



AWS Certified Security - Specialty Crash Course

Welcome!



AWS Certified Security - Specialty Crash Course

Exam Details

How Important Is Security?

“It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it.”

-Stephane Nappo

Exam Logistics - By the Numbers

Number of questions:	65
Time for exam	170 minutes
Answer choices	4-6
Score required	750/1000
Number of unscored questions	?
Penalty for guessing	0

Exam Strategy - 3 Passes

First Pass: Low hanging fruit

Second Pass: Longer question text

Third Pass: Guesses

Question Domains

12% Incident Response

20% Logging and Monitoring

26% Infrastructure Security

20% Identity and Access Management

22% Data Protection

Question Domains

12% Incident Response

20% Logging and Monitoring

26% Infrastructure Security

20% Identity and Access Management

22% Data Protection

Concentrate
study **HERE**



What IS Covered

1. Question domains
2. Sample questions
3. Answer strategies
4. Key terms and buzzwords
5. Options for security services and features

Strategies for achieving certification are IN scope

What is NOT Covered

1. Introduction to AWS
2. Common service basics
3. Architecture strategies
4. Operational details

Learning how to be a security professional in
AWS is NOT in scope



AWS Certified Security - Specialty Crash Course

Certification Candidate Skills

Successful Candidate Skills

An understanding of specialized data classifications and AWS data protection mechanisms.

Know how to differentiate between public and differing degrees of private information

Successful Candidate Skills

An understanding of data encryption methods
and AWS mechanisms to implement them

Requires knowledge of data encryption at rest

Successful Candidate Skills

An understanding of secure Internet protocols and AWS mechanisms to implement them

Requires knowledge of data encryption in-transit

Successful Candidate Skills

A working knowledge of how to implement AWS security services and features to provide a secure production environment

*The key word is **working**. Reading documentation isn't enough. You need to DO it!*

Successful Candidate Skills

Competency gained from two or more years of production deployment experience using AWS security services and features

There is no substitute for hands-on experience!

Successful Candidate Skills

Ability to make trade-off decisions with regard to cost, security, and deployment complexity given a set of application requirements

Requires understanding of AWS architecture principles

Successful Candidate Skills

An understanding of security operations
and risk

*Requires understanding of AWS SysOps
principles and when to recognize when
you're “secure enough”*

Themes

Prevention

The act of stopping something from happening or arising

Recognition

Acknowledgement of something's existence

Mitigation

The act of reducing the severity, seriousness, or painfulness of something



AWS Certified Security - Specialty Crash Course

Incident Response
12%

Question Domain Main Points

1. Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys
2. Verify that the Incident Response plan includes relevant AWS services
3. Evaluate the configuration of automated alerting and execute possible remediation of security-related incidents and emerging issues

Abuse Notice Strategies

- Evaluate the suspected compromised instance
 - GuardDuty
 - VPC Flow logs
 - VPC Traffic Mirroring
 - Isolate from network
 - Launch replacement from AMI
- Evaluate exposed access keys
 - Access Advisor
 - GuardDuty
 - CloudTrail logs
 - Disable keys, create replacements

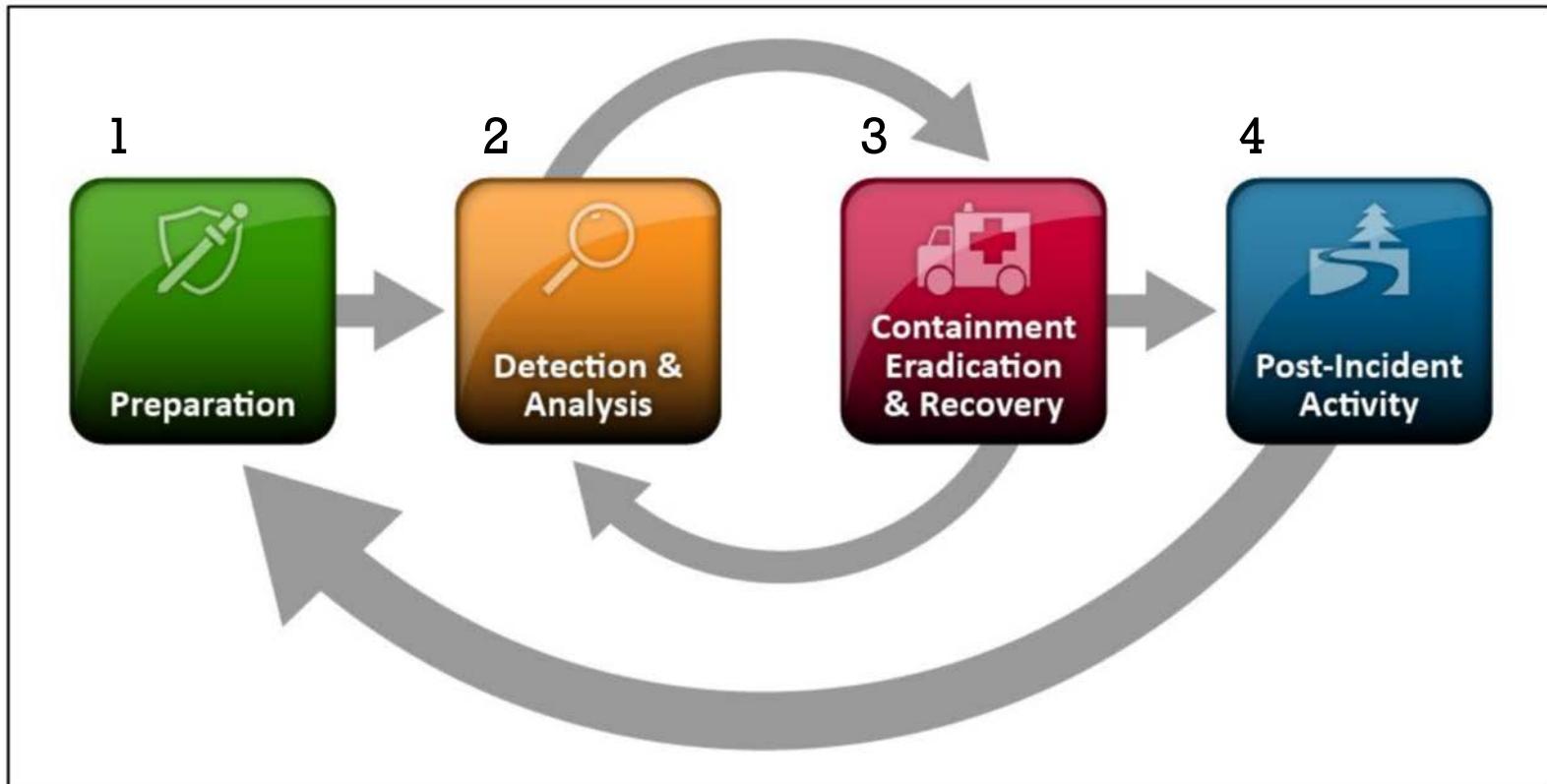
Incident Response Plan

Let's use an official source!

<https://www.nist.gov>

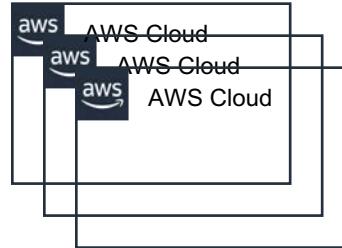
Computer Security Incident Handling Guide

Incident Response Life Cycle

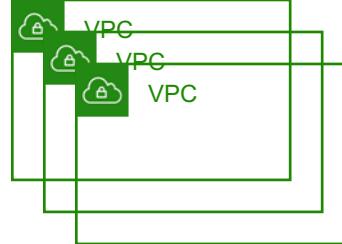


1. Limit the Blast Radius

AWS Organizations



AWS VPC



1. Self-Documenting Infrastructure



AWS Config



AWS CloudFormation



AWS SSM

1. Procedures and Run Books

Separate AWS account?



Highly available

Soft copies in offline storage?

1. Normal Behavior Baseline



AWS CloudWatch



AWS GuardDuty

1. Clean Images for Restoration and Recovery

EC2 AMI



EBS Snapshots



Backups stored in S3



Configuration files in S3



Licenses, keys in SSM Parameter Store



1. Risk Assessment



Amazon Inspector



AWS GuardDuty



Amazon Macie

1. Network Security

VPC NACL



VPC SG



VPC Flow Logs



AWS WAF



1. Store Relevant Event Information

CloudWatch Logs



AWS Config streams



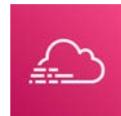
CloudWatch Events



Access logs stored in S3



CloudTrail Logs



2. Recognizing Signs of an Intrusion Attempt

CloudWatch



CloudTrail



GuardDuty



VPC Flow Logs



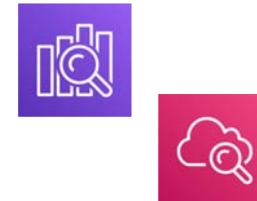
2. Incident Analysis

- Visualize performance baseline
 - CloudWatch Metrics
 - SSM Dashboards
- Understand normal behavior
 - GuardDuty Dashboard
 - Macie Dashboard
 - CloudTrail Insights



2. Incident Analysis

- Implement log retention policy
 - CloudWatch Logs expiration
 - S3 Lifecycle policies
 - Glacier Vault lock policy
- Correlate events between logs and metrics
 - Amazon ElasticSearch & Kibana
 - CloudWatch Logs Insights



2. Incident Notification

SNS



SES



Trusted Advisor



2. Use All Help Resources

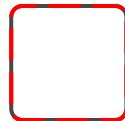
Open a support case

Search the AWS forums

Great justification for premium support!

3. Containment Strategy

Security Group rules



Revoke IAM sessions



WAF ACL rules



IAM policies



Access Key rotation



KMS CMK rotation



3. Evidence Gathering and Handling

CloudTrail



CloudWatch Logs



VPC Flow Logs



IAM Access Advisor



3. Identify the Attacking Entity



DNS lookup



GuardDuty findings

3. Eradication of Potentially Compromised Resources

EC2 Instance termination

Disable compromised keys

Segregate compromised data for analysis

3. Recovery Steps

Know your RTO/RPO

Repaired resources

Replaced resources

Can you automate?

3. Cleanup

Remove temporary resources



KMS key audit



Full IAM audit

Review further findings

4. Lessons Learned

- Evidence retention
 - S3
 - Glacier
 - AMI
 - Snapshots
- Proposals for improvement
 - Back to step 1





AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

Your security team has been informed that one of your IAM username/password pairs has been published to social media and has been used several times by unauthorized sources. How can the security team stop the unauthorized access, and determine what actions were taken with the compromised account, with minimal impact on existing account resources?

- A. Immediately change the IAM user password, ask the user what actions they normally take, then compare with current AWS inventory
- B. Delete the IAM user account, remove all resources created by the user, and analyze CloudTrail logs for unauthorized actions
- C. Immediately change the IAM user password, and remove all resources created by the user
- D. Immediately change the IAM user password, and analyze CloudTrail logs for unauthorized actions

Question Breakdown - Answers

Stops the usage of the IAM account, but doesn't really address actions taken with the compromised credentials

- A. Immediately change the IAM user password, ask the user what actions they normally take, then compare with current AWS inventory
- B. Delete the IAM user account, remove all resources created by the user, and analyze CloudTrail logs for unauthorized actions
- C. Immediately change the IAM user password, and remove all resources created by the user
- D. Immediately change the IAM user password, and analyze CloudTrail logs for unauthorized actions

Question Breakdown - Answers

Stops the usage of the IAM account, analyzes unauthorized usage, but impacts existing resources

- A. Immediately change the IAM user password, ask the user what actions they normally take, then compare with current AWS inventory
- B. Delete the IAM user account, remove all resources created by the user, and analyze CloudTrail logs for unauthorized actions
- C. Immediately change the IAM user password, and remove all resources created by the user
- D. Immediately change the IAM user password, and analyze CloudTrail logs for unauthorized actions

Question Breakdown - Answers

Stops the usage of the IAM account, but impacts existing resources

- A. Immediately change the IAM user password, ask the user what actions they normally take, then compare with current AWS inventory
- B. Delete the IAM user account, remove all resources created by the user, and analyze CloudTrail logs for unauthorized actions
- C. Immediately change the IAM user password, and remove all resources created by the user
- D. Immediately change the IAM user password, and analyze CloudTrail logs for unauthorized actions

Question Breakdown - Answers

Stops the usage of the IAM account, and analyzes unauthorized usage, without impacting existing resources

- A. Immediately change the IAM user password, ask the user what actions they normally take, then compare with current AWS inventory
- B. Delete the IAM user account, remove all resources created by the user, and analyze CloudTrail logs for unauthorized actions
- C. Immediately change the IAM user password, and remove all resources created by the user
- D. Immediately change the IAM user password, and analyze CloudTrail logs for unauthorized actions

Question Breakdown - Correct Answer

Correct Answer: D

- A. Immediately change the IAM user password, ask the user what actions they normally take, then compare with current AWS inventory
- B. Delete the IAM user account, remove all resources created by the user, and analyze CloudTrail logs for unauthorized actions
- C. Immediately change the IAM user password, and remove all resources created by the user
- D. Immediately change the IAM user password, and analyze CloudTrail logs for unauthorized actions



AWS Certified Security - Specialty Crash Course

Logging and Monitoring
20%

Question Domain Main Points

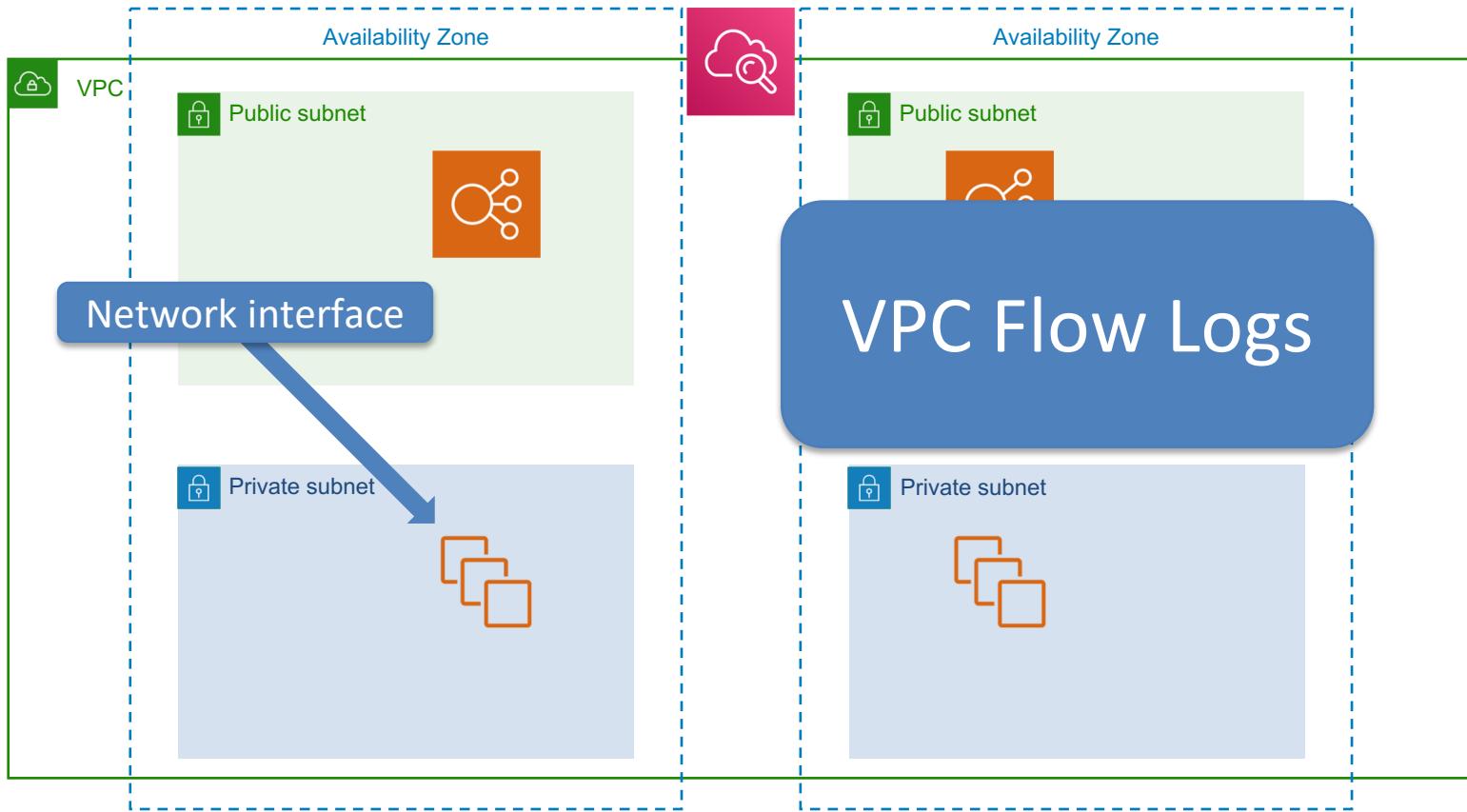
1. Design and implement security monitoring and alerting
2. Troubleshoot security monitoring and alerting
3. Design and implement a logging solution
4. Troubleshoot logging solutions



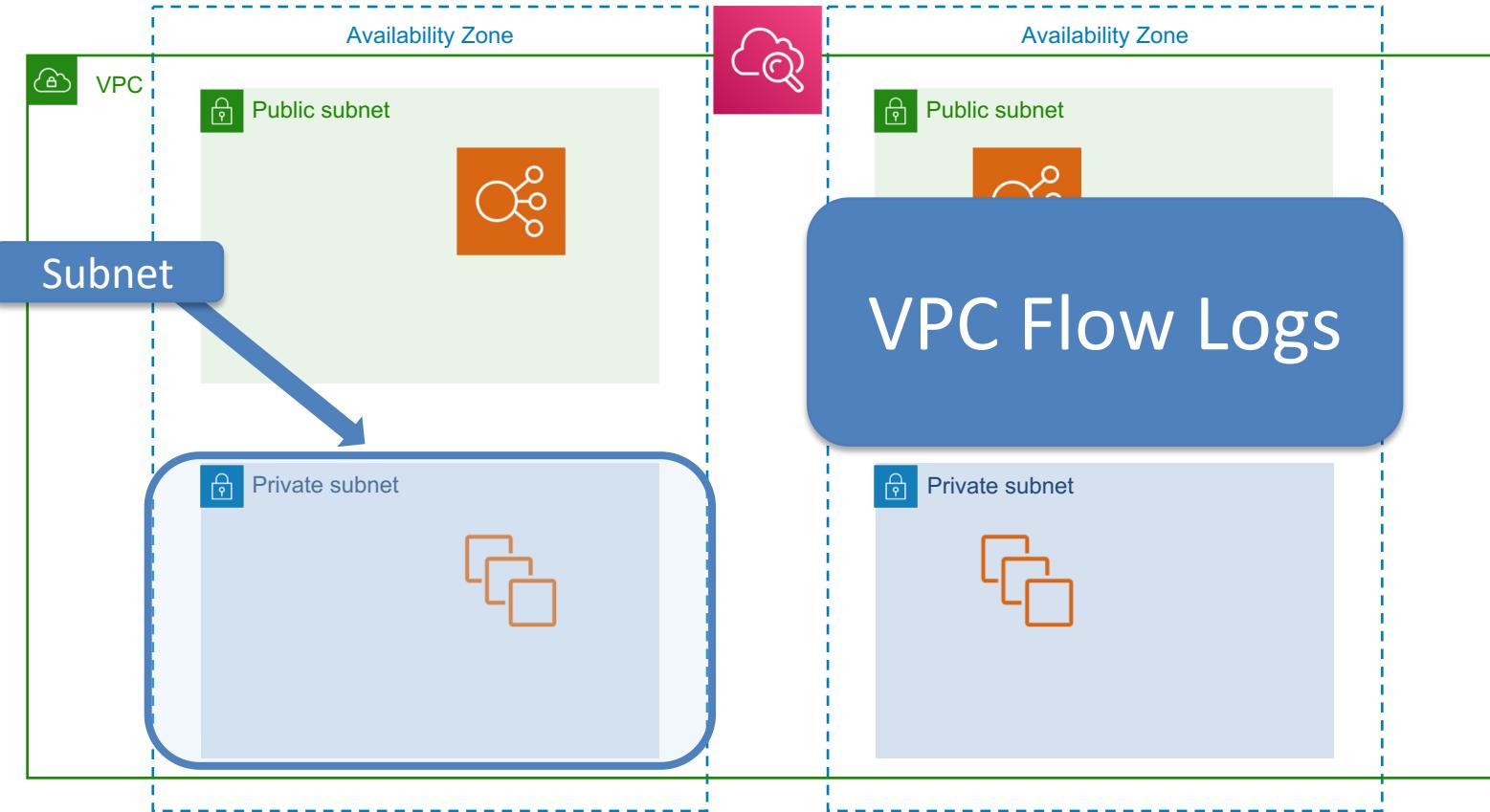
Logging and Monitoring

Design, implement and troubleshoot
security monitoring and alerting

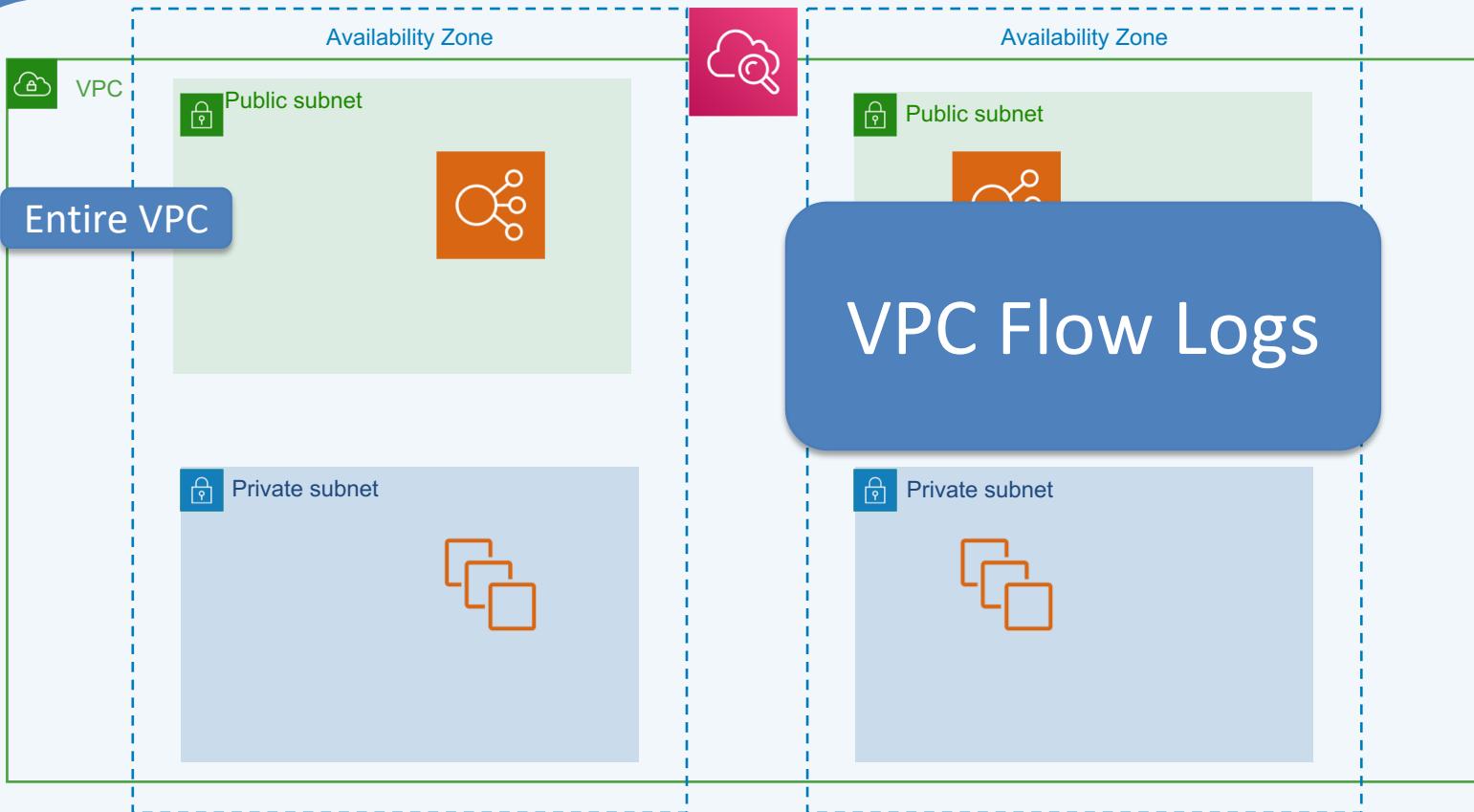
Infrastructure Security Monitoring



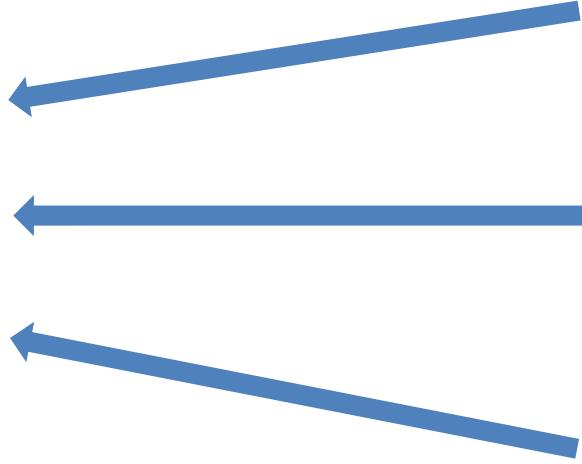
Infrastructure Security Monitoring



Infrastructure Security Monitoring



Infrastructure Security Monitoring



CloudTrail Logs

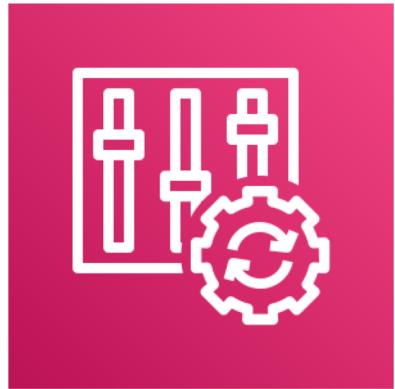


VPC Flow Logs

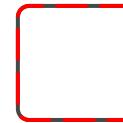
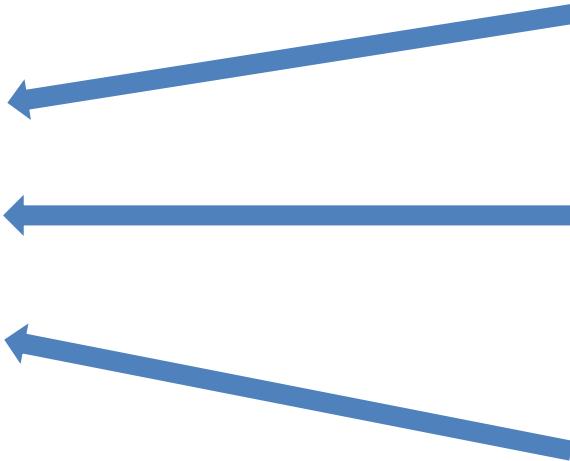


DNS Logs

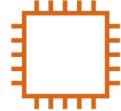
Infrastructure Security Monitoring



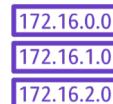
Config Rules



Security Group
Changes

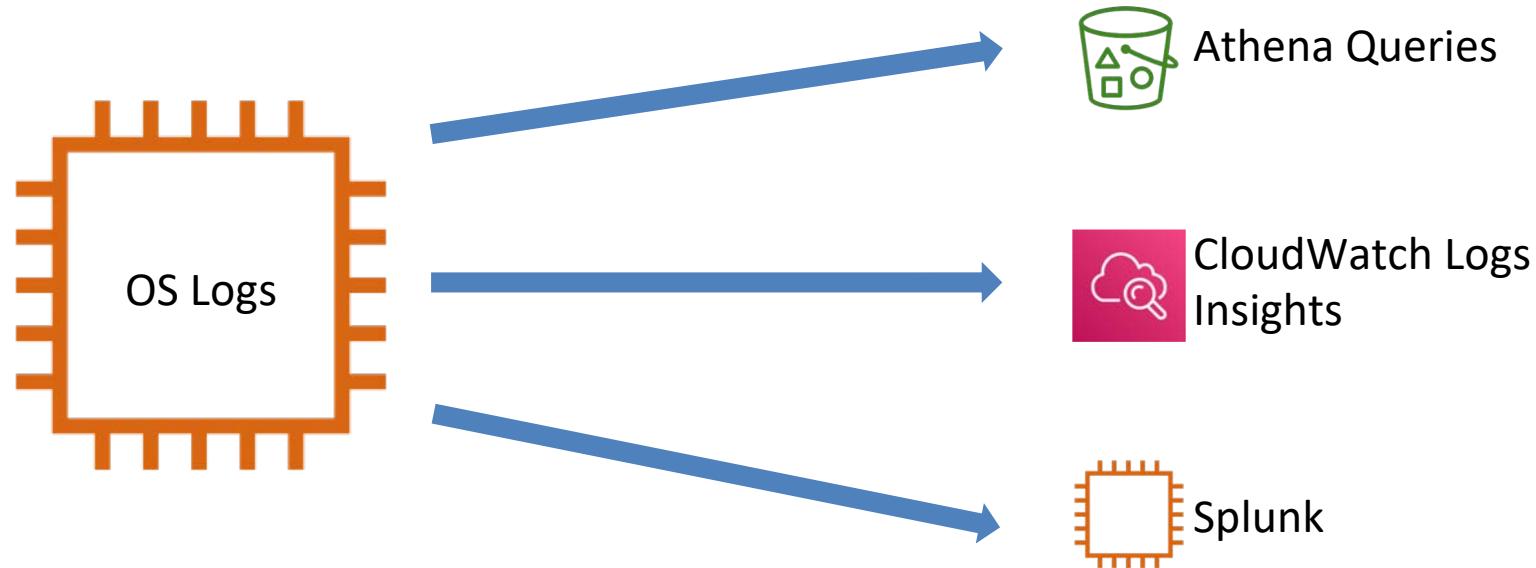


New Instance
Launch



Route Table
Addition

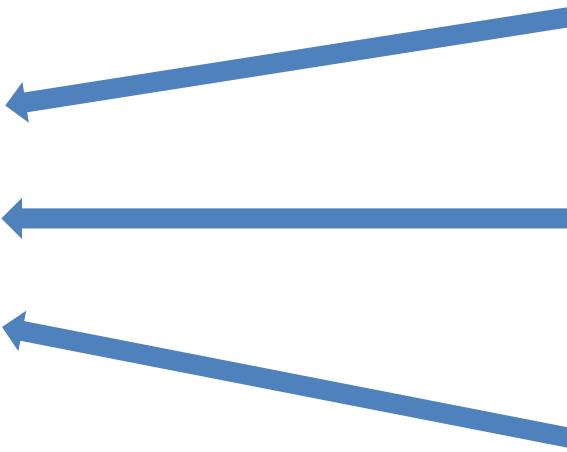
Infrastructure Security Monitoring



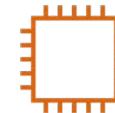
Application Security Monitoring



CloudWatch Logs



Lambda Execution
Logs



EC2 Application
Logs

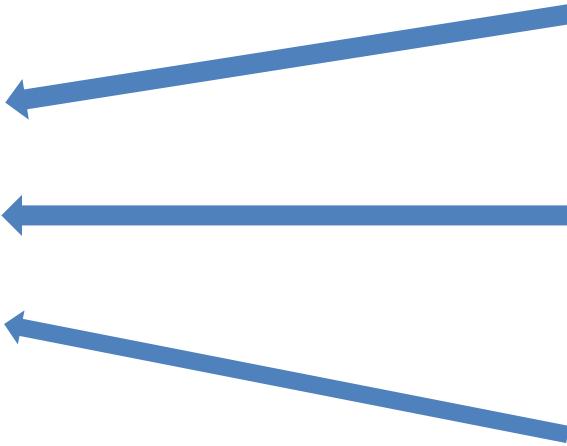


ECS/EKS Container
Logs

Application Security Monitoring



CloudTrail



Cognito User
Authentication
Logs



Step Functions
Logs

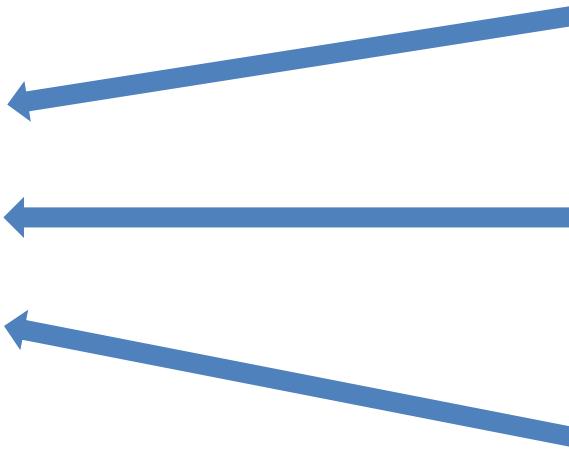


Deployments via
CodeDeploy

Application Security Monitoring



S3



ALB Access Logs



CloudFront Access Logs

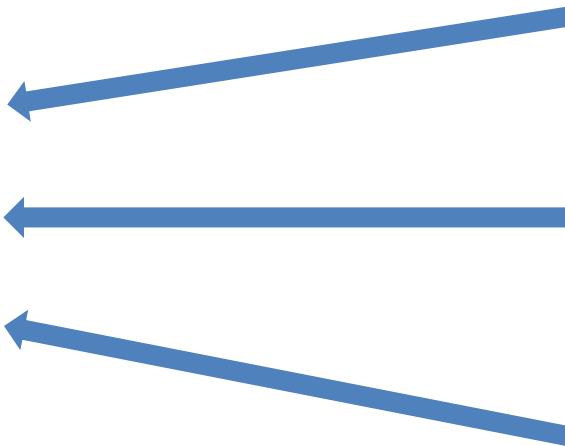


Redshift Audit Logs

Account Security Monitoring



CloudWatch Events



GuardDuty
Findings



CloudTrail Events



AWS Organizations
Events



AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

An application running in EC2 has a requirement for independent, periodic security checks against the application code. These checks can send notifications upon warning, but for critical alerts they must shut down the application on the instance. How can your security team perform these checks without injecting code into the application, while meeting the notification and active response requirement?

Question Breakdown

- A. Install the AWS Inspector agent on the instance, and schedule regular audit jobs. Send the findings to an SNS topic with a Lambda function subscribed that parses the findings and responds appropriately
- B. Deploy a second application on the EC2 instance with the security audit code. Send security audit results to CloudWatch Events, and create a rule to send warning events to SNS, and critical events to SSM Run Command to stop the application
- C. Install CloudWatch Logs agent on the instance, streaming all application logs. Create a CloudWatch Logs metric filters with alarms for notifications and a Lambda function to stop the application
- D. Install the AWS Inspector agent on the instance, and schedule regular audit jobs. Send the findings to CloudWatch Events, and create a rule to send warning events to SNS, and critical events to SSM Run Command to stop the application

Question Breakdown - Answers

AWS Inspector cannot audit your custom application code, but sending findings to Lambda is a good option

- A. Install the AWS Inspector agent on the instance, and schedule regular audit jobs. Send the findings to an SNS topic with a Lambda function subscribed that parses the findings and responds appropriately

Question Breakdown - Answers

This meets all of the requirements

B. Deploy a second application on the EC2 instance with the security audit code. Send security audit results to CloudWatch Events, and create a rule to send warning events to SNS, and critical events to SSM Run Command to stop the application

Question Breakdown - Answers

This does not act as an independent audit, relying on application logs

- C. Install CloudWatch Logs agent on the instance, streaming all application logs. Create a CloudWatch Logs metric filters with alarms for notifications and a Lambda function to stop the application

Question Breakdown - Answers

Again, Inspector cannot audit custom code. The passive/active response mechanism is appropriate

D. Install the AWS Inspector agent on the instance, and schedule regular audit jobs. Send the findings to CloudWatch Events, and create a rule to send warning events to SNS, and critical events to SSM Run Command to stop the application

Question Breakdown - Correct Answer

Correct Answer: B

- B. Deploy a second application on the EC2 instance with the security audit code. Send security audit results to CloudWatch Events, and create a rule to send warning events to SNS, and critical events to SSM Run Command to stop the application



Logging and Monitoring

Design and implement, and troubleshoot a logging solution

Access Logs - API Gateway



CloudWatch Logs

Access Logs - CloudFront

Bucket ACL



S3 Bucket

* best-effort delivery!!!

Access Logs - ELB

Bucket Policy



S3 Bucket

* best-effort delivery!!!

Access Logs - S3

Bucket ACL



S3 Bucket

* best-effort delivery!!!

Execution Logs - API Gateway



IAM Role

CloudWatch Logs

Execution Logs - Lambda

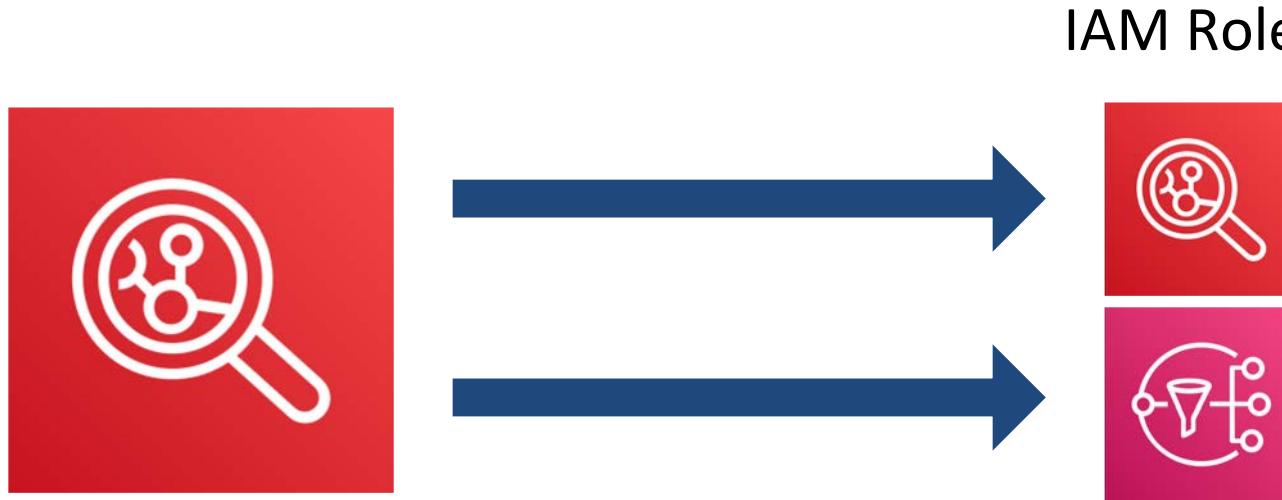


CloudWatch Logs

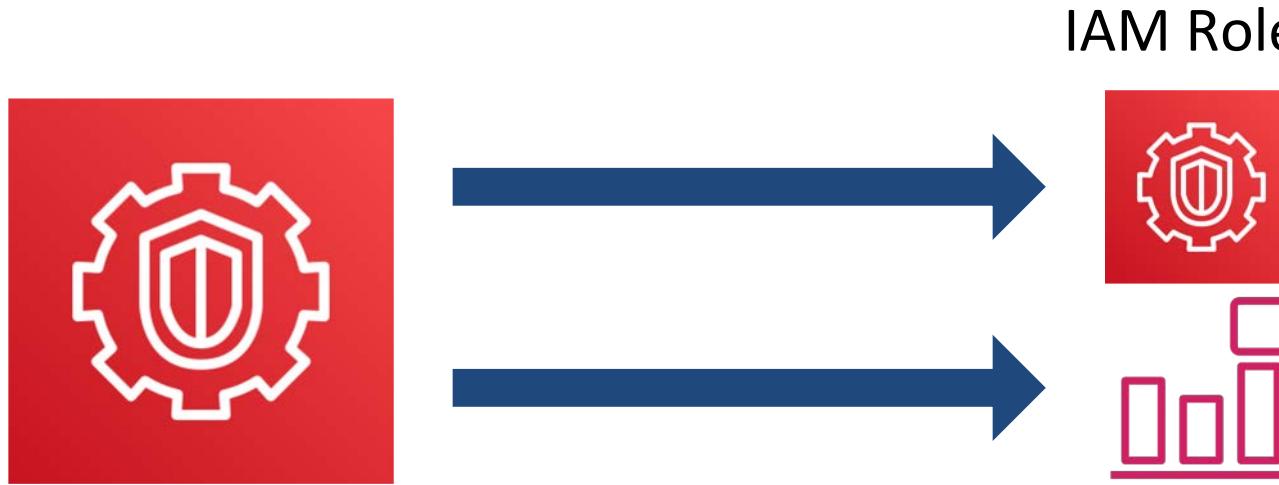
Execution Logs - Custom EC2



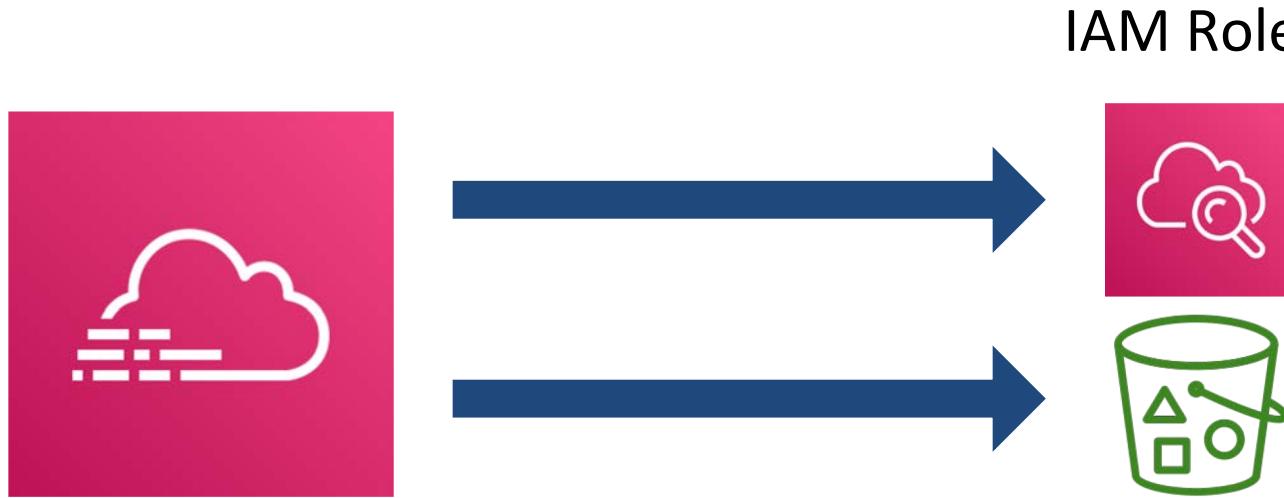
Security Logs - Amazon Inspector



Security Logs - Amazon GuardDuty



Security Logs - AWS CloudTrail



Security Logs - VPC Flow Logs



Log Processing - So Many Choices!

1. Kinesis
2. Athena
3. RedShift
4. AWS Glue
5. Elastic MapReduce
6. Amazon ElasticSearch/Kibana
7. CloudWatch Insights
8. Lambda
9. EC2 Marketplace



AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

You've been asked to stream application logs from CloudWatch Logs to Splunk. There is an existing subscription filter on the log group, set up for Kinesis Firehose to S3. What is the most appropriate way to ingest the logs in near real-time for Splunk analysis?

- A. Create a Lambda function subscribed to the CloudWatch log group that streams log entries to the Splunk endpoint
- B. Create a Splunk connector to the S3 bucket destination for the Kinesis Firehose
- C. Enable Source record transformation on the Kinesis Firehose. Create a Lambda function using the Splunk blueprints which decompresses the log entries and pushes to Splunk
- D. Write a shell script that uses the AWS CLI to export logs from the CloudWatch log group and ingest into Splunk

Question Breakdown - Answers

CloudWatch log groups only support one subscription filter at a time

- A. Create a Lambda function subscribed to the CloudWatch log group that streams log entries to the Splunk endpoint
- B. Create a Splunk connector to the S3 bucket destination for the Kinesis Firehose
- C. Enable Source record transformation on the Kinesis Firehose. Create a Lambda function using the Splunk blueprints which decompresses the log entries and pushes to Splunk
- D. Write a shell script that uses the AWS CLI to export logs from the CloudWatch log group and ingest into Splunk

Question Breakdown - Answers

S3 ingestion will not be near real-time

- A. Create a Lambda function subscribed to the CloudWatch log group that streams log entries to the Splunk endpoint
- B. Create a Splunk connector to the S3 bucket destination for the Kinesis Firehose
- C. Enable Source record transformation on the Kinesis Firehose. Create a Lambda function using the Splunk blueprints which decompresses the log entries and pushes to Splunk
- D. Write a shell script that uses the AWS CLI to export logs from the CloudWatch log group and ingest into Splunk

Question Breakdown - Answers

Addresses the single subscription filter issue, and allows for near real-time streaming

- A. Create a Lambda function subscribed to the CloudWatch log group that streams log entries to the Splunk endpoint
- B. Create a Splunk connector to the S3 bucket destination for the Kinesis Firehose
- C. Enable Source record transformation on the Kinesis Firehose. Create a Lambda function using the Splunk blueprints which decompresses the log entries and pushes to Splunk
- D. Write a shell script that uses the AWS CLI to export logs from the CloudWatch log group and ingest into Splunk

Question Breakdown - Answers

May be functional but not reliable or near real-time

- A. Create a Lambda function subscribed to the CloudWatch log group that streams log entries to the Splunk endpoint
- B. Create a Splunk connector to the S3 bucket destination for the Kinesis Firehose
- C. Enable Source record transformation on the Kinesis Firehose. Create a Lambda function using the Splunk blueprints which decompresses the log entries and pushes to Splunk
- D. Write a shell script that uses the AWS CLI to export logs from the CloudWatch log group and ingest into Splunk

Question Breakdown - Correct Answer

Correct Answer:C

- A. Create a Lambda function subscribed to the CloudWatch log group that streams log entries to the Splunk endpoint
- B. Create a Splunk connector to the S3 bucket destination for the Kinesis Firehose
- C. Enable Source record transformation on the Kinesis Firehose. Create a Lambda function using the Splunk blueprints which decompresses the log entries and pushes to Splunk
- D. Write a shell script that uses the AWS CLI to export logs from the CloudWatch log group and ingest into Splunk



AWS Certified Security - Specialty Crash Course

Infrastructure Security Part I 26%

Question Domain Main Points

1. Design edge security on AWS
2. Design and implement a secure network infrastructure

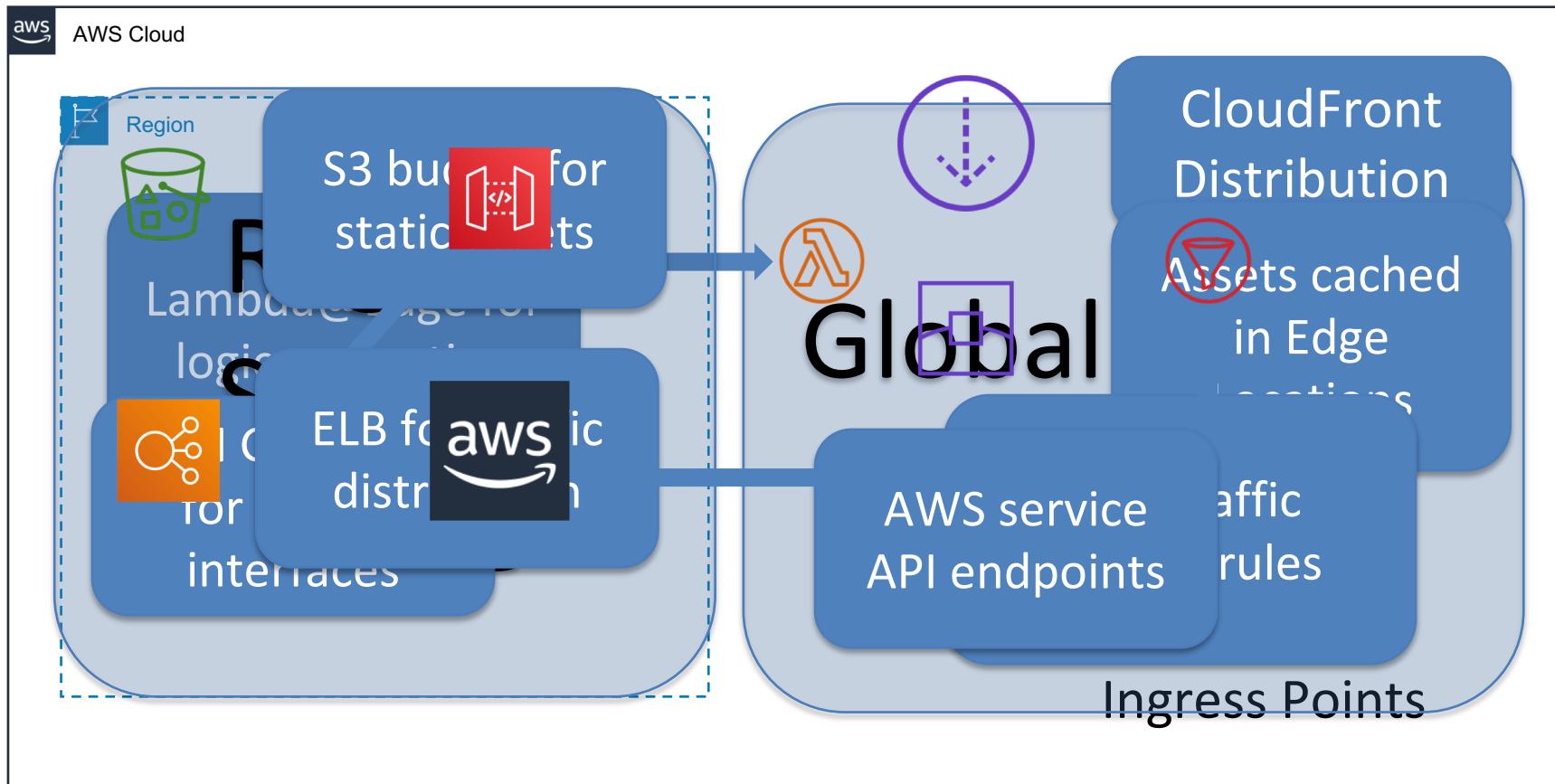


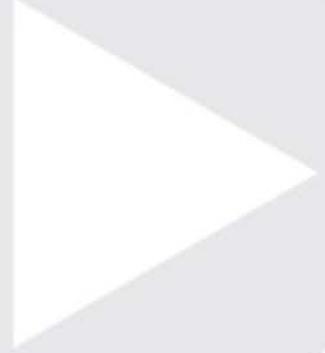
Infrastructure Security Part I

Design edge security on AWS

Edge Security - Ingress Points

- CloudFront
- S3
- API Gateway
- Elastic Load Balancer
- AWS Service API endpoints
- VPC Ingress (next section)





Infrastructure Security Part I

Design and implement a secure
network infrastructure

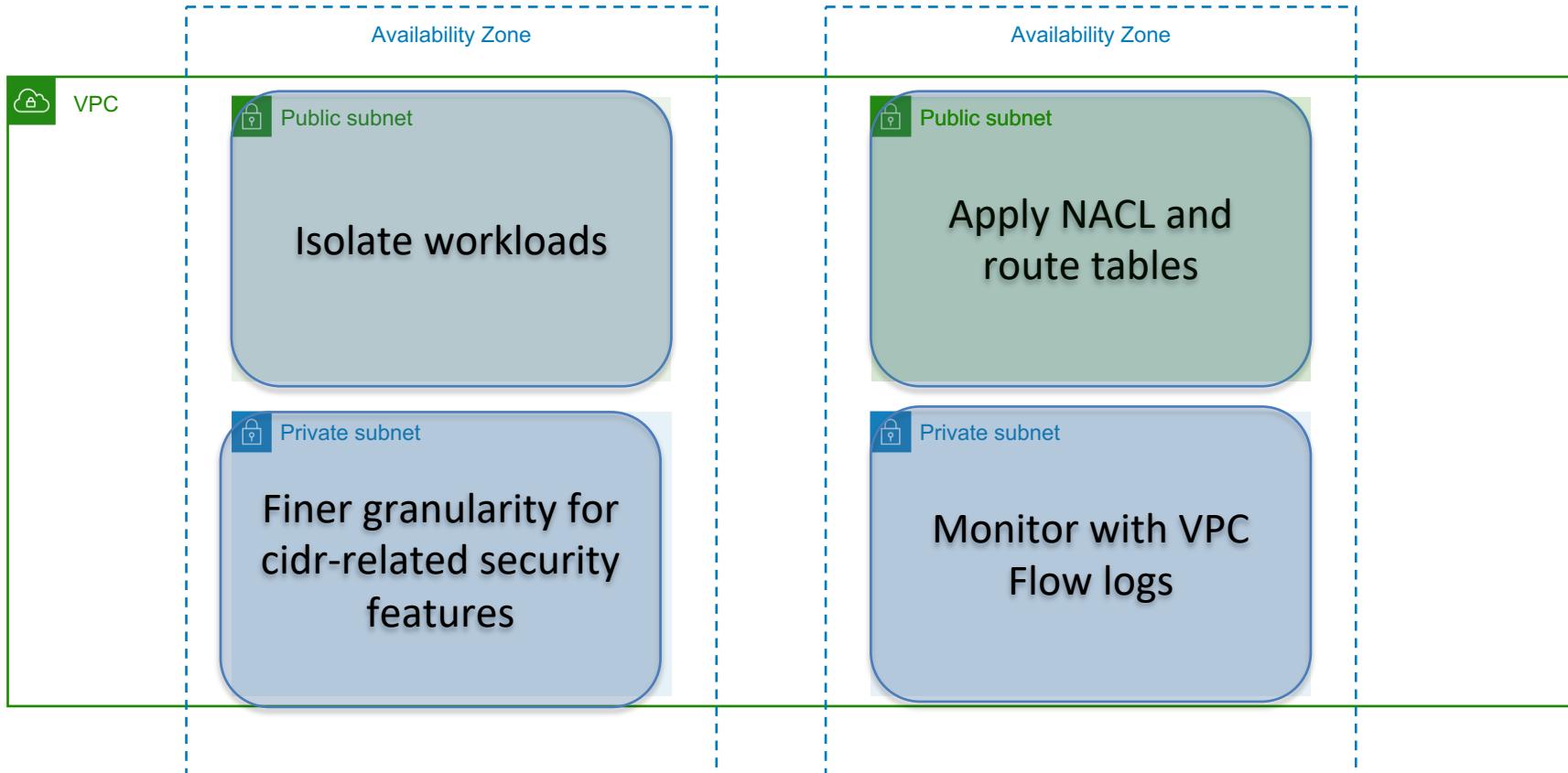
Network Security - Single VPC

- Subnet
- NACL
- Route Table
- Security Group

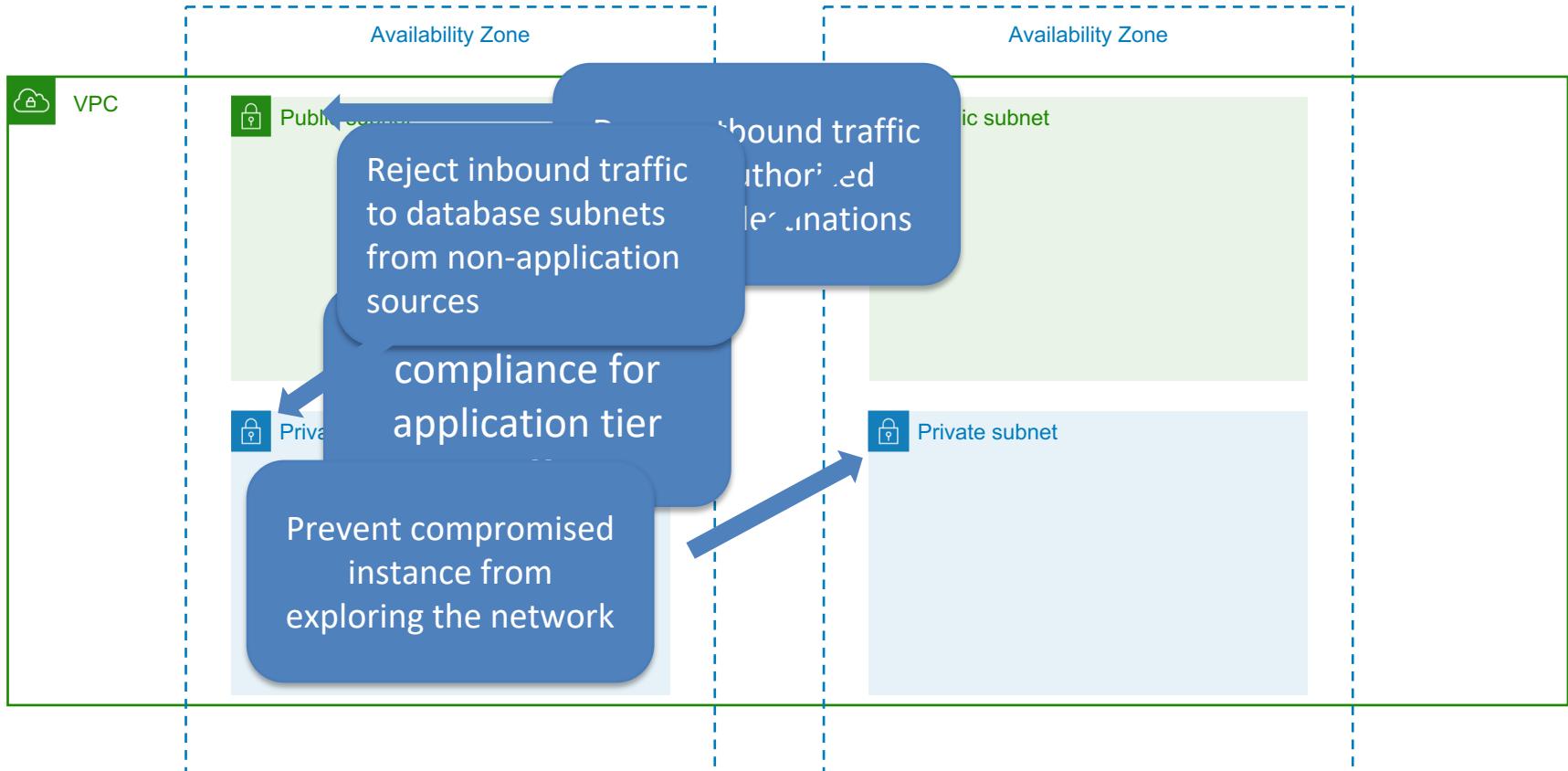
Network Security - VPC Egress

- Internet Gateway
- Virtual Private Gateway
- VPC Peering Connection
- Gateway Endpoint
- Interface Endpoint (PrivateLink)
- NAT Gateway
- DiY

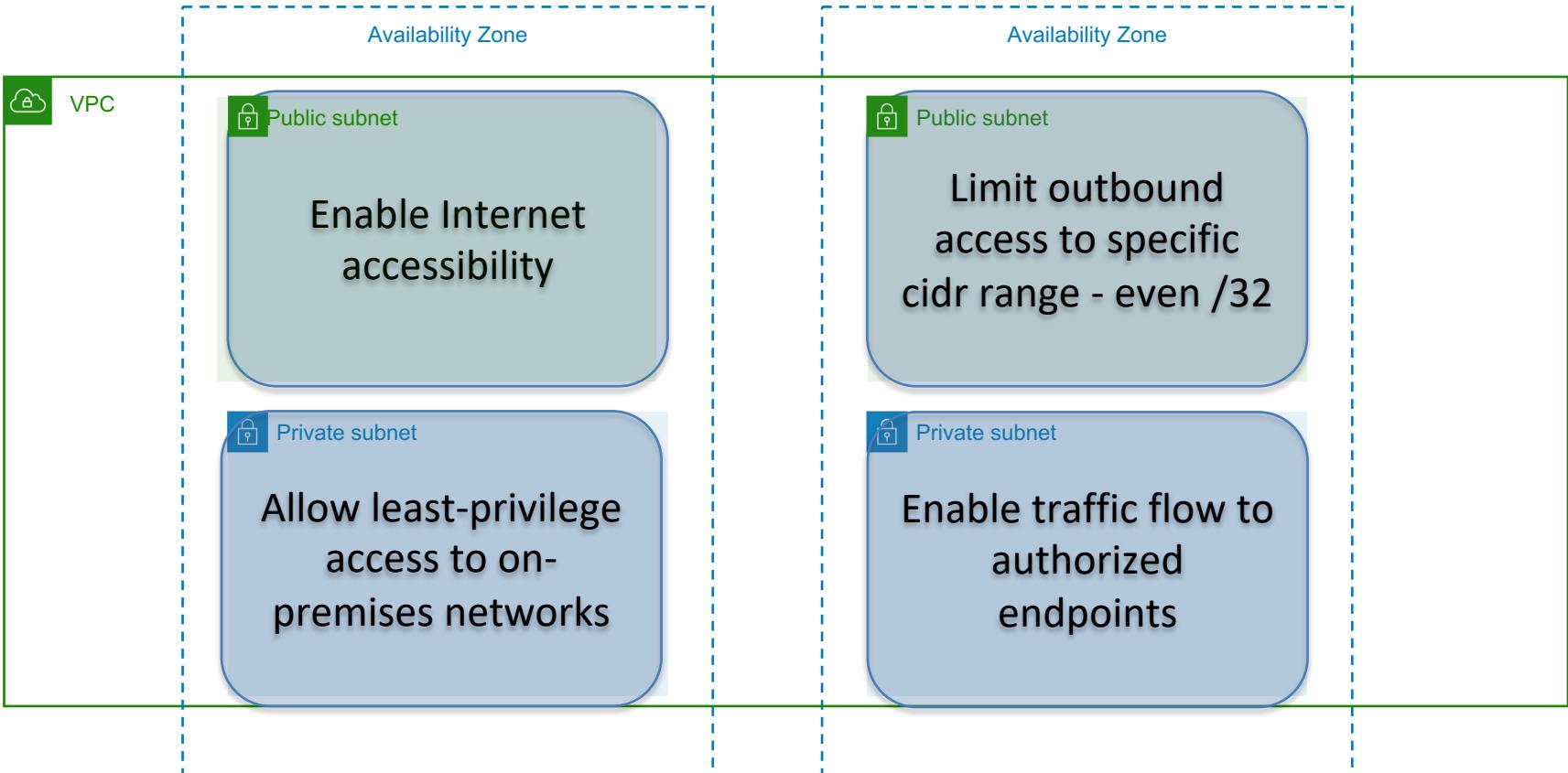
Single VPC - Subnet



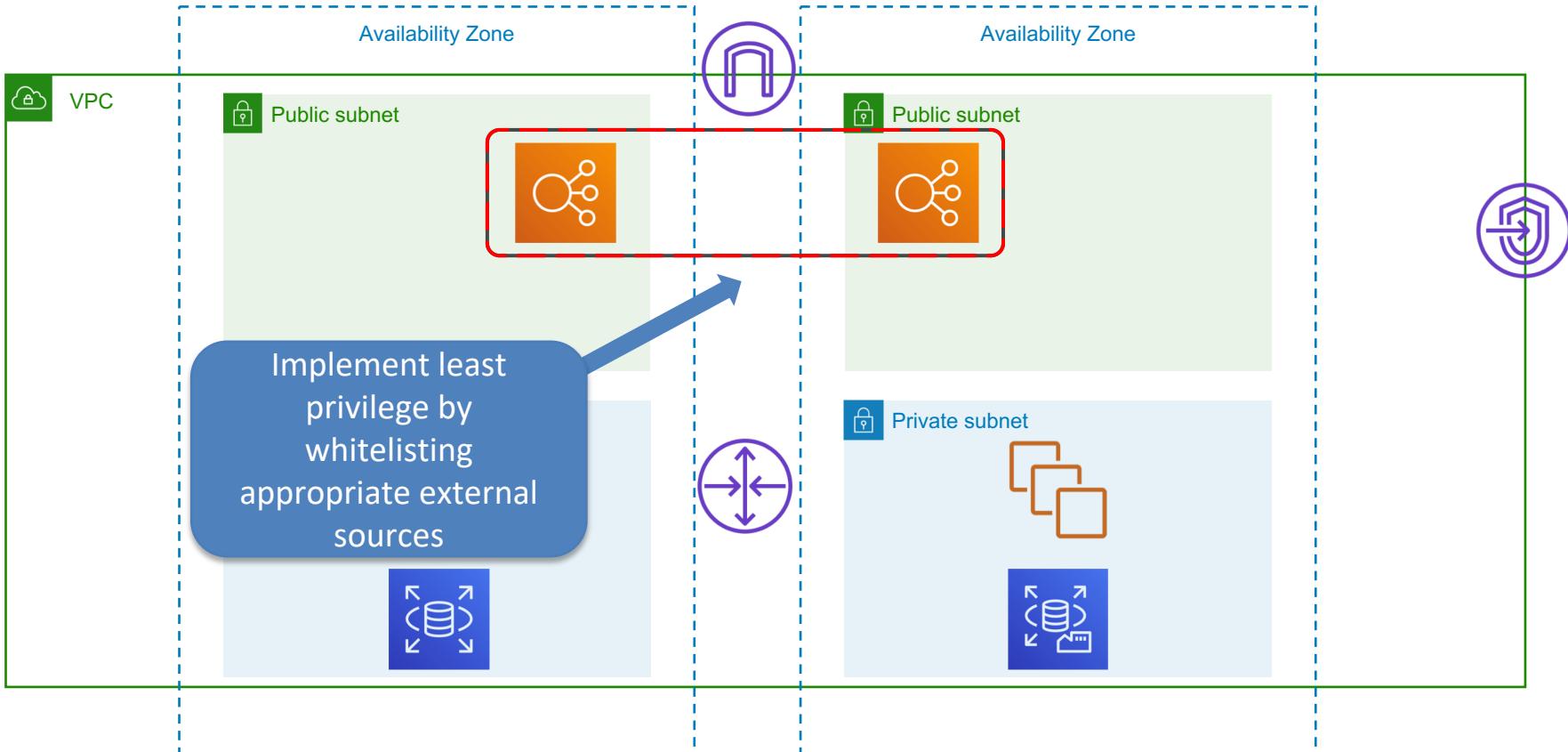
Single VPC - NACL



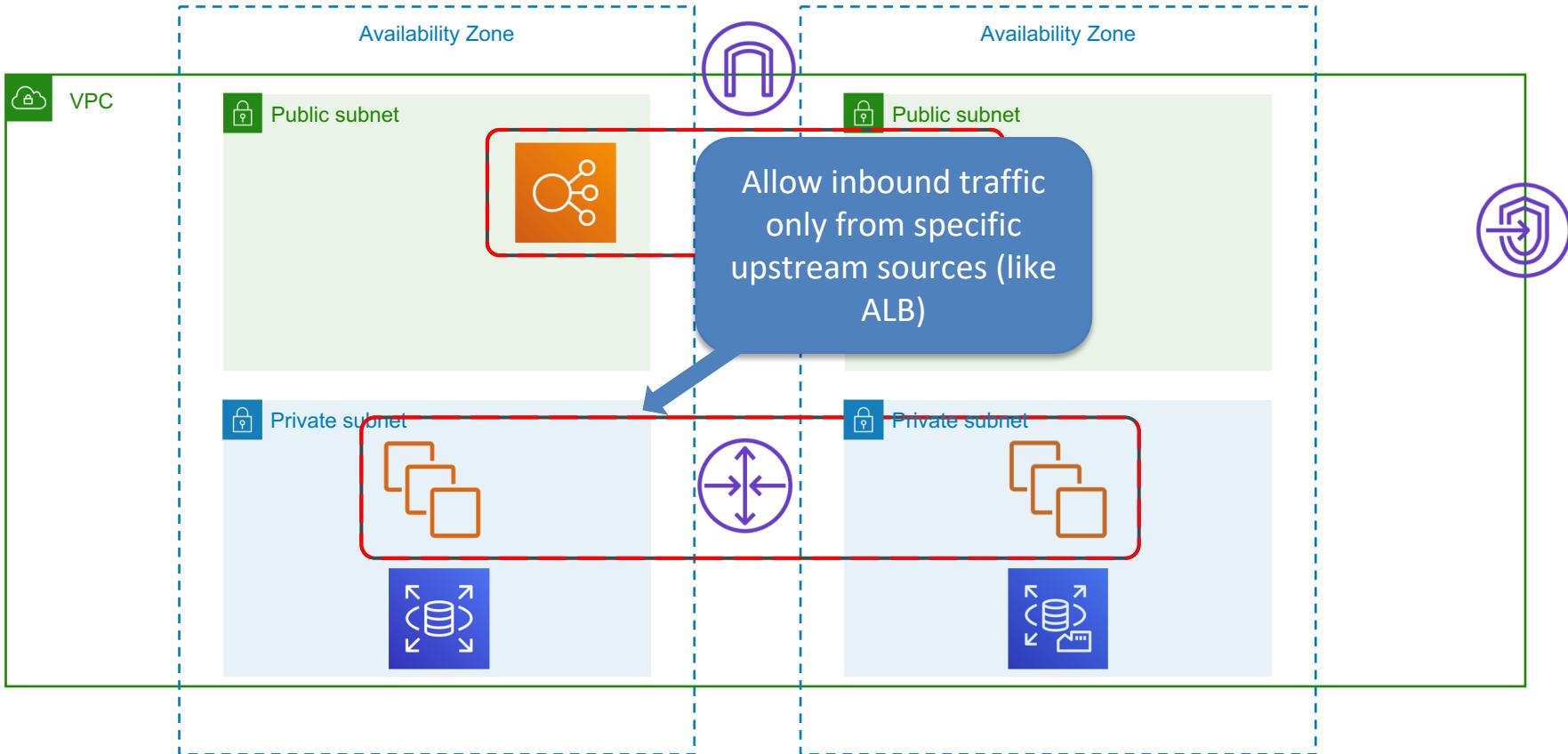
Single VPC - Route Table



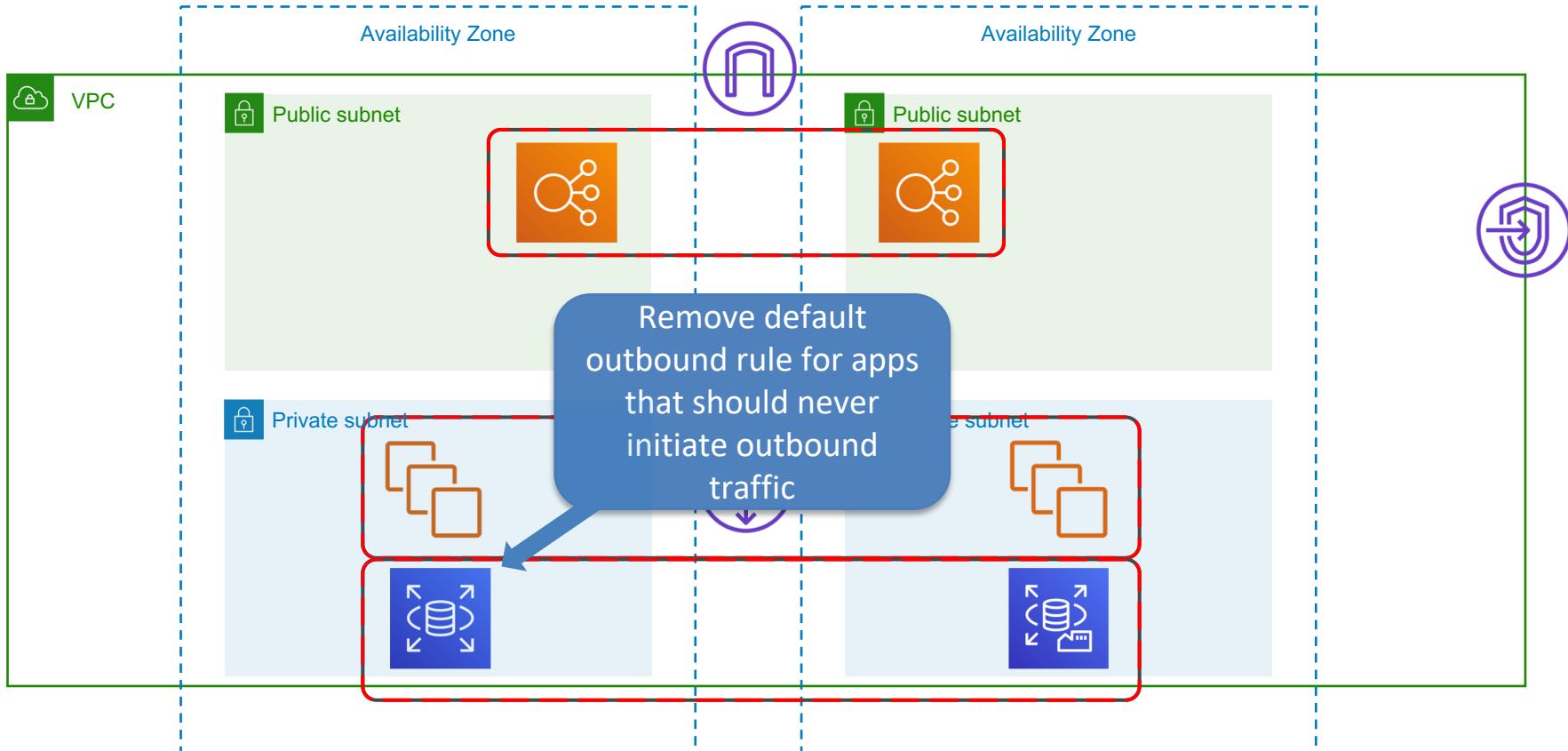
Single VPC - Security Group



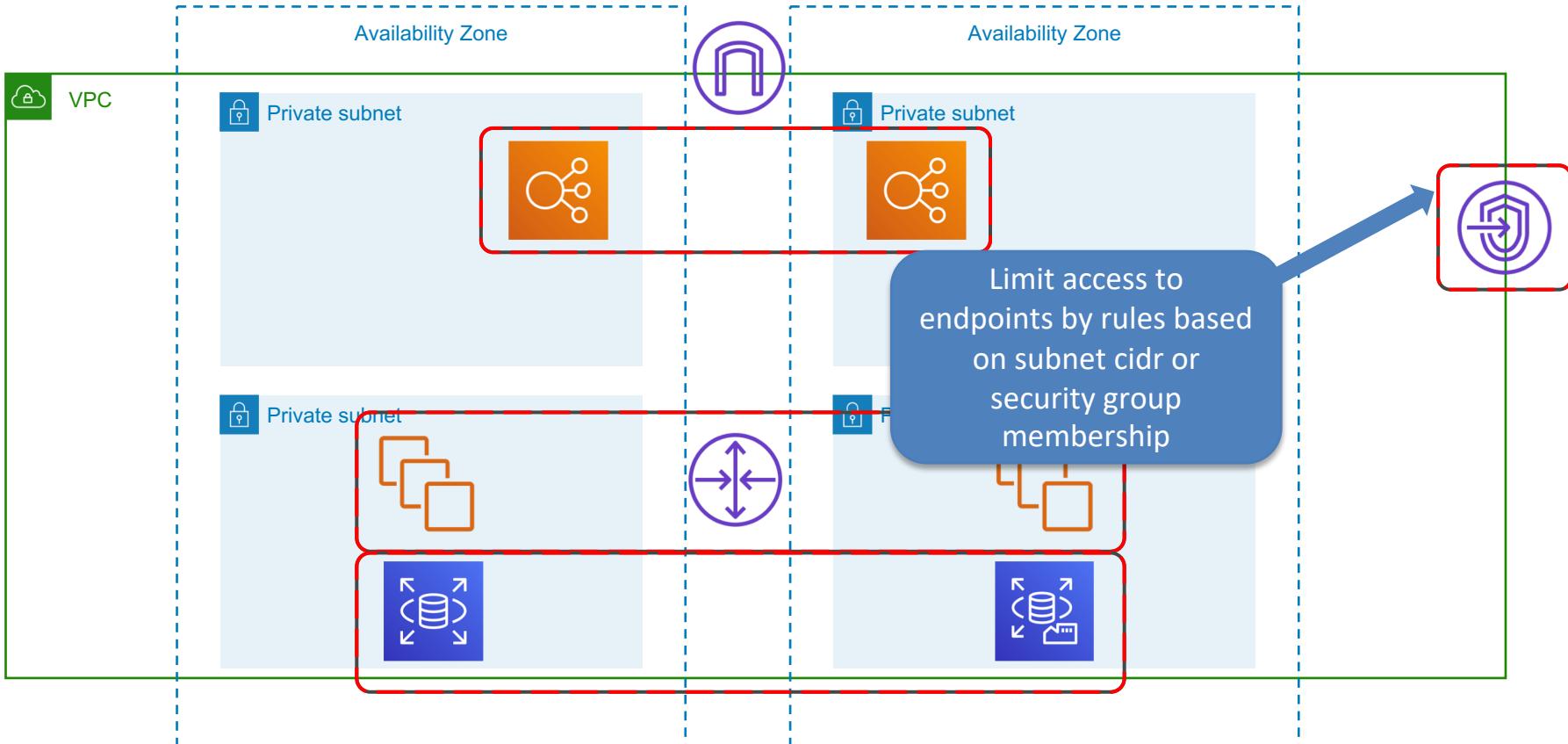
Single VPC - Security Group



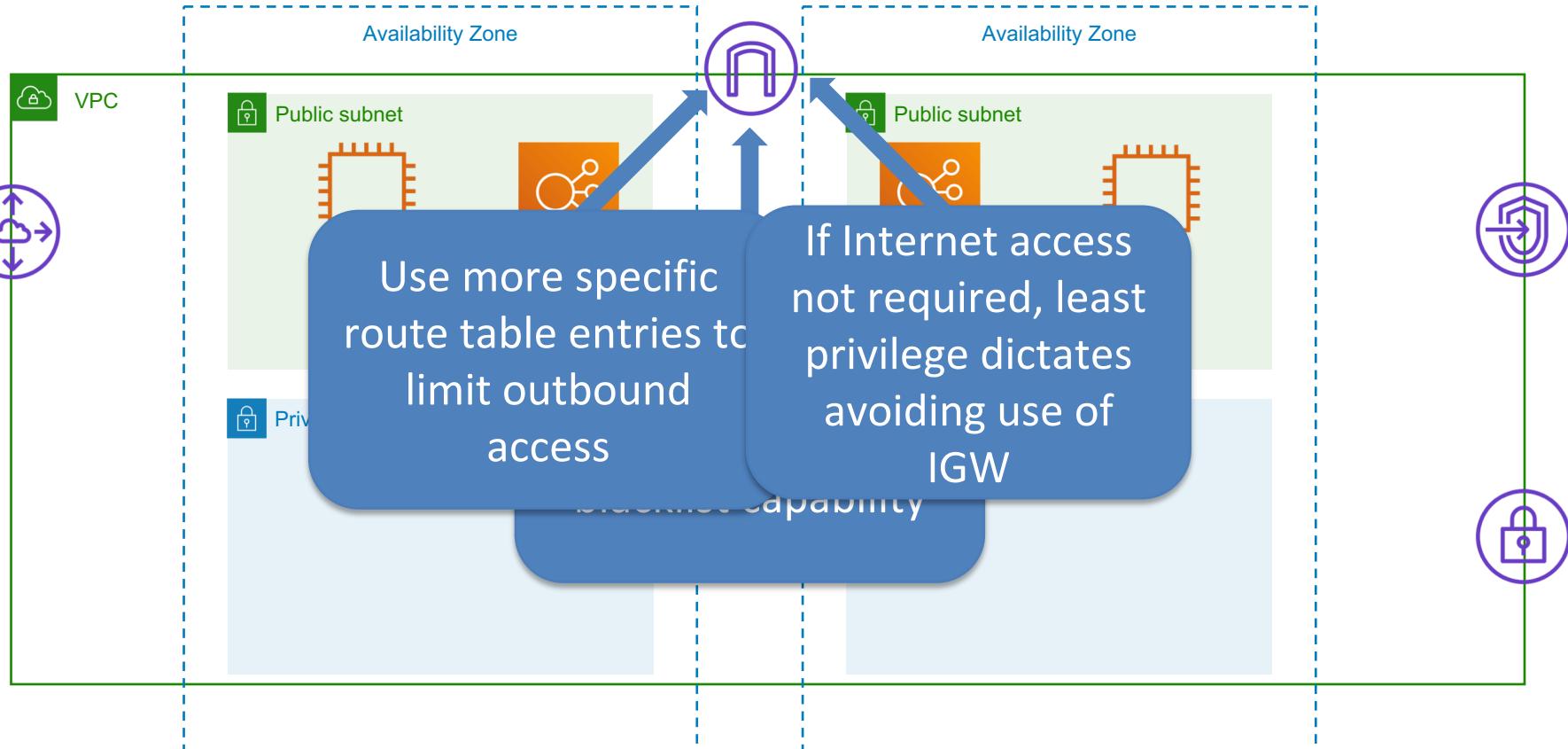
Single VPC - Security Group



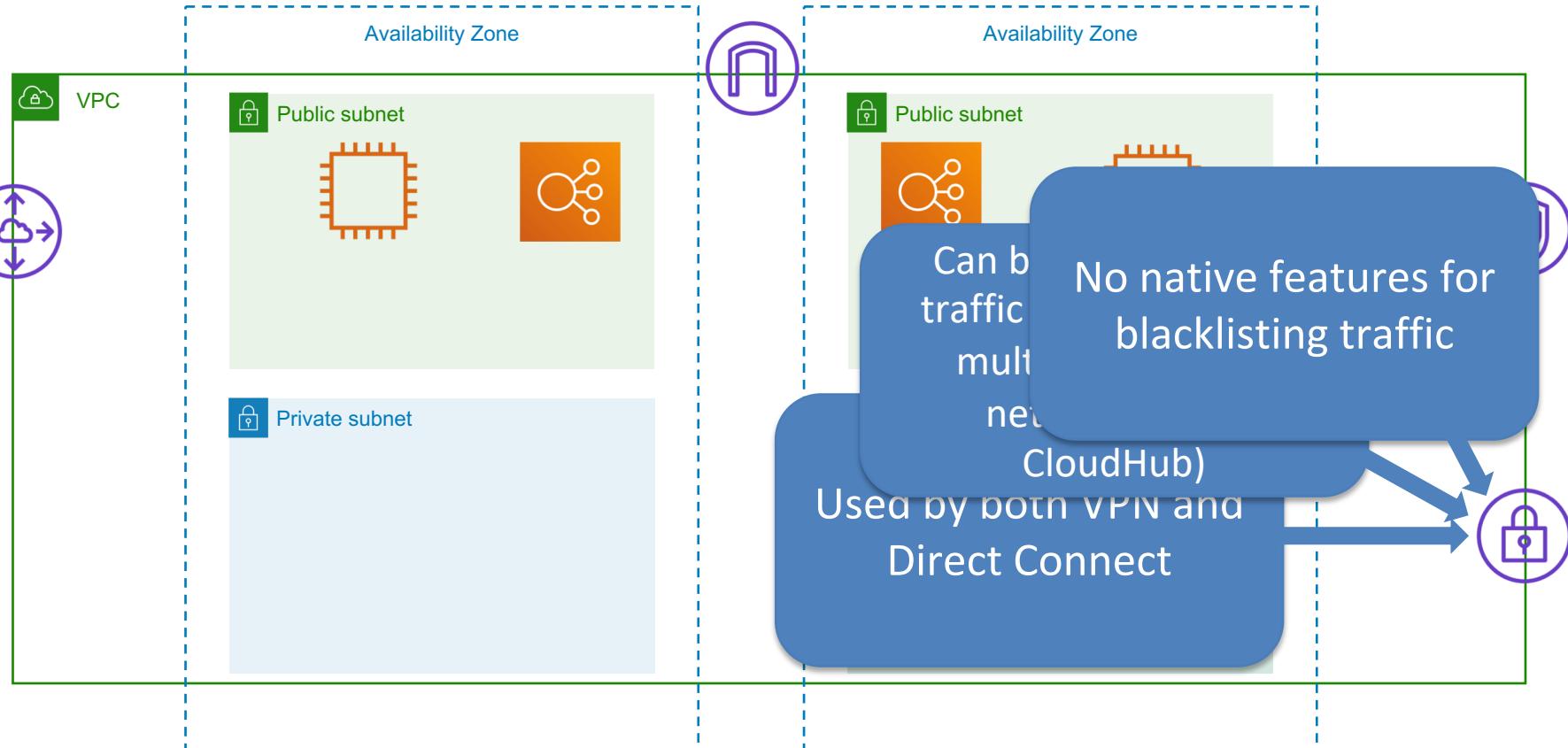
Single VPC - Security Group



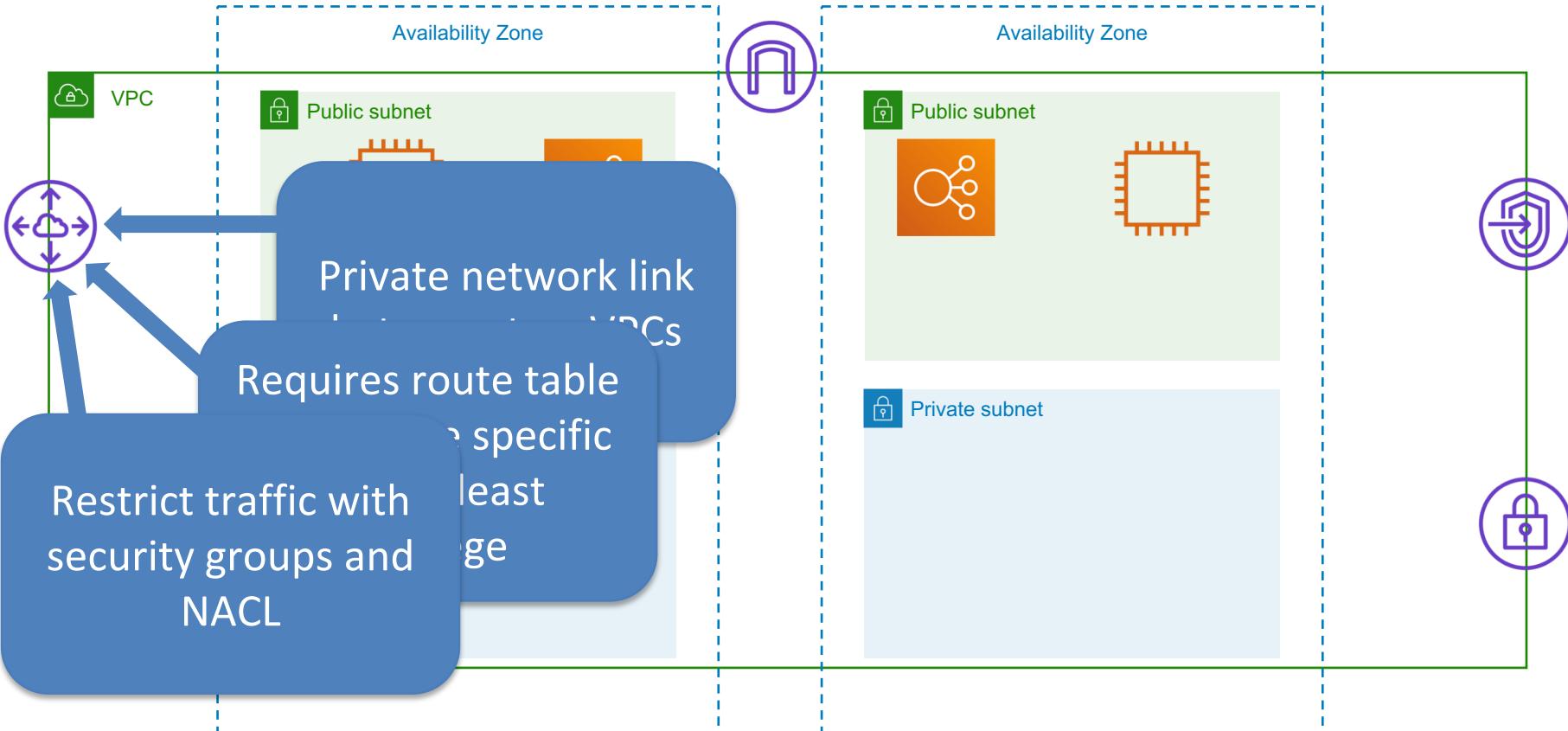
VPC Egress - Internet Gateway



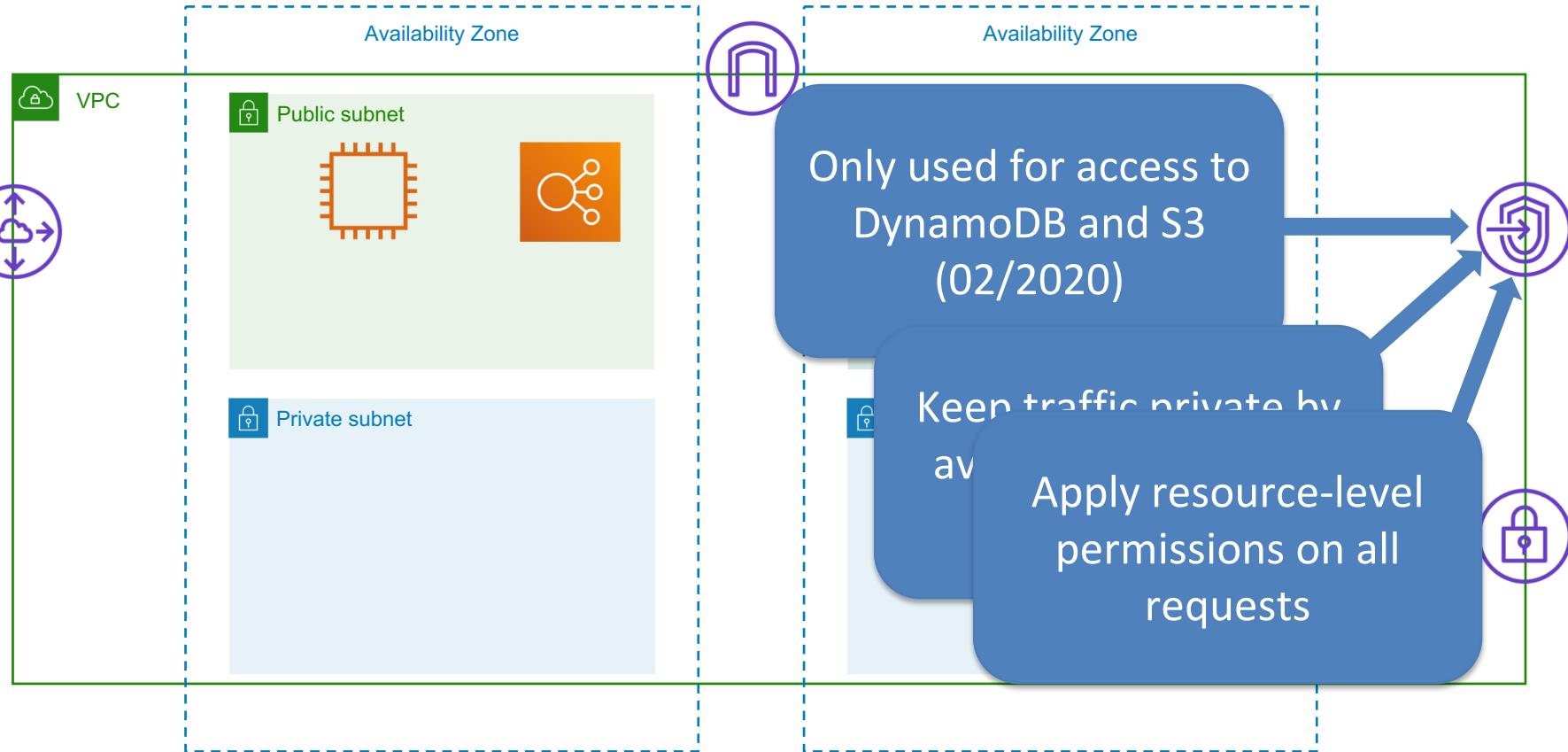
VPC Egress - Virtual Private Gateway



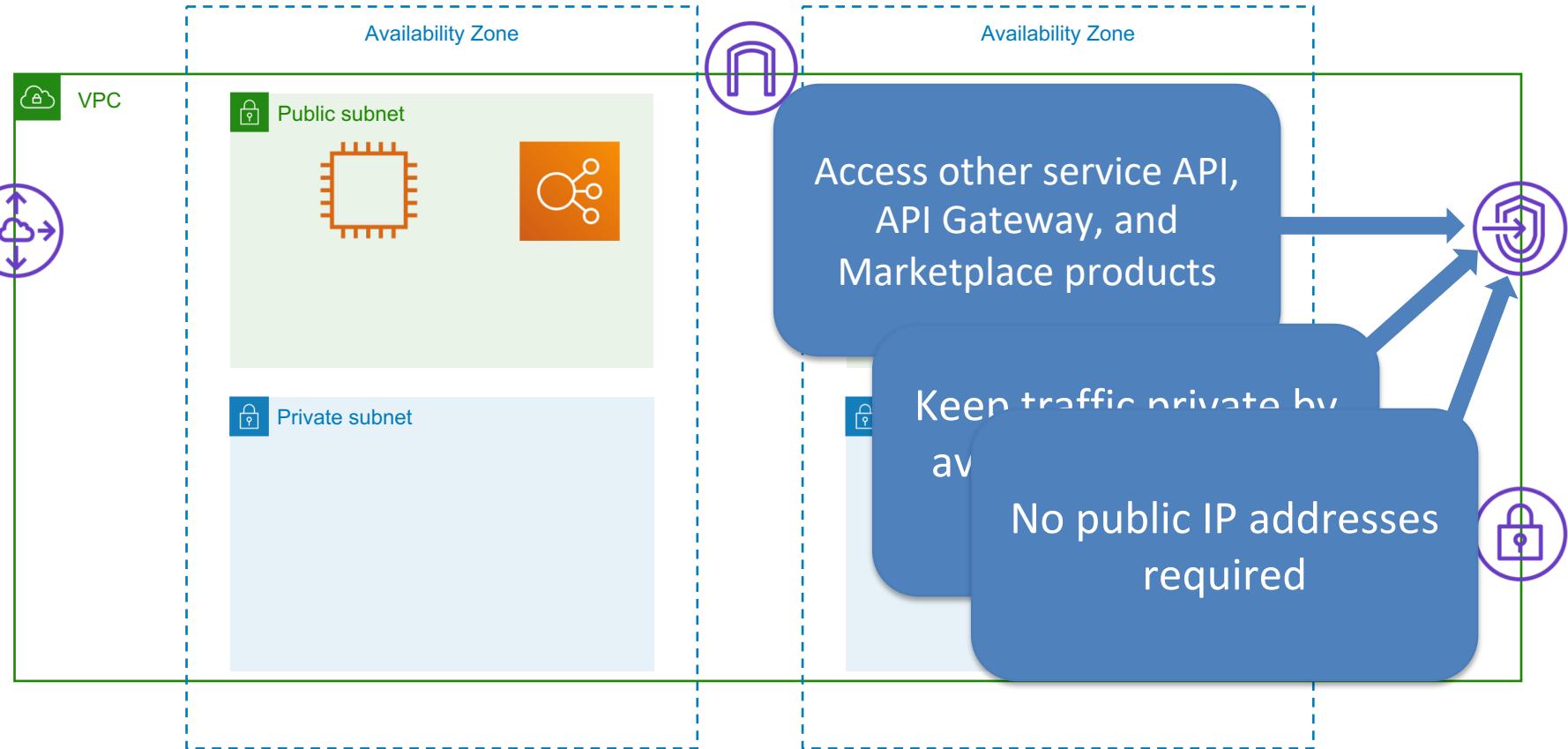
VPC Egress - VPC Peering Connection



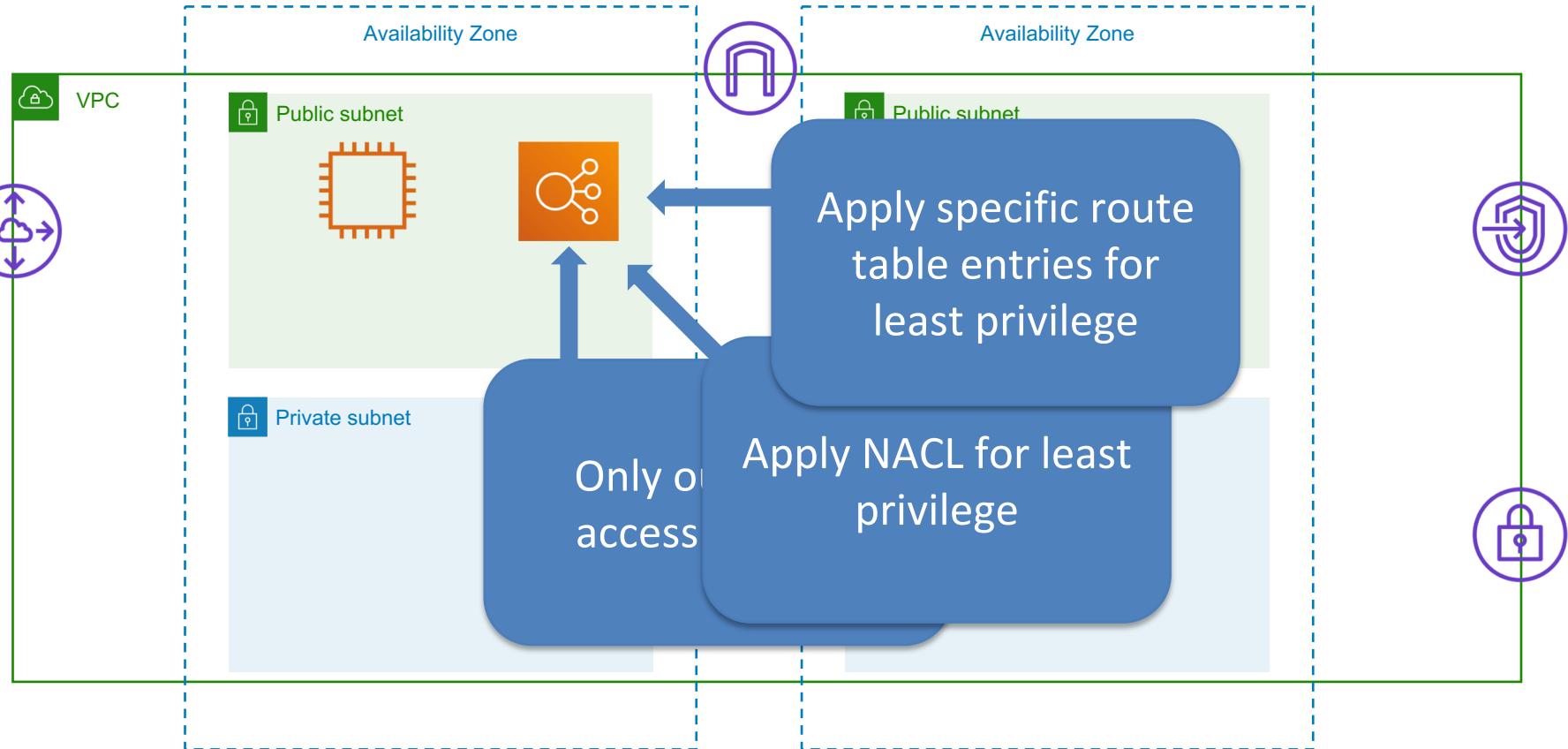
VPC Egress - Gateway Endpoint



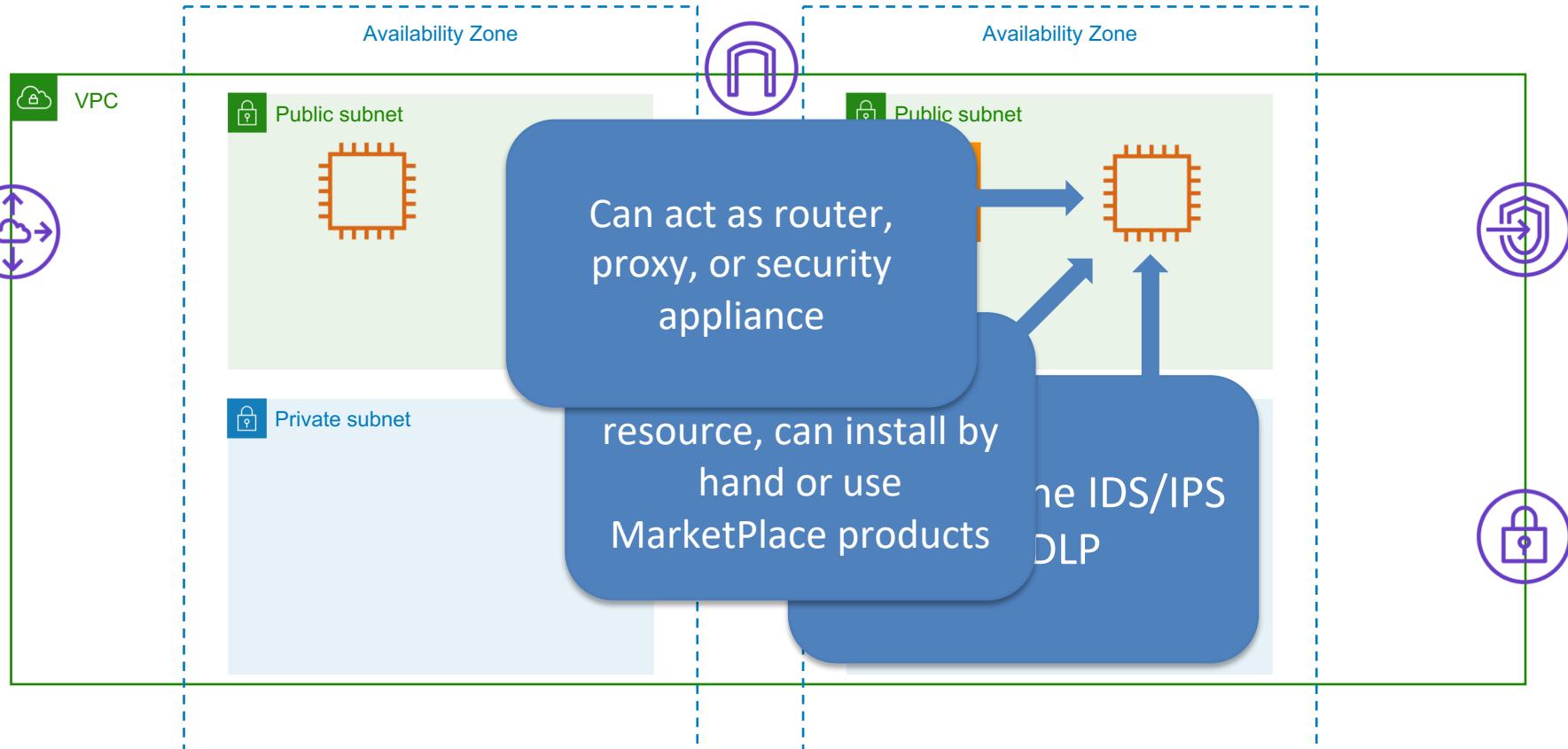
VPC Egress - Interface Endpoint



VPC Egress - NAT Gateway



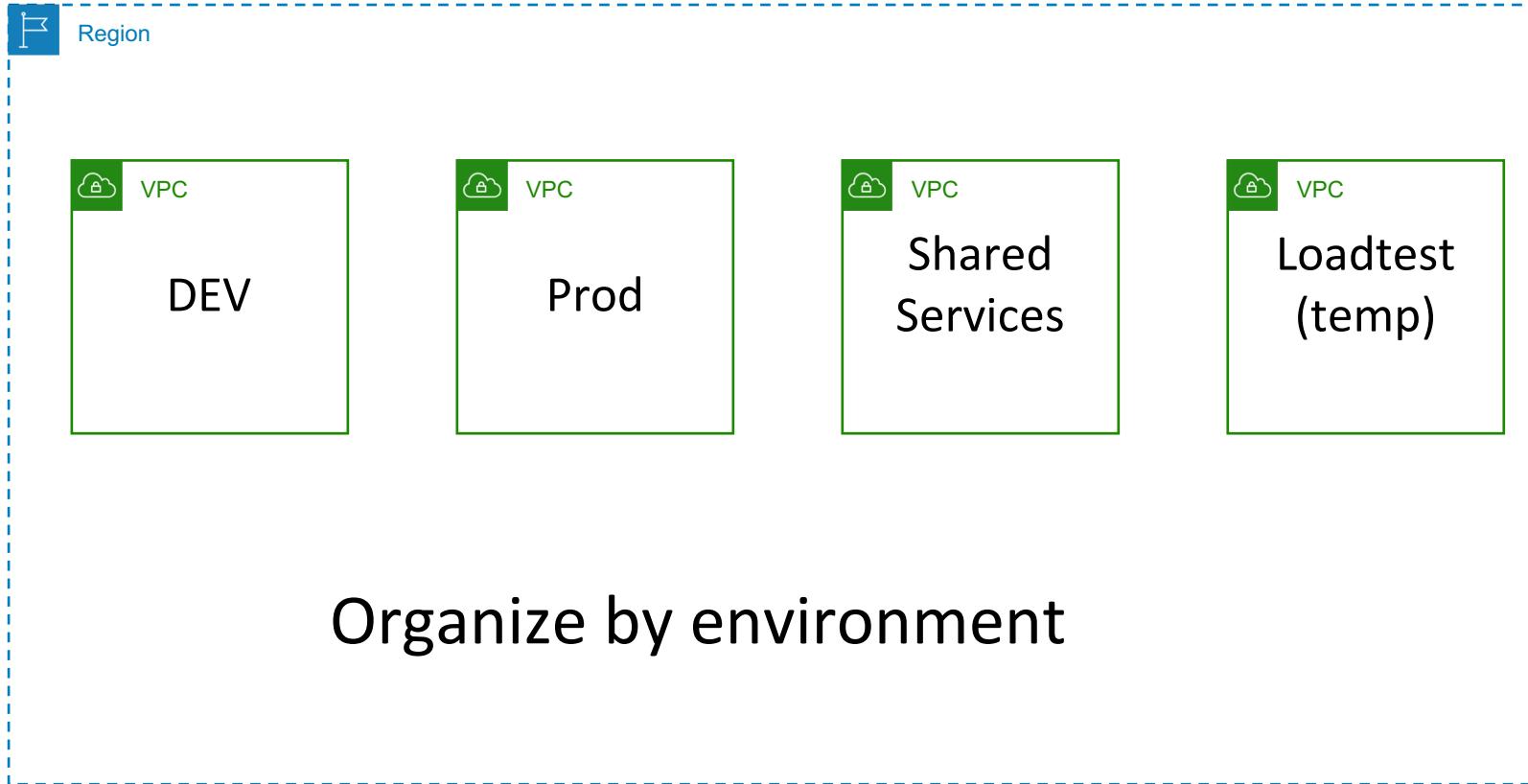
VPC Egress - DiY



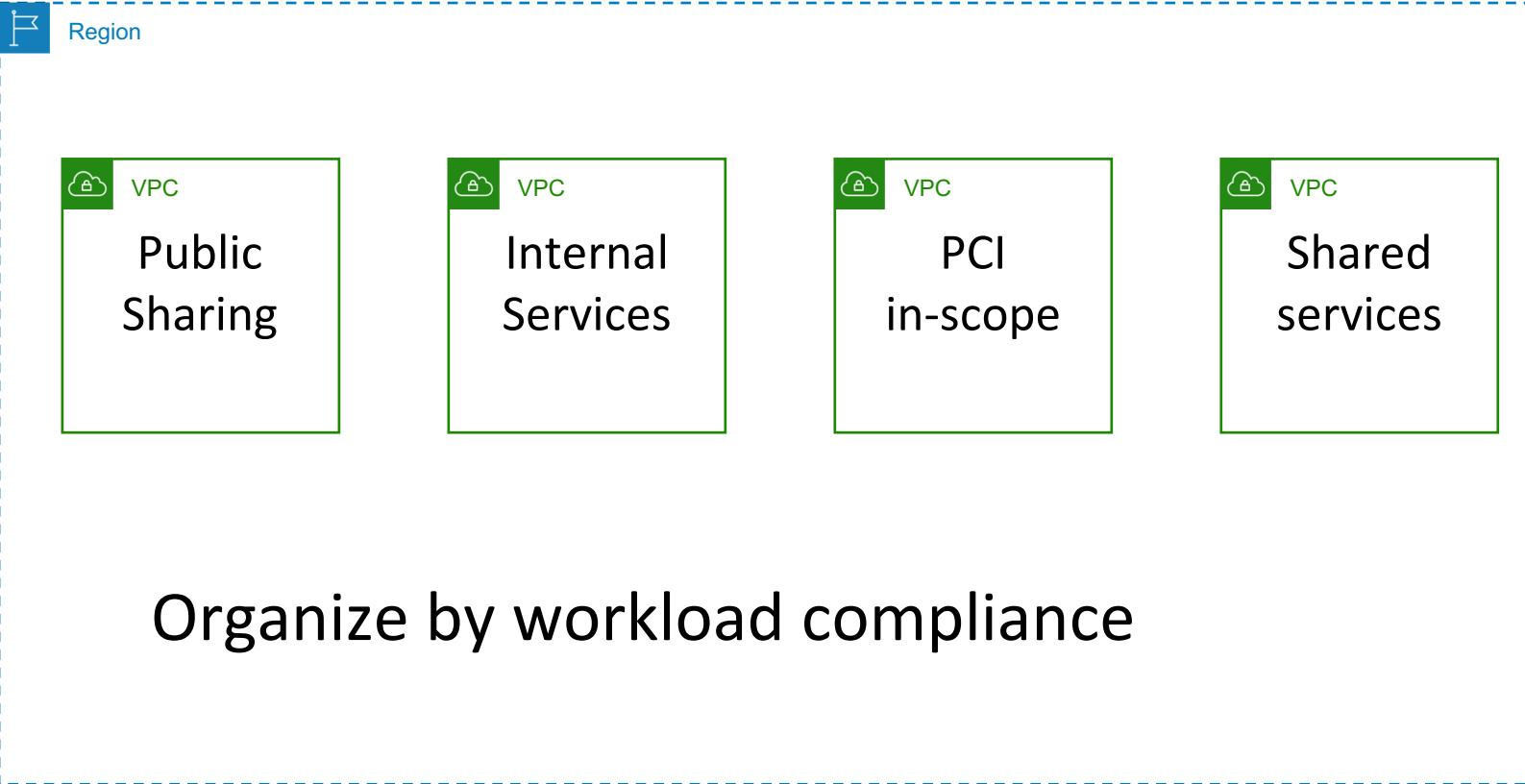
Network Security - Multiple VPC

- Same region
- Different region
- Different account
- Transit gateway

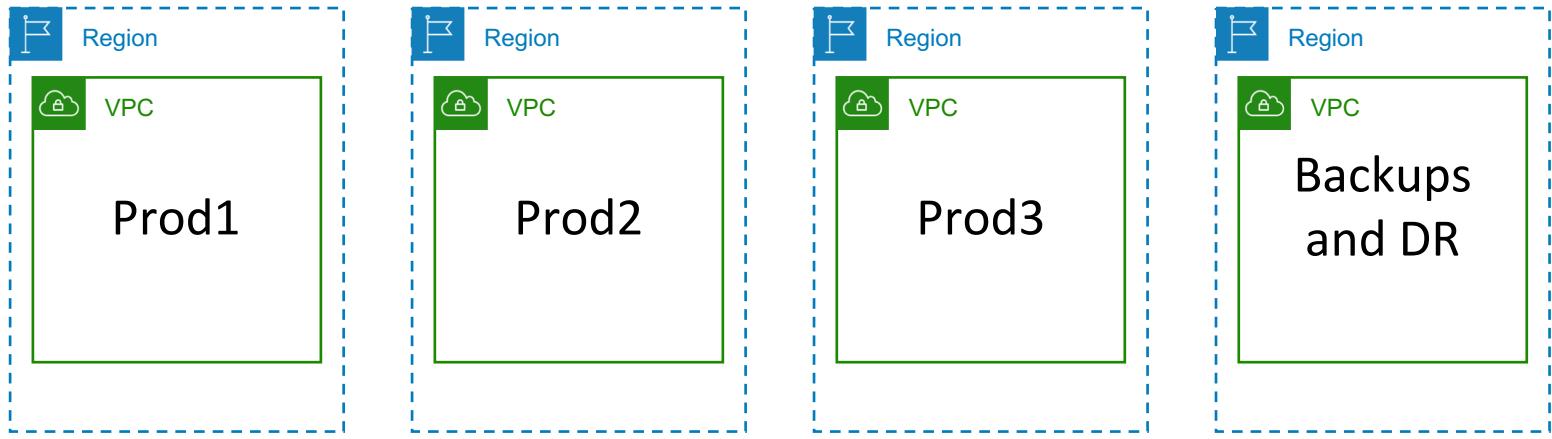
Multiple VPC - Same Region



Multiple VPC - Same Region

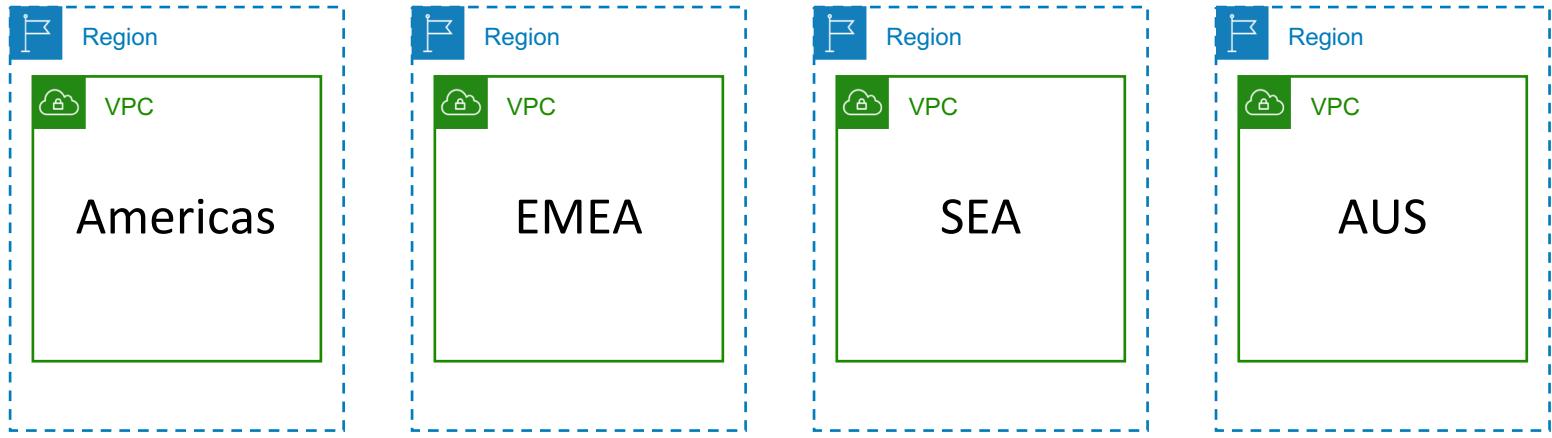


Multiple VPC - Different Region



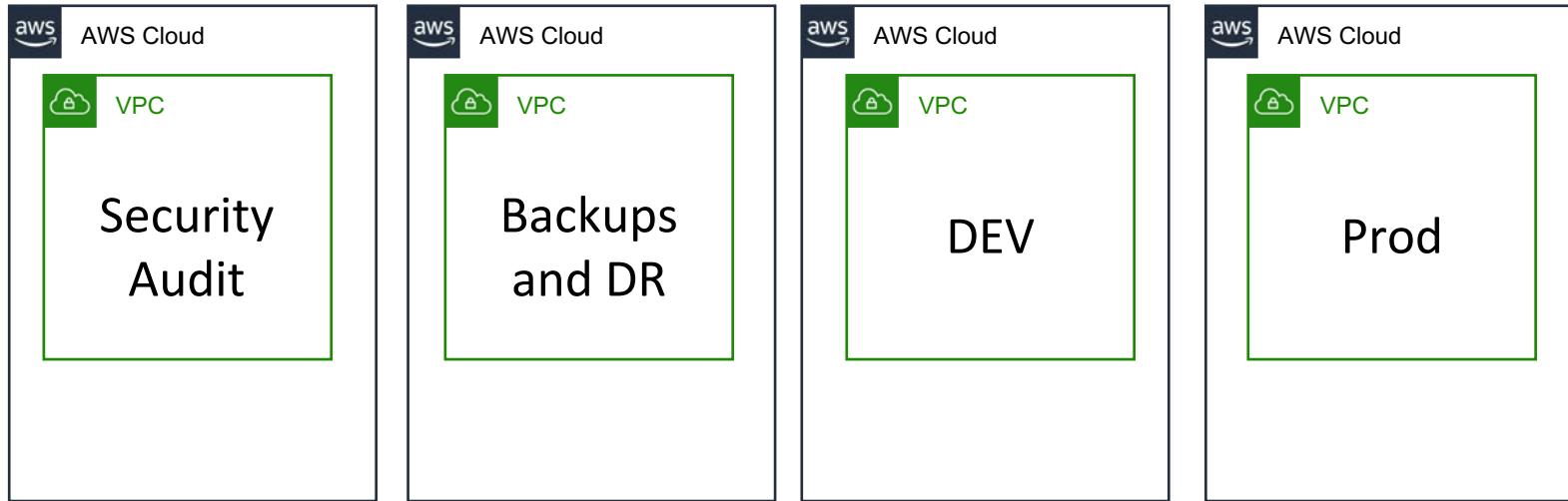
Organize by availability requirements

Multiple VPC - Different Region



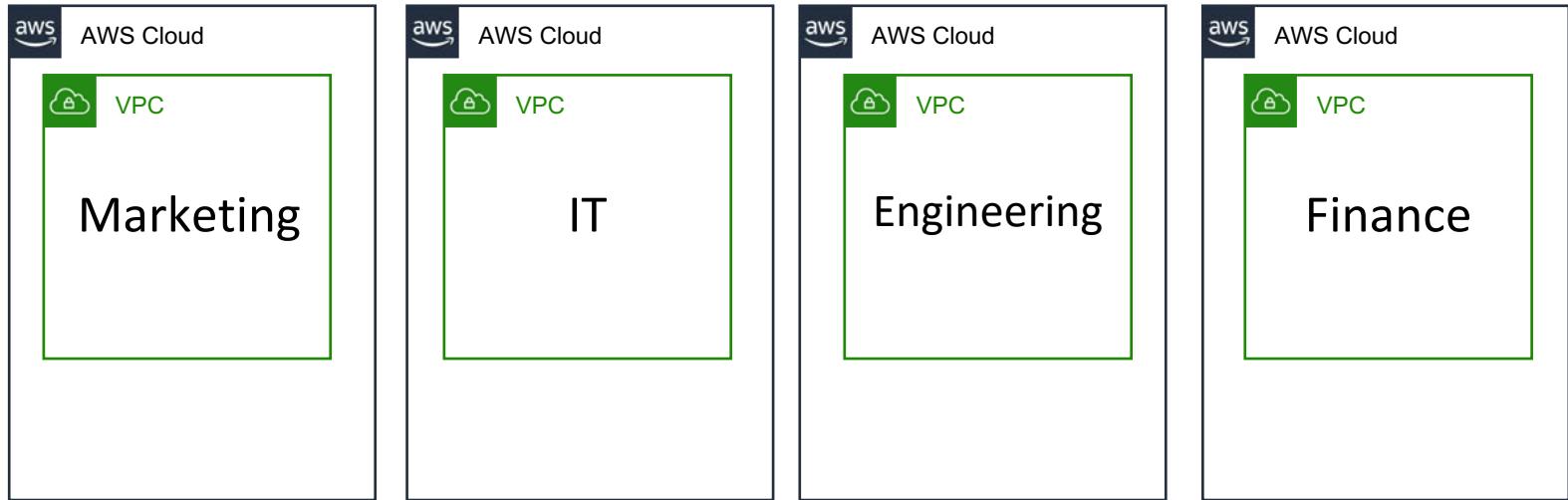
Organize by locality requirements

Multiple VPC - Different Account



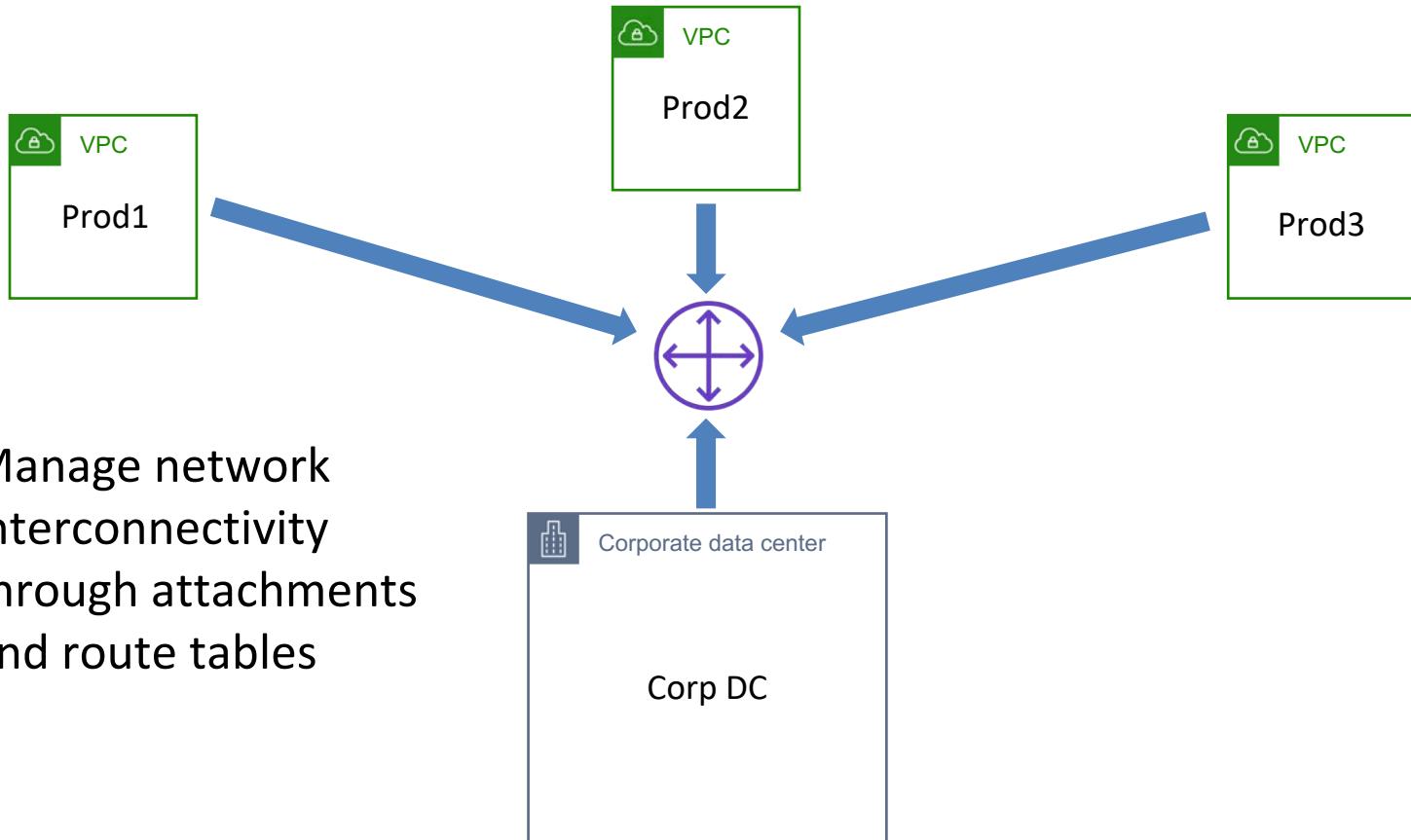
Organize by security requirements

Multiple VPC - Different Account



Organize to match company hierarchy

Multiple VPC - Transit Gateway



Multiple VPC - Considerations

- More Security Groups
- More NACL
- More route tables (use Transit Gateway)
- More routes
- More egress points
- Higher operational overhead



AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

Your R&D team is designing a new application which will consist of multiple tiers as follows:

Customer-facing: Web front-end accessible by browser (ports 80/443)

REST API: Application front-end available to client apps and partners (port 443)

Application: Business logic implementation (port 8080)

Database: Relational data (port 3306)

Both the customer-facing and REST API tiers need access to the application tier, and only the application tier needs access to the database. Each tier is launched into dedicated subnets.

Which combination of **security group** and **NACL rules** would be part of a **least-privilege network security configuration?** (pick four)

Question Breakdown - Answers

- A. NACL: deny ALL outbound from Customer-facing to Database subnets
- B. SG: allow ALL tcp inbound from REST API SG to Application SG
- C. SG: allow inbound 3306 from Application subnets to DB subnets
- D. NACL: deny ALL inbound from REST API to Database
- E. SG: remove default outbound rule from all SG
- F. NACL: allow ALL tcp inbound and outbound to Customer-facing subnets

Question Breakdown - Answers

This is good practice, and ensures no direct access to the DB from the web tier

- A. NACL: deny ALL outbound from Customer-facing to Database subnets
- B. SG: allow ALL tcp inbound from REST API SG to Application SG
- C. SG: allow inbound 3306 from Application subnets to DB subnets
- D. NACL: deny ALL inbound from REST API to Database
- E. SG: remove default outbound rule from all SG
- F. NACL: allow ALL tcp inbound and outbound to Customer-facing subnets

Question Breakdown - Answers

Any time you're allowing ALL inbound, you should look for ways to restrict to a range or single port

- A. NACL: deny ALL outbound from Customer-facing to Database subnets
- B. SG: allow ALL tcp inbound from REST API SG to Application SG
- C. SG: allow inbound 3306 from Application subnets to DB subnets
- D. NACL: deny ALL inbound from REST API to Database
- E. SG: remove default outbound rule from all SG
- F. NACL: allow ALL tcp inbound and outbound to Customer-facing subnets

Question Breakdown - Answers

This is similar to allowing inbound 3306 from the app SG, but reduces the lookup time for new connections

- A. NACL: deny ALL outbound from Customer-facing to Database subnets
- B. SG: allow ALL tcp inbound from REST API SG to Application SG
- C. SG: allow inbound 3306 from Application subnets to DB subnets
- D. NACL: deny ALL inbound from REST API to Database
- E. SG: remove default outbound rule from all SG
- F. NACL: allow ALL tcp inbound and outbound to Customer-facing subnets

Question Breakdown - Answers

This is a good practice, and ensures all DB traffic flows through the app tier

- A. NACL: deny ALL outbound from Customer-facing to Database subnets
- B. SG: allow ALL tcp inbound from REST API SG to Application SG
- C. SG: allow inbound 3306 from Application subnets to DB subnets
- D. NACL: deny ALL inbound from REST API to Database
- E. SG: remove default outbound rule from all SG
- F. NACL: allow ALL tcp inbound and outbound to Customer-facing subnets

Question Breakdown - Answers

While it may increase complexity by requiring outbound rules, this increases overall security

- A. NACL: deny ALL outbound from Customer-facing to Database subnets
- B. SG: allow ALL tcp inbound from REST API SG to Application SG
- C. SG: allow inbound 3306 from Application subnets to DB subnets
- D. NACL: deny ALL inbound from REST API to Database
- E. SG: remove default outbound rule from all SG
- F. NACL: allow ALL tcp inbound and outbound to Customer-facing subnets

Question Breakdown - Answers

This is the default configuration. If the web tier only allows 80/443, it would be good to restrict this NACL to match

- A. NACL: deny ALL outbound from Customer-facing to Database subnets
- B. SG: allow ALL tcp inbound from REST API SG to Application SG
- C. SG: allow inbound 3306 from Application subnets to DB subnets
- D. NACL: deny ALL inbound from REST API to Database
- E. SG: remove default outbound rule from all SG
- F. NACL: allow ALL tcp inbound and outbound to Customer-facing subnets

Question Breakdown - Correct Answer

Correct Answer:A,C,D,E

- A. NACL: deny ALL outbound from Customer-facing to Database subnets
- B. SG: allow ALL tcp inbound from REST API SG to Application SG
- C. SG: allow inbound 3306 from Application subnets to DB subnets
- D. NACL: deny ALL inbound from REST API to Database
- E. SG: remove default outbound rule from all SG
- F. NACL: allow ALL tcp inbound and outbound to Customer-facing subnets

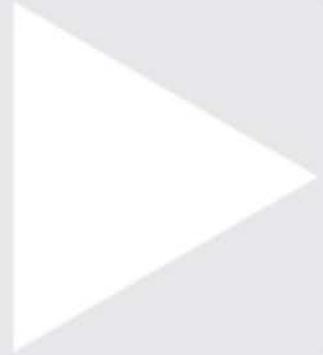


AWS Certified Security - Specialty Crash Course

Infrastructure Security Part II 26%

Question Domain Main Points

1. Troubleshoot a secure network infrastructure
2. Design and implement host-based security



Infrastructure Security Part II

Troubleshoot a secure network infrastructure

Network Troubleshooting Scenarios

- Traffic rejected between A and B
- Application cannot contact dependency
- User cannot modify network resource

Network Troubleshooting Scenarios

Traffic rejected between A and B

- Security group rules (inbound/outbound)
- NACL rules (inbound/outbound)
- Route table entries (with correct target)
- Resource level permissions
 - S3 bucket policy
- Physical data center firewall
- Host-based firewall
- VPC DIY firewall

Network Troubleshooting Scenarios

Application cannot contact dependency

- Application level permissions
- VPC security features (see prev slide)
- Failed authentication

Network Troubleshooting Scenarios

User cannot modify network resource

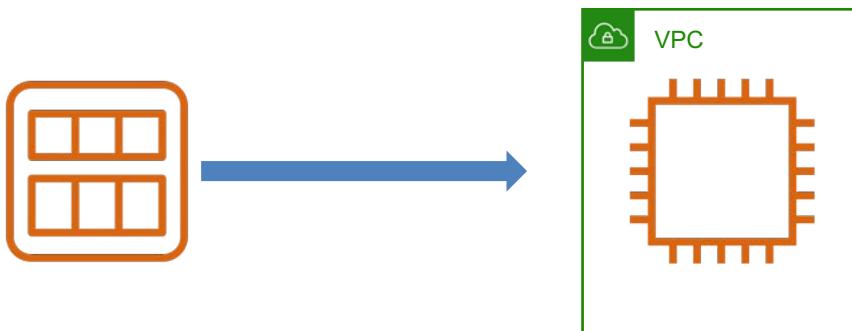
- User permissions
 - IAM Policy
- Account permissions
 - AWS Organizations SCP
- Compliance automation
 - Config rule to detect changes
 - Lambda function to revert changes
 - CloudFormation drift detection



Infrastructure Security Part II

Design and implement host-based security

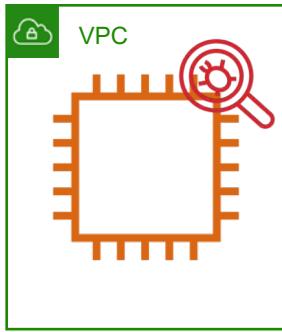
Host-based Security



- OS Firewall
- Disable unneeded services
- Remove insecure packages
- AWS monitoring
- Third-party monitoring
- Restrict user access
- Immutable OS

Implement additional security

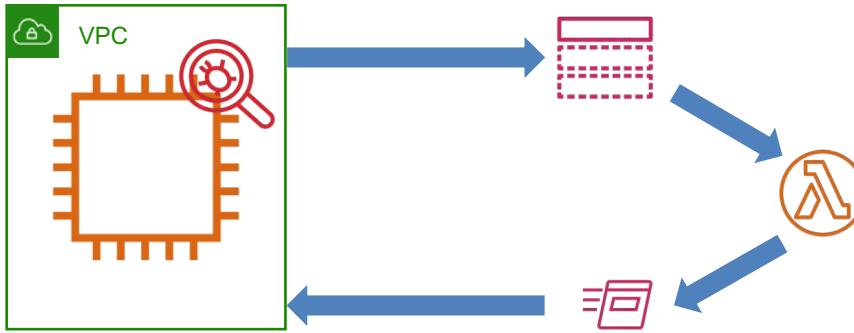
Host-based Security



- Install Inspector Agent
- Create SNS topic
- Configure assessment template
- Schedule assessment runs
- Execute assessment

Use Amazon Inspector

Host-based Security



- Finding posted to SNS
- Lambda parses finding
- Lambda invokes SSM Run Command
- Run Command installs patch on EC2 instance

Automatically remediate findings



AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

A company has recently completed a number of improvements to their network security. Some of the modifications included **removing the Internet Gateway** and **implementing Gateway VPC endpoints for S3** access from inside the VPC. An application that was previously functional is now **unable to access S3**. Which of the following troubleshooting steps would NOT identify the root cause?

- A. Analyze the Network ACL rules associated with the application subnets
- B. Analyze the route table associated with the application subnets
- C. Analyze the bucket policy associated with the S3 bucket
- D. Analyze the application security group inbound rules
- E. Analyze the application security group outbound rules

Question Breakdown - Answers

NACL rules must be permissive in both directions for the traffic to flow

- A. Analyze the Network ACL rules associated with the application subnets
- B. Analyze the route table associated with the application subnets
- C. Analyze the bucket policy associated with the S3 bucket
- D. Analyze the application security group inbound rules
- E. Analyze the application security group outbound rules

Question Breakdown - Answers

The VPC endpoint requires a route table entry for functionality

- A. Analyze the Network ACL rules associated with the application subnets
- B. **Analyze the route table associated with the application subnets**
- C. Analyze the bucket policy associated with the S3 bucket
- D. Analyze the application security group inbound rules
- E. Analyze the application security group outbound rules

Question Breakdown - Answers

The S3 bucket must allow access for functionality

- A. Analyze the Network ACL rules associated with the application subnets
- B. Analyze the route table associated with the application subnets
- C. **Analyze the bucket policy associated with the S3 bucket**
- D. Analyze the application security group inbound rules
- E. Analyze the application security group outbound rules

Question Breakdown - Answers

Security group inbound rules will not impact ability to reach S3 through the Gateway VPC endpoint

- A. Analyze the Network ACL rules associated with the application subnets
- B. Analyze the route table associated with the application subnets
- C. Analyze the bucket policy associated with the S3 bucket
- D. **Analyze the application security group inbound rules**
- E. Analyze the application security group outbound rules

Question Breakdown - Answers

Security group outbound rules must be permissive enough to allow the application to reach S3

- A. Analyze the Network ACL rules associated with the application subnets
- B. Analyze the route table associated with the application subnets
- C. Analyze the bucket policy associated with the S3 bucket
- D. Analyze the application security group inbound rules
- E. **Analyze the application security group outbound rules**

Question Breakdown - Correct Answer

Correct Answer:D

- A. Analyze the Network ACL rules associated with the application subnets
- B. Analyze the route table associated with the application subnets
- C. Analyze the bucket policy associated with the S3 bucket
- D. Analyze the application security group inbound rules
- E. Analyze the application security group outbound rules



AWS Certified Security - Specialty Crash Course

Identity and Access Management
20%

Question Domain Main Points

1. Design and implement a scalable authorization and authentication system to access AWS resources
2. Troubleshoot an authorization and authentication system to access AWS resources

Definitions and Keywords

Authentication

- Proof of identity
- User/pass
- Keys
- MFA
- Federation

Authorization

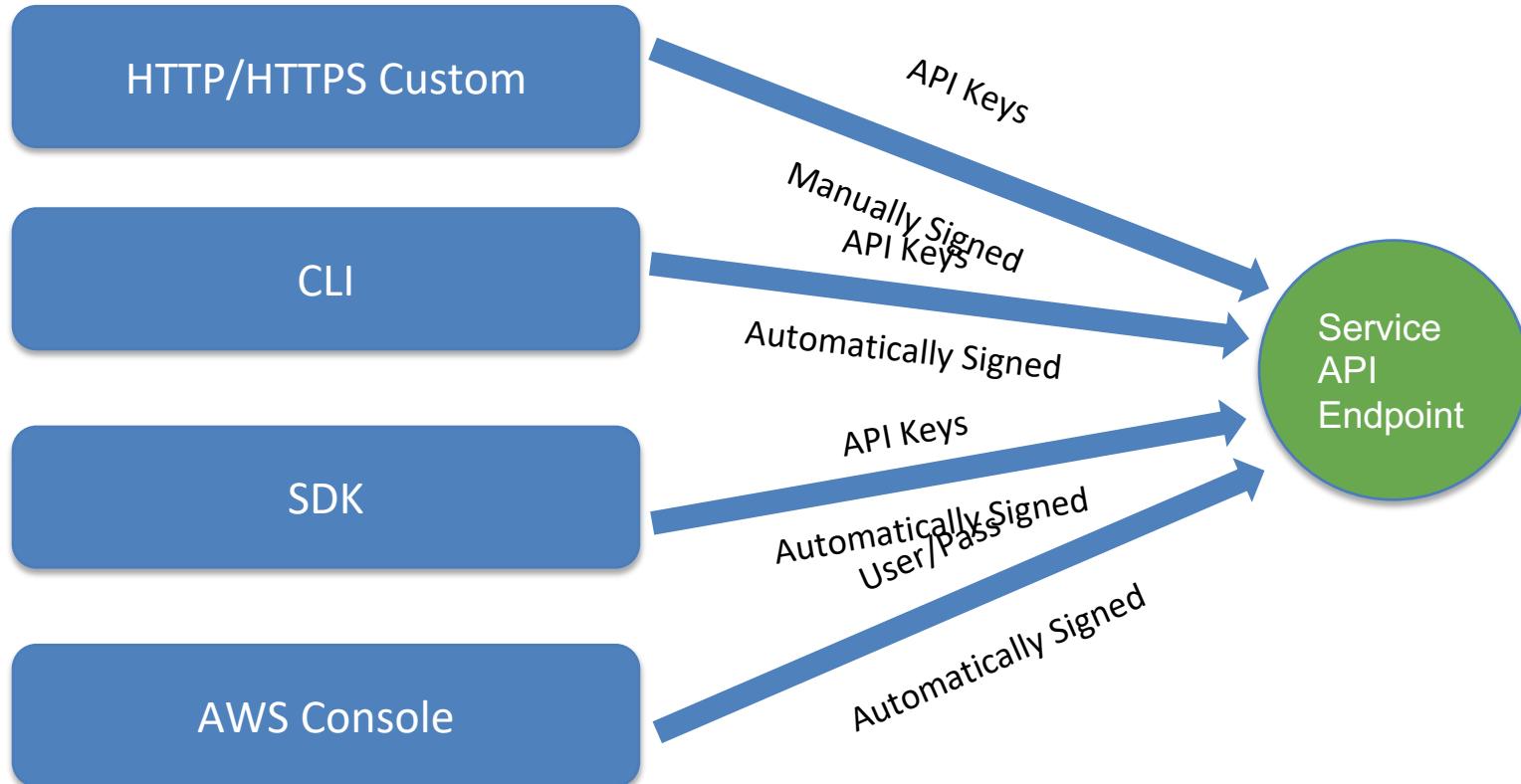
- Permissions for actions
- User-based access control
- Resource-based access control
- Implicit deny



Identity and Access Management

IAM Policies and IAM Roles

How To Access AWS - Direct



How To Access AWS - Other

Cross-service API calls = IAM Role & STS

SAML Federation = IAM Role & STS

QuickSight/Cognito = Email address

WorkMail/WorkSpaces = AWS Directory Service

AWS SSO = AWS Directory Service

Benefits of Signing Requests

Authentication - prove identity

Avoid tampering (MitM)

Avoid replays (wireshark/tcpdump)

Anatomy of an IAM Policy

Version	Action
Id	NotAction
Statement	Resource
Sid	NotResource
Effect	Condition
Principal	
NotPrincipal	

IAM Policy Study Focus

Version

Id

Statement

Sid

Effect

Principal

NotPrincipal

Action

NotAction

Resource

NotResource

Condition

IAM Policy Reference

Version

Policy language version, and should be static

Default: **2012-10-17**

Previous: **2008-10-17**

IAM Policy Reference

Id

Optional identifier for the policy

Only required by some services

Recommended value: UUID

IAM Policy Reference

Statement

Main policy element

All the logic is placed in here

All other values are placed in here

IAM Policy Reference

Sid

Optional identifier for the statement

Only required by some services

Not directly exposed in the IAM API

IAM Policy Reference

Effect

Determines whether the policy results in an explicit allow or explicit deny

Required element

Valid values: **allow** and **deny**

Both values are in scope for the exam!

IAM Policy Reference

Principal

The entity that is allowed or denied access to the resource

This is where it gets interesting!

IAM Policy Reference

Principal

1 or more specific AWS accounts

1 or more IAM users

Federated users (web identity)

Federated users (SAML)

Principal Options

IAM Policy Reference

Principal

IAM Role

Specific assumed-role user

AWS service

Everyone (anonymous users)

Principal
Options

IAM Policy Reference

notPrincipal

Same concept as Principal

Use for exceptions

Easier than defining a long list

Learn the
NOTs

IAM Policy Reference

notPrincipal

Avoid using with Allow statements

Use with Deny to implement least privilege policies

IAM Policy Reference

Action

Specific action or actions that can be allowed or denied

Each service has different actions

Combine actions from multiple services

IAM Policy Reference

Action

Everything in AWS

Everything in a single service

Named actions in a single service

Named actions in multiple services

Wildcards using *

Principal Options

IAM Policy Reference

notAction

Same concept as Action

Use for exceptions

Easier than defining a long list

IAM Policy Reference

notAction

Use with Allow statements for allowing all except specific actions

Use with Deny statements for shorter least-privilege policies

IAM Policy Reference

Resource

Object or objects that are covered by
the statement

Always specified using ARN

IAM Policy Reference

Resource

All resources

Specific resource

Not all services support resources

IAM Policy Reference

notResource

Same concept as Resource

Use for exceptions

Easier than defining a long list

IAM Policy Reference

notResource

Use carefully

Can grant or deny access in an
unintentional manner

IAM Policy Reference

Condition

Specify conditions for when a policy is in effect

Condition key names are case insensitive

Some conditions are service specific

This is where policies get complicated

IAM Policy Reference

Condition

Exact match

Partial match

Negated match

String
Condition

IAM Policy Reference

Condition

Exact match

Negated match

Inequality

Numeric
Condition

IAM Policy Reference

Condition

Exact date/time

Negated date/time

Before a specific date/time

After a specific date/time

Date
Condition

IAM Policy Reference

Condition

Evaluate statement as true or false

Another way to evaluate strings

One way to force SSL transport

Boolean
Condition

IAM Policy Reference

Condition

Test key values in binary format
Compare value to base-64 encoded
binary value in policy

Binary Condition

IAM Policy Reference

Condition

Compare against IPv4 or IPv6
CIDR format required

IP Address
Condition

IAM Policy Reference

Condition

Case sensitive match of any or all elements of ARN

Negated match of ARN

Not supported by all services

ARN Condition

IAM Policy Reference

Condition

Add as postfix to other conditions
Checks if the key exists as part of another check

...IfExists
Condition

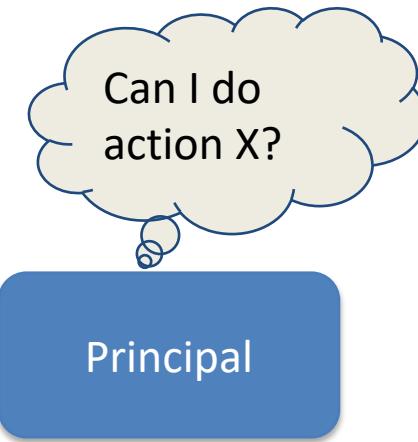
IAM Policy Reference

Condition

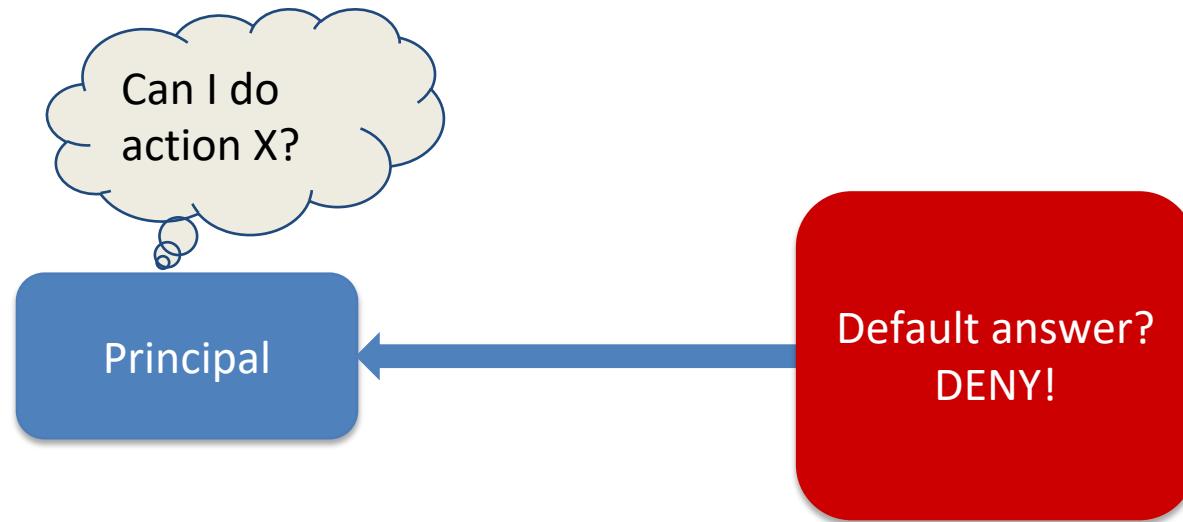
Checks if the key exists as a standalone check

Null Check

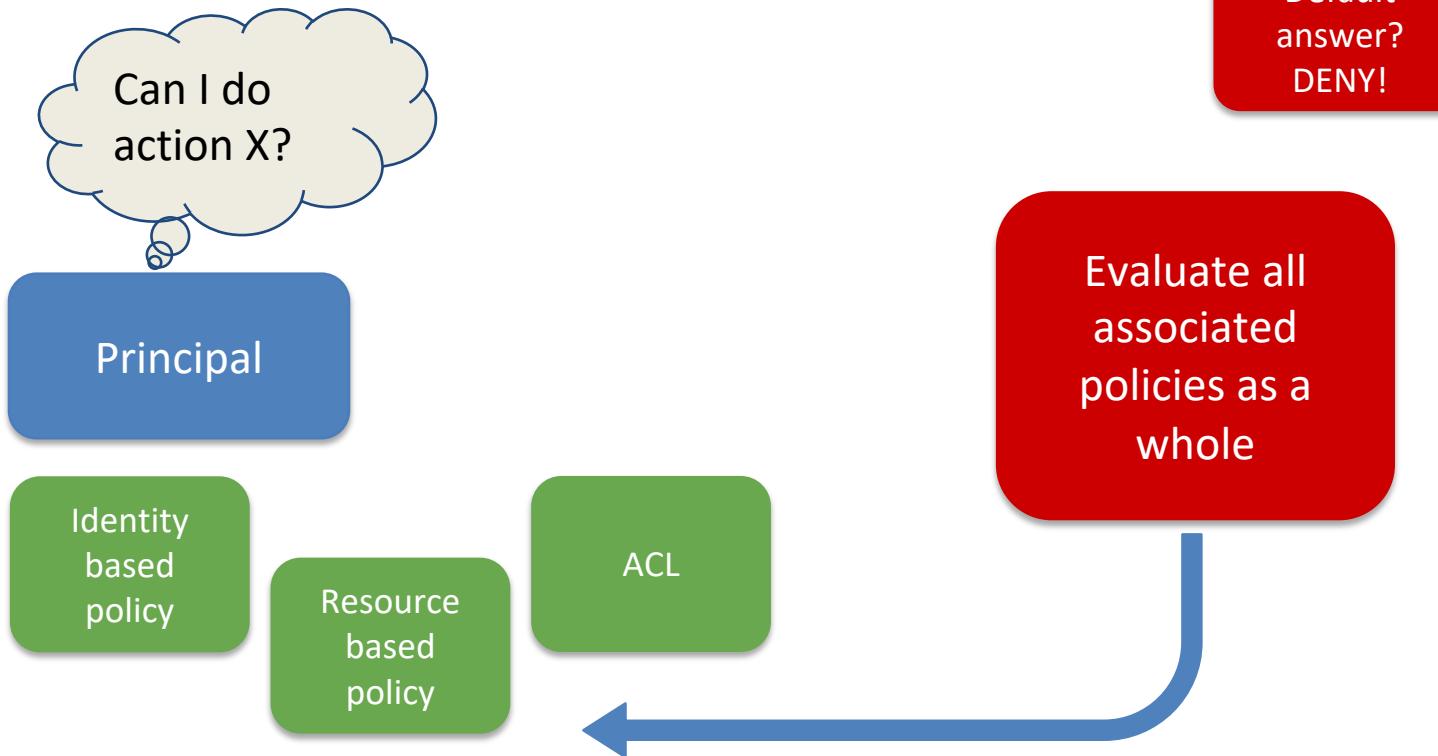
IAM Policy Evaluation



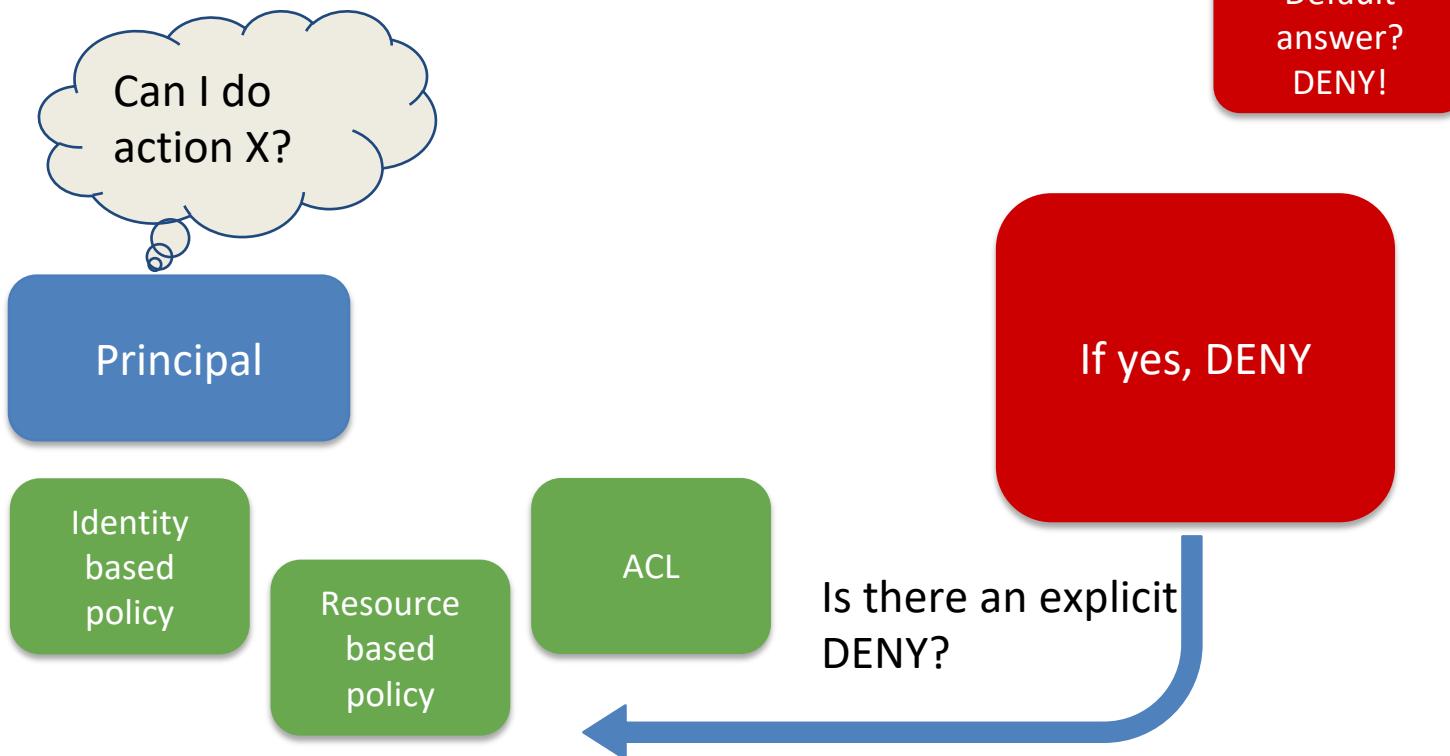
IAM Policy Evaluation



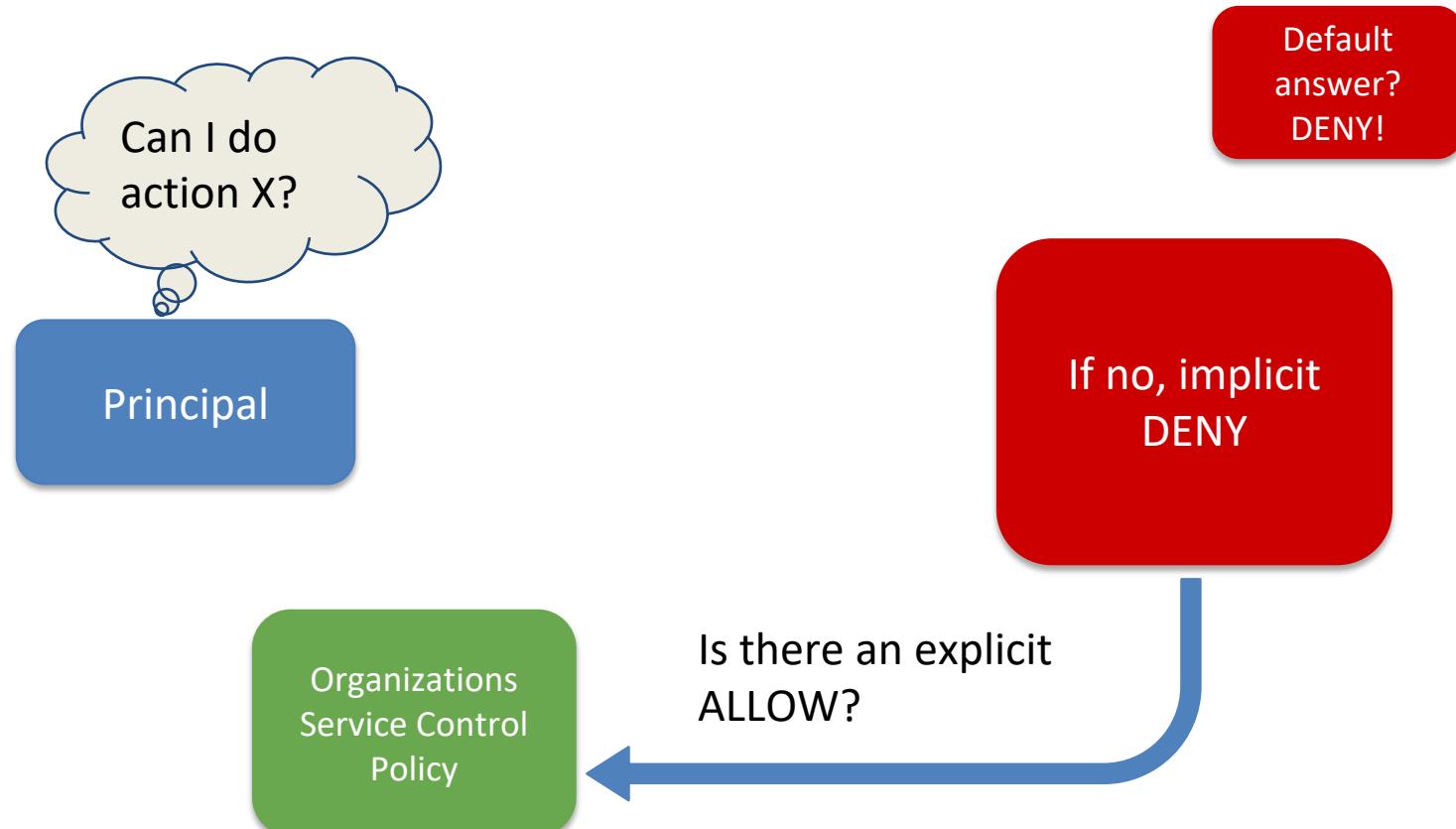
IAM Policy Evaluation



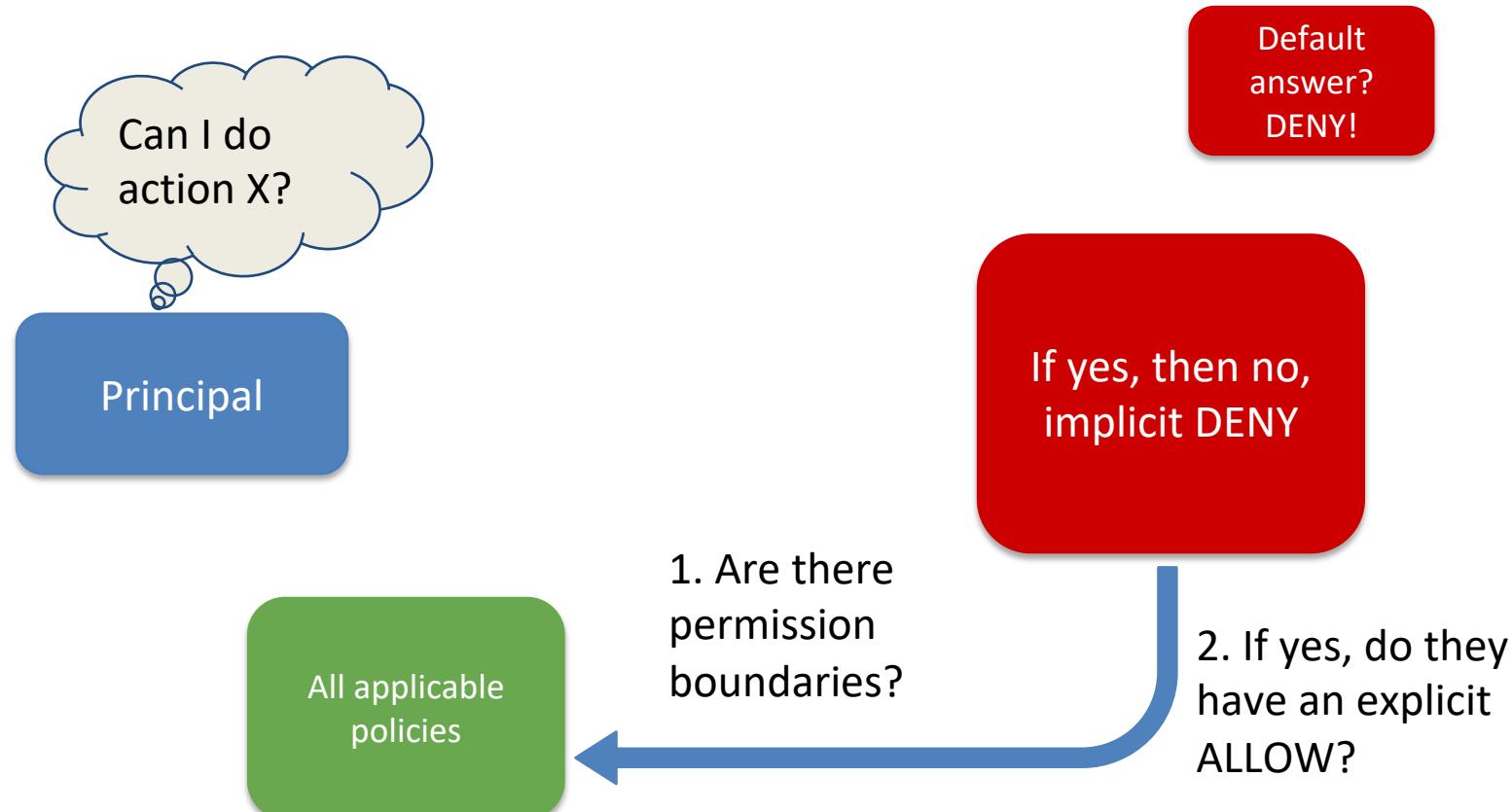
IAM Policy Evaluation



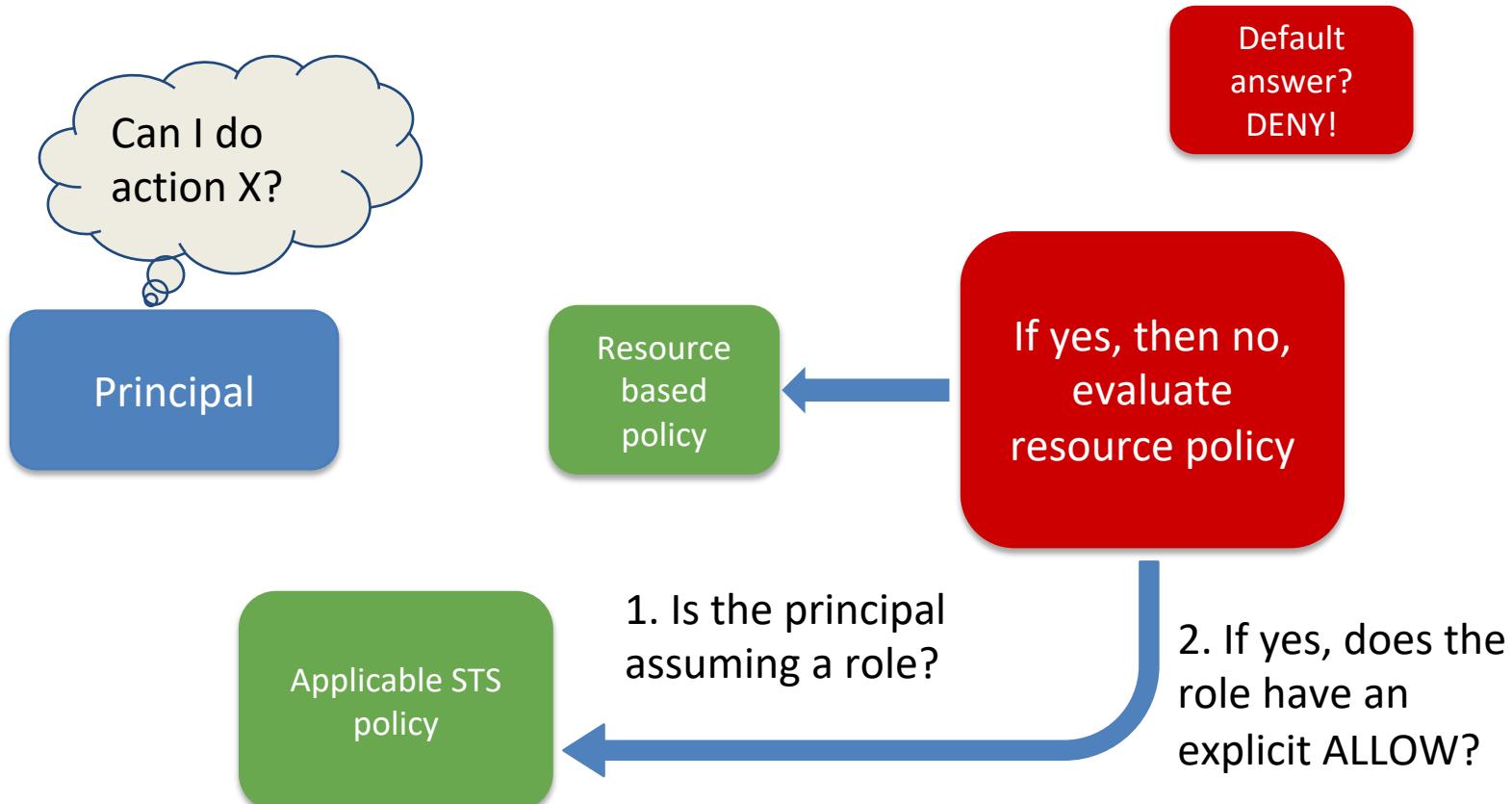
IAM Policy Evaluation



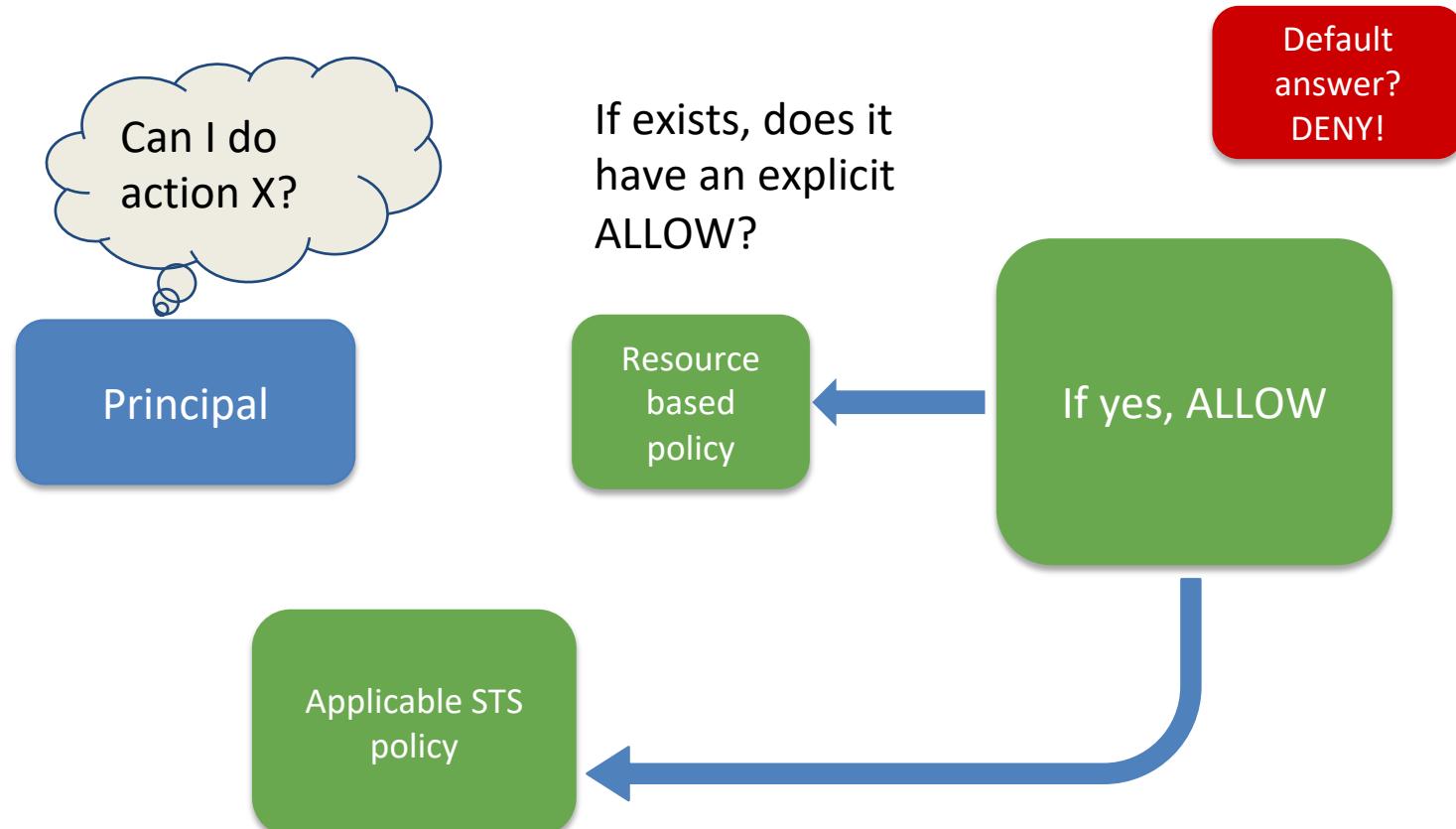
IAM Policy Evaluation



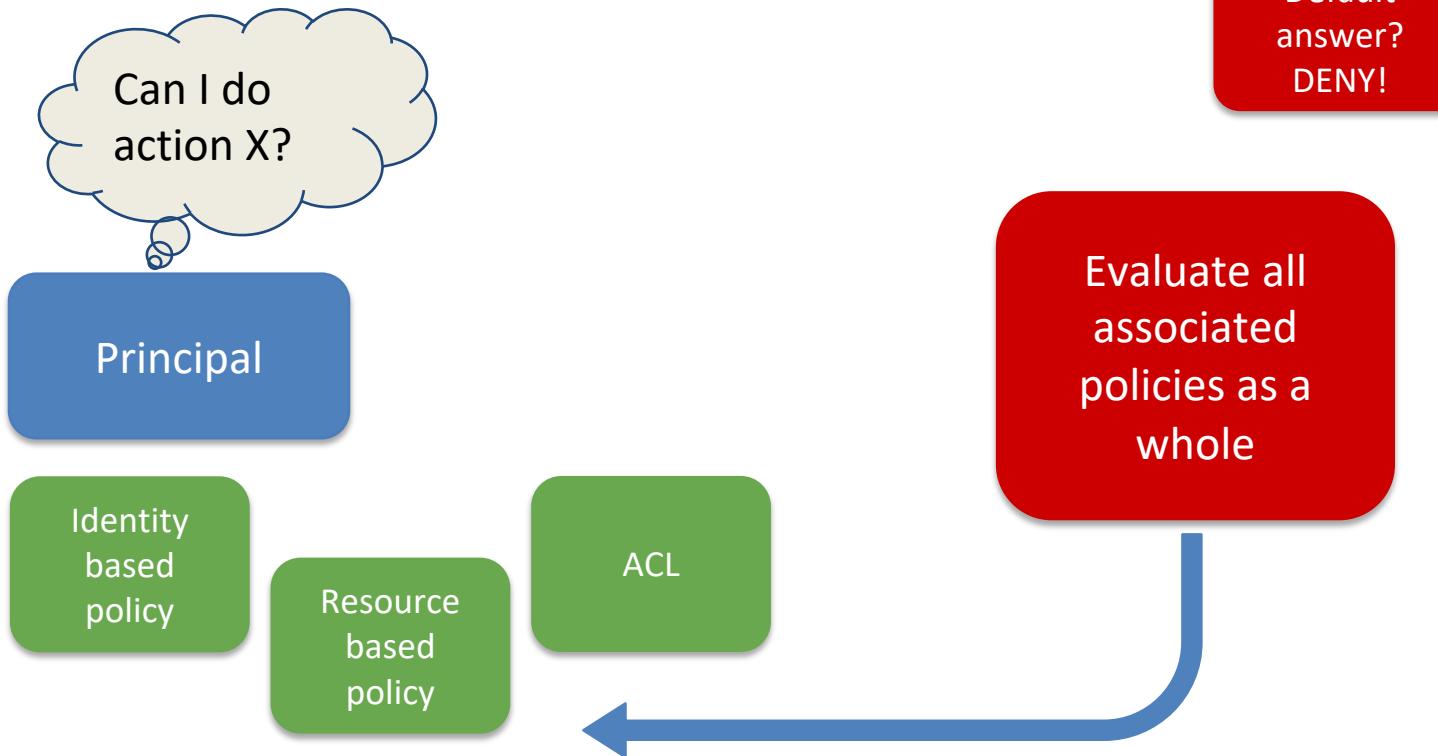
IAM Policy Evaluation



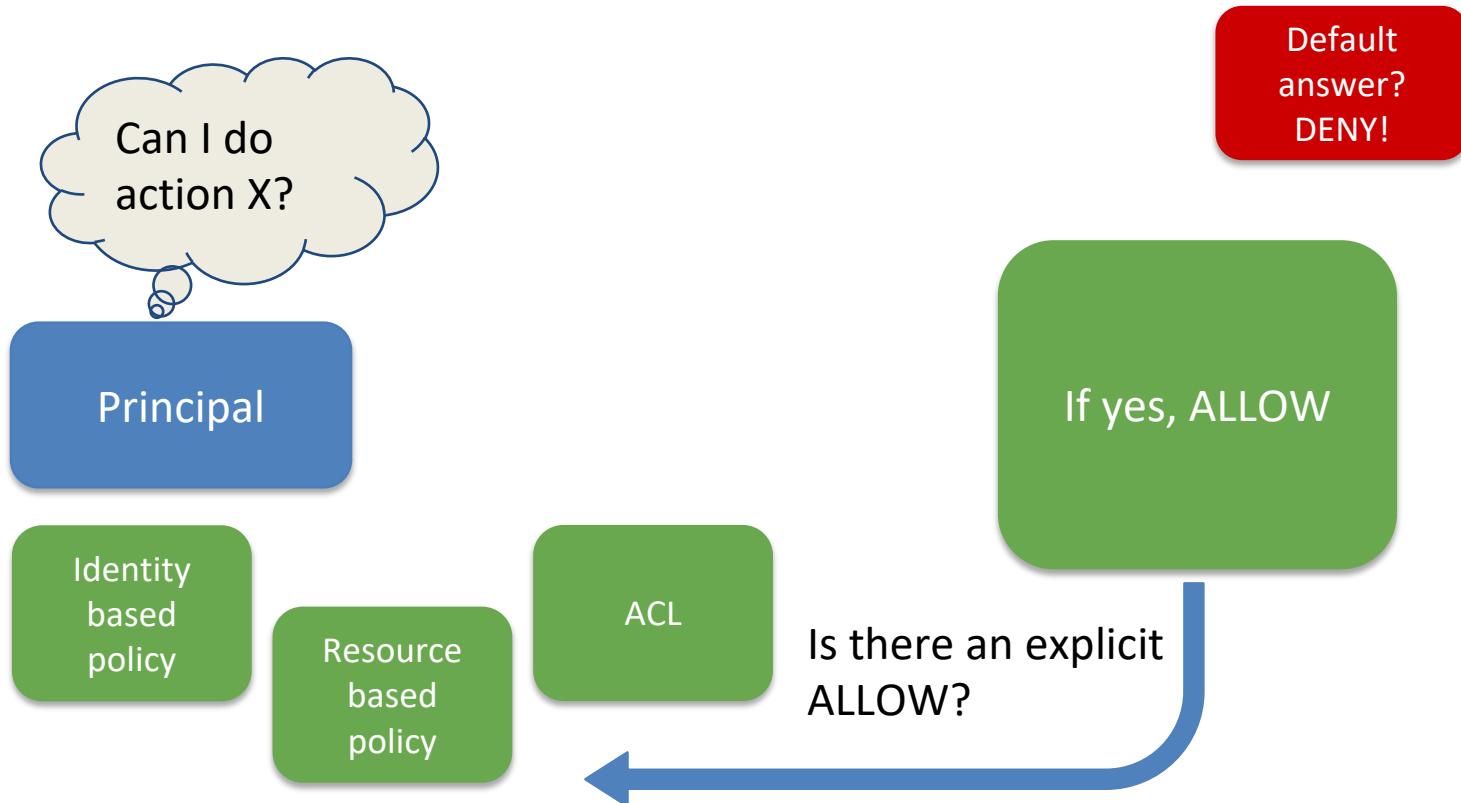
IAM Policy Evaluation



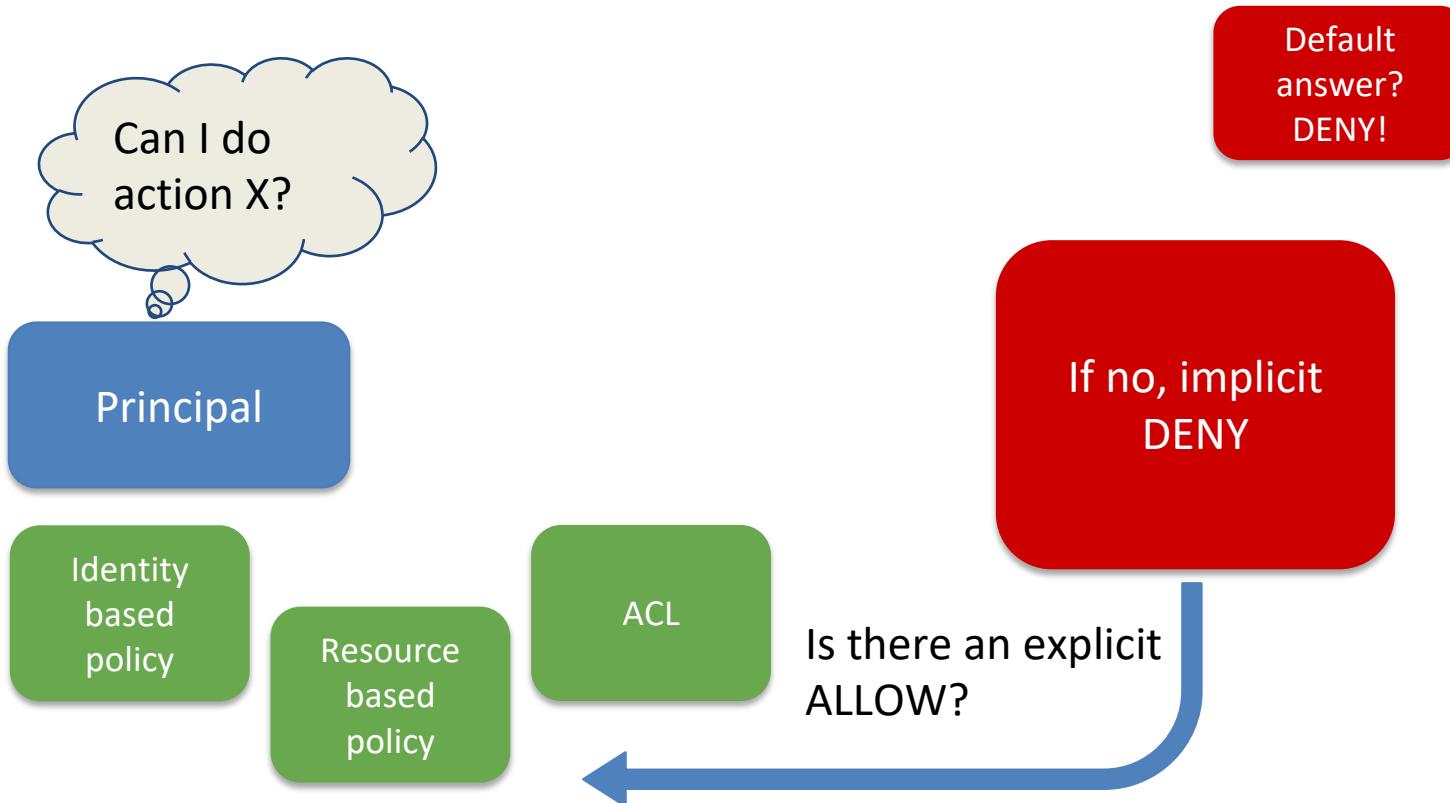
IAM Policy Evaluation



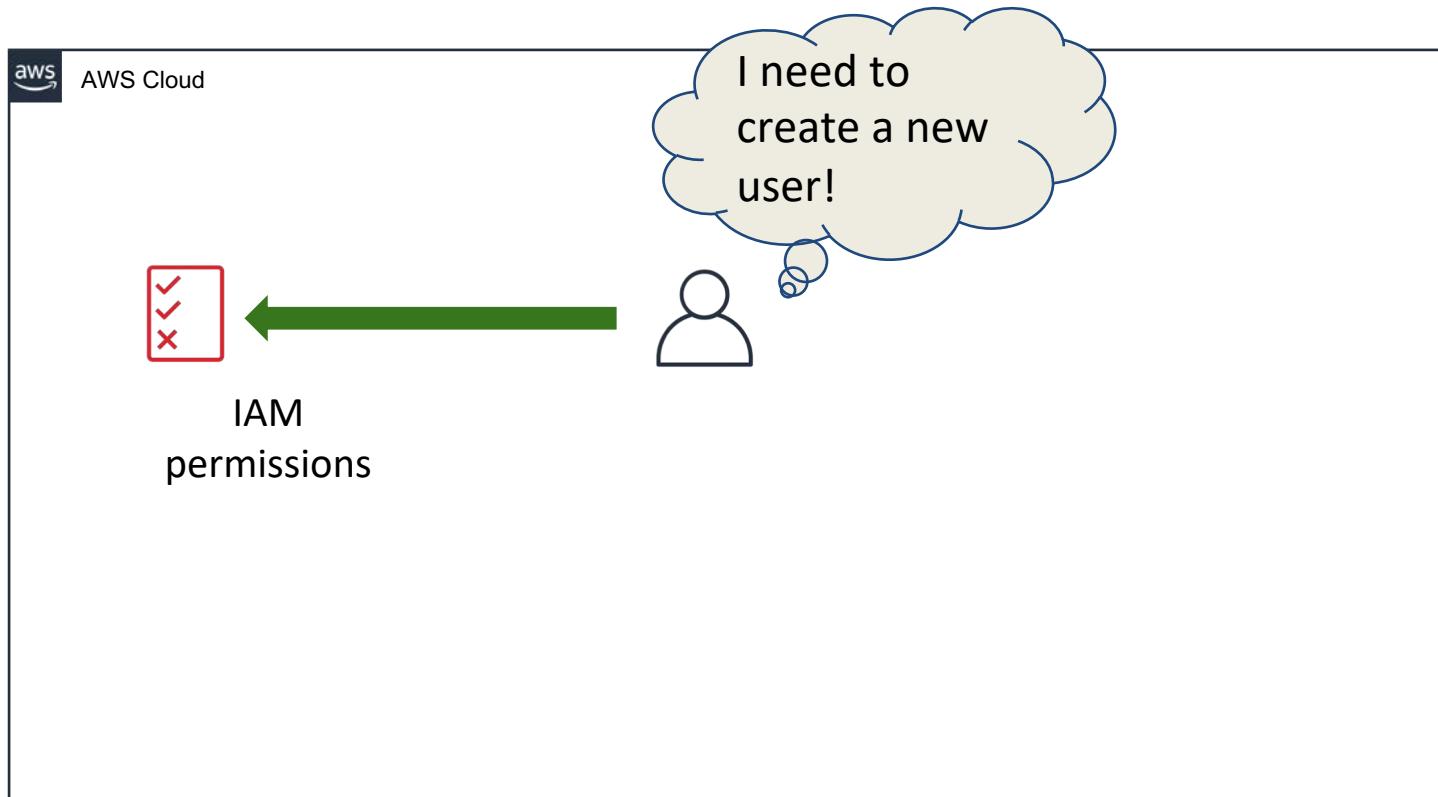
IAM Policy Evaluation



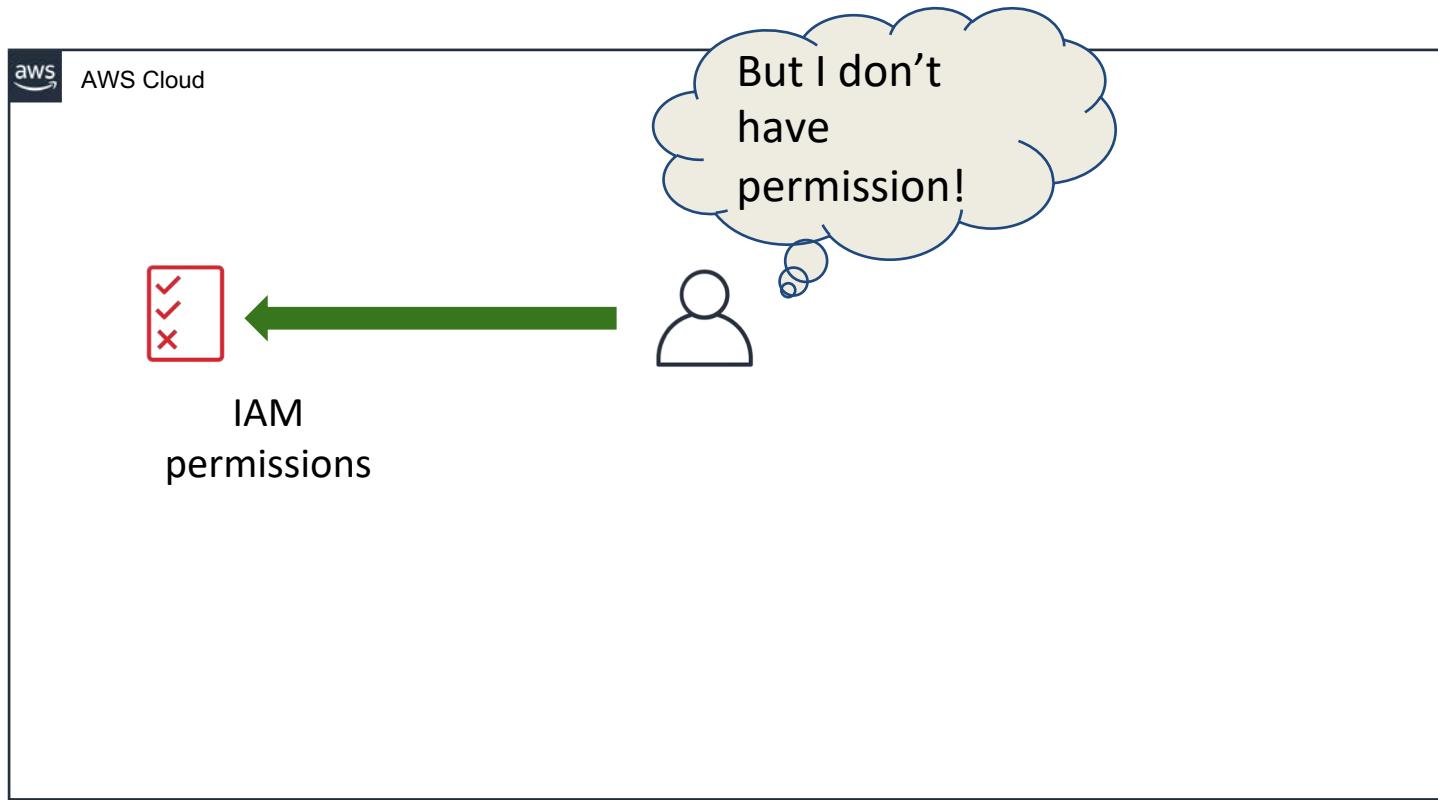
IAM Policy Evaluation



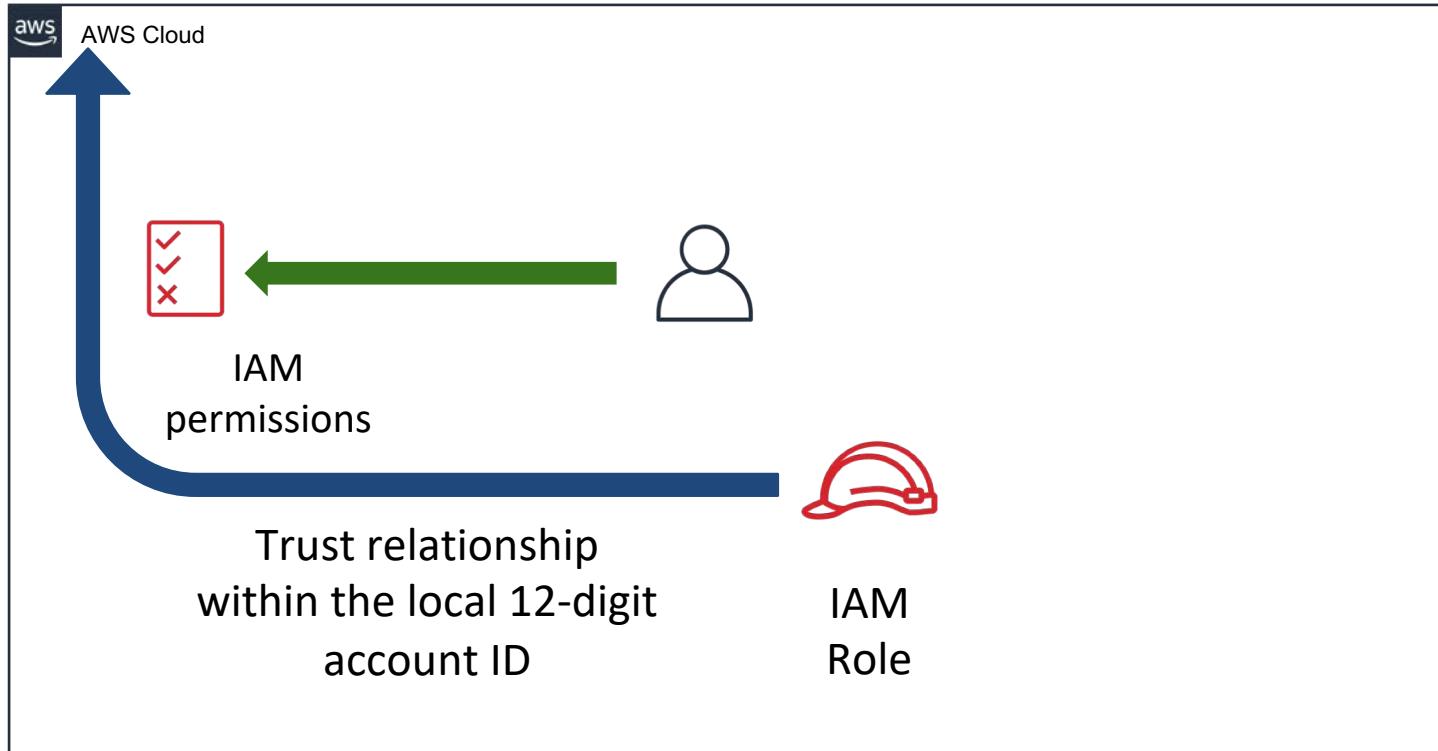
IAM Role To Elevate Privileges



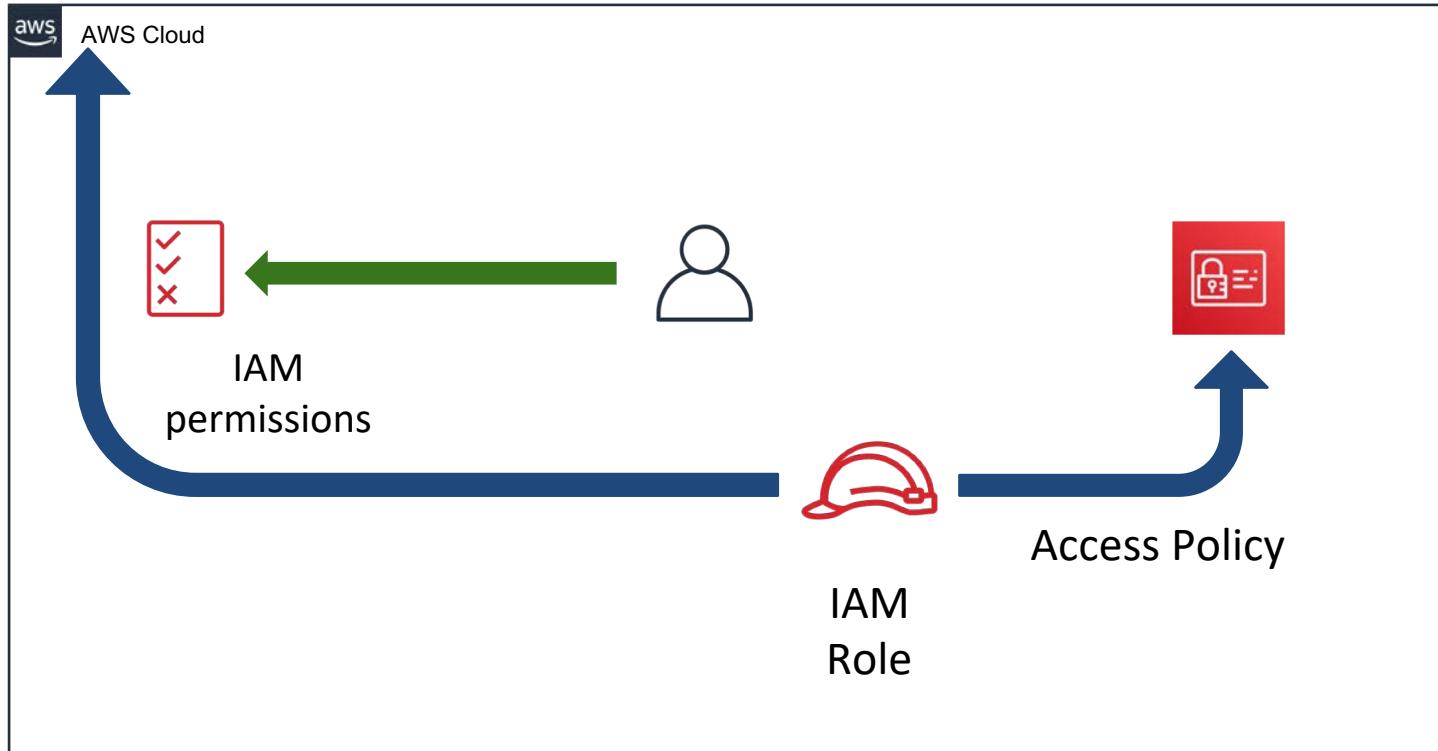
IAM Role To Elevate Privileges



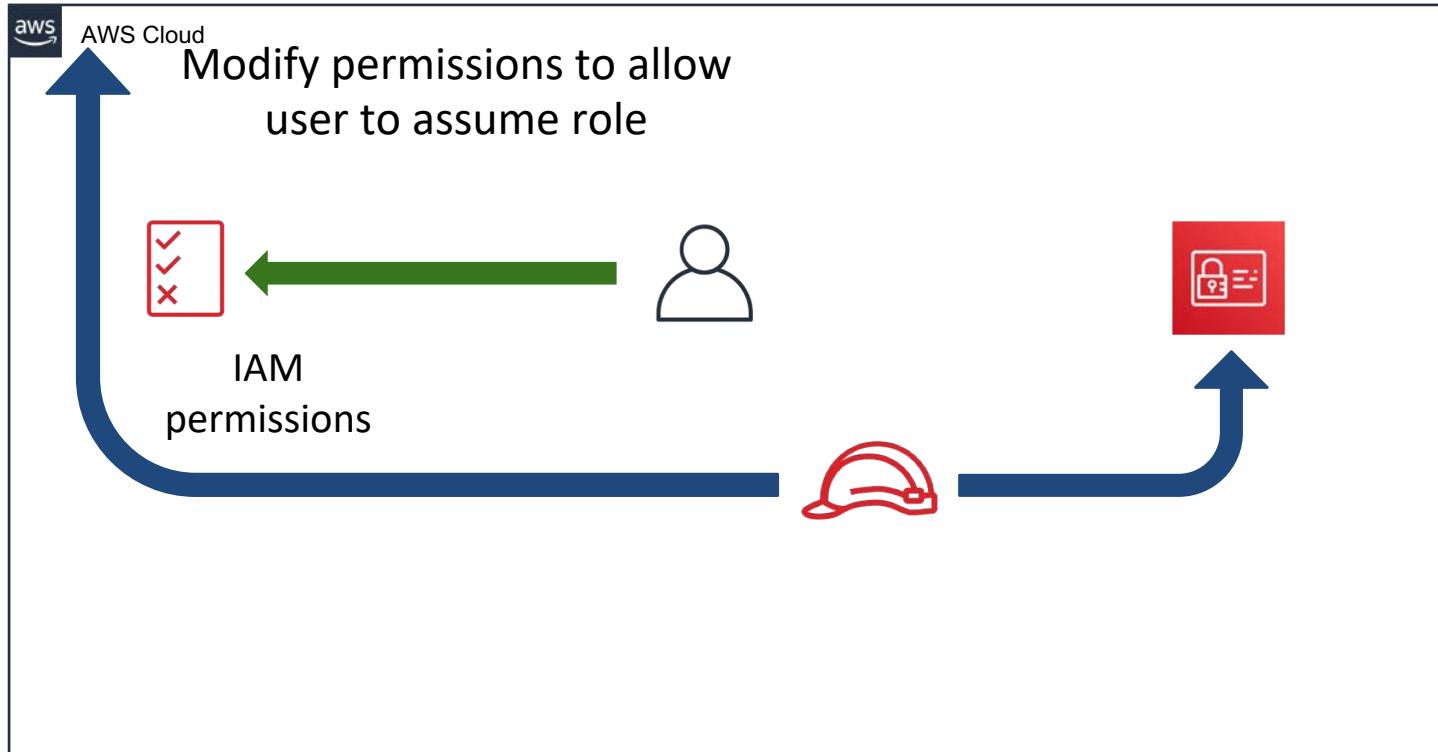
IAM Role To Elevate Privileges



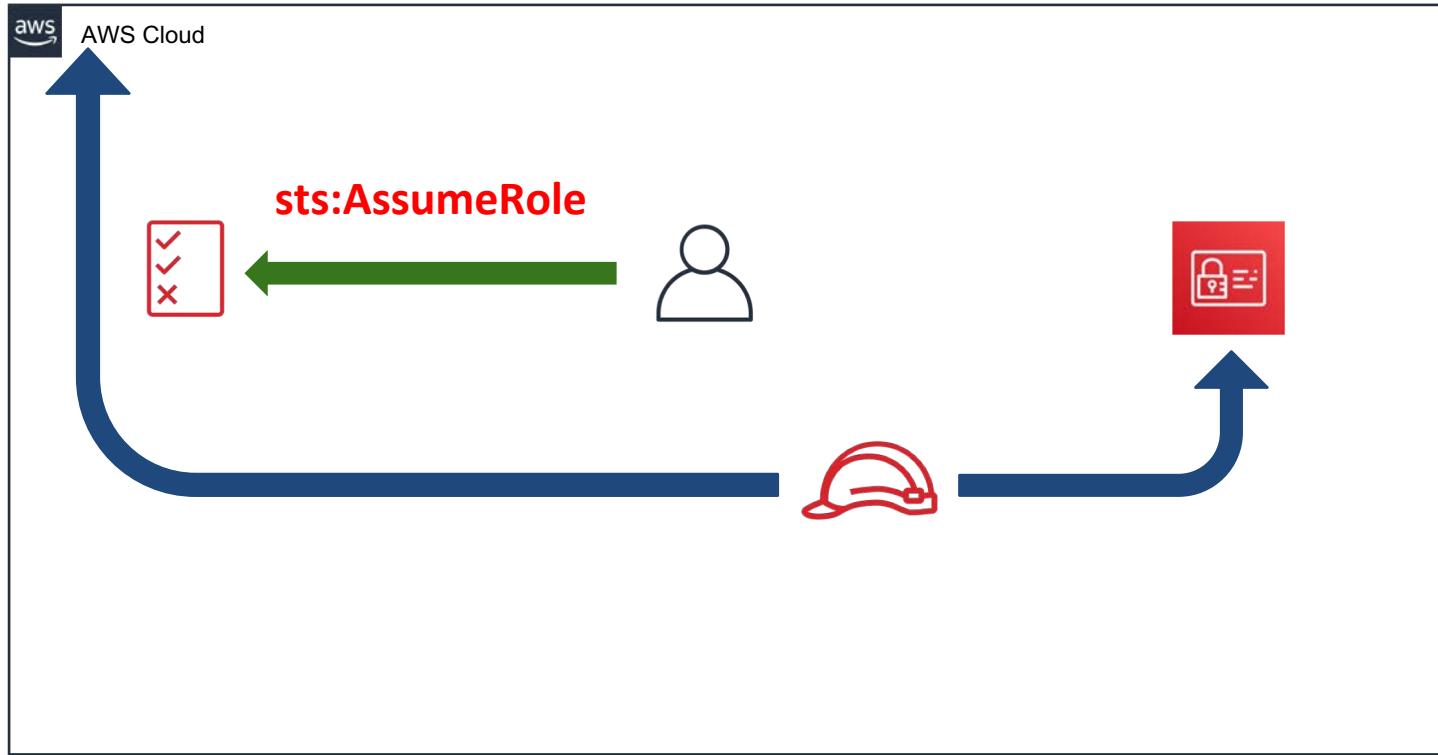
IAM Role To Elevate Privileges



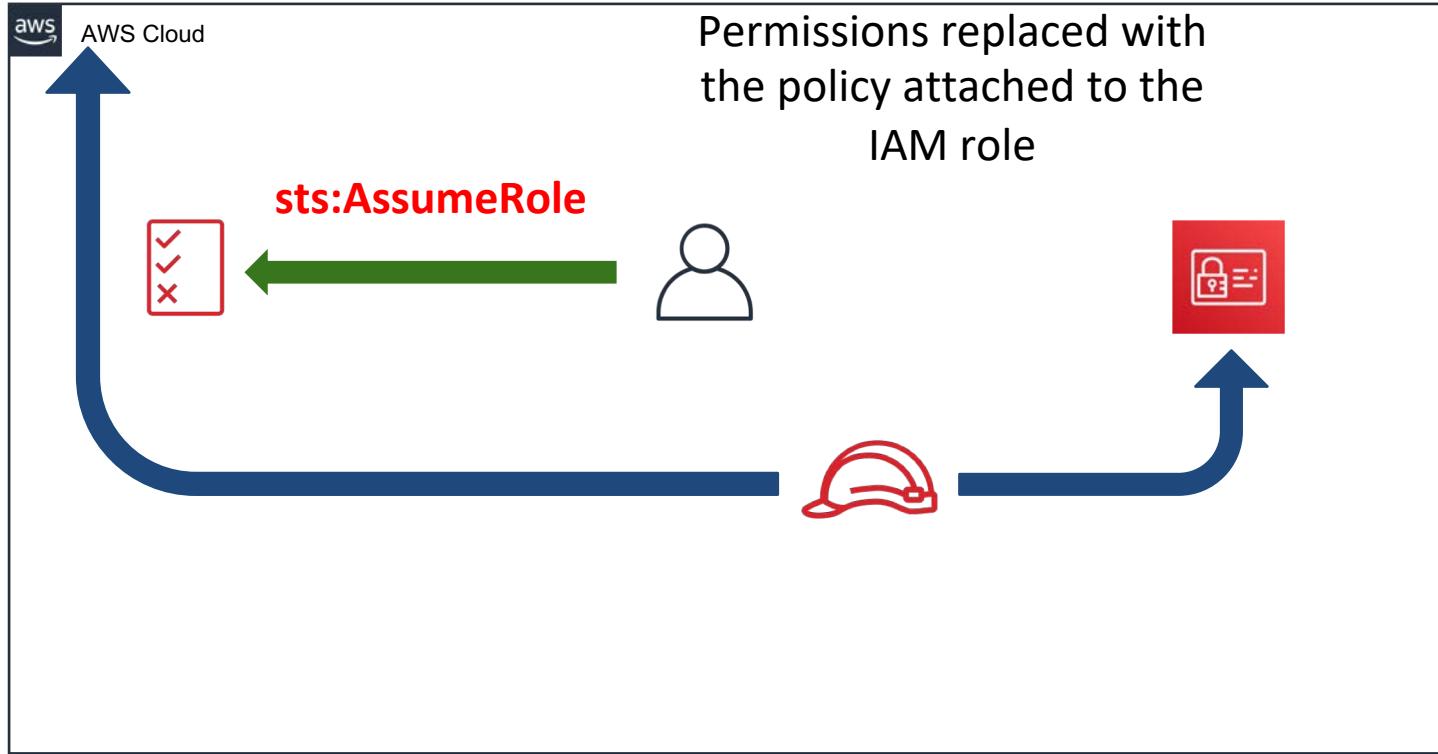
IAM Role To Elevate Privileges



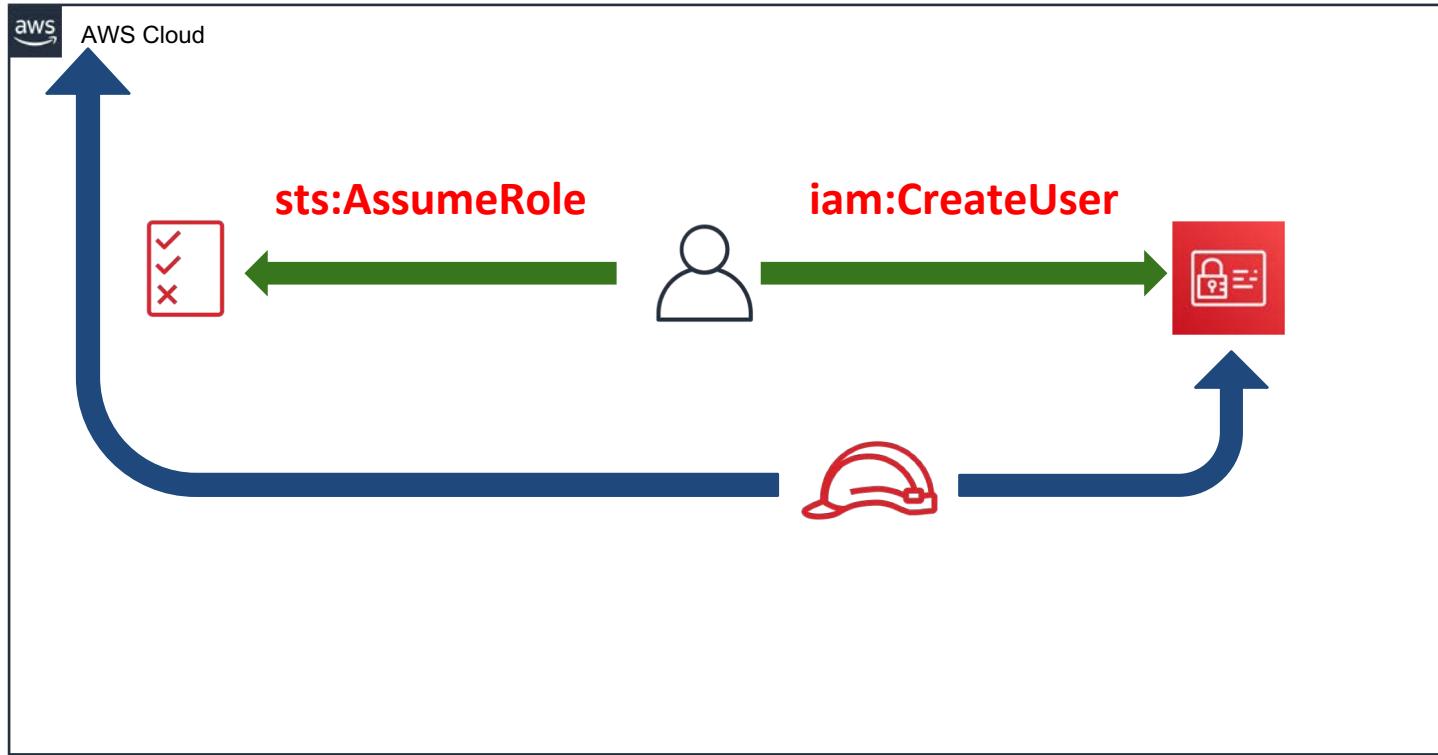
IAM Role To Elevate Privileges



IAM Role To Elevate Privileges



IAM Role To Elevate Privileges



IAM Role for Cross Account

- External ID
 - Optional string supplied during role assumption
 - Helps prevent unauthorized access through trusted account
- Trust relationship is with entire remote account
 - Not specific IAM resource

Service-Linked IAM Roles

- Allow services to call each other
- Predefined by service
- Options (depends on service)
 - Create automatically (assumes privileges)
 - Create as part of wizard
 - Create manually (or programmatically)
- Cannot attach permissions policy to any other entity



AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

Your company has recently signed a partnership agreement to **share data** with another company. The data is stored in an **S3 bucket**, and the partner is also using AWS. Which of the following are required to configure **least-privilege access** for the partner? (select all that apply)

- A. Create IAM policy in partner account granting access to assume our IAM role
- B. Create S3 bucket ACL on our bucket granting full access to the partner account ID
- C. Create IAM policy in our account granting appropriate access to the S3 bucket in question
- D. Create IAM role in our account with trust for partner account and external ID, then attach an IAM policy with S3 access
- E. Create an IAM user in our account with full access to S3 and send credentials to partner



Question Breakdown - Answers

One possible standalone solution

- A. Create IAM policy in partner account granting access to assume our IAM role
- B. Create S3 bucket ACL on our bucket granting full access to the partner account ID
- C. Create IAM policy in our account granting appropriate access to the S3 bucket in question
- D. Create IAM role in our account with trust for partner account and external ID, then attach an IAM policy with S3 access
- E. Create an IAM user in our account with full access to S3 and send credentials to partner

Question Breakdown - Answers

Another possible standalone solution

- A. Create IAM policy in partner account granting access to assume our IAM role
- B. Create S3 bucket ACL on our bucket granting full access to the partner account ID
- C. Create IAM policy in our account granting appropriate access to the S3 bucket in question
- D. Create IAM role in our account with trust for partner account and external ID, then attach an IAM policy with S3 access
- E. Create an IAM user in our account with full access to S3 and send credentials to partner

Question Breakdown - Answers

A possible multi-step solution

- A. Create IAM policy in partner account granting access to assume our IAM role
- B. Create S3 bucket ACL on our bucket granting full access to the partner account ID
- C. Create IAM policy in our account granting appropriate access to the S3 bucket in question
- D. Create IAM role in our account with trust for partner account and external ID, then attach an IAM policy with S3 access
- E. Create an IAM user in our account with full access to S3 and send credentials to partner

Question Breakdown - Answers

Only one solution attempts to handle least privilege

- A. Create IAM policy in partner account granting access to assume our IAM role
- B. Create S3 bucket ACL on our bucket granting full access to the partner account ID
- C. Create IAM policy in our account granting appropriate access to the S3 bucket in question
- D. Create IAM role in our account with trust for partner account and external ID, then attach an IAM policy with S3 access
- E. Create an IAM user in our account with full access to S3 and send credentials to partner

Question Breakdown - Correct Answer

Correct Answer:A,C,D

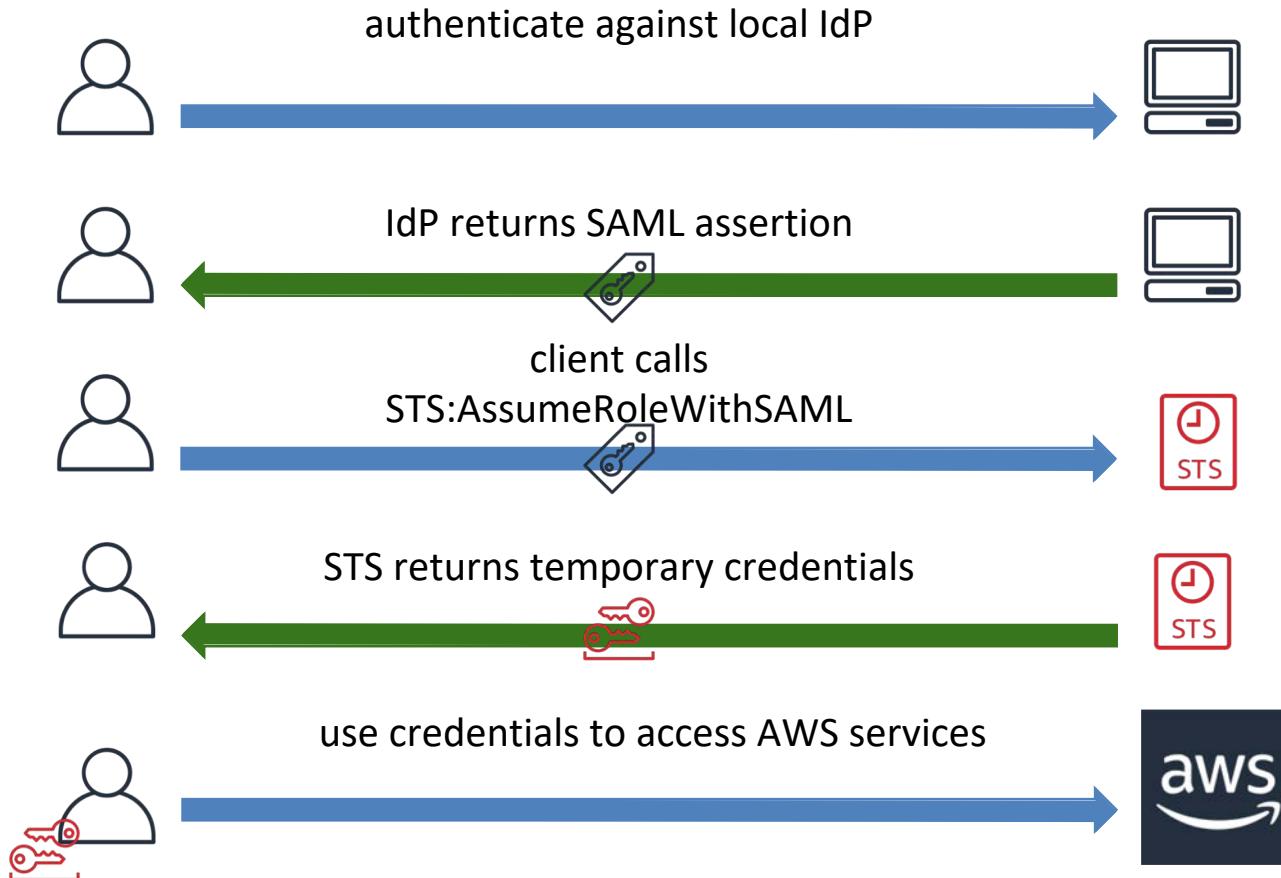
- A. Create IAM policy in partner account granting access to assume our IAM role
- B. Create S3 bucket ACL on our bucket granting full access to the partner account ID
- C. Create IAM policy in our account granting appropriate access to the S3 bucket in question
- D. Create IAM role in our account with trust for partner account and external ID, then attach an IAM policy with S3 access
- E. Create an IAM user in our account with full access to S3 and send credentials to partner



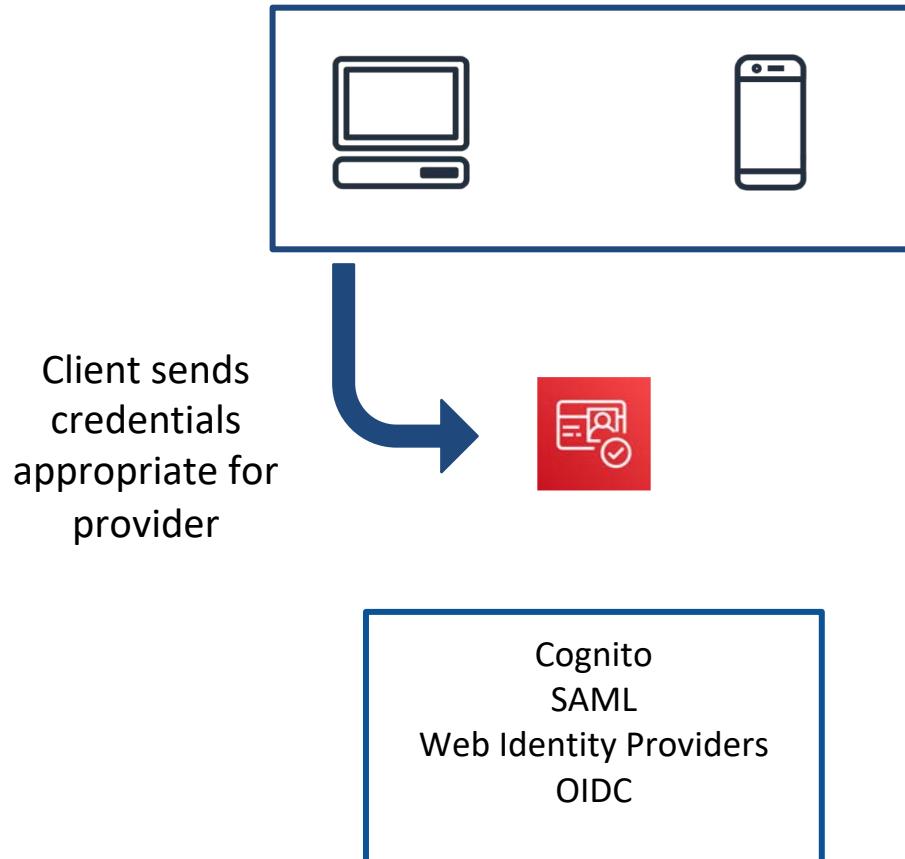
Identity and Access Management

Federation and Resource-based access control

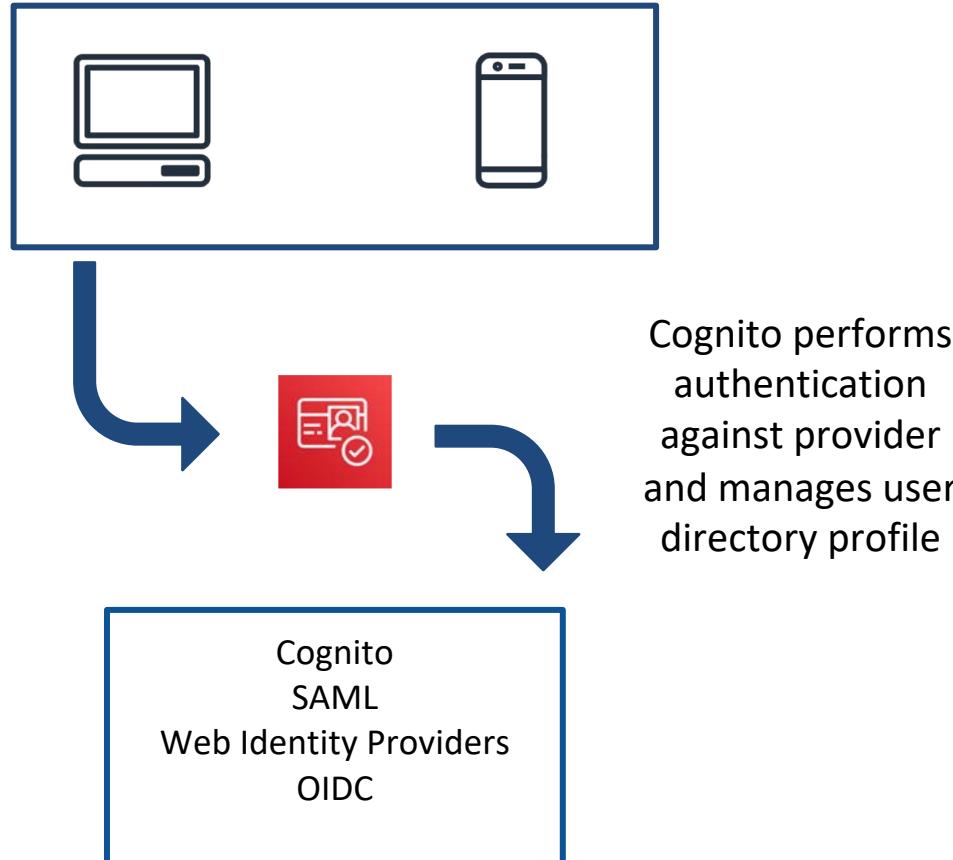
Federation - SAML 2.0



Federation - Cognito User Pools



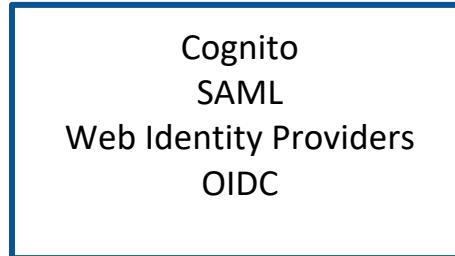
Federation - Cognito User Pools



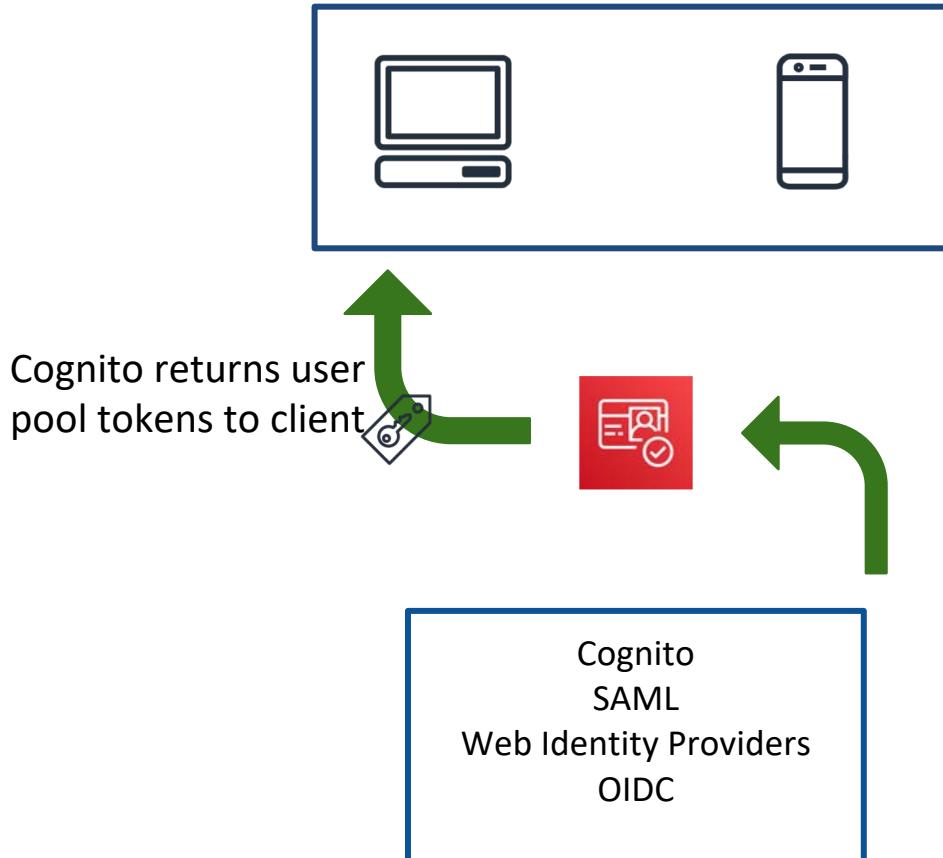
Federation - Cognito User Pools



Cognito accepts
tokens from IdP



Federation - Cognito User Pools

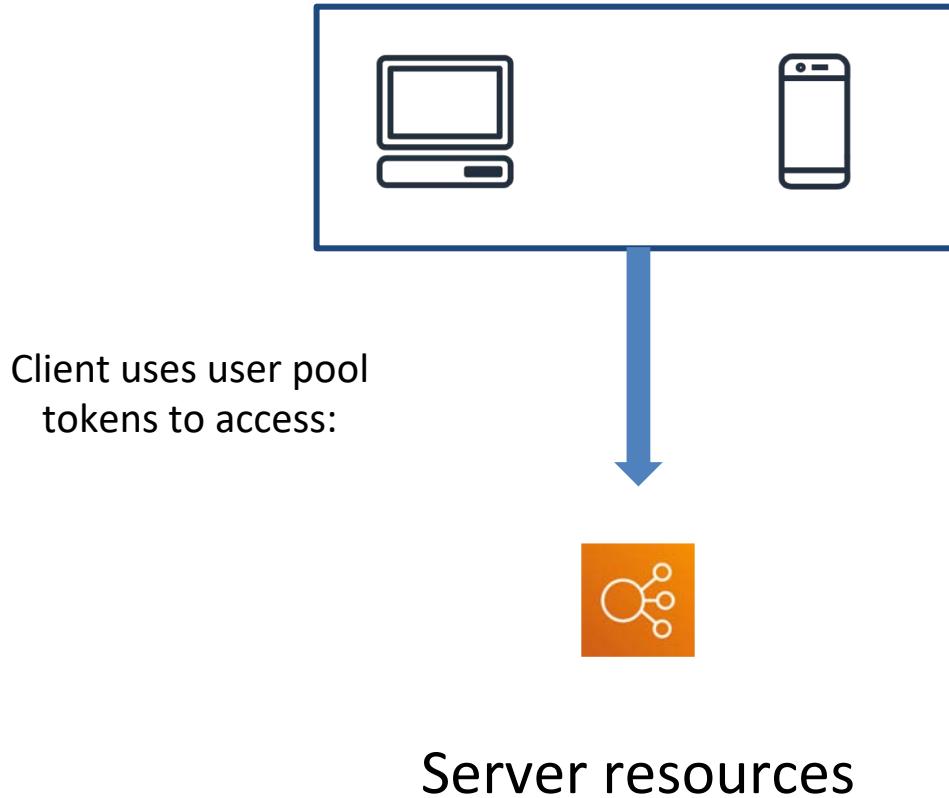


Federation - Cognito User Pools

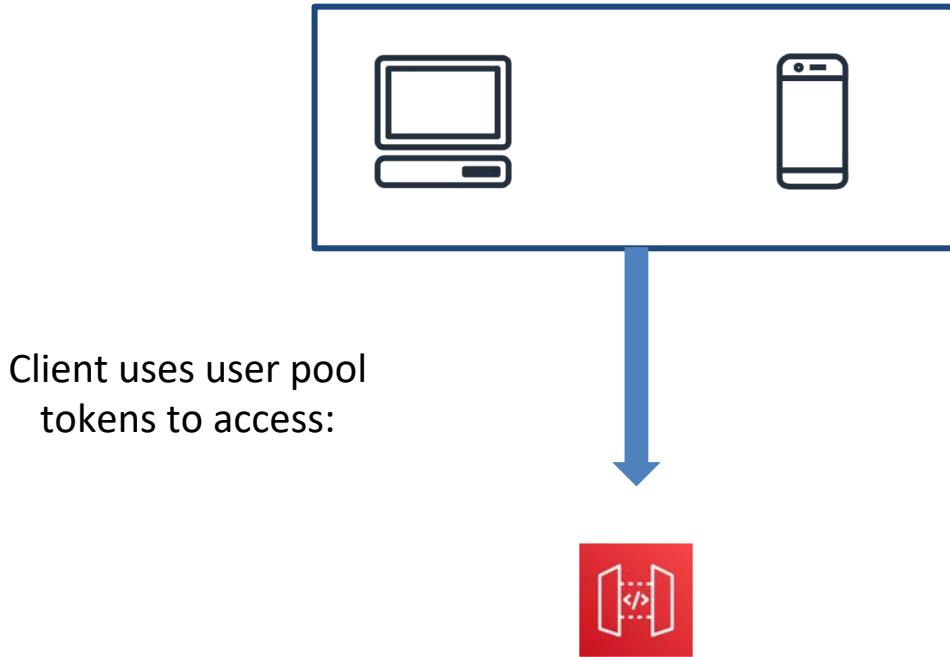


Client uses user pool
tokens to access:

Federation - Cognito User Pools

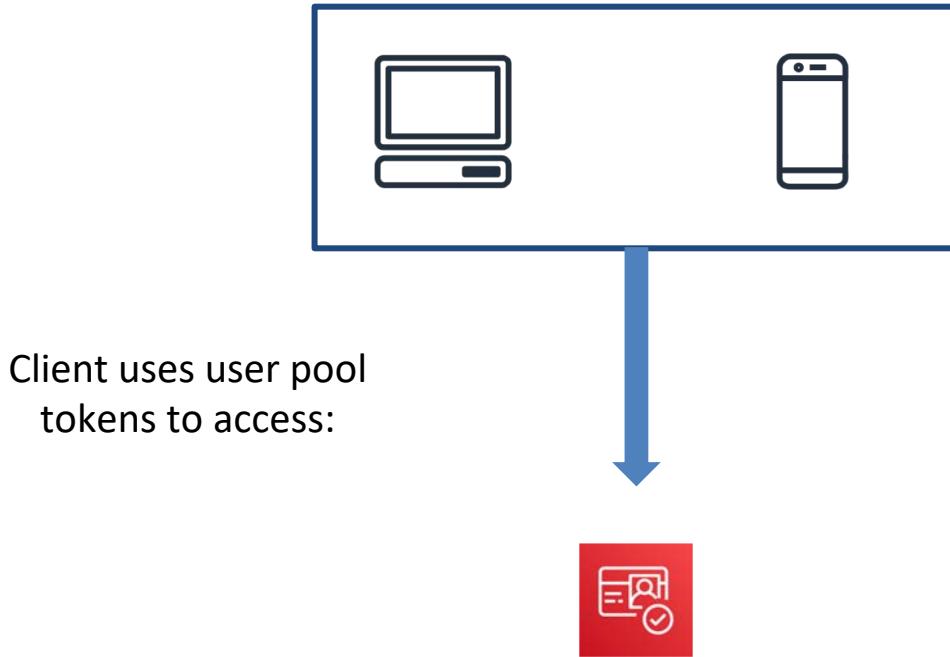


Federation - Cognito User Pools



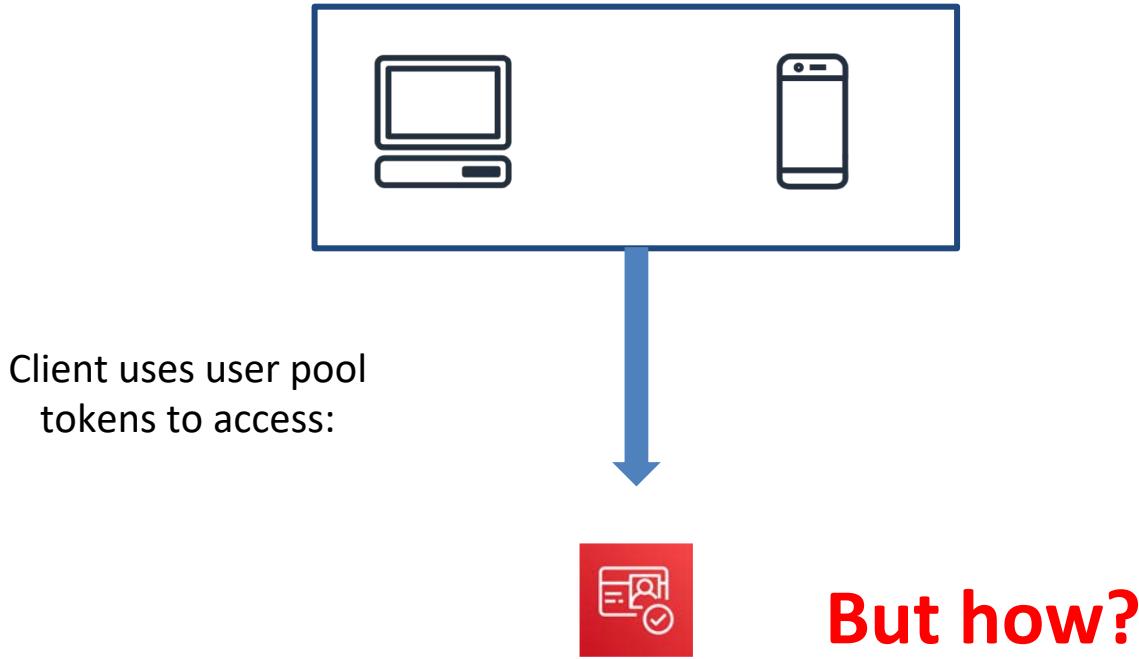
API Gateway Endpoints

Federation - Cognito User Pools



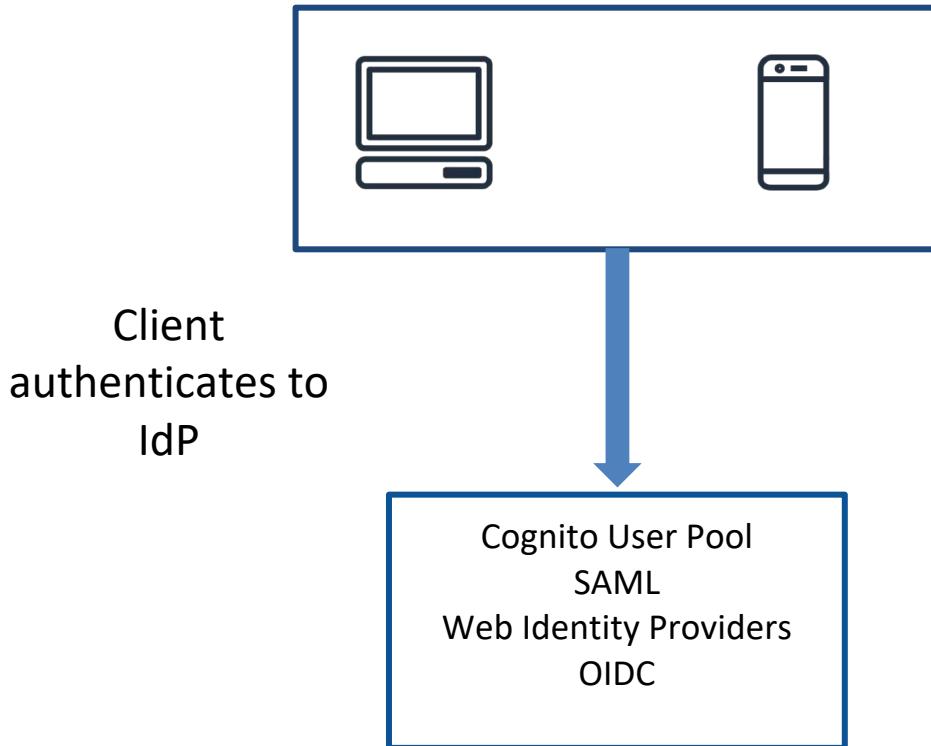
Trade for AWS credentials

Federation - Cognito User Pools

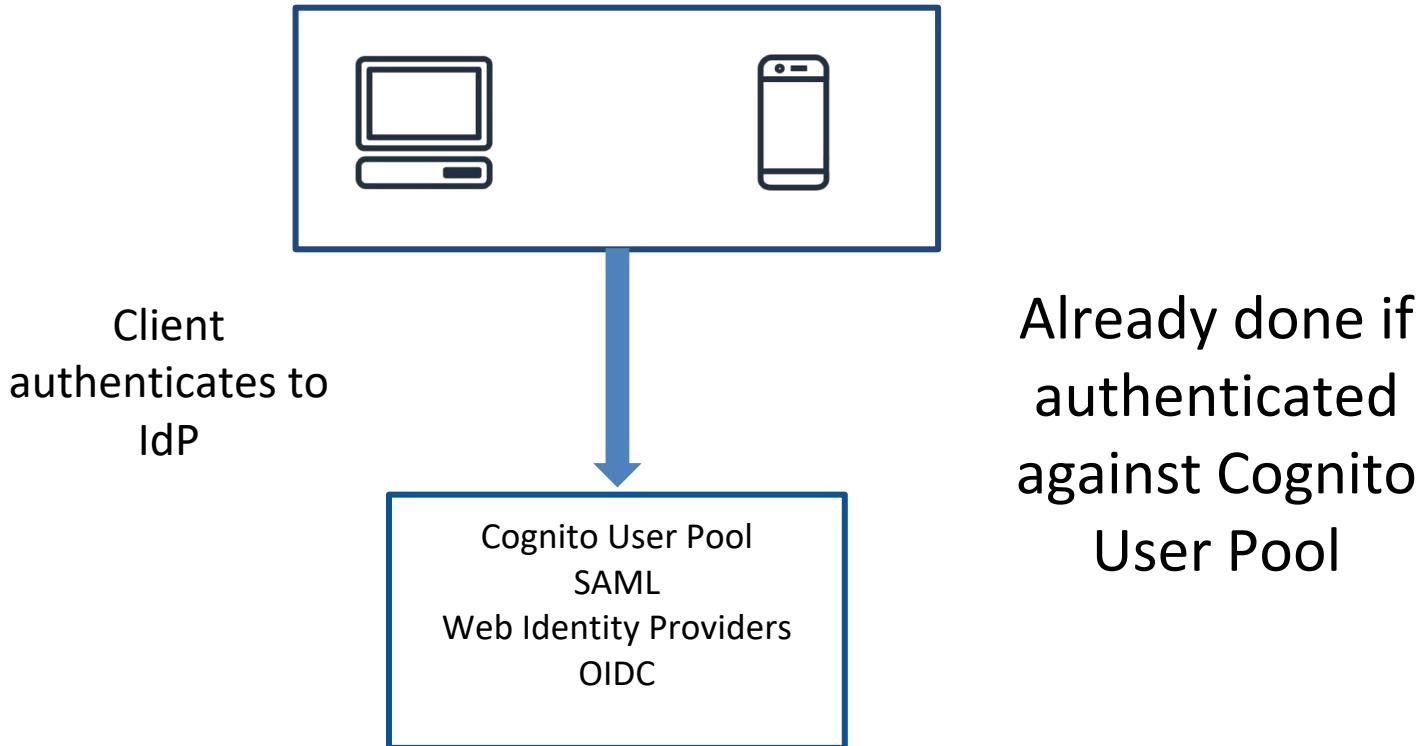


Trade for AWS credentials

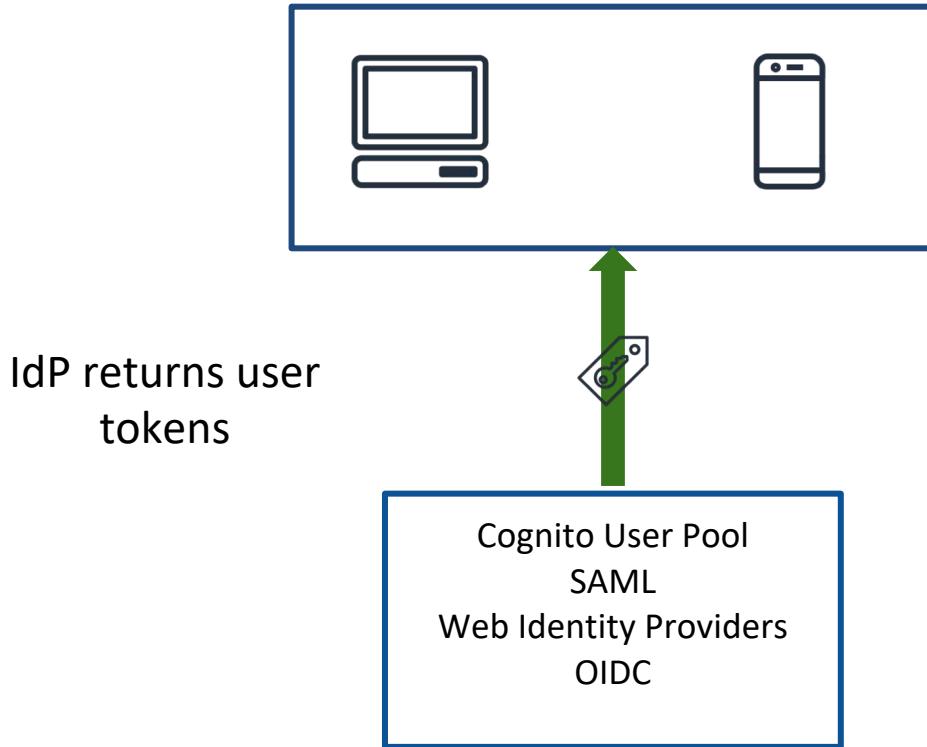
Federation - Cognito Identity Pools



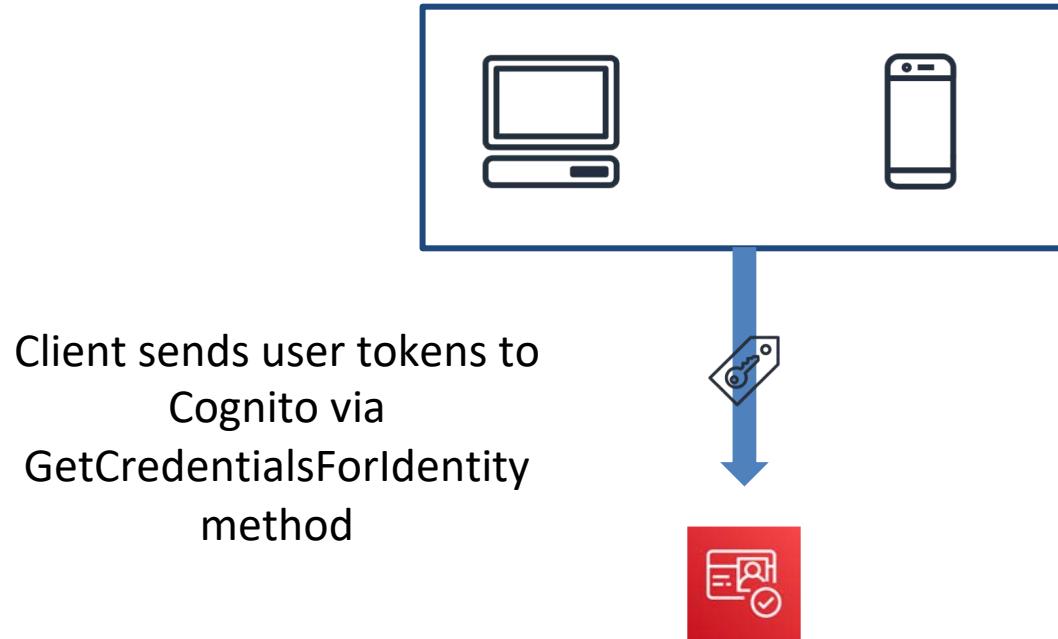
Federation - Cognito Identity Pools



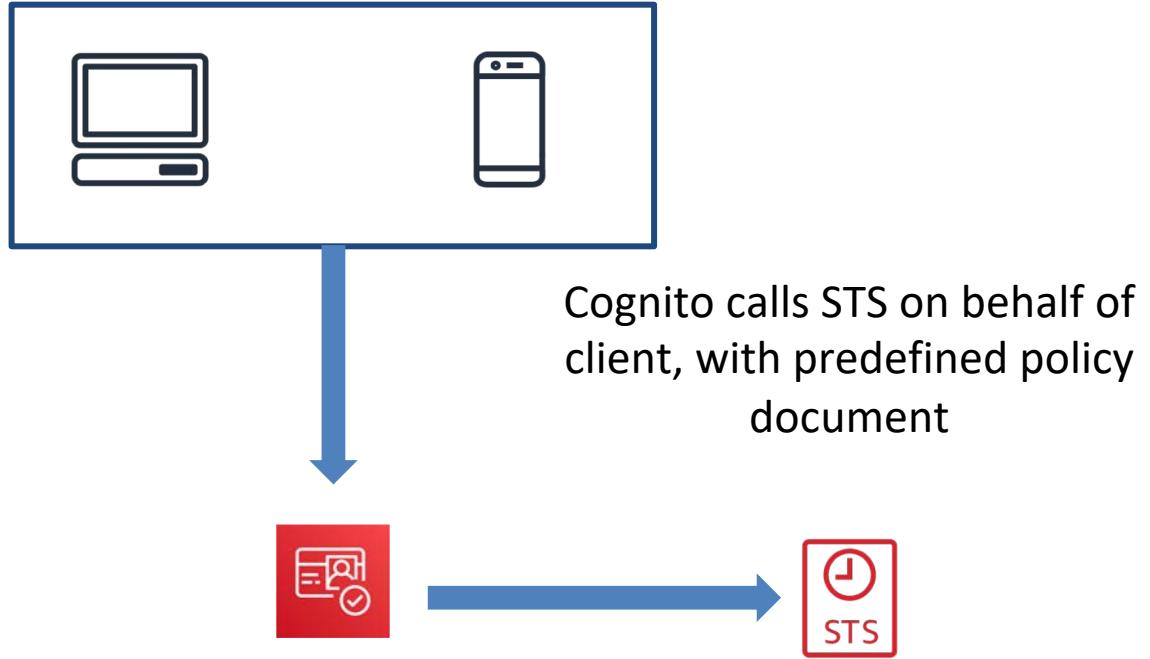
Federation - Cognito Identity Pools



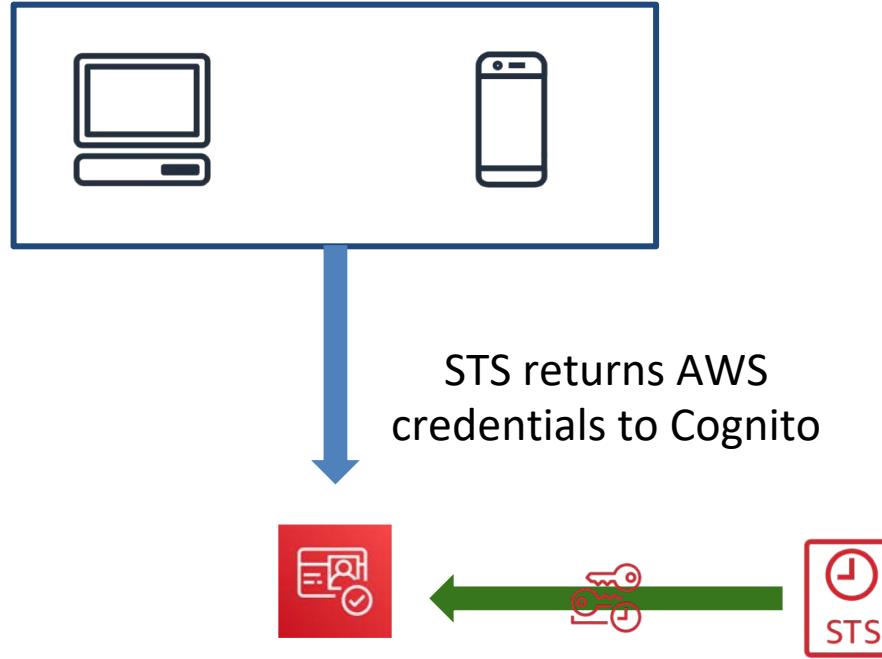
Federation - Cognito Identity Pools



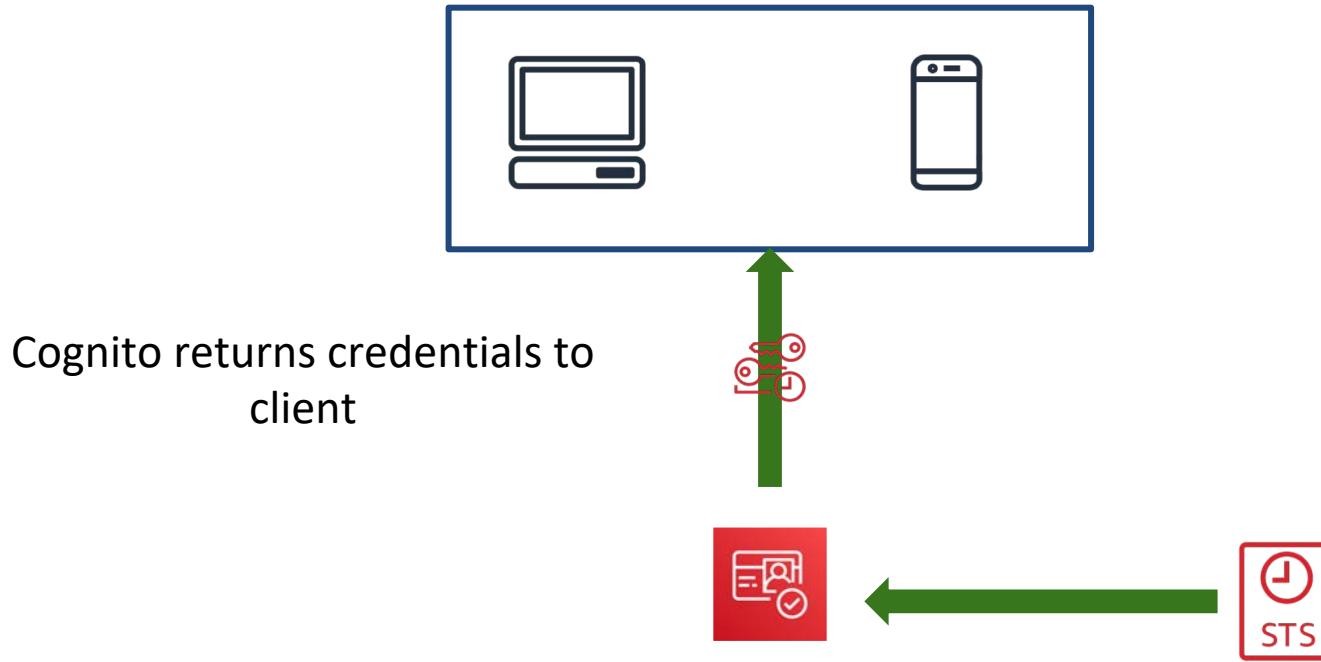
Federation - Cognito Identity Pools



Federation - Cognito Identity Pools

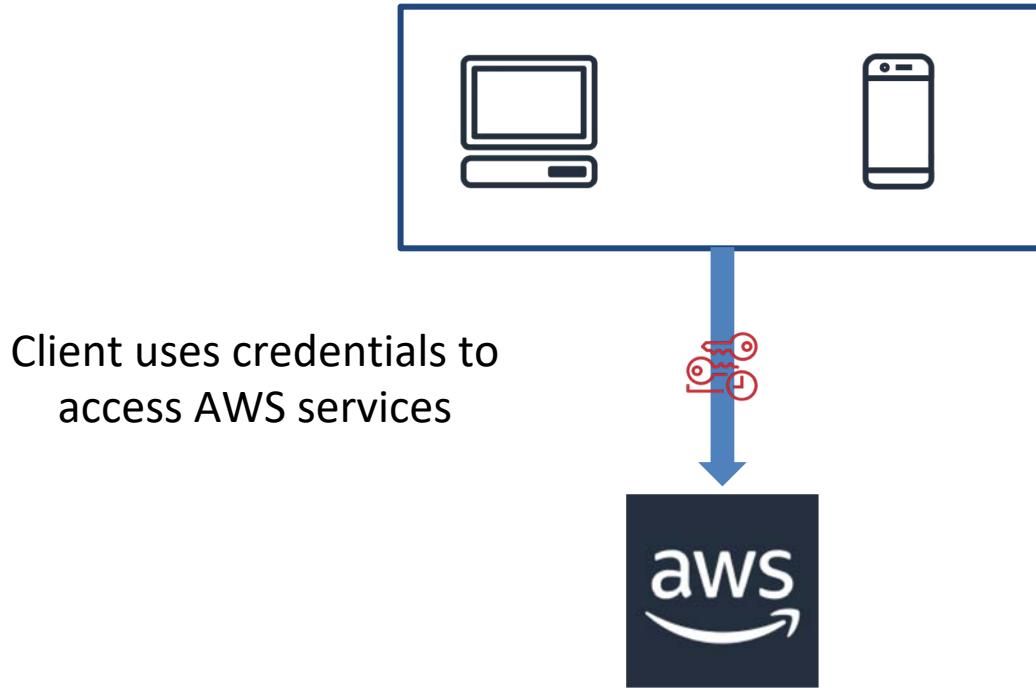


Federation - Cognito Identity Pools

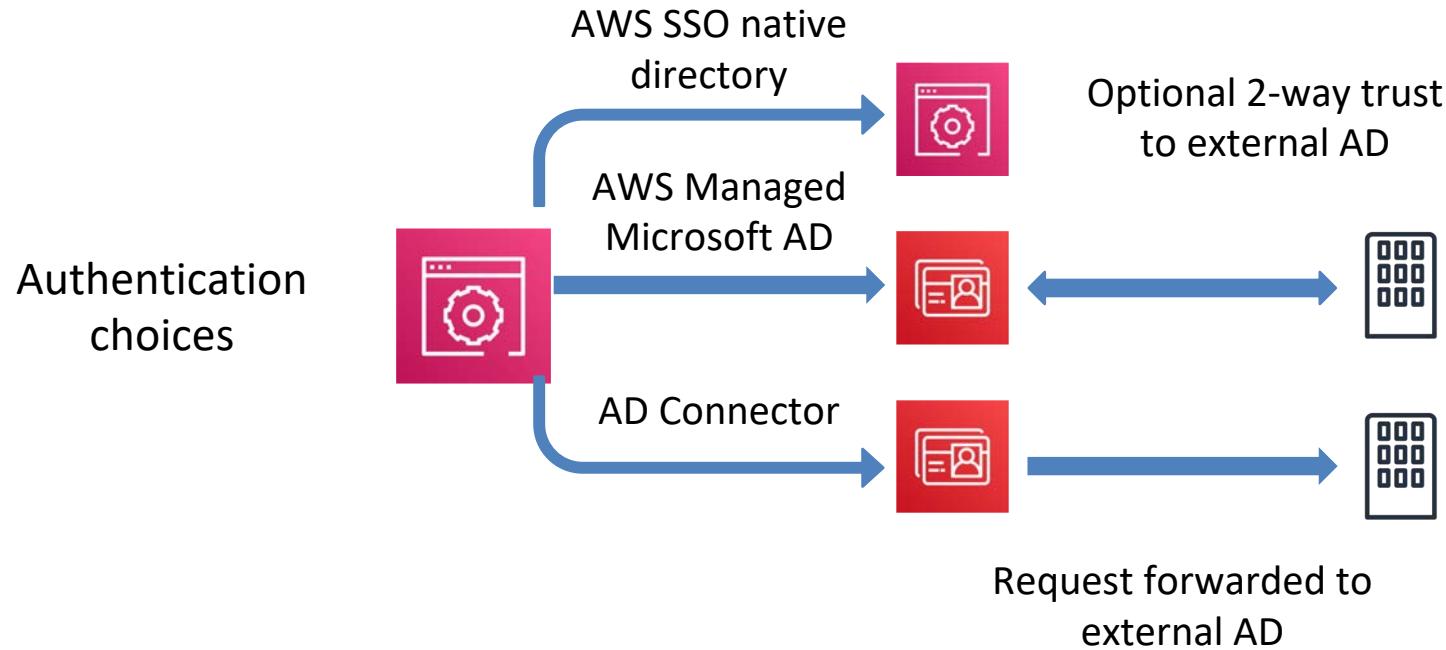


Cognito returns credentials to
client

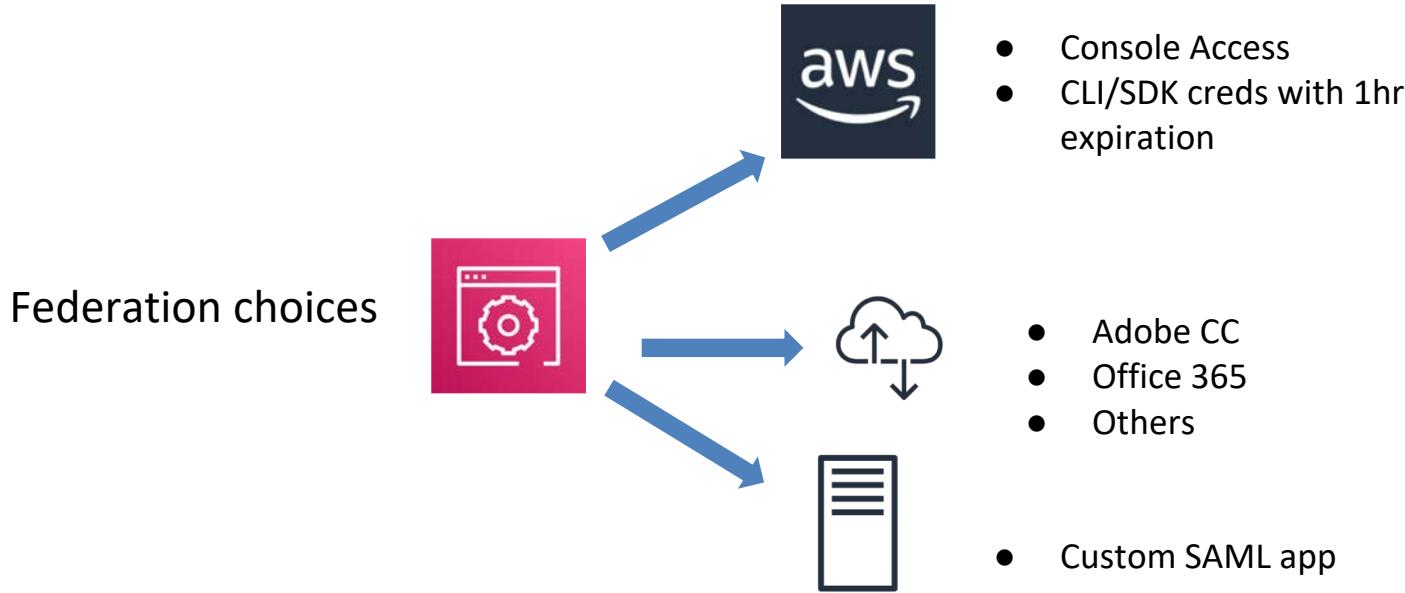
Federation - Cognito Identity Pools



Federation - AWS Single Sign-On (SSO)



Federation - AWS Single Sign-On (SSO)



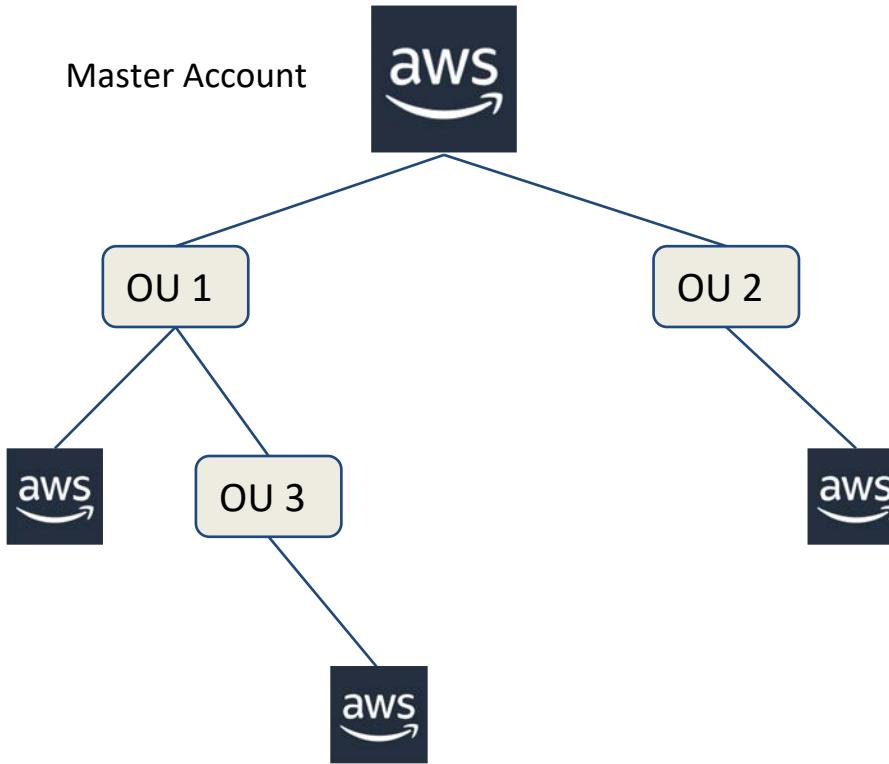
Resource-based Access Control

1. AWS Organizations
2. Amazon S3
3. Amazon API Gateway
4. AWS Lambda
5. AWS KMS (*covered in next section*)

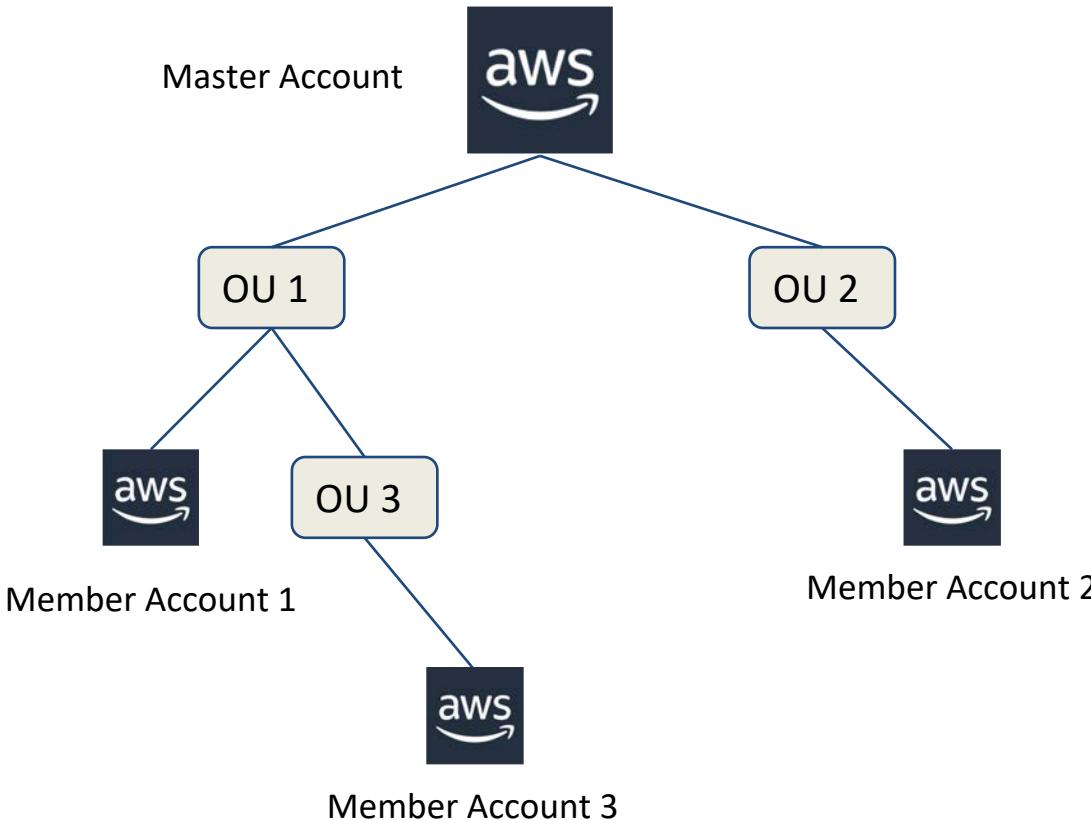
AWS Organizations

- Resource being protected is the AWS account
- Treat accounts like an OU in a directory
- Create accounts programmatically
- Invite standalone accounts to join
- SCP can blacklist or whitelist
- Master account not affected by SCP

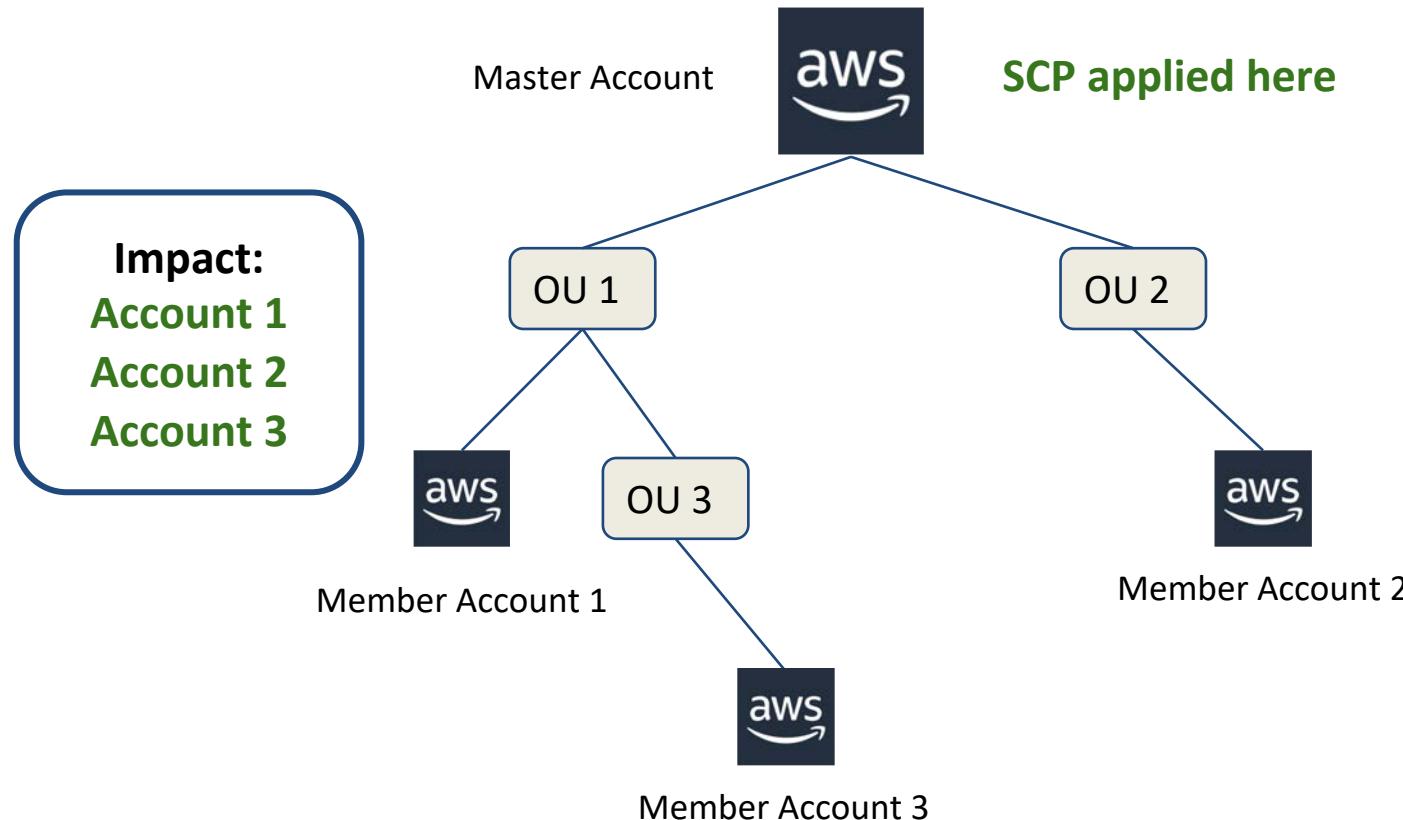
AWS Organizations Hierarchy



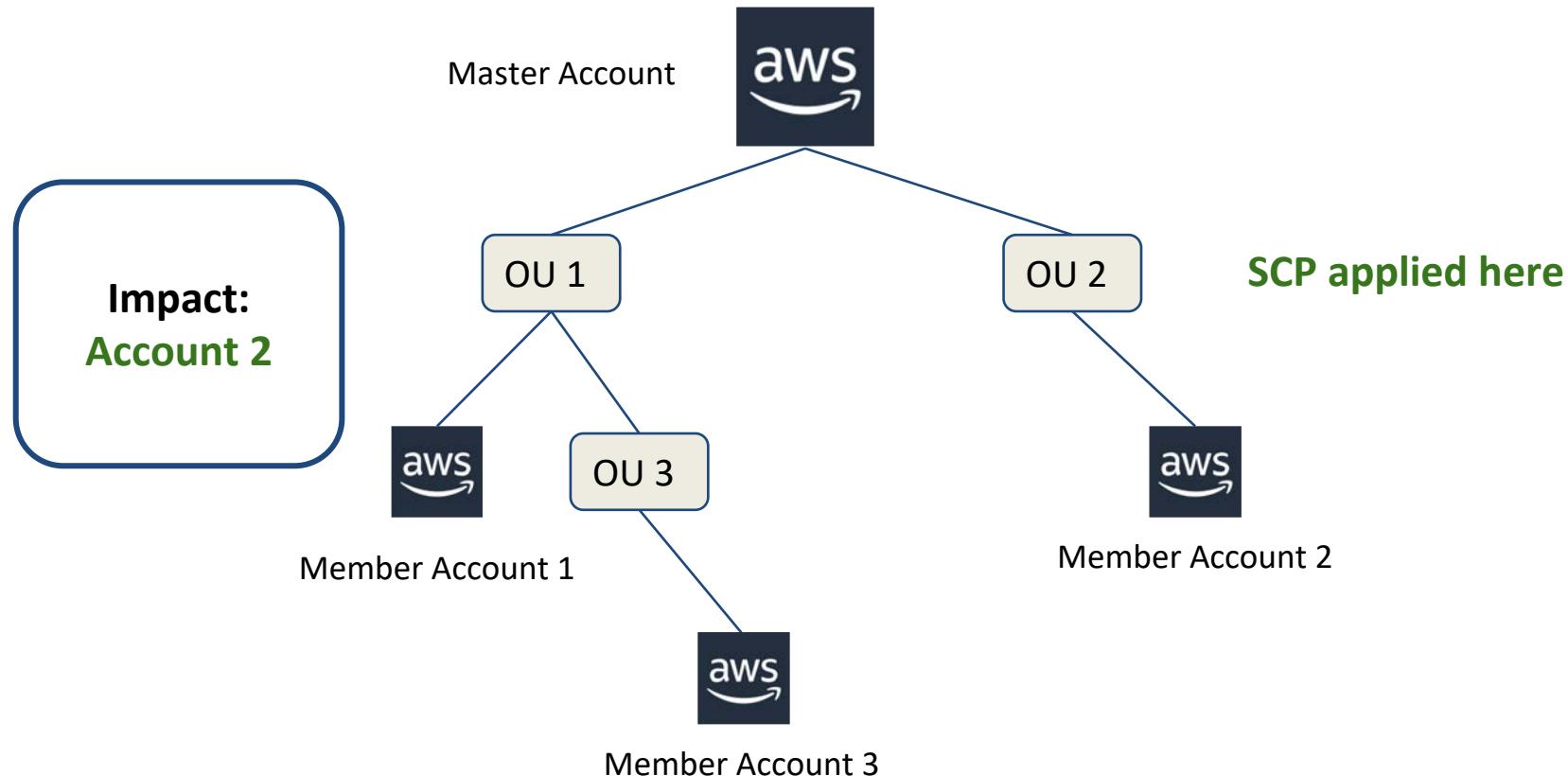
AWS Organizations Hierarchy



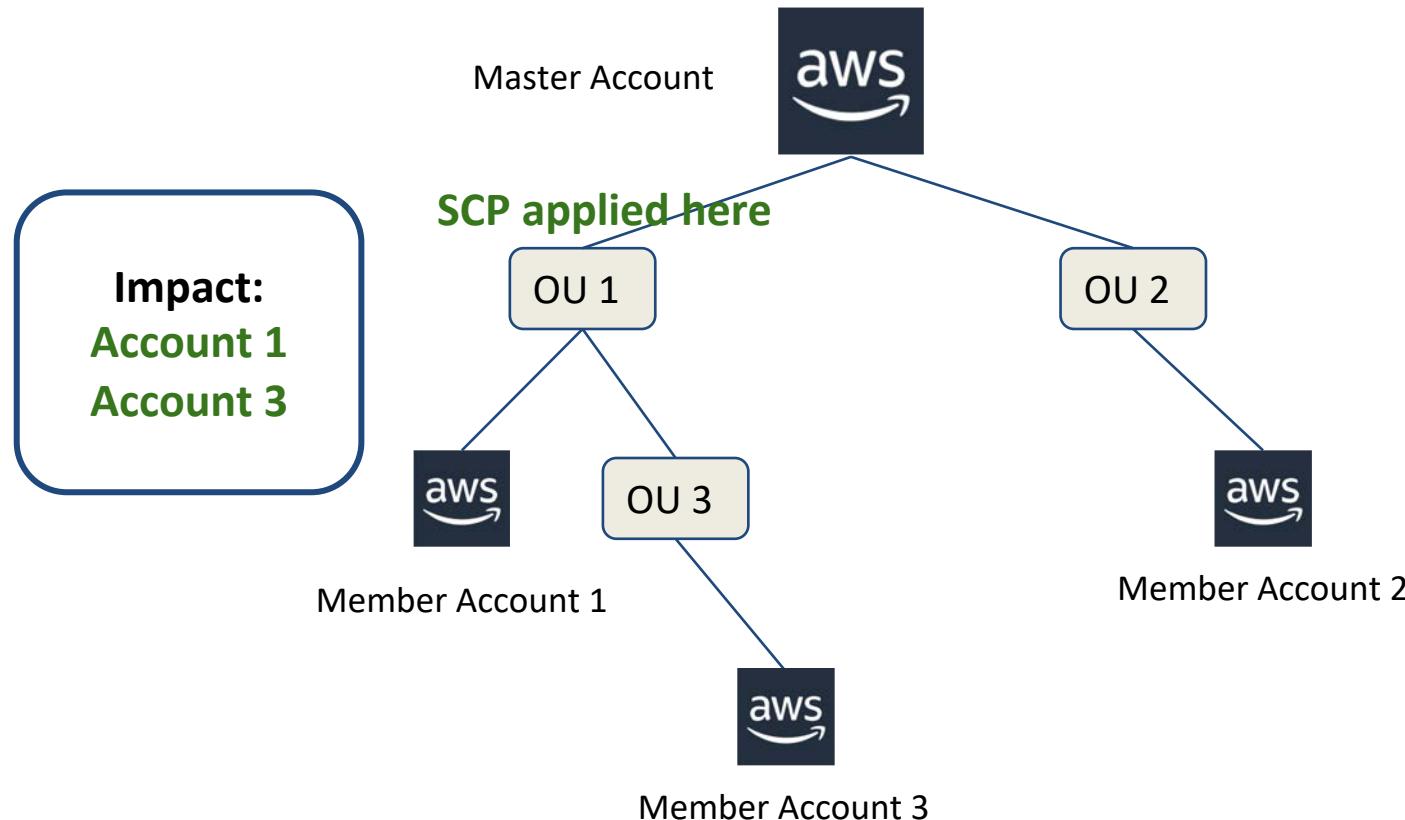
AWS Organizations SCP



AWS Organizations SCP



AWS Organizations SCP



S3 Bucket and Object ACLs

- Primitive
- Pre-date IAM
- XML (not JSON)
- Grantee - AWS Account
- Grantee - Predefined S3 Group

ACL Permissions

READ

Bucket



Object



List objects in
the bucket

Read object
data and
metadata

ACL Permissions

WRITE

Bucket



Object



Create,
overwrite or
delete any
object in the
bucket

N/A

ACL Permissions

READ_ACP

Bucket



Object



Read the bucket
ACL

Read the object
ACL

ACL Permissions

WRITE_ACP

Bucket



Object



Write the bucket
ACL

Write the object
ACL

ACL Permissions

FULL_CONTROL

Bucket



Object



Grant all other
permissions on
the bucket

Grant all other
permissions on
the object

Canned ACLs

private

public-read

public-read-write

aws-exec-read

authenticated-read

bucket-owner-read

bucket-owner-full-control

log-delivery-write

Canned ACLs

private	default
public-read	
public-read-write	not recommended use for AMI bundle
aws-exec-read	
authenticated-read	
bucket-owner-read	
bucket-owner-full-control	cross-account copies use for access logging
log-delivery-write	

S3 Bucket Policies

- 1 per bucket
- Same format as IAM policy
- Only applies to the attached bucket
 - Still must define bucket in the resource section

S3 Block Public Access

- Default on all buckets after Nov. 15, 2018
- Scopes
 - Account
 - Bucket
- Features
 - Block at ACL level
 - Block at bucket policy level

API Gateway Access Policy Principals

- IAM User
- Source IP address or CIDR
- VPC ID
- VPC Endpoint (cross-account possible)

Lambda Function Access Policies

- Cross-service permissions can be created on the function itself or assigned via IAM Role
- Cross-account invocation permissions require alias name
- Permissions can restrict function version
- Lambda layers can be shared



Identity and Access Management

Troubleshooting Authentication and Authorization

Troubleshooting - Scenarios

- User cannot perform action X
 - Scenario details
 - Conditions
- Application cannot contact service Y
 - Credential and environment details
- Permissions seem to be granted but don't work

Troubleshooting - Root Causes

- Understand the order of evaluation for actions
- Learn where deny statements override
 - All it takes is one!
- Know which services have resource-level access control
 - S3, KMS, etc
- Memorize condition possibilities
- Learn how permissions boundaries work
 - Allowed by policy, but not within boundaries
- Limits on API endpoints
 - Request must be within 5 mins of true time
 - Too many requests = throttling

Troubleshooting - Tools

- CloudTrail
- Access Advisor reports
- CloudWatch Logs Insights
- VPC Flow Logs
- Kibana and AWS ElasticSearch
- Command error output
 - Learn about error codes



AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

Your company just completed an acquisition, and the acquired company has an AWS account with resources that cannot be migrated to your existing account. How can your IT department manage account access and permissions across both accounts most effectively?

- A. Enable AWS Organizations on the company account, invite the acquired account to join, then manage both using AWS SSO
- B. Manage both accounts using cross-account IAM Roles for IT administrators
- C. Enable Consolidated Billing on both accounts and configure cross-account IAM roles
- D. Configure SAML federation for both accounts with your existing AD organization and use that for SSO

Question Breakdown - Answers

This covers permissions and access, from a central location. Might be the right answer?

- A. Enable AWS Organizations on the company account, invite the acquired account to join, then manage both using AWS SSO
- B. Manage both accounts using cross-account IAM Roles for IT administrators
- C. Enable Consolidated Billing on both accounts and configure cross-account IAM roles
- D. Configure SAML federation for both accounts with your existing AD organization and use that for SSO



Question Breakdown - Answers

This covers permissions and access, but requires management from both accounts, which isn't as effective as A

- A. Enable AWS Organizations on the company account, invite the acquired account to join, then manage both using AWS SSO
- B. Manage both accounts using cross-account IAM Roles for IT administrators
- C. Enable Consolidated Billing on both accounts and configure cross-account IAM roles
- D. Configure SAML federation for both accounts with your existing AD organization and use that for SSO



Question Breakdown - Answers

This is similar to B with the added (but irrelevant) benefit of consolidated billing

- A. Enable AWS Organizations on the company account, invite the acquired account to join, then manage both using AWS SSO
- B. Manage both accounts using cross-account IAM Roles for IT administrators
- C. Enable Consolidated Billing on both accounts and configure cross-account IAM roles
- D. Configure SAML federation for both accounts with your existing AD organization and use that for SSO

Question Breakdown - Answers

This appears to meet the requirements as well, but requires effort in both AWS accounts to configure IAM roles, not as effective as A

- A. Enable AWS Organizations on the company account, invite the acquired account to join, then manage both using AWS SSO
- B. Manage both accounts using cross-account IAM Roles for IT administrators
- C. Enable Consolidated Billing on both accounts and configure cross-account IAM roles
- D. Configure SAML federation for both accounts with your existing AD organization and use that for SSO

Question Breakdown - Correct Answer

Correct Answer:A

- A. Enable AWS Organizations on the company account, invite the acquired account to join, then manage both using AWS SSO
- B. Manage both accounts using cross-account IAM Roles for IT administrators
- C. Enable Consolidated Billing on both accounts and configure cross-account IAM roles
- D. Configure SAML federation for both accounts with your existing AD organization and use that for SSO





AWS Certified Security - Specialty Crash Course

Data Protection

22%

Question Domain Main Points

1. Design and implement key management and use
2. Troubleshoot key management
3. Design and implement a data encryption solution for data at rest and data in transit



Data Protection

Design and implement key management and use

Symmetric Data Encryption in AWS



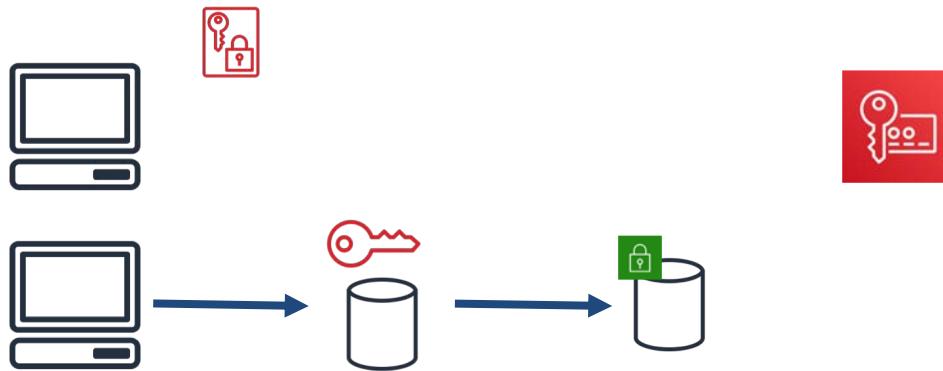
Application/service requests new
data encryption key from key
management infrastructure

Symmetric Data Encryption in AWS



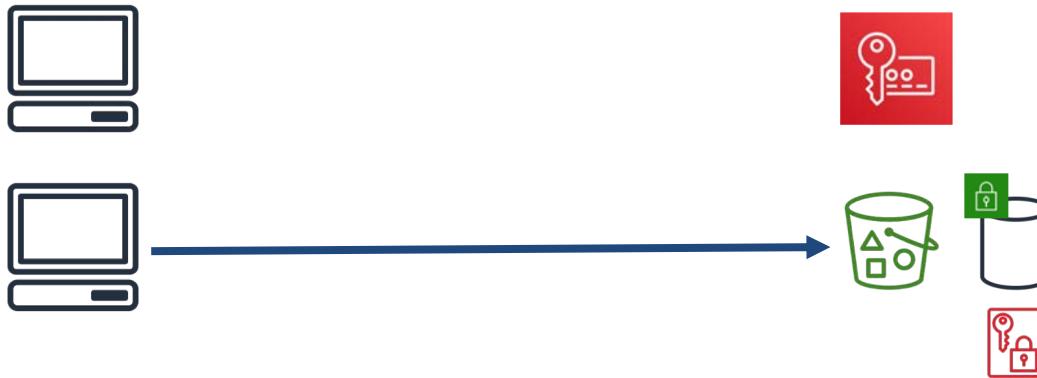
Key management infrastructure returns plaintext encryption key and encryption key ***encrypted*** by master key

Symmetric Data Encryption in AWS



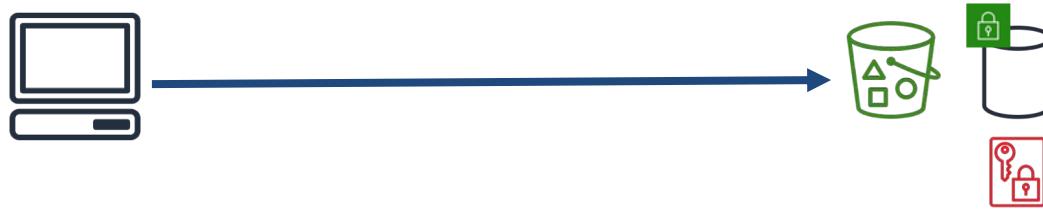
Application uses plaintext key to
encrypt data object (AES256)

Symmetric Data Encryption in AWS



Application puts encrypted data in storage, attaching encrypted data key as metadata

Symmetric Data Decryption in AWS



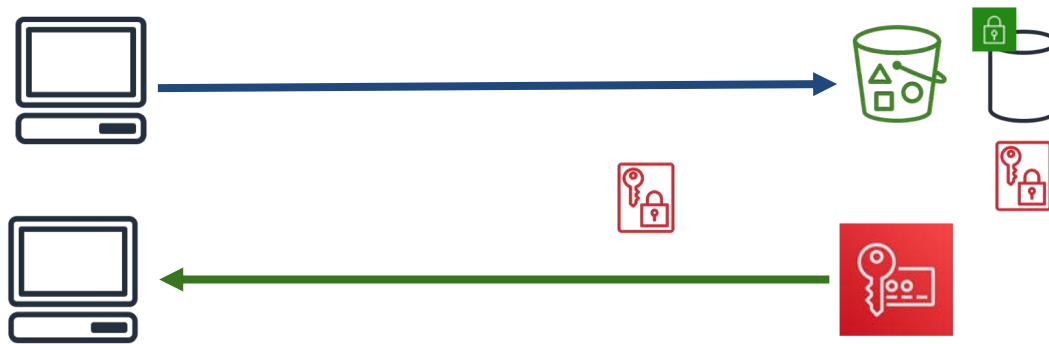
Application requests encrypted data
key from storage

Symmetric Data Decryption in AWS



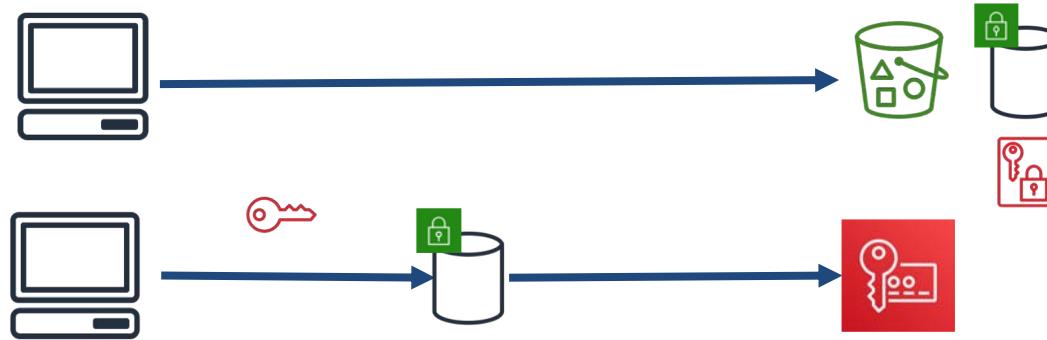
Application sends encrypted data
key to key management
infrastructure

Symmetric Data Decryption in AWS



Key management infrastructure
returns plaintext data key to
application

Symmetric Data Decryption in AWS



Application decrypts data using
plaintext data key

Symmetric Data Encryption Considerations

What keys are involved?

- Root CA
- Master Key
- Data Encryption Key

Who owns the keys?

- AWS
- Customer
- Third Party

Symmetric Data Encryption Considerations

Where is the encryption performed?

- Server/Service
- Client

How is key access control implemented?

- User-based
- Resource-based

Key Management Services

- KMS
- CloudHSM
- AWS Certificate Manager
- EC2 Marketplace
- DIY

Symmetric Data Encryption Services

- KMS
 - CloudHSM
 - AWS Certificate Manager
 - EC2 Marketplace
 - DIY
-
- The diagram consists of a vertical list of five items. To the right of each item is a horizontal blue arrow pointing towards a light gray rounded rectangular callout box. The callout box contains the text "Concentrate study **HERE**".

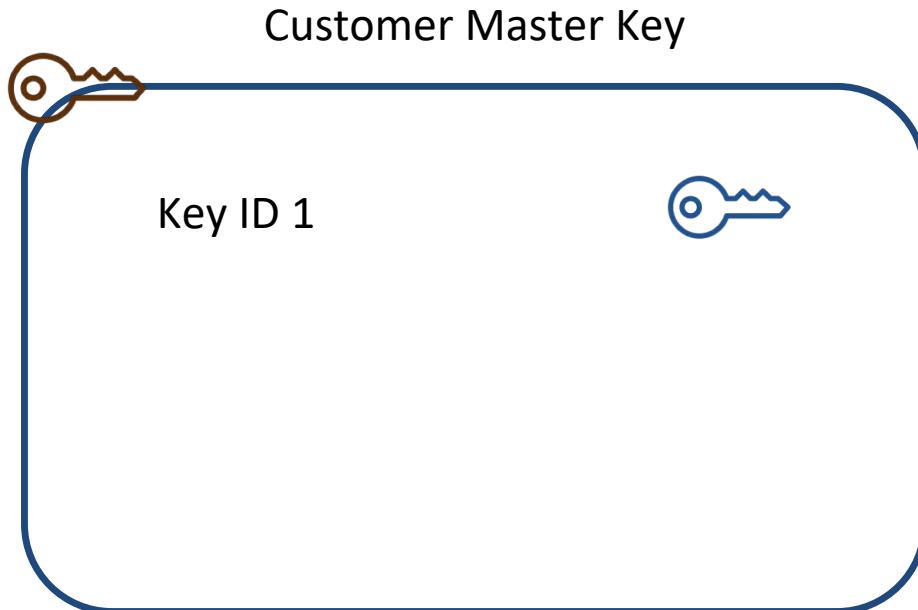
AWS KMS Basics

- Key Management Service
- Region scoped
- Multi-tenant service
- Generate/store master keys
- Upload master keys
- Generate data keys
- Does NOT encrypt data
- KMS Custom Key Store available
 - CloudHSM-backed CMK
 - Stores CMK using single-tenancy

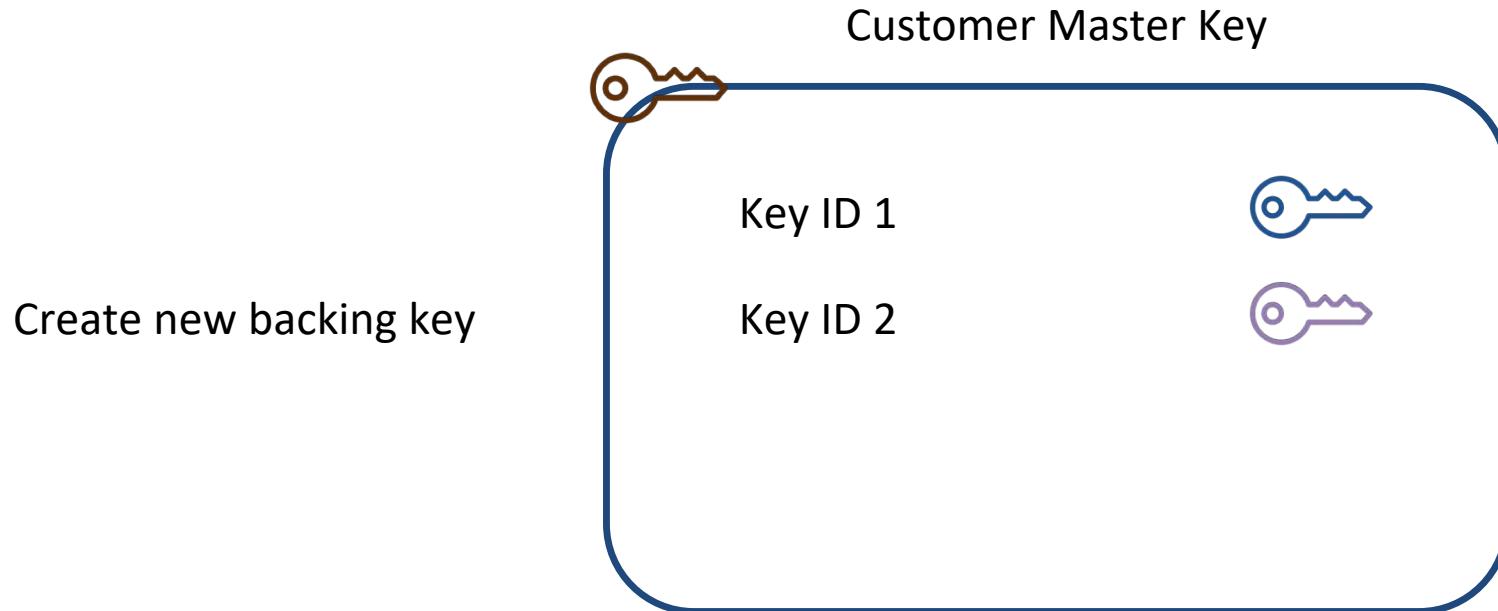


AWS KMS CMK Basics

- CMK is logical object
- Contains 1+ backing keys
- Create backing key in KMS
- Upload backing key
- Rotate backing key on demand
- Rotate backing key on schedule

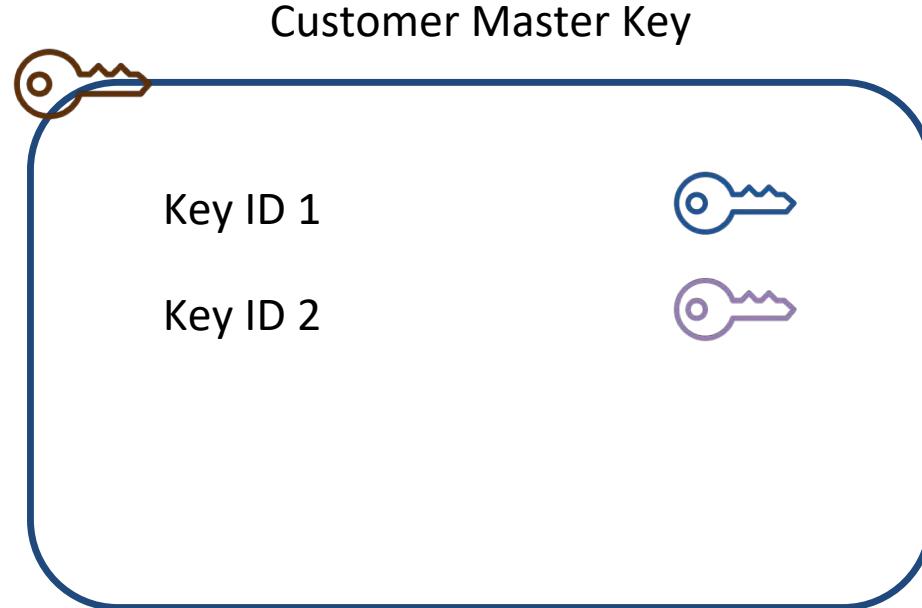


AWS KMS CMK Key Rotation



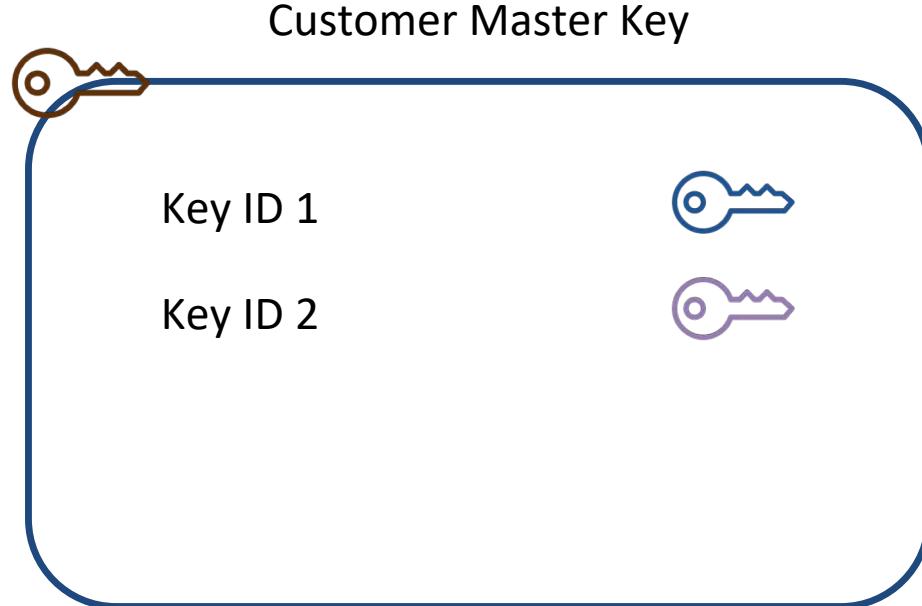
AWS KMS CMK Key Rotation

Still used for decrypting
previous data keys



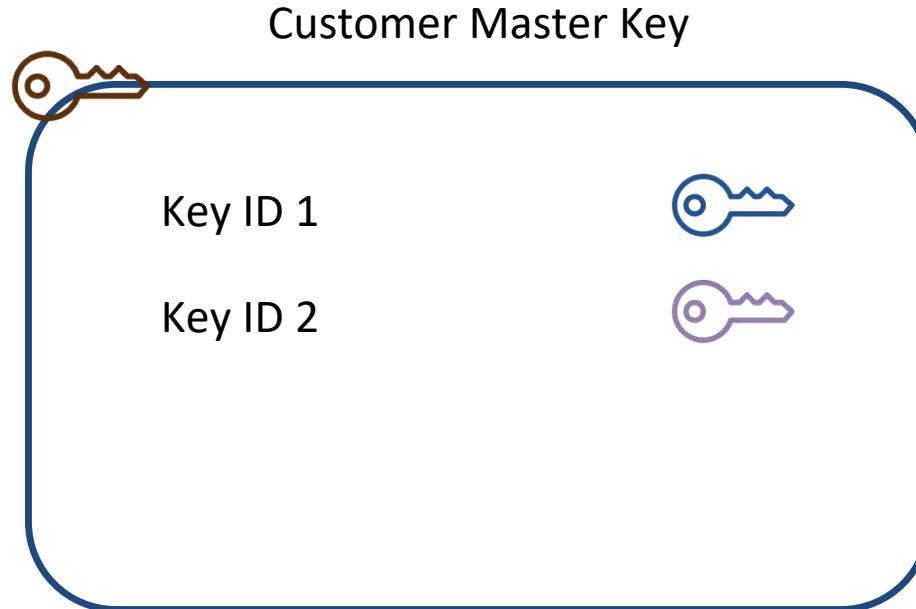
AWS KMS CMK Key Rotation

Can be deleted if
compromise suspected

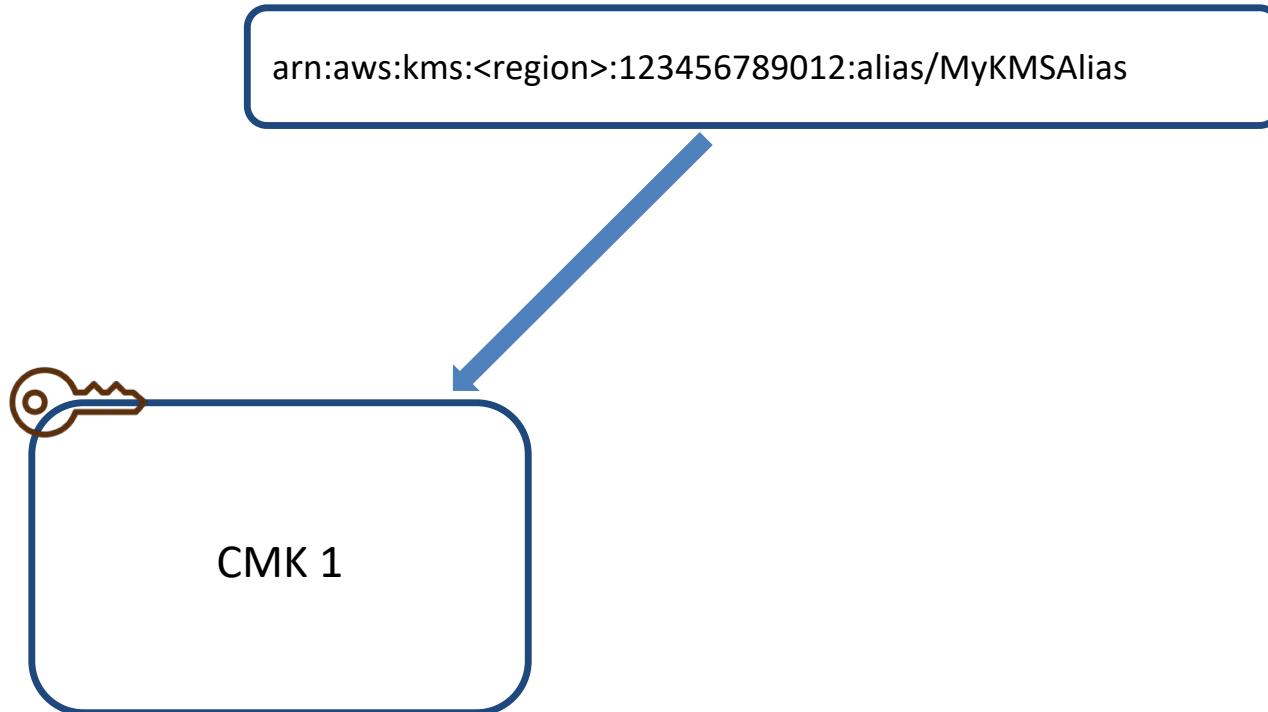


AWS KMS CMK Key Rotation

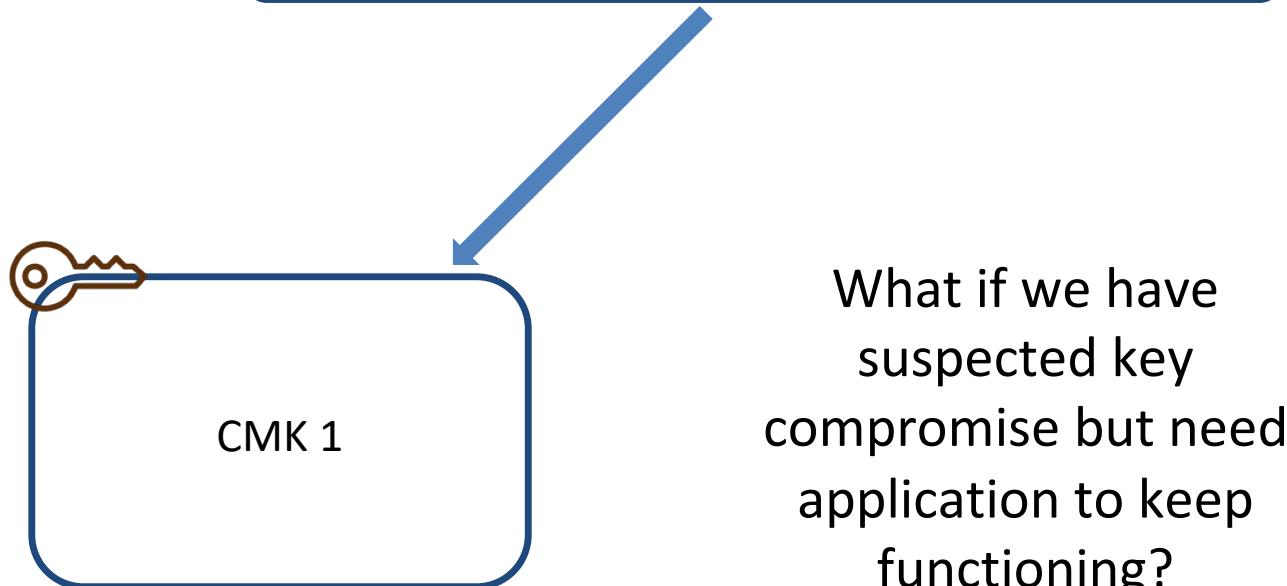
Used for
encrypting/decrypting data
keys from time of rotation



AWS KMS CMK Alias Basics

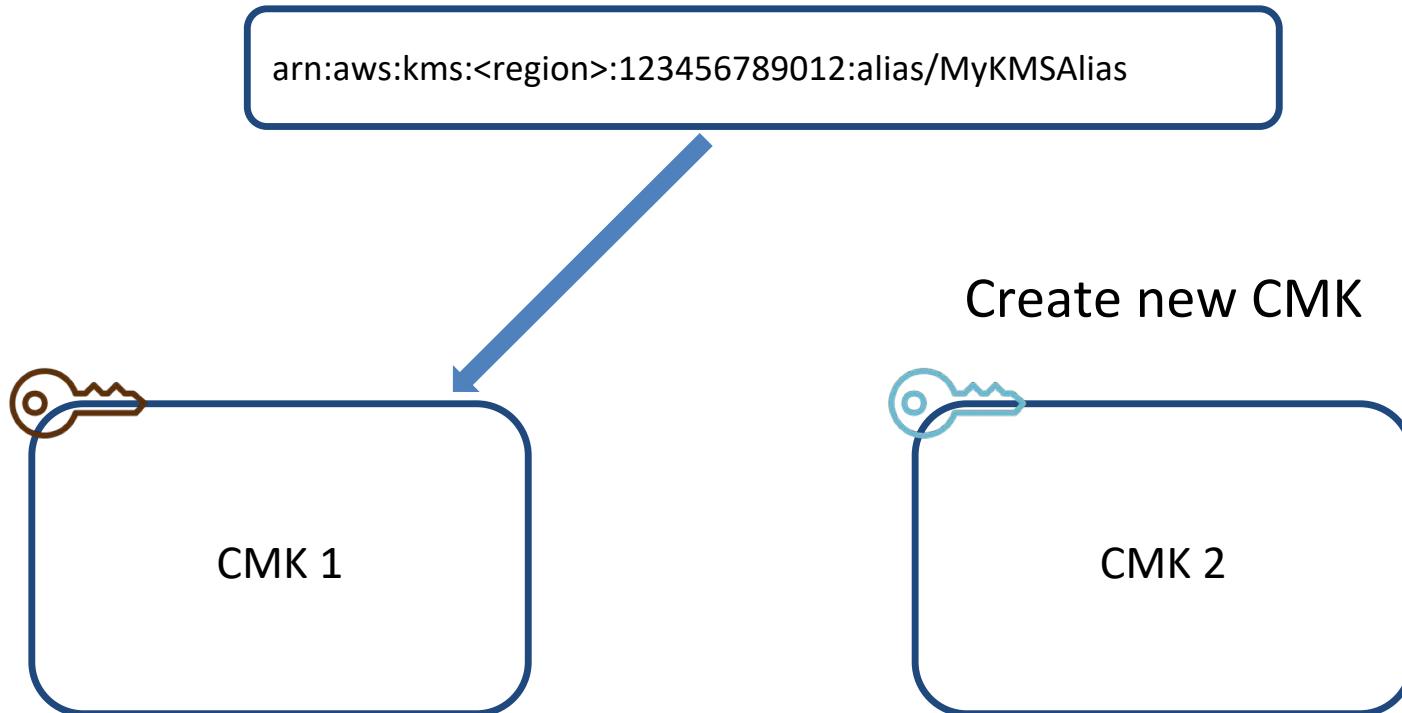


AWS KMS CMK Alias Basics

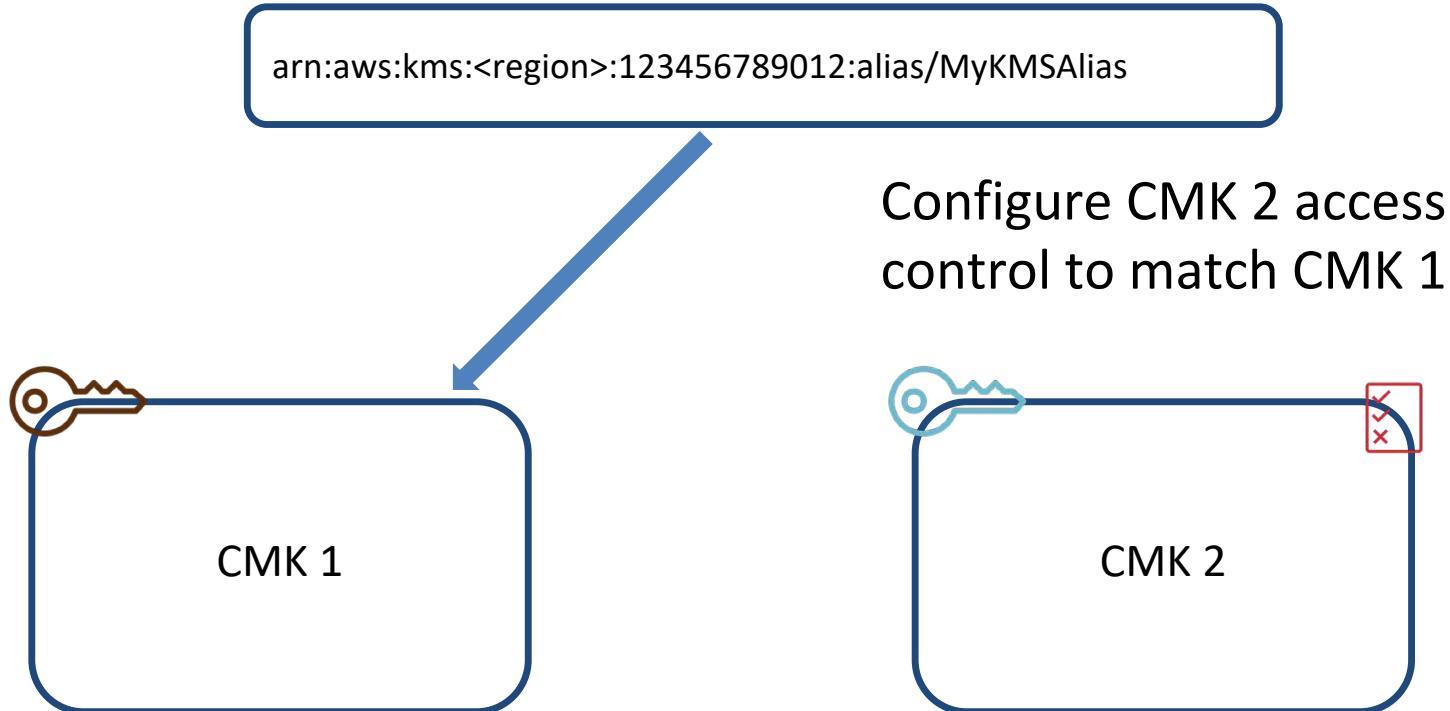


What if we have
suspected key
compromise but need
application to keep
functioning?

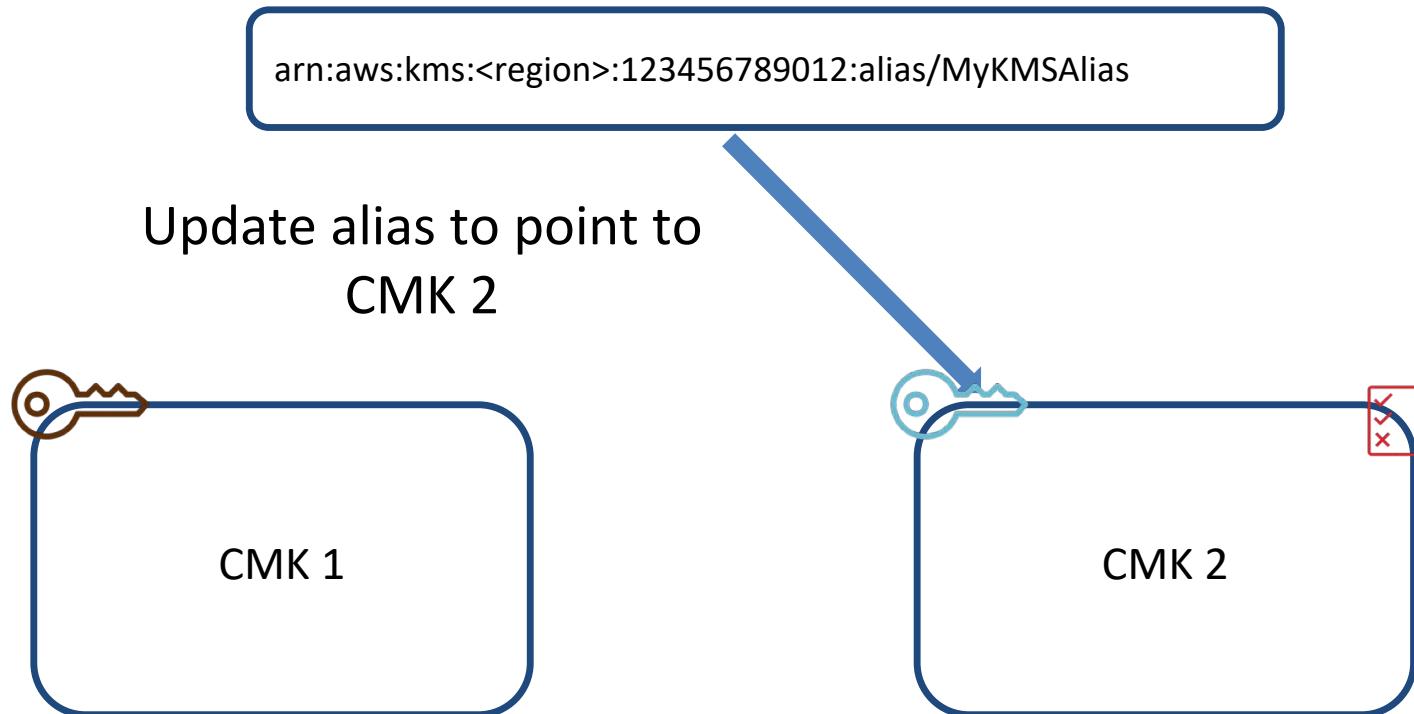
AWS KMS CMK Alias Basics



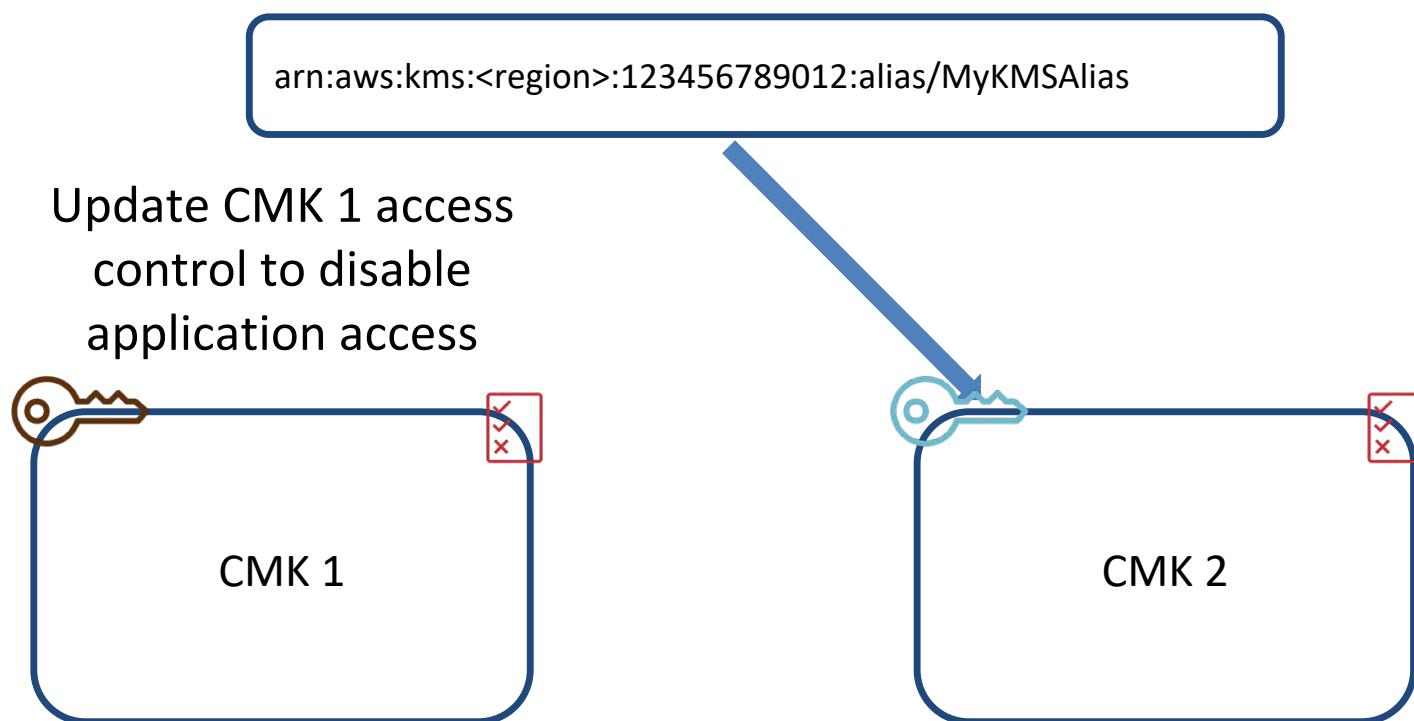
AWS KMS CMK Alias Basics



AWS KMS CMK Alias Basics



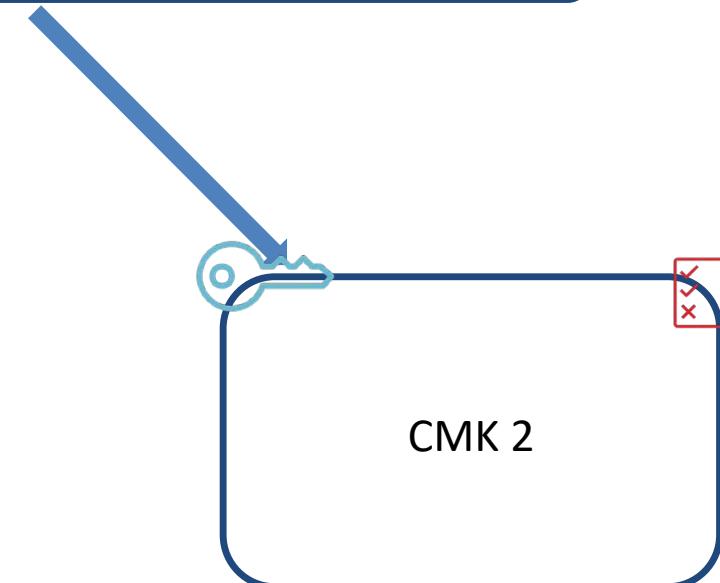
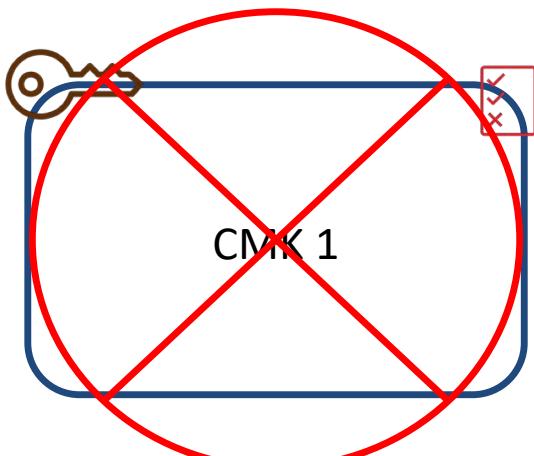
AWS KMS CMK Alias Basics



AWS KMS CMK Alias Basics

arn:aws:kms:<region>:123456789012:alias/MyKMSAlias

Disable CMK 1 when appropriate



KMS Access Control - IAM



KMS Access Control - IAM

Appropriate for general access to KMS



KMS Access Control - IAM

Appropriate for general access to KMS

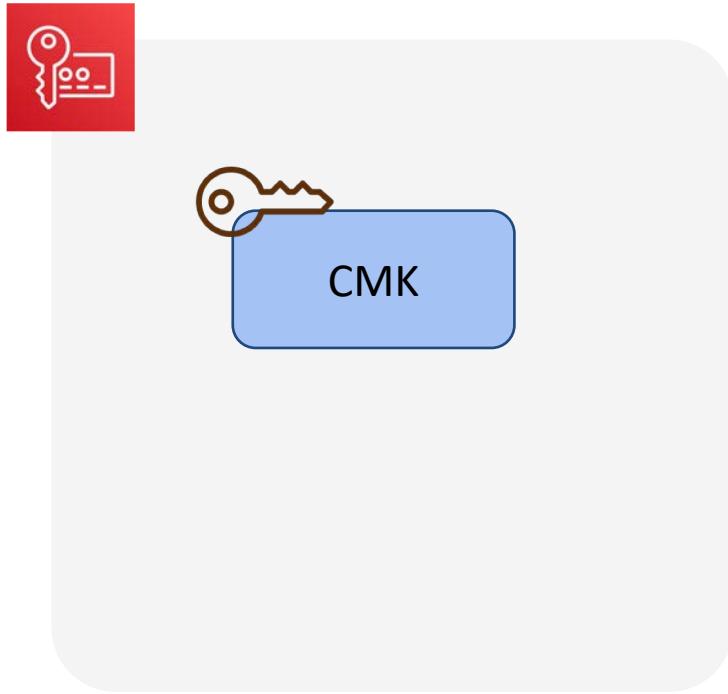


- Create CMKs
- Audit usage
- Inventory CMKs

KMS CMK Access Control - Choices

1. Key policy Required
2. IAM in combination
with key policy Optional
3. Grants in combination
with key policy Optional

KMS Access Control - Key Policy



KMS Access Control - Key Policy



CMK



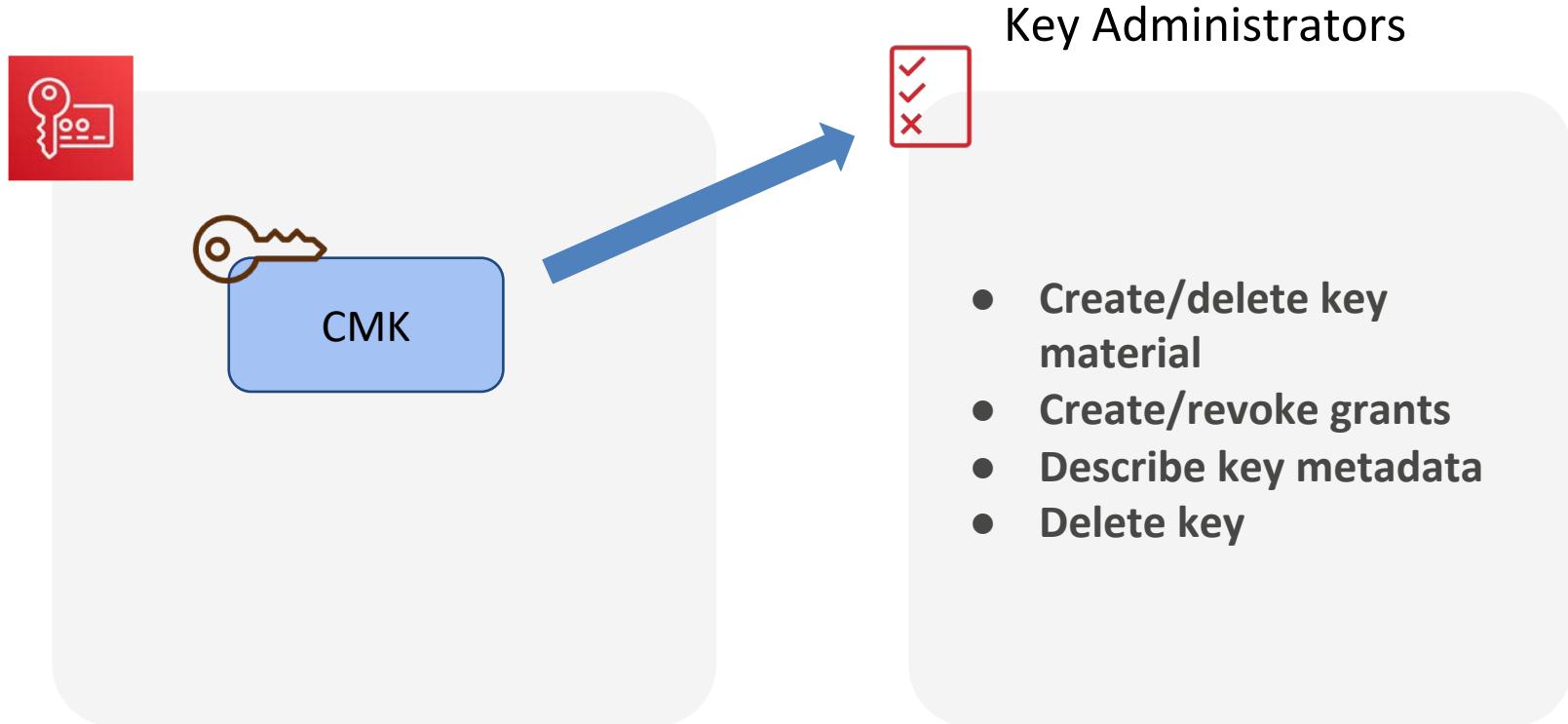
Basics



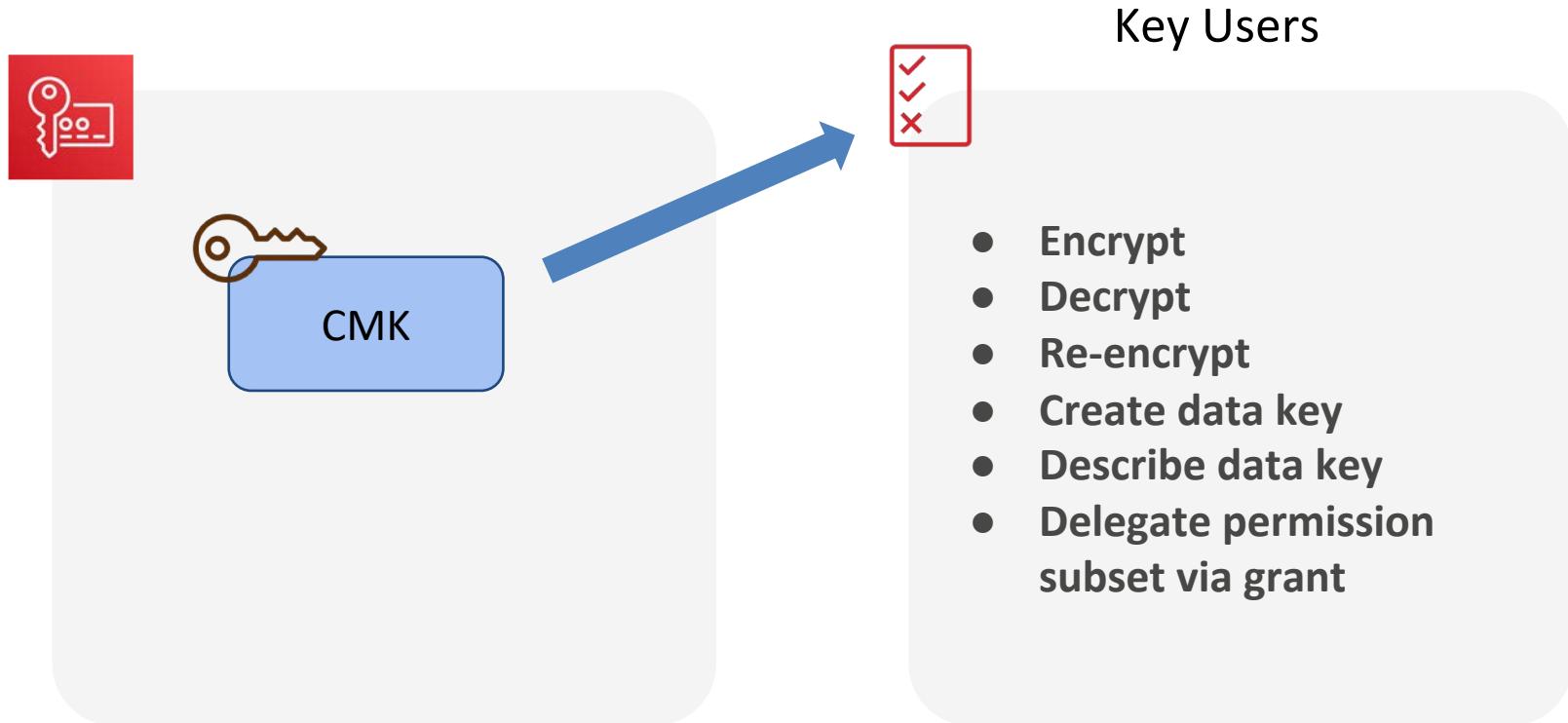
No default root access
Principals include:

- users
- roles
- accounts
- services

KMS Access Control - Key Policy



KMS Access Control - Key Policy



KMS Access Control - Grants



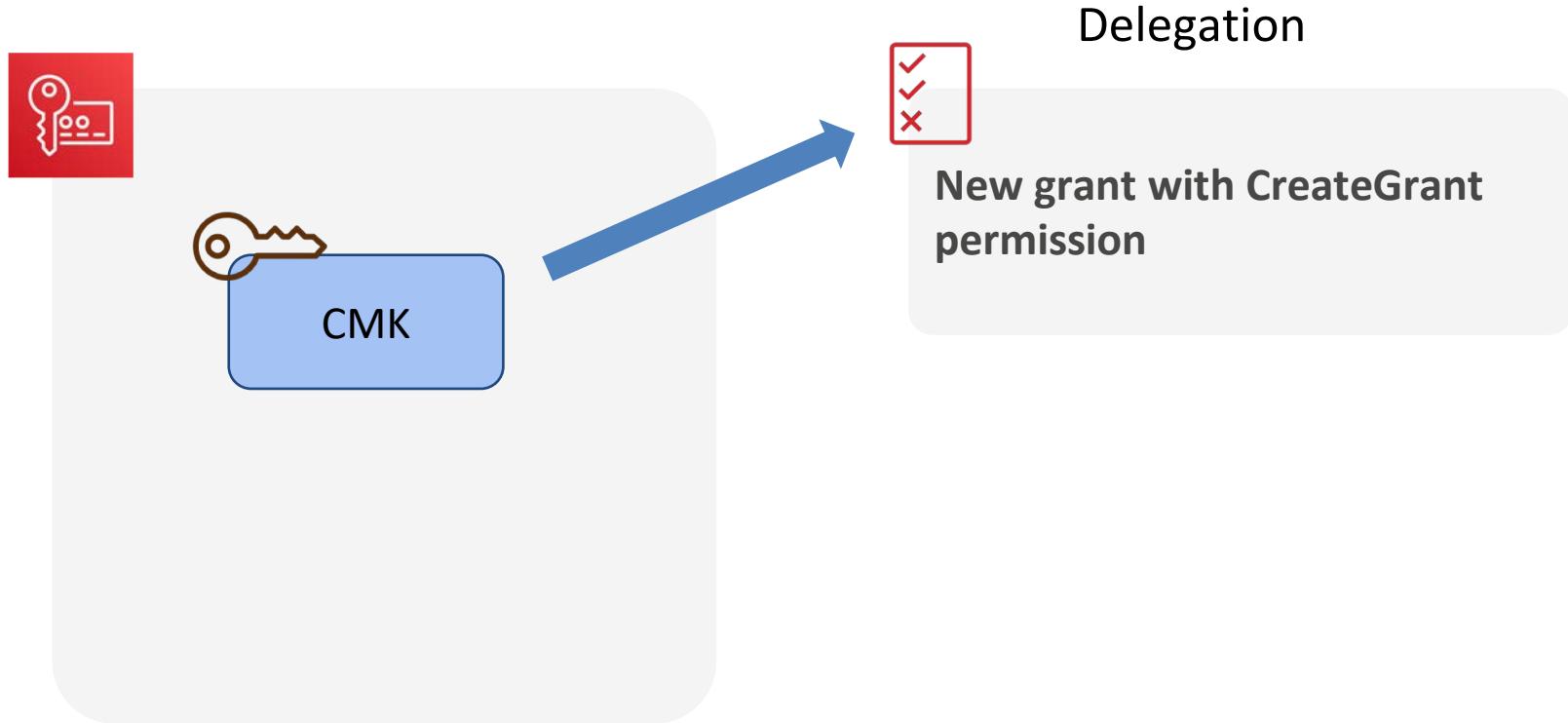
CMK



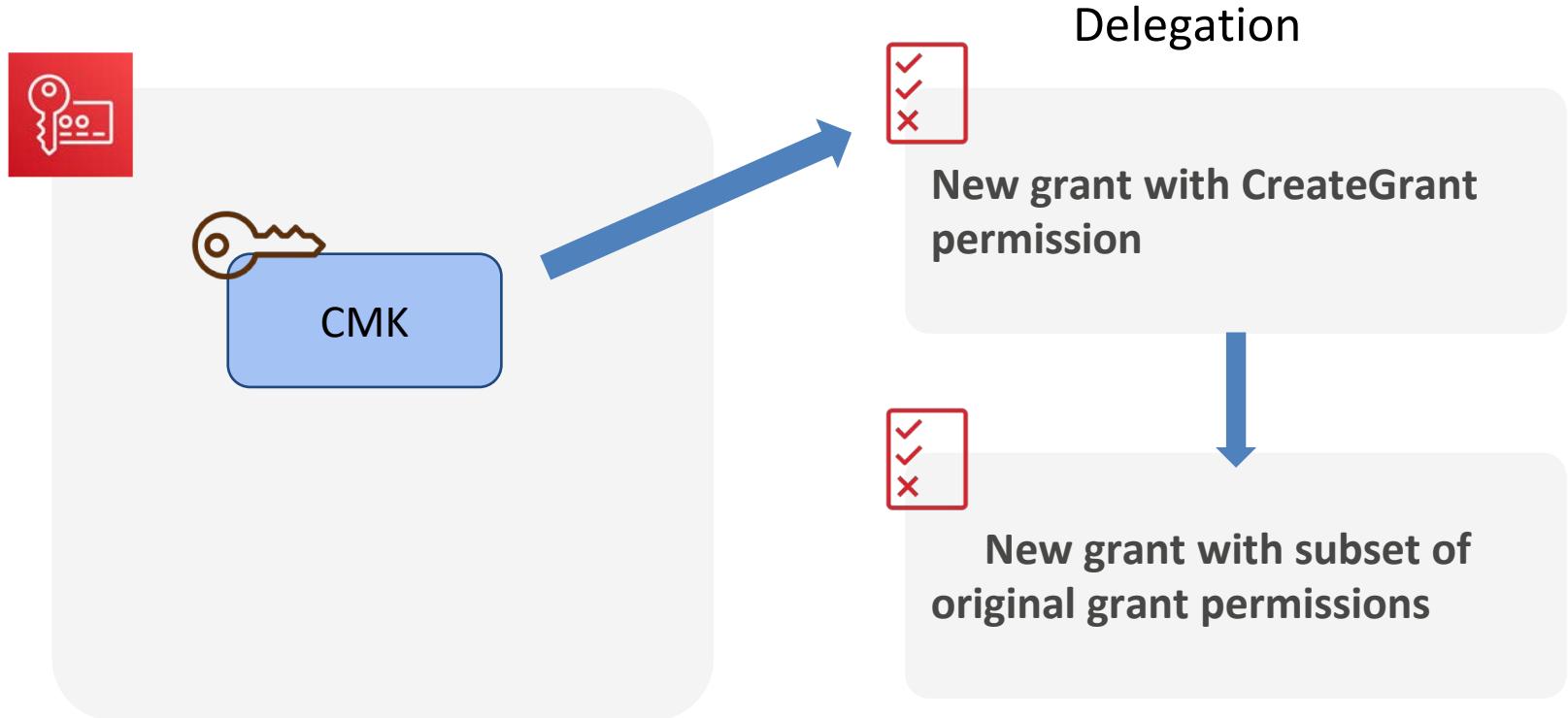
Basics

Delegate temporary permissions
Allow only, no deny
Not recommended for key management
Revoke at any time

KMS Access Control - Grants



KMS Access Control - Grants



AWS CloudHSM Basics

- Current
 - Dedicated generic HSM
- CloudHSM Classic
 - SafeNet technology
- AZ scoped
- Single tenancy
- Generate/store master keys
- Generate/store data keys
- Can encrypt data (bulk crypto)

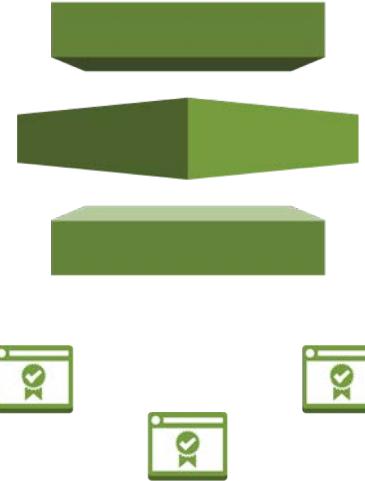


AWS CloudHSM Niches

- TDE for RDS Microsoft SQL Server
- TDE for RDS Oracle Server
- High-performance bulk crypto
- PKI (Public Key Infrastructure)
- Redshift database encryption with full chain of trust ownership

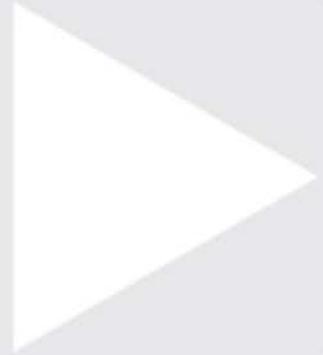
AWS Certificate Manager Basics

- Provision SSL/TLS certificates
 - Region scope
- Upload custom certificates
- Use in AWS web services
 - CloudFront
 - Elastic Load Balancer
 - API Gateway
- Managed renewal
- Private CA capability



Using Keys for Authentication

- EC2 keypair
 - SSH or decrypt Administrator password
- CodeCommit keypair
 - Git
- AWS Secrets Manager
 - Key/value pairs
 - DB connection strings
- AWS SSM Parameter Store
 - Unstructured or structured text



Data Protection

Troubleshoot Key Management

Troubleshooting - Scenarios

- Service cannot access KMS for encrypting objects
- Service cannot access KMS for decrypting objects
- Service cannot access CloudHSM for encryption or decryption
- Service cannot access secret for application authentication

Troubleshooting - Root Causes

- IAM Role permissions misconfigured
- KMS Key Policy misconfigured
- CMK backing key deleted
- Individual CloudHSM resource has failed



AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

An application has a requirement to **store data locally** on EC2 using encryption. The objects must be encrypted using **unique data keys**, and the application must be able to **delegate permission to each client** to decrypt the object once it is transferred to the client. Which solution meets these requirements in the **most secure and efficient** manner?

- A. Custom key management solution; all workloads handled by the application
- B. KMS; IAM role for application, KMS Key policy for application, KMS grant for clients
- C. CloudHSM; Built-in permissions for application and client
- D. KMS; Static credentials for application, IAM role for clients

Question Breakdown - Answers

Requires a lot of overhead to manage the infrastructure, not necessarily secure

- A. Custom key management solution; all workloads handled by the application
- B. KMS; IAM role for application, KMS Key policy for application, KMS grant for clients
- C. CloudHSM; Built-in permissions for application and client
- D. KMS; Static credentials for application, IAM role for clients

Question Breakdown - Answers

Meets requirements, uses least-privilege

- A. Custom key management solution; all workloads handled by the application
- B. KMS; IAM role for application, KMS Key policy for application, KMS grant for clients
- C. CloudHSM; Built-in permissions for application and client
- D. KMS; Static credentials for application, IAM role for clients

Question Breakdown - Answers

Secure, but requires a lot of permissions management

- A. Custom key management solution; all workloads handled by the application
- B. KMS; IAM role for application, KMS Key policy for application, KMS grant for clients
- C. CloudHSM; Built-in permissions for application and client
- D. KMS; Static credentials for application, IAM role for clients

Question Breakdown - Answers

Similar to B, appears to meet requirements?

- A. Custom key management solution; all workloads handled by the application
- B. KMS; IAM role for application, KMS Key policy for application, KMS grant for clients
- C. CloudHSM; Built-in permissions for application and client
- D. KMS; Static credentials for application, IAM role for clients

Question Breakdown - Correct Answer

Correct Answer:B

- A. Custom key management solution; all workloads handled by the application
- B. KMS; IAM role for application, KMS Key policy for application, KMS grant for clients
- C. CloudHSM; Built-in permissions for application and client
- D. KMS; Static credentials for application, IAM role for clients



Data Protection

Design and implement a data encryption solution for data at rest

Data Encrypted at Rest by Default

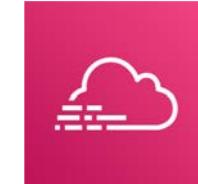
Glacier



Snowball



CloudTrail



Storage Gateway



DynamoDB



Elasticsearch



Data Encrypted at Rest by Default

FSx for Lustre



FSx for Windows



Secrets
Manager



Data Encrypted at Rest Optionally

RDS



RedShift



ElastiCache



DocumentDB



Neptune



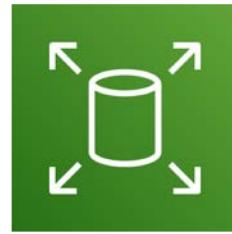
Databases

Data Encrypted at Rest Optionally

EFS



EBS



S3



Filesystems and Object Storage

Data Encrypted at Rest Optionally

SQS



SNS



Kinesis



Messaging

Data Encrypted at Rest Optionally

CloudWatch
Logs



SSM
Parameter
Store



Other

Encrypting Data at Rest - Operations

- Enable encryption upon resource creation
 - Least overall effort
- Enable encryption after resource creation
 - More effort and not always possible
- Disable encryption after creation
 - More effort, but always possible



Data Protection

Design and implement a data encryption solution for data in transit

Data Encrypted in Transit - Options

CloudFront



Elastic
Load
Balancer



API
Gateway



Web Traffic Using TLS

Data Encrypted in Transit - Options

RDS



RedShift



Elasticache



Database Traffic Using TLS

Data Encrypted in Transit - Options

FSx for Lustre



FSx for Windows



EFS



Storage Traffic Encryption

Data Encrypted in Transit - Options

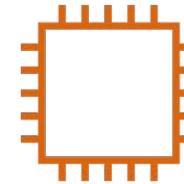
VPG with VPN



Direct Connect
with VPN



DIY on EC2



Network Traffic Using IPSEC

Encrypting Data in Transit - AWS API

- All services support SSL/TLS
- Can enforce via IAM policy conditions
- Recognize where encryption impacts performance



AWS Certified Security - Specialty Crash Course

Question Breakdown

Question Breakdown - Key Terms

For regulatory reasons, your application data must be **encrypted** during all steps of every workflow, both **in-transit and at rest**. The storage of data on the back end of the application is entirely **filesystem-based**. Which **storage options** meet the requirement of in-transit and at-rest encryption? (pick two)

- A. EFS volume, encrypted filesystem, and EFS mount helper on all clients
- B. Instance-store volumes, no extra configuration
- C. EBS volume, no extra configuration
- D. EBS volume, volume encryption enabled
- E. EFS volume, no extra configuration
- F. AWS Storage Gateway - File Gateway, no extra configuration

Question Breakdown - Answers

This meets both requirements

- A. EFS volume, encrypted filesystem, and EFS mount helper on all clients
- B. Instance-store volumes, no extra configuration
- C. EBS volume, no extra configuration
- D. EBS volume, volume encryption enabled
- E. EFS volume, no extra configuration
- F. AWS Storage Gateway - File Gateway, no extra configuration

Question Breakdown - Answers

There is no native encryption on instance-store volumes

- A. EFS volume, encrypted filesystem, and EFS mount helper on all clients
- B. Instance-store volumes, no extra configuration
- C. EBS volume, no extra configuration
- D. EBS volume, volume encryption enabled
- E. EFS volume, no extra configuration
- F. AWS Storage Gateway - File Gateway, no extra configuration

Question Breakdown - Answers

EBS volumes are not encrypted by default

- A. EFS volume, encrypted filesystem, and EFS mount helper on all clients
- B. Instance-store volumes, no extra configuration
- C. EBS volume, no extra configuration
- D. EBS volume, volume encryption enabled
- E. EFS volume, no extra configuration
- F. AWS Storage Gateway - File Gateway, no extra configuration

Question Breakdown - Answers

Enabling volume encryption meets all requirements

- A. EFS volume, encrypted filesystem, and EFS mount helper on all clients
- B. Instance-store volumes, no extra configuration
- C. EBS volume, no extra configuration
- D. EBS volume, volume encryption enabled
- E. EFS volume, no extra configuration
- F. AWS Storage Gateway - File Gateway, no extra configuration

Question Breakdown - Answers

EFS volumes have no encryption enabled by default

- A. EFS volume, encrypted filesystem, and EFS mount helper on all clients
- B. Instance-store volumes, no extra configuration
- C. EBS volume, no extra configuration
- D. EBS volume, volume encryption enabled
- E. EFS volume, no extra configuration
- F. AWS Storage Gateway - File Gateway, no extra configuration

Question Breakdown - Answers

This is a tricky one - File Gateway encrypts data at rest and in transit to S3 but does not encrypt from the NFS clients to the gateway itself

- A. EFS volume, encrypted filesystem, and EFS mount helper on all clients
- B. Instance-store volumes, no extra configuration
- C. EBS volume, no extra configuration
- D. EBS volume, volume encryption enabled
- E. EFS volume, no extra configuration
- F. AWS Storage Gateway - File Gateway, no extra configuration

Question Breakdown - Correct Answer

Correct Answer:A,D

- A. EFS volume, encrypted filesystem, and EFS mount helper on all clients
- B. Instance-store volumes, no extra configuration
- C. EBS volume, no extra configuration
- D. EBS volume, volume encryption enabled
- E. EFS volume, no extra configuration
- F. AWS Storage Gateway - File Gateway, no extra configuration



AWS Certified Security - Specialty Crash Course

Next Steps

Next Steps 1

- Sample questions
 - Why correct answer is correct
 - Why incorrect answer is incorrect
 - Recognize gaps in your knowledge
- Study
 - ***Subjects*** identified by gaps

Next Steps 2

- Practice test
 - Why correct answer is correct
 - Why incorrect answer is incorrect
 - Recognize gaps in your knowledge
- Study
 - ***Question domains*** identified by gap
- Take the exam!

Thank You!

Thank you for
attending!