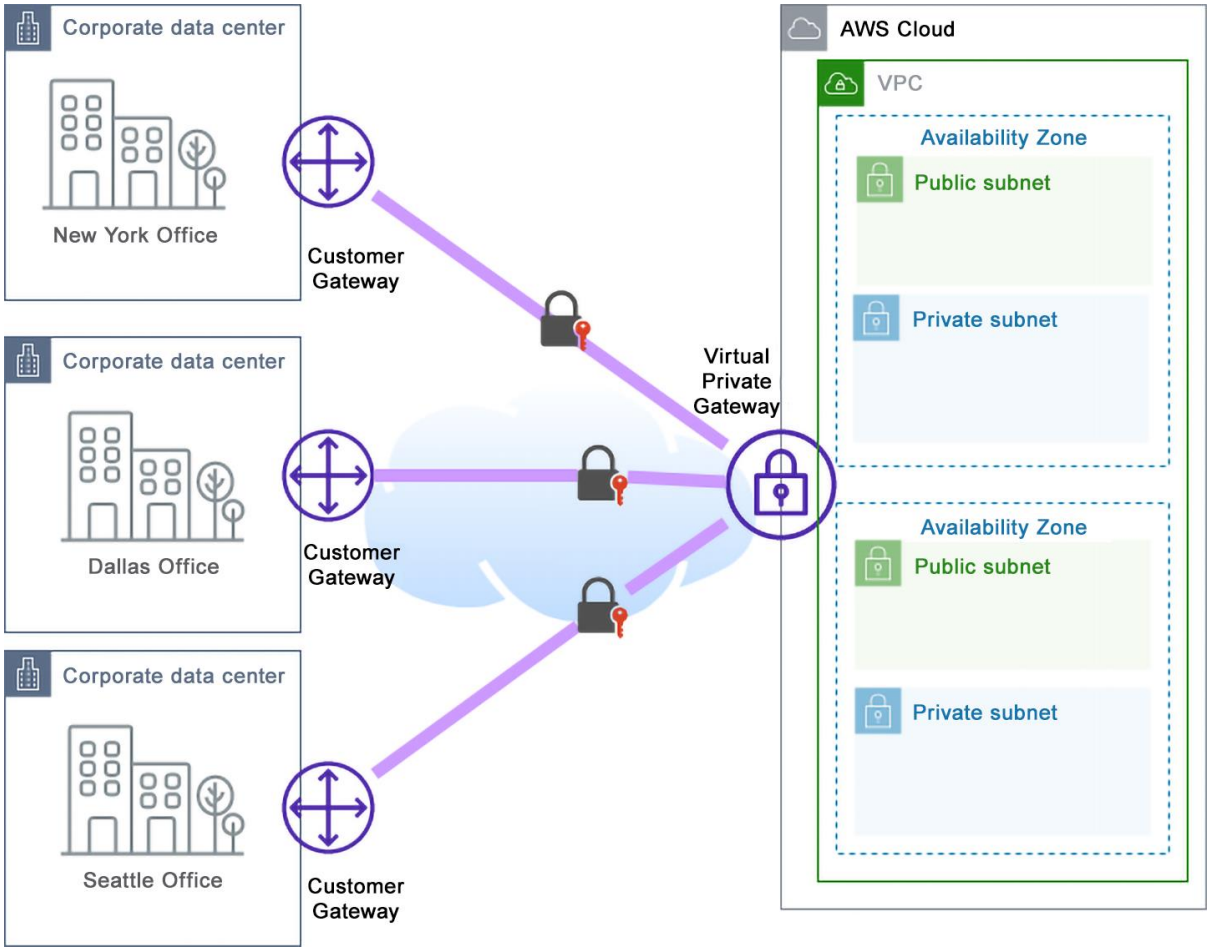
Name	Subnet ID	Associated with	Availability Z...	IPv4 CIDR
MyPublicSubnet	subnet-008e1f8337cab...	acl-07104d0abbb81d306	us-east-2c	10.0.1.0/24
MyPrivateSubnet	subnet-060e9b168c531...	acl-07104d0abbb81d306	us-east-2c	10.0.2.0/24





Subnet address	Range of addresses	Hosts	Join
10.0.0.0/21	10.0.0.0 - 10.0.7.255	2046	/21 /20 /19 /18 /17 /16
10.0.8.0/21	10.0.8.0 - 10.0.15.255	2046	/21 /20 /19 /18 /17 /16
10.0.16.0/21	10.0.16.0 - 10.0.23.255	2046	/21 /20 /19 /18 /17 /16
10.0.24.0/21	10.0.24.0 - 10.0.31.255	2046	/21 /20 /19 /18 /17 /16
10.0.32.0/21	10.0.32.0 - 10.0.39.255	2046	/21 /20 /19 /18 /17 /16
10.0.40.0/21	10.0.40.0 - 10.0.47.255	2046	/21 /20 /19 /18 /17 /16
10.0.48.0/21	10.0.48.0 - 10.0.55.255	2046	/21 /20 /19 /18 /17 /16
10.0.56.0/21	10.0.56.0 - 10.0.63.255	2046	/21 /20 /19 /18 /17 /16
10.0.64.0/21	10.0.64.0 - 10.0.71.255	2046	/21 /20 /19 /18 /17 /16
10.0.72.0/21	10.0.72.0 - 10.0.79.255	2046	/21 /20 /19 /18 /17 /16
10.0.80.0/20	10.0.80.0 - 10.0.95.255	4094	/20 /19 /18 /17 /16
10.0.96.0/19	10.0.96.0 - 10.0.127.255	8190	/19 /18 /17 /16
10.0.128.0/17	10.0.128.0 - 10.0.255.255	32766	/17 /16


VPC
Public subnet
Private subnet
SSH
Internet Gateway
Bastion Host
EC2 Instance
RDS Database
VPC 2
subnet
Peering Connectin
VPC 1
subnet
Peering Connection
VPC 3
subnet
Region
VPC 1
VPC 2
VPC 3
ENI
ENI
ENI
Routing Table
Routing Table
Transit Gateway
Direct Connect
VPN Connection



Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Endpoint settings

Name tag - *optional*

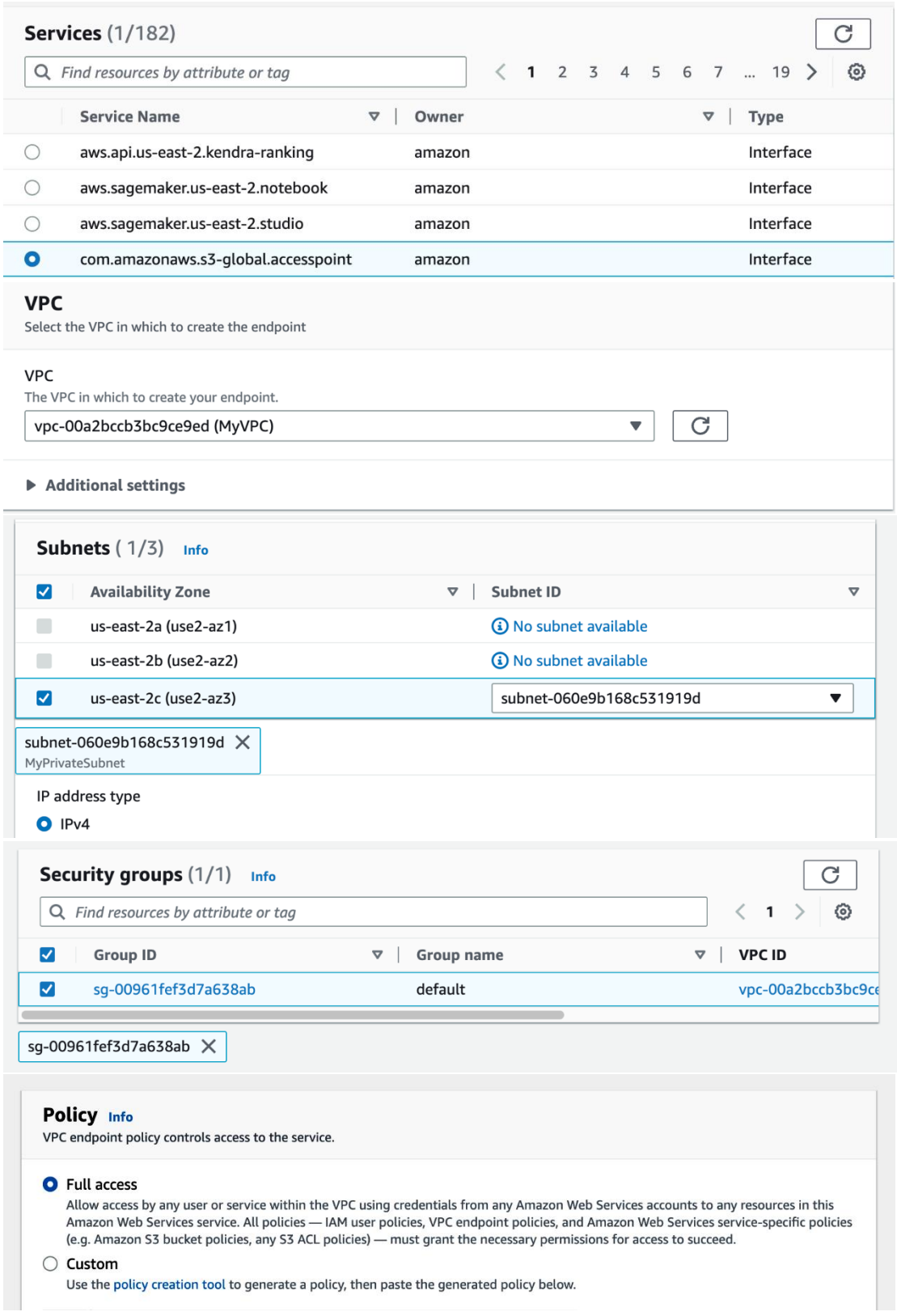
Creates a tag with a key of 'Name' and a value that you specify.

chapt10-s3

Service category

Select the service category

- (●) **AWS services** — Services provided by Amazon
- ( ) **PrivateLink Ready partner services** — Services with an AWS Service Ready designation
- ( ) **AWS Marketplace services** — Services that you've purchased through AWS Marketplace
- ( ) **Other endpoint services** — Find services shared with you by service name


Services (1/182)
Find resources by attribute or tag
1 2 3 4 5 6 7 ... 19
Service Name
Owner
Type
aws.api.us-east-2.kendra-ranking
amazon
Interface
aws.sagemaker.us-east-2.notebook
amazon
Interface
aws.sagemaker.us-east-2.studio
amazon
Interface
com.amazonaws.s3-global.accesspoint
amazon
Interface
VPC
Select the VPC in which to create the endpoint
VPC
The VPC in which to create your endpoint.
vpc-00a2bccb3bc9ce9ed (MyVPC)
Additional settings
Subnets (1/3) Info
Availability Zone
Subnet ID
us-east-2a (use2-az1)
No subnet available
us-east-2b (use2-az2)
No subnet available
us-east-2c (use2-az3)
subnet-060e9b168c531919d
subnet-060e9b168c531919d
MyPrivateSubnet
IP address type
IPv4
Security groups (1/1) Info
Find resources by attribute or tag
1
Group ID
Group name
VPC ID
sg-00961fef3d7a638ab
default
vpc-00a2bccb3bc9ce
sg-00961fef3d7a638ab
Policy Info
VPC endpoint policy controls access to the service.
Full access
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.
Custom
Use the policy creation tool to generate a policy, then paste the generated policy below.

Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 10

Configuring Infrastructure Security

Summary

In this chapter, you reviewed the foundational networking component of the AWS cloud, the VPC. You learned how to create a VPC network using a CloudFormation template with both a public and private subnet and then attach an IGW for internet connectivity. After creation, you explored the different components of the VPC to become familiar with them.

You then reviewed the different network connectivity options available for the VPCs in the account you are working on as well as other accounts and then the network traffic back to data centers that need to connect to AWS resources. These included options for connecting over public networks, such as VPNs to keep your transmissions secure and encrypted, along with Direct Connect, peering, and endpoints to keep your transmissions off the public internet.

Chapter 11, Securing EC2 Instances, will discuss how to secure EC2 instances when you are inside the perimeter of your network.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

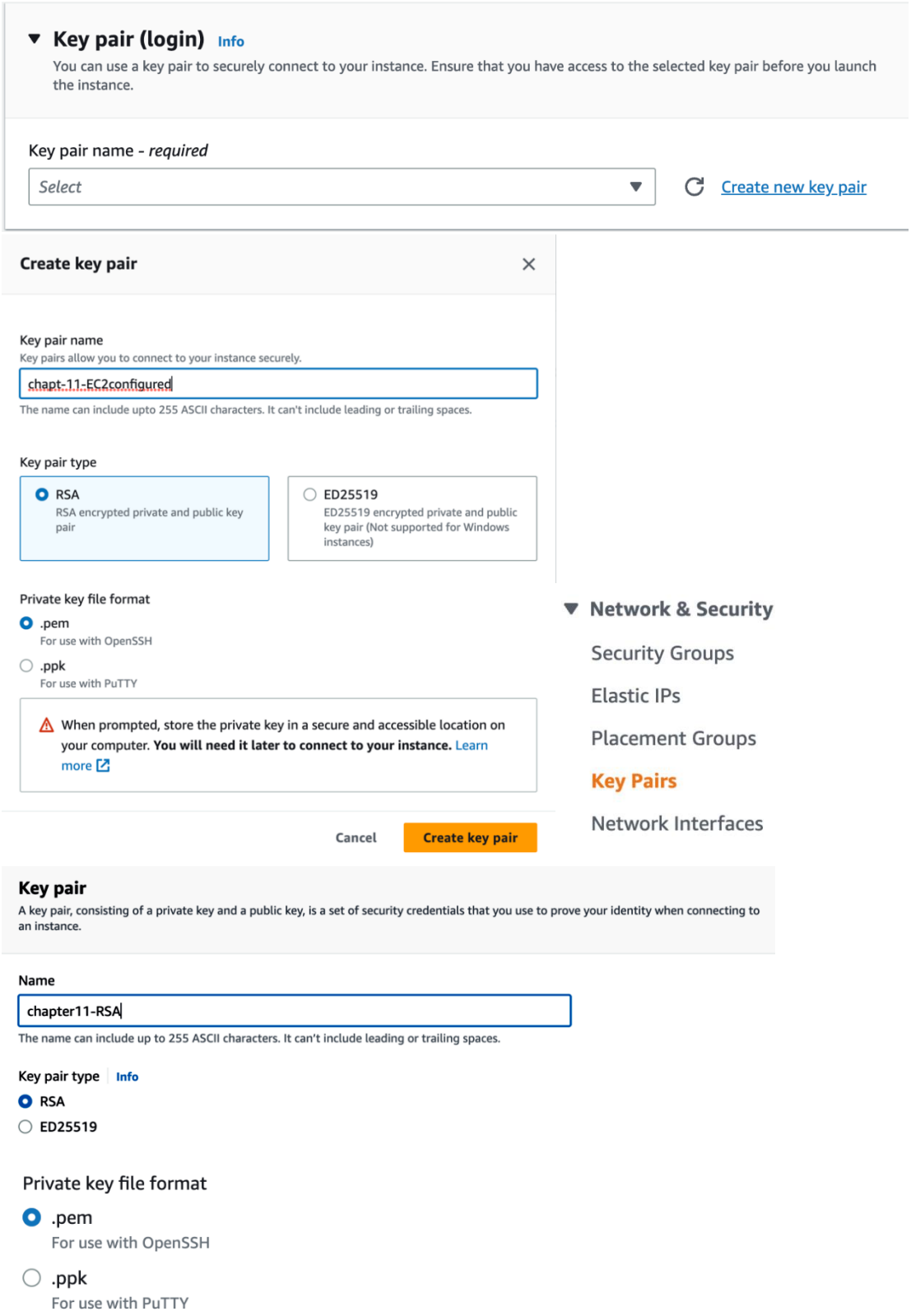
Select Quiz

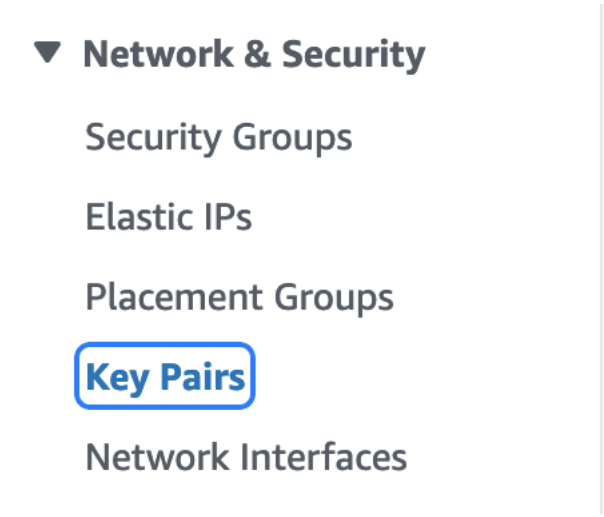
Quiz 1

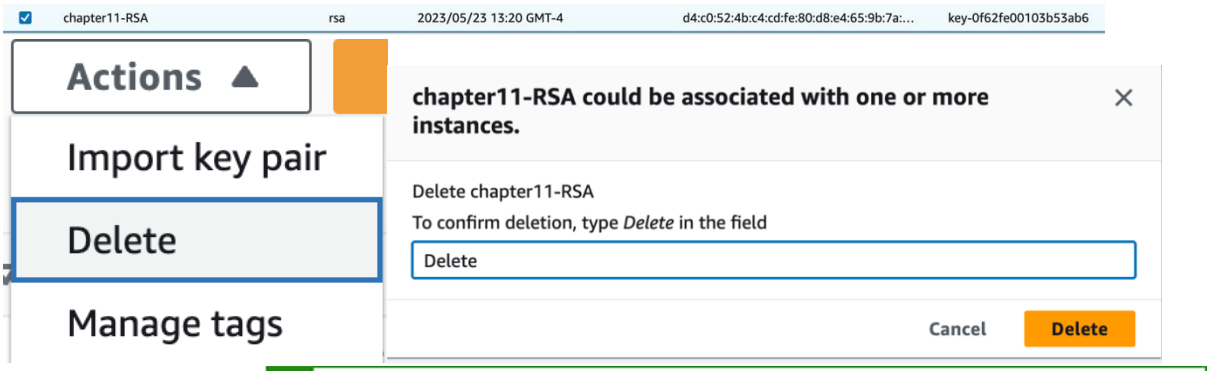
SHOW QUIZ DETAILS

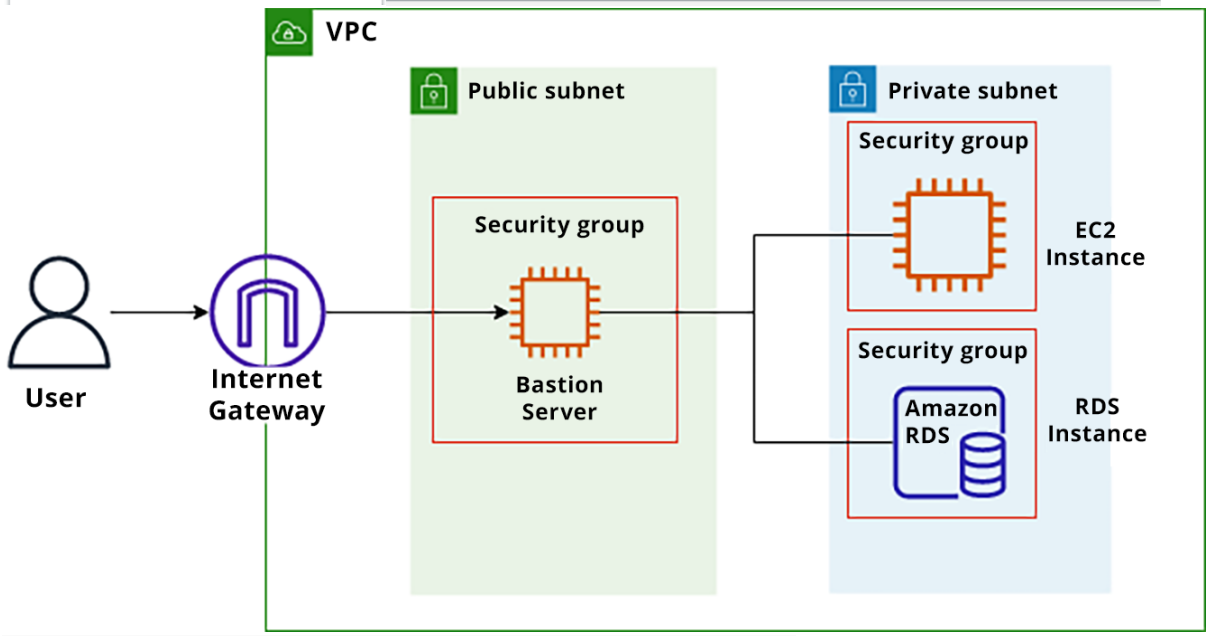
START

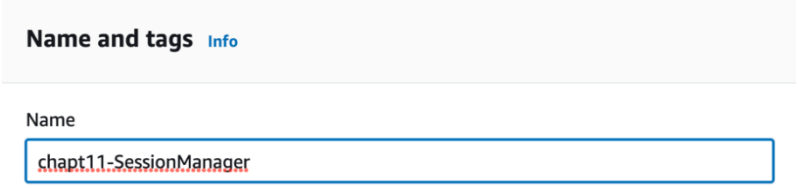
Chapter 11:

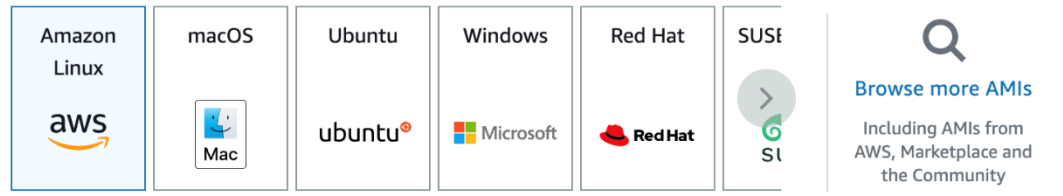

Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Select
Create new key pair
Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
chapt-11-EC2configured
The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more
Cancel
Create key pair
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.
Name
chapter11-RSA
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type Info
RSA
ED25519
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY


Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces


chapter11-RSA
rsa
2023/05/23 13:20 GMT-4
d4:c0:52:4b:c4:cd:fe:80:d8:e4:65:9b:7a:...
key-0f62fe00103b53ab6
Actions
Import key pair
Delete
Manage tags
chapter11-RSA could be associated with one or more instances.
Delete chapter11-RSA
To confirm deletion, type Delete in the field
Delete
Cancel
Delete


VPC
Public subnet
Private subnet
Security group
Security group
EC2 Instance
Security group
Amazon RDS
RDS Instance
User
Internet Gateway
Bastion Server


Name and tags Info
Name
chapt11-SessionManager



Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-08333bccc35d71140 (64-bit (x86)) / ami-062531c465b1004a1 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.0.20230503.0 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86)

AMI ID: ami-08333bccc35d71140 — Verified provider

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Proceed without a key pair (Not recommended) — Default value

Create new key pair

VPC - *required* Info

vpc-00a2bccb3bc9ce9ed (MyVPC)
10.0.0.0/16

Subnet Info

subnet-060e9b168c531919d — MyPrivateSubnet
VPC: vpc-00a2bccb3bc9ce9ed Owner: 182968331794 Availability Zone: us-east-2c
IP addresses available: 251 CIDR: 10.0.2.0/24)

Auto-assign public IP Info

Disable

Select trusted entity Info

Trusted entity type

- AWS service — Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account — Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity — Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

Permissions policies (903) Info

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

SSM

Role name

Enter a meaningful name to identify this role.

chapt11-SSM

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

- Node Management
  - Fleet Manager
  - Compliance
  - Inventory
  - Hybrid Activations
  - Session Manager
  - Run Command
  - State Manager

IAM instance profile Info

chapt11-SSM
arn:aws:iam::182968331794:instance-profile/chapt11-SSM

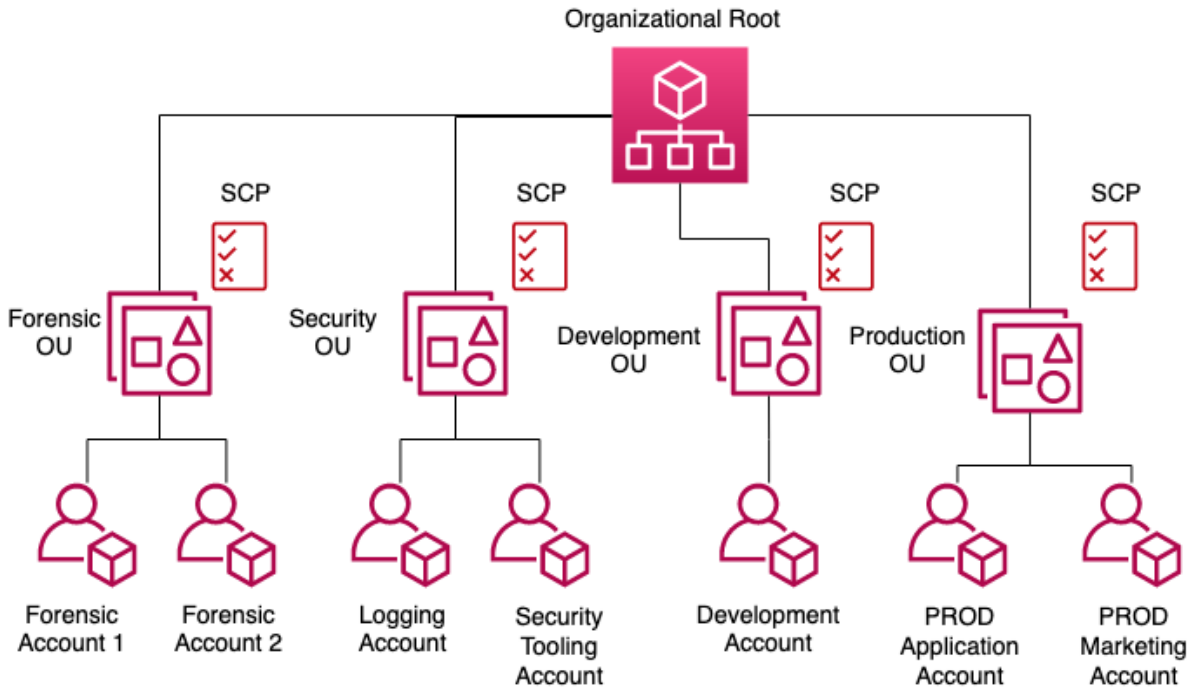
Target instances

Filter instances

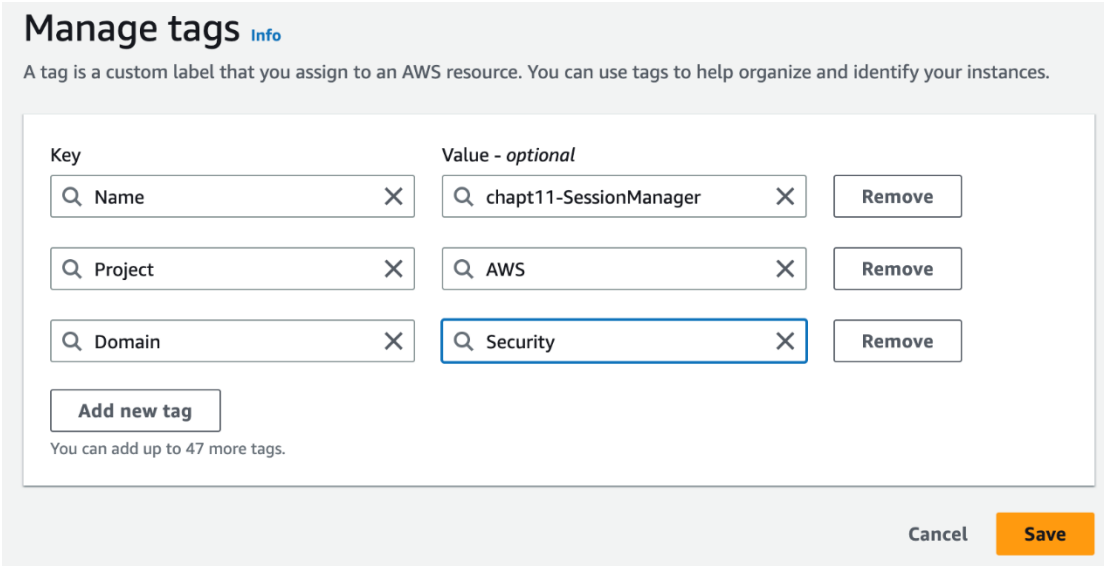
1

	Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
◉	chapt11-SessionManager	i-0de9b3f4fe0fcde3c	3.1.1927.0	running	us-east-2c	Amazon Linux

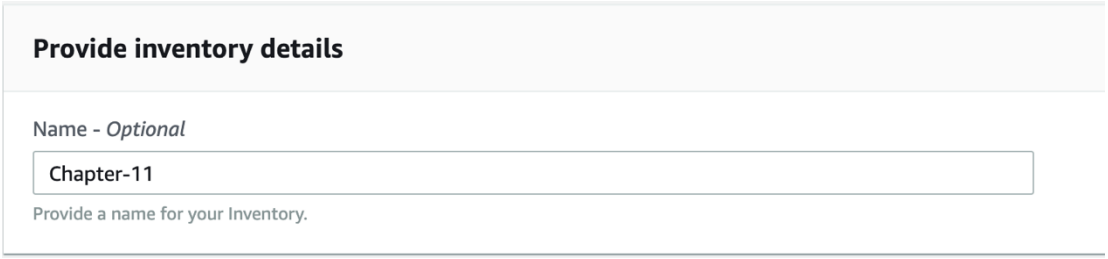
Start session

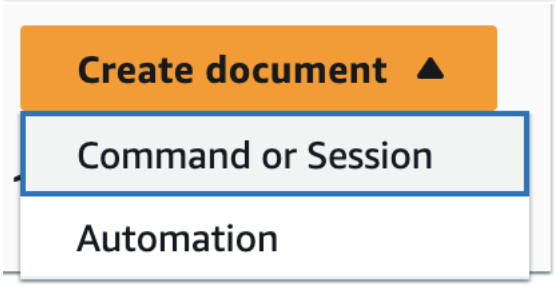


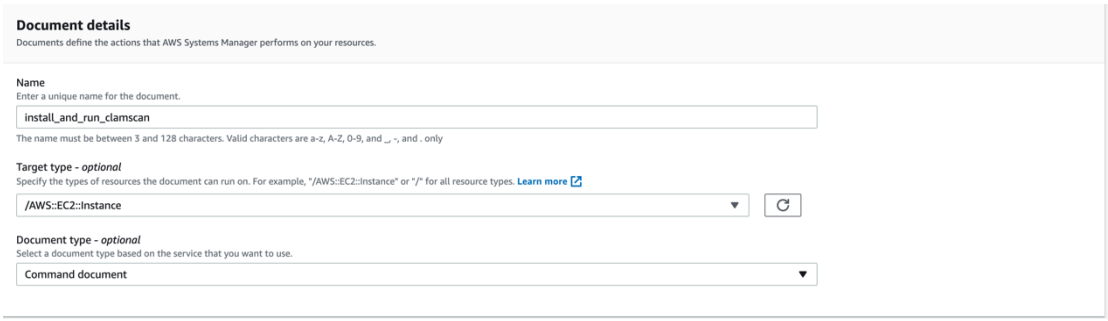
Details | Status and alarms New | Monitoring | Security | Networking | Storage | Tags


Manage tags Info
A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.
Key
Value - optional
Name
chapt11-SessionManager
Remove
Project
AWS
Remove
Domain
Security
Remove
Add new tag
You can add up to 47 more tags.
Cancel
Save


Node Management
Fleet Manager
Compliance
Inventory
Hybrid Activations
Session Manager
Run Command
State Manager
Patch Manager
Distributor


Provide inventory details
Name - Optional
Chapter-11
Provide a name for your Inventory.


Create document
Command or Session
Automation


Document details
Documents define the actions that AWS Systems Manager performs on your resources.
Name
Enter a unique name for the document.
install_and_run_clamscan
The name must be between 3 and 128 characters. Valid characters are a-z, A-Z, 0-9, and _, -, and . only
Target type - optional
Specify the types of resources the document can run on. For example, "/AWS::EC2::Instance" or "/" for all resource types. Learn more
/AWS::EC2::Instance
Document type - optional
Select a document type based on the service that you want to use.
Command document

Content

JSON
Specify document content in JSON format.

YAML
Specify document content in YAML format.

Owned by Amazon | Owned by me | Shared with me | Favorites - new | All documents

Target selection

Target selection
Choose a method for selecting targets.

Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.

Choose instances manually
Manually select the instances you want to register as targets.

Choose a resource group
Choose a resource group that includes the resources you want to target.

Specify instance tags
Specify one or more instance tag key-value pairs to identify the instances where the tasks will run

Tag key | Tag value (optional) | Add

Enter a tag key and optional value applied to the instances you want to target, and then choose **Add**.

Domain : Security

Output options

Write command output to an Amazon S3 bucket
Write all command output to an Amazon S3 bucket. Command output in the console is truncated after 24,000 characters.

Enable an S3 bucket

Send command output to Amazon CloudWatch logs
You can stream and encrypt log data for all commands in your account to a CloudWatch Logs log group in your account. **Learn more**

Enable CloudWatch logs

Amazon Linux 2 AMI with Amazon Inspector Agent

By: Amazon Web Services Latest Version: 1.0

Amazon Inspector is an on-demand, pay-as-you-go vulnerability assessment service. Inspector analyzes the configuration of operating systems, applications, and networks to identify

Show more

Linux/Unix

Continue to Subscribe

Save to List

Typical Total Price
$0.133/hr
Total pricing per instance for services hosted on m3.large in US East (N. Virginia). View Details

```
sh-5.2$ cd -
sh-5.2$ wget https://inspector-agent.amazonaws.com/linux/latest/install
--2024-04-01 11:18:01--  https://inspector-agent.amazonaws.com/linux/latest/install
Resolving inspector-agent.amazonaws.com (inspector-agent.amazonaws.com)... 3.160.19.138, 2600:9000:25f3:e400:4:6195:f553:e781, 2600:9000:25f3:1c00:4:6195:f553:e781, ...
Connecting to inspector-agent.amazonaws.com (inspector-agent.amazonaws.com)|3.160.19.138|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31083 (30K) [binary/octet-stream]
Saving to: 'install'

install                             100%[=========================================================================================>]  30.35K  --.-KB/s    in 0s

2024-04-01 11:18:01 (308 MB/s) - 'install' saved [31083/31083]
```

Delegated administrator

Delegate permissions to manage Inspector for this organization

Delegate

The delegated administrator is granted all of the permissions required to administer Inspector for your organization. When you choose a delegated administrator, Inspector is activated for that account.

Delegated administrator account ID

Enter account ID (ex: 012345678901)

Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 11

Securing EC2 Instances

Summary

In this chapter, you learned how to create key pairs for your EC2 instances so that you could securely access your instances over either the SSH or RDP protocols. Then, you examined how to securely access your private AWS infrastructure using a hardened bastion server or the AWS Session Manager service.

You also saw how to take your previously configured EC2 instance and then install the Amazon Inspector agent on it so that the latter can inform you if it finds any vulnerabilities.

In *Chapter 12, Managing Key Infrastructure*, you will examine the Amazon-managed encryption service KMS. You will go through steps to create your customer-managed keys and learn how different permissions can be set so that users from various groups in your organization can access data using those keys. You will also see how keys can be either rotated automatically or manually based on the needs of your organization.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

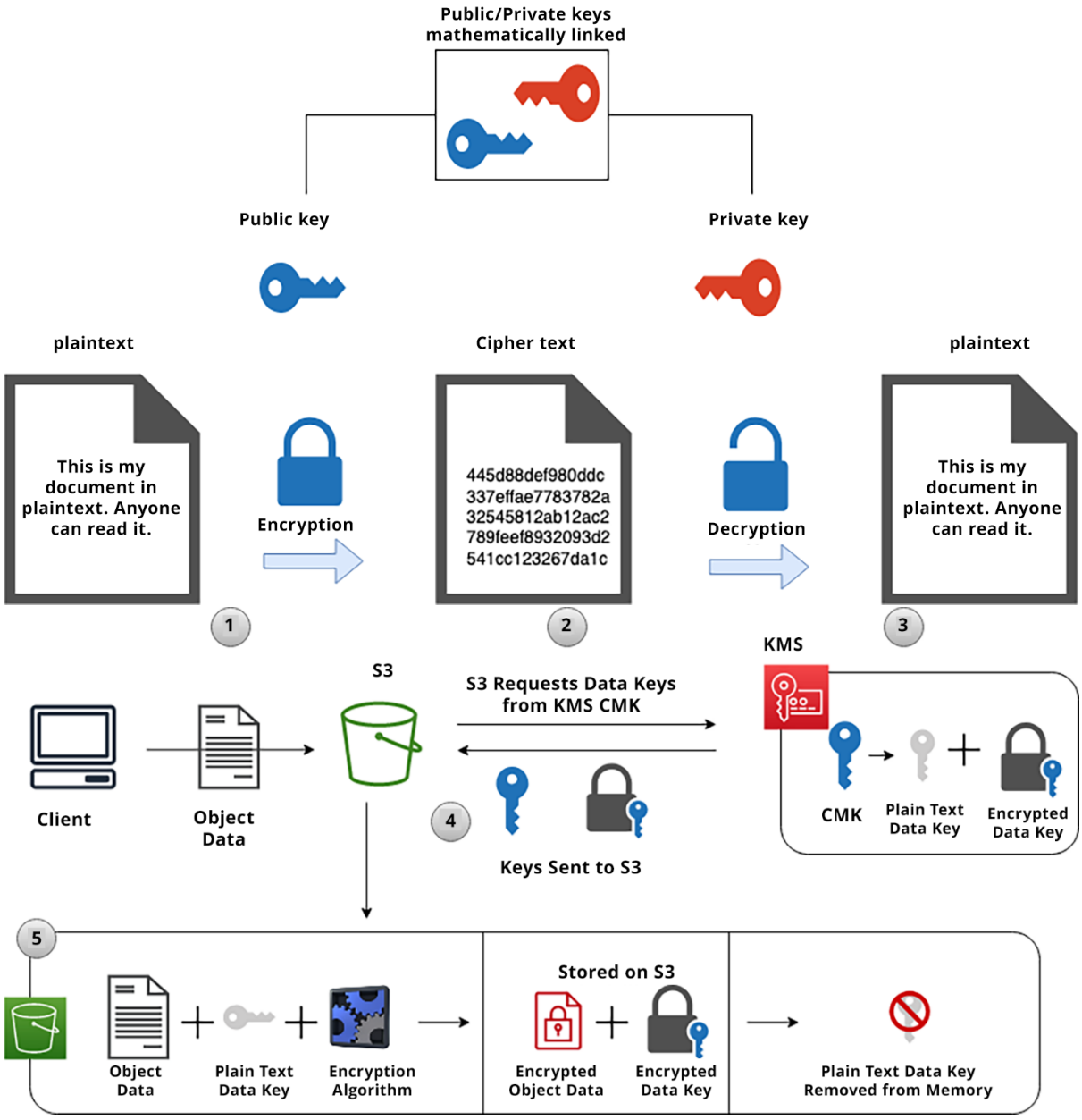
Select Quiz

Quiz 1

SHOW QUIZ DETAILS

START

Chapter 12:


Public/Private keys mathematically linked
Public key
Private key
plaintext
This is my document in plaintext. Anyone can read it.
Encryption
Cipher text
445d88def980ddc
337effae7783782a
32545812ab12ac2
789feef8932093d2
541cc123267da1c
Decryption
plaintext
This is my document in plaintext. Anyone can read it.
1
2
3
KMS
S3
S3 Requests Data Keys from KMS CMK
Client
Object Data
CMK
Plain Text Data Key
Encrypted Data Key
4
Keys Sent to S3
5
Object Data
Plain Text Data Key
Encryption Algorithm
Stored on S3
Encrypted Object Data
Encrypted Data Key
Plain Text Data Key Removed from Memory

Advanced options

Key material origin Help me choose

- KMS
- External (Import Key material)
- AWS CloudHSM key store
- External key store

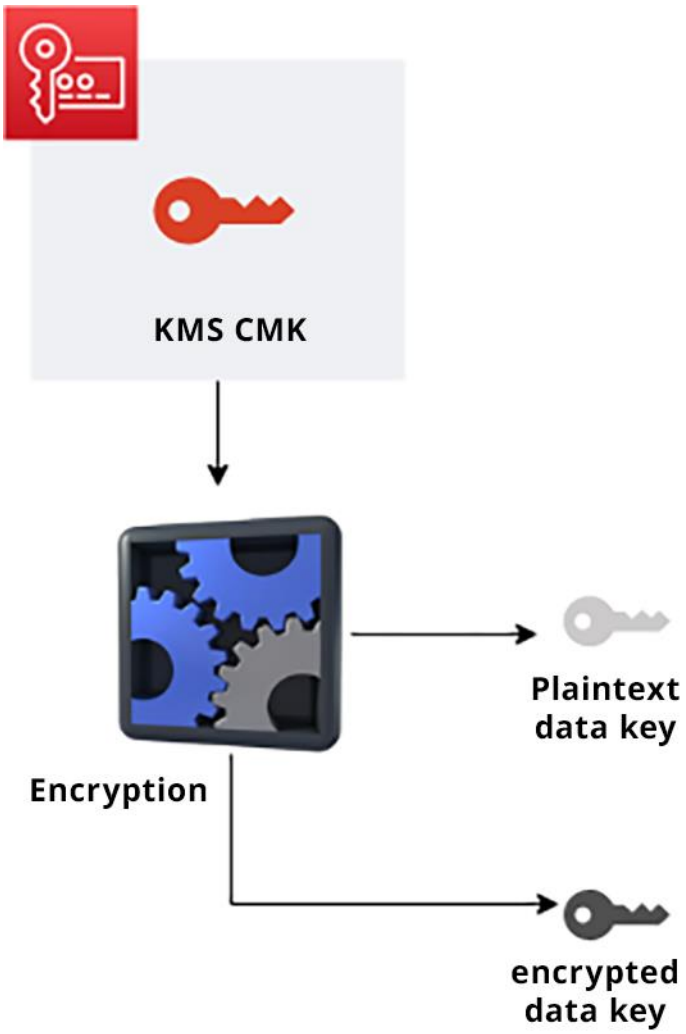
You can import symmetric 256-bit key material from your key management infrastructure into AWS KMS and use it like any other AWS KMS key.

I understand the security, availability, and durability implications of using an imported key.

Regionality

You cannot change this setting after the key is created. Help me choose

- Single-Region key
  Never allow this key to be replicated into other Regions
- Multi-Region key
  Allow this key to be replicated into other Regions



Configure key

Key type Help me choose

- (•) Symmetric
  A single key used for encrypting and decrypting data or generating and verifying HMAC codes
- ( ) Asymmetric
  A public and private key pair used for encrypting and decrypting data or signing and verifying messages

Key usage Help me choose

- (•) Encrypt and decrypt
  Use the key only to encrypt and decrypt data.
- ( ) Generate and verify MAC
  Use the key only to generate and verify hash-based message authentication codes (HMAC).

▼ Advanced options

Key material origin Help me choose

- (•) KMS
- ( ) External (Import Key material)

Regionality

You cannot change this setting after the key is created. Help me choose

- ( ) Single-Region key
  Never allow this key to be replicated into other Regions
- (•) Multi-Region key
  Allow this key to be replicated into other Regions

Cancel **Next**

Add labels

Alias

You can change the alias at any time. Learn more

Alias

Chapter12-USEAST2

Description - *optional*

You can change the description at any time.

Description

This is my symmetrickey

Key deletion

- [x] Allow key administrators to delete this key.

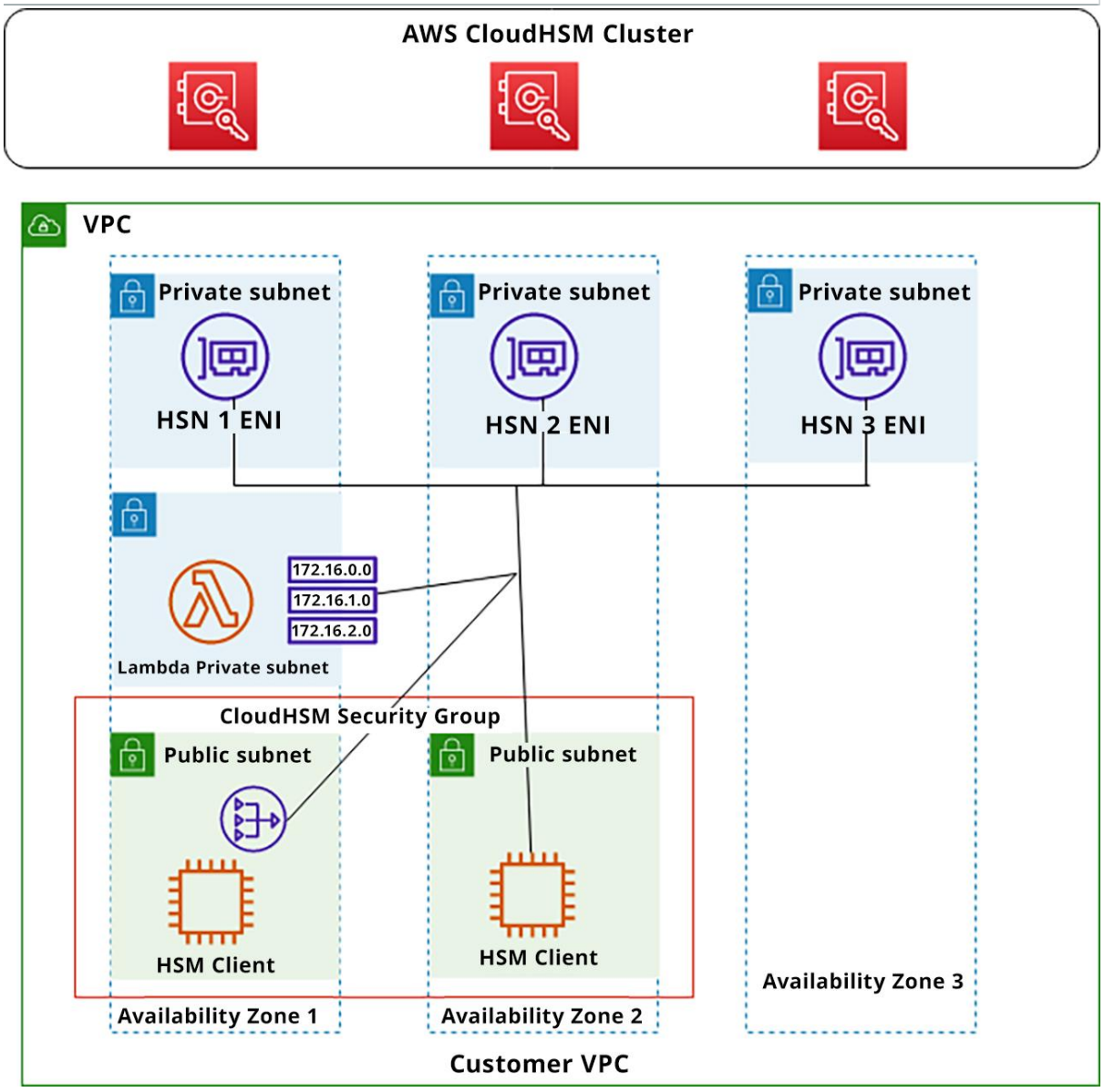
Key policy | Cryptographic configuration | Tags | Key rotation | Regionality | Aliases

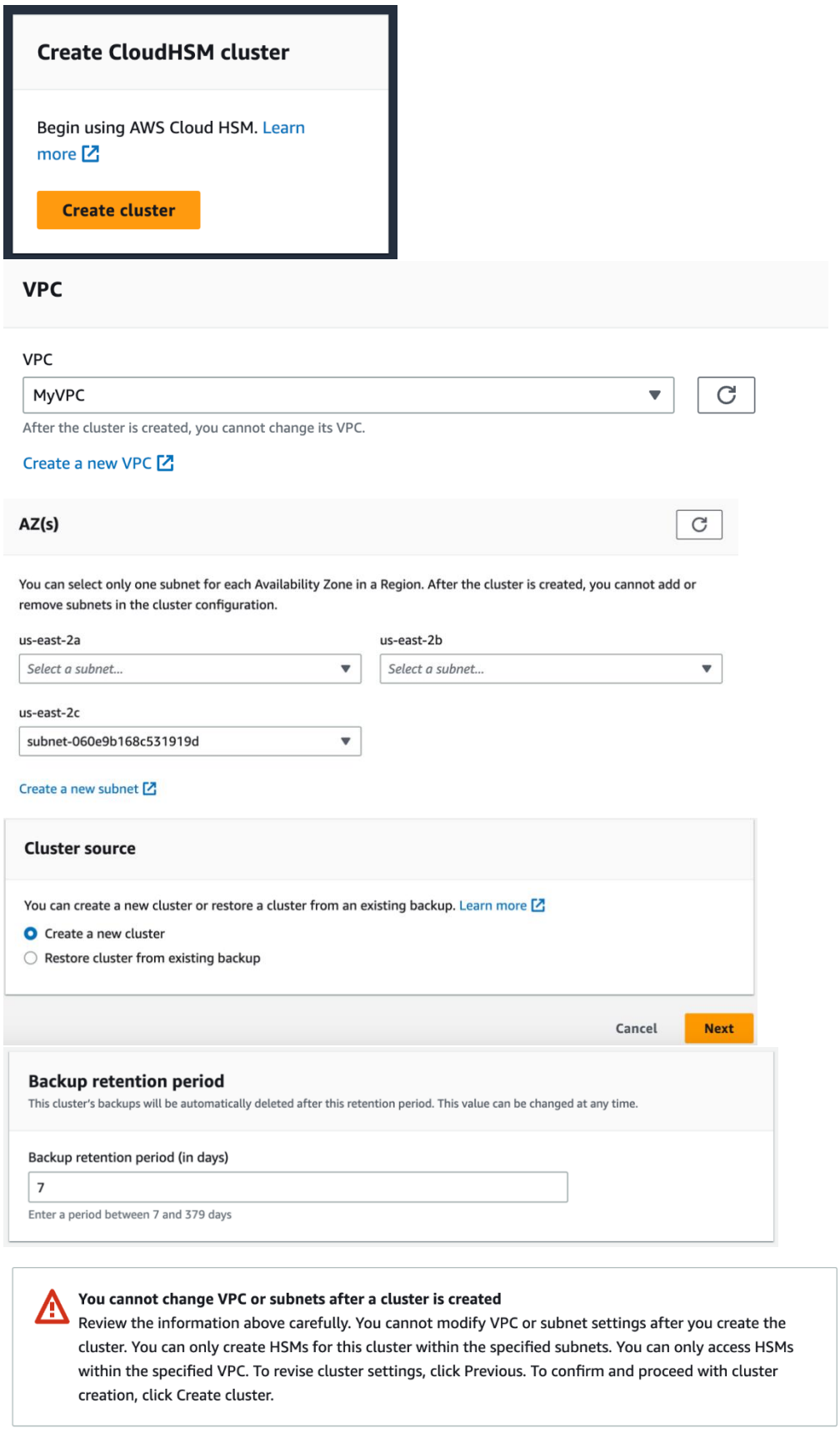
Select replica Regions

Choose Regions for your new replica keys

Choose Regions

US West (Oregon) ×
us-west-2




Create CloudHSM cluster
Begin using AWS Cloud HSM. Learn more
Create cluster
VPC
VPC
MyVPC
After the cluster is created, you cannot change its VPC.
Create a new VPC
AZ(s)
You can select only one subnet for each Availability Zone in a Region. After the cluster is created, you cannot add or remove subnets in the cluster configuration.
us-east-2a
Select a subnet...
us-east-2b
Select a subnet...
us-east-2c
subnet-060e9b168c531919d
Create a new subnet
Cluster source
You can create a new cluster or restore a cluster from an existing backup. Learn more
Create a new cluster
Restore cluster from existing backup
Cancel
Next
Backup retention period
This cluster's backups will be automatically deleted after this retention period. This value can be changed at any time.
Backup retention period (in days)
7
Enter a period between 7 and 379 days
You cannot change VPC or subnets after a cluster is created
Review the information above carefully. You cannot modify VPC or subnet settings after you create the cluster. You can only create HSMs for this cluster within the specified subnets. You can only access HSMs within the specified VPC. To revise cluster settings, click Previous. To confirm and proceed with cluster creation, click Create cluster.

Practice Resources

SHARE FEEDBACK

sk

DASHBOARD > CHAPTER 12

Managing Key Infrastructure

Summary

In this chapter, you looked at the leading service for encrypting data at rest in AWS, Key Management Service, or KMS. You were given a basic introduction to encryption, and the difference between symmetric and asymmetric encryption keys was explained. You learned all about the major components of the KMS service: customer-managed keys, data encryption keys, key material, key policies, and grants.

You saw how the AWS Artifact service can help you check the compliance of the KMS keys you are using and the compliance of other services. You also learned how AWS Artifact is a self-service document repository that can help you with auditing or if you need to look up something that could be found in the customer agreement.

In *Chapter 13, Access Management*, you will review a new section regarding IAM. This section will begin with access management and discuss how you can allow users access to your systems natively with the IAM service, along with creating groups of users.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

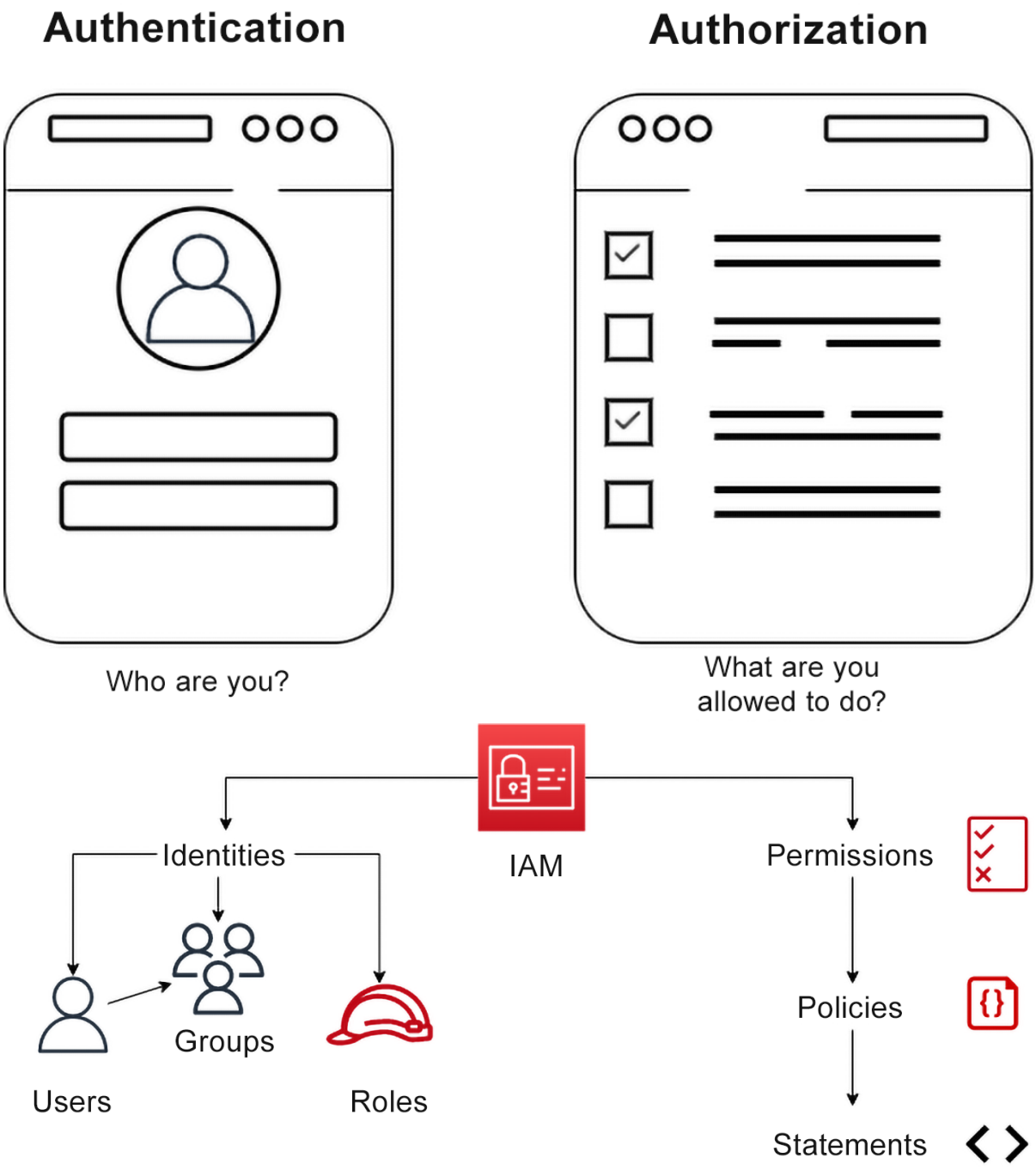
Select Quiz

Quiz 1

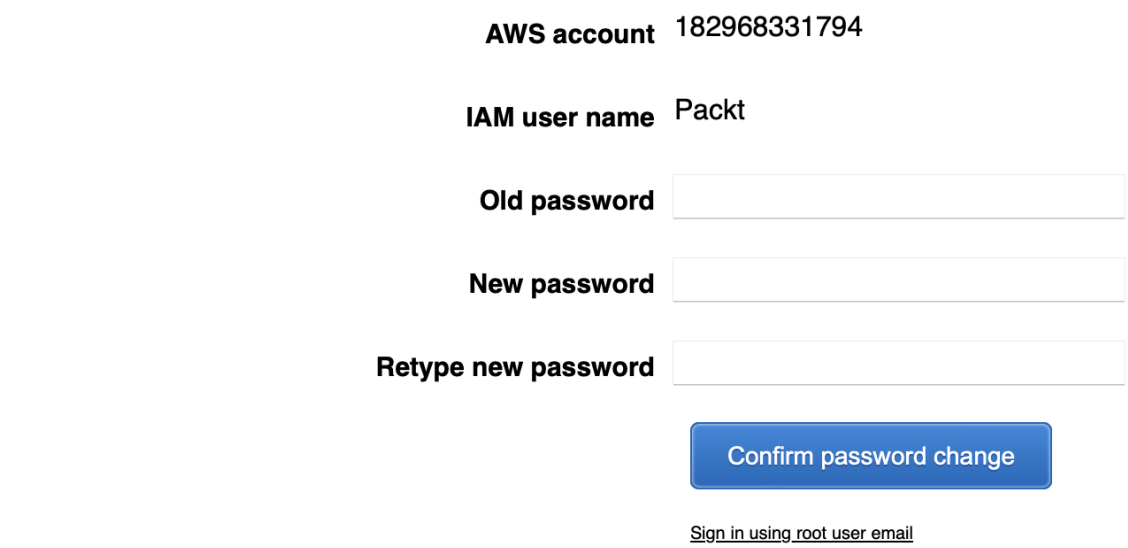
SHOW QUIZ DETAILS

START

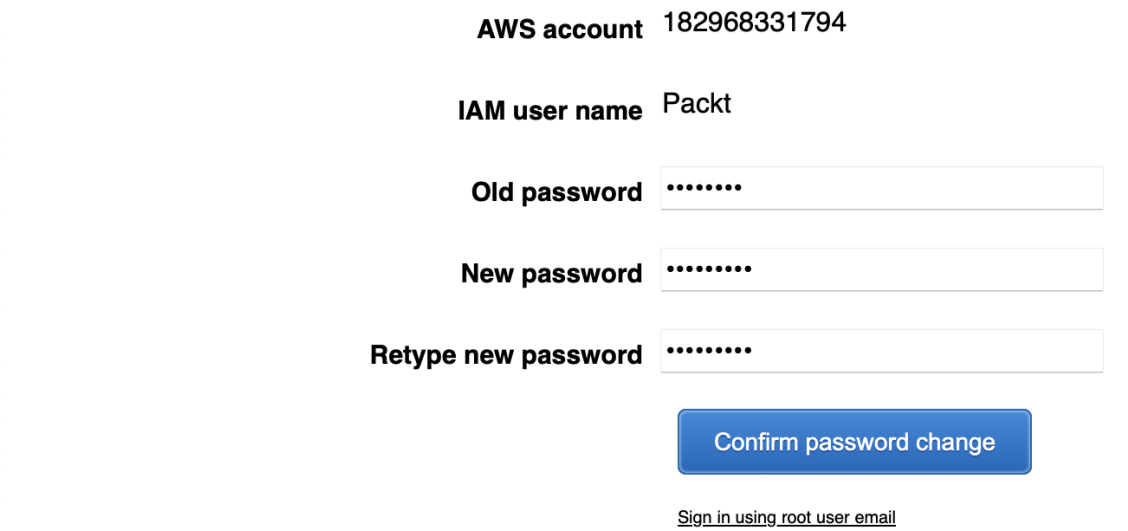
Chapter 13:

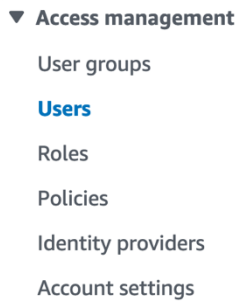

Authentication
Authorization
Who are you?
What are you allowed to do?
IAM
Identities
Users
Groups
Roles
Permissions
Policies
Statements

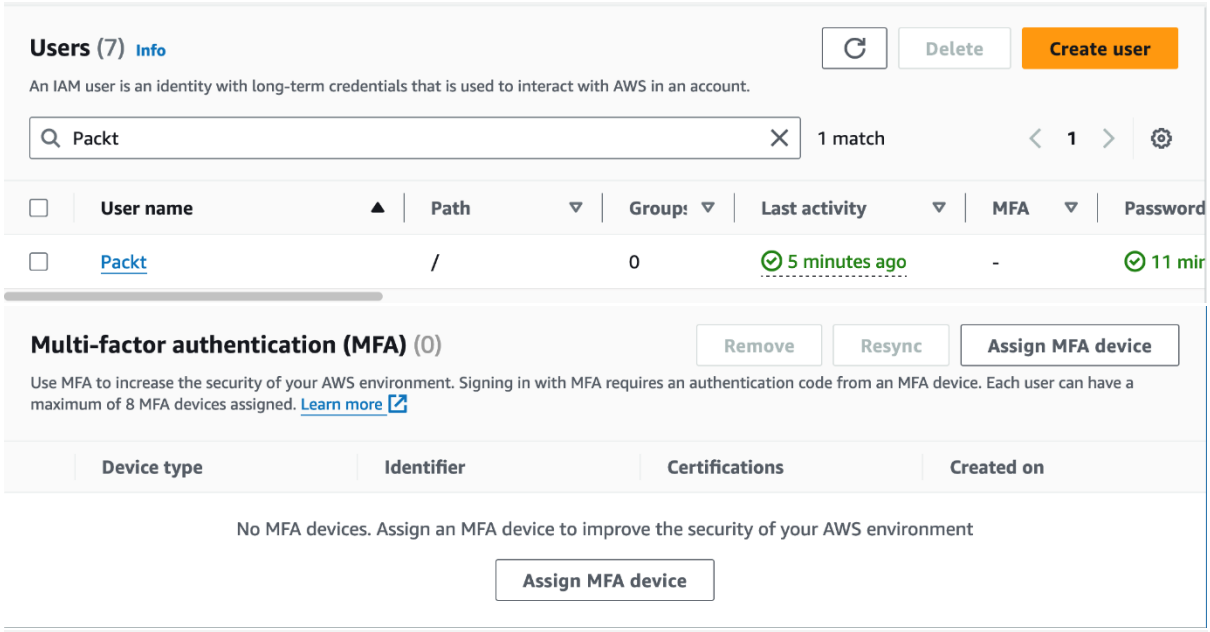
You must change your password to continue

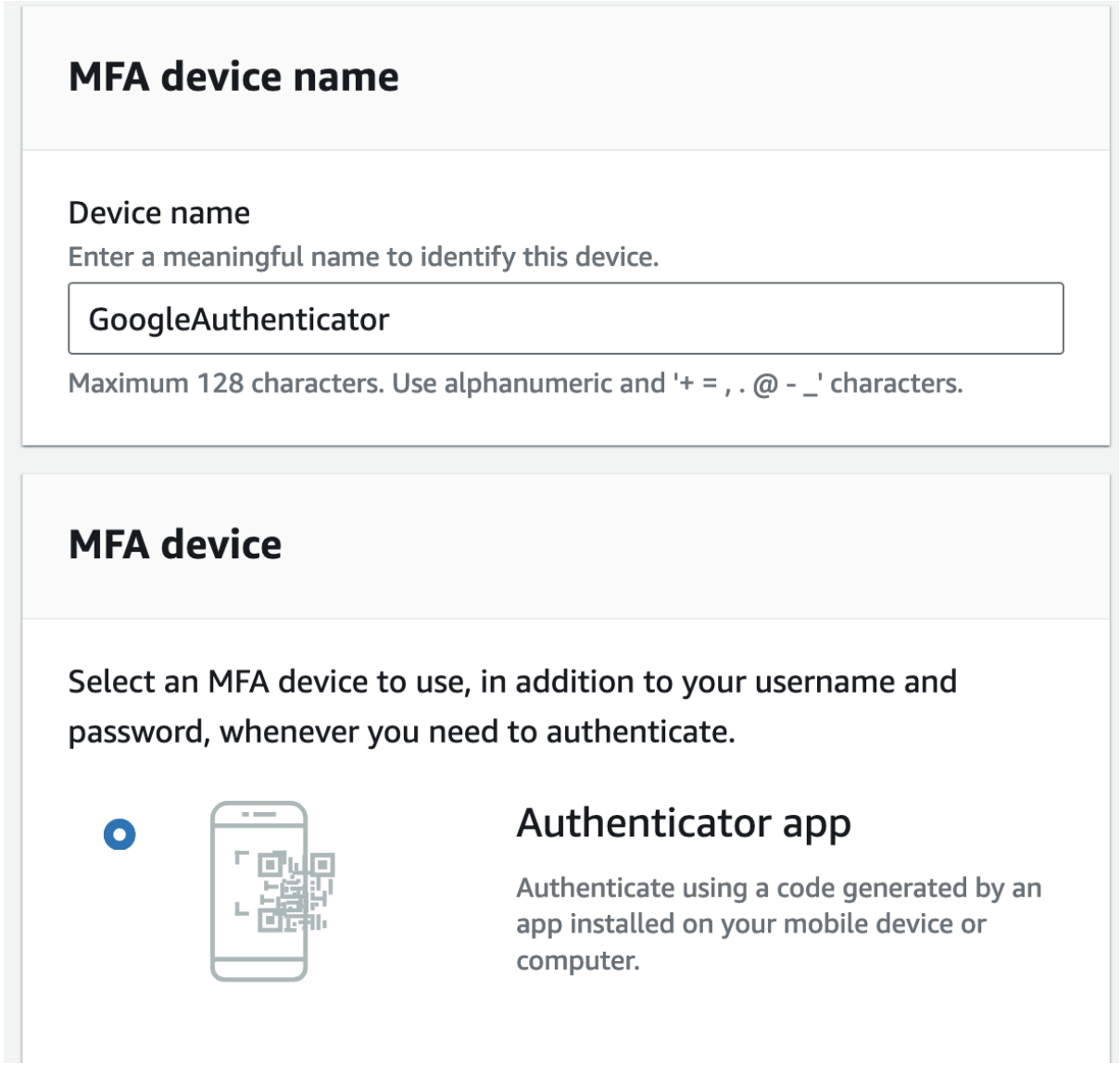


You must change your password to continue





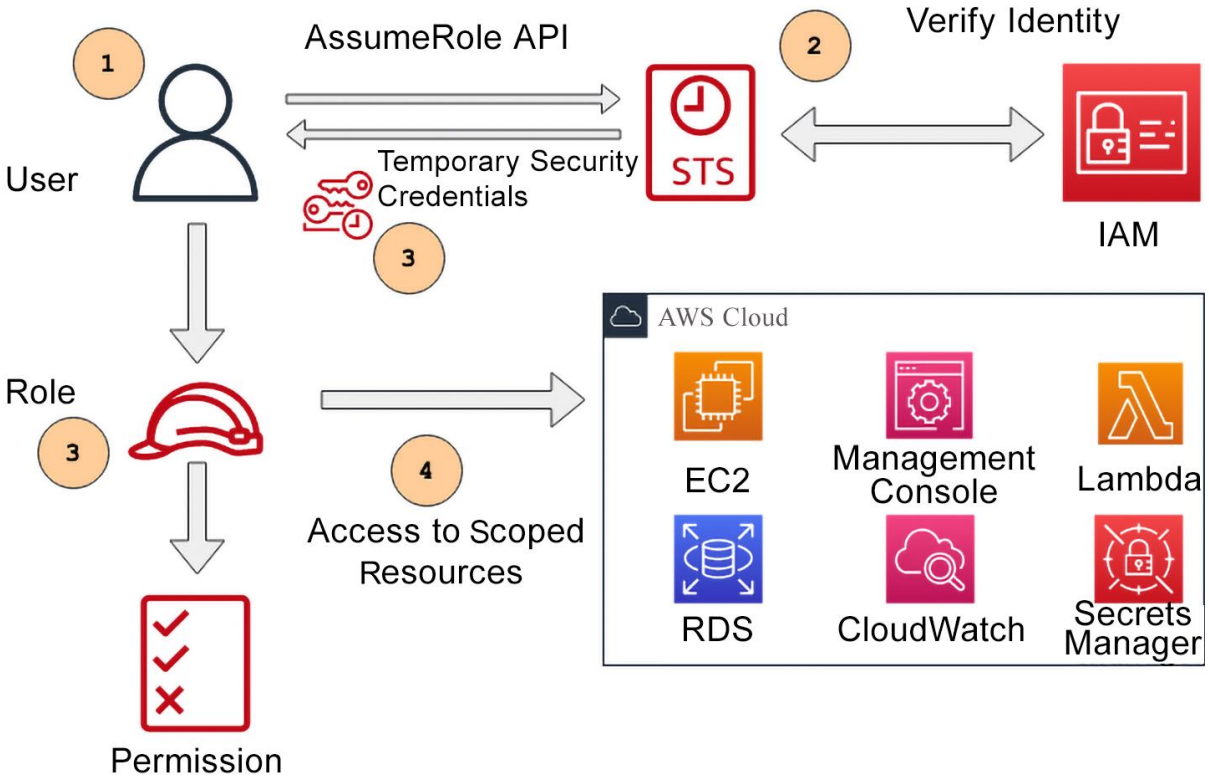

Users (7) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Packt
1 match
1
User name
Path
Groups
Last activity
MFA
Password
Packt
/
0
5 minutes ago
-
11 min
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Device type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device


MFA device name
Device name
Enter a meaningful name to identify this device.
GoogleAuthenticator
Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.
MFA device
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.
Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

2

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.
Show secret key

Fill in two consecutive codes from your MFA device.



Practice Resources

SHARE FEEDBACK

sk

DASHBOARD > CHAPTER 13

Access Management

Summary

This chapter discussed the IAM service. You saw how authentication and authorization form the basis of IAM and discovered some of the best practices for using IAM. You completed an exercise of creating a group in IAM, creating a new user, adding a policy to that user, and then adding that user to the previously created group.

You also saw how STS could be used to create temporary security credentials, which are more secure than providing long-term security credentials for both users and roles. Finally, you reviewed AWS IAM Identity Center and how it can help manage user accounts across many accounts in an AWS organization and provide consolidated access to those same users to SaaS applications outside of your AWS environment.

In *Chapter 14, Working with Access Policies*, you will examine the policies and constructs used in IAM policies, service control policies, and other policies.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

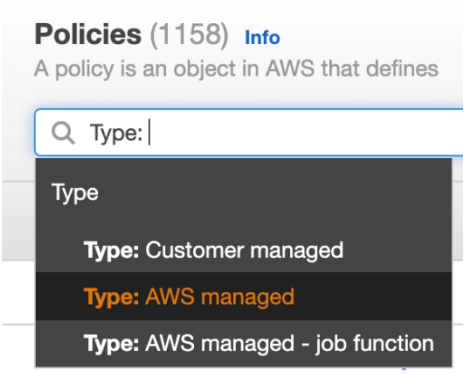
Select Quiz

Quiz 1

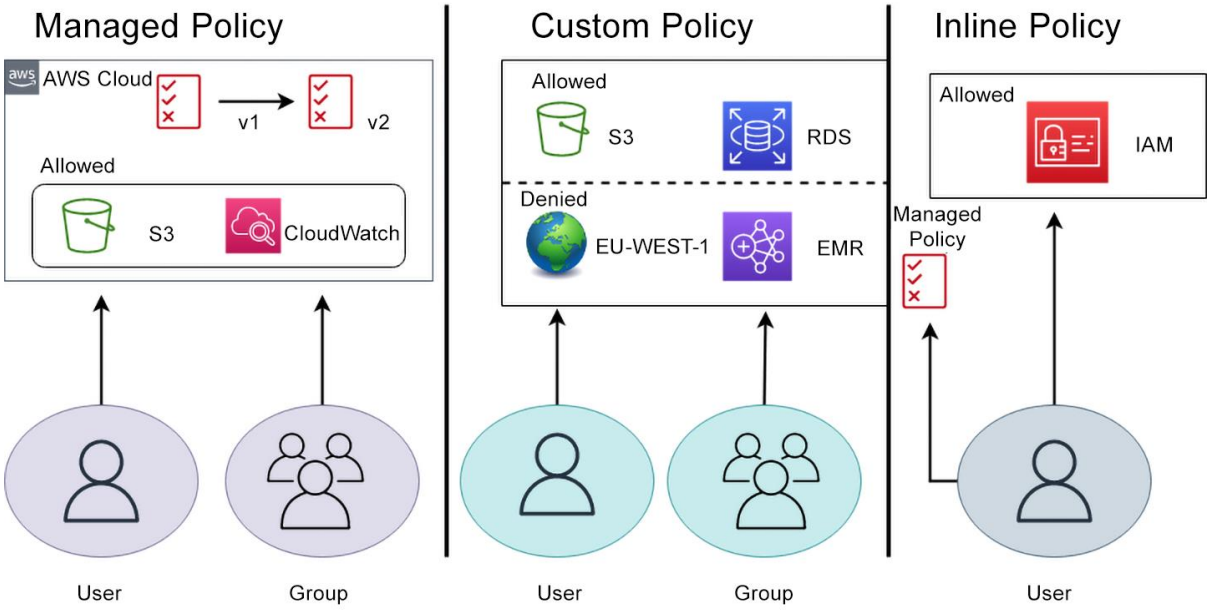
SHOW QUIZ DETAILS

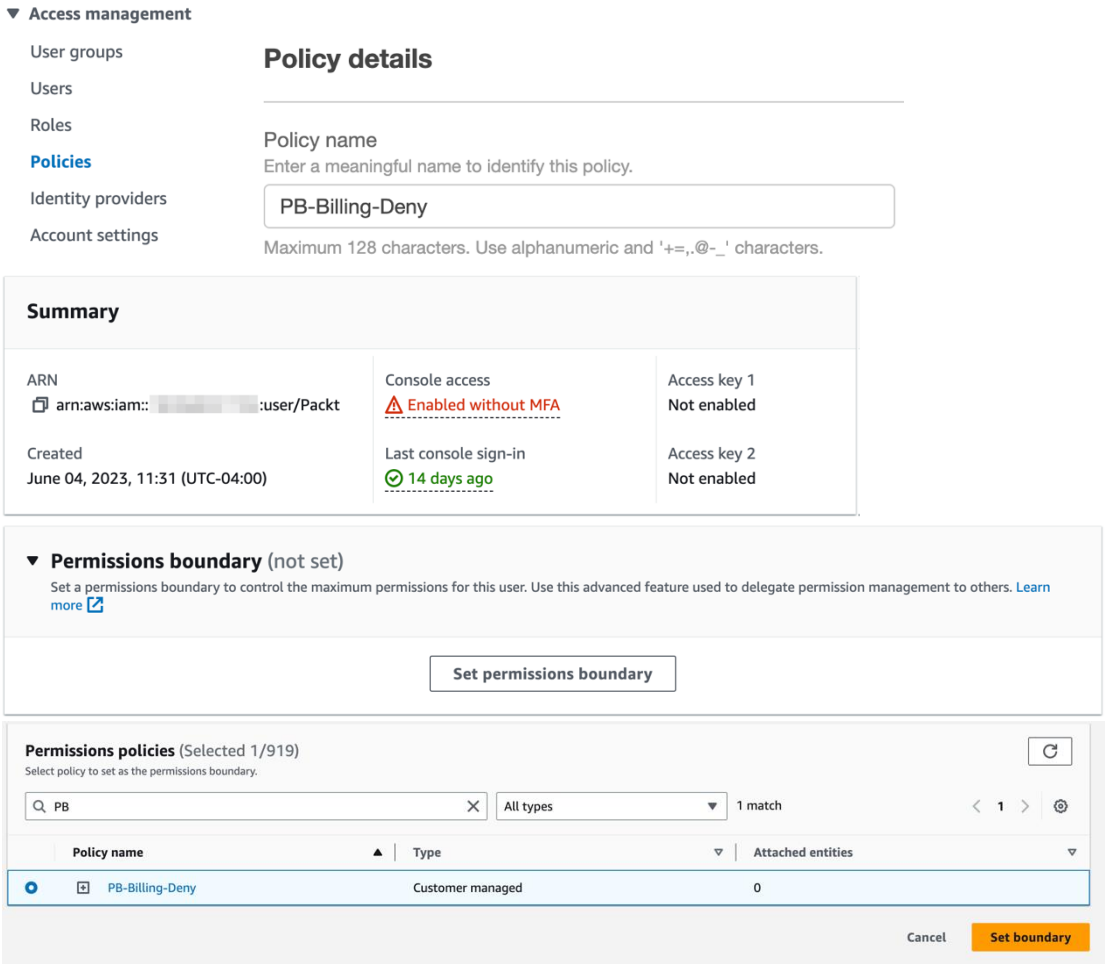
START

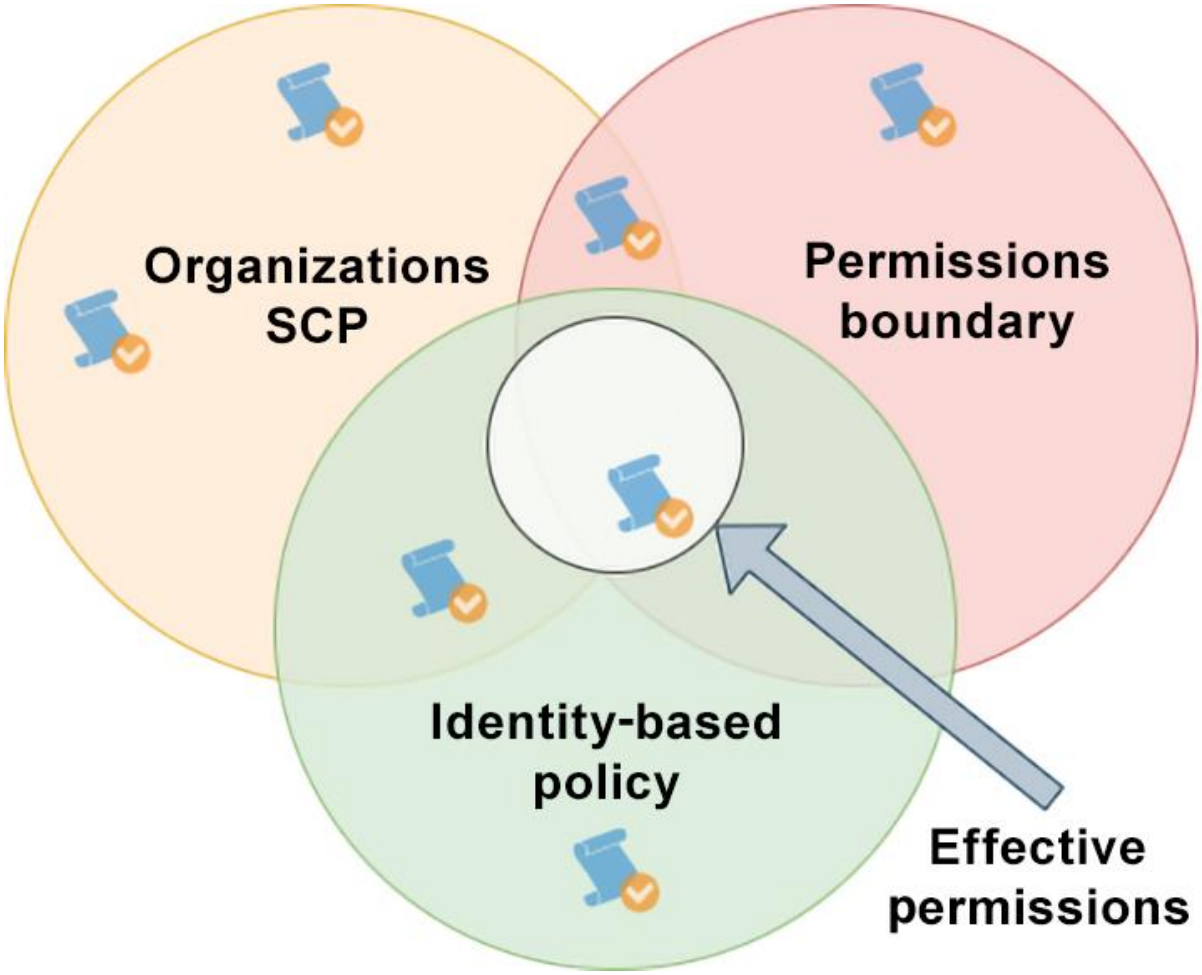
Chapter 14:



⊞	AmazonWorkSpacesApplicationManagerAdminAccess	AWS managed
⊞	AmazonAPIGatewayAdministrator	AWS managed
⊞	AmazonWorkSpacesAdmin	AWS managed
⊞	AWSCodeBuildAdminAccess	AWS managed
⊞	AWSCloud9Administrator	AWS managed
⊞	AWSServiceCatalogAdminFullAccess	AWS managed
⊞	CloudWatchAgentAdminPolicy	AWS managed
⊞	AWSAppSyncAdministrator	AWS managed
⊞	AWSFMAdminFullAccess	AWS managed
⊞	AWSFMAdminReadOnlyAccess	AWS managed
⊞	AWSSSOMasterAccountAdministrator	AWS managed
⊞	AWSSSOMemberAccountAdministrator	AWS managed




Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Policy details
Policy name
Enter a meaningful name to identify this policy.
PB-Billing-Deny
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Summary
ARN
arn:aws:iam::
:user/Packt
Console access
Enabled without MFA
Access key 1
Not enabled
Created
June 04, 2023, 11:31 (UTC-04:00)
Last console sign-in
14 days ago
Access key 2
Not enabled
Permissions boundary (not set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
Set permissions boundary
Permissions policies (Selected 1/919)
Select policy to set as the permissions boundary.
PB
All types
1 match
1
Policy name
Type
Attached entities
PB-Billing-Deny
Customer managed
0
Cancel
Set boundary



IAM > Policies > ABC-ABAC-User-Service-Policy

ABC-ABAC-User-Service-Policy

Delete

access to all items tagged with workload ABC

Policy details

Type	Creation time	Edited time	ARN
Customer managed	February 23, 2023, 08:38 (UTC-05:00)	February 23, 2023, 12:34 (UTC-05:00)	arn:aws:iam::182968331794:policy/ABC-ABAC-User-Service-Policy

Permissions | Entities attached | Tags | Policy versions | Access Advisor

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

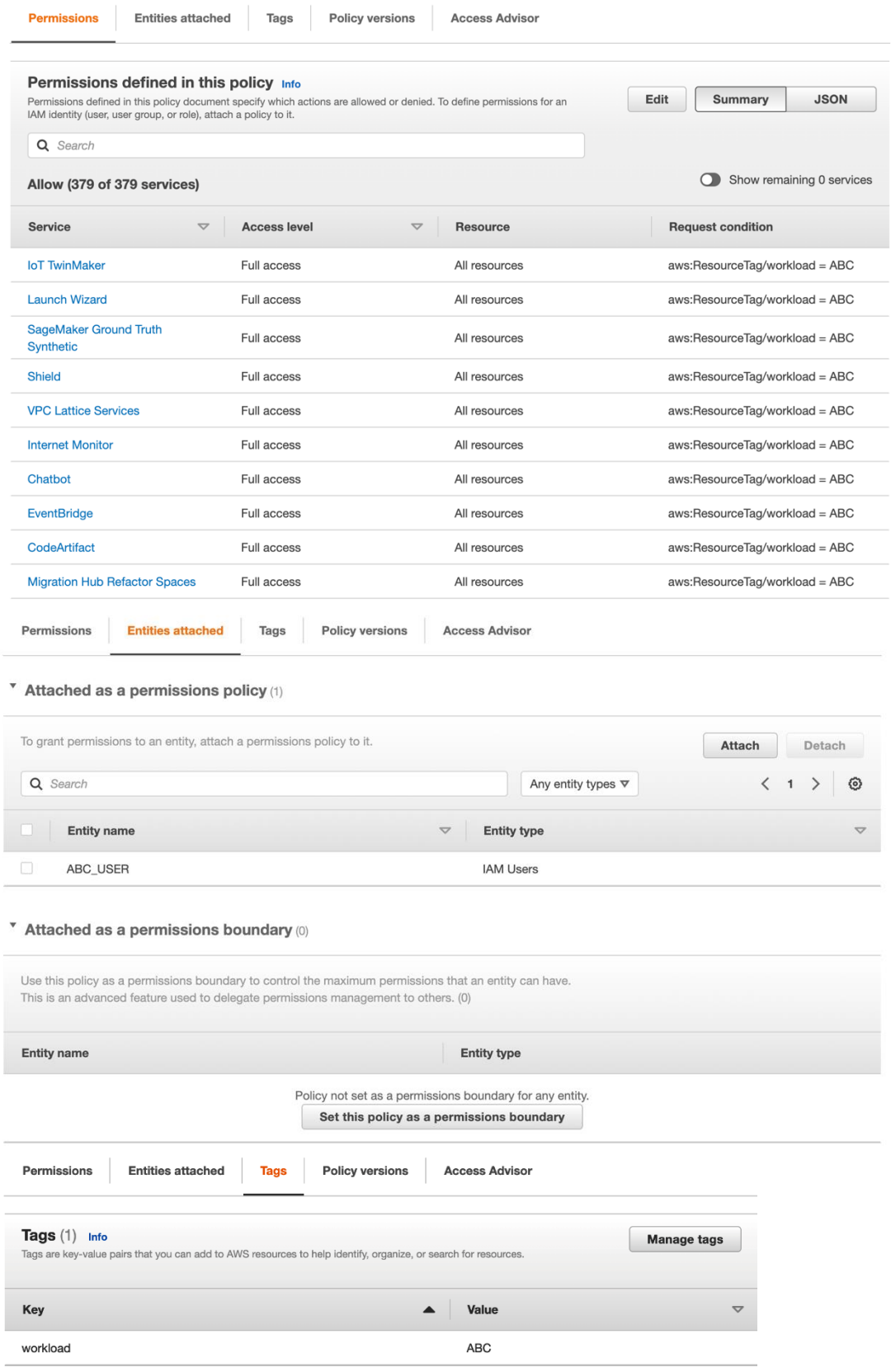
Edit | Summary | JSON

Search

Allow (379 of 379 services)

Show remaining 0 services

Service	Access level	Resource	Request condition
IoT TwinMaker	Full access	All resources	aws:ResourceTag/workload = ABC
Launch Wizard	Full access	All resources	aws:ResourceTag/workload = ABC



Permissions | Entities attached | Tags | Policy versions | Access Advisor

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Edit | Summary | JSON

Search

Allow (379 of 379 services)

Show remaining 0 services

Service	Access level	Resource	Request condition
IoT TwinMaker	Full access	All resources	aws:ResourceTag/workload = ABC
Launch Wizard	Full access	All resources	aws:ResourceTag/workload = ABC
SageMaker Ground Truth Synthetic	Full access	All resources	aws:ResourceTag/workload = ABC
Shield	Full access	All resources	aws:ResourceTag/workload = ABC
VPC Lattice Services	Full access	All resources	aws:ResourceTag/workload = ABC
Internet Monitor	Full access	All resources	aws:ResourceTag/workload = ABC
Chatbot	Full access	All resources	aws:ResourceTag/workload = ABC
EventBridge	Full access	All resources	aws:ResourceTag/workload = ABC
CodeArtifact	Full access	All resources	aws:ResourceTag/workload = ABC
Migration Hub Refactor Spaces	Full access	All resources	aws:ResourceTag/workload = ABC

Permissions | Entities attached | Tags | Policy versions | Access Advisor

Attached as a permissions policy (1)

To grant permissions to an entity, attach a permissions policy to it.

Attach | Detach

Search | Any entity types | 1

Entity name	Entity type
ABC_USER	IAM Users

Attached as a permissions boundary (0)

Use this policy as a permissions boundary to control the maximum permissions that an entity can have.
This is an advanced feature used to delegate permissions management to others. (0)

Entity name	Entity type

Policy not set as a permissions boundary for any entity.

Set this policy as a permissions boundary

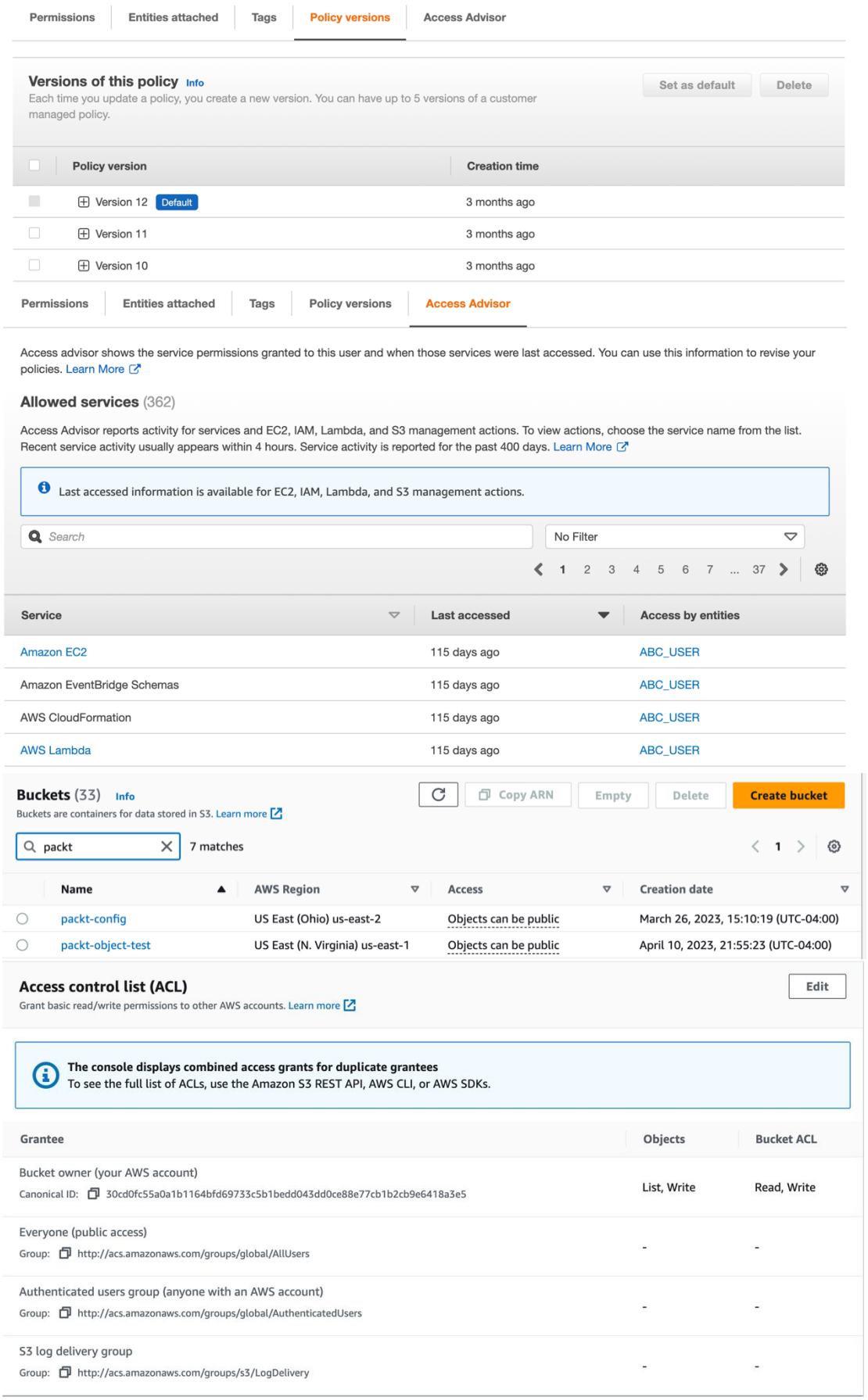
Permissions | Entities attached | Tags | Policy versions | Access Advisor

Tags (1) Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

Manage tags

Key	Value
workload	ABC


Permissions
Entities attached
Tags
Policy versions
Access Advisor
Versions of this policy Info
Each time you update a policy, you create a new version. You can have up to 5 versions of a customer managed policy.
Set as default
Delete
Policy version
Creation time
Version 12 Default
3 months ago
Version 11
3 months ago
Version 10
3 months ago
Permissions
Entities attached
Tags
Policy versions
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
Allowed services (362)
Access Advisor reports activity for services and EC2, IAM, Lambda, and S3 management actions. To view actions, choose the service name from the list. Recent service activity usually appears within 4 hours. Service activity is reported for the past 400 days. Learn More
Last accessed information is available for EC2, IAM, Lambda, and S3 management actions.
Search
No Filter
1 2 3 4 5 6 7 ... 37
Service
Last accessed
Access by entities
Amazon EC2
115 days ago
ABC_USER
Amazon EventBridge Schemas
115 days ago
ABC_USER
AWS CloudFormation
115 days ago
ABC_USER
AWS Lambda
115 days ago
ABC_USER
Buckets (33) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
packt
7 matches
1
Name
AWS Region
Access
Creation date
packt-config
US East (Ohio) us-east-2
Objects can be public
March 26, 2023, 15:10:19 (UTC-04:00)
packt-object-test
US East (N. Virginia) us-east-1
Objects can be public
April 10, 2023, 21:55:23 (UTC-04:00)
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
Edit
The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Canonical ID: 30cd0fc55a0a1b1164bfd69733c5b1bedd043dd0ce88e77cb1b2cb9e6418a3e5
List, Write
Read, Write
Everyone (public access)
Group: http://acs.amazonaws.com/groups/global/AllUsers
-
-
Authenticated users group (anyone with an AWS account)
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers
-
-
S3 log delivery group
Group: http://acs.amazonaws.com/groups/s3/LogDelivery
-
-

Access for other AWS accounts

Grantee	Objects	Bucket ACL	
Enter canonical ID	☐ List ☐ Write	☐ Read ☐ Write	Remove

Add grantee

Trusted entity type

- ○ **AWS service**
  Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ◉ **AWS account**
  Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ○ **Web identity**
  Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ○ **SAML 2.0 federation**
  Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ○ **Custom trust policy**
  Create a custom trust policy to enable others to perform actions in this account.

Permissions policies (973) Info

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

Filter by Type

S3FullAccess | All types | 1 match | 1

Policy name	Type	Description
☐ AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the…

Role details

Role name
Enter a meaningful name to identify this role.

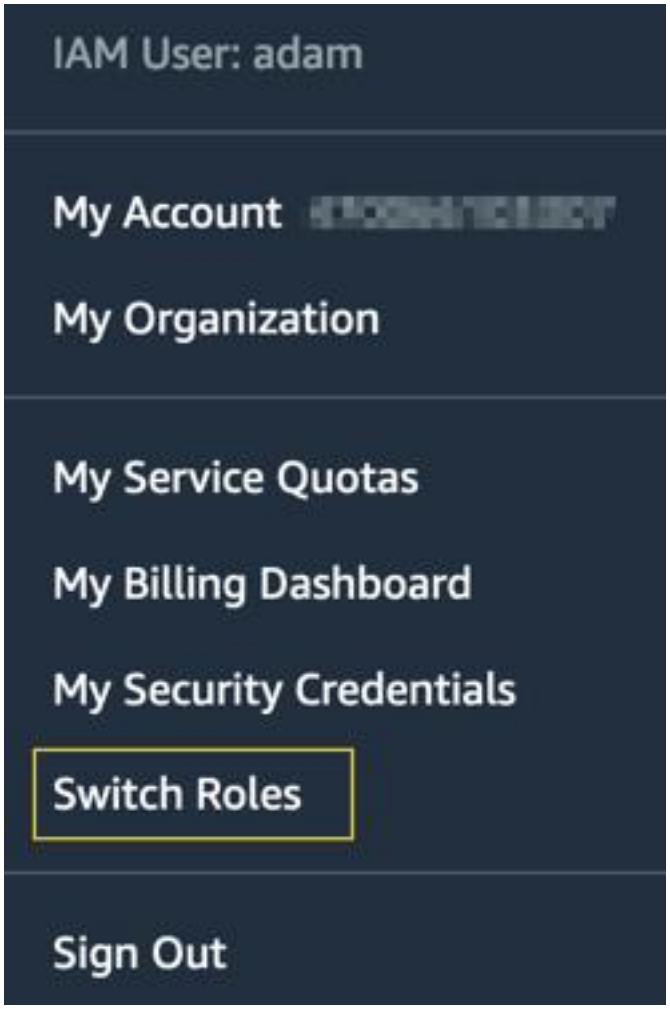
AssumeS3

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.

Allows our other account to assume full S3 access

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.



Account* 01234567980

Role* AssumeS3

Display Name AccountA_S3

Color a a a a a a

Working with Access Policies

Summary

This chapter discussed the different types of access policies used in AWS. These included SCPs, identity-based policies, resource-based policies, and permissions boundaries. You saw some of the granular constructs of creating policies, especially in the case of conditions, and how you can use those constructs to narrow down the scope of the permissions of a policy to the least-privileged access.

You also reviewed how to provide access to a secondary account using roles rather than separate accounts. Using this method can allow you to provide access to third parties who need access to your account for a specific reason and already have their own AWS accounts and IAM users. In addition to using roles, you also learned how using ACLs can enable cross-account access for different types of resources.

In *Chapter 15, Federated and Mobile Access*, you will examine what federated access is as well as how to allow access to your account from mobile devices using identity providers. You will learn how to use the AWS Cognito service and learn the differences between user pools and identity pools.

Chapter Review Questions

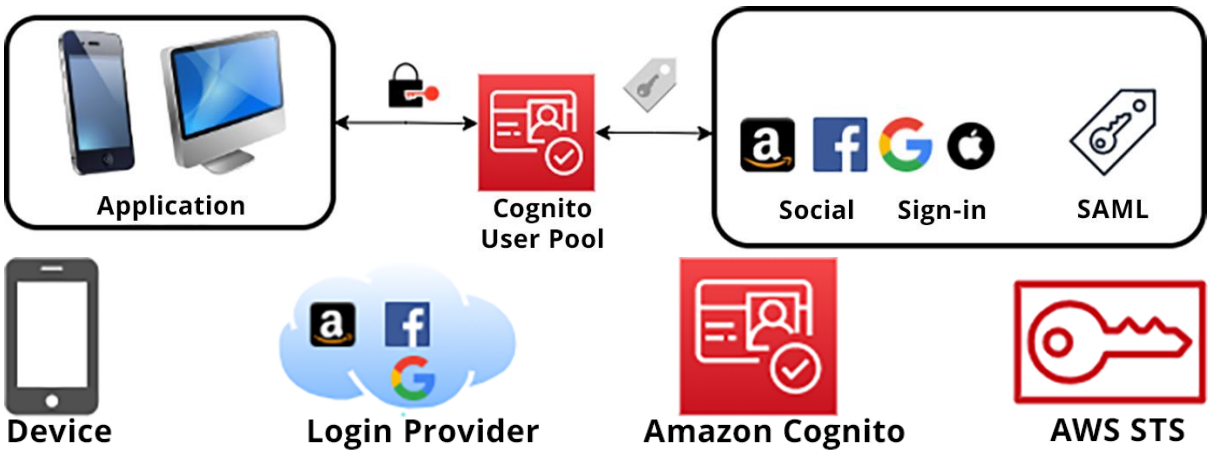
The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

Select Quiz

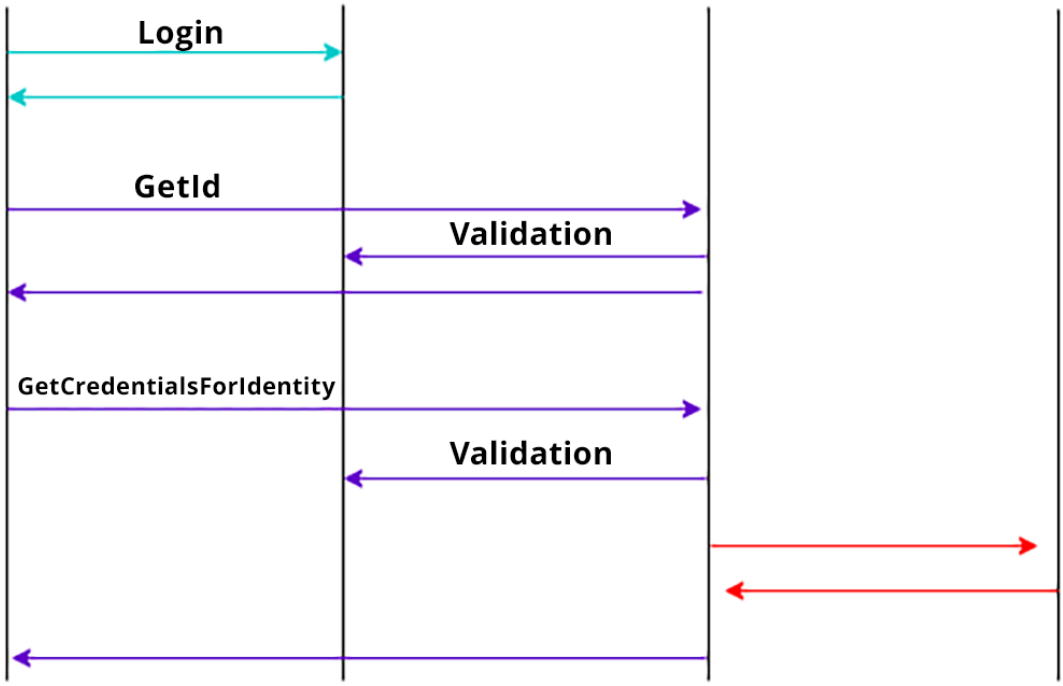
Quiz 1 START

SHOW QUIZ DETAILS

Chapter 15:


Application
Cognito
User Pool
Social
Sign-in
SAML

Device
Login Provider
Amazon Cognito
AWS STS


Login
GetId
Validation
GetCredentialsForIdentity
Validation

Practice Resources

SHARE FEEDBACK

sk

DASHBOARD > CHAPTER 15

Federated and Mobile Access

Summary

In this chapter, you looked at federated access, what it is, and when (and when not) to use it. You also learned about SAML and how it is primarily used for enterprise federations where trusted entities exchange authentication and authorization data.

Finally, as the chapter wrapped up, you reviewed the Amazon Cognito service. You read in depth about the differences between user pools and identity pools and went through the job function for each pool type. You saw how, once a user is authenticated to a user pool, they are issued a JWT. You also learned how user data is stored in the JWT for later use in the user pool.

In the next chapter, you will look extensively at AWS Directory Service and the different varieties of it available to you in AWS.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

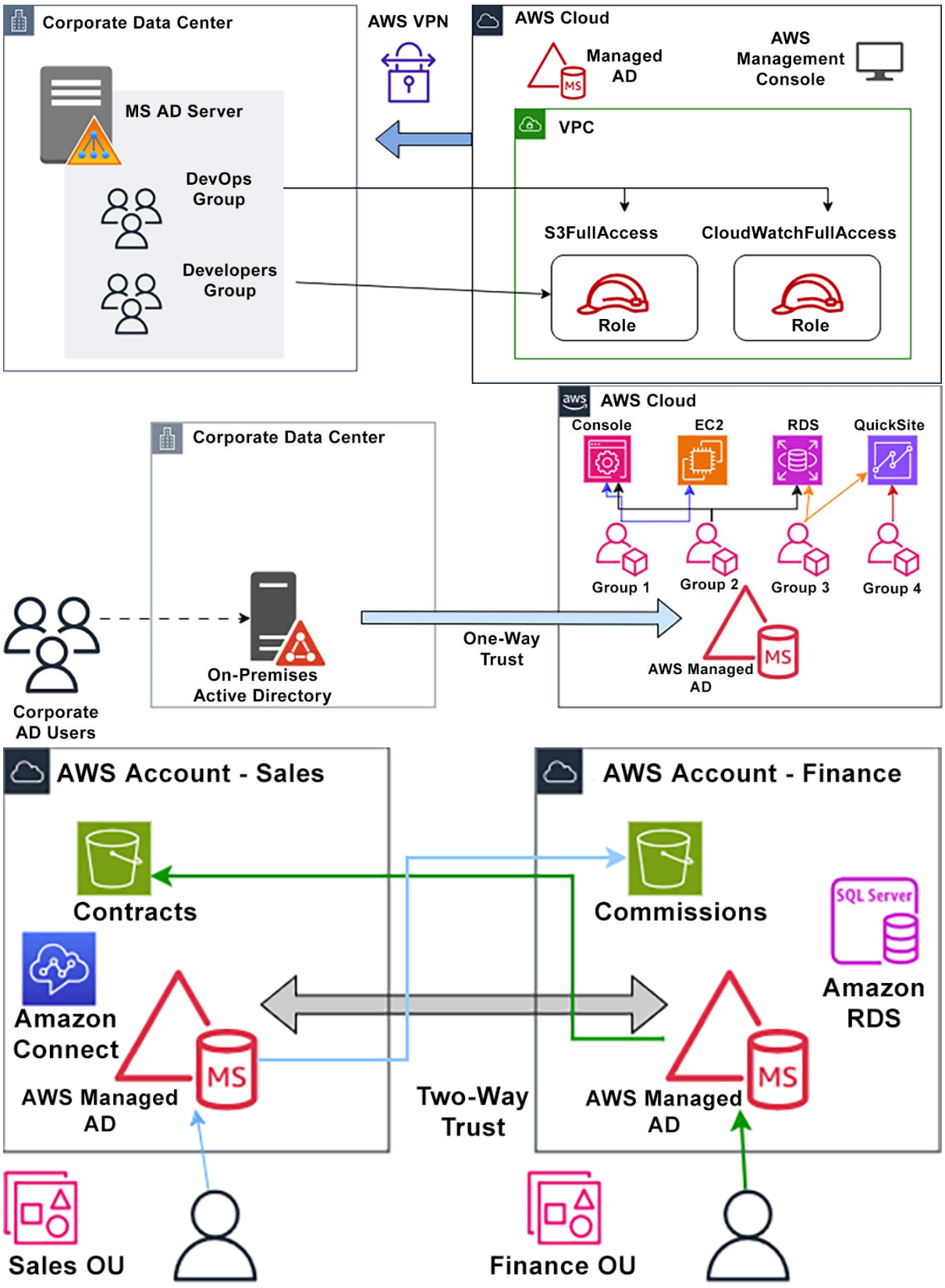
Select Quiz

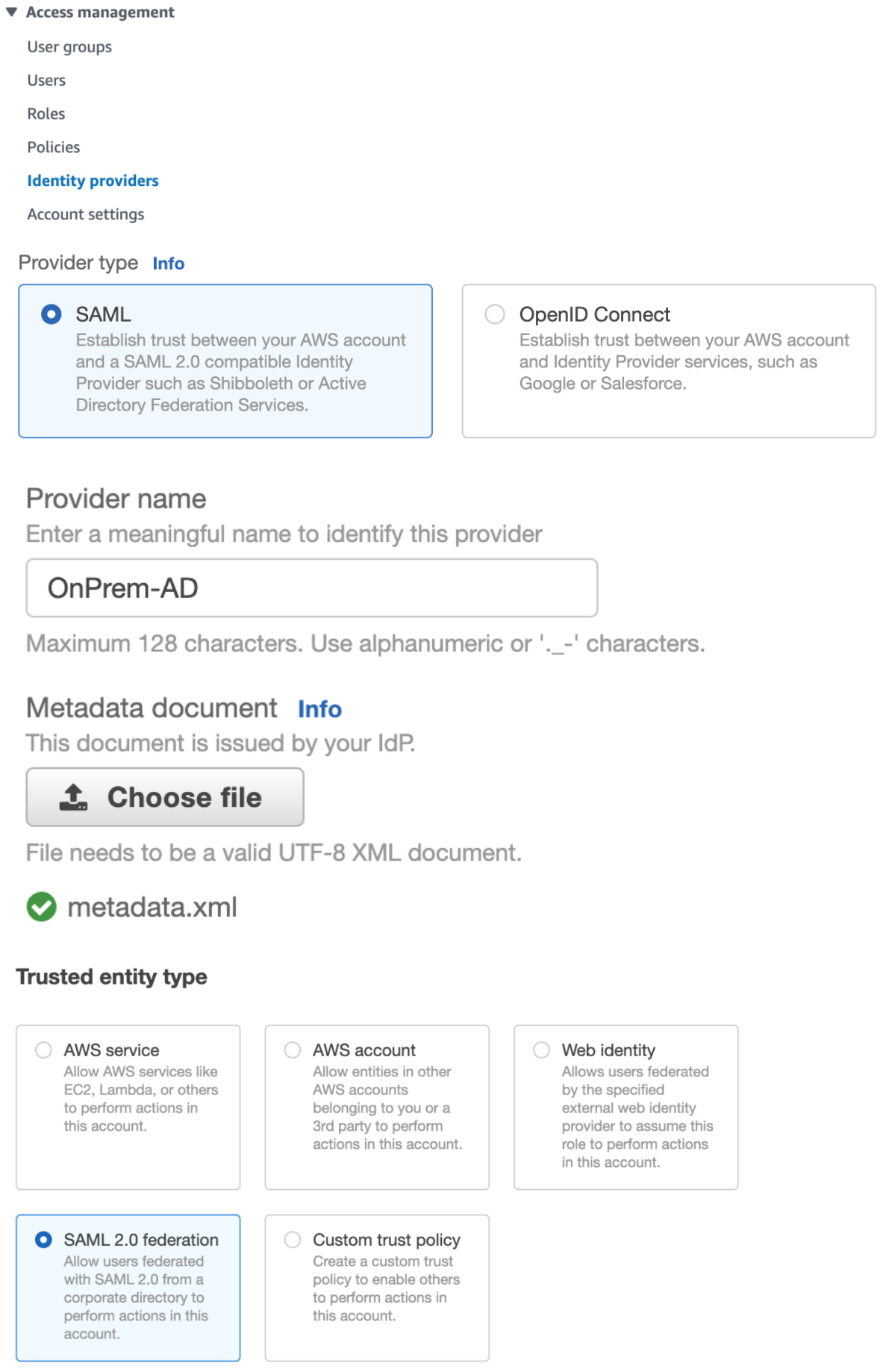
Quiz 1

SHOW QUIZ DETAILS

START

Chapter 16:


Corporate Data Center
MS AD Server
DevOps Group
Developers Group
AWS VPN
AWS Cloud
Managed AD
AWS Management Console
VPC
S3FullAccess
CloudWatchFullAccess
Role
Role
Corporate Data Center
On-Premises Active Directory
Corporate AD Users
One-Way Trust
AWS Cloud
Console
EC2
RDS
QuickSite
Group 1
Group 2
Group 3
Group 4
AWS Managed AD
AWS Account - Sales
Contracts
Amazon Connect
AWS Managed AD
Two-Way Trust
AWS Account - Finance
Commissions
SQL Server
Amazon RDS
AWS Managed AD
Sales OU
Finance OU


Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Provider type Info
SAML
Establish trust between your AWS account and a SAML 2.0 compatible Identity Provider such as Shibboleth or Active Directory Federation Services.
OpenID Connect
Establish trust between your AWS account and Identity Provider services, such as Google or Salesforce.
Provider name
Enter a meaningful name to identify this provider
OnPrem-AD
Maximum 128 characters. Use alphanumeric or '._-' characters.
Metadata document Info
This document is issued by your IdP.
Choose file
File needs to be a valid UTF-8 XML document.
metadata.xml
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 16

Using Active Directory Services to Manage Access

Summary

In this chapter, you examined the different varieties of Microsoft AD that are available in AWS. This included learning about the ways to connect your on-premises AD to AWS: Managed Microsoft AD and AD Connector. You also read about examples of both one-way trust and two-way trust. You looked at securing AD in AWS both from a practical and logistical standpoint. Finally, you also went through a detailed comparison chart of all the services that emphasized how they differ from one another.

Chapter 17 marks the beginning of the final section of this book and will address the best practices of data protection. This section begins with protecting data in flight and at rest. In this chapter, you will learn how to secure data stored in S3 buckets and EBS volumes so that any resting data is protected. You will also learn about techniques to keep your data safe while it is traveling to and from different services.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

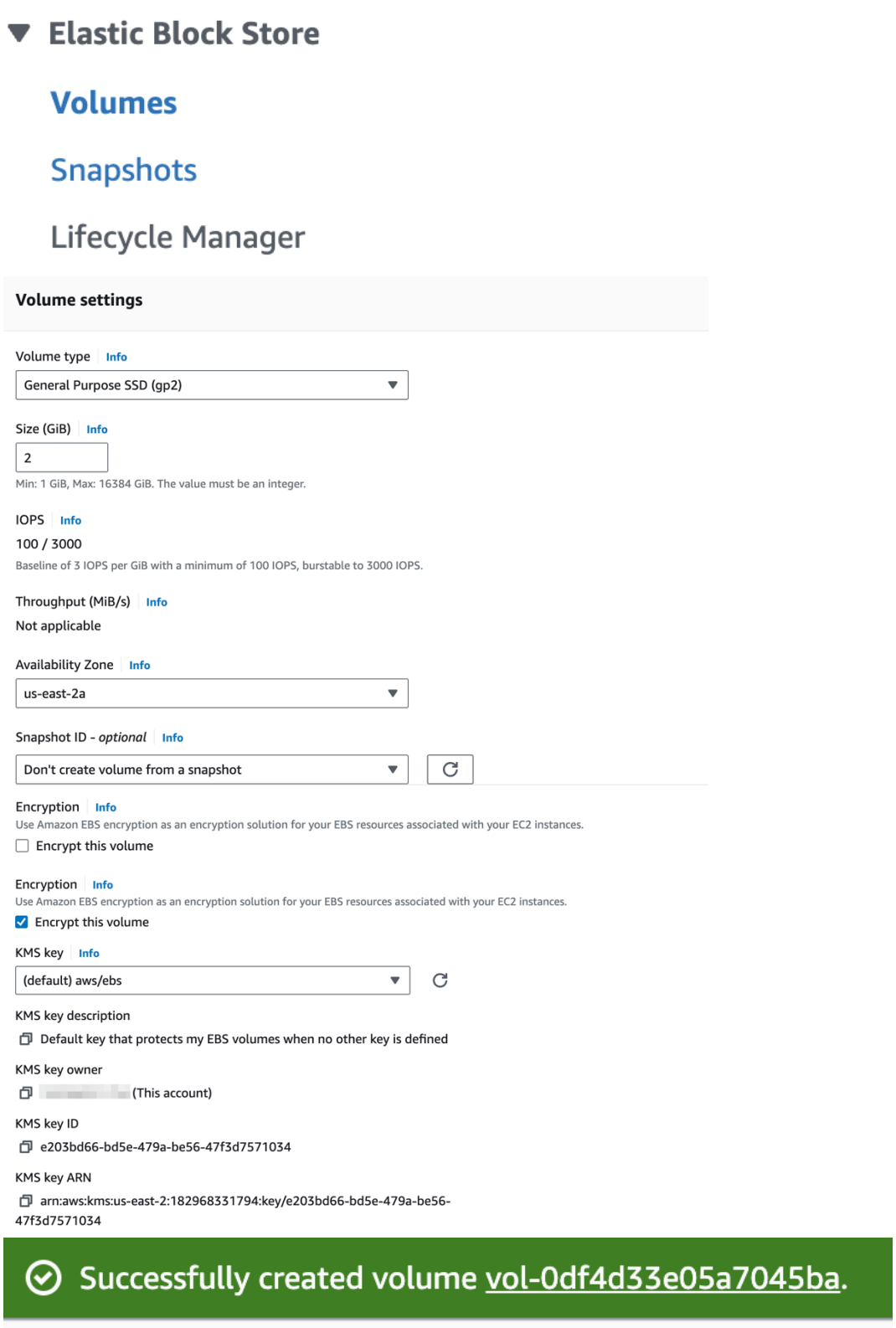
Select Quiz

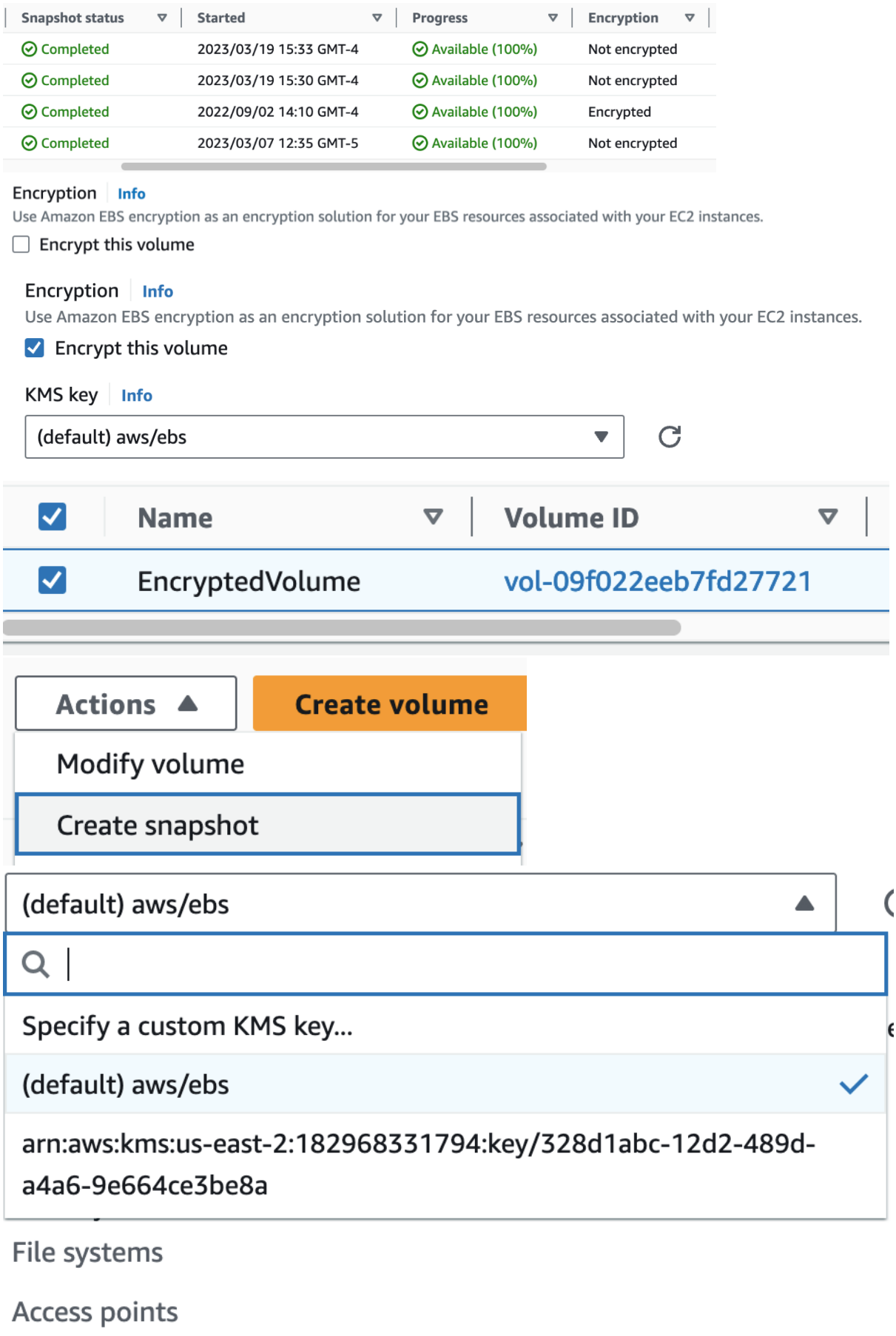
Quiz 1

SHOW QUIZ DETAILS

START

Chapter 17:


Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Volume settings
Volume type Info
General Purpose SSD (gp2)
Size (GiB) Info
2
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.
IOPS Info
100 / 3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.
Throughput (MiB/s) Info
Not applicable
Availability Zone Info
us-east-2a
Snapshot ID - optional Info
Don't create volume from a snapshot
Encryption Info
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
Encrypt this volume
Encryption Info
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
Encrypt this volume
KMS key Info
(default) aws/ebs
KMS key description
Default key that protects my EBS volumes when no other key is defined
KMS key owner
(This account)
KMS key ID
e203bd66-bd5e-479a-be56-47f3d7571034
KMS key ARN
arn:aws:kms:us-east-2:182968331794:key/e203bd66-bd5e-479a-be56-47f3d7571034
Successfully created volume vol-0df4d33e05a7045ba.


Snapshot status
Started
Progress
Encryption
Completed
2023/03/19 15:33 GMT-4
Available (100%)
Not encrypted
Completed
2023/03/19 15:30 GMT-4
Available (100%)
Not encrypted
Completed
2022/09/02 14:10 GMT-4
Available (100%)
Encrypted
Completed
2023/03/07 12:35 GMT-5
Available (100%)
Not encrypted
Encryption Info
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
Encrypt this volume
Encryption Info
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
Encrypt this volume
KMS key Info
(default) aws/ebs
Name
Volume ID
EncryptedVolume
vol-09f022eeb7fd27721
Actions
Create volume
Modify volume
Create snapshot
(default) aws/ebs
Specify a custom KMS key...
(default) aws/ebs
arn:aws:kms:us-east-2:182968331794:key/328d1abc-12d2-489d-a4a6-9e664ce3be8a
File systems
Access points

Create file system

Create an EFS file system with recommended settings, including Elastic Throughput, Lifecycle Management, and Automatic Backups. These settings are designed to optimize the price-performance of your file system. Learn more

Name - *optional*

Name your file system.

chapter_17

Name can include letters, numbers, and +-=._:/ symbols, up to 256 characters.

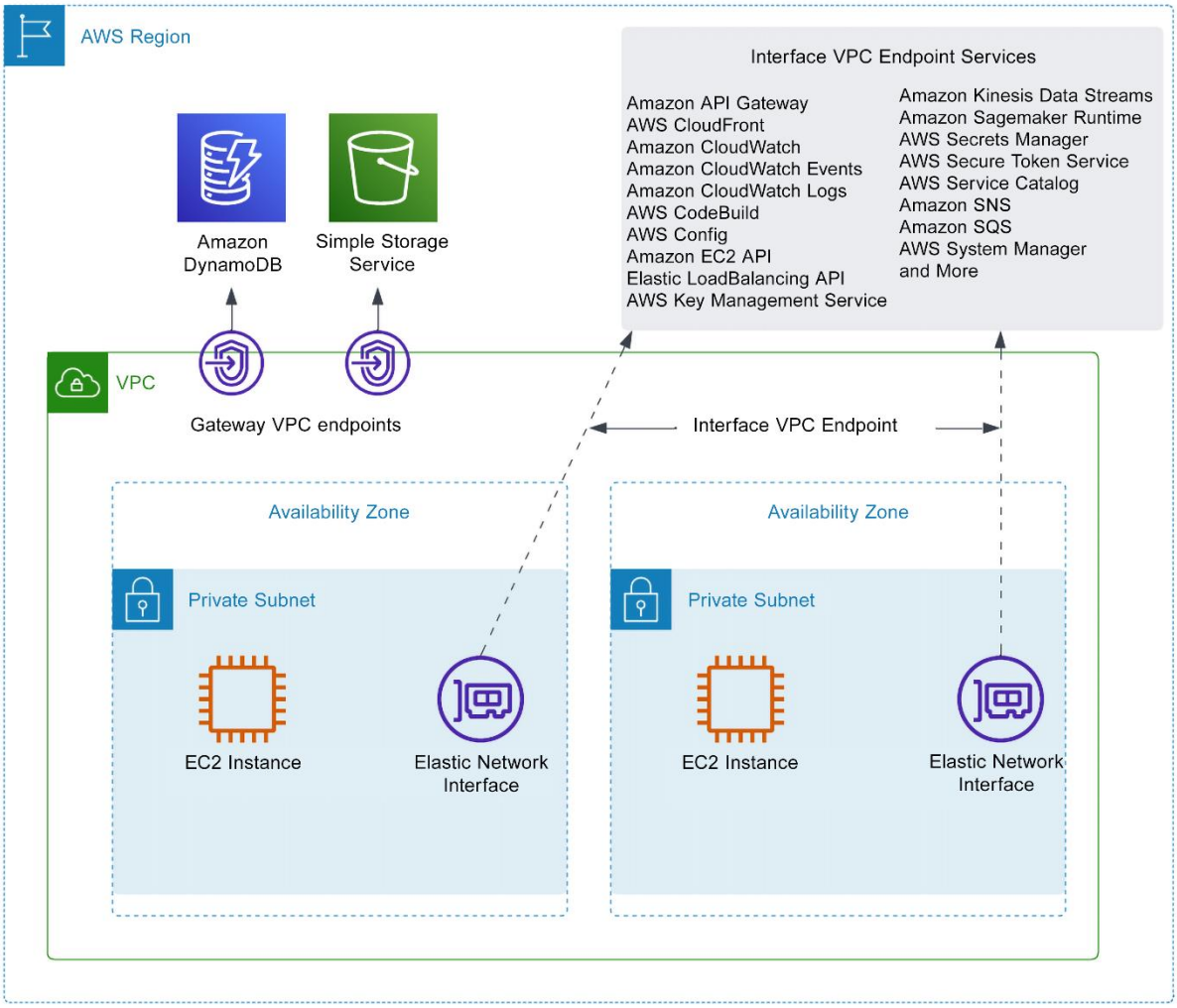
Virtual Private Cloud (VPC)

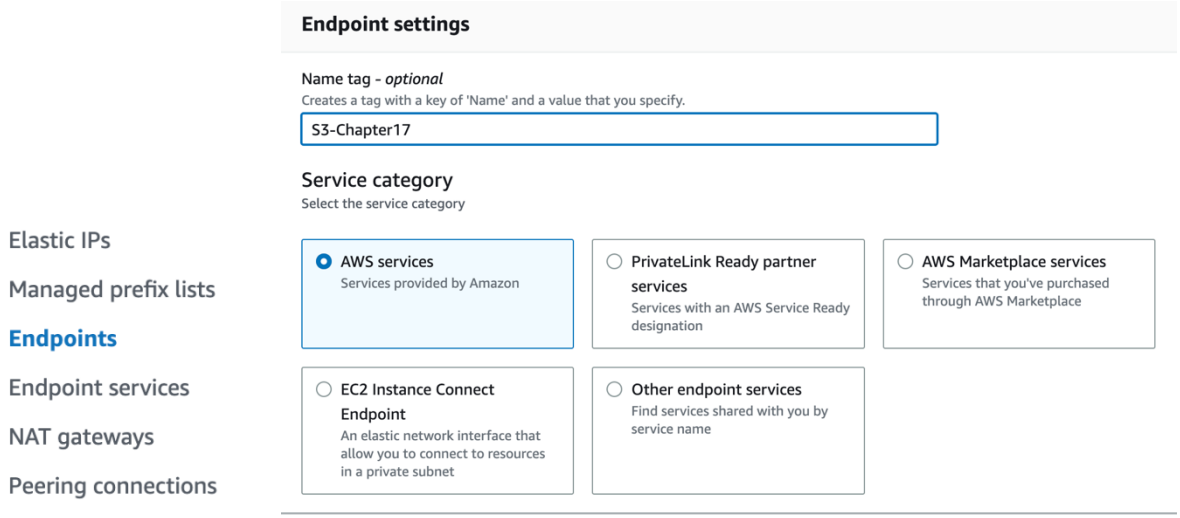
Choose the VPC where you want EC2 instances to connect to your file system.

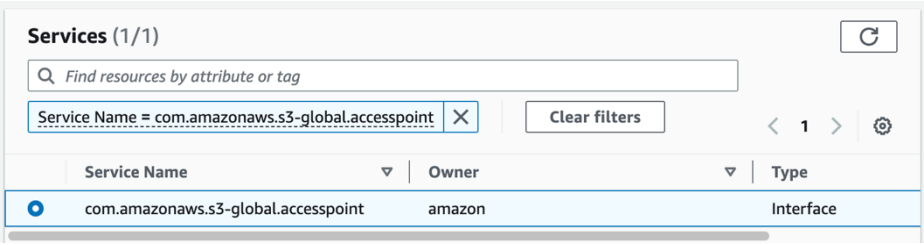
vpc-f80e0490
default

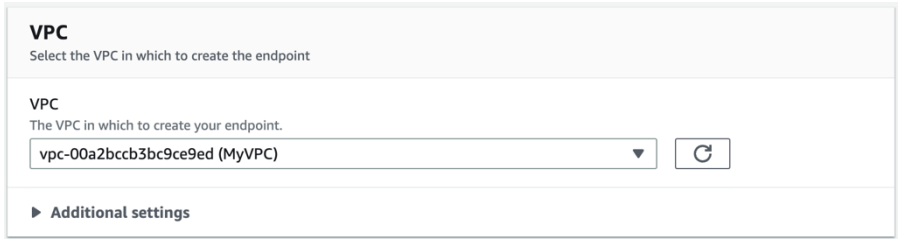
Cancel | Customize | Create

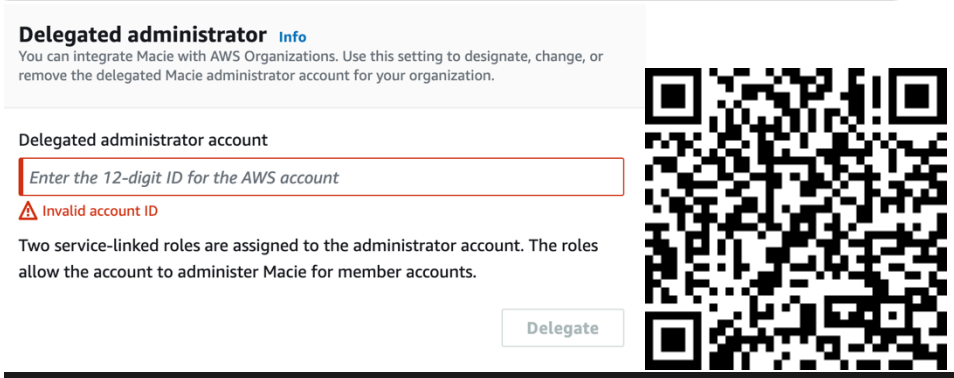
Name	File system ID	Encrypted	Total size	Size in Standard / One Zone	Size in Standard-IA / One Zone-IA	Provisioned Throughput (MiB/s)
chapter_17	fs-0d12ccadfc623895d	Encrypted	6.00 KiB	6.00 KiB	0 Bytes	-

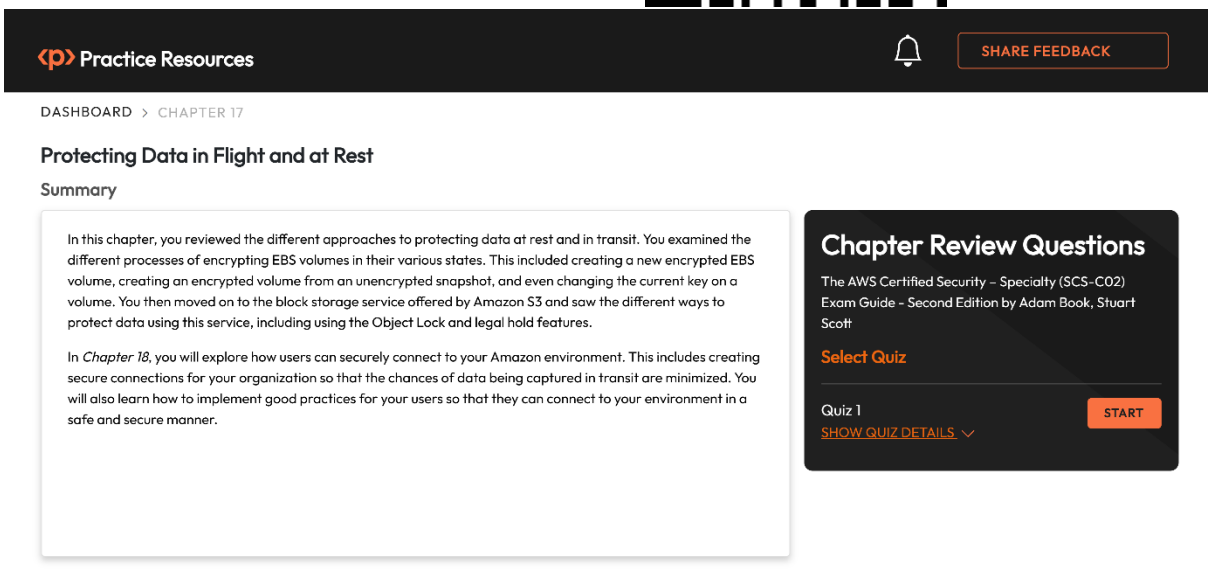

AWS Region
Interface VPC Endpoint Services
Amazon API Gateway
AWS CloudFront
Amazon CloudWatch
Amazon CloudWatch Events
Amazon CloudWatch Logs
AWS CodeBuild
AWS Config
Amazon EC2 API
Elastic LoadBalancing API
AWS Key Management Service
Amazon Kinesis Data Streams
Amazon Sagemaker Runtime
AWS Secrets Manager
AWS Secure Token Service
AWS Service Catalog
Amazon SNS
Amazon SQS
AWS System Manager
and More
Amazon DynamoDB
Simple Storage Service
VPC
Gateway VPC endpoints
Interface VPC Endpoint
Availability Zone
Availability Zone
Private Subnet
Private Subnet
EC2 Instance
Elastic Network Interface
EC2 Instance
Elastic Network Interface


Endpoint settings
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
S3-Chapter17
Service category
Select the service category
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
AWS services
Services provided by Amazon
PrivateLink Ready partner services
Services with an AWS Service Ready designation
AWS Marketplace services
Services that you've purchased through AWS Marketplace
EC2 Instance Connect Endpoint
An elastic network interface that allow you to connect to resources in a private subnet
Other endpoint services
Find services shared with you by service name

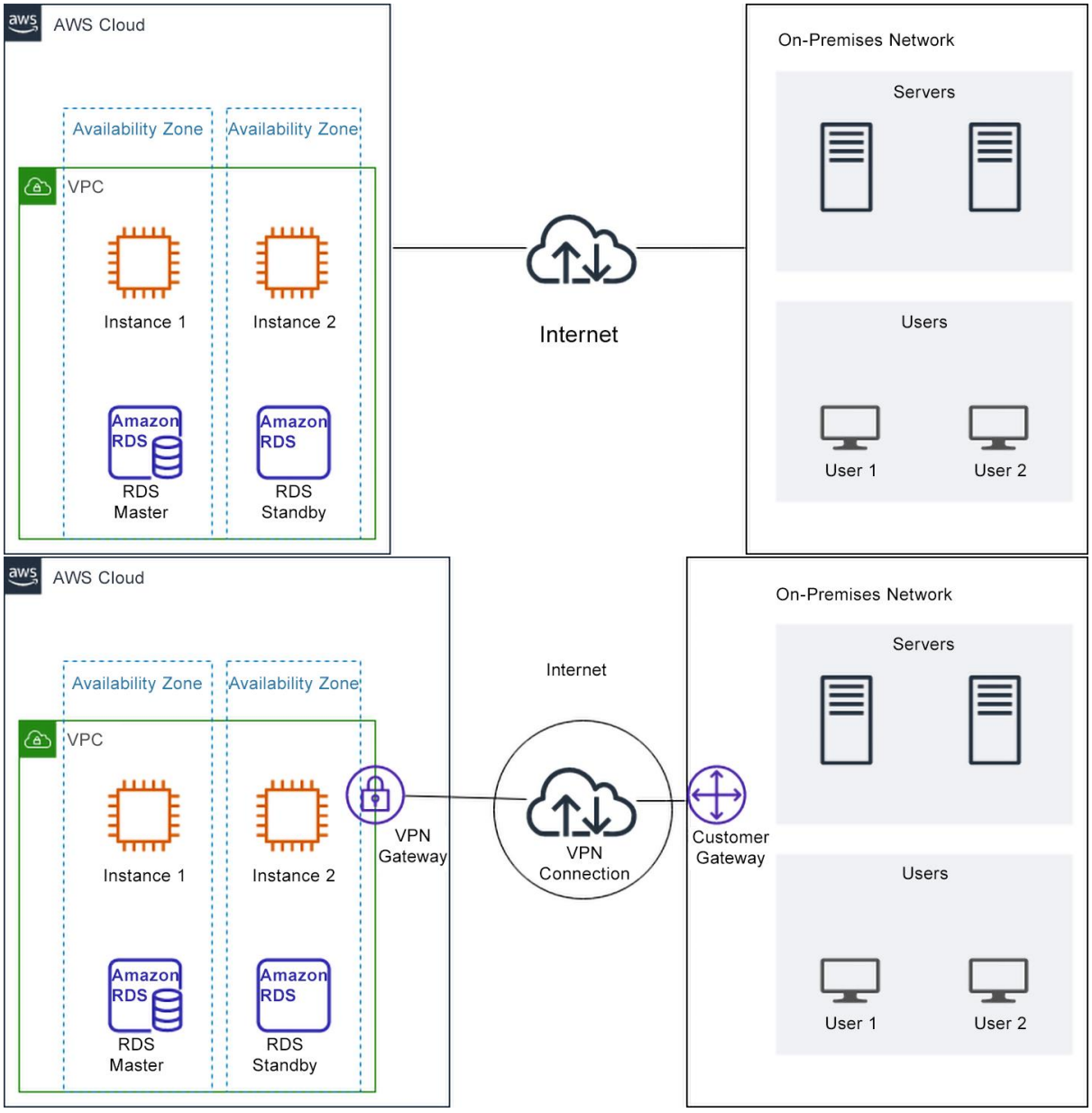

Services (1/1)
Find resources by attribute or tag
Service Name = com.amazonaws.s3-global.accesspoint
Clear filters
1
Service Name
Owner
Type
com.amazonaws.s3-global.accesspoint
amazon
Interface

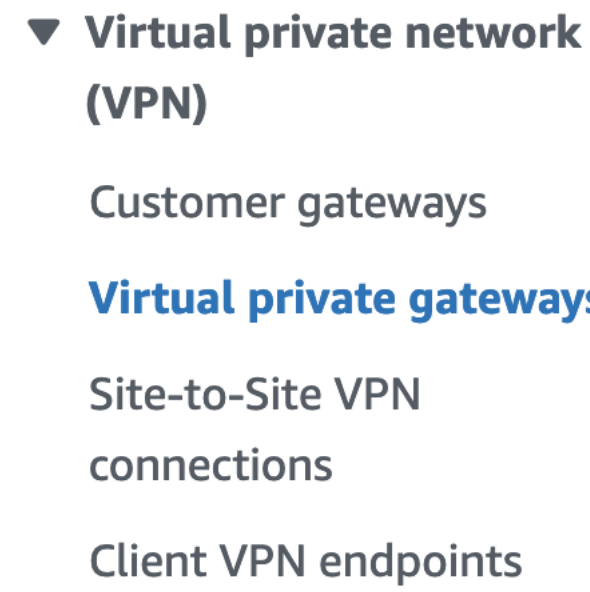

VPC
Select the VPC in which to create the endpoint
VPC
The VPC in which to create your endpoint.
vpc-00a2bccb3bc9ce9ed (MyVPC)
Additional settings


Delegated administrator Info
You can integrate Macie with AWS Organizations. Use this setting to designate, change, or remove the delegated Macie administrator account for your organization.
Delegated administrator account
Enter the 12-digit ID for the AWS account
Invalid account ID
Two service-linked roles are assigned to the administrator account. The roles allow the account to administer Macie for member accounts.
Delegate


Practice Resources
SHARE FEEDBACK
DASHBOARD > CHAPTER 17
Protecting Data in Flight and at Rest
Summary
In this chapter, you reviewed the different approaches to protecting data at rest and in transit. You examined the different processes of encrypting EBS volumes in their various states. This included creating a new encrypted EBS volume, creating an encrypted volume from an unencrypted snapshot, and even changing the current key on a volume. You then moved on to the block storage service offered by Amazon S3 and saw the different ways to protect data using this service, including using the Object Lock and legal hold features.
In Chapter 18, you will explore how users can securely connect to your Amazon environment. This includes creating secure connections for your organization so that the chances of data being captured in transit are minimized. You will also learn how to implement good practices for your users so that they can connect to your environment in a safe and secure manner.
Chapter Review Questions
The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott
Select Quiz
Quiz 1
START
SHOW QUIZ DETAILS

Chapter 18:


AWS Cloud
Availability Zone
Availability Zone
VPC
Instance 1
Instance 2
Amazon RDS
RDS Master
Amazon RDS
RDS Standby
Internet
On-Premises Network
Servers
Users
User 1
User 2
AWS Cloud
Availability Zone
Availability Zone
VPC
Instance 1
Instance 2
Amazon RDS
RDS Master
Amazon RDS
RDS Standby
VPN Gateway
Internet
VPN Connection
Customer Gateway
On-Premises Network
Servers
Users
User 1
User 2



Details

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

Chapter18-Demo-VPG

Value must be 256 characters or less in length.

Autonomous System Number (ASN)

- (●) Amazon default ASN
- ( ) Custom ASN

	Name	Virtual private gateway ID	State	Type	VPC
○	Chapter18-Demo-VPG	vgw-0acc6481d2b72265a	Detached	ipsec.1	–

○	Chapter18-Demo-VPG	vgw-0acc6481d2b72265a	Attaching	ipsec.1

Details

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

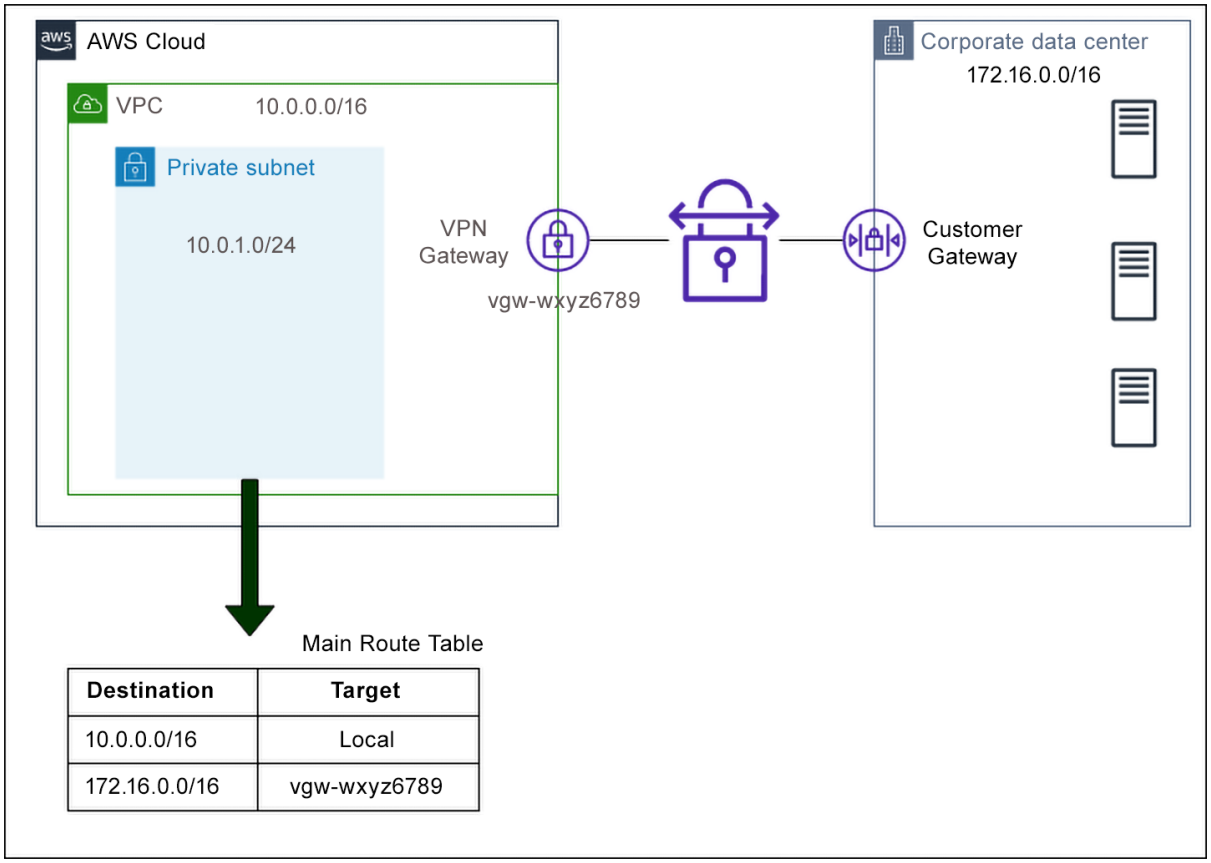
Chapter18-CustomerGateway

Value must be 256 characters or less in length.

IP address | Info

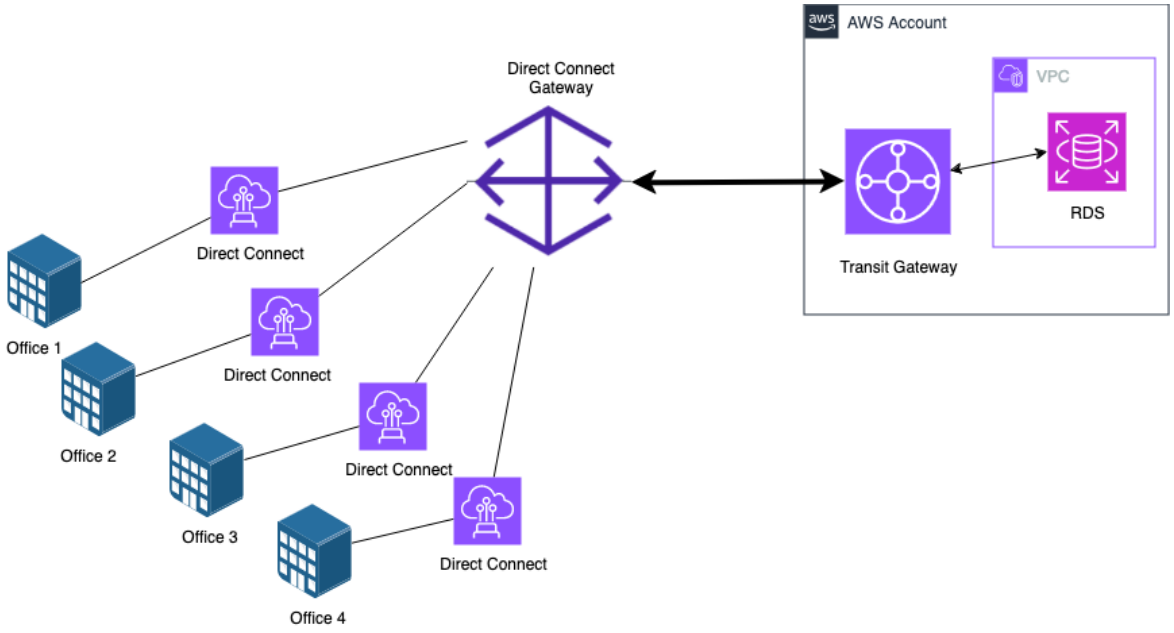
Specify the IP address for your customer gateway device's external interface.

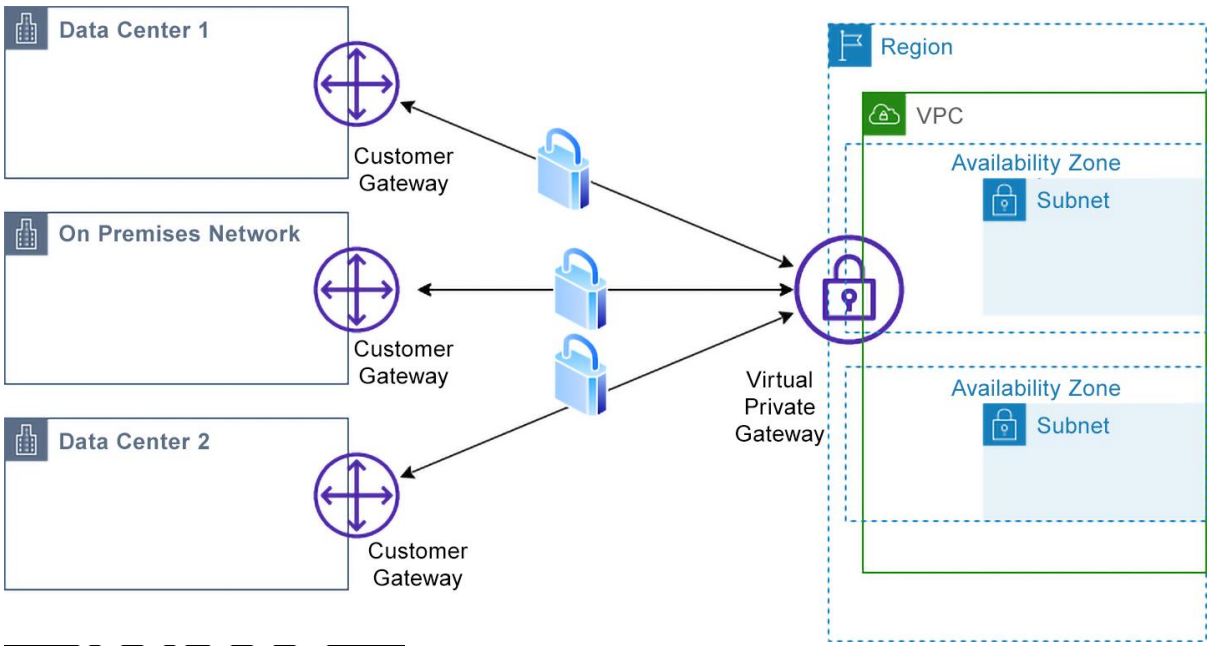
192.0.2.1



Main Route Table

Destination	Target
10.0.0.0/16	Local
172.16.0.0/16	vgw-wxyz6789





Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 18

Securely Connecting to Your AWS Environment

Summary

In this chapter, you looked at the different ways you can secure the connections you and your company make into your AWS environment. You started by reviewing the default connection from an on-premises network to AWS that is simply a connection over the internet, which is an insecure manner of operation. You were then introduced to the two main services that can help you protect your data in transit: AWS VPN and AWS Direct Connect.

In the final section of this chapter, you looked at AWS VPN CloudHub and how it can connect multiple remote sites to a VPN connection using a hub-and-spoke model, thereby simplifying your networking and security tasks for connectivity for remote offices.

In the next chapter, we will look at how to further protect data in transit by using and creating certificates using the AWS Certificate Manager service

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

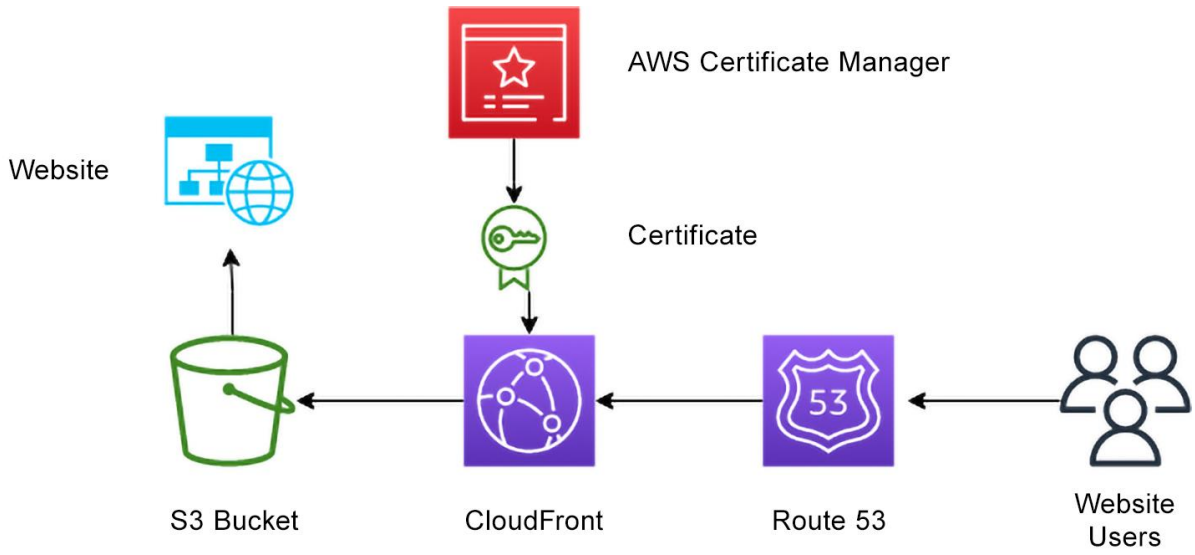
Select Quiz

Quiz 1

SHOW QUIZ DETAILS

START

Chapter 19:



Secure listener settings Info

These settings will apply to all of your secure listeners. Once created, you can manage these settings per listener.

Security policy Info

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. Compare security policies

Security category: All security policies

Policy name: ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)

Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

Certificate source

- (•) From ACM
- ( ) From IAM
- ( ) Import certificate

Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

Select a certificate

Request new ACM certificate

Certificate type Info

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

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

Domain names

Provide one or more domain names for your certificate.

Fully qualified domain name Info

*.example.com

Add another name to this certificate

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

Key algorithm Info

Select an encryption algorithm. Some algorithms may not be supported by all AWS services.

- (●) RSA 2048
  RSA is the most widely used key type.
- ( ) ECDSA P 256
  Equivalent in cryptographic strength to RSA 3072.
- ( ) ECDSA P 384
  Equivalent in cryptographic strength to RSA 7680.

Using Certificates and Certificate Services in AWS

Summary

In this chapter, you looked at using and storing public and private trust certificates via the ACM service. You examined the difference between public and private certificates and how both can be used with the ACM service. You looked at how public certificates can help secure transmissions for public-facing websites and web apps being served from other AWS services, such as S3 buckets and ELBs.

You also looked at how a private CA could be managed from the ACM service, as well as use cases where using private certificates both does and does not make sense for you and your organization.

In the next chapter, we will discuss how to make your operating environment more secure by storing confidential information such as passwords and API tokens. This can be accomplished in several ways using AWS native services that will be discussed; you will also review some walk-through examples of how to use the services.

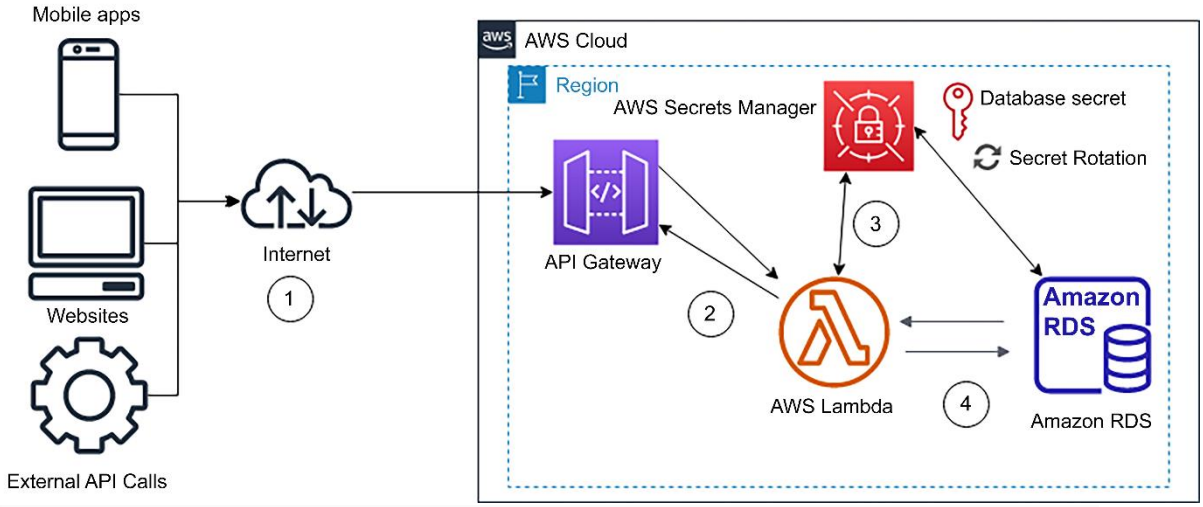
Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

Select Quiz

No exams found

Chapter 20:



Choose a database creation method Info

- ○ **Standard create**
  You set all of the configuration options, including ones for availability, security, backups, and maintenance.
- ◉ **Easy create**
  Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Secret type Info

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

Credentials Info

User name

admin

Password

grEcyvTAprziNpsRxbYYgrEcyvTAprziNpsRxbYY

☑ Show password

Database Info

Search instances

1

	DB instance	DB engine	Status	Creation date (UTC)
◉	secrets-rotation	mysql	available	September 1, 2023 …

Secret name and description Info

Secret name
A descriptive name that helps you find your secret later.

test/rds/MySQL

Secret name must contain only alphanumeric characters and the characters /_+=.@-

Description - *optional*

Access to MYSQL prod database for my AppBeta

Maximum 250 characters.

Configure automatic rotation Info

Configure AWS Secrets Manager to rotate this secret automatically.

Automatic rotation

Rotation schedule Info

Schedule expression builder | Schedule expression

Schedule expression

rate(30 days)

Enter a cron expression such as cron(a b c d e f) or a rate expression such as rate(10 days).

Window duration - *optional*

4h

Enter the time in hours.

Rotate immediately when the secret is stored. The next rotation will begin on your schedule.

Rotation function Info

Create a rotation function

Use a rotation function from your account

Lambda rotation function

Secrets Manager adds the prefix 'SecretsManager' to your function name.

SecretsManager chapter20-mysql-rotation

Function name is required. Rotation function name including prefix must be maximum 64 alphanumeric characters, hyphens, and underscores.

Use separate credentials to rotate this secret Info

No

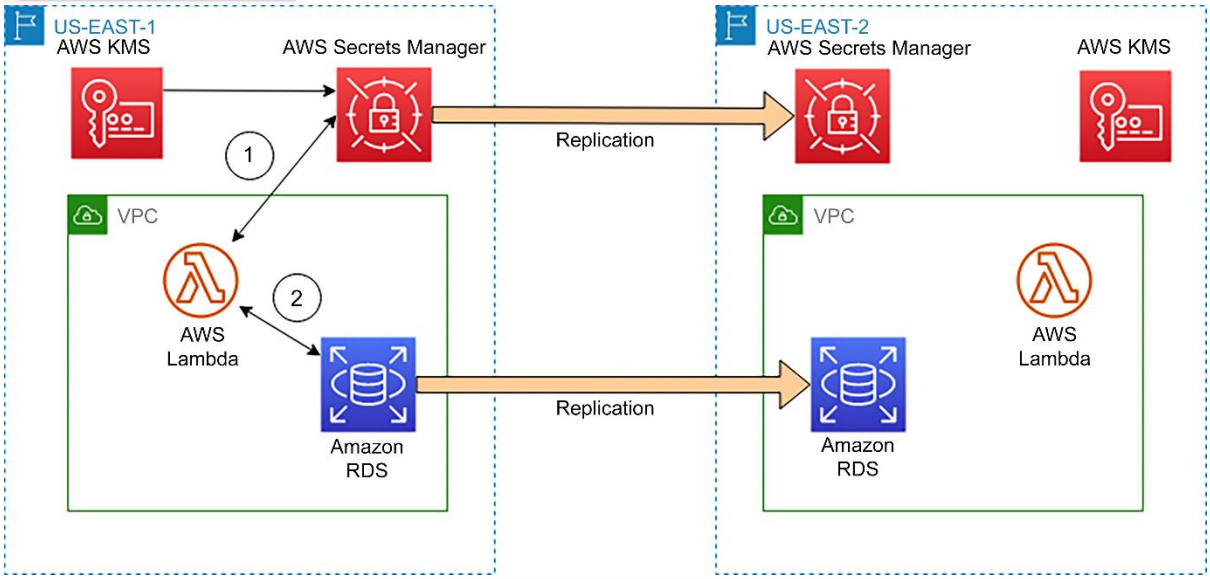
Do not use separate credentials.

Yes

Choose a secret that can update the credentials in this secret.

Secret name

test/rds/MySQL



Application Management

Application Manager

AppConfig

Parameter Store

Parameter details

Name

ps-mysql-pass

Tier

Parameter Store offers standard and advanced parameters.

Standard

Limit of 10,000 parameters. Parameter value size up to 4 KB. Parameter policies are not available. No additional charge.

Advanced

Can create more than 10,000 parameters. Parameter value size up to 8 KB. Parameter policies are available. Charges apply

Type

- String
  Any string value.
- StringList
  Separate strings using commas.
- SecureString
  Encrypt sensitive data using KMS keys from your account or another account.

KMS key source

- My current account
  Use the default KMS key for this account or specify a customer-managed key for this account. Learn more
- Another account
  Use a KMS key from another account Learn more

KMS Key ID

alias/aws/ssm

Name
ps-mysql-pass

Tier
Standard

Type
SecureString

Last modified date
Mon, 11 Sep 2023 20:05:54 GMT

Value
****
Show

Managing Secrets Securely in AWS

Summary

In this chapter, you examined how to use the native services of AWS Secrets Manager and Systems Manager Parameter Store to store secret material, such as passwords and API keys, securely. You gained insights into why centralized secrets management is a critical part of a strong security strategy, both from a risk perspective and from the ability to audit the use of the secrets.

You learned how to store the secrets using different native AWS services, including AWS Secrets Manager and Systems Manager Parameter Store, and how to retrieve those secrets once they had been stored in the respective service(s).

This chapter marks the end of this comprehensive guide on the AWS Certified Security Specialty exam. This book covered all six domains of the exam, starting with the fundamentals of the AWS Shared Responsibility Model. You learned about what you are responsible for securing and what AWS is responsible for securing. You also reviewed the fundamental services that AWS provides and how attacks can happen once your organization moves its workloads and data to a cloud environment.

Incident response was discussed in the context of how to deal with incidents in AWS. You were introduced to the tools that help remediate the compliance and security posture of your account in AWS Config, GuardDuty, and Security Hub, respectively.

You then dove into logging and monitoring, exploring the kinds of logs generated by different AWS services. After that, you explored the main service used to capture log events, CloudWatch, and looked at how logs and metrics are used in the service. But what good are logs if you can't find the information you are looking for? The section on logging concluded by showing you how to search and parse your logs for information relevant to your needs at that moment.

Securing accounts is something that each AWS security specialist needs a solid understanding of, which is what you learned about in the *Infrastructure Security* section. You examined security techniques from both an account and infrastructure level. You also learned about managing key infrastructure.

Securing your AWS accounts is about not only the infrastructure but also managing permissions, which involves giving your users only the permissions that they need to perform their job duties. You explored this in the *Identity and Access Management* section. You examined IAM policies and how they were constructed, **Service Control Policies** (**SCPs**) and how they provide guardrails around your accounts, and even how to allow outside users measured access to your accounts by using federation.

In the final section, you learned about data protection, learning how to connect to your AWS environment in a secure fashion, along with learning about secure certificates and the AWS Certificate Manager service so that you can generate your own certificates.

Chapter Review Questions

The AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition by Adam Book, Stuart Scott

Select Quiz

Chapter 20 START

SHOW QUIZ DETAILS

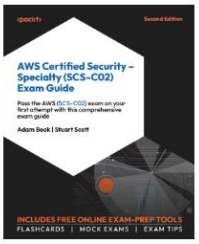
Chapter 21:

Practice Resources

REPORT ISSUE

UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.



AWS Certified Security – Specialty (SCS-C02) Exam Guide

Book ISBN: 9781837633982

Adam Book • Stuart Scott • Mar 2024 • pages

Do you have a Packt account?

◯ Yes, I have an existing Packt account ◯ No, I don't have a Packt account

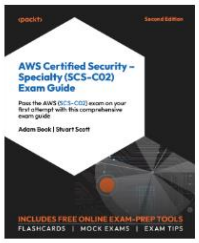
PROCEED

Practice Resources

REPORT ISSUE

UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.



AWS Certified Security – Specialty (SCS-C02) Exam Guide

Book ISBN: 9781837633982

Adam Book • Stuart Scott • Mar 2024 • pages

ENTER YOUR PURCHASE DETAILS

Enter Unique Code *

E.g 123456789 ⓘ Where To Find This?

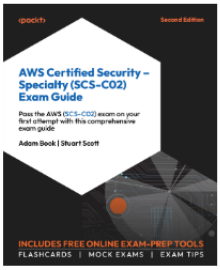
☐ Check this box to receive emails from us about new features and promotions on our other certification books. You can opt out anytime.

REQUEST ACCESS

Practice Resources REPORT ISSUE

PACKT PRACTICE RESOURCES

You've just unlocked the free online content that came with your book.



AWS Certified Security – Specialty (SCS-C02) Exam Guide

Book ISBN: 9781837633982

Adam Book • Stuart Scott • Mar 2024 • pages

Unlock Successful

Click the following link to access your practice resources at any time.

Pro Tip: You can switch seamlessly between the ebook version of the book and the practice resources. You'll find the ebook version of this title in your Owned Content

OPEN PRACTICE RESOURCES

Practice Resources SHARE FEEDBACK

DASHBOARD

AWS Certified Security – Specialty (SCS-C02) Exam Guide

Get all the guidance you need to pass the AWS (SCS-C02) exam on your first attempt

- Mock Exams
- Hands-On Activities
- Chapter Review Questions
- Flashcards
- Exam Tips

BACK TO THE BOOK

AWS Certified Security – Specialty (SCS-C02) Exam Guide - Second Edition

Adam Book, Stuart Scott