



AWS Certified Solutions
Architect - Professional Exam
Crash Course
-Chad Smith



Exam Guide and Logistics

Exam Logistics - By the Numbers

Number of questions:	75
Time for exam	180 minutes
Answer choices	4-6
Score required	750/1000
Number of unscored questions	10
Penalty for guessing	0

Question Domains

12.5% Design for Organizational Complexity

31% Design for New Solutions

15% Migration Planning

12.5% Cost Control

29% Continuous Improvement for Existing Solutions

Exam Guide As A Job Description

Validating an examinee's ability to:

Design **and deploy** dynamically scalable, highly available, fault-tolerant, and reliable applications on AWS.

Well-Architected Framework pillars represented here.

Bold red text is the difference between Associate and Professional

Exam Guide As A Job Description

Validating an examinee's ability to:

Select appropriate AWS services to design ***and***
deploy an application based on given requirements.

Again, "deploy" is what separates Associate from Professional. You must have the skills to do both!

Exam Guide As A Job Description

Validating an examinee's ability to:

Migrate **complex**, multi-tier applications on AWS.

Migration requires a combination of architecture and operational skills, and scenarios frequently require math skills for times and data sizes

Exam Guide As A Job Description

Validating an examinee's ability to:

Design and deploy ***enterprise-wide*** scalable operations on AWS.

Scalable implies automation. Learn the AWS offerings which centralize and automate operations!

Exam Guide As A Job Description

Validating an examinee's ability to:

Implement cost-control strategies.

This is more than just designing or recognizing cost optimized architectures - this is implementation and improvement

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

2 or more years of hands-on experience designing and deploying cloud architecture on AWS

It is EXTREMELY difficult to memorize your way to this certification. Hands-on experience is vital!

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Ability to evaluate cloud application requirements and make architectural recommendations for implementation, deployment, and provisioning applications on AWS

This requires end-to-end skills and cannot be achieved by simply being proficient in one area

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Ability to provide best practice guidance on the architectural design across multiple applications and projects of the enterprise

It is critical to know how multi-region and multi-account architectures integrate and communicate with each other

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Familiarity with a scripting language

It is more important to understand what can be automated via scripting than to be proficient with a single language

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Familiarity with Windows and Linux environments

This is primarily for OS configuration, operations, patching, and other tasks - and how to perform them in AWS

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Familiarity with AWS CLI, AWS APIs, AWS CloudFormation templates, the AWS Billing Console, and the AWS Management Console

Learn the different ways of interacting with AWS, either for manual or automated tasks

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Explain and apply the five pillars of the AWS Well-Architected Framework

Self-explanatory. That said, know these IN DETAIL!

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Map business objectives to application/architecture requirements

This is different than translating technical requirements and requires extra skills

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Design a hybrid architecture using key AWS technologies (e.g., VPN, AWS Direct Connect)

This is much like the skills tested in the Advanced Networking - Specialty certification

Exam Guide As A Job Description

Recommended AWS and General IT Knowledge and Experience

Architect a continuous integration and deployment process

This is much like the skills tested in the DevOps - Professional certification



Domain 1: Design for Organizational Complexity

12.5%

Question Domain 1 Points

1.1 Determine cross-account authentication and access strategy for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements)

Question Domain 1 Points

1.2 Determine how to design networks for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements)

Question Domain 1 Points

1.3 Determine how to design a multi-account AWS environment for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements)



Multi-Account Scenario

Scenario Description

A company has many AWS accounts that have been provisioned in an AWS Organization using the CLI. No actions have been taken to configure the accounts after creation except using cross-account IAM roles and Organizations SCPs for compliance purposes.

The company is divesting one business unit as a separate company.

The AWS admins for the new company have attempted to leave the AWS Organization, but the action fails.

What could be the cause?

Scenario Questions to Ask



What would a multi-account Organization look like?
How are accounts created?
How can an account leave the organization?

Multiple Accounts Using Organizations

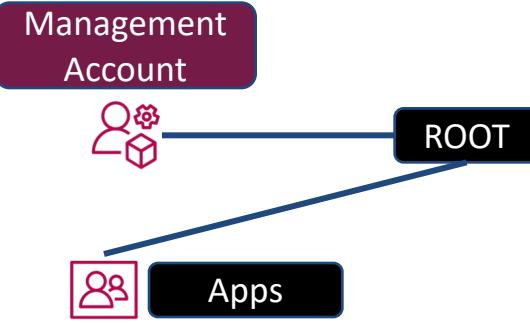
Management
Account



ROOT

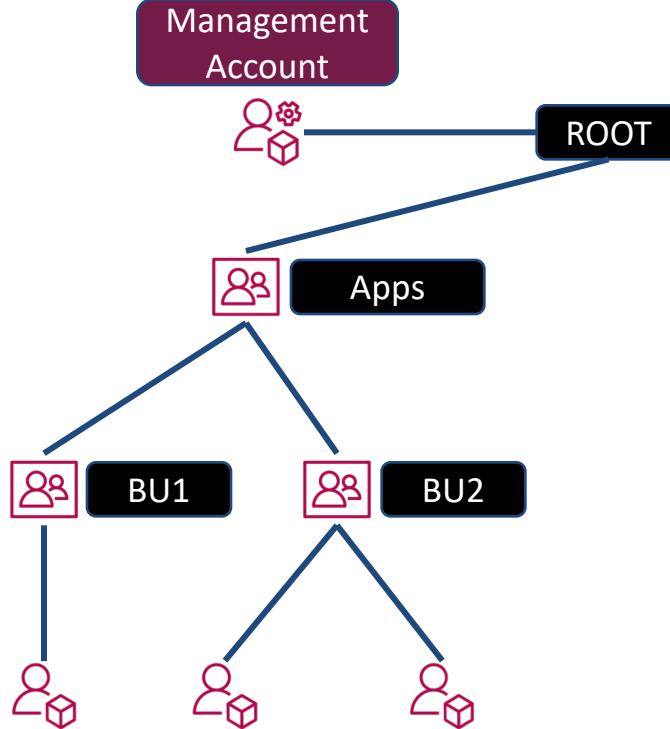
The Management account has very few resources such as SSO

Multiple Accounts Using Organizations



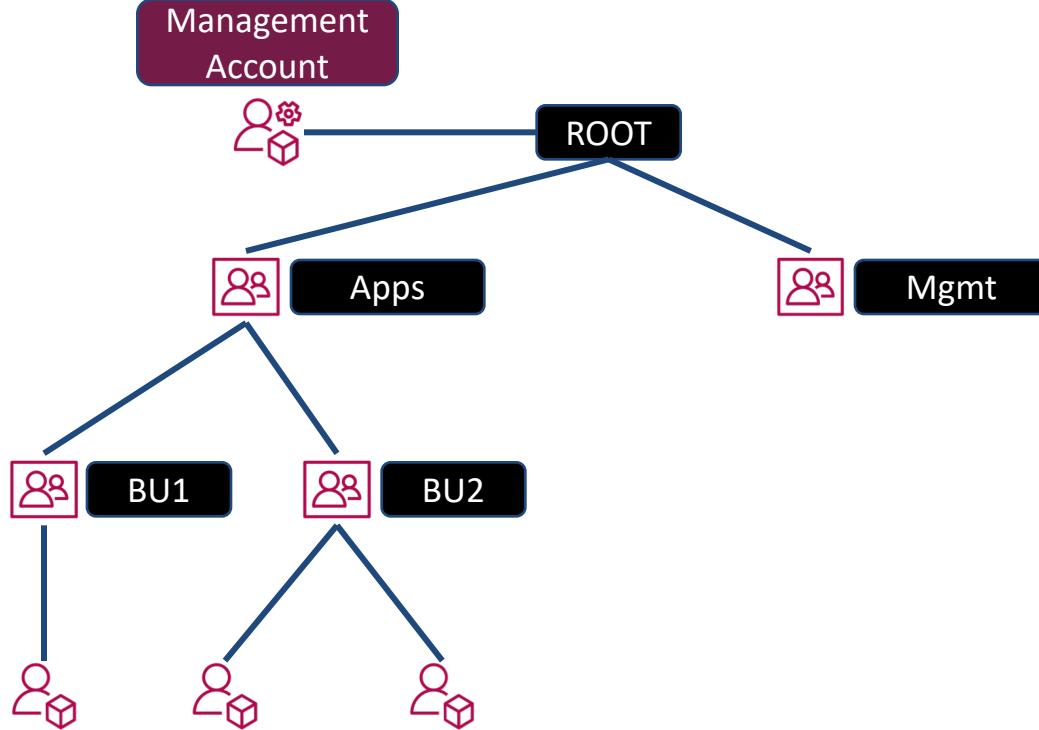
The Apps OU is
for all product
related
infrastructure

Multiple Accounts Using Organizations



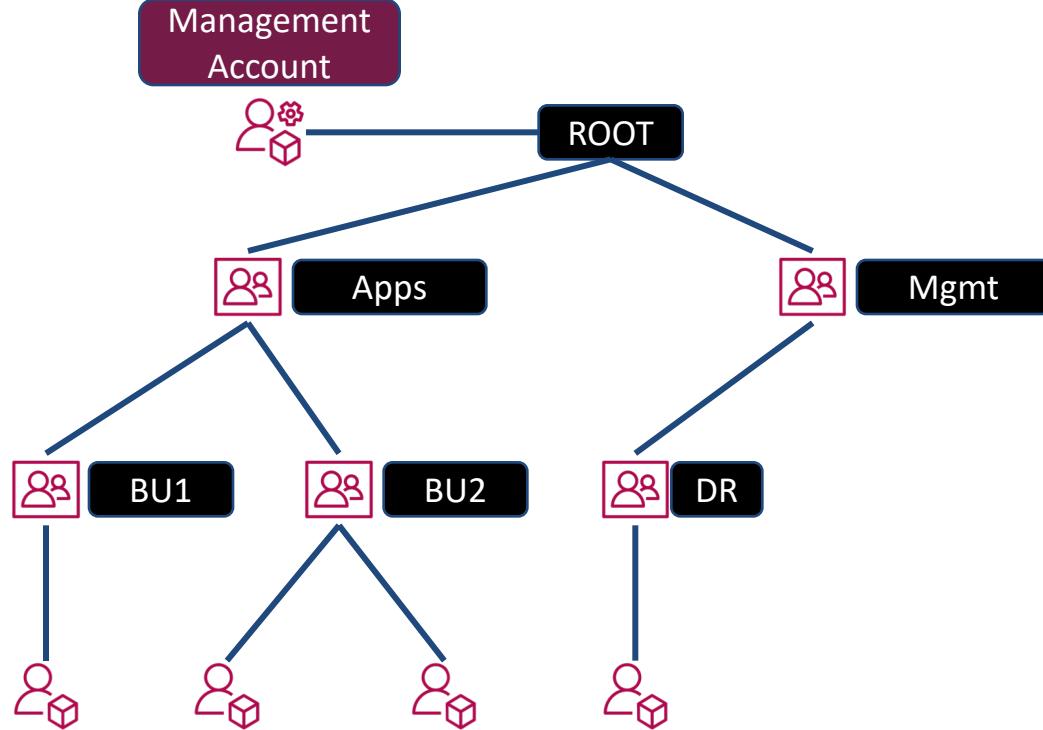
Create OUs for departmental or business unit environments

Multiple Accounts Using Organizations



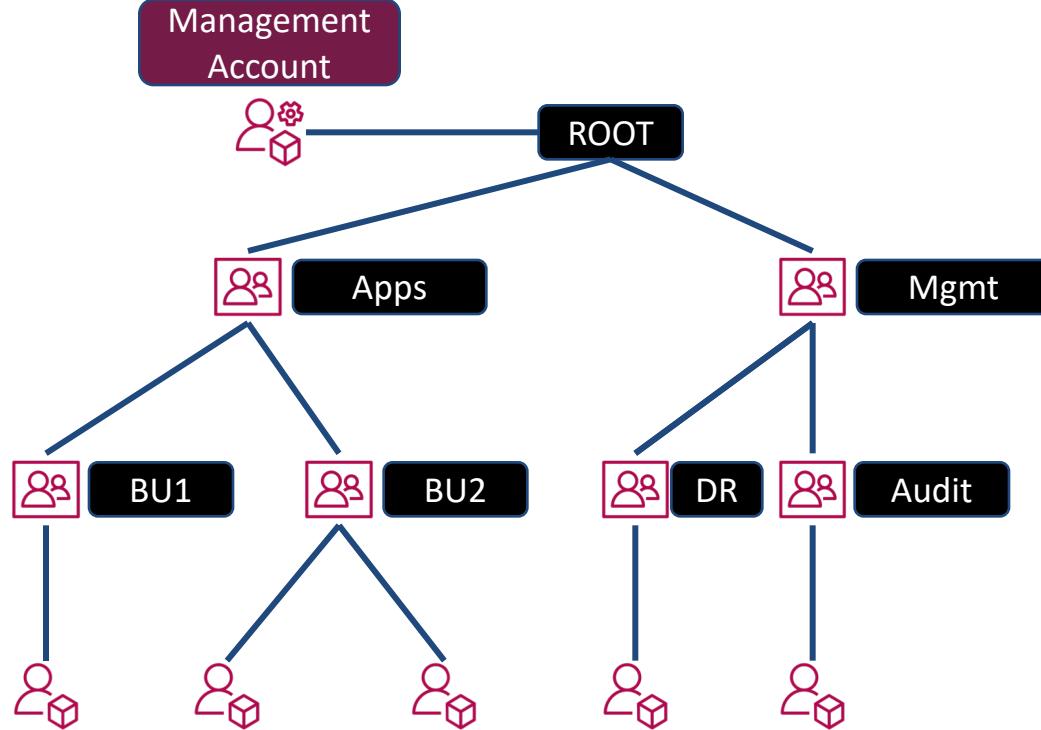
Another OU for
all management
activities

Multiple Accounts Using Organizations



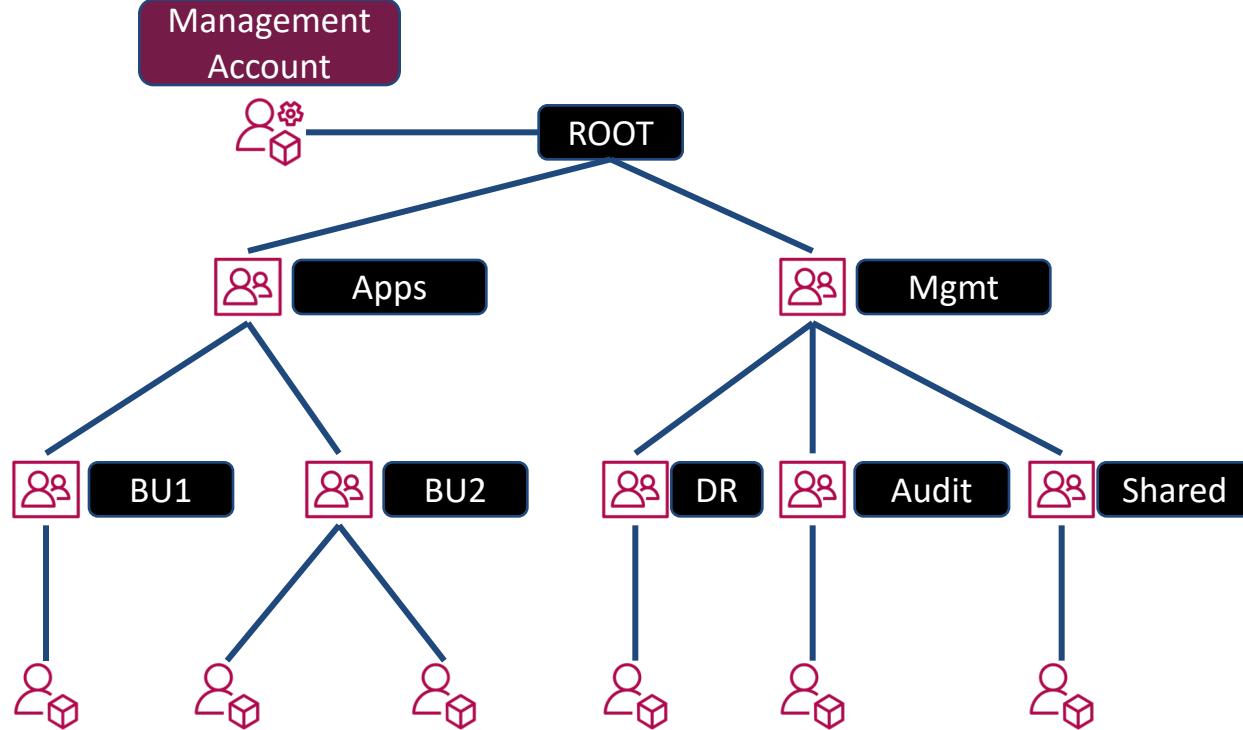
Business continuity is isolated into an OU and separate account

Multiple Accounts Using Organizations



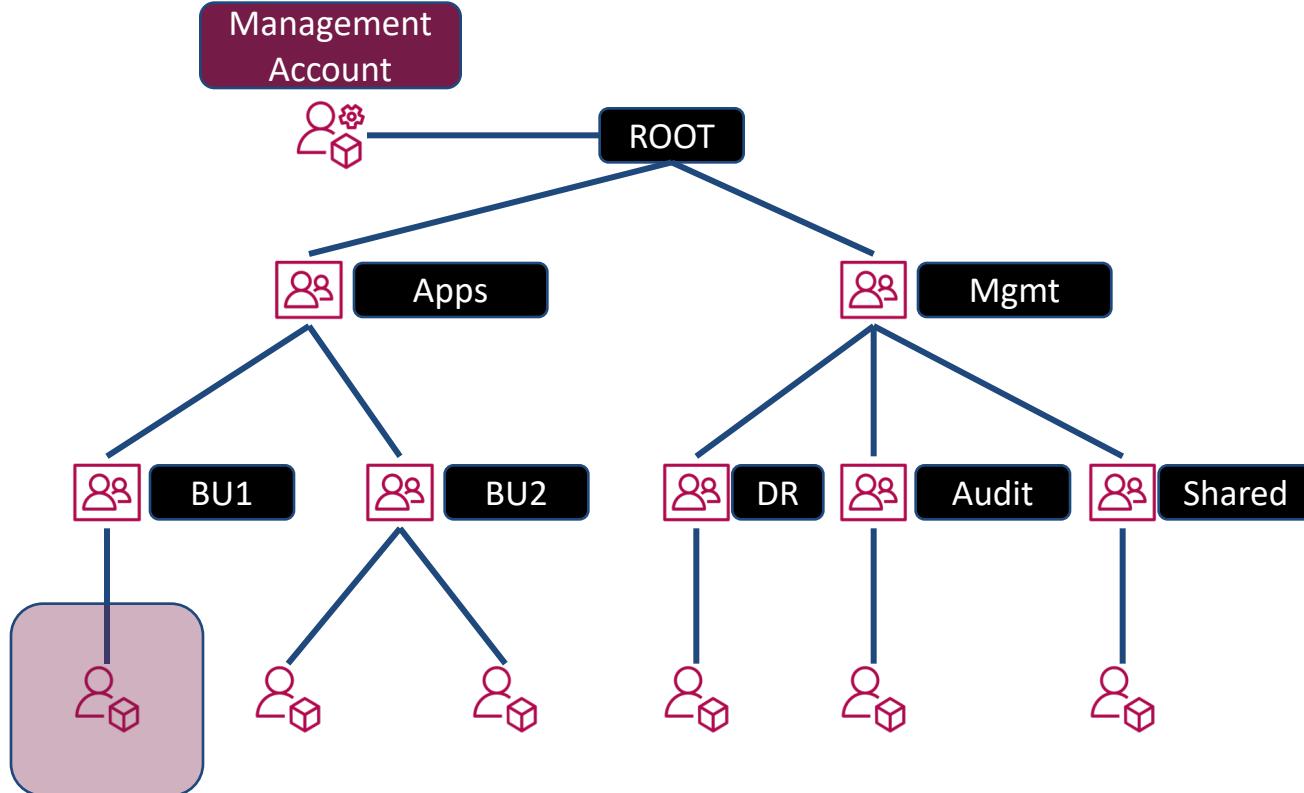
So is security and compliance auditing infrastructure

Multiple Accounts Using Organizations



Finally, all shared resources can be placed in a separate OU and account

Multiple Accounts Using Organizations



How does an AWS account leave an Organization?

First, let's cover what happens when accounts are created via Organizations CLI

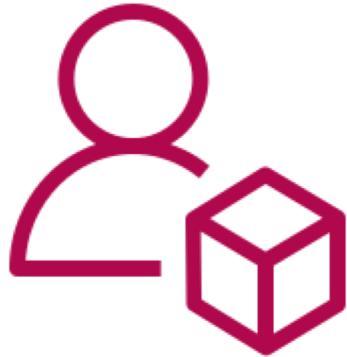
AWS Account Creation Using CLI

```
aws organizations create-account \
--email <valid-email-address> \
--account-name <unique descriptive name>
```

This is all the information required to provision an account

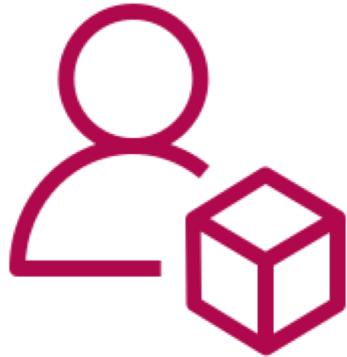
Can this account operate standalone with this information?

Requirements for Standalone Account



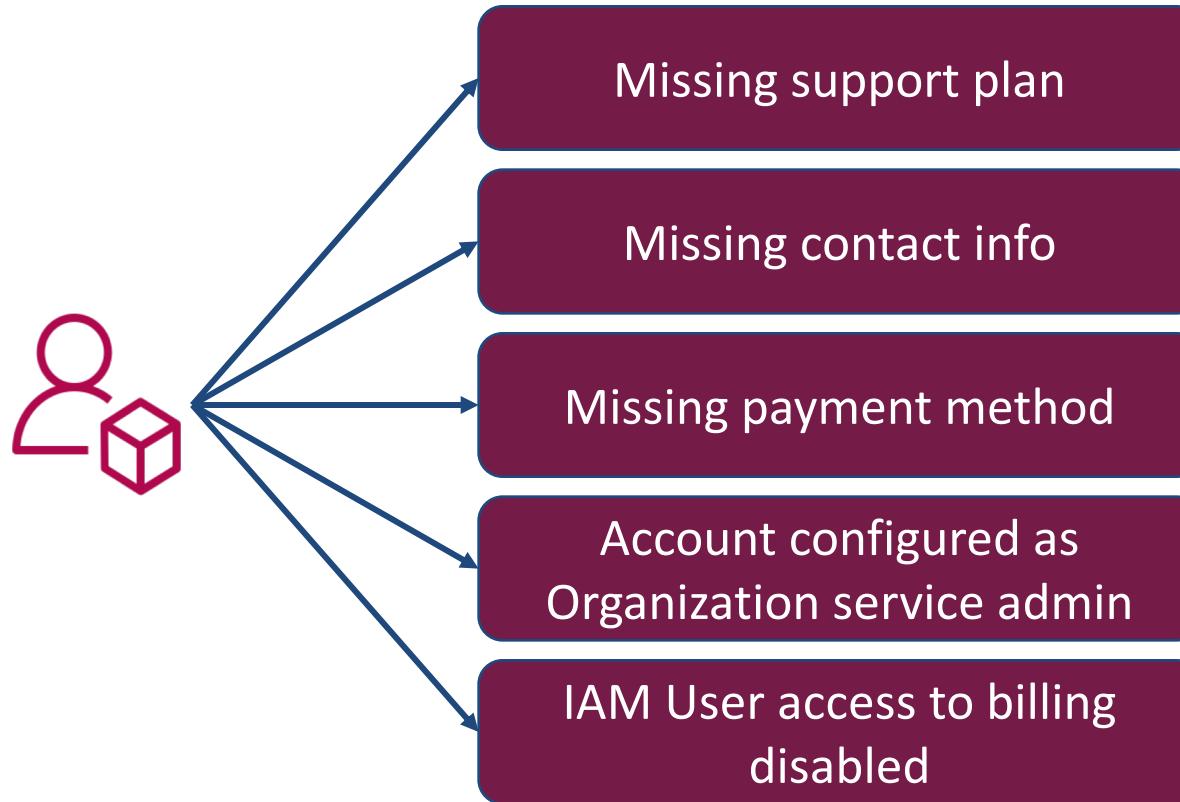
- Support plan
- Verified contact info
- Payment method
- Root acct password?

Leave Organization as Member Account



- Cannot be delegated admin account for any Organization service
- Appropriate permissions
- Enable IAM user access to billing

Scenario Root Cause Possibilities



Question Breakdown

Question Scenario

Your company has several AWS accounts, all using Consolidated Billing.

In the payer account, a user wants to view the Cost Allocation Report, organized by a tag named "costcenter" that is used in all accounts.

The Cost Allocation Report is missing the required tag.

What actions can resolve the issue?
(pick two)

Answer Choices

- A. In the payer account, use the AWS CLI with appropriate permissions to enable a User-Defined Cost Allocation Tag for "costcenter"
- B. In the payer account and all member accounts, use the AWS CLI with appropriate permissions to enable a User-Defined Cost Allocation Tag for "costcenter"
- C. In the payer account, log into the AWS Console and enable a User-Defined Cost Allocation Tag for "costcenter"
- D. In the payer account and all member accounts, log into the AWS Console and enable a User-Defined Cost Allocation Tag for "costcenter"
- E. Submit a request to AWS Support to enable the User-Defined Cost Allocation Tag

Answer A

When viewing the various services and their availability in the CLI, there is newly implemented (06/2022) integration for Cost Allocation tags, therefore this is a viable option.

In the payer account, use the AWS CLI with appropriate permissions to enable a User-Defined Cost Allocation Tag for "costcenter"

Answer B

You cannot implement Cost Allocation tags in a member account while using Consolidated Billing (or Organizations).

In the payer account and all member accounts, use the AWS CLI with appropriate permissions to enable a User-Defined Cost Allocation Tag for "costcenter"

Answer C

Answers C and D follow a similar pattern to A and B. When working with Consolidated Billing (and Organizations), User-Defined Cost Allocation Tags are enabled in the management/payer account only.

In the payer account, log into the AWS Console and enable a User-Defined Cost Allocation Tag for "costcenter"

Answer D

This is similar to C, with the impossible step of attempting to enable Cost Allocation Tags in the member accounts. Only the payer account is required to make the change.

In the payer account and all member accounts, log into the AWS Console and enable a User-Defined Cost Allocation Tag for "costcenter"

Answer E

This is similar to C, with the unnecessary step of attempting to enable Cost Allocation Tags in the member accounts. Only the payer account is required to make the change.

In the payer account and all member accounts, log into the AWS Console and enable a User-Defined Cost Allocation Tag for "costcenter"

Correct Answers

- A. In the payer account, use the AWS CLI with appropriate permissions to enable a User-Defined Cost Allocation Tag for "costcenter"
- B. In the payer account and all member accounts, use the AWS CLI with appropriate permissions to enable a User-Defined Cost Allocation Tag for "costcenter"
- C. In the payer account, log into the AWS Console and enable a User-Defined Cost Allocation Tag for "costcenter"
- D. In the payer account and all member accounts, log into the AWS Console and enable a User-Defined Cost Allocation Tag for "costcenter"
- E. Submit a request to AWS Support to enable the User-Defined Cost Allocation Tag



Multi-Network Scenario

Scenario Description

An enterprise has hundreds of AWS accounts with at least one VPC in each, in many regions. The CIDR ranges do not overlap. The VPCs are used to host a mix of non-production and production applications.

A new mandate has been given for a global enterprise-wide network to be established using the existing VPCs.

The global network solution must be reliable, scalable, secure and minimize operational overhead.

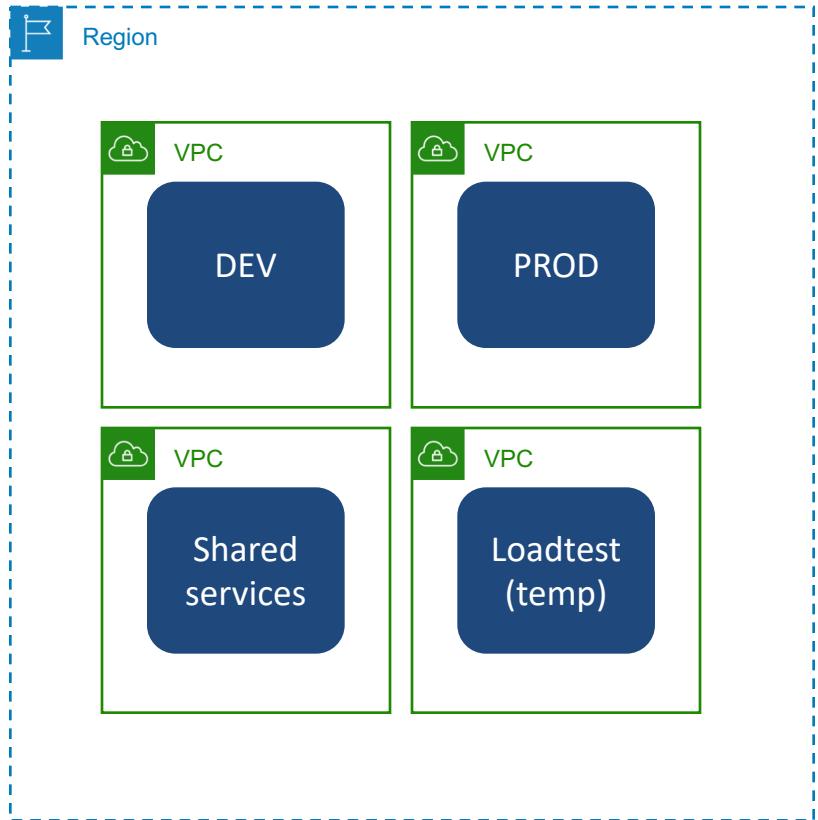
What solution should be proposed to meet these requirements?

Scenario Questions to Ask



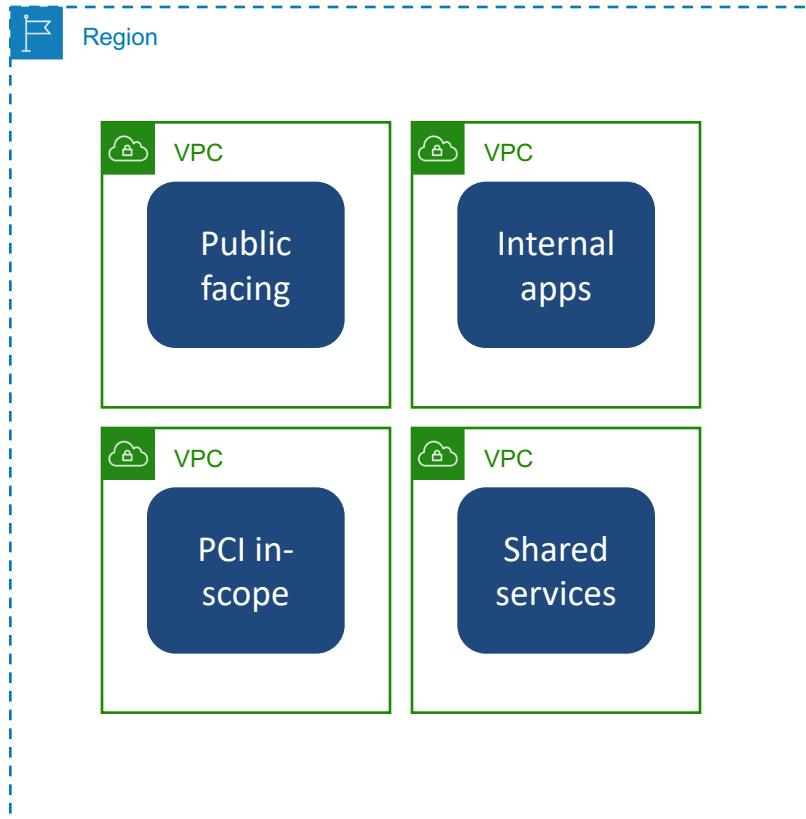
- How do workloads get distributed into many VPCs?
- What is a global network?
- What are the options for connecting VPC networks to each other?

VPC Workload Isolation Strategies



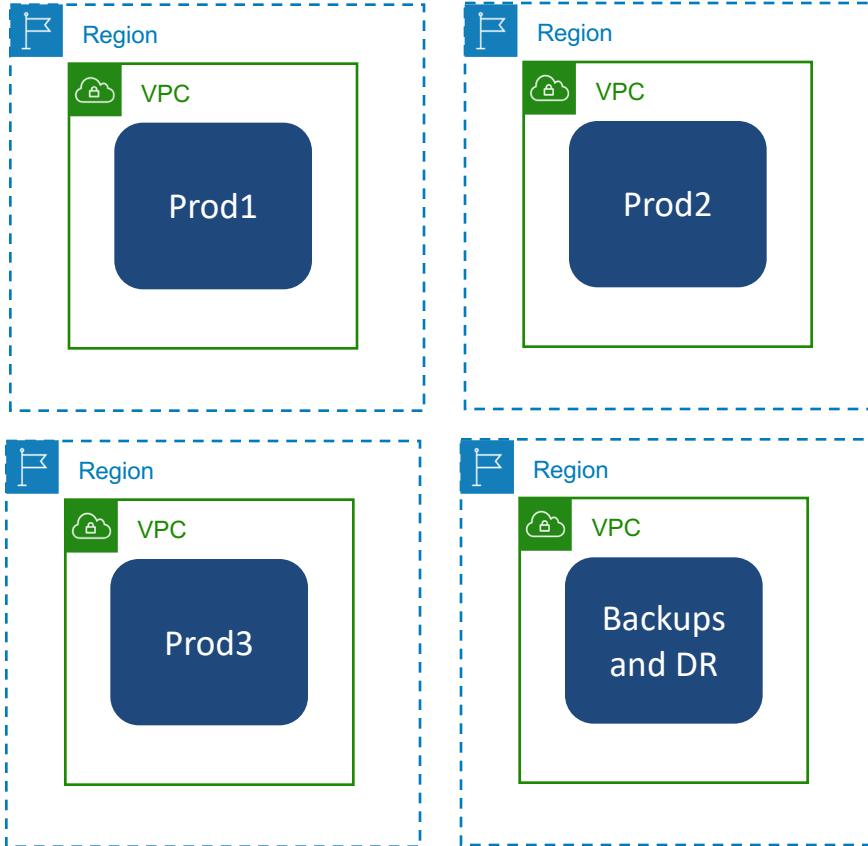
Organize by
environment

VPC Workload Isolation Strategies



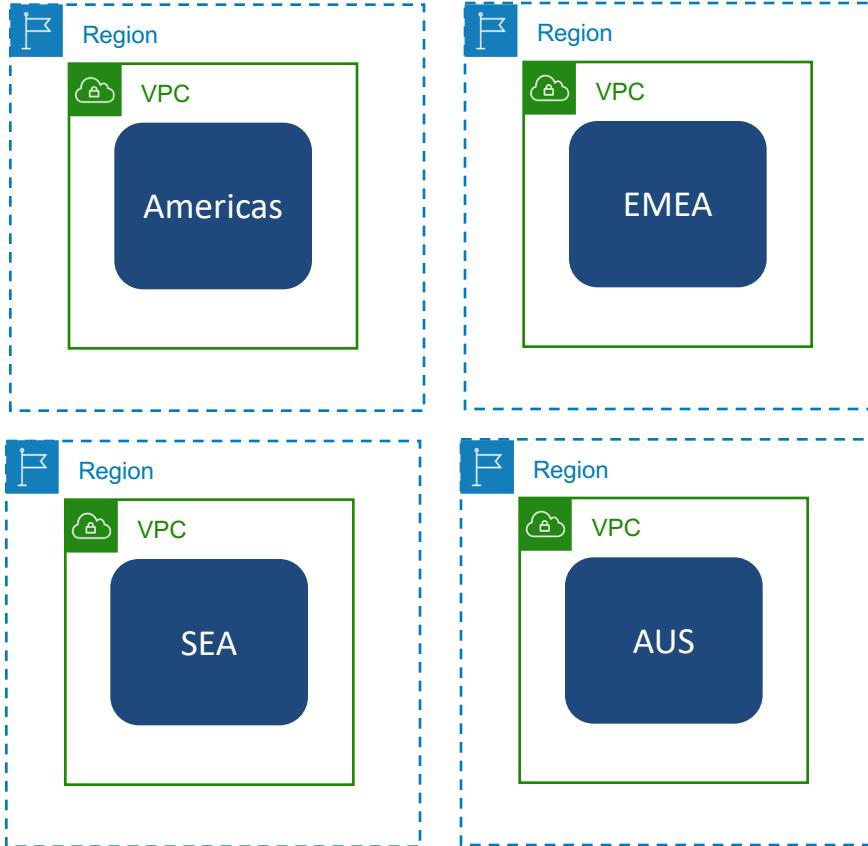
Organize by workload
compliance

VPC Workload Isolation Strategies



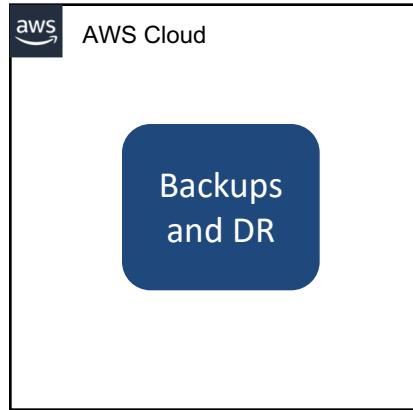
Organize by business continuity

VPC Workload Isolation Strategies

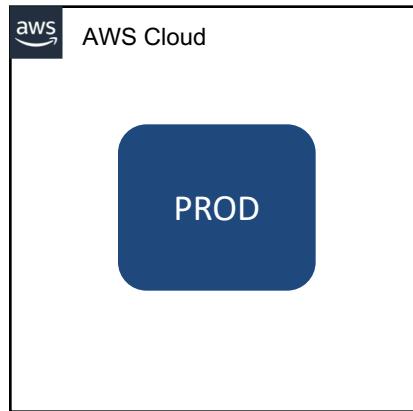
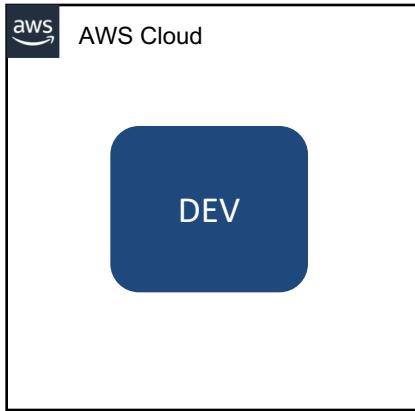


Organize by data sovereignty

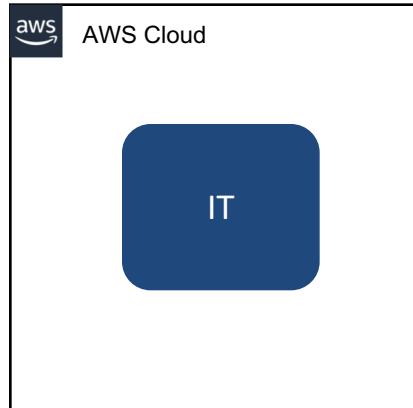
VPC Workload Isolation Strategies



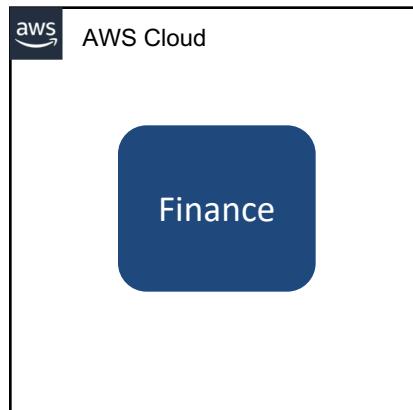
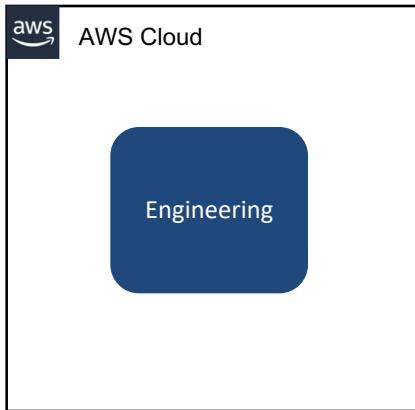
Organize by security requirements



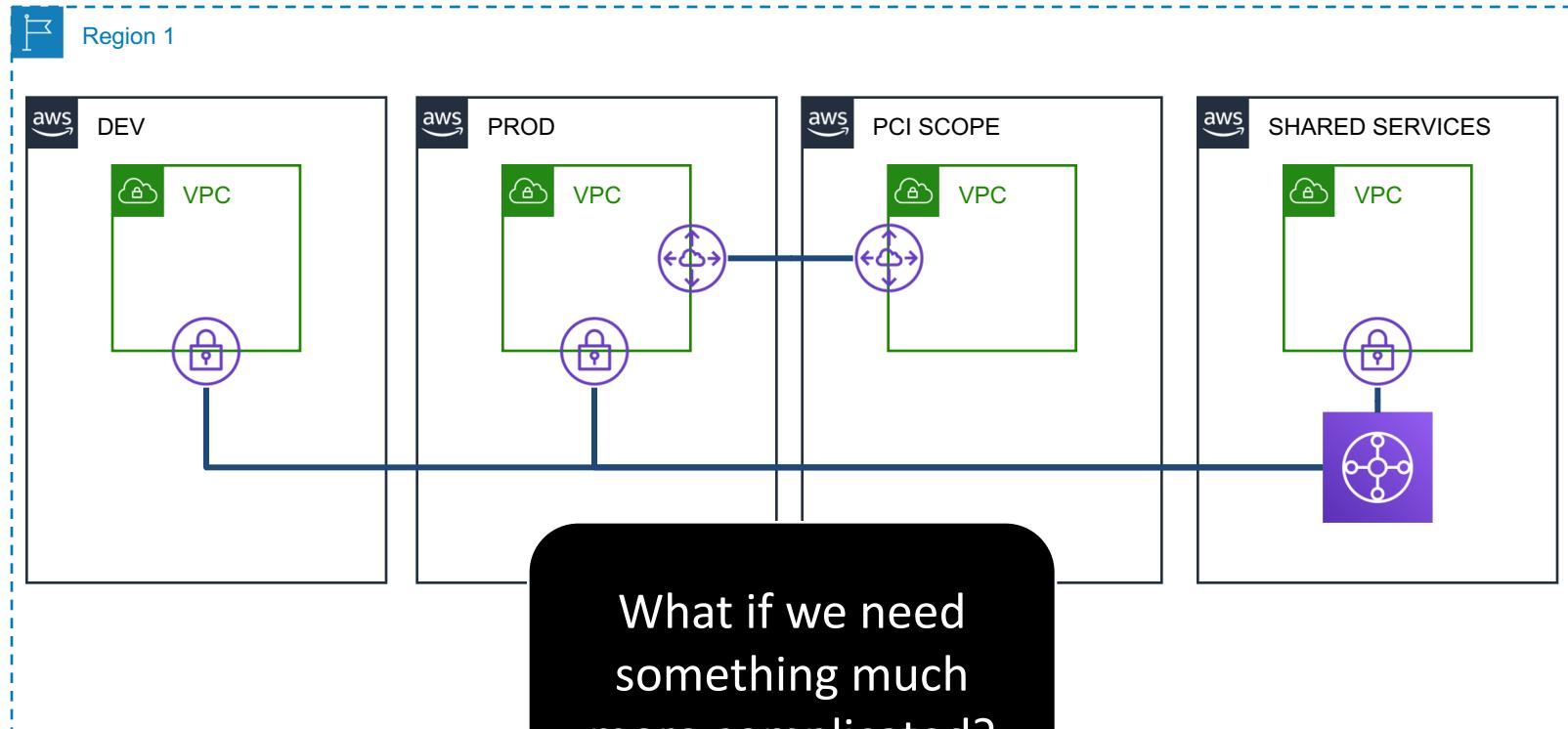
VPC Workload Isolation Strategies



Organize to match
company hierarchy



Simple Global Multi-Account Network

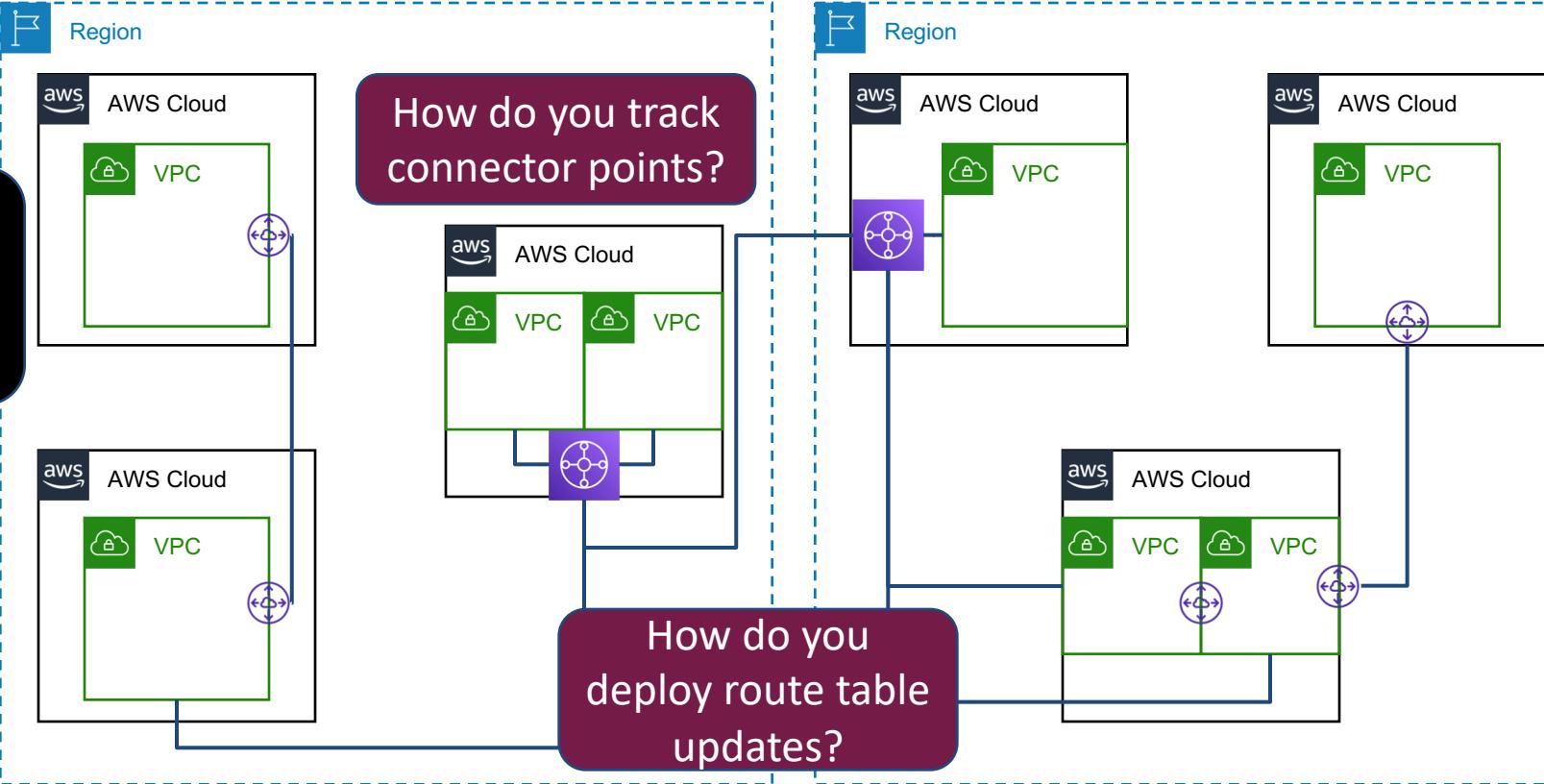


Complex Multi-Account Network

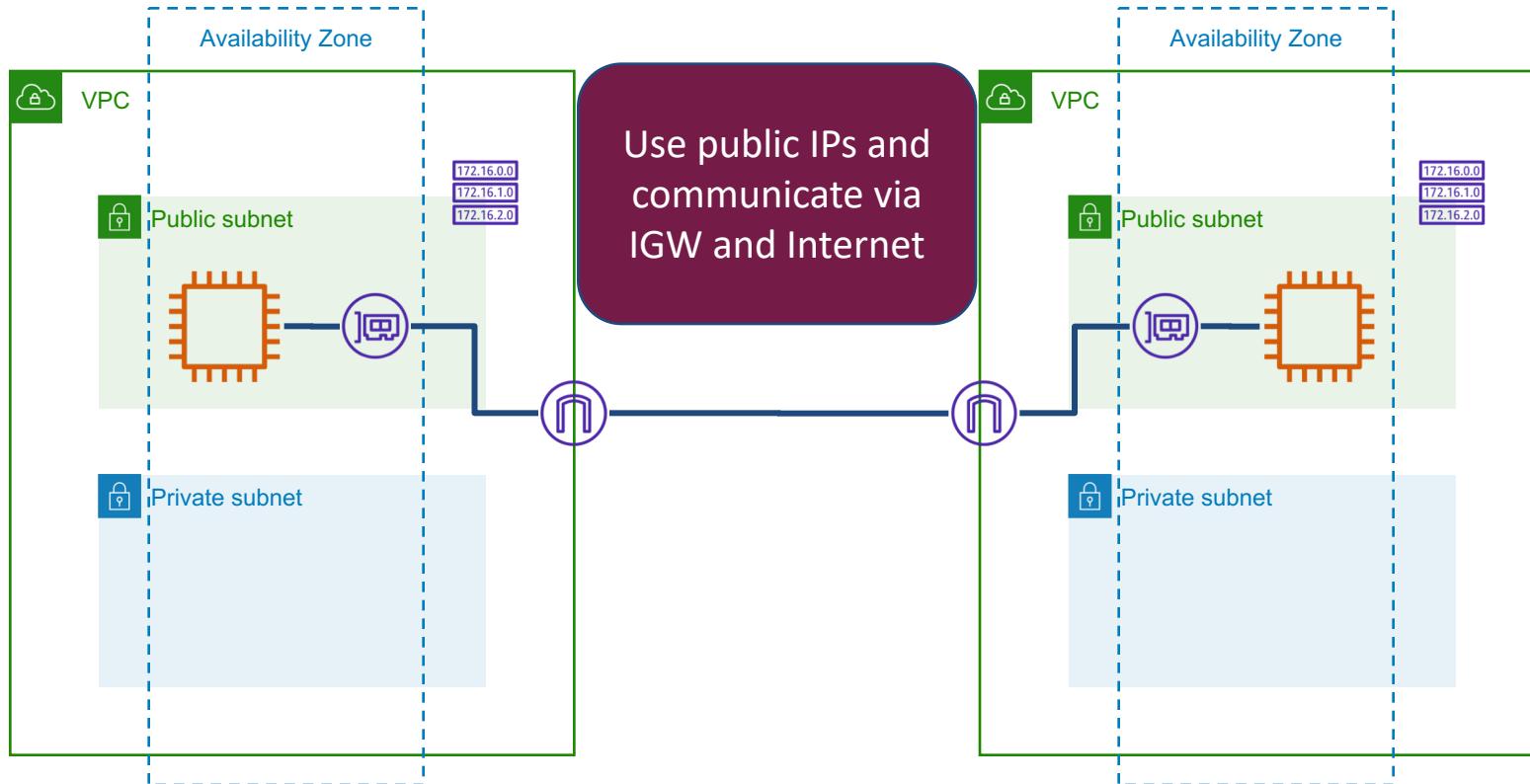
Can this possibly scale?

How do you track connector points?

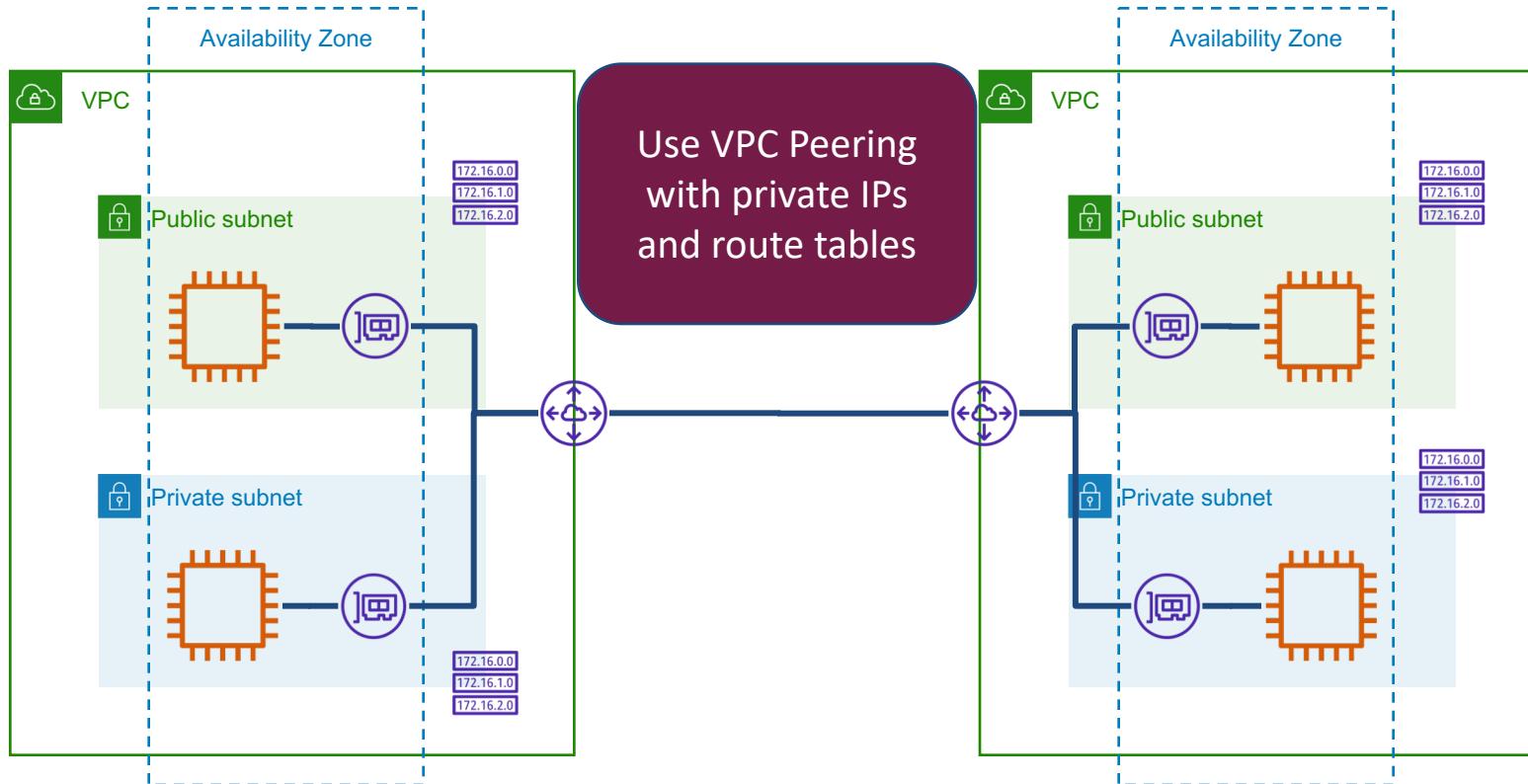
How do you deploy route table updates?



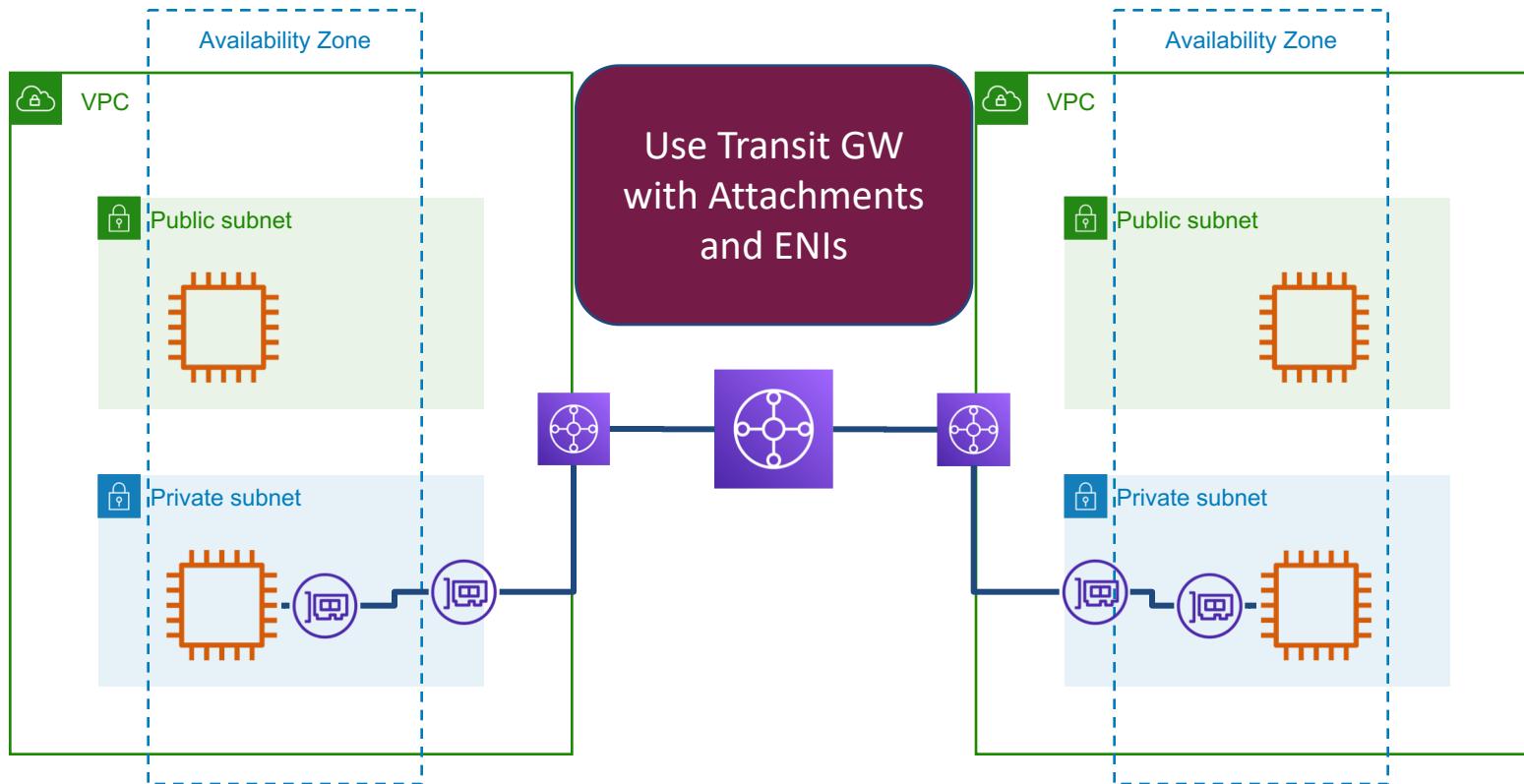
VPC to VPC Connectivity Options



VPC to VPC Connectivity Options



VPC to VPC Connectivity Options



Other Options

EC2 to VPG VPN



Other Options

EC2 to VPG VPN



NLB and PrivateLink



Other Options

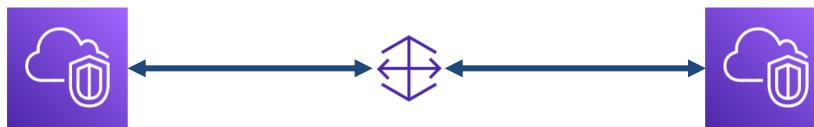
EC2 to VPG VPN



NLB and PrivateLink



Direct Connect Gateway



Other Options

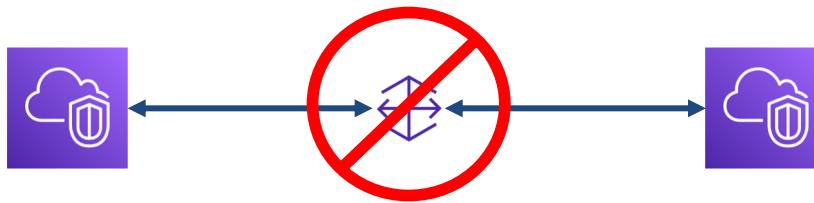
EC2 to VPG VPN



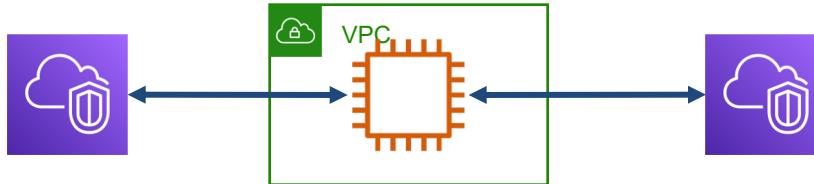
NLB and PrivateLink



Direct Connect Gateway



Transit VPC with EC2



Option Summary

IGW and Public IP

Scalable

Efficient

Option Summary

IGW and Public IP

Scalable

Efficient

VPC Peering

Reliable

Secure

Option Summary

IGW and Public IP

Scalable

Efficient

VPC Peering

Reliable

Secure

Transit GW

Reliable

Scalable

Secure

Efficient

Option Summary

IGW and Public IP

Scalable

Efficient

VPC Peering

Reliable

Secure

Transit GW

Reliable

Scalable

Secure

Efficient

EC2 VPN

Secure

Option Summary

IGW and Public IP

Scalable

Efficient

VPC Peering

Reliable

Secure

Transit GW

Reliable

Scalable

Secure

Efficient

EC2 VPN

Secure

NLB/PrivateLink

Reliable

Secure

Option Summary

IGW and Public IP	Scalable	Efficient		
VPC Peering	Reliable	Secure		
Transit GW	Reliable	Scalable	Secure	Efficient
EC2 VPN	Secure			
NLB/PrivateLink	Reliable	Secure		
DX GW	Reliable	Scalable	Secure	Efficient

Option Summary

IGW and Public IP	Scalable	Efficient		
VPC Peering	Reliable	Secure		
Transit GW	Reliable	Scalable	Secure	Efficient
EC2 VPN		Secure		
NLB/PrivateLink	Reliable	Secure		
DX GW	Reliable	Scalable	Secure	Efficient
Transit VPC		Efficient		

Question Breakdown

Question Scenario

A company's VPCs are all configured within the 10.1.0.0/16 CIDR range. The on-premises data center CIDR range is 10.0.0.0/20, which has several unused ranges currently. There is an on-premises inventory software licensed for the 10.0.0.0/20 range which cannot be changed.

Upper management wants to use the inventory software in the AWS VPC networks.

Which combination of the following will meet the requirements with the least effort?
(pick two)

Answer Choices

- A. Create new VPC networks using the open 10.0.0.0/20 CIDR ranges.
Manually migrate all instances to the new networks
- B. Add secondary CIDR ranges to all existing VPCs within the 10.0.0.0/20 range and create subnets to match the existing ranges. Add secondary ENIs to all EC2 instances in the new subnets
- C. Add secondary IP addresses to existing ENIs in the 10.0.0.0/20 CIDR range
- D. Modify all EC2 instance OS configurations with a secondary IP in the 10.0.0.0/20 CIDR range
- E. Configure a site-to-site VPN from the on-premises network to each VPC and route the 10.0.0.0/20 traffic from the inventory software to the EC2 instances

Answer A

This solution resolves the CIDR conflict issue for licensing, but would involve a large amount of effort.

**Create new VPC networks using the open 10.0.0.0/20 CIDR ranges.
Manually migrate all instances to the new networks**

Answer B

Like A, this solution resolves the CIDR conflict issue for licensing. It does not involve migrating instances, and would be preferable. VPC networks support up to 5 additional CIDR ranges, so this is technically feasible. Secondary ENIs are allowed as long as the subnets are in the same AZ as the EC2 instance.

Add secondary CIDR ranges to all existing VPCs within the 10.0.0.0/20 range and create subnets to match the existing ranges. Add secondary ENIs to all EC2 instances in the new subnets

Answer C

This solution sounds preferable to both A and B in terms of effort. ENIs do not allow secondary IPs to be added which are not in the primary IPv4 subnet, so this solution will not work.

Add secondary IP addresses to existing ENIs in the 10.0.0.0/20 CIDR range

Answer D

While this might work, depending on the Operating System of the individual EC2 instances, routing the 172.16.0.0/20 network will be difficult and potentially prone to problems, causing more effort over time.

Modify all EC2 instance OS configurations with a secondary IP in the 10.0.0.0/20 CIDR range

Answer E

Regardless of the other solutions, this will be required to route the private CIDR range traffic between the on-premises network and the VPC networks.

Configure a site-to-site VPN from the on-premises network to each VPC and route the 10.0.0.0/20 traffic from the inventory software to the EC2 instances

Correct Answer

- A. Create new VPC networks using the open 10.0.0.0/20 CIDR ranges.
Manually migrate all instances to the new networks
- B. Add secondary CIDR ranges to all existing VPCs within the 10.0.0.0/20 range and create subnets to match the existing ranges. Add secondary ENIs to all EC2 instances in the new subnets
- C. Add secondary IP addresses to existing ENIs in the 10.0.0.0/20 CIDR range
- D. Modify all EC2 instance OS configurations with a secondary IP in the 10.0.0.0/20 CIDR range
- E. Configure a site-to-site VPN from the on-premises network to each VPC and route the 10.0.0.0/20 traffic from the inventory software to the EC2 instances



Domain 2: Design for New Solutions

31%

Question Domain 2 Points

2.1 Determine **security** requirements and controls when designing and implementing a solution

Question Domain 2 Points

2.2 Determine a solution design
and implementation strategy to
meet **reliability** requirements

Question Domain 2 Points

2.3 Determine a solution design
to ensure **business continuity**

Question Domain 2 Points

2.4 Determine a solution design
to meet **performance** objectives

Question Domain 2 Points

2.5 Determine a **deployment strategy** to meet business requirements when designing and implementing a solution



Security Scenario

Scenario Description

A company currently uses VPCs with private subnets for critical resources. NAT Gateways are deployed for outbound traffic. All EC2 instances are launched into these private subnets and use the NAT Gateways for outbound traffic on ports 80 and 443.

There is a new security control requiring all outbound traffic be inspected for DLP and to reject unauthorized destinations.

The control requires a resilient solution that can scale to include all ports and protocols.

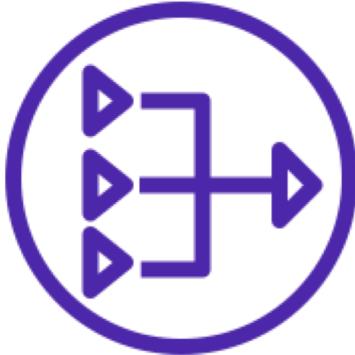
What actions can be taken to meet the new requirements?

Scenario Questions to Ask



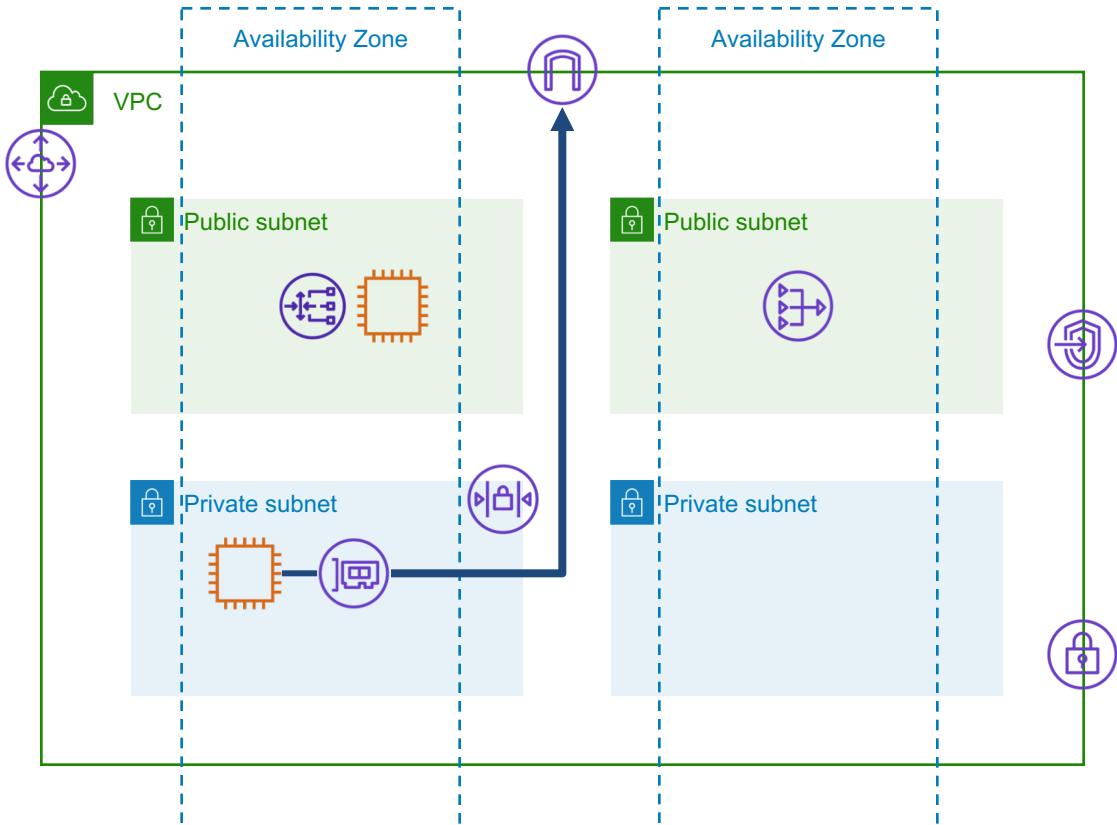
- What does NAT Gateway do?
- Can it meet requirements?
- What other managed options are available?
- Does this require a custom solution?

NAT Gateway Basics



- AZ scope
- Highly available
- Scalable to 45Gbps
- No Security Group
- Passive
- Layer 4 - Not stateful
- TCP, UDP, ICMP

Options for Outbound Traffic

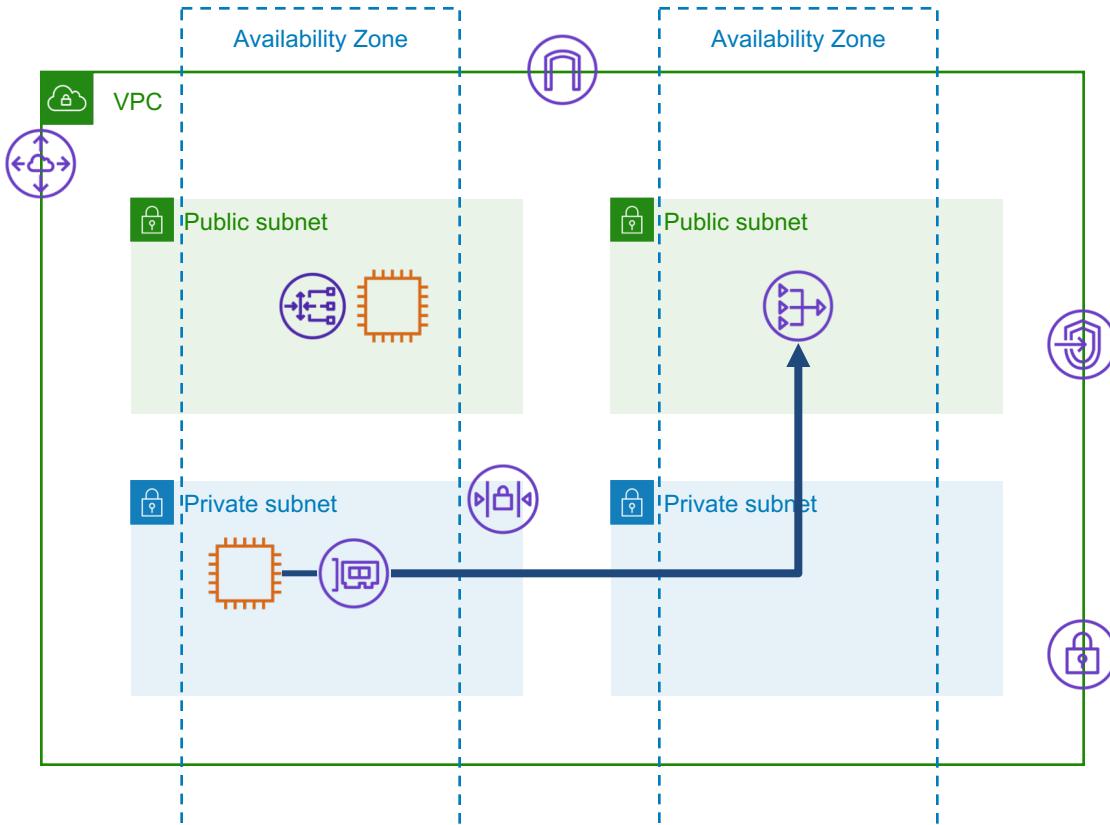


Use local OS-based software to perform inspection and DLP

Use Network ACLs to deny unauthorized destination IP addresses

Is this a viable solution?

Options for Outbound Traffic

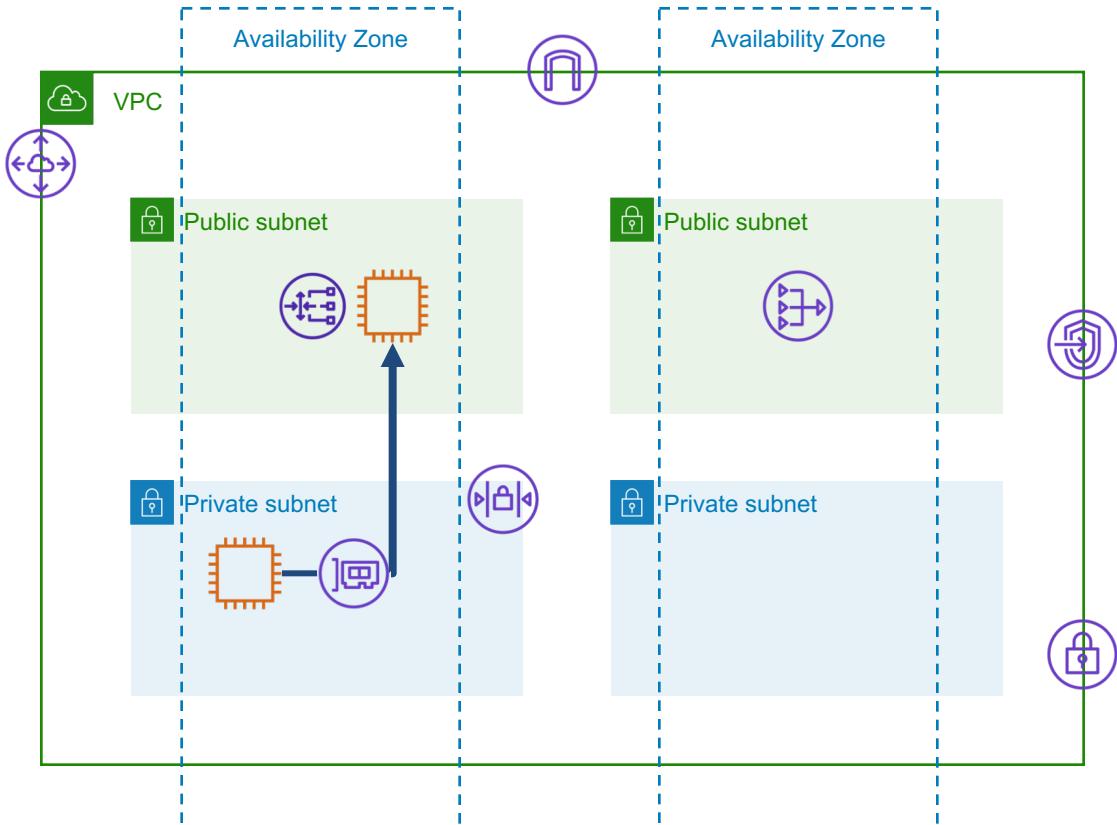


Keep the existing NAT Gateway solution

Use Network ACLs to deny unauthorized destination IP addresses

Is this a viable solution?

Options for Outbound Traffic

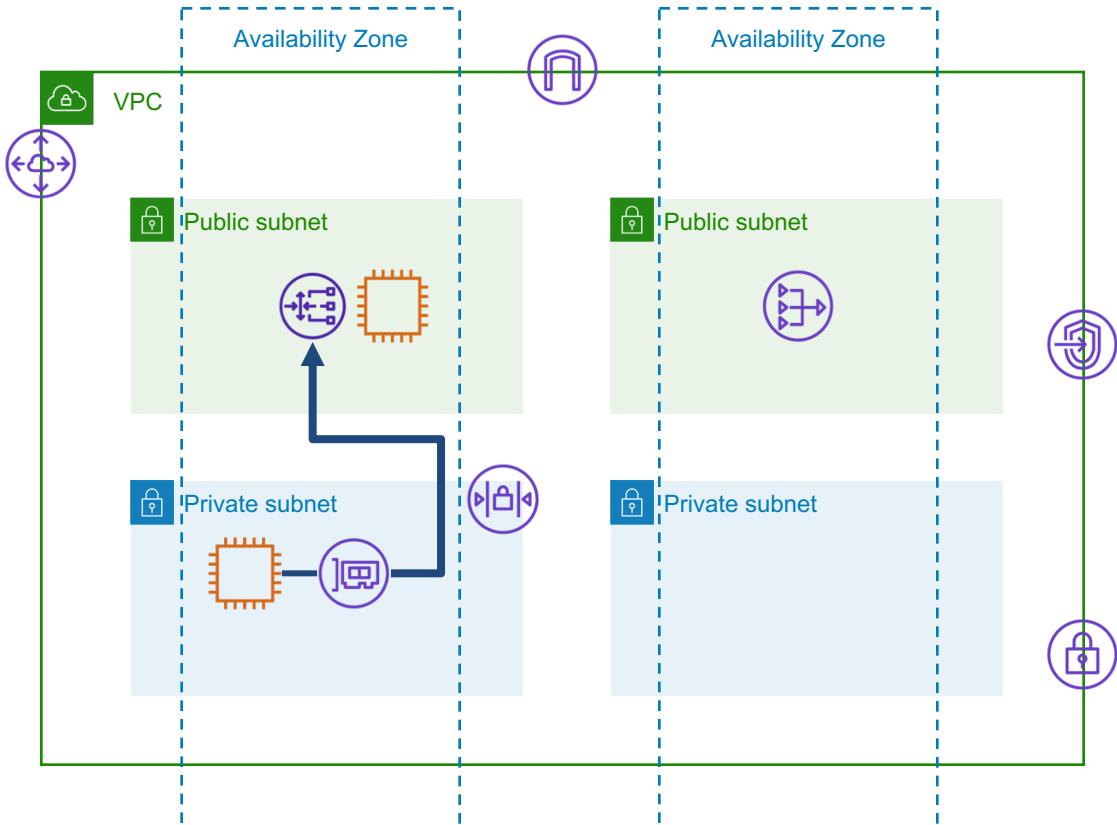


Deploy an EC2-based appliance to perform DLP

Use the EC2 appliance to deny unauthorized destinations

Is this a viable solution?

Options for Outbound Traffic

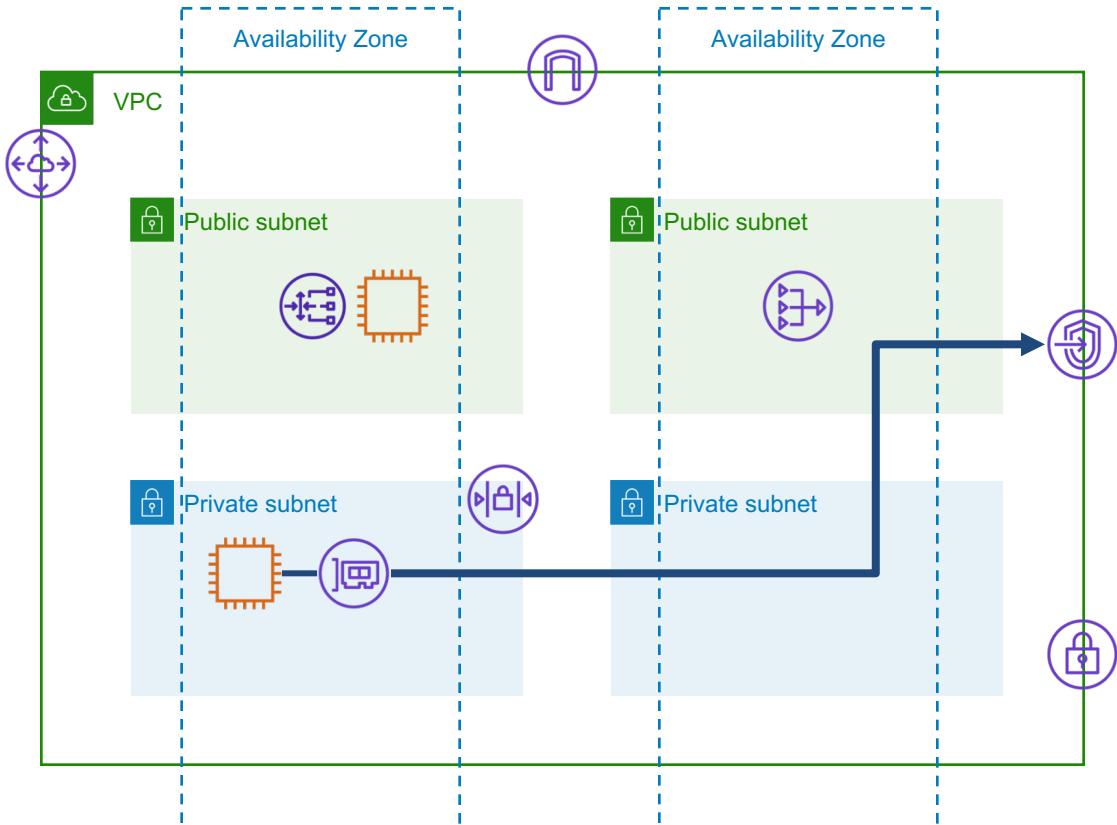


Deploy a GateWay LB to perform DLP

Use the GWLB to deny unauthorized destinations

Is this a viable
solution?

Options for Outbound Traffic

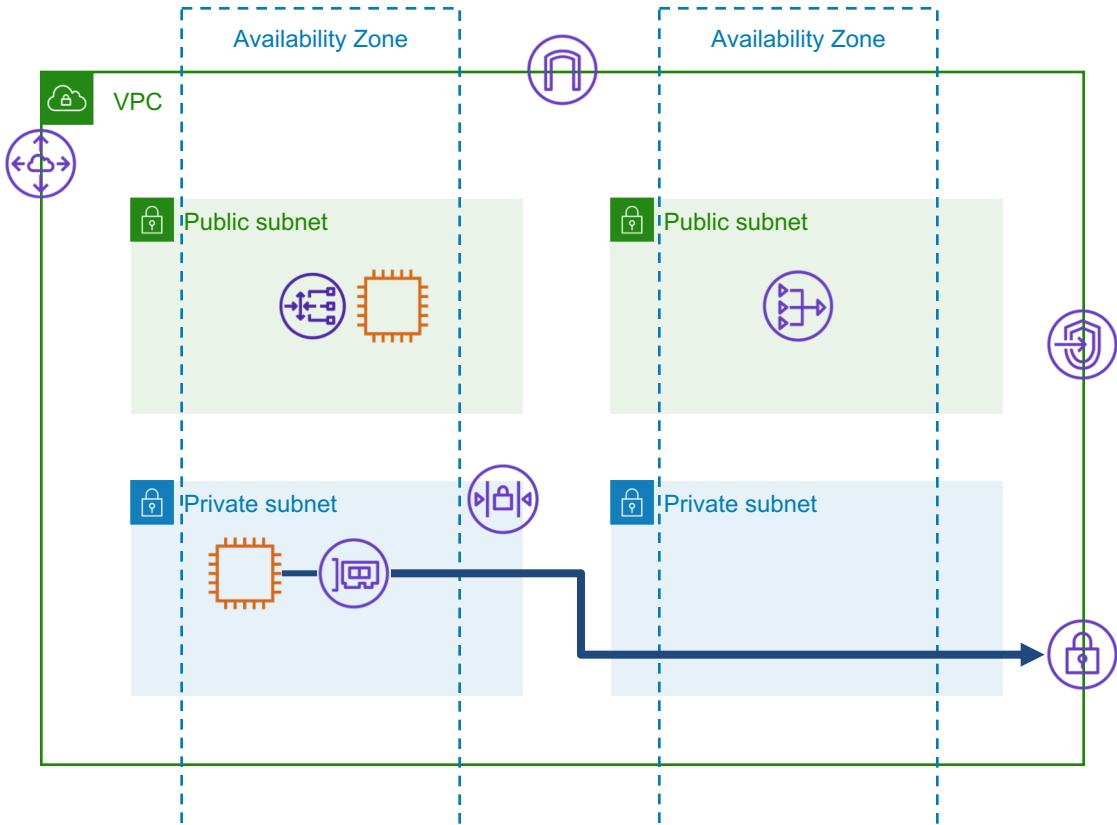


Deploy a GateWay LB endpoint to perform DLP

Use the GWLB in the remote VPC to deny unauthorized destinations

Is this a viable solution?

Options for Outbound Traffic

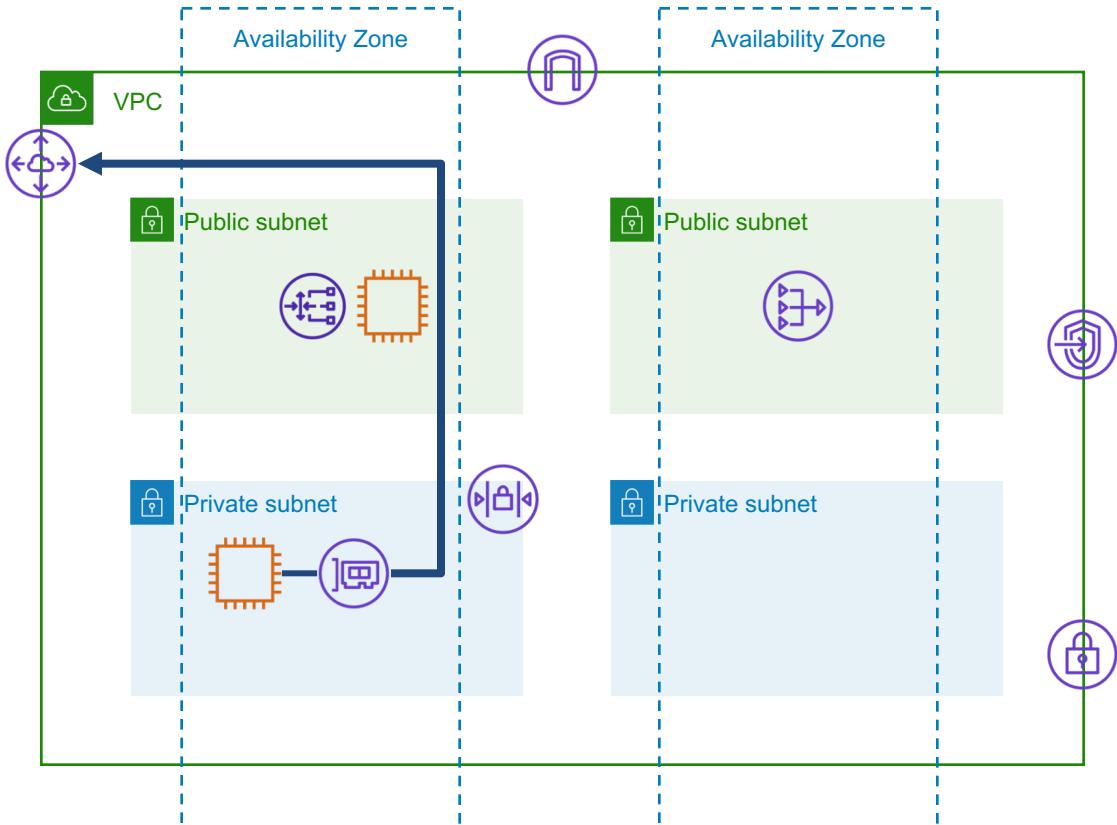


Deploy a VPG and perform DLP in the on-premises network

Use the on-premises network to deny unauthorized destinations

Is this a viable solution?

Options for Outbound Traffic



Deploy a DLP solution in a remote VPC and reach via VPC Peering

Use the remote VPC solution to deny unauthorized IP addresses

Is this a viable solution?

Option Summary

OS/NACL

Feasible

Resilient

Layer 3

More info
needed



Almost!

Option Summary



Option Summary



Option Summary

	Feasible	Resilient	Layer 3	More info needed
OS/NACL				
NAT GW		✓		
EC2 Appliance	✓	✓		
GWLB	✓	✓	✓	

Option Summary

	Feasible	Resilient	Layer 3	More info needed
OS/NACL				
NAT GW		✓		
EC2 Appliance	✓			
GWLB	✓	✓		
GWLBI	✓	✓		

Option Summary

	Feasible	Resilient	Layer 3	More info needed
OS/NACL		✓		Almost!
NAT GW		✓		
EC2 Appliance	✓			
GWLB	✓	✓		
GWLBI	✓	✓	✓	
VPG	✓	?	?	✓

Option Summary

	Feasible	Resilient	Layer 3	More info needed
OS/NACL		✓		Almost!
NAT GW		✓		
EC2 Appliance	✓			
GWLB	✓	✓		
GWLBI	✓	✓		
VPG	✓	?	?	
VPC Peering	✓	?	?	✓

Question Breakdown

Question Scenario

A storage team is responsible for all data storage in AWS, including block storage for EC2 instances.

The storage team has been given a mandate to ensure all EBS data volumes are encrypted at-rest.

There is a requirement to implement as quickly as possible and monitor compliance afterward.

Which of the following steps can meet the mandate?
(pick FIVE)

Answer Choices

- A. Create an EBS snapshot of each data volume, then perform a same-region copy, enabling encryption.
- B. Using the AWS Console or CLI, convert all EBS volumes to encrypted volumes, then reboot each instance to enable encryption
- C. Restore an unencrypted EBS snapshot of each volume as a new volume, enable encryption and attach to the instance
- D. Detach and re-attach each EBS data volume to enable encryption
- E. Create a new volume from the encrypted snapshot and attach to the instance
- F. Replace the old volume with the new encrypted volume within the instance OS
- G. Create a new encrypted volume, attach to the instance and copy all data from the old volume to the new volume

Answer A

This is a feasible task, and makes it possible to create an encrypted snapshot from an unencrypted snapshot.

Create an EBS snapshot of each data volume, then perform a same-region copy, enabling encryption.

Answer B

This sounds feasible, but it is not possible to perform a single-step conversion of an existing volume from unencrypted to encrypted.

Using the AWS Console or CLI, convert all EBS volumes to encrypted volumes, then reboot each instance to enable encryption

Answer C

This is also feasible, and another way to convert an unencrypted volume to an encrypted volume.

Restore an unencrypted EBS snapshot of each volume as a new volume, enable encryption and attach to the instance

Answer D

This is not a possible method for encrypting an unencrypted volume.

Detach and re-attach each EBS data volume to enable encryption

Answer E

Once an encrypted snapshot exists, it must be restored to a new volume before becoming usable.

Create a new volume from the encrypted snapshot and attach to the instance

Answer F

For any solution that involves two volumes attached to the instance, the old volume will have to be replaced by the new volume.

Replace the old volume with the new encrypted volume within the instance OS

Answer G

This is an interesting solution that does not involve any EBS snapshots.

Create a new encrypted volume, attach to the instance and copy all data from the old volume to the new volume

Correct Answer

- A. Create an EBS snapshot of each data volume, then perform a same-region copy, enabling encryption.
- B. Using the AWS Console or CLI, convert all EBS volumes to encrypted volumes, then reboot each instance to enable encryption
- C. Restore an unencrypted EBS snapshot of each volume as a new volume, enable encryption and attach to the instance
- D. Detach and re-attach each EBS data volume to enable encryption
- E. Create a new volume from the encrypted snapshot and attach to the instance
- F. Replace the old volume with the new encrypted volume within the instance OS
- G. Create a new encrypted volume, attach to the instance and copy all data from the old volume to the new volume





Reliability Scenario

Scenario Description

A new application will be deployed as a mobile back end for a customer support site. This application allows users to upload screenshots attached to support requests.

The application requires a repository for image storage, and a searchable persistence tier for ticket data.

The solution must emphasize reliability and data redundancy as a top priority.

What solution should be recommended for the application?

Scenario Questions to Ask



- What services would be appropriate for image storage?
- What services would be appropriate for ticket data?
- Which solution(s) provide the most redundancy and resilience?

Image Storage Options



EBS



EFS

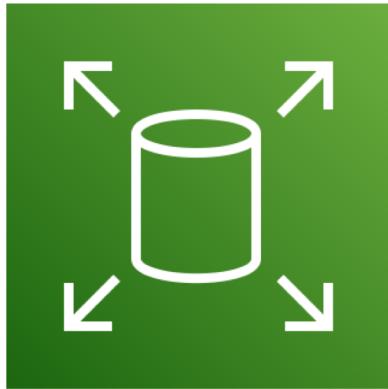


FSx



S3

- What is the resource scope?
- What is the uptime SLA?
- How is redundancy attained?
- How are uploads achieved?



- AZ scope
- 5 9s SLA
- Synchronous writes
- Requires EC2 (SPoF)

Reliability issue

Redundancy issue

Reliability issue



- Region scope
- 4 9s SLA
- 3x data replication
- Requires EC2
(SPoF)

Reliability issue

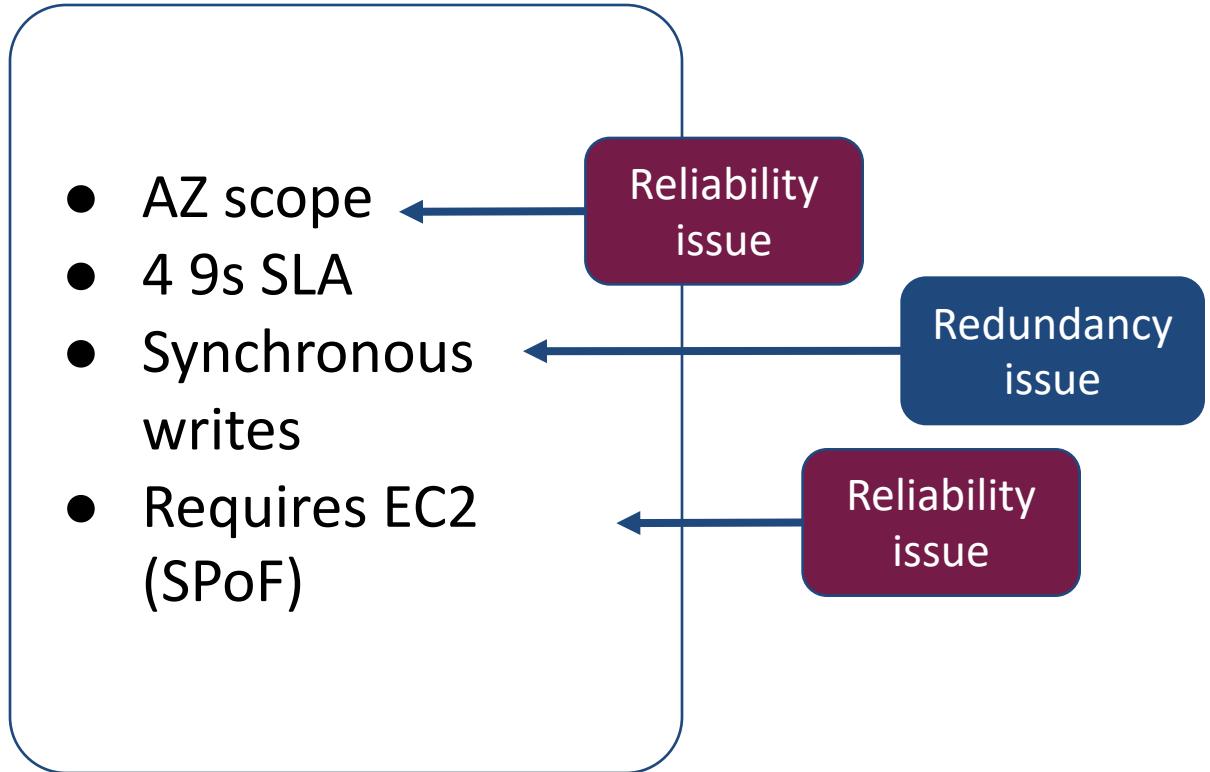


- AZ scope
- 4 9s SLA
- Synchronous writes
- Requires EC2 (SPoF)

Reliability issue

Redundancy issue

Reliability issue





- Region scope
- 4 9s SLA
- 3x data replication
- Direct access

Image Storage Summary



Ticket Data Persistence Options



RDS



Elasticache
/Redis



DynamoDB



Athena/S3



Redshift

- What is the resource scope?
- What is the uptime SLA?
- How is redundancy attained?
- Where can queries originate from?



Pearson

RDS



- AZ scope
- 3.5 9s SLA
- Multi-AZ
- Any client with network access

Reliability issue

Redundancy issue

Elasticache/Redis



- AZ scope
- 3 9s SLA
- Async replication
- Any client with network access

Reliability issue

DynamoDB



- Region scope
- 4 9s SLA
- 3x replication
- Any client with service api access

Athena/S3



- Region scope
- 4 9s SLA
- 3x replication
- Any client with service api access

Redshift



- AZ scope
- 3 9s multi-node
- 3x replication (S3)
- Any client with network access

Reliability issue

Ticket Data Persistence Summary



DynamoDB



Athena/S3



Maybe. We
will revisit
this

Solution Options



S3



DynamoDB

- S3 event notifications can trigger lambda functions
- Lambda can associate the object with a DDb item

Solution Options



S3



Athena/S3

This is extremely efficient, using the same service to store images and the tickets

Solution Options



S3



Redshift

- What if we use Redshift Spectrum to address all of the data in S3?
- This is similar to, but likely faster than the Athena solution

Question Breakdown

Question Scenario

A company's web application is deployed in AWS. The application uses CloudFront, an Application Load Balancer, and an Auto-scaling group of EC2 instances to service the application requests.

There is a new requirement to analyze page clicks on the website.

The page clicks must be processed in near real-time and in correct order, ensuring resilience of the click data.

Which of the following solutions will meet the requirements?

Answer Choices

- A. Enable access logs on the CloudFront distribution. Create an EMR job to analyze the logs hourly, ingesting front and delivering results to S3
- B. Enable access logs on the Application Load Balancer. Create an EMR job to analyze the logs hourly, ingesting from and delivering results to S3
- C. Modify the client application pages to deliver click information to a Kinesis data stream. Launch an Auto Scaling group of EC2 instances with Kinesis clients to process the stream.
- D. Modify the client application pages to deliver click information to an SQS FIFO queue. Launch an Auto Scaling group of EC2 instances to process the message queue entries.

Answer A

This solution will meet the functional requirements of analyzing clicks in order. However, EMR is by default a batch-based service and will not be able to perform the analysis in real time.

Enable access logs on the CloudFront distribution. Create an EMR job to analyze the logs hourly, ingesting front and delivering results to S3

Answer B

This solution will also meet the functional requirements of analyzing clicks in order. However, as answer A is eliminated by using the batch-based EMR, this answer is as well.

Enable access logs on the Application Load Balancer. Create an EMR job to analyze the logs hourly, ingesting from and delivering results to S3

Answer C

This is a third functional solution. The Kinesis data stream allows the clients to process in near real-time, but the order is only guaranteed within the same shard, and not guaranteed overall.

Modify the client application pages to deliver click information to a Kinesis data stream. Launch an Auto Scaling group of EC2 instances with Kinesis clients to process the stream.

Answer D

The FIFO queue guarantees an absolute order of the messages, regardless of the session involved. SQS can be used as a near real-time service, and the analysis can meet all of the requirements.

Modify the client application pages to deliver click information to an SQS FIFO queue. Launch an Auto Scaling group of EC2 instances to process the message queue entries.

Correct Answer

- A. Enable access logs on the CloudFront distribution. Create an EMR job to analyze the logs hourly, ingesting front and delivering results to S3
- B. Enable access logs on the Application Load Balancer. Create an EMR job to analyze the logs hourly, ingesting from and delivering results to S3
- C. Modify the client application pages to deliver click information to a Kinesis data stream. Launch an Auto Scaling group of EC2 instances with Kinesis clients to process the stream.
- D. Modify the client application pages to deliver click information to an SQS FIFO queue. Launch an Auto Scaling group of EC2 instances to process the message queue entries.



Business Continuity Scenario

Scenario Description

A company is currently serving a Java application from a single EC2 instance with Apache, MySQL and hard-coded plaintext database credentials, along with other plaintext passwords and API keys on the local filesystem.

The company is requiring new business continuity architecture to ensure failover to a different region with an RTO of 30 minutes and RPO of 5 minutes.

The proposal must meet the RTO and RPO.

What new infrastructure should be recommended for the application?

Scenario Questions to Ask



- What services are appropriate for separating the application tiers?
- What can be done to centralize management of the keys and credentials?
- How can replication/failover be achieved within the RTO/RPO?

Reverse Proxy Options



ELB



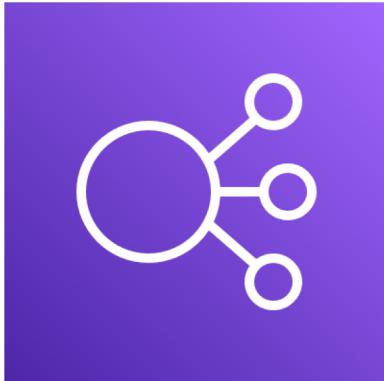
API GW



CloudFront

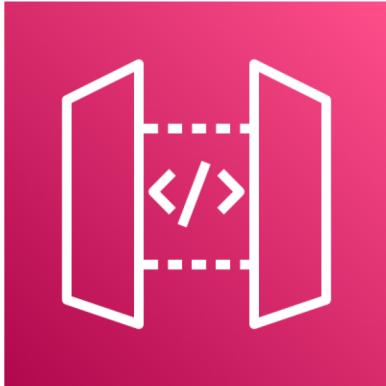
- What is the resource scope?
- Does the solution support multiple regions?





- AZ-scoped but supports multiple AZ
- No support for multiple regions

API Gateway



- Region-scoped
- No support for multiple regions

CloudFront



- Global-scoped
- Supports multiple regions via multiple origins

Secret/Credential Options



Secrets
Manager



Parameter
Store



S3

- What is the resource scope?
- How is the data secured?
- Does the service support multiple regions?



Secrets Manager



- Region-scoped
- Everything encrypted at-rest and in-transit
- Supports multi-region secrets

Parameter Store

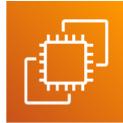


- Region-scoped
- Optional at-rest
and in-transit
encryption
- No support for
multiple regions



- Region-scoped
- Optional at-rest
and in-transit
encryption
- Supports multiple
regions via
replication

Java Runtime Options



EC2



Beanstalk



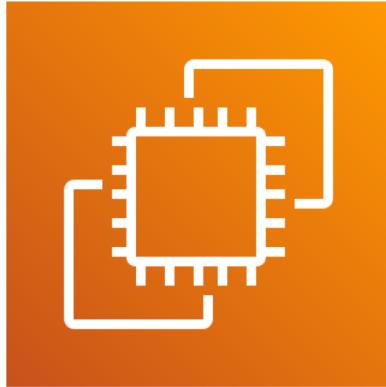
Lambda



ECS

- What is the resource scope?
- Can code be replicated across regions?

EC2



- AZ-scoped
- Flexible code locations

Beanstalk



- AZ-scoped but supports Auto Scaling in multiple AZ
- Code artifacts must be in the same region

Lambda



- Region-scoped
- Code artifacts must be in the same region



- AZ-scoped but supports auto scaling in multiple AZ
- Container images can be in any region

MySQL Options

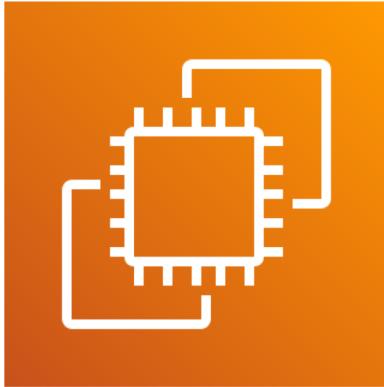


EC2



RDS

- What is the resource scope?
- How can the database be replicated to a remote region?



- AZ-scoped
- Cross-region replication requires custom implementation



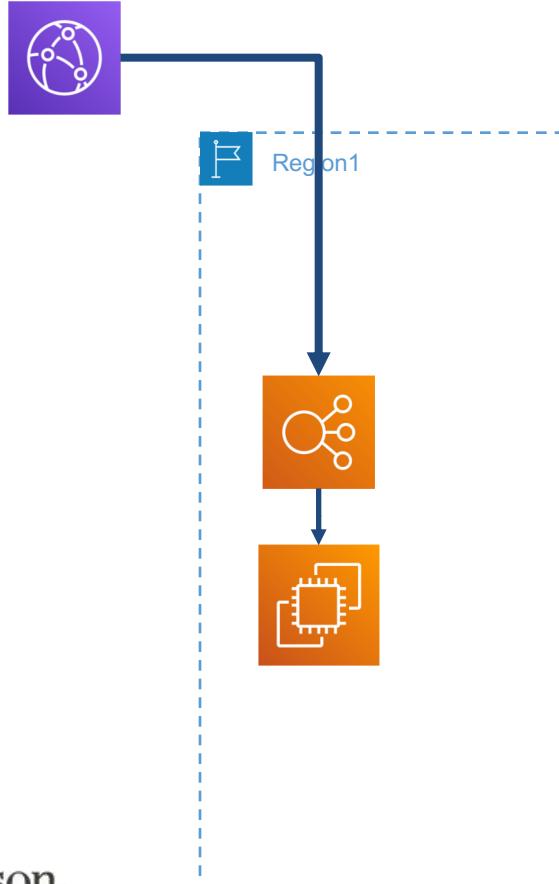
- AZ-scoped but supports multi-AZ
- Supports cross-region read replica (except for MSSQL)

Solution Option



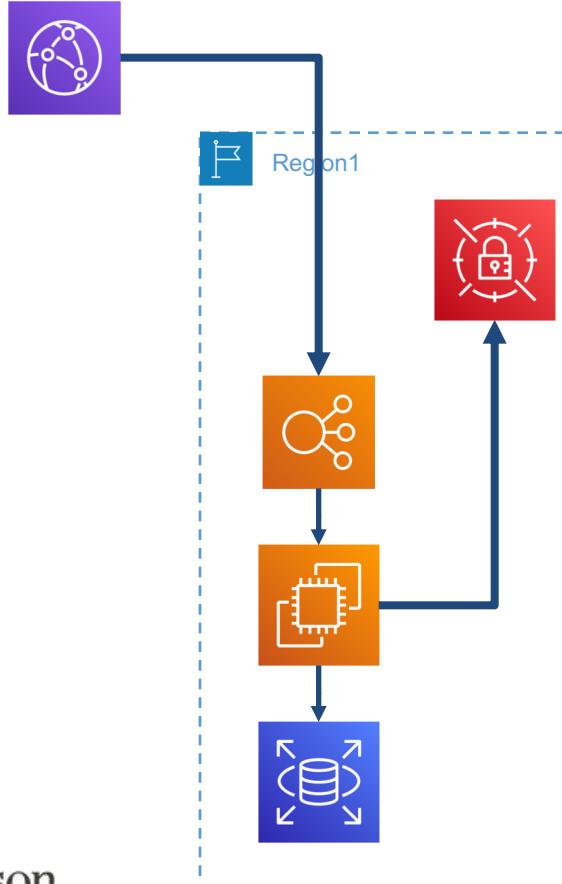
It makes sense to start with CloudFront because it supports multiple regions

Solution Option



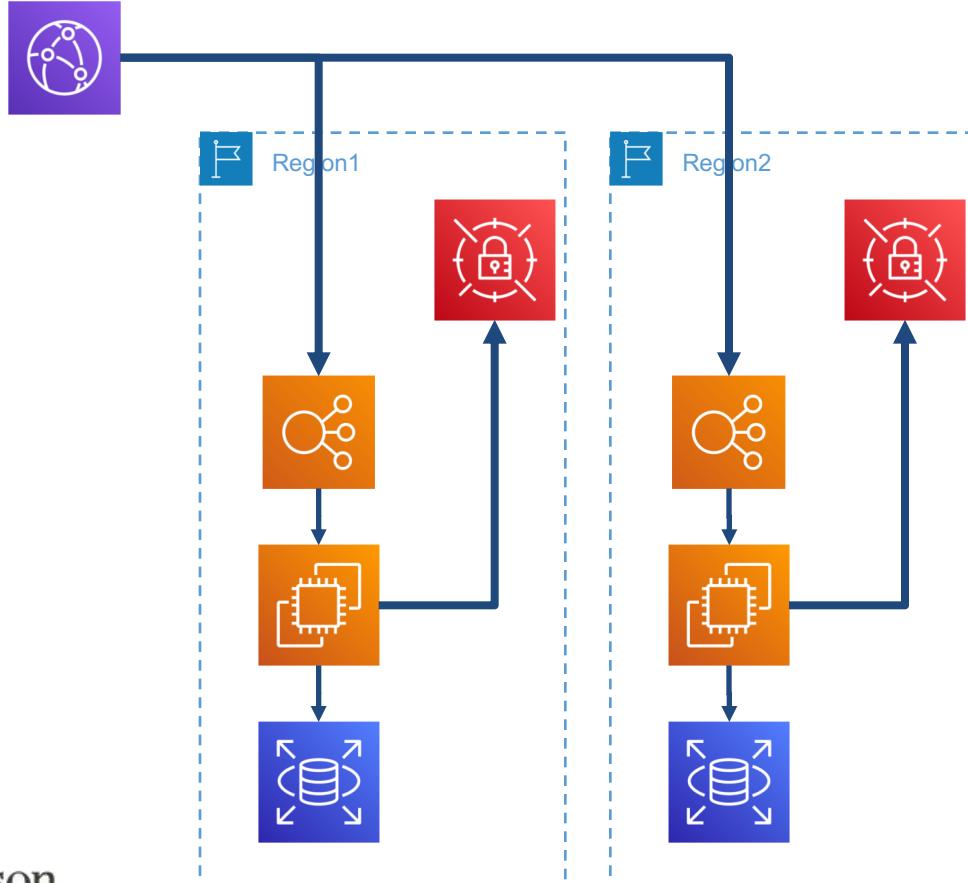
Deploy an ELB with an
Auto Scaling group of EC2
instances running the Java
code

Solution Option



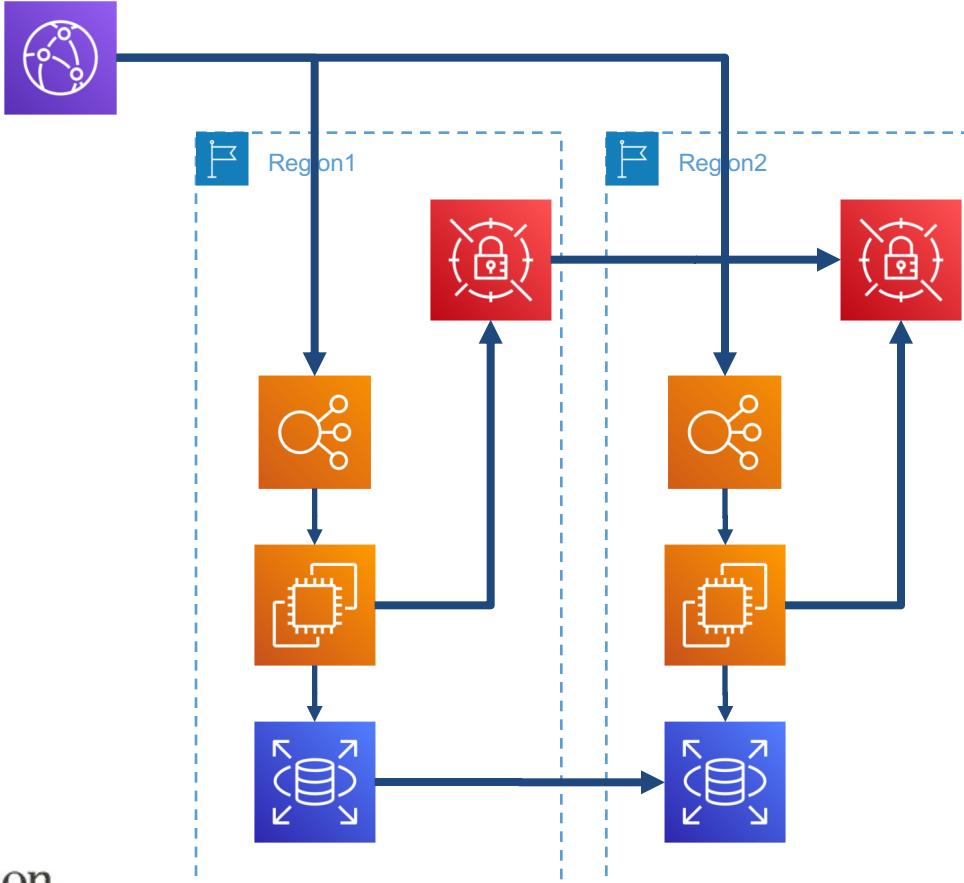
Deploy RDS for the database, and Secrets Manager for credentials and keys

Solution Option



Deploy a parallel infrastructure into a second region and use CloudFront origin failover

Solution Option



Replicate secrets and database using intrinsic cross-region features

Replicate AMIs using DLM, AWS Backup, or EventBridge + Lambda

Question Breakdown

Question Scenario

A security team is responsible for deploying new EC2 AMIs when they become available. Previously, new AMIs must be manually deployed across multiple accounts within 30 days or the company's application must be shut down due to noncompliance, impacting revenue.

The requirements have changed so that new AMIs must be deployed within 24 hours.

The security team must design a workflow for rapid AMI deployment. Which of the following will meet the business continuity objectives with the shortest deployment time?

Answer Choices

- A. When the new AMI is ready, invoke a Lambda function which shares the AMI with all accounts. Schedule a EventBridge rule to trigger a Lambda function every 2 hours in each target account, checking for new AMIs. If the new AMI exists, deploy it to all resources.
- B. Configure an EventBridge rule to capture new AMI events and forward to each account's event bus, with EventBridge rules in all accounts to trigger a Lambda function deploying the AMI to all resources.
- C. Configure an Config rule to capture new AMI events and forward to each account's event bus, with EventBridge rules in all accounts to trigger a Lambda function deploying the AMI to all resources.
- D. Configure a CloudWatch Logs Insights query to capture new CloudTrail AMI events and a CloudWatch alarm with an SNS topic notification. Subscribe a Lambda function to the SNS topic which shares the AMI with all target accounts. Configure EventBridge rules in target accounts to trigger a Lambda function which deploys the new AMI to all resources.

Answer A

This is a functional, low-maintenance solution to meet the requirements. It is also entirely automated, which is preferable.

When the new AMI is ready, invoke a Lambda function which shares the AMI with all accounts. Schedule a EventBridge rule to trigger a Lambda function every 2 hours in each target account, checking for new AMIs. If the new AMI exists, deploy it to all resources.

Answer B

Like A, this solution is functional and entirely automated. Unlike A, this solution is also entirely event-driven rather than being invoked on a schedule, it will complete in less overall time.

Configure an EventBridge rule to capture new AMI events and forward to each account's event bus, with EventBridge rules in all accounts to trigger a Lambda function deploying the AMI to all resources.

Answer C

This solution sounds identical to A, just changing EventBridge to Config. Unfortunately, Config rules cannot deliver to EventBridge in remote accounts, making this an impossible solution.

Configure an Config rule to capture new AMI events and forward to each account's event bus, with EventBridge rules in all accounts to trigger a Lambda function deploying the AMI to all resources.

Answer D

This is another functional solution, like A and B. This is also entirely event-driven, similar to B. CloudTrail logs, however, are not delivered in real-time, which will cause a delay before the Insights query catches the new AMI event.

Configure a CloudWatch Logs Insights query to capture new CloudTrail AMI events and a CloudWatch alarm with an SNS topic notification. Subscribe a Lambda function to the SNS topic which shares the AMI with all target accounts. Configure EventBridge rules in target accounts to trigger a Lambda function which deploys the new AMI to all resources.

Correct Answer

- A. When the new AMI is ready, invoke a Lambda function which shares the AMI with all accounts. Schedule a EventBridge rule to trigger a Lambda function every 2 hours in each target account, checking for new AMIs. If the new AMI exists, deploy it to all resources.
- B. Configure an EventBridge rule to capture new AMI events and forward to each account's event bus, with EventBridge rules in all accounts to trigger a Lambda function deploying the AMI to all resources.
- C. Configure an Config rule to capture new AMI events and forward to each account's event bus, with EventBridge rules in all accounts to trigger a Lambda function deploying the AMI to all resources.
- D. Configure a CloudWatch Logs Insights query to capture new CloudTrail AMI events and a CloudWatch alarm with an SNS topic notification. Subscribe a Lambda function to the SNS topic which shares the AMI with all target accounts. Configure EventBridge rules in target accounts to trigger a Lambda function which deploys the new AMI to all resources.



Performance Scenario

Scenario Description

A new E-commerce application will be deployed into AWS. The shopping cart data for each user is estimated at 20Kb. There is a predicted concurrency rate of 1 million users that could spike to 10 million during special events.

The shopping cart storage system must be able to handle the usual access concurrency and the special event traffic.

The infrastructure priority is performance, but should also be highly available.

What proposal will meet the requirements?

Scenario Questions to Ask



- What services are appropriate for shopping cart data?
- Can the solution scale to handle the traffic spikes?

Shopping Cart Storage Options



DynamoDB



RDS



S3



Elasticache
/Redis

- What is the resource scope?
- What is the SLA?
- Is the service appropriate for many concurrent reads/writes?

DynamoDB



- Region scope
- 4 9s SLA
- Designed for high throughput and HA access to partially or fully structured data

RDS



- AZ scope
- 3.5 9s SLA
- Designed for relational data and performance varies



- Region scope
- 4 9s SLA
- Designed for HA, unstructured data and durability but not high concurrency

Elasticache/Redis



- AZ scope
- 3 9s SLA
- Designed for partially or fully structured data and low latency

DynamoDB Storage Scaling



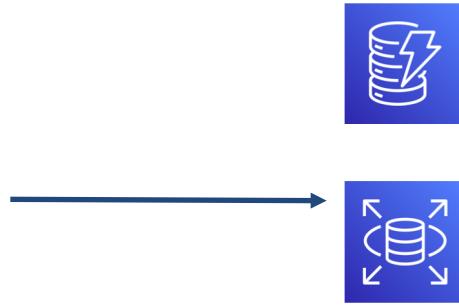
- Partition as an atomic unit of performance
- Minimum 1 read or write op per table

DynamoDB Storage Scaling



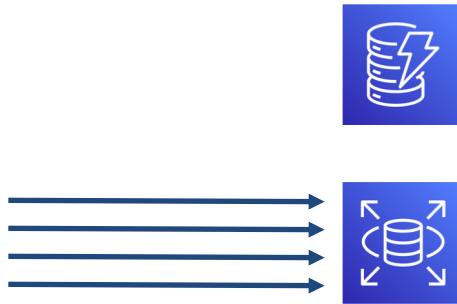
- Partition key is essential
- Instant scaling can handle the expected traffic spikes
- Implement DAX for further read scaling

RDS Storage Scaling



- Throughput is based on underlying single host and storage

RDS Storage Scaling



- Writes are dependent on the largest underlying single node performance
- Add RRs to improve read performance
- Scaling takes time

S3 Storage Scaling



- Prefix is an atomic unit of performance with 3500 writes and 5500 reads per second

S3 Storage Scaling



- Implement random hash naming convention to guarantee 1 prefix per object
- No low-latency or rapid query engine available

Elasticache/Redis Storage Scaling



- Throughput is based on underlying single host and storage

Elasticache/Redis Storage Scaling



- Single endpoint for writes
- Scale reads by adding replicas
- Scaling takes time

Question Breakdown

Question Scenario

Your marketing team has proposed a new product which requires access to very large data set (1Pb). There will be potentially thousands of EC2 instances required to concurrently access the data set for processing.

The required throughput can spike to 10 Gigabytes/second.

A successful proposal will emphasize security.

Which solution meets the requirement with minimal latency for data access?

Answer Choices

- A. Create an S3 bucket and store all files in the bucket. Access the objects using the AWS CLI and SDK.
- B. Deploy a single EFS filesystem with default security options, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.
- C. Deploy a single FSx filesystem, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.
- D. Create a shared, clustered filesystem with Provisioned IOPS EBS volumes mounted on each EC2 instance, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.

Answer A

S3 can meet the capacity and security requirements but not the throughput or latency requirements.

Create an S3 bucket and store all files in the bucket. Access the objects using the AWS CLI and SDK.

Answer B

EFS is a good solution, meeting most of the requirements EXCEPT default security options would end up with traditional NFS clients using unencrypted channels to communicate with the filesystem.

Deploy a single EFS filesystem with default security options, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.

Answer C

FSX can meet the capacity, throughput and security requirements.

Deploy a single FSx filesystem, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.

Answer D

This is an interesting solution, and could potentially meet the capacity and throughput requirements, reliability could be an issue.

Create a shared, clustered file system with Provisioned IOPS EBS volumes mounted on each EC2 instance, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.

Correct Answer

- A. Create an S3 bucket and store all files in the bucket. Access the objects using the AWS CLI and SDK.
- B. Deploy a single EFS filesystem with default security options, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.
- C. Deploy a single FSx filesystem, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.
- D. Create a shared, clustered filesystem with Provisioned IOPS EBS volumes mounted on each EC2 instance, provisioned to the appropriate size and throughput. Mount the filesystem on all EC2 clients.



Domain 3: Migration Planning

15%

Question Domain 3 Points

3.1 Select existing workloads and processes for potential migration to the cloud

Question Domain 3 Points

3.2 Select migration tools and/or services for new and migrated solutions based on detailed AWS knowledge

Question Domain 3 Points

3.3 Determine a new cloud architecture for an existing solution

Question Domain 3 Points

3.4 Determine a strategy for migrating existing on-premises workloads to the cloud



Migration Tools Scenario

Scenario Description

A company has a legacy application deployed on-premises in VMware. This app must be migrated to AWS. The application license is tied to the mac address of the instance and can be migrated once, but must remain static afterward.

The software is discontinued, and the company has no access to installation materials or support.

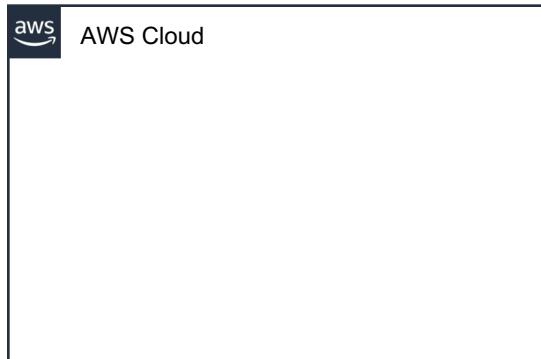
How can the customer migrate the VM while meeting the technical restrictions?

Scenario Questions to Ask

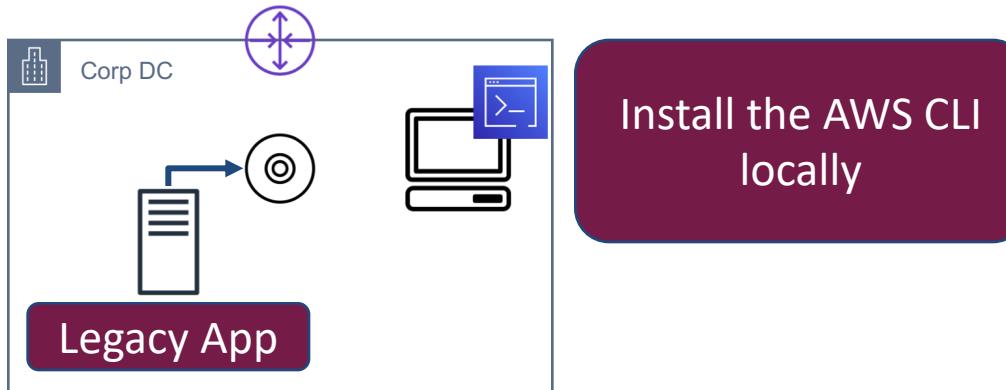
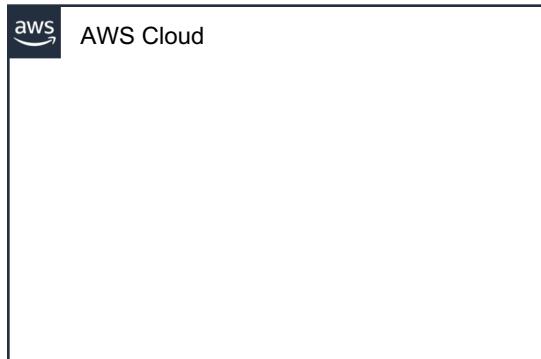


- How can an on-premises VM be deployed into AWS (EC2)?
- Are there tools to copy as-is?
- How can the MAC address remain static after migration?

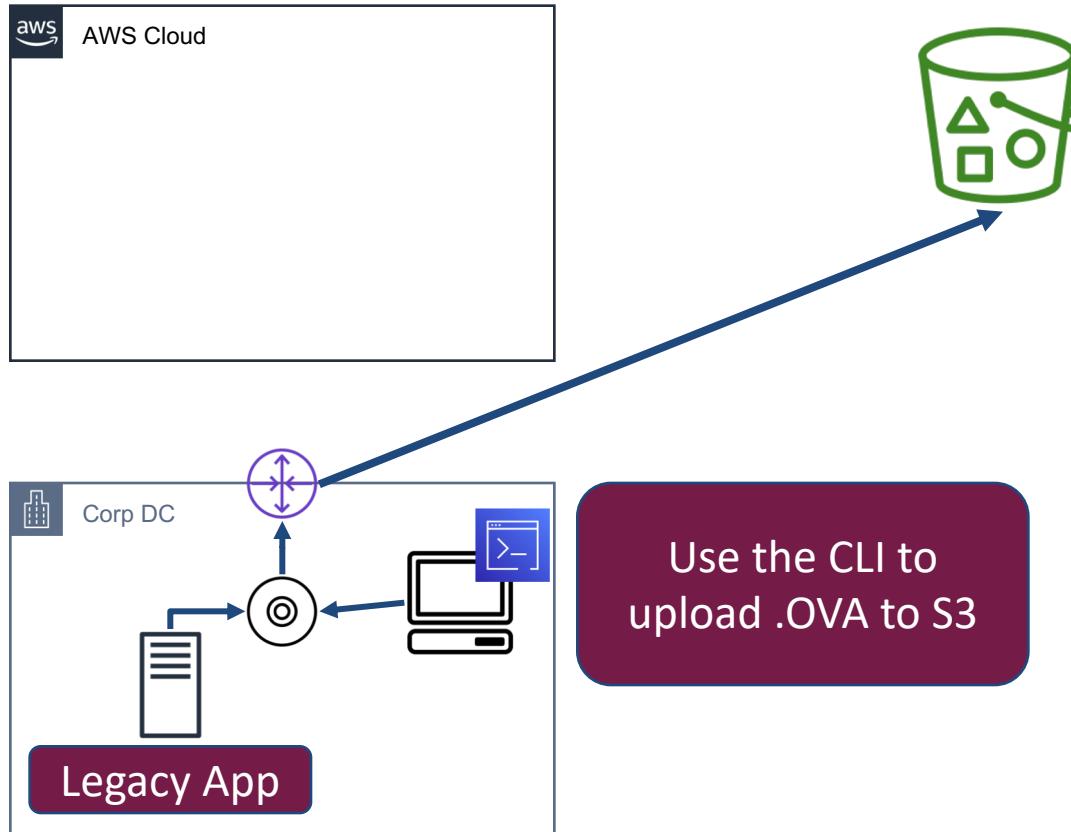
VM Import/Export Tool Option



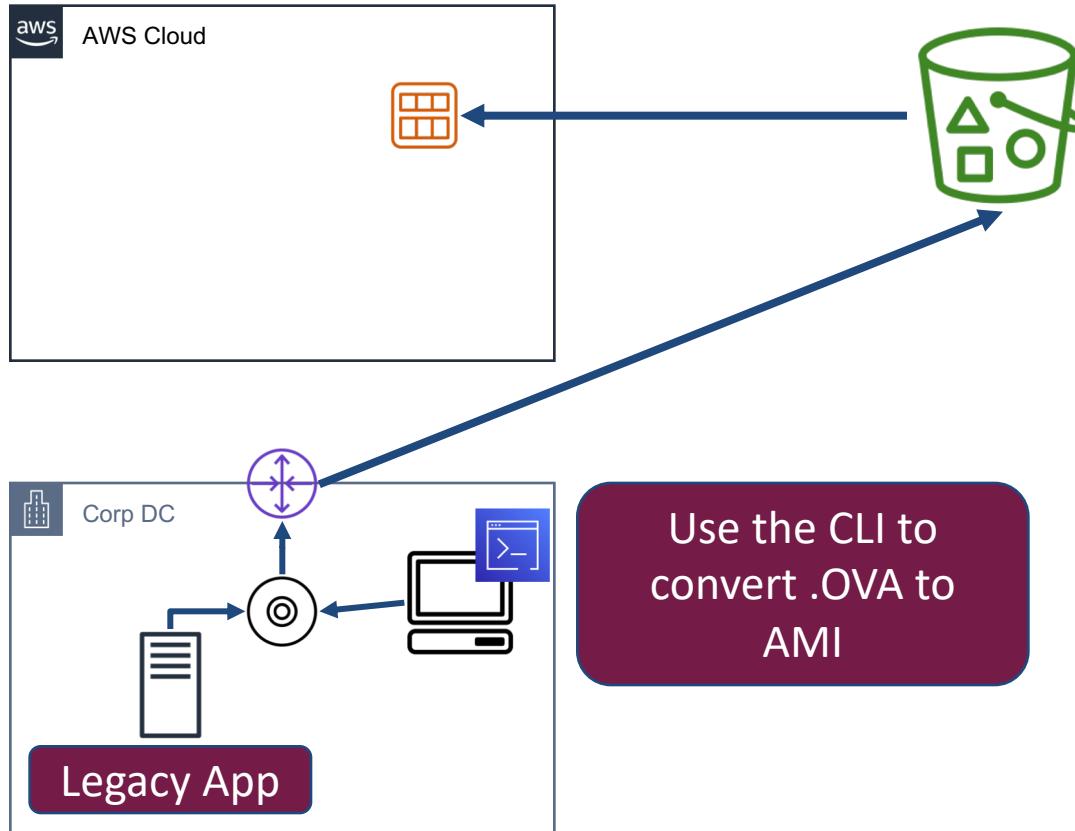
VM Import/Export Tool Option



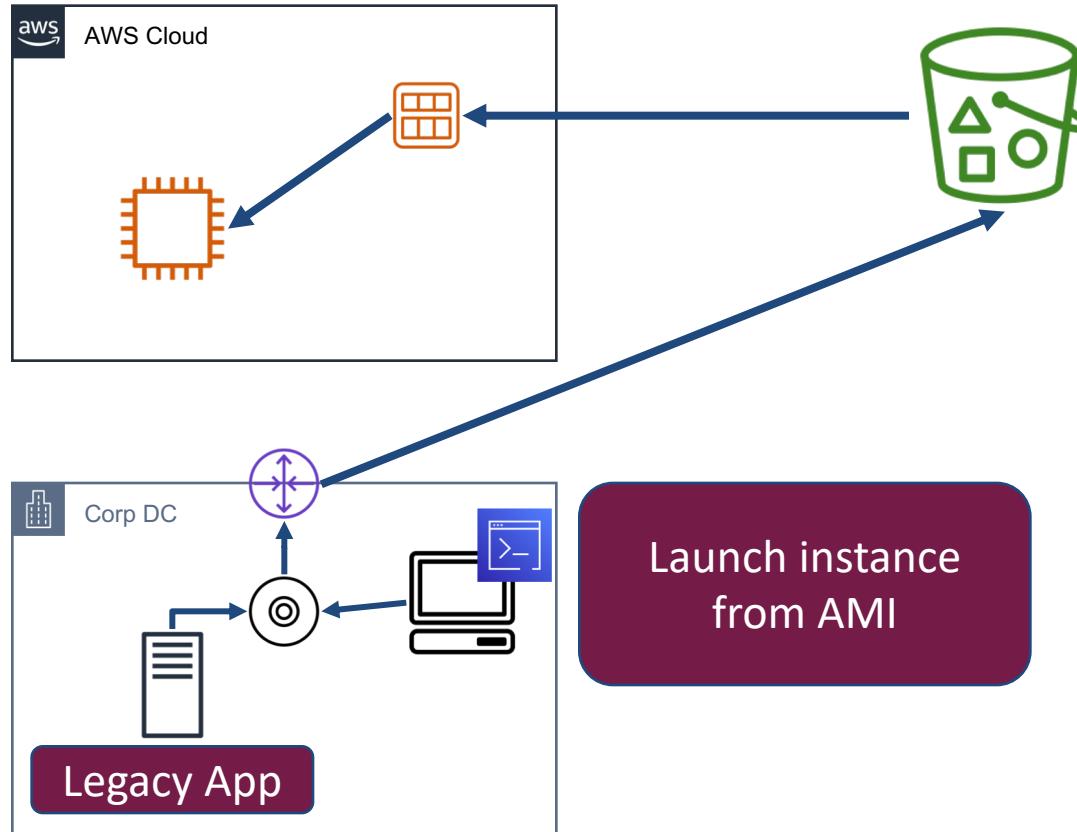
VM Import/Export Tool Option



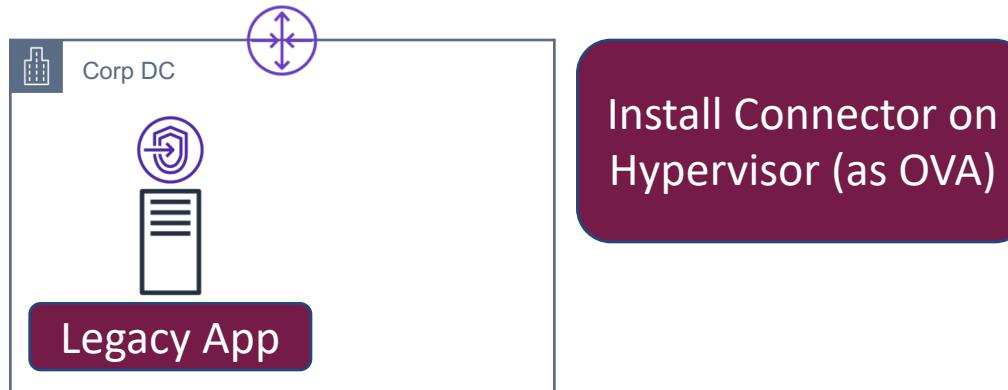
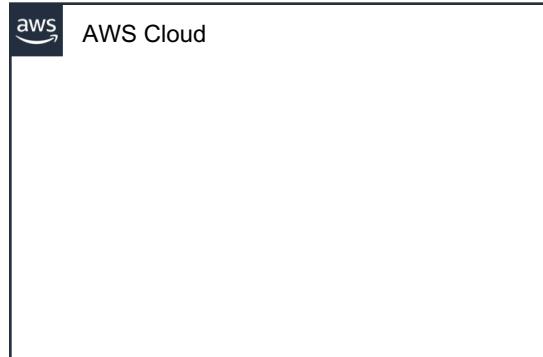
VM Import/Export Tool Option



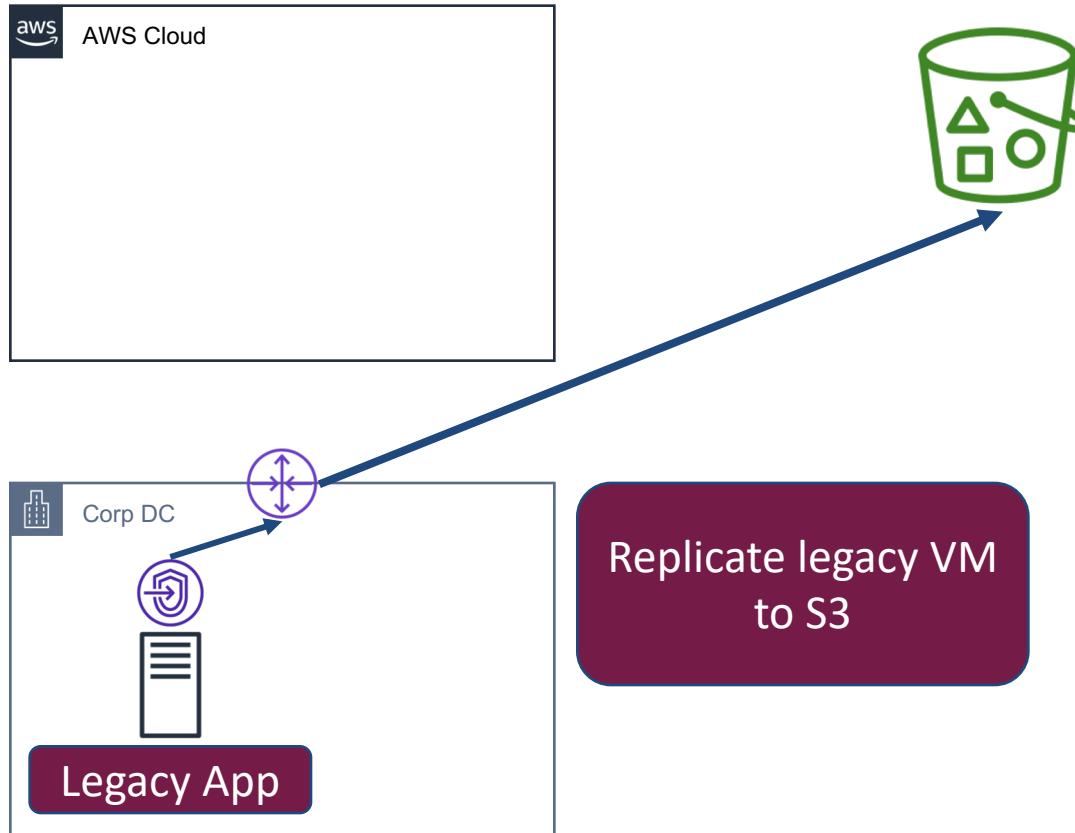
VM Import/Export Tool Option



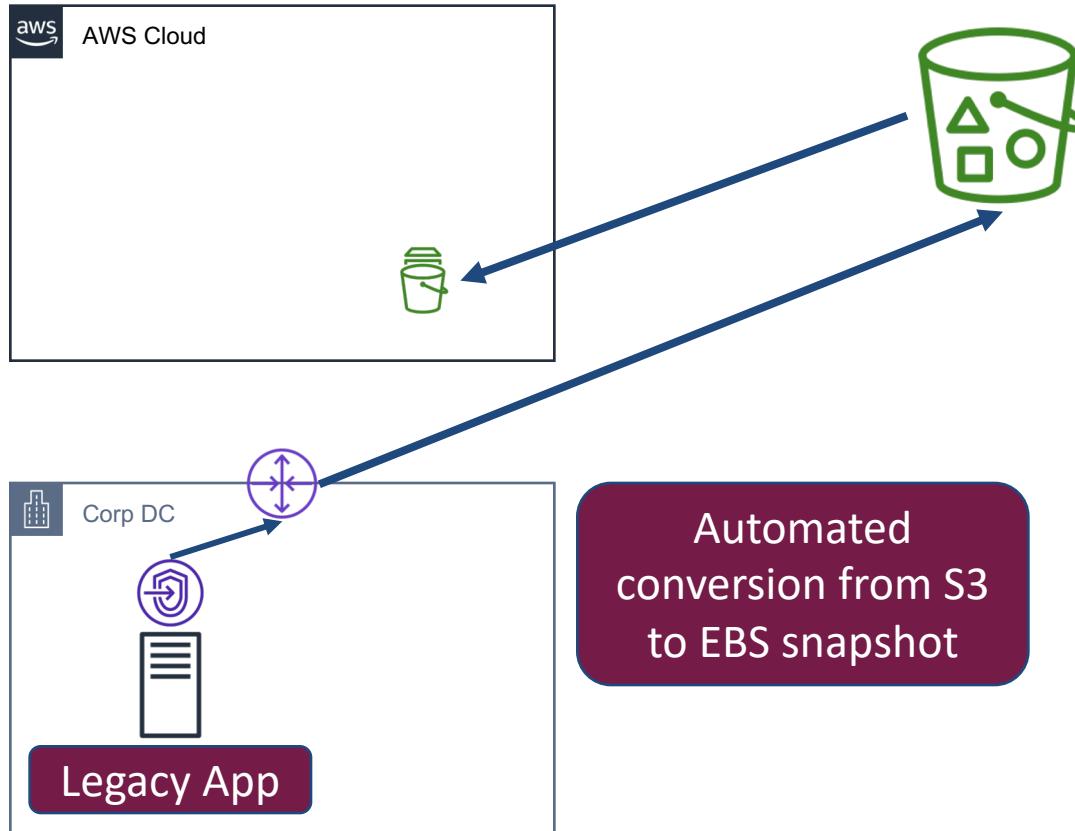
Server Migration Service Option



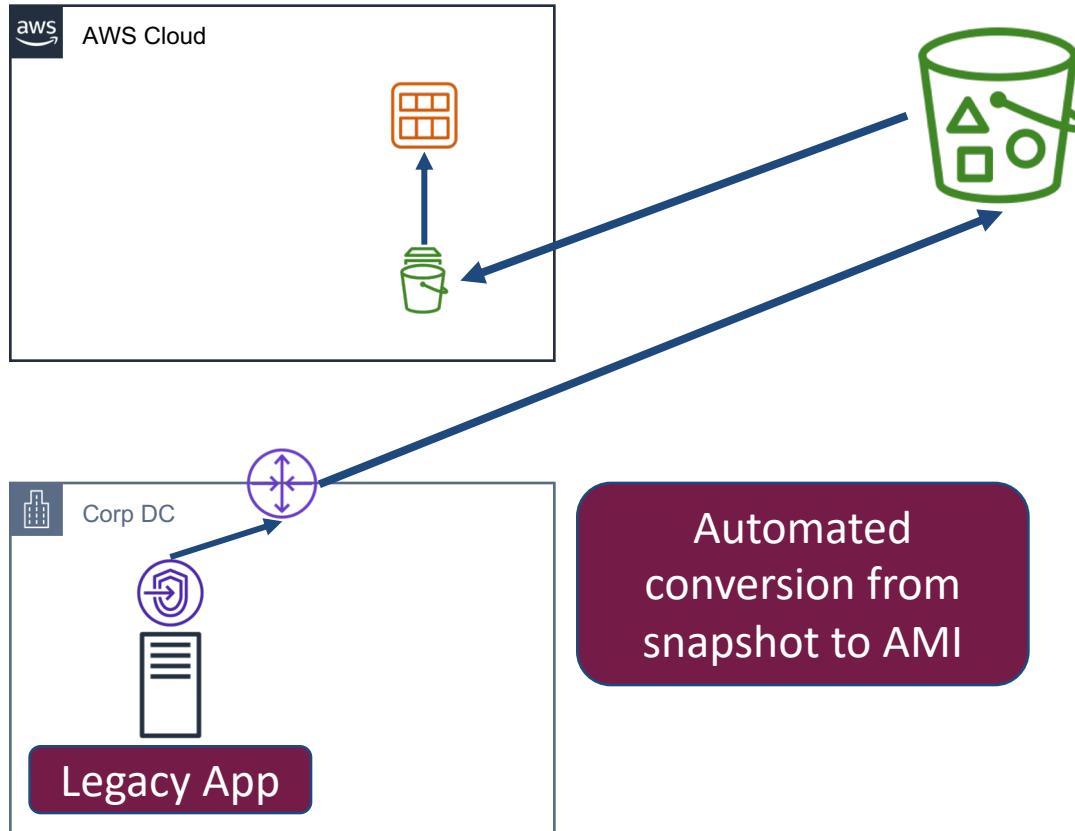
Server Migration Service Option



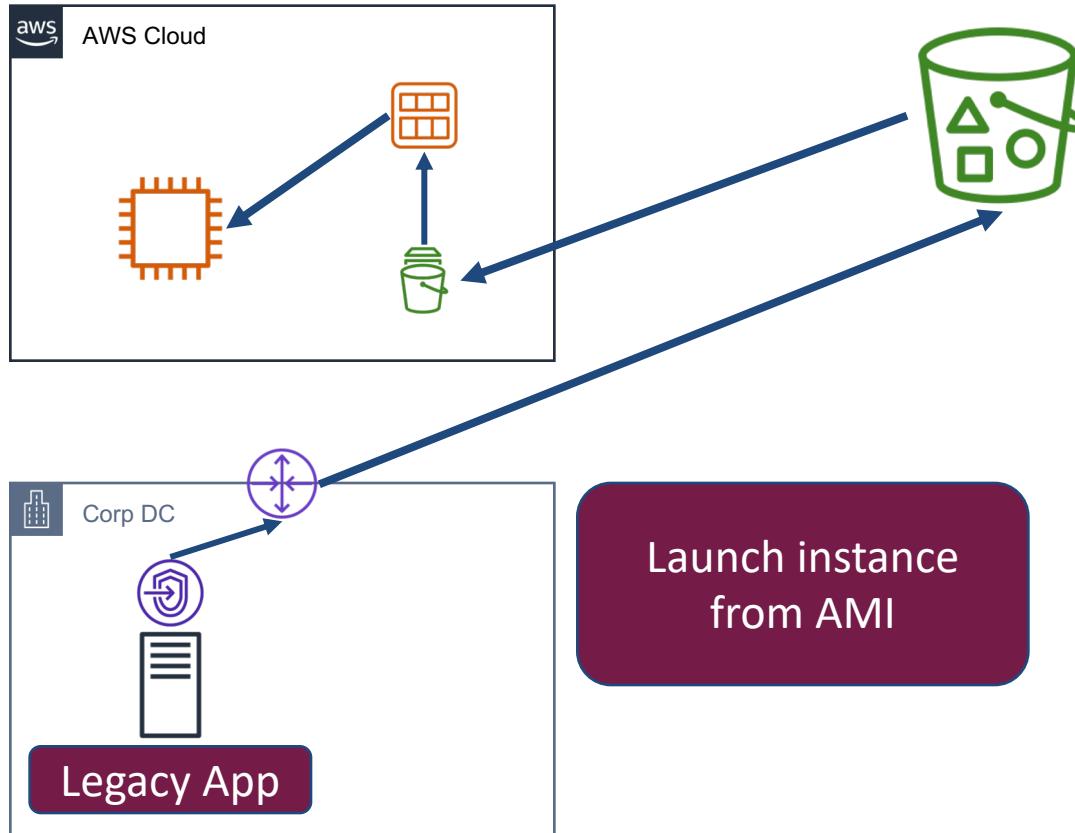
Server Migration Service Option



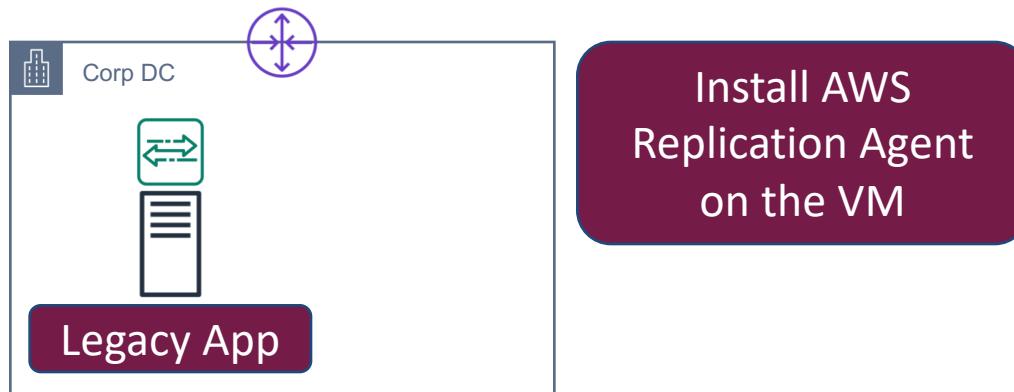
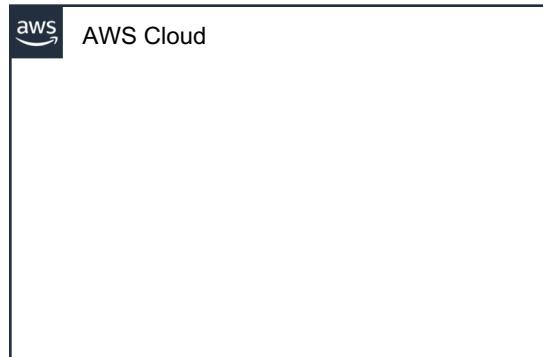
Server Migration Service Option



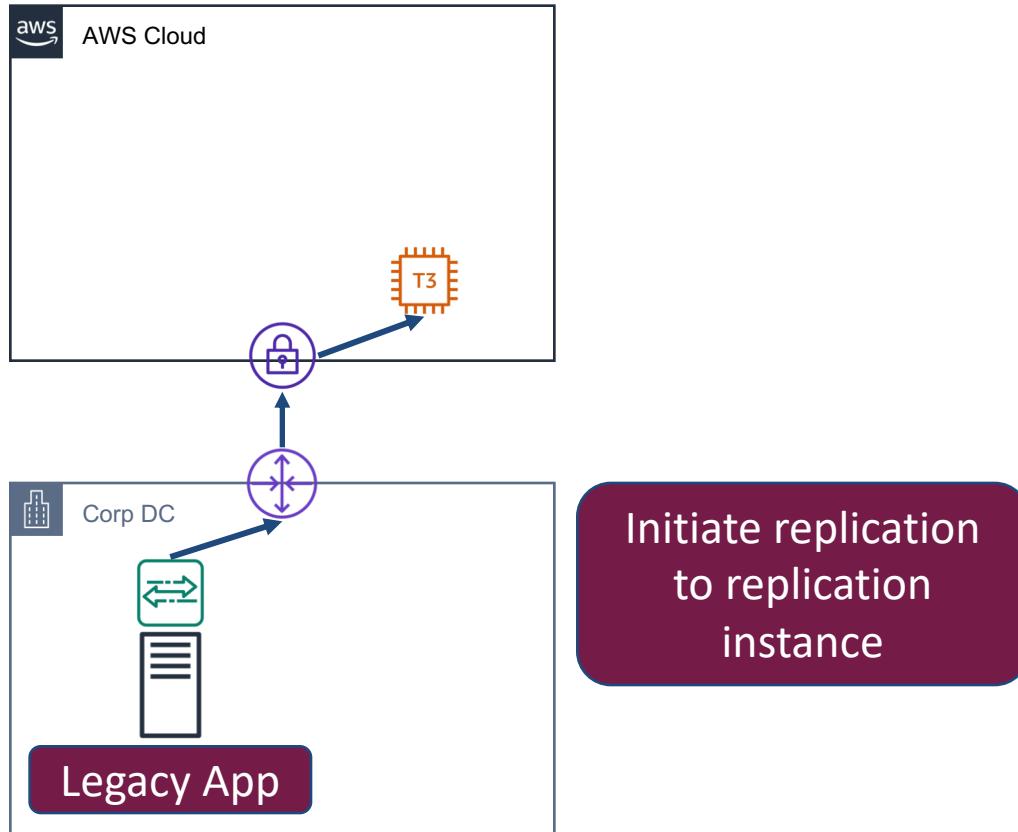
Server Migration Service Option



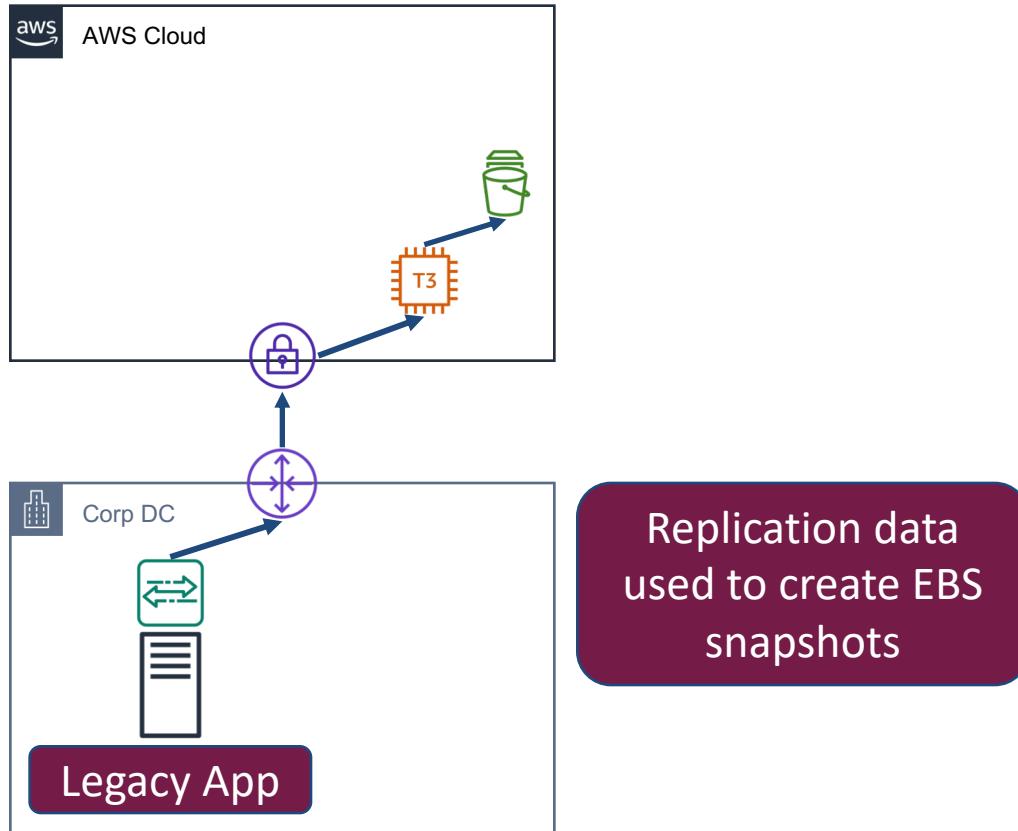
Application Migration Service Option



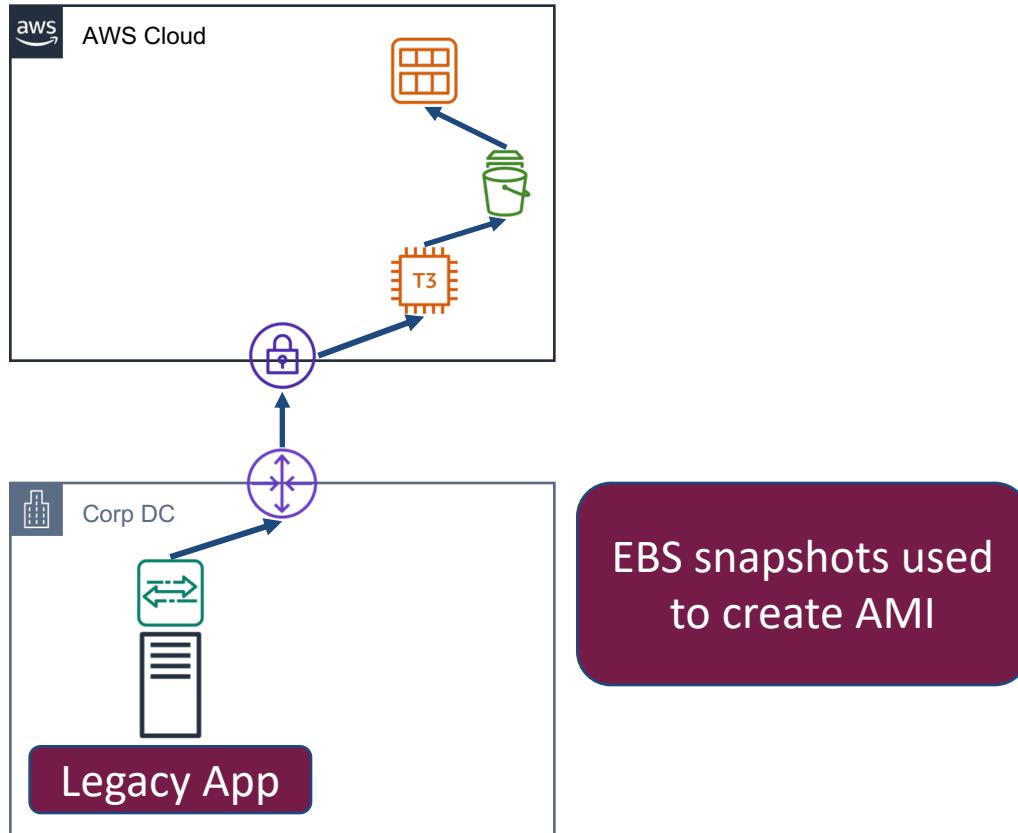
Application Migration Service Option



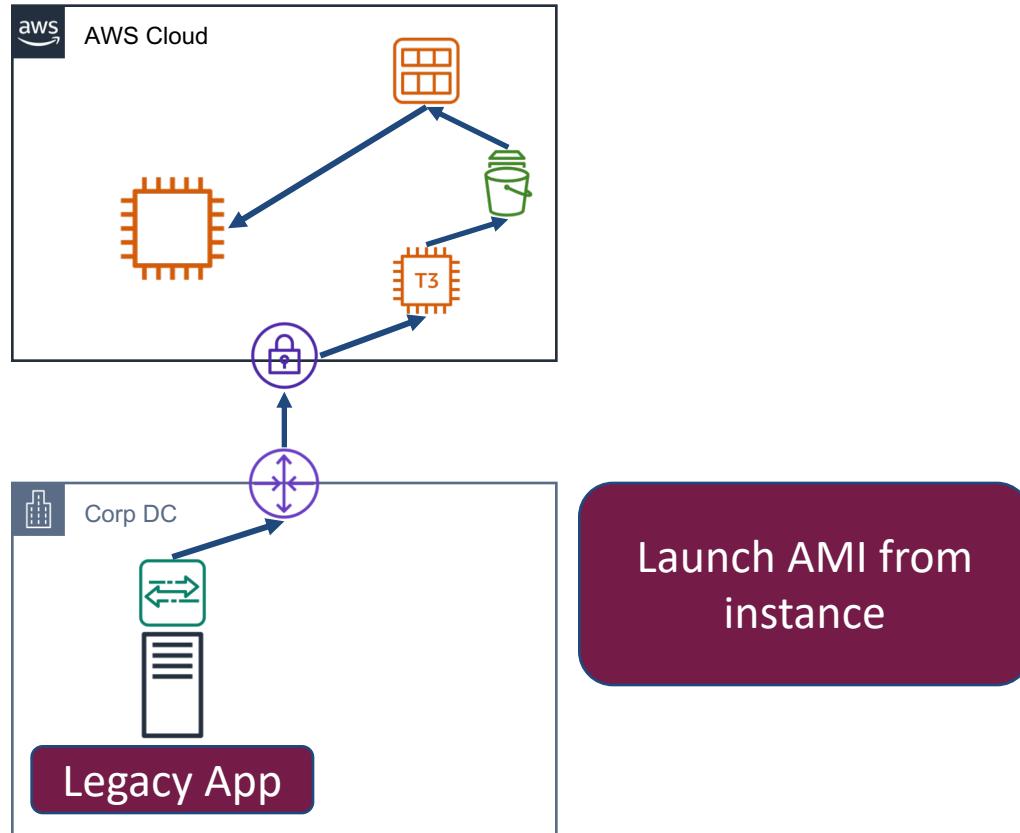
Application Migration Service Option



Application Migration Service Option



Application Migration Service Option



EC2 Primary Elastic Network Interface



- Subnet*
- Private IP*
- Private DNS*
- MAC*
- Secondary private IPs
- Public IP
- Public DNS
- Cannot detach

* = static

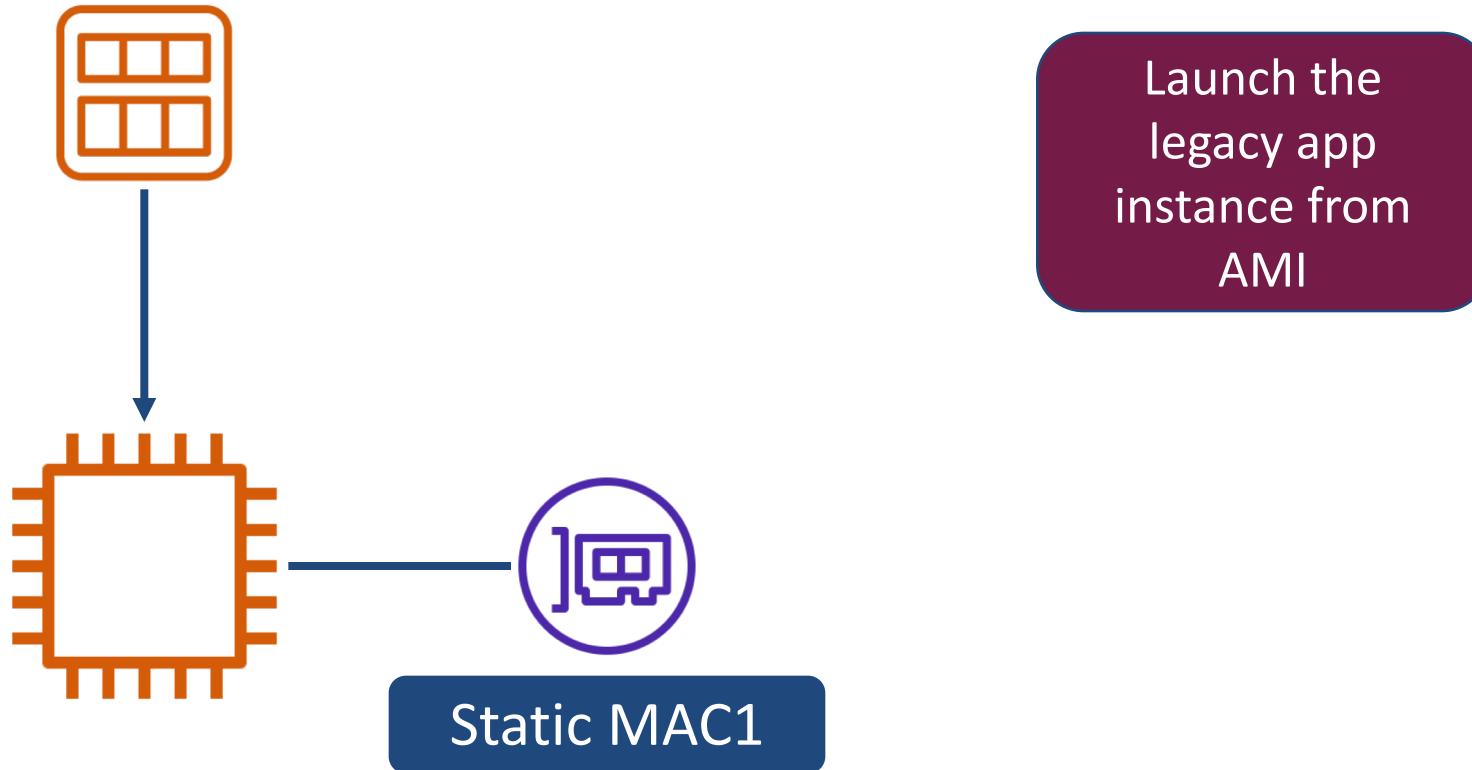
Standalone Elastic Network Interface



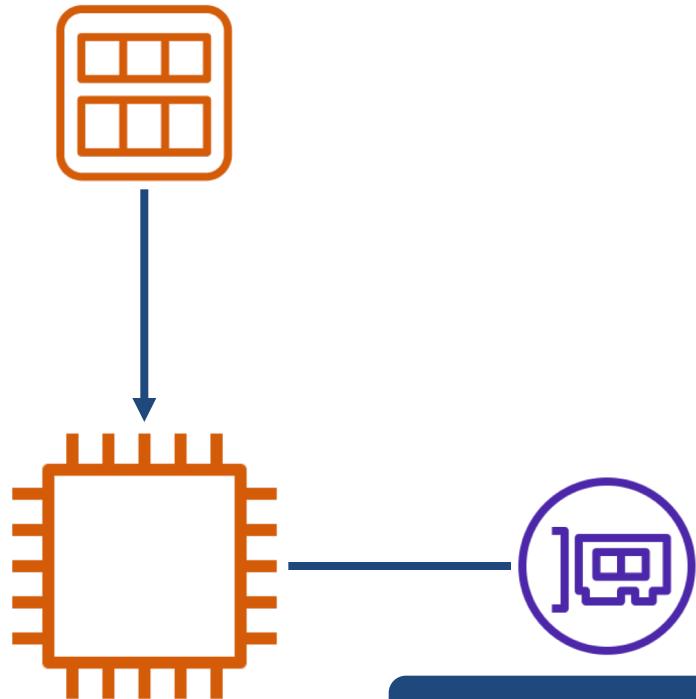
- Subnet*
- Private IP*
- Private DNS*
- MAC*
- Secondary private IPs
- Public IP
- Public DNS
- **CAN detach**

* = static

EC2 Static MAC Implementation

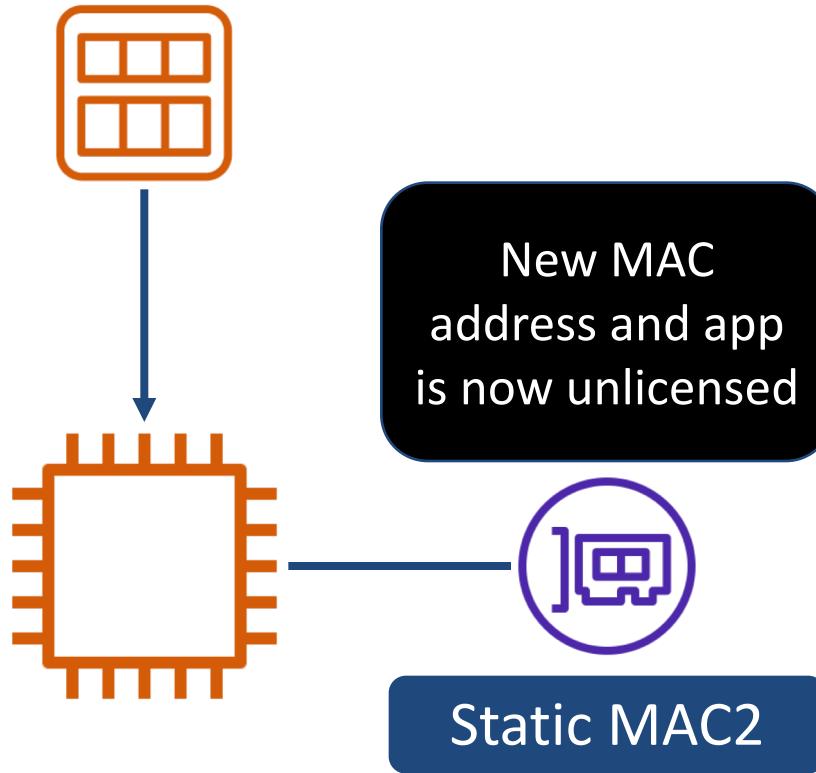


EC2 Static MAC Implementation



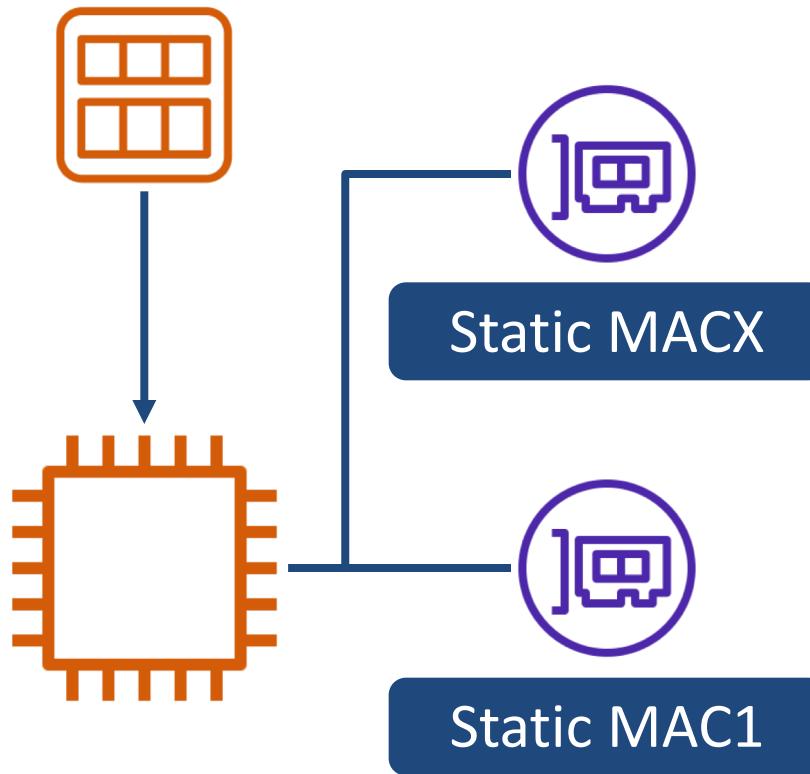
What if the
instance must be
re-launched?

EC2 Static MAC Implementation



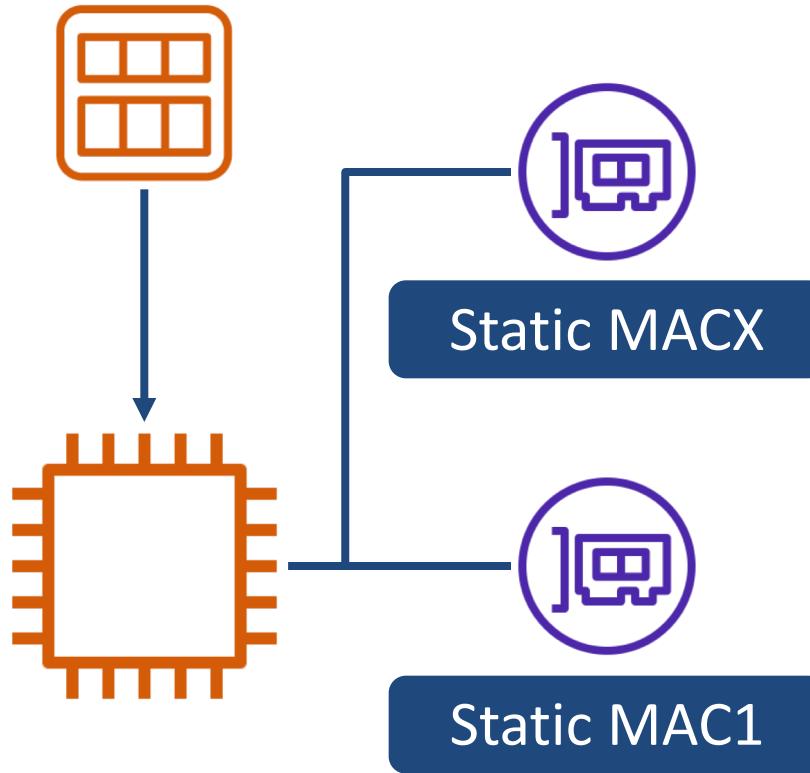
What if the instance must be re-launched?

EC2 Static MAC Implementation



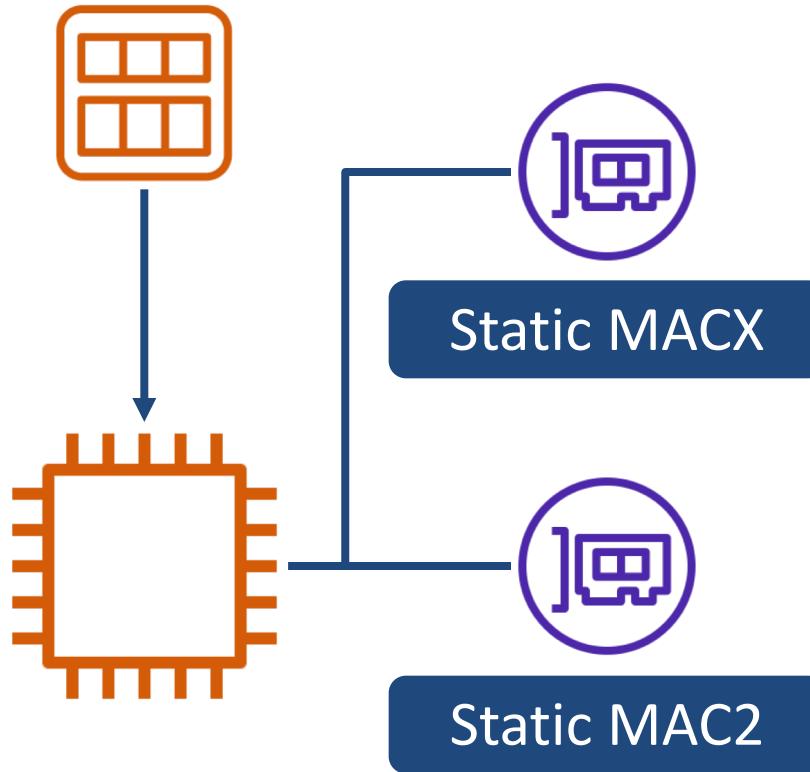
Instead, attach a secondary ENI

EC2 Static MAC Implementation



And if the
instance must be
replaced....

EC2 Static MAC Implementation



The secondary ENI can simply be reattached

Question Breakdown

Question Scenario

An operations team in a large company has been tasked with the migration of multiple applications. These applications share a Microsoft SQL Server database server with 1Tb of data. None of the database tables are shared across more than one application.

The target database will be Amazon Aurora with MySQL compatibility.

The migration must be completed with as little downtime as possible.

Which combination of steps would allow the migration to meet the requirements?
(pick two)

Answer Choices

- A. Export the schema and data from the source using SSMS and perform any conversion manually
- B. Use AWS SCT to convert and migrate the source schema to Aurora MySQL
- C. Use AWS SCT to convert the source schema to Aurora MySQL and migrate data using the SCT replication agent and DMS
- D. Use DMS to migrate data using a full-load task + CDC, then cut over apps individually
- E. Use DMS to migrate data using a full-load task, then schedule downtime to cut over all apps
- F. Manually import the exported schema and data into Aurora MySQL

Answer A

This would be part of a functional solution, but does not account for any schema or data copy/import tasks

Export the schema and data from the source using SSMS and perform any conversion manually

Answer B

This would also be part of a functional solution (like A) but does account for the full schema migration to the target, and requires little or no downtime

Use AWS SCT to convert and migrate the source schema to Aurora MySQL

Answer C

This looks like a great solution to combine the migration of schema and data. The SCT replication agent uses Snowball Edge as an asynchronous mechanism for very large-scale migrations. As this DB is only 1Tb, this is not appropriate.

Use AWS SCT to convert the source schema to Aurora MySQL and migrate data using the SCT replication agent and DMS

Answer D

Using DMS for full-load + CDC will ensure ongoing replication and minimize the need for downtime as applications are cut over individually.

Use DMS to migrate data using a full-load task + CDC, then cut over apps individually

Answer E

This is an interesting solution, and could potentially meet the capacity and throughput requirements, security could be an issue.

Use DMS to migrate data using a full-load task, then schedule downtime to cut over all apps

Answer F

Combining this answer with A would result in a fully functional workflow, but would require enough downtime to perform the data import, which could be substantial.

Manually import the exported schema and data into Aurora MySQL

Correct Answer

- A. Export the schema and data from the source using SSMS and perform any conversion manually
- B. Use AWS SCT to convert and migrate the source schema to Aurora MySQL
- C. Use AWS SCT to convert the source schema to Aurora MySQL and migrate data using the SCT replication agent and DMS
- D. Use DMS to migrate data using a full-load task + CDC, then cut over apps individually
- E. Use DMS to migrate data using a full-load task, then schedule downtime to cut over all apps
- F. Manually import the exported schema and data into Aurora MySQL



Migration Execution Scenario

Scenario Description

An on-premises operations team has been tasked with migrating 900Tb data into a single AWS S3 bucket. The data is currently stored on a NAS and accessed via NFS mounts. The company has Direct Connect connectivity to AWS with 10Gb bandwidth.

The data must remain available on-premises during the transfer.

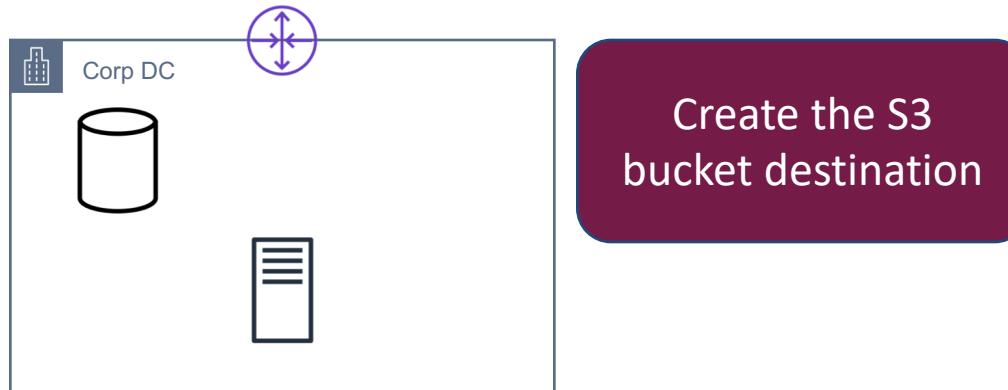
Which migration solution can meet the availability requirement with the least operational overhead?

Scenario Questions to Ask



- What storage solutions can migrate data to S3?
- What are data size limitations for each solution?

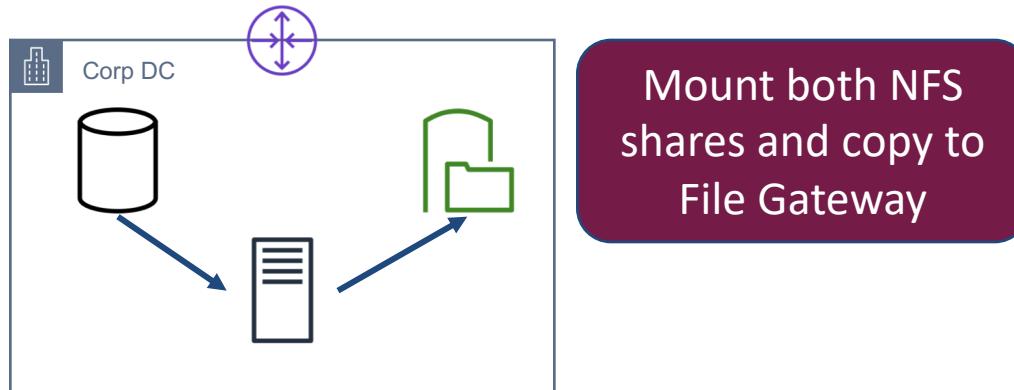
Storage Gateway Option



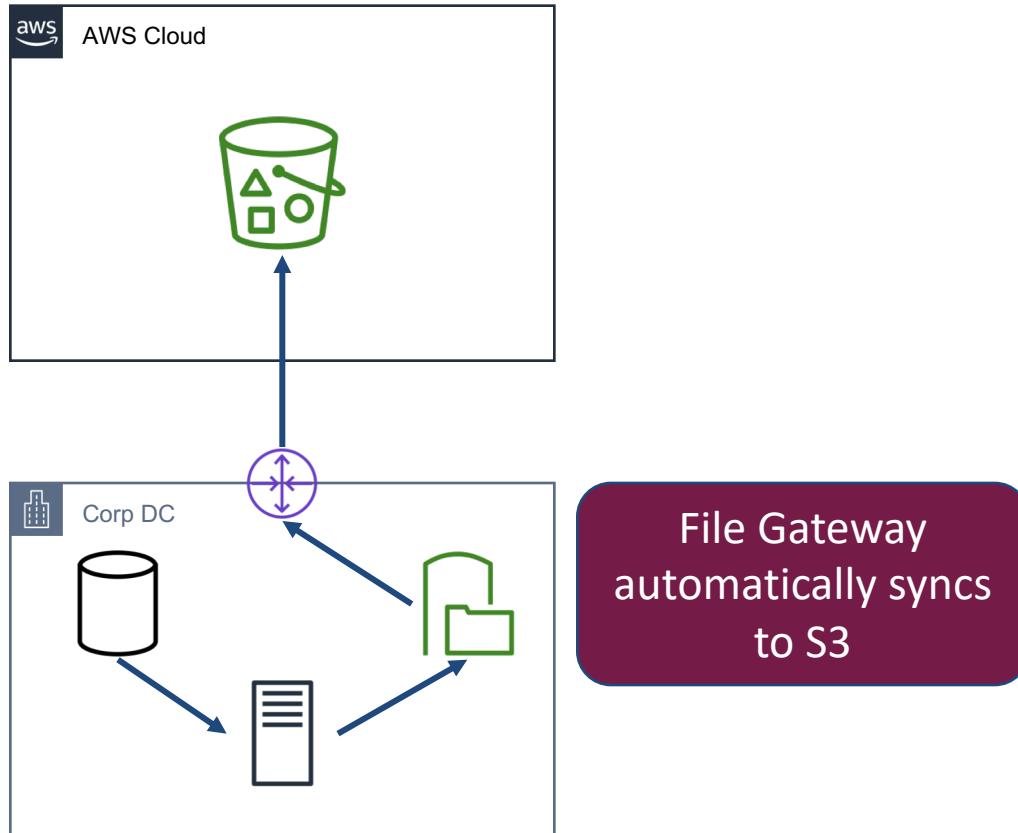
Storage Gateway Option



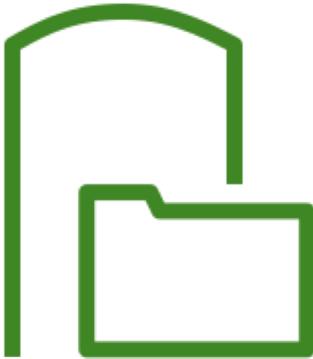
Storage Gateway Option



Storage Gateway Option

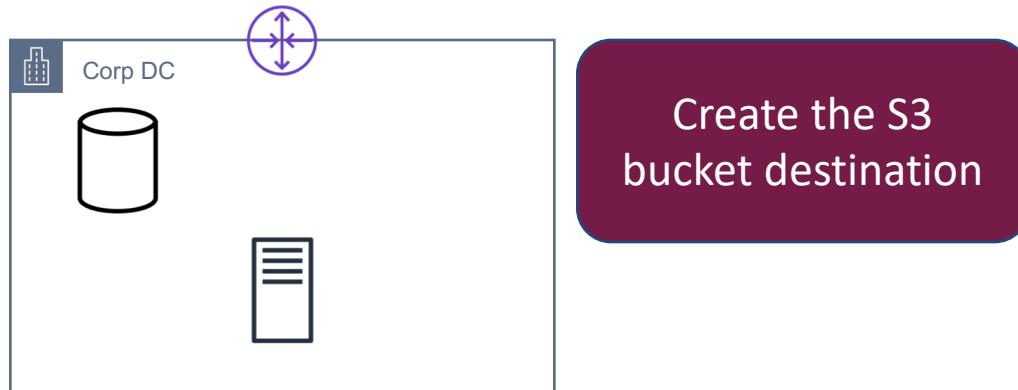


Storage Gateway Considerations

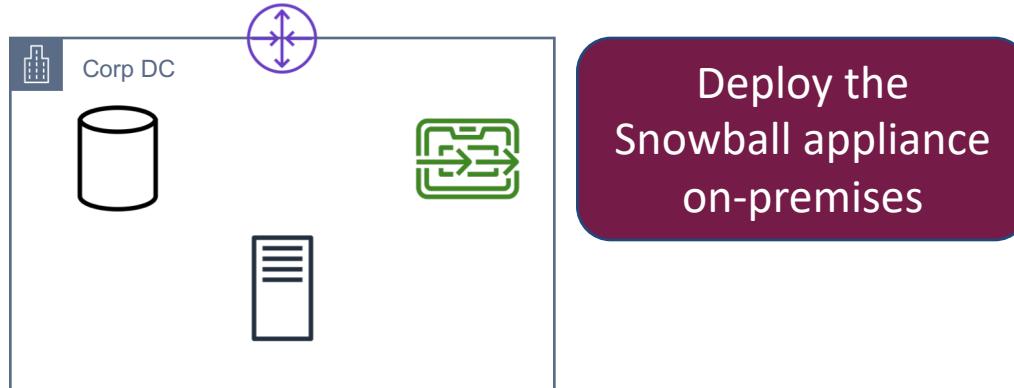


Requires on-premises storage
Cannot store entire data set (64Tb)

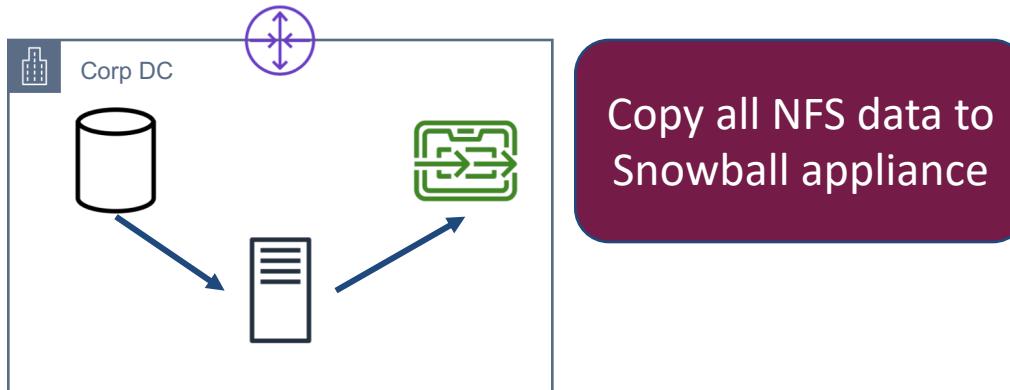
Snowball Option



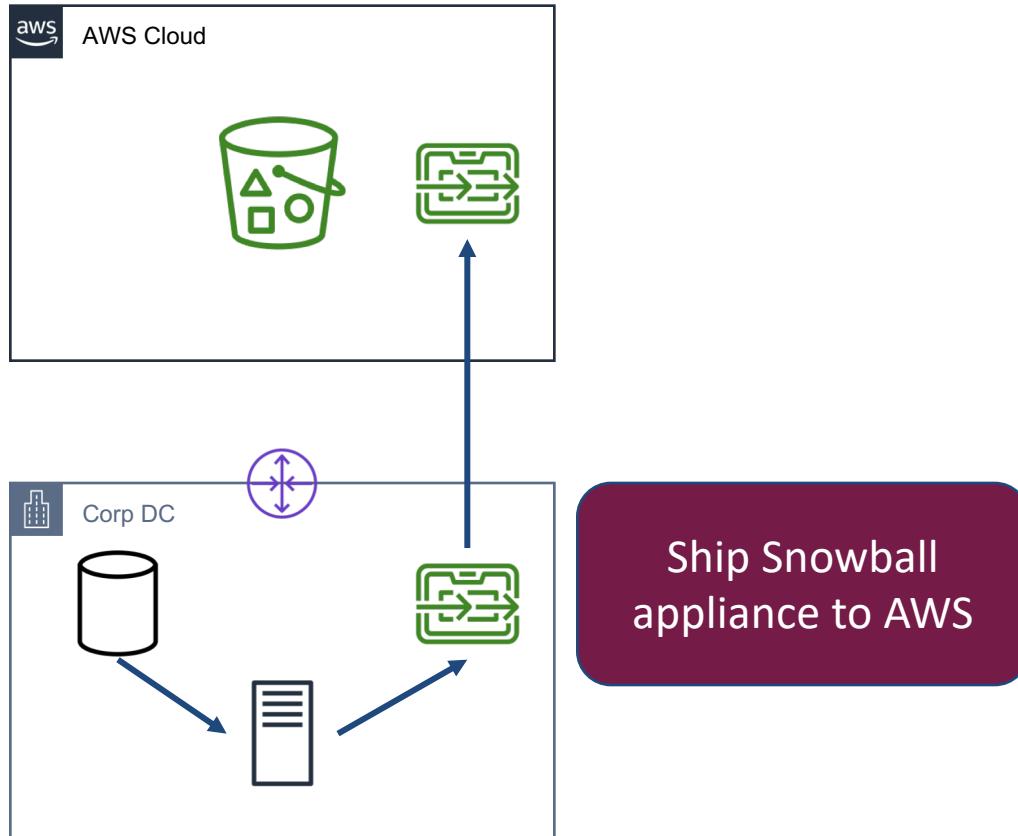
Snowball Option



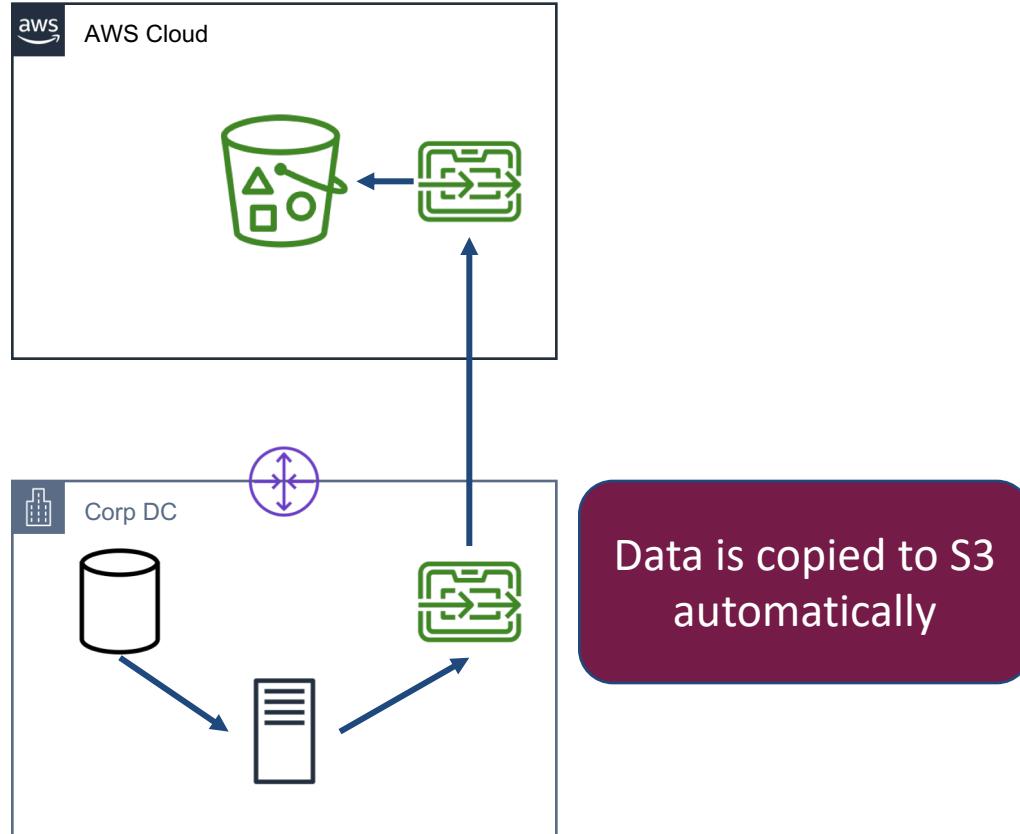
Snowball Option



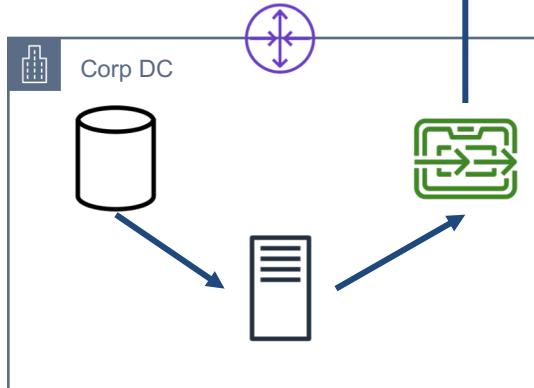
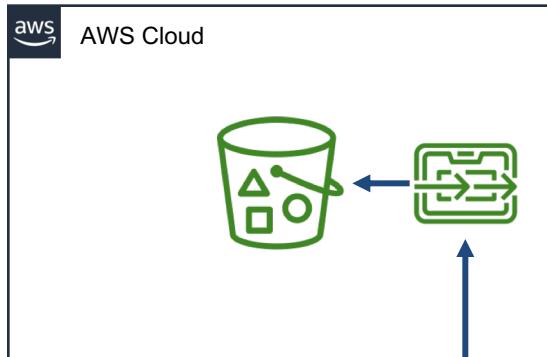
Snowball Option



Snowball Option



Snowball Option



You'll need at least 9 of these to copy the data

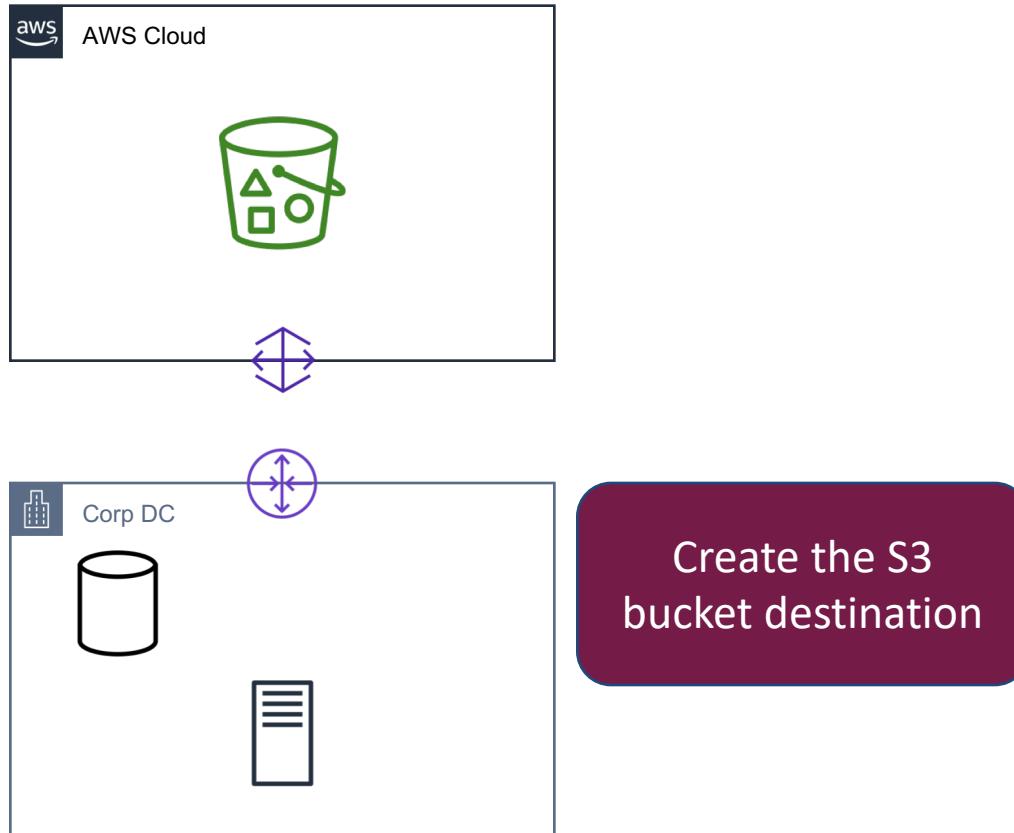
But wait, Snowball only supports 100Tb

Snowball Considerations

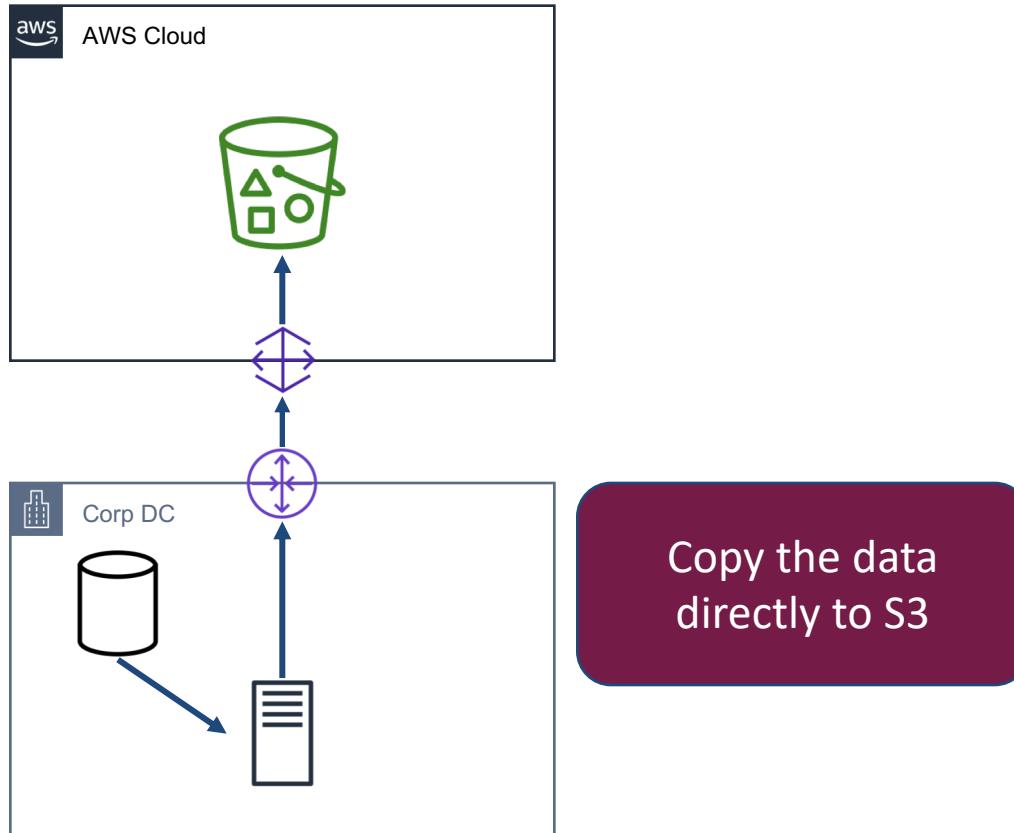


- Appliance-based
- Cannot perform direct copy
- Cannot store entire data set
- Requires time to ship

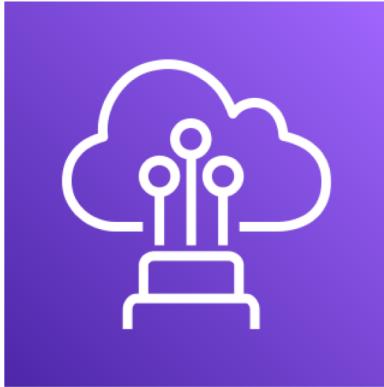
Direct Connect Option



Direct Connect Option

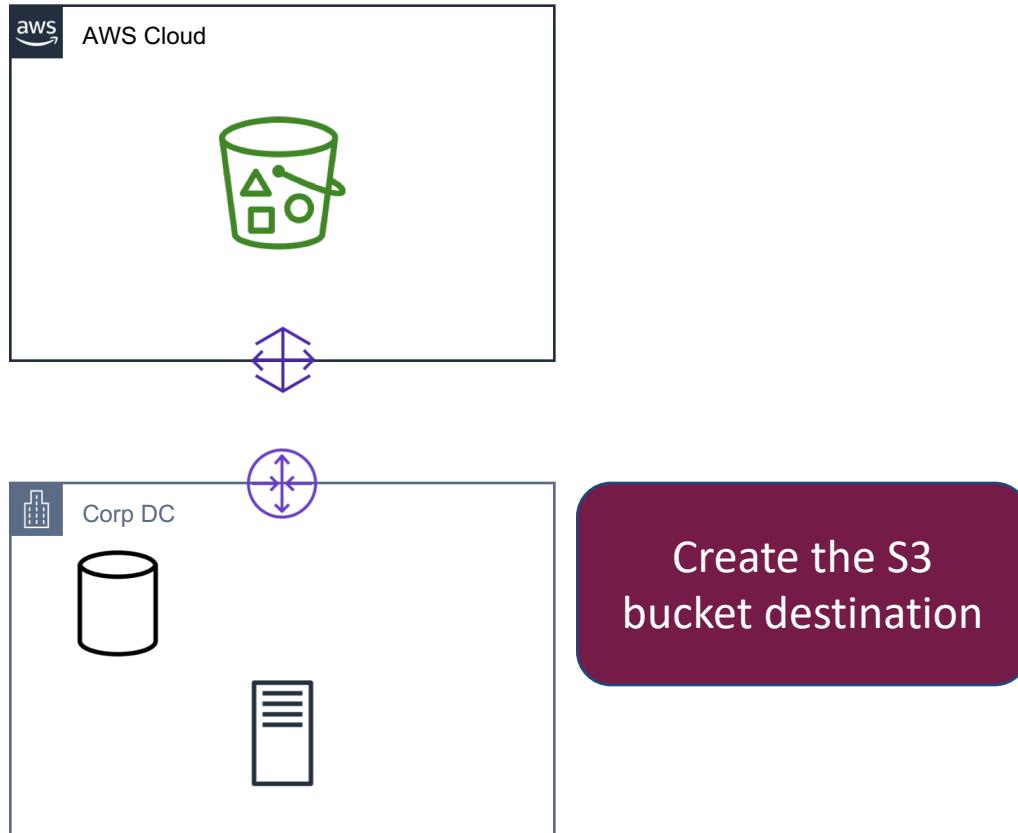


Direct Connect Considerations

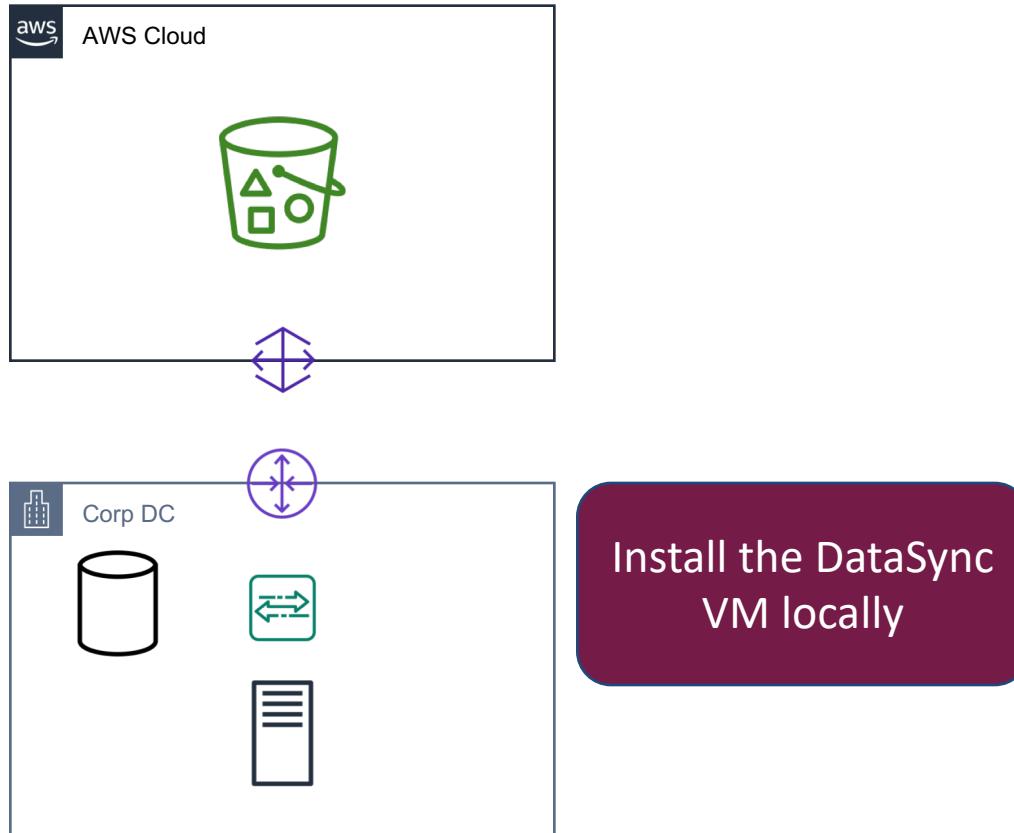


- Direct copy only
- No storage hardware
- Copy could use all DX bandwidth

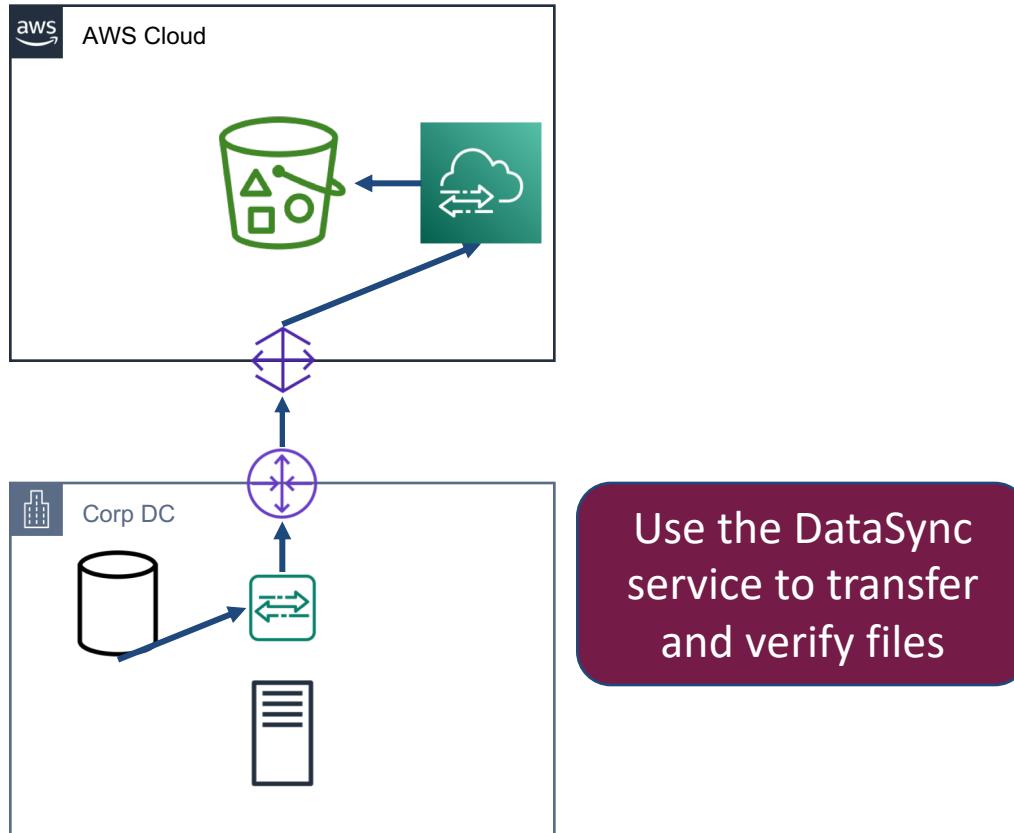
DataSync Option (Using DX)



DataSync Option (Using DX)



DataSync Option (Using DX)



DataSync Option (Using DX)



- Direct copy only
- No storage hardware
- Copy could use all DX bandwidth
- File integrity is ensured
- Handles synchronization

Question Breakdown

Question Scenario

A production application has been scheduled to be migrated to AWS. The application is a two-tier architecture with load balancer and VM app servers. The company has planned migrations to ALB, and EC2.

The application is revenue critical, and there must be minimal downtime during migration and cutover.

The migration can take as much time as needed to meet the requirements.

Which of the following tasks should the proposal include?

Answer Choices

- A. Configure weighted Route 53 records for both the current endpoint and the new ALB. When the cutover window is active, gradually change weights until the ALB endpoint is taking 100% of the traffic.
- B. Configure latency Route 53 records for both the current endpoint and the new ALB. When the cutover window is active, remove the record for the current endpoint.
- C. Deploy a CloudFront distribution and add the current and new endpoints as separate origins. Configure CloudFront origin failover with current endpoint as primary and new endpoint as secondary. Migrate the DNS endpoint to CloudFront.
- D. Deploy a CloudFront distribution and add the current and new endpoints in a single origin group. Configure CloudFront origin failover with current endpoint as primary and new endpoint as secondary. Migrate the DNS endpoint to CloudFront.

Answer A

This set of tasks would meet the functional requirements. This is essentially a blue/green deployment with a gradual shift of traffic until AWS is taking all of it, and would indeed minimize downtime.

Configure weighted Route 53 records for both the current endpoint and the new ALB. When the cutover window is active, gradually change weights until the ALB endpoint is taking 100% of the traffic.

Answer B

This solution is functional, and would optimize for performance (latency) from the end user to the endpoints, but could possibly have a long outage with cached DNS records not recognizing the removal of the on-premises endpoint.

Configure latency Route 53 records for both the current endpoint and the new ALB. When the cutover window is active, remove the record for the current endpoint.

Answer C

This is a functional, but incomplete, solution. There is no mention of an actual cutover, but if we assume that origin failover will cover the deprovisioning of the on-premises endpoint, the outage would be based on the thresholds set for healthy endpoints.

Deploy a CloudFront distribution and add the current and new endpoints as separate origins. Configure CloudFront origin failover with current endpoint as primary and new endpoint as secondary. Migrate the DNS endpoint to CloudFront.

Answer D

This is very similar to answer C, and seems functional. However, you cannot configure origin failover within the same origin group, so this solution will not work.

Deploy a CloudFront distribution and add the current and new endpoints in a single origin group. Configure CloudFront origin failover with current endpoint as primary and new endpoint as secondary. Migrate the DNS endpoint to CloudFront.

Correct Answer

- A. Configure weighted Route 53 records for both the current endpoint and the new ALB. When the cutover window is active, gradually change weights until the ALB endpoint is taking 100% of the traffic.
- B. Configure latency Route 53 records for both the current endpoint and the new ALB. When the cutover window is active, remove the record for the current endpoint.
- C. Deploy a CloudFront distribution and add the current and new endpoints as separate origins. Configure CloudFront origin failover with current endpoint as primary and new endpoint as secondary. Migrate the DNS endpoint to CloudFront.
- D. Deploy a CloudFront distribution and add the current and new endpoints in a single origin group. Configure CloudFront origin failover with current endpoint as primary and new endpoint as secondary. Migrate the DNS endpoint to CloudFront.



Domain 4: Cost Control

12.5%

Question Domain 4 Points

4.1 Select a cost-effective pricing model for a solution

Question Domain 4 Points

4.2 Determine which controls to design and implement that will ensure cost optimization

Question Domain 4 Points

4.3 Identify opportunities to reduce cost in an existing solution



Pricing Model Scenario

Scenario Description

An analysis application has been deployed for your company's partners. Partner data is uploaded through the app and stored on EFS. The app inserts a message into SQS for each data set upload. The app has unpredictable traffic.

Your company would like to analyze data as quickly as possible without a large static cluster of EC2 instances waiting for work.

The analysis solution must optimize for cost.

Which analysis solution will meet the requirements?

Scenario Questions to Ask



- What compute options are available for analysis?
- How can scaling happen based on SQS?
- What solutions have integration with EFS?

Analysis Compute Options



EC2



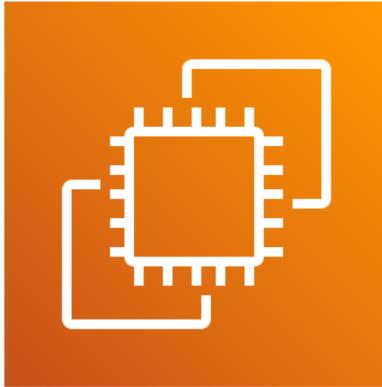
ECS



Lambda

- What are the upper limits on CPU and memory?
- How is scaling achieved?
- Can scaling happen based on messages in SQS?





- Very large resource ceiling
- Scale vertically by resizing
- Scale horizontally by Auto Scaling
- Can scale according to SQS message queue depth

ECS on Fargate



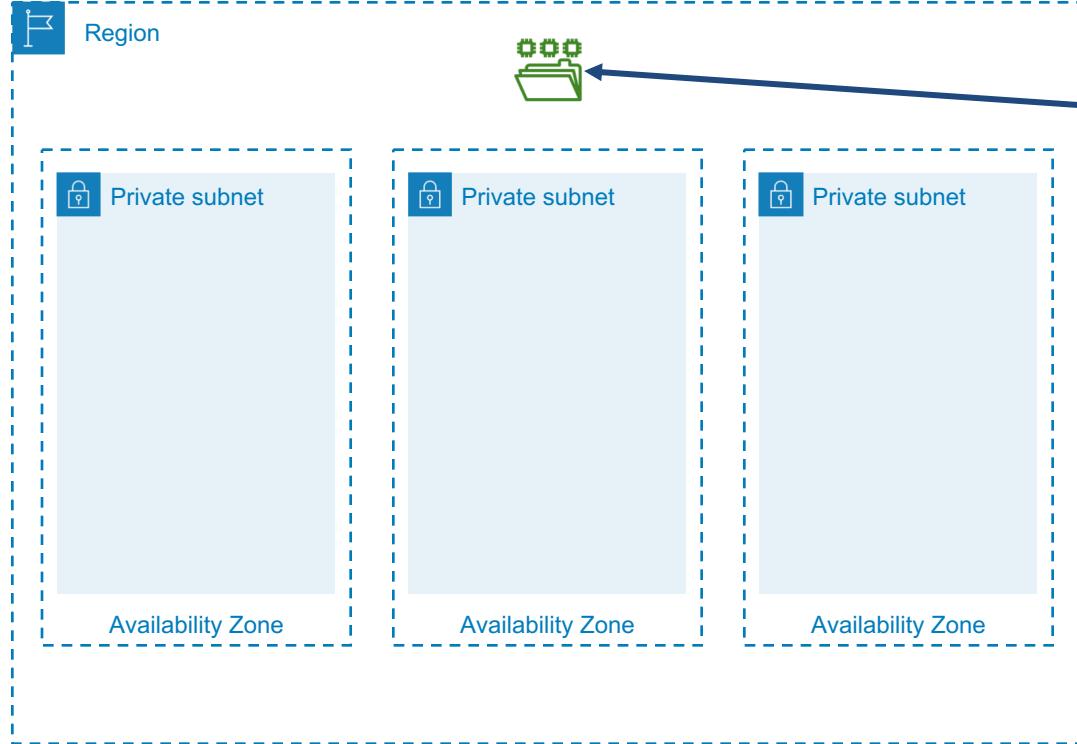
- 4 vCPU, 30Gb mem
- Scale horizontally by Auto Scaling
- Can scale according to SQS message queue depth

Lambda



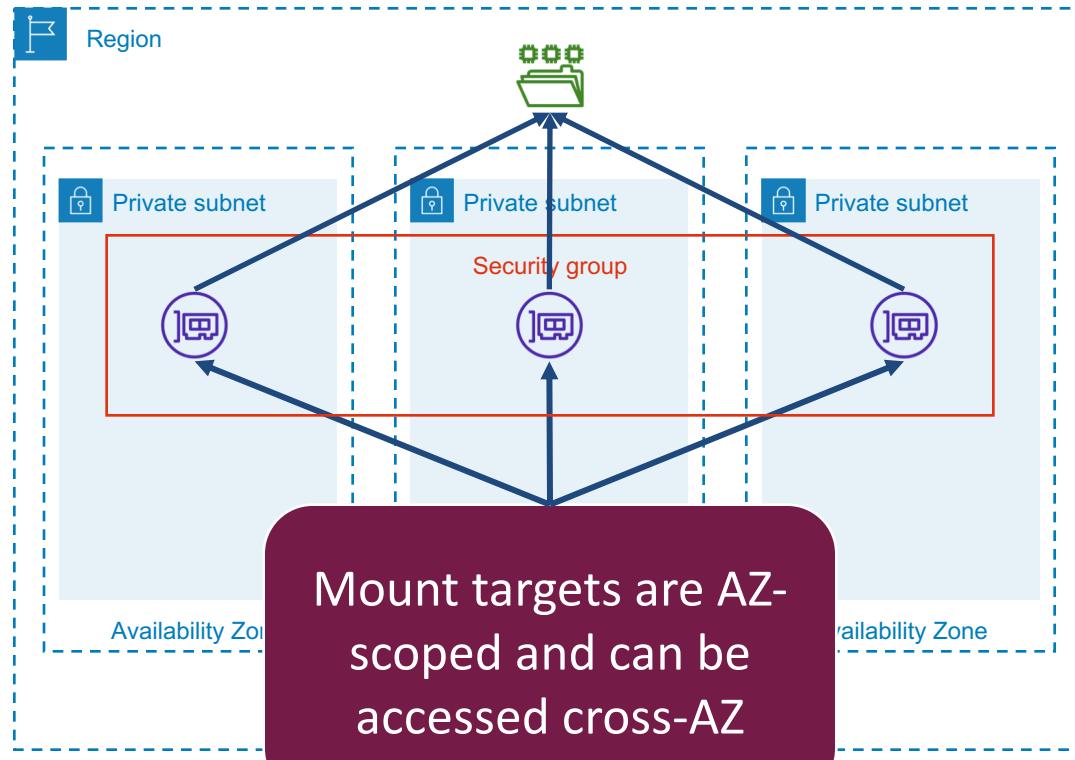
- 6 vCPU, 10Gb mem
- 15min runtime
- Scale horizontally by concurrency value
- Can scale according to SQS message queue depth

EFS Implementation



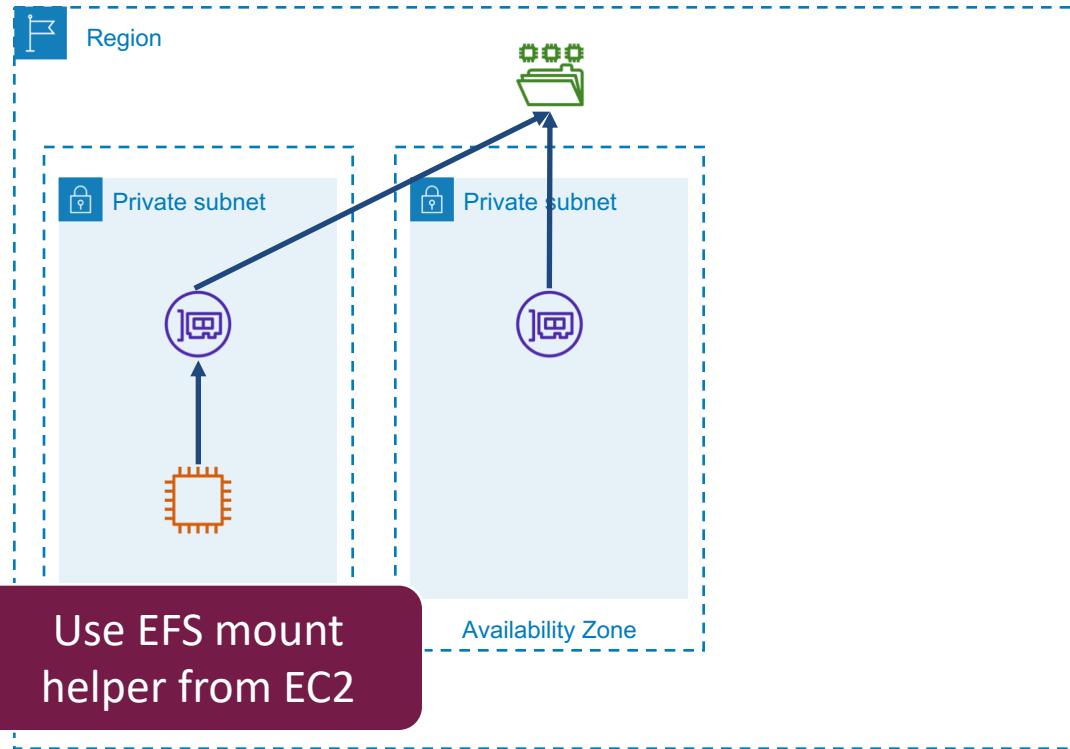
EFS file system
resource is region-
scoped

EFS Implementation

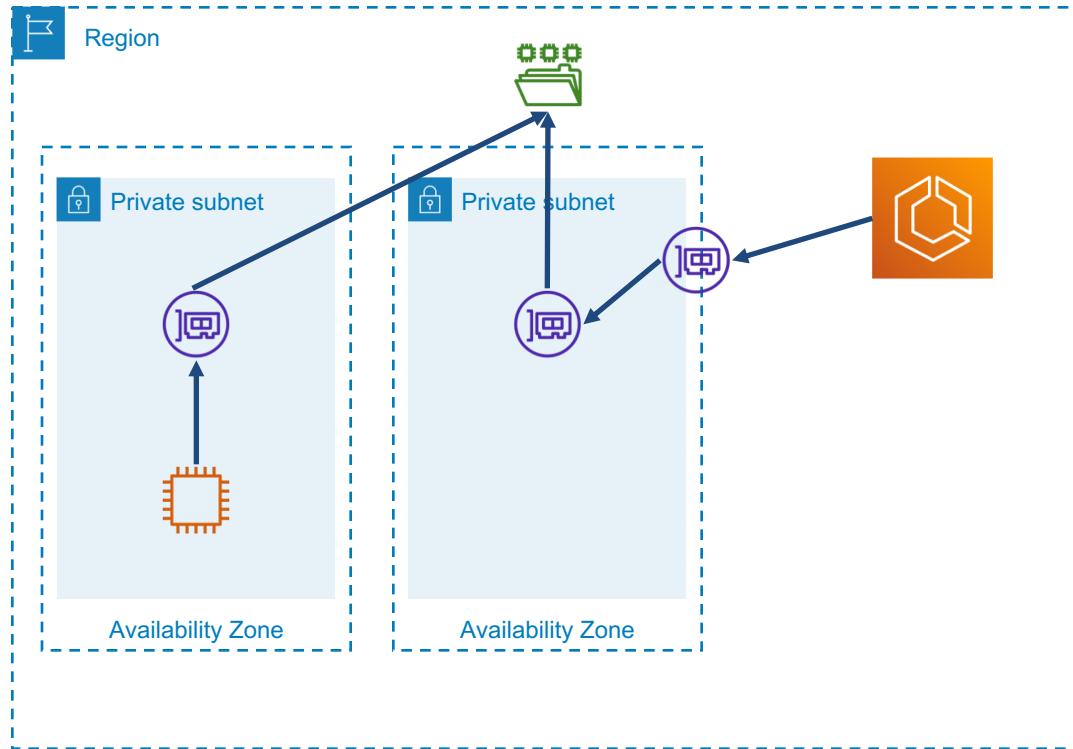


Pro tip: use the DNS name of the filesystem when mounting to automatically use the closest mount target!

EFS Mounts

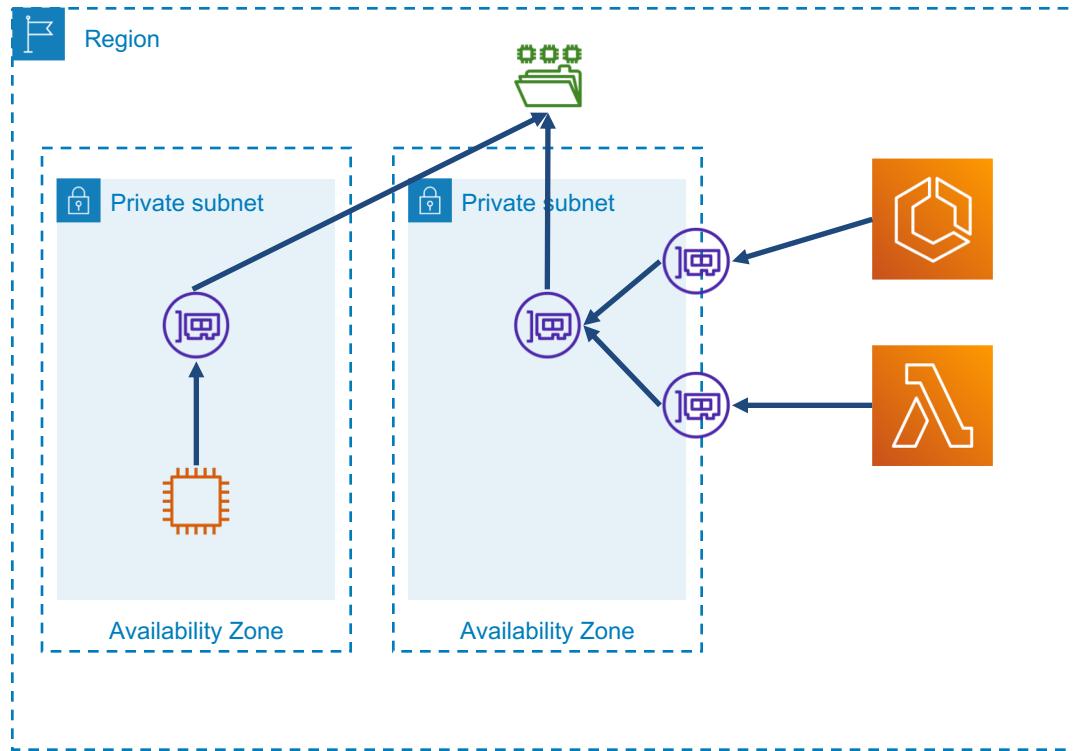


EFS Mounts



Mount on ECS
containers in Fargate

EFS Mounts



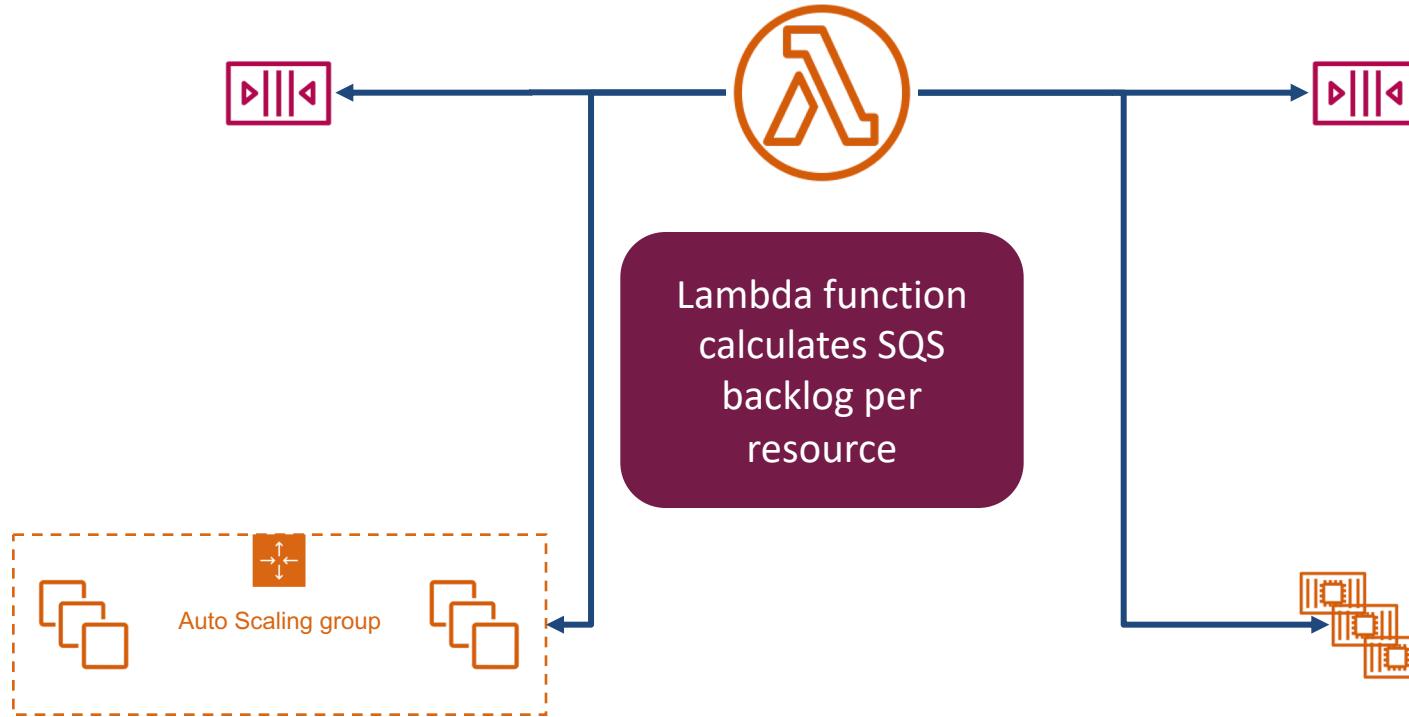
Mount on Lambda
functions

Auto Scaling EC2 and ECS with SQS

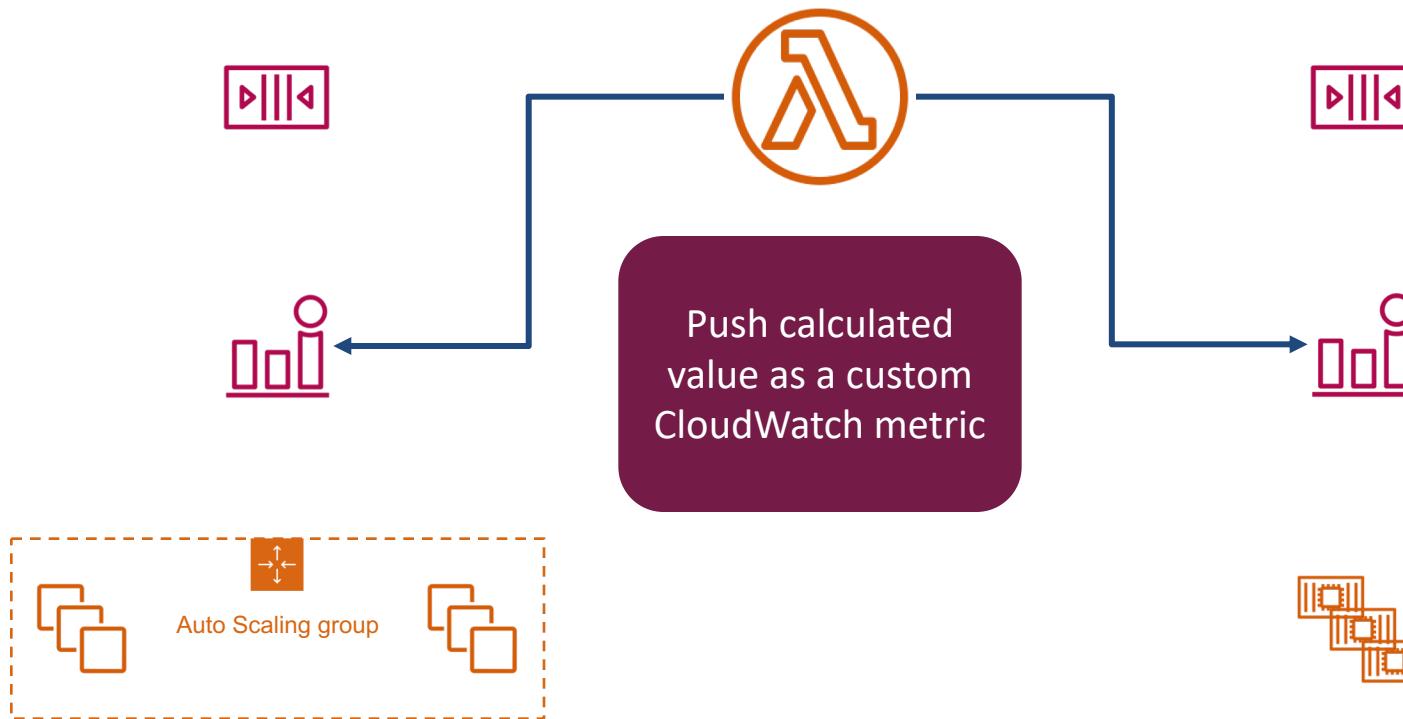


Execute scheduled
Lambda function
every minute

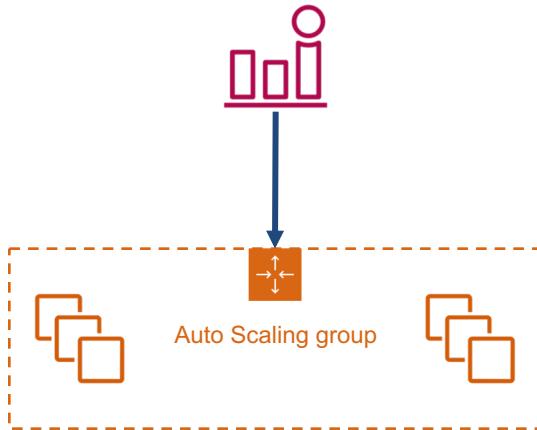
Auto Scaling EC2 and ECS with SQS



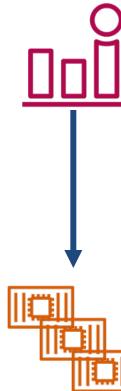
Auto Scaling EC2 and ECS with SQS



Auto Scaling EC2 and ECS with SQS



Compare custom metric to acceptable backlog target value and scale accordingly

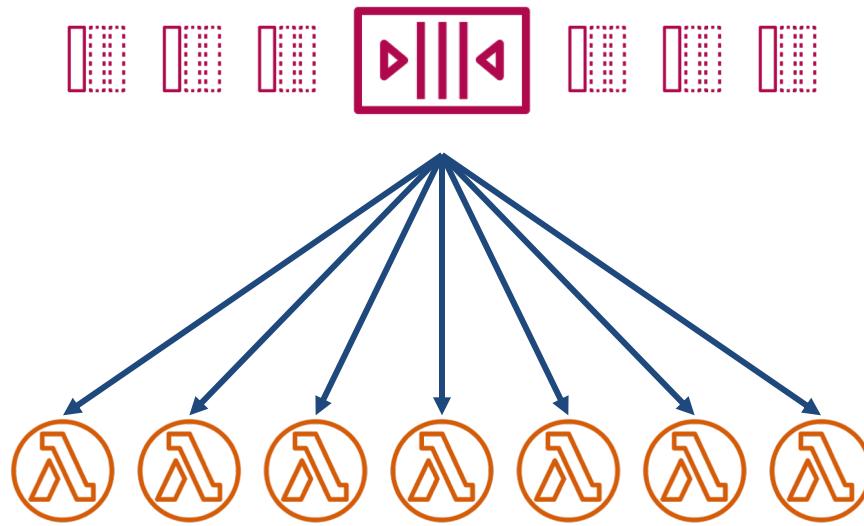


Auto Scaling Lambda with SQS



Configure Lambda
function with SQS
trigger

Auto Scaling Lambda with SQS



Configure Lambda function concurrency to acceptable value for parallel processing

Question Breakdown

Question Scenario

A load testing infrastructure generates ELB access logs that are delivered to S3. The environment isn't used all the time, but when it is in use, it generates a large amount of logs.

There is a requirement to analyze the access logs in AWS OpenSearch as quickly as possible.

The analysis pipeline must maximize availability in case logs are generated, and minimize ongoing costs.

What analysis architecture will meet these requirements?

Answer Choices

- A. Configure an EventBridge rule to trigger a Lambda function hourly. From the Lambda function, trigger an EMR job to deliver the access logs to Elasticsearch.
- B. Configure S3 event notifications to trigger a Lambda function upon log delivery. From the Lambda function, invoke an AWS Batch job to insert the log entries directly into the Elasticsearch cluster.
- C. Configure S3 event notifications to trigger a Lambda function upon log delivery. Insert the log entries directly into the OpenSearch cluster.
- D. Configure S3 event notifications to trigger a Lambda function upon log delivery. Insert the log entries into a Kinesis Data Firehose. Configure the OpenSearch cluster as the destination.

Answer A

This solution meets the functional requirements. Since it is triggered hourly, there may be another solution which operates closer to real-time.

Configure an EventBridge rule to trigger a Lambda function hourly. From the Lambda function, trigger an EMR job to deliver the access logs to OpenSearch.

Answer B

This solution would be similar to A in that it is a batch function. It may be better as it uses S3 event notifications, but it is still not optimized for speed.

Configure S3 event notifications to trigger a Lambda function upon log delivery. From the Lambda function, invoke an AWS Batch job to insert the log entries directly into the OpenSearch cluster.

Answer C

This solution is functional, and entirely event-driven. A major concern is that log delivery will be spiky according to load test jobs, and may overload the OpenSearch cluster unless it is upsized....which impacts cost.

Configure S3 event notifications to trigger a Lambda function upon log delivery. Insert the log entries directly into the OpenSearch cluster.

Answer D

This solution is similar to C, with the insertion of the Kinesis Data Firehose between Lambda and OpenSearch. That middle tier will absorb any spiky log delivery and ensure the OpenSearch cluster can be minimally sized to optimize cost.

Configure S3 event notifications to trigger a Lambda function upon log delivery. Insert the log entries into a Kinesis Data Firehose. Configure the OpenSearch cluster as the destination.

Correct Answer

- A. Configure an EventBridge rule to trigger a Lambda function hourly. From the Lambda function, trigger an EMR job to deliver the access logs to Elasticsearch.
- B. Configure S3 event notifications to trigger a Lambda function upon log delivery. From the Lambda function, invoke an AWS Batch job to insert the log entries directly into the OpenSearch cluster.
- C. Configure S3 event notifications to trigger a Lambda function upon log delivery. Insert the log entries directly into the OpenSearch cluster.
- D. Configure S3 event notifications to trigger a Lambda function upon log delivery. Insert the log entries into a Kinesis Data Firehose. Configure the OpenSearch cluster as the destination.



Cost Reduction Scenario

Scenario Description

A company is using Redshift as a data warehouse for a large data set. The current cluster is running on 50 ds2 nodes. The data has grown organically over several months and the cluster is nearly out of space.

Most of the data is only queried occasionally, but must be available when a query is issued.

The company wants to address the disk space while reducing costs.

How can the cluster be re-deployed using cost reduction strategies?

Scenario Questions to Ask

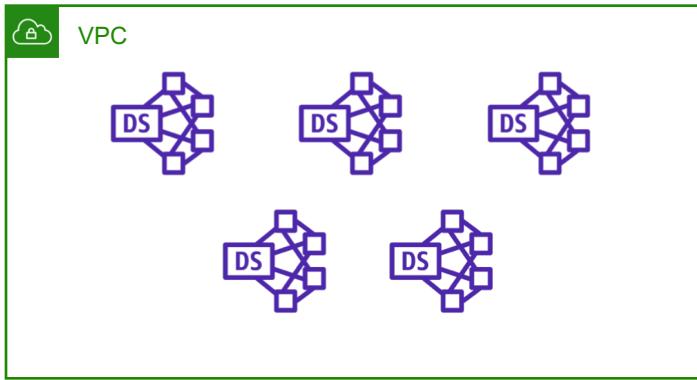


- Can the existing architecture be cost optimized?
- Are there cheaper Redshift compute options than ds2?
- Can the data be queried from another location?

Existing Redshift Infrastructure



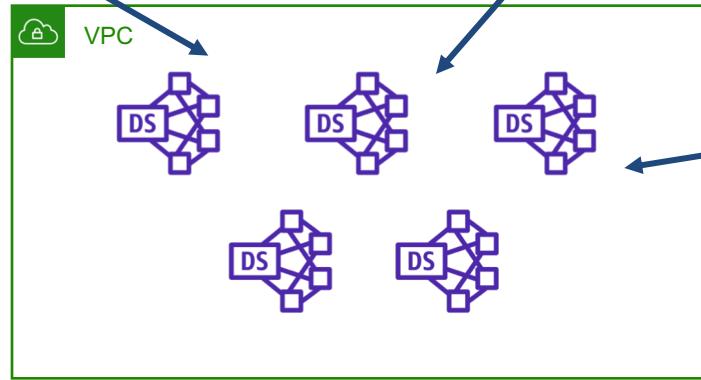
10 ds2 nodes



Improving Existing Architecture

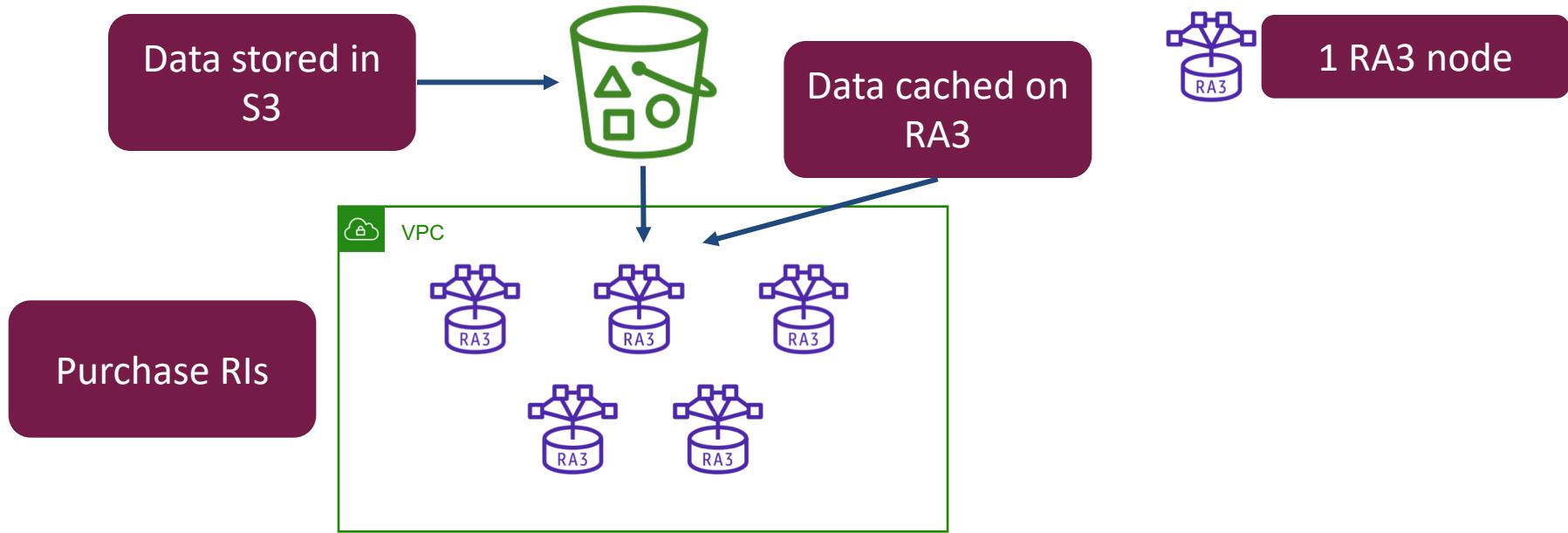
Purchase RIs

Remove temporary data

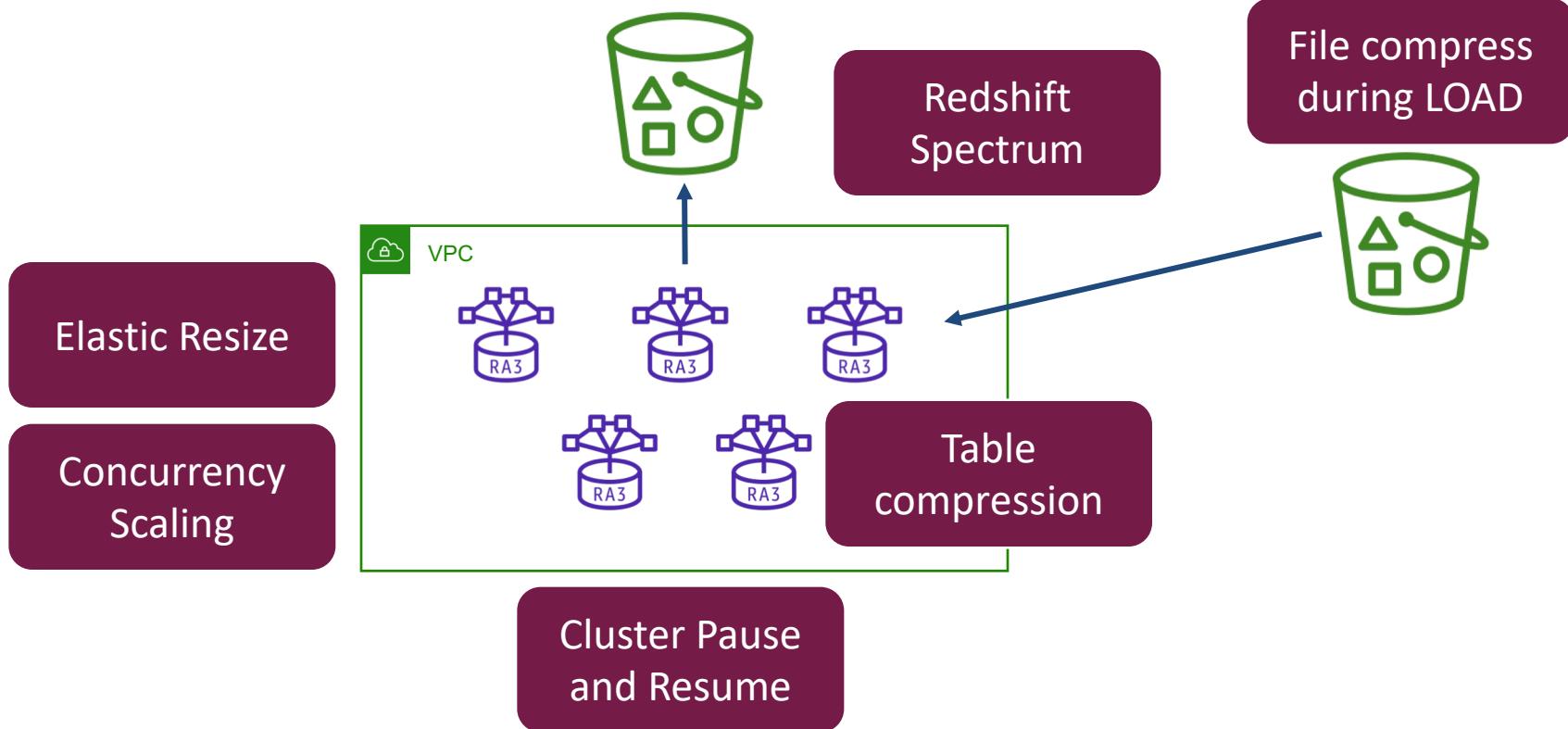


Archive unused data to S3

Cost-Effective New Architecture



Cost Reduction Features



Question Breakdown

Question Scenario

You've been retained as an AWS cost consultant for a company's application. The application back end uses DynamoDB, read and written directly by the mobile client. Extreme traffic spikes have resulted in the table being configured for On-Demand Scaling.

DynamoDB costs are much higher than expected, and it has been determined that mobile clients need read access but not write access if there is an alternative.

The proposed solution must optimize DynamoDB cost reduction.
What changes can meet this requirement?
(pick two)

Answer Choices

- A. Reconfigure the DynamoDB table to use Provisioned read and write operations at the daily average to avoid unexpected charges due to On-Demand scaling.
- B. Deploy a DynamoDB Accelerator (DAX) cluster to improve read and write performance on the table.
- C. Purchase reservations for read and write capacity throughput for the minimum daily values of each.
- D. Reconfigure the mobile application to deliver writes to an SQS queue, triggering a Lambda function to insert into the table with limited concurrency.
- E. Reconfigure the DynamoDB table to use Auto Scaling based on the daily minimum and maximum read and write operations.

Answer A

Static provisioning would at least guarantee a consistent charge for use of the table read/write operations, but may not meet the application requirements for functionality during traffic peaks.

Reconfigure the DynamoDB table to use Provisioned read and write operations at the daily average to avoid unexpected charges due to On-Demand scaling.

Answer B

DAX is great for improving table performance, but is deployed inside a VPC using compute resources, which may not be reachable from the application, nor reduce costs.

Deploy a DynamoDB Accelerator (DAX) cluster to improve read and write performance on the table.

Answer C

This recommendation is sure to reduce costs, as the minimum usage will now be charged at a discount for the reservation.

Purchase reservations for read and write capacity throughput for the minimum daily values of each.

Answer D

This option is more overall effort, but may deliver the best cost reduction, as it eliminates writes entirely from the mobile application, while simultaneously flattening the spikes into smoother curves which can be controlled via Lambda function concurrency values.

Reconfigure the mobile application to deliver writes to an SQS queue, triggering a Lambda function to insert into the table with limited concurrency.

Answer E

This option may not make any difference whatsoever, as it is just duplicating the function of On-Demand scaling. The only possible cost reduction here would be if the traffic spikes grow larger over time, which is not stated in the scenario.

Reconfigure the DynamoDB table to use Auto Scaling based on the daily minimum and maximum read and write operations.

Correct Answer

- A. Reconfigure the DynamoDB table to use Provisioned read and write operations at the daily average to avoid unexpected charges due to On-Demand scaling.
- B. Deploy a DynamoDB Accelerator (DAX) cluster to improve read and write performance on the table.
- C. Purchase reservations for read and write capacity throughput for the minimum daily values of each.
- D. Reconfigure the mobile application to deliver writes to an SQS queue, triggering a Lambda function to insert into the table with limited concurrency.
- E. Reconfigure the DynamoDB table to use Auto Scaling based on the daily minimum and maximum read and write operations.



Domain 5: Continuous Improvement for Existing Solutions

29%

Question Domain 5 Points

5.1 Troubleshoot solution
architectures

Question Domain 5 Points

5.2 Determine a strategy to improve an existing solution for **operational excellence**

Question Domain 5 Points

5.3 Determine a strategy to improve the **reliability** of an existing solution

Question Domain 5 Points

5.4 Determine a strategy to improve the **performance** of an existing solution

Question Domain 5 Points

5.5 Determine a strategy to improve the **security** of an existing solution

Question Domain 5 Points

5.6 Determine how to improve
the **deployment** of an existing
solution



Architecture Troubleshooting Scenario

Scenario Description

An application provisioning process launches an EC2 instance, then attaches an encrypted EBS volume to the instance for an initial copy of a base data set. The process utilizes an IAM user with static credentials to perform the attachment.

Recently, the EBS volume attachment fails, with no changes to the provisioning process.

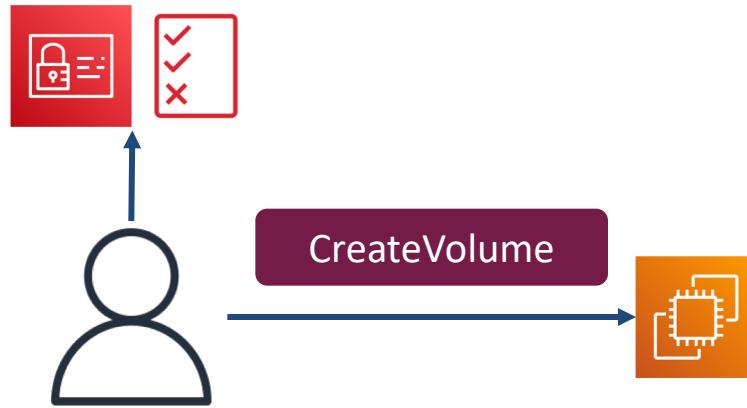
What could be the root cause for the failed EBS volume attachment in the provisioning process?

Scenario Questions to Ask



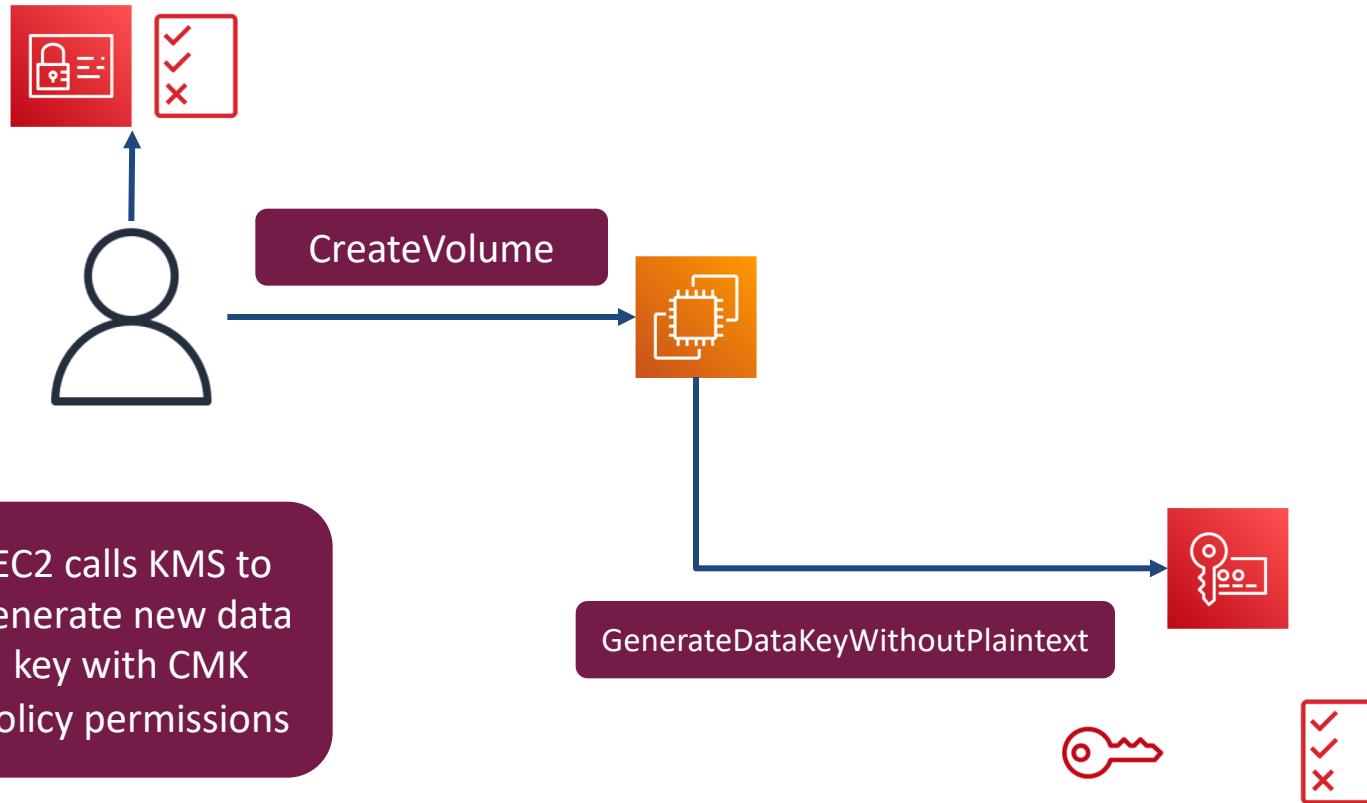
- What happens when an encrypted volume is attached to an EC2 instance?
- Where can failures occur during the attachment process?

EBS Volume Encryption Process

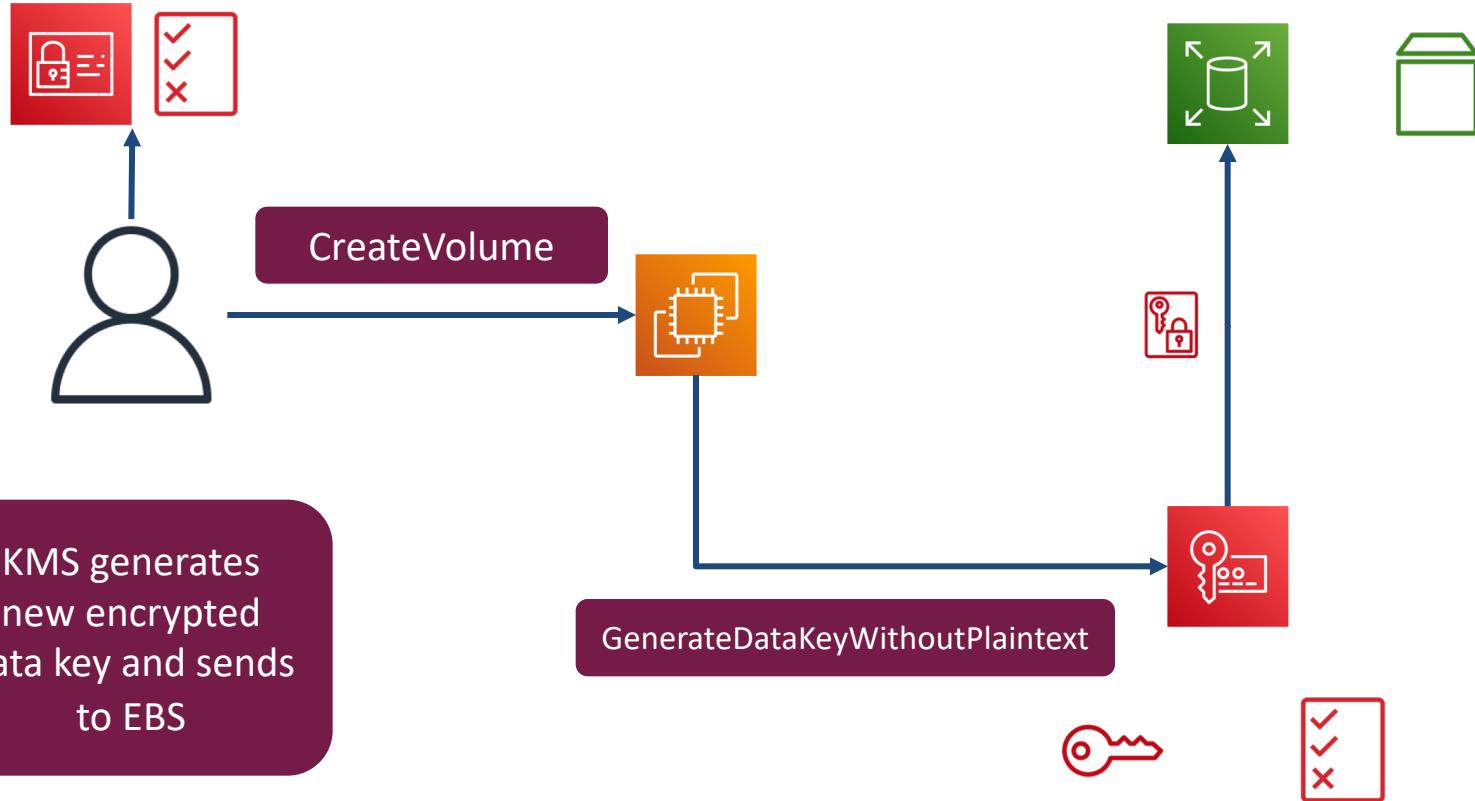


User creates EBS
Volume with IAM
permissions

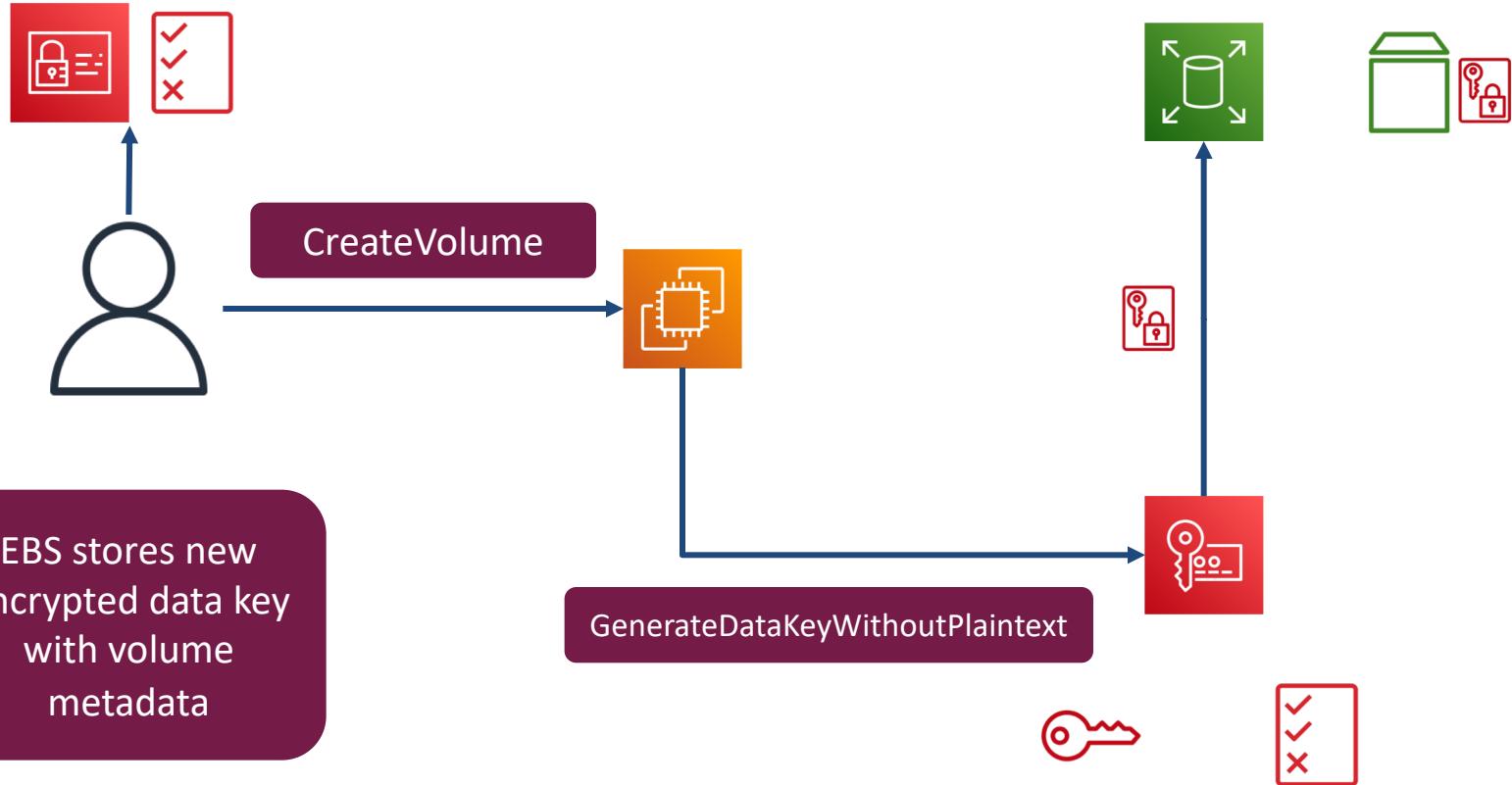
EBS Volume Encryption Process



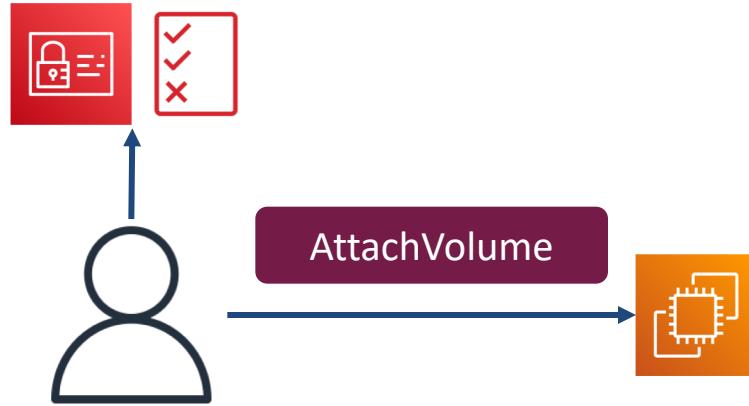
EBS Volume Encryption Process



EBS Volume Encryption Process

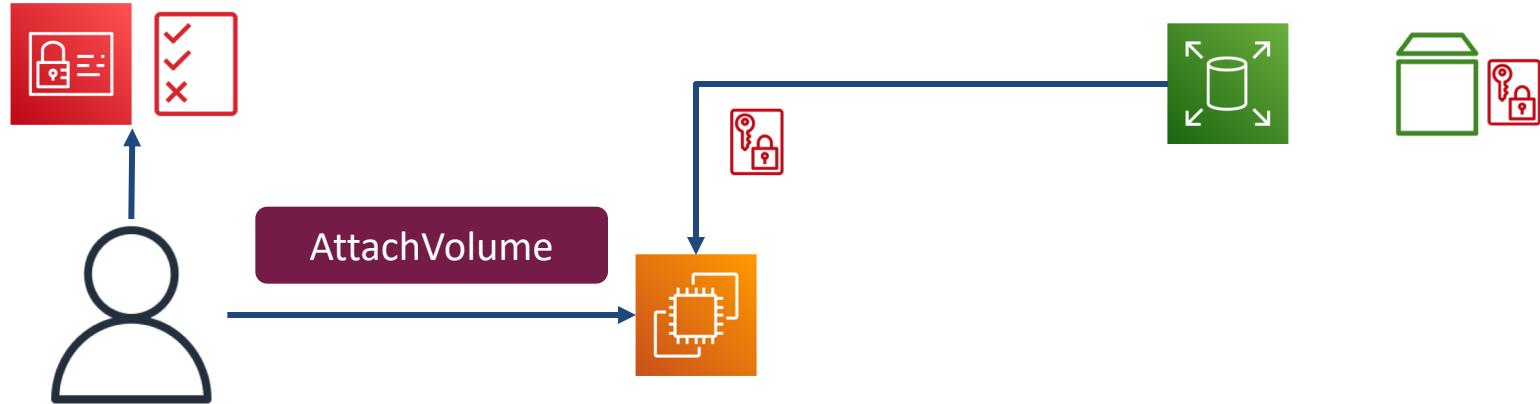


Encrypted Volume Attachment



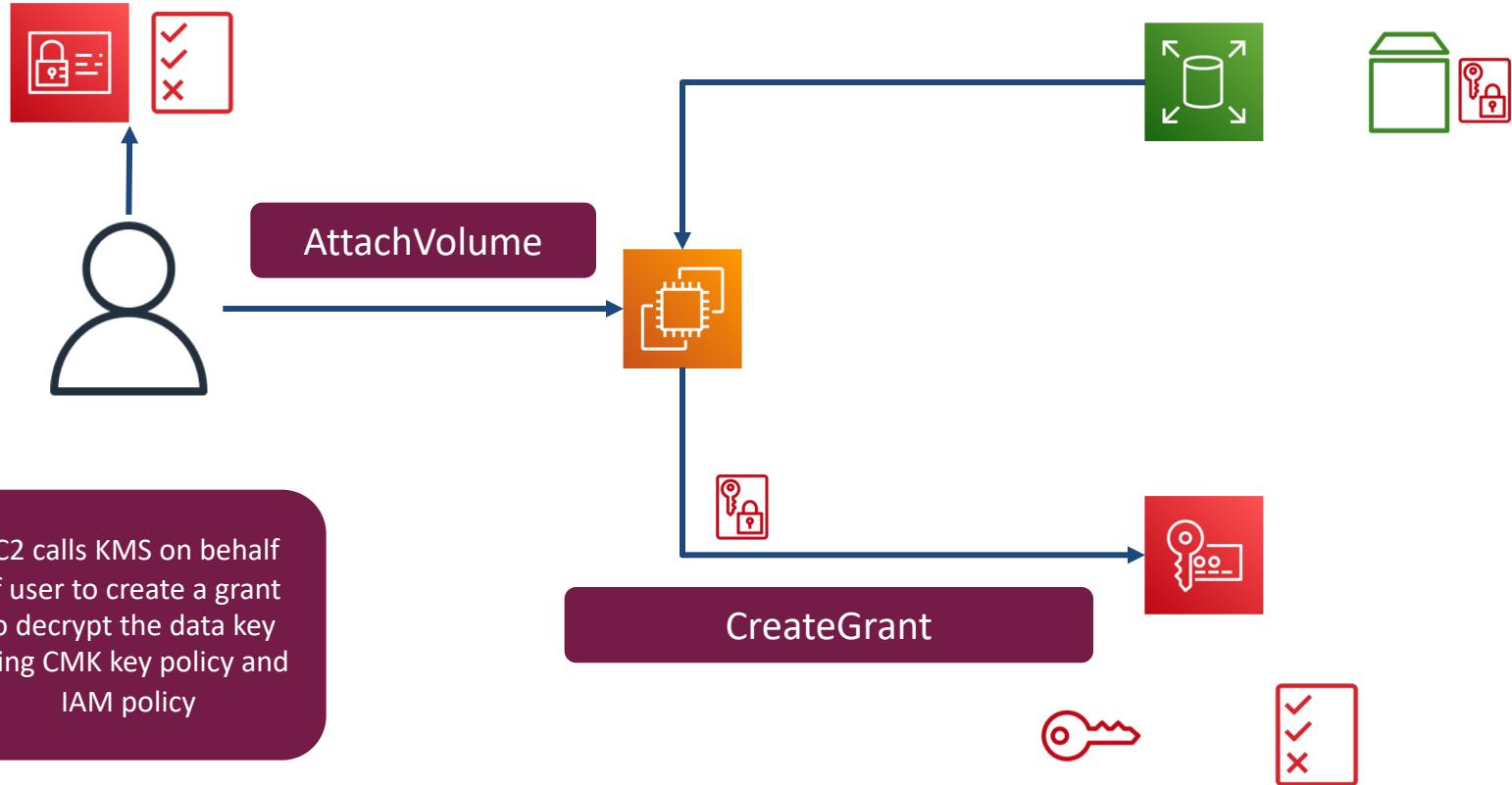
User attaches EBS
Volume with IAM
permissions

Encrypted Volume Attachment

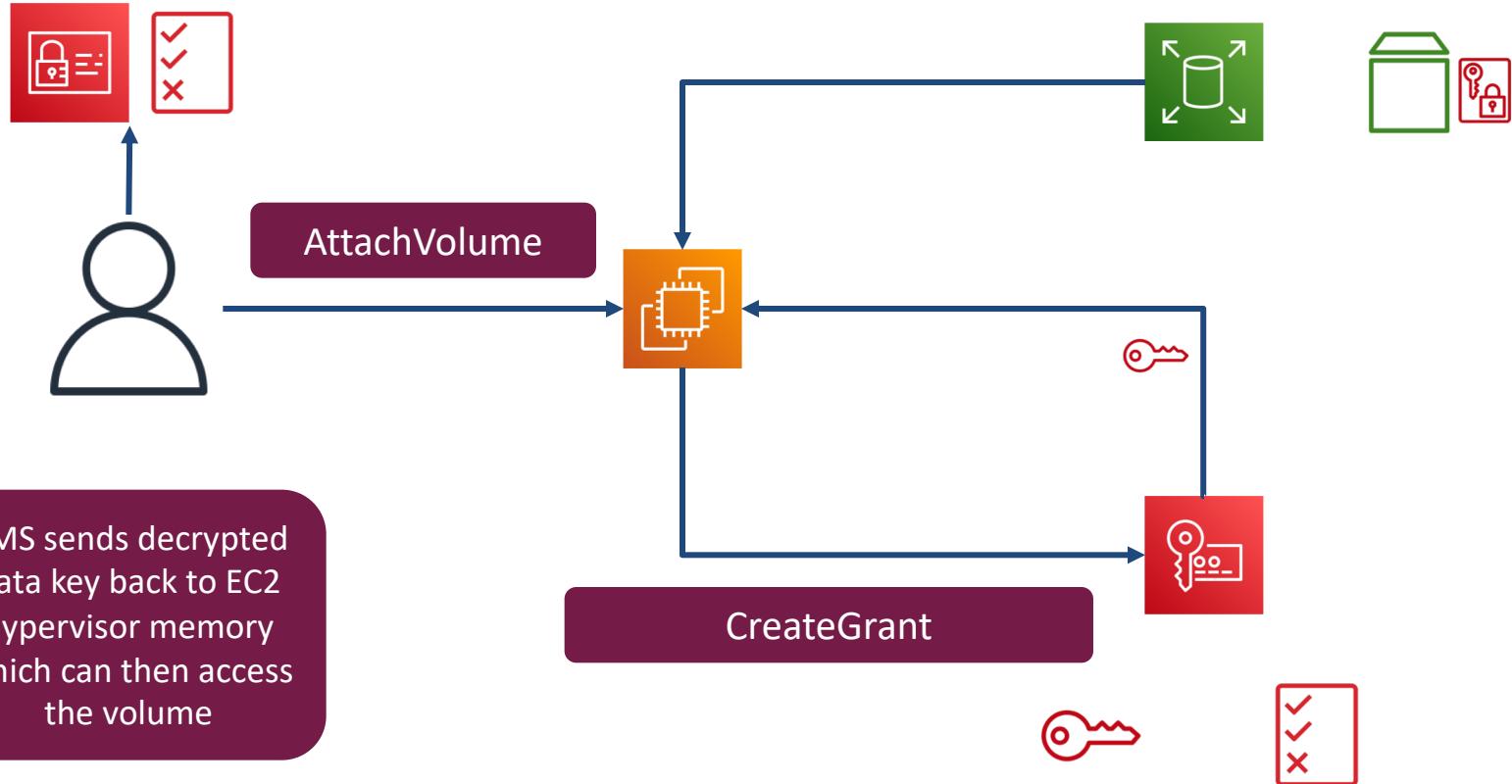


EC2 extracts
encrypted data key
from EBS

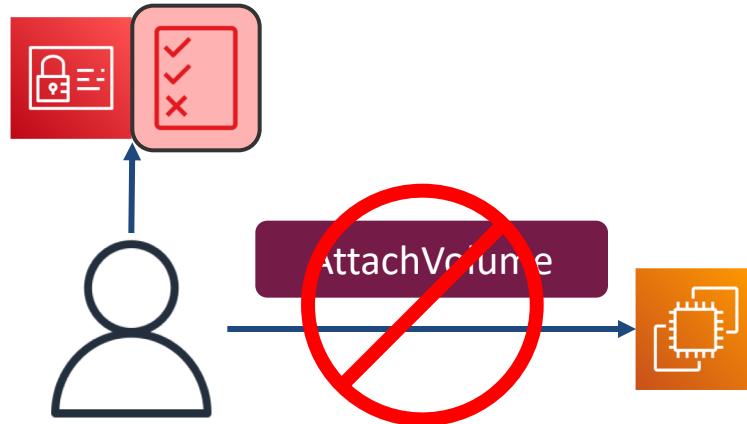
Encrypted Volume Attachment



Encrypted Volume Attachment

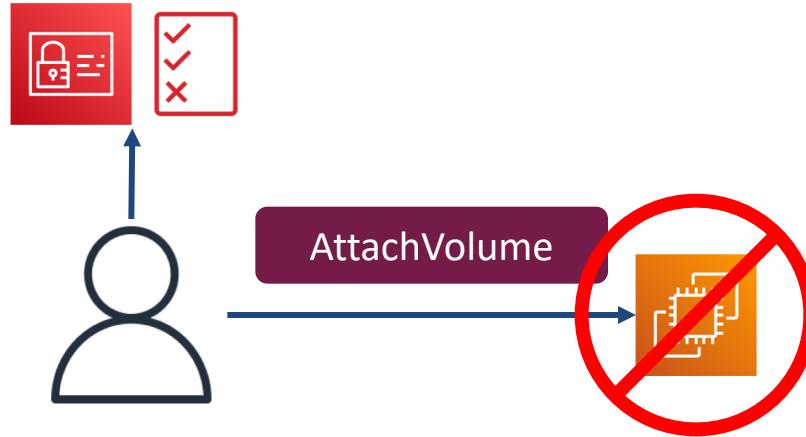


Where Can Errors Occur?



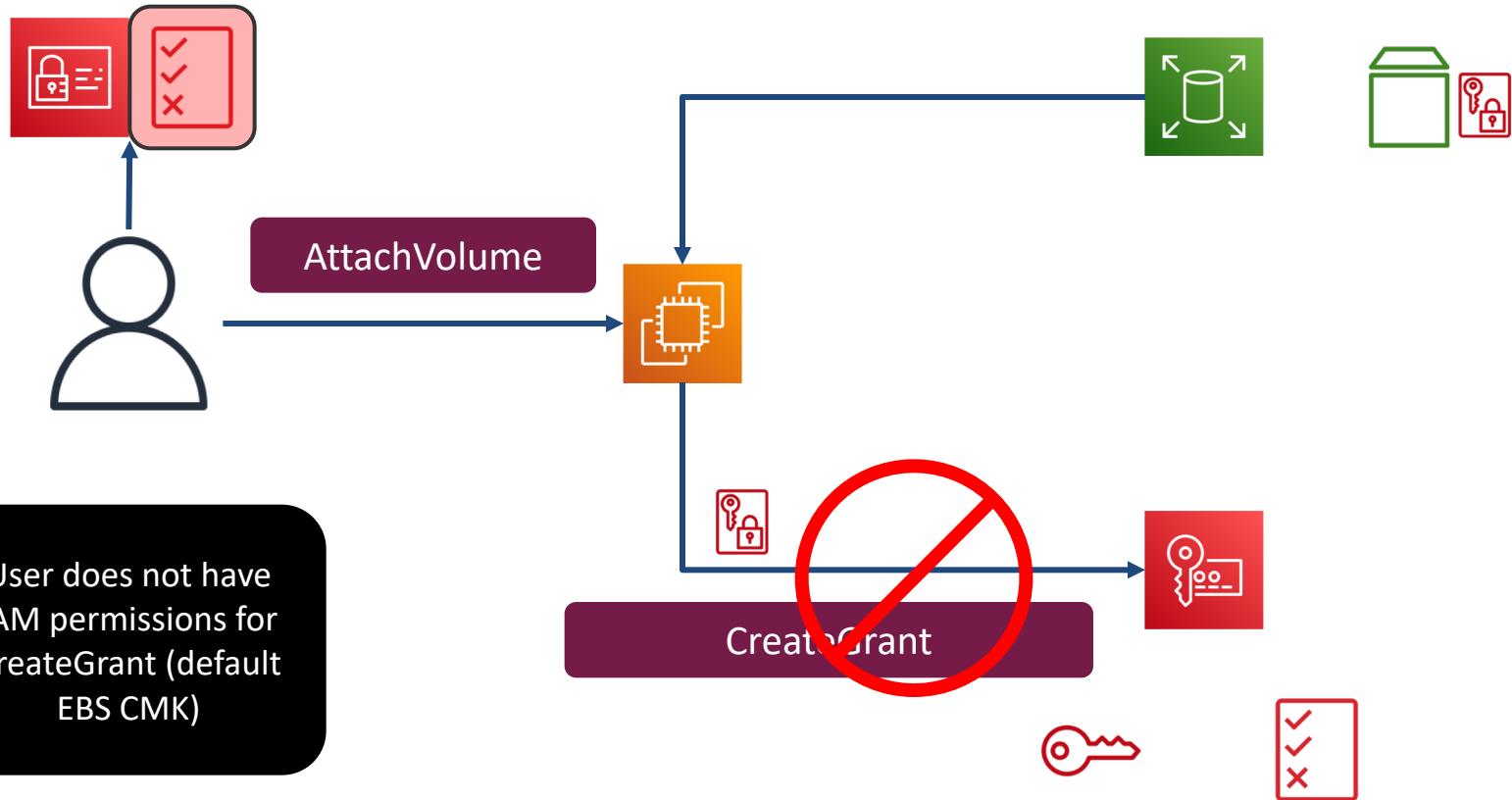
User does not
have IAM
permissions

Where Can Errors Occur?

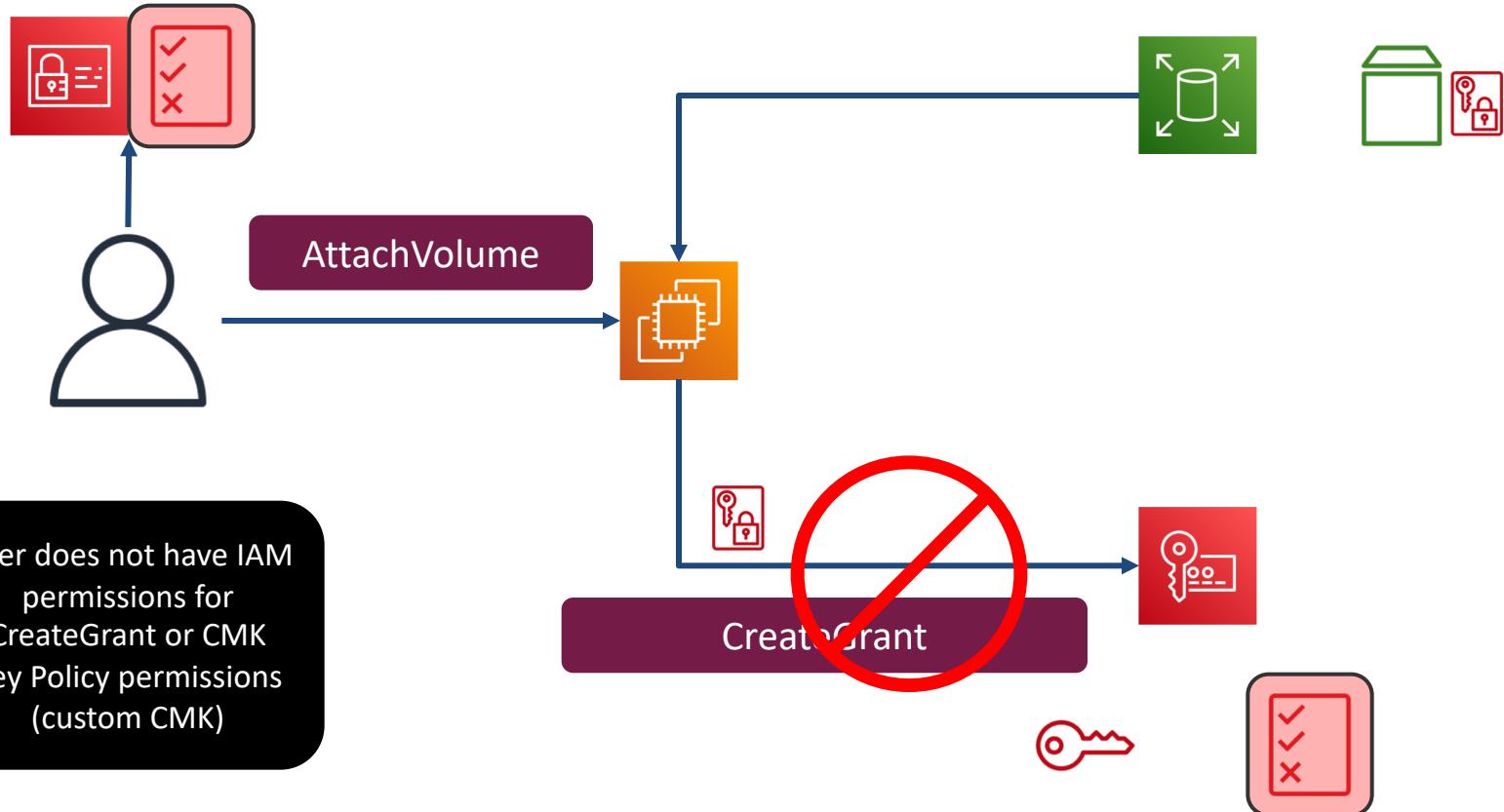


EC2 instance type
does not support
encrypted EBS
volume

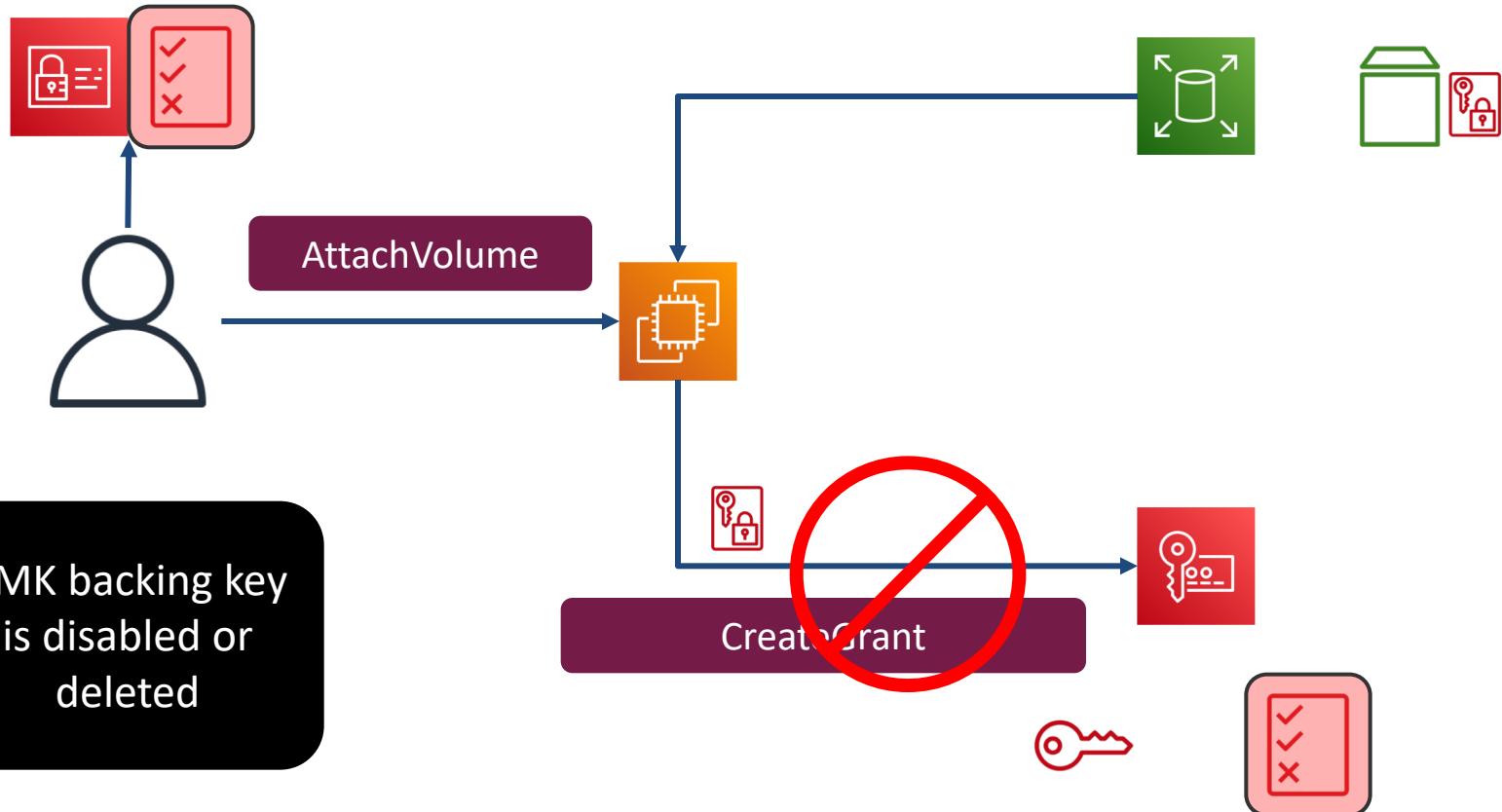
Where Can Errors Occur?



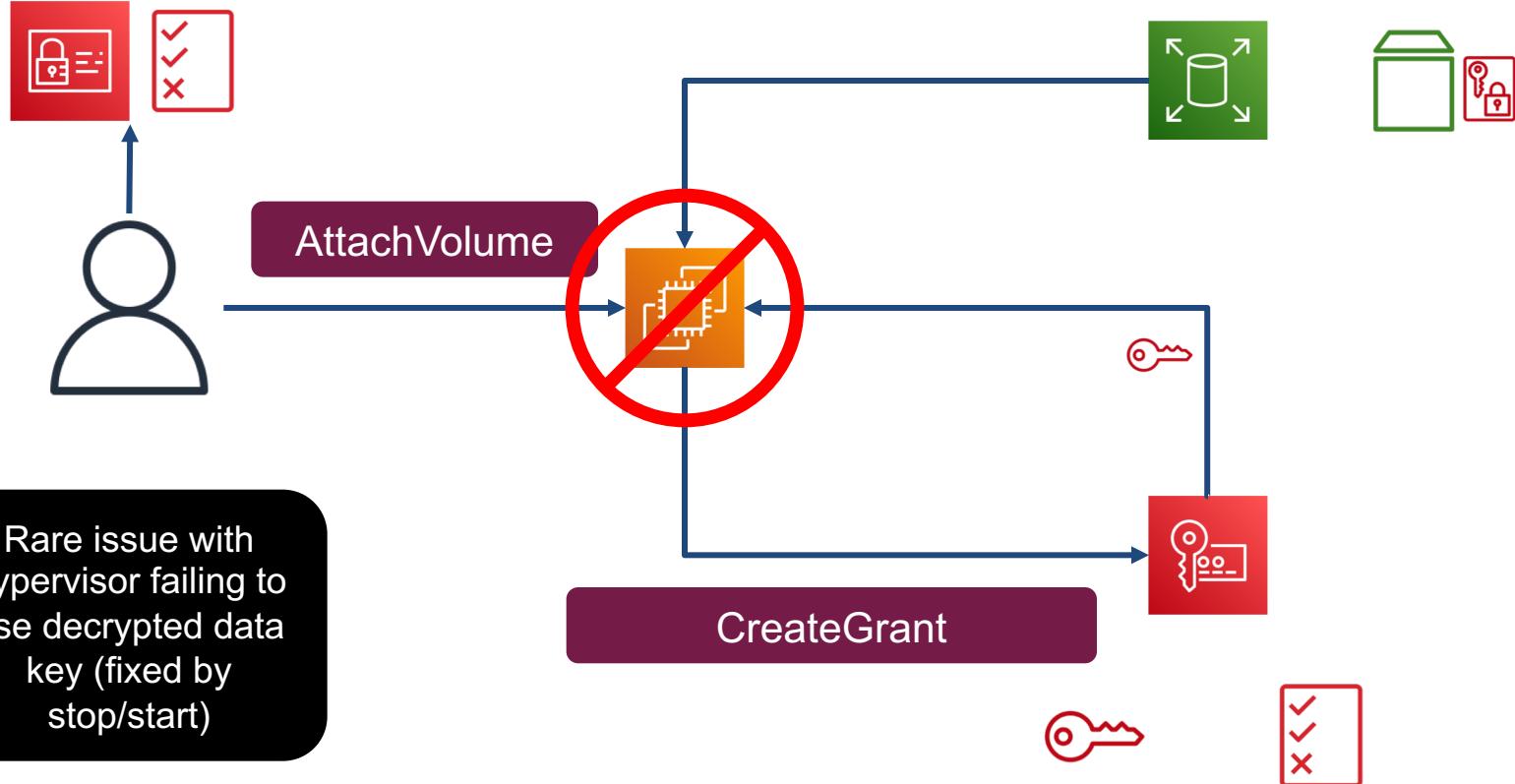
Where Can Errors Occur?



Where Can Errors Occur?



Where Can Errors Occur?



Question Breakdown

Question Scenario

A company's website static assets have been served from an S3 bucket configured as a static website. The marketing team has recently learned that all static assets have been served using HTTP requests.

To improve the company website search engine rankings, the marketing team would like to serve all static assets via HTTPS.

The web operations team attempts to meet the requirement by testing HTTPS access to the static assets, but the requests hang. What could be the root cause?

Answer Choices

- A. The TLS certificate configured on the S3 bucket does not match the website address.
- B. The S3 bucket is not configured for HTTPS access as a static website.
- C. S3 static websites do not support HTTPS traffic.
- D. The S3 bucket static website can only be accessed by HTTPS using the s3-website.amazonaws.com TLS certificate.

Answer A

This sounds like a possible root cause, and certainly would cause problems with a browser, S3 buckets do not support custom TLS certificates.

The TLS certificate configured on the S3 bucket does not match the website address.

Answer B

Another reasonable-sounding root cause, however S3 buckets do not support any HTTPS-related configuration at all except for the default S3 TLS certificate used to reach objects in an S3 bucket that is not configured as a static website.

The S3 bucket is not configured for HTTPS access as a static website.

Answer C

This is a true statement. Enabling the static website functionality on an S3 bucket disables the ability to access objects using HTTPS.

S3 static websites do not support HTTPS traffic.

Answer D

Enabling the static website functionality on an S3 bucket does indeed change the bucket endpoint to include "-website", but also disables any HTTPS access to the objects.

The S3 bucket static website can only be accessed by HTTPS using the s3-website.amazonaws.com TLS certificate.

Correct Answer

- A. The TLS certificate configured on the S3 bucket does not match the website address.
- B. The S3 bucket is not configured for HTTPS access as a static website.
- C. S3 static websites do not support HTTPS traffic.
- D. The S3 bucket static website can only be accessed by HTTPS using the s3-website.amazonaws.com TLS certificate.



Reliability Improvement Scenario

Scenario Description

A mobile application back end consists of an ALB with EC2 instances in an Auto Scaling group. The client uploads important data which occasionally gets lost if EC2 is scaling in or if the application is experiencing issues. The data uploads are less than 100k

Users are complaining about the lost data becoming a more frequent problem.

You've been asked to improve the reliability of the data upload process.

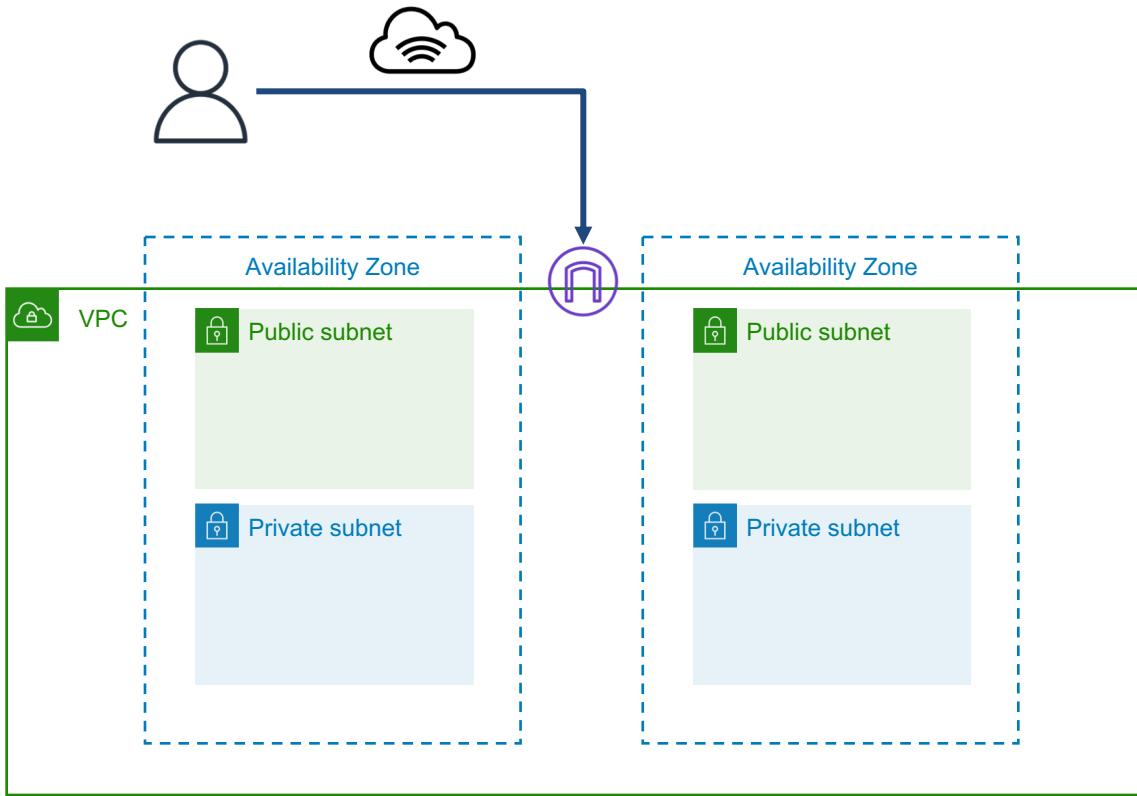
What solution would meet the reliability requirements?

Scenario Questions to Ask



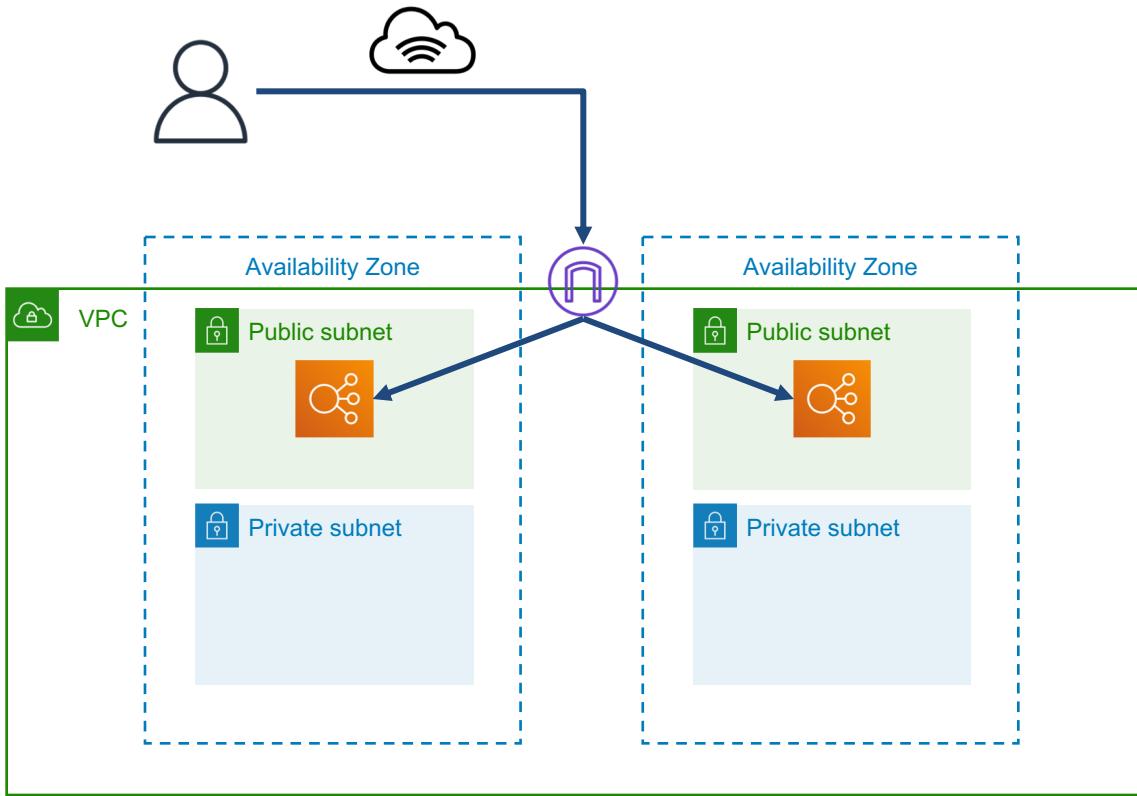
- Where can lost uploads occur in the current infrastructure?
- What modifications can be made to improve upload reliability?

Application Architecture



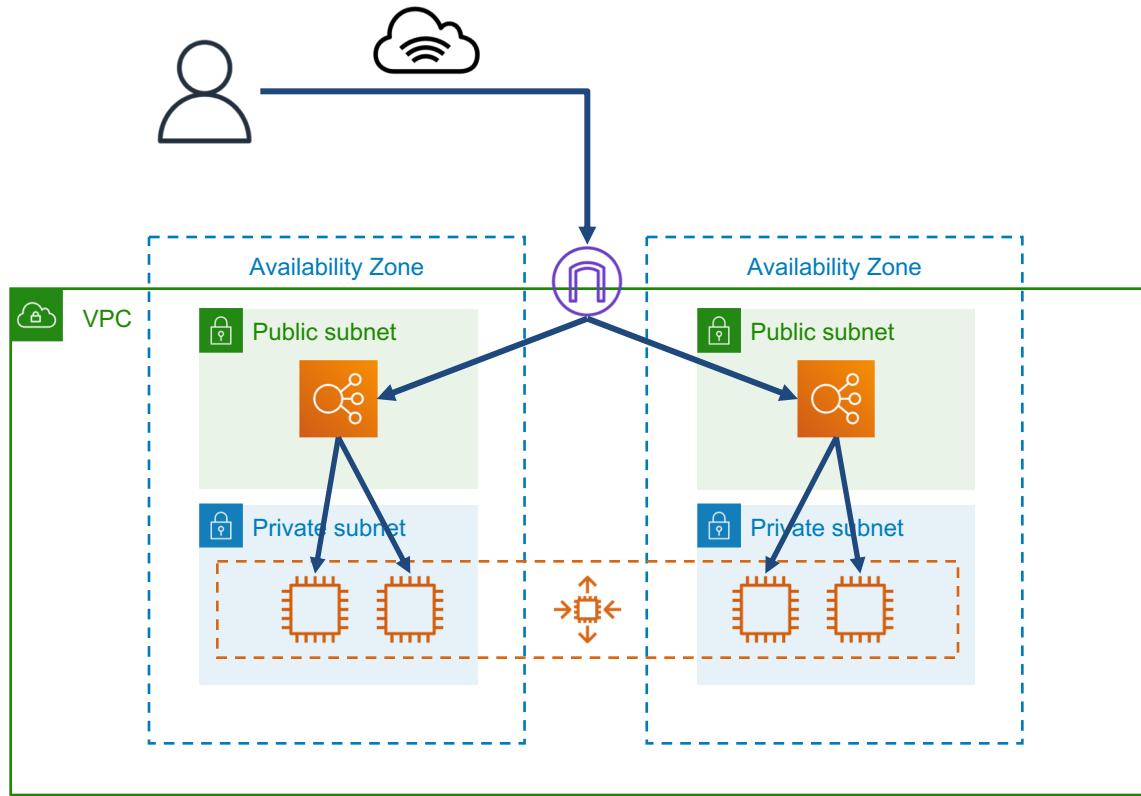
Mobile application
is dependent on
network resilience
to deliver traffic to
AWS

Application Architecture



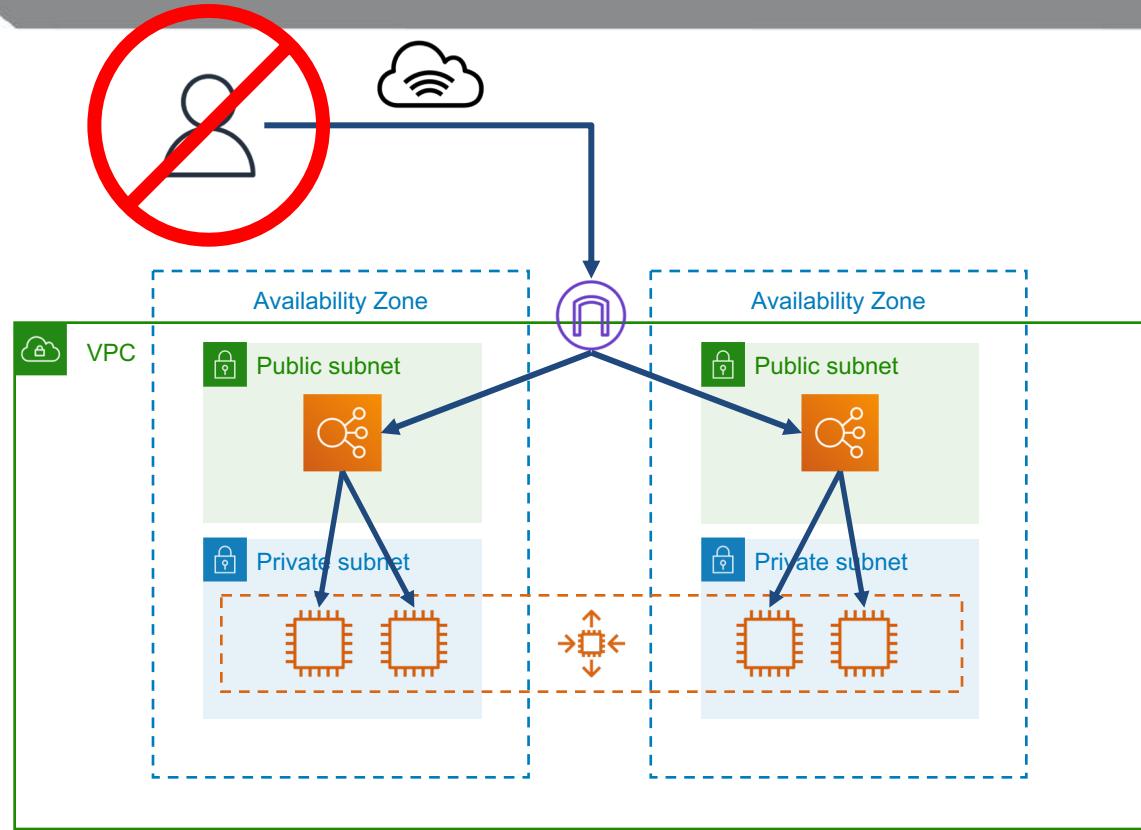
Mobile application
delivers upload to
ALB resources

Application Architecture



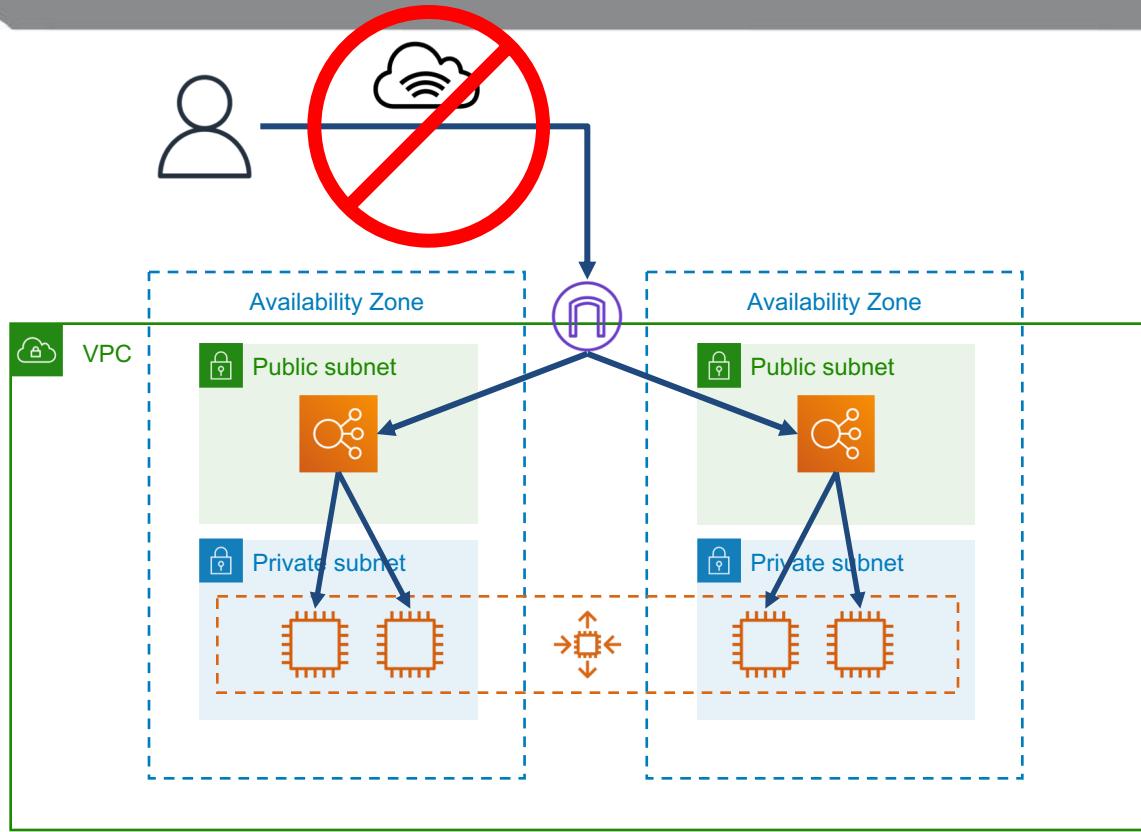
ALB proxies traffic and delivers to EC2 in the Auto Scaling group

Where Can Problems Occur?



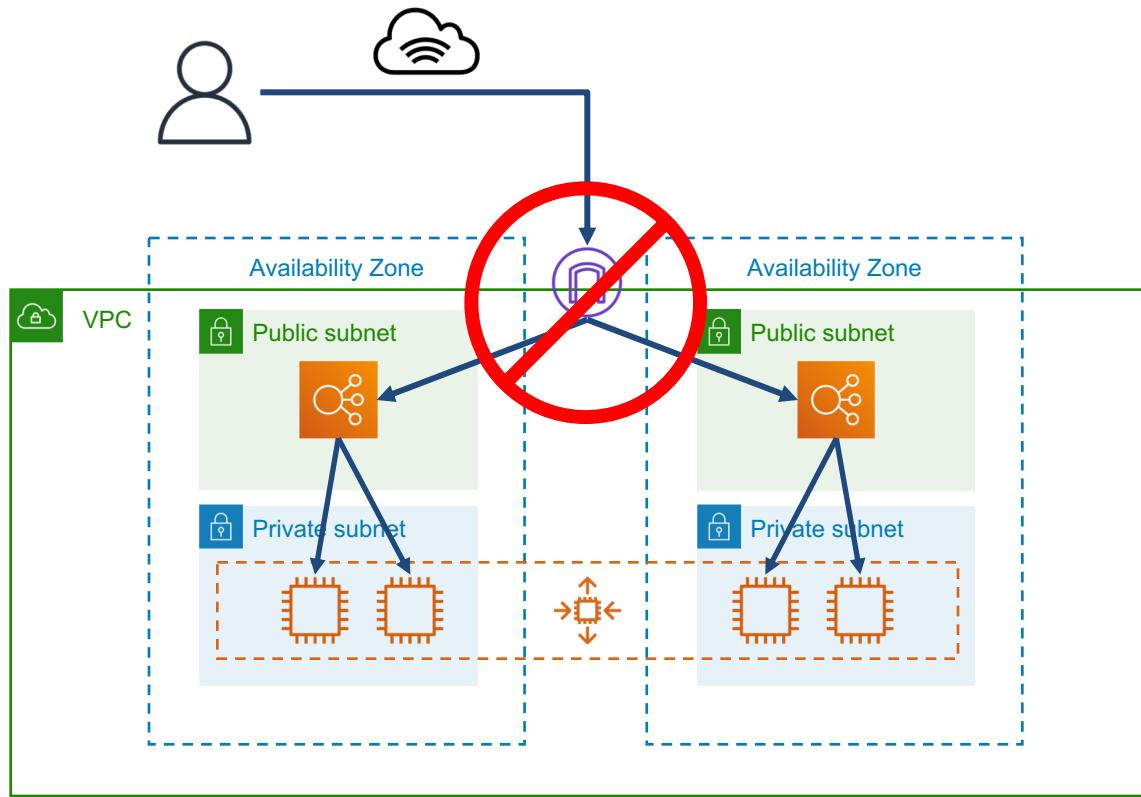
Local error on
the mobile
application

Where Can Problems Occur?



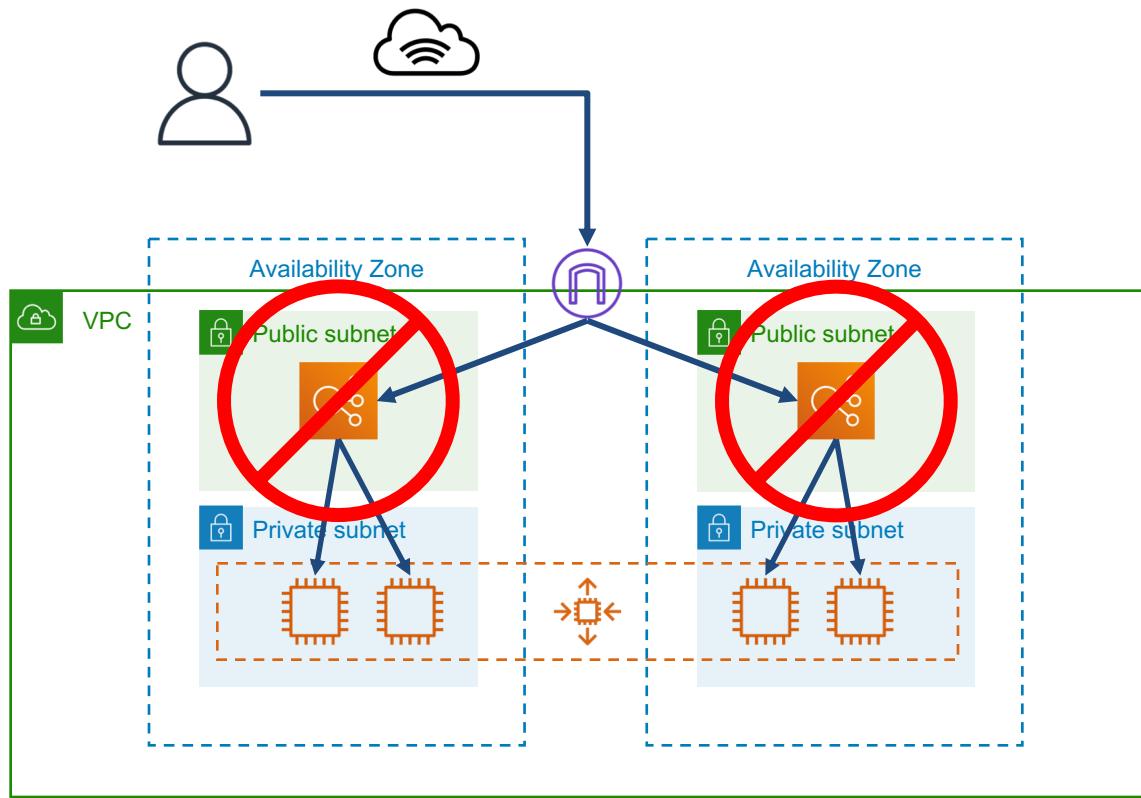
Transient
network error
during
transmission

Where Can Problems Occur?



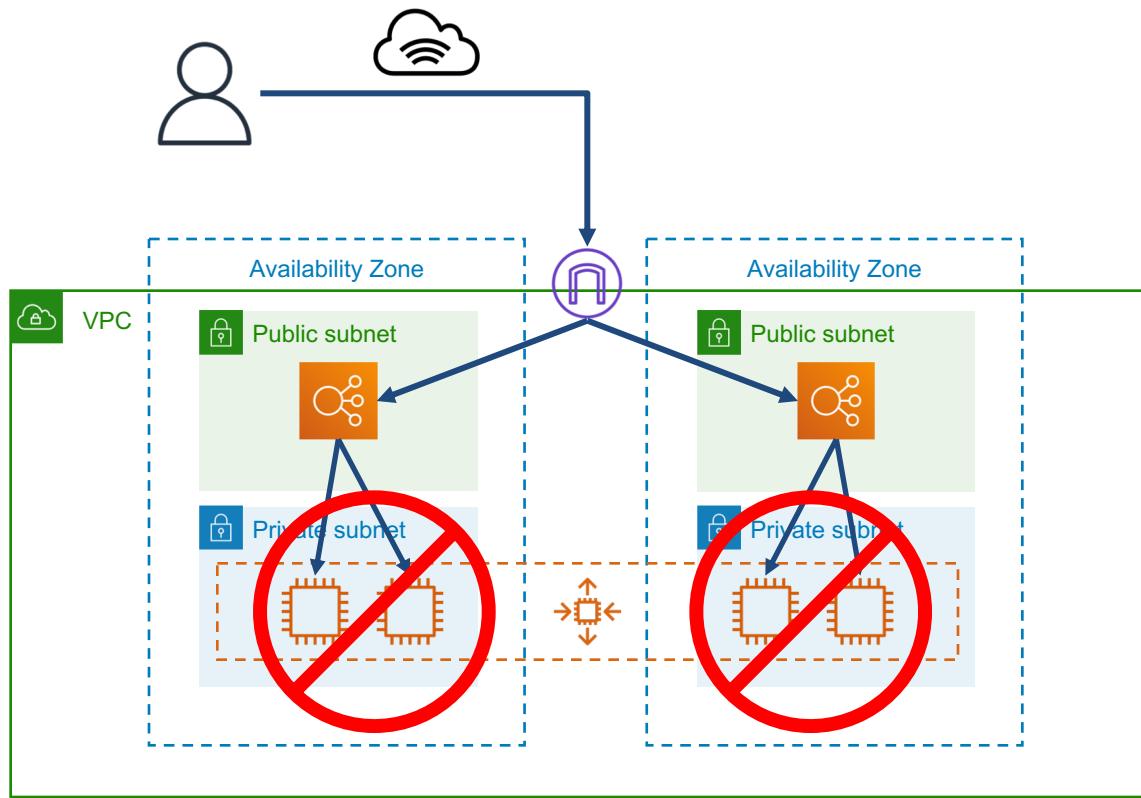
AWS network
error delivering
to ALB

Where Can Problems Occur?



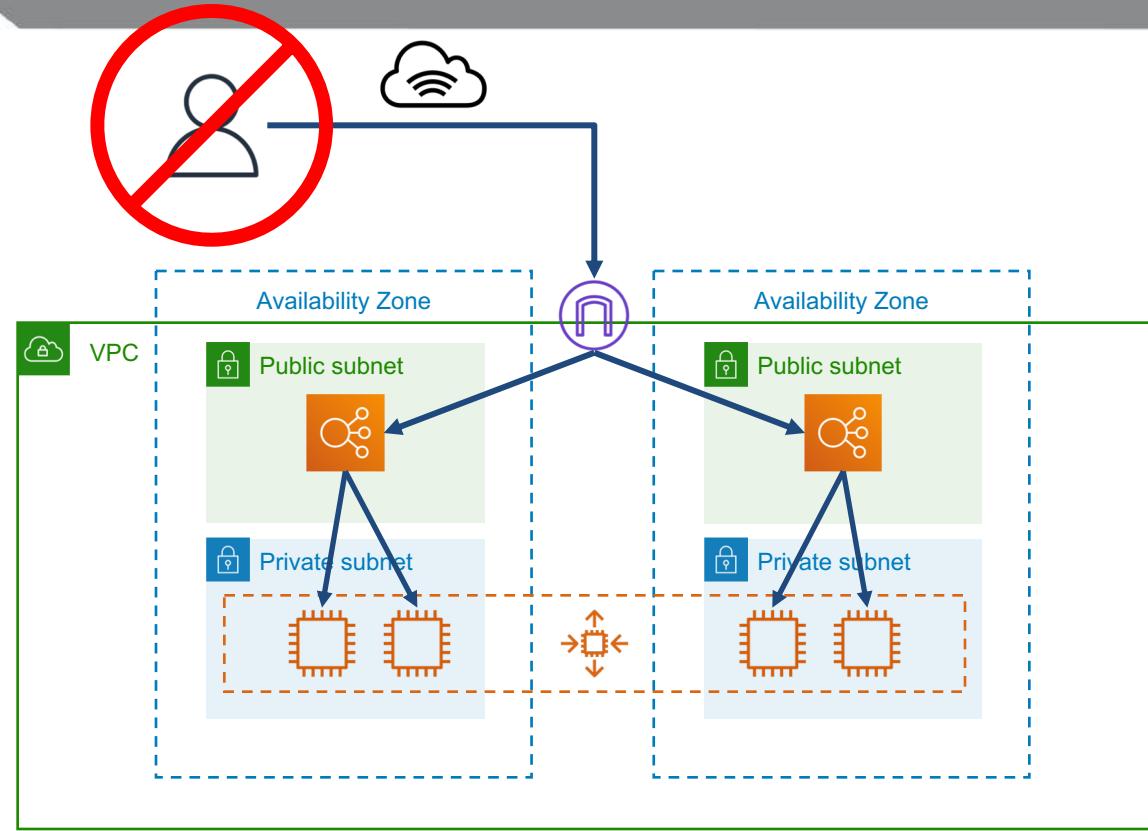
ALB failure on
individual
resource

Where Can Problems Occur?



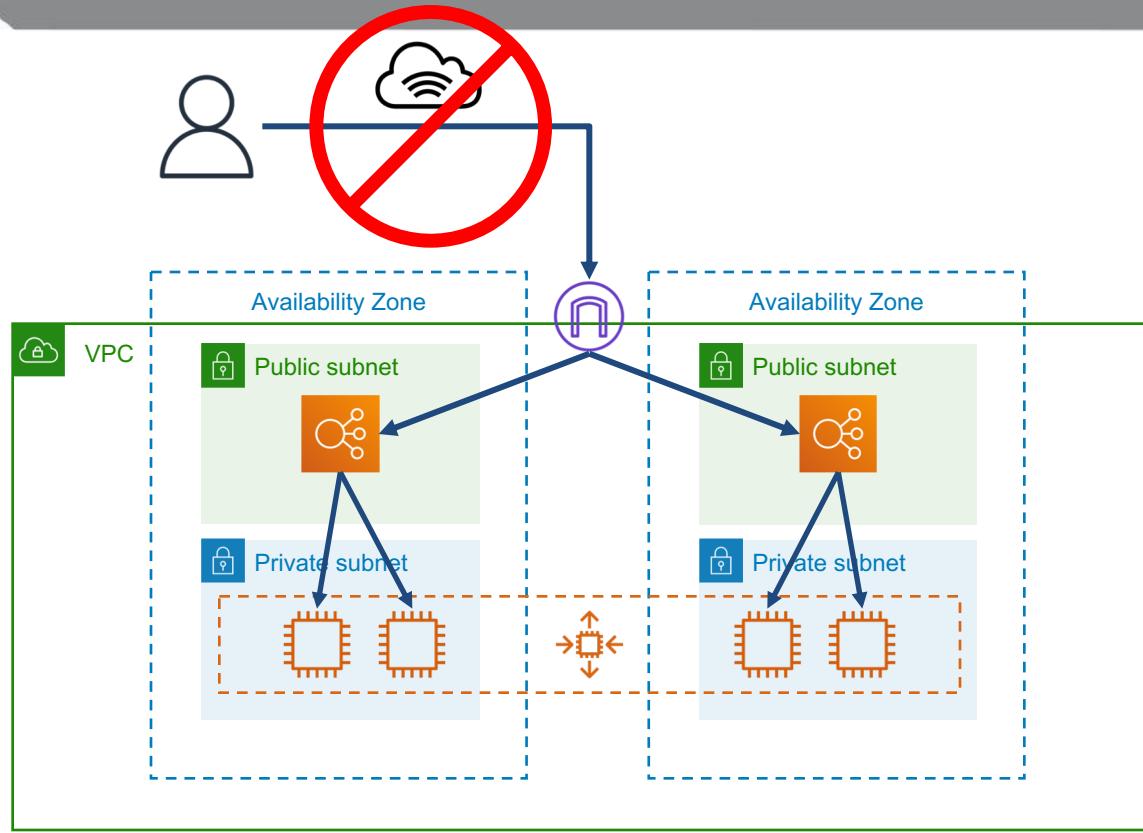
EC2 individual failure

How Can We Address Problems?



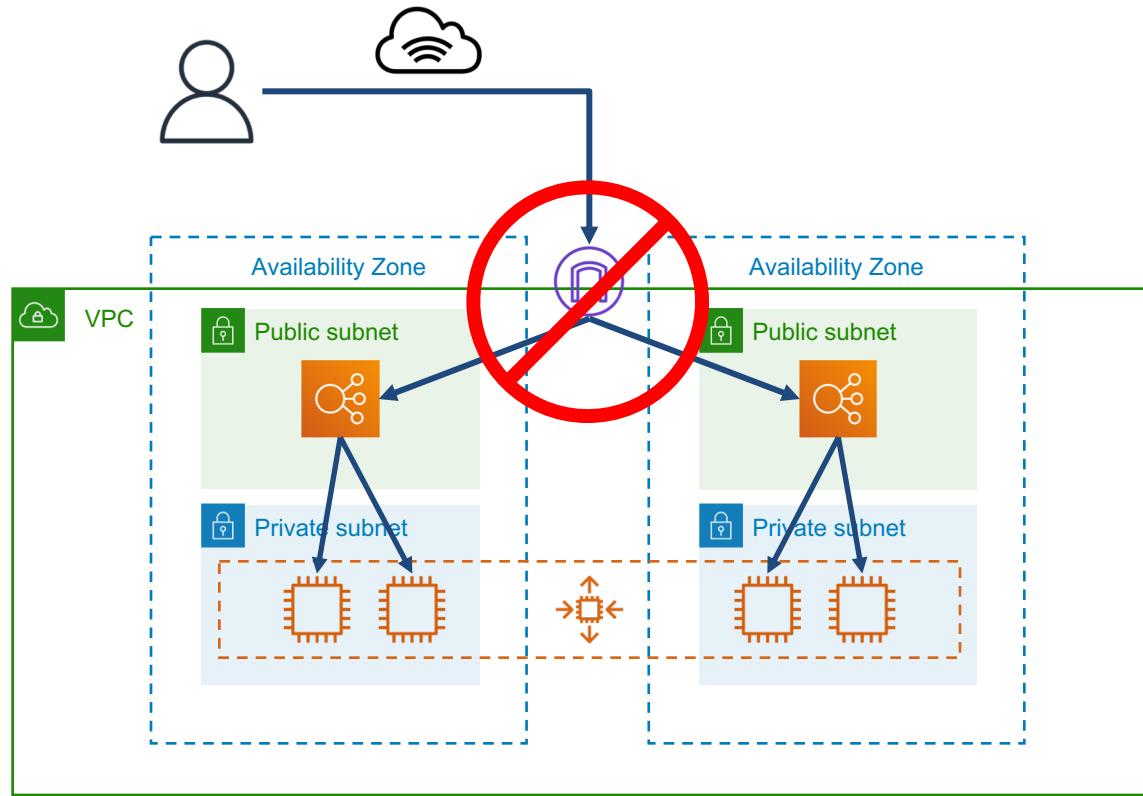
Nothing we can do here from an AWS perspective

How Can We Address Problems?



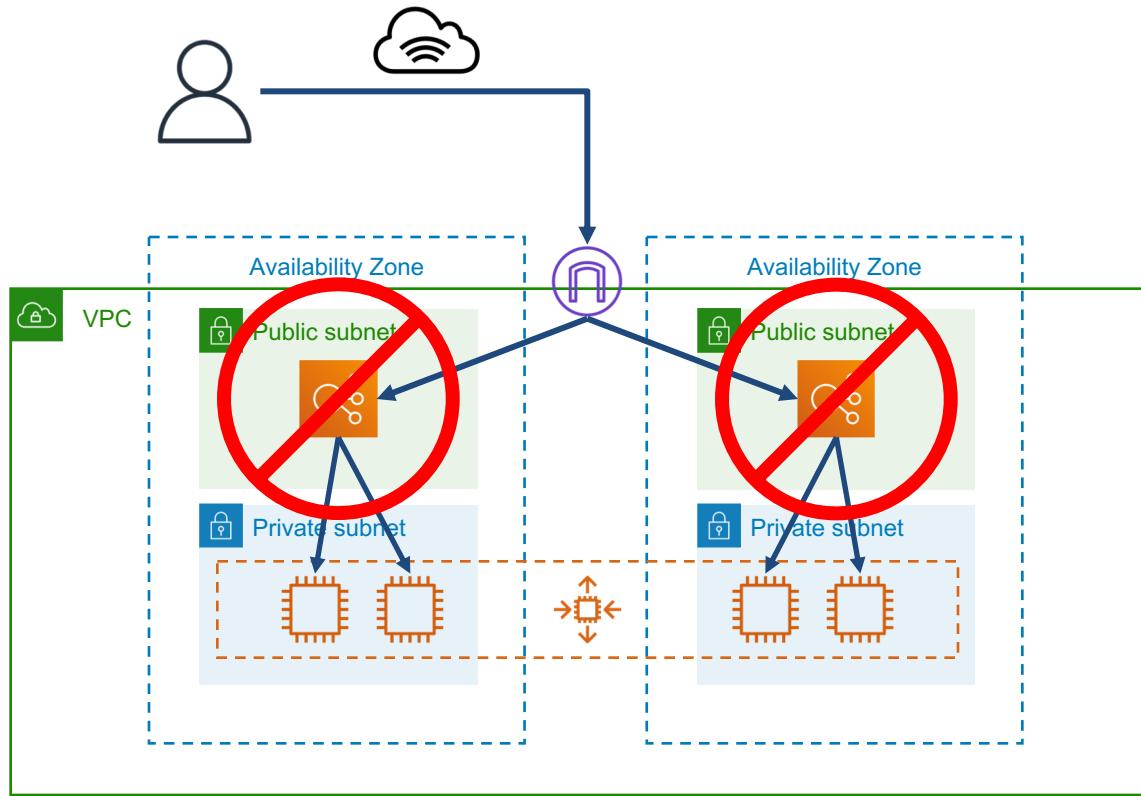
Nothing we can do here from an AWS perspective

How Can We Address Problems?



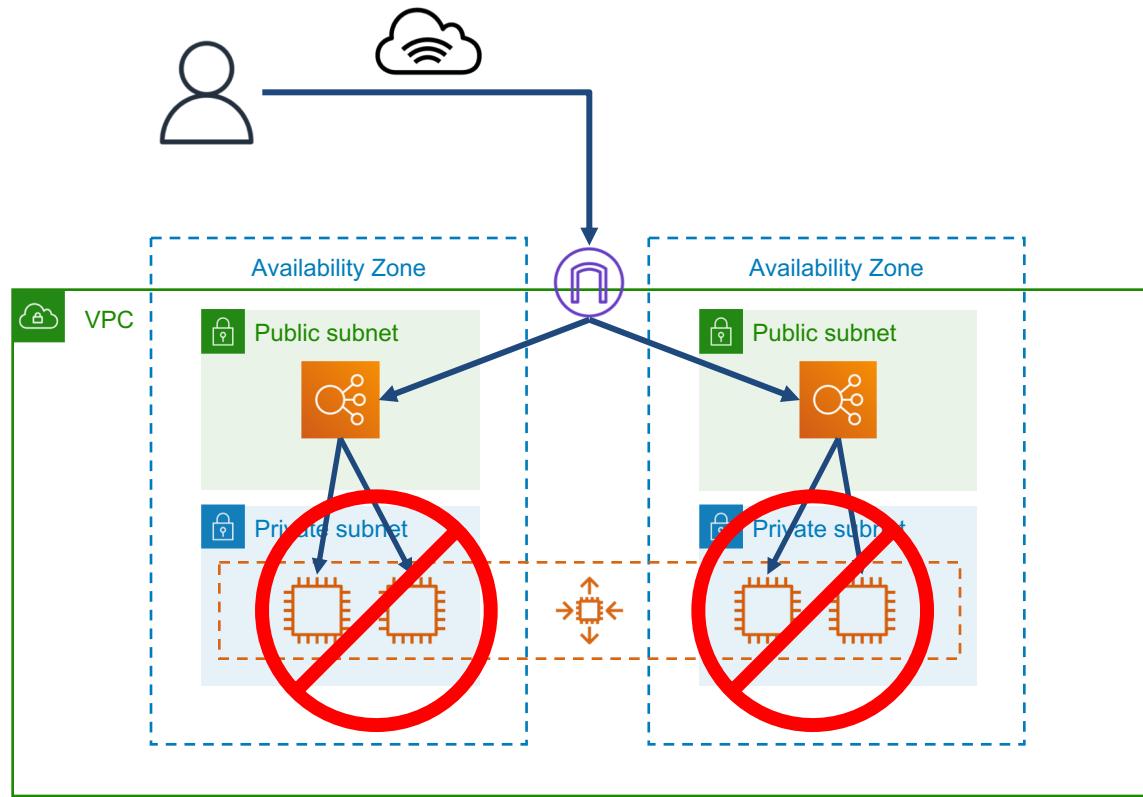
We could try multiple VPCs for redundancy?

How Can We Address Problems?



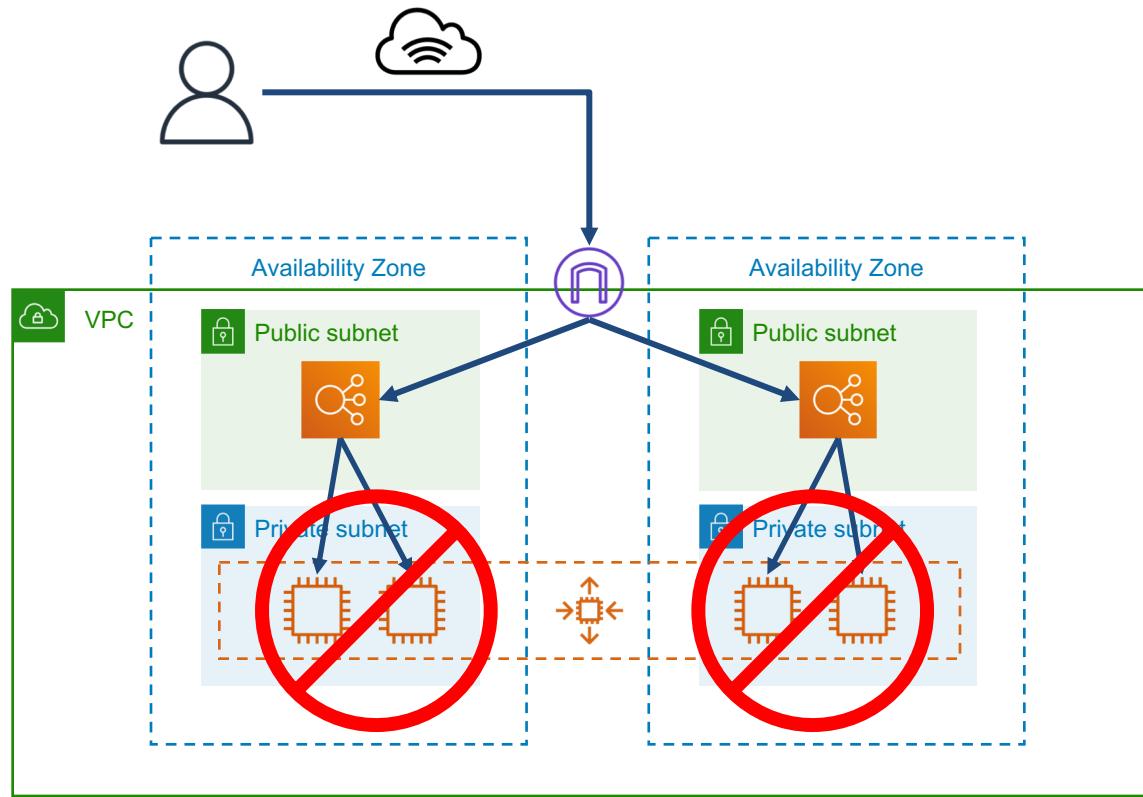
Deploy multiple ALB or client re-
try

How Can We Address Problems?



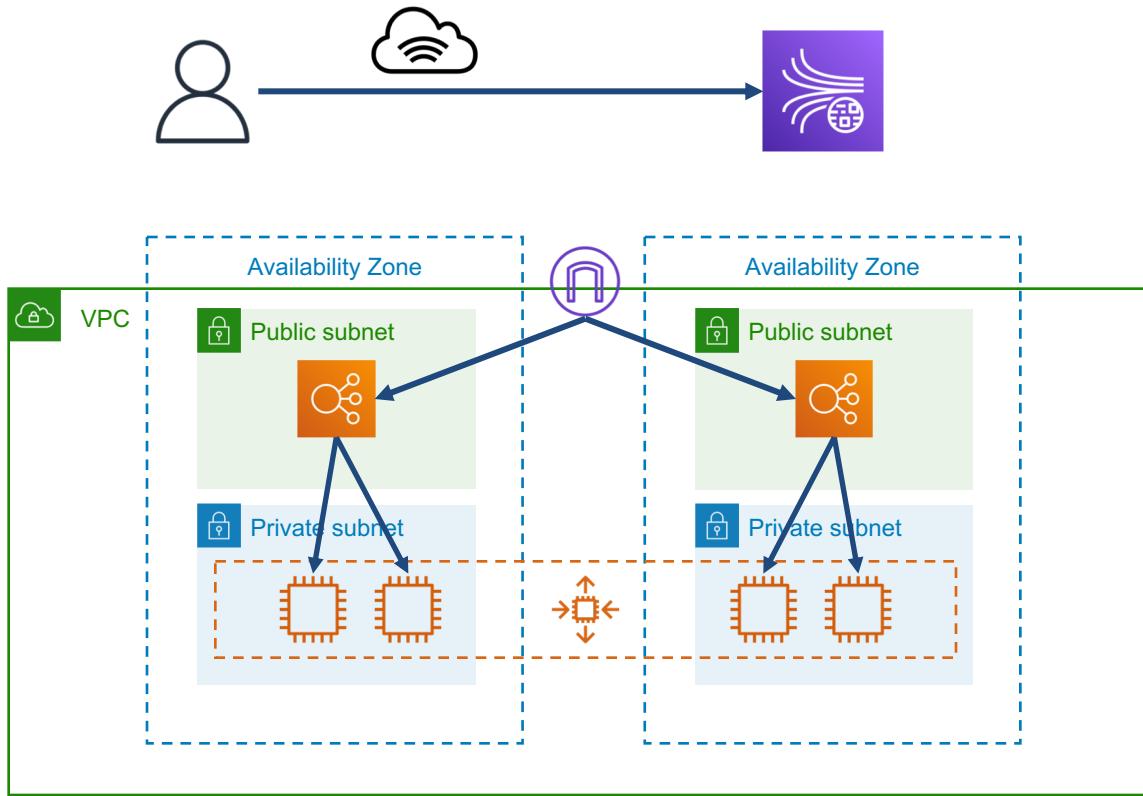
Better health checks to ensure traffic arrives

How Can We Address Problems?



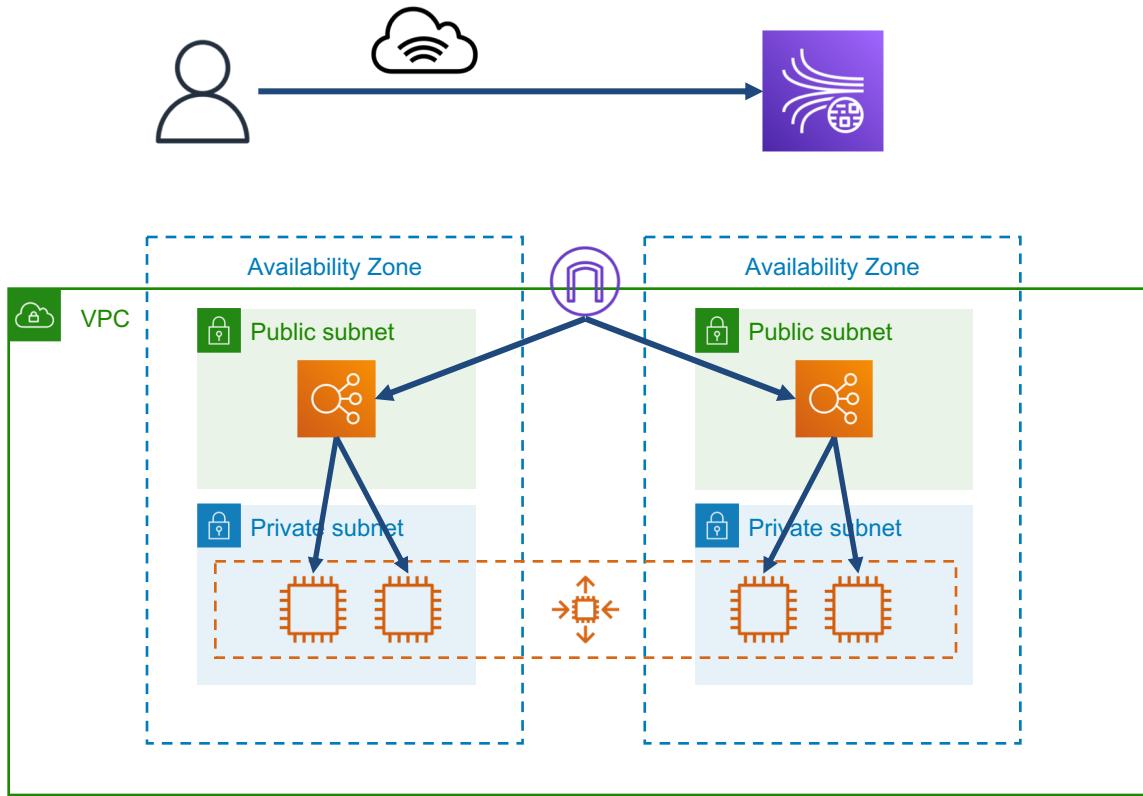
Implement Auto Scaling lifecycle hooks

Alternative Solution

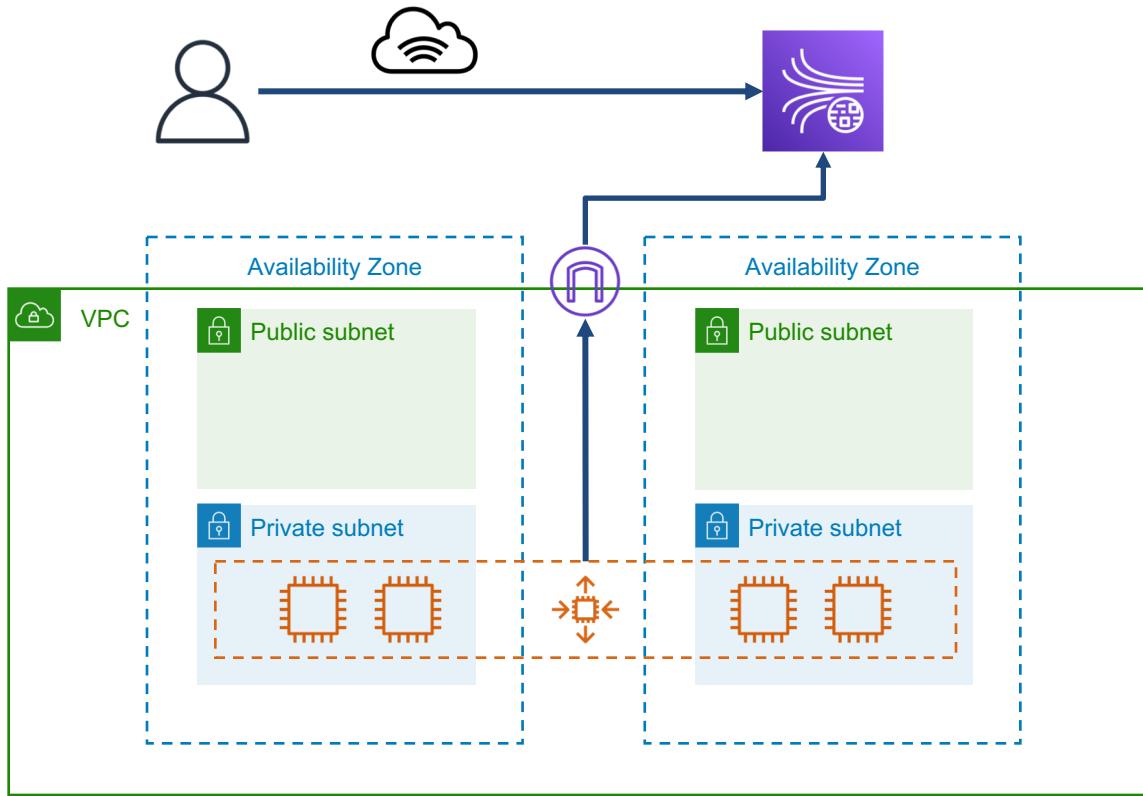


Deploy Kinesis
Data Stream as
upload endpoint

Alternative Solution



Alternative Solution



Reconfigure
backend to use
KCL

Question Breakdown

Question Scenario

Your company's production site is deployed using EC2 instances in an Auto Scaling group in a single AZ. Recently, an outage in that AZ caused all instances to be unreachable, and the production site was down for several hours.

Application Operations have determined the site requires a minimum of 30 total instances for a good user experience.

The site must handle a single AZ outage without degradation of the user experience.

Which of these recommendations meet the requirements?
(pick two)

Answer Choices

- A. Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 40 instances.
- B. Deploy an Auto Scaling group into 4 Availability Zones with a minimum of 40 instances.
- C. Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 50 instances.
- D. Deploy an Auto Scaling group into 3 Availability Zones with a minimum of 50 instances.
- E. Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 55 instances.

Answer A

This is better than the original architecture, but in the case of an AZ failure, only allows for 20 instances, less than the 30 instance minimum.

Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 40 instances.

Answer B

This solution appears similar to A, but in the event of a single AZ outage, it will still maintain 30 total minimum instances, which meets the minimum requirements.

Deploy an Auto Scaling group into 4 Availability Zones with a minimum of 40 instances.

Answer C

This solution is very similar to A, with the addition of 10 instances. In the event of an AZ failure, there will be only 25 instances, however, which does not meet the minimum requirements.

Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 50 instances.

Answer D

This solution extends to 3 AZs, and if there is a single AZ outage, will maintain a minimum ~32 instances, meeting the minimum requirements.

Deploy an Auto Scaling group into 3 Availability Zones with a minimum of 50 instances.

Answer E

This solution has the largest number of minimum instances, but since they are split into 2 AZ, it still does not meet the minimum 30 instance requirement for a single AZ outage.

Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 55 instances.

Correct Answer

- A. Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 40 instances.
- B. Deploy an Auto Scaling group into 4 Availability Zones with a minimum of 40 instances.
- C. Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 50 instances.
- D. Deploy an Auto Scaling group into 3 Availability Zones with a minimum of 50 instances.
- E. Deploy an Auto Scaling group into 2 Availability Zones with a minimum of 55 instances.





Performance Improvement Scenario

Scenario Description

A popular desktop game releases updates on a quarterly basis, and makes them available via download from an S3 bucket. As the game grows in popularity, the number of downloads are also increasing. The concurrency of downloads are beyond the capacity of S3.

Updates initiated from the client are failing during periods of high traffic.

How can the company improve the infrastructure performance to handle the quarterly traffic spikes?

Scenario Questions to Ask



- How is S3 bucket performance calculated?
- How can S3 overall performance be improved?

S3 Prefix Performance

BucketName/Application/DLC/download1.exe

BucketName/Application/DLC/download2.exe

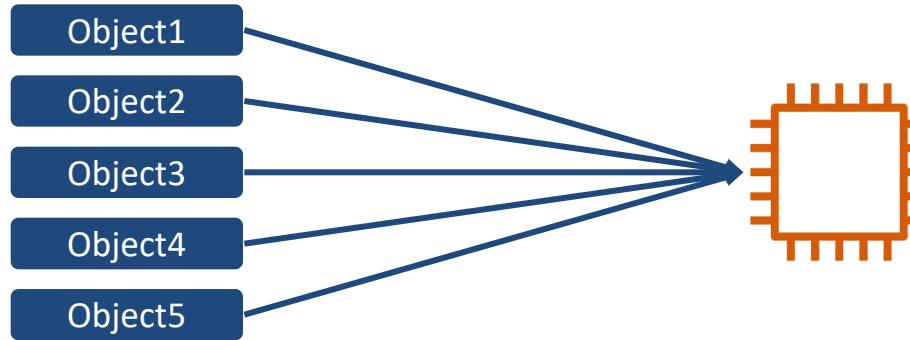
BucketName/Application/DLC/download3.exe

BucketName/Application/DLC/download4.exe

Prefix

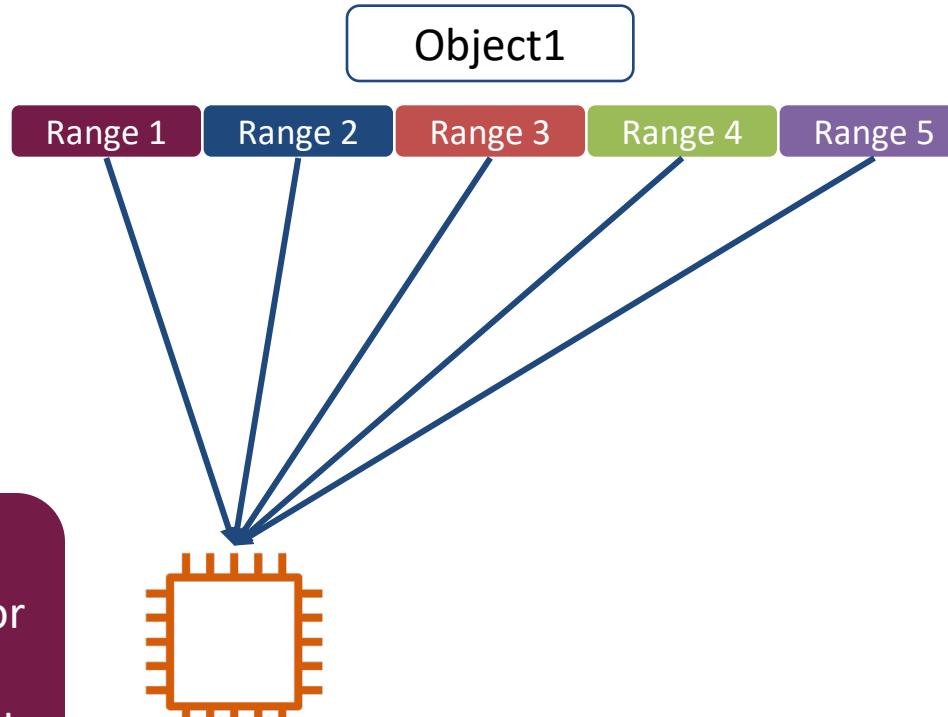
Each prefix can support
5500 read (HTTP GET)
requests per second

S3 Download Performance



```
aws configure set default.s3.max_concurrent_requests 20
```

S3 Download Performance



Byte ranges are usually 8-16MB, or same size as a multi-part upload

Improving Prefix Performance

<RANDOMHASH1>/download.exe

<RANDOMHASH2>/download.exe

<RANDOMHASH3>/download.exe

<RANDOMHASH4>/download.exe

Modify app to support
multiple downloads
within the same bucket

Prefix

Improving S3 Data Transfer

Download hosted here



Improving S3 Data Transfer

Download hosted here

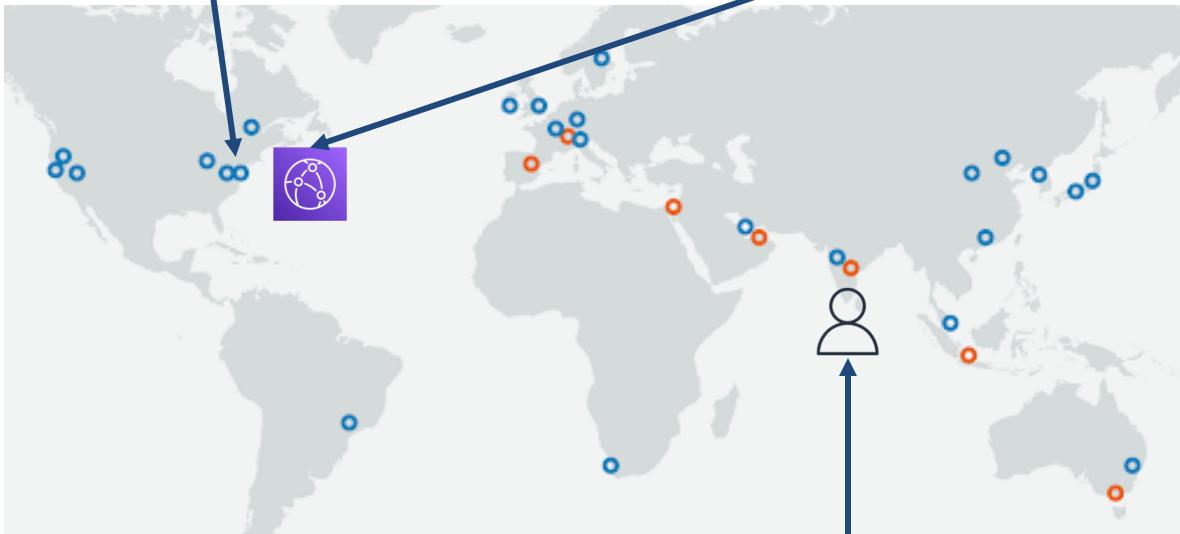


Customer is here

Improving S3 Data Transfer

Download hosted here

Implement CloudFront



Customer is here

Improving S3 Data Transfer

Doesn't help for
the first
download to
each Edge
Location!

Download hosted here

Implement CloudFront



Cache downloads closer

Customer is here

Improving S3 Data Transfer

Download hosted here



Customer is here

Improving S3 Data Transfer

Download hosted here

Implement S3 Multi-Region
Access Point



Replicate download here

Customer is here

Improving S3 Data Transfer

Download hosted here

Implement S3 Multi-Region
Access Point



Replicate download here

Customer is here

Improving S3 Data Transfer

Customer uses global access point and directed to closest download

Download hosted here

Implement S3 Multi-Region Access Point



Replicate download here

Customer is here

Question Breakdown

Question Scenario

A company's internal application consists of a Java application running on statically deployed instances that generate requests through an internal NLB to a second Java application.

Over time, it is apparent that some instances behind the NLB have higher load than others, and it is impacting response latency on those instances.

The application support team would like to identify the root cause of the issue and deploy a resilient fix.

Which of these describes the problem and solution?

Answer Choices

- A. The NLB is naturally sticky for network flows. The Java clients should reset connections regularly to mitigate this.
- B. The NLB is naturally sticky for network flows. The Java clients should be restarted regularly to mitigate this.
- C. The requests are unequal with the back end load generated. The mitigation is to deploy a second NLB just for those heavier requests.
- D. The instances with higher load are experiencing noisy neighbors on the same hardware. The mitigation is to stop/start or re-deploy those instances.

Answer A

The NLB uses HyperPlane, which balances network flows, and is indeed naturally sticky. One flow is delivered to the same back end during the duration of the session. A connection reset does indeed instruct the NLB to re-balance the new flow.

The NLB is naturally sticky for network flows. The Java clients should reset connections regularly to mitigate this.

Answer B

It has been established that the NLB is indeed sticky. A Java client restart could end up causing interruptions, and is not part of a resilient solution.

The NLB is naturally sticky for network flows. The Java clients should be restarted regularly to mitigate this.

Answer C

This is a possible root cause but not mentioned as part of the scenario, and so this answer is unlikely. The solution could be a correct mitigation if the root cause were correct as well.

The requests are unequal with the back end load generated. The mitigation is to deploy a second NLB just for those heavier requests.

Answer D

This is difficult to prove, and the least likely of all the answer choices. If it were indeed the cause, a stop/start guarantees migration to new hardware.

The instances with higher load are experiencing noisy neighbors on the same hardware. The mitigation is to stop/start or re-deploy those instances.

Correct Answer

- A. The NLB is naturally sticky for network flows. The Java clients should reset connections regularly to mitigate this.
- B. The NLB is naturally sticky for network flows. The Java clients should be restarted regularly to mitigate this.
- C. The requests are unequal with the back end load generated. The mitigation is to deploy a second NLB just for those heavier requests.
- D. The instances with higher load are experiencing noisy neighbors on the same hardware. The mitigation is to stop/start or re-deploy those instances.



Security Improvement Scenario

Scenario Description

An application runs on EC2 instances in a VPC and accesses a DynamoDB table that contains sensitive data. The EC2 instances use an IAM role granting access to the table.

The company would like to ensure that access to the table is only allowed through the EC2 application.

There is a further requirement to enforce this restriction with active guardrails if possible.

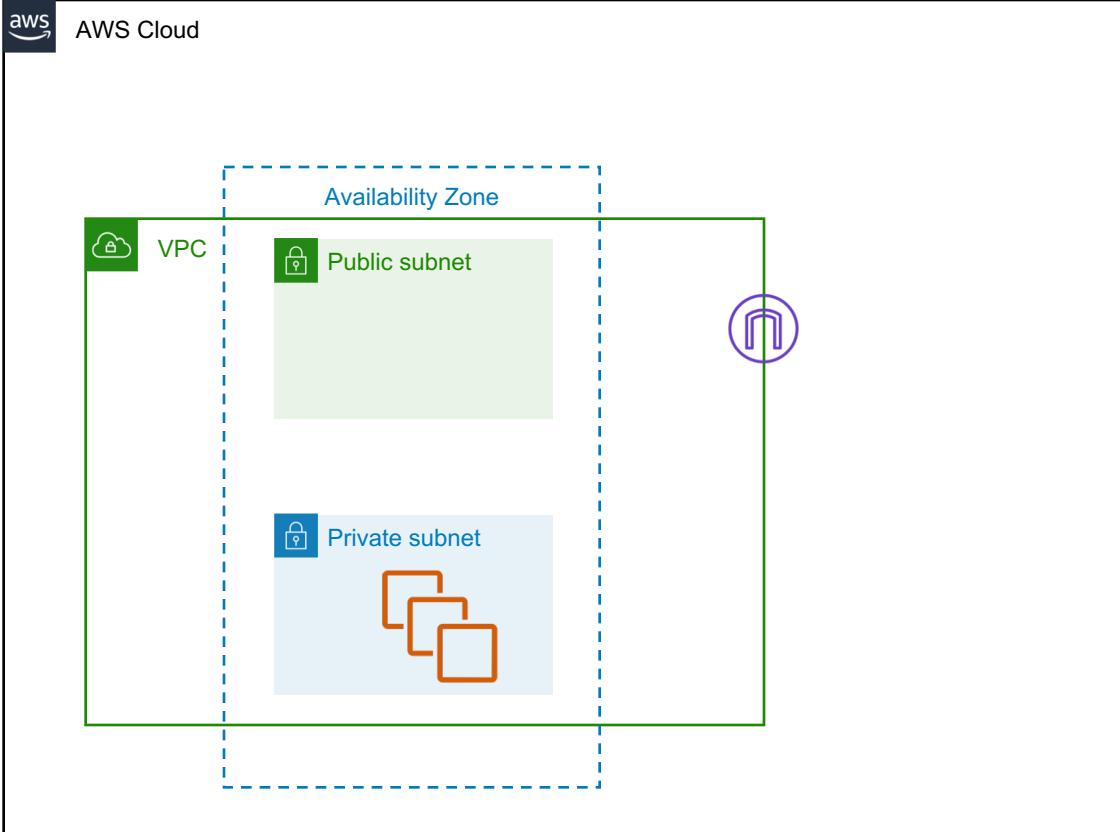
How can the company meet the requirement?

Scenario Questions to Ask



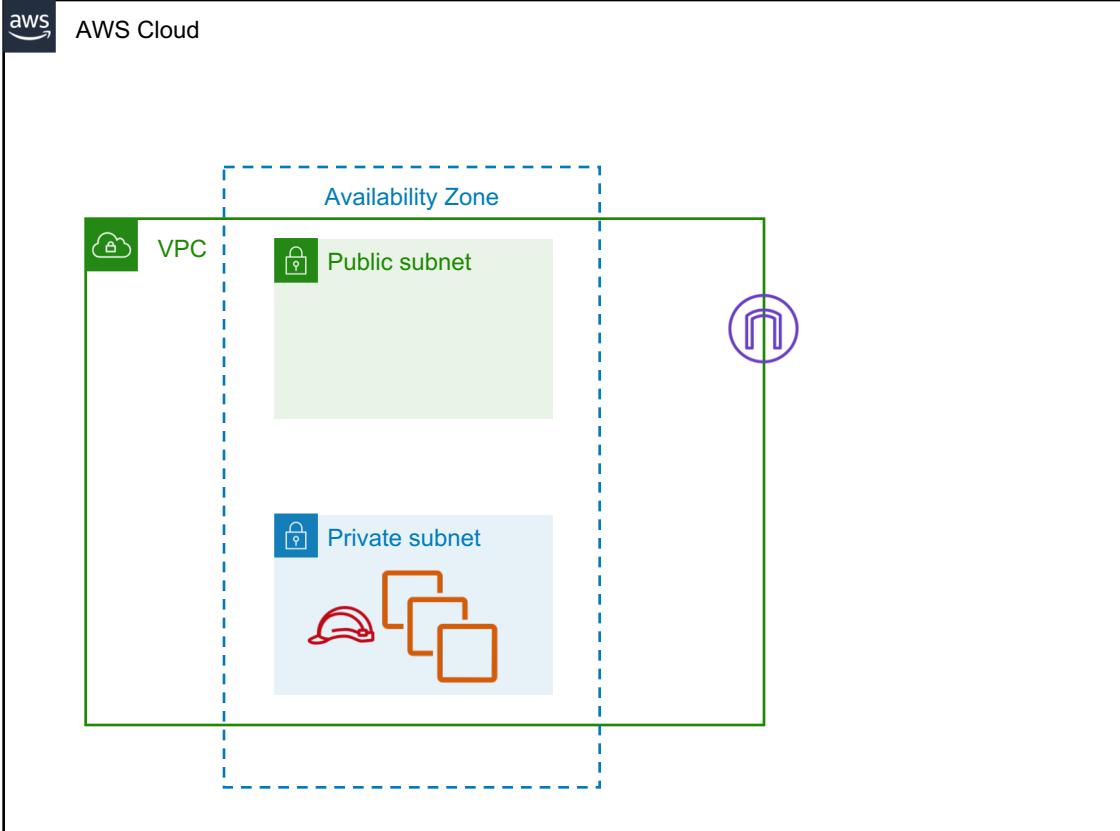
- What does the current infrastructure look like?
- How can the infrastructure be improved?
- How can the permissions be modified?

Current Infrastructure



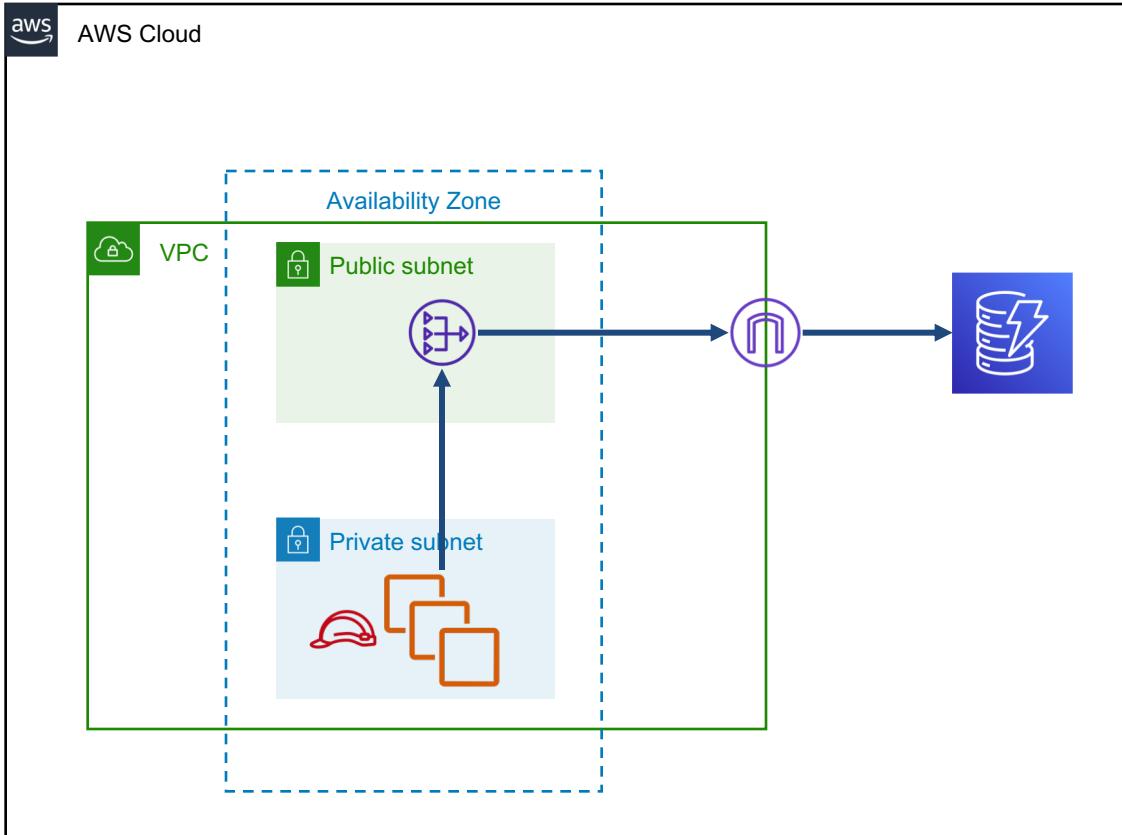
Application instances
launched into private
subnet

Current Infrastructure



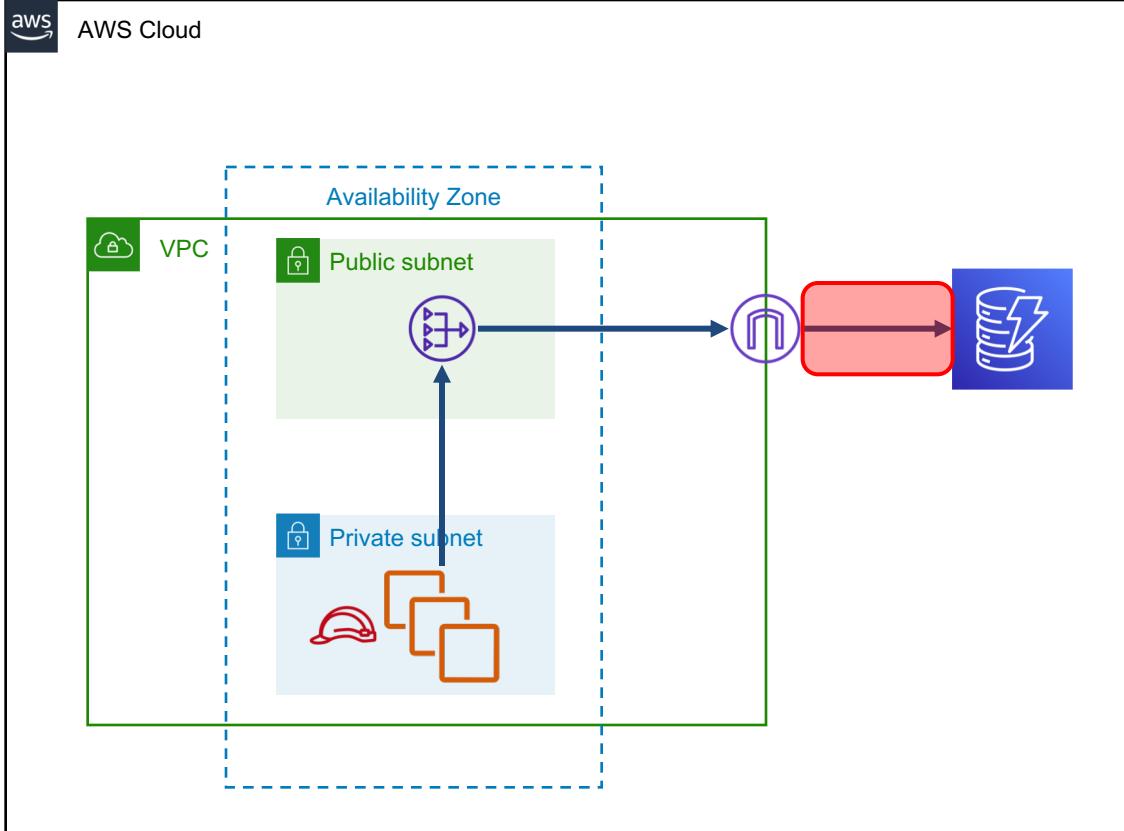
IAM role attached to instances with
DynamoDB permissions

Current Infrastructure



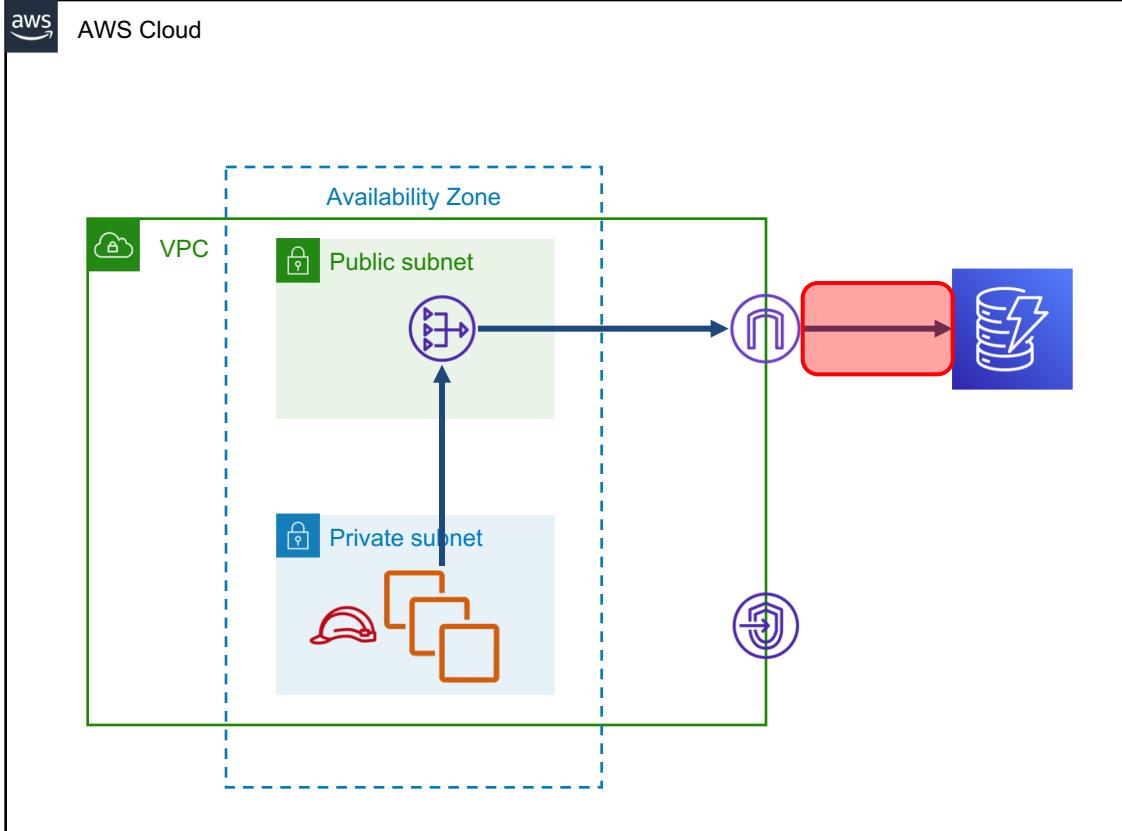
Instances communicate with DynamoDB via NAT GW and IGW

Infrastructure Improvements



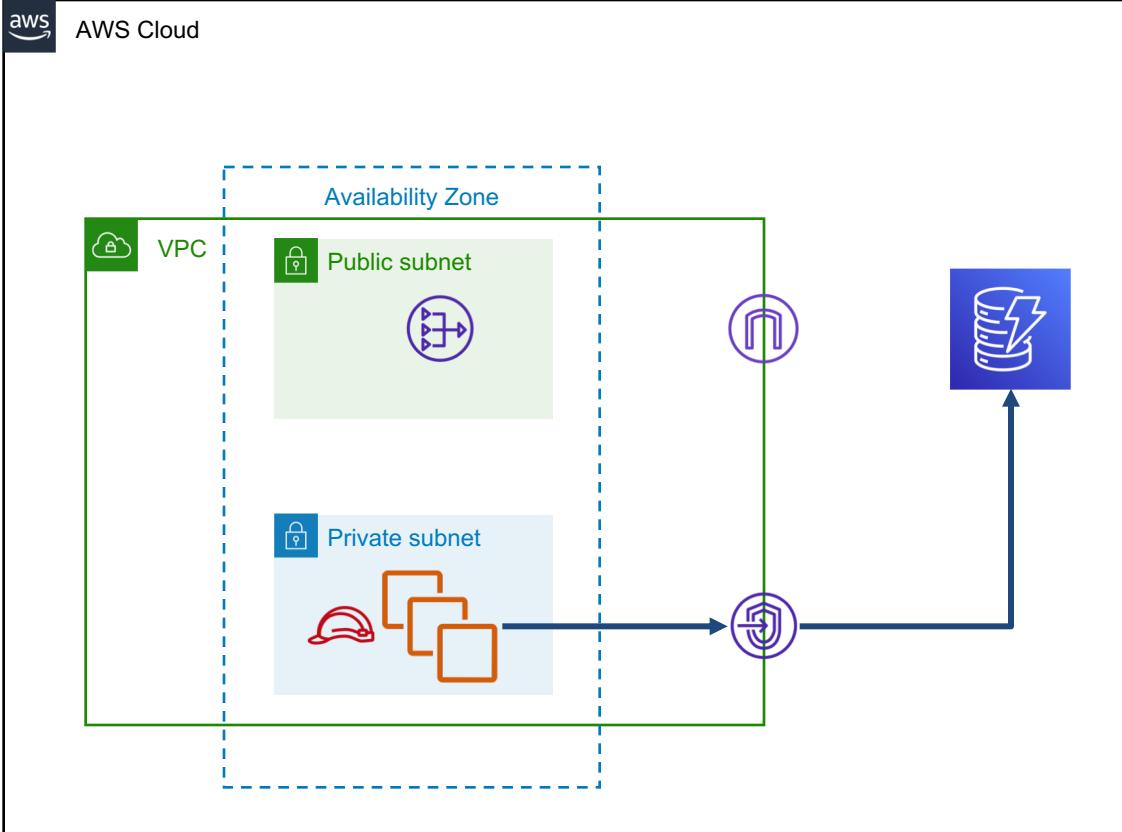
IGW traffic uses AWS public network

Infrastructure Improvements



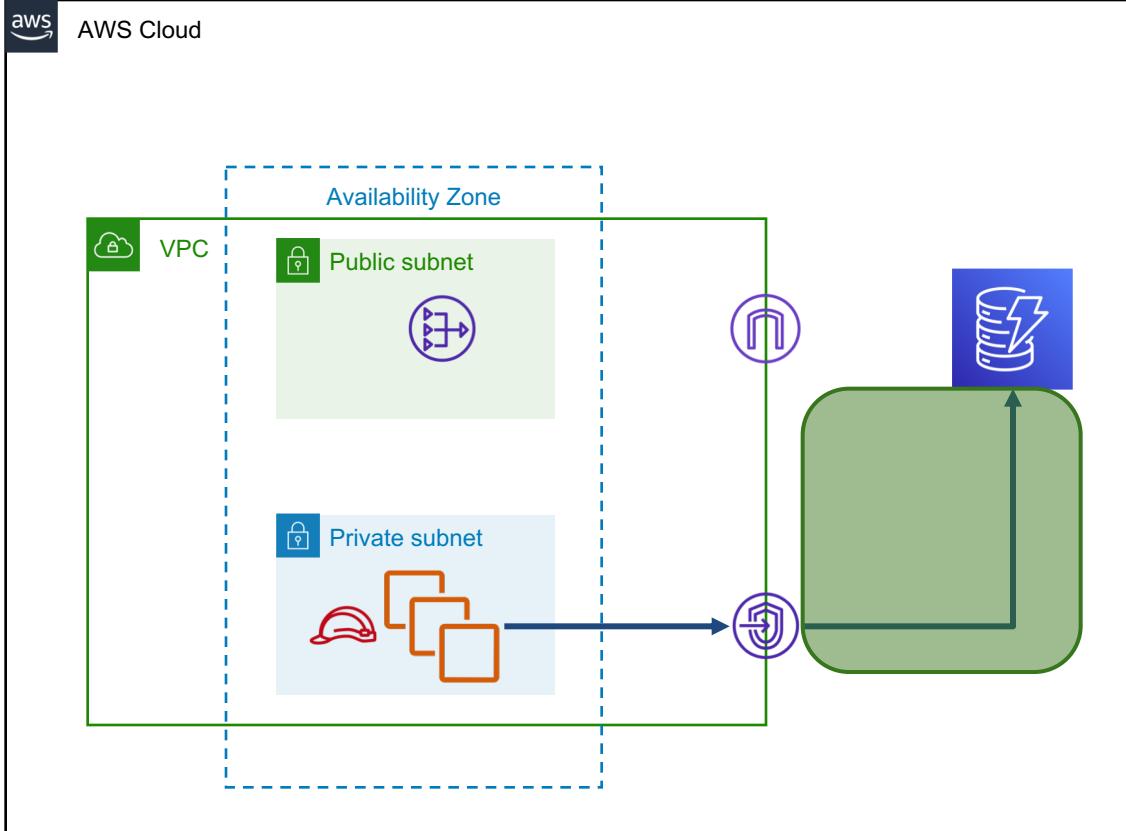
Add a Gateway endpoint

Infrastructure Improvements



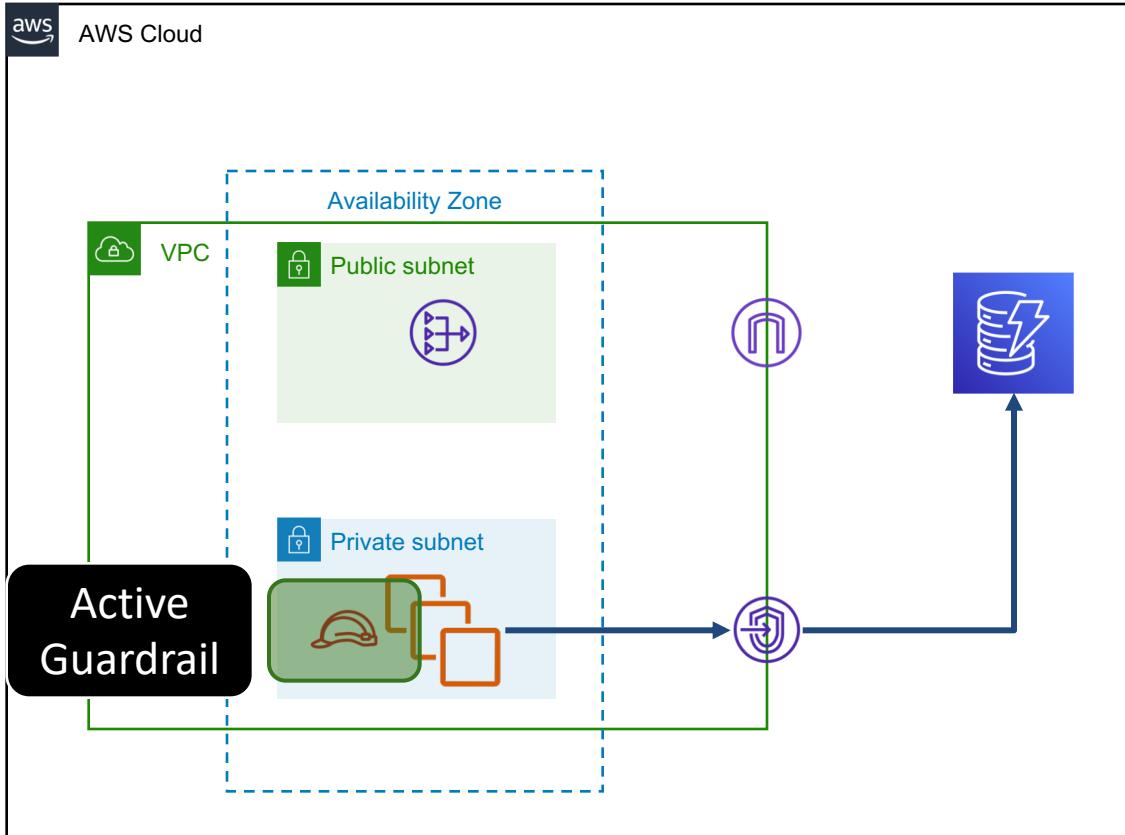
Route traffic through endpoint instead of NAT GW and IGW

Infrastructure Improvements



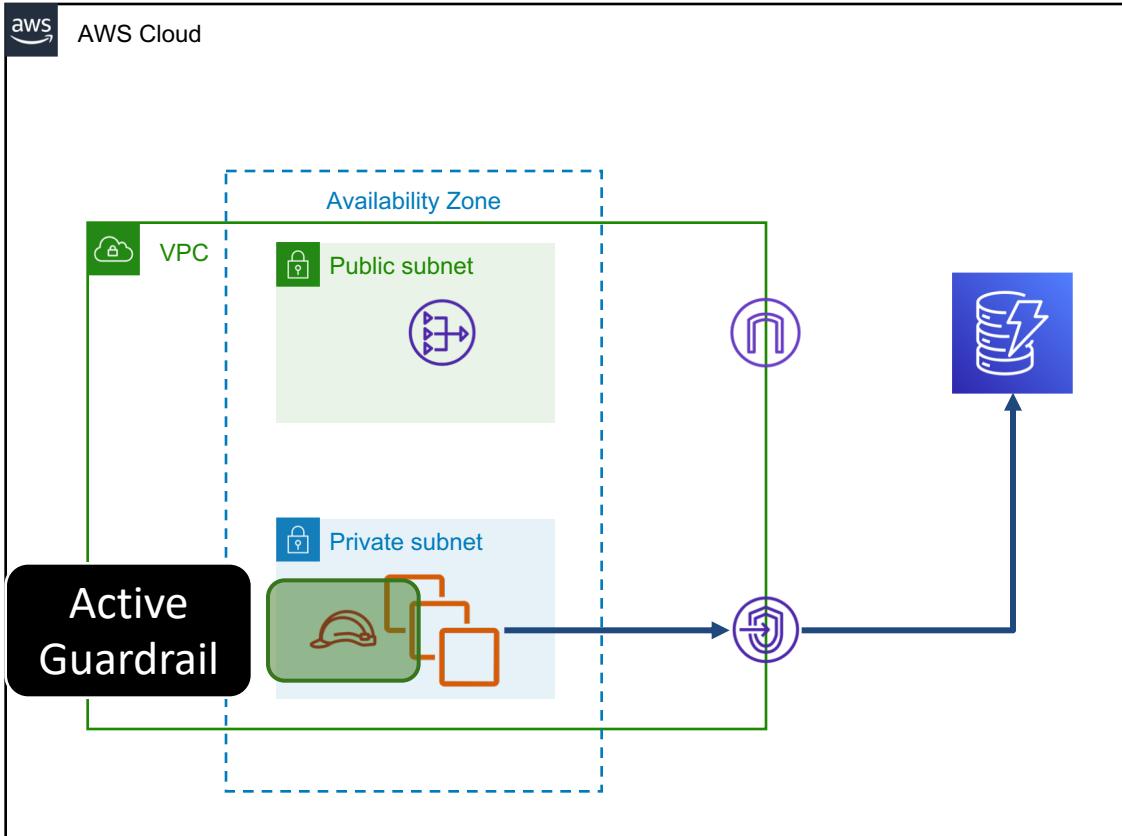
Traffic is now proxied privately to the
DynamoDB endpoint
(and FREE!)

Permissions Improvements



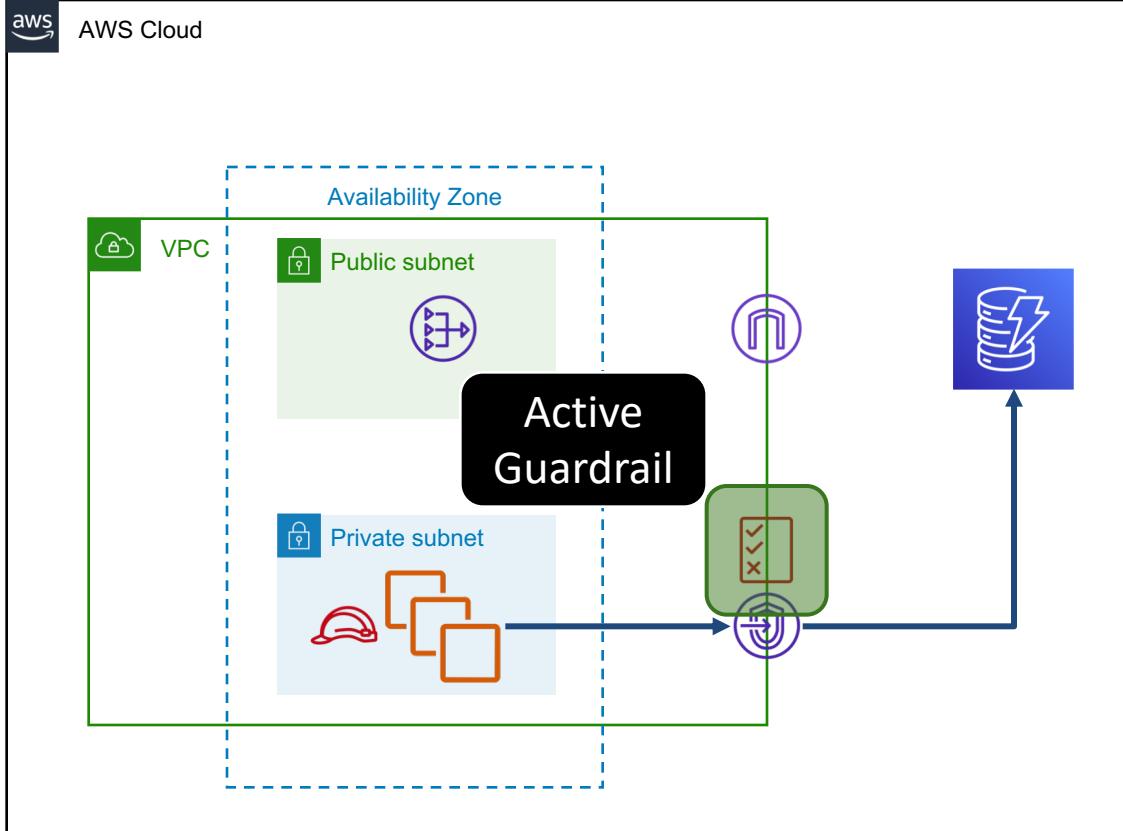
Add condition to IAM role policy only allowing requests from VPC ID

Permissions Improvements



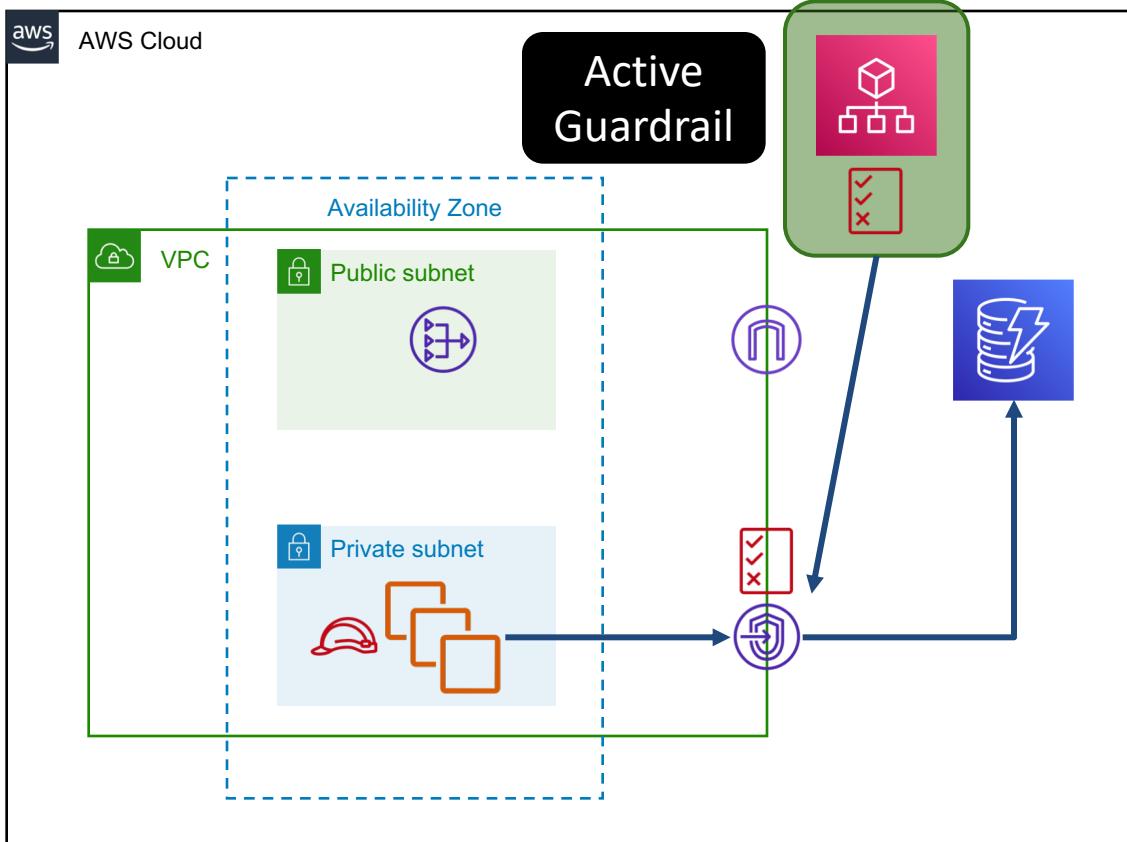
Configure a permissions boundary on the policy to ensure least privilege

Permissions Improvements



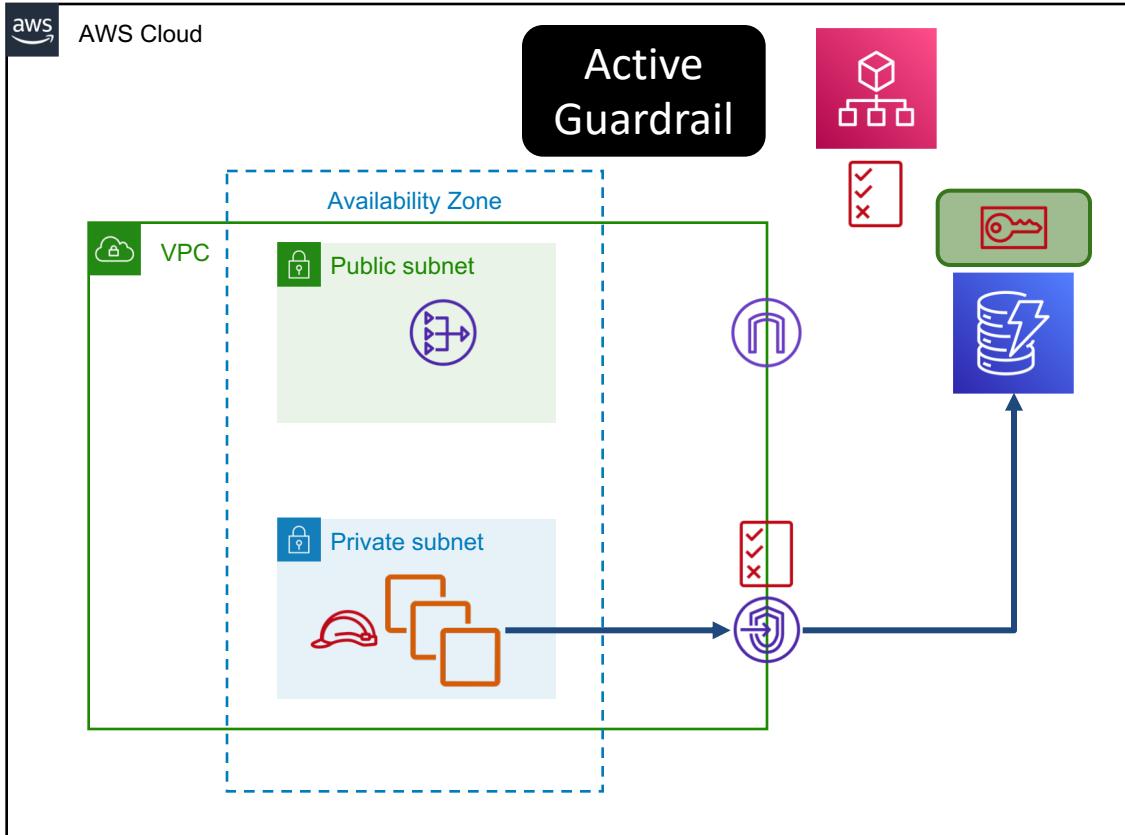
Add Endpoint policy
with condition for
traffic only from
application subnet

Permissions Improvements



Add Organizations SCP
to deny DynamoDB
table access except
through Gateway
endpoint

Permissions Improvements



Use KMS encryption on the table and allow the IAM role as the only key user

Question Breakdown

Question Scenario

Your company's AWS infrastructure is deployed entirely on EC2 instances in a single VPC. Network security is implemented with public and private subnets, Network ACLs and Security groups.

The company has a new security mandate to evaluate all outbound traffic for Data Loss Prevention (DLP) and reject inappropriate data transfer.

Desired options for security modifications will include active traffic rejection and low operational overhead.

Which of the following will NOT meet these requirements?

Answer Choices

- A. Deploy a GateWay Load Balancer and an Auto Scaling group of EC2 instance with network analysis + proxy software. Route all Internet-bound traffic to the GWLB via route table entries.
- B. Deploy an EC2 instance with network analysis + proxy software. Route all Internet-bound traffic to the ENI of the instance via route table entries.
- C. Deploy a NAT Gateway managed resource in each AZ in the VPC. Route all Internet-bound traffic to the NAT GW via route table entries.
- D. Deploy an Application Load Balancer and Auto Scaling group of EC2 instances with web proxy software. Configure all other EC2 instances to use the ALB endpoint for all outbound web traffic.

Answer A

This is a functional solution and also has the benefit of being resilient AND able to scale to support small or large amounts of traffic.

Deploy a GateWay Load Balancer and an Auto Scaling group of EC2 instance with network analysis + proxy software. Route all Internet-bound traffic to the GWLB via route table entries.

Answer B

This is functional, and before the GWLB, would have been a recommended solution. It is also a SPoF and potentially a bottleneck, but meets the requirements.

**Deploy an EC2 instance with network analysis + proxy software.
Route all Internet-bound traffic to the ENI of the instance via route table entries.**

Answer C

This could be a great solution with low operational overhead, except that the customer has zero visibility into the actual traffic passing through the NAT Gateway, nor can the customer filter or reject traffic from within the OS of the NAT Gateway. The only options are Network ACLs and outbound Security Group rules on the source instance.

Deploy a NAT Gateway managed resource in each AZ in the VPC. Route all Internet-bound traffic to the NAT GW via route table entries.

Answer D

This is a (mostly) functional solution. This will cover all web traffic, but the requirements in the scenario imply that the solution should address Layer 3 (IP) traffic, not layer 7 (Application).

Deploy an Application Load Balancer and Auto Scaling group of EC2 instances with web proxy software. Configure all other EC2 instances to use the ALB endpoint for all outbound web traffic.

Correct Answer

- A. Deploy a GateWay Load Balancer and an Auto Scaling group of EC2 instance with network analysis + proxy software. Route all Internet-bound traffic to the GWLB via route table entries.
- B. Deploy an EC2 instance with network analysis + proxy software. Route all Internet-bound traffic to the ENI of the instance via route table entries.
- C. Deploy a NAT Gateway managed resource in each AZ in the VPC. Route all Internet-bound traffic to the NAT GW via route table entries.
- D. *Deploy an Application Load Balancer and Auto Scaling group of EC2 instances with web proxy software. Configure all other EC2 instances to use the ALB endpoint for all outbound web traffic.*



Wrap up and QA