

Question 1:

A company needs to architect a hybrid DNS solution. This solution will use an Amazon Route 53 private hosted zone for the domain cloud.example.com for the resources stored within VPCs.

The company has the following DNS resolution requirements:

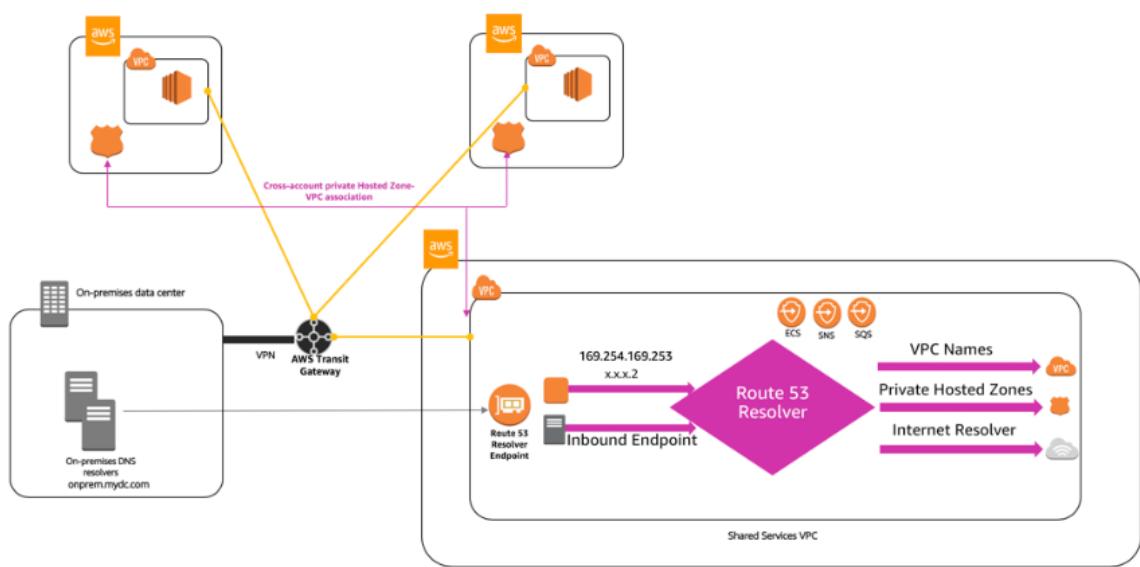
- On-premises systems should be able to resolve and connect to cloud.example.com.
- All VPCs should be able to resolve cloud.example.com.
- There is already an AWS Direct Connect connection between the on-premises corporate network and AWS Transit Gateway.

Which architecture should the company use to meet these requirements with the HIGHEST performance?

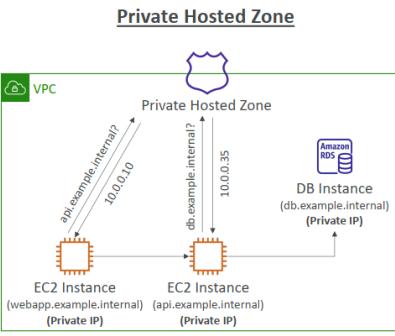
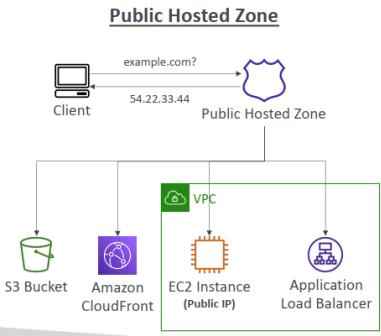
- A. Associate the private hosted zone to all the VPCs. Create a Route 53 inbound resolver in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.
- B. Associate the private hosted zone to all the VPCs. Deploy an Amazon EC2 conditional forwarder in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the conditional forwarder.
- C. Associate the private hosted zone to the shared services VPC. Create a Route 53 outbound resolver in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the outbound resolver.
- D. Associate the private hosted zone to the shared services VPC. Create a Route 53 inbound resolver in the shared services VPC. Attach the shared services VPC to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.

A.

<https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/>

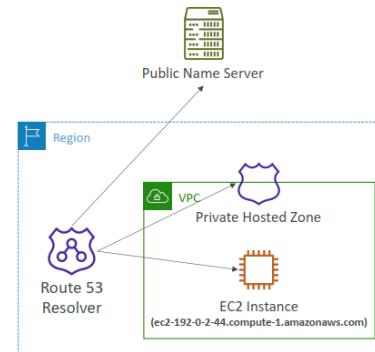


Route 53 – Public vs. Private Hosted Zones

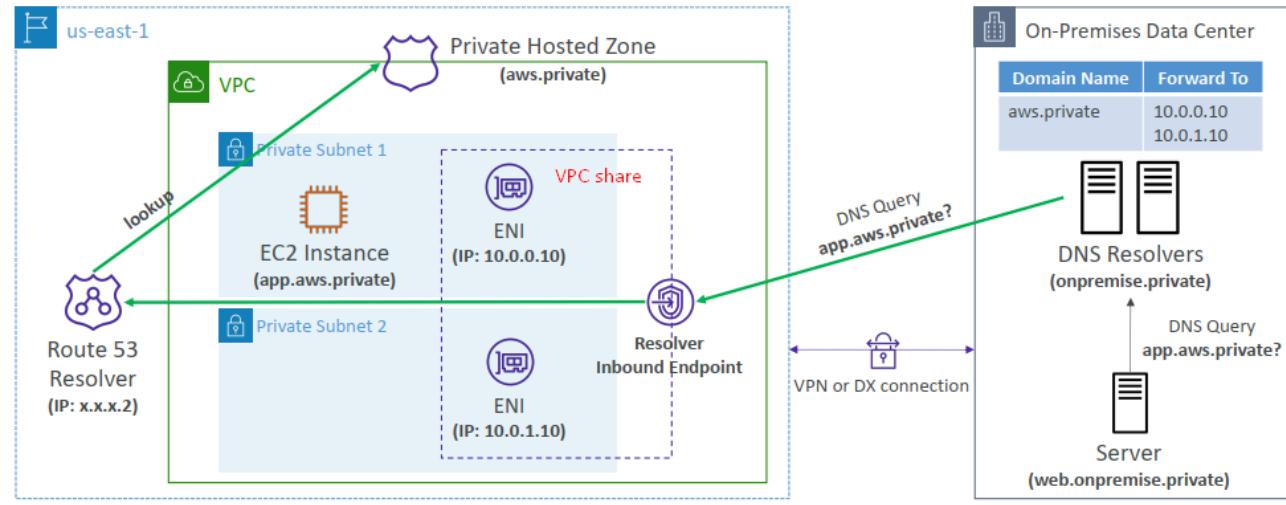


Route 53 – Hybrid DNS

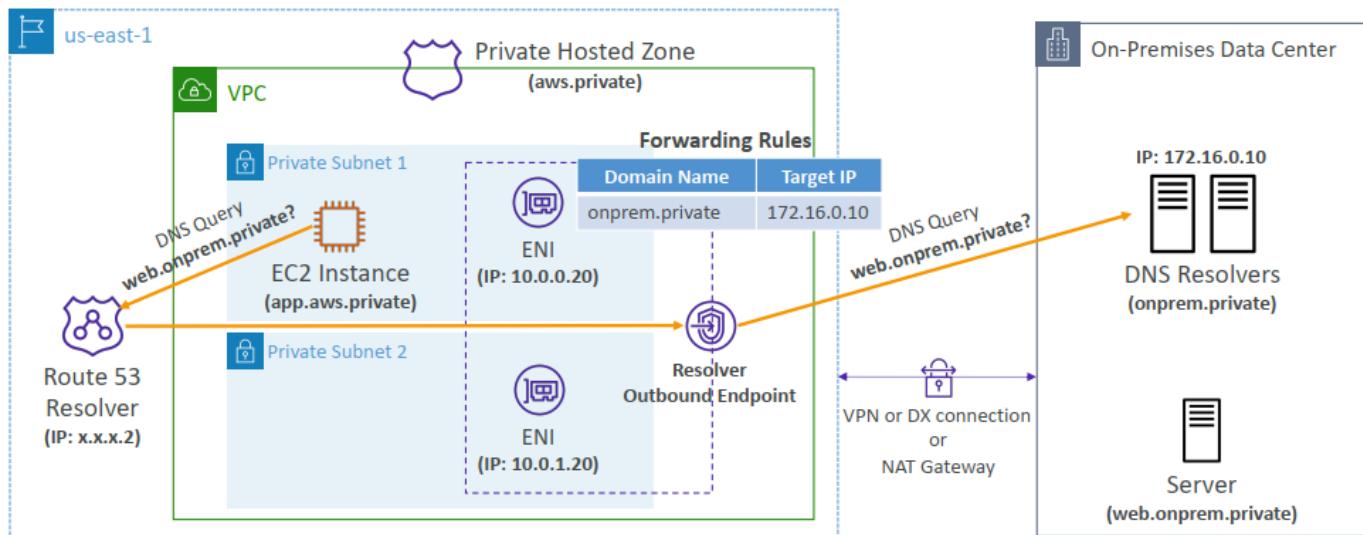
- By default, Route 53 Resolver automatically answers DNS queries for:
 - Local domain names for EC2 instances
 - Records in Private Hosted Zones
 - Records in public Name Servers
- Hybrid DNS – resolving DNS queries between VPC (Route 53 Resolver) and your networks (other DNS Resolvers)
- Networks can be:
 - VPC itself / Peered VPC
 - On-premises Network (connected through Direct Connect or AWS VPN)



Route 53 – Resolver Inbound Endpoints



Route 53 – Resolver Outbound Endpoints



Question 2:

A company is providing weather data over a REST-based API to several customers. The API is hosted by Amazon API Gateway and is integrated with different AWS Lambda functions for each API operation. The company uses Amazon Route 53 for DNS and has created a resource record of `weather.example.com`. The company stores data for the API in Amazon DynamoDB tables. The company needs a solution that will give the API the ability to fail over to a different AWS Region.

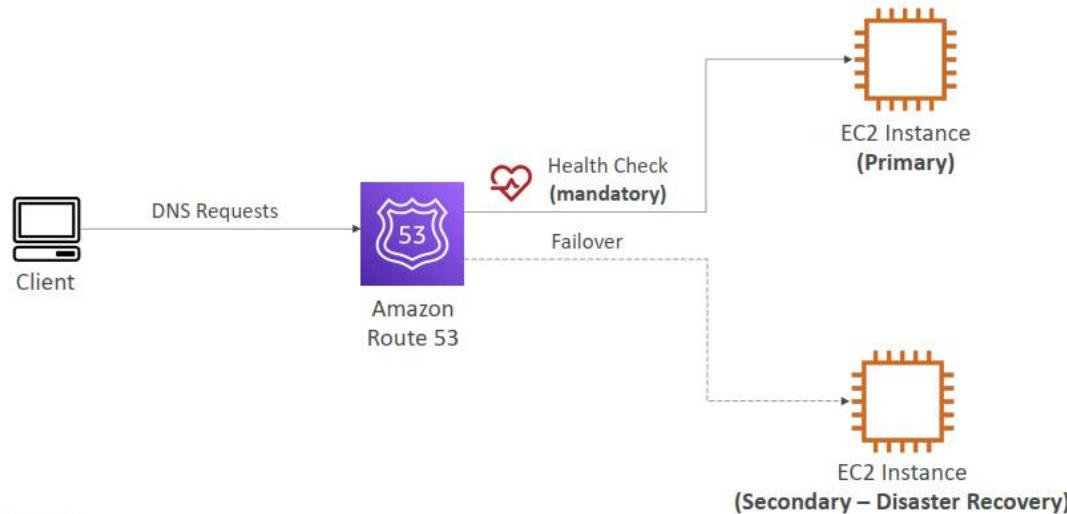
Which solution will meet these requirements?

- A. Deploy a new set of Lambda functions in a new Region. Update the API Gateway API to use an edge-optimized API endpoint with Lambda functions from both Regions as targets. Convert the DynamoDB tables to global tables.
- B. Deploy a new API Gateway API and Lambda functions in another Region. Change the Route 53 DNS record to a multivalue answer. Add both API Gateway APIs to the answer. Enable target health monitoring. Convert the DynamoDB tables to global tables.
- C. Deploy a new API Gateway API and Lambda functions in another Region. Change the Route 53 DNS record to a failover record. Enable target health monitoring. Convert the DynamoDB tables to global tables.
- D. Deploy a new API Gateway API in a new Region. Change the Lambda functions to global functions. Change the Route 53 DNS record to a multivalue answer. Add both API Gateway APIs to the answer. Enable target health monitoring. Convert the DynamoDB tables to global tables.

C

fail over to a different AWS Region ➔ Route 53 failover (active-passive) and DynamoDB global

Routing Policies – Failover (Active-Passive)



Question 3:

A company uses AWS Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU. Administrators use deny list SCPs in the root of the organization to manage access to restricted services.

The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization. Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company's policies.

Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?

- A. Remove the organization's root SCPs that limit access to AWS Config. Create AWS Service Catalog products for the company's standard AWS Config rules and deploy them throughout the organization, including the new account.
- B. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the new account to the Production OU when adjustments to AWS Config are complete.
- C. Convert the organization's root SCPs from deny list SCPs to allow list SCPs to allow the required services only. Temporarily apply an SCP to the organization's root that allows AWS Config actions for principals only in the new account.
- D. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the organization's root SCP to the Production OU. Move the new account to the Production OU when adjustments to AWS Config are complete.

D.

<https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/transitional-ou.html>

Question 4:

A company is running a two-tier web-based application in an on-premises data center. The application layer consists of a single server running a stateful application. The application connects to a PostgreSQL database running on a separate server. The application's user base is expected to grow significantly, so the company is migrating the application and database to AWS. The solution will use Amazon Aurora PostgreSQL, Amazon EC2 Auto Scaling, and Elastic Load Balancing.

Which solution will provide a consistent user experience that will allow the application and database tiers to scale?

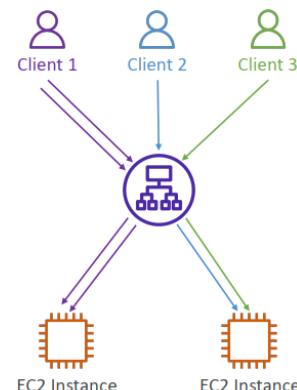
- A. Enable Aurora Auto Scaling for Aurora Replicas. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.
- B. Enable Aurora Auto Scaling for Aurora writers. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled.
- C. Enable Aurora Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the round robin routing and sticky sessions enabled.
- D. Enable Aurora Scaling for Aurora writers. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.

C

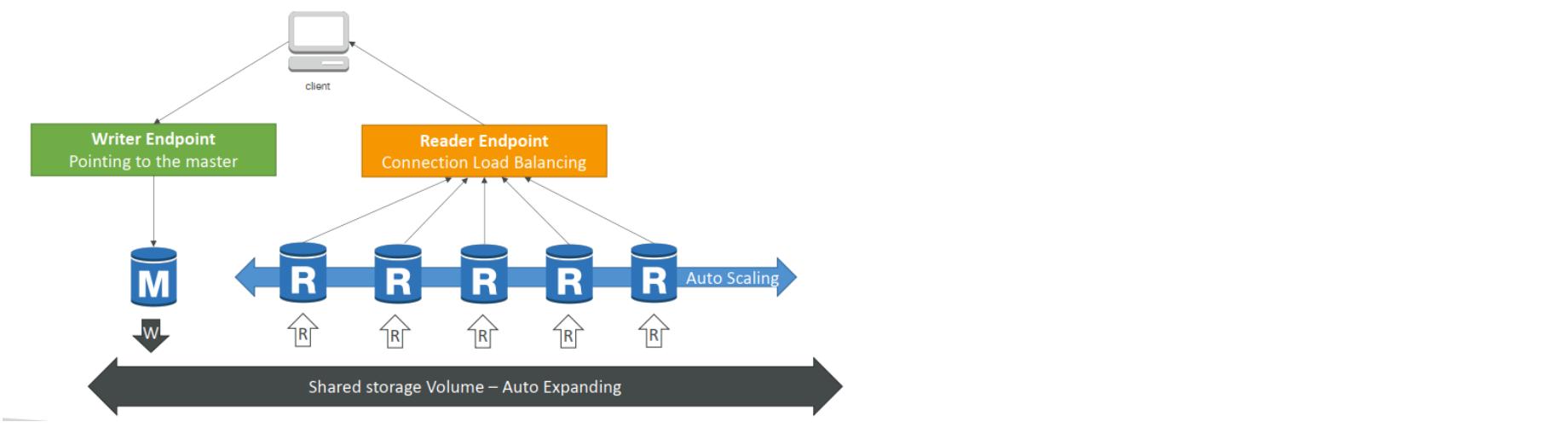
A, D is incorrect because sticky sessions don't work for NLB

Sticky Sessions (Session Affinity)

- It is possible to implement stickiness so that the same client is always redirected to the same instance behind a load balancer
- This works for Classic Load Balancers & Application Load Balancers
- The “cookie” used for stickiness has an expiration date you control
- Use case: make sure the user doesn't lose his session data
- Enabling stickiness may bring imbalance to the load over the backend EC2 instances



Aurora DB Cluster



Question 5:

A company uses a service to collect metadata from applications that the company hosts on premises. Consumer devices such as TVs and internet radios access the applications. Many older devices do not support certain HTTP headers and exhibit errors when these headers are present in responses. The company has configured an on-premises load balancer to remove the unsupported headers from responses sent to older devices, which the company identified by the User-Agent headers.

The company wants to migrate the service to AWS, adopt serverless technologies, and retain the ability to support the older devices. The company has already migrated the applications into a set of AWS Lambda functions.

Which solution will meet these requirements?

- Create an Amazon CloudFront distribution for the metadata service. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the ALB. Configure the ALB to invoke the correct Lambda function for each type of request. Create a CloudFront function to remove the problematic headers based on the value of the User-Agent header.
- Create an Amazon API Gateway REST API for the metadata service. Configure API Gateway to invoke the correct Lambda function for each type of request. Modify the default gateway responses to remove the problematic headers based on the value of the User-Agent header.
- Create an Amazon API Gateway HTTP API for the metadata service. Configure API Gateway to invoke the correct Lambda function for each type of request. Create a response mapping template to remove the problematic headers based on the value of the User-Agent. Associate the response data mapping with the HTTP API.
- Create an Amazon CloudFront distribution for the metadata service. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the ALB. Configure the ALB to invoke the correct Lambda function for each type of request. Create a Lambda@Edge function that will remove the problematic headers in response to viewer requests based on the value of the User-Agent header.

D.

CloudFront Functions vs. Lambda@Edge – Use Cases

CloudFront Functions

- Cache key normalization
 - Transform request attributes (headers, cookies, query strings, URL) to create an optimal Cache Key
- Header manipulation thao tác
 - Insert/modify/delete HTTP headers in the request or response
- URL rewrites or redirects
- Request authentication & authorization
 - Create and validate user-generated tokens (e.g., JWT) to allow/deny requests

Lambda@Edge

- Longer execution time (several ms)
- Adjustable CPU or memory
- Your code depends on a 3rd libraries (e.g., AWS SDK to access other AWS services)
- Network access to use external services for processing
- File system access or access to the body of HTTP requests

Question 6:

A retail company needs to provide a series of data files to another company, which is its business partner. These files are saved in an Amazon S3 bucket under Account A, which belongs to the retail company. The business partner company wants one of its IAM users, User_DataProcessor, to access the files from its own AWS account (Account B).

Which combination of steps must the companies take so that User_DataProcessor can access the S3 bucket successfully? (Choose two.)

A. Turn on the cross-origin resource sharing (CORS) feature for the S3 bucket in Account A.

B. In Account A, set the S3 bucket policy to the following:

```
{  
    "Effect": "Allow",  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": "arn:aws:s3:::AccountABucketName/*"  
}
```

C. In Account A, set the S3 bucket policy to the following:

```
{  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"  
    },  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": [  
        "arn:aws:s3:::AccountABucketName/*"  
    ]  
}
```

D. In Account B, set the permissions of User_DataProcessor to the following:

```
{  
    "Effect": "Allow",  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": "arn:aws:s3:::AccountABucketName/*"  
}
```

E. In Account B, set the permissions of User_DataProcessor to the following:

```
{  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"  
    },  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": [  
        "arn:aws:s3:::AccountABucketName/*"  
    ]  
}
```

C and D

<https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example4.html>

Principal element: Who can access the objects inside the bucket

Resource element: The objects that they can access

Action element: How they can access the objects inside the bucket

Question 7:

A company is running a traditional web application on Amazon EC2 instances. The company needs to refactor the application as microservices that run on containers. Separate versions of the application exist in two distinct environments: production and testing. Load for the application is variable, but the minimum load and the maximum load are known. A solutions architect needs to design the updated application with a serverless architecture that minimizes operational complexity.

Which solution will meet these requirements MOST cost-effectively?

- A. Upload the container images to AWS Lambda as functions. Configure a concurrency limit for the associated Lambda functions to handle the expected peak load. Configure two separate Lambda integrations within Amazon API Gateway: one for production and one for testing.
- B. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto scaled Amazon Elastic Container Service (Amazon ECS) clusters with the Fargate launch type to handle the expected load. Deploy tasks from the ECR images. Configure two separate Application Load Balancers to direct traffic to the ECS clusters.
- C. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto scaled Amazon Elastic Kubernetes Service (Amazon EKS) clusters with the Fargate launch type to handle the expected load. Deploy tasks from the ECR images. Configure two separate Application Load Balancers to direct traffic to the EKS clusters.
- D. Upload the container images to AWS Elastic Beanstalk. In Elastic Beanstalk, create separate environments and deployments for production and testing. Configure two separate Application Load Balancers to direct traffic to the Elastic Beanstalk deployments.

B

MOST cost-effectively and microservices that run on containers ➔ ECS is cheaper than EKS

Question 8:

A company has a multi-tier web application that runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB and the Auto Scaling group are replicated in a backup AWS Region. The minimum value and the maximum value for the Auto Scaling group are set to zero. An Amazon RDS Multi-AZ DB instance stores the application's data. The DB instance has a read replica in the backup Region. The application presents an endpoint to end users by using an Amazon Route 53 record.

The company needs to reduce its RTO to less than 15 minutes by giving the application the ability to automatically fail over to the backup Region. The company does not have a large enough budget for an active-active strategy.

What should a solutions architect recommend to meet these requirements?

- A. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALBs. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Create an Amazon CloudWatch alarm that is based on the `HTTPCode_Target_5XX_Count` metric for the ALB in the primary Region. Configure the CloudWatch alarm to invoke the Lambda function.

B. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Configure Route 53 with a health check that monitors the web application and sends an Amazon Simple Notification Service (Amazon SNS) notification to the Lambda function when the health check status is unhealthy. Update the application's Route 53 record with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.

C. Configure the Auto Scaling group in the backup Region to have the same values as the Auto Scaling group in the primary Region. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALBs. Remove the read replica. Replace the read replica with a standalone RDS DB instance. Configure Cross-Region Replication between the RDS DB instances by using snapshots and Amazon S3.

D. Configure an endpoint in AWS Global Accelerator with the two ALBs as equal weighted targets. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Create an Amazon CloudWatch alarm that is based on the HTTPCode_Target_5XX_Count metric for the ALB in the primary Region. Configure the CloudWatch alarm to invoke the Lambda function.

B.

Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Configure Route 53 with a health check that monitors the web application and sends an Amazon Simple Notification Service (Amazon SNS) notification to the Lambda function when the health check status is unhealthy. Update the application's Route 53 record with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.

https://docs.amazonaws.cn/en_us/Route53/latest/DeveloperGuide/welcome-health-checks.html

Option A - This option will not work as needed: The client will get errors when the closest region is the application's backup region

Option B - This option implements an active-passive strategy as needed: When the health check fails, Route 53 will resolve to the backup region and the Lambda function will ensure the backup region has resources to function

Option C - This option implements an active-active strategy

Option D - This option will not work as needed: The client will get errors 50% of the time

Question 9:

A company is hosting a critical application on a single Amazon EC2 instance. The application uses an Amazon ElastiCache for Redis single-node cluster for an in-memory data store. The application uses an Amazon RDS for MariaDB DB instance for a relational database. For the application to function, each piece of the infrastructure must be healthy and must be in an active state.

A solutions architect needs to improve the application's architecture so that the infrastructure can automatically recover from failure with the least possible downtime.

Which combination of steps will meet these requirements? (Choose three.)

A. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are part of an Auto Scaling group that has a minimum capacity of two instances.

B. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are configured in unlimited mode.

C. Modify the DB instance to create a read replica in the same Availability Zone. Promote the read replica to be the primary DB instance in failure scenarios.

D. Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.

E. Create a replication group for the ElastiCache for Redis cluster. Configure the cluster to use an Auto Scaling group that has a minimum capacity of two instances.

F. Create a replication group for the ElastiCache for Redis cluster. Enable Multi-AZ on the cluster.

ADF

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html>

A. Using an Elastic Load Balancer (ELB) to distribute traffic across multiple EC2 instances can help ensure that the application remains available in the event that one of the instances becomes unavailable. By configuring the instances as part of an Auto Scaling group with a minimum capacity of two instances, you can ensure that there is always at least one healthy instance to handle traffic.

D. Modifying the DB instance to create a Multi-AZ deployment that extends across two availability zones can help ensure that the database remains available in the event of a failure. In the event of a failure, traffic will automatically be directed to the secondary availability zone, reducing the amount of downtime.

F. Creating a replication group for the ElastiCache for Redis cluster and enabling Multi-AZ can help ensure that the in-memory data store remains available in the event of a failure. This will allow traffic to be automatically directed to the secondary availability zone, reducing the amount of downtime.

Question 10:

A retail company is operating its ecommerce application on AWS. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses an Amazon RDS DB instance as the database backend. Amazon CloudFront is configured with one origin that points to the ALB. Static content is cached. Amazon Route 53 is used to host all public zones.

After an update of the application, the ALB occasionally returns a 502 status code (Bad Gateway) error. The root cause is malformed HTTP headers that are returned to the ALB. The webpage returns successfully when a solutions architect reloads the webpage immediately after the error occurs.

While the company is working on the problem, the solutions architect needs to provide a custom error page instead of the standard ALB error page to visitors.

Which combination of steps will meet this requirement with the LEAST amount of operational overhead? (Choose two.)

A. Create an Amazon S3 bucket. Configure the S3 bucket to host a static webpage. Upload the custom error pages to Amazon S3.

B. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Target.FailedHealthChecks is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a publicly accessible web server.

C. Modify the existing Amazon Route 53 records by adding health checks. Configure a fallback target if the health check fails. Modify DNS records to point to a publicly accessible webpage.

D. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Elb.InternalError is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a public accessible web server.

E. Add a custom error response by configuring a CloudFront custom error page. Modify DNS records to point to a publicly accessible web page.

A and E

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GeneratingCustomErrorResponse.html#custom-error-pages-procedure>

E4PQU25CJ499Y

[View metrics](#)

General | Security | Origins | Behaviors | **Error pages** | Invalidations | Tags

Error pages

[Edit](#)

[Delete](#)

Create custom error response

HTTP error code ▲

Minimum TTL (seconds) ▼

Response page path ▼

HTTP response code ▼

No error pages

You don't have any error pages.

[Create custom error response](#)

Question 11:

A company has many AWS accounts and uses AWS Organizations to manage all of them. A solutions architect must implement a solution that the company can use to share a common network across multiple accounts.

The company's infrastructure team has a dedicated infrastructure account that has a VPC. The infrastructure team must use this account to manage the network. Individual accounts cannot have the ability to manage their own networks. However, individual accounts must be able to create AWS resources within subnets.

Which combination of actions should the solutions architect perform to meet these requirements? (Choose two.)

- A. Create a transit gateway in the infrastructure account.
- B. Enable resource sharing from the AWS Organizations management account.
- C. Create VPCs in each AWS account within the organization in AWS Organizations. Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account. Peer the VPCs in each individual account with the VPC in the infrastructure account.
- D. Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each subnet to associate with the resource share.
- E. Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each prefix list to associate with the resource share.

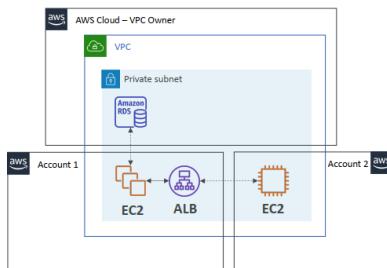
B and D

A is wrong. No TGW needed as customer has just 1 VPC.

E is wrong - can't share resources via RAM using prefix lists.

C is wrong - talks about creating VPCs with same CIDR ranges and VPC peering (not possible with overlapping CIDRs and not needed for this solution as there is just 1 VPC).

Resource Access Manager – VPC example



- Each account...
 - is responsible for its own resources
 - cannot view, modify or delete other resources in other accounts
- Network is shared so...
 - Anything deployed in the VPC can talk to other resources in the VPC
 - Applications are accessed easily across accounts, using private IP
 - Security groups from other accounts can be referenced for maximum security
- Use cases
 - Applications within the same trust boundaries *Các ứng dụng trong cùng 1 danh giới tin cậy*
 - Applications with a high degree of interconnectivity *Các ứng dụng có độ liên kết cao*

AWS Resource Access Manager (RAM)

- Share AWS resources that you own with other AWS accounts
- Share with any account or within your Organization
- Avoid resource duplication!
- **VPC Subnets**
 - Allow to have all the resources launched in the same subnets
 - Must be from the same AWS Organizations.
 - Cannot share security groups and default VPC
 - Participants can manage their own resources in there
 - Participants can't view, modify, delete resources that belong to other participants or the owner
- **AWS Transit Gateway**
- Route 53 (Resolver Rules, DNS Firewall Rule Groups)
- License Manager Configurations



Resource Access Manager Managed Prefix List

- A set of one or more CIDR blocks
- Makes it easier to configure and maintain Security Groups and Route Tables
- **Customer-Managed Prefix List**
 - Set of CIDRs that you define and manage by you
 - Can be shared with other AWS accounts or AWS Organization
 - Modify to update many security groups at once
- **AWS-Managed Prefix List**
 - Set of CIDRs for AWS services
 - You can't create, modify, share, or delete them

Question 12:

A company wants to use a third-party software-as-a-service (SaaS) application. The third-party SaaS application is consumed through several API calls. The third-party SaaS application also runs on AWS inside a VPC.

The company will consume the third-party SaaS application from inside a VPC. The company has internal security policies that mandate the use of private connectivity that does not traverse the internet. No resources that run in the company VPC are allowed to be accessed from outside the company's VPC. All permissions must conform to the principles of least privilege.

Which solution meets these requirements?

- A. Create an AWS PrivateLink interface VPC endpoint. Connect this endpoint to the endpoint service that the third-party SaaS application provides. Create a security group to limit the access to the endpoint. Associate the security group with the endpoint.
- B. Create an AWS Site-to-Site VPN connection between the third-party SaaS application and the company VPC. Configure network ACLs to limit access across the VPN tunnels.
- C. Create a VPC peering connection between the third-party SaaS application and the company VPC. Update route tables by adding the needed routes for the peering connection.
- D. Create an AWS PrivateLink endpoint service. Ask the third-party SaaS provider to create an interface VPC endpoint for this endpoint service. Grant permissions for the endpoint service to the specific account of the third-party SaaS provider.

A.

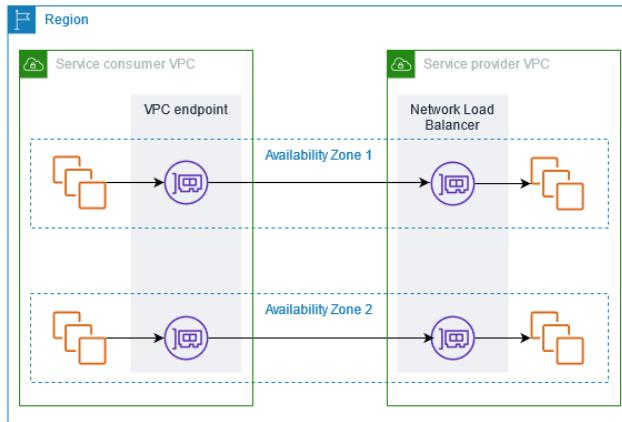
<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html>

Using AWS PrivateLink, you can access SaaS products privately, as if they were running in your own VPC.

You can discover, purchase, and provision SaaS products powered by AWS PrivateLink through AWS Marketplace. For more information, see AWS Marketplace: - PrivateLink.

You can also find SaaS products powered by AWS PrivateLink from AWS Partners. For more information see AWS PrivateLink Partners.

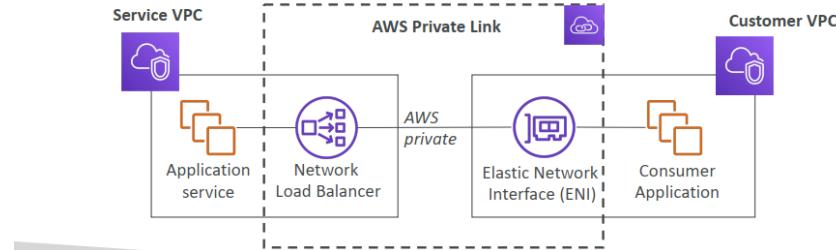
The following diagram shows how you use VPC endpoints to connect to SaaS products. The service provider creates an endpoint service and grants their customers access to the endpoint service. As the service consumer, you create an interface VPC endpoint, which establishes connections between one or more subnets in your VPC and the endpoint service.



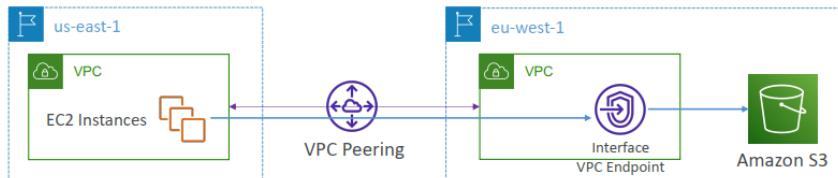
AWS PrivateLink (VPC Endpoint Services)



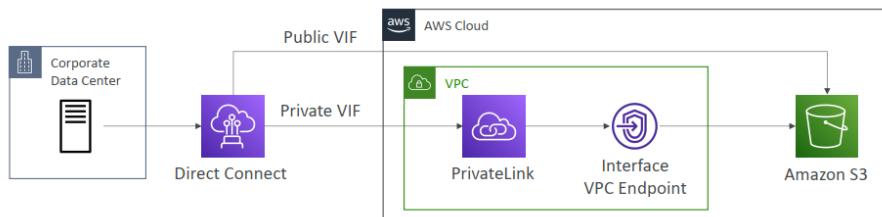
- Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts)
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)
- If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!



VPC Endpoints / PrivateLink and VPC Peering



PrivateLink for Amazon S3 with Direct Connect



Question 13:

A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching. Management requires a single report showing the patch status of all the servers and instances.

Which set of actions should a solutions architect take to meet these requirements?

- A. Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instances. Use Systems Manager to generate patch compliance reports.
- B. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use Amazon QuickSight integration with OpsWorks to generate patch compliance reports.
- C. Use an Amazon EventBridge rule to apply patches by scheduling an AWS Systems Manager patch remediation job. Use Amazon Inspector to generate patch compliance reports.
- D. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use AWS X-Ray to post the patch status to AWS Systems Manager OpsCenter to generate patch compliance reports.

A

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patch-management-hybrid-cloud/design-on-premises.html>

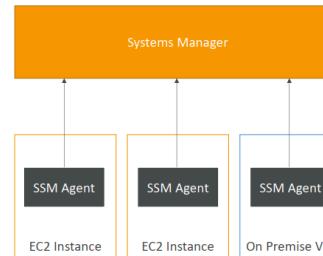
AWS Systems Manager Overview

- Helps you manage your EC2 and on-premises systems at scale
- Get operational insights about the state of your infrastructure
- Easily detect problems
- Patching automation for enhanced compliance
- Works for both Windows and Linux OS
- Integrated with CloudWatch metrics / dashboards
- Integrated with AWS Config
- Free service



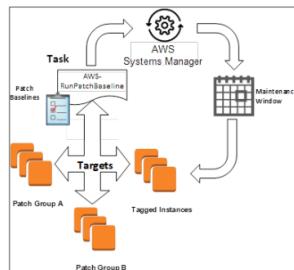
How Systems Manager works

- We need to install the SSM agent onto the systems we control
- Installed by default on Amazon Linux AMI & some Ubuntu AMI
- If an instance can't be controlled with Systems Manager, it's probably an issue with the SSM agent!
- Make sure the EC2 instances have a proper IAM role to allow Systems Manager actions



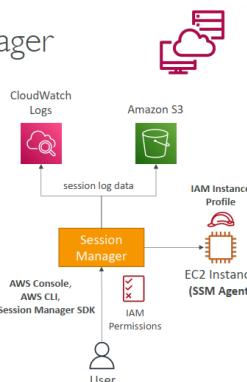
Systems Manager Patch Managers – Steps

1. Define a patch baseline to use (or multiple if you have multiple environments)
2. Define patch groups: define based on tags, example different environments (dev, test, prod) – use tag Patch Group
3. Define Maintenance Windows (schedule, duration, registered targets/patch groups and registered tasks)
4. Add the AWS-RunPatchBaseline Run Command as part of the registered tasks of the Maintenance Window (works cross platform Linux & Windows)
5. Define Rate Control (concurrency & error threshold) for the task
6. Monitor Patch Compliance using SSM Inventory



Systems Manager Session Manager

- Allows you to start a secure shell on your EC2 and on-premises servers
- Access through AWS Console, AWS CLI, or Session Manager SDK
- Does not need SSH access, bastion hosts, or SSH keys
- Supports Linux, macOS, and Windows
- Log connections to your instances and executed commands
- Session log data can be sent to S3 or CloudWatch Logs
- CloudTrail can intercept StartSession events



Question 14:

A company is running an application on several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The load on the application varies throughout the day, and EC2 instances are scaled in and out on a regular basis. Log files from the EC2 instances are copied to a central Amazon S3 bucket every 15 minutes. The security team discovers that log files are missing from some of the terminated EC2 instances.

Which set of actions will ensure that log files are copied to the central S3 bucket from the terminated EC2 instances?

- A. Create a script to copy log files to Amazon S3, and store the script in a file on the EC2 instance. Create an Auto Scaling lifecycle hook and an Amazon EventBridge rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to send ABANDON to the Auto Scaling group to prevent termination, run the script to copy the log files, and terminate the instance using the AWS SDK.
- B. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook and an Amazon EventBridge rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance.
- C. Change the log delivery rate to every 5 minutes. Create a script to copy log files to Amazon S3, and add the script to EC2 instance user data. Create an Amazon EventBridge rule to detect EC2 instance termination. Invoke an AWS Lambda function from the EventBridge rule that uses the AWS CLI to run the user-data script to copy the log files and terminate the instance.
- D. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook that publishes a message to an Amazon Simple Notification Service (Amazon SNS) topic. From the SNS notification, call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send ABANDON to the Auto Scaling group to terminate the instance.

B

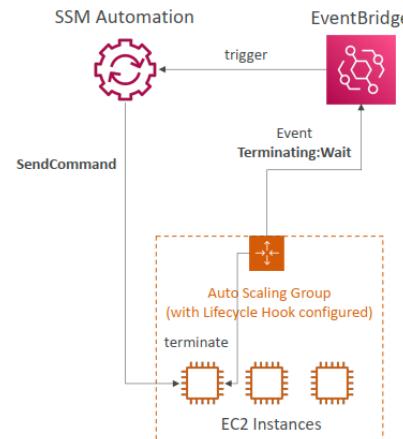
As an example of using lifecycle hooks with Auto Scaling instances:

When a scale-out event occurs, your newly launched instance completes its startup sequence and transitions to a wait state. While the instance is in a wait state, it runs a script to download and install the needed software packages for your application, making sure that your instance is fully ready before it starts receiving traffic. When the script is finished installing software, it sends the complete-lifecycle-action command to continue.

When a scale-in event occurs, a lifecycle hook pauses the instance before it is terminated and sends you a notification using Amazon EventBridge. While the instance is in the wait state, you can invoke an AWS Lambda function or connect to the instance to download logs or other data before the instance is fully terminated.

AWS Systems Manager – Send Command before an ASG Instance is Terminated

- Perform any action before the ASG terminates an EC2 instance
- Create a ASG Lifecycle Hook that puts the instance in **Terminating:Wait** state
- Monitor the **Terminating:Wait** state using EventBridge
- Trigger a SSM Automation Document to perform the actions on the instance before termination



Question 15:

A company is using multiple AWS accounts. The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A. The company's applications and databases are running in Account B.

A solutions architect will deploy a two-tier application in a new VPC. To simplify the configuration, the db.example.com CNAME record set for the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53.

During deployment, the application failed to start. Troubleshooting revealed that db.example.com is not resolvable on the Amazon EC2 instance. The solutions architect confirmed that the record set was created correctly in Route 53.

Which combination of steps should the solutions architect take to resolve this issue? (Choose two.)

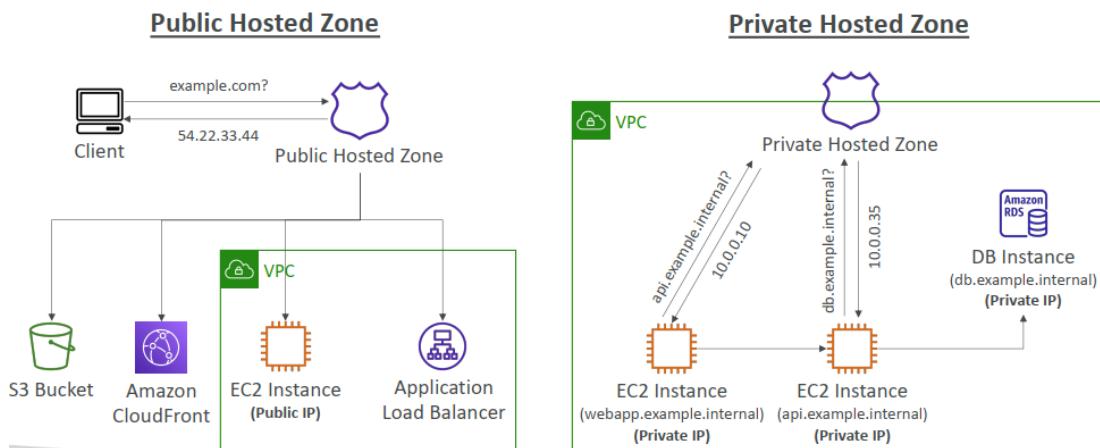
- Deploy the database on a separate EC2 instance in the new VPC. Create a record set for the instance's private IP in the private hosted zone.
- Use SSH to connect to the application tier EC2 instance. Add an RDS endpoint IP address to the /etc/resolv.conf file.
- Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B.
- Create a private hosted zone for the example com domain in Account B. Configure Route 53 replication between AWS accounts.
- Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization in Account A.

C and E

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-associate-vpcs-different-accounts.html>

<https://repost.aws/knowledge-center/route53-private-hosted-zone>

Route 53 – Public vs. Private Hosted Zones



To associate an Amazon VPC and a private hosted zone that you created with different AWS accounts

1. Using the account that created the hosted zone, authorize the association of the VPC with the private hosted zone by using one of the following methods:

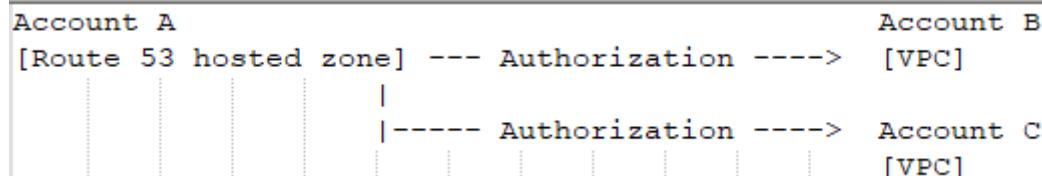
- AWS CLI – See [create-vpc-association-authorization](#) in the AWS CLI Command Reference
- AWSSDK or AWS Tools for Windows PowerShell – See the applicable documentation on the [AWS Documentation](#) page
- Amazon Route 53 API – See [CreateVPCAssociationAuthorization](#) in the Amazon Route 53 API Reference

Note the following:

- If you want to associate multiple VPCs that you created with one account with a hosted zone that you created with a different account, you must submit one authorization request for each VPC.
- When you authorize the association, you must specify the hosted zone ID, so the private hosted zone must already exist.
- You can't use the Route 53 console either to authorize the association of a VPC with a private hosted zone or to make the association.

2. Using the account that created the VPC, associate the VPC with the hosted zone. As with authorizing the association, you can use the AWS SDK, Tools for Windows PowerShell, the AWS CLI, or the Route 53 API. If you're using the API, use the [AssociateVPCWithHostedZone](#) action.

3. Recommended – Delete the authorization to associate the VPC with the hosted zone. Deleting the authorization does not affect the association, it just prevents you from reassociating the VPC with the hosted zone in the future. If you want to reassociate the VPC with the hosted zone, you'll need to repeat steps 1 and 2 of this procedure.



Question 16:

A company used Amazon EC2 instances to deploy a web fleet to host a blog site. The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto Scaling group. The web application stores all blog content on an Amazon EFS volume.

The company recently added a feature for bloggers to add video to their posts, attracting 10 times the previous user traffic. At peak times of day, users report buffering and timeout issues while attempting to reach the site or watch videos.

Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?

- A. Reconfigure Amazon EFS to enable maximum I/O.
- B. Update the blog site to use instance store volumes for storage. Copy the site contents to the volumes at launch and to Amazon S3 at shutdown.
- C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
- D. Set up an Amazon CloudFront distribution for all site contents, and point the distribution at the ALB.

C

Amazon CloudFront is a content delivery network (CDN) that can be used to deliver content to users with low latency and high data transfer speeds. By configuring a CloudFront distribution for the blog site and pointing it at an S3 bucket, the videos can be cached at edge locations closer to users, reducing buffering and timeout issues. Additionally, S3 is designed for scalable storage and can handle high levels of user traffic. Migrating the videos from EFS to S3, would also improve the performance and scalability of the website.

Question 17:

A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region. The company's on-premises network uses the connection to communicate with the company's resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC.

A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions.

Which solution meets these requirements?

- A. Provision a Direct Connect gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway. Connect the Direct Connect gateway to the single VPC.
- B. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
- C. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the single VPC.

D. Provision a transit gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway. Associate the transit gateway with the single VPC.

A

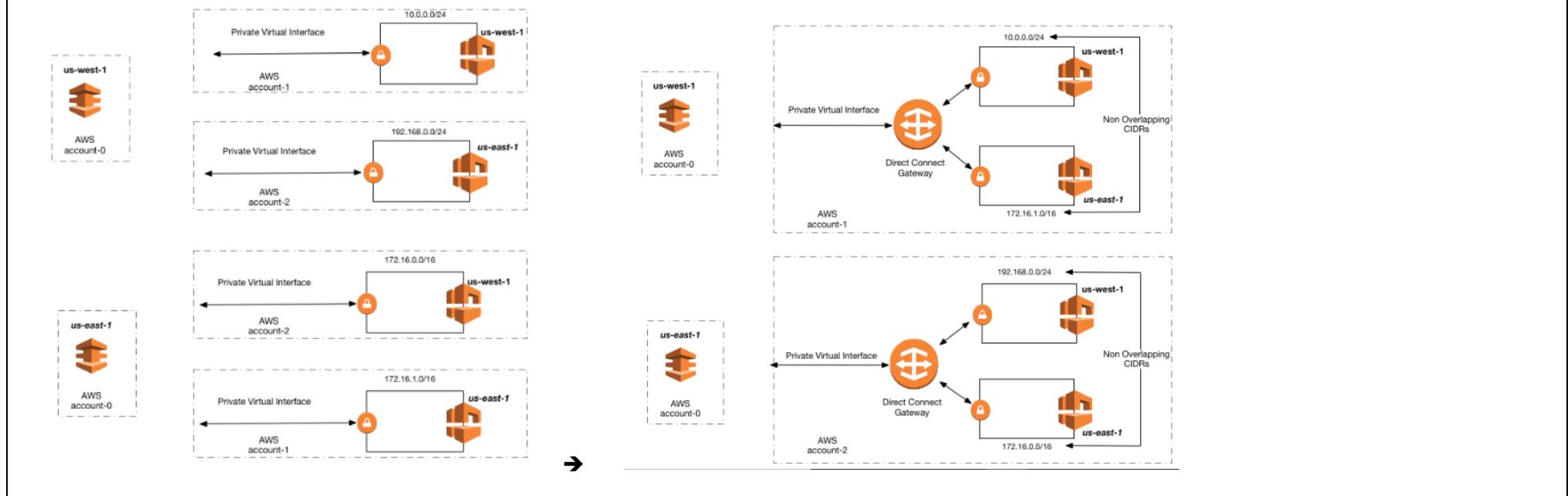
<https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/>

Option A - This option might work however it is missing a step: Connecting the Direct Connect Gateway to a Virtual Private Gateway in the single VPC (and any VPC in a new region)

Option B - This option will not work: It does not allow to grow into new regions and it does not create a redundant link

Option C - This option will not work: Using a Public Virtual interface does not connect VPC resources to on-premise

Option D - This option might work however it is missing multiple steps: Each VPC will require its own Transit Gateway. Each Transit Gateway will connect through an association with Direct Connect gateway. Each Direct Connect connection will connect to the Direct Connect Gateway using a Transit VIF.



Question 18:

A company has a web application that allows users to upload short videos. The videos are stored on Amazon EBS volumes and analyzed by custom recognition software for categorization.

The website contains static content that has variable traffic with peaks in certain months. The architecture consists of Amazon EC2 instances running in an Auto Scaling group for the web application and EC2 instances running in an Auto Scaling group to process an Amazon SQS queue. The company wants to re-architect the application to reduce operational overhead using AWS managed services where possible and remove dependencies on third-party software.

Which solution meets these requirements?

- A. Use Amazon ECS containers for the web application and Spot instances for the Auto Scaling group that processes the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.
- B. Store the uploaded videos in Amazon EFS and mount the file system to the EC2 instances for the web application. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- C. Host the web application in Amazon S3. Store the uploaded videos in Amazon S3. Use S3 event notification to publish events to the SQS queue. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- D. Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the web application and launch a worker environment to process the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.

C.

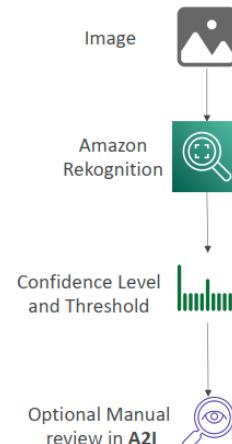
Amazon Rekognition



- Find objects, people, text, scenes in images and videos using ML
- Facial analysis phân tích khuôn mặt and facial search to do user verification, people counting
- Create a database of “familiar faces” or compare against celebrities
- Use cases:
 - Labeling
 - Content Moderation Kiểm duyệt nội dung
 - Text Detection
 - Face Detection and Analysis (gender, age range, emotions...)
 - Face Search and Verification
 - Celebrity Recognition
 - Pathing (ex: for sports game analysis)

Amazon Rekognition – Content Moderation

- phát hiện nội dung không phù hợp, không mong muốn hoặc gây khó chịu
- Detect content that is inappropriate, unwanted, or offensive (image and videos)
- Used in social media, broadcast media, advertising, and e-commerce situations to create a safer user experience
- Set a Minimum Confidence Threshold for items that will be flagged
- Flag sensitive content for manual review in Amazon Augmented AI (A2I)
- Help comply with regulations



Question 19:

A company has a serverless application comprised of Amazon CloudFront, Amazon API Gateway, and AWS Lambda functions. The current deployment process of the application code is to create a new version number of the Lambda function and run an AWS CLI script to update. If the new function version has errors, another CLI script reverts by deploying the previous working version of the function. The company would like to decrease the time to deploy new versions of the application logic provided by the Lambda functions, and also reduce the time to detect and revert when errors are identified.

How can this be accomplished?

- Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function. For changes to Lambda, create an AWS CloudFormation change set and deploy; if errors are triggered, revert the AWS CloudFormation change set to the previous version.
- Use AWS SAM and built-in AWS CodeDeploy to deploy the new Lambda version, gradually shift traffic to the new version, and use pre-traffic and post-traffic test functions to verify code. Rollback if Amazon CloudWatch alarms are triggered.
- Refactor the AWS CLI scripts into a single script that deploys the new Lambda version. When deployment is completed, the script tests execute. If errors are detected, revert to the previous Lambda version.
- Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version. Change the CloudFront origin to the new API Gateway endpoint, monitor errors and if detected, change the AWS CloudFront origin to the previous API Gateway endpoint.

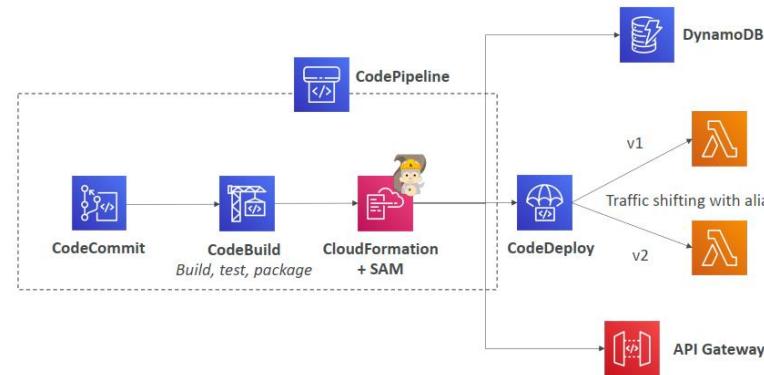
B

AWS SAM - Serverless Application Model



- SAM = Serverless Application Model
- Framework for developing and deploying serverless applications
- All the configuration is YAML code. Examples:
 - Lambda Functions (AWS::Serverless::Function)
 - DynamoDB tables (AWS::Serverless::SimpleTable)
 - API Gateway (AWS::Serverless::API)
 - StepFunction - State Machine (AWS::Serverless::StateMachine)
- SAM can help you to run Lambda, API Gateway, DynamoDB locally
- SAM can use CodeDeploy to deploy Lambda functions (traffic shifting)
- Leverages CloudFormation in the backend

CICD Architecture for SAM



PreTraffic: Before traffic shifting starts, CodeDeploy invokes the pre-traffic hook Lambda function. This Lambda function must call back to CodeDeploy and indicate success or failure. If the function fails, it aborts and reports a failure back to AWS CloudFormation. If the function succeeds, CodeDeploy proceeds to traffic shifting.

PostTraffic: After traffic shifting completes, CodeDeploy invokes the post-traffic hook Lambda function. This is similar to the pre-traffic hook, where the function must call back to CodeDeploy to report a success or failure. Use post-traffic hooks to run integration tests or other validation actions.

Question 20:

A company is planning to store a large number of archived documents and make the documents available to employees through the corporate intranet. Employees will access the system by connecting through a client VPN service that is attached to a VPC. The data must not be accessible to the public.

The documents that the company is storing are copies of data that is held on physical media elsewhere. The number of requests will be low. Availability and speed of retrieval are not concerns of the company.

Which solution will meet these requirements at the LOWEST cost?

- Create an Amazon S3 bucket. Configure the S3 bucket to use the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class as default. Configure the S3 bucket for website hosting. Create an S3 interface endpoint. Configure the S3 bucket to allow access only through that endpoint.
- Launch an Amazon EC2 instance that runs a web server. Attach an Amazon Elastic File System (Amazon EFS) file system to store the archived data in the EFS One Zone-Infrequent Access (EFS One Zone-IA) storage class. Configure the instance security groups to allow access only from private networks.
- Launch an Amazon EC2 instance that runs a web server. Attach an Amazon Elastic Block Store (Amazon EBS) volume to store the archived data. Use the Cold HDD (sc1) volume type. Configure the instance security groups to allow access only from private networks.
- Create an Amazon S3 bucket. Configure the S3 bucket to use the S3 Glacier Deep Archive storage class as default. Configure the S3 bucket for website hosting. Create an S3 interface endpoint. Configure the S3 bucket to allow access only through that endpoint.

A.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>

D incorrect because if use S3 Glacier Deep Archive will take time up to 12 hours for retrieval data.

the company is storing are copies of data that is held on physical media elsewhere ➔ storing secondary backup copies of on-premise data. ➔ S3 One Zone-IA

S3 Storage Classes – Infrequent Access

- For data that is less frequently accessed, but requires rapid access when needed
- Lower cost than S3 Standard
- Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
 - 99.9% Availability
 - Use cases: Disaster Recovery, backups
- Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)
 - High durability (99.99999999%) in a single AZ; data lost when AZ is destroyed
 - 99.5% Availability
 - Use Cases: Storing secondary backup copies of on-premise data, or data you can recreate



Amazon S3 Glacier Storage Classes

- **Low-cost** object storage meant for archiving / backup
- Pricing: price for storage + object retrieval cost
- **Amazon S3 Glacier Instant Retrieval**
 - truy suất 1 phần nghìn giây, dùng cho truy cập dữ liệu 1 quý 1 lần Millisecond retrieval, great for data accessed once a quarter
 - Minimum storage duration of 90 days Lưu trữ tối thiểu 90 ngày
- **Amazon S3 Glacier Flexible Retrieval** (formerly Amazon S3 Glacier):
 - Expedited (1 to 5 minutes), Standard (3 to 5 hours), Bulk (5 to 12 hours) – free
 - Minimum storage duration of 90 days
- **Amazon S3 Glacier Deep Archive** – for long term storage:
 - Standard (12 hours), Bulk (48 hours)
 - Minimum storage duration of 180 days

Question 21:

A company is using an on-premises Active Directory service for user authentication. The company wants to use the same authentication service to sign in to the company's AWS accounts, which are using AWS Organizations. AWS Site-to-Site VPN connectivity already exists between the on-premises environment and all the company's AWS accounts.

The company's security policy requires conditional access to the accounts based on user groups and roles. User identities must be managed in a single location.

Which solution will meet these requirements?

- A. Configure AWS IAM Identity Center (AWS Single Sign-On) to connect to Active Directory by using SAML 2.0. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using attribute-based access controls (ABACs).
- B. Configure AWS IAM Identity Center (AWS Single Sign-On) by using IAM Identity Center as an identity source. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using IAM Identity Center permission sets.
- C. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use a SAML 2.0 identity provider. Provision IAM users that are mapped to the federated users. Grant access that corresponds to appropriate groups in Active Directory. Grant access to the required AWS accounts by using cross-account IAM users.
- D. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use an OpenID Connect (OIDC) identity provider. Provision IAM roles that grant access to the AWS account for the federated users that correspond to appropriate groups in Active Directory. Grant access to the required AWS accounts by using cross-account IAM roles.

A

based on user groups and roles → attribute-based access controls (ABACs)

AWS IAM Identity Center
(successor to AWS Single Sign-On)



- One login (single sign-on) for all your
 - AWS accounts in AWS Organizations
 - Business cloud applications (e.g., Salesforce, Box, Microsoft 365, ...)
 - SAML2.0-enabled applications
 - EC2 Windows Instances
- Identity providers
 - Built-in identity store in IAM Identity Center
 - 3rd party: Active Directory (AD), OneLogin, Okta...



AWS IAM Identity Center

Fine-grained Permissions and Assignments



- Multi-Account Permissions

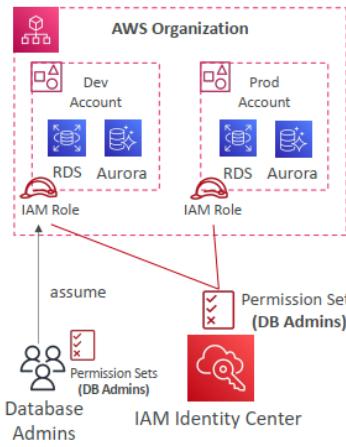
- Manage access across AWS accounts in your AWS Organization
- Permission Sets – a collection of one or more IAM Policies assigned to users and groups to define AWS access

- Application Assignments

- SSO access to many SAML 2.0 business applications (Salesforce, Box, Microsoft 365, ...)
- Provide required URLs, certificates, and metadata

- Attribute-Based Access Control (ABAC)

- Fine-grained permissions based on users' attributes stored in IAM Identity Center Identity Store
- Example: cost center, title, locale, ...
- Use case: Define permissions once, then modify AWS access by changing the attributes



Question 22:

A software company has deployed an application that consumes a REST API by using Amazon API Gateway, AWS Lambda functions, and an Amazon DynamoDB table. The application is showing an increase in the number of errors during PUT requests. Most of the PUT calls come from a small number of clients that are authenticated with specific API keys.

A solutions architect has identified that a large number of the PUT requests originate from one client. The API is noncritical, and clients can tolerate retries of unsuccessful calls. However, the errors are displayed to customers and are causing damage to the API's reputation.

What should the solutions architect recommend to improve the customer experience?

- Implement retry logic with exponential backoff and irregular variation in the client application. Ensure that the errors are caught and handled with descriptive error messages.
- Implement API throttling through a usage plan at the API Gateway level. Ensure that the client application handles code 429 replies without error.
- Turn on API caching to enhance responsiveness for the production stage. Run 10-minute load tests. Verify that the cache capacity is appropriate for the workload.
- Implement reserved concurrency at the Lambda function level to provide the resources that are needed during sudden increases in traffic.

B

API throttling is a technique that can be used to control the rate of requests to an API. This can be useful in situations where a small number of clients are making a large number of requests, which is causing errors. By implementing API throttling through a usage plan at the API Gateway level, the solutions architect can limit the number of requests that a client can make, which will help to reduce the number of errors.

It's important that the client application handles the code 429 replies without error, this will help to improve the customer experience by reducing the number of errors that are displayed to customers. Additionally, it will prevent the API's reputation from being damaged by the errors.

API Gateway – Usage Plans & API Keys

- If you want to make an API available as an offering (\$) to your customers
- **Usage Plan:**
 - who can access one or more deployed API stages and methods
 - how much and how fast they can access them
 - uses API keys to identify API clients and meter access
 - configure throttling limits and quota limits that are enforced on individual client
- **API Keys:**
 - alphanumeric string values to distribute to your customers
 - Ex: WBjHxNtoAb4WPKBC7cGm64CBiblb24b4jt8jjHo9
 - Can use with usage plans to control access
 - Throttling limits are applied to the API keys
 - Quotas limits is the overall number of maximum requests
- **429 Too Many Requests:**
 - Account level throttling across all APIs in a region
 - Clients must implement retry mechanisms

Question 23:

A company is running a data-intensive application on AWS. The application runs on a cluster of hundreds of Amazon EC2 instances. A shared file system also runs on several EC2 instances that store 200 TB of data. The application reads and modifies the data on the shared file system and generates a report. The job runs once monthly, reads a subset of the files from the shared file system, and takes about 72 hours to complete. The compute instances scale in an Auto Scaling group, but the instances that host the shared file system run continuously. The compute and storage instances are all in the same AWS Region.

A solutions architect needs to reduce costs by replacing the shared file system instances. The file system must provide high performance access to the needed data for the duration of the 72-hour run.

Which solution will provide the LARGEST overall cost reduction while meeting these requirements?

A. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Intelligent-Tiering storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using lazy loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.

B. Migrate the data from the existing shared file system to a large Amazon Elastic Block Store (Amazon EBS) volume with Multi-Attach enabled. Attach the EBS volume to each of the instances by using a user data script in the Auto Scaling group launch template. Use the EBS volume as the shared storage for the duration of the job. Detach the EBS volume when the job is complete

C. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Standard storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using batch loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.

D. Migrate the data from the existing shared file system to an Amazon S3 bucket. Before the job runs each month, use AWS Storage Gateway to create a file gateway with the data from Amazon S3. Use the file gateway as the shared storage for the job. Delete the file gateway when the job is complete.

A

<https://aws.amazon.com/blogs/storage/new-enhancements-for-moving-data-between-amazon-fsx-for-lustre-and-amazon-s3/>

S3 Intelligent-Tiering

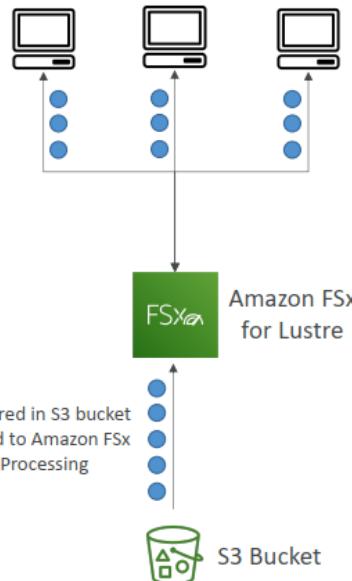


phi theo dõi hàng tháng và tự động phân cấp nhỏ

- Small monthly monitoring and auto-tiering fee
- Moves objects automatically between Access Tiers based on usage
- There are no retrieval charges in S3 Intelligent-Tiering
- Frequent Access tier (automatic): default tier
- Infrequent Access tier (automatic): objects not accessed for 30 days
- Archive Instant Access tier (automatic): objects not accessed for 90 days
- Archive Access tier (optional): configurable from 90 days to 700+ days
- Deep Archive Access tier (optional): config. from 180 days to 700+ days

FSx for Lustre – Data Lazy Loading

- Any data processing job on Lustre with S3 as an input data source can be started without Lustre doing a full download of the dataset first
- Data is lazy loaded: only the data that is actually processed is loaded, meaning you can decrease your costs and latency
- Data is also loaded only once, therefore you reduce your requests on Amazon S3



FSx for Lustre là một dịch vụ quản lý hệ thống tệp Lustre được cung cấp bởi Amazon Web Services (AWS). Lazy loading là một tính năng quan trọng trong FSx for Lustre, cho phép tải dữ liệu từ hệ thống tệp tự động và hiệu quả khi cần thiết.

Khi bạn sử dụng FSx for Lustre với lazy loading, dữ liệu trên hệ thống tệp được lưu trữ trên network storage và chỉ được tải lên vào bộ nhớ đệm (cache) trên các node EC2 khi cần thiết. Khi một tệp hoặc một phần của tệp được yêu cầu, nó sẽ được tải lên bộ nhớ đệm và truy cập từ đó. Các tệp không được yêu cầu sẽ không được tải lên, giúp tiết kiệm không gian lưu trữ và tăng hiệu suất của hệ thống.

Điều này rất hữu ích trong các trường hợp khi không cần phải tải toàn bộ dữ liệu từ hệ thống tệp Lustre xuống các node EC2. Thay vào đó, chỉ những phần dữ liệu cần thiết được tải lên, giảm thiểu thời gian và băng thông mạng cần thiết cho việc truy cập dữ liệu.

Lazy loading trong FSx for Lustre giúp tối ưu hóa việc sử dụng tài nguyên và cải thiện hiệu suất truy cập dữ liệu từ hệ thống tệp Lustre.

Question 24:

A company is developing a new service that will be accessed using TCP on a static port. A solutions architect must ensure that the service is highly available, has redundancy across Availability Zones, and is accessible using the DNS name my.service.com, which is publicly accessible. The service must use fixed address assignments so other companies can add the addresses to their allow lists.

Assuming that resources are deployed in multiple Availability Zones in a single Region, which solution will meet these requirements?

- A. Create Amazon EC2 instances with an Elastic IP address for each instance. Create a Network Load Balancer (NLB) and expose the static TCP port. Register EC2 instances with the NLB. Create a new name server record set named my.service.com, and assign the Elastic IP addresses of the EC2 instances to the record set. Provide the Elastic IP addresses of the EC2 instances to the other companies to add to their allow lists.

B. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP addresses for the ECS cluster. Create a Network Load Balancer (NLB) and expose the TCP port. Create a target group and assign the ECS cluster name to the NLB. Create a new A record set named my.service.com, and assign the public IP addresses of the ECS cluster to the record set. Provide the public IP addresses of the ECS cluster to the other companies to add to their allow lists.

C. Create Amazon EC2 instances for the service. Create one Elastic IP address for each Availability Zone. Create a Network Load Balancer (NLB) and expose the assigned TCP port. Assign the Elastic IP addresses to the NLB for each Availability Zone. Create a target group and register the EC2 instances with the NLB. Create a new A (alias) record set named my.service.com, and assign the NLB DNS name to the record set.

D. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP address for each host in the cluster. Create an Application Load Balancer (ALB) and expose the static TCP port. Create a target group and assign the ECS service definition name to the ALB. Create a new CNAME record set and associate the public IP addresses to the record set. Provide the Elastic IP addresses of the Amazon EC2 instances to the other companies to add to their allow lists.

C

architect must ensure that the service is highly available, has redundancy across Availability Zones → Multi AZ
must use fixed address assignments → Elastic IP → NLB

Network Load Balancer (v2)



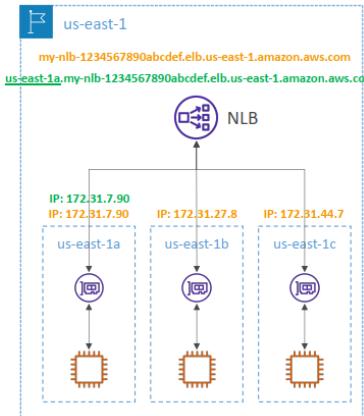
- Network load balancers (Layer 4) allow to:
 - Forward TCP & UDP traffic to your instances
 - Handle millions of requests per second
 - Less latency ~100 ms (vs 400 ms for ALB)
- NLB has one static IP per AZ, and supports assigning Elastic IP (helpful for whitelisting specific IP)
- NLB are used for extreme performance, TCP or UDP traffic
- Not included in the AWS free tier

Network Load Balancer – Zonal DNS Name

- Resolving Regional NLB DNS name returns the IP addresses for all NLB nodes in all enabled AZs
 - my-nlb-1234567890abcdef.elb.us-east-1.amazonaws.com

Zonal DNS Name

- NLB has DNS names for each of its nodes
- Use to determine the IP address of each node
 - us-east-1a.my-nlb-1234567890abcdef.elb.us-east-1.amazonaws.com
- Used to minimize latency and data transfer costs
- You need to implement app specific logic



Question 25:

A company uses an on-premises data analytics platform. The system is highly available in a fully redundant configuration across 12 servers in the company's data center.

The system runs scheduled jobs, both hourly and daily, in addition to one-time requests from users. Scheduled jobs can take between 20 minutes and 2 hours to finish running and have tight SLAs. The scheduled jobs account for 65% of the system usage. User jobs typically finish running in less than 5 minutes and have no SLA. The user jobs account for 35% of system usage. During system failures, scheduled jobs must continue to meet SLAs. However, user jobs can be delayed.

A solutions architect needs to move the system to Amazon EC2 instances and adopt a consumption-based model to reduce costs with no long-term commitments. The solution must maintain high availability and must not affect the SLAs.

Which solution will meet these requirements MOST cost-effectively?

- Split the 12 instances across two Availability Zones in the chosen AWS Region. Run two instances in each Availability Zone as On-Demand Instances with Capacity Reservations. Run four instances in each Availability Zone as Spot Instances.
- Split the 12 instances across three Availability Zones in the chosen AWS Region. In one of the Availability Zones, run all four instances as On-Demand Instances with Capacity Reservations. Run the remaining instances as Spot Instances.
- Split the 12 instances across three Availability Zones in the chosen AWS Region. Run two instances in each Availability Zone as On-Demand Instances with a Savings Plan. Run two instances in each Availability Zone as Spot Instances.
- Split the 12 instances across three Availability Zones in the chosen AWS Region. Run three instances in each Availability Zone as On-Demand Instances with Capacity Reservations. Run one instance in each Availability Zone as a Spot Instance.

D

MOST cost-effectively → mix On Demand and Spot Instance

Option A - This option might not work: it might not provide sufficient processing capacity for the batch jobs to meet the SLAs during outages. Moreover, 4 servers will not provide sufficient capacity to meet the SLAs of batch jobs

Option B - This option might not work: In case of an outage affecting the On-Demand instances there might not be enough processing capacity to meet batch job SLAs

Option C - This option will not meet the requirement not to make any long-term commitments

Option D - This option will work: There is enough sufficient processing capacity to meet the SLAs of batch jobs and keep processing One-off jobs

Question 26:

A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an encrypted file in Amazon S3. For the next version of the application, the security engineer wants to implement the following application design changes to improve security:

- The database must use strong, randomly generated passwords stored in a secure AWS managed service.
- The application resources must be deployed through AWS CloudFormation.
- The application must rotate credentials for the database every 90 days.

A solutions architect will generate a CloudFormation template to deploy the application.

Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead?

A. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.

B. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Create an AWS Lambda function resource to rotate the database password. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.

C. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.

D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days.

A

LEAST amount of operational overhead → A

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/cloudformation.html>

Option B is wrong. The ParameterStore::RotationSchedule resource does not exist in CloudFormation.

Option C is wrong. It does not meet the requirement because it does not use CloudFormation.

Option D is wrong. The AWS::AppSync::DataSource resource is what to create data sources for resolvers in AWS AppSync to connect to.

CloudFormation – Integration with Secrets Manager

```
Resources:
  # Secret resource with a randomly generated password in its SecureString JSON
  MyRDSDBInstanceRotationSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      GenerateSecretString:
        SecretStringTemplate: '{"username": "admin"}'
        GenerateStringKey: password
        PasswordLength: 16
        ExcludeCharacters: "\"@\\\""

  # RDS Instance resource. Its master username and password use dynamic references
  # to resolve values from Secrets Manager
  MyRDSDBInstance:
    Type: AWS::RDS::DBInstance
    Properties:
      DBInstanceClass: db.t2.micro
      Engine: mysql
      MasterUsername: !Sub "${{resolve:secretsmanager:${MyRDSDBInstanceRotationSecret}:username}}"
      MasterUserPassword: !Sub "${{resolve:secretsmanager:${MyRDSDBInstanceRotationSecret}:password}}"

  # SecretTargetAttachment resource which updates the referenced Secret with properties
  # about the referenced RDS instance
  SecretRDSDBInstanceAttachment:
    Type: AWS::SecretsManager::SecretTargetAttachment
    Properties:
      TargetType: AWS::RDS::DBInstance
      SecretId: !Ref MyRDSDBInstanceRotationSecret
      TargetId: !Ref MyRDSDBInstance
```

secret is generated

reference secret in RDS DB instance

link the secret to RDS DB instance

Question 27:

A company is storing data in several Amazon DynamoDB tables. A solutions architect must use a serverless architecture to make the data accessible publicly through a simple API over HTTPS. The solution must scale automatically in response to demand.

Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon API Gateway REST API. Configure this API with direct integrations to DynamoDB by using API Gateway's AWS integration type.
- B. Create an Amazon API Gateway HTTP API. Configure this API with direct integrations to Dynamo DB by using API Gateway's AWS integration type.
- C. Create an Amazon API Gateway HTTP API. Configure this API with integrations to AWS Lambda functions that return data from the DynamoDB tables.
- D. Create an accelerator in AWS Global Accelerator. Configure this accelerator with AWS Lambda@Edge function integrations that return data from the DynamoDB tables.
- E. Create a Network Load Balancer. Configure listener rules to forward requests to the appropriate AWS Lambda functions.

A and C

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-overview-developer-experience.html>
<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>

REST APIs and HTTP APIs are both RESTful API products. REST APIs support more features than HTTP APIs, while HTTP APIs are designed with minimal features so that they can be offered at a lower price. Choose REST APIs if you need features such as API keys, per-client throttling, request validation, AWS WAF integration, or private API endpoints. Choose HTTP APIs if you don't need the features included with REST APIs.

The following sections summarize core features that are available in REST APIs and HTTP APIs. When necessary, additional links are provided to navigate between the REST API and HTTP API sections of the API Gateway Developer Guide.

Endpoint type

The endpoint type refers to the endpoint that API Gateway creates for your API.

For more information, see [API endpoint types for REST APIs in API Gateway](#).

Endpoint types	REST API	HTTP API
Edge-optimized	Yes	No
Regional	Yes	Yes
Private	Yes	No

Security

API Gateway provides a number of ways to protect your API from certain threats, like malicious actors or spikes in traffic. To learn more, see [Protect your REST APIs in API Gateway](#) and [Protect your HTTP APIs in API Gateway](#).

Security features	REST API	HTTP API
Mutual TLS authentication	Yes	Yes
Certificates for backend authentication	Yes	No
AWS WAF	Yes	No

API management

Choose REST APIs if you need API management capabilities such as API keys and per-client rate limiting. For more information, see [Distribute your REST APIs to clients in API Gateway](#), [Custom domain name for REST APIs in API Gateway](#), and [Custom domain names for HTTP APIs in API Gateway](#).

Features	REST API	HTTP API
Custom domains	Yes	Yes
API keys	Yes	No
Per-client rate limiting	Yes	No
Per-client usage throttling	Yes	No

Question 28:

A company has registered 10 new domain names. The company uses the domains for online marketing. The company needs a solution that will redirect online visitors to a specific URL for each domain. All domains and target URLs are defined in a JSON document. All DNS records are managed by Amazon Route 53.

A solutions architect must implement a redirect service that accepts HTTP and HTTPS requests.

Which combination of steps should the solutions architect take to meet these requirements with the LEAST amount of operational effort? (Choose three.)

- A. Create a dynamic webpage that runs on an Amazon EC2 instance. Configure the webpage to use the JSON document in combination with the event message to look up and respond with a redirect URL.
- B. Create an Application Load Balancer that includes HTTP and HTTPS listeners.
- C. Create an AWS Lambda function that uses the JSON document in combination with the event message to look up and respond with a redirect URL.
- D. Use an Amazon API Gateway API with a custom domain to publish an AWS Lambda function.
- E. Create an Amazon CloudFront distribution. Deploy a Lambda@Edge function.
- F. Create an SSL certificate by using AWS Certificate Manager (ACM). Include the domains as Subject Alternative Names.

C,E,F

C: By creating an AWS Lambda function, the solution architect can use the JSON document to look up the target URLs for each domain and respond with the appropriate redirect URL. This way, the solution does not need to rely on a web server to handle the redirects, which reduces operational effort.

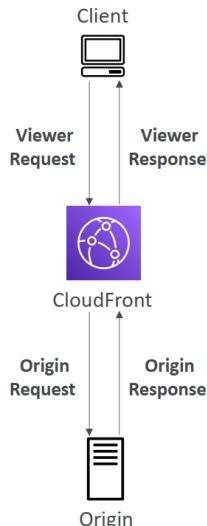
E: By creating an Amazon CloudFront distribution, the solution architect can deploy a Lambda@Edge function that can look up the target URLs for each domain and respond with the appropriate redirect URL. This way, CloudFront can handle the redirection, which reduces operational effort.

F: By creating an SSL certificate with ACM and including the domains as Subject Alternative Names, the solution architect can ensure that the redirect service can handle both HTTP and HTTPS requests, which is required by the company.

LEAST amount of operational effort → A, B are incorrect because they would require configuring and maintaining a web server to handle the redirects, which would increase operational effort.

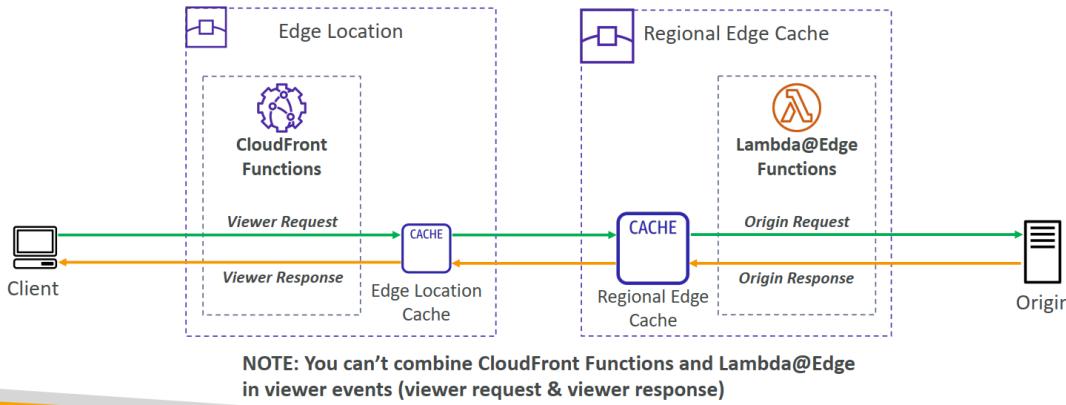
CloudFront – Lambda@Edge

- Lambda functions written in NodeJS or Python
- Scales to 1000s of requests/second
- Runs at the nearest Regional Edge Cache
- VM-based isolation
- Used to change CloudFront requests and responses:
 - Viewer Request – after CloudFront receives a request from a viewer
 - Origin Request – before CloudFront forwards the request to the origin
 - Origin Response – after CloudFront receives the response from the origin
 - Viewer Response – before CloudFront forwards the response to the viewer
- Author your functions in one AWS Region (us-east-1), then CloudFront replicates to its locations



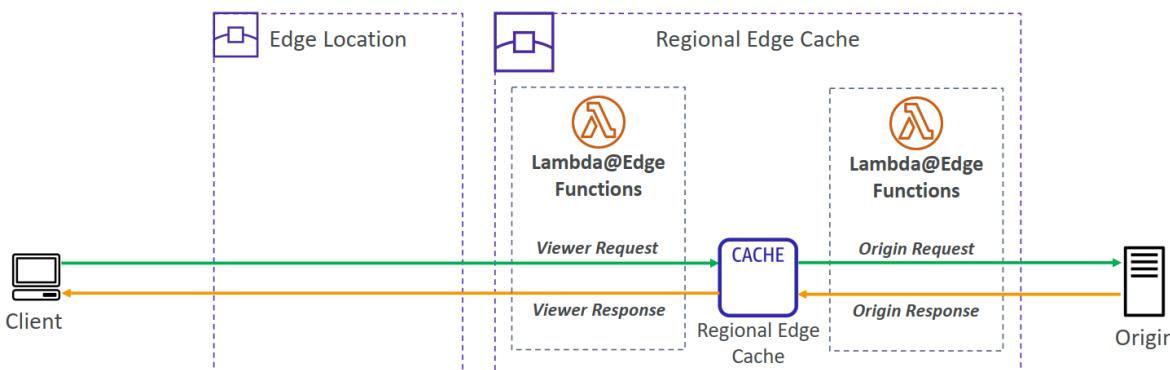
CloudFront Functions with Lambda@Edge

CloudFront Functions and Lambda@Edge can be used together



Using Lambda@Edge Only

Use when you need some of the capabilities of Lambda@Edge that aren't available with CloudFront Functions (e.g., longer execution time, network access, ...)



Question 29:

A company that has multiple AWS accounts is using AWS Organizations. The company's AWS accounts host VPCs, Amazon EC2 instances, and containers.

The company's compliance team has deployed a security tool in each VPC where the company has deployments. The security tools run on EC2 instances and send information to the AWS account that is dedicated for the compliance team. The company has tagged all the compliance-related resources with a key of "costCenter" and a value or "compliance".

The company wants to identify the cost of the security tools that are running on the EC2 instances so that the company can charge the compliance team's AWS account. The cost calculation must be as accurate as possible.

What should a solutions architect do to meet these requirements?

- A. In the management account of the organization, activate the costCenter user-defined tag. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account. Use the tag breakdown in the report to obtain the total cost for the costCenter tagged resources.
- B. In the member accounts of the organization, activate the costCenter user-defined tag. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account. Schedule a monthly AWS Lambda function to retrieve the reports and calculate the total cost for the costCenter tagged resources.
- C. In the member accounts of the organization activate the costCenter user-defined tag. From the management account, schedule a monthly AWS Cost and Usage Report. Use the tag breakdown in the report to calculate the total cost for the costCenter tagged resources.
- D. Create a custom report in the organization view in AWS Trusted Advisor. Configure the report to generate a monthly billing summary for the costCenter tagged resources in the compliance team's AWS account.

A

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/configurecostallocreport.html>

AWS Cost Allocation Tags

- With Tags we can track resources that relate to each other có thẻ theo dõi các resources có liên quan với nhau
- With Cost Allocation Tags we can enable detailed costing reports báo cáo chi phí chi tiết
- Just like Tags, but they show up as columns in Reports Hiển thị dạng cột
- AWS Generated Cost Allocation Tags
 - Automatically applied to the resource you create tự động áp dụng cho các tài nguyên đã tạo
 - Starts with Prefix aws: (e.g. aws: createdBy)
 - They're not applied to resources created before the activation không được áp dụng cho các tài nguyên tạo trước đó
- User tags
 - Defined by the user
 - Starts with Prefix user:
- Cost Allocation Tags just appear in the Billing Console
- Takes up to 24 hours for the tags to show up in the report

Mất 24 giờ để tags hiển thị trong báo cáo

Question 30:

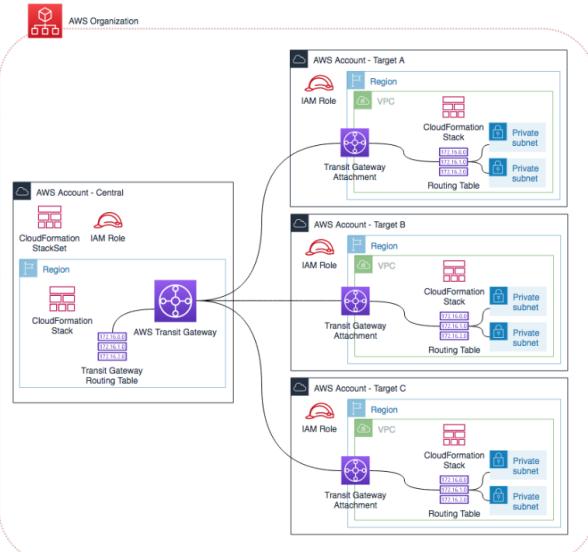
A company has 50 AWS accounts that are members of an organization in AWS Organizations. Each account contains multiple VPCs. The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account. Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.

Which combination of steps will meet these requirements? (Choose two.)

- A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager.
- B. From the management account, share the transit gateway with member accounts by using an AWS Organizations SCP.
- C. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a VPC transit gateway attachment in a member account. Associate the attachment with the transit gateway in the management account by using the transit gateway ID.
- D. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a peering transit gateway attachment in a member account. Share the attachment with the transit gateway in the management account by using a transit gateway service-linked role.
- E. From the management account, share the transit gateway with member accounts by using AWS Service Catalog.

A and C

<https://aws.amazon.com/ko/blogs/networking-and-content-delivery/automating-aws-transit-gateway-attachments-to-a-transit-gateway-in-a-central-account/>



Using a CloudFormation template, you can create a transit gateway in a central account and then share it with your organization using AWS Resource Access Manager (AWS RAM). You then can launch a stack set that automates the creation of a transit gateway attachment.

AWS Resource Access Manager (RAM)

- Share AWS resources that you own with other AWS accounts
- Share with any account or within your Organization
- Avoid resource duplication!
- **VPC Subnets**
 - Allow to have all the resources launched in the same subnets
 - Must be from the same AWS Organizations.
 - Cannot share security groups and default VPC
 - Participants can manage their own resources in there
 - Participants can't view, modify, delete resources that belong to other participants or the owner
- **AWS Transit Gateway**
- Route 53 (Resolver Rules, DNS Firewall Rule Groups)
- License Manager Configurations

AWS Resource Access Manager (RAM)

- Aurora DB Clusters
- ACM Private Certificate Authority
- CodeBuild Project
- EC2 (Dedicated Hosts, Capacity Reservation)
- AWS Glue (Catalog, Database, Table)
- AWS Network Firewall Policies
- AWS Resource Groups
- Systems Manager Incident Manager (Contacts, Response Plans)
- AWS Outposts (Outpost, Site)

Question 31:

An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy

indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement. The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers. Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access.

What is the MOST efficient way to design an architecture to meet these requirements?

- A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the PowerUserAccess managed policy to the role. Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.
- B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the AdministratorAccess managed policy to the role. Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
- C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
- D. Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developers. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Apply the SCP to all the shared services accounts in the organization.

C

<https://aws.amazon.com/blogs/awsmarketplace/controlling-access-to-a-well-architected-private-marketplace-using-iam-and-aws-organizations/>

AWS Marketplace là một dịch vụ của Amazon Web Services (AWS) cung cấp một nền tảng trực tuyến cho phép khách hàng tìm kiếm, so sánh, mua và triển khai các phần mềm và dịch vụ từ các nhà cung cấp độc lập (ISV - Independent Software Vendors) trên nền tảng AWS.

AWS Marketplace cung cấp một cách tiếp cận đơn giản và tiện lợi để tìm và sử dụng các ứng dụng, công cụ và dịch vụ phổ biến trên AWS. Nó hỗ trợ cả việc tìm kiếm các ứng dụng miễn phí và trả phí, từ các ứng dụng mã nguồn mở cho đến các giải pháp doanh nghiệp cao cấp.

Các đặc điểm chính của AWS Marketplace bao gồm:

Đa dạng và phong phú: AWS Marketplace cung cấp hàng ngàn ứng dụng và dịch vụ từ các nhà cung cấp khác nhau, bao gồm cả phần mềm ứng dụng, công cụ phân tích dữ liệu, giải pháp bảo mật, phần mềm dựa trên AI/ML và nhiều hơn nữa. Người dùng có thể tìm kiếm và chọn từ một loạt các tùy chọn.

Đánh giá và đánh giá: AWS Marketplace cung cấp đánh giá, đánh giá và bình luận từ người dùng khác, giúp bạn đưa ra quyết định thông minh khi chọn ứng dụng hoặc dịch vụ. Bạn có thể xem xét kinh nghiệm của người dùng trước đó để đánh giá chất lượng và hiệu suất của sản phẩm.

Tính linh hoạt và thanh toán dễ dàng: AWS Marketplace giúp bạn dễ dàng triển khai và quản lý các ứng dụng và dịch vụ bằng cách cung cấp các tùy chọn thanh toán linh hoạt, bao gồm cả các tùy chọn giá trả trước và trả sau. Bạn chỉ cần trả phí cho những gì bạn thực sự sử dụng.

Tích hợp và triển khai tự động: AWS Marketplace cho phép bạn triển khai ứng dụng và dịch vụ một cách tự động và tích hợp vào môi trường AWS hiện có của bạn. Bạn có thể sử dụng các công cụ quản lý như AWS CloudFormation và AWS Marketplace AMI để đơn giản hóa việc triển khai và quản lý.

Tóm lại, AWS Marketplace cung cấp một thị trường trực tuyến cho phép khách hàng tìm kiếm, so sánh và triển khai các ứng dụng và dịch vụ từ các nhà cung cấp độc lập trên nền tảng AWS.

Private Marketplace là một tính năng trong AWS Marketplace cho phép bạn tạo ra một thị trường riêng tư và tùy chỉnh cho tổ chức của mình. Thay vì sử dụng AWS Marketplace công khai, bạn có thể tạo ra một phiên bản riêng của nó được tùy chỉnh để phù hợp với nhu cầu và yêu cầu bảo mật của tổ chức.

- With Private Marketplace, you can choose specific products and services from AWS Marketplace to be displayed in your own private edition. This helps you control what's available in your organization and ensures that only approved products are used.

Một số tính năng và lợi ích của Private Marketplace bao gồm:

Tùy chỉnh: Bạn có thể tùy chỉnh Private Marketplace để chỉ hiển thị những sản phẩm và dịch vụ cụ thể từ AWS Marketplace. Bạn có thể chọn các sản phẩm đã được phê duyệt và kiểm tra bởi tổ chức của bạn hoặc các sản phẩm được phê duyệt bởi AWS.

Quản lý quyền truy cập: Private Marketplace cho phép bạn kiểm soát quyền truy cập vào phiên bản riêng của mình. Bạn có thể xác định người dùng nào có quyền truy cập vào thị trường riêng tư và quyền hạn của họ để mua và triển khai các sản phẩm.

Đơn giản hóa việc mua sắm: Private Marketplace tạo ra một trung tâm mua sắm tập trung cho tổ chức của bạn, giúp đơn giản hóa quy trình mua sắm và triển khai các sản phẩm. Người dùng chỉ cần truy cập vào Private Marketplace để tìm và chọn những sản phẩm đã được phê duyệt.

Tuân thủ chính sách nội bộ: Private Marketplace cho phép bạn thực hiện chính sách và tiêu chuẩn bảo mật nội bộ của tổ chức. Bạn có thể đảm bảo rằng chỉ những sản phẩm đáp ứng yêu cầu và tuân thủ chính sách bảo mật mới có thể được mua và triển khai.

Private Marketplace cung cấp sự linh hoạt và kiểm soát cho tổ chức của bạn khi sử dụng AWS Marketplace. Nó giúp bạn tạo ra một thị trường riêng tư và tùy chỉnh để quản lý việc mua sắm và triển khai phần mềm và dịch vụ trên nền tảng AWS.

Question 32:

A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2, Amazon S3, and Amazon DynamoDB. The developers account resides in a dedicated organizational unit (OU). The solutions architect has implemented the following SCP on the developers account:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowEC2",  
            "Effect": "Allow",  
            "Action": "ec2:*",  
            "Resource": "*"  
        },  
        {  
            "Sid": "AllowDynamoDB",  
            "Effect": "Allow",  
            "Action": "dynamodb:*",  
            "Resource": "*"  
        },  
        {  
            "Sid": "AllowS3",  
            "Effect": "Allow",  
            "Action": "s3:*",  
            "Resource": "*"  
        }  
    ]  
}
```

When this policy is deployed, IAM users in the developers account are still able to use AWS services that are not listed in the policy.

What should the solutions architect do to eliminate the developers' ability to use services outside the scope of this policy?

- A. Create an explicit deny statement for each AWS service that should be constrained.
- B. Remove the FullAWSAccess SCP from the developers account's OU.

- C. Modify the FullAWSAccess SCP to explicitly deny all services.
- D. Add an explicit deny statement using a wildcard to the end of the SCP.

B

AWS Organizations attaches an AWS managed SCP policy named FullAWSAccess which allows all services and actions. If this policy is removed and not replaced at any level of the organization, all OUs and accounts under that level would be blocked from taking any actions.
C is incorrect because all service will be deny.

Question 33:

A company is hosting a monolithic REST-based API for a mobile app on five Amazon EC2 instances in public subnets of a VPC. Mobile clients connect to the API by using a domain name that is hosted on Amazon Route 53. The company has created a Route 53 multivalue answer routing policy with the IP addresses of all the EC2 instances. Recently, the app has been overwhelmed by large and sudden increases to traffic. The app has not been able to keep up with the traffic.

A solutions architect needs to implement a solution so that the app can handle the new and varying load.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Separate the API into individual AWS Lambda functions. Configure an Amazon API Gateway REST API with Lambda integration for the backend. Update the Route 53 record to point to the API Gateway API.
- B. Containerize the API logic. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Run the containers in the cluster by using Amazon EC2. Create a Kubernetes ingress. Update the Route 53 record to point to the Kubernetes ingress.
- C. Create an Auto Scaling group. Place all the EC2 instances in the Auto Scaling group. Configure the Auto Scaling group to perform scaling actions that are based on CPU utilization. Create an AWS Lambda function that reacts to Auto Scaling group changes and updates the Route 53 record.
- D. Create an Application Load Balancer (ALB) in front of the API. Move the EC2 instances to private subnets in the VPC. Add the EC2 instances as targets for the ALB. Update the Route 53 record to point to the ALB.

A

needs to implement a solution so that the app can handle the new and varying load and LEAST operational overhead ➔ A

Question 34:

A company has created an OU in AWS Organizations for each of its engineering teams. Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts.

A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts.

Which solution meets these requirements?

- A. Create an AWS Cost and Usage Report (CUR) for each OU by using AWS Resource Access Manager. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- C. Create an AWS Cost and Usage Report (CUR) in each AWS Organizations member account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- D. Create an AWS Cost and Usage Report (CUR) by using AWS Systems Manager. Allow each team to visualize the CUR through Systems Manager OpsCenter dashboards.

B

<https://aws.amazon.com/blogs/mt/visualize-and-gain-insights-into-your-aws-cost-and-usage-with-cloud-intelligence-dashboards-using-amazon-quicksight/>
<https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html>

After you create a Cost and Usage Report, AWS sends your report to the Amazon S3 bucket that you specify. AWS updates your report at least once a day until your charges are finalized.

Your report files consist of a .csv file or a collection of .csv files and a manifest file. You can choose to configure your report data for integration with Amazon Athena, Amazon Redshift, or Amazon QuickSight.

Question 35:

A company is storing data on premises on a Windows file server. The company produces 5 GB of new data daily.

The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS.

Which data migration strategy should the company use?

- A. Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway.
- B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
- C. Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).
- D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).

B

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-fsx.html>

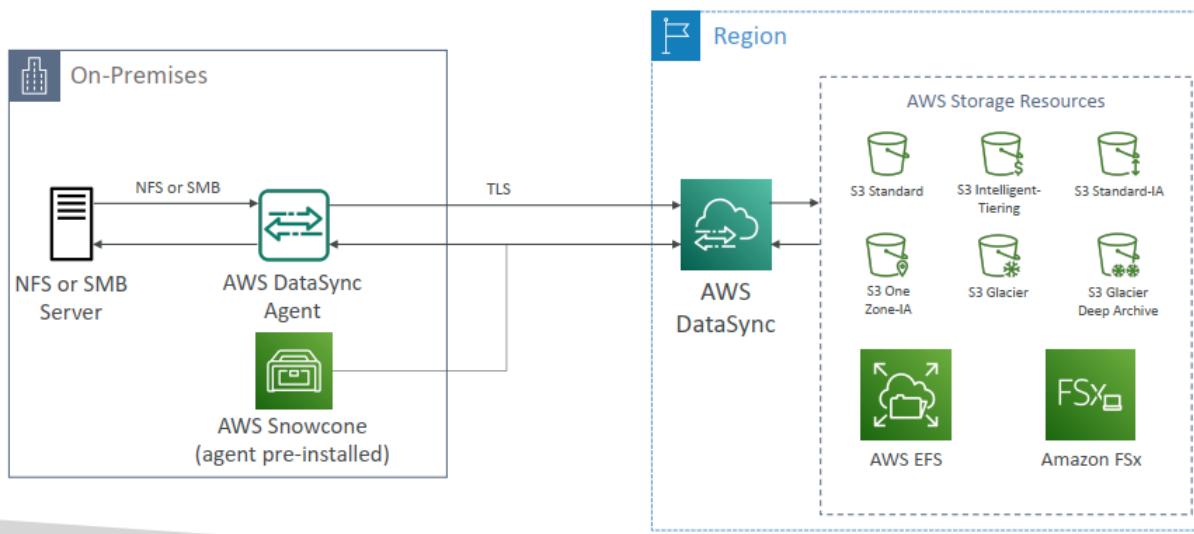
D is incorrect because EFS is linux

AWS DataSync



- Move large amount of data to and from
 - On-premises / other cloud to AWS (NFS, SMB, HDFS, S3 API...) – needs agent
 - AWS to AWS (different storage services) – no agent needed
- Can synchronize to:
 - Amazon S3 (any storage classes – including Glacier)
 - Amazon EFS
 - Amazon FSx (Windows, Lustre, NetApp, OpenZFS...)
- Replication tasks can be scheduled hourly, daily, weekly
- File permissions and metadata are preserved (NFS POSIX, SMB...)
- One agent task can use 10 Gbps, can setup a bandwidth limit

AWS DataSync NFS / SMB to AWS (S3, EFS, FSx...)



Question 36:

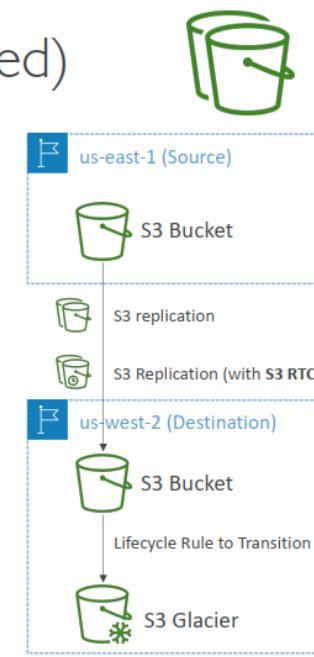
A company's solutions architect is reviewing a web application that runs on AWS. The application references static assets in an Amazon S3 bucket in the us-east-1 Region. The company needs resiliency across multiple AWS Regions. The company already has created an S3 bucket in a second Region.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Configure the application to write each object to both S3 buckets. Set up an Amazon Route 53 public hosted zone with a record set by using a weighted routing policy for each S3 bucket. Configure the application to reference the objects by using the Route 53 DNS name.
- B. Create an AWS Lambda function to copy objects from the S3 bucket in us-east-1 to the S3 bucket in the second Region. Invoke the Lambda function each time an object is written to the S3 bucket in us-east-1. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.
- C. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.
- D. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region. If failover is required, update the application code to load S3 objects from the S3 bucket in the second Region.

C

S3 – Replication (Versioning enabled)



- Cross Region Replication (CRR)
- Same Region Replication (SRR)
- Combine with Lifecycle Rules
- Helpful to reduce latency, disaster recovery, security
- **S3 Replication Time Control (S3 RTC)**
 - Replicates most objects that you upload to Amazon S3 in seconds, and 99.99% of those objects within 15 minutes
 - Helpful for compliance, DR, etc..

Question 37:

A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database. A solutions architect must design a scalable and highly available solution to meet the demand of 200,000 daily users.

Which steps should the solutions architect take to design an appropriate solution?

- A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.
- B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.
- C. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Region. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.
- D. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

B

High Availability: The use of an Application Load Balancer (ALB) and Amazon Aurora Multi-AZ deployment ensures high availability and fault tolerance for the web application and the MySQL database. The Multi-AZ setup for Aurora provides automatic failover.

Scalability: Using an EC2 Auto Scaling group across multiple Availability Zones allows the application to automatically scale to meet traffic demands. This is crucial for handling the surge in traffic from 200,000 daily users.

Deletion Policy: The Retain deletion policy for the Aurora MySQL DB cluster ensures that even if the CloudFormation stack is deleted, the database is retained, which is important for data preservation and recovery.

Route 53 Routing: Route 53 with an alias record provides efficient DNS routing, directing traffic to the ALB, which then distributes it to the EC2 instances. This ensures that users can access the application reliably.

Retaining Data on Deletes

Giữ lại dữ liệu khi xóa

- You can put a DeletionPolicy on any resource to control what happens when the CloudFormation template is deleted
- **DeletionPolicy=Retain:**
 - Specify on resources to preserve / backup in case of CloudFormation deletes
 - To keep a resource, specify Retain (works for any resource / nested stack)
- **DeletionPolicy=Snapshot:**
 - EBS Volume, ElastiCache Cluster, ElastiCache ReplicationGroup
 - RDS DBInstance, RDS DBCluster, Redshift Cluster
- **DeletePolicy=Delete (default behavior):**
 - Note: for AWS::RDS::DBCluster resources, the default policy is Snapshot
 - Note: to delete an S3 bucket, you need to first empty the bucket of its content

Question 38:

A company is using AWS Organizations to manage multiple AWS accounts. For security purposes, the company requires the creation of an Amazon Simple Notification Service (Amazon SNS) topic that enables integration with a third-party alerting system in all the Organizations member accounts.

A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of CloudFormation stacks. Trusted access has been enabled in Organizations.

What should the solutions architect do to deploy the CloudFormation StackSets in all AWS accounts?

- Create a stack set in the Organizations member accounts. Use service-managed permissions. Set deployment options to deploy to an organization. Use CloudFormation StackSets drift detection.
- Create stacks in the Organizations member accounts. Use self-service permissions. Set deployment options to deploy to an organization. Enable the CloudFormation StackSets automatic deployment.
- Create a stack set in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.
- Create stacks in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.

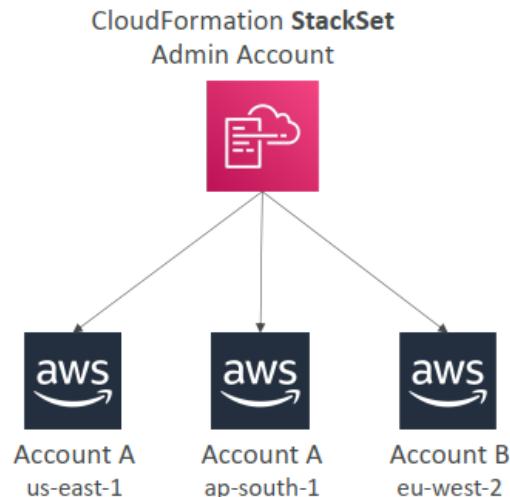
C

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-drift.html>

all account → management account.

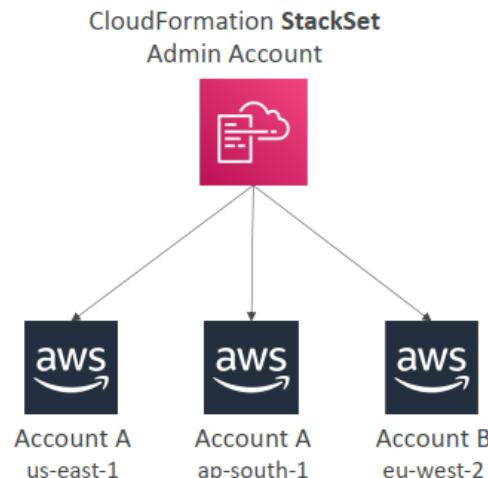
CloudFormation – StackSets

- Create, update, or delete stacks across multiple accounts and regions with a single operation
- Administrator account to create StackSets
- Trusted accounts to create, update, delete stack instances from StackSets
- When you update a stack set, all associated stack instances are updated throughout all accounts and regions
- Enable **Automatic Deployment** feature to automatically deploy to accounts in AWS Organization or OUs



CloudFormation – StackSets

- Create, update, or delete stacks across multiple accounts and regions with a single operation
- Administrator account to create StackSets
- Trusted accounts to create, update, delete stack instances from StackSets
- When you update a stack set, *all* associated stack instances are updated throughout all accounts and regions
- Enable **Automatic Deployment** feature to automatically deploy to accounts in AWS Organization or OUs



Question 39:

A company wants to migrate its workloads from on premises to AWS. The workloads run on Linux and Windows. The company has a large on-premises infrastructure that consists of physical machines and VMs that host numerous applications.

The company must capture details about the system configuration, system performance, running processes, and network connections of its on-premises workloads. The company also must divide the on-premises applications into groups for AWS migrations. The company needs recommendations for Amazon EC2 instance types so that the company can run its workloads on AWS in the most cost-effective manner.

Which combination of steps should a solutions architect take to meet these requirements? (Choose three.)

- Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs.
- Assess the existing applications by installing AWS Systems Manager Agent on the physical machines and VMs.
- Group servers into applications for migration by using AWS Systems Manager Application Manager.
- Group servers into applications for migration by using AWS Migration Hub.

E. Generate recommended instance types and associated costs by using AWS Migration Hub.

F. Import data about server sizes into AWS Trusted Advisor. Follow the recommendations for cost optimization.

A,D,E

<https://docs.aws.amazon.com/migrationhub/latest/ug/ec2-recommendations.html>

capture details about the system configuration, system performance, running processes, and network connections of its on-premises workloads → Application Discovery Agent

AWS Application Discovery Service

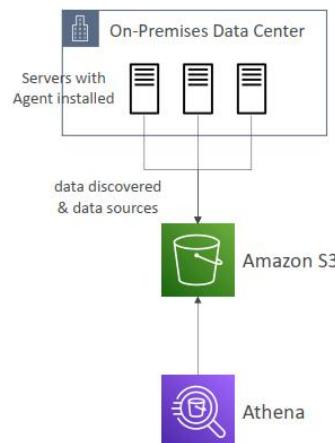


- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping are important for migrations
- **Agentless Discovery (AWS Agentless Discovery Connector)**
 - Open Virtual Appliance (OVA) package that can be deployed to a VMware host
 - VM inventory, configuration, and performance history such as CPU, memory, and disk usage
 - OS agnostic
- **Agent-based Discovery (AWS Application Discovery Agent)**
 - System configuration, system performance, running processes, and details of the network connections between systems
 - Supports Microsoft Server, Amazon Linux, Ubuntu, RedHat, CentOS, SUSE...
- Resulting data can be exported as CSV or viewed within AWS Migration Hub
- Data can be explored using pre-defined queries in Amazon Athena

AWS Application Discovery Service – Migration Hub Data Exploration

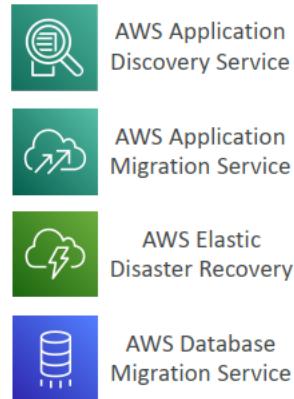


- Allows you to use Amazon Athena to analyze data collected from on-premises servers during discovery
- Data is automatically stored in S3 bucket at regular intervals
- Use Pre-defined or custom queries in Amazon Athena to analyze data
- Example: type of processes running on each server
- Ability to upload additional data sources such as Configuration Management Database (CMDB) exports
- Integrate Athena with QuickSight to visualize data



On-premises strategy with AWS

- Ability to download Amazon Linux 2 AMI as a VM (.iso format)
 - VMWare, KVM, VirtualBox (Oracle VM), Microsoft Hyper-V
- AWS Application Discovery Service
 - Gather information about your on-premises servers to plan a migration
 - Server utilization and dependency mappings
 - Track with AWS Migration Hub
- AWS Application Migration Service (MGN)
 - Replacing AWS Server Migration Services & CloudEndure Migration
 - Incremental replication of on-premises live servers to AWS
 - Migrates the entire VM into AWS
- AWS Elastic Disaster Recovery (DRS)
 - Replacing CloudEndure Disaster Recovery
 - Recover on-premises workloads onto AWS
- AWS Database Migration Service (DMS)
 - replicate on-premises => AWS , AWS => AWS, AWS => on-premises
 - Works with various database technologies (Oracle, MySQL, DynamoDB, etc..)



Question 40:

A company is hosting an image-processing service on AWS in a VPC. The VPC extends across two Availability Zones. Each Availability Zone contains one public subnet and one private subnet.

The service runs on Amazon EC2 instances in the private subnets. An Application Load Balancer in the public subnets is in front of the service. The service needs to communicate with the internet and does so through two NAT gateways. The service uses Amazon S3 for image storage. The EC2 instances retrieve approximately 1 TB of data from an S3 bucket each day.

The company has promoted the service as highly secure. A solutions architect must reduce cloud expenditures as much as possible without compromising the service's security posture or increasing the time spent on ongoing operations.

Which solution will meet these requirements?

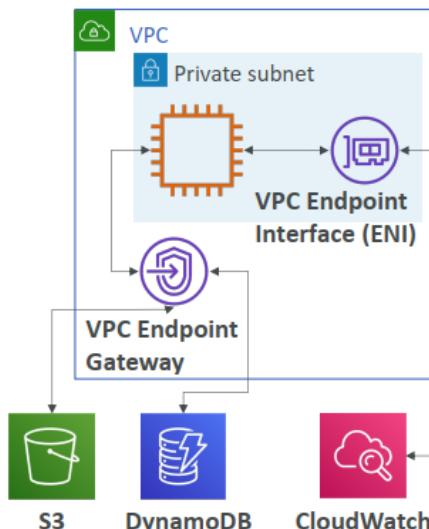
- Replace the NAT gateways with NAT instances. In the VPC route table, create a route from the private subnets to the NAT instances.
- Move the EC2 instances to the public subnets. Remove the NAT gateways.
- Set up an S3 gateway VPC endpoint in the VPC. Attach an endpoint policy to the endpoint to allow the required actions on the S3 bucket.
- Attach an Amazon Elastic File System (Amazon EFS) volume to the EC2 instances. Host the images on the EFS volume.

C

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables



Question 41:

A company recently deployed an application on AWS. The application uses Amazon DynamoDB. The company measured the application load and configured the RCUs and WCUs on the DynamoDB table to match the expected peak load. The peak load occurs once a week for a 4-hour period and is double the average load. The application load is close to the average load for the rest of the week. The access pattern includes many more writes to the table than reads of the table.

A solutions architect needs to implement a solution to minimize the cost of the table.

Which solution will meet these requirements?

- Use AWS Application Auto Scaling to increase capacity during the peak period. Purchase reserved RCUs and WCUs to match the average load.
- Configure on-demand capacity mode for the table.
- Configure DynamoDB Accelerator (DAX) in front of the table. Reduce the provisioned read capacity to match the new peak load on the table.
- Configure DynamoDB Accelerator (DAX) in front of the table. Configure on-demand capacity mode for the table.

A

<https://docs.aws.amazon.com/autoscaling/application/userguide/services-that-can-integrate-dynamodb.html>

<https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/#:~:text=You%20can%20approximate%20a%20blend,save%20money%20as%20reserved%20capacity>

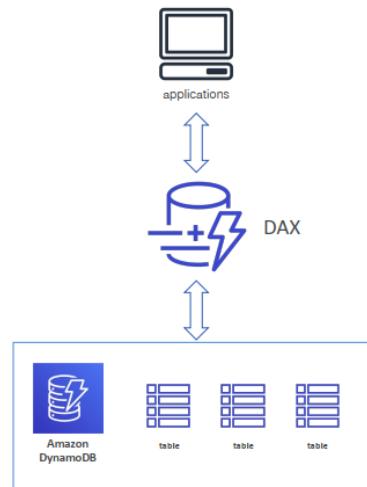
DynamoDB – in short



- NoSQL database, fully managed, massive scale (1,000,000 rps)
- Similar to Apache Cassandra (can migrate to DynamoDB)
- No disk space to provision, max object size is 400 KB
- Capacity: provisioned (WCU, RCU, & Auto Scaling) or on-demand
- Supports CRUD (Create Read Update Delete)
- Read: eventually or strong consistency
- Supports transactions across multiple tables (ACID support)
- Backups available, point in time recovery
- Table classes: Standard and Infrequent Access (IA)

DynamoDB - DAX

- DAX = DynamoDB Accelerator
Lien mạch
- Seamless cache for DynamoDB, no application re-write
- Writes go through DAX to DynamoDB
- Micro second latency for cached reads & queries
- Solves the Hot Key problem (too many reads)
- 5 minutes TTL for cache by default
- Up to 10 nodes in the cluster
- Multi AZ (3 nodes minimum recommended for production)
- Secure (Encryption at rest with KMS, VPC, IAM, CloudTrail...)



Question 42:

A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.

What is the MOST cost-effective migration recommendation?

- A. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in an Amazon S3 bucket.
- B. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files. Store the processed files in Amazon EFS. Shut down the EC2 instance after the task is complete.
- C. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in Amazon EFS.
- D. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. Use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. Scale the EC2 instances based on the SQS queue length. Store the processed files in an Amazon S3 bucket.

D

Each media file can take up to 1 hour to process → Can not use Lambda

Not A - Lambda max execution time is 15 minutes, image processing can take up to 1 hour

Not B - Amazon MQ is not needed (more expensive than SQS) and EFS is more expensive than S3

Not C - Amazon MQ is not needed (more expensive than SQS) and Lambda max execution time is 15 minutes, image processing can take up to 1 hour

D does the job with the lower cost thanks to SQS, S3 and EC2 Auto Scaling Group

Timeout

15 min 3 sec

 The maximum timeout is 15 minutes.

Question 43:

A company is using Amazon OpenSearch Service to analyze data. The company loads data into an OpenSearch Service cluster with 10 data nodes from an Amazon S3 bucket that uses S3 Standard storage. The data resides in the cluster for 1 month for read-only analysis. After 1 month, the company deletes the index that contains the data from the cluster. For compliance purposes, the company must retain a copy of all input data.

The company is concerned about ongoing costs and asks a solutions architect to recommend a new solution.

Which solution will meet these requirements MOST cost-effectively?

- A. Replace all the data nodes with UltraWarm nodes to handle the expected capacity. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.
- B. Reduce the number of data nodes in the cluster to 2. Add UltraWarm nodes to handle the expected capacity. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data. Transition the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy.
- C. Reduce the number of data nodes in the cluster to 2. Add UltraWarm nodes to handle the expected capacity. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data. Add cold storage nodes to the cluster. Transition the indexes from UltraWarm to cold storage. Delete the input data from the S3 bucket after 1 month by using an S3 Lifecycle policy.
- D. Reduce the number of data nodes in the cluster to 2. Add instance-backed data nodes to handle the expected capacity. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.

B

B is the most cost-effective solution as it reduces the number of data nodes in the cluster to 2 and adds UltraWarm nodes to handle the expected capacity. By configuring the indexes to transition to UltraWarm when OpenSearch Service ingests the data, the company can take advantage of the lower storage costs of UltraWarm. Additionally, by transitioning the input data to S3 Glacier Deep Archive after 1 month using an S3 Lifecycle policy, the company can further reduce costs by using the lower storage costs of S3 Glacier Deep Archive for long-term data retention.

Amazon S3 Glacier Storage Classes

- **Low-cost** object storage meant for archiving / backup
- Pricing: price for storage + object retrieval cost
- Amazon S3 Glacier Instant Retrieval
truy xuất 1 phần nghìn giây, dùng cho truy cập dữ liệu 1 quý 1 lần
 - Millisecond retrieval, great for data accessed once a quarter
 - Minimum storage duration of 90 days Lưu trữ tối thiểu 90 ngày
- Amazon S3 Glacier Flexible Retrieval (formerly Amazon S3 Glacier):
 - Expedited (1 to 5 minutes), Standard (3 to 5 hours), Bulk (5 to 12 hours) – free
 - Minimum storage duration of 90 days
- Amazon S3 Glacier Deep Archive – for long term storage:
 - Standard (12 hours), Bulk (48 hours)
 - Minimum storage duration of 180 days



Question 44:

A company has 10 accounts that are part of an organization in AWS Organizations. AWS Config is configured in each account. All accounts belong to either the Prod OU or the NonProd OU.

The company has set up an Amazon EventBridge rule in each AWS account to notify an Amazon Simple Notification Service (Amazon SNS) topic when an Amazon EC2 security group inbound rule is created with 0.0.0.0/0 as the source. The company's security team is subscribed to the SNS topic.

For all accounts in the NonProd OU, the security team needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Modify the EventBridge rule to invoke an AWS Lambda function to remove the security group inbound rule and to publish to the SNS topic. Deploy the updated rule to the NonProd OU.
- B. Add the vpc-sg-open-only-to-authorized-ports AWS Config managed rule to the NonProd OU.
- C. Configure an SCP to allow the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp condition key is not 0.0.0.0/0. Apply the SCP to the NonProd OU.
- D. Configure an SCP to deny the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp condition key is 0.0.0.0/0. Apply the SCP to the NonProd OU.

D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_syntax.html

Element	Purpose	Supported effects
Version	Specifies the language syntax rules to use for processing the policy.	Allow, Deny
Statement	Serves as the container for policy elements. You can have multiple statements in SCPs.	Allow, Deny
Statement ID (Sid)	(Optional) Provides a friendly name for the statement.	Allow, Deny
Effect	Defines whether the SCP statement allows or denies access to the IAM users and roles in an account.	Allow, Deny
Action	Specifies AWS service and actions that the SCP allows or denies.	Allow, Deny
NotAction	Specifies AWS service and actions that are exempt from the SCP. Used instead of the <code>Action</code> element.	Deny
Resource	Specifies the AWS resources that the SCP applies to.	Deny
Condition	Specifies conditions for when the statement is in effect.	Deny

Question 45:

A company hosts a Git repository in an on-premises data center. The company uses webhooks to invoke functionality that runs in the AWS Cloud. The company hosts the webhook logic on a set of Amazon EC2 instances in an Auto Scaling group that the company set as a target for an Application Load Balancer (ALB). The Git server calls the ALB for the configured webhooks. The company wants to move the solution to a serverless architecture.

Which solution will meet these requirements with the LEAST operational overhead?

- A. For each webhook, create and configure an AWS Lambda function URL. Update the Git servers to call the individual Lambda function URLs.
- B. Create an Amazon API Gateway HTTP API. Implement each webhook logic in a separate AWS Lambda function. Update the Git servers to call the API Gateway endpoint.
- C. Deploy the webhook logic to AWS App Runner. Create an ALB, and set App Runner as the target. Update the Git servers to call the ALB endpoint.
- D. Containerize the webhook logic. Create an Amazon Elastic Container Service (Amazon ECS) cluster, and run the webhook logic in AWS Fargate. Create an Amazon API Gateway REST API, and set Fargate as the target. Update the Git servers to call the API Gateway endpoint.

B

This solution sets up a serverless AWS Cloud environment that includes the following components:

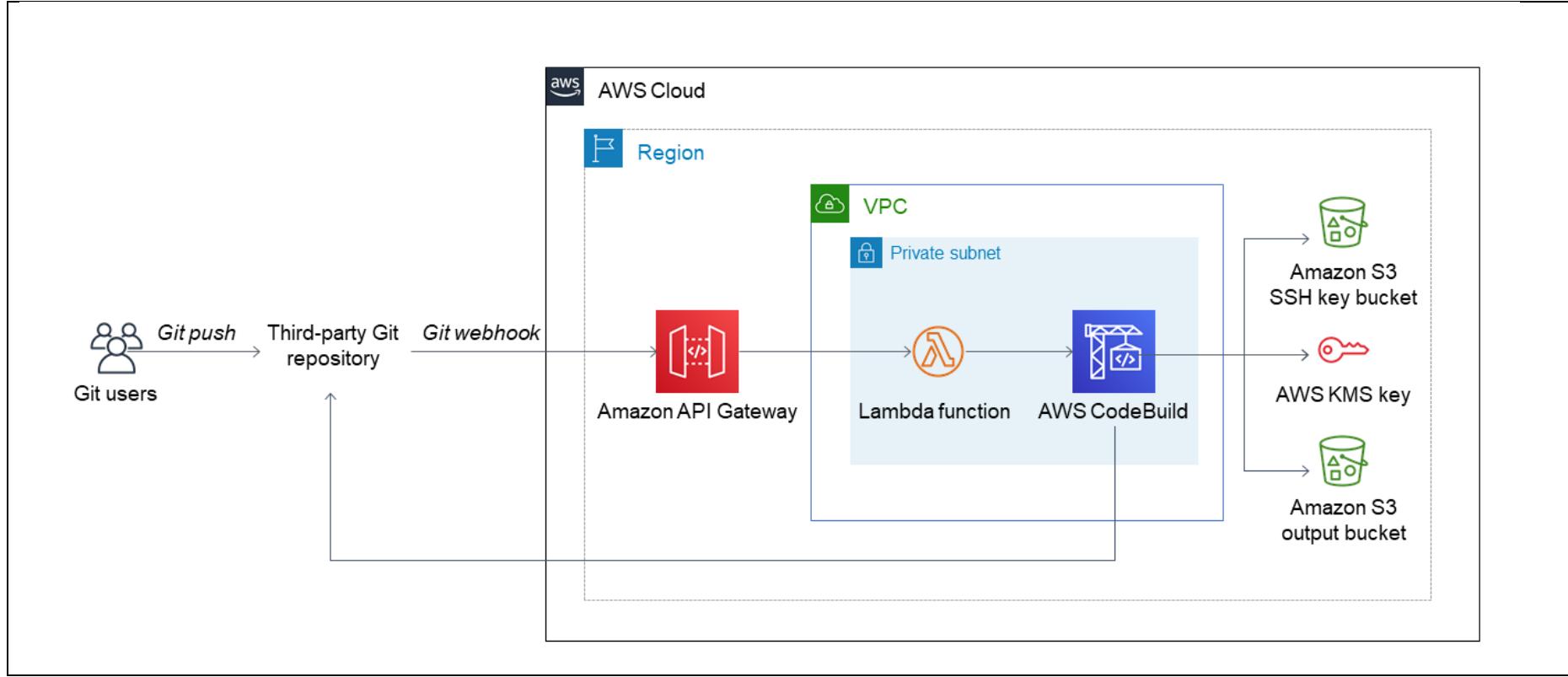
An Amazon API Gateway endpoint to receive Git webhook requests and forward them to AWS Lambda.

An AWS Lambda function to process Git webhook requests from API Gateway and invoke an AWS CodeBuild project.

An AWS CodeBuild project to connect to your Git service, then retrieve, zip, and upload the latest version of your Git repository to Amazon S3.

An AWS Key Management Service (AWS KMS) key to encrypt/decrypt SSH (Secure Shell) keys used by CodeBuild to connect to your Git repository using SSH. The SSH key pair is generated by a Lambda-backed AWS CloudFormation custom resource when the stack is deployed.

Two Amazon S3 buckets: one for Git repository contents, and another for encrypted SSH keys. A Lambda-backed AWS CloudFormation custom resource deletes the contents of the S3 buckets when you delete the stack. If you need backups, copy the S3 buckets before deleting the stack.



Question 46:

A company is planning to migrate 1,000 on-premises servers to AWS. The servers run on several VMware clusters in the company's data center. As part of the migration plan, the company wants to gather server metrics such as CPU details, RAM usage, operating system information, and running processes. The company then wants to query and analyze the data.

Which solution will meet these requirements?

- Deploy and configure the AWS Agentless Discovery Connector virtual appliance on the on-premises hosts. Configure Data Exploration in AWS Migration Hub. Use AWS Glue to perform an ETL job against the data. Query the data by using Amazon S3 Select.
- Export only the VM performance information from the on-premises hosts. Directly import the required data into AWS Migration Hub. Update any missing information in Migration Hub. Query the data by using Amazon QuickSight.
- Create a script to automatically gather the server information from the on-premises hosts. Use the AWS CLI to run the put-resource-attributes command to store the detailed server data in AWS Migration Hub. Query the data directly in the Migration Hub console.

D. Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3.

D

the company wants to gather server metrics such as CPU details, RAM usage, operating system information, and running processes → AWS Application Discovery Agent
then wants to query and analyze the data → S3 and Athena

AWS Application Discovery Service

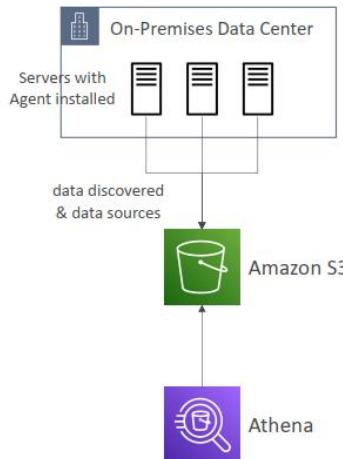


- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping are important for migrations
- **Agentless Discovery (AWS Agentless Discovery Connector)**
 - Open Virtual Appliance (OVA) package that can be deployed to a VMware host
 - VM inventory, configuration, and performance history such as CPU, memory, and disk usage
 - OS agnostic
- **Agent-based Discovery (AWS Application Discovery Agent)**
 - System configuration, system performance, running processes, and details of the network connections between systems
 - Supports Microsoft Server, Amazon Linux, Ubuntu, RedHat, CentOS, SUSE...
- Resulting data can be exported as CSV or viewed within AWS Migration Hub
- Data can be explored using pre-defined queries in Amazon Athena

AWS Application Discovery Service – Migration Hub Data Exploration



- Allows you to use Amazon Athena to analyze data collected from on-premises servers during discovery
- Data is automatically stored in S3 bucket at regular intervals
- Use Pre-defined or custom queries in Amazon Athena to analyze data
- Example: type of processes running on each server
- Ability to upload additional data sources such as Configuration Management Database (CMDB) exports
- Integrate Athena with QuickSight to visualize data



Question 47

A company is building a serverless application that runs on an AWS Lambda function that is attached to a VPC. The company needs to integrate the application with a new service from an external provider. The external provider supports only requests that come from public IPv4 addresses that are in an allow list.

The company must provide a single public IP address to the external provider before the application can start using the new service.

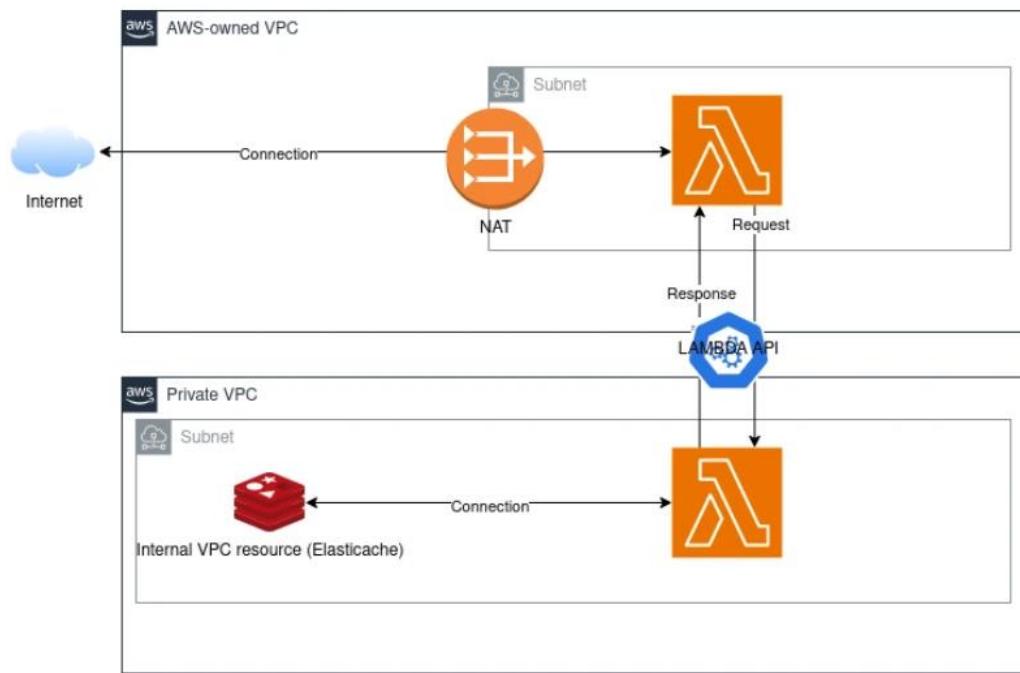
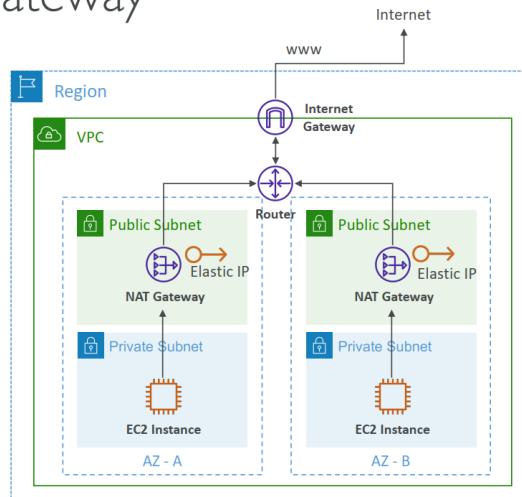
Which solution will give the application the ability to access the new service?

- Deploy a NAT gateway. Associate an Elastic IP address with the NAT gateway. Configure the VPC to use the NAT gateway.
- Deploy an egress-only internet gateway. Associate an Elastic IP address with the egress-only internet gateway. Configure the elastic network interface on the Lambda function to use the egress-only internet gateway.
- Deploy an internet gateway. Associate an Elastic IP address with the internet gateway. Configure the Lambda function to use the internet gateway.
- Deploy an internet gateway. Associate an Elastic IP address with the internet gateway. Configure the default route in the public VPC route table to use the internet gateway.

A

VPC Basics – NAT Gateway

- Managed NAT solution, bandwidth scales automatically
- Resilient to failure within a single AZ
- Must deploy multiple NAT Gateways in multiple AZ for HA
- Has an Elastic IP external services see the IP of the NAT Gateway as the source



Question 48:

A solutions architect has developed a web application that uses an Amazon API Gateway Regional endpoint and an AWS Lambda function. The consumers of the web application are all close to the AWS Region where the application will be deployed. The Lambda function only queries an Amazon Aurora MySQL database. The solutions architect has configured the database to have three read replicas.

During testing, the application does not meet performance requirements. Under high load, the application opens a large number of database connections. The solutions architect must improve the application's performance.

Which actions should the solutions architect take to meet these requirements? (Choose two.)

- A. Use the cluster endpoint of the Aurora database.
- B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.
- C. Use the Lambda Provisioned Concurrency feature.
- D. Move the code for opening the database connection in the Lambda function outside of the event handler.
- E. Change the API Gateway endpoint to an edge-optimized endpoint.

B, D

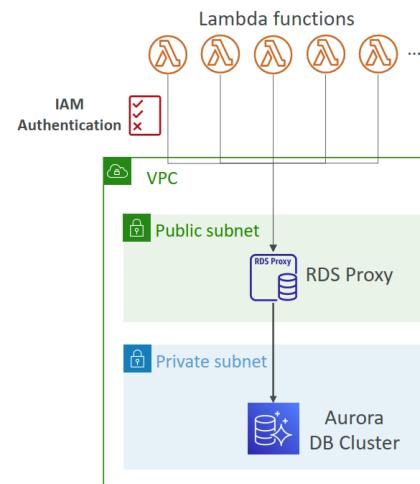
Lab: <https://awstut.com/en/2022/04/30/connect-to-rds-outside-of-lambda-handler-method-to-improve-performance-en/>

B. Using RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database can help improve the performance of the application by reducing the number of connections opened to the database. RDS Proxy manages the connection pool and routes incoming connections to the available read replicas, which can help with connection management and reduce the number of connections that need to be opened and closed.

D. Moving the code for opening the database connection in the Lambda function outside of the event handler can help to improve the performance of the application by allowing the database connection to be reused across multiple requests. This avoids the need to open and close a new connection for each request, which can be time-consuming and resource-intensive.

RDS Proxy for AWS Lambda

- When using Lambda functions with RDS, it opens and maintains a database connection
- This can result in a “TooManyConnections” exception
- With [RDS Proxy](#), you no longer need code that handles cleaning up idle connections and managing connection pools
- Supports IAM authentication or DB authentication, auto-scaling
- The Lambda function must have connectivity to the Proxy (public proxy => public Lambda, private proxy => Lambda in VPC)



Question 49:

A company is planning to host a web application on AWS and wants to load balance the traffic across a group of Amazon EC2 instances. One of the security requirements is to enable end-to-end encryption in transit between the client and the web server.

Which solution will meet this requirement?

- Place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Export the SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
- Associate the EC2 instances with a target group. Provision an SSL certificate using AWS Certificate Manager (ACM). Create an Amazon CloudFront distribution and configure it to use the SSL certificate. Set CloudFront to use the target group as the origin server.
- Place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Provision a third-party SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
- Place the EC2 instances behind a Network Load Balancer (NLB). Provision a third-party SSL certificate and install it on the NLB and on each EC2 instance. Configure the NLB to listen on port 443 and to forward traffic to port 443 on the instances.

C

Amazon-issued public certificates can't be installed on an EC2 instance. To enable end-to-end encryption, you must use a third-party SSL certificate.

Question 50

A company wants to migrate its data analytics environment from on premises to AWS. The environment consists of two simple Node.js applications. One of the applications collects sensor data and loads it into a MySQL database. The other application aggregates the data into reports. When the aggregation jobs run, some of the load jobs fail to run correctly.

The company must resolve the data loading issue. The company also needs the migration to occur without interruptions or changes for the company's customers.

What should a solutions architect do to meet these requirements?

- A. Set up an Amazon Aurora MySQL database as a replication target for the on-premises database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind a Network Load Balancer (NLB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the NLB.
- B. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Move the aggregation jobs to run against the Aurora MySQL database. Set up collection endpoints behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- C. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- D. Set up an Amazon Aurora MySQL database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as an Amazon Kinesis data stream. Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the Kinesis data stream.

C

migrate its data analytics environment from on premises to AWS → DMS

DMS – Database Migration Service



- Quickly and securely migrate databases to AWS, resilient, self healing
- The source database remains available during the migration
- Supports:
 - Homogeneous migrations: ex Oracle to Oracle
 - Heterogeneous migrations: ex Microsoft SQL Server to Aurora
- Continuous Data Replication using CDC
- You must create an EC2 instance to perform the replication tasks



DMS Sources and Targets

SOURCES:

- On-premises and EC2 instances databases: *Oracle, MS SQL Server, MySQL, MariaDB, PostgreSQL, MongoDB, SAP, DB2*
- Azure: *Azure SQL Database*
- Amazon RDS: all including Aurora
- Amazon S3
- DocumentDB

TARGETS:

- On-premises and EC2 instances databases: *Oracle, MS SQL Server, MySQL, MariaDB, PostgreSQL, SAP*
- Amazon RDS including Aurora
- Amazon Redshift
- Amazon DynamoDB
- Amazon S3
- OpenSearch Service
- Kinesis Data Streams
- DocumentDB

Question 51:

A health insurance company stores personally identifiable information (PII) in an Amazon S3 bucket. The company uses server-side encryption with S3 managed encryption keys (SSE-S3) to encrypt the objects. According to a new requirement, all current and future objects in the S3 bucket must be encrypted by keys that the company's security team manages. The S3 bucket does not have versioning enabled.

Which solution will meet these requirements?

- A. In the S3 bucket properties, change the default encryption to SSE-S3 with a customer managed key. Use the AWS CLI to re-upload all objects in the S3 bucket. Set an S3 bucket policy to deny unencrypted PutObject requests.
- B. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to deny unencrypted PutObject requests. Use the AWS CLI to re-upload all objects in the S3 bucket.
- C. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to automatically encrypt objects on GetObject and PutObject requests.
- D. In the S3 bucket properties, change the default encryption to AES-256 with a customer managed key. Attach a policy to deny unencrypted PutObject requests to any entities that access the S3 bucket. Use the AWS CLI to re-upload all objects in the S3 bucket.

B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html>

S3 Encryption for Objects

- SSE-S3: encrypts S3 objects using keys handled & managed by AWS
- SSE-KMS: leverage KMS to manage encryption keys
 - Key usage appears in CloudTrail
 - objects made public can never be read
 - On s3:PutObject, make the permission kms:GenerateDataKey is allowed
- SSE-C: when you want to manage your own encryption keys
- Client-Side Encryption
- Glacier: all data is AES-256 encrypted, key under AWS control

Question 52:

A company is running a web application in the AWS Cloud. The application consists of dynamic content that is created on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group that is configured as a target group for an Application Load Balancer (ALB).

The company is using an Amazon CloudFront distribution to distribute the application globally. The CloudFront distribution uses the ALB as an origin. The company uses Amazon Route 53 for DNS and has created an A record of example.com for the CloudFront distribution.

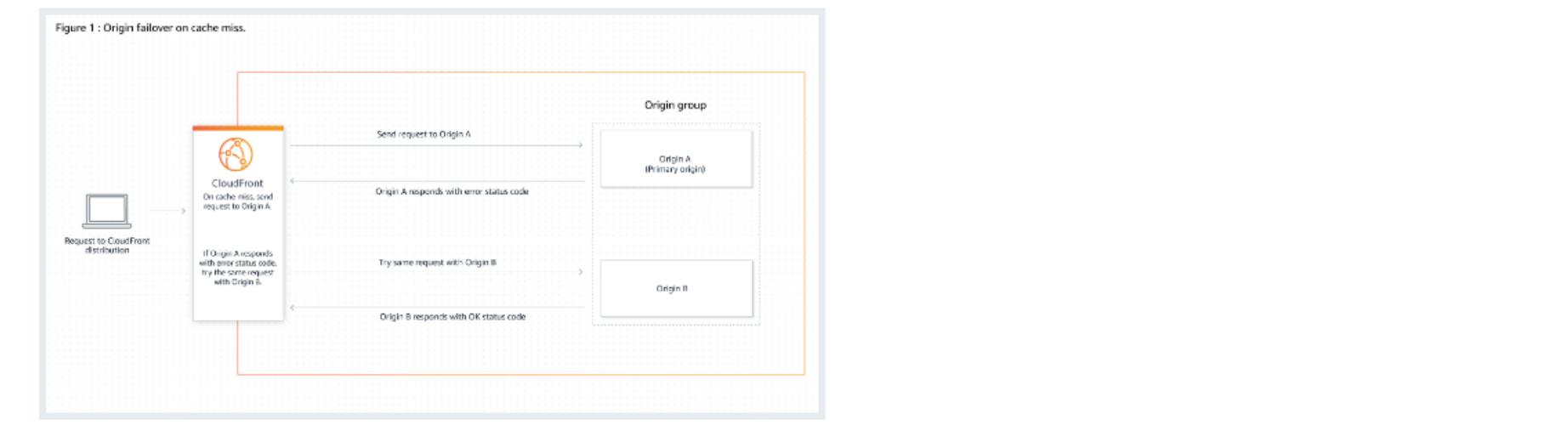
A solutions architect must configure the application so that it is highly available and fault tolerant.

Which solution meets these requirements?

- A. Provision a full, secondary application deployment in a different AWS Region. Update the Route 53 A record to be a failover record. Add both of the CloudFront distributions as values. Create Route 53 health checks.
- B. Provision an ALB, an Auto Scaling group, and EC2 instances in a different AWS Region. Update the CloudFront distribution, and create a second origin for the new ALB. Create an origin group for the two origins. Configure one origin as primary and one origin as secondary.
- C. Provision an Auto Scaling group and EC2 instances in a different AWS Region. Create a second target for the new Auto Scaling group in the ALB. Set up the failover routing algorithm on the ALB.
- D. Provision a full, secondary application deployment in a different AWS Region. Create a second CloudFront distribution, and add the new application setup as an origin. Create an AWS Global Accelerator accelerator. Add both of the CloudFront distributions as endpoints.

B

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html



Origin name	Origin domain	Origin path	Origin type
apigw-api	fmjmgg4znc.execute-api.ap-southeast-1.amazonaws.com	/uat	API Gateway
alb-api	nonprod-infra-public-all-alb-1203828303.ap-southeast-1.elb.a...		Elastic Load Bal...
s3-storage	uat-ingress-workplace-migrate-s3.s3.ap-southeast-1.amazona...	S3	
s3-static-web	uat-workplace-public-s3.s3.ap-southeast-1.amazonaws.com	S3	

Origin groups

Settings

Origins
Choose the origins for this group, then put them in priority order.

Choose origins to add to group ▾ Add

1: apigw-api (primary) X ▲ ▼

2: s3-storage X ▲ ▼

Name
Enter a name for this origin group.

Failover criteria
Select the origin errors to use as failover criteria.

400 Bad Request
 403 Forbidden
 404 Not found
 416 Range Not Satisfiable
 500 Internal server error
 502 Bad gateway
 503 Service unavailable
 504 Gateway timeout

Question 53:

A company has an organization in AWS Organizations that has a large number of AWS accounts. One of the AWS accounts is designated as a transit account and has a transit gateway that is shared with all of the other AWS accounts. AWS Site-to-Site VPN connections are configured between all of the company's global offices and the transit account. The company has AWS Config enabled on all of its accounts.

The company's networking team needs to centrally manage a list of internal IP address ranges that belong to the global offices. Developers will reference this list to gain access to their applications securely.

Which solution meets these requirements with the LEAST amount of operational overhead?

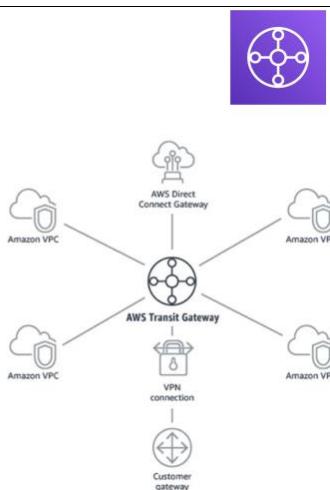
- A. Create a JSON file that is hosted in Amazon S3 and that lists all of the internal IP address ranges. Configure an Amazon Simple Notification Service (Amazon SNS) topic in each of the accounts that can be invoked when the JSON file is updated. Subscribe an AWS Lambda function to the SNS topic to update all relevant security group rules with the updated IP address ranges.
- B. Create a new AWS Config managed rule that contains all of the internal IP address ranges. Use the rule to check the security groups in each of the accounts to ensure compliance with the list of IP address ranges. Configure the rule to automatically remediate any noncompliant security group that is detected.
- C. In the transit account, create a VPC prefix list with all of the internal IP address ranges. Use AWS Resource Access Manager to share the prefix list with all of the other accounts. Use the shared prefix list to configure security group rules in the other accounts.
- D. In the transit account, create a security group with all of the internal IP address ranges. Configure the security groups in the other accounts to reference the transit account's security group by using a nested security group reference of "/sg-1a2b3c4d".

C

[https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-network-routing-and-security-administration-with-vpc-prefix-lists/#:-text=A%20Prefix%20List%20is%20a,Resource%20Access%20Manager%20\(RAM\)](https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-network-routing-and-security-administration-with-vpc-prefix-lists/#:-text=A%20Prefix%20List%20is%20a,Resource%20Access%20Manager%20(RAM))

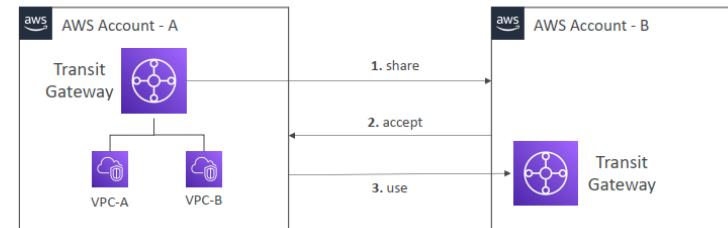
Transit Gateway

- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager (RAM)
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with other VPC
- Works with Direct Connect Gateway, VPN connections
- Supports IP Multicast (not supported by any other AWS service)
- Instances in a VPC can access a NAT Gateway, NLB, PrivateLink, and EFS in other VPCs attached to the AWS Transit Gateway.



Transit Gateway – Sharing through RAM

- You can use AWS RAM to share a Transit Gateway for VPC attachments across accounts or across AWS Organization



Resource Access Manager Managed Prefix List

- A set of one or more CIDR blocks
- Makes it easier to configure and maintain Security Groups and Route Tables
- **Customer-Managed Prefix List**
 - Set of CIDRs that you define and manage by you
 - Can be shared with other AWS accounts or AWS Organization
 - Modify to update many security groups at once
- **AWS-Managed Prefix List**
 - Set of CIDRs for AWS services
 - You can't create, modify, share, or delete them



NOT FOR DISTRIBUTION © Stephane Maarek www.datacumulus.com

Question 54:

A company runs a new application as a static website in Amazon S3. The company has deployed the application to a production AWS account and uses Amazon CloudFront to deliver the website. The website calls an Amazon API Gateway REST API. An AWS Lambda function backs each API method.

The company wants to create a CSV report every 2 weeks to show each API Lambda function's recommended configured memory, recommended cost, and the price difference between current configurations and the recommendations. The company will store the reports in an S3 bucket.

HANCHE

Which solution will meet these requirements with the LEAST development time?

- A. Create a Lambda function that extracts metrics data for each API Lambda function from Amazon CloudWatch Logs for the 2-week period. Collate the data into tabular format. Store the data as a .csv file in an S3 bucket. Create an Amazon EventBridge rule to schedule the Lambda function to run every 2 weeks.
- B. Opt in to AWS Compute Optimizer. Create a Lambda function that calls the ExportLambdaFunctionRecommendations operation. Export the .csv file to an S3 bucket. Create an Amazon EventBridge rule to schedule the Lambda function to run every 2 weeks.
- C. Opt in to AWS Compute Optimizer. Set up enhanced infrastructure metrics. Within the Compute Optimizer console, schedule a job to export the Lambda recommendations to a .csv file. Store the file in an S3 bucket every 2 weeks.
- D. Purchase the AWS Business Support plan for the production account. Opt in to AWS Compute Optimizer for AWS Trusted Advisor checks. In the Trusted Advisor console, schedule a job to export the cost optimization checks to a .csv file. Store the file in an S3 bucket every 2 weeks.

B

LEAST development time → B

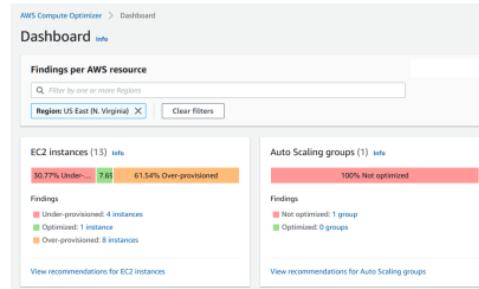
Lab: <https://aws.amazon.com/blogs/compute/optimizing-aws-lambda-cost-and-performance-using-aws-compute-optimizer/>

https://docs.aws.amazon.com/compute-optimizer/latest/APIReference/API_ExportLambdaFunctionRecommendations.html

AWS Compute Optimizer



- Reduce costs and improve performance by recommending optimal AWS resources for your workloads
- Helps you choose optimal configurations and right-size your workloads (over/under provisioned)
- Uses Machine Learning to analyze your resources' configurations and their utilization CloudWatch metrics
- Supported resources
 - EC2 instances
 - EC2 Auto Scaling Groups
 - EBS volumes
 - Lambda functions
- Lower your costs by up to 25%
- Recommendations can be exported to S3



Memory [Info](#)

Your function is allocated CPU proportional to the memory configured.

128 MB

Set memory to between 128 MB and 10240 MB

Question 55:

A company's factory and automation applications are running in a single VPC. More than 20 applications run on a combination of Amazon EC2, Amazon Elastic Container Service (Amazon ECS), and Amazon RDS.

The company has software engineers spread across three teams. One of the three teams owns each application, and each team is responsible for the cost and performance of all of its applications. Team resources have tags that represent their application and team. The teams use IAM access for daily activities.

The company needs to determine which costs on the monthly AWS bill are attributable to each application or team. The company also must be able to create reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. A solutions architect must recommend an AWS Billing and Cost Management solution that provides these cost reports.

Which combination of actions will meet these requirements? (Choose three.)

- A. Activate the user-defined cost allocation tags that represent the application and the team.
- B. Activate the AWS generated cost allocation tags that represent the application and the team.
- C. Create a cost category for each application in Billing and Cost Management.
- D. Activate IAM access to Billing and Cost Management.
- E. Create a cost budget.
- F. Enable Cost Explorer.

A,C,F

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html>

Cost Explorer



- Visualize, understand, and manage your AWS costs and usage over time
- Create custom reports that analyze cost and usage data.
- Analyze your data at a high level: total costs and usage across all accounts
- Or Monthly, hourly, resource level granularity
- Choose an optimal **Savings Plan** (to lower prices on your bill)
- Forecast usage up to 12 months based on previous usage

Question 56:

An AWS customer has a web application that runs on premises. The web application fetches data from a third-party API that is behind a firewall. The third party accepts only one public CIDR block in each client's allow list.

The customer wants to migrate their web application to the AWS Cloud. The application will be hosted on a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in a VPC. The ALB is located in public subnets. The EC2 instances are located in private subnets. NAT gateways provide internet access to the private subnets.

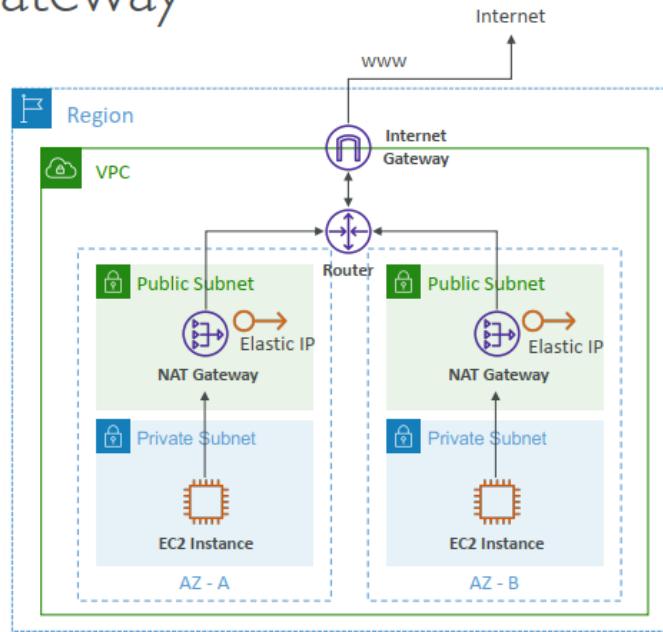
How should a solutions architect ensure that the web application can continue to call the third-party API after the migration?

- Associate a block of customer-owned public IP addresses to the VPC. Enable public IP addressing for public subnets in the VPC.
- Register a block of customer-owned public IP addresses in the AWS account. Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC.
- Create Elastic IP addresses from the block of customer-owned IP addresses. Assign the static Elastic IP addresses to the ALB.
- Register a block of customer-owned public IP addresses in the AWS account. Set up AWS Global Accelerator to use Elastic IP addresses from the address block. Set the ALB as the accelerator endpoint.

B

VPC Basics – NAT Gateway

- Managed NAT solution, bandwidth scales automatically
- Resilient to failure within a single AZ
- Must deploy multiple NAT Gateways in multiple AZ for HA
- Has an Elastic IP, external services see the IP of the NAT Gateway as the source



Question 57:

A company with several AWS accounts is using AWS Organizations and service control policies (SCPs). An administrator created the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-1111-1111:Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the administrator address this problem?

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowsAllActions",  
            "Effect": "Allow",  
            "Action": "*",  
            "Resource": "*"  
        },  
        {  
            "Sid": "DenyCloudTrail",  
            "Effect": "Deny",  
            "Action": "cloudtrail:*",  
            "Resource": "*"  
        }  
    ]  
}
```

- A. Add s3:CreateBucket with "Allow" effect to the SCP.
- B. Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111.
- C. Instruct the developers to add Amazon S3 permissions to their IAM entities.
- D. Remove the SCP from account 1111-1111-1111.

C

C is the answer. SCP DONT grant permissions. They just set boundaries on what account is capable of giving access to all users. For example, we applied a SCP on an OU that has account A. This SCP has S3fullAWSaccess. This does NOT mean that any IAM user can perform any S3 action. You still need to explicitly define IAM permissions for user to perform action on S3. This is called whitelisting. Another example, You wrote an SCP that DENIES S3 access and applied it to an OU that has account B. Now Lets say ROOT user of Account B (who got admin privileges) tries to create S3 bucket, they get DENIED error as SCP has already set a bounday saying NOONE in this OU can access S3.

Service Control Policies (SCP)

- Define allowlist or blocklist IAM actions
- Applied at the **OU** or **Account** level
- Does not apply to the Management Account
- SCP is applied to all the **Users and Roles** in the account, including Root user
- The SCP does not affect Service-linked roles
 - **Service-linked roles** enable other AWS services to integrate with AWS Organizations and can't be restricted by SCPs.
- SCP must have an explicit Allow (does not allow anything by default)
- Use cases:
 - Restrict access to certain services (for example: can't use EMR)
 - Enforce PCI compliance by explicitly disabling services

Question 58:

A company has a monolithic application that is critical to the company's business. The company hosts the application on an Amazon EC2 instance that runs Amazon Linux 2. The company's application team receives a directive from the legal department to back up the data from the instance's encrypted Amazon Elastic Block Store (Amazon EBS) volume to an Amazon S3 bucket. The application team does not have the administrative SSH key pair for the instance. The application must continue to serve the users.

Which solution will meet these requirements?

- A. Attach a role to the instance with permission to write to Amazon S3. Use the AWS Systems Manager Session Manager option to gain access to the instance and run commands to copy data into Amazon S3.
- B. Create an image of the instance with the reboot option turned on. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3.
- C. Take a snapshot of the EBS volume by using Amazon Data Lifecycle Manager (Amazon DLM). Copy the data to Amazon S3.

D. Create an image of the instance. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3.

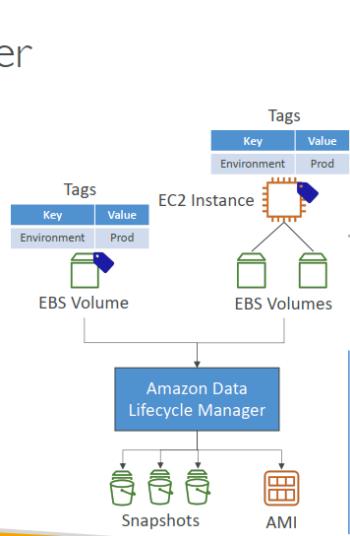
A

Not B and D. because when you create an image of the instance, by default Amazon EC2 shuts down the instance, takes snapshots of any attached volumes, creates AMI, and then reboots the instance. This breaks the requirement to keep the app running <https://docs.aws.amazon.com/toolkit-for-visual-studio/latest/user-guide/tkv-create-ami-from-instance.html>

Not C. Because EBS snapshots taken by DLM are stored on S3 that is not accessible from users. also you cannot copy snapshots to S3 (you can copy across regions and across accounts, but still in S3 not accessible from users) <https://repost.aws/knowledge-center/ebs-copy-snapshot-data-s3-create-volume>.

Amazon Data Lifecycle Manager

- Automate the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs
- Schedule backups, cross-account snapshot copies, delete outdated backups, ...
nhin dang
- Uses resource tags to identify the resources (EC2 instances, EBS volumes)
- Can't be used to manage snapshots/AMIs created outside DLM
- Can't be used to manage instance-store backed AMIs



Question 59:

A solutions architect needs to copy data from an Amazon S3 bucket in an AWS account to a new S3 bucket in a new AWS account. The solutions architect must implement a solution that uses the AWS CLI.

Which combination of steps will successfully copy the data? (Choose three.)

- Create a bucket policy to allow the source bucket to list its contents and to put objects and set object ACLs in the destination bucket. Attach the bucket policy to the destination bucket.
- Create a bucket policy to allow a user in the destination account to list the source bucket's contents and read the source bucket's objects. Attach the bucket policy to the source bucket.

C. Create an IAM policy in the source account. Configure the policy to allow a user in the source account to list contents and get objects in the source bucket, and to list contents, put objects, and set object ACLs in the destination bucket. Attach the policy to the user.

D. Create an IAM policy in the destination account. Configure the policy to allow a user in the destination account to list contents and get objects in the source bucket, and to list contents, put objects, and set objectACLs in the destination bucket. Attach the policy to the user.

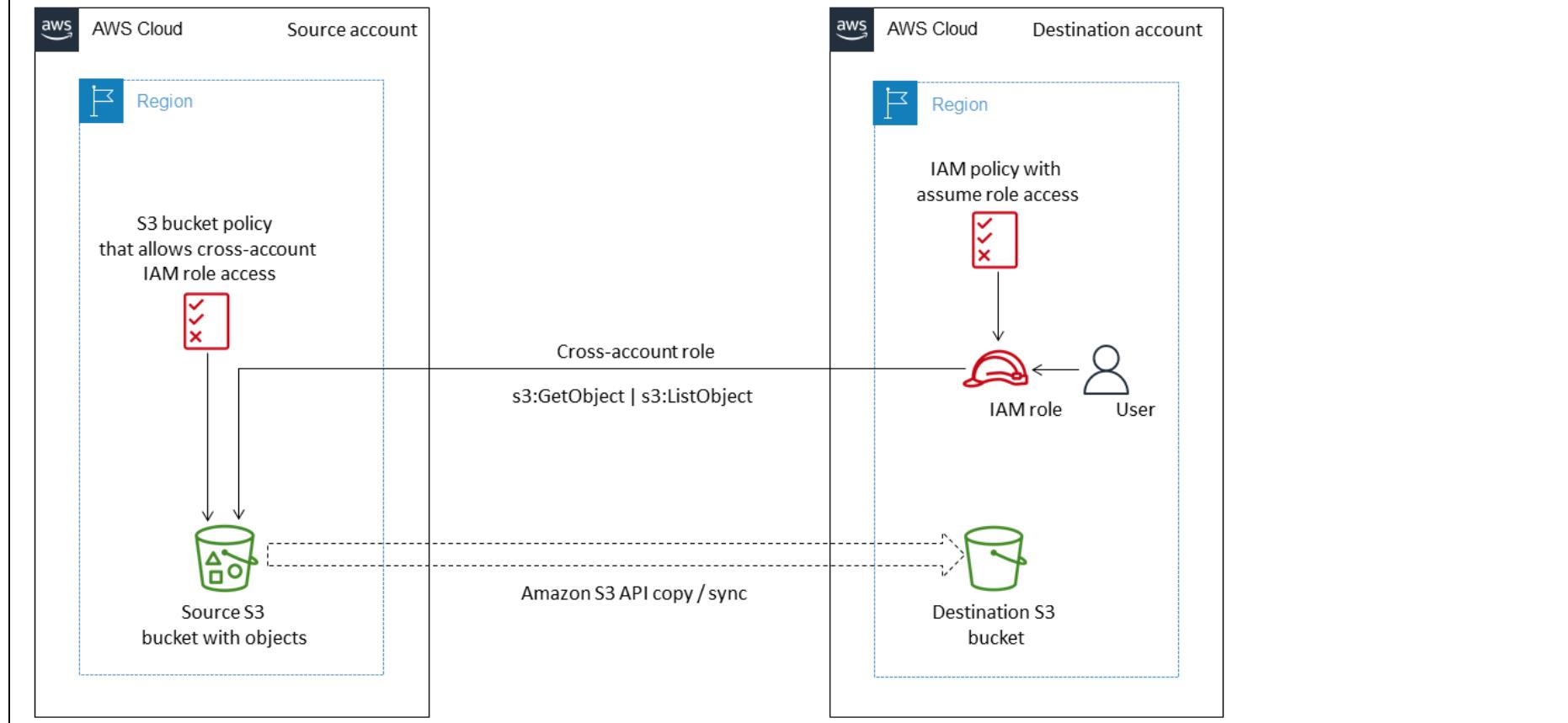
E. Run the aws s3 sync command as a user in the source account. Specify the source and destination buckets to copy the data.

F. Run the aws s3 sync command as a user in the destination account. Specify the source and destination buckets to copy the data.

B,D,F

LAB: <https://medium.com/tensult/copy-s3-bucket-objects-across-aws-accounts-e46c15c4b9e1>

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/copy-data-from-an-s3-bucket-to-another-account-and-region-by-using-the-aws-cli.html>



Question 60:

A company built an application based on AWS Lambda deployed in an AWS CloudFormation stack. The last production release of the web application introduced an issue that resulted in an outage lasting several minutes. A solutions architect must adjust the deployment process to support a canary release.

Which solution will meet these requirements?

- A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load.
- B. Deploy the application into a new CloudFormation stack. Use an Amazon Route 53 weighted routing policy to distribute the load.
- C. Create a version for every new deployed Lambda function. Use the AWS CLI update-function-configuration command with the routing-config parameter to distribute the load.
- D. Configure AWS CodeDeploy and use CodeDeployDefault.OneAtATime in the Deployment configuration to distribute the load.

A

The screenshot shows the 'Create alias' configuration page in the AWS Lambda console. The URL in the browser is [Lambda > Functions > lambda-ec2 > Create alias](#). The page title is 'Create alias'. Under the 'Alias configuration' section, there is a note: 'An alias is a pointer to one or two versions. Choose each version that you want the alias to point to.' Below this are fields for 'Name' (input field), 'Description - optional' (input field), and 'Version' (dropdown menu). At the bottom left, there is a link '► Weighted alias'.

Question 61:

A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties. The company runs its own SFTP server on an Amazon EC2 instance in a public subnet of a VPC. After the files are uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS sftp.example.com through the use of Amazon Route 53.

What should a solutions architect do to improve the reliability and scalability of the SFTP solution?

- A. Move the EC2 instance into an Auto Scaling group. Place the EC2 instance behind an Application Load Balancer (ALB). Update the DNS record sftp.example.com in Route 53 to point to the ALB.
- B. Migrate the SFTP server to AWS Transfer for SFTP. Update the DNS record sftp.example.com in Route 53 to point to the server endpoint hostname.
- C. Migrate the SFTP server to a file gateway in AWS Storage Gateway. Update the DNS record sftp.example.com in Route 53 to point to the file gateway endpoint.
- D. Place the EC2 instance behind a Network Load Balancer (NLB). Update the DNS record sftp.example.com in Route 53 to point to the NLB.

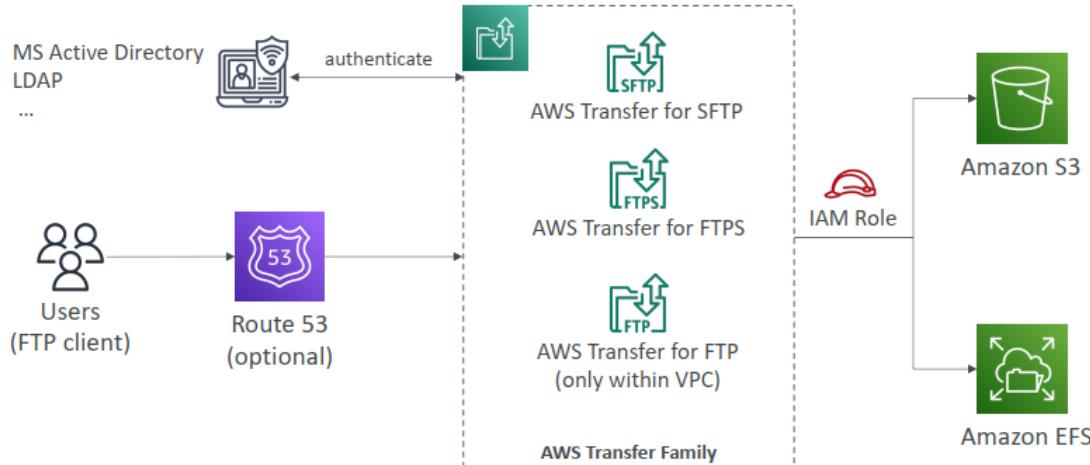
B

AWS Transfer Family



- A fully-managed service for file transfers into and out of Amazon S3 or Amazon EFS using the FTP protocol
- Supported Protocols
 - AWS Transfer for FTP (File Transfer Protocol (FTP))
 - AWS Transfer for FTPS (File Transfer Protocol over SSL (FTPS))
 - AWS Transfer for SFTP (Secure File Transfer Protocol (SFTP))
- Managed infrastructure, Scalable, Reliable, Highly Available (multi-AZ)
- Pay per provisioned endpoint per hour + data transfers in GB
- Store and manage users' credentials within the service
- Integrate with existing authentication systems (Microsoft Active Directory, LDAP, Okta, Amazon Cognito, custom)
- Usage: sharing files, public datasets, CRM, ERP, ...

AWS Transfer Family



Question 62:

A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration.

What should the solutions architect do to meet these requirements?

- Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server. Use the SMB share to host the VMware data store. Use VM Import/Export to move the VMs to Amazon EC2.
- Use the VMware vSphere client to export the application as an image in Open Virtualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command.
- Configure AWS Storage Gateway for files service to export a Common Internet File System (CIFS) share. Create a backup copy to the shared folder. Sign in to the AWS Management Console and create an AMI from the backup copy. Launch an EC2 instance that is based on the AMI.
- Create a managed-instance activation for a hybrid environment in AWS Systems Manager. Download and install Systems Manager Agent on the on-premises VM. Register the VM with Systems Manager to be a managed instance. Use AWS Backup to create a snapshot of the VM and create an AMI. Launch an EC2 instance that is based on the AMI.

B.

This approach allows the solutions architect to export the application as an image in OVF format, which preserves the software and configuration settings, and then import it into Amazon EC2 using the EC2 import command.

<https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

You can use VM Import/Export to import virtual machine (VM) images from your virtualization environment to Amazon EC2 as Amazon Machine Images (AMI), which you can use to launch instances. Subsequently, you can export the VM images from an instance back to your virtualization environment. This enables you to leverage your investments in the VMs that you have built to meet your IT security, configuration management, and compliance requirements by bringing them into Amazon EC2.

Question 63:

A video processing company has an application that downloads images from an Amazon S3 bucket, processes the images, stores a transformed image in a second S3 bucket, and updates metadata about the image in an Amazon DynamoDB table. The application is written in Node.js and runs by using an AWS Lambda function. The Lambda function is invoked when a new image is uploaded to Amazon S3.

The application ran without incident for a while. However, the size of the images has grown significantly. The Lambda function is now failing frequently with timeout errors. The function timeout is set to its maximum value. A solutions architect needs to refactor the application's architecture to prevent invocation failures. The company does not want to manage the underlying infrastructure.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR).
- B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargate. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- C. Create an AWS Step Functions state machine with a Parallel state to invoke the Lambda function. Increase the provisioned concurrency of the Lambda function.
- D. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of Amazon EC2. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- E. Modify the application to store images on Amazon Elastic File System (Amazon EFS) and to store metadata on an Amazon RDS DB instance. Adjust the Lambda function to mount the EFS file share.

A, B

The correct answer is A and B. A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR). - This step is necessary to package the application code in a container and make it available for running on ECS. B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargate. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS

task definition when a new file arrives in Amazon S3. - This step is necessary to run the containerized application on Fargate, which is a fully managed container orchestration service that eliminates the need to provision and scale the underlying infrastructure.

Question 64:

A company has an organization in AWS Organizations. The company is using AWS Control Tower to deploy a landing zone for the organization. The company wants to implement governance and policy enforcement. The company must implement a policy that will detect Amazon RDS DB instances that are not encrypted at rest in the company's production OU.

Which solution will meet this requirement?

- A. Turn on mandatory guardrails in AWS Control Tower. Apply the mandatory guardrails to the production OU.
- B. Enable the appropriate guardrail from the list of strongly recommended guardrails in AWS Control Tower. Apply the guardrail to the production OU.
- C. Use AWS Config to create a new mandatory guardrail. Apply the rule to all accounts in the production OU.
- D. Create a custom SCP in AWS Control Tower. Apply the SCP to the production OU.

B

AWS Control Tower



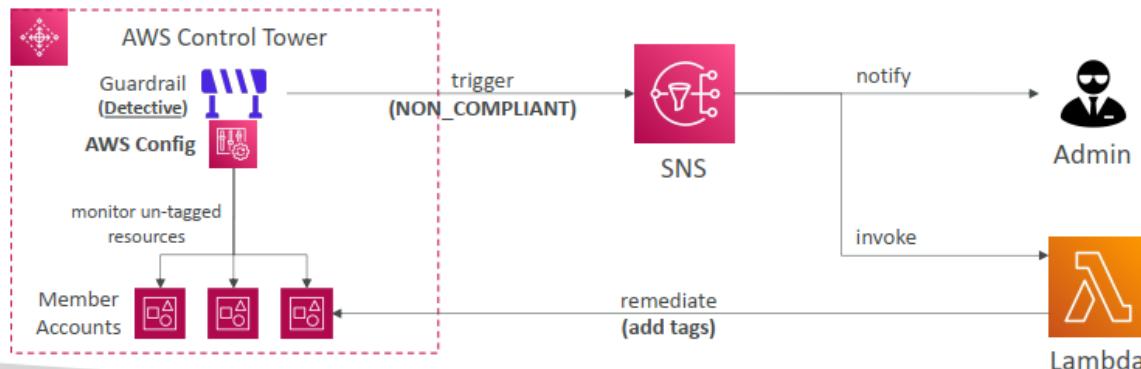
- Easy way to set up and govern a secure and compliant multi-account AWS environment based on best practices
- Benefits:
 - Automate the set up of your environment in a few clicks
 - Automate ongoing policy management using guardrails
 - Detect policy violations and remediate them
 - Monitor compliance through an interactive dashboard
- AWS Control Tower runs on top of AWS Organizations:
 - It automatically sets up AWS Organizations to organize accounts and implement SCPs (Service Control Policies)

AWS Control Tower – Detect and Remediate Policy Violations

- **Guardrail**

(adj): tiếp tục, tiếp diễn

- Provides ongoing governance for your Control Tower environment (AWS Accounts)
- Preventive – using SCPs (e.g., Disallow Creation of Access Keys for the Root User)
- Detective – using AWS Config (e.g., Detect Whether MFA for the Root User is Enabled)
- Example: identify non-compliant resources (e.g., untagged resources)



AWS Control Tower – Guardrails Levels

- **Mandatory**

- Automatically enabled and enforced by AWS Control Tower
- Example: Disallow public Read access to the Log Archive account

- **Strongly Recommended**

- Based on AWS best practices (optional)
- Example: Enable encryption for EBS volumes attached to EC2 instances

- **Elective** Tù chọn

- Commonly used by enterprises (optional)
- Example: Disallow delete actions without MFA in S3 buckets

Question 65:

A startup company hosts a fleet of Amazon EC2 instances in private subnets using the latest Amazon Linux 2 AMI. The company's engineers rely heavily on SSH access to the instances for troubleshooting.

The company's existing architecture includes the following:

- A VPC with private and public subnets, and a NAT gateway.
- Site-to-Site VPN for connectivity with the on-premises environment.
- EC2 security groups with direct SSH access from the on-premises environment.

The company needs to increase security controls around SSH access and provide auditing of commands run by the engineers.

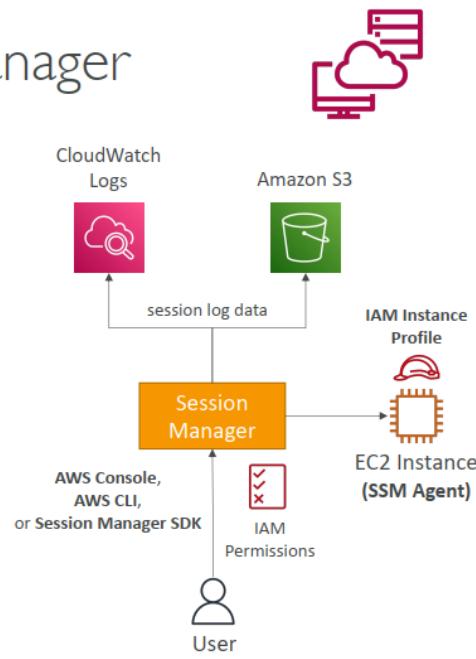
Which strategy should a solutions architect use?

- A. Install and configure EC2 Instance Connect on the fleet of EC2 instances. Remove all security group rules attached to EC2 instances that allow inbound TCP on port 22. Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI.
- B. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs.
- C. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Enable AWS Config for EC2 security group resource changes. Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules.
- D. Create an IAM role with the AmazonSSMManagedInstanceCore managed policy attached. Attach the IAM role to all the EC2 instances. Remove all security group rules attached to the EC2 instances that allow inbound TCP on port 22. Have the engineers install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager.

D

Systems Manager Session Manager

- Allows you to start a secure shell on your EC2 and on-premises servers
- Access through AWS Console, AWS CLI, or Session Manager SDK
- Does not need SSH access, bastion hosts, or SSH keys**
- Supports Linux, macOS, and Windows
- Log connections to your instances and executed commands
- Session log data can be sent to S3 or CloudWatch Logs
- CloudTrail can intercept StartSession events
chặn



Question 66:

A company that uses AWS Organizations allows developers to experiment on AWS. As part of the landing zone that the company has deployed, developers use their company email address to request an account. The company wants to ensure that developers are not launching costly services or running services unnecessarily. The company must give developers a fixed monthly budget to limit their AWS costs.

Which combination of steps will meet these requirements? (Choose three.)

- Create an SCP to set a fixed monthly account usage limit. Apply the SCP to the developer accounts.
- Use AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process.
- Create an SCP to deny access to costly services and components. Apply the SCP to the developer accounts.
- Create an IAM policy to deny access to costly services and components. Apply the IAM policy to the developer accounts.
- Create an AWS Budgets alert action to terminate services when the budgeted amount is reached. Configure the action to terminate all services.
- Create an AWS Budgets alert action to send an Amazon Simple Notification Service (Amazon SNS) notification when the budgeted amount is reached. Invoke an AWS Lambda function to terminate all services.

B,C,F

<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html>

ensure that developers are not launching costly services or running services unnecessarily → SCP to deny → C
a fixed monthly budget to limit their AWS costs → AWS Budget → B



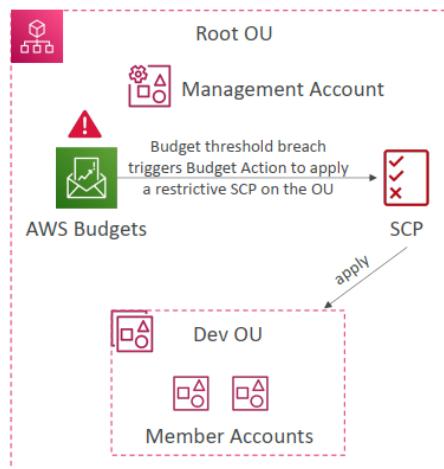
AWS Budgets

- Create budget and send alarms when costs exceeds the budget
- 4 types of budgets: Usage, Cost, Reservation, Savings Plans
- For Reserved Instances (RI)
 - Track utilization
 - Supports EC2, ElastiCache, RDS, Redshift
- Up to 5 SNS notifications per budget
- Can filter by: Service, Linked Account, Tag, Purchase Option, Instance Type, Region, Availability Zone, API Operation, etc...
- Same options as AWS Cost Explorer!
- 2 budgets are free, then \$0.02/day/budget

Budget Actions

Thay đổi hành động khi vượt quá budget hoặc vượt quá
nhiều sử dụng

- Run actions on your behalf when a budget exceeds a certain cost or usage threshold
- Supports 3 action types:
 - Applying an IAM Policy to a user, group, or IAM role
 - Applying Service Control Policy (SCP) to an OU
 - Stop EC2 or RDS Instances
- Actions can be executed automatically or require a workflow approval process
- Reduces unintentional overspending in your account



Question 67:

A company has applications in an AWS account that is named Source. The account is in an organization in AWS Organizations. One of the applications uses AWS Lambda functions and stores inventory data in an Amazon Aurora database. The application deploys the Lambda functions by using a deployment package. The company has configured automated backups for Aurora.

The company wants to migrate the Lambda functions and the Aurora database to a new AWS account that is named Target. The application processes critical data, so the company must minimize downtime.

Which solution will meet these requirements?

- A. Download the Lambda function deployment package from the Source account. Use the deployment package and create new Lambda functions in the Target account. Share the automated Aurora DB cluster snapshot with the Target account.
- B. Download the Lambda function deployment package from the Source account. Use the deployment package and create new Lambda functions in the Target account. Share the Aurora DB cluster with the Target account by using AWS Resource Access Manager (AWS RAM). Grant the Target account permission to clone the Aurora DB cluster.
- C. Use AWS Resource Access Manager (AWS RAM) to share the Lambda functions and the Aurora DB cluster with the Target account. Grant the Target account permission to clone the Aurora DB cluster.
- D. Use AWS Resource Access Manager (AWS RAM) to share the Lambda functions with the Target account. Share the automated Aurora DB cluster snapshot with the Target account.

B

Lambda > Functions > uat-ingress-sso-lambda-get-qr-code

uat-ingress-sso-lambda-get-qr-code

Throttle Copy ARN Actions ▾

Function overview Info

Export to Application Composer Download ▾

Download function code .zip
Download AWS SAM file
Download both

Description uat-ingress-sso-lambda-get-qr-code

Diagram Template

uat-ingress-sso-

AWS Resource Access Manager (RAM)

- Share AWS resources that you own with other AWS accounts
- Share with any account or within your Organization
- Avoid resource duplication!
- **VPC Subnets**
 - Allow to have all the resources launched in the same subnets
 - Must be from the same AWS Organizations.
 - Cannot share security groups and default VPC
 - Participants can manage their own resources in there
 - Participants can't view, modify, delete resources that belong to other participants or the owner
- **AWS Transit Gateway**
- Route 53 (Resolver Rules, DNS Firewall Rule Groups)
- License Manager Configurations

AWS Resource Access Manager (RAM)

- Aurora DB Clusters
- ACM Private Certificate Authority
- CodeBuild Project
- EC2 (Dedicated Hosts, Capacity Reservation)
- AWS Glue (Catalog, Database, Table)
- AWS Network Firewall Policies
- AWS Resource Groups
- Systems Manager Incident Manager (Contacts, Response Plans)
- AWS Outposts (Outpost, Site)

Question 68:

A company runs a Python script on an Amazon EC2 instance to process data. The script runs every 10 minutes. The script ingests files from an Amazon S3 bucket and processes the files. On average, the script takes approximately 5 minutes to process each file. The script will not reprocess a file that the script has already processed.

The company reviewed Amazon CloudWatch metrics and noticed that the EC2 instance is idle for approximately 40% of the time because of the file processing speed. The company wants to make the workload highly available and scalable. The company also wants to reduce long-term management overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the data processing script to an AWS Lambda function. Use an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure Amazon S3 to send event notifications to the SQS queue. Create an EC2 Auto Scaling group with a minimum size of one instance. Update the data processing script to poll the SQS queue. Process the S3 objects that the SQS message identifies.
- C. Migrate the data processing script to a container image. Run the data processing container on an EC2 instance. Configure the container to poll the S3 bucket for new objects and to process the resulting objects.
- D. Migrate the data processing script to a container image that runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Create an AWS Lambda function that calls the Fargate RunTaskAPI operation when the container processes the file. Use an S3 event notification to invoke the Lambda function.

A

Question 69:

A financial services company in North America plans to release a new online web application to its customers on AWS. The company will launch the application in the us-east-1 Region on Amazon EC2 instances. The application must be highly available and must dynamically scale to meet user traffic. The company also wants to implement a disaster recovery environment for the application in the us-west-1 Region by using active-passive failover.

Which solution will meet these requirements?

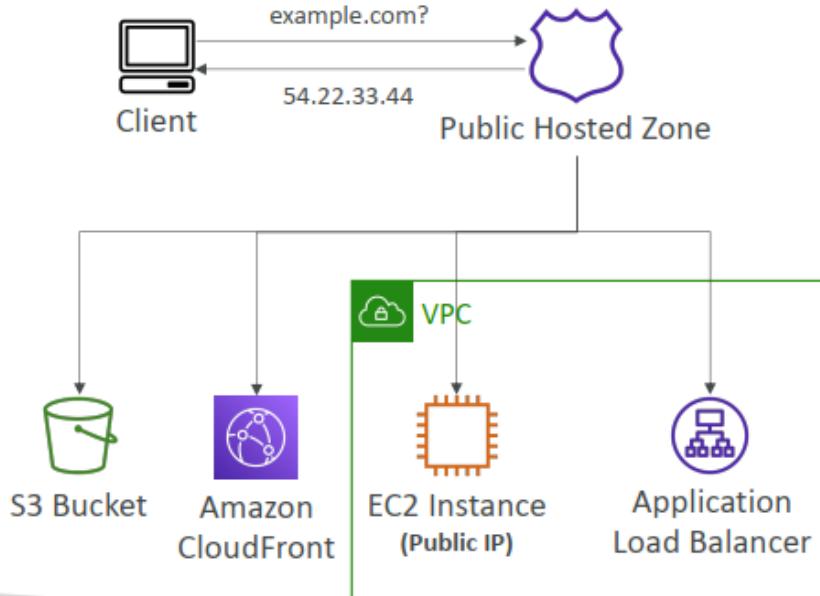
- A. Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB.
- B. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC. Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC. Create an Amazon Route 53 hosted zone. Create separate records for each ALB. Enable health checks to ensure high availability between Regions.
- C. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC. Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC. Create an Amazon Route 53 hosted zone. Create separate records for each ALB. Enable health checks and configure a failover routing policy for each record.

D. Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB. Create an Amazon Route 53 hosted zone. Create a record for the ALB.

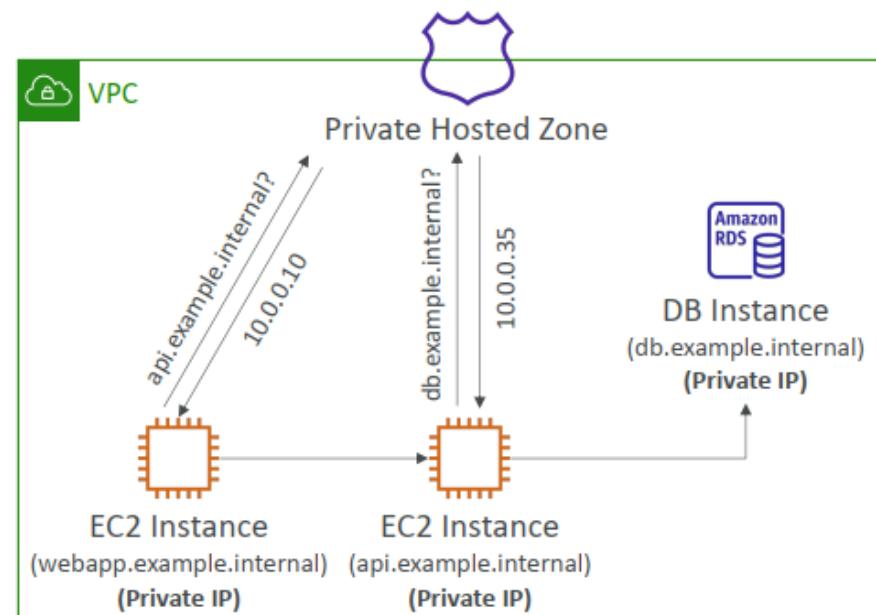
C

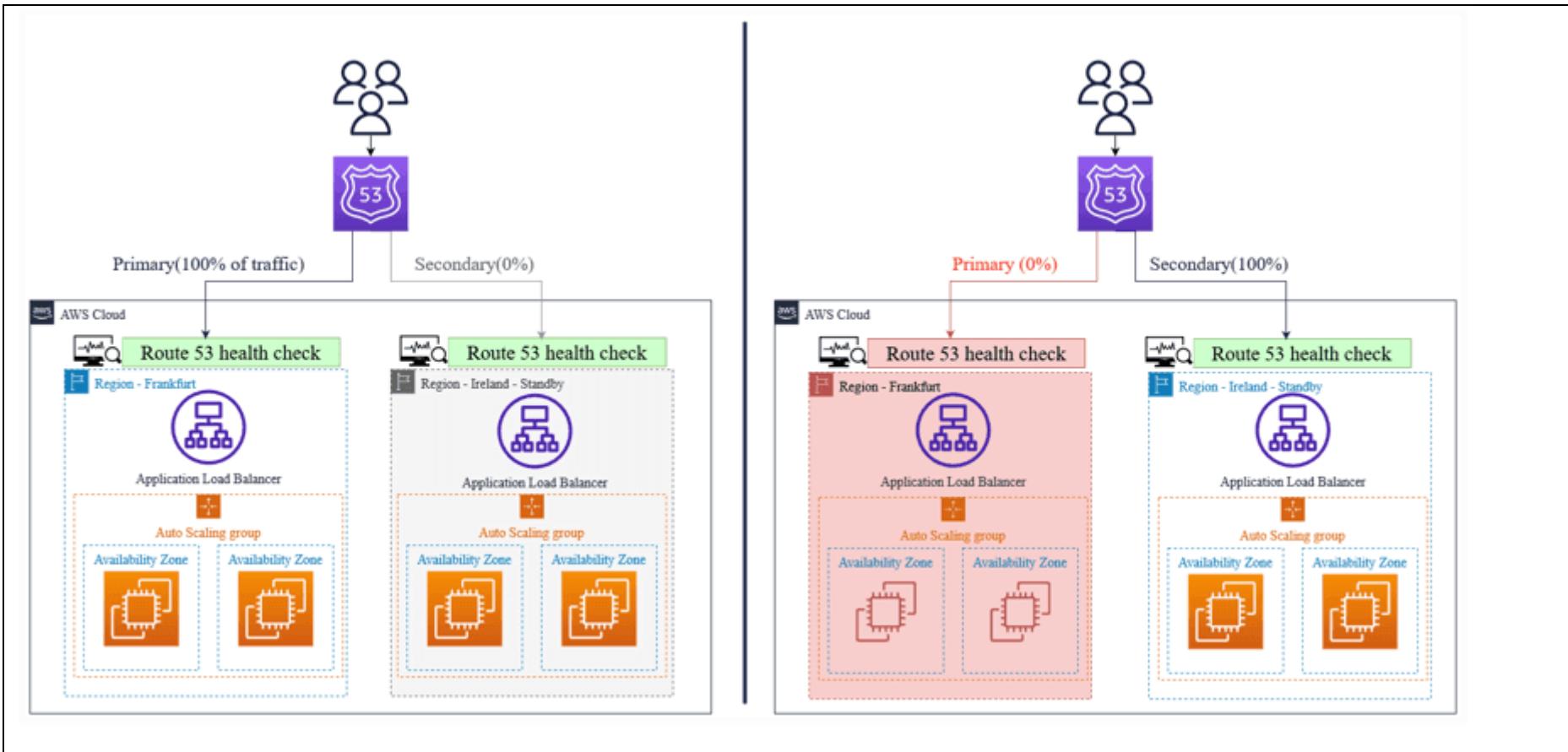
Route 53 – Public vs. Private Hosted Zones

Public Hosted Zone



Private Hosted Zone





Question 70:

A company has an environment that has a single AWS account. A solutions architect is reviewing the environment to recommend what the company could improve specifically in terms of access to the AWS Management Console. The company's IT support workers currently access the console for administrative tasks, authenticating with named IAM users that have been mapped to their job role.

The IT support workers no longer want to maintain both their Active Directory and IAM user accounts. They want to be able to access the console by using their existing Active Directory credentials. The solutions architect is using AWS IAM Identity Center (AWS Single Sign-On) to implement this functionality.

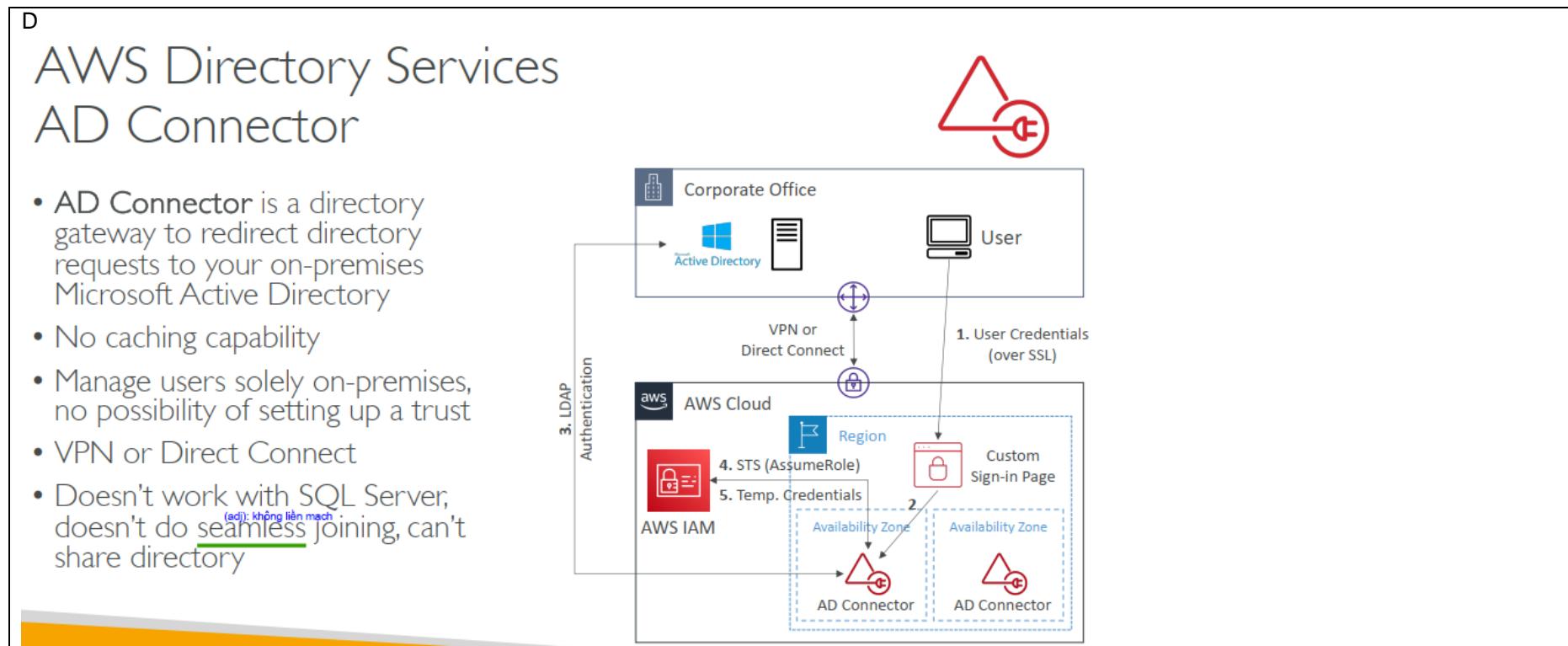
Which solution will meet these requirements MOST cost-effectively?

A. Create an organization in AWS Organizations. Turn on the IAM Identity Center feature in Organizations. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure IAM Identity Center and set the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.

B. Create an organization in AWS Organizations. Turn on the IAM Identity Center feature in Organizations. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure IAM Identity Center and select the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.

C. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure IAM Identity Center and select the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.

D. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure IAM Identity Center and set the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.



Question 71:

A video streaming company recently launched a mobile app for video sharing. The app uploads various files to an Amazon S3 bucket in the us-east-1 Region. The files range in size from 1 GB to 10 GB.

Users who access the app from Australia have experienced uploads that take long periods of time. Sometimes the files fail to completely upload for these users. A solutions architect must improve the app's performance for these uploads.

Which solutions will meet these requirements? (Choose two.)

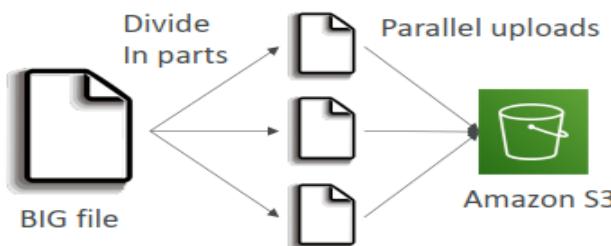
- A. Enable S3 Transfer Acceleration on the S3 bucket. Configure the app to use the Transfer Acceleration endpoint for uploads.
- B. Configure an S3 bucket in each Region to receive the uploads. Use S3 Cross-Region Replication to copy the files to the distribution S3 bucket.
- C. Set up Amazon Route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region.
- D. Configure the app to break the video files into chunks. Use a multipart upload to transfer files to Amazon S3.
- E. Modify the app to add random prefixes to the files before uploading.

A, D

S3 Performance

- **Multi-Part upload:**

- recommended for files > 100MB, must use for files > 5GB
- Can help parallelize uploads (speed up transfers)



- **S3 Transfer Acceleration**

- Increase transfer speed by transferring file to an AWS edge location which will forward the data to the S3 bucket in the target region
- Compatible with multi-part upload



Question 72:

An application is using an Amazon RDS for MySQL Multi-AZ DB instance in the us-east-1 Region. After a failover test, the application lost the connections to the database and could not re-establish the connections. After a restart of the application, the application re-established the connections.

A solutions architect must implement a solution so that the application can re-establish connections to the database without requiring a restart.

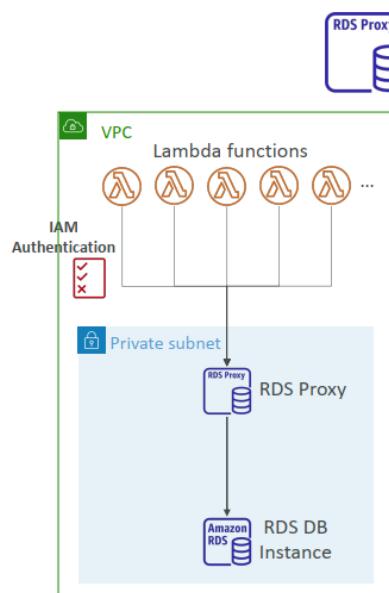
Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL Serverless v1 DB instance. Migrate the RDS DB instance to the Aurora Serverless v1 DB instance. Update the connection settings in the application to point to the Aurora reader endpoint.
- B. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.
- C. Create a two-node Amazon Aurora MySQL DB cluster. Migrate the RDS DB instance to the Aurora DB cluster. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.
- D. Create an Amazon S3 bucket. Export the database to Amazon S3 by using AWS Database Migration Service (AWS DMS). Configure Amazon Athena to use the S3 bucket as a data store. Install the latest Open Database Connectivity (ODBC) driver for the application. Update the connection settings in the application to point to the Athena endpoint.

B

Amazon RDS Proxy

- Fully managed database proxy for RDS
- Allows apps to pool and share DB connections established with the database
- Improving database efficiency by reducing the stress on database resources (e.g., CPU, RAM) and minimize open connections (and timeouts)
- Serverless, autoscaling, highly available (multi-AZ)
- Reduced RDS & Aurora failover time by up 66%
- Supports RDS (MySQL, PostgreSQL, MariaDB, MS SQL Server) and Aurora (MySQL, PostgreSQL)
- No code changes required for most apps
- Enforce IAM Authentication for DB, and securely store credentials in AWS Secrets Manager
- RDS Proxy is never publicly accessible (must be accessed from VPC)



Amazon RDS Proxy is a fully managed database proxy service for Amazon Relational Database Service (RDS) that makes applications more scalable, resilient, and secure. It allows applications to pool and share connections to an RDS database, which can help reduce database connection overhead, improve scalability, and provide automatic failover and high availability.

By using an RDS proxy, your application can automatically reconnect to the database after a failover event, without the need to restart the application. Solution A, migrating to Aurora Serverless, may not solve the problem because Aurora Serverless does not support Multi-AZ. Solution C and D are not the correct solutions because it does not solve the problem of reconnecting to the database after a failover event.

Question 73:

A company is building a solution in the AWS Cloud. Thousands of devices will connect to the solution and send data. Each device needs to be able to send and receive data in real time over the MQTT protocol. Each device must authenticate by using a unique X.509 certificate.

Which solution will meet these requirements with the LEAST operational overhead?

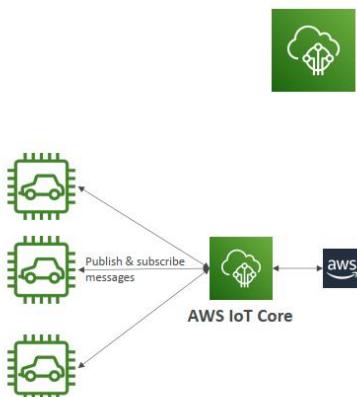
- Set up AWS IoT Core. For each device, create a corresponding Amazon MQ queue and provision a certificate. Connect each device to Amazon MQ.
- Create a Network Load Balancer (NLB) and configure it with an AWS Lambda authorizer. Run an MQTT broker on Amazon EC2 instances in an Auto Scaling group. Set the Auto Scaling group as the target for the NLB. Connect each device to the NLB.
- Set up AWS IoT Core. For each device, create a corresponding AWS IoT thing and provision a certificate. Connect each device to AWS IoT Core.
- Set up an Amazon API Gateway HTTP API and a Network Load Balancer (NLB). Create integration between API Gateway and the NLB. Configure a mutual TLS certificate authorizer on the HTTP API. Run an MQTT broker on an Amazon EC2 instance that the NLB targets. Connect each device to the NLB.

C

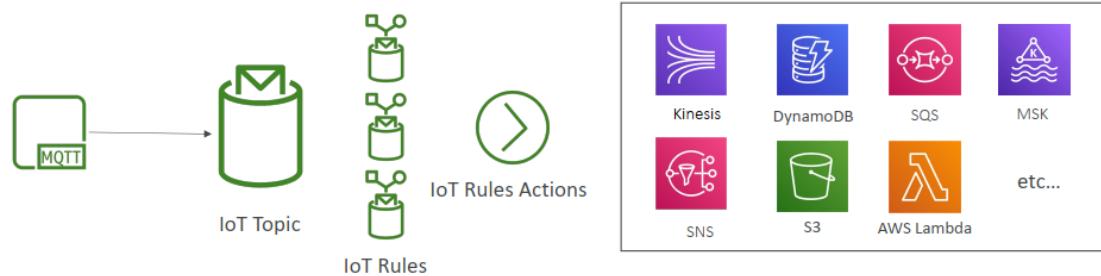
<https://docs.aws.amazon.com/iot/latest/developerguide/iot-connect-devices.html>

AWS IoT Core

- IoT stands for “Internet of Things” – the network of internet-connected devices that are able to collect and transfer data
- AWS IoT Core allows you to easily connect IoT devices to the AWS Cloud
- Serverless, secure & scalable to billions of devices and trillions of messages
- Integrates with a lot of AWS services (Lambda, S3, SageMaker, etc.)
- Build IoT applications that gather, process, analyze, and act on data



IoT Core - Integrations



Question 74:

A company is running several workloads in a single AWS account. A new company policy states that engineers can provision only approved resources and that engineers must use AWS CloudFormation to provision these resources. A solutions architect needs to create a solution to enforce the new restriction on the IAM role that the engineers use for access.

What should the solutions architect do to create the solution?

- Upload AWS CloudFormation templates that contain approved resources to an Amazon S3 bucket. Update the IAM policy for the engineers' IAM role to only allow access to Amazon S3 and AWS CloudFormation. Use AWS CloudFormation templates to provision resources.
- Update the IAM policy for the engineers' IAM role with permissions to only allow provisioning of approved resources and AWS CloudFormation. Use AWS CloudFormation templates to create stacks with approved resources.
- Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation actions. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new IAM service role. Assign the IAM service role to AWS CloudFormation during stack creation.
- Provision resources in AWS CloudFormation stacks. Update the IAM policy for the engineers' IAM role to only allow access to their own AWS CloudFormation stack.

C

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html>

A = doesn't prevent to have a CloudFormation template with non-approved resources deployed

B = this doesn't prevent engineers to provision resources from console or cli

D = doesn't prevent to provision non-approved resources or to provision only via CloudFormation

Question 75:

A solutions architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted.

The solutions architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.

Which storage strategy is the MOST cost-effective and meets the design requirements?

- A. Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieval. Configure a lifecycle policy to delete data older than 120 days.
- B. Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.
- C. Design the application to store each incoming record in a single table in an Amazon RDS MySQL database. Run a nightly cron job that runs a query to delete any records older than 120 days.
- D. Design the application to batch incoming records before writing them to an Amazon S3 bucket. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search feature to retrieve the data. Configure a lifecycle policy to delete the data after 120 days.

B

- A. No, because millions of writes to a single .csv file would cause read and write latency
- B. Yes, because DynamoDB can support peaks of more than 20 million requests per second.
- C. No, because creating nightly cron is unnecessary, and a relation database isn't designed to ingest millions of small records per minute
- D. No, because S3 supports 210,000 PUT requests per minute (3,500 requests per second * 60 seconds per min) which is far less than 1,000,000+ writes per minute

DynamoDB – in short

- NoSQL database, fully managed, massive scale (1,000,000 rps)
- Similar to Apache Cassandra (can migrate to DynamoDB)
- No disk space to provision, max object size is 400 KB
- Capacity: provisioned (WCU, RCU, & Auto Scaling) or on-demand
- Supports CRUD (Create Read Update Delete)
- Read: eventually or strong consistency
- Supports transactions across multiple tables (ACID support)
- Backups available, point in time recovery
- Table classes: Standard and Infrequent Access (IA)



S3 – Overview

- Object storage, serverless, unlimited storage, pay-as-you-go
- Good to store static content (image, video files)
- Access objects by key, no indexing facility
- Not a filesystem, cannot be mounted natively on EC2
- Anti patterns:
 - Lots of small files
 - POSIX file system (use EFS instead), file locks
 - Search features, queries, rapidly changing data
 - Website with dynamic content

Question 76:

A retail company is hosting an ecommerce website on AWS across multiple AWS Regions. The company wants the website to be operational at all times for online purchases. The website stores data in an Amazon RDS for MySQL DB instance.

Which solution will provide the HIGHEST availability for the database?

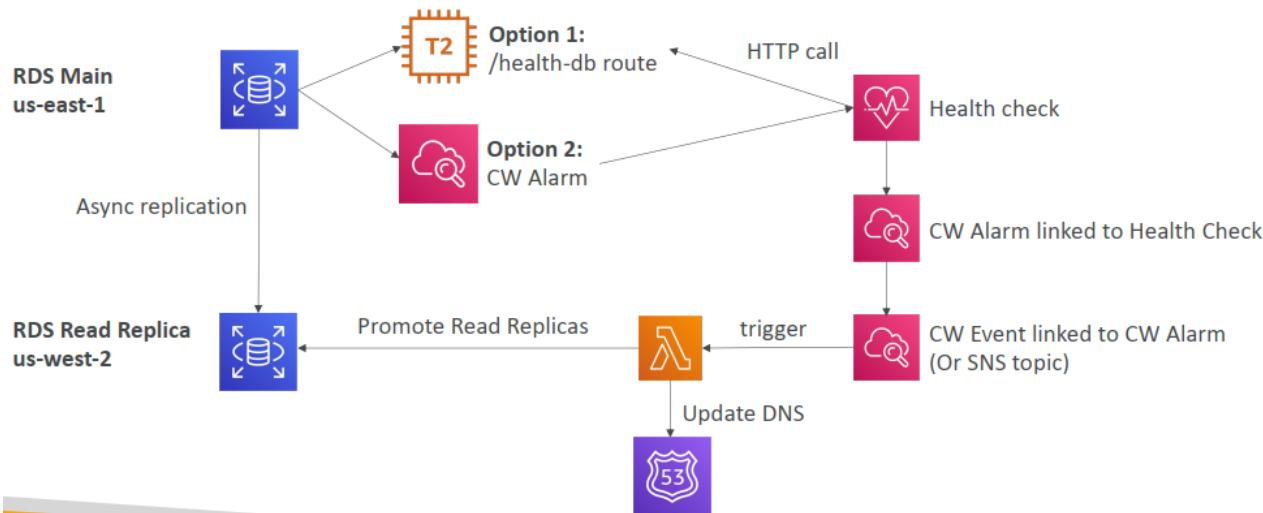
- A. Configure automated backups on Amazon RDS. In the case of disruption, promote an automated backup to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source.
- B. Configure global tables and read replicas on Amazon RDS. Activate the cross-Region scope. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- C. Configure global tables and automated backups on Amazon RDS. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- D. Configure read replicas on Amazon RDS. In the case of disruption, promote a cross-Region and read replica to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source.

D

A = you cannot promote an automated backup to a standalone DB (you restore a backup into a new DB instance instead). Creating a read replica could help in this scenario in case it is cross-region.

B = RDS does not support global table

RDS Solution Architecture Cross Region Failover



Question 77:

Example Corp. has an on-premises data center and a VPC named VPC A in the Example Corp. AWS account. The on-premises network connects to VPC A through an AWS Site-To-Site VPN. The on-premises servers can properly access VPC A. Example Corp. just acquired AnyCompany, which has a VPC named VPC B. There is no IP address overlap among these networks. Example Corp. has peered VPC A and VPC B.

Example Corp. wants to connect from its on-premise servers to VPC B. Example Corp. has properly set up the network ACL and security groups.

Which solution will meet this requirement with the LEAST operational effort?

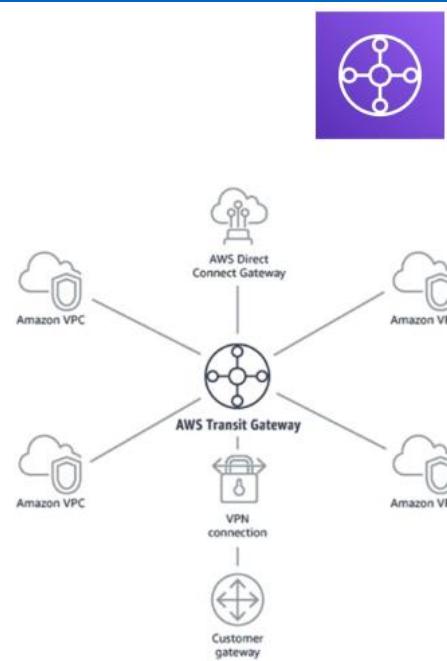
- Create a transit gateway. Attach the Site-to-Site VPN, VPC A, and VPC B to the transit gateway. Update the transit gateway route tables for all networks to add IP range routes for all other networks.
- Create a transit gateway. Create a Site-to-Site VPN connection between the on-premises network and VPC B, and connect the VPN connection to the transit gateway. Add a route to direct traffic to the peered VPCs, and add an authorization rule to give clients access to the VPCs A and B.
- Update the route tables for the Site-to-Site VPN and both VPCs for all three networks. Configure BGP propagation for all three networks. Wait for up to 5 minutes for BGP propagation to finish.
- Modify the Site-to-Site VPN's virtual private gateway definition to include VPC A and VPC B. Split the two routers of the virtual private gateway between the two VPCs.

A

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html>

Transit Gateway

- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager (RAM)
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with other VPC
- Works with Direct Connect Gateway, VPN connections
- Supports IP Multicast (not supported by any other AWS service)
- Instances in a VPC can access a NAT Gateway, NLB, PrivateLink, and EFS in other VPCs attached to the AWS Transit Gateway.



Question 78:

A company recently completed the migration from an on-premises data center to the AWS Cloud by using a replatforming strategy. One of the migrated servers is running a legacy Simple Mail Transfer Protocol (SMTP) service that a critical application relies upon. The application sends outbound email messages to the company's customers. The legacy SMTP server does not support TLS encryption and uses TCP port 25. The application can use SMTP only.

The company decides to use Amazon Simple Email Service (Amazon SES) and to decommission the legacy SMTP server. The company has created and validated the SES domain. The company has lifted the SES limits.

What should the company do to modify the application to send email messages from Amazon SES?

- A. Configure the application to connect to Amazon SES by using TLS Wrapper. Create an IAM role that has ses:SendEmail and ses:SendRawEmail permissions. Attach the IAM role to an Amazon EC2 instance.
- B. Configure the application to connect to Amazon SES by using STARTTLS. Obtain Amazon SES SMTP credentials. Use the credentials to authenticate with Amazon SES.
- C. Configure the application to use the SES API to send email messages. Create an IAM role that has ses:SendEmail and ses:SendRawEmail permissions. Use the IAM role as a service role for Amazon SES.
- D. Configure the application to use AWS SDKs to send email messages. Create an IAM user for Amazon SES. Generate API access keys. Use the access keys to authenticate with Amazon SES.

B

<https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>

The Amazon SES SMTP endpoint requires that all connections be encrypted using Transport Layer Security (TLS). (Note that TLS is often referred to by the name of its predecessor protocol, SSL.) Amazon SES supports two mechanisms for establishing a TLS-encrypted connection: STARTTLS and TLS Wrapper.

STARTTLS

STARTTLS is a means of upgrading an unencrypted connection to an encrypted connection. There are versions of STARTTLS for a variety of protocols; the SMTP version is defined in [RFC 3207](#).

To set up a STARTTLS connection, the SMTP client connects to the Amazon SES SMTP endpoint on port 25, 587, or 2587, issues an EHLO command, and waits for the server to announce that it supports the STARTTLS SMTP extension. The client then issues the STARTTLS command, initiating TLS negotiation. When negotiation is complete, the client issues an EHLO command over the new encrypted connection, and the SMTP session proceeds normally.

TLS Wrapper

TLS Wrapper (also known as SMTPS or the Handshake Protocol) is a means of initiating an encrypted connection without first establishing an unencrypted connection. With TLS Wrapper, the Amazon SES SMTP endpoint doesn't perform TLS negotiation: it's the client's responsibility to connect to the endpoint using TLS, and to continue using TLS for the entire conversation. TLS Wrapper is an older protocol, but many clients still support it.

To set up a TLS Wrapper connection, the SMTP client connects to the Amazon SES SMTP endpoint on port 465 or 2465. The server presents its certificate, the client issues an EHLO command, and the SMTP session proceeds normally.

Question 79:

A company recently acquired several other companies. Each company has a separate AWS account with a different billing and reporting method. The acquiring company has consolidated all the accounts into one organization in AWS Organizations. However, the acquiring company has found it difficult to generate a cost report that contains meaningful groups for all the teams.

The acquiring company's finance team needs a solution to report on costs for all the companies through a self-managed application.

Which solution will meet these requirements?

- A. Create an AWS Cost and Usage Report for the organization. Define tags and cost categories in the report. Create a table in Amazon Athena. Create an Amazon QuickSight dataset based on the Athena table. Share the dataset with the finance team.
- B. Create an AWS Cost and Usage Report for the organization. Define tags and cost categories in the report. Create a specialized template in AWS Cost Explorer that the finance department will use to build reports.
- C. Create an Amazon QuickSight dataset that receives spending information from the AWS Price List Query API. Share the dataset with the finance team.
- D. Use the AWS Price List Query API to collect account spending information. Create a specialized template in AWS Cost Explorer that the finance department will use to build reports.

A

Amazon QuickSight

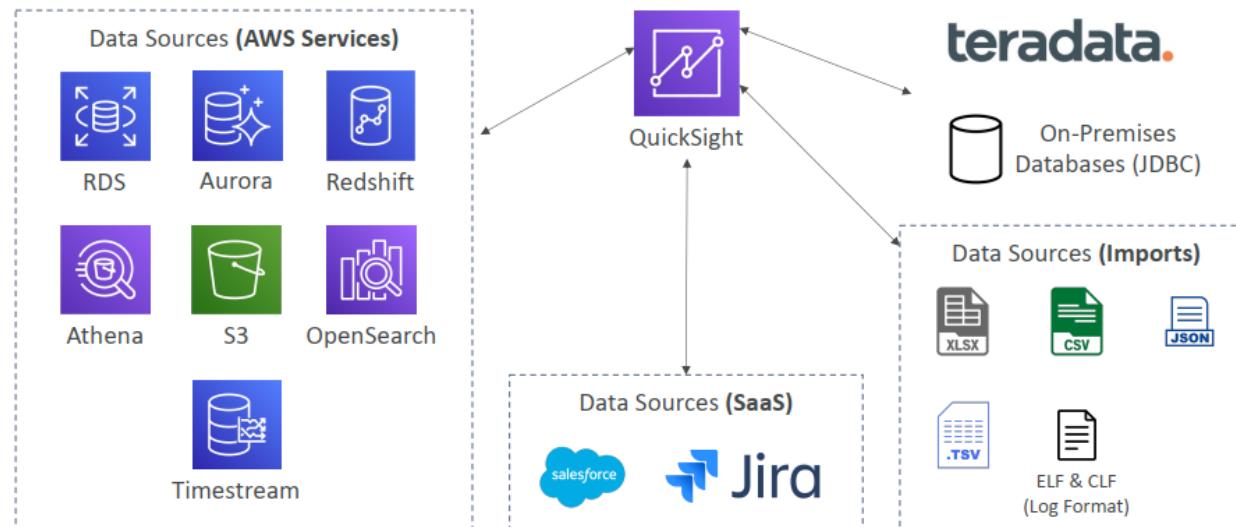


- Serverless machine learning-powered business intelligence service to create interactive dashboards
- Fast, automatically scalable, embeddable, with per-session pricing
- Use cases:
 - Business analytics
 - Building visualizations
 - Perform ad-hoc analysis
 - Get business insights using data
- Integrated with RDS, Aurora, Athena, Redshift, S3...
- In-memory computation using SPICE engine if data is imported into QuickSight
- Enterprise edition: Possibility to setup Column-Level security (CLS)



<https://aws.amazon.com/quicksight/>

QuickSight Integrations



QuickSight – Dashboard & Analysis

- Define Users (standard versions) and Groups (enterprise version)
 - These users & groups only exist within QuickSight, not IAM !!
- A *dashboard*...
 - is a read-only snapshot of an analysis that you can share
 - preserves the configuration of the analysis (filtering, parameters, controls, sort)
Duy trì cấu hình của việc phân tích
- You can share the analysis or the dashboard with Users or Groups
- To share a dashboard, you must first publish it
- Users who see the dashboard can also see the underlying data

Question 80:

A company runs an IoT platform on AWS. IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume.

The number of sensors the company has deployed in the field has increased over time, and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency.

Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Choose two.)

- A. Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS.
- B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas.
- C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data.
- D. Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load.
- E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance.

C,E

Option C: Leveraging Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data would help to resolve the issues with the API servers being consistently overloaded. By using Kinesis, the data can be ingested and processed in real-time, allowing the API servers to handle the increased load. Using Lambda to process the data can also help to improve the overall performance and scalability of the platform.

Option E: Re-architecting the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance would help to resolve the issues with high write latency. DynamoDB is a NoSQL database that is designed for high performance and scalability, making it a good fit for this use case. Additionally, DynamoDB supports auto-scaling, which can help to ensure that the database can handle the expected growth in the number of sensors.

Question 81:

A company is building an electronic document management system in which users upload their documents. The application stack is entirely serverless and runs on AWS in the eu-central-1 Region. The system includes a web application that uses an Amazon CloudFront distribution for delivery with Amazon S3 as the origin. The web application communicates with Amazon API Gateway Regional endpoints. The API Gateway APIs call AWS Lambda functions that store metadata in an Amazon Aurora Serverless database and put the documents into an S3 bucket.

The company is growing steadily and has completed a proof of concept with its largest customer. The company must improve latency outside of Europe.

Which combination of actions will meet these requirements? (Choose two.)

- A. Enable S3 Transfer Acceleration on the S3 bucket. Ensure that the web application uses the Transfer Acceleration signed URLs.
- B. Create an accelerator in AWS Global Accelerator. Attach the accelerator to the CloudFront distribution.

C. Change the API Gateway Regional endpoints to edge-optimized endpoints.

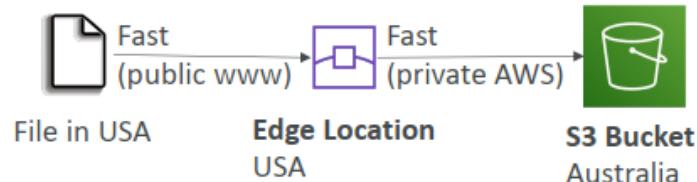
D. Provision the entire stack in two other locations that are spread across the world. Use global databases on the Aurora Serverless cluster.

E. Add an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database.

A,C
improve latency outside of Europe → API Gateway Edge-Optimize.

• S3 Transfer Acceleration

- Increase transfer speed by transferring file to an AWS edge location which will forward the data to the S3 bucket in the target region
- Compatible with multi-part upload



API Gateway - Endpoint Types

- Edge-Optimized (default): For global clients
 - Requests are routed through the CloudFront Edge locations (improves latency)
 - The API Gateway still lives in only one region
- Regional:
 - For clients within the same region
 - Could manually combine with CloudFront (more control over the caching strategies and the distribution)
- Private:
 - Can only be accessed from your VPC using an interface VPC endpoint (ENI)
 - Use a resource policy to define access

Question 82:

An adventure company has launched a new feature on its mobile app. Users can use the feature to upload their hiking and rafting photos and videos anytime. The photos and videos are stored in Amazon S3 Standard storage in an S3 bucket and are served through Amazon CloudFront.

The company needs to optimize the cost of the storage. A solutions architect discovers that most of the uploaded photos and videos are accessed infrequently after 30 days. However, some of the uploaded photos and videos are accessed frequently after 30 days. The solutions architect needs to implement a solution that maintains millisecond retrieval availability of the photos and videos at the lowest possible cost.

Which solution will meet these requirements?

- A. Configure S3 Intelligent-Tiering on the S3 bucket.
- B. Configure an S3 Lifecycle policy to transition image objects and video objects from S3 Standard to S3 Glacier Deep Archive after 30 days.
- C. Replace Amazon S3 with an Amazon Elastic File System (Amazon EFS) file system that is mounted on Amazon EC2 instances.
- D. Add a Cache-Control: max-age header to the S3 image objects and S3 video objects. Set the header to 30 days.

A

S3 Intelligent-Tiering



phi theo dõi hàng tháng và tự động phân cấp nhỏ

- Small monthly monitoring and auto-tiering fee
- Moves objects automatically between Access Tiers based on usage
- There are no retrieval charges in S3 Intelligent-Tiering
- Frequent Access tier (automatic): default tier
- Infrequent Access tier (automatic): objects not accessed for 30 days
- Archive Instant Access tier (automatic): objects not accessed for 90 days
- Archive Access tier (optional): configurable from 90 days to 700+ days
- Deep Archive Access tier (optional): config. from 180 days to 700+ days

Question 83:

A company uses Amazon S3 to store files and images in a variety of storage classes. The company's S3 costs have increased substantially during the past year.

A solutions architect needs to review data trends for the past 12 months and identify the appropriate storage class for the objects.

Which solution will meet these requirements?

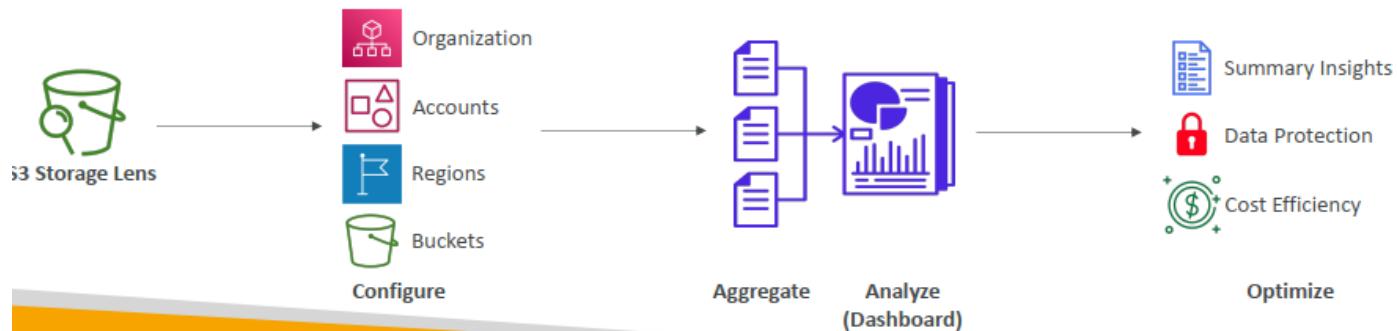
- A. Download AWS Cost and Usage Reports for the last 12 months of S3 usage. Review AWS Trusted Advisor recommendations for cost savings.
- B. Use S3 storage class analysis. Import data trends into an Amazon QuickSight dashboard to analyze storage trends.
- C. Use Amazon S3 Storage Lens. Upgrade the default dashboard to include advanced metrics for storage trends.
- D. Use Access Analyzer for S3. Download the Access Analyzer for S3 report for the last 12 months. Import the .csv file to an Amazon QuickSight dashboard.

C

S3 – Storage Lens



- Understand, analyze, and optimize storage across entire AWS Organization
- Discover anomalies, identify cost efficiencies, and apply data protection best practices across entire AWS Organization (30 days usage & activity metrics)
- Aggregate data for Organization, specific accounts, regions, buckets, or prefixes
- Default dashboard or create your own dashboards
- Can be configured to export metrics daily to an S3 bucket (CSV, Parquet)



▼ Getting started with Storage Lens



Create dashboard

Configure your dashboard scope, specify your metrics selection (free or advanced), attach Storage Lens groups, and enable a metrics export.



Storage Lens generates daily metrics aggregation

Your Storage Lens dashboard is updated daily to include metrics that are aggregated by account, Region, storage class, bucket, prefix, or Storage Lens group.



Analyze your storage

Use the interactive dashboard to explore usage and activity trends and insights, and contextual recommendations for best practices to optimize your storage.

Question 84:

A company has its cloud infrastructure on AWS. A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts.

What should the solutions architect do to meet these requirements?

- A. Use AWS CloudFormation templates. Add IAM policies to control the various accounts, Deploy the templates across the multiple Regions.
- B. Use AWS Organizations. Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts.
- C. Use AWS Organizations and AWS CloudFormation StackSets. Deploy a Cloud Formation template from an account that has the necessary IAM permissions.
- D. Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

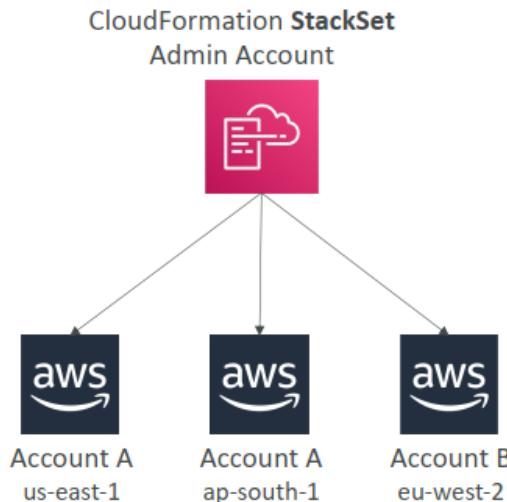
C

<https://aws.amazon.com/blogs/aws/new-use-aws-cloudformation-stacksets-for-multiple-accounts-in-an-aws-organization/>

D incorrect - nested stack allows to provision resources by using different CloudFormation templates

CloudFormation – StackSets

- Create, update, or delete stacks across multiple accounts and regions with a single operation
- Administrator account to create StackSets
- Trusted accounts to create, update, delete stack instances from StackSets
- When you update a stack set, all associated stack instances are updated throughout all accounts and regions
- Enable **Automatic Deployment** feature to automatically deploy to accounts in AWS Organization or OUs



Question 85:

A company has its cloud infrastructure on AWS. A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts.

What should the solutions architect do to meet these requirements?

- Use AWS CloudFormation templates. Add IAM policies to control the various accounts, Deploy the templates across the multiple Regions.
- Use AWS Organizations. Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts.
- Use AWS Organizations and AWS CloudFormation StackSets. Deploy a Cloud Formation template from an account that has the necessary IAM permissions.
- Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

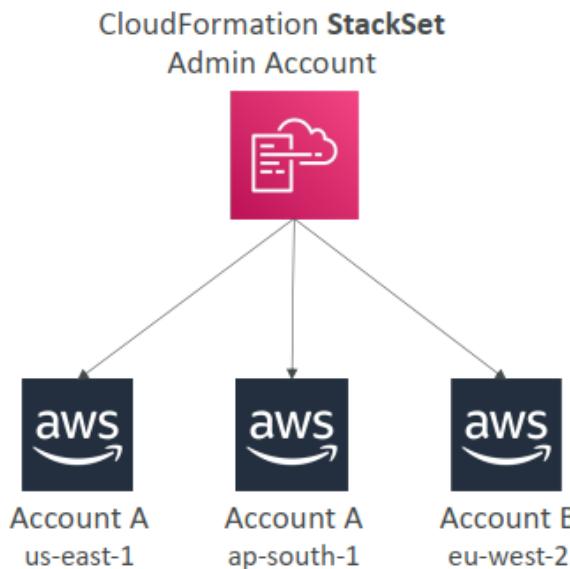
C

<https://aws.amazon.com/blogs/aws/new-use-aws-cloudformation-stacksets-for-multiple-accounts-in-an-aws-organization/>

D incorrect - nested stack allows to provision resources by using different CloudFormation templates

CloudFormation – StackSets

- Create, update, or delete stacks across multiple accounts and regions with a single operation
- Administrator account to create StackSets
- Trusted accounts to create, update, delete stack instances from StackSets
- When you update a stack set, all associated stack instances are updated throughout all accounts and regions
- Enable Automatic Deployment feature to automatically deploy to accounts in AWS Organization or OUs



Question 86:

A company plans to refactor a monolithic application into a modern application design deployed on AWS. The CI/CD pipeline needs to be upgraded to support the modern design for the application with the following requirements:

- It should allow changes to be released several times every hour.
- It should be able to roll back the changes as quickly as possible.

Which design will meet these requirements?

A. Deploy a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances.

B. Specify AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CI/CD pipeline of the application. To deploy, swap the staging and production environment URLs.

C. Use AWS Systems Manager to re-provision the infrastructure for each deployment. Update the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment.

D. Roll out the application updates as part of an Auto Scaling event using prebuilt AMIs. Use new versions of the AMIs to add instances. and phase out all instances that use the previous AMI version with the configured termination policy during a deployment event.

B

The correct answer is B. Specifying AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CI/CD pipeline of the application and swapping the staging and production environment URLs. This approach allows the company to deploy updates several times an hour and quickly roll back changes as needed.

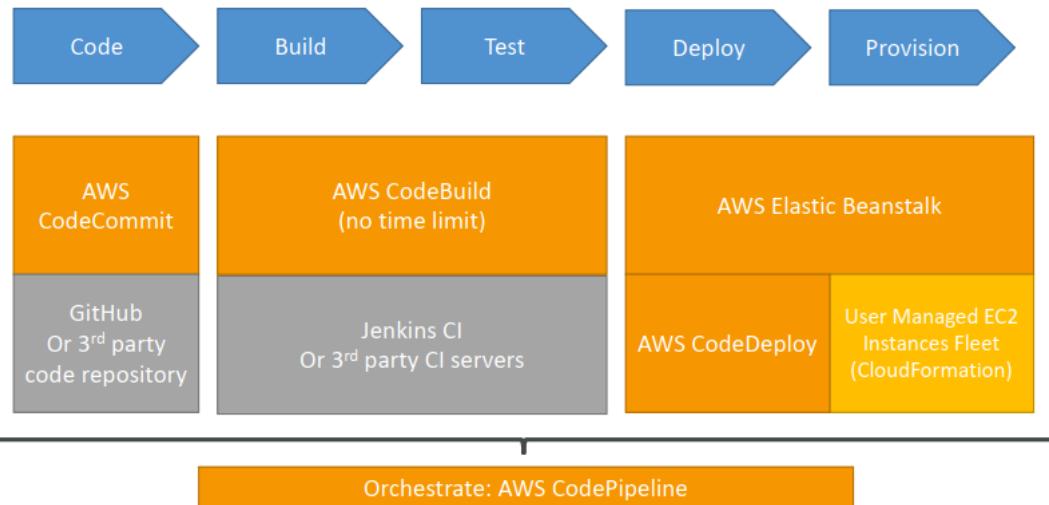
Option A, Deploying a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances, while it may provide a way to roll back changes by replacing instances with previous versions, it may not allow for rapid deployment of updates multiple times per hour.

AWS Elastic Beanstalk Overview



- Elastic Beanstalk is a developer centric view of deploying an application on AWS
- It uses all the component's we've seen before: EC2, Auto Scaling Group, Elastic Load Balancers, RDS, etc...
- But it's all in one view that's easy to make sense of!
- We still have full control over the configuration of each component
- Beanstalk is free but you pay for the underlying instances

Technology Stack for CICD



Question 87:

A company has an application that runs on Amazon EC2 instances. A solutions architect is designing VPC infrastructure in an AWS Region where the application needs to access an Amazon Aurora DB Cluster. The EC2 instances are all associated with the same security group. The DB cluster is associated with its own security group.

The solutions architect needs to add rules to the security groups to provide the application with least privilege access to the DB Cluster.

Which combination of steps will meet these requirements? (Choose two.)

- A. Add an inbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the source over the default Aurora port.
- B. Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port.
- C. Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port.
- D. Add an outbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the destination over the default Aurora port.
- E. Add an outbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the destination over the ephemeral ports.

B, C

<https://docs.aws.amazon.com/quicksight/latest/user/vpc-security-groups.html>

Question 88:

A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall cloud spending with the head of each business unit. The company uses AWS Organizations to manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold.

Which solution is the MOST cost-effective way to meet these requirements?

- A. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in each account to create monthly reports for each business unit.
- B. Configure AWS Budgets in the organization's management account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's management account to create monthly reports for each business unit.
- C. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit.
- D. Enable AWS Cost and Usage Reports in the organization's management account and configure reports grouped by application, environment, and owner. Create an AWS Lambda function that processes AWS Cost and Usage Reports, sends budget alerts, and sends monthly reports to each business unit's email list.

B

send notifications → SNS

each business unit receives monthly reports → config in the organization's management account and use Cost Explorer

Option A is not the most cost-effective solution because it requires configuring budgets and reports in multiple accounts, which increases the complexity and cost of managing the cloud spending for each business unit.

Option C is not the most cost-effective solution because it requires the cloud governance team to access the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit, which increases the complexity and cost of managing the cloud spending for each business unit.

Option D is not the most cost-effective solution because it requires creating an AWS Lambda function to process AWS Cost and Usage Reports, which increases the complexity and cost of managing the cloud spending for each business unit.

AWS Budgets



- Create budget and send alarms when costs exceeds the budget
- 4 types of budgets: Usage, Cost, Reservation, Savings Plans
- For Reserved Instances (RI)
 - Track utilization
 - Supports EC2, ElastiCache, RDS, Redshift
- Up to 5 SNS notifications per budget
- Can filter by: Service, Linked Account, Tag, Purchase Option, Instance Type, Region, Availability Zone, API Operation, etc...
- Same options as AWS Cost Explorer!
- 2 budgets are free, then \$0.02/day/budget

Cost Explorer



- Visualize, understand, and manage your AWS costs and usage over time
- Create custom reports that analyze cost and usage data.
- Analyze your data at a high level: total costs and usage across all accounts
- Or Monthly, hourly, resource level granularity
- Choose an optimal Savings Plan (to lower prices on your bill)
- Forecast usage up to 12 months based on previous usage

Question 89:

A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that, if a production CloudFormation stack is deleted, important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted.

How can the company prevent users from accidentally deleting data in this way?

- A. Modify the CloudFormation templates to add a `DeletionPolicy` attribute to RDS and EBS resources.
- B. Configure a stack policy that disallows the deletion of RDS and EBS resources.
- C. Modify IAM policies to deny deleting RDS and EBS resources that are tagged with an "aws:cloudformation:stack-name" tag.
- D. Use AWS Config rules to prevent deleting RDS and EBS resources.

A

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html>

Retaining Data on Deletes Giữ lại dữ liệu khi xóa

- You can put a `DeletionPolicy` on any resource to control what happens when the CloudFormation template is deleted
- **DeletionPolicy=Retain:** duy trì
 - Specify on resources to preserve / backup in case of CloudFormation deletes
 - To keep a resource, specify `Retain` (works for any resource / nested stack)
- **DeletionPolicy=Snapshot:**
 - EBS Volume, ElastiCache Cluster, ElastiCache ReplicationGroup
 - RDS DBInstance, RDS DBCluster, Redshift Cluster
- **DeletePolicy=Delete (default behavior):**
 - Note: for `AWS::RDS::DBCluster` resources, the default policy is `Snapshot`
 - Note: to delete an S3 bucket, you need to first empty the bucket of its content

Question 90:

A company has VPC flow logs enabled for its NAT gateway. The company is seeing Action = ACCEPT for inbound traffic that comes from public IP address 198.51.100.2 destined for a private Amazon EC2 instance.

A solutions architect must determine whether the traffic represents unsolicited inbound connections from the internet. The first two octets of the VPC CIDR block are 203.0.

Which set of steps should the solutions architect take to meet these requirements?

A. Open the AWS CloudTrail console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

B. Open the Amazon CloudWatch console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

C. Open the AWS CloudTrail console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

D. Open the Amazon CloudWatch console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

B

VPC Flow Logs

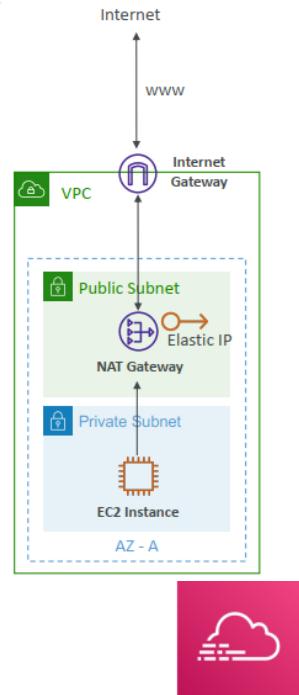


- Capture information about IP traffic going into your interfaces:
 - VPC Flow Logs
 - Subnet Flow Logs
 - Elastic Network Interface (ENI) Flow Logs
- Helps to monitor & troubleshoot connectivity issues
- Flow logs data can go to S3, CloudWatch Logs, and Kinesis Data Firehose
- Captures network information from AWS managed interfaces too: ELB, RDS, ElastiCache, Redshift, WorkSpaces, NATGW, Transit Gateway...

VPC Flow Logs – with NAT Gateway

- My Virtual Private Cloud (VPC) flow logs show Action = ACCEPT for inbound traffic coming from public IP addresses. However, my understanding of network address translation (NAT) gateways was that they don't accept traffic from the internet. Is my NAT gateway accepting inbound traffic from the internet?
- Inbound traffic is permitted by Security Group or NACLs
 - Traffic isn't permitted by the NAT Gateway, it's dropped
 - To confirm run the following query in CloudWatch Log Group

```
filter (dstAddr like 'xxx.xxx' and srcAddr like 'public IP') | stats sum(bytes) as bytesTransferred by srcAddr, dstAddr | limit 10
```
- Make 'xxx.xxx' the first two octets of your VPC CIDR
- Replace Public IP with the IP you see in logs
- You will see traffic on the Private IP of the NAT Gateway but nowhere else: traffic was unsolicited and then dropped



AWS CloudTrail

- Provides governance, compliance and audit for your AWS Account
- CloudTrail is enabled by default!
- Get an history of events / API calls made within your AWS Account by:
 - Console
 - SDK
 - CLI
 - AWS Services
- Can put logs from CloudTrail into CloudWatch Logs or S3
- A trail can be applied to All Regions (default) or a single Region.
- If a resource is deleted in AWS, investigate CloudTrail first!

Question 91:

A company consists of two separate business units. Each business unit has its own AWS account within a single organization in AWS Organizations. The business units regularly share sensitive documents with each other. To facilitate sharing, the company created an Amazon S3 bucket in each account and configured low-way replication between the S3 buckets. The S3 buckets have millions of objects.

Recently, a security audit identified that neither S3 bucket has encryption at rest enabled. Company policy requires that all documents must be stored with encryption at rest. The company wants to implement server-side encryption with Amazon S3 managed encryption keys (SSE-S3).

What is the MOST operationally efficient solution that meets these requirements?

- A. Turn on SSE-S3 on both S3 buckets. Use S3 Batch Operations to copy and encrypt the objects in the same location.
- B. Create an AWS Key Management Service (AWS KMS) key in each account. Turn on server-side encryption with AWS KMS keys (SSE-KMS) on each S3 bucket by using the corresponding KMS key in that AWS account. Encrypt the existing objects by using an S3 copy command in the AWS CLI.
- C. Turn on SSE-S3 on both S3 buckets. Encrypt the existing objects by using an S3 copy command in the AWS CLI.
- D. Create an AWS Key Management Service, (AWS KMS) key in each account. Turn on server-side encryption with AWS KMS keys (SSE-KMS) on each S3 bucket by using the corresponding KMS key in that AWS account. Use S3 Batch Operations to copy the objects into the same location.

A.

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

LAB: <https://aws.amazon.com/blogs/aws/new-amazon-s3-batch-operations/>

The new Amazon S3 Batch Operations feature lets you perform repetitive or bulk actions like copying or tagging across millions of objects with a single request.

Batch Operations Info

A job is used to execute batch operations on a list of S3 objects. The list of S3 objects is contained in a manifest object, which can be an S3 inventory report or a list of objects that you generate. After the total number of objects listed in the manifest has been confirmed, the job status will update to *Awaiting your confirmation to run*, and you must **Run job** within 30 days. Job events are published to [CloudWatch Events](#). Jobs are deleted 90 days after they finish or fail. [Learn more](#)

The screenshot shows the 'Batch Operations' page in the Amazon S3 console. At the top, there's a search bar labeled 'Search by job ID or description' and a dropdown menu set to 'All status types'. Below the header is a table with the following columns: Job ID, Status, Description, Operation, Date created, Total objects, % Complete, Total failed (rate), and Priority. A 'Create job' button is located at the bottom left of the table area. A message 'You don't have any jobs in the Asia Pacific (Singapore) ap-southeast-1 Region' is displayed in the center of the table area.

Question 92:

A company is running an application in the AWS Cloud. The application collects and stores a large amount of unstructured data in an Amazon S3 bucket. The S3 bucket contains several terabytes of data and uses the S3 Standard storage class. The data increases in size by several gigabytes every day.

The company needs to query and analyze the data. The company does not access data that is more than 1 year old. However, the company must retain all the data indefinitely for compliance reasons.

Which solution will meet these requirements MOST cost-effectively?

- A. Use S3 Select to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- B. Use Amazon Redshift Spectrum to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- C. Use an AWS Glue Data Catalog and Amazon Athena to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- D. Use Amazon Redshift Spectrum to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Intelligent-Tiering.

C

<https://www.upsolver.com/blog/aws-serverless-redshift-spectrum-athena>

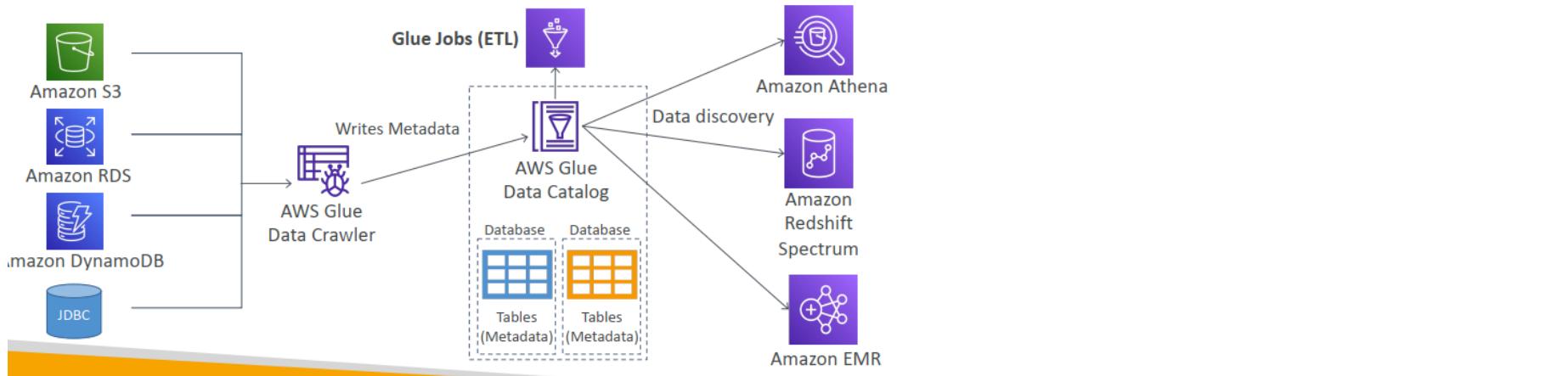
Redshift is used in structure data (SQL)

Athena is used in unstructured data (noSQL)

Glue Data Catalog



- Glue Data Catalog: catalog of datasets



Question 93:

A video processing company wants to build a machine learning (ML) model by using 600 TB of compressed data that is stored as thousands of files in the company's on-premises network attached storage system. The company does not have the necessary compute resources on premises and wants to use AWS.

The company needs to complete the data transfer to AWS within 3 weeks. The data transfer will be a one-time transfer. The data must be encrypted in transit. The measured upload speed of the company's internet connection is 100 Mbps. and multiple departments share the connection.

Which solution will meet these requirements MOST cost-effectively?

- Order several AWS Snowball Edge Storage Optimized devices by using the AWS Management Console. Configure the devices with a destination S3 bucket. Copy the data to the devices. Ship the devices back to AWS.
- Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.
- Create a VPN connection between the on-premises network attached storage and the nearest AWS Region. Transfer the data over the VPN connection.

D. Deploy an AWS Storage Gateway file gateway on premises. Configure the file gateway with a destination S3 bucket. Copy the data to the file gateway.

A

This option will meet the requirements to complete the data transfer within 3 weeks, as the Snowball Edge devices can transfer large amounts of data quickly and securely. The data will be encrypted in transit and at rest. The company's internet connection speed is not a bottleneck as the data transfer will happen on the devices and not over the internet.

AWS Snow Family

- Highly-secure, portable devices to collect and process data at the edge, and migrate data into and out of AWS

- Data migration:



Snowcone



Snowball Edge



Snowmobile

- Edge computing:



Snowcone



Snowball Edge

Question 94:

A company has migrated its forms-processing application to AWS. When users interact with the application, they upload scanned forms as files through a web application. A database stores user metadata and references to files that are stored in Amazon S3. The web application runs on Amazon EC2 instances and an Amazon RDS for PostgreSQL database.

When forms are uploaded, the application sends notifications to a team through Amazon Simple Notification Service (Amazon SNS). A team member then logs in and processes each form. The team member performs data validation on the form and extracts relevant data before entering the information into another system that uses an API.

A solutions architect needs to automate the manual processing of the forms. The solution must provide accurate form extraction, minimize time to market, and minimize long-term operational overhead.

Which solution will meet these requirements?

A. Develop custom libraries to perform optical character recognition (OCR) on the forms. Deploy the libraries to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster as an application tier. Use this tier to process the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data into an Amazon DynamoDB table. Submit the data to the target system's API. Host the new application tier on EC2 instances.

B. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use artificial intelligence and machine learning (AI/ML) models that are trained and hosted on an EC2 instance to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.

C. Host a new application tier on EC2 instances. Use this tier to call endpoints that host artificial intelligence and machine teaming (AI/ML) models that are trained and hosted in Amazon SageMaker to perform optical character recognition (OCR) on the forms. Store the output in Amazon ElastiCache. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.

D. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.

D

This solution meets the requirements of accurate form extraction, minimal time to market, and minimal long-term operational overhead. Amazon Textract and Amazon Comprehend are fully managed and serverless services that can perform OCR and extract relevant data from the forms, which eliminates the need to develop custom libraries or train and host models. Using AWS Step Functions and Lambda allows for easy automation of the process and the ability to scale as needed.

AWS Step Functions

- Build serverless visual workflow to orchestrate your Lambda functions
- Represent flow as a JSON state machine
- Features: sequence, parallel, conditions, timeouts, error handling...
- Maximum execution time of 1 year
- Possibility to implement human approval feature
- If you chain Lambda functions using Step Functions, be mindful of the added latency to pass the calls.



Hãy chú ý đến thêm độ trễ

Amazon Comprehend Medical



- Amazon Comprehend Medical detects and returns useful information in unstructured clinical text:
 - Physician's notes
 - Discharge summaries Tóm tắt xuất viện
 - Test results
 - Case notes
- Uses NLP to detect Protected Health Information (PHI) – DetectPHI API
- Store your documents in Amazon S3, analyze real-time data with Kinesis Data Firehose, or use Amazon Transcribe to transcribe patient narratives chuyển lời bệnh nhân thành dạng văn bản into text that can be analyzed by Amazon Comprehend Medical.

Amazon Textract



- Automatically extracts text, handwriting, and data from any scanned documents using AI and ML



- Extract data from forms and tables
- Read and process any type of document (PDFs, images, ...)
- Use cases:
 - Financial Services (e.g., invoices, financial reports)
 - Healthcare (e.g., medical records, insurance claims)
 - Public Sector (e.g., tax forms, ID documents, passports)

Question 95:

A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs, RabbitMQ to connect the front end to the backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- B. Create a custom AWS Lambda runtime to mimic the web server environment. Create an Amazon API Gateway API to replace the front-end web servers. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- C. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up Amazon MQ to replace the on-premises messaging queue. Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend.
- D. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.

A

Amazon MQ



- SQS, SNS are “cloud-native” services: dộc quyền proprietary protocols from AWS
- Traditional applications running from on-premises may use open protocols such as: MQTT, AMQP, STOMP, Openwire, WSS
- When migrating to the cloud, instead of re-engineering the application to use SQS and SNS, we can use Amazon MQ
- Amazon MQ is a managed message broker service for



- Amazon MQ doesn't “scale” as much as SQS / SNS
- Amazon MQ runs on servers, can run in Multi-AZ with failover
- Amazon MQ has both queue feature (~SQS) and topic features (~SNS)

Question 96:

A solutions architect needs to implement a client-side encryption mechanism for objects that will be stored in a new Amazon S3 bucket. The solutions architect created a CMK that is stored in AWS Key Management Service (AWS KMS) for this purpose.

The solutions architect created the following IAM policy and attached it to an IAM role:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "DownloadUpload",  
            "Action": [  
                "s3:GetObject",  
                "s3:GetObjectVersion",  
                "s3:PutObject",  
                "s3:PutObjectAcl"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:s3:::BucketName/*"  
        },  
        {  
            "Sid": "KMSAccess",  
            "Action": [  
                "kms:Decrypt",  
                "kms:Encrypt"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:kms:Region:Account:key/Key ID"  
        }  
    ]  
}
```

During tests, the solutions architect was able to successfully get existing test objects in the S3 bucket. However, attempts to upload a new object resulted in an error message. The error message stated that the action was forbidden.

Which action must the solutions architect add to the IAM policy to meet all the requirements?

- A. kms:GenerateDataKey
- B. kms:GetKeyPolicy
- C. kms:GetPublicKey
- D. kms:Sign

A

S3 Encryption for Objects

- SSE-S3: encrypts S3 objects using keys handled & managed by AWS
- SSE-KMS: leverage KMS to manage encryption keys
 - Key usage appears in CloudTrail
 - objects made public can never be read
 - On `s3:PutObject`, make the permission kms:GenerateDataKey is allowed
- SSE-C: when you want to manage your own encryption keys
- Client-Side Encryption
- Glacier: all data is AES-256 encrypted, key under AWS control

Question 97:

A company has developed a web application. The company is hosting the application on a group of Amazon EC2 instances behind an Application Load Balancer. The company wants to improve the security posture of the application and plans to use AWS WAF web ACLs. The solution must not adversely affect legitimate traffic to the application.

How should a solutions architect configure the web ACLs to meet these requirements?

- A. Set the action of the web ACL rules to Count. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Count to Block.

B. Use only rate-based rules in the web ACLs, and set the throttle limit as high as possible. Temporarily block all requests that exceed the limit. Define nested rules to narrow the scope of the rate tracking.

C. Set the action of the web ACL rules to Block. Use only AWS managed rule groups in the web ACLs. Evaluate the rule groups by using Amazon CloudWatch metrics with AWS WAF sampled requests or AWS WAF logs.

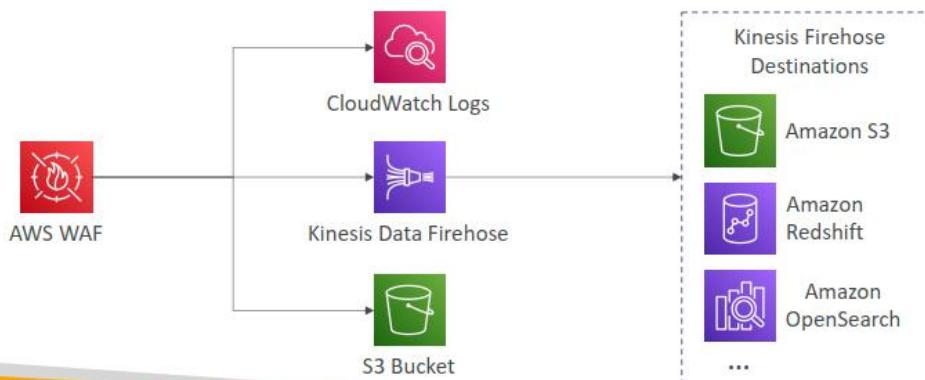
D. Use only custom rule groups in the web ACLs, and set the action to Allow. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Allow to Block.

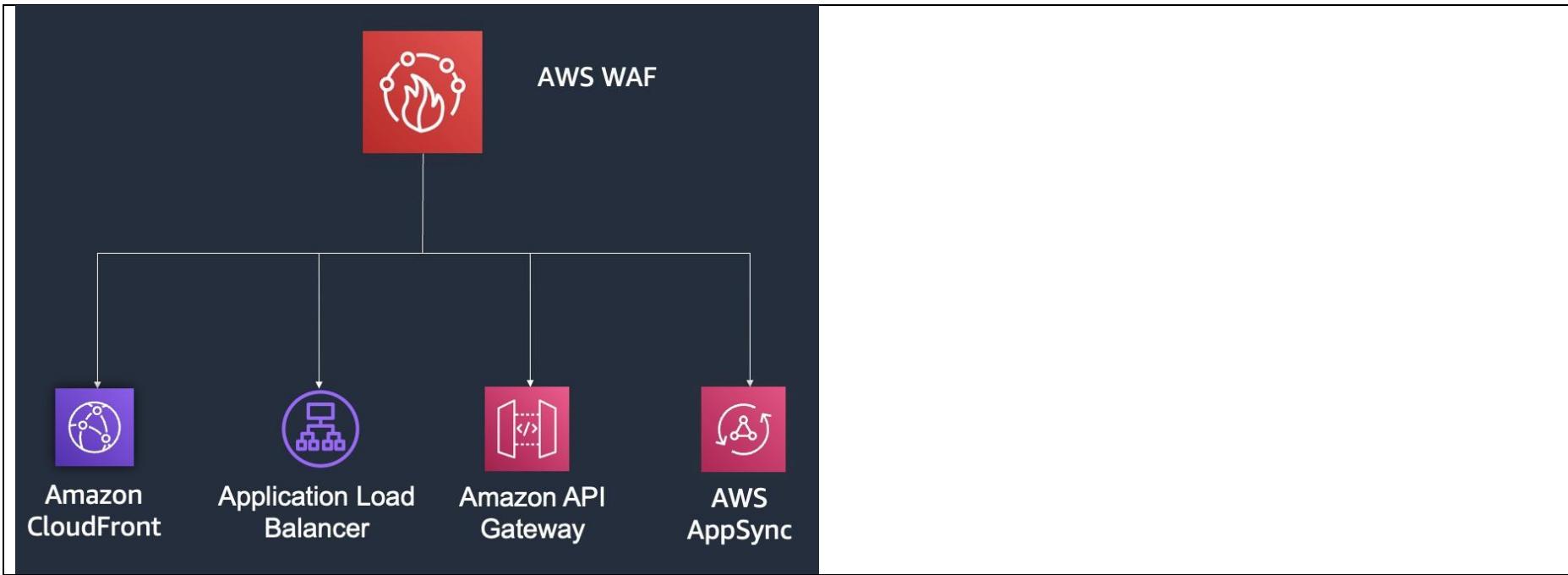
A

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing.html>

WAF - Web ACL – Logging

- You can send your logs to an:
 - Amazon CloudWatch Logs log group – 5 MB per second
 - Amazon Simple Storage Service (Amazon S3) bucket – 5 minutes interval
 - Amazon Kinesis Data Firehose – limited by Firehose quotas





Question 98:

A company has an organization that has many AWS accounts in AWS Organizations. A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.

The company has a common set of IP CIDR ranges in an allow list in each AWS account to allow access to and from the company's on-premises network. Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list.

The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts.

Which solution meets these requirements with the LEAST amount of operational overhead?

A. Set up an Amazon Simple Notification Service (Amazon SNS) topic in the security team's AWS account. Deploy an AWS Lambda function in each AWS account. Configure the Lambda function to run every time an SNS topic receives a message. Configure the Lambda function to take an IP address as input and add it to a list of security groups in the account. Instruct the security team to distribute changes by publishing messages to its SNS topic.

B. Create new customer-managed prefix lists in each AWS account within the organization. Populate the prefix lists in each account with all internal CIDR ranges. Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups. Instruct the security team to share updates with each AWS account owner.

C. Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.

D. Create an IAM role in each account in the organization. Grant permissions to update security groups. Deploy an AWS Lambda function in the security team's AWS account. Configure the Lambda function to take a list of internal IP addresses as input, assume a role in each organization account, and add the list of IP addresses to the security groups in each account.

C

Resource Access Manager Managed Prefix List

- A set of one or more CIDR blocks
- Makes it easier to configure and maintain Security Groups and Route Tables
- Customer-Managed Prefix List
 - Set of CIDRs that you define and manage by you
 - Can be shared with other AWS accounts or AWS Organization
 - Modify to update many security groups at once
- AWS-Managed Prefix List
 - Set of CIDRs for AWS services
 - You can't create, modify, share, or delete them



Jane Maarek

Question 99:

A company has introduced a new policy that allows employees to work remotely from their homes if they connect by using a VPN. The company is hosting internal applications with VPCs in multiple AWS accounts. Currently, the applications are accessible from the company's on-premises office network through an AWS Site-to-Site VPN connection. The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts.

A solutions architect must design a scalable AWS Client VPN solution for employees to use while they work from home.

What is the MOST cost-effective solution that meets these requirements?

- A. Create a Client VPN endpoint in each AWS account. Configure required routing that allows access to internal applications.
- B. Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications.
- C. Create a Client VPN endpoint in the main AWS account. Provision a transit gateway that is connected to each AWS account. Configure required routing that allows access to internal applications.
- D. Create a Client VPN endpoint in the main AWS account. Establish connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN.

B

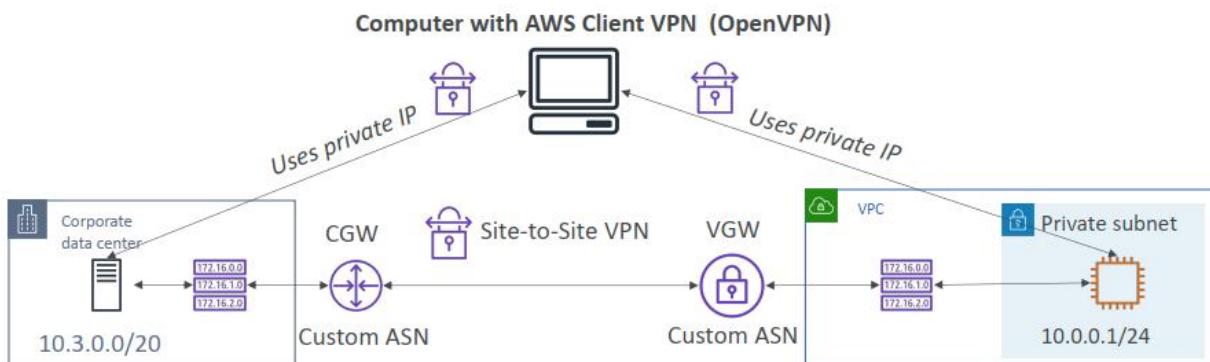
Option B: - the question is asking for " MOST cost-effective" solution. AWS Transit gateway charged for the number of connections that you make to the Transit Gateway per hour and the amount of traffic that flows through AWS Transit Gateway. AWS Site-to-Site VPN connection pricing still applies in addition to AWS Transit Gateway VPN attachment pricing.

AWS Client VPN is a fully-managed remote access VPN solution used by your remote workforce to securely access resources within both AWS and your on-premises network. Fully elastic, it automatically scales up, or down, based on demand.

AWS Client VPN



- Connect from your computer using OpenVPN to your private network in AWS and on-premises



Question 100:

A company is running an application in the AWS Cloud. Recent application metrics show inconsistent response times and a significant increase in error rates. Calls to third-party services are causing the delays. Currently, the application calls third-party services synchronously by directly invoking an AWS Lambda function.

A solutions architect needs to decouple the third-party service calls and ensure that all the calls are eventually completed.

Which solution will meet these requirements?

- A. Use an Amazon Simple Queue Service (Amazon SQS) queue to store events and invoke the Lambda function.
- B. Use an AWS Step Functions state machine to pass events to the Lambda function.
- C. Use an Amazon EventBridge rule to pass events to the Lambda function.
- D. Use an Amazon Simple Notification Service (Amazon SNS) topic to store events and Invoke the Lambda function.

A

Using an Amazon Simple Queue Service (SQS) queue to store events and invoke the Lambda function is a good solution to decouple the third-party service calls and ensure that all the calls are eventually completed. SQS is a fully managed, reliable, and highly scalable message queuing service that allows applications to send, store, and receive messages between distributed components. By sending the third-party service calls to an SQS queue, it allows the application to continue processing without waiting for the third-party services to respond, which can result in faster response times and lower error rates.

Question 101:

A company is running applications on AWS in a multi-account environment. The company's sales team and marketing team use separate AWS accounts in AWS Organizations.

The sales team stores petabytes of data in an Amazon S3 bucket. The marketing team uses Amazon QuickSight for data visualizations. The marketing team needs access to data that the sales team stores in the S3 bucket. The company has encrypted the S3 bucket with an AWS Key Management Service (AWS KMS) key. The marketing team has already created the IAM service role for QuickSight to provide QuickSight access in the marketing AWS account. The company needs a solution that will provide secure access to the data in the S3 bucket across AWS accounts.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new S3 bucket in the marketing account. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket.
- B. Create an SCP to grant access to the S3 bucket to the marketing account. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- C. Update the S3 bucket policy in the marketing account to grant access to the QuickSight role. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- D. Create an IAM role in the sales account and grant access to the S3 bucket. From the marketing account, assume the IAM role in the sales account to access the S3 bucket. Update the QuickSight role, to create a trust relationship with the new IAM role in the sales account.

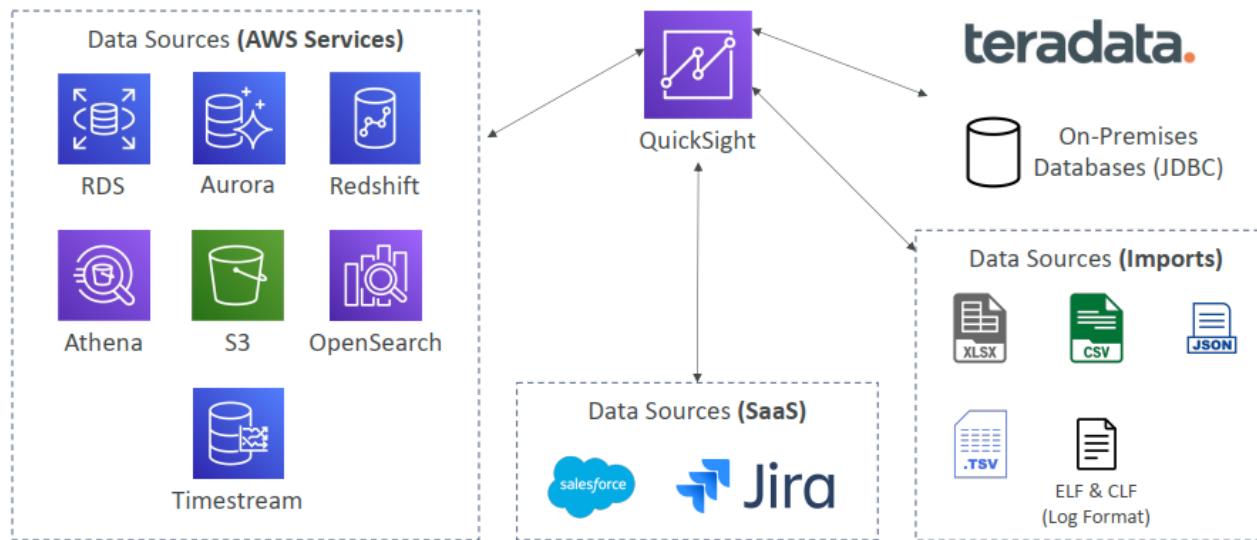
D

This solution meets the requirements by allowing the marketing team to access the data in the S3 bucket in the sales account through assuming an IAM role, which eliminates the need to copy the data or share the KMS key, and also eliminates the need to modify the S3 bucket policy or create a KMS grant. This solution allows to use the same access to the bucket without duplicating data and re-encrypting it.

A. Create a new S3 bucket in the marketing account. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket is not correct because it would create unnecessary data duplication and increased storage costs.

B. Create an SCP to grant access to the S3 bucket to the marketing account. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket is not correct because it does not provide a secure way to share the KMS key between accounts and also it would create unnecessary data duplication and increased storage costs.

QuickSight Integrations



Question 102:

A company is planning to migrate its business-critical applications from an on-premises data center to AWS. The company has an on-premises installation of a Microsoft SQL Server Always On cluster. The company wants to migrate to an AWS managed database service. A solutions architect must design a heterogeneous database migration on AWS.

Which solution will meet these requirements?

- A. Migrate the SQL Server databases to Amazon RDS for MySQL by using backup and restore utilities.

B. Use an AWS Snowball Edge Storage Optimized device to transfer data to Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.

C. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MySQL. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.

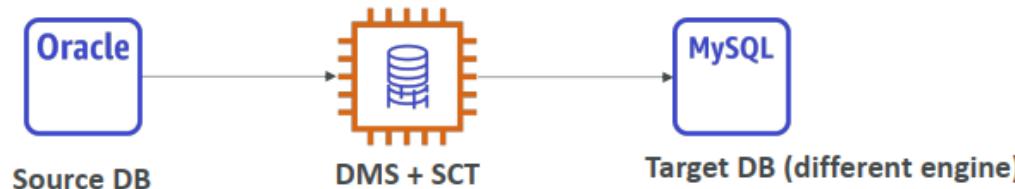
D. Use AWS DataSync to migrate data over the network between on-premises storage and Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.

C

must design a heterogeneous database migration on AWS → that mean is not the same engine → SCT

AWS Schema Conversion Tool (SCT)

- Convert your Database's Schema from one engine to another
- Example OLTP: (SQL Server or Oracle) to MySQL, PostgreSQL, Aurora
- Example OLAP: (Teradata or Oracle) to Amazon Redshift



- You do not need to use SCT if you are migrating the same DB engine
 - Ex: on-premises PostgreSQL => RDS PostgreSQL
 - The DB engine is still PostgreSQL (RDS is the platform)

Question 103:

A publishing company's design team updates the icons and other static assets that an ecommerce web application uses. The company serves the icons and assets from an Amazon S3 bucket that is hosted in the company's production account. The company also uses a development account that members of the design team can access.

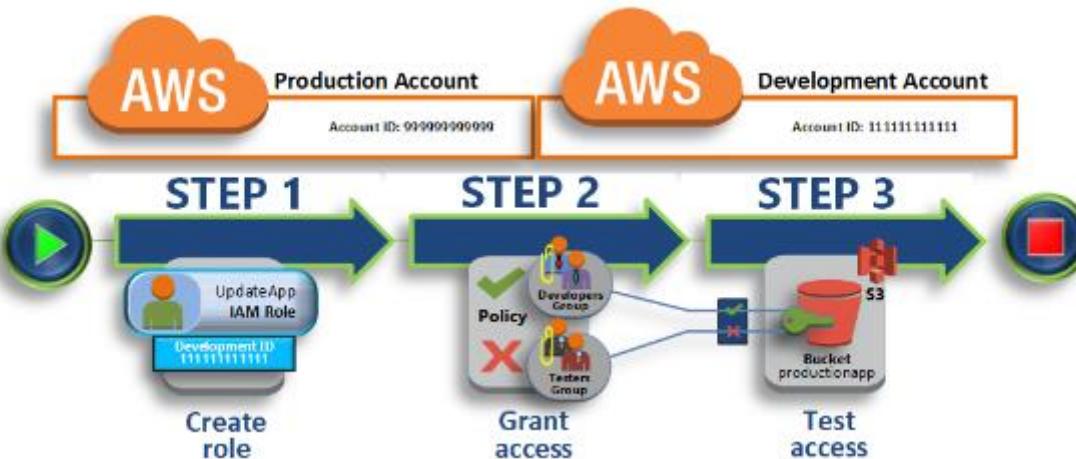
After the design team tests the static assets in the development account, the design team needs to load the assets into the S3 bucket in the production account. A solutions architect must provide the design team with access to the production account without exposing other parts of the web application to the risk of unwanted changes.

Which combination of steps will meet these requirements? (Choose three.)

- A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket.
- B. In the development account, create a new IAM policy that allows read and write access to the S3 bucket.
- C. In the production account, create a role. Attach the new policy to the role. Define the development account as a trusted entity.
- D. In the development account, create a role. Attach the new policy to the role Define the production account as a trusted entity.
- E. In the development account, create a group that contains all the IAM users of the design team. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account.
- F. In the development account, create a group that contains all the IAM users of the design team Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the development account.

A,C,E

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html



1. Create a role in the Destination Account (production account)

```
{  
  "Version": "2012-10-17",
```

```

"Statement": [
    {
        "Effect": "Allow",
        "Action": "s3>ListAllMyBuckets",
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3>ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws:s3:::shared-container"
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3GetObject",
            "s3PutObject",
            "s3DeleteObject"
        ],
        "Resource": "arn:aws:s3:::shared-container/*"
    }
]
}

```

2. Grant access to the role (development account)

```

{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "stsAssumeRole",
        "Resource": "arn:aws:iam::PRODUCTION-ACCOUNT-ID:role/UpdateData"
    }
}

```

Question 104:

A company developed a pilot application by using AWS Elastic Beanstalk and Java. To save costs during development, the company's development team deployed the application into a single-instance environment. Recent tests indicate that the application consumes more CPU than expected. CPU utilization is regularly greater than 85%, which causes some performance bottlenecks.

A solutions architect must mitigate the performance issues before the company launches the application to production.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new Elastic Beanstalk application. Select a load-balanced environment type. Select all Availability Zones. Add a scale-out rule that will run if the maximum CPU utilization is over 85% for 5 minutes.
- B. Create a second Elastic Beanstalk environment. Apply the traffic-splitting deployment policy. Specify a percentage of incoming traffic to direct to the new environment if the average CPU utilization is over 85% for 5 minutes.
- C. Modify the existing environment's capacity configuration to use a load-balanced environment type. Select all Availability Zones. Add a scale-out rule that will run if the average CPU utilization is over 85% for 5 minutes.
- D. Select the Rebuild environment action with the load balancing option. Select an Availability Zones. Add a scale-out rule that will run if the sum CPU utilization is over 85% for 5 minutes.

C

LEAST operational overhead ➔ A,B,D are incorrect

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

AWS Elastic Beanstalk Overview



- Elastic Beanstalk is a developer centric view of deploying an application on AWS
- It uses all the components we've seen before:
EC2, Auto Scaling Group, Elastic Load Balancers, RDS, etc...
- But it's all in one view that's easy to make sense of!
- We still have full control over the configuration of each component
- Beanstalk is free but you pay for the underlying instances

In AWS Elastic Beanstalk, you can create a load-balanced, scalable environment or a single-instance environment. The type of environment that you require depends on the application that you deploy. For example, you can develop and test an application in a single-instance environment to save costs and then upgrade that environment to a load-balanced, scalable environment when the application is ready for production.

Question 105:

A finance company is running its business-critical application on current-generation Linux EC2 instances. The application includes a self-managed MySQL database performing heavy I/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand.

Which of the following actions would allow the database to handle the month-end load with the LEAST impact on performance?

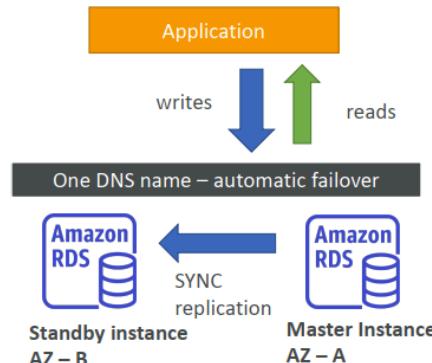
- A. Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes.
- B. Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.
- C. Using Amazon CloudWatch with AWS Lambda to change the type, size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric.
- D. Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards.

B

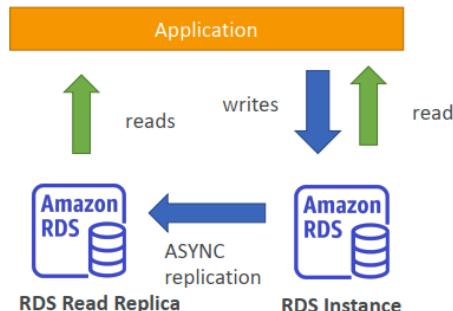
This is the optimal solution as migrating the database to Amazon RDS will provide the ability to easily scale read replicas for handling increased read traffic during the end of the month. Additionally, RDS will manage the underlying infrastructure and provide automatic backups, software patching, and monitoring, which will reduce the operational overhead for the company.

RDS – Multi AZ & Read Replicas

- Multi-AZ: Standby instance for failover in case of outage



- Read Replicas: Increase read throughput. Eventual consistency. Can be cross-region.

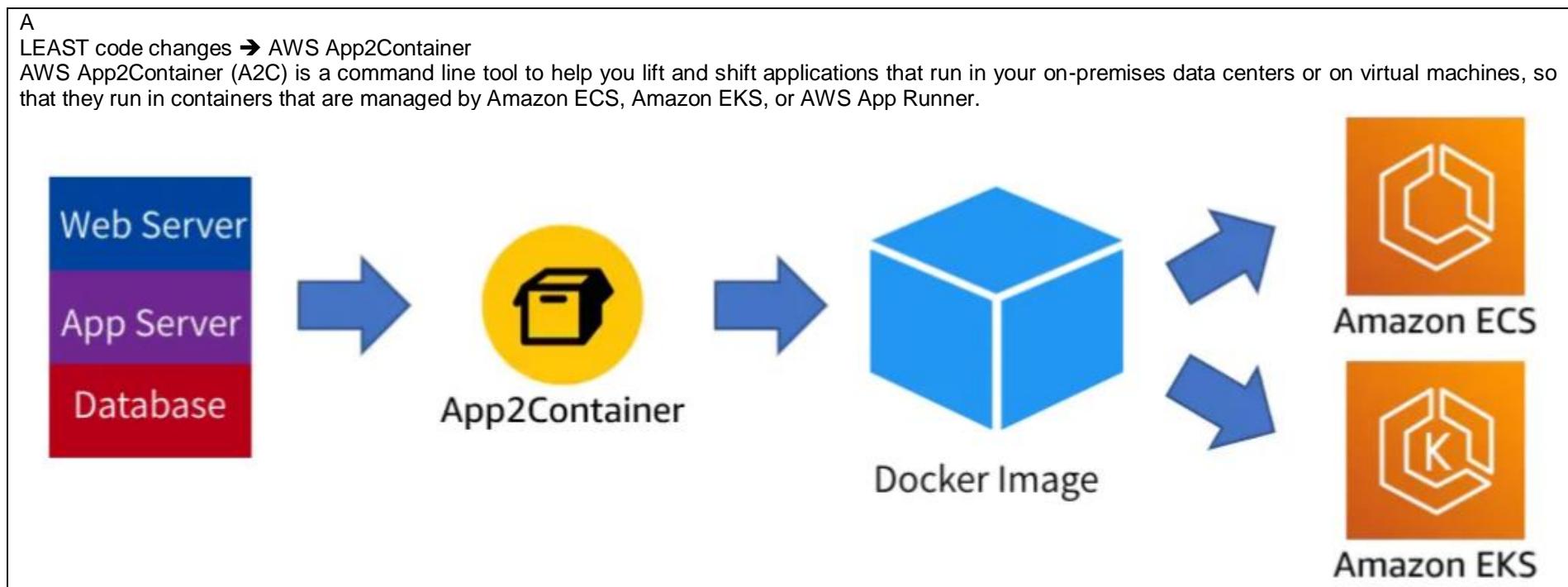


Question 106:

A company runs a Java application that has complex dependencies on VMs that are in the company's data center. The application is stable, but the company wants to modernize the technology stack. The company wants to migrate the application to AWS and minimize the administrative overhead to maintain the servers.

Which solution will meet these requirements with the LEAST code changes?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Grant the ECS task execution role permission to access the ECR image repository. Configure Amazon ECS to use an Application Load Balancer (ALB). Use the ALB to interact with the application.
- B. Migrate the application code to a container that runs in AWS Lambda. Build an Amazon API Gateway REST API with Lambda integration. Use API Gateway to interact with the application.
- C. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) on EKS managed node groups by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Give the EKS nodes permission to access the ECR image repository. Use Amazon API Gateway to interact with the application.
- D. Migrate the application code to a container that runs in AWS Lambda. Configure Lambda to use an Application Load Balancer (ALB). Use the ALB to interact with the application.



Question 107:

A company has an asynchronous HTTP application that is hosted as an AWS Lambda function. A public Amazon API Gateway endpoint invokes the Lambda function. The Lambda function and the API Gateway endpoint reside in the us-east-1 Region. A solutions architect needs to redesign the application to support failover to another AWS Region.

Which solution will meet these requirements?

- Create an API Gateway endpoint in the us-west-2 Region to direct traffic to the Lambda function in us-east-1. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.
- Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure API Gateway to direct traffic to the SQS queue instead of to the Lambda function. Configure the Lambda function to pull messages from the queue for processing.
- Deploy the Lambda function to the us-west-2 Region. Create an API Gateway endpoint in us-west-2 to direct traffic to the Lambda function in us-west-2. Configure AWS Global Accelerator and an Application Load Balancer to manage traffic across the two API Gateway endpoints.
- Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.

D

<https://aws.amazon.com/blogs/architecture/implementing-multi-region-disaster-recovery-using-event-driven-architecture/>

failover to another AWS Region → Amazon Route 53 to use a failover routing policy

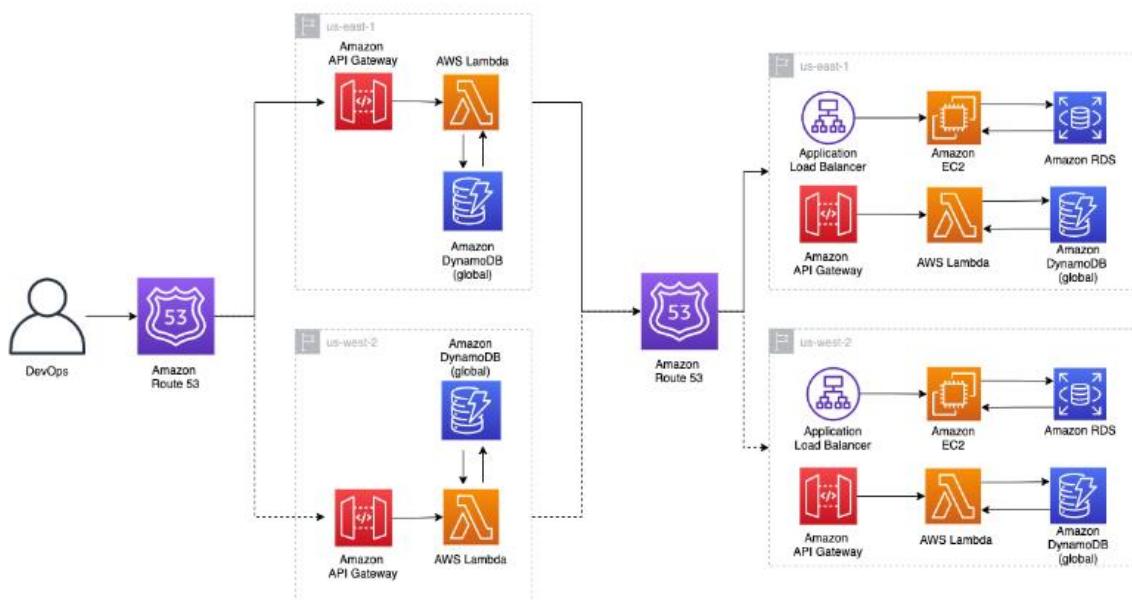


Figure 2. DR implementation architecture on multi-Region active/passive workloads

Question 108:

A retail company has structured its AWS accounts to be part of an organization in AWS Organizations. The company has set up consolidated billing and has mapped its departments to the following OUs: Finance, Sales, Human Resources (HR), Marketing, and Operations. Each OU has multiple AWS accounts, one for each environment within a department. These environments are development, test, pre-production, and production.

The HR department is releasing a new system that will launch in 3 months. In preparation, the HR department has purchased several Reserved Instances (RIs) in its production AWS account. The HR department will install the new application on this account. The HR department wants to make sure that other departments cannot share the RI discounts.

Which solution will meet these requirements?

- A. In the AWS Billing and Cost Management console for the HR department's production account turn off RI sharing.
- B. Remove the HR department's production AWS account from the organization. Add the account to the consolidating billing configuration only.
- C. In the AWS Billing and Cost Management console, use the organization's management account, turn off RI Sharing for the HR department's production AWS account.
- D. Create an SCP in the organization to restrict access to the RIs. Apply the SCP to the OUs of the other departments.

C

Reserved Instances

- Reserved Instances in an AWS Organization
 - all accounts share the Reserved Instances and Savings Plan
 - The payer account (Management account) of an organization can turn off Reserved Instance (RI) discount and Savings Plans discount sharing for any accounts in that organization, including the payer account
- Renewal of Reserved Instances
 - You can queue (schedule and reserve ahead of time) your reserved instances
 - To renew a RI, just queue an RI purchase whenever the previous one expires

Management account --> Billing Dashboard --> Billing preferences, this option is there to choose enable/disable RI discounts sharing
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

You can deactivate sharing discounts for individual member accounts.
To deactivate shared Reserved Instances and Savings Plans discounts
Sign in to the AWS Management Console and open the AWS Billing and Cost Management console at <https://console.aws.amazon.com/billing/>.
In the navigation pane, choose **Billing preferences**.
Under **Reserved Instances and Savings Plans discount sharing preference by account**, select the accounts that you want to deactivate discount sharing for.
Choose **Deactivate**.
In the **Deactivate Reserved Instance and Savings Plan sharing** dialog box, choose **Deactivate**.

Question 109:

A large company is running a popular web application. The application runs on several Amazon EC2 Linux instances in an Auto Scaling group in a private subnet. An Application Load Balancer is targeting the instances in the Auto Scaling group in the private subnet. AWS Systems Manager Session Manager is configured, and AWS Systems Manager Agent is running on all the EC2 instances.

The company recently released a new version of the application. Some EC2 instances are now being marked as unhealthy and are being terminated. As a result, the application is running at reduced capacity. A solutions architect tries to determine the root cause by analyzing Amazon CloudWatch logs that are collected from the application, but the logs are inconclusive.

How should the solutions architect gain access to an EC2 instance to troubleshoot the issue?

- A. Suspend the Auto Scaling group's HealthCheck scaling process. Use Session Manager to log in to an instance that is marked as unhealthy.
- B. Enable EC2 instance termination protection. Use Session Manager to log in to an instance that is marked as unhealthy.
- C. Set the termination policy to OldestInstance on the Auto Scaling group. Use Session Manager to log in to an instance that is marked as unhealthy.
- D. Suspend the Auto Scaling group's Terminate process. Use Session Manager to log in to an instance that is marked as unhealthy.

D

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html>

This topic describes how to suspend and then resume one or more of the processes for your Auto Scaling group to temporarily disable certain operations. Suspending processes can be useful when you need to investigate or troubleshoot an issue without interference from scaling policies or scheduled actions. It also helps prevent Amazon EC2 Auto Scaling from marking instances unhealthy and replacing them while you are making changes to your Auto Scaling group.

Question 110:

A company wants to deploy an AWS WAF solution to manage AWS WAF rules across multiple AWS accounts. The accounts are managed under different OUs in AWS Organizations.

Administrators must be able to add or remove accounts or OUs from managed AWS WAF rule sets as needed. Administrators also must have the ability to automatically update and remediate noncompliant AWS WAF rules in all accounts.

Which solution meets these requirements with the LEAST amount of operational overhead?

HANCHE

A. Use AWS Firewall Manager to manage AWS WAF rules across accounts in the organization. Use an AWS Systems Manager Parameter Store parameter to store account numbers and OUs to manage. Update the parameter as needed to add or remove accounts or OUs. Use an Amazon EventBridge rule to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account.

B. Deploy an organization-wide AWS Config rule that requires all resources in the selected OUs to associate the AWS WAF rules. Deploy automated remediation actions by using AWS Lambda to fix noncompliant resources. Deploy AWS WAF rules by using an AWS CloudFormation stack set to target the same OUs where the AWS Config rule is applied.

C. Create AWS WAF rules in the management account of the organization. Use AWS Lambda environment variables to store account numbers and OUs to manage. Update environment variables as needed to add or remove accounts or OUs. Create cross-account IAM roles in member accounts. Assume the roles by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts.

D. Use AWS Control Tower to manage AWS WAF rules across accounts in the organization. Use AWS Key Management Service (AWS KMS) to store account numbers and OUs to manage. Update AWS KMS as needed to add or remove accounts or OUs. Create IAM users in member accounts. Allow AWS Control Tower in the management account to use the access key and secret access key to create and update AWS WAF rules in the member accounts.

A

<https://aws.amazon.com/solutions/implementations/automations-for-aws-firewall-manager/>

<https://aws.amazon.com/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/>

<https://docs.aws.amazon.com/solutions/latest/automations-for-aws-firewall-manager/architecture-overview.html>

AWS Firewall Manager



- Manage rules in all accounts of an AWS Organization
- Security policy: common set of security rules
 - WAF rules (Application Load Balancer, API Gateways, CloudFront)
 - AWS Shield Advanced (ALB, CLB, NLB, Elastic IP, CloudFront)
 - Security Groups for EC2, Application Load Balancer and ENI resources in VPC
 - AWS Network Firewall (VPC Level)
 - Amazon Route 53 Resolver DNS Firewall
 - Policies are created at the region level
- Rules are applied to new resources as they are created (good for compliance) across all and future accounts in your Organization

được áp dụng với các resource mới khi chúng được tạo

Question 111:

A solutions architect is auditing the security setup or an AWS Lambda function for a company. The Lambda function retrieves the latest changes from an Amazon Aurora database. The Lambda function and the database run in the same VPC. Lambda environment variables are providing the database credentials to the Lambda function.

The Lambda function aggregates data and makes the data available in an Amazon S3 bucket that is configured for server-side encryption with AWS KMS managed encryption keys (SSE-KMS). The data must not travel across the Internet. If any database credentials become compromised, the company needs a solution that minimizes the impact of the compromise.

What should the solutions architect recommend to meet these requirements?

- A. Enable IAM database authentication on the Aurora DB cluster. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- B. Enable IAM database authentication on the Aurora DB cluster. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication. Enforce HTTPS on the connection to Amazon S3 during data transfers.
- C. Save the database credentials in AWS Systems Manager Parameter Store. Set up password rotation on the credentials in Parameter Store. Change the IAM role for the Lambda function to allow the function to access Parameter Store. Modify the Lambda function to retrieve the credentials from Parameter Store. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- D. Save the database credentials in AWS Secrets Manager. Set up password rotation on the credentials in Secrets Manager. Change the IAM role for the Lambda function to allow the function to access Secrets Manager. Modify the Lambda function to retrieve the credentials from Secrets Manager. Enforce HTTPS on the connection to Amazon S3 during data transfers.

A

LAB: <https://aws.amazon.com/pt/blogs/database/iam-role-based-authentication-to-amazon-aurora-from-serverless-applications/>

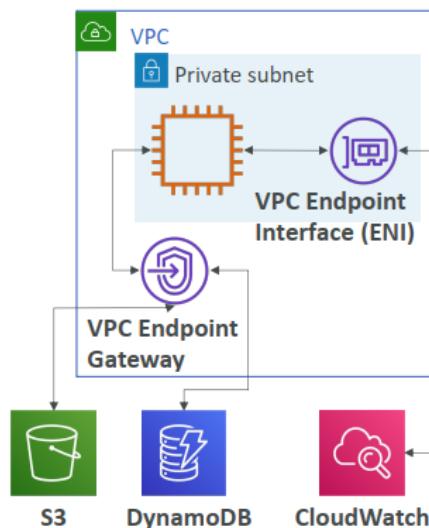
RDS - IAM Authentication

- IAM database authentication works with MariaDB, MySQL and PostgreSQL
- You don't need a password, just an authentication token obtained through IAM & RDS API calls
- Auth token has a lifetime of 15 minutes
- Benefits:
 - Network in/out must be encrypted using SSL
 - IAM to centrally manage users instead of DB
 - Can leverage IAM Roles and EC2 Instance profiles for easy integration



VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables



Question 112:

A large mobile gaming company has successfully migrated all of its on-premises infrastructure to the AWS Cloud. A solutions architect is reviewing the environment to ensure that it was built according to the design and that it is running in alignment with the Well-Architected Framework.

While reviewing previous monthly costs in Cost Explorer, the solutions architect notices that the creation and subsequent termination of several large instance types account for a high proportion of the costs. The solutions architect finds out that the company's developers are launching new Amazon EC2 instances as part of their testing and that the developers are not using the appropriate instance types.

The solutions architect must implement a control mechanism to limit the instance types that only the developers can launch.

Which solution will meet these requirements?

- A. Create a desired-instance-type managed rule in AWS Config. Configure the rule with the instance types that are allowed. Attach the rule to an event to run each time a new EC2 instance is launched.
- B. In the EC2 console, create a launch template that specifies the instance types that are allowed. Assign the launch template to the developers' IAM accounts.
- C. Create a new IAM policy. Specify the instance types that are allowed. Attach the policy to an IAM group that contains the IAM accounts for the developers
- D. Use EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image.

C

In this solution, a new IAM policy is created that specifies the allowed instance types. This policy is then attached to an IAM group that contains the IAM accounts for the developers. This will ensure that the developers can only launch instances of the specified types, thus limiting the costs associated with the creation and termination of large instances.

```
{  
    "Sid": "limitedSize",  
    "Effect": "Deny",  
    "Action": "ec2:RunInstances",  
    "Resource": "arn:aws:ec2:*:instance/*",  
    "Condition": {  
        "ForAnyValue:StringNotLike": {  
            "ec2:InstanceType": [  
                "*.nano",  
                "*.small",  
                "*.micro",  
                "*.medium"  
            ]  
        }  
    }  
}
```

- A. Creating a desired-instance-type managed rule in AWS Config is not a sufficient solution, as it only identifies when an instance is launched with an unauthorized type, it does not prevent it.
- B. Creating a launch template that specifies the instance types that are allowed is not a sufficient solution, because it limits the instances types that can be launched in the EC2 console, but it does not prevent the launch of instances through the AWS SDK, AWS CLI, or other AWS services.
- D. Using EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image is not a direct solution to the problem of limiting the instance types that only the developers can launch. It can be useful for creating standardize images for the developers, but it does not provide the necessary control mechanism to limit the instance types.

Question 113:

A company is developing and hosting several projects in the AWS Cloud. The projects are developed across multiple AWS accounts under the same organization in AWS Organizations. The company requires the cost for cloud infrastructure to be allocated to the owning project. The team responsible for all of the AWS accounts has discovered that several Amazon EC2 instances are lacking the Project tag used for cost allocation.

Which actions should a solutions architect take to resolve the problem and prevent it from happening in the future? (Choose three.)

- A. Create an AWS Config rule in each account to find resources with missing tags.
- B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing.
- C. Use Amazon Inspector in the organization to find resources with missing tags.
- D. Create an IAM policy in each account with a deny action for ec2:RunInstances if the Project tag is missing.
- E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag.
- F. Use AWS Security Hub to aggregate a list of EC2 instances with the missing Project tag.

A, B, E

<https://docs.aws.amazon.com/config/latest/developerguide/WhatsConfig.html>

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

A. Create an AWS Config rule in each account to find resources with missing tags. By creating an AWS Config rule in each account, you can check if resources are missing tags or have tags that are not conforming to your organization's standards. You can also use AWS Config to automatically remediate non-compliant resources by applying tags. This can help ensure that resources are properly tagged for cost allocation purposes. Here is the AWS Config documentation for creating rules: https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html

B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing. By creating a Service Control Policy (SCP) in the organization, you can enforce a deny action for EC2 instances that do not have the required Project tag. This can prevent users from launching instances that are not tagged correctly and ensure that new instances are tagged properly for cost allocation. Here is the AWS Organizations documentation for creating SCPs. https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag. By creating an AWS Config aggregator, you can collect a list of EC2 instances across multiple accounts in the organization that are missing the required Project tag. This can help you identify instances that need to be tagged properly for cost allocation. Here is the AWS Config documentation for creating aggregators: <https://docs.aws.amazon.com/config/latest/developerguide/config-aggregator.html>

AWS Config Rules

- Can use AWS managed config rules (over 75)
- Can make custom config rules (must be defined in AWS Lambda)
 - Evaluate if each EBS disk is of type gp2
 - Evaluate if each EC2 instance is t2.micro
- Rules can be evaluated / triggered:
 - For each config change
 - And / or: at regular time intervals
- Trigger Amazon EventBridge if the rule is non-compliant (chain with Lambda)
- Rules can have auto remediations through **SSM Automations**
 - If a resource is not compliant, you can trigger an auto remediation
 - Ex: remediate security group rules, stop instances with non-approved tags

AWS Config



- Helps with auditing and recording **compliance** of your AWS resources
- Helps record configurations and changes over time
- **AWS Config Rules does not prevent actions from happening (no deny)**
Không ngăn chặn các hành động xảy ra
- Questions that can be solved by AWS Config:
 - Is there unrestricted SSH access to my security groups?
 - Do my buckets have any public access?
 - How has my ALB configuration changed over time?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per-region service
- **Can be aggregated across regions and accounts**
tổng hợp

Question 114:

A company has an on-premises monitoring solution using a PostgreSQL database for persistence of events. The database is unable to scale due to heavy ingestion and it frequently runs out of storage.

The company wants to create a hybrid solution and has already set up a VPN connection between its network and AWS. The solution should include the following attributes:

- Managed AWS services to minimize operational complexity.
- A buffer that automatically scales to match the throughput of data and requires no ongoing administration.
- A visualization tool to create dashboards to observe events in near-real time.
- Support for semi-structured JSON data and dynamic schemas.

Which combination of components will enable the company to create a monitoring solution that will satisfy these requirements? (Choose two.)

- A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events.
- B. Create an Amazon Kinesis data stream to buffer events. Create an AWS Lambda function to process and transform events.
- C. Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.
- D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards.
- E. Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.

A, D

A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events. Amazon Kinesis Data Firehose provides a fully managed service for effortlessly loading streaming data into AWS services such as Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk. It scales automatically to match the throughput of data and requires no ongoing administration. AWS Lambda can be used in conjunction with Kinesis Data Firehose to process and transform the data before it's loaded into the destination, supporting dynamic schemas and semi-structured JSON data. Additionally, Amazon Kinesis Data Firehose has built-in buffering capabilities and can be used to observe events in near-real time, making it a more appropriate choice for the given scenario.

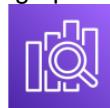
D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards. Amazon Elasticsearch Service (Amazon ES) is a managed service that makes it easy to deploy, secure, operate, and scale Elasticsearch to search, analyze, and visualize data in real-time. Kibana is an open-source visualization tool designed to work with Elasticsearch, providing powerful and easy-to-use features to create dashboards that can visualize data in near-real-time.

Option B includes using an Amazon Kinesis data stream to buffer events, which is a valid solution for a streaming data use case. However, it requires more ongoing administration compared to using Amazon Kinesis Data Firehose, which is a fully managed service. Additionally, the use of Amazon Kinesis Data Firehose allows the company to take advantage of built-in data transformation and processing capabilities, which can reduce the amount of code required to implement the solution. Therefore, I selected option A over option B as it better meets the requirement of minimizing operational complexity.

Option C: Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards. is incorrect because Amazon Aurora is a relational database service and does not support JSON data or dynamic schemas

Option E: Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards. is incorrect because Amazon Neptune is a graph database service and does not support JSON data or dynamic schemas.

Amazon OpenSearch (ex ElasticSearch)



- New name is Amazon OpenSearch
- ElasticSearch => OpenSearch
- Kibana => OpenSearch Dashboards
- Managed version of OpenSearch (open-source project, fork of ElasticSearch)
- Needs to run on servers (not a serverless offering)
- Use cases:
 - Log Analytics
 - Real Time application monitoring
 - Security Analytics
 - Full Text Search
 - Clickstream Analytics
 - Indexing

Elastic search

Kibana

OpenSearch + OS Dashboards + Logstash

- OpenSearch (ex ElasticSearch): provide search and indexing capability
 - You must specify instance types, multi-AZ, etc
- OpenSearch Dashboards (ex Kibana):
 - Provide real-time dashboards on top of the data that sits in OpenSearch
 - Alternative to CloudWatch dashboards (more advanced capabilities)
- Logstash:
 - Log ingestion mechanism, use the “Logstash Agent”
 - Alternative to CloudWatch Logs (you decide on retention and granularity)

Question 115:

A team collects and routes behavioral data for an entire company. The company runs a Multi-AZ VPC environment with public subnets, private subnets, and an internet gateway. Each public subnet also contains a NAT gateway. Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads run in private subnets.

A solutions architect must review the infrastructure. The solution architect needs to reduce costs and maintain the function of the applications. The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high. A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.

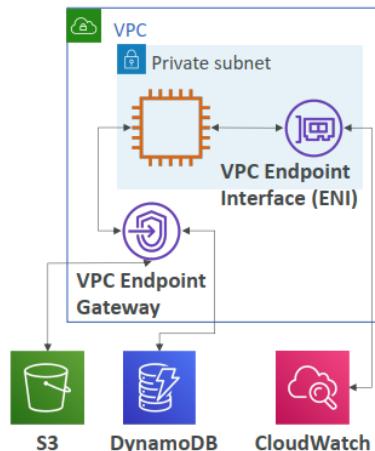
What should the solutions architect do to meet these requirements?

- A. Enable VPC Flow Logs. Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are blocking traffic that is responsible for high costs.
- B. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
- C. Enable VPC Flow Logs and Amazon Detective. Review Detective findings for traffic that is not related to Kinesis Data Streams. Configure security groups to block that traffic.
- D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that the VPC endpoint policy allows traffic from the applications.

D
NatGateway-Bytes charges are increasing the cost in the EC2-Other category ➔ should reduce internet traffic
Connect to KDS using a private network instead of the public network via NAT GW

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables



VPC Endpoints Interface

- Provision an ENI that will have a private endpoint interface hostname
- Leverage Security Groups for security
- Private DNS (setting when you create the endpoint)
 - The public hostname of a service will resolve to the private Endpoint Interface hostname
 - VPC Setting: "Enable DNS hostnames" and "Enable DNS Support" must be 'true'
 - Example for Athena:
 - vpce-0b7d2995e9dfe5418-mwrths3x.athena.us-east-1.vpce.amazonaws.com
 - vpce-0b7d2995e9dfe5418-mwrths3x-us-east-1a.athena.us-east-1.vpce.amazonaws.com
 - vpce-0b7d2995e9dfe5418-mwrths3x-us-east-1b.athena.us-east-1.vpce.amazonaws.com
 - athena.us-east-1.amazonaws.com (private DNS name)
- Interface can be accessed from Direct Connect and Site-to-Site VPN

Question 116:

A retail company has an on-premises data center in Europe. The company also has a multi-Region AWS presence that includes the eu-west-1 and us-east-1 Regions. The company wants to be able to route network traffic from its on-premises infrastructure into VPCs in either of those Regions. The company also needs to support traffic that is routed directly between VPCs in those Regions. No single points of failure can exist on the network.

The company already has created two 1 Gbps AWS Direct Connect connections from its on-premises data center. Each connection goes into a separate Direct Connect location in Europe for high availability. These two locations are named DX-A and DX-B, respectively. Each Region has a single AWS Transit Gateway that is configured to route all inter-VPC traffic within that Region.

Which solution will meet these requirements?

A. Create a private VIF from the DX-A connection into a Direct Connect gateway. Create a private VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with the Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing.

B. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Associate the eu-west-1 transit gateway with this Direct Connect gateway. Create a transit VIF from the DX-B connection into a separate Direct Connect gateway. Associate the us-east-1 transit gateway with this separate Direct Connect gateway. Peer the Direct Connect gateways with each other to support high availability and cross-Region routing.

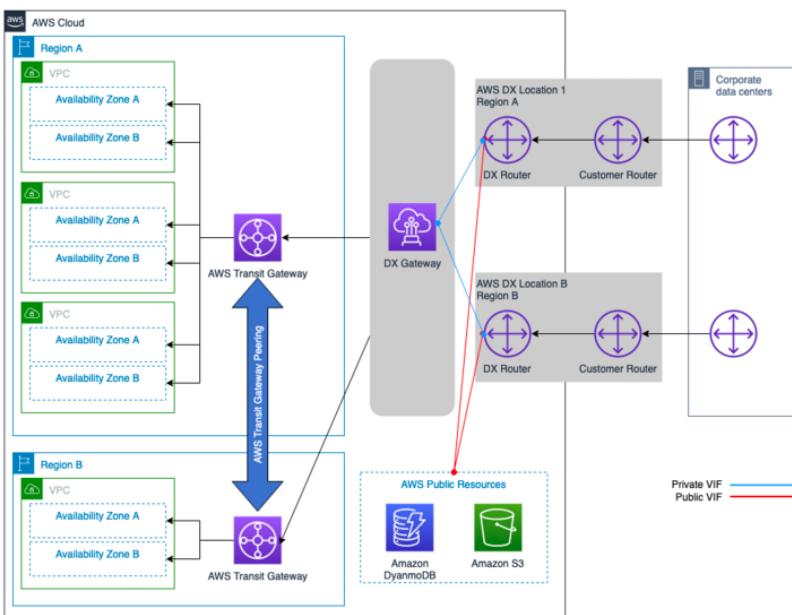
C. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway. Configure the Direct Connect gateway to route traffic between the transit gateways.

D. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing.

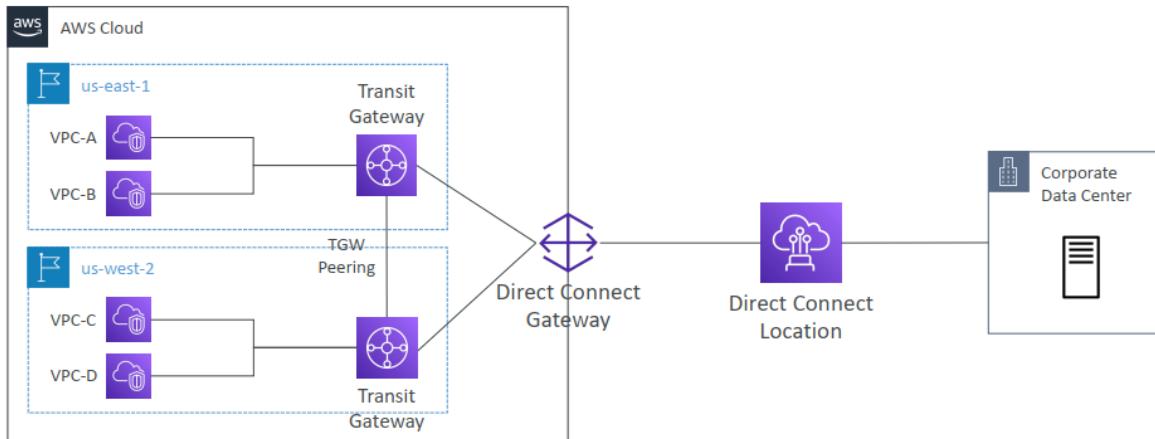
D

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-and-aws-public-peering.html>

The company also needs to support traffic that is routed directly between VPCs in those Regions ➔ Transit VIF



Transit Gateway to Direct Connect Gateway



Question 117:

A company is running an application in the AWS Cloud. The company's security team must approve the creation of all new IAM users. When a new IAM user is created, all access for the user must be removed automatically. The security team must then receive a notification to approve the user. The company has a multi-Region AWS CloudTrail trail in the AWS account.

Which combination of steps will meet these requirements? (Choose three.)

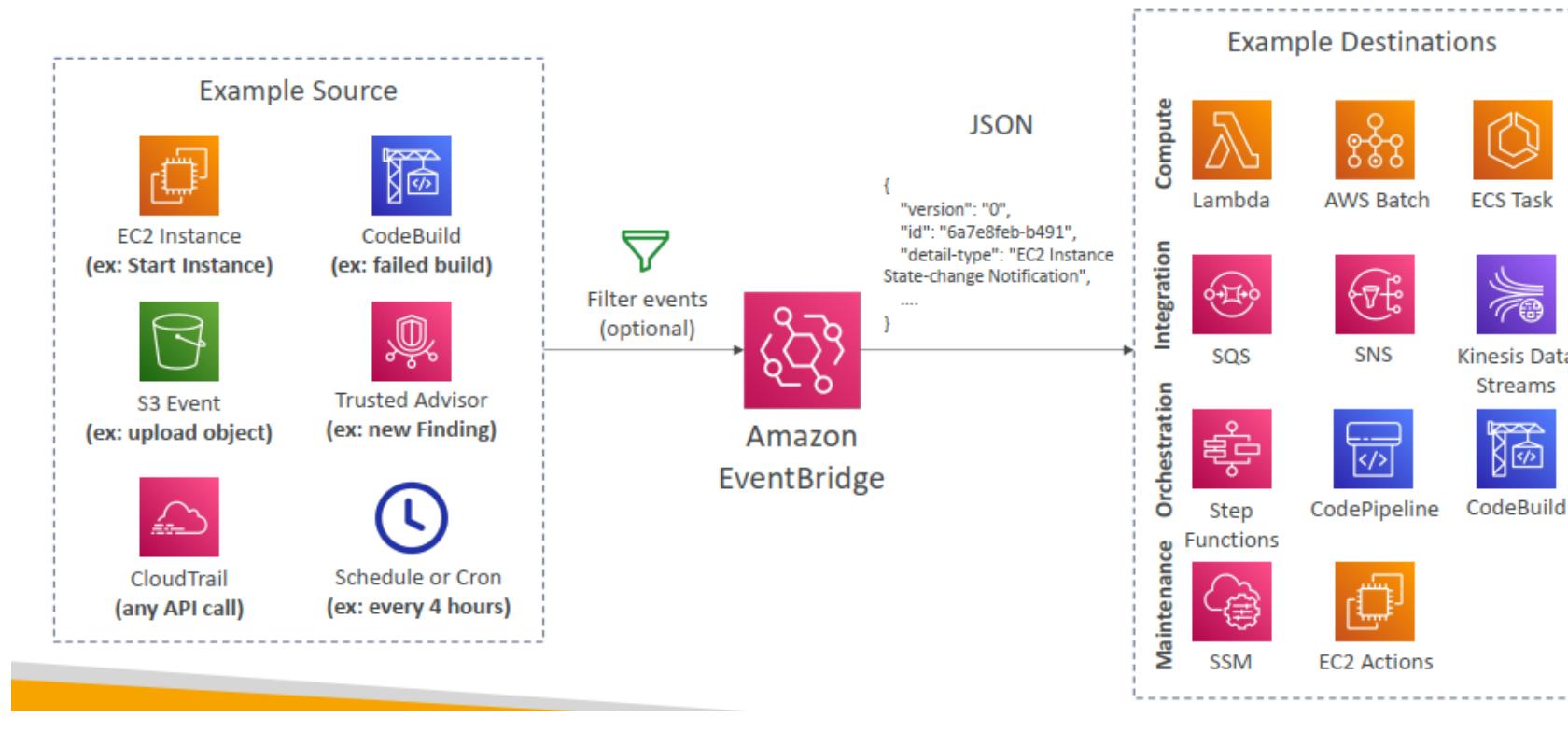
- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.
- B. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargate technology to remove access.
- D. Invoke an AWS Step Functions state machine to remove access.
- E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.
- F. Use Amazon Pinpoint to notify the security team.

A,D,E

Event Bus (EventBridge) system to receive event notification (Option A). Step function can get triggered with workflow of doing steps like removing access and sending email etc..(Option D, E) EventBridge enables you to create event rules that match events from different sources, such as AWS services, SaaS applications, custom applications, and other AWS accounts. Once an event rule is triggered, EventBridge can route the event to one or more targets, such as AWS Lambda functions, Amazon SNS topics, Amazon SQS queues, or custom HTTP endpoints. AWS Step Functions supports several AWS services, such as AWS Lambda, Amazon Simple Notification Service (SNS), and Amazon Simple Queue Service (SQS). You can use these services to trigger actions and pass data between steps in your state machine.

B is incorrect because the CloudTrail can not send event to the SNS topic. (CloudTrail → EventBridge → SNS topic)

Amazon EventBridge Rules



Question 118:

A company wants to migrate to AWS. The company wants to use a multi-account structure with centrally managed access to all accounts and applications. The company also wants to keep the traffic on a private network. Multi-factor authentication (MFA) is required at login, and specific roles are assigned to user groups.

The company must create separate accounts for development, staging, production, and shared network. The production account and the shared network account must have connectivity to all accounts. The development account and the staging account must have access only to each other.

Which combination of steps should a solutions architect take to meet these requirements? (Choose three.)

- A. Deploy a landing zone environment by using AWS Control Tower. Enroll accounts and invite existing accounts into the resulting organization in AWS Organizations.
- B. Enable AWS Security Hub in all accounts to manage cross-account access. Collect findings through AWS CloudTrail to force MFA login.
- C. Create transit gateways and transit gateway VPC attachments in each account. Configure appropriate route tables.
- D. Set up and enable AWS IAM Identity Center (AWS Single Sign-On). Create appropriate permission sets with required MFA for existing accounts.
- E. Enable AWS Control Tower in all accounts to manage routing between accounts. Collect findings through AWS CloudTrail to force MFA login.
- F. Create IAM users and groups. Configure MFA for all users. Set up Amazon Cognito user pools and Identity pools to manage access to accounts and between accounts.

A,C,D

a multi-account structure with centrally managed access to all accounts and applications → Control Tower
keep the traffic on a private network → transit gateway

Multi-factor authentication (MFA) is required at login, and specific roles are assigned to user groups → AWS IAM Identity Center (AWS Single Sign-On)

A. Deploying a landing zone environment using AWS Control Tower and enrolling accounts in an organization in AWS Organizations allows for a centralized management of access to all accounts and applications.

C. Creating transit gateways and transit gateway VPC attachments in each account and configuring appropriate route tables allows for private network traffic, and ensures that the production account and shared network account have connectivity to all accounts, while the development and staging accounts have access only to each other.

D. Setting up and enabling AWS IAM Identity Center (AWS Single Sign-On) and creating appropriate permission sets with required MFA for existing accounts allows for multi-factor authentication at login and specific roles to be assigned to user groups.

AWS Control Tower



- Easy way to set up and govern a secure and compliant multi-account AWS environment based on best practices
- Benefits:
 - Automate the set up of your environment in a few clicks
 - Automate ongoing policy management using guardrails
 - Detect policy violations and remediate them
 - Monitor compliance through an interactive dashboard
- AWS Control Tower runs on top of AWS Organizations:
 - It automatically sets up AWS Organizations to organize accounts and implement SCPs (Service Control Policies)

AWS IAM Identity Center (successor to AWS Single Sign-On)



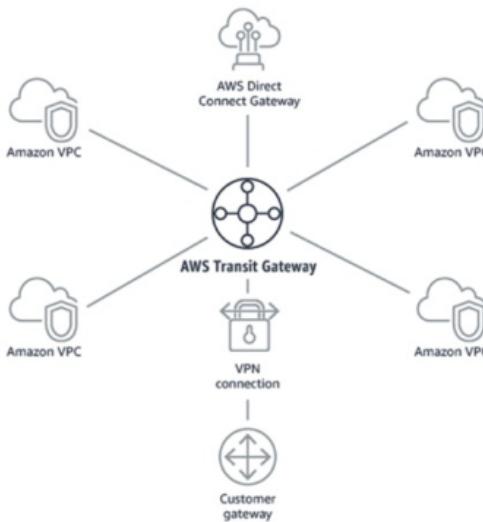
- One login (single sign-on) for all your
 - AWS accounts in AWS Organizations
 - Business cloud applications (e.g., Salesforce, Box, Microsoft 365, ...)
 - SAML2.0-enabled applications
 - EC2 Windows Instances
- Identity providers
 - Built-in identity store in IAM Identity Center
 - 3rd party: Active Directory (AD), OneLogin, Okta...



Transit Gateway



- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager (RAM)
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with other VPC
- Works with Direct Connect Gateway, VPN connections
- Supports IP Multicast (not supported by any other AWS service)
- Instances in a VPC can access a NAT Gateway, NLB, PrivateLink, and EFS in other VPCs attached to the AWS Transit Gateway.



Question 119:

A company runs its application in the eu-west-1 Region and has one account for each of its environments: development, testing, and production. All the environments are running 24 hours a day, 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases. The databases are between 500 GB and 800 GB in size.

The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day, 7 days a week. The company wants to reduce costs. All resources are tagged with an environment tag with either development, testing, or production as the key.

What should a solutions architect do to reduce costs with the LEAST operational effort?

- Create an Amazon EventBridge rule that runs once every day. Configure the rule to invoke one AWS Lambda function that starts or stops instances based on me tag, day, and time.
- Create an Amazon EventBridge rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag. Create a second EventBridge rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that starts instances based on the tag.

C. Create an Amazon EventBridge rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that terminates instances based on the tag. Create a second EventBridge rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.

D. Create an Amazon EventBridge rule that runs every hour. Configure the rule to invoke one AWS Lambda function that terminates or restores instances from their last backup based on the tag, day, and time.

B

C, D are incorrect ➔ AWS Lambda function that **terminates**

Running Jobs on AWS

**Strategy 1: Provision EC2 instance
(long running - CRON jobs)**



EC2

Strategy 3: Reactive Workflow

EventBridge
S3 Events
API Gateway
SQS, SNS
Etc...

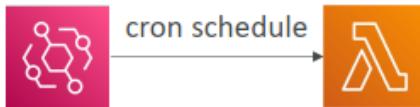


Strategy 5: use Fargate



EventBridge Fargate

**Strategy 2: Amazon EventBridge + Lambda
(cron)**



EventBridge

Strategy 4: use AWS Batch



EventBridge

Batch

**Strategy 6: Use EMR
(step execution or cluster)**



EMR

Question 120:

A company is building a software-as-a-service (SaaS) solution on AWS. The company has deployed an Amazon API Gateway REST API with AWS Lambda integration in multiple AWS Regions and in the same production account.

The company offers tiered pricing that gives customers the ability to pay for the capacity to make a certain number of API calls per second. The premium tier offers up to 3,000 calls per second, and customers are identified by a unique API key. Several premium tier customers in various Regions report that they receive error responses of 429 Too Many Requests from multiple API methods during peak usage hours. Logs indicate that the Lambda function is never invoked.

What could be the cause of the error messages for these customers?

- A. The Lambda function reached its concurrency limit.
- B. The Lambda function its Region limit for concurrency.
- C. The company reached its API Gateway account limit for calls per second.
- D. The company reached its API Gateway default per-method limit for calls per second.

C

<https://docs.aws.amazon.com/apigateway/latest/developerguide/limits.html>

LAB: <https://trello.com/c/zIKvMtmV/488-api-gateway-throttling-429-too-many-requests>

Account-level throttling per Region

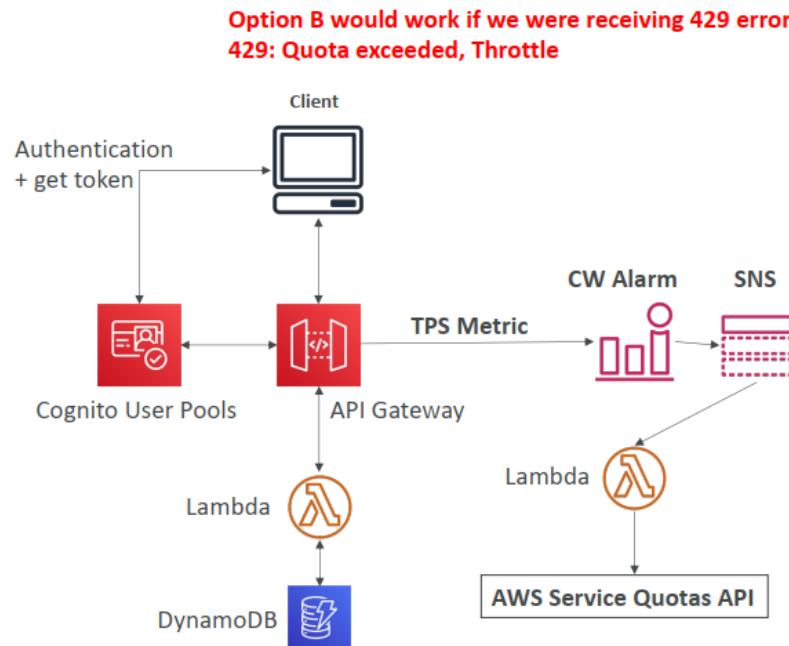
By default, API Gateway limits the steady-state requests per second (RPS) across all APIs within an AWS account, per Region. It also limits the burst (that is, the maximum bucket size) across all APIs within an AWS account, per Region. In API Gateway, the burst limit represents the target maximum number of concurrent request submissions that API Gateway will fulfill before returning 429 Too Many Requests error responses. For more information on throttling quotas, see [Amazon API Gateway quotas and important notes](#).

API Gateway - Errors

- 4xx means Client errors
 - 400: Bad Request
 - 403: Access Denied, WAF filtered
 - 429: Quota exceeded, Throttle
- 5xx means Server errors
 - 502: Bad Gateway Exception, usually for an incompatible output returned from a Lambda proxy integration backend and occasionally for out-of-order invocations due to heavy loads.
 - 503: Service Unavailable Exception
 - 504: Integration Failure – ex Endpoint Request Timed-out Exception
API Gateway requests time out after 29 second maximum

Option B

- Configure notification alerts for the limit of transactions per second on the API Gateway endpoint and create a Lambda function that will increase this limit, as needed.



Question 121:

A financial company is planning to migrate its web application from on premises to AWS. The company uses a third-party security tool to monitor the inbound traffic to the application. The company has used the security tool for the last 15 years, and the tool has no cloud solutions available from its vendor. The company's security team is concerned about how to integrate the security tool with AWS technology.

The company plans to deploy the application migration to AWS on Amazon EC2 instances. The EC2 instances will run in an Auto Scaling group in a dedicated VPC. The company needs to use the security tool to inspect all packets that come in and out of the VPC. This inspection must occur in real time and must not affect the application's performance. A solutions architect must design a target architecture on AWS that is highly available within an AWS Region.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

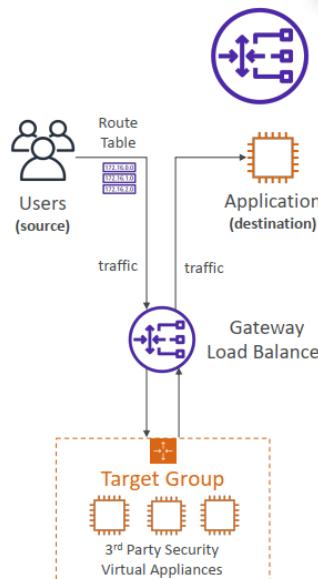
- A. Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC
- B. Deploy the web application behind a Network Load Balancer
- C. Deploy an Application Load Balancer in front of the security tool instances
- D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool
- E. Provision a transit gateway to facilitate communication between VPCs.

A, D

inspect all packets that come in and out of the VPC ➔ Gateway Load Balancer

Gateway Load Balancer

- Deploy, scale, and manage a fleet of 3rd party network virtual appliances in AWS
- Example: Firewalls, Intrusion Detection and Prevention Systems, Deep Packet Inspection Systems, payload manipulation, ...
- Operates at Layer 3 (Network Layer) – IP Packets
- Combines the following functions:
 - Transparent Network Gateway – single entry/exit for all traffic
 - Load Balancer – distributes traffic to your virtual appliances
- Uses the GENEVE protocol on port 6081



Question 122:

A company has purchased appliances from different vendors. The appliances all have IoT sensors. The sensors send status information in the vendors' proprietary formats to a legacy application that parses the information into JSON. The parsing is simple, but each vendor has a unique format. Once daily, the application parses all the JSON records and stores the records in a relational database for analysis.

The company needs to design a new data analysis solution that can deliver faster and optimize costs.

Which solution will meet these requirements?

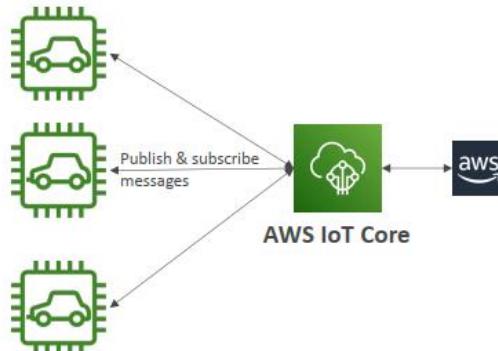
- A. Connect the IoT sensors to AWS IoT Core. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the files. Use Amazon Athena and Amazon QuickSight for analysis.
- B. Migrate the application server to AWS Fargate, which will receive the information from IoT sensors and parse the information into a relational format. Save the parsed information to Amazon Redshift for analysis.
- C. Create an AWS Transfer for SFTP server. Update the IoT sensor code to send the information as a .csv file through SFTP to the server. Use AWS Glue to catalog the files. Use Amazon Athena for analysis.
- D. Use AWS Snowball Edge to collect data from the IoT sensors directly to perform local analysis. Periodically collect the data into Amazon Redshift to perform global analysis.

A IoT sensors → AWS IoT Core

AWS IoT Core



- IoT stands for “Internet of Things” – the network of internet-connected devices that are able to collect and transfer data
- AWS IoT Core allows you to **easily connect IoT devices to the AWS Cloud**
- Serverless, secure & scalable to billions of devices and trillions of messages
- Integrates with a lot of AWS services (Lambda, S3, SageMaker, etc.)
- Build IoT applications that gather, process, analyze, and act on data



Question 123:

A company is migrating some of its applications to AWS. The company wants to migrate and modernize the applications quickly after it finalizes networking and security strategies. The company has set up an AWS Direct Connect connection in a central network account.

The company expects to have hundreds of AWS accounts and VPCs in the near future. The corporate network must be able to access the resources on AWS seamlessly and also must be able to communicate with all the VPCs. The company also wants to route its cloud resources to the internet through its on-premises data center.

Which combination of steps will meet these requirements? (Choose three.)

- Create a Direct Connect gateway in the central account. In each of the accounts, create an association proposal by using the Direct Connect gateway and the account ID for every virtual private gateway.
- Create a Direct Connect gateway and a transit gateway in the central network account. Attach the transit gateway to the Direct Connect gateway by using a transit VIF.
- Provision an internet gateway. Attach the internet gateway to subnets. Allow internet traffic through the gateway.
- Share the transit gateway with other accounts. Attach VPCs to the transit gateway.
- Provision VPC peering as necessary.
- Provision only private subnets. Open the necessary route on the transit gateway and customer gateway to allow outbound internet traffic from AWS to flow through NAT services that run in the data center.

B, D, F

must be able to communicate with all the VPCs → Transit Gateway

wants to route its cloud resources to the internet through its on-premises data center →

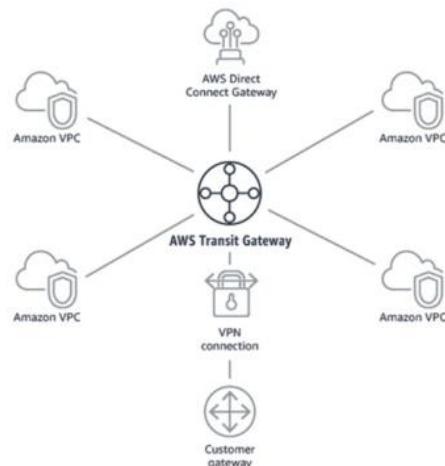
AWS

[Private subnet] -----> Transit Gateway -----DX----> On prem ---> NAT service -----> Internet
[route table allow outbound]

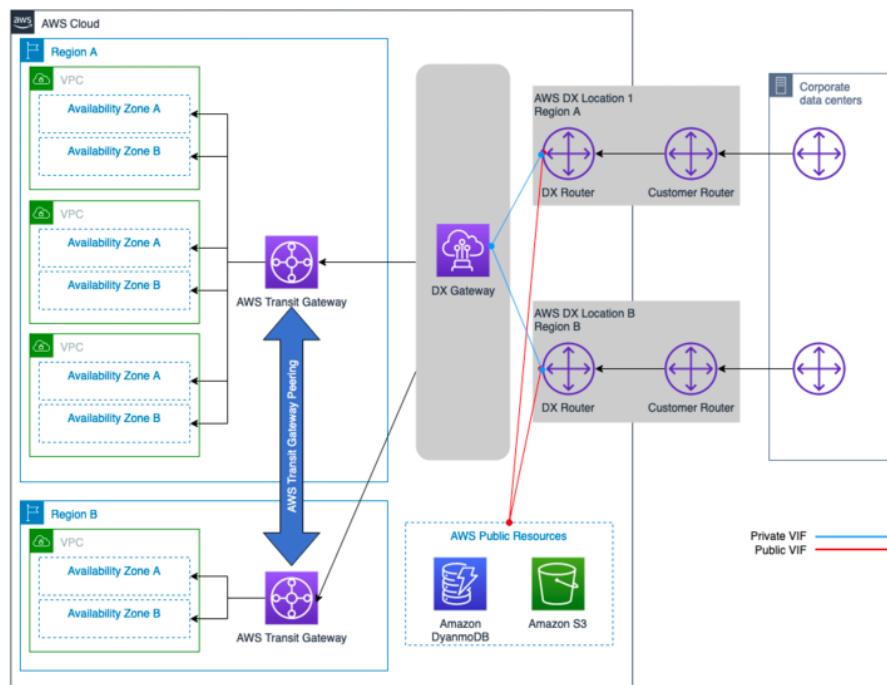
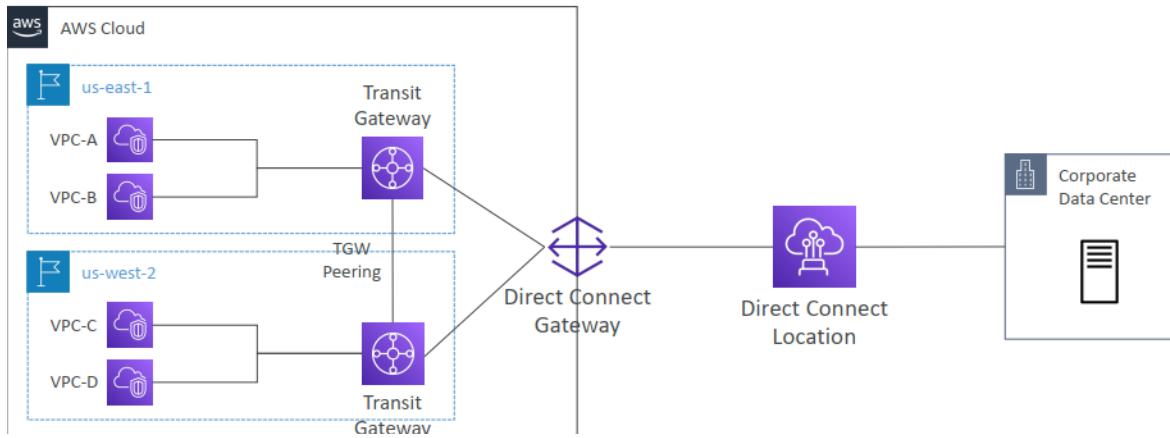


Transit Gateway

- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager (RAM)
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with other VPC
- Works with Direct Connect Gateway, VPN connections
- Supports IP Multicast (not supported by any other AWS service)
- Instances in a VPC can access a NAT Gateway, NLB, PrivateLink, and EFS in other VPCs attached to the AWS Transit Gateway.



Transit Gateway to Direct Connect Gateway



Question 124:

A company has hundreds of AWS accounts. The company recently implemented a centralized internal process for purchasing new Reserved Instances and modifying existing Reserved Instances. This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement. Previously, business units directly purchased or modified Reserved Instances in their own respective AWS accounts autonomously.

A solutions architect needs to enforce the new process in the most secure way possible.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Ensure that all AWS accounts are part of an organization in AWS Organizations with all features enabled.
- B. Use AWS Config to report on the attachment of an IAM policy that denies access to the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- C. In each AWS account, create an IAM policy that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- D. Create an SCP that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action. Attach the SCP to each OU of the organization.
- E. Ensure that all AWS accounts are part of an organization in AWS Organizations that uses the consolidated billing feature.

A, D

a centralized internal process → Ensure that all AWS accounts are part of an organization in AWS Organizations

SCP is applied for OU and AWS Config is applied for an account

A and D are the correct answer. A: By ensuring all AWS accounts are part of an organization in AWS Organizations, it allows for centralized management and control of the accounts. This can help enforce the new purchasing process by giving a dedicated team the ability to manage and enforce policies across all accounts. D: By creating an SCP (Service Control Policy) that denies access to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions, it enforces the new centralized purchasing process. Attaching the SCP to each OU (organizational unit) within the organization ensures that all business units are adhering to the new process.

B and C are not the correct answer, because AWS Config and IAM policies are used for monitoring and managing access to resources in an account, respectively. They don't enforce the new process for purchasing reserved instances.

E is not the correct answer as this is not related to the new process for purchasing reserved instances.

AWS Config



- Helps with auditing and recording **compliance** of your AWS resources
- Helps record configurations and changes over time
- AWS Config Rules does not prevent actions from happening (no deny)
Không ngăn chặn các hành động xảy ra
- Questions that can be solved by AWS Config:
 - Is there unrestricted SSH access to my security groups?
 - Do my buckets have any public access?
 - How has my ALB configuration changed over time?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per-region service
- Can be aggregated across regions and accounts
tổng hợp

SCP vs AWS Config: <https://trello.com/c/As3BAAwU/489-scp-vs-aws-config>

Question 125:

A company is running a critical application that uses an Amazon RDS for MySQL database to store data. The RDS DB instance is deployed in Multi-AZ mode.

A recent RDS database failover test caused a 40-second outage to the application. A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Use Amazon ElastiCache for Memcached in front of the database
- B. Use Amazon ElastiCache for Redis in front of the database
- C. Use RDS Proxy in front of the database.
- D. Migrate the database to Amazon Aurora MySQL.
- E. Create an Amazon Aurora Replica.
- F. Create an RDS for MySQL read replica

C,D,E

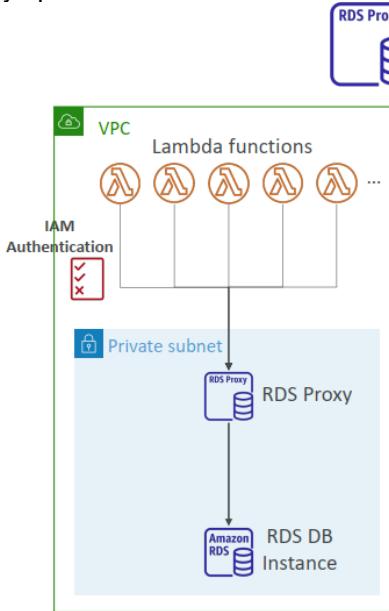
<https://aws.amazon.com/blogs/database/improving-application-availability-with-amazon-rds-proxy/>

One of the benefits of Amazon RDS Proxy is that it can improve application recovery time after database failovers.

RDS Proxy reduces client recovery time after failover by up to 79% for Amazon Aurora MySQL and by up to 32% for Amazon RDS for MySQL.

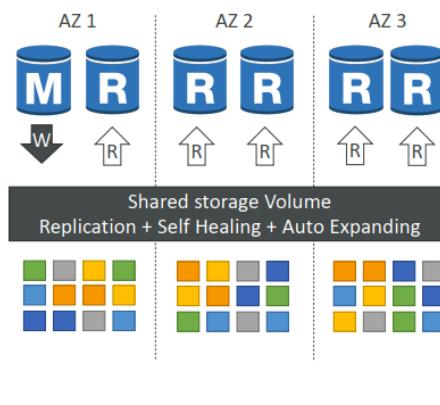
Amazon RDS Proxy

- Fully managed database proxy for RDS
- Allows apps to pool and share DB connections established with the database
- Improving database efficiency by reducing the stress on database resources (e.g., CPU, RAM) and minimize open connections (and timeouts)
- Serverless, autoscaling, highly available (multi-AZ)
- Reduced RDS & Aurora failover time by up 66%
- Supports RDS (MySQL, PostgreSQL, MariaDB, MS SQL Server) and Aurora (MySQL, PostgreSQL)
- No code changes required for most apps
- Enforce IAM Authentication for DB, and securely store credentials in AWS Secrets Manager
- RDS Proxy is never publicly accessible (must be accessed from VPC)



Aurora High Availability and Read Scaling

- 6 copies of your data across 3 AZ:
 - 4 copies out of 6 needed for writes
 - 3 copies out of 6 need for reads
 - Self healing with peer-to-peer replication
 - Storage is striped across 100s of volumes
- Automated failover for master in less than 30 seconds
- Master + up to 15 Aurora Read Replicas serve reads
- Support for Cross Region Replication



<https://trello.com/c/0kFMvQ0i/490-elasticache-redis-vs-rds-proxy>

Question 126:

An AWS partner company is building a service in AWS Organizations using its organization named org1. This service requires the partner company to have access to AWS resources in a customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account.

What is the MOST secure way to allow org1 to access resources in org2?

- A. The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks.
- B. The customer should create an IAM user and assign the required permissions to the IAM user. The customer should then provide the credentials to the partner company to log in and perform the required tasks.
- C. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) when requesting access to perform the required tasks.
- D. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN), including the external ID in the IAM role's trust policy, when requesting access to perform the required tasks.

D

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

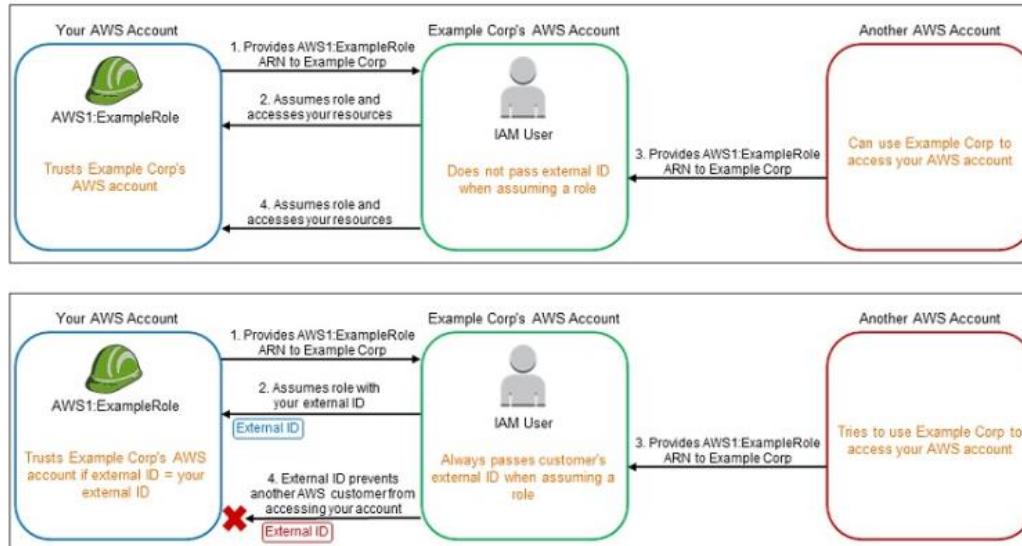
An external ID to uniquely associate with the role. The external ID can be any identifier that is known only by you and the third party.

Providing Access to AWS Accounts Owned by Third Parties

- Zone of trust = accounts, organizations that you own
- Outside Zone of Trust = 3rd parties
- Use IAM Access Analyzer to find out which resources are exposed
- For granting access to a 3rd party:
 - The 3rd party AWS account ID
 - An External ID (secret between you and the 3rd party)
 - To uniquely associate with the role between you and 3rd party
 - Must be provided when defining the trust and when assuming the role
 - Must be chosen by the 3rd party
- Define permissions in the IAM policy

The confused deputy

(n): đại diện



<https://trello.com/c/YtHKO7xi/491-generate-external-id>

Question 127:

A delivery company needs to migrate its third-party route planning application to AWS. The third party supplies a supported Docker image from a public registry. The image can run in as many containers as required to generate the route map.

The company has divided the delivery area into sections with supply hubs so that delivery drivers travel the shortest distance possible from the hubs to the customers. To reduce the time necessary to generate route maps, each section uses its own set of Docker containers with a custom configuration that processes orders only in the section's area.

The company needs the ability to allocate resources cost-effectively based on the number of running containers.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on Amazon EC2. Use the Amazon EKS CLI to launch the planning application in pods by using the --tags option to assign a custom tag to the pod.
- B. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on AWS Fargate. Use the Amazon EKS CLI to launch the planning application. Use the AWS CLI tag-resource API call to assign a custom tag to the pod.

C. Create an Amazon Elastic Container Service (Amazon ECS) cluster on Amazon EC2. Use the AWS CLI with run-tasks set to true to launch the planning application by using the --tags option to assign a custom tag to the task.

D. Create an Amazon Elastic Container Service (Amazon ECS) cluster on AWS Fargate. Use the AWS CLI run-task command and set enableECSManagedTags to true to launch the planning application. Use the --tags option to assign a custom tag to the task.

D

Since the question where the requirement is the least operational overhead and we are between EKS and ECS, I would go for ECS, I believe EKS has more operational overhead for deploying and for operating. Also, you would probably have to apply less steps to build this structure using ECS when comparing with EKS.

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-using-tags.html>

Question 128:

A software company hosts an application on AWS with resources in multiple AWS accounts and Regions. The application runs on a group of Amazon EC2 instances in an application VPC located in the us-east-1 Region with an IPv4 CIDR block of 10.10.0.0/16. In a different AWS account, a shared services VPC is located in the us-east-2 Region with an IPv4 CIDR block of 10.10.10.0/24. When a cloud engineer uses AWS CloudFormation to attempt to peer the application VPC with the shared services VPC, an error message indicates a peering failure.

Which factors could cause this error? (Choose two.)

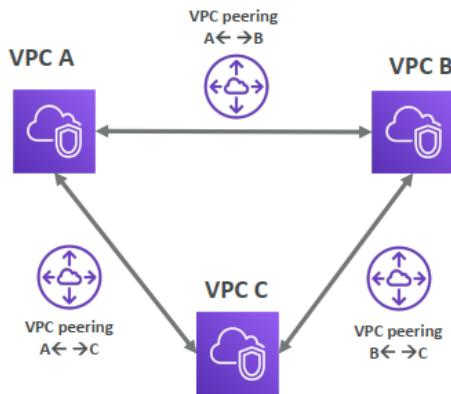
- A. The IPv4 CIDR ranges of the two VPCs overlap
- B. The VPCs are not in the same Region
- C. One or both accounts do not have access to an Internet gateway
- D. One of the VPCs was not shared through AWS Resource Access Manager
- E. The IAM role in the peer accepter account does not have the correct permissions

A, E

E is correct because the IAM role in the peer accepter account does not have the correct permissions. The role must have permissions to create, modify, and delete VPC peering connections in order for the peering to be established.

VPC Peering

- Connect two VPC, privately using AWS' network
- Make them behave as if they were in the same network
- Must not have overlapping CIDR
- VPC Peering connection is **not transitive** (must be established for each VPC that need to communicate with one another)
- You can do VPC peering with another AWS account
- You must update route tables in each VPC's subnets to ensure instances can communicate



VPC Peering – Good to know

Liên vùng => multi region

- VPC peering can work inter-region, cross-account
- You can reference a security group of a peered VPC (works cross account)

Type	Protocol	Port Range	Source
HTTP	TCP	80	sg-00d2b0f5fd6de757e
HTTP	TCP	80	sg-013347765f7a63aae/12356788

Question 129:

An external audit of a company's serverless application reveals IAM policies that grant too many permissions. These policies are attached to the company's AWS Lambda execution roles. Hundreds of the company's Lambda functions have broad access permissions such as full access to Amazon S3 buckets and Amazon DynamoDB tables. The company wants each function to have only the minimum permissions that the function needs to complete its task.

A solutions architect must determine which permissions each Lambda function needs.

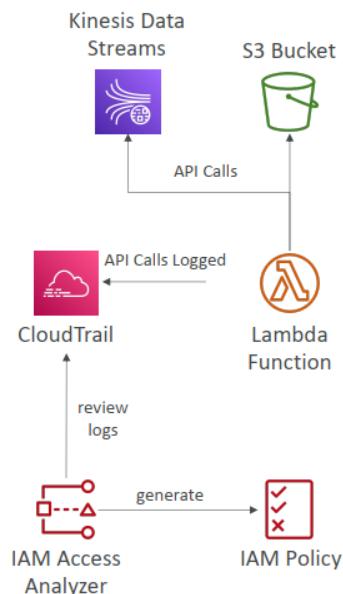
What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Set up Amazon CodeGuru to profile the Lambda functions and search for AWS API calls. Create an inventory of the required API calls and resources for each Lambda function. Create new IAM access policies for each Lambda function. Review the new policies to ensure that they meet the company's business requirements.
- B. Turn on AWS CloudTrail logging for the AWS account. Use AWS Identity and Access Management Access Analyzer to generate IAM access policies based on the activity recorded in the CloudTrail log. Review the generated policies to ensure that they meet the company's business requirements.
- C. Turn on AWS CloudTrail logging for the AWS account. Create a script to parse the CloudTrail log, search for AWS API calls by Lambda execution role, and create a summary report. Review the report. Create IAM access policies that provide more restrictive permissions for each Lambda function.
- D. Turn on AWS CloudTrail logging for the AWS account. Export the CloudTrail logs to Amazon S3. Use Amazon EMR to process the CloudTrail logs in Amazon S3 and produce a report of API calls and resources used by each execution role. Create a new IAM access policy for each role. Export the generated roles to an S3 bucket. Review the generated policies to ensure that they meet the company's business requirements.

B

IAM Access Analyzer

- **IAM Access Analyzer Policy Validation**
 - Validates your policy against IAM policy grammar and best practices
 - General warnings, security warnings, errors, suggestions
 - Provides actionable recommendations
- **IAM Access Analyzer Policy Generation**
 - Generates IAM policy based on access activity
 - CloudTrail logs is reviewed to generate the policy with the fine-grained permissions and the appropriate Actions and Services
 - Reviews CloudTrail logs for up to 90 days



Question 130:

A solutions architect must analyze a company's Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine whether the company is using resources efficiently. The company is running several large, high-memory EC2 instances to host database clusters that are deployed in active/passive configurations. The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern.

The solutions architect must analyze the environment and take action based on the findings.

Which solution meets these requirements MOST cost-effectively?

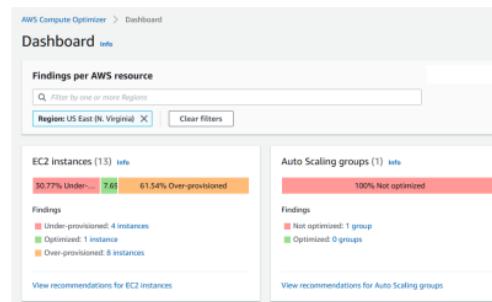
- A. Create a dashboard by using AWS Systems Manager OpsCenter. Configure visualizations for Amazon CloudWatch metrics that are associated with the EC2 instances and their EBS volumes. Review the dashboard periodically, and identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- B. Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes. Create and review a dashboard that is based on the metrics. Identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- C. Install the Amazon CloudWatch agent on each of the EC2 instances. Turn on AWS Compute Optimizer, and let it run for at least 12 hours. Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed.
- D. Sign up for the AWS Enterprise Support plan. Turn on AWS Trusted Advisor. Wait 12 hours. Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed.

C

AWS Compute Optimizer

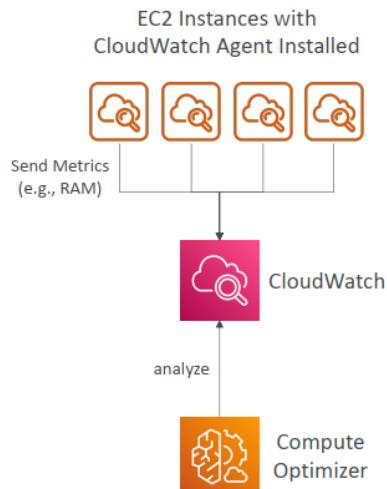


- Reduce costs and improve performance by recommending optimal AWS resources for your workloads
- Helps you choose optimal configurations and right-size your workloads (over/under provisioned)
- Uses Machine Learning to analyze your resources' configurations and their utilization CloudWatch metrics
- Supported resources
 - EC2 instances
 - EC2 Auto Scaling Groups
 - EBS volumes
 - Lambda functions
- Lower your costs by up to 25%
- Recommendations can be exported to S3



Compute Optimizer – CloudWatch Agent

- Needed to analyze Memory Utilization
- Not needed for CPU, NetworkIn/Out, DiskReadOps, DiskWriteOps, ...



Question 131:

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company uses AWS Control Tower for governance and uses AWS Transit Gateway for VPC connectivity across accounts.

In an AWS application account, the company's application team has deployed a web application that uses AWS Lambda and Amazon RDS. The company's database administrators have a separate DBA account and use the account to centrally manage all the databases across the organization. The database administrators use an Amazon EC2 instance that is deployed in the DBA account to access an RDS database that is deployed in the application account.

The application team has stored the database credentials as secrets in AWS Secrets Manager in the application account. The application team is manually sharing the secrets with the database administrators. The secrets are encrypted by the default AWS managed key for Secrets Manager in the application account. A solutions architect needs to implement a solution that gives the database administrators access to the database and eliminates the need to manually share the secrets.

Which solution will meet these requirements?

A. Use AWS Resource Access Manager (AWS RAM) to share the secrets from the application account with the DBA account. In the DBA account, create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the shared secrets. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

B. In the application account, create an IAM role that is named DBA-Secret. Grant the role the required permissions to access the secrets. In the DBA account, create an IAM role that is named DBA-Admin. Grant the DBA-Admin role the required permissions to assume the DBA-Secret role in the application account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

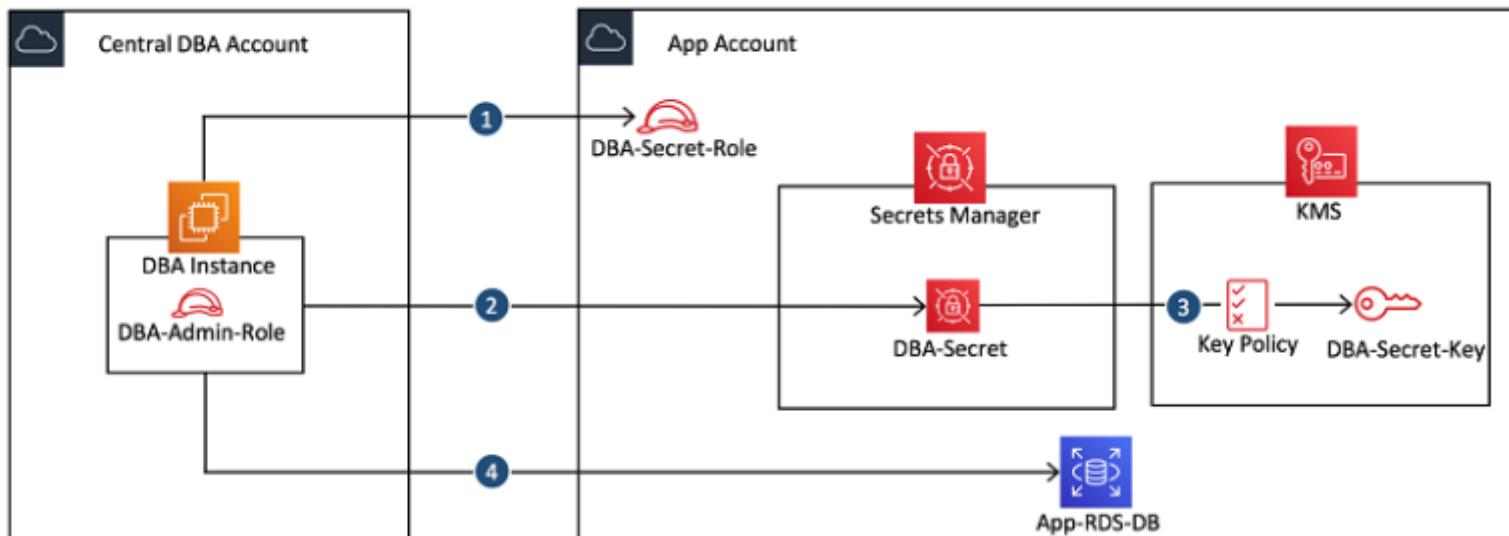
C. In the DBA account create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the secrets and the default AWS managed key in the application account. In the application account, attach resource-based policies to the key to allow access from the DBA account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

D. In the DBA account, create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the secrets in the application account. Attach an SCP to the application account to allow access to the secrets from the DBA account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

B

eliminates the need to manually share the secrets ➔ auto share the secrets

<https://aws.amazon.com/blogs/database/design-patterns-to-access-cross-account-secrets-stored-in-aws-secrets-manager/>



Question 132:

A company manages multiple AWS accounts by using AWS Organizations. Under the root OU, the company has two OUs: Research and DataOps.

Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally, EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types.

A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance.

Which combination of steps will meet these requirements? (Choose two.)

- A. Create an IAM role in one account under the DataOps OU. Use the ec2:InstanceType condition key in an inline policy on the role to restrict access to specific instance type.
- B. Create an IAM user in all accounts under the root OU. Use the aws:RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1.
- C. Create an SCP. Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU.
- D. Create an SCP. Use the ec2:Region condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU, the DataOps OU, and the Research OU.
- E. Create an SCP. Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU.

C, E

C. Create an SCP. Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU. This will ensure that all resources deployed in the organization reside in the ap-northeast-1 Region.

E. Create an SCP. Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU. This will ensure that EC2 instances deployed in the DataOps OU use only the predefined list of instance types.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessOnlyToSpecificRegion",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "ap-northeast-1"
        }
      }
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificInstanceTypes",
      "Effect": "Deny",
      "Action": [
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": [
            "t2.micro",
            "t3.micro"
          ]
        }
      }
    }
  ]
}
```

Question 133:

A company runs a serverless application in a single AWS Region. The application accesses external URLs and extracts metadata from those sites. The company uses an Amazon Simple Notification Service (Amazon SNS) topic to publish URLs to an Amazon Simple Queue Service (Amazon SQS) queue. An AWS Lambda function uses the queue as an event source and processes the URLs from the queue. Results are saved to an Amazon S3 bucket.

The company wants to process each URL in other Regions to compare possible differences in site localization. URLs must be published from the existing Region. Results must be written to the existing S3 bucket in the current Region.

Which combination of changes will produce multi-Region deployment that meets these requirements? (Choose two.)

- A. Deploy the SQS queue with the Lambda function to other Regions.
- B. Subscribe the SNS topic in each Region to the SQS queue.
- C. Subscribe the SQS queue in each Region to the SNS topic.
- D. Configure the SQS queue to publish URLs to SNS topics in each Region.
- E. Deploy the SNS topic and the Lambda function to other Regions.

A, C

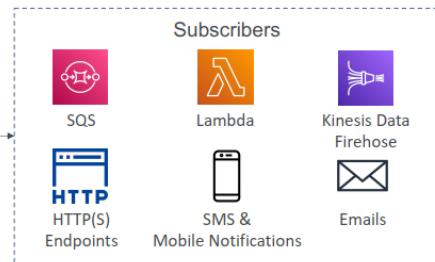
<https://docs.aws.amazon.com/sns/latest/dg/sns-cross-region-delivery.html>

wants to process each URL in other Regions → SQS and Lambda are deployed to other Region → A

Amazon SNS



- The “event producer” only sends message to one SNS topic
- As many “event receivers” (subscriptions) as we want to listen to the SNS topic notifications
- Each subscriber to the topic will get all the messages (note: new feature to filter messages)
- Up to 12,500,000 subscriptions per topic
- 100,000 topics limit



Amazon SNS supports cross-region
SNS in Region A, SQS + Lambda in Region A & B, S3 Bucket in Region A

Question 134:

A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instances. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded, uses 2 GB of RAM, and is highly CPU intensive. The application is scheduled to run every 4 hours and runs for up to 20 minutes. A solutions architect wants to revise the architecture for the solution.

Which strategy should the solutions architect use?

- A. Use AWS Lambda to run the application. Use Amazon CloudWatch Logs to invoke the Lambda function every 4 hours.
- B. Use AWS Batch to run the application. Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours.
- C. Use AWS Fargate to run the application. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours.
- D. Use Amazon EC2 Spot Instances to run the application. Use AWS CodeDeploy to deploy and run the application every 4 hours.

C

A incorrect because Lambda's max running time is 15 mins.

B incorrect because Step Function needs Event Bridge as the scheduler.

D. Using Amazon EC2 Spot Instances would not be the best option for this scenario because the application is running for up to 20 minutes and EC2 Spot instances can be terminated at any time.



AWS Batch

- Run batch jobs as Docker images
- Two options:
 1. Run on AWS Fargate (fully serverless offering)
 2. Dynamic provisioning of the instances (EC2 & Spot Instances) – in VPC
- Optimal quantity and type based on volume and requirements
- No need to manage clusters, fully **serverless**
- You just pay for the underlying resources used
- Example: batch process of images, running thousands of concurrent jobs
- Schedule Batch Jobs using Amazon EventBridge
- Orchestrate Batch Jobs using AWS Step Functions

EC2 Instance Launch Types

- On Demand Instances: short workload, predictable pricing, reliable
có thể dự đoán giá tin cậy
- Spot Instances: short workloads, for cheap, can lose instances (not reliable)
- Reserved: (MINIMUM 1 year)
 - Reserved Instances: long workloads
 - Convertible Reserved Instances: long workloads with flexible instances
không chia sẻ phần cứng
- Dedicated Instances: no other customers will share your hardware
- Dedicated Hosts: book an entire physical server; control instance placement
book 1 server vật lý
 - Great for **software licenses** that operate at the core, or socket level
 - Can define **host affinity** so that instance reboots are kept on the same host
xác định sự liên kết (affinity) giữa instance và host, đảm bảo rằng khi instance khởi động lại, nó sẽ được giữ trên cùng một host. Điều này có ý nghĩa là các instance sẽ được gắn kết với một máy chủ cụ thể và không bị di chuyển sang máy chủ khác trong quá trình khởi động lại.

Question 135:

A company is creating a sequel for a popular online game. A large number of users from all over the world will play the game within the first week after launch. Currently, the game consists of the following components deployed in a single AWS Region:

- Amazon S3 bucket that stores game assets
- Amazon DynamoDB table that stores player scores

A solutions architect needs to design a multi-Region solution that will reduce latency, improve reliability, and require the least effort to implement.

What should the solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Cross-Region Replication. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.
- B. Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Same-Region Replication. Create a new DynamoDB table in a new Region. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC).

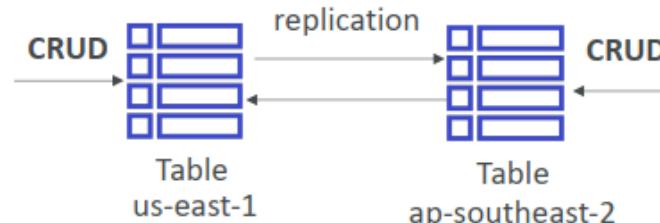
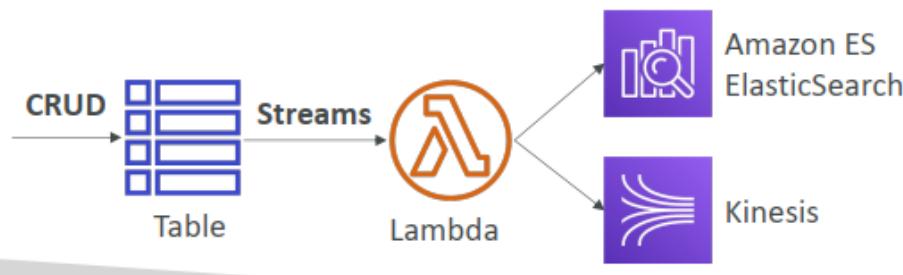
C. Create another S3 bucket in a new Region, and configure S3 Cross-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region. Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region.

D. Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.

C

DynamoDB – Important Features

- TTL: automatically expire row after a specified epoch date
- **DynamoDB Streams:**
 - react to changes to DynamoDB tables in real time
 - Can be read by AWS Lambda, EC2...
 - 24 hours retention of data
- **Global Tables:** (cross region replication)
 - Active Active replication, many regions
 - Must enable DynamoDB Streams
 - Useful for low latency, DR purposes



C. Regarding DynamoDB Streams - Global tables use DynamoDB Streams to replicate data across different Regions. When you create a replica for a global table, a stream is created by default. Any changes to a replica are replicated to all the other replicas within the same global table within a second using DynamoDB Streams.

Question 136:

A company has an on-premises website application that provides real estate information for potential renters and buyers. The website uses a Java backend and a NoSQL MongoDB database to store subscriber data.

The company needs to migrate the entire application to AWS with a similar structure. The application must be deployed for high availability, and the company cannot make changes to the application.

Which solution will meet these requirements?

- A. Use an Amazon Aurora DB cluster as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.
- B. Use MongoDB on Amazon EC2 instances as the database for the subscriber data. Deploy EC2 instances in an Auto Scaling group in a single Availability Zone for the Java backend application.
- C. Configure Amazon DocumentDB (with MongoDB compatibility) with appropriately sized instances in multiple Availability Zones as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.
- D. Configure Amazon DocumentDB (with MongoDB compatibility) in on-demand capacity mode in multiple Availability Zones as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.

C

DocumentDB



- Aurora is an “AWS-implementation” of PostgreSQL / MySQL ...
- DocumentDB is the same for MongoDB (which is a NoSQL database)
- MongoDB is used to store, query, and index JSON data

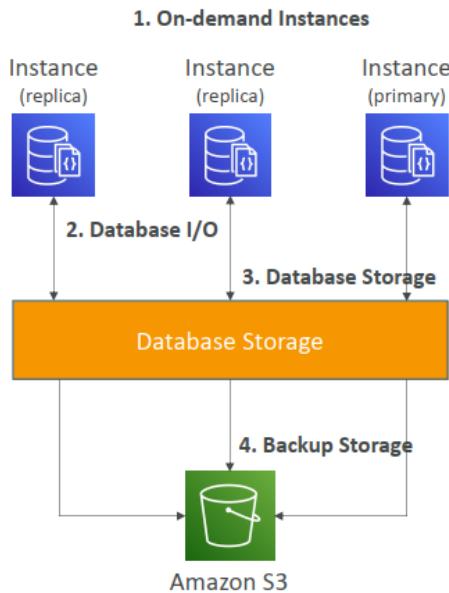
- Similar “deployment concepts” as Aurora
- Fully Managed, highly available with replication across 3 AZ
- DocumentDB storage automatically grows in increments of 10GB

- Automatically scales to workloads with millions of requests per seconds

DocumentDB – Pricing

- Pay for what you use, no upfront costs không có chi phí trả trước
- On-demand Instances (per second with minimum of 10 minutes)
- Database I/O – amount of I/O used when read and write (per million I/Os)
- Database Storage (per GB/month)
- Backup Storage (per GB/month)

There is no on-demand capacity for DocumentDB



Question 137:

A digital marketing company has multiple AWS accounts that belong to various teams. The creative team uses an Amazon S3 bucket in its AWS account to securely store images and media files that are used as content for the company's marketing campaigns. The creative team wants to share the S3 bucket with the strategy team so that the strategy team can view the objects.

A solutions architect has created an IAM role that is named `strategy_reviewer` in the Strategy account. The solutions architect also has set up a custom AWS Key Management Service (AWS KMS) key in the Creative account and has associated the key with the S3 bucket. However, when users from the Strategy account assume the IAM role and try to access objects in the S3 bucket, they receive an Access Denied error.

The solutions architect must ensure that users in the Strategy account can access the S3 bucket. The solution must provide these users with only the minimum permissions that they need.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to the account ID of the Strategy account.
- Update the `strategy_reviewer` IAM role to grant full permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.

- C. Update the custom KMS key policy in the Creative account to grant decrypt permissions to the strategy_reviewer IAM role.
- D. Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to an anonymous user.
- E. Update the custom KMS key policy in the Creative account to grant encrypt permissions to the strategy_reviewer IAM role.
- F. Update the strategy_reviewer IAM role to grant read permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.

A,C,F

<https://repost.aws/knowledge-center/cross-account-access-denied-error-s3>

The bucket policy in Account A must grant access to the user in Account B

```
{
  "Id": "ExamplePolicy1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ExampleStmt1",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
      "Principal": {
        "AWS": [
          "111122223333"
        ]
      }
    }
  ]
}
```

The AWS KMS key policy in Account A must grant access to the user in Account B

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/role_name"
    ]
  },
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

```
}
```

The IAM user policy in Account B must grant the user access to both the bucket and key in Account A

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ExampleStmt1",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    },
    {
      "Sid": "ExampleStmt2",
      "Action": [
        "kms:Decrypt"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:kms:us-west-2:44445556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

Question 138:

A life sciences company is using a combination of open source tools to manage data analysis workflows and Docker containers running on servers in its on-premises data center to process genomics data. Sequencing data is generated and stored on a local storage area network (SAN), and then the data is processed. The research and development teams are running into capacity issues and have decided to re-architect their genomics analysis platform on AWS to scale based on workload demands and reduce the turnaround time from weeks to days.

The company has a high-speed AWS Direct Connect connection. Sequencers will generate around 200 GB of data for each genome, and individual jobs can take several hours to process the data with ideal compute capacity. The end result will be stored in Amazon S3. The company is expecting 10-15 job requests each day.

Which solution meets these requirements?

- A. Use regularly scheduled AWS Snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use S3 events to trigger an AWS Lambda function to process the data.

B. Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto Scaling group to launch custom-AMI EC2 instances running the Docker containers to process the data.

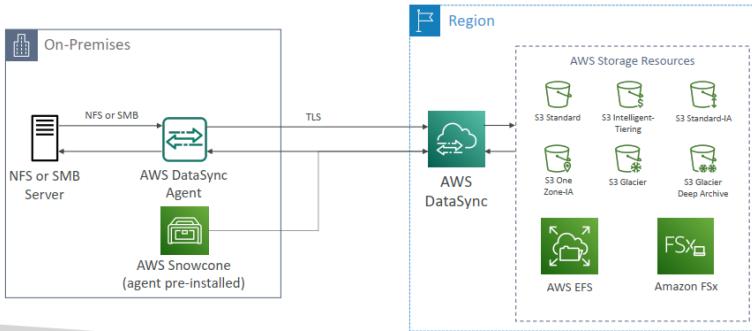
C. Use AWS DataSync to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Lambda function that starts an AWS Step Functions workflow. Store the Docker images in Amazon Elastic Container Registry (Amazon ECR) and trigger AWS Batch to run the container and process the sequencing data.

D. Use an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Batch job that executes on Amazon EC2 instances running the Docker containers to process the data.

C

Step Function Integrations

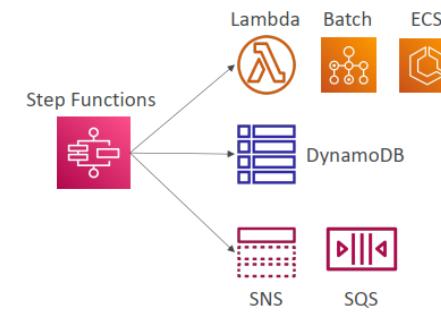
AWS DataSync NFS / SMB to AWS (S3, EFS, FSx...)



AWS Batch

- Run batch jobs as Docker images
- Two options:
 1. Run on AWS Fargate (fully serverless offering)
 2. Dynamic provisioning of the instances (EC2 & Spot Instances) – in VPC
- Optimal quantity and type based on volume and requirements
- No need to manage clusters, fully **serverless**
- You just pay for the underlying resources used
- Example: batch process of images, running thousands of concurrent jobs
- Schedule Batch Jobs using Amazon EventBridge
- Orchestrate Batch Jobs using AWS Step Functions

- **Optimized Integrations** Tích hợp được tối ưu hóa
 - Can invoke a Lambda function
 - Run an AWS Batch job
 - Run an ECS task and wait for it to complete
 - Insert an item from DynamoDB
 - Publish message to SNS, SQS
 - Launch an EMR, Glue, or SageMaker jobs
 - Launch another Step Function workflow...
- **AWS SDK Integrations**
 - Access 200+ AWS services from your State Machine
 - Works like standard AWS SDK API call



Question 139:

A company runs a content management application on a single Windows Amazon EC2 instance in a development environment. The application reads and writes static content to a 2 TB Amazon Elastic Block Store (Amazon EBS) volume that is attached to the instance as the root device. The company plans to deploy this application in production as a highly available and fault-tolerant solution that runs on at least three EC2 instances across multiple Availability Zones.

A solutions architect must design a solution that joins all the instances that run the application to an Active Directory domain. The solution also must implement Windows ACLs to control access to file contents. The application always must maintain exactly the same content on all running instances at any given point in time.

Which solution will meet these requirements with the LEAST management overhead?

- A. Create an Amazon Elastic File System (Amazon EFS) file share. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application, join the instance to the AD domain, and mount the EFS file share.
- B. Create a new AMI from the current EC2 Instance that is running. Create an Amazon FSx for Lustre file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to join the instance to the AD domain and mount the FSx for Lustre file system.
- C. Create an Amazon FSx for Windows File Server file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application and mount the FSx for Windows File Server file system. Perform a seamless domain join to join the instance to the AD domain.
- D. Create a new AMI from the current EC2 instance that is running. Create an Amazon Elastic File System (Amazon EFS) file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three Instances. Perform a seamless domain join to join the instance to the AD domain.

C EFS and FSx for Lustre == Linux FSx Windows File == Windows

Amazon FSx for Windows (File Server)



- FSx for Windows is a fully managed Windows file system share drive chia sẻ ổ đĩa
- Supports SMB protocol & Windows NTFS
- Microsoft Active Directory integration, ACLs, user quotas
- Can be mounted on Linux EC2 instances
- Supports Microsoft's Distributed File System (DFS) Namespaces (group files across multiple FS)
- Scale up to 10s of GB/s, millions of IOPS, 100s PB of data
- Storage Options:
 - SSD – latency sensitive workloads (databases, media processing, data analytics, ...)
 - HDD – broad spectrum of workloads (home directory, CMS, ...) phạm vi rộng của khối lượng công việc
- Can be accessed from your on-premises infrastructure (VPN or Direct Connect)
- Can be configured to be Multi-AZ (high availability)
- Data is backed-up daily to S3

Question 140:

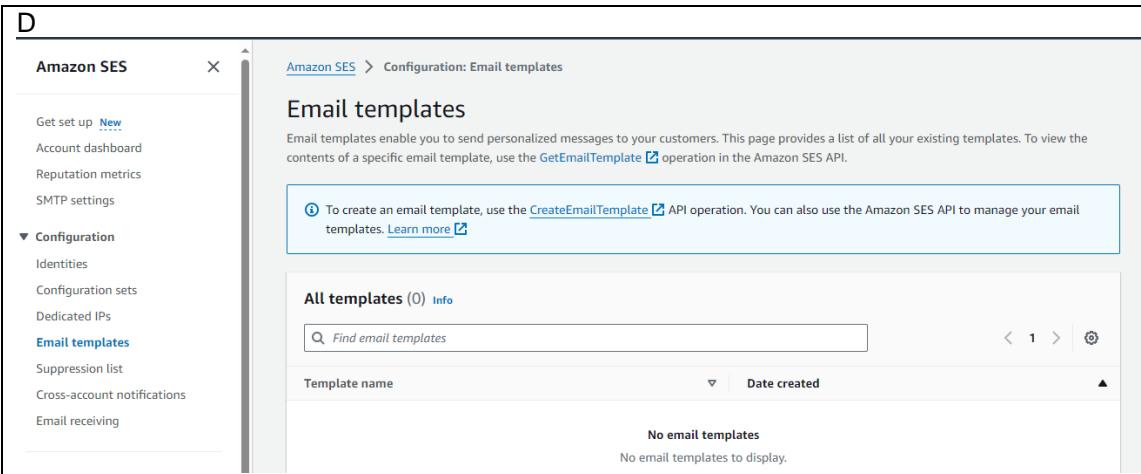
A software as a service (SaaS) based company provides a case management solution to customers A3 part of the solution. The company uses a standalone Simple Mail Transfer Protocol (SMTP) server to send email messages from an application. The application also stores an email template for acknowledgement email messages that populate customer data before the application sends the email message to the customer.

The company plans to migrate this messaging functionality to the AWS Cloud and needs to minimize operational overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplace. Store the email template in an Amazon S3 bucket. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the template. Use an SDK in the Lambda function to send the email message.
- B. Set up Amazon Simple Email Service (Amazon SES) to send email messages. Store the email template in an Amazon S3 bucket. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the template. Use an SDK in the Lambda function to send the email message.
- C. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplace. Store the email template in Amazon Simple Email Service (Amazon SES) with parameters for the customer data. Create an AWS Lambda function to call the SES template and to pass customer data to replace the parameters. Use the AWS Marketplace SMTP server to send the email message.
- D. Set up Amazon Simple Email Service (Amazon SES) to send email messages. Store the email template on Amazon SES with parameters for the customer data. Create an AWS Lambda function to call the SendTemplatedEmail API operation and to pass customer data to replace the parameters and the email destination.

D



Amazon Simple Email Service (Amazon SES)



- Fully managed service to send emails securely, globally and at scale
- Allows inbound/outbound emails
- Reputation dashboard, performance insights, anti-spam feedback
- Provides statistics such as email deliveries, bounces, feedback loop results, email open
- Supports DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF)
- Flexible IP deployment: shared, dedicated, and customer-owned IPs
- Send emails using your application using AWS Console, APIs, or SMTP
- Use cases: transactional, marketing and bulk email communications

[liên lạc email hàng loạt \(email số lượng lớn\)](#)

Question 141:

A company is processing videos in the AWS Cloud by Using Amazon EC2 instances in an Auto Scaling group. It takes 30 minutes to process a video Several EC2 instances scale in and out depending on the number of videos in an Amazon Simple Queue Service (Amazon SQS) queue.

The company has configured the SQS queue with a redrive policy that specifies a target dead-letter queue and a maxReceiveCount of 1. The company has set the visibility timeout for the SQS queue to 1 hour. The company has set up an Amazon CloudWatch alarm to notify the development team when there are messages in the dead-letter queue.

Several times during the day, the development team receives notification that messages are in the dead-letter queue and that videos have not been processed properly. An investigation finds no errors in the application logs.

How can the company solve this problem?

- A. Turn on termination protection for the EC2 Instances
- B. Update the visibility timeout for the SQS queue to 3 hours
- C. Configure scale-in protection for the instances during processing
- D. Update the redrive policy and set maxReceiveCount to 0.

C

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-instance-protection.html>

The correct answer is C. The company can solve the problem by configuring scale-in protection for the instances during processing. This will ensure that the instances are not terminated while they are processing videos. This will prevent the messages from moving to the dead-letter queue and ensure that videos are processed properly.

- The goal of an Auto Scaling Group (ASG) is to:
 - Scale out (add EC2 instances) to match an increased load
 - Scale in (remove EC2 instances) to match a decreased load
 - Ensure we have a minimum and a maximum number of EC2 instances running
 - Automatically register new instances to a load balancer
 - Re-create an EC2 instance in case a previous one is terminated (ex: if unhealthy)

High Availability & Scalability For EC2

- Vertical Scaling: Increase instance size (= scale up / down)
 - From: t2.nano - 0.5G of RAM, 1 vCPU
 - To: u-12tb1.metal – 12.3 TB of RAM, 448 vCPUs
- Horizontal Scaling: Increase number of instances (= scale out / in)
 - Auto Scaling Group
 - Load Balancer
- High Availability: Run instances for the same application across multi-AZ
 - Auto Scaling Group multi-AZ
 - Load Balancer multi-AZ

Option A is incorrect because turning on termination protection for the EC2 instances will not solve the problem as it will impact the ability of the Auto Scaling group to scale instances in and out based on the number of videos in the queue.

Option B is incorrect because the company has specified a visibility timeout of 1 hour, which is enough time for the instances to process a video and there is no need to update the timeout to 3 hours.

Option D is incorrect because the company has set the maxReceiveCount to 1 and changing it to 0 will not solve the problem. maxReceiveCount allowed range is 1 to 1000.

Question 142:

A company has developed APIs that use Amazon API Gateway with Regional endpoints. The APIs call AWS Lambda functions that use API Gateway authentication mechanisms. After a design review, a solutions architect identifies a set of APIs that do not require public access.

The solutions architect must design a solution to make the set of APIs accessible only from a VPC. All APIs need to be called with an authenticated user

Which solution will meet these requirements with the LEAST amount of effort?

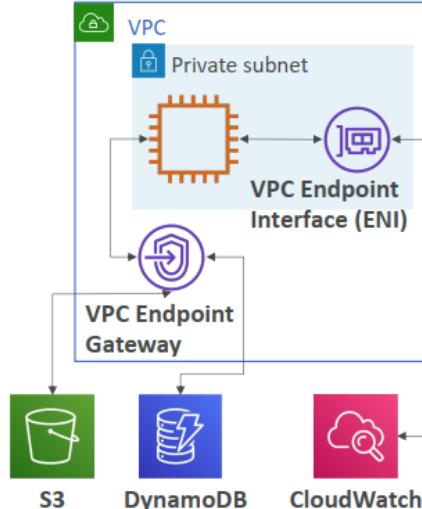
- Create an internal Application Load Balancer (ALB). Create a target group. Select the Lambda function to call. Use the ALB DNS name to call the API from the VPC.
- Remove the DNS entry that is associated with the API in API Gateway. Create a hosted zone in Amazon Route 53. Create a CNAME record in the hosted zone. Update the API in API Gateway with the CNAME record. Use the CNAME record to call the API from the VPC.
- Update the API endpoint from Regional to private in API Gateway. Create an interface VPC endpoint in the VPC. Create a resource policy, and attach it to the API. Use the VPC endpoint to call the API from the VPC.
- Deploy the Lambda functions inside the VPC Provision an EC2 instance, and install an Apache server. From the Apache server, call the Lambda functions. Use the internal CNAME record of the EC2 instance to call the API from the VPC.

C

do not require public access ➔ private API Gateway

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables



<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html>

https://viblo.asia/p/tim-hieu-aws-api-gateway-RnB5pMW2KPG#_2-throttle-2

<https://aws.amazon.com/blogs/compute/introducing-amazon-api-gateway-private-endpoints/>

Question 143:

A weather service provides high-resolution weather maps from a web application hosted on AWS in the eu-west-1 Region. The weather maps are updated frequently and stored in Amazon S3 along with static HTML content. The web application is fronted by Amazon CloudFront.

The company recently expanded to serve users in the us-east-1 Region, and these new users report that viewing their respective weather maps is slow from time to time.

Which combination of steps will resolve the us-east-1 performance issues? (Choose two.)

- Configure the AWS Global Accelerator endpoint for the S3 bucket in eu-west-1. Configure endpoint groups for TCP ports 80 and 443 in us-east-1.
- Create a new S3 bucket in us-east-1. Configure S3 cross-Region replication to synchronize from the S3 bucket in eu-west-1.
- Use Lambda@Edge to modify requests from North America to use the S3 Transfer Acceleration endpoint in us-east-1.
- Use Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1.

E. Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the CloudFront distribution. Use Lambda@Edge to modify requests from North America to use the new origin.

B,D

B is correct because it involves creating a new S3 bucket in the us-east-1 region and configuring cross-Region replication to synchronize from the existing S3 bucket in eu-west-1. This will allow users in us-east-1 to access the weather maps from a closer location, improving performance.

D is correct because it involves using Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1. This will also allow users in us-east-1 to access the weather maps from a closer location, improving performance.

A and E are not correct because they do not involve creating a new S3 bucket in us-east-1, which is necessary for improving performance for the users in that region.

C is not correct because it involves using the S3 Transfer Acceleration endpoint, which is a different service and not necessary for this scenario.

Question 144:

A solutions architect is investigating an issue in which a company cannot establish new sessions in Amazon Workspaces. An initial analysis indicates that the issue involves user profiles. The Amazon Workspaces environment is configured to use Amazon FSx for Windows File Server as the profile share storage. The FSx for Windows File Server file system is configured with 10 TB of storage.

The solutions architect discovers that the file system has reached its maximum capacity. The solutions architect must ensure that users can regain access. The solution also must prevent the problem from occurring again.

Which solution will meet these requirements?

A. Remove old user profiles to create space. Migrate the user profiles to an Amazon FSx for Lustre file system.

B. Increase capacity by using the update-file-system command. Implement an Amazon CloudWatch metric that monitors free space. Use Amazon EventBridge to invoke an AWS Lambda function to increase capacity as required.

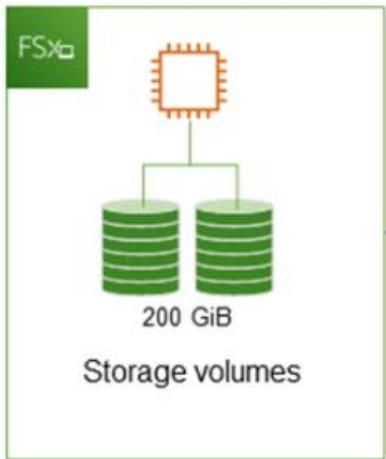
C. Monitor the file system by using the FreeStorageCapacity metric in Amazon CloudWatch. Use AWS Step Functions to increase the capacity as required.

D. Remove old user profiles to create space. Create an additional FSx for Windows File Server file system. Update the user profile redirection for 50% of the users to use the new file system.

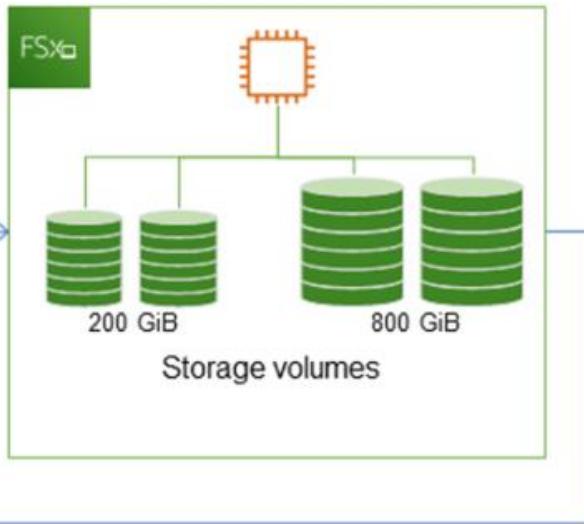
B

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-capacity.html>

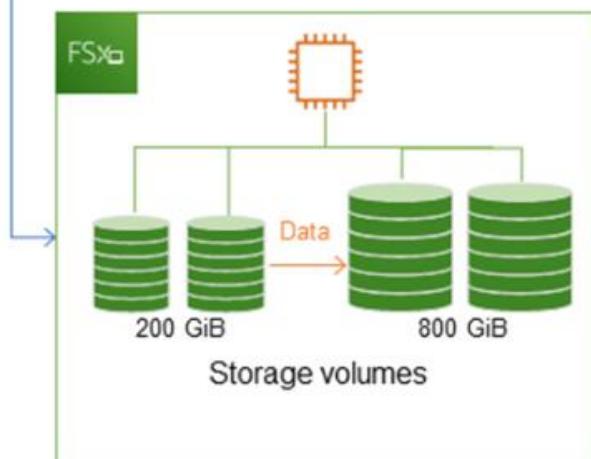
Step 1: Storage capacity increase request to 800 GiB.



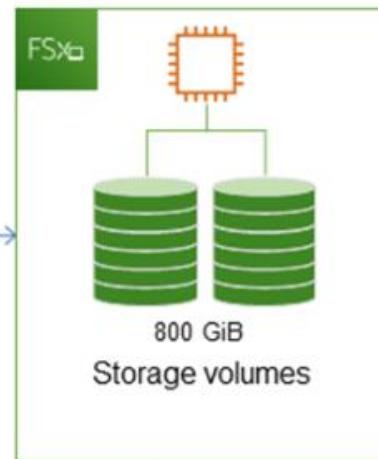
Step 2: Amazon FSx adds the new, larger disks.



Step 3: Amazon FSx migrates data to larger disks.



Step 4: Amazon FSx removes smaller disks.



B is correct. It can prevent the issue from happening again by monitoring the file system with the FreeStorageCapacity metric in Amazon CloudWatch and using Amazon EventBridge to invoke an AWS Lambda function to increase the capacity as required. This ensures that the file system always has enough free space to store user profiles and avoids reaching maximum capacity.

A: Removing old user profiles may not be sufficient to create enough space and does not prevent the problem from happening again.

C: AWS Step Functions cannot be used to increase capacity, it is a service for creating and running workflows that stitch together multiple AWS services.

D: Creating an additional FSx for Windows File Server file system and updating user profile redirection for a portion of the users may not be sufficient to prevent the problem from happening again and does not address the current capacity issue.

Question 145:

An international delivery company hosts a delivery management system on AWS. Drivers use the system to upload confirmation of delivery. Confirmation includes the recipient's signature or a photo of the package with the recipient. The driver's handheld device uploads signatures and photos through FTP to a single Amazon EC2 instance. Each handheld device saves a file in a directory based on the signed-in user, and the file name matches the delivery number. The EC2 instance then adds metadata to the file after querying a central database to pull delivery information. The file is then placed in Amazon S3 for archiving.

As the company expands, drivers report that the system is rejecting connections. The FTP server is having problems because of dropped connections and memory issues in response to these problems, a system engineer schedules a cron task to reboot the EC2 instance every 30 minutes. The billing team reports that files are not always in the archive and that the central system is not always updated.

A solutions architect needs to design a solution that maximizes scalability to ensure that the archive always receives the files and that systems are always updated. The handheld devices cannot be modified, so the company cannot deploy a new application.

Which solution will meet these requirements?

- A. Create an AMI of the existing EC2 instance. Create an Auto Scaling group of EC2 instances behind an Application Load Balancer. Configure the Auto Scaling group to have a minimum of three instances.
- B. Use AWS Transfer Family to create an FTP server that places the files in Amazon Elastic File System (Amazon EFS). Mount the EFS volume to the existing EC2 instance. Point the EC2 instance to the new path for file processing.
- C. Use AWS Transfer Family to create an FTP server that places the files in Amazon S3. Use an S3 event notification through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function. Configure the Lambda function to add the metadata and update the delivery system.
- D. Update the handheld devices to place the files directly in Amazon S3. Use an S3 event notification through Amazon Simple Queue Service (Amazon SQS) to invoke an AWS Lambda function. Configure the Lambda function to add the metadata and update the delivery system.

C

C is correct. Using AWS Transfer Family to create an FTP server that places the files in Amazon S3 and using S3 event notifications through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function will ensure that the archive always receives the files and that the central system is always updated. This solution maximizes scalability and eliminates the need for manual intervention, such as rebooting the EC2 instance.

Option A and B still use EC2 instance, which is the source of the problem.

Option D requires modification to the handheld devices which is not possible.

Question 146:

A company is running an application in the AWS Cloud. The application runs on containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS tasks use the Fargate launch type. The application's data is relational and is stored in Amazon Aurora MySQL. To meet regulatory requirements, the application must be able to recover to a separate AWS Region in the event of an application failure. In case of a failure, no data can be lost.

Which solution will meet these requirements with the LEAST amount of operational overhead?

- A. Provision an Aurora Replica in a different Region.
- B. Set up AWS DataSync for continuous replication of the data to a different Region.
- C. Set up AWS Database Migration Service (AWS DMS) to perform a continuous replication of the data to a different Region.
- D. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule a snapshot every 5 minutes.

A

A is correct. Provision an Aurora Replica in a different Region will meet the requirement of the application being able to recover to a separate AWS Region in the event of an application failure, and no data can be lost, with the least amount of operational overhead.
B. AWS DataSync can replicate data, but it is not a fully managed service and requires more configuration and management.
C. AWS DMS is a fully managed service for migrating data between databases, but it may require additional configuration and management to continuously replicate data in real-time.
D. Amazon DLM can be used for scheduling snapshots, but it does not provide real-time replication and may not meet the requirement of no data loss in case of a failure.

Question 147:

A financial services company receives a regular data feed from its credit card servicing partner. Approximately 5,000 records are sent every 15 minutes in plaintext, delivered over HTTPS directly into an Amazon S3 bucket with server-side encryption. This feed contains sensitive credit card primary account number (PAN) data. The company needs to automatically mask the PAN before sending the data to another S3 bucket for additional internal processing. The company also needs to remove and merge specific fields, and then transform the record into JSON format. Additionally, extra feeds are likely to be added in the future, so any design needs to be easily expandable.

Which solutions will meet these requirements?

- A. Invoke an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Invoke another Lambda function when new messages arrive in the SQS queue to process the records, writing the results to a temporary location in Amazon S3. Invoke a final Lambda function once the SQS queue is empty to transform the records into JSON format and send the results to another S3 bucket for internal processing.
- B. Invoke an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Configure an AWS Fargate container application to automatically scale to a single instance when the SQS queue contains messages. Have the application process each record, and transform the record into JSON format. When the queue is empty, send the results to another S3 bucket for internal processing and scale down the AWS Fargate instance.
- C. Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match. Invoke an AWS Lambda function on file delivery to start an AWS Glue ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, have the ETL job send the results to another S3 bucket for internal processing.
- D. Create an AWS Glue crawler and custom classifier based upon the data feed formats and build a table definition to match. Perform an Amazon Athena query on file delivery to start an Amazon EMR ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, send the results to another S3 bucket for internal processing and scale down the EMR cluster.

C

Option C is the most suitable solution for the described scenario:

- 1) AWS Glue Crawler and Custom Classifier: Use AWS Glue to create a crawler and custom classifier to understand and catalogue the data feed formats. This step ensures that AWS Glue can work with the incoming data effectively.
- 2) AWS Glue ETL Job: Create an AWS Lambda function that triggers an AWS Glue ETL job when a new data file is delivered. This ETL job can perform the required transformation, including masking, field removal, and converting records to JSON format. AWS Glue is a suitable service for data preparation and transformation.
- 3) Output to S3 Bucket. This approach is scalable, easily expandable to handle additional feeds in the future, and leverages AWS Glue's capabilities for data transformation and processing. It also maintains a clear separation of tasks, making it a robust and efficient solution for the given requirements.

Question 148:

A company wants to use AWS to create a business continuity solution in case the company's main on-premises application fails. The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store. All the company's on-premises applications use operating systems that are compatible with Amazon EC2.

Which solution will achieve the company's goal with the LEAST operational overhead?

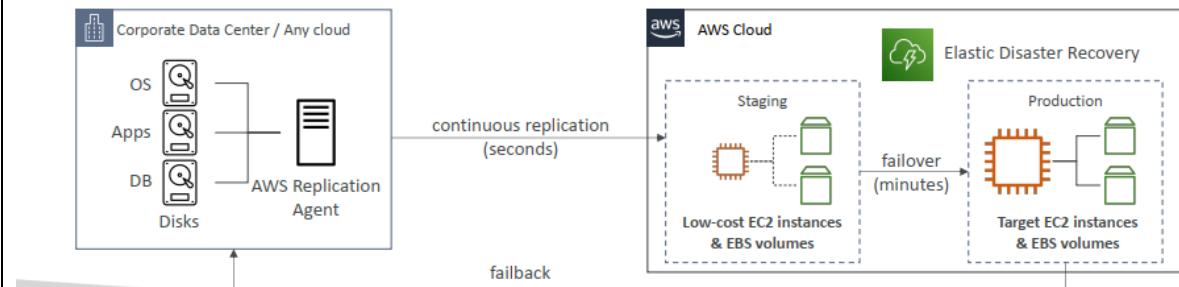
- A. Install the AWS Replication Agent on the source servers, including the MySQL servers. Set up replication for all servers. Launch test instances for regular drills. Cut over to the test instances to fail over the workload in the case of a failure event.
- B. Install the AWS Replication Agent on the source servers, including the MySQL servers. Initialize AWS Elastic Disaster Recovery in the target AWS Region. Define the launch settings. Frequently perform failover and fallback from the most recent point in time.
- C. Create AWS Database Migration Service (AWS DMS) replication servers and a target Amazon Aurora MySQL DB cluster to host the database. Create a DMS replication task to copy the existing data to the target DB cluster. Create a local AWS Schema Conversion Tool (AWS SCT) change data capture (CDC) task to keep the data synchronized. Install the rest of the software on EC2 instances by starting with a compatible base AMI.
- D. Deploy an AWS Storage Gateway Volume Gateway on premises. Mount volumes on all on-premises servers. Install the application and the MySQL database on the new volumes. Take regular snapshots. Install all the software on EC2 Instances by starting with a compatible base AMI. Launch a Volume Gateway on an EC2 instance. Restore the volumes from the latest snapshot. Mount the new volumes on the EC2 instances in the case of a failure event.

B

AWS Elastic Disaster Recovery (DRS)



- Used to be named "CloudEndure Disaster Recovery"
- Quickly and easily **recover** your physical, virtual, and cloud-based servers into AWS
- Example: protect your most critical databases (including Oracle, MySQL, and SQL Server), enterprise apps (SAP), protect your data from ransomware attacks, ...
- Continuous block-level replication for your servers



On-premises strategy with AWS

- Ability to download Amazon Linux 2 AMI as a VM (.iso format)
 - VMWare, KVM, VirtualBox (Oracle VM), Microsoft Hyper-V
- AWS Application Discovery Service**
 - Gather information about your on-premises servers to plan a migration
 - Server utilization and dependency mappings
 - Track with AWS Migration Hub
- AWS Application Migration Service (MGN)**
 - Replacing AWS Server Migration Services & CloudEndure Migration
 - Incremental replication of on-premises live servers to AWS
 - Migrates the entire VM into AWS
- AWS Elastic Disaster Recovery (DRS)**
 - Replacing CloudEndure Disaster Recovery
 - Recover on-premises workloads onto AWS
- AWS Database Migration Service (DMS)**
 - replicate on-premises => AWS, AWS => AWS, AWS => on-premises
 - Works with various database technologies (Oracle, MySQL, DynamoDB, etc.)



AWS Application Discovery Service



AWS Application Migration Service



AWS Elastic Disaster Recovery



AWS Database Migration Service

Question 149:

A company is subject to regulatory audits of its financial information. External auditors who use a single AWS account need access to the company's AWS account. A solutions architect must provide the auditors with secure, read-only access to the company's AWS account. The solution must comply with AWS security best practices.

Which solution will meet these requirements?

- A. In the company's AWS account, create resource policies for all resources in the account to grant access to the auditors' AWS account. Assign a unique external ID to the resource policy.
- B. In the company's AWS account, create an IAM role that trusts the auditors' AWS account. Create an IAM policy that has the required permissions. Attach the policy to the role. Assign a unique external ID to the role's trust policy.
- C. In the company's AWS account, create an IAM user. Attach the required IAM policies to the IAM user. Create API access keys for the IAM user. Share the access keys with the auditors.
- D. In the company's AWS account, create an IAM group that has the required permissions. Create an IAM user in the company's account for each auditor. Add the IAM users to the IAM group.

B

Option B is the best solution. This solution creates an IAM role that trusts the auditors' AWS account and attaches the required IAM policies to the role. This ensures that the auditors have read-only access to the company's AWS account while ensuring that the company's AWS account is secure and complies with AWS security best practices. Additionally, the unique external ID assigned to the role's trust policy adds an extra layer of security.

Option A is incorrect because it grants access to all resources in the company's AWS account and does not provide a way to restrict the permissions that the external auditors have.

Option C is incorrect because it creates an IAM user in the company's account and shares the API access keys with the external auditors, which is not secure and does not comply with AWS security best practices.

Option D is incorrect because it creates an IAM user in the company's account for each auditor, which would be tedious and difficult to manage for the company. It would be more secure and efficient to use an IAM role that trusts the auditors' AWS account instead of creating individual users for each auditor.

Providing Access to AWS Accounts Owned by Third Parties

- Zone of trust = accounts, organizations that you own
- Outside Zone of Trust = 3rd parties
- Use IAM Access Analyzer to find out which resources are exposed
- For granting access to a 3rd party:
 - The 3rd party AWS account ID
 - An External ID (secret between you and the 3rd party)
 - To uniquely associate with the role between you and 3rd party
 - Must be provided when defining the trust and when assuming the role
 - Must be chosen by the 3rd party
- Define permissions in the IAM policy

Question 150:

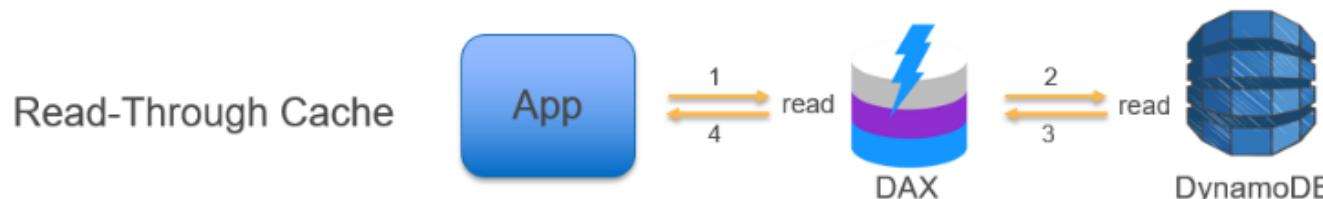
A company has a latency-sensitive trading platform that uses Amazon DynamoDB as a storage backend. The company configured the DynamoDB table to use on-demand capacity mode. A solutions architect needs to design a solution to improve the performance of the trading platform. The new solution must ensure high availability for the trading platform.

Which solution will meet these requirements with the LEAST latency?

- A. Create a two-node DynamoDB Accelerator (DAX) cluster. Configure an application to read and write data by using DAX.
- B. Create a three-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.
- C. Create a three-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data directly from the DynamoDB table and to write data by using DAX.
- D. Create a single-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.

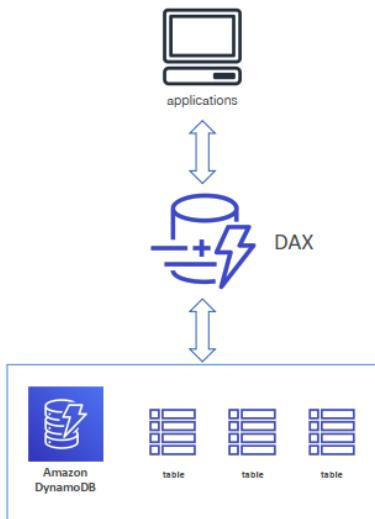
B

<https://aws.amazon.com/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>



DynamoDB - DAX

- DAX = DynamoDB Accelerator
Lien mạch
- Seamless cache for DynamoDB, no application rewrite
- Writes go through DAX to DynamoDB
- Micro second latency for cached reads & queries
- Solves the Hot Key problem (too many reads)
- 5 minutes TTL for cache by default
- Up to 10 nodes in the cluster
- Multi AZ (3 nodes minimum recommended for production)
- Secure (Encryption at rest with KMS, VPC, IAM, CloudTrail...)



Question 151:

A company has migrated an application from on premises to AWS. The application frontend is a static website that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB). The application backend is a Python application that runs on three EC2 instances behind another ALB. The EC2 instances are large, general purpose On-Demand Instances that were sized to meet the on-premises specifications for peak usage of the application.

The application averages hundreds of thousands of requests each month. However, the application is used mainly during lunchtime and receives minimal traffic during the rest of the day.

A solutions architect needs to optimize the infrastructure cost of the application without negatively affecting the application availability.

Which combination of steps will meet these requirements? (Choose two.)

- Change all the EC2 instances to compute optimized instances that have the same number of cores as the existing EC2 instances.
- Move the application frontend to a static website that is hosted on Amazon S3.
- Deploy the application frontend by using AWS Elastic Beanstalk. Use the same instance type for the nodes.
- Change all the backend EC2 instances to Spot Instances.
- Deploy the backend Python application to general purpose burstable EC2 instances that have the same number of cores as the existing EC2 instances.

B, E

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html>

Option E suggests deploying the backend Python application to general purpose burstable EC2 instances that have the same number of cores as the existing EC2 instances. Burstable instances provide a baseline level of CPU performance with the ability to burst above the baseline when needed. This can be a cost-effective option for workloads that have variable CPU usage and can benefit from the ability to burst during periods of high demand. However, if the workload consistently requires high CPU usage, using burstable instances may not provide significant cost savings compared to using larger general purpose instances.

The EC2 burstable instances consist of T4g, T3a and T3 instance types, and the previous generation T2 instance types.

The T4g instance types are the latest generation of burstable instances. They provide the best price for performance, and provide you with the lowest cost of all the EC2 instance types. The T4g instance types are powered by Arm-based AWS Graviton2 processors with extensive ecosystem support from operating systems vendors, independent software vendors, and popular AWS services and applications.

Question 152:

A company is running an event ticketing platform on AWS and wants to optimize the platform's cost-effectiveness. The platform is deployed on Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 and is backed by an Amazon RDS for MySQL DB instance. The company is developing new application features to run on Amazon EKS with AWS Fargate.

The platform experiences infrequent high peaks in demand. The surges in demand depend on event dates.

Which solution will provide the MOST cost-effective setup for the platform?

- A. Purchase Standard Reserved Instances for the EC2 instances that the EKS cluster uses in its baseline load. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet predicted peak load for the year.
- B. Purchase Compute Savings Plans for the predicted medium load of the EKS cluster. Scale the cluster with On-Demand Capacity Reservations based on event dates for peaks. Purchase 1-year No Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale out database read replicas during peaks.
- C. Purchase EC2 Instance Savings Plans for the predicted base load of the EKS cluster. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale up the DB instance manually during peaks.
- D. Purchase Compute Savings Plans for the predicted base load of the EKS cluster. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale up the DB instance manually during peaks.

B

Option A, C and D are wrong. They all mention using spot instances and EKS based on EC2. A spot instance is not appropriate for a production server and the company is developing new application designed for AWS Fargate, which means we must plan the future cost improvement including AWS Fargate.

C,D: manually scale up DB

AWS Savings Plan



- New pricing model to get a discount based on long-term usage
Cam kết sử dụng T loại
- Commit to a certain type of usage: ex \$10 per hour for 1 to 3 years
- Any usage beyond the savings plan is billed at the on-demand price
- EC2 Instance Savings plan (up to 72% - same discount as Standard RIs)
 - Select instance family (e.g. M5, C5...), and locked to a specific region
 - Flexible across size (m5.large to m5.4xlarge), OS (Windows to Linux), thuê tenancy (dedicated or default)
- Compute Savings plan (up to 66% - same discount as Convertible RIs)
 - Ability to move between instance family (move from C5 to M5), region (Ireland to US), compute type (EC2, Fargate, Lambda), OS & tenancy
- SageMaker Savings plan (up to 64% off)

Question 153:

A company has deployed an application on AWS Elastic Beanstalk. The application uses Amazon Aurora for the database layer. An Amazon CloudFront distribution serves web requests and includes the Elastic Beanstalk domain name as the origin server. The distribution is configured with an alternate domain name that visitors use when they access the application.

Each week, the company takes the application out of service for routine maintenance. During the time that the application is unavailable, the company wants visitors to receive an informational message instead of a CloudFront error message.

A solutions architect creates an Amazon S3 bucket as the first step in the process.

Which combination of steps should the solutions architect take next to meet the requirements? (Choose three.)

- Upload static informational content to the S3 bucket.
- Create a new CloudFront distribution. Set the S3 bucket as the origin.
- Set the S3 bucket as a second origin in the original CloudFront distribution. Configure the distribution and the S3 bucket to use an origin access identity (OAI).
- During the weekly maintenance, edit the default cache behavior to use the S3 origin. Revert the change when the maintenance is complete.

E. During the weekly maintenance, create a cache behavior for the S3 origin on the new distribution. Set the path pattern to \ Set the precedence to 0. Delete the cache behavior when the maintenance is complete.

F. During the weekly maintenance, configure Elastic Beanstalk to serve traffic from the S3 bucket.

A,C,D

Step 1: The solutions architect should upload static informational content to the S3 bucket, this content will be shown to the users when the application is down for maintenance.

Step 2: The solutions architect should set the S3 bucket as a second origin in the original CloudFront distribution. To keep the S3 bucket secure, the solutions architect should configure the distribution and the S3 bucket to use an origin access identity (OAI). This will ensure that only CloudFront has access to the S3 bucket.

Step 3: During the weekly maintenance, the solutions architect should edit the default cache behavior of the CloudFront distribution to use the S3 origin. This will redirect all incoming traffic to the S3 bucket and show the static informational content to the users. Once the maintenance is complete, the solutions architect should revert the change back to the original Elastic Beanstalk origin.

Option B: Creating a new CloudFront distribution and setting the S3 bucket as the origin is unnecessary and could cause confusion for the users.

Option E: During the weekly maintenance, creating a cache behavior for the S3 origin on the new distribution is unnecessary, it is more complex and prone to human error.

Option F: Configuring Elastic Beanstalk to serve traffic from the S3 bucket is not necessary because CloudFront is already being used as the web request server.

Question 154:

A company gives users the ability to upload images from a custom application. The upload process invokes an AWS Lambda function that processes and stores the image in an Amazon S3 bucket. The application invokes the Lambda function by using a specific function version ARN.

The Lambda function accepts image processing parameters by using environment variables. The company often adjusts the environment variables of the Lambda function to achieve optimal image processing output. The company tests different parameters and publishes a new function version with the updated environment variables after validating results. This update process also requires frequent changes to the custom application to invoke the new function version ARN. These changes cause interruptions for users.

A solutions architect needs to simplify this process to minimize disruption to users.

Which solution will meet these requirements with the LEAST operational overhead?

A. Directly modify the environment variables of the published Lambda function version. Use the SLATEST version to test image processing parameters.

B. Create an Amazon DynamoDB table to store the image processing parameters. Modify the Lambda function to retrieve the image processing parameters from the DynamoDB table.

C. Directly code the image processing parameters within the Lambda function and remove the environment variables. Publish a new function version when the company updates the parameters.

D. Create a Lambda function alias. Modify the client application to use the function alias ARN. Reconfigure the Lambda alias to point to new versions of the function when the company finishes testing.

D

<https://aws.amazon.com/blogs/contact-center/invoke-an-aws-lambda-function-alias-from-amazon-connect/>
<https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html>

You can create aliases for your Lambda function. A Lambda alias is a pointer to a function version that you can update. The function's users can access the function version using the alias Amazon Resource Name (ARN). When you deploy a new version, you can update the alias to use the new version, or split traffic between two versions.

Question 155:

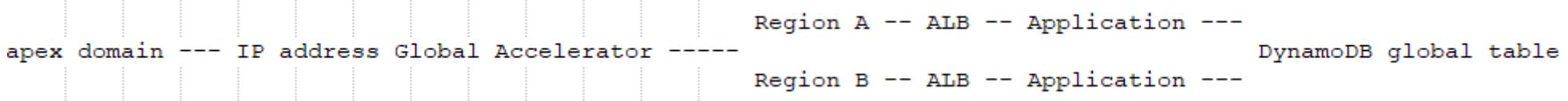
A global media company is planning a multi-Region deployment of an application. Amazon DynamoDB global tables will back the deployment to keep the user experience consistent across the two continents where users are concentrated. Each deployment will have a public Application Load Balancer (ALB). The company manages public DNS internally. The company wants to make the application available through an apex domain.

Which solution will meet these requirements with the LEAST effort?

- A. Migrate public DNS to Amazon Route 53. Create CNAME records for the apex domain to point to the ALB. Use a geolocation routing policy to route traffic based on user location.
- B. Place a Network Load Balancer (NLB) in front of the ALB. Migrate public DNS to Amazon Route 53. Create a CNAME record for the apex domain to point to the NLB's static IP address. Use a geolocation routing policy to route traffic based on user location.
- C. Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Regions. Use the accelerator's static IP address to create a record in public DNS for the apex domain.
- D. Create an Amazon API Gateway API that is backed by AWS Lambda in one of the AWS Regions. Configure a Lambda function to route traffic to application deployments by using the round robin method. Create CNAME records for the apex domain to point to the API's URL.

C

<https://aws.amazon.com/blogs/networking-and-content-delivery/solving-dns-zone-apex-challenges-with-third-party-dns-providers-using-aws/>



Apex domain (tên miền gốc) là tên miền cấp cao nhất trong một tên miền phân cấp. Nó là phần không có tiền tố của tên miền và được đặt sau ký tự "www" (nếu có). Ví dụ, trong tên miền "www.example.com", "example.com" là apex domain.

Apex domain thường đại diện cho trang web chính hoặc trang chủ của một tổ chức hoặc doanh nghiệp trên Internet. Nó là trang mà người dùng thường nhất truy cập khi truy cập vào tên miền đó. Trên apex domain, bạn có thể cấu hình các bản ghi DNS như A, AAAA, CNAME, MX, TXT, v.v. để chỉ định địa chỉ IP hoặc cấu hình khác cho tên miền.

Lưu ý rằng apex domain không bao gồm tiền tố "www" hay bất kỳ tiền tố con nào khác. Tuy nhiên, trong một số trường hợp, người ta có thể sử dụng tiền tố con như "www" để chỉ định một dịch vụ cụ thể hoặc mục đích khác trên cùng một tên miền.

AWS Global Accelerator

- Works with Elastic IP, EC2 instances, ALB, NLB, public or private
- Supports Client IP Address Preservation Hỗ trợ bảo quản IP của khách hàng ngoại trừ NLB và EIPs endpoint
- Consistent Performance Hiệu suất nhất quán
 - Intelligent routing to lowest latency and fast regional failover
 - No issue with client cache (because the IP doesn't change)
 - Internal AWS network
- Health Checks
 - Global Accelerator performs a health check of your applications
 - Helps make your application global (failover less than 1 minute for unhealthy)
 - Great for disaster recovery (thanks to the health checks)
- Security
 - only 2 external IP need to be whitelisted
 - DDoS protection thanks to AWS Shield

Route 53 – Record Types

- A – maps a hostname to IPv4
- AAAA – maps a hostname to IPv6
- CNAME – maps a hostname to another hostname
 - The target is a domain name which must have an A or AAAA record
 - Can't create a CNAME record for the top node of a DNS namespace (Zone Apex)
 - Example: you can't create for example.com, but you can create for www.example.com
- NS – Name Servers for the Hosted Zone
 - Control how traffic is routed for a domain

Question 156:

A company is developing a new serverless API by using Amazon API Gateway and AWS Lambda. The company integrated the Lambda functions with API Gateway to use several shared libraries and custom classes.

A solutions architect needs to simplify the deployment of the solution and optimize for code reuse.

Which solution will meet these requirements?

- A. Deploy the shared libraries and custom classes into a Docker image. Store the image in an S3 bucket. Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.
- B. Deploy the shared libraries and custom classes to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.
- C. Deploy the shared libraries and custom classes to a Docker container in Amazon Elastic Container Service (Amazon ECS) by using the AWS Fargate launch type. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the deployed container as a Lambda layer.
- D. Deploy the shared libraries, custom classes, and code for the API's Lambda functions to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Configure the API's Lambda functions to use the Docker image as the deployment package.

<https://www.examtopics.com/discussions/amazon/view/95494-exam-aws-certified-solutions-architect-professional-sap-c02/>

D

Option A, B and C are wrong. An AWS Lambda Layer does not support a Docker image or a deployed container as the source.

Create layer

Layer configuration

Name

myLayerName

Description - optional

Description

Upload a .zip file

Upload a file from Amazon S3

 **Upload**

For files larger than 10 MB, consider uploading using Amazon S3.

LAB:

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/#:-text=Lambda%20functions%20packaged%20as%20container,Lambda%20layers%20with%20container%20images.>

HANCHE

Create function Info

Choose one of the following options to create your function.

Author from scratch

Start with a simple Hello World example.

Use a blueprint

Build a Lambda application from sample code and configuration presets for common use cases.

Container image

Select a container image to deploy for your function.

Basic information

Function name

Enter a name that describes the purpose of your function.

container_lambda

Use only letters, numbers, hyphens, or underscores with no spaces.

Container image URI Info

The location of the container image to use for your function.

804920470405.dkr.ecr.ap-southeast-1.amazonaws.com/tienbm-test@sha256:950535

Requires a valid Amazon ECR image URI.

Question 157:

A manufacturing company is building an inspection solution for its factory. The company has IP cameras at the end of each assembly line. The company has used Amazon SageMaker to train a machine learning (ML) model to identify common defects from still images.

The company wants to provide local feedback to factory workers when a defect is detected. The company must be able to provide this feedback even if the factory's internet connectivity is down. The company has a local Linux server that hosts an API that provides local feedback to the workers.

How should the company deploy the ML model to meet these requirements?

- A. Set up an Amazon Kinesis video stream from each IP camera to AWS. Use Amazon EC2 instances to take still images of the streams. Upload the images to an Amazon S3 bucket. Deploy a SageMaker endpoint with the ML model. Invoke an AWS Lambda function to call the inference endpoint when new images are uploaded. Configure the Lambda function to call the local API when a defect is detected.
- B. Deploy AWS IoT Greengrass on the local server. Deploy the ML model to the Greengrass server. Create a Greengrass component to take still images from the cameras and run inference. Configure the component to call the local API when a defect is detected.
- C. Order an AWS Snowball device. Deploy a SageMaker endpoint with the ML model and an Amazon EC2 instance on the Snowball device. Take still images from the cameras. Run inference from the EC2 instance. Configure the instance to call the local API when a defect is detected.
- D. Deploy Amazon Monitron devices on each IP camera. Deploy an Amazon Monitron Gateway on premises. Deploy the ML model to the Amazon Monitron devices. Use Amazon Monitron health state alarms to call the local API from an AWS Lambda function when a defect is detected.

HANCHE

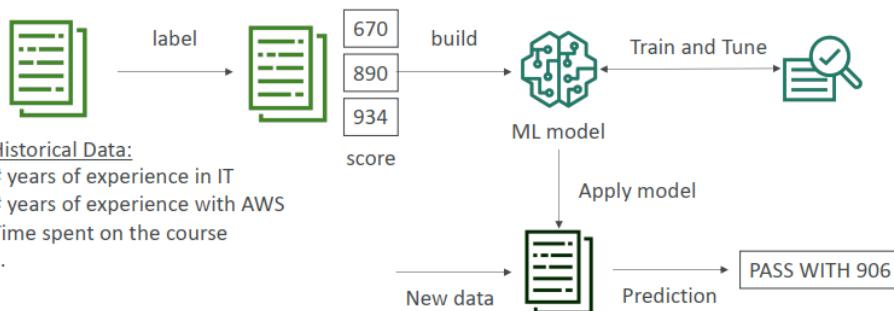
B

Offline operation: AWS IoT Greengrass supports offline operation by enabling devices to continue processing data even when they are disconnected from the internet. AWS IoT Greengrass is software that extends cloud capabilities to local devices. This enables devices to collect and analyze data closer to the source of information, react autonomously to local events, and communicate securely with each other on local networks. Local devices can also communicate securely with AWS IoT Core and export IoT data to the AWS Cloud. AWS IoT Greengrass developers can use AWS Lambda functions and prebuilt connectors to create serverless applications that are deployed to devices for local execution.

Amazon SageMaker



- Fully managed service for developers / data scientists to build ML models
thông thường, khô thực hiện toàn bộ tiến trình trên 1 nơi + provision các server
- Typically, difficult to do all the processes in one place + provision servers
- Machine learning process (simplified): predicting your exam score



AWS IoT Greengrass là một dịch vụ tích hợp của Amazon Web Services (AWS) được thiết kế để hỗ trợ việc triển khai và quản lý các ứng dụng IoT (Internet of Things) phức tạp trên các thiết bị nằm ở Edge (rim hệ thống).

Với AWS IoT Greengrass, bạn có thể triển khai và chạy các ứng dụng IoT trực tiếp trên các thiết bị như gateways, máy tính nhúng và các thiết bị thông minh khác mà không cần phải gửi dữ liệu lên đám mây. Điều này giúp giảm độ trễ, tiết kiệm băng thông và tăng tính linh hoạt trong việc xử lý dữ liệu IoT.

Các tính năng chính của AWS IoT Greengrass bao gồm:

Local compute và messaging: AWS IoT Greengrass cho phép bạn chạy các ứng dụng và xử lý dữ liệu ngay trên các thiết bị Edge, giúp giảm độ trễ và tăng tốc độ phản hồi.

Lambda functions at the Edge: Bạn có thể sử dụng AWS Lambda để triển khai các hàm xử lý dữ liệu tại Edge và xác định các luật và quy tắc để điều khiển thiết bị IoT.

Local data caching: AWS IoT Greengrass cung cấp khả năng lưu trữ và đồng bộ dữ liệu tại Edge, giúp giảm thiểu việc truyền dữ liệu qua mạng và tăng tốc độ truy cập dữ liệu.

Secure connectivity: Dịch vụ này cung cấp các tính năng bảo mật mạnh mẽ như mã hóa dữ liệu, xác thực và quản lý khóa để đảm bảo an toàn cho các ứng dụng và dữ liệu IoT tại Edge.

Remote device management: Bạn có thể quản lý từ xa các thiết bị Greengrass thông qua AWS IoT Core, bao gồm việc cập nhật phần mềm, quản lý quyền hạn và giám sát hoạt động của các thiết bị.

AWS IoT Greengrass giúp đơn giản hóa quá trình triển khai, quản lý và mở rộng các ứng dụng IoT phức tạp tại Edge, mang lại tính linh hoạt và hiệu suất cao cho các hệ thống IoT.

Question 158:

A solutions architect must create a business case for migration of a company's on-premises data center to the AWS Cloud. The solutions architect will use a configuration management database (CMDB) export of all the company's servers to create the case.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Well-Architected Tool to import the CMDB data to perform an analysis and generate recommendations.
- B. Use Migration Evaluator to perform an analysis. Use the data import template to upload the data from the CMDB export.
- C. Implement resource matching rules. Use the CMDB export and the AWS Price List Bulk API to query CMDB data against AWS services in bulk.
- D. Use AWS Application Discovery Service to import the CMDB data to perform an analysis.

B

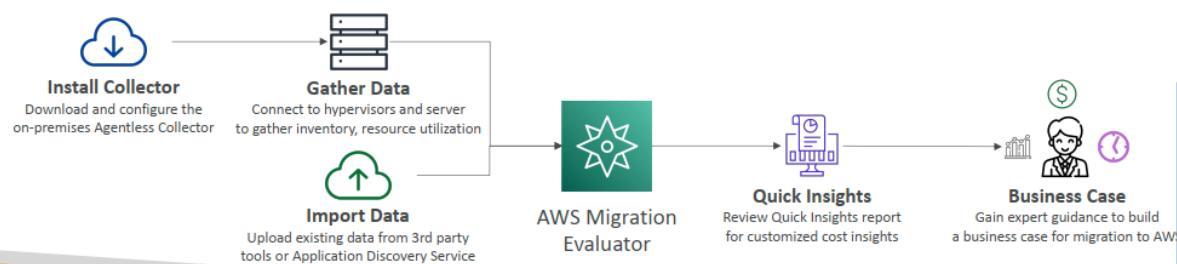
<https://aws.amazon.com/blogs/architecture/accelerating-your-migration-to-aws/>

AWS Migration Evaluator



dựa trên dữ liệu

- Helps you build a data-driven business case for migration to AWS
- Provides a clear baseline of what your organization is running today
- Install Agentless Collector to conduct broad-based discovery
- Take a snapshot of on-premises foot-print, server dependencies, ...
- Analyze current state, define target state, then develop migration plan



Phân tích ứng dụng: Dịch vụ cung cấp khả năng phân tích tự động

các ứng dụng hiện có của bạn, bao gồm danh sách các ứng dụng, đánh giá về cấu trúc, quan hệ và khối lượng dữ liệu. Điều này giúp bạn hiểu rõ hơn về các ứng dụng và sự phụ thuộc của chúng, từ đó đưa ra quyết định về quá trình di chuyển.

Dánh giá khả năng di chuyển: AWS Migration Evaluator giúp bạn đánh giá khả năng di chuyển của các ứng dụng và công việc IT sang AWS. Nó đưa ra các khuyến nghị về việc sử dụng các dịch vụ AWS phù hợp, phân tích khối lượng công việc và tài nguyên cần thiết, và ước tính chi phí dự kiến cho việc di chuyển.

Tối ưu hóa di chuyển: Dịch vụ cung cấp các phân tích và gợi ý để tối ưu hóa quá trình di chuyển. Bạn có thể tìm hiểu về các tùy chọn tối ưu, sử dụng các hướng dẫn và tài liệu để triển khai các phương pháp di chuyển tốt nhất.

Đưa ra kế hoạch di chuyển: AWS Migration Evaluator giúp bạn xây dựng kế hoạch di chuyển chi tiết và tổ chức các công việc di chuyển theo từng giai đoạn. Bạn có thể xác định các công việc, nguồn lực và thời gian cần thiết để thực hiện di chuyển một cách hiệu quả.

Question 159:

A company has a website that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB is associated with an AWS WAF web ACL.

The website often encounters attacks in the application layer. The attacks produce sudden and significant increases in traffic on the application server. The access logs show that each attack originates from different IP addresses. A solutions architect needs to implement a solution to mitigate these attacks.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an Amazon CloudWatch alarm that monitors server access. Set a threshold based on access by IP address. Configure an alarm action that adds the IP address to the web ACL's deny list.
- B. Deploy AWS Shield Advanced in addition to AWS WAF. Add the ALB as a protected resource.
- C. Create an Amazon CloudWatch alarm that monitors user IP addresses. Set a threshold based on access by IP address. Configure the alarm to invoke an AWS Lambda function to add a deny rule in the application server's subnet route table for any IP addresses that activate the alarm.
- D. Inspect access logs to find a pattern of IP addresses that launched the attacks. Use an Amazon Route 53 geolocation routing policy to deny traffic from the countries that host those IP addresses.

B

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-app-layer-protections.html>

This solution offers comprehensive protection with minimal operational overhead. AWS Shield Advanced enhances the capabilities of AWS WAF, providing automated, managed DDoS protection and significantly reducing the need for manual intervention. The integration with AWS WAF allows for seamless mitigation of application layer attacks.

AWS Shield



- AWS Shield Standard:

- Free service that is activated for every AWS customer
- Provides protection from attacks such as SYN/UDP Floods, Reflection attacks and other layer 3/layer 4 attacks

- AWS Shield Advanced:

- Optional DDoS mitigation service ([\\$3,000 per month per organization](#))
- Protect against more [\(adj\): tinh vi sophisticated](#) attack on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, Route 53
- 24/7 access to AWS DDoS response team (DRP)
- Protect against higher fees during usage spikes due to DDoS

bảo vệ khỏi mức phí cao hơn trong thời gian sử dụng tăng đột biến do DDoS

Question 160:

A company has a critical application in which the data tier is deployed in a single AWS Region. The data tier uses an Amazon DynamoDB table and an Amazon Aurora MySQL DB cluster. The current Aurora MySQL engine version supports a global database. The application tier is already deployed in two Regions.

Company policy states that critical applications must have application tier components and data tier components deployed across two Regions. The RTO and RPO must be no more than a few minutes each. A solutions architect must recommend a solution to make the data tier compliant with company policy.

Which combination of steps will meet these requirements? (Choose two.)

- A. Add another Region to the Aurora MySQL DB cluster
- B. Add another Region to each table in the Aurora MySQL DB cluster
- C. Set up scheduled cross-Region backups for the DynamoDB table and the Aurora MySQL DB cluster
- D. Convert the existing DynamoDB table to a global table by adding another Region to its configuration
- E. Use Amazon Route 53 Application Recovery Controller to automate database backup and recovery to the secondary Region.

A, D

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GlobalTables.html>

Global Aurora

- Aurora Cross Region Read Replicas
 - Useful for disaster recovery
 - Simple to put in place
- Aurora Global Database (recommended)
 - 1 Primary Region (read / write)
 - Up to 5 secondary (read-only) regions, replication lag is less than 1 second
 - Up to 16 Read Replicas per secondary region
 - Helps for decreasing latency
 - Promoting another region (for disaster recovery) has an RTO of < 1 minute
 - Ability to manage the RPO in Aurora for PostgreSQL



Amazon DynamoDB global tables are a fully managed, multi-Region, and multi-active database option that delivers fast and localized read and write performance for massively scaled global applications.

Global tables provide a fully managed solution for deploying a multi-Region, multi-active database, without having to build and maintain your own replication solution. You can specify the AWS Regions where you want the tables to be available and DynamoDB will propagate ongoing data changes to all of them.

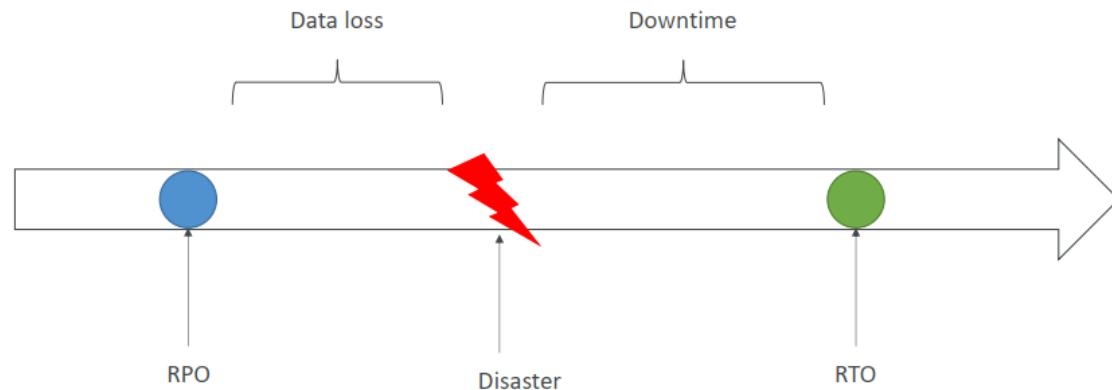
Specific benefits for using global tables include:

- Replicating your DynamoDB tables automatically across your choice of AWS Regions
- Eliminating the difficult work of replicating data between Regions and resolving update conflicts, so you can focus on your application's business logic.
- Helping your applications stay highly available even in the unlikely event of isolation or degradation of an entire Region.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>

- RPO: Recovery Point Objective
- RTO: Recovery Time Objective

RPO and RTO



Question 161:

A telecommunications company is running an application on AWS. The company has set up an AWS Direct Connect connection between the company's on-premises data center and AWS. The company deployed the application on Amazon EC2 instances in multiple Availability Zones behind an internal Application Load Balancer (ALB). The company's clients connect from the on-premises network by using HTTPS. The TLS terminates in the ALB. The company has multiple target groups and uses path-based routing to forward requests based on the URL path.

The company is planning to deploy an on-premises firewall appliance with an allow list that is based on IP address. A solutions architect must develop a solution to allow traffic flow to AWS from the on-premises network so that the clients can continue to access the application.

Which solution will meet these requirements?

- A. Configure the existing ALB to use static IP addresses. Assign IP addresses in multiple Availability Zones to the ALB. Add the ALB IP addresses to the firewall appliance.
- B. Create a Network Load Balancer (NLB). Associate the NLB with one static IP addresses in multiple Availability Zones. Create an ALB-type target group for the NLB and add the existing ALB. Add the NLB IP addresses to the firewall appliance. Update the clients to connect to the NLB.
- C. Create a Network Load Balancer (NLB). Associate the NLB with one static IP addresses in multiple Availability Zones. Add the existing target groups to the NLB. Update the clients to connect to the NLB. Delete the ALB Add the NLB IP addresses to the firewall appliance.
- D. Create a Gateway Load Balancer (GWLB). Assign static IP addresses to the GWLB in multiple Availability Zones. Create an ALB-type target group for the GWLB and add the existing ALB. Add the GWLB IP addresses to the firewall appliance. Update the clients to connect to the GWLB.

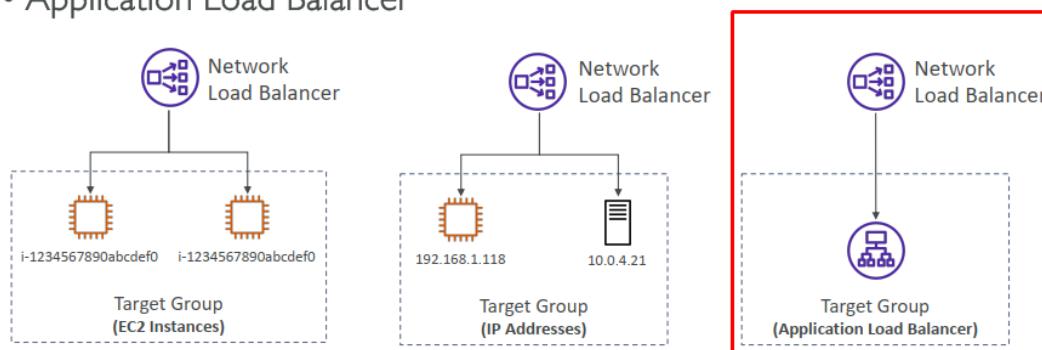
B

You can't assign a static IP address to an Application Load Balancer. If your Application Load Balancer requires a static IP address, then it's a best practice to register it behind a Network Load Balancer. The static IP address that's assigned to a Network Load Balancer doesn't change and provides a fixed entry point for your Application Load Balancer.

Note: The following resolution uses the new launch experience on the Amazon Elastic Compute Cloud (Amazon EC2) console. To complete the steps, toggle on this feature in the Amazon EC2 console.

Network Load Balancer – Target Groups

- EC2 instances
- IP Addresses – must be private IPs
- Application Load Balancer



<https://trello.com/c/7co4KhVb/492-nlb-ft-alb>

Question 162:

A company runs an application on a fleet of Amazon EC2 instances that are in private subnets behind an internet-facing Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. An AWS WAF web ACL that contains various AWS managed rules is associated with the CloudFront distribution.

The company needs a solution that will prevent internet traffic from directly accessing the ALB.

Which solution will meet these requirements with the LEAST operational overhead?

- Create a new web ACL that contains the same rules that the existing web ACL contains. Associate the new web ACL with the ALB.
- Associate the existing web ACL with the ALB.
- Add a security group rule to the ALB to allow traffic from the AWS managed prefix list for CloudFront only.
- Add a security group rule to the ALB to allow only the various CloudFront IP address ranges.

C

LAB:<https://aws.amazon.com/blogs/networking-and-content-delivery/limit-access-to-your-origins-using-the-aws-managed-prefix-list-for-amazon-cloudfront/#:~:text=To%20add%20a%20managed%20prefix,will%20use%20this%20security%20group.&text=You%20can%20find%20the%20Prefix,from%20the%20Amazon%20VPC%20console.>

https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html

If your origin is hosted on Amazon and protected by an Amazon VPC security group, you can use the CloudFront managed prefix list to allow inbound traffic to your origin only from CloudFront's origin-facing servers, preventing any non-CloudFront traffic from reaching your origin , imagine that your origin is an Amazon EC2 instance in the Europe (London) Region (eu-west-2). If the instance is in a VPC, you can create a security group rule that allows inbound HTTPS access from the CloudFront managed prefix list. This allows all of CloudFront's global origin-facing servers to reach the instance. If you remove all other inbound rules from the security group, you prevent any non-CloudFront traffic from reaching the instance

Question 163:

A company is running an application that uses an Amazon ElastiCache for Redis cluster as a caching layer. A recent security audit revealed that the company has configured encryption at rest for ElastiCache. However, the company did not configure ElastiCache to use encryption in transit. Additionally, users can access the cache without authentication.

A solutions architect must make changes to require user authentication and to ensure that the company is using end-to-end encryption.

Which solution will meet these requirements?

- A. Create an AUTH token. Store the token in AWS System Manager Parameter Store, as an encrypted parameter. Create a new cluster with AUTH, and configure encryption in transit. Update the application to retrieve the AUTH token from Parameter Store when necessary and to use the AUTH token for authentication.
- B. Create an AUTH token. Store the token in AWS Secrets Manager. Configure the existing cluster to use the AUTH token, and configure encryption in transit. Update the application to retrieve the AUTH token from Secrets Manager when necessary and to use the AUTH token for authentication.
- C. Create an SSL certificate. Store the certificate in AWS Secrets Manager. Create a new cluster, and configure encryption in transit. Update the application to retrieve the SSL certificate from Secrets Manager when necessary and to use the certificate for authentication.
- D. Create an SSL certificate. Store the certificate in AWS Systems Manager Parameter Store, as an encrypted advanced parameter. Update the existing cluster to configure encryption in transit. Update the application to retrieve the SSL certificate from Parameter Store when necessary and to use the certificate for authentication.

B

App – no encrypt – Redis (encrypt) – DB

Creating an AUTH token provides a form of authentication for accessing the ElastiCache cluster.

Storing the AUTH token in AWS Secrets Manager ensures secure and centralized management of the token.

Configuring the existing ElastiCache cluster to use the AUTH token enables authentication for accessing the cache.

Enabling encryption in transit ensures that data is encrypted when it is transferred between the client and the ElastiCache cluster.

Updating the application to retrieve the AUTH token from Secrets Manager and use it for authentication ensures that only authorized users can access the cache.

Question 164:

A company is running a compute workload by using Amazon EC2 Spot Instances that are in an Auto Scaling group. The launch template uses two placement groups and a single instance type.

Recently, a monitoring system reported Auto Scaling instance launch failures that correlated with longer wait times for system users. The company needs to improve the overall reliability of the workload.

Which solution will meet this requirement?

- A. Replace the launch template with a launch configuration to use an Auto Scaling group that uses attribute-based instance type selection.
- B. Create a new launch template version that uses attribute-based instance type selection. Configure the Auto Scaling group to use the new launch template version.
- C. Update the launch template Auto Scaling group to increase the number of placement groups.
- D. Update the launch template to use a larger instance type.

B

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-mixed-instances-group-attribute-based-instance-type-selection.html#use-attribute-based-instance-type-selection-prerequisites>

With attribute-based instance type selection, instead of providing a list of specific instance types, you provide a list of instance attributes that your instances require, such as:

- vCPU count – The minimum and maximum number of vCPUs per instance.
- Memory – The minimum and maximum GiBs of memory per instance.
- Local storage – Whether to use EBS or instance store volumes for local storage.
- Burstable performance – Whether to use the T instance family, including T4g, T3a, T3, and T2 types.

There are many options available for defining your instance requirements. For a description of each option and the default values, see [InstanceRequirements](#) in the Amazon EC2 Auto Scaling API Reference.

When your Auto Scaling group needs to launch an instance, it will search for instance types that match your specified attributes and are available in that Availability Zone. The allocation strategy then determines which of the matching instance types to launch.

Question 165:

A company is migrating a document processing workload to AWS. The company has updated many applications to natively use the Amazon S3 API to store, retrieve, and modify documents that a processing server generates at a rate of approximately 5 documents every second. After the document processing is finished, customers can download the documents directly from Amazon S3.

During the migration, the company discovered that it could not immediately update the processing server that generates many documents to support the S3 API. The server runs on Linux and requires fast local access to the files that the server generates and modifies. When the server finishes processing, the files must be available to the public for download within 30 minutes.

Which solution will meet these requirements with the LEAST amount of effort?

- A. Migrate the application to an AWS Lambda function. Use the AWS SDK for Java to generate, modify, and access the files that the company stores directly in Amazon S3.
- B. Set up an Amazon S3 File Gateway and configure a file share that is linked to the document store. Mount the file share on an Amazon EC2 instance by using NFS. When changes occur in Amazon S3, initiate a RefreshCache API call to update the S3 File Gateway.
- C. Configure Amazon FSx for Lustre with an import and export policy. Link the new file system to an S3 bucket. Install the Lustre client and mount the document store to an Amazon EC2 instance by using NFS.
- D. Configure AWS DataSync to connect to an Amazon EC2 instance. Configure a task to synchronize the generated files to and from Amazon S3.

B

A = migrating to lambda requires a lot of work and doesn't solve the need to have fast access to files

C = FSx for Lustre doesn't support NFS

D = DataSync can schedule transfer hourly, daily or weekly, cannot meet 30

Amazon S3 File Gateway và FSx Lustre là hai dịch vụ khác nhau trong hệ sinh thái lưu trữ của Amazon Web Services (AWS) và có các ưu điểm và sự khác biệt riêng. Dưới đây là một so sánh giữa Amazon S3 File Gateway và FSx Lustre:

Mục tiêu sử dụng:

Amazon S3 File Gateway: Dịch vụ này được sử dụng để kết nối các ứng dụng và hệ thống tệp tin hiện có của bạn với Amazon S3. Nó cung cấp giao diện tệp tin truyền thông để truy cập và quản lý dữ liệu trên S3.

FSx Lustre: Dịch vụ này cung cấp một hệ thống tệp tin phân tán và hiệu năng cao dựa trên Lustre. FSx Lustre thích hợp cho các ứng dụng tính toán cao và xử lý dữ liệu lớn.

Giao diện truy cập:

Amazon S3 File Gateway: Sử dụng giao diện tệp tin truyền thống như NFS hoặc SMB để truy cập dữ liệu trên Amazon S3.

FSx Lustre: Sử dụng giao diện tệp tin Lustre cho việc truy cập và quản lý dữ liệu trên hệ thống tệp tin Lustre.

Hiệu suất:

Amazon S3 File Gateway: Hiệu suất truy cập dữ liệu trên Amazon S3 phụ thuộc vào hiệu suất của S3 và cấu hình mạng.

FSx Lustre: FSx Lustre cung cấp hiệu suất cao cho các ứng dụng tính toán cao và xử lý dữ liệu lớn. Nó có tốc độ đọc/ghi dữ liệu nhanh và khả năng mở rộng linh hoạt.

Question 166:

A delivery company is running a serverless solution in the AWS Cloud. The solution manages user data, delivery information, and past purchase details. The solution consists of several microservices. The central user service stores sensitive data in an Amazon DynamoDB table. Several of the other microservices store a copy of parts of the sensitive data in different storage services.

The company needs the ability to delete user information upon request. As soon as the central user service deletes a user, every other microservice must also delete its copy of the data immediately.

Which solution will meet these requirements?

- A. Activate DynamoDB Streams on the DynamoDB table. Create an AWS Lambda trigger for the DynamoDB stream that will post events about user deletion in an Amazon Simple Queue Service (Amazon SQS) queue. Configure each microservice to poll the queue and delete the user from the DynamoDB table.
 - B. Set up DynamoDB event notifications on the DynamoDB table. Create an Amazon Simple Notification Service (Amazon SNS) topic as a target for the DynamoDB event notification. Configure each microservice to subscribe to the SNS topic and to delete the user from the DynamoDB table.
 - C. Configure the central user service to post an event on a custom Amazon EventBridge event bus when the company deletes a user. Create an EventBridge rule for each microservice to match the user deletion event pattern and invoke logic in the microservice to delete the user from the DynamoDB table.
 - D. Configure the central user service to post a message on an Amazon Simple Queue Service (Amazon SQS) queue when the company deletes a user. Configure each microservice to create an event filter on the SQS queue and to delete the user from the DynamoDB table.

C

In this case, you can create an EventBridge rule for each microservice to match the user deletion event pattern and invoke the logic in the microservice to delete the corresponding user data from their respective storage services, including the DynamoDB table.

Question 167:

A company is running a web application in a VPC. The web application runs on a group of Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is using AWS WAF.

An external customer needs to connect to the web application. The company must provide IP addresses to all external customers.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Replace the ALB with a Network Load Balancer (NLB). Assign an Elastic IP address to the NLB.
 - B. Allocate an Elastic IP address. Assign the Elastic IP address to the ALB. Provide the Elastic IP address to the customer.
 - C. Create an AWS Global Accelerator standard accelerator. Specify the ALB as the accelerator's endpoint. Provide the accelerator's IP addresses to the customer.
 - D. Configure an Amazon CloudFront distribution. Set the ALB as the origin. Ping the distribution's DNS name to determine the distribution's public IP address. Provide the IP address to the customer.

C

WAF deploy on ALB, API Gateway, CloudFront. → A is incorrect

Can not assign IP address to ALB → B is incorrect

```

graph LR
    Client[Client] --> GA[Global Accelerator]
    GA --> ALB[ALB]
    ALB --> VPC[VPC]
    subgraph IP_Address [IP address]
        ALB
        WAF[WAF]
    end
    VPC --- WAF

```

The diagram illustrates the network architecture. It starts with a 'Client' connected to a 'Global Accelerator'. The 'Global Accelerator' is connected to an 'ALB' (Application Load Balancer). The 'ALB' is connected to a 'VPC' (Virtual Private Cloud). Below the 'ALB' and 'VPC' connection, there is a box labeled 'IP address' containing the 'ALB' and 'WAF' (Web Application Firewall) components. A line connects the 'VPC' to the 'WAF' component.

AWS WAF – Web Application Firewall



AWS Global Accelerator

- Works with Elastic IP, EC2 instances, ALB, NLB, public or private
 - Hỗ trợ bảo quản IP của khách hàng
- Supports Client IP Address Preservation ngoại trừ NLB và EIPs endpoint
- Consistent Performance Hiệu suất nhất quán
 - Intelligent routing to lowest latency and fast regional failover
 - No issue with client cache (because the IP doesn't change)
 - Internal AWS network
- Health Checks
 - Global Accelerator performs a health check of your applications
 - Helps make your application global (failover less than 1 minute for unhealthy)
 - Great for disaster recovery (thanks to the health checks)
- Security
 - only 2 external IP need to be whitelisted
 - DDoS protection thanks to AWS Shield

- Protects your web applications from common web exploits (Layer 7)
- Deploy on **Application Load Balancer** (localized rules)
- Deploy on **API Gateway** (rules running at the regional or edge level)
- Deploy on **CloudFront** (rules globally on edge locations)
 - Used to front other solutions: CLB, EC2 instances, custom origins, S3 websites
- Deploy on AppSync (protect your GraphQL APIs)
- WAF is not for DDoS protection
- Define Web ACL (Web Access Control List):
 - Rules can include **IP addresses**, HTTP headers, HTTP body, or URI strings
 - Protects from common attack - **SQL injection** and Cross-Site Scripting (XSS)
 - Size constraints, Geo match
 - Rate-based rules (to count occurrences of events)
- Rule Actions: Count | Allow | Block | CAPTCHA

Question 168:

A company has a few AWS accounts for development and wants to move its production application to AWS. The company needs to enforce Amazon Elastic Block Store (Amazon EBS) encryption at rest current production accounts and future production accounts only. The company needs a solution that includes built-in blueprints and guardrails.

Which combination of steps will meet these requirements? (Choose three.)

- Use AWS CloudFormation StackSets to deploy AWS Config rules on production accounts.
- Create a new AWS Control Tower landing zone in an existing developer account. Create OUs for accounts. Add production and development accounts to production and development OUs, respectively.
- Create a new AWS Control Tower landing zone in the company's management account. Add production and development accounts to production and development OUs, respectively.
- Invite existing accounts to join the organization in AWS Organizations. Create SCPs to ensure compliance.
- Create a guardrail from the management account to detect EBS encryption.
- Create a guardrail for the production OU to detect EBS encryption.

C,D,F

<https://docs.aws.amazon.com/controlltower/latest/controlreference/controls.html>

AWS Control Tower



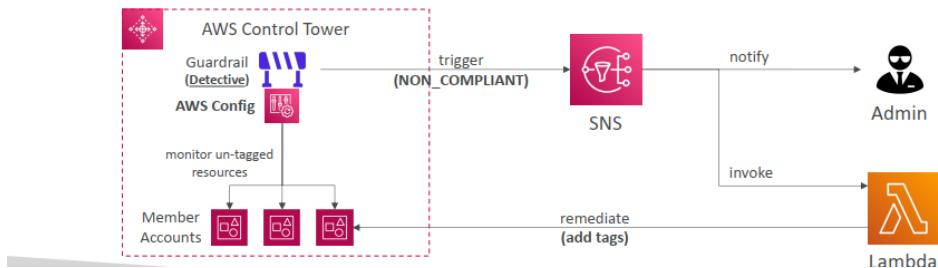
- Easy way to set up and govern a secure and compliant multi-account AWS environment based on best practices
- Benefits:
 - Automate the set up of your environment in a few clicks
 - Automate ongoing policy management using guardrails
 - Detect policy violations and remediate them
 - Monitor compliance through an interactive dashboard
- AWS Control Tower runs on top of AWS Organizations:
 - It automatically sets up AWS Organizations to organize accounts and implement SCPs (Service Control Policies)

AWS Control Tower – Detect and Remediate Policy Violations

• Guardrail

(adj): tiếp tục, tiếp diễn

- Provides ongoing governance for your Control Tower environment (AWS Accounts)
- Preventive – using SCPs (e.g., Disallow Creation of Access Keys for the Root User)
- Detective – using AWS Config (e.g., Detect Whether MFA for the Root User is Enabled)
- Example: identify non-compliant resources (e.g., untagged resources)



A control is a high-level rule that provides ongoing governance for your overall AWS environment. It's expressed in plain language. AWS Control Tower implements preventive, detective, and proactive controls that help you govern your resources and monitor compliance across groups of AWS accounts.

A control applies to an entire organizational unit (OU), and every AWS account within the OU is affected by the control. Therefore, when users perform work in any AWS account in your landing zone, they're always subject to the controls that are governing their account's OU.

Question 169:

A company is running a critical stateful web application on two Linux Amazon EC2 instances behind an Application Load Balancer (ALB) with an Amazon RDS for MySQL database. The company hosts the DNS records for the application in Amazon Route 53. A solutions architect must recommend a solution to improve the resiliency of the application.

The solution must meet the following objectives:

- Application tier: RPO of 2 minutes. RTO of 30 minutes
- Database tier: RPO of 5 minutes. RTO of 30 minutes

The company does not want to make significant changes to the existing application architecture. The company must ensure optimal latency after a failover.

Which solution will meet these requirements?

- A. Configure the EC2 instances to use AWS Elastic Disaster Recovery. Create a cross-Region read replica for the RDS DB instance. Create an ALB in a second AWS Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs. Update DNS records to point to the Global Accelerator endpoint.

B. Configure the EC2 instances to use Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes. Configure RDS automated backups. Configure backup replication to a second AWS Region. Create an ALB in the second Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs. Update DNS records to point to the Global Accelerator endpoint.

C. Create a backup plan in AWS Backup for the EC2 instances and RDS DB instance. Configure backup replication to a second AWS Region. Create an ALB in the second Region. Configure an Amazon CloudFront distribution in front of the ALB. Update DNS records to point to CloudFront.

D. Configure the EC2 instances to use Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes. Create a cross-Region read replica for the RDS DB instance. Create an ALB in a second AWS Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs.

A

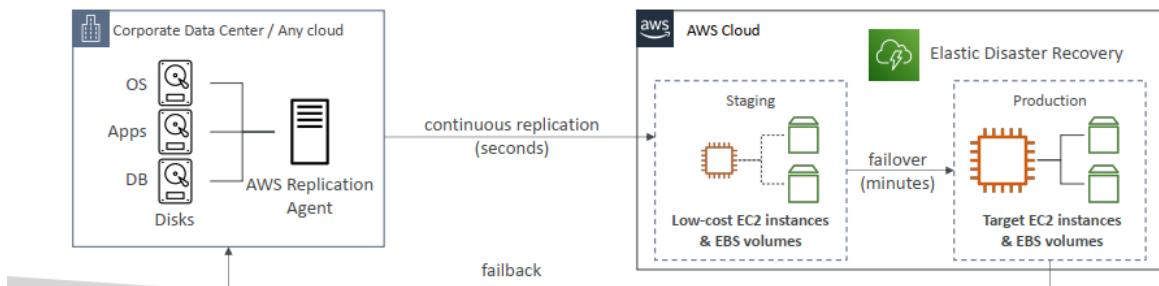
AWS Global Accelerator

- Works with Elastic IP, EC2 instances, ALB, NLB, public or private
 - Hỗ trợ bảo quản IP của khách hàng
- Supports Client IP Address Preservation người truy cập NLB và EIPs endpoint except for NLBs and EIPs endpoints
- Consistent Performance Hiệu suất nhất quán
 - Intelligent routing to lowest latency and fast regional failover
 - No issue with client cache (because the IP doesn't change)
 - Internal AWS network
- Health Checks
 - Global Accelerator performs a health check of your applications
 - Helps make your application global (failover less than 1 minute for unhealthy)
 - Great for disaster recovery (thanks to the health checks)
- Security
 - only 2 external IP need to be whitelisted
 - DDoS protection thanks to AWS Shield

AWS Elastic Disaster Recovery (DRS)



- Used to be named "CloudEndure Disaster Recovery"
- Quickly and easily recover your physical, virtual, and cloud-based servers into AWS
- Example: protect your most critical databases (including Oracle, MySQL, and SQL Server), enterprise apps (SAP), protect your data from ransomware attacks, ...
- Continuous block-level replication for your servers



Question 170:

A solutions architect wants to cost-optimize and appropriately size Amazon EC2 instances in a single AWS account. The solutions architect wants to ensure that the instances are optimized based on CPU, memory, and network metrics.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

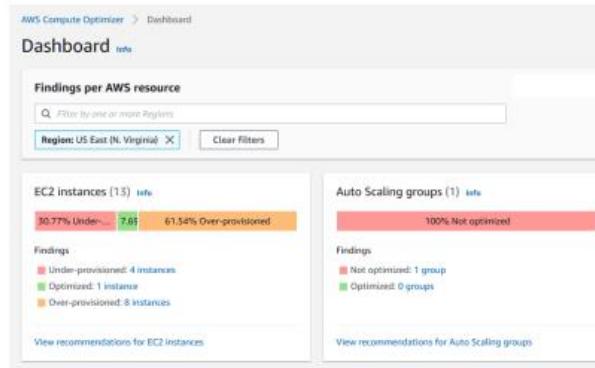
- Purchase AWS Business Support or AWS Enterprise Support for the account.
- Turn on AWS Trusted Advisor and review any "Low Utilization Amazon EC2 Instances" recommendations.
- Install the Amazon CloudWatch agent and configure memory metric collection on the EC2 instances.
- Configure AWS Compute Optimizer in the AWS account to receive findings and optimization recommendations.
- Create an EC2 Instance Savings Plan for the AWS Regions, instance families, and operating systems of interest.

C,D

AWS Compute Optimizer



- Reduce costs and improve performance by recommending optimal AWS resources for your workloads
- Helps you choose optimal configurations and right-size your workloads (over/under provisioned)
- Uses Machine Learning to analyze your resources' configurations and their utilization CloudWatch metrics
- Supported resources
 - EC2 instances
 - EC2 Auto Scaling Groups
 - EBS volumes
 - Lambda functions
- Lower your costs by up to 25%
- Recommendations can be exported to S3



Trusted Advisor



- No need to install anything – high level AWS account assessment
- Analyze your AWS accounts and provides recommendation:
 - Cost Optimization & Recommendations
 - Performance
 - Security
 - Fault Tolerance
 - Service Limits
- Core Checks and recommendations – all customers
- Can enable weekly email notification from the console
- Full Trusted Advisor – Available for Business & Enterprise support plans
 - Ability to set CloudWatch alarms when reaching limits
 - Programmatic Access using AWS Support API

<https://trello.com/c/DR687m6D/494-aws-compute-optimizer-vs-trust-advisor>

Question 171:

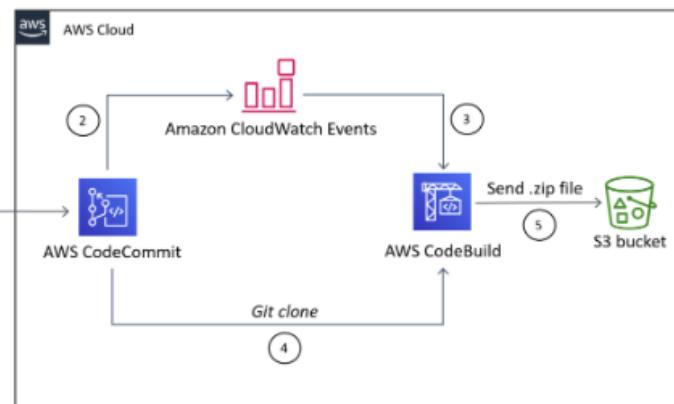
A company uses an AWS CodeCommit repository. The company must store a backup copy of the data that is in the repository in a second AWS Region.

Which solution will meet these requirements?

- A. Configure AWS Elastic Disaster Recovery to replicate the CodeCommit repository data to the second Region.
- B. Use AWS Backup to back up the CodeCommit repository on an hourly schedule. Create a cross-Region copy in the second Region.
- C. Create an Amazon EventBridge rule to invoke AWS CodeBuild when the company pushes code to the repository. Use CodeBuild to clone the repository. Create a .zip file of the content. Copy the file to an S3 bucket in the second Region.
- D. Create an AWS Step Functions workflow on an hourly schedule to take a snapshot of the CodeCommit repository. Configure the workflow to copy the snapshot to an S3 bucket in the second Region,

C

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-event-driven-backups-from-codecommit-to-amazon-s3-using-codebuild-and-cloudwatch-events.html>



Question 172:

A company has multiple business units that each have separate accounts on AWS. Each business unit manages its own network with several VPCs that have CIDR ranges that overlap. The company's marketing team has created a new internal application and wants to make the application accessible to all the other business units. The solution must use private IP addresses only.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Instruct each business unit to add a unique secondary CIDR range to the business unit's VPC. Peer the VPCs and use a private NAT gateway in the secondary range to route traffic to the marketing team.
- B. Create an Amazon EC2 instance to serve as a virtual appliance in the marketing account's VPC. Create an AWS Site-to-Site VPN connection between the marketing team and each business unit's VPC. Perform NAT where necessary.
- C. Create an AWS PrivateLink endpoint service to share the marketing application. Grant permission to specific AWS accounts to connect to the service. Create interface VPC endpoints in other accounts to access the application by using private IP addresses.
- D. Create a Network Load Balancer (NLB) in front of the marketing application in a private subnet. Create an API Gateway API. Use the Amazon API Gateway private integration to connect the API to the NLB. Activate IAM authorization for the API. Grant access to the accounts of the other business units.

C

The solution must use private IP addresses only → private network → VPC endpoint interface

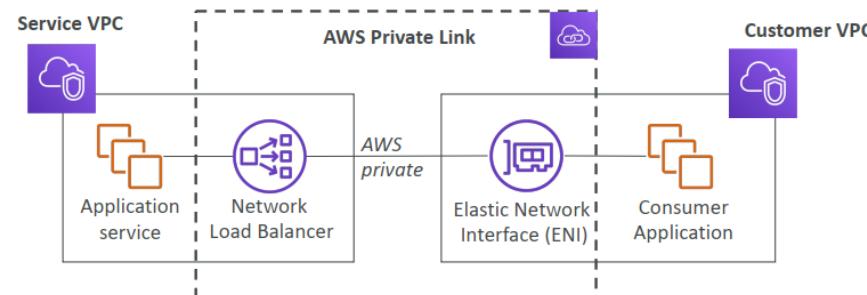
Private link is the solution for IP Overlapping and Securely access the app between accounts.

AWS PrivateLink provides secure and scalable private connectivity between VPCs, AWS services, and on-premises applications, without using public IP addresses. In this case, you can create an AWS PrivateLink endpoint service for the marketing application, which allows other business units to access the application using private IP addresses. By granting permission to specific AWS accounts to connect to the PrivateLink endpoint service, you can control access to the marketing application. Then, in each business unit's VPC, you can create interface VPC endpoints to connect to the PrivateLink service, allowing them to access the marketing application privately.

AWS PrivateLink (VPC Endpoint Services)

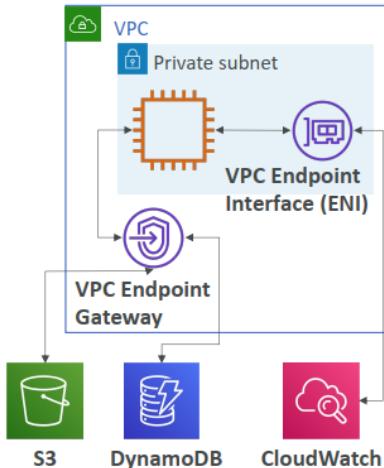


- Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts)
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)
- If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!



VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables



Question 173:

A company needs to audit the security posture of a newly acquired AWS account. The company's data security team requires a notification only when an Amazon S3 bucket becomes publicly exposed. The company has already established an Amazon Simple Notification Service (Amazon SNS) topic that has the data security team's email address subscribed.

Which solution will meet these requirements?

- Create an S3 event notification on all S3 buckets for the `isPublic` event. Select the SNS topic as the target for the event notifications.
- Create an analyzer in AWS Identity and Access Management Access Analyzer. Create an Amazon EventBridge rule for the event type "Access Analyzer Finding" with a filter for "`isPublic: true`." Select the SNS topic as the EventBridge rule target.
- Create an Amazon EventBridge rule for the event type "Bucket-Level API Call via CloudTrail" with a filter for "`PutBucketPolicy`." Select the SNS topic as the EventBridge rule target.
- Activate AWS Config and add the `cloudtrail-s3-dataevents-enabled` rule. Create an Amazon EventBridge rule for the event type "Config Rules Re-evaluation Status" with a filter for "`NON_COMPLIANT`." Select the SNS topic as the EventBridge rule target.

B

A. No, because Amazon S3 can NOT currently publish notifications for `isPublic` events. [Amazon S3 Event Notifications](https://docs.aws.amazon.com/AmazonS3/latest/userguide/EventNotifications.html)
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/EventNotifications.html>

B. Yes, because IAM Access Analyzer for S3 alerts you to S3 buckets that are configured to allow access to anyone on the internet or other AWS accounts. How to prioritize IAM Access Analyzer findings
<https://aws.amazon.com/blogs/security/how-to-prioritize-iam-access-analyzer-findings/>

- C. No, because PutBucketPolicy notifies us of an Amazon S3 bucket policy event to an Amazon S3 bucket, and we are looking for a SPECIFIC event to the bucket permissions, not ALL events.
- D. No, because cloudtrail-s3-dataevents-enabled checks if at least one AWS CloudTrail trail is logging Amazon Simple Storage Service (Amazon S3) data events for all S3 buckets. cloudtrail-s3-dataevents-enabled
<https://docs.aws.amazon.com/config/latest/developerguide/cloudtrail-s3-dataevents-enabled.html>

Question 174:

A solutions architect needs to assess a newly acquired company's portfolio of applications and databases. The solutions architect must create a business case to migrate the portfolio to AWS. The newly acquired company runs applications in an on-premises data center. The data center is not well documented. The solutions architect cannot immediately determine how many applications and databases exist. Traffic for the applications is variable. Some applications are batch processes that run at the end of each month.

The solutions architect must gain a better understanding of the portfolio before a migration to AWS can begin.

Which solution will meet these requirements?

- A. Use AWS Server Migration Service (AWS SMS) and AWS Database Migration Service (AWS DMS) to evaluate migration. Use AWS Service Catalog to understand application and database dependencies.
- B. Use AWS Application Migration Service. Run agents on the on-premises infrastructure. Manage the agents by using AWS Migration Hub. Use AWS Storage Gateway to assess local storage needs and database dependencies.
- C. Use Migration Evaluator to generate a list of servers. Build a report for a business case. Use AWS Migration Hub to view the portfolio. Use AWS Application Discovery Service to gain an understanding of application dependencies.
- D. Use AWS Control Tower in the destination account to generate an application portfolio. Use AWS Server Migration Service (AWS SMS) to generate deeper reports and a business case. Use a landing zone for core accounts and resources.

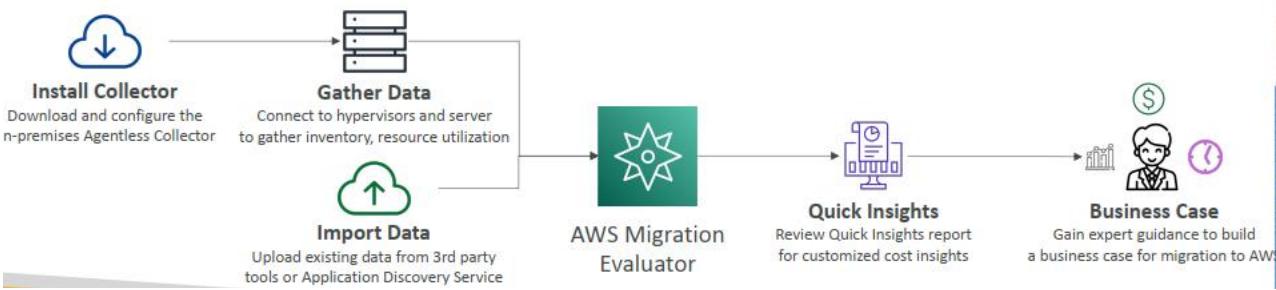
- C
create a business case to migrate the portfolio to AWS ➔ Migration Evaluator

AWS Migration Evaluator



dựa trên dữ liệu

- Helps you build a data-driven business case for migration to AWS
- Provides a clear baseline of what your organization is running today
- Install Agentless Collector to conduct broad-based discovery
- Take a snapshot of on-premises foot-print, server dependencies, ...
- Analyze current state, define target state, then develop migration plan



AWS Application Discovery Service

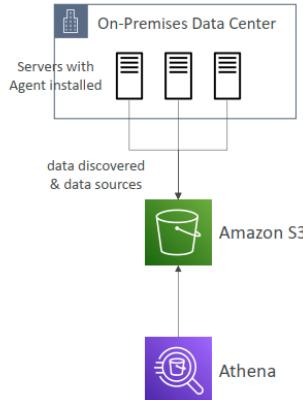


- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping are important for migrations
- **Agentless Discovery (AWS Agentless Discovery Connector)**
 - Open Virtual Appliance (OVA) package that can be deployed to a VMware host
 - VM inventory, configuration, and performance history such as CPU, memory, and disk usage
 - OS agnostic
- **Agent-based Discovery (AWS Application Discovery Agent)**
 - System configuration, system performance, running processes, and details of the network connections between systems
 - Supports Microsoft Server, Amazon Linux, Ubuntu, RedHat, CentOS, SUSE...
- Resulting data can be exported as CSV or viewed within AWS Migration Hub
- Data can be explored using pre-defined queries in Amazon Athena

AWS Application Discovery Service – Migration Hub Data Exploration



- Allows you to use Amazon Athena to analyze data collected from on-premises servers during discovery
- Data is automatically stored in S3 bucket at regular intervals
- Use Pre-defined or custom queries in Amazon Athena to analyze data
- Example: type of processes running on each server
- Ability to upload additional data sources such as Configuration Management Database (CMDB) exports
- Integrate Athena with QuickSight to visualize data



Question 175:

A company has an application that runs as a ReplicaSet of multiple pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster has nodes in multiple Availability Zones. The application generates many small files that must be accessible across all running instances of the application. The company needs to back up the files and retain the backups for 1 year.

Which solution will meet these requirements while providing the FASTEST storage performance?

- Create an Amazon Elastic File System (Amazon EFS) file system and a mount target for each subnet that contains nodes in the EKS cluster. Configure the ReplicaSet to mount the file system. Direct the application to store files in the file system. Configure AWS Backup to back up and retain copies of the data for 1 year.
- Create an Amazon Elastic Block Store (Amazon EBS) volume. Enable the EBS Multi-Attach feature. Configure the ReplicaSet to mount the EBS volume. Direct the application to store files in the EBS volume. Configure AWS Backup to back up and retain copies of the data for 1 year.
- Create an Amazon S3 bucket. Configure the ReplicaSet to mount the S3 bucket. Direct the application to store files in the S3 bucket. Configure S3 Versioning to retain copies of the data. Configure an S3 Lifecycle policy to delete objects after 1 year.
- Configure the ReplicaSet to use the storage available on each of the running application pods to store the files locally. Use a third-party tool to back up the EKS cluster for 1 year.

A

Amazon EFS provides shared file storage that is highly available and durable. It is an ideal solution to share files between containers running on multiple instances in a cluster. Mounting an Amazon EFS file system on each subnet provides a shared file system for multiple instances running in different Availability Zones. Additionally, AWS Backup provides automated backup and recovery of Amazon EFS file systems.

<https://www.msp360.com/resources/blog/amazon-s3-vs-ebs-vs-efs/>

Amazon S3 vs EFS vs EBS Comparison

In summary, we distinguished a few specific features of all three storage services to help you choose between them:

AMAZON S3	AMAZON EBS	AMAZON EFS
Can be publicly accessible	Accessible only via the given EC2 Machine	Accessible via several EC2 machines and AWS services
Web interface	File System interface	Web and file system interface
Object Storage	Block Storage	Object storage
Scalable	Hardly scalable	Scalable
Slower than EBS and EFS	Faster than S3 and EFS	Faster than S3, slower than EBS
Good for storing backups and other static data	Is meant to be EC2 drive	Good for applications and shareable workloads

Question 176:

A company runs a customer service center that accepts calls and automatically sends all customers a managed, interactive, two-way experience survey by text message. The applications that support the customer service center run on machines that the company hosts in an on-premises data center. The hardware that the company uses is old, and the company is experiencing downtime with the system. The company wants to migrate the system to AWS to improve reliability.

Which solution will meet these requirements with the LEAST ongoing operational overhead?

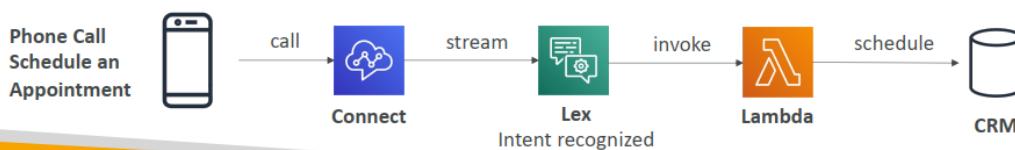
- A. Use Amazon Connect to replace the old call center hardware. Use Amazon Pinpoint to send text message surveys to customers.
- B. Use Amazon Connect to replace the old call center hardware. Use Amazon Simple Notification Service (Amazon SNS) to send text message surveys to customers.
- C. Migrate the call center software to Amazon EC2 instances that are in an Auto Scaling group. Use the EC2 instances to send text message surveys to customers.
- D. Use Amazon Pinpoint to replace the old call center hardware and to send text message surveys to customers.

A

Amazon Connect is a cloud-based contact center service that allows you to set up a virtual call center for your business. It provides an easy-to-use interface for managing customer interactions through voice and chat. Amazon Connect integrates with other AWS services, such as Amazon S3 and Amazon Kinesis, to help you collect, store, and analyze customer data for insights into customer behavior and trends. On the other hand, Amazon Pinpoint is a marketing automation and analytics service that allows you to engage with your customers across different channels, such as email, SMS, push notifications, and voice. It helps you create personalized campaigns based on user behavior and enables you to track user engagement and retention. While both services allow you to communicate with your customers, they serve different purposes. Amazon Connect is focused on customer support and service, while Amazon Pinpoint is focused on marketing and engagement.

Amazon Lex & Connect

- **Amazon Lex:** (same technology that powers Alexa)
 - Automatic Speech Recognition (ASR) to convert speech to text
 - Natural Language Understanding to recognize the intent of text, callers
 - Helps build chatbots, call center bots
- **Amazon Connect:**
 - Receive calls, create contact flows, cloud-based virtual contact center
 - Can integrate with other CRM systems or AWS
 - No upfront payments, 80% cheaper than traditional contact center solutions



Question 177:

A company is building a call center by using Amazon Connect. The company's operations team is defining a disaster recovery (DR) strategy across AWS Regions. The contact center has dozens of contact flows, hundreds of users, and dozens of claimed phone numbers.

Which solution will provide DR with the LOWEST RTO?

- A. Create an AWS Lambda function to check the availability of the Amazon Connect instance and to send a notification to the operations team in case of unavailability. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. After notification, instruct the operations team to use the AWS Management Console to provision a new Amazon Connect instance in a second Region. Deploy the contact flows, users, and claimed phone numbers by using an AWS CloudFormation template.
- B. Provision a new Amazon Connect instance with all existing users in a second Region. Create an AWS Lambda function to check the availability of the Amazon Connect instance. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. In the event of an issue, configure the Lambda function to deploy an AWS CloudFormation template that provisions contact flows and claimed numbers in the second Region.

C. Provision a new Amazon Connect instance with all existing contact flows and claimed phone numbers in a second Region. Create an Amazon Route 53 health check for the URL of the Amazon Connect instance. Create an Amazon CloudWatch alarm for failed health checks. Create an AWS Lambda function to deploy an AWS CloudFormation template that provisions all users. Configure the alarm to invoke the Lambda function.

D. Provision a new Amazon Connect instance with all existing users and contact flows in a second Region. Create an Amazon Route 53 health check for the URL of the Amazon Connect instance. Create an Amazon CloudWatch alarm for failed health checks. Create an AWS Lambda function to deploy an AWS CloudFormation template that provisions claimed phone numbers. Configure the alarm to invoke the Lambda function.

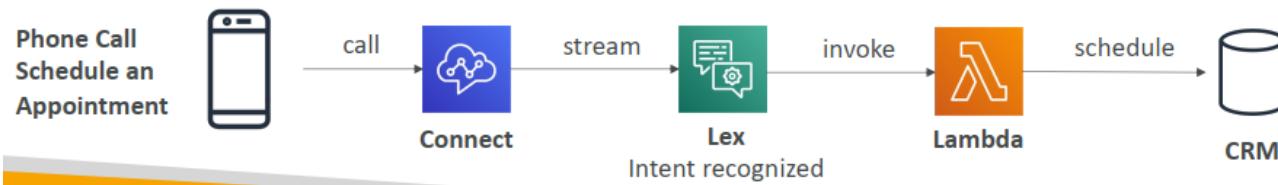
D

a disaster recovery (DR) strategy across AWS Regions → second Region, Route 53 healthcheck

Option D provisions a new Amazon Connect instance with all existing users and contact flows in a second Region. It also sets up an Amazon Route 53 health check for the URL of the Amazon Connect instance, an Amazon CloudWatch alarm for failed health checks, and an AWS Lambda function to deploy an AWS CloudFormation template that provisions claimed phone numbers. This option allows for the fastest recovery time because all the necessary components are already provisioned and ready to go in the second Region. In the event of a disaster, the failed health check will trigger the AWS Lambda function to deploy the CloudFormation template to provision the claimed phone numbers, which is the only missing component.

Amazon Lex & Connect

- **Amazon Lex:** (same technology that powers Alexa)
 - Automatic Speech Recognition (ASR) to convert speech to text
 - Natural Language Understanding to recognize the intent of text, callers
 - Helps build chatbots, call center bots
- **Amazon Connect:**
 - Receive calls, create contact flows, cloud-based virtual contact center
 - Can integrate with other CRM systems or AWS
 - No upfront payments, 80% cheaper than traditional contact center solutions



Question 178:

A company runs an application on AWS. The company curates data from several different sources. The company uses proprietary algorithms to perform data transformations and aggregations. After the company performs ETL processes, the company stores the results in Amazon Redshift tables. The company sells this data to other companies. The company downloads the data as files from the Amazon Redshift tables and transmits the files to several data customers by using FTP. The number of data customers has grown significantly. Management of the data customers has become difficult.

The company will use AWS Data Exchange to create a data product that the company can use to share data with customers. The company wants to confirm the identities of the customers before the company shares data. The customers also need access to the most recent data when the company publishes the data.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Data Exchange for APIs to share data with customers. Configure subscription verification. In the AWS account of the company that produces the data, create an Amazon API Gateway Data API service integration with Amazon Redshift. Require the data customers to subscribe to the data product.
- B. In the AWS account of the company that produces the data, create an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster. Configure subscription verification. Require the data customers to subscribe to the data product.
- C. Download the data from the Amazon Redshift tables to an Amazon S3 bucket periodically. Use AWS Data Exchange for S3 to share data with customers. Configure subscription verification. Require the data customers to subscribe to the data product.
- D. Publish the Amazon Redshift data to an Open Data on AWS Data Exchange. Require the customers to subscribe to the data product in AWS Data Exchange. In the AWS account of the company that produces the data, attach IAM resource-based policies to the Amazon Redshift tables to allow access only to verified AWS accounts.

B

When creating AWS Data Exchange datashares and adding them to an AWS Data Exchange product, providers can license data in Amazon Redshift that consumers can discover, subscribe to, and query up-to-date data in Amazon Redshift when they have active AWS Data Exchange subscriptions.

With AWS Data Exchange datashares added to an AWS Data Exchange product, consumers automatically have access to a product's datashares when their subscription starts and retain their access as long as their subscription is active.



Efficient data queries

Customers can find and subscribe to third-party data in AWS Data Exchange and directly query the data in minutes in Amazon Redshift without extracting, transforming, or loading it.



Simple management of data licensing

Customers can easily license third-party data in Amazon Redshift through AWS Data Exchange. Access is automatically granted when a customer subscribes and automatically revoked when a subscription ends.



Streamlined data procurement

Customers can use the data as soon as its published. Meanwhile, invoices are automatically generated, and payments are automatically collected and disbursed through AWS.

Option (A) uses AWS Data Exchange for APIs, which requires you to create an Amazon API Gateway Data API service integration with Amazon Redshift. This is a more complex solution than using a datashare.

Option (C) uses AWS Data Exchange for S3, which requires you to download the data from Amazon Redshift to Amazon S3 periodically. This is also a more complex solution than using a datashare.

Option (D) publishes the data to an Open Data on AWS Data Exchange, which does not allow you to configure subscription verification. This means that anyone can access the data, which is not ideal for a company that wants to protect its proprietary algorithms.

Question 179:

A solutions architect is designing a solution to process events. The solution must have the ability to scale in and out based on the number of events that the solution receives. If a processing error occurs, the event must move into a separate queue for review.

Which solution will meet these requirements?

- A. Send event details to an Amazon Simple Notification Service (Amazon SNS) topic. Configure an AWS Lambda function as a subscriber to the SNS topic to process the events. Add an on-failure destination to the function. Set an Amazon Simple Queue Service (Amazon SQS) queue as the target.
- B. Publish events to an Amazon Simple Queue Service (Amazon SQS) queue. Create an Amazon EC2 Auto Scaling group. Configure the Auto Scaling group to scale in and out based on the ApproximateAgeOfOldestMessage metric of the queue. Configure the application to write failed messages to a dead-letter queue.
- C. Write events to an Amazon DynamoDB table. Configure a DynamoDB stream for the table. Configure the stream to invoke an AWS Lambda function. Configure the Lambda function to process the events.
- D. Publish events to an Amazon EventBridge event bus. Create and run an application on an Amazon EC2 instance with an Auto Scaling group that is behind an Application Load Balancer (ALB). Set the ALB as the event bus target. Configure the event bus to retry events. Write messages to a dead-letter queue if the application cannot process the messages.

B

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

publishing events to an SQS queue, creating an EC2 Auto Scaling group that scales based on the queue's ApproximateAgeOfOldestMessage metric, and configuring the application to write failed messages to a dead-letter queue provides a scalable, fault-tolerant, and cost-effective solution for event processing with the ability to handle processing errors separately.

Question 180:

A company runs a processing engine in the AWS Cloud. The engine processes environmental data from logistics centers to calculate a sustainability index. The company has millions of devices in logistics centers that are spread across Europe. The devices send information to the processing engine through a RESTful API.

The API experiences unpredictable bursts of traffic. The company must implement a solution to process all data that the devices send to the processing engine. Data loss is unacceptable.

Which solution will meet these requirements?

- A. Create an Application Load Balancer (ALB) for the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create a listener and a target group for the ALB. Add the SQS queue as the target. Use a container that runs in Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to process messages in the queue.

B. Create an Amazon API Gateway HTTP API that implements the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create an API Gateway service integration with the SQS queue. Create an AWS Lambda function to process messages in the SQS queue.

C. Create an Amazon API Gateway REST API that implements the RESTful API. Create a fleet of Amazon EC2 instances in an Auto Scaling group. Create an API Gateway Auto Scaling group proxy integration. Use the EC2 instances to process incoming data.

D. Create an Amazon CloudFront distribution for the RESTful API. Create a data stream in Amazon Kinesis Data Streams. Set the data stream as the origin for the distribution. Create an AWS Lambda function to consume and process data in the data stream.

B

Data loss is unacceptable. → Amazon SQS

The devices send information to the processing engine through a RESTful API → Amazon API Gateway HTTP API that implements the RESTful API

Option A is incorrect because Application Load Balancer (ALB) can't directly target an Amazon SQS queue.

Option C is incorrect because while Amazon API Gateway and EC2 Auto Scaling can handle high loads, they don't provide a built-in mechanism to ensure that all messages are processed without loss.

Option D is incorrect because Amazon CloudFront is a content delivery network (CDN), and it is not typically used to handle incoming API requests. It is primarily used to cache and deliver content to users.

Question 181:

A company is designing its network configuration in the AWS Cloud. The company uses AWS Organizations to manage a multi-account setup. The company has three OUs. Each OU contains more than 100 AWS accounts. Each account has a single VPC, and all the VPCs in each OU are in the same AWS Region.

The CIDR ranges for all the AWS accounts do not overlap. The company needs to implement a solution in which VPCs in the same OU can communicate with each other but cannot communicate with VPCs in other OUs.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS CloudFormation stack set that establishes VPC peering between accounts in each OU. Provision the stack set in each OU.

B. In each OU, create a dedicated networking account that has a single VPC. Share this VPC with all the other accounts in the OU by using AWS Resource Access Manager (AWS RAM). Create a VPC peering connection between the networking account and each account in the OU.

C. Provision a transit gateway in an account in each OU. Share the transit gateway across the organization by using AWS Resource Access Manager (AWS RAM). Create transit gateway VPC attachments for each VPC.

D. In each OU, create a dedicated networking account that has a single VPC. Establish a VPN connection between the networking account and the other accounts in the OU. Use third-party routing software to route transitive traffic between the VPCs.

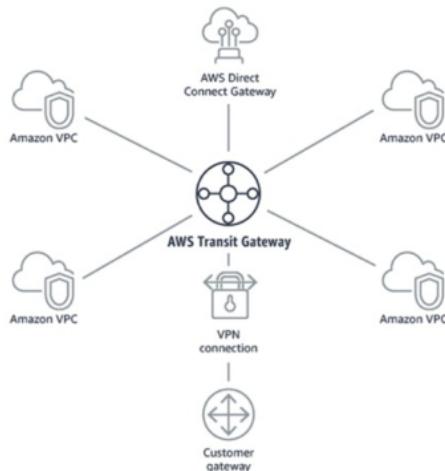
C

needs to implement a solution in which VPCs in the same OU can communicate with each other + LEAST operational overhead → Transit Gateway

Transit Gateway

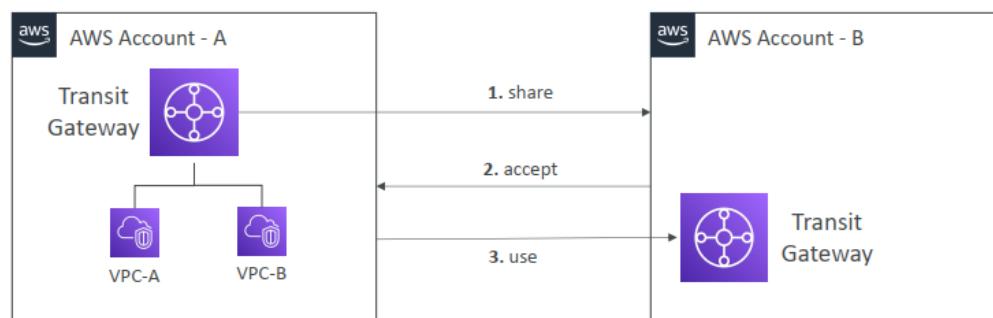


- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager (RAM)
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with other VPC
- Works with Direct Connect Gateway, VPN connections
- Supports IP Multicast (not supported by any other AWS service)
- Instances in a VPC can access a NAT Gateway, NLB, PrivateLink, and EFS in other VPCs attached to the AWS Transit Gateway.



Transit Gateway – Sharing through RAM

- You can use AWS RAM to share a Transit Gateway for VPC attachments across accounts or across AWS Organization



Question 182:

A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large important documents within the application with the following requirements:

- The data must be highly durable and available
- The data must always be encrypted at rest and in transit
- The encryption key must be managed by the company and rotated periodically

Which of the following solutions should the solutions architect recommend?

- A. Deploy the storage gateway to AWS in file gateway mode. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.
- B. Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.
- C. Use Amazon DynamoDB with SSL to connect to DynamoDB. Use an AWS KMS key to encrypt DynamoDB objects at rest.
- D. Deploy instances with Amazon EBS volumes attached to store this data. Use EBS volume encryption using an AWS KMS key to encrypt the data.

B

The data must always be encrypted at rest and in transit => HTTPS
store large important documents → store in S3

AWS KMS (Key Management Service)



- Anytime you hear “**encryption**” for an AWS service, it’s most likely **KMS**
- Easy way to control access to your data, AWS manages keys for us
- Fully integrated with IAM for authorization
- Seamlessly integrated into:
 - Amazon EBS: encrypt volumes
 - Amazon S3: Server-side encryption of objects
 - Amazon Redshift: encryption of data
 - Amazon RDS: encryption of data
 - Amazon SSM: Parameter store
 - Etc...
- But you can also use the CLI / SDK

Question 183:

A company's public API runs as tasks on Amazon Elastic Container Service (Amazon ECS). The tasks run on AWS Fargate behind an Application Load Balancer (ALB) and are configured with Service Auto Scaling for the tasks based on CPU utilization. This service has been running well for several months.

Recently, API performance slowed down and made the application unusable. The company discovered that a significant number of SQL injection attacks had occurred against the API and that the API service had scaled to its maximum amount.

A solutions architect needs to implement a solution that prevents SQL injection attacks from reaching the ECS API service. The solution must allow legitimate traffic through and must maximize operational efficiency.

Which solution meets these requirements?

- A. Create a new AWS WAF web ACL to monitor the HTTP requests and HTTPS requests that are forwarded to the ALB in front of the ECS tasks.
- B. Create a new AWS WAF Bot Control implementation. Add a rule in the AWS WAF Bot Control managed rule group to monitor traffic and allow only legitimate traffic to the ALB in front of the ECS tasks.
- C. Create a new AWS WAF web ACL. Add a new rule that blocks requests that match the SQL database rule group. Set the web ACL to allow all other traffic that does not match those rules. Attach the web ACL to the ALB in front of the ECS tasks.
- D. Create a new AWS WAF web ACL. Create a new empty IP set in AWS WAF. Add a new rule to the web ACL to block requests that originate from IP addresses in the new IP set. Create an AWS Lambda function that scrapes the API logs for IP addresses that send SQL injection attacks, and add those IP addresses to the IP set. Attach the web ACL to the ALB in front of the ECS tasks.

C

- A. No, because this does not prevent SQL injection attacks from reaching the ECS API service
- B. No, because with Bot Control, you can easily monitor, block, or rate limit bots such as scrapers, scanners, crawlers, status monitors, and search engines.
- C. The SQL database rule group contains rules to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Evaluate this rule group for use if your application interfaces with an SQL database
- D. No, because because this is a reactive response after a SQL injection attack has occurred for new IP addresses.

AWS WAF – Web Application Firewall



- Protects your web applications from common web exploits (Layer 7)
- Deploy on **Application Load Balancer** (localized rules)
- Deploy on **API Gateway** (rules running at the regional or edge level)
- Deploy on **CloudFront** (rules globally on edge locations)
 - Used to front other solutions: CLB, EC2 instances, custom origins, S3 websites
- Deploy on AppSync (protect your GraphQL APIs)
- **WAF is not for DDoS protection**
- Define Web ACL (Web Access Control List):
 - Rules can include IP addresses, HTTP headers, HTTP body, or URI strings
 - Protects from common attack - **SQL injection** and Cross-Site Scripting (XSS)
 - Size constraints, Geo match
 - Rate-based rules (to count occurrences of events)
- Rule Actions: Count | Allow | Block | CAPTCHA

AWS WAF – Managed Rules

- Library of over 190 managed rules
- Ready-to-use rules that are managed by AWS and AWS Marketplace Sellers
- **Baseline Rule Groups** – general protection from common threats
 - AWSManagedRulesCommonRuleSet, AWSManagedRulesAdminProtectionRuleSet, ...
- **Use-case Specific Rule Groups** – protection for many AWS WAF use cases
 - AWSManagedRulesSqlRuleSet, AWSManagedRulesWindowsRuleSet, AWSManagedRulesPhpRuleSet, AWSManagedRulesWordPressRuleSet, ...
- **IP Reputation Rule Groups** – block requests based on source (e.g., malicious IPs)
 - AWSManagedRulesAmazonIpReputationList, AWSManagedRulesAnonymousIpList
- **Bot Control Managed Rule Group** – block and manage requests from bots
 - AWSManagedRulesBotControlRuleSet

Question 184:

An environmental company is deploying sensors in major cities throughout a country to measure air quality. The sensors connect to AWS IoT Core to ingest timeseries data readings. The company stores the data in Amazon DynamoDB.

For business continuity, the company must have the ability to ingest and store data in two AWS Regions.

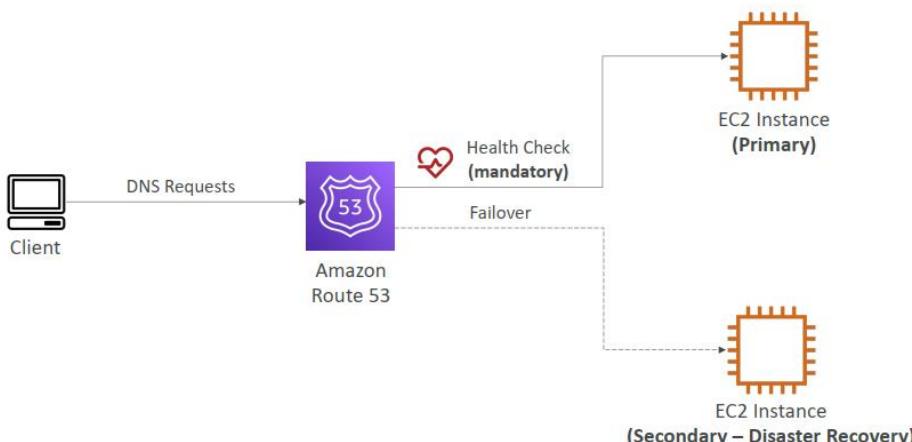
Which solution will meet these requirements?

- A. Create an Amazon Route 53 alias failover routing policy with values for AWS IoT Core data endpoints in both Regions. Migrate data to Amazon Aurora global tables.
- B. Create a domain configuration for AWS IoT Core in each Region. Create an Amazon Route 53 latency-based routing policy. Use AWS IoT Core data endpoints in both Regions as values. Migrate the data to Amazon MemoryDB for Redis and configure cross-Region replication.
- C. Create a domain configuration for AWS IoT Core in each Region. Create an Amazon Route 53 health check that evaluates domain configuration health. Create a failover routing policy with values for the domain name from the AWS IoT Core domain configurations. Update the DynamoDB table to a global table.
- D. Create an Amazon Route 53 latency-based routing policy. Use AWS IoT Core data endpoints in both Regions as values. Configure DynamoDB streams and cross-Region data replication.

C

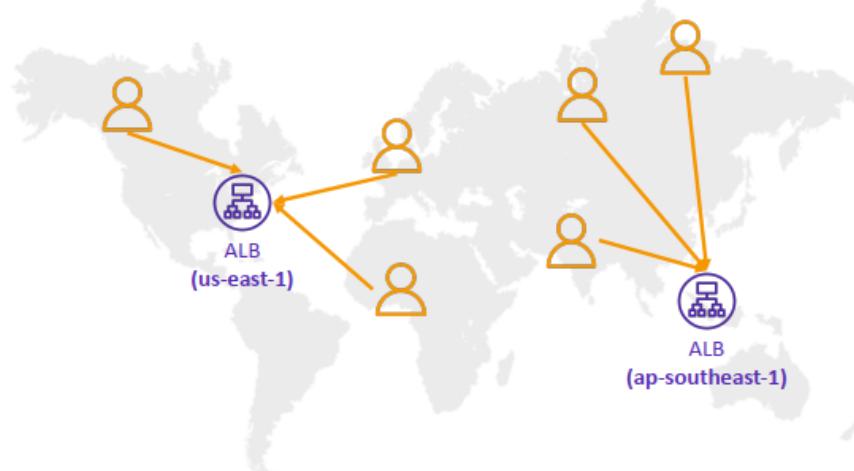
store data in two AWS Regions → DynamoDB table to a global table

Routing Policies – Failover (Active-Passive)



Routing Policies – Latency-based

- Redirect to the resource that has the least latency close to us
- Super helpful when latency for users is a priority
- Latency is based on traffic between users and AWS Regions
- Germany users may be directed to the US (if that's the lowest latency)
- Can be associated with Health Checks (has a failover capability)



Question 185:

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company's finance team has a data processing application that uses AWS Lambda and Amazon DynamoDB. The company's marketing team wants to access the data that is stored in the DynamoDB table.

The DynamoDB table contains confidential data. The marketing team can have access to only specific attributes of data in the DynamoDB table. The finance team and the marketing team have separate AWS accounts.

What should a solutions architect do to provide the marketing team with the appropriate access to the DynamoDB table?

- Create an SCP to grant the marketing team's AWS account access to the specific attributes of the DynamoDB table. Attach the SCP to the OU of the finance team.
- Create an IAM role in the finance team's account by using IAM policy conditions for specific DynamoDB attributes (fine-grained access control). Establish trust with the marketing team's account. In the marketing team's account, create an IAM role that has permissions to assume the IAM role in the finance team's account.
- Create a resource-based IAM policy that includes conditions for specific DynamoDB attributes (fine-grained access control). Attach the policy to the DynamoDB table. In the marketing team's account, create an IAM role that has permissions to access the DynamoDB table in the finance team's account.

D. Create an IAM role in the finance team's account to access the DynamoDB table. Use an IAM permissions boundary to limit the access to the specific attributes. In the marketing team's account, create an IAM role that has permissions to assume the IAM role in the finance team's account.

B

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_dynamodb_attributes.html

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "dynamodb:GetItem",  
                "dynamodb:BatchGetItem",  
                "dynamodb:Query",  
                "dynamodb:PutItem",  
                "dynamodb:UpdateItem",  
                "dynamodb:DeleteItem",  
                "dynamodb:BatchWriteItem"  
            ],  
            "Resource": ["arn:aws:dynamodb:*:*:table/table-name"],  
            "Condition": {  
                "ForAllValues:StringEquals": {  
                    "dynamodb:Attributes": [  
                        "column-name-1",  
                        "column-name-2",  
                        "column-name-3"  
                    ]  
                },  
                "StringEqualsIfExists": {"dynamodb:Select": "SPECIFIC_ATTRIBUTES"}  
            }  
        }  
    ]  
}
```

Question 186:

A solutions architect is creating an application that stores objects in an Amazon S3 bucket. The solutions architect must deploy the application in two AWS Regions that will be used simultaneously. The objects in the two S3 buckets must remain synchronized with each other.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

- A. Create an S3 Multi-Region Access Point Change the application to refer to the Multi-Region Access Point

- B. Configure two-way S3 Cross-Region Replication (CRR) between the two S3 buckets
- C. Modify the application to store objects in each S3 bucket
- D. Create an S3 Lifecycle rule for each S3 bucket to copy objects from one S3 bucket to the other S3 bucket
- E. Enable S3 Versioning for each S3 bucket
- F. Configure an event notification for each S3 bucket to invoke an AWS Lambda function to copy objects from one S3 bucket to the other S3 bucket.

A,B,E

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiRegionAccessPointRequestRouting.html>

LAB: <https://medium.com/@mahesh22/aws-s3-multi-region-access-points-d98eced9f799>

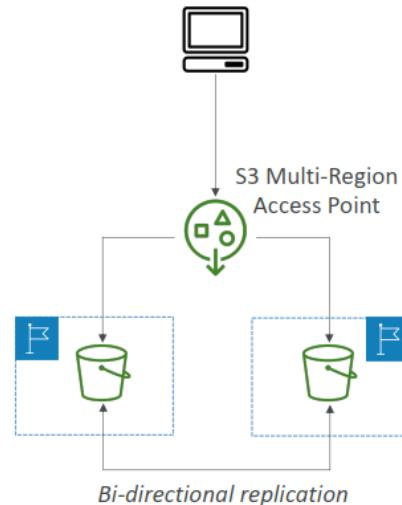
When you make a request through a Multi-Region Access Point, Amazon S3 determines which of the buckets that are associated with the Multi-Region Access Point is closest to you. Amazon S3 then directs the request to that bucket, regardless of the AWS Region it is located in.

After the Multi-Region Access Point routes the request to the closest-proximity bucket, Amazon S3 processes the request as if you made it directly to that bucket. Multi-Region Access Points aren't aware of the data contents of an Amazon S3 bucket. Therefore, the bucket that gets the request might not contain the requested data. To create consistent datasets in the Amazon S3 buckets that are associated with a Multi-Region Access Point, you can configure S3 Cross-Region Replication (CRR). Then any bucket can fulfill the request successfully.

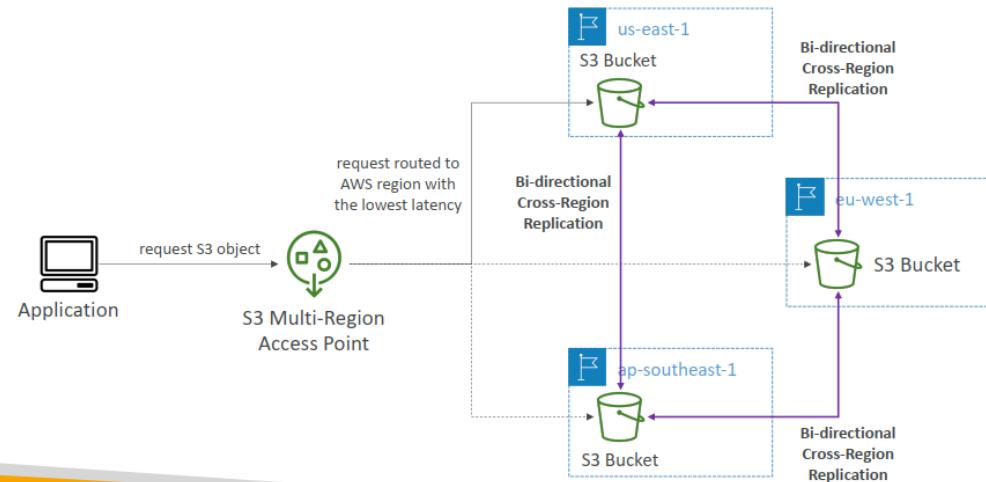
Cross Region Replication(CRR) requires versioning to be activated due to the way that data is replicated between S3 buckets

S3 – Multi-Region Access Points

- Provide a global endpoint that spans S3 buckets in multiple AWS regions
- Dynamically route requests to the nearest S3 bucket (lowest latency)
- Bi-directional S3 bucket replication rules are created to keep data in sync across regions
- Failover Controls – allows you to shift requests across S3 buckets in different AWS regions within minutes (Active-Active or Active-Passive)

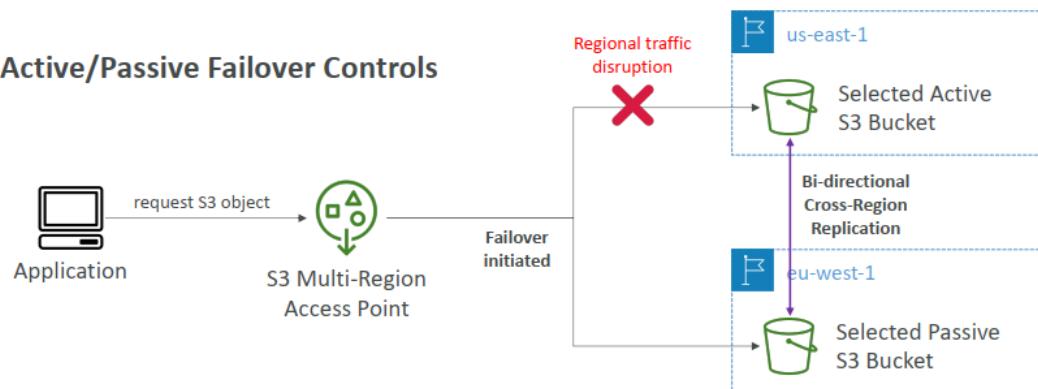


S3 – Multi-Region Access Points



Multi-Region Access Points – Failover Controls

Active/Passive Failover Controls



Works with active/active or active/passive setups

Question 187:

A company has an IoT platform that runs in an on-premises environment. The platform consists of a server that connects to IoT devices by using the MQTT protocol. The platform collects telemetry data from the devices at least once every 5 minutes. The platform also stores device metadata in a MongoDB cluster.

An application that is installed on an on-premises machine runs periodic jobs to aggregate and transform the telemetry and device metadata. The application creates reports that users view by using another web application that runs on the same on-premises machine. The periodic jobs take 120-600 seconds to run. However, the web application is always running.

The company is moving the platform to AWS and must reduce the operational overhead of the stack.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

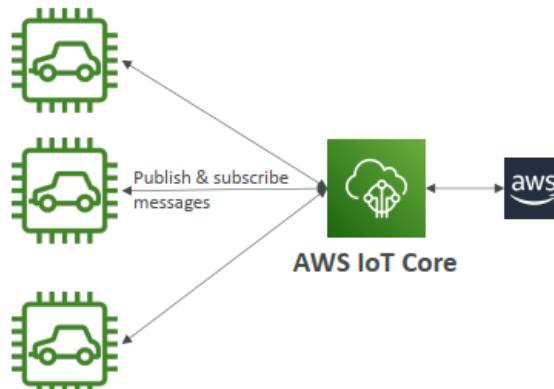
- A. Use AWS Lambda functions to connect to the IoT devices
- B. Configure the IoT devices to publish to AWS IoT Core
- C. Write the metadata to a self-managed MongoDB database on an Amazon EC2 instance
- D. Write the metadata to Amazon DocumentDB (with MongoDB compatibility)
- E. Use AWS Step Functions state machines with AWS Lambda tasks to prepare the reports and to write the reports to Amazon S3. Use Amazon CloudFront with an S3 origin to serve the reports
- F. Use an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with Amazon EC2 instances to prepare the reports. Use an ingress controller in the EKS cluster to serve the reports

B,D,E

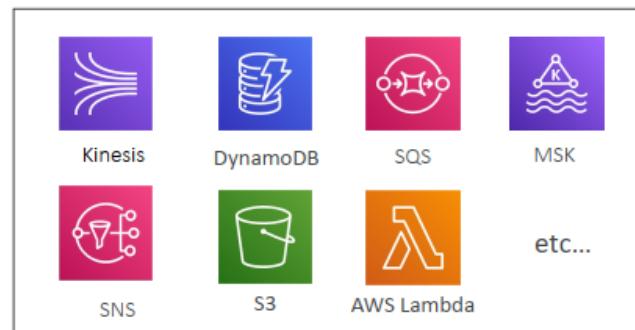
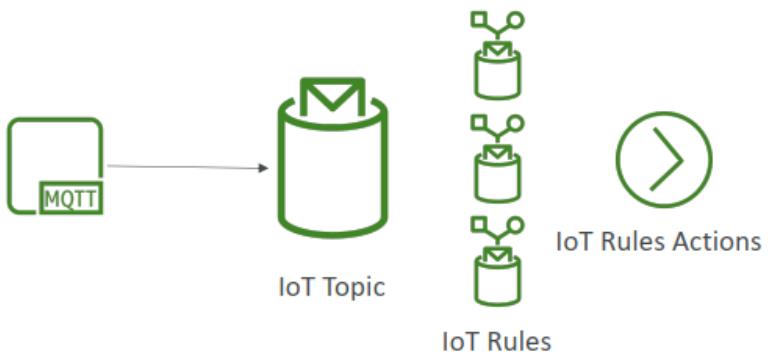
AWS IoT Core



- IoT stands for “Internet of Things” – the network of internet-connected devices that are able to collect and transfer data
- AWS IoT Core allows you to **easily** connect IoT devices to the AWS Cloud
- Serverless, secure & scalable to billions of devices and trillions of messages
- Integrates with a lot of AWS services (Lambda, S3, SageMaker, etc.)
- Build IoT applications that gather, process, analyze, and act on data



IoT Core - Integrations



The application creates reports that users view by using another web application that runs on the same on-premises machine => S3 host static web
MQTT (Message Queuing Telemetry Transport):

- Style: is a lightweight, publish-subscribe messaging protocol.
- Features: Primarily used in IoT and applications with low bandwidth or high latency, it ensures efficient communication between devices.

Question 188:

A global manufacturing company plans to migrate the majority of its applications to AWS. However, the company is concerned about applications that need to remain within a specific country or in the company's central on-premises data center because of data regulatory requirements or requirements for latency of single-digit milliseconds. The company also is concerned about the applications that it hosts in some of its factory sites, where limited network infrastructure exists.

The company wants a consistent developer experience so that its developers can build applications once and deploy on premises, in the cloud, or in a hybrid architecture. The developers must be able to use the same tools, APIs, and services that are familiar to them.

Which solution will provide a consistent hybrid experience to meet these requirements?

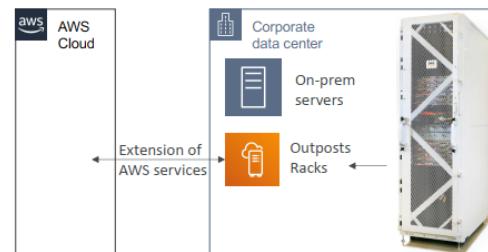
- Migrate all applications to the closest AWS Region that is compliant. Set up an AWS Direct Connect connection between the central on-premises data center and AWS. Deploy a Direct Connect gateway.
- Use AWS Snowball Edge Storage Optimized devices for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds. Retain the devices on premises. Deploy AWS Wavelength to host the workloads in the factory sites.
- Install AWS Outposts for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds. Use AWS Snowball Edge Compute Optimized devices to host the workloads in the factory sites.
- Migrate the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds to an AWS Local Zone. Deploy AWS Wavelength to host the workloads in the factory sites.

C

AWS Outposts



- Hybrid Cloud: businesses that keep an on-premises infrastructure alongside a cloud infrastructure
- Therefore, two ways of dealing with IT systems:
 - One for the AWS cloud (using the AWS console, CLI, and AWS APIs)
 - One for their on-premises infrastructure
- AWS Outposts are “server racks” that offers the same AWS infrastructure, services, APIs & tools to build your own applications on-premises just as in the cloud
- AWS will setup and manage “Outposts Racks” within your on-premises infrastructure and you can start leveraging AWS services on-premises
- You are responsible for the Outposts Rack physical security



AWS Outposts



- Benefits:
 - Low-latency access to on-premises systems
 - Local data processing
 - Data residency
 - Easier migration from on-premises to the cloud
 - Fully managed service
- Some services that work on Outposts:



Amazon EC2



Amazon EBS



Amazon S3



Amazon EKS



Amazon ECS



Amazon RDS



Amazon EMR

Key comment: "specific country or in the company's central on-premises data center because of data regulatory requirements or requirements for latency of single-digit milliseconds."

A - No - Region doesn't assure you have in country presence for data sovereignty

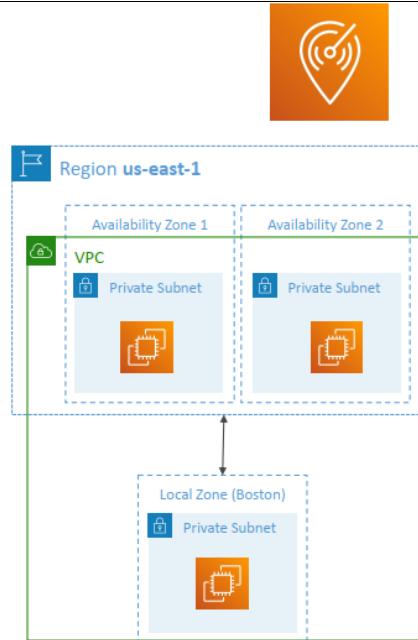
B - No - Snowball part is correct. However, Wavelength access is only via mobile networks, and not in every country, so this is not possible unless all developers are connecting over the mobile network that will have speed variations

D - No - Local Zones can be fast with a DX connection, but this option like Wavelength is not in every country

Correct answer is C. 100% of the time you are on premise providing single-digit milliseconds latency as Outposts (rack or server) and Snowball will be in the country for the requirements

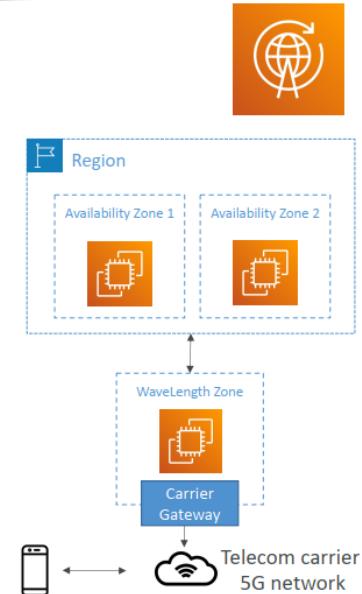
AWS Local Zones

- Places AWS compute, storage, database, and other selected AWS services **closer** to end users to run **latency-sensitive** applications
- Extend your VPC to more locations – “**Extension of an AWS Region**”
- Compatible with EC2, RDS, ECS, EBS, ElastiCache, Direct Connect ...
- Example:
 - AWS Region: N.Virginia (us-east-1)
 - AWS Local Zones: Boston, Chicago, Dallas, Houston, Miami, ...



AWS WaveLength

- WaveLength Zones** are infrastructure deployments embedded within the telecommunications providers' datacenters at the edge of the 5G networks
- Brings AWS services to the edge of the 5G networks
- Example: EC2, EBS, VPC...
- Ultra-low latency applications through 5G networks
- Traffic doesn't leave the Communication Service Provider's (CSP) network
- High-bandwidth and secure connection to the parent AWS Region
- No additional charges or service agreements
- Use cases: Smart Cities, ML-assisted diagnostics, Connected Vehicles, Interactive Live Video Streams, AR/VR, Real-time Gaming, ...



Question 189:

A company is updating an application that customers use to make online orders. The number of attacks on the application by bad actors has increased recently.

The company will host the updated application on an Amazon Elastic Container Service (Amazon ECS) cluster. The company will use Amazon DynamoDB to store application data. A public Application Load Balancer (ALB) will provide end users with access to the application. The company must prevent attacks and ensure business continuity with minimal service interruptions during an ongoing attack.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an Amazon CloudFront distribution with the ALB as the origin. Add a custom header and random value on the CloudFront domain. Configure the ALB to conditionally forward traffic if the header and value match.
- B. Deploy the application in two AWS Regions. Configure Amazon Route 53 to route to both Regions with equal weight.
- C. Configure auto scaling for Amazon ECS tasks Create a DynamoDB Accelerator (DAX) cluster.
- D. Configure Amazon ElastiCache to reduce overhead on DynamoDB.
- E. Deploy an AWS WAF web ACL that includes an appropriate rule group. Associate the web ACL with the Amazon CloudFront distribution.

A, E

Option A: By adding a custom header and random value on the CloudFront domain and configuring the ALB to conditionally forward traffic if the header and value match, you can implement a form of request validation. This helps to filter out potentially malicious requests and prevent attacks from reaching the application.
Option E: Deploying an AWS WAF web ACL that includes an appropriate rule group and associating it with the Amazon CloudFront distribution adds an additional layer of protection. The web ACL can include rules to block common attack patterns and provide protection against various types of attacks, such as SQL injection and cross-site scripting (XSS).

Question 190:

A company runs a web application on AWS. The web application delivers static content from an Amazon S3 bucket that is behind an Amazon CloudFront distribution. The application serves dynamic content by using an Application Load Balancer (ALB) that distributes requests to a fleet of Amazon EC2 instances in Auto Scaling groups. The application uses a domain name setup in Amazon Route 53.

Some users reported occasional issues when the users attempted to access the website during peak hours. An operations team found that the ALB sometimes returned HTTP 503 Service Unavailable errors. The company wants to display a custom error message page when these errors occur. The page should be displayed immediately for this error code.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Set up a Route 53 failover routing policy. Configure a health check to determine the status of the ALB endpoint and to fail over to the failover S3 bucket endpoint.
- B. Create a second CloudFront distribution and an S3 static website to host the custom error page. Set up a Route 53 failover routing policy. Use an active-passive configuration between the two distributions.

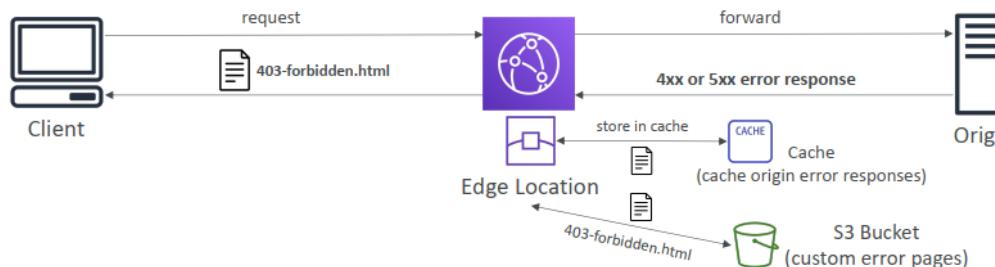
C. Create a CloudFront origin group that has two origins. Set the ALB endpoint as the primary origin. For the secondary origin, set an S3 bucket that is configured to host a static website. Set up origin failover for the CloudFront distribution. Update the S3 static website to incorporate the custom error page.

D. Create a CloudFront function that validates each HTTP response code that the ALB returns. Create an S3 static website in an S3 bucket. Upload the custom error page to the S3 bucket as a failover. Update the function to read the S3 bucket and to serve the error page to the end users.

C

CloudFront – Custom Error Pages

- Return an object to the viewer (e.g., .html) when your origin returns an HTTP 4xx or 5xx status code to CloudFront
- Use **Error Caching Minimum TTL** to specify how long CloudFront caches the custom error pages



Question 191:

A company is planning to migrate an application to AWS. The application runs as a Docker container and uses an NFS version 4 file share.

A solutions architect must design a secure and scalable containerized solution that does not require provisioning or management of the underlying infrastructure.

Which solution will meet these requirements?

- Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Use Amazon Elastic File System (Amazon EFS) for shared storage. Reference the EFS file system ID, container mount point, and EFS authorization IAM role in the ECS task definition.
- Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Use Amazon FSx for Lustre for shared storage. Reference the FSx for Lustre file system ID, container mount point, and FSx for Lustre authorization IAM role in the ECS task definition.

C. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type and auto scaling turned on. Use Amazon Elastic File System (Amazon EFS) for shared storage. Mount the EFS file system on the ECS container instances. Add the EFS authorization IAM role to the EC2 instance profile.

D. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type and auto scaling turned on. Use Amazon Elastic Block Store (Amazon EBS) volumes with Multi-Attach enabled for shared storage. Attach the EBS volumes to ECS container instances. Add the EBS authorization IAM role to an EC2 instance profile.

A

Amazon EFS is a managed NAS filer for EC2 instances based on Network File System (NFS) version 4.

Question 192:

A company is running an application in the AWS Cloud. The core business logic is running on a set of Amazon EC2 instances in an Auto Scaling group. An Application Load Balancer (ALB) distributes traffic to the EC2 instances. Amazon Route 53 record api.example.com is pointing to the ALB.

The company's development team makes major updates to the business logic. The company has a rule that when changes are deployed, only 10% of customers can receive the new logic during a testing window. A customer must use the same version of the business logic during the testing window.

How should the company deploy the updates to meet these requirements?

A. Create a second ALB, and deploy the new logic to a set of EC2 instances in a new Auto Scaling group. Configure the ALB to distribute traffic to the EC2 instances. Update the Route 53 record to use weighted routing, and point the record to both of the ALBs.

B. Create a second target group that is referenced by the ALB. Deploy the new logic to EC2 instances in this new target group. Update the ALB listener rule to use weighted target groups. Configure ALB target group stickiness.

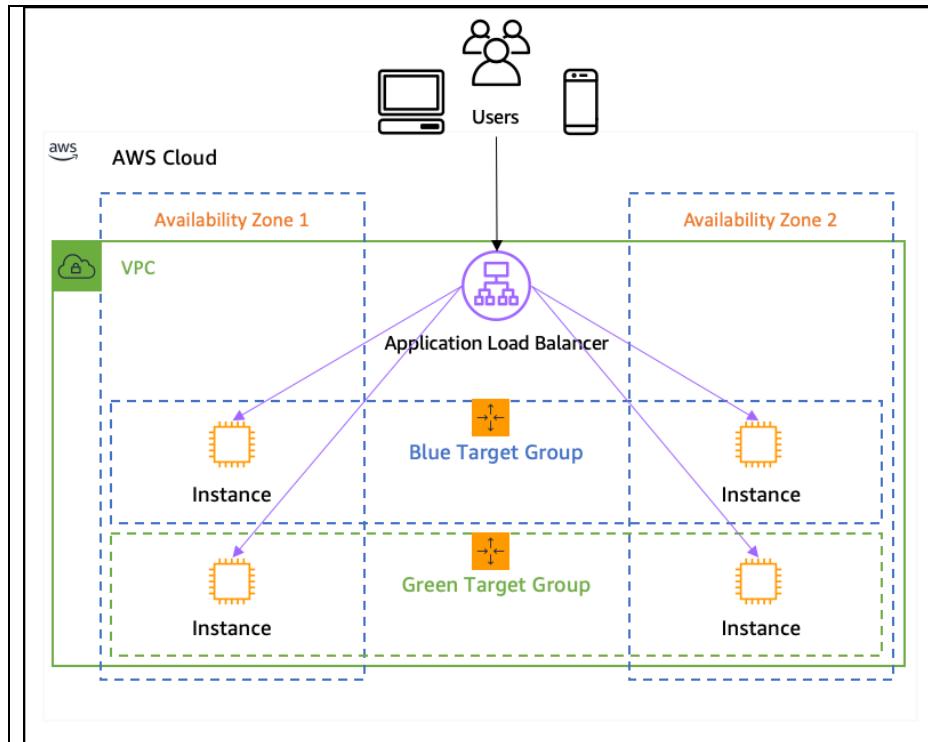
C. Create a new launch configuration for the Auto Scaling group. Specify the launch configuration to use the AutoScalingRollingUpdate policy, and set the MaxBatchSize option to 10. Replace the launch configuration on the Auto Scaling group. Deploy the changes.

D. Create a second Auto Scaling group that is referenced by the ALB. Deploy the new logic on a set of EC2 instances in this new Auto Scaling group. Change the ALB routing algorithm to least outstanding requests (LOR). Configure ALB session stickiness.

B

<https://docs.aws.amazon.com/prescriptive-guidance/latest/load-balancer-stickiness/target-group-stickiness.html>

LAB: <https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>



Target group

Target group	Weight	Percent
prod-ingress-enterprise-tg Target type: IP, IPv4	2	66.67%
test-prod-external-mcweb-tg Target type: IP, IPv4	1	33.33%

Question 193:

A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities. The company is storing user profiles on an Amazon FSx for Windows File Server file system. The file system is configured with a DNS alias and is connected to a self-managed Active Directory. As more users begin to use the Workspaces, login time increases to unacceptable levels.

An investigation reveals a degradation in performance of the file system. The company created the file system on HDD storage with a throughput of 16 MBps. A solutions architect must improve the performance of the file system during a defined maintenance window.

What should the solutions architect do to meet these requirements with the LEAST administrative effort?

A. Use AWS Backup to create a point-in-time backup of the file system. Restore the backup to a new FSx for Windows File Server file system. Select SSD as the storage type. Select 32 MBps as the throughput capacity. When the backup and restore process is completed, adjust the DNS alias accordingly. Delete the original file system.

B. Disconnect users from the file system. In the Amazon FSx console, update the throughput capacity to 32 MBps. Update the storage type to SSD. Reconnect users to the file system.

C. Deploy an AWS DataSync agent onto a new Amazon EC2 instance. Create a task. Configure the existing file system as the source location. Configure a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput as the target location. Schedule the task. When the task is completed, adjust the DNS alias accordingly. Delete the original file system.

D. Enable shadow copies on the existing file system by using a Windows PowerShell command. Schedule the shadow copy job to create a point-in-time backup of the file system. Choose to restore previous versions. Create a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput. When the copy job is completed, adjust the DNS alias. Delete the original file system.

A

LEAST administrative effort → A

It can't be B because Amazon FSx does not support in-place upgrades of storage type from HDD to SSD or direct changes to throughput capacity on the existing file system.

Amazon FSx for Windows (File Server)



- FSx for Windows is a fully managed Windows file system [share drive](#)
- Supports SMB protocol & Windows NTFS
- Microsoft Active Directory integration, ACLs, user quotas
- Can be mounted on Linux EC2 instances
- Supports Microsoft's Distributed File System (DFS) Namespaces (group files across multiple FS)
- Scale up to 10s of GB/s, millions of IOPS, 100s PB of data
- Storage Options:
 - SSD – latency sensitive workloads (databases, media processing, data analytics, ...)
 - HDD – [broad spectrum of workloads](#) (home directory, CMS, ...) phạm vi rộng của khởi lượng công việc
- Can be accessed from your on-premises infrastructure (VPN or Direct Connect)
- Can be configured to be Multi-AZ (high availability)
- Data is backed-up daily to S3

AWS Backup

point in time recovery



- Supports [PITR](#) for supported services
- On-Demand and Scheduled backups
- Tag-based backup policies
- You create backup policies known as **Backup Plans**
 - Backup frequency (every 12 hours, daily, weekly, monthly, cron expression)
 - Backup window
 - Transition to Cold Storage (Never, Days, Weeks, Months, Years)
 - Retention Period (Always, Days, Weeks, Months, Years)

Question 194:

A company hosts an application on AWS. The application reads and writes objects that are stored in a single Amazon S3 bucket. The company must modify the application to deploy the application in two AWS Regions.

Which solution will meet these requirements with the LEAST operational overhead?

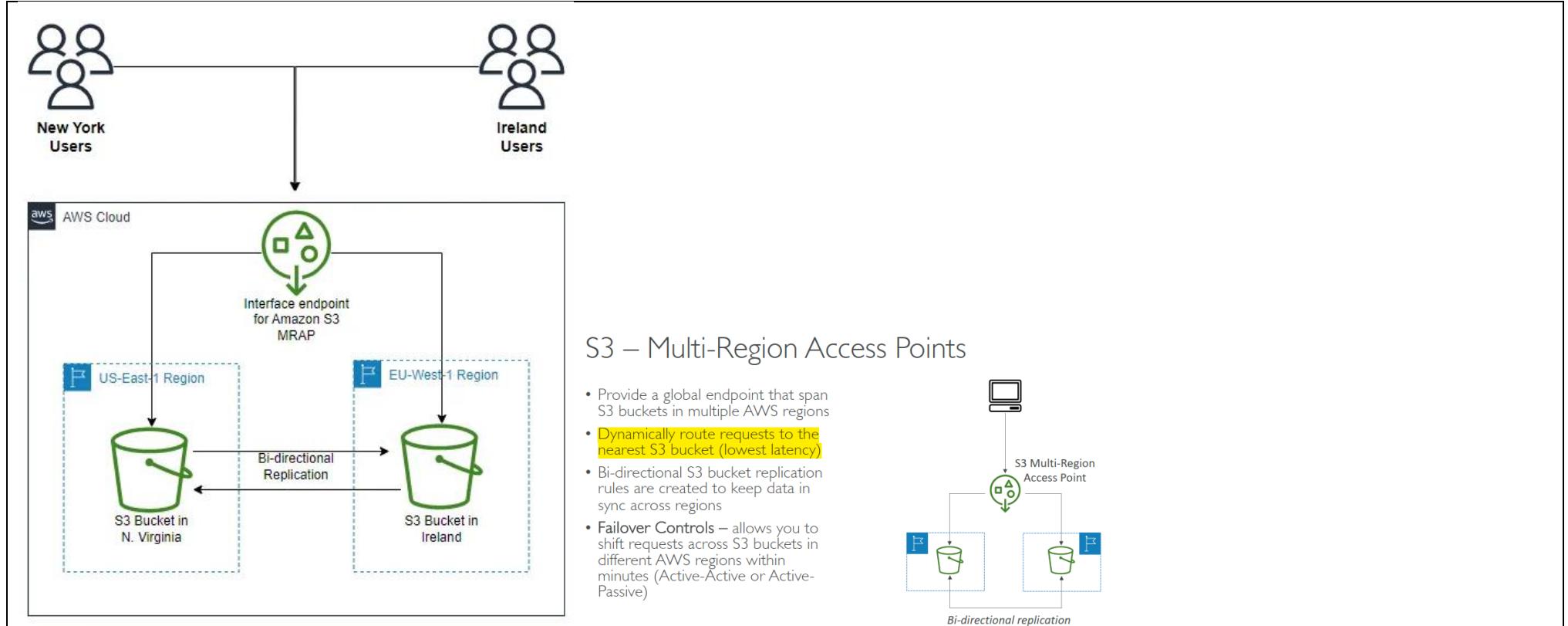
- A. Set up an Amazon CloudFront distribution with the S3 bucket as an origin. Deploy the application to a second Region. Modify the application to use the CloudFront distribution. Use AWS Global Accelerator to access the data in the S3 bucket.
- B. Create a new S3 bucket in a second Region. Set up bidirectional S3 Cross-Region Replication (CRR) between the original S3 bucket and the new S3 bucket. Configure an S3 Multi-Region Access Point that uses both S3 buckets. Deploy a modified application to both Regions.
- C. Create a new S3 bucket in a second Region. Deploy the application in the second Region. Configure the application to use the new S3 bucket. Set up S3 Cross-Region Replication (CRR) from the original S3 bucket to the new S3 bucket.
- D. Set up an S3 gateway endpoint with the S3 bucket as an origin. Deploy the application to a second Region. Modify the application to use the new S3 gateway endpoint. Use S3 Intelligent-Tiering on the S3 bucket.

B

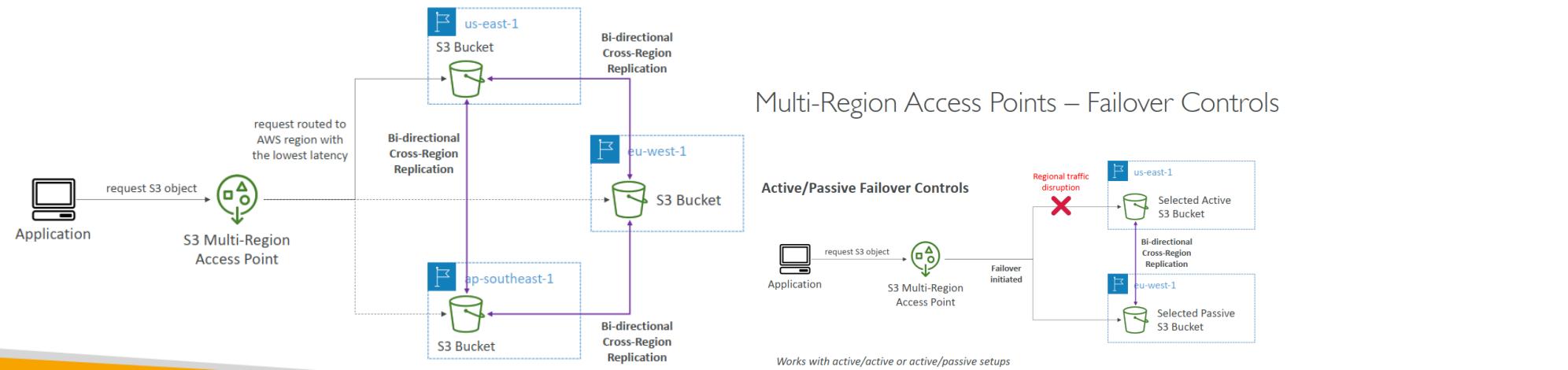
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiRegionAccessPointRequestRouting.html>

LAB: <https://medium.com/@mahesh22/aws-s3-multi-region-access-points-d98eced9f799>

Option B creates a new S3 bucket in a second Region and sets up bidirectional S3 Cross-Region Replication (CRR) between the original S3 bucket and the new S3 bucket. S3 CRR is a feature that enables automatic, asynchronous copying of objects across S3 buckets in different AWS Regions. You can use S3 CRR to keep your data synchronized across Regions for lower latency, compliance, security, disaster recovery, and regional efficiency.



S3 – Multi-Region Access Points



Question 195:

An online gaming company needs to rehost its gaming platform on AWS. The company's gaming application requires high performance computing (HPC) processing and has a leaderboard that changes frequently. An Ubuntu instance that is optimized for compute generation hosts a Node.js application for game display. Game state is tracked in an on-premises Redis instance.

The company needs a migration strategy that optimizes application performance.

Which solution will meet these requirements?

- Create an Auto Scaling group of m5.large Amazon EC2 Spot Instances behind an Application Load Balancer. Use an Amazon ElastiCache for Redis cluster to maintain the leaderboard.
- Create an Auto Scaling group of c5.large Amazon EC2 Spot Instances behind an Application Load Balancer. Use an Amazon OpenSearch Service cluster to maintain the leaderboard.
- Create an Auto Scaling group of c5.large Amazon EC2 On-Demand Instances behind an Application Load Balancer. Use an Amazon ElastiCache for Redis cluster to maintain the leaderboard.
- Create an Auto Scaling group of m5.large Amazon EC2 On-Demand Instances behind an Application Load Balancer. Use an Amazon DynamoDB table to maintain the leaderboard.

C

<https://aws.amazon.com/blogs/database/building-a-real-time-gaming-leaderboard-with-amazon-elasticsearch-for-redis/>

EC2 Instance Launch Types

- **On Demand Instances:** short workload, predictable pricing, reliable
- **Spot Instances:** short workloads, for cheap, can lose instances (not reliable)
- **Reserved:** (MINIMUM 1 year)
 - Reserved Instances: long workloads
 - Convertible Reserved Instances: long workloads with flexible instances
 - Highest to lowest discount: All Upfront payment, Partial Upfront payment, no Upfront
- **Dedicated Instances:** no other customers will share your hardware
- **Dedicated Hosts:** book an entire physical server; control instance placement
 - Great for software licenses that operate at the core, or CPU socket level
 - Can define host affinity so that instance reboots are kept on the same host

<https://trello.com/c/v194Dnq8/495-on-demand-vs-spot-instance>

Question 196:

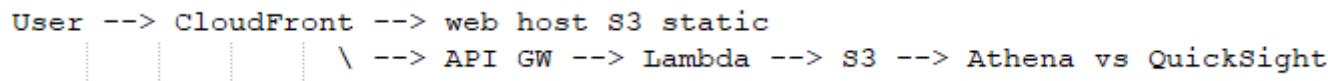
A solutions architect is designing an application to accept timesheet entries from employees on their mobile devices. Timesheets will be submitted weekly, with most of the submissions occurring on Friday. The data must be stored in a format that allows payroll administrators to run monthly reports. The infrastructure must be highly available and scale to match the rate of incoming data and reporting requests.

Which combination of steps meets these requirements while minimizing operational overhead? (Choose two.)

- Deploy the application to Amazon EC2 On-Demand Instances with load balancing across multiple Availability Zones. Use scheduled Amazon EC2 Auto Scaling to add capacity before the high volume of submissions on Fridays.
- Deploy the application in a container using Amazon Elastic Container Service (Amazon ECS) with load balancing across multiple Availability Zones. Use scheduled ServiceAuto Scaling to add capacity before the high volume of submissions on Fridays.
- Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront. Deploy the application backend using Amazon API Gateway with an AWS Lambda proxy integration.
- Store the timesheet submission data in Amazon Redshift. Use Amazon QuickSight to generate the reports using Amazon Redshift as the data source.
- Store the timesheet submission data in Amazon S3. Use Amazon Athena and Amazon QuickSight to generate the reports using Amazon S3 as the data source.

C,E
minimizing operational overhead, then No EC2, NO ECS. a lot of operational work to maintain it.

C. By deploying the application front end to an Amazon S3 bucket served by Amazon CloudFront, you can benefit from the scalability, high availability, and low latency of the S3 and CloudFront services. This combination allows for efficient content delivery and a smooth user experience on mobile devices. Using Amazon API Gateway with an AWS Lambda proxy integration for the backend enables serverless execution and eliminates the need for managing and scaling infrastructure. It provides an efficient way to handle the timesheet submissions.



Question 197:

A company is storing sensitive data in an Amazon S3 bucket. The company must log all activities for objects in the S3 bucket and must keep the logs for 5 years. The company's security team also must receive an email notification every time there is an attempt to delete data in the S3 bucket.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

- A. Configure AWS CloudTrail to log S3 data events.
 - B. Configure S3 server access logging for the S3 bucket.
 - C. Configure Amazon S3 to send object deletion events to Amazon Simple Email Service (Amazon SES).
 - D. Configure Amazon S3 to send object deletion events to an Amazon EventBridge event bus that publishes to an Amazon Simple Notification Service (Amazon SNS) topic.
 - E. Configure Amazon S3 to send the logs to Amazon Timestream with data storage tiering.
 - F. Configure a new S3 bucket to store the logs with an S3 Lifecycle policy.

B,D,F

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/enable-server-access-logging.html>

LAB: <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-s3-object-created-tutorial.html>

must receive an email notification every time there is an attempt to delete data in the S3 bucket → SNS, S3 object deletion

must keep the logs for 5 years → F. Lifecycle policy

Server access logging provides detailed records for the requests that are made to an Amazon S3 bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits. This information can also help you learn about your customer base and understand your Amazon S3 bill.

Question 198:

A company is building a hybrid environment that includes servers in an on-premises data center and in the AWS Cloud. The company has deployed Amazon EC2 instances in three VPCs. Each VPC is in a different AWS Region. The company has established an AWS Direct Connect connection to the data center from the Region that is closest to the data center.

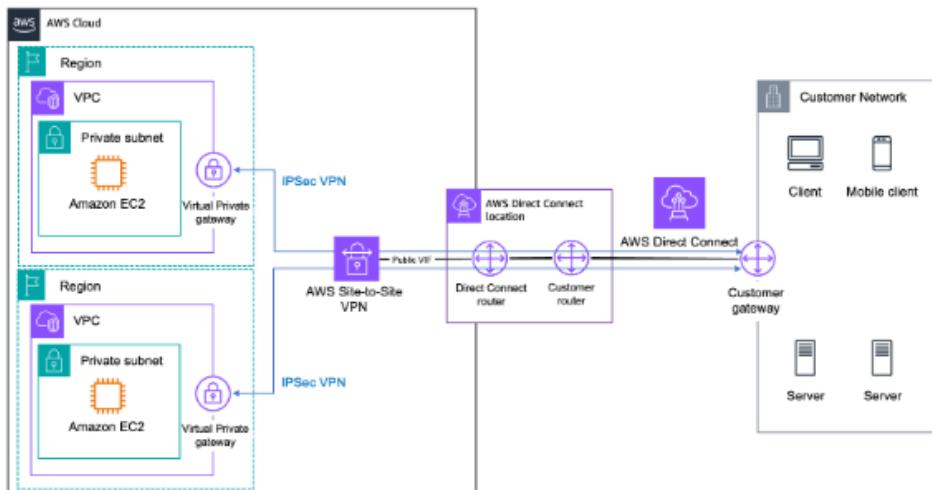
The company needs the servers in the on-premises data center to have access to the EC2 instances in all three VPCs. The servers in the on-premises data center also must have access to AWS public services.

Which combination of steps will meet these requirements with the LEAST cost? (Choose two.)

- A. Create a Direct Connect gateway in the Region that is closest to the data center. Attach the Direct Connect connection to the Direct Connect gateway. Use the Direct Connect gateway to connect the VPCs in the other two Regions.
- B. Set up additional Direct Connect connections from the on-premises data center to the other two Regions.
- C. Create a private VIF. Establish an AWS Site-to-Site VPN connection over the private VIF to the VPCs in the other two Regions.
- D. Create a public VIF. Establish an AWS Site-to-Site VPN connection over the public VIF to the VPCs in the other two Regions.
- E. Use VPC peering to establish a connection between the VPCs across the Regions. Create a private VIF with the existing Direct Connect connection to connect to the peered VPCs.

A,D

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-site-to-site-vpn.html>



C, E are wrong → private VIF can only connect to the vpc which is in the same region with direct connection, you can't extend private VIF to the VPCs in other 2 regions.

Question 199:

A company is using an organization in AWS Organizations to manage hundreds of AWS accounts. A solutions architect is working on a solution to provide baseline protection for the Open Web Application Security Project (OWASP) top 10 web application vulnerabilities. The solutions architect is using AWS WAF for all existing and new Amazon CloudFront distributions that are deployed within the organization.

Which combination of steps should the solutions architect take to provide the baseline protection? (Choose three.)

- A. Enable AWS Config in all accounts

- B. Enable Amazon GuardDuty in all accounts
- C. Enable all features for the organization
- D. Use AWS Firewall Manager to deploy AWS WAF rules in all accounts for all CloudFront distributions
- E. Use AWS Shield Advanced to deploy AWS WAF rules in all accounts for all CloudFront distributions
- F. Use AWS Security Hub to deploy AWS WAF rules in all accounts for all CloudFront distributions

A,C,D

LAB: <https://aws.amazon.com/blogs/security/using-aws-firewall-manager-and-waf-to-protect-your-web-applications-with-master-rules-and-application-specific-rules/>
AWS Config and All Features should be enabled in the organization.

AWS Config



- Helps with auditing and recording **compliance** of your AWS resources
- Helps record configurations and changes over time
- **AWS Config Rules does not prevent actions from happening (no deny)**
- Questions that can be solved by AWS Config:
 - Is there unrestricted SSH access to my security groups?
 - Do my buckets have any public access?
 - How has my ALB configuration changed over time?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per-region service
- Can be aggregated across regions and accounts

Amazon GuardDuty



Phát hiện mối đe dọa để bảo vệ account của bạn

- Intelligent Threat discovery to protect your AWS Account
- Uses Machine Learning algorithms, anomaly detection, 3rd party data
- One click to enable (30 days trial), no need to install software
- Input data includes:
 - CloudTrail Events Logs – unusual API calls, unauthorized deployments
 - CloudTrail Management Events – create VPC subnet, create trail, ...
 - CloudTrail S3 Data Events – get object, list objects, delete object, ...
 - VPC Flow Logs – unusual internal traffic, unusual IP address
 - DNS Logs – compromised EC2 instances sending encoded data within DNS queries
 - ^{xâm phạm} các phiên bản EC2 bị xâm phạm đang gửi dữ liệu được mã hóa trong các truy vấn DNS
 - Optional Feature – EKS Audit Logs, RDS & Aurora, EBS, Lambda, S3 Data Events...
- Can setup EventBridge rules to be notified in case of findings
- EventBridge rules can target AWS Lambda or SNS
- Can protect against CryptoCurrency attacks (has a dedicated “finding” for it)

Question 200:

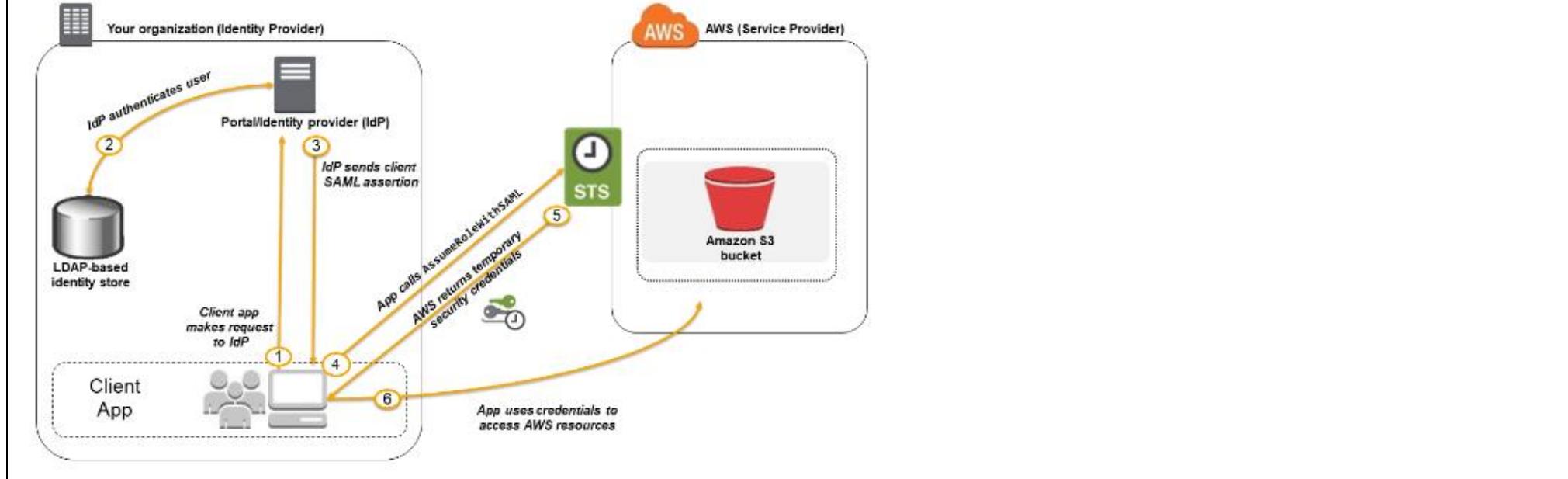
A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal, access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment.

Which items should the solutions architect check to ensure identity federation is properly configured? (Choose three.)

- A. The IAM user's permissions policy has allowed the use of SAML federation for that user.
- B. The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.
- C. Test users are not in the AWSFederatedUsers group in the company's IdP.
- D. The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdP.
- E. The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs.
- F. The company's IdP defines SAML assertions that properly map users or groups. In the company to IAM roles with appropriate permissions.

B,D,F

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html



Question 201:

A solutions architect needs to improve an application that is hosted in the AWS Cloud. The application uses an Amazon Aurora MySQL DB instance that is experiencing overloaded connections. Most of the application's operations insert records into the database. The application currently stores credentials in a text-based configuration file.

The solutions architect needs to implement a solution so that the application can handle the current connection load. The solution must keep the credentials secure and must provide the ability to rotate the credentials automatically on a regular basis.

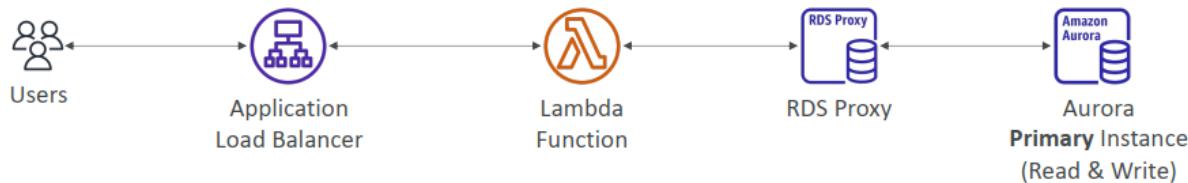
Which solution will meet these requirements?

- A. Deploy an Amazon RDS Proxy layer in front of the DB instance. Store the connection credentials as a secret in AWS Secrets Manager.
- B. Deploy an Amazon RDS Proxy layer in front of the DB instance. Store the connection credentials in AWS Systems Manager Parameter Store
- C. Create an Aurora Replica. Store the connection credentials as a secret in AWS Secrets Manager
- D. Create an Aurora Replica. Store the connection credentials in AWS Systems Manager Parameter Store.

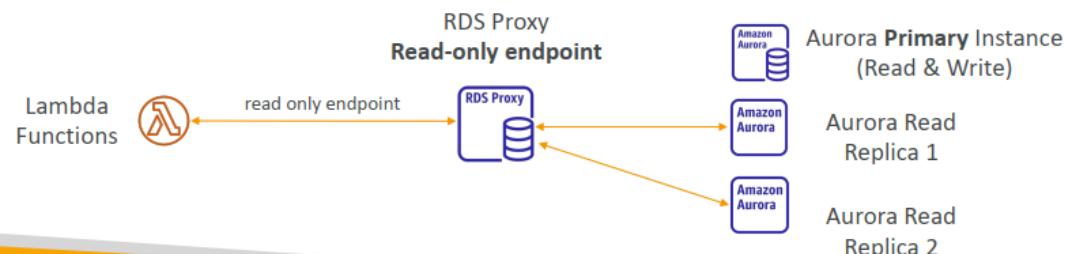
A

Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool. This approach avoids the memory and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created.

RDS Proxy for Aurora



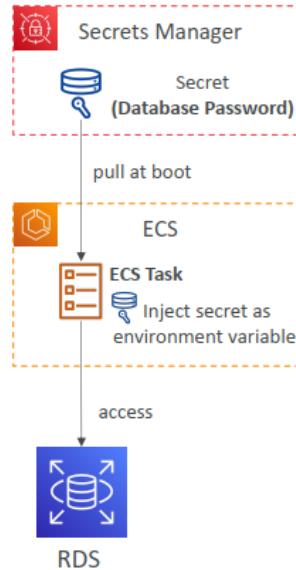
- Ability to create an additional read-only endpoint that connects to Aurora Read Replicas only



AWS Secrets Manager



- Meant for storing secrets (e.g., passwords, API keys, ...)
- Capability to force **rotation of secrets** every X days
 - Automate generation of secrets on rotation (uses Lambda)
 - Natively supports Amazon RDS (all supported DB engines), Redshift, DocumentDB
 - Support other databases and services (custom Lambda function)
- Control access to secrets using Resource-based Policy
- Integration with other AWS services to natively pull secrets from Secrets Manager: *CloudFormation, CodeBuild, ECS, EMR, Fargate, EKS, Parameter Store...*



Question 202:

A company needs to build a disaster recovery (DR) solution for its ecommerce website. The web application is hosted on a fleet of t3.large Amazon EC2 instances and uses an Amazon RDS for MySQL DB instance. The EC2 instances are in an Auto Scaling group that extends across multiple Availability Zones.

In the event of a disaster, the web application must fail over to the secondary environment with an RPO of 30 seconds and an RTO of 10 minutes.

Which solution will meet these requirements MOST cost-effectively?

- A. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create a cross-Region read replica for the DB instance. Set up a backup plan in AWS Backup to create cross-Region backups for the EC2 instances and the DB instance. Create a cron expression to back up the EC2 instances and the DB instance every 30 seconds to the DR Region. Recover the EC2 instances from the latest EC2 backup. Use an Amazon Route 53 geolocation routing policy to automatically fail over to the DR Region in the event of a disaster.

B. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create a cross-Region read replica for the DB instance. Set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. Run the EC2 instances at the minimum capacity in the DR Region. Use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster. Increase the desired capacity of the Auto Scaling group.

C. Set up a backup plan in AWS Backup to create cross-Region backups for the EC2 instances and the DB instance. Create a cron expression to back up the EC2 instances and the DB instance every 30 seconds to the DR Region. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Manually restore the backed-up data on new instances. Use an Amazon Route 53 simple routing policy to automatically fail over to the DR Region in the event of a disaster.

D. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create an Amazon Aurora global database. Set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. Run the Auto Scaling group of EC2 instances at full capacity in the DR Region. Use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster.

B

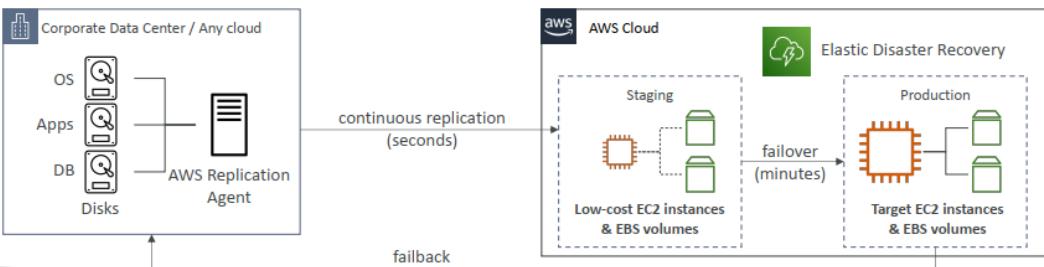
<https://aws.amazon.com/disaster-recovery/>

MOST cost-effectively ➔ Run the EC2 instances at the minimum capacity in the DR Region
the web application must fail over to the secondary environment ➔ Route 53

AWS Elastic Disaster Recovery (DRS)



- Used to be named "CloudEndure Disaster Recovery"
- Quickly and easily recover your physical, virtual, and cloud-based servers into AWS
- Example: protect your most critical databases (including Oracle, MySQL, and SQL Server), enterprise apps (SAP), protect your data from ransomware attacks, ...
- Continuous block-level replication for your servers



Question 203:

A company is planning a one-time migration of an on-premises MySQL database to Amazon Aurora MySQL in the us-east-1 Region. The company's current internet connection has limited bandwidth. The on-premises MySQL database is 60 TB in size. The company estimates that it will take a month to transfer the data to AWS over the current internet connection. The company needs a migration solution that will migrate the database more quickly.

Which solution will migrate the database in the LEAST amount of time?

- A. Request a 1 Gbps AWS Direct Connect connection between the on-premises data center and AWS. Use AWS Database Migration Service (AWS DMS) to migrate the on-premises MySQL database to Aurora MySQL.
- B. Use AWS DataSync with the current internet connection to accelerate the data transfer between the on-premises data center and AWS. Use AWS Application Migration Service to migrate the on-premises MySQL database to Aurora MySQL.
- C. Order an AWS Snowball Edge device. Load the data into an Amazon S3 bucket by using the S3 interface. Use AWS Database Migration Service (AWS DMS) to migrate the data from Amazon S3 to Aurora MySQL.
- D. Order an AWS Snowball device. Load the data into an Amazon S3 bucket by using the S3 Adapter for Snowball. Use AWS Application Migration Service to migrate the data from Amazon S3 to Aurora MySQL.

C

On-premises strategy with AWS

- Ability to download Amazon Linux 2 AMI as a VM (.iso format)
 - VMWare, KVM, VirtualBox (Oracle VM), Microsoft Hyper-V
- AWS Application Discovery Service
 - Gather information about your on-premises servers to plan a migration
 - Server utilization and dependency mappings
 - Track with AWS Migration Hub
- AWS Application Migration Service (MGN)
 - Replacing AWS Server Migration Services & CloudEndure Migration
 - ~~tăng dần~~
Incremental replication of on-premises live servers to AWS
 - Migrates the entire VM into AWS
- AWS Elastic Disaster Recovery (DRS)
 - Replacing CloudEndure Disaster Recovery
 - Recover on-premises workloads onto AWS
- AWS Database Migration Service (DMS)
 - replicate on-premises => AWS , AWS => AWS, AWS => on-premises
 - Works with various database technologies (Oracle, MySQL, DynamoDB, etc..)



AWS Application Discovery Service



AWS Application Migration Service



AWS Elastic Disaster Recovery



AWS Database Migration Service

C=SnowBall Edge, D=SnowBall Device. The basic difference between Snowball and Snowball Edge is the capacity they provide. Snowball provides a total of 50 TB or 80 TB, out of which 42 TB or 72 TB is available, while Amazon Snowball Edge provides 100 TB, out of which 83 TB is available. 2- C=AWS Database Migration . D=Application Migration Service, Application Migration Service simplifies, expedites, and reduces the cost of migrating and modernizing applications. Not for Database

Question 204:

A company has an application in the AWS Cloud. The application runs on a fleet of 20 Amazon EC2 instances. The EC2 instances are persistent and store data on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes.

The company must maintain backups in a separate AWS Region. The company must be able to recover the EC2 instances and their configuration within 1 business day, with loss of no more than 1 day's worth of data. The company has limited staff and needs a backup solution that optimizes operational efficiency and cost. The company already has created an AWS CloudFormation template that can deploy the required network configuration in a secondary Region.

Which solution will meet these requirements?

- A. Create a second CloudFormation template that can recreate the EC2 instances in the secondary Region. Run daily multivolume snapshots by using AWS Systems Manager Automation runbooks. Copy the snapshots to the secondary Region. In the event of a failure launch the CloudFormation templates, restore the EBS volumes from snapshots, and transfer usage to the secondary Region.
- B. Use Amazon Data Lifecycle Manager (Amazon DLM) to create daily multivolume snapshots of the EBS volumes. In the event of a failure, launch the CloudFormation template and use Amazon DLM to restore the EBS volumes and transfer usage to the secondary Region.
- C. Use AWS Backup to create a scheduled daily backup plan for the EC2 instances. Configure the backup task to copy the backups to a vault in the secondary Region. In the event of a failure, launch the CloudFormation template, restore the instance volumes and configurations from the backup vault, and transfer usage to the secondary Region.
- D. Deploy EC2 instances of the same size and configuration to the secondary Region. Configure AWS DataSync daily to copy data from the primary Region to the secondary Region. In the event of a failure, launch the CloudFormation template and transfer usage to the secondary Region.

C

Amazon Data Lifecycle Manager vs. AWS Backup

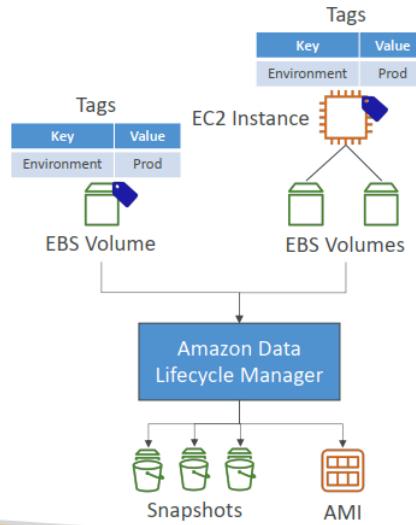
- Use Data Lifecycle Manager
 - when you want to automate the creation, retention, and deletion of EBS Snapshots
- Use AWS Backup
 - to manage and monitor backups across the AWS services you use, including EBS volumes, from a single place



Amazon Data Lifecycle Manager

- Automate the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs
- Schedule backups, cross-account snapshot copies, delete outdated backups, ...
nhận dạng
- Uses resource tags to identify the resources (EC2 instances, EBS volumes)
- Can't be used to manage snapshots/AMIs created outside DLM
- Can't be used to manage instance-store backed AMIs

Hane Maarek



Question 205:

A company is designing a new website that hosts static content. The website will give users the ability to upload and download large files. According to company requirements, all data must be encrypted in transit and at rest. A solutions architect is building the solution by using Amazon S3 and Amazon CloudFront.

Which combination of steps will meet the encryption requirements? (Choose three.)

- Turn on S3 server-side encryption for the S3 bucket that the web application uses.
- Add a policy attribute of "aws:SecureTransport": "true" for read and write operations in the S3 ACLs.
- Create a bucket policy that denies any unencrypted operations in the S3 bucket that the web application uses.
- Configure encryption at rest on CloudFront by using server-side encryption with AWS KMS keys (SSE-KMS).
- Configure redirection of HTTP requests to HTTPS requests in CloudFront.
- Use the RequireSSL option in the creation of presigned URLs for the S3 bucket that the web application uses.

A,C,E

<https://aws.amazon.com/tw/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/>

A. SSE S3 encrypt in rest data

C. Bucket Policy avoid upload unencrypted
D is incorrect because CloudFront can not using KMS

Question 206:

A company is implementing a serverless architecture by using AWS Lambda functions that need to access a Microsoft SQL Server DB instance on Amazon RDS. The company has separate environments for development and production, including a clone of the database system.

The company's developers are allowed to access the credentials for the development database. However, the credentials for the production database must be encrypted with a key that only members of the IT security team's IAM user group can access. This key must be rotated on a regular basis.

What should a solutions architect do in the production environment to meet these requirements?

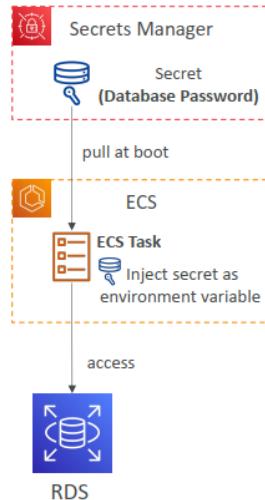
- A. Store the database credentials in AWS Systems Manager Parameter Store by using a SecureString parameter that is encrypted by an AWS Key Management Service (AWS KMS) customer managed key. Attach a role to each Lambda function to provide access to the SecureString parameter. Restrict access to the SecureString parameter and the customer managed key so that only the IT security team can access the parameter and the key.
- B. Encrypt the database credentials by using the AWS Key Management Service (AWS KMS) default Lambda key. Store the credentials in the environment variables of each Lambda function. Load the credentials from the environment variables in the Lambda code. Restrict access to the KMS key so that only the IT security team can access the key.
- C. Store the database credentials in the environment variables of each Lambda function. Encrypt the environment variables by using an AWS Key Management Service (AWS KMS) customer managed key. Restrict access to the customer managed key so that only the IT security team can access the key.
- D. Store the database credentials in AWS Secrets Manager as a secret that is associated with an AWS Key Management Service (AWS KMS) customer managed key. Attach a role to each Lambda function to provide access to the secret. Restrict access to the secret and the customer managed key so that only the IT security team can access the secret and the key.

D
Rotation = Secret Manager (and Not Parameter store)

AWS Secrets Manager



- Meant for storing secrets (e.g., passwords, API keys, ...)
- Capability to force **rotation of secrets** every X days
 - Automate generation of secrets on rotation (uses Lambda)
 - Natively supports Amazon RDS (all supported DB engines), Redshift, DocumentDB
 - Support other databases and services (custom Lambda function)
- Control access to secrets using Resource-based Policy
- Integration with other AWS services to natively pull secrets from Secrets Manager: *CloudFormation, CodeBuild, ECS, EMR, Fargate, EKS, Parameter Store...*



SSM Parameter Store vs Secrets Manager

- **Secrets Manager (\$\$\$):**
 - Automatic rotation of secrets with AWS Lambda
 - Lambda function is provided for RDS, Redshift, DocumentDB
 - KMS encryption is mandatory
 - Can integrate with CloudFormation
- **SSM Parameter Store (\$):**
 - Simple API
 - No secret rotation (can enable rotation using Lambda triggered by EventBridge)
 - KMS encryption is optional
 - Can integrate with CloudFormation
 - Can pull a Secrets Manager secret using the SSM Parameter Store API

Question 207:

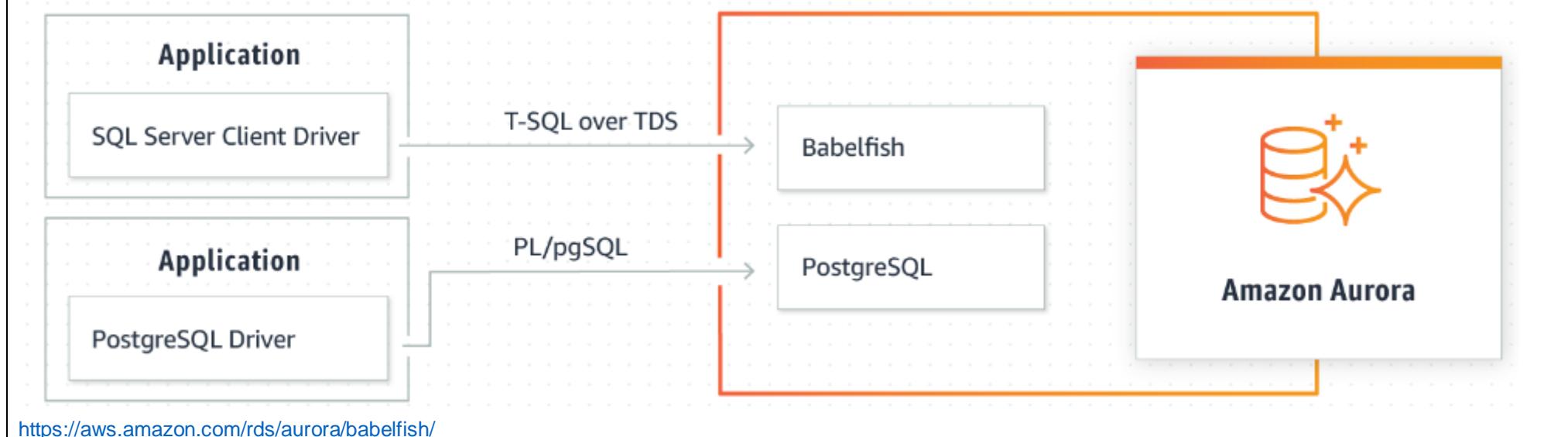
An online retail company is migrating its legacy on-premises .NET application to AWS. The application runs on load-balanced frontend web servers, load-balanced application servers, and a Microsoft SQL Server database.

The company wants to use AWS managed services where possible and does not want to rewrite the application. A solutions architect needs to implement a solution to resolve scaling issues and minimize licensing costs as the application scales.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer for the web tier and for the application tier. Use Amazon Aurora PostgreSQL with Babelfish turned on to replatform the SQL Server database.
- B. Create images of all the servers by using AWS Database Migration Service (AWS DMS). Deploy Amazon EC2 instances that are based on the on-premises imports. Deploy the instances in an Auto Scaling group behind a Network Load Balancer for the web tier and for the application tier. Use Amazon DynamoDB as the database tier.
- C. Containerize the web frontend tier and the application tier. Provision an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Create an Auto Scaling group behind a Network Load Balancer for the web tier and for the application tier. Use Amazon RDS for SQL Server to host the database.
- D. Separate the application functions into AWS Lambda functions. Use Amazon API Gateway for the web frontend tier and the application tier. Migrate the data to Amazon S3. Use Amazon Athena to query the data.

A.
load-balanced application servers and “does not want to rewrite the application” → application is hosted on the server at the on-prem → application is hosted on the EC2 instance at AWS.



Run Microsoft SQL Server applications on PostgreSQL with little to no code change

Question 208:

A software-as-a-service (SaaS) provider exposes APIs through an Application Load Balancer (ALB). The ALB connects to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that is deployed in the us-east-1 Region. The exposed APIs contain usage of a few non-standard REST methods: LINK, UNLINK, LOCK, and UNLOCK.

Users outside the United States are reporting long and inconsistent response times for these APIs. A solutions architect needs to resolve this problem with a solution that minimizes operational overhead.

Which solution meets these requirements?

- A. Add an Amazon CloudFront distribution. Configure the ALB as the origin.
- B. Add an Amazon API Gateway edge-optimized API endpoint to expose the APIs. Configure the ALB as the target.
- C. Add an accelerator in AWS Global Accelerator. Configure the ALB as the origin.
- D. Deploy the APIs to two additional AWS Regions: eu-west-1 and ap-southeast-2. Add latency-based routing records in Amazon Route 53.

C

A. Add an Amazon CloudFront distribution. Configure the ALB as the origin. CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. By configuring CloudFront with your Application Load Balancer (ALB) as the origin, users can access your API through the CloudFront edge location that's closest to them, reducing latency.

B. Amazon API Gateway, does not support non-standard REST methods.

C. AWS Global Accelerator, is a networking service that improves your applications' availability and performance, but its benefits are more noticeable for TCP/UDP-based workloads rather than HTTP(S)-based APIs.

D. deploying the APIs in multiple regions and using Amazon Route 53 latency-based routing, would require much more operational overhead compared to the recommended solution.

Question 209:

A company runs an IoT application in the AWS Cloud. The company has millions of sensors that collect data from houses in the United States. The sensors use the MQTT protocol to connect and send data to a custom MQTT broker. The MQTT broker stores the data on a single Amazon EC2 instance. The sensors connect to the broker through the domain named `iot.example.com`. The company uses Amazon Route 53 as its DNS service. The company stores the data in Amazon DynamoDB.

On several occasions, the amount of data has overloaded the MQTT broker and has resulted in lost sensor data. The company must improve the reliability of the solution.

Which solution will meet these requirements?

- A. Create an Application Load Balancer (ALB) and an Auto Scaling group for the MQTT broker. Use the Auto Scaling group as the target for the ALB. Update the DNS record in Route 53 to an alias record. Point the alias record to the ALB. Use the MQTT broker to store the data.

B. Set up AWS IoT Core to receive the sensor data. Create and configure a custom domain to connect to AWS IoT Core. Update the DNS record in Route 53 to point to the AWS IoT Core Data-ATS endpoint. Configure an AWS IoT rule to store the data.

C. Create a Network Load Balancer (NLB). Set the MQTT broker as the target. Create an AWS Global Accelerator accelerator. Set the NLB as the endpoint for the accelerator. Update the DNS record in Route 53 to a multivalue answer record. Set the Global Accelerator IP addresses as values. Use the MQTT broker to store the data.

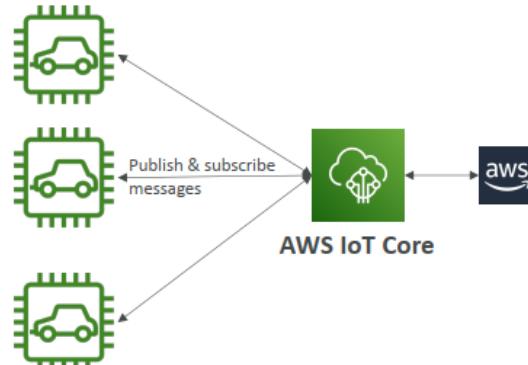
D. Set up AWS IoT Greengrass to receive the sensor data. Update the DNS record in Route 53 to point to the AWS IoT Greengrass endpoint. Configure an AWS IoT rule to invoke an AWS Lambda function to store the data.

B

AWS IoT Core



- IoT stands for “Internet of Things” – the network of internet-connected devices that are able to collect and transfer data
- AWS IoT Core allows you to easily connect IoT devices to the AWS Cloud
- Serverless, secure & scalable to billions of devices and trillions of messages
- Integrates with a lot of AWS services (Lambda, S3, SageMaker; etc.)
- Build IoT applications that gather, process, analyze, and act on data



MQTT (Message Queuing Telemetry Transport) is a lightweight, publish-subscribe messaging protocol.

Features: Primarily used in IoT and applications with low bandwidth or high latency, it ensures efficient communication between devices.

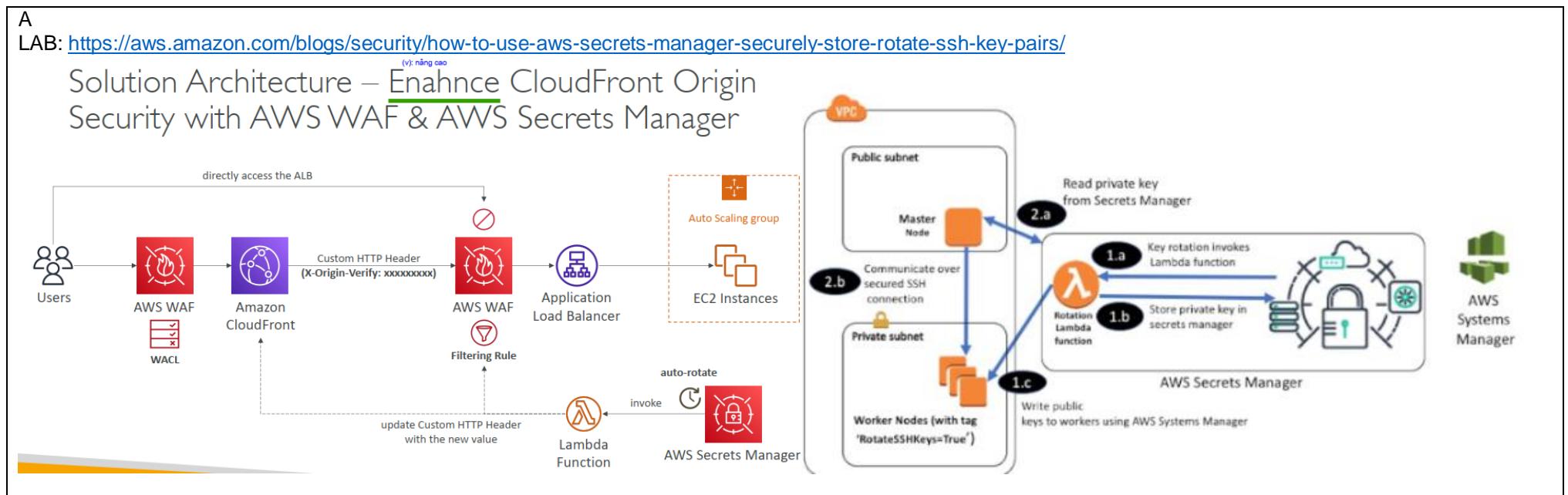
Question 210:

A company has Linux-based Amazon EC2 instances. Users must access the instances by using SSH with EC2 SSH key pairs. Each machine requires a unique EC2 key pair.

The company wants to implement a key rotation policy that will, upon request, automatically rotate all the EC2 key pairs and keep the keys in a securely encrypted place. The company will accept less than 1 minute of downtime during key rotation.

Which solution will meet these requirements?

- A. Store all the keys in AWS Secrets Manager. Define a Secrets Manager rotation schedule to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances. Update the private keys in Secrets Manager.
- B. Store all the keys in Parameter Store, a capability of AWS Systems Manager, as a string. Define a Systems Manager maintenance window to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances. Update the private keys in Parameter Store.
- C. Import the EC2 key pairs into AWS Key Management Service (AWS KMS). Configure automatic key rotation for these key pairs. Create an Amazon EventBridge scheduled rule to invoke an AWS Lambda function to initiate the key rotation in AWS KMS.
- D. Add all the EC2 instances to Fleet Manager, a capability of AWS Systems Manager. Define a Systems Manager maintenance window to issue a Systems Manager Run Command document to generate new key pairs and to rotate public keys to all the instances in Fleet Manager.



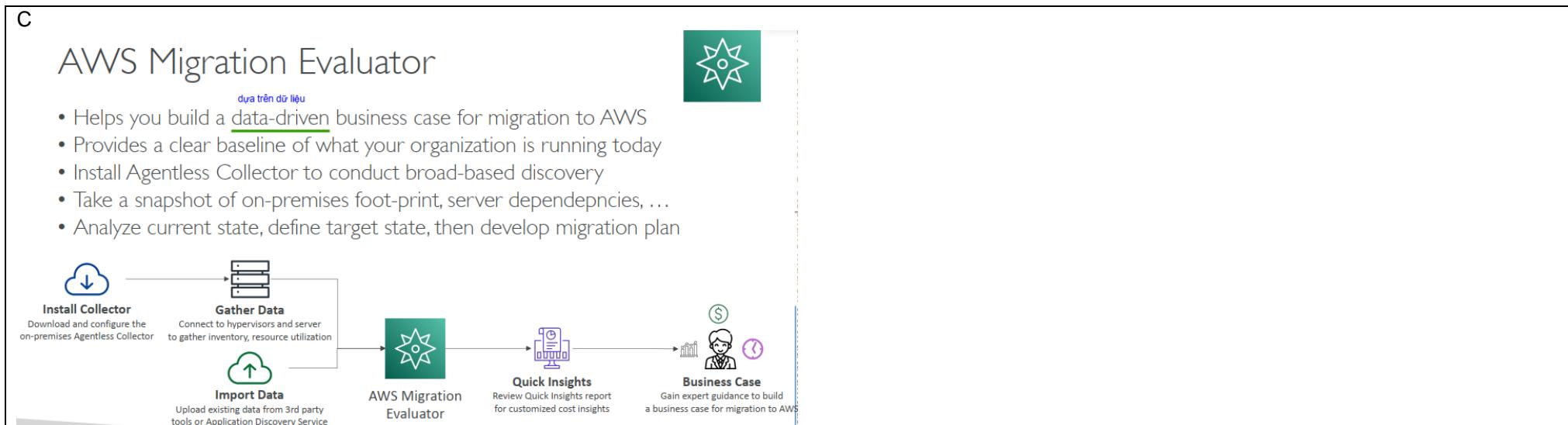
Question 211:

A company wants to migrate to AWS. The company is running thousands of VMs in a VMware ESXi environment. The company has no configuration management database and has little knowledge about the utilization of the VMware portfolio.

A solutions architect must provide the company with an accurate inventory so that the company can plan for a cost-effective migration.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Systems Manager Patch Manager to deploy Migration Evaluator to each VM. Review the collected data in Amazon QuickSight. Identify servers that have high utilization. Remove the servers that have high utilization from the migration list. Import the data to AWS Migration Hub.
- B. Export the VMware portfolio to a .csv file. Check the disk utilization for each server. Remove servers that have high utilization. Export the data to AWS Application Migration Service. Use AWS Server Migration Service (AWS SMS) to migrate the remaining servers.
- C. Deploy the Migration Evaluator agentless collector to the ESXi hypervisor. Review the collected data in Migration Evaluator. Identify inactive servers. Remove the inactive servers from the migration list. Import the data to AWS Migration Hub.
- D. Deploy the AWS Application Migration Service Agent to each VM. When the data is collected, use Amazon Redshift to import and analyze the data. Use Amazon QuickSight for data visualization.



Question 212:

A company runs a microservice as an AWS Lambda function. The microservice writes data to an on-premises SQL database that supports a limited number of concurrent connections. When the number of Lambda function invocations is too high, the database crashes and causes application downtime. The company has an AWS Direct Connect connection between the company's VPC and the on-premises data center. The company wants to protect the database from crashes.

Which solution will meet these requirements?

- A. Write the data to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda function to read from the queue and write to the existing database. Set a reserved concurrency limit on the Lambda function that is less than the number of connections that the database supports.
- B. Create a new Amazon Aurora Serverless DB cluster. Use AWS DataSync to migrate the data from the existing database to Aurora Serverless. Reconfigure the Lambda function to write to Aurora.

C. Create an Amazon RDS Proxy DB instance. Attach the RDS Proxy DB instance to the Amazon RDS DB instance. Reconfigure the Lambda function to write to the RDS Proxy DB instance.

D. Write the data to an Amazon Simple Notification Service (Amazon SNS) topic. Invoke the Lambda function to write to the existing database when the topic receives new messages. Configure provisioned concurrency for the Lambda function to be equal to the number of connections that the database supports.

A

C is incorrect because RDS Proxy is not support on-premises database.

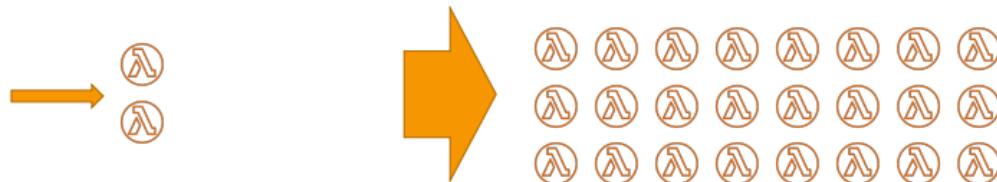
Amazon SQS



- Serverless, managed queue, integrated with IAM
- Can handle extreme scale, no provisioning required
- Used to **decouple** services
- Message size of max 256 KB (use a pointer to S3 for large messages)
- Can be read from EC2 (optional ASG), Lambda
- SQS could be used as a write buffer for DynamoDB
- **SQS FIFO:**
 - receive messages in order they were sent Nhận message theo thứ tự được gửi
 - 300 messages/s without batching, 3000 /s with batching

Lambda Concurrency and Throttling

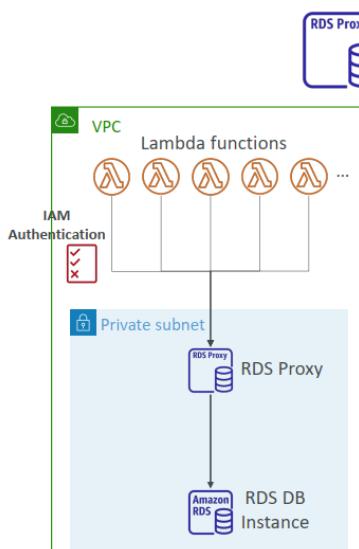
- Concurrency limit: up to 1000 concurrent executions



- Can set a “reserved concurrency” at the function level (=limit)
- Each invocation over the concurrency limit will trigger a “Throttle”
- Can request a quota increase in AWS Service Quotas

Amazon RDS Proxy

- Fully managed database proxy for RDS
- Allows apps to pool and share DB connections established with the database
- Improving database efficiency by reducing the stress on database resources (e.g., CPU, RAM) and minimize open connections (and timeouts)
- Serverless, autoscaling, highly available (multi-AZ)
- Reduced RDS & Aurora failover time by up 66%
- Supports RDS (MySQL, PostgreSQL, MariaDB, MS SQL Server) and Aurora (MySQL, PostgreSQL)
- No code changes required for most apps
- Enforce IAM Authentication for DB, and securely store credentials in AWS Secrets Manager
- RDS Proxy is never publicly accessible (must be accessed from VPC)



Question 213:

A company uses a Grafana data visualization solution that runs on a single Amazon EC2 instance to monitor the health of the company's AWS workloads. The company has invested time and effort to create dashboards that the company wants to preserve. The dashboards need to be highly available and cannot be down for longer than 10 minutes. The company needs to minimize ongoing maintenance.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Migrate to Amazon CloudWatch dashboards. Recreate the dashboards to match the existing Grafana dashboards. Use automatic dashboards where possible.
- B. Create an Amazon Managed Grafana workspace. Configure a new Amazon CloudWatch data source. Export dashboards from the existing Grafana instance. Import the dashboards into the new workspace.
- C. Create an AMI that has Grafana pre-installed. Store the existing dashboards in Amazon Elastic File System (Amazon EFS). Create an Auto Scaling group that uses the new AMI. Set the Auto Scaling group's minimum, desired, and maximum number of instances to one. Create an Application Load Balancer that serves at least two Availability Zones.
- D. Configure AWS Backup to back up the EC2 instance that runs Grafana once each hour. Restore the EC2 instance from the most recent snapshot in an alternate Availability Zone when required.

B

<https://docs.aws.amazon.com/grafana/latest/userguide/AMG-workspace-content-migration.html>

<https://github.com/aws-observability/amazon-managed-grafana-migrator>

Migrating content between workspaces

[PDF](#) | [RSS](#)

There are times that you want to migrate your content (including data sources, dashboards, folder, and alert rules) from one workspace to another. For example, you are migrating from an on-premise Grafana workspace to an Amazon Managed Grafana workspace, and you want to migrate your existing content to the new workspace.

Amazon Managed Grafana does not directly support migrating content between workspaces, however, AWS does provide an open-source migration utility that can handle this scenario by providing export and import functionality within a workspace. This utility is called the **Amazon Managed Grafana Migrator**.

For more information, see [Amazon Managed Grafana Migrator](#) on GitHub.

Question 214:

A company needs to migrate its customer transactions database from on premises to AWS. The database resides on an Oracle DB instance that runs on a Linux server. According to a new security requirement, the company must rotate the database password each year.

Which solution will meet these requirements with the LEAST operational overhead?

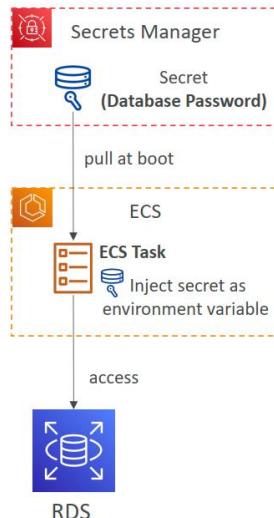
- A. Convert the database to Amazon DynamoDB by using the AWS Schema Conversion Tool (AWS SCT). Store the password in AWS Systems Manager Parameter Store. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function for yearly passtard rotation.
- B. Migrate the database to Amazon RDS for Oracle. Store the password in AWS Secrets Manager. Turn on automatic rotation. Configure a yearly rotation schedule.
- C. Migrate the database to an Amazon EC2 instance. Use AWS Systems Manager Parameter Store to keep and rotate the connection string by using an AWS Lambda function on a yearly schedule.
- D. Migrate the database to Amazon Neptune by using the AWS Schema Conversion Tool (AWS SCT). Create an Amazon CloudWatch alarm to invoke an AWS Lambda function for yearly password rotation.

B

LAB: <https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>

AWS Secrets Manager

- Meant for storing secrets (e.g., passwords, API keys, ...)
- Capability to force **rotation of secrets** every X days
 - Automate generation of secrets on rotation (uses Lambda)
 - Natively supports Amazon RDS (all supported DB engines), Redshift, DocumentDB
 - Support other databases and services (custom Lambda function)
- Control access to secrets using Resource-based Policy
- Integration with other AWS services to natively pull secrets from Secrets Manager: *CloudFormation, CodeBuild, ECS, EMR, Fargate, EKS, Parameter Store...*



Question 215:

A solutions architect is designing an AWS account structure for a company that consists of multiple teams. All the teams will work in the same AWS Region. The company needs a VPC that is connected to the on-premises network. The company expects less than 50 Mbps of total traffic to and from the on-premises network.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to each AWS account.
- B. Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to a shared services account. Share the subnets by using AWS Resource Access Manager.
- C. Use AWS Transit Gateway along with an AWS Site-to-Site VPN for connectivity to the on-premises network. Share the transit gateway by using AWS Resource Access Manager.
- D. Use AWS Site-to-Site VPN for connectivity to the on-premises network.
- E. Use AWS Direct Connect for connectivity to the on-premises network.

B,D

MOST cost-effectively → D because VPN is cheaper than DX

needs a VPC that is connected to the on-premises network → provision a VPC and share VPC's subnet with all account.

https://docs.aws.amazon.com/vpn/latest/s2vpn/VPC_VPN.html

https://aws.amazon.com/vpn/pricing/#AWS_Site-to-Site_VPN_and_Accelerated_Site-to-Site_VPN_Connection_Pricing

Question 216:

A solutions architect at a large company needs to set up network security for outbound traffic to the internet from all AWS accounts within an organization in AWS Organizations. The organization has more than 100 AWS accounts, and the accounts route to each other by using a centralized AWS Transit Gateway. Each account has both an internet gateway and a NAT gateway for outbound traffic to the internet. The company deploys resources only into a single AWS Region.

The company needs the ability to add centrally managed rule-based filtering on all outbound traffic to the internet for all AWS accounts in the organization. The peak load of outbound traffic will not exceed 25 Gbps in each Availability Zone.

Which solution meets these requirements?

- A. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Create an Auto Scaling group of Amazon EC2 instances that run an open-source internet proxy for rule-based filtering across all Availability Zones in the Region. Modify all default routes to point to the proxy's Auto Scaling group.
- B. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Use an AWS Network Firewall for rule-based filtering. Create Network Firewall endpoints in each Availability Zone. Modify all default routes to point to the Network Firewall endpoints.
- C. Create an AWS Network Firewall firewall for rule-based filtering in each AWS account. Modify all default routes to point to the Network Firewall firewalls in each account.

D. In each AWS account, create an Auto Scaling group of network-optimized Amazon EC2 instances that run an open-source internet proxy for rule-based filtering. Modify all default routes to point to the proxy's Auto Scaling group.

B

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-nat-gateway-with-firewall.html>

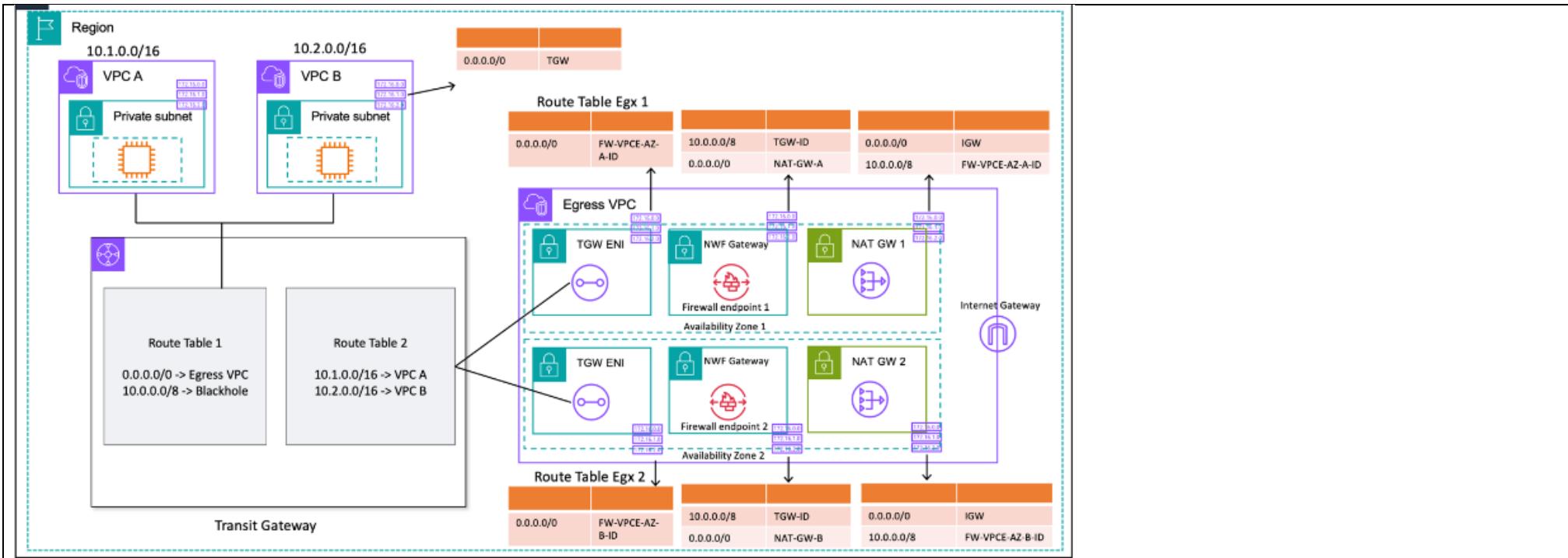
AWS Firewall Manager



- Manage rules in all accounts of an AWS Organization
- Security policy: common set of security rules
 - WAF rules (Application Load Balancer; API Gateways, CloudFront)
 - AWS Shield Advanced (ALB, CLB, NLB, Elastic IP, CloudFront)
 - Security Groups for EC2, Application Load Balancer and ENI resources in VPC
 - AWS Network Firewall (VPC Level)
 - Amazon Route 53 Resolver DNS Firewall
 - Policies are created at the region level
- Rules are applied to new resources as they are created (good for compliance) across all and future accounts in your Organization

được áp dụng với các resource mới khi chúng được tạo

||



Question 217:

A company uses a load balancer to distribute traffic to Amazon EC2 instances in a single Availability Zone. The company is concerned about security and wants a solutions architect to re-architect the solution to meet the following requirements:

- Inbound requests must be filtered for common vulnerability attacks.
- Rejected requests must be sent to a third-party auditing application.

All resources should be highly available.

Which solution meets these requirements?

- A. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Use Amazon Inspector to monitor traffic to the ALB and EC2 instances. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB. Use an AWS Lambda function to frequently push the Amazon Inspector report to the third-party auditing application.

B. Configure an Application Load Balancer (ALB) and add the EC2 instances as targets. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB name and enable logging with Amazon CloudWatch Logs. Use an AWS Lambda function to frequently push the logs to the third-party auditing application.

C. Configure an Application Load Balancer (ALB) along with a target group adding the EC2 instances as targets. Create an Amazon Kinesis Data Firehose with the destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

D. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Create an Amazon Kinesis Data Firehose with a destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the WebACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

D

Amazon inspector does NOT inspect traffic coming to an Application Load Balancer (ALB)

D is correct answer Inbound requests must be filtered for common vulnerability attacks -> WAF Rejected requests must be sent to a third-party auditing application-> Enable access log and use kinesis stream to send logs to third party All resources should be highly available -> Muti AZ auto scaling group.

Amazon Inspector

dánh giá bảo mật tự động

- Automated Security Assessments

- For EC2 instances

- Leveraging the AWS System Manager (SSM) agent
- Analyze against unintended network accessibility
- Analyze the running OS against known vulnerabilities

phân tích khả năng truy cập
mạng ngoài ý muốn

phân tích hệ điều đang
chạy dựa trên lỗ hổng
đã biết

- For Container Images push to Amazon ECR

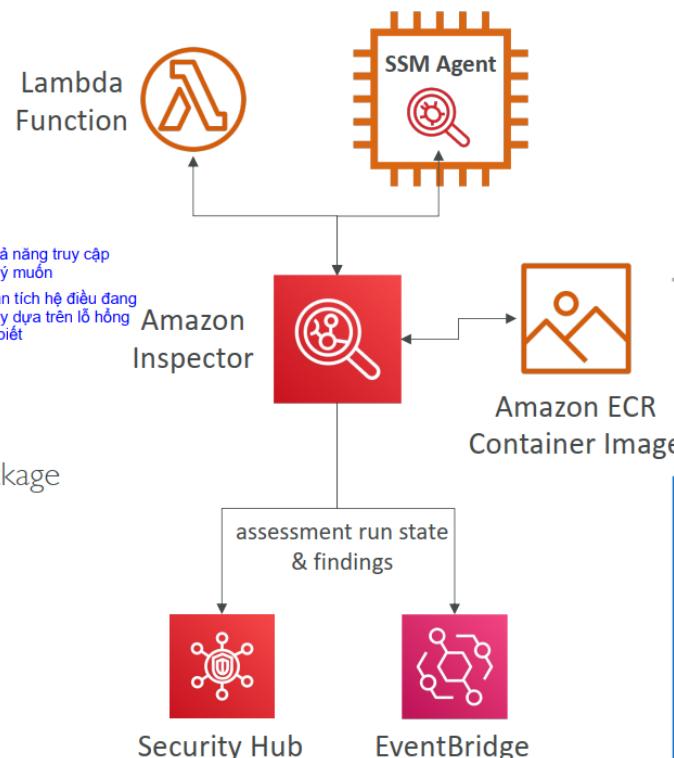
- Assessment of Container Images as they are pushed

- For Lambda Functions

- Identifies software vulnerabilities in function code and package dependencies
- Assessment of functions as they are deployed

- Reporting & integration with AWS Security Hub

- Send findings to Amazon Event Bridge



Question 218:

A company is running an application in the AWS Cloud. The application consists of microservices that run on a fleet of Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer. The company recently added a new REST API that was implemented in Amazon API Gateway. Some of the older microservices that run on EC2 instances need to call this new API.

The company does not want the API to be accessible from the public internet and does not want proprietary data to traverse the public internet.

What should a solutions architect do to meet these requirements?

- A. Create an AWS Site-to-Site VPN connection between the VPC and the API Gateway. Use API Gateway to generate a unique API Key for each microservice. Configure the API methods to require the key.
- B. Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API. Add a resource policy to API Gateway to only allow access from the VPC endpoint. Change the API Gateway endpoint type to private.
- C. Modify the API Gateway to use IAM authentication. Update the IAM policy for the IAM role that is assigned to the EC2 instances to allow access to the API Gateway. Move the API Gateway into a new VPDeploy a transit gateway and connect the VPCs.
- D. Create an accelerator in AWS Global Accelerator, and connect the accelerator to the API Gateway. Update the route table for all VPC subnets with a route to the created Global Accelerator endpoint IP address. Add an API key for each service to use for authentication.

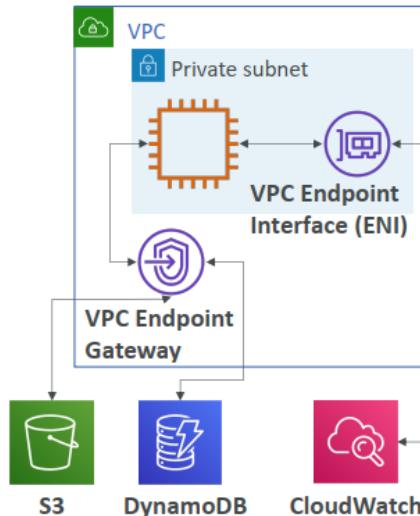
B

API Gateway - Endpoint Types

- Edge-Optimized (default): For global clients
 - Requests are routed through the CloudFront Edge locations (improves latency)
 - The API Gateway still lives in only one region
- Regional:
 - For clients within the same region
 - Could manually combine with CloudFront (more control over the caching strategies and the distribution)
- Private:
 - Can only be accessed from your VPC using an interface VPC endpoint (ENI)
 - Use a resource policy to define access

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables



Question 219:

A company has set up its entire infrastructure on AWS. The company uses Amazon EC2 instances to host its ecommerce website and uses Amazon S3 to store static data. Three engineers at the company handle the cloud administration and development through one AWS account. Occasionally, an engineer alters an EC2 security group configuration of another engineer and causes noncompliance issues in the environment.

A solutions architect must set up a system that tracks changes that the engineers make. The system must send alerts when the engineers make noncompliant changes to the security settings for the EC2 instances.

What is the FASTEST way for the solutions architect to meet these requirements?

- Set up AWS Organizations for the company. Apply SCPs to govern and track noncompliant security group changes that are made to the AWS account.
- Enable AWS CloudTrail to capture the changes to EC2 security groups. Enable Amazon CloudWatch rules to provide alerts when noncompliant security settings are detected.
- Enable SCPs on the AWS account to provide alerts when noncompliant security group changes are made to the environment.
- Enable AWS Config on the EC2 security groups to track any noncompliant changes. Send the changes as alerts through an Amazon Simple Notification Service (Amazon SNS) topic.

D

send alerts when the engineers make noncompliant changes to the security settings for the EC2 instances → SNS

AWS Config



- Helps with auditing and recording **compliance** of your AWS resources
- Helps record configurations and changes over time
- AWS Config Rules does not prevent actions from happening (no deny)
Không ngăn chặn các hành động xảy ra
- Questions that can be solved by AWS Config:
 - Is there unrestricted SSH access to my security groups?
 - Do my buckets have any public access?
 - How has my ALB configuration changed over time?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per-region service
- Can be aggregated across regions and accounts
tổng hợp

Question 220:

A company has IoT sensors that monitor traffic patterns throughout a large city. The company wants to read and collect data from the sensors and perform aggregations on the data.

A solutions architect designs a solution in which the IoT devices are streaming to Amazon Kinesis Data Streams. Several applications are reading from the stream. However, several consumers are experiencing throttling and are periodically encountering a ReadProvisionedThroughputExceeded error.

Which actions should the solutions architect take to resolve this issue? (Choose three.)

- Reshard the stream to increase the number of shards in the stream.
- Use the Kinesis Producer Library (KPL). Adjust the polling frequency.
- Use consumers with the enhanced fan-out feature.
- Reshard the stream to reduce the number of shards in the stream.
- Use an error retry and exponential backoff mechanism in the consumer logic.

F. Configure the stream to use dynamic partitioning.

A,C,E

To resolve the issue of throttling and ReadProvisionedThroughputExceeded errors in the Amazon Kinesis Data Streams scenario, the solutions architect should take the following actions:

1. A. Reshard the stream to increase the number of shards in the stream: By increasing the number of shards, you can increase the overall throughput capacity of the stream, allowing for more concurrent consumers to read from the stream without being throttled.
2. C. Use consumers with the enhanced fan-out feature: Enhanced fan-out allows for multiple consumers to read from the same shard concurrently, without being limited by the read capacity of the shard. This helps distribute the load and reduces the chances of throttling.
3. E. Use an error retry and exponential backoff mechanism in the consumer logic: Implementing an error retry mechanism with exponential backoff in the consumer logic will help handle throttling errors gracefully. When a ReadProvisionedThroughputExceeded error occurs, the consumer can retry the read operation after a certain delay, gradually increasing the delay between retries to avoid overwhelming the system.

AWS Kinesis Overview

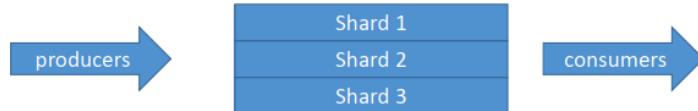


- Kinesis is a managed “data streaming” service
- Great for application logs, metrics, IoT, clickstreams
- Great for “real-time” big data
- Great for streaming processing frameworks (Spark, NiFi, etc...)
- Data is automatically replicated synchronously to 3 AZ

- Kinesis Streams: low latency streaming ingest at scale
- Kinesis Analytics: perform real-time analytics on streams using SQL
- Kinesis Firehose: load streams into S3, Redshift, ElasticSearch & Splunk

Kinesis Streams Overview

- Streams are divided in ordered Shards / Partitions



- Data retention is 24 hours by default, can go up to 365 days
- Ability to reprocess / replay data
Nhiều ứng dụng có thể sử dụng cùng 1 luồng
- Multiple applications can consume the same stream
- Real-time processing with scale of throughput
- Once data is inserted in Kinesis, it can't be deleted (immutability)

Kinesis Producers & Consumers

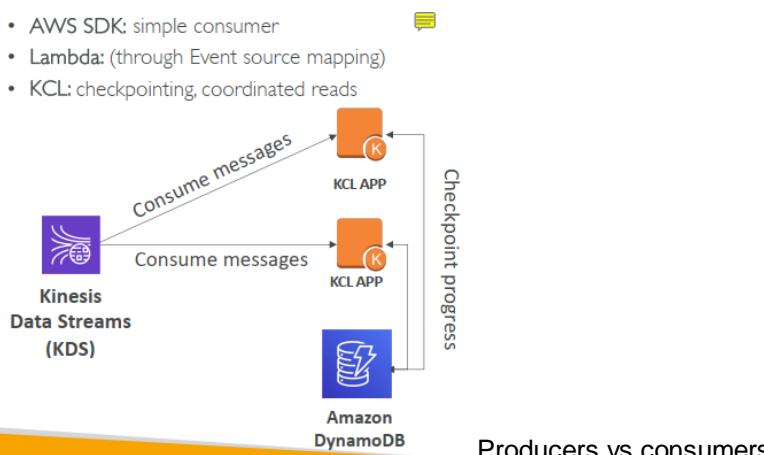
KINESIS PRODUCERS

- AWS SDK: simple producer
- Kinesis Producer Library (KPL):** batch, compression, retries, C++, Java
- Kinesis Agent:
 - Monitor log files and sends them to Kinesis directly
 - can write to Kinesis Data Streams AND Kinesis Data Firehose

Stephane Maarek

KINESIS CONSUMERS

- AWS SDK: simple consumer
- Lambda: (through Event source mapping)
- KCL: checkpointing, coordinated reads



Kinesis Streams Shards

- Two modes for capacity:
 - On-demand: no capacity planning, Kinesis scales shards automatically
 - Provisioned: you manage the shards over time
- Batching available or per message calls.
- The number of shards can evolve over time (reshard / merge)
- Records are ordered per shard
Số lượng phân đoạn có thể phát triển theo thời gian
Các bản ghi được sắp xếp theo từng phân đoạn



Kinesis Data Streams Limits to know

- Producer:
 - 1MB/s or 1000 messages/s at write PER SHARD
 - “ProvisionedThroughputException” otherwise
- Consumer Classic:
 - 2MB/s at read PER SHARD across all consumers
 - 5 API calls per second PER SHARD across all consumers
- Consumer Enhanced Fan-Out:
 - 2MB/s at read PER SHARD, PER ENHANCED CONSUMER
 - No API calls needed (push model)
- Data Retention:
 - 24 hours data retention by default
 - Can be extended to 365 days

Question 221:

A company uses AWS Organizations to manage its AWS accounts. The company needs a list of all its Amazon EC2 instances that have underutilized CPU or memory usage. The company also needs recommendations for how to downsize these underutilized instances.

Which solution will meet these requirements with the LEAST effort?

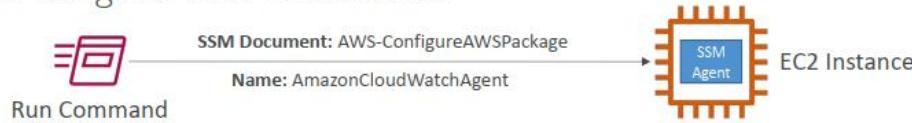
- A. Install a CPU and memory monitoring tool from AWS Marketplace on all the EC2 instances. Store the findings in Amazon S3. Implement a Python script to identify underutilized instances. Reference EC2 instance pricing information for recommendations about downsizing options.
- B. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in the organization's management account. Use the recommendations to downsize underutilized instances in all accounts of the organization.
- C. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in each account of the organization. Use the recommendations to downsize underutilized instances in all accounts of the organization.
- D. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Create an AWS Lambda function to extract CPU and memory usage from all the EC2 instances. Store the findings as files in Amazon S3. Use Amazon Athena to find underutilized instances. Reference EC2 instance pricing information for recommendations about downsizing options.

B

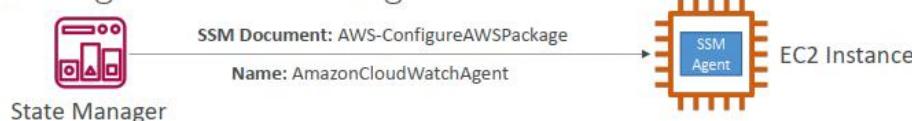
Install the Amazon CloudWatch agent on all the EC2 instances using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in the organization's management account. Use the recommendations to downsize underutilized instances in all accounts of the organization. This solution leverages the capabilities of AWS CloudWatch and AWS Cost Explorer to monitor and analyze the CPU and memory usage of EC2 instances. By installing the CloudWatch agent, you can collect the necessary metrics for monitoring. AWS Cost Explorer provides resource optimization recommendations, which can be accessed from the organization's management account. These recommendations can then be used to identify underutilized instances and make informed decisions about downsizing. This solution requires minimal effort as it utilizes existing AWS services and tools, eliminating the need for additional installations or custom scripts. It also provides a centralized approach by retrieving recommendations from the organization's management account, allowing for efficient management of all accounts within the organization.

CloudWatch Agent – Integration with SSM

- Install CW Agent using SSM Run Command



- Install CW Agent using SSM State Manager



- Configure CW Agent by storing config. in SSM Parameter Store



Cost Explorer



- Visualize, understand, and manage your AWS costs and usage over time
- Create custom reports that analyze cost and usage data.
- Analyze your data at a high level: total costs and **usage across all accounts**
- Or Monthly, hourly, resource level granularity
- Choose an optimal **Savings Plan** (to lower prices on your bill)
- Forecast usage up to 12 months based on previous usage

Question 222:

A company wants to run a custom network analysis software package to inspect traffic as traffic leaves and enters a VPC. The company has deployed the solution by using AWS CloudFormation on three Amazon EC2 instances in an Auto Scaling group. All network routing has been established to direct traffic to the EC2 instances.

Whenever the analysis software stops working, the Auto Scaling group replaces an instance. The network routes are not updated when the instance replacement occurs.

Which combination of steps will resolve this issue? (Choose three.)

- Create alarms based on EC2 status check metrics that will cause the Auto Scaling group to replace the failed instance.
- Update the CloudFormation template to install the Amazon CloudWatch agent on the EC2 instances. Configure the CloudWatch agent to send process metrics for the application.
- Update the CloudFormation template to install AWS Systems Manager Agent on the EC2 instances. Configure Systems Manager Agent to send process metrics for the application.
- Create an alarm for the custom metric in Amazon CloudWatch for the failure scenarios. Configure the alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
- Create an AWS Lambda function that responds to the Amazon Simple Notification Service (Amazon SNS) message to take the instance out of service. Update the network routes to point to the replacement instance.
- In the CloudFormation template, write a condition that updates the network routes when a replacement instance is launched.

B,D,E

a custom network analysis software package to inspect traffic as traffic leaves and enters a VPC → CloudWatch → CloudWatch agent + custom metric
The network routes are not updated when the instance replacement occurs. → Create an AWS Lambda function that responds to the Amazon Simple Notification Service (Amazon SNS) message to take the instance out of service. Update the network routes to point to the replacement instance.

Question 223:

A company is developing a new on-demand video application that is based on microservices. The application will have 5 million users at launch and will have 30 million users after 6 months. The company has deployed the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. The company developed the application by using ECS services that use the HTTPS protocol.

A solutions architect needs to implement updates to the application by using blue/green deployments. The solution must distribute traffic to each ECS service through a load balancer. The application must automatically adjust the number of tasks in response to an Amazon CloudWatch alarm.

Which solution will meet these requirements?

- A. Configure the ECS services to use the blue/green deployment type and a Network Load Balancer. Request increases to the service quota for tasks per service to meet the demand.
- B. Configure the ECS services to use the blue/green deployment type and a Network Load Balancer. Implement Auto Scaling group for each ECS service by using the Cluster Autoscaler.
- C. Configure the ECS services to use the blue/green deployment type and an Application Load Balancer. Implement an Auto Scaling group for each ECS service by using the Cluster Autoscaler.
- D. Configure the ECS services to use the blue/green deployment type and an Application Load Balancer. Implement Service Auto Scaling for each ECS service.

D

<https://repost.aws/knowledge-center/ecs-fargate-service-auto-scaling>

Amazon ECS – Service Auto Scaling



- Automatically increase/decrease the desired number of tasks
- Amazon ECS leverages AWS Application Auto Scaling
- CPU and RAM is tracked in CloudWatch at the ECS Service level
- Target Tracking – scale based on target value for a specific CloudWatch metric
- Step Scaling – scale based on a specified CloudWatch Alarm
- Scheduled Scaling – scale based on a specified date/time (predictable changes)
- **ECS Service Auto Scaling (task level) ≠ EC2 Auto Scaling (EC2 instance level)**
- Fargate Auto Scaling is much easier to setup (because Serverless)

Question 224:

A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.

The company uses Amazon Elastic Container Registry (Amazon ECR) to store its container images. When a new image version is uploaded, the new image version receives a unique tag.

The company needs a solution that inspects new image versions for common vulnerabilities and exposures. The solution must automatically delete new image tags that have Critical or High severity findings. The solution also must notify the development team when such a deletion occurs.

Which solution meets these requirements?

- A. Configure scan on push on the repository. Use Amazon EventBridge to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity findings. Use the Step Functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service (Amazon SNS).
- B. Configure scan on push on the repository. Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Lambda function when a new message is added to the SQS queue. Use the Lambda function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).

C. Schedule an AWS Lambda function to start a manual image scan every hour. Configure Amazon EventBridge to invoke another Lambda function when a scan is complete. Use the second Lambda function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).

D. Configure periodic image scan on the repository. Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Step Functions state machine when a new message is added to the SQS queue. Use the Step Functions state machine to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).

A

notify the development team → Amazon SNS → A or C, C is incorrect because no automation (Schedule an AWS Lambda function to start a manual image scan every hour)

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/ecr-eventbridge.html>

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html>

Amazon ECR events and EventBridge

[PDF](#) | [RSS](#)

Amazon EventBridge enables you to automate your AWS services and to respond automatically to system events such as application availability issues or resource changes. Events from AWS services are delivered to EventBridge in near real time.

You can write simple rules to indicate which events are of interest to you and include automated actions to take when an event matches a rule. The actions that can be automatically triggered include the following:

- Adding events to log groups in CloudWatch Logs
- Invoking an AWS Lambda function
- Invoking Amazon EC2 Run Command
- Relaying the event to Amazon Kinesis Data Streams
- Activating an AWS Step Functions state machine
- Notifying an Amazon SNS topic or an Amazon SQS queue

For more information, see [Getting Started with Amazon EventBridge](#) in the [Amazon EventBridge User Guide](#).

Question 225:

A company runs many workloads on AWS and uses AWS Organizations to manage its accounts. The workloads are hosted on Amazon EC2, AWS Fargate, and AWS Lambda. Some of the workloads have unpredictable demand. Accounts record high usage in some months and low usage in other months.

The company wants to optimize its compute costs over the next 3 years. A solutions architect obtains a 6-month average for each of the accounts across the organization to calculate usage.

Which solution will provide the MOST cost savings for all the organization's compute usage?

- A. Purchase Reserved Instances for the organization to match the size and number of the most common EC2 instances from the member accounts.
- B. Purchase a Compute Savings Plan for the organization from the management account by using the recommendation at the management account level.
- C. Purchase Reserved Instances for each member account that had high EC2 usage according to the data from the last 6 months.
- D. Purchase an EC2 Instance Savings Plan for each member account from the management account based on EC2 usage data from the last 6 months.

B

- A. Incorrect: RI's Supports only EC2 instances.
- B. Correct: Compute savings plan supports EC2, Fargate and Lambda. Applied in Organization's management account.
- C. Incorrect: RI's Supports only EC2 instances and Changes to be applied at Organizations management account.
- D. Incorrect: Instance Saving plan supports only EC2.

AWS Savings Plan



- New pricing model to get a discount based on long-term usage
Cam kết sử dụng 1 loại
- Commit to a certain type of usage: ex \$10 per hour for 1 to 3 years
- Any usage beyond the savings plan is billed at the on-demand price
- **EC2 Instance Savings plan** (up to 72% - same discount as Standard RIs)
 - Select instance family (e.g. M5, C5...), and locked to a specific region
 - Flexible across size (m5.large to m5.4xlarge), OS (Windows to Linux), *thuê* *tenancy* (dedicated or default)
- **Compute Savings plan** (up to 66% - same discount as Convertible RIs)
 - Ability to move between instance family (move from C5 to M5), region (Ireland to US), compute type (**EC2, Fargate, Lambda**), OS & tenancy
- **SageMaker Savings plan** (up to 64% off)

Question 226:

A company has hundreds of AWS accounts. The company uses an organization in AWS Organizations to manage all the accounts. The company has turned on all features.

A finance team has allocated a daily budget for AWS costs. The finance team must receive an email notification if the organization's AWS costs exceed 80% of the allocated budget. A solutions architect needs to implement a solution to track the costs and deliver the notifications.

Which solution will meet these requirements?

- A. In the organization's management account, use AWS Budgets to create a budget that has a daily period. Add an alert threshold and set the value to 80%. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.
- B. In the organization's management account, set up the organizational view feature for AWS Trusted Advisor. Create an organizational view report for cost optimization. Set an alert threshold of 80%. Configure notification preferences. Add the email addresses of the finance team.
- C. Register the organization with AWS Control Tower. Activate the optional cost control (guardrail). Set a control (guardrail) parameter of 80%. Configure control (guardrail) notification preferences. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.
- D. Configure the member accounts to save a daily AWS Cost and Usage Report to an Amazon S3 bucket in the organization's management account. Use Amazon EventBridge to schedule a daily Amazon Athena query to calculate the organization's costs. Configure Athena to send an Amazon CloudWatch alert if the total costs are more than 80% of the allocated budget. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.

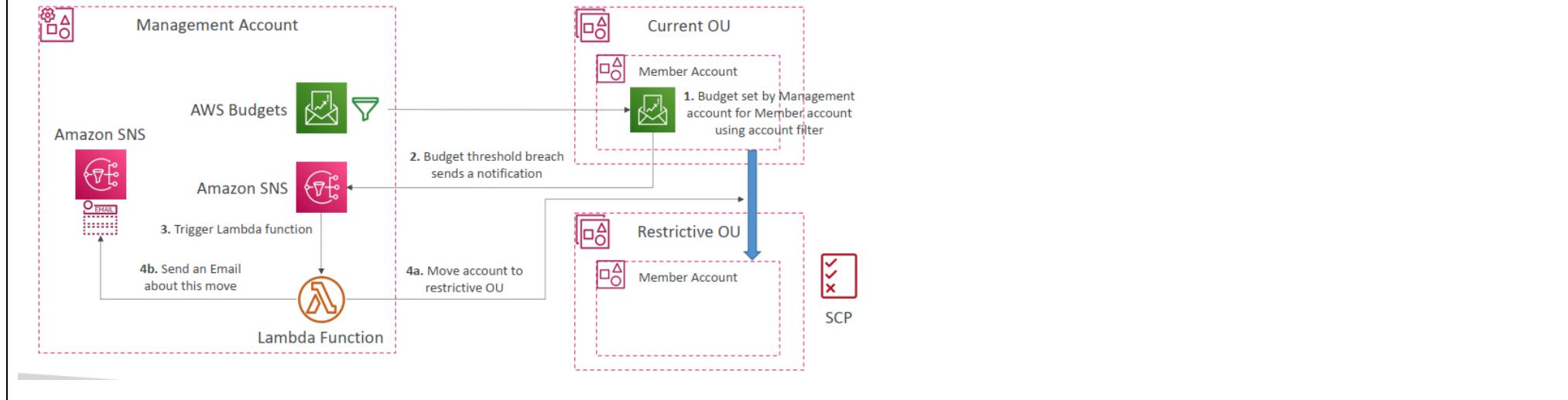
A

AWS Budgets



- Create budget and send alarms when costs exceeds the budget
- 4 types of budgets: Usage, Cost, Reservation, Savings Plans
- For Reserved Instances (RI)
 - Track utilization
 - Supports EC2, ElastiCache, RDS, Redshift
- Up to 5 SNS notifications per budget
- Can filter by: Service, Linked Account, Tag, Purchase Option, Instance Type, Region, Availability Zone, API Operation, etc...
- Same options as AWS Cost Explorer!
- 2 budgets are free, then \$0.02/day/budget

Centralized Budget Management



Question 227:

A company provides auction services for artwork and has users across North America and Europe. The company hosts its application in Amazon EC2 instances in the us-east-1 Region. Artists upload photos of their work as large-size, high-resolution image files from their mobile phones to a centralized Amazon S3 bucket created in the us-east-1 Region. The users in Europe are reporting slow performance for their image uploads.

How can a solutions architect improve the performance of the image upload process?

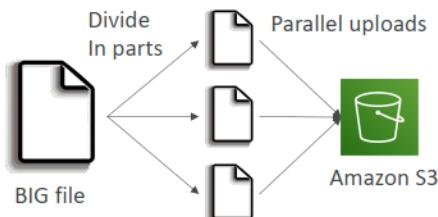
- A. Redeploy the application to use S3 multipart uploads.
- B. Create an Amazon CloudFront distribution and point to the application as a custom origin.
- C. Configure the buckets to use S3 Transfer Acceleration.
- D. Create an Auto Scaling group for the EC2 instances and create a scaling policy.

C

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

S3 Performance

- Multi-Part upload:
 - recommended for files > 100MB, must use for files > 5GB
 - Can help parallelize uploads (speed up transfers)



- S3 Transfer Acceleration
 - Increase transfer speed by transferring file to an AWS edge location which will forward the data to the S3 bucket in the target region
 - Compatible with multi-part upload



Question 228:

A company wants to containerize a multi-tier web application and move the application from an on-premises data center to AWS. The application includes web, application, and database tiers. The company needs to make the application fault tolerant and scalable. Some frequently accessed data must always be available across application servers. Frontend web servers need session persistence and must scale to meet increases in traffic.

Which solution will meet these requirements with the LEAST ongoing operational overhead?

- Run the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Use Amazon Elastic File System (Amazon EFS) for data that is frequently accessed between the web and application tiers. Store the frontend web server session data in Amazon Simple Queue Service (Amazon SQS).
- Run the application on Amazon Elastic Container Service (Amazon ECS) on Amazon EC2. Use Amazon ElastiCache for Redis to cache frontend web server session data. Use Amazon Elastic Block Store (Amazon EBS) with Multi-Attach on EC2 instances that are distributed across multiple Availability Zones.
- Run the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node groups. Use ReplicaSets to run the web servers and applications. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system across all EKS pods to store frontend web server session data.
- Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node groups. Run the web servers and application as Kubernetes deployments in the EKS cluster. Store the frontend web server session data in an Amazon DynamoDB table. Create an Amazon Elastic File System (Amazon EFS) volume that all applications will mount at the time of deployment.

D

A is incorrect ➔ “Store the frontend web server session data in Amazon Simple Queue Service (Amazon SQS)”

Question 229:

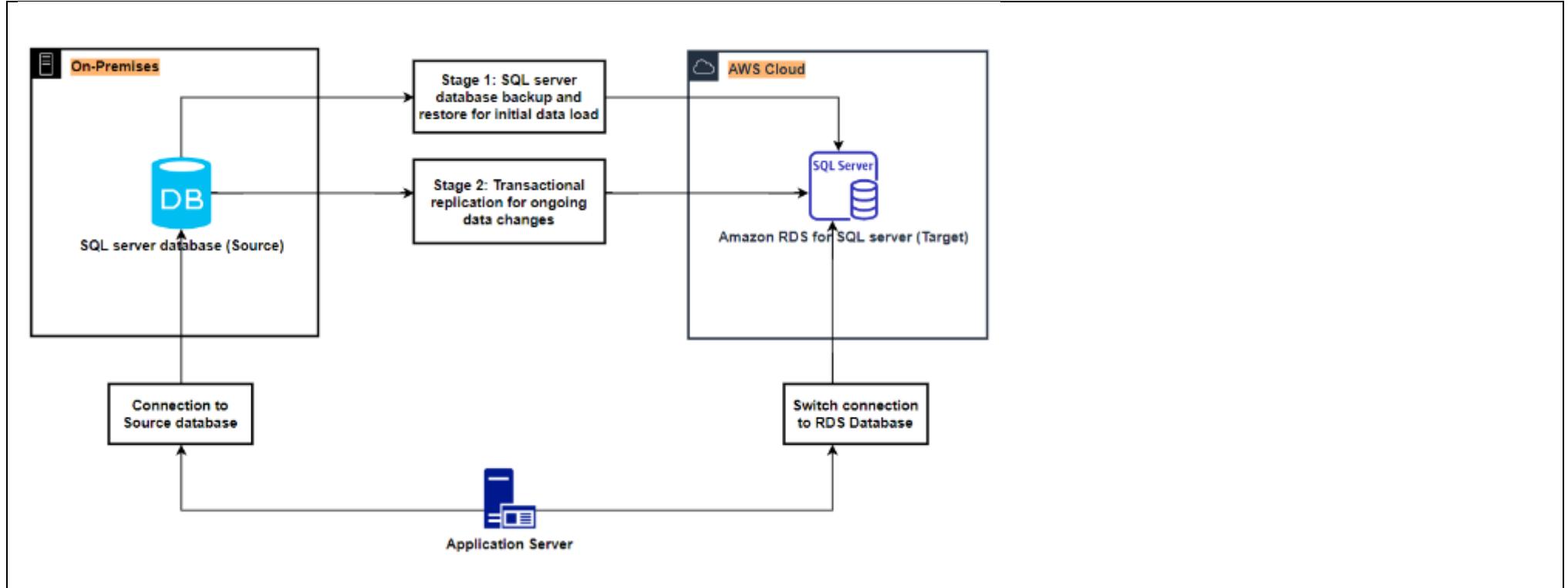
A solutions architect is planning to migrate critical Microsoft SQL Server databases to AWS. Because the databases are legacy systems, the solutions architect will move the databases to a modern data architecture. The solutions architect must migrate the databases with near-zero downtime.

Which solution will meet these requirements?

- A. Use AWS Application Migration Service and the AWS Schema Conversion Tool (AWS SCT). Perform an in-place upgrade before the migration. Export the migrated data to Amazon Aurora Serverless after cutover. Repoint the applications to Amazon Aurora.
- B. Use AWS Database Migration Service (AWS DMS) to rehost the database. Set Amazon S3 as a target. Set up change data capture (CDC) replication. When the source and destination are fully synchronized, load the data from Amazon S3 into an Amazon RDS for Microsoft SQL Server DB instance.
- C. Use native database high availability tools. Connect the source system to an Amazon RDS for Microsoft SQL Server DB instance. Configure replication accordingly. When data replication is finished, transition the workload to an Amazon RDS for Microsoft SQL Server DB instance.
- D. Use AWS Application Migration Service. Rehost the database server on Amazon EC2. When data replication is finished, detach the database and move the database to an Amazon RDS for Microsoft SQL Server DB instance. Reattach the database and then cut over all networking.

C

<https://aws.amazon.com/blogs/database/part-3-migrating-to-amazon-rds-for-sql-server-using-transactional-replication-with-native-backup-and-restore/>
<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-sql-server-to-aws-using-distributed-availability-groups.html>



Question 230:

A company's solutions architect is analyzing costs of a multi-application environment. The environment is deployed across multiple Availability Zones in a single AWS Region. After a recent acquisition, the company manages two organizations in AWS Organizations. The company has created multiple service provider applications as AWS PrivateLink-powered VPC endpoint services in one organization. The company has created multiple service consumer applications in the other organization.

Data transfer charges are much higher than the company expected, and the solutions architect needs to reduce the costs. The solutions architect must recommend guidelines for developers to follow when they deploy services. These guidelines must minimize data transfer charges for the whole environment.

Which guidelines meet these requirements? (Choose two.)

- Use AWS Resource Access Manager to share the subnets that host the service provider applications with other accounts in the organization.
- Place the service provider applications and the service consumer applications in AWS accounts in the same organization.
- Turn off cross-zone load balancing for the Network Load Balancer in all service provider application deployments.

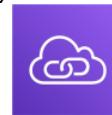
D. Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name.

E. Create a Savings Plan that provides adequate coverage for the organization's planned inter-Availability Zone data transfer usage.

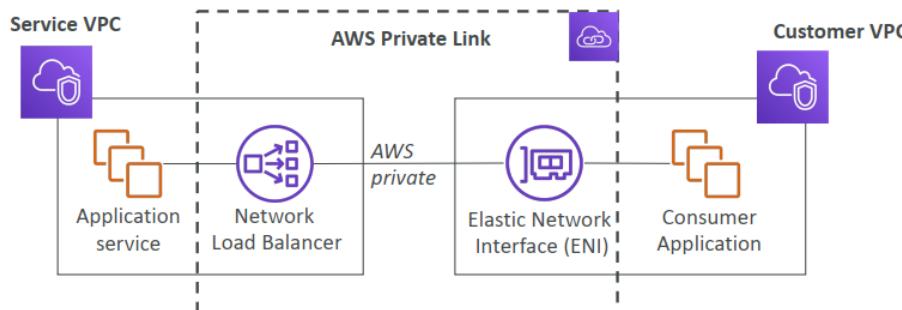
B,D

Answers: B and D Not C, this is compromising on the application's high availability. A - RAM cannot share resources across orgs E - not a relevant answer

AWS PrivateLink (VPC Endpoint Services)



- Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts)
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)
- If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!



Question 231:

A company has an on-premises Microsoft SQL Server database that writes a nightly 200 GB export to a local drive. The company wants to move the backups to more robust cloud storage on Amazon S3. The company has set up a 10 Gbps AWS Direct Connect connection between the on-premises data center and AWS.

Which solution meets these requirements MOST cost-effectively?

- Create a new S3 bucket. Deploy an AWS Storage Gateway file gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share.
- Create an Amazon FSx for Windows File Server Single-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.
- Create an Amazon FSx for Windows File Server Multi-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.

D. Create a new S3 bucket. Deploy an AWS Storage Gateway volume gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share on the volume gateway, and automate copies of this data to an S3 bucket.

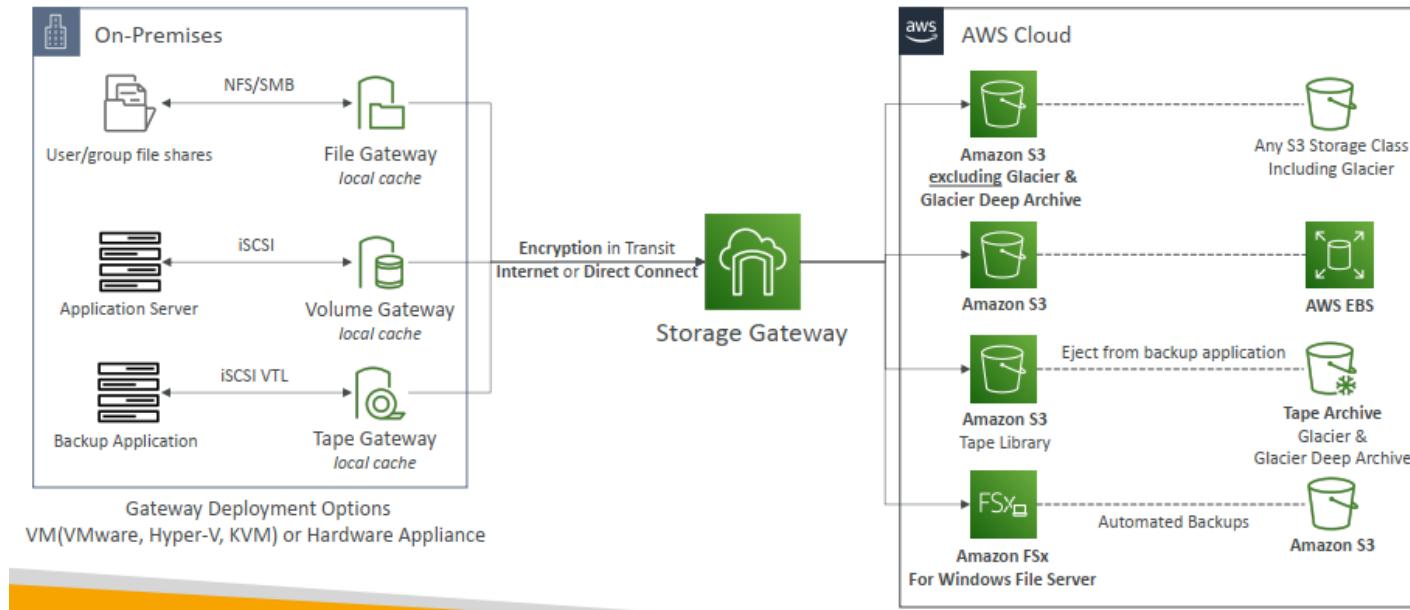
A.

Storage on S3 → AWS Storage Gateway

File Gateway == SMB , NFS Volumes Gateway == iSCSI Tape Gateway = VTL

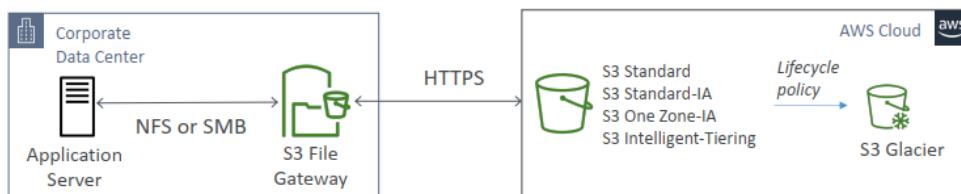
<https://aws.amazon.com/storagegateway/features/>

AWS Storage Gateway



Amazon S3 File Gateway

- Configured S3 buckets are accessible using the NFS and SMB protocol
- Most recently used data is cached in the file gateway
- Supports S3 Standard, S3 Standard IA, S3 One Zone A, S3 Intelligent Tiering
- Transition to S3 Glacier using a Lifecycle Policy
- Bucket access using IAM roles for each File Gateway
- SMB Protocol has integration with Active Directory (AD) for user authentication



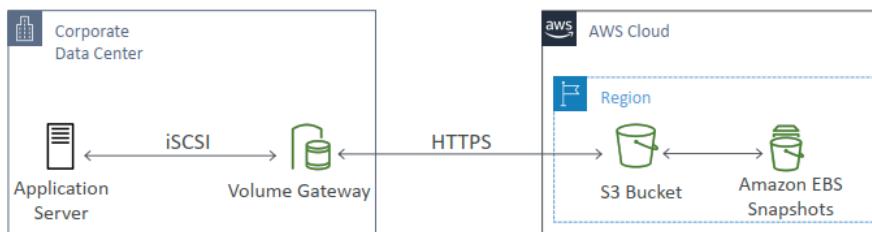
Amazon FSx File Gateway

- Native access to Amazon FSx for Windows File Server
- Local cache for frequently accessed data
- Windows native compatibility (SMB, NTFS, Active Directory...)
- Useful for group file shares and home directories



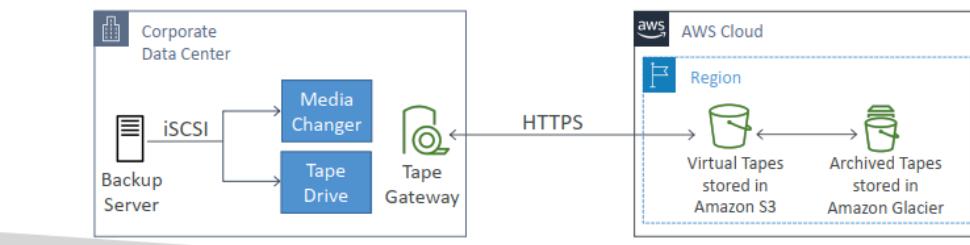
Volume Gateway

- Block storage using iSCSI protocol backed by S3
- Backed by EBS snapshots which can help restore on-premises volumes!
- **Cached volumes:** low latency access to most recent data
- **Stored volumes:** entire dataset is on premise, scheduled backups to S3



Tape Gateway

- Some companies have backup processes using physical tapes (!)
- With Tape Gateway, companies use the same processes but, in the cloud
- Virtual Tape Library (VTL) backed by Amazon S3 and Glacier
- Back up data using existing tape-based processes (and iSCSI interface)
- Works with leading backup software vendors



Question 232:

A company needs to establish a connection from its on-premises data center to AWS. The company needs to connect all of its VPCs that are located in different AWS Regions with transitive routing capabilities between VPC networks. The company also must reduce network outbound traffic costs, increase bandwidth throughput, and provide a consistent network experience for end users.

Which solution will meet these requirements?

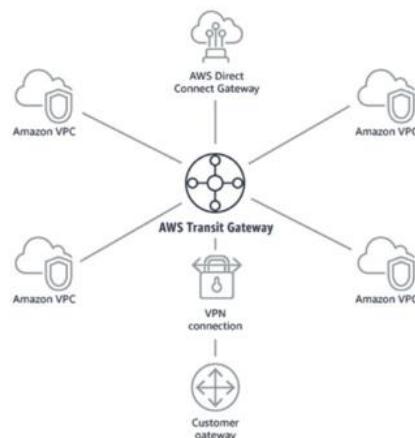
- A. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VPC. Create VPC peering connections that initiate from the central VPC to all other VPCs.
- B. Create an AWS Direct Connect connection between the on-premises data center and AWS. Provision a transit VIF, and connect it to a Direct Connect gateway. Connect the Direct Connect gateway to all the other VPCs by using a transit gateway in each Region.
- C. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VPC. Use a transit gateway with dynamic routing. Connect the transit gateway to all other VPCs.
- D. Create an AWS Direct Connect connection between the on-premises data center and AWS. Establish an AWS Site-to-Site VPN connection between all VPCs in each Region. Create VPC peering connections that initiate from the central VPC to all other VPCs.

B

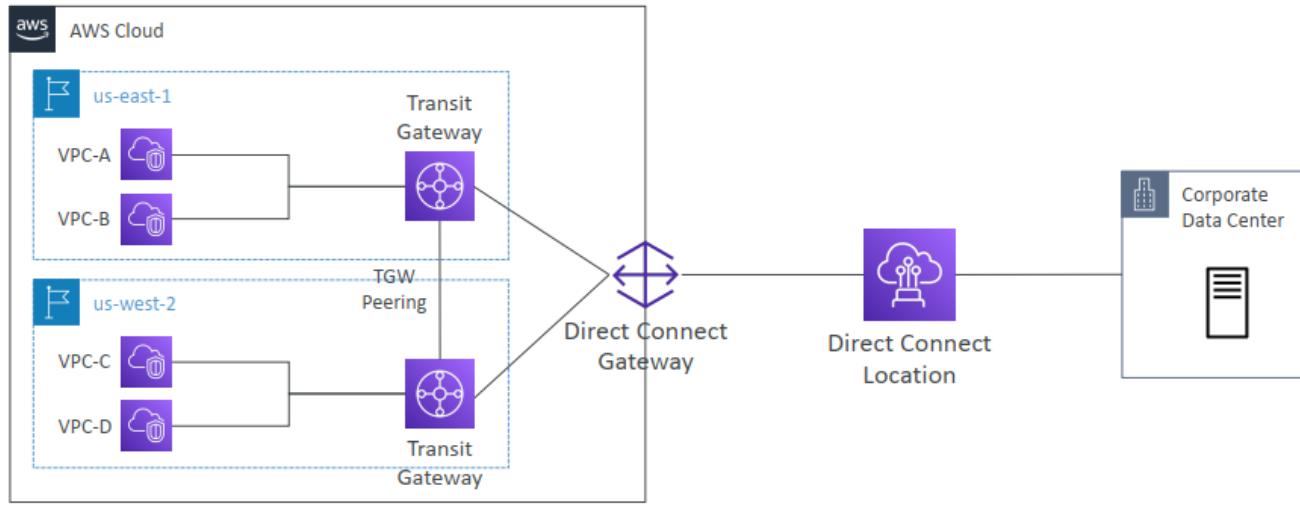
provide a consistent network experience for end users → DX
direct connect + vpc = direct connect gw + TGW

Transit Gateway

- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager (RAM)
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with other VPC
- Works with Direct Connect Gateway, VPN connections
- Supports IP Multicast (not supported by any other AWS service)
- Instances in a VPC can access a NAT Gateway, NLB, PrivateLink, and EFS in other VPCs attached to the AWS Transit Gateway.



Transit Gateway to Direct Connect Gateway



Question 233:

A company is migrating its development and production workloads to a new organization in AWS Organizations. The company has created a separate member account for development and a separate member account for production. Consolidated billing is linked to the management account. In the management account, a solutions architect needs to create an IAM user that can stop or terminate resources in both member accounts.

Which solution will meet this requirement?

- A. Create an IAM user and a cross-account role in the management account. Configure the cross-account role with least privilege access to the member accounts.
- B. Create an IAM user in each member account. In the management account, create a cross-account role that has least privilege access. Grant the IAM users access to the cross-account role by using a trust policy.
- C. Create an IAM user in the management account. In the member accounts, create an IAM group that has least privilege access. Add the IAM user from the management account to each IAM group in the member accounts.
- D. Create an IAM user in the management account. In the member accounts, create cross-account roles that have least privilege access. Grant the IAM user access to the roles by using a trust policy.

D

Cross account role should be created in destination(member) account. The role has trust entity to master account.

IAM – What should you know by now

- **Users:** long term credentials
- **Groups**
- **Roles:** short-term credentials, uses STS
 - EC2 Instance Roles: uses the **EC2 metadata** service. One role at a time per instance
 - Service Roles: API Gateway, CodeDeploy, etc...
 - Cross Account roles
- **Policies**
 - AWS Managed
 - Customer Managed
 - Inline Policies
- **Resource Based Policies** (S3 bucket, SQS queue, etc...)

Question 234:

A company wants to use AWS for disaster recovery for an on-premises application. The company has hundreds of Windows-based servers that run the application. All the servers mount a common share.

The company has an RTO of 15 minutes and an RPO of 5 minutes. The solution must support native failover and fallback capabilities.

Which solution will meet these requirements MOST cost-effectively?

- Create an AWS Storage Gateway File Gateway. Schedule daily Windows server backups. Save the data to Amazon S3. During a disaster, recover the on-premises servers from the backup. During failback, run the on-premises servers on Amazon EC2 instances.
- Create a set of AWS CloudFormation templates to create infrastructure. Replicate all data to Amazon Elastic File System (Amazon EFS) by using AWS DataSync. During a disaster, use AWS CodePipeline to deploy the templates to restore the on-premises servers. Fail back the data by using DataSync.
- Create an AWS Cloud Development Kit (AWS CDK) pipeline to stand up a multi-site active-active environment on AWS. Replicate data into Amazon S3 by using the s3 sync command. During a disaster, swap DNS endpoints to point to AWS. Fail back the data by using the s3 sync command.

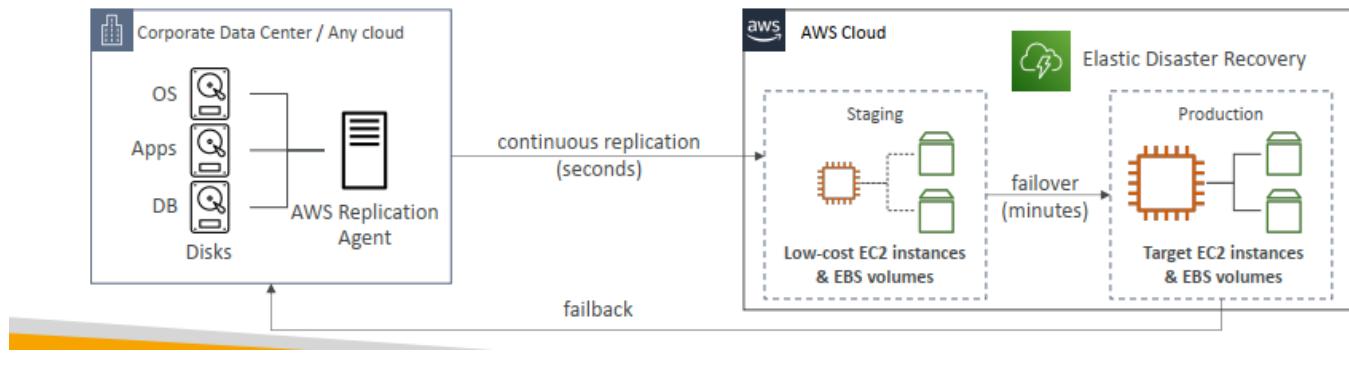
D. Use AWS Elastic Disaster Recovery to replicate the on-premises servers. Replicate data to an Amazon FSx for Windows File Server file system by using AWS DataSync. Mount the file system to AWS servers. During a disaster, fail over the on-premises servers to AWS. Fail back to new or existing servers by using Elastic Disaster Recovery.

D

AWS Elastic Disaster Recovery (DRS)



- Used to be named "CloudEndure Disaster Recovery"
- Quickly and easily recover your physical, virtual, and cloud-based servers into AWS
- Example: protect your most critical databases (including Oracle, MySQL, and SQL Server), enterprise apps (SAP), protect your data from ransomware attacks, ...
- Continuous block-level replication for your servers



Question 235:

A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations.

Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Choose three.)

- A. Ensure the HPC cluster is launched within a single Availability Zone.
- B. Launch the EC2 instances and attach elastic network interfaces in multiples of four.

- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.
- D. Ensure the cluster is launched across multiple Availability Zones.
- E. Replace Amazon EFS with multiple Amazon EBS volumes in a RAID array.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

A,C,F

a tightly coupled workload → Elastic Fabric Adapter

a large number of shared files stored in Amazon EFS → Linux

A. Ensure the HPC cluster is launched within a single Availability Zone: This choice ensures that the EC2 instances in the cluster have low network latency and high bandwidth, as they are located within the same data center.

C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled: EFA is a network interface that provides low-latency, high-bandwidth communication between EC2 instances. By selecting instance types with EFA enabled, the cluster can benefit from improved inter-instance communication.

F. Replace Amazon EFS with Amazon FSx for Lustre: Amazon FSx for Lustre is a high-performance file system optimized for HPC workloads. By using FSx for Lustre instead of Amazon EFS, the cluster can achieve better performance for the large number of shared files generated by the workload.

Compute and Networking

nâng cao

- EC2 Enhanced Networking (SR-IOV)
 - Higher bandwidth, higher PPS (packet per second), lower latency
 - Option 1: Elastic Network Adapter (ENA) up to 100 Gbps
 - Option 2: Intel 82599 VF up to 10 Gbps – LEGACY
- Elastic Fabric Adapter (EFA)
 - Improved ENA for HPC, only works for Linux
 - Great for inter-node communications, tightly coupled workloads khối lượng công việc được kết nối chặt chẽ
 - Leverages Message Passing Interface (MPI) standard
 - Bypasses the underlying Linux OS to provide low-latency, reliable transport

Storage

- Instance-attached storage:
 - EBS: scale up to 256,000 IOPS with io2 Block Express
 - Instance Store: scale to millions of IOPS, linked to EC2 instance, low latency
- Network storage:
 - Amazon S3: large blob, not a file system
 - Amazon EFS: scale IOPS based on total size, or use provisioned IOPS
 - Amazon FSx for Lustre:
 - HPC optimized distributed file system, millions of IOPS
 - Backed by S3

Question 236:

A company is designing an AWS Organizations structure. The company wants to standardize a process to apply tags across the entire organization. The company will require tags with specific values when a user creates a new resource. Each of the company's OUs will have unique tag values.

Which solution will meet these requirements?

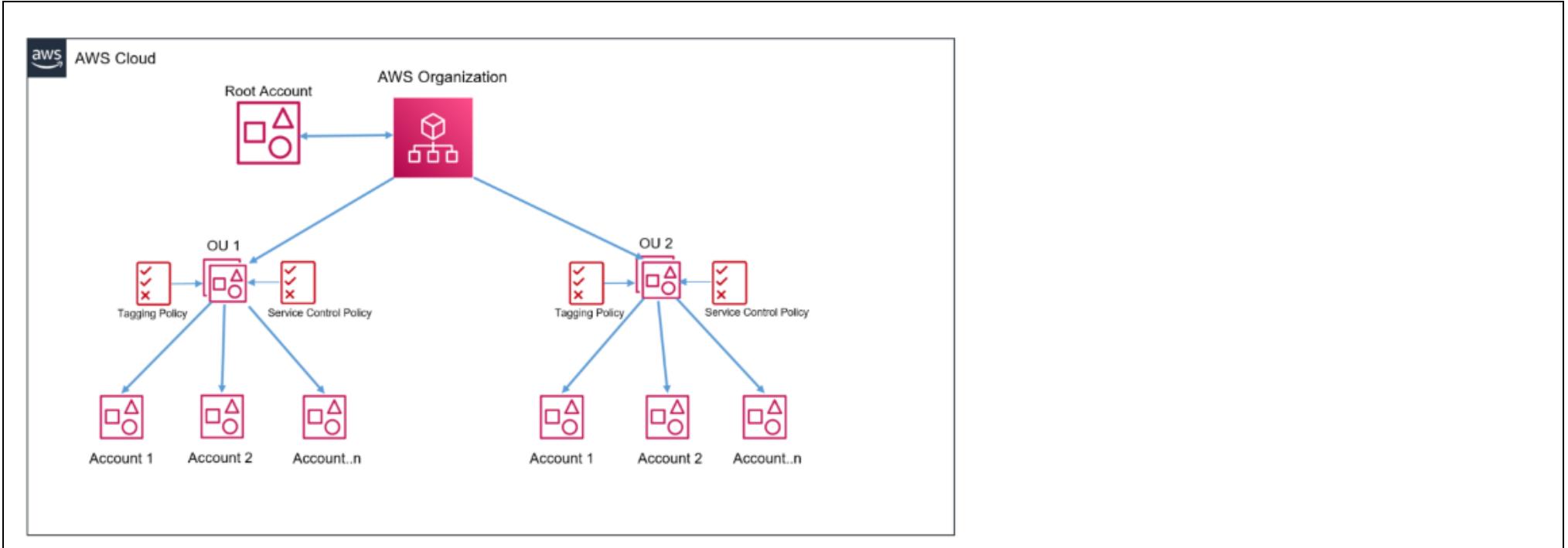
- Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the OUs.
- Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the organization's management account.
- Use an SCP to allow the creation of resources only when the resources have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the OUs.
- Use an SCP to deny the creation of resources that do not have the required tags. Define the list of tags. Attach the SCP to the OUs.

A

an AWS Organizations structure → multi OUs →

go to the management account -> Organizations console -> Policies -> Tag policies -> "name of the policy" -> attach to OU

LAB: <https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>



Question 237:

A company has more than 10,000 sensors that send data to an on-premises Apache Kafka server by using the Message Queuing Telemetry Transport (MQTT) protocol. The on-premises Kafka server transforms the data and then stores the results as objects in an Amazon S3 bucket.

Recently, the Kafka server crashed. The company lost sensor data while the server was being restored. A solutions architect must create a new design on AWS that is highly available and scalable to prevent a similar occurrence.

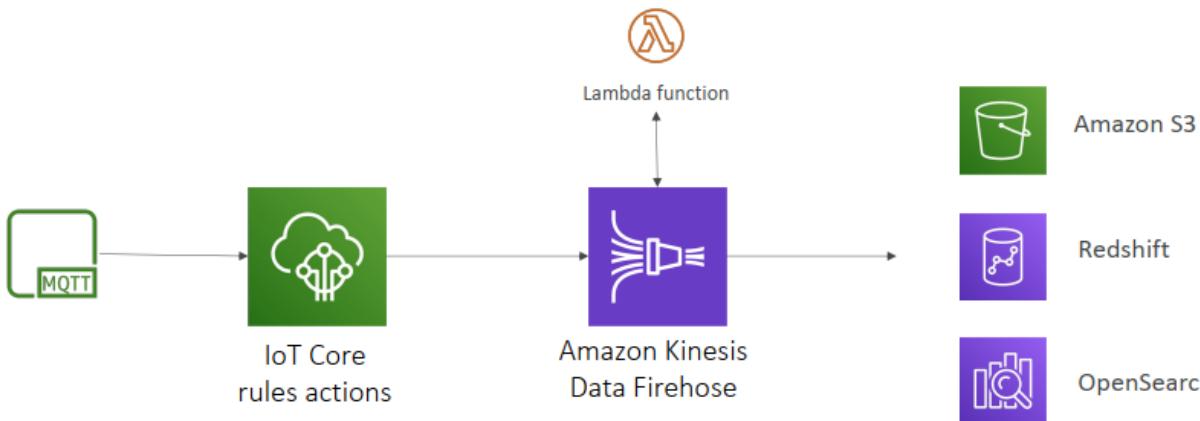
Which solution will meet these requirements?

- Launch two Amazon EC2 instances to host the Kafka server in an active/standby configuration across two Availability Zones. Create a domain name in Amazon Route 53. Create a Route 53 failover policy. Route the sensors to send the data to the domain name.
- Migrate the on-premises Kafka server to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create a Network Load Balancer (NLB) that points to the Amazon MSK broker. Enable NLB health checks. Route the sensors to send the data to the NLB.
- Deploy AWS IoT Core, and connect it to an Amazon Kinesis Data Firehose delivery stream. Use an AWS Lambda function to handle data transformation. Route the sensors to send the data to AWS IoT Core.

D. Deploy AWS IoT Core, and launch an Amazon EC2 instance to host the Kafka server. Configure AWS IoT Core to send the data to the EC2 instance. Route the sensors to send the data to AWS IoT Core.

C
IoT perfect for MQTT

IoT Core – Kinesis Data Firehose

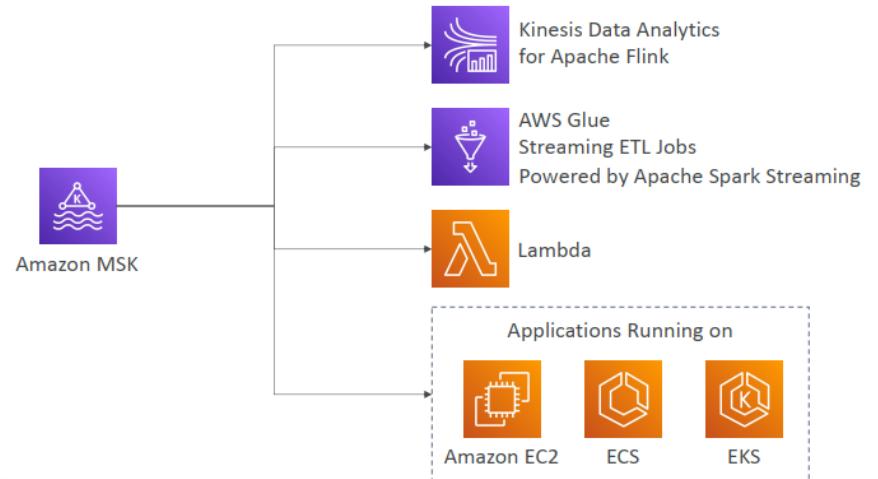


Amazon MSK Consumers

Amazon Managed Streaming for Apache Kafka (Amazon MSK)



- Alternative to Amazon Kinesis
- Fully managed Apache Kafka on AWS
 - Allow you to create, update, delete clusters
 - MSK creates & manages Kafka brokers nodes & Zookeeper nodes for you
 - Deploy the MSK cluster in your VPC, multi-AZ (up to 3 for HA)
 - Automatic recovery from common Apache Kafka failures
 - Data is stored on EBS volumes **for as long as you want**
- **MSK Serverless**
 - Run Apache Kafka on MSK without managing the capacity
 - MSK automatically provisions resources and scales compute & storage



Question 238:

A company recently started hosting new application workloads in the AWS Cloud. The company is using Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) file systems, and Amazon RDS DB instances.

To meet regulatory and business requirements, the company must make the following changes for data backups:

- Backups must be retained based on custom daily, weekly, and monthly requirements.
- Backups must be replicated to at least one other AWS Region immediately after capture.
- The backup solution must provide a single source of backup status across the AWS environment.
- The backup solution must send immediate notifications upon failure of any resource backup.

Which combination of steps will meet these requirements with the LEAST amount of operational overhead? (Choose three.)

- A. Create an AWS Backup plan with a backup rule for each of the retention requirements.
- B. Configure an AWS Backup plan to copy backups to another Region.
- C. Create an AWS Lambda function to replicate backups to another Region and send notification if a failure occurs.
- D. Add an Amazon Simple Notification Service (Amazon SNS) topic to the backup plan to send a notification for finished jobs that have any status except BACKUP_JOB_COMPLETED.
- E. Create an Amazon Data Lifecycle Manager (Amazon DLM) snapshot lifecycle policy for each of the retention requirements.
- F. Set up RDS snapshots on each database.

A,B,D

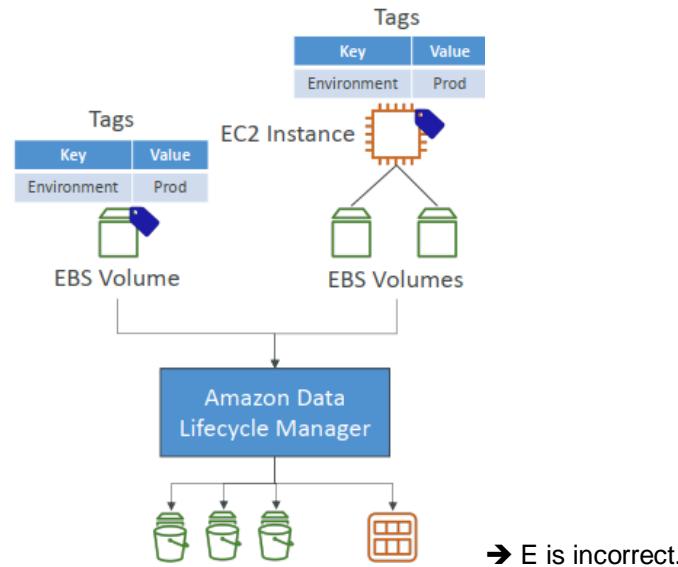
Backups must be retained based on custom daily, weekly, and monthly requirements → Create an AWS Backup plan with a backup rule for each of the retention requirements

Configure an AWS Backup plan to copy backups to another Region → Configure an AWS Backup plan to copy backups to another Region

The backup solution must send immediate notifications upon failure of any resource backup → Add an Amazon Simple Notification Service (Amazon SNS) topic to the backup plan to send a notification for finished jobs that have any status except BACKUP_JOB_COMPLETED.

Amazon Data Lifecycle Manager

- Automate the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs
- Schedule backups, cross-account snapshot copies, delete outdated backups, ...
nhận dạng
- Uses resource tags to identify the resources (EC2 instances, EBS volumes)
- Can't be used to manage snapshots/AMIs created outside DLM
- Can't be used to manage instance-store backed AMIs



→ E is incorrect.

Question 239:

A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers. The data platform must meet the following requirements:

- Provide near-real-time analytics of the inbound genomic data
- Ensure the data is flexible, parallel, and durable
- Deliver results of processing to a data warehouse

Which strategy should a solutions architect use to meet these requirements?

- A. Use Amazon Kinesis Data Firehose to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon RDS instance.
- B. Use Amazon Kinesis Data Streams to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon Redshift cluster using Amazon EMR.
- C. Use Amazon S3 to collect the inbound device data, analyze the data from Amazon SQS with Kinesis, and save the results to an Amazon Redshift cluster.

D. Use an Amazon API Gateway to put requests into an Amazon SQS queue, analyze the data with an AWS Lambda function, and save the results to an Amazon Redshift cluster using Amazon EMR.

B

Option A might be close enough, near-real time, which is Firehose, but the target is RDS but the ask is for Datawarehouse (Redshift)
Deliver results of processing to a data warehouse ➔ Redshift

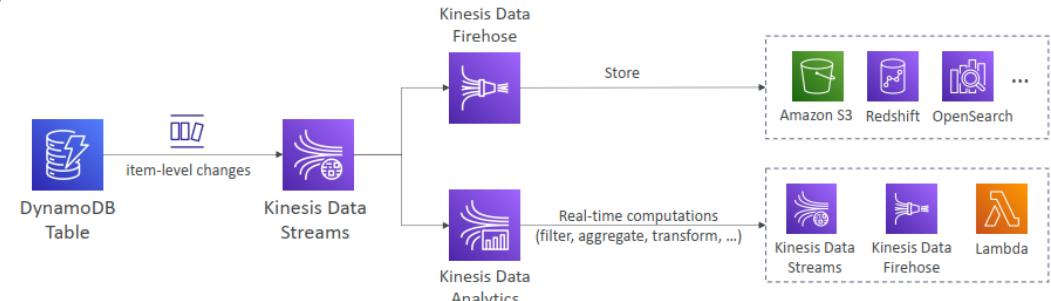
Redshift Overview

- Redshift is based on PostgreSQL, but it's not used for OLTP online transaction processing
=> Redshift is datawarehouse
- It's OLAP – online analytical processing (analytics and data warehousing)
- 10x better performance than other data warehouses, scale to PBs of data
- Columnar storage of data (instead of row based)
- Massively Parallel Query Execution (MPP)
- Pay as you go based on the instances provisioned
- Has a SQL interface for performing the queries
- BI tools such as AWS Quicksight or Tableau integrate with it



Amazon Kinesis Data Streams for DynamoDB

- You can use Kinesis Data Streams to capture item-level changes in DynamoDB
- Custom and longer data retention period (> 24 hours in DynamoDB Streams)



Kinesis Data Firehose



- Fully Managed Service, no administration, automatic scaling, serverless
 - AWS: Redshift / Amazon S3 / OpenSearch
 - 3rd party partner: Splunk / MongoDB / DataDog / NewRelic / ...
 - Custom: send to any HTTP endpoint
- Pay for data going through Firehose
- **Near Real Time**
 - 60 seconds latency minimum for non full batches
 - Or minimum 1MB of data at a time
- Supports many data formats, conversions, transformations, compression
- Supports custom data transformations using AWS Lambda
- Can send failed or all data to a backup S3 bucket

Question 240:

A solutions architect needs to define a reference architecture for a solution for three-tier applications with web, application, and NoSQL data layers. The reference architecture must meet the following requirements:

- High availability within an AWS Region
- Able to fail over in 1 minute to another AWS Region for disaster recovery
- Provide the most efficient solution while minimizing the impact on the user experience

Which combination of steps will meet these requirements? (Choose three.)

- A. Use an Amazon Route 53 weighted routing policy set to 100/0 across the two selected Regions. Set Time to Live (TTL) to 1 hour.
- B. Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.
- C. Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.
- D. Back up data from an Amazon DynamoDB table in the primary Region every 60 minutes and then write the data to Amazon S3. Use S3 cross-Region replication to copy the data from the primary Region to the disaster recovery Region. Have a script import the data into DynamoDB in a disaster recovery scenario.
- E. Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.
- F. Use Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use Spot Instances for the required resources.

B,C,E

while minimizing the impact on the user experience → long workloads → Reserved Instances

EC2 Instance Launch Types

- On Demand Instances: short workload, có thể dự đoán giá, tin cậy
- Spot Instances: short workloads, for cheap, can lose instances (not reliable)
- Reserved: (MINIMUM 1 year)
 - Reserved Instances: long workloads
 - Convertible Reserved Instances: long workloads with flexible instances không chia sẻ phần cứng
- Dedicated Instances: no other customers will share your hardware
- Dedicated Hosts: book an entire physical server, control instance placement
 - Great for software licenses that operate at the core, or socket level
 - Can define host affinity so that instance reboots are kept on the same host

xác định sự liên kết (affinity) giữa instance và host, đảm bảo rằng khi instance khởi động lại, nó sẽ được giữ trên cùng một host. Điều này có ý nghĩa là các instance sẽ được gắn kết với một máy chủ cụ thể và không bị di chuyển sang máy chủ khác trong quá trình khởi động lại.

Question 241:

A company manufactures smart vehicles. The company uses a custom application to collect vehicle data. The vehicles use the MQTT protocol to connect to the application. The company processes the data in 5-minute intervals. The company then copies vehicle telematics data to on-premises storage. Custom applications analyze this data to detect anomalies.

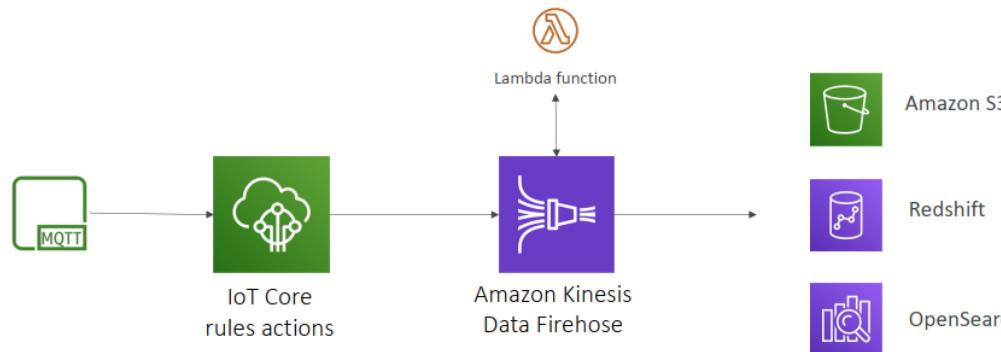
The number of vehicles that send data grows constantly. Newer vehicles generate high volumes of data. The on-premises storage solution is not able to scale for peak traffic, which results in data loss. The company must modernize the solution and migrate the solution to AWS to resolve the scaling challenges.

Which solution will meet these requirements with the LEAST operational overhead?

- Use AWS IoT Greengrass to send the vehicle data to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create an Apache Kafka application to store the data in Amazon S3. Use a pretrained model in Amazon SageMaker to detect anomalies.
- Use AWS IoT Core to receive the vehicle data. Configure rules to route data to an Amazon Kinesis Data Firehose delivery stream that stores the data in Amazon S3. Create an Amazon Kinesis Data Analytics application that reads from the delivery stream to detect anomalies.
- Use AWS IoT FleetWise to collect the vehicle data. Send the data to an Amazon Kinesis data stream. Use an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use the built-in machine learning transforms in AWS Glue to detect anomalies.
- Use Amazon MQ for RabbitMQ to collect the vehicle data. Send the data to an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use Amazon Lookout for Metrics to detect anomalies.

B

IoT Core – Kinesis Data Firehose



Question 242

During an audit, a security team discovered that a development team was putting IAM user secret access keys in their code and then committing it to an AWS CodeCommit repository. The security team wants to automatically find and remediate instances of this security vulnerability.

Which solution will ensure that the credentials are appropriately secured automatically?

- A. Run a script nightly using AWS Systems Manager Run Command to search for credentials on the development instances. If found, use AWS Secrets Manager to rotate the credentials
- B. Use a scheduled AWS Lambda function to download and scan the application code from CodeCommit. If credentials are found, generate new credentials and store them in AWS KMS.
- C. Configure Amazon Macie to scan for credentials in CodeCommit repositories. If credentials are found, trigger an AWS Lambda function to disable the credentials and notify the user.
- D. Configure a CodeCommit trigger to invoke an AWS Lambda function to scan new code submissions for credentials. If credentials are found, disable them in AWS IAM and notify the user.

D

LAB: <https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/>

AWS Macie



- Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.
- Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII)



Question 243:

A company has a data lake in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function.

To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs for each application.

Which combination of steps should the solutions architect take to implement this solution? (Choose two.)

- Create an S3 access point for each application in the AWS account that owns the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
- Create an interface endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Create a VPC gateway attachment for the S3 endpoint.
- Create a gateway endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Specify the route table that is used to access the access point.
- Create an S3 access point for each application in each AWS account and attach the access points to the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.

E. Create a gateway endpoint for Amazon S3 in the data lake's VPC. Attach an endpoint policy to allow access to the S3 bucket. Specify the route table that is used to access the bucket.

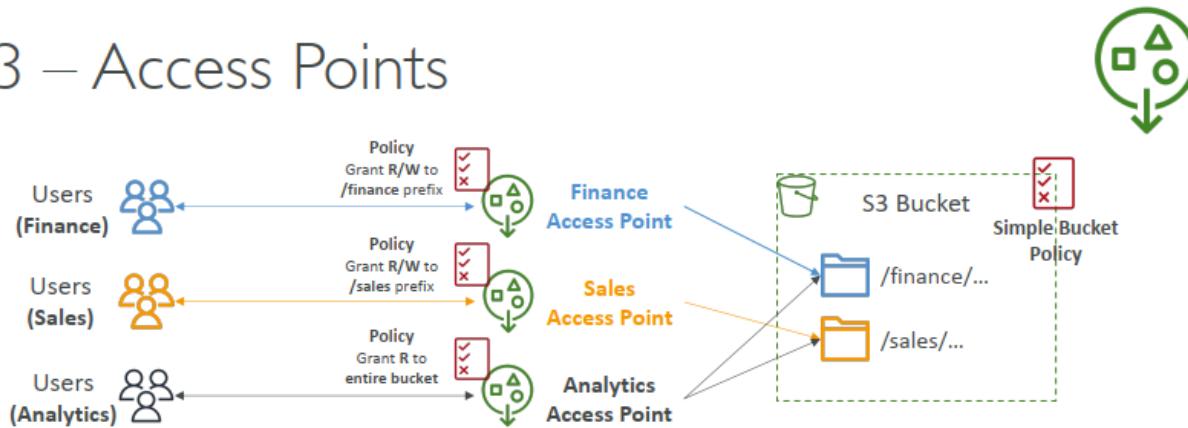
A,C

LAB: <https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

A. By creating an S3 access point for each application in the AWS account that owns the S3 bucket and configuring it to be accessible only from the application's VPC, you ensure that each application has the minimum necessary permissions and can access the data lake securely.

C. Creating a gateway endpoint for Amazon S3 in each application's VPC and configuring the endpoint policy to allow access to an S3 access point ensures that traffic from each VPC is directed through the S3 access point and adheres to the security requirements. Specifying the route table that is used to access the access point is an essential part of the configuration. This combination of steps helps you meet your security and access requirements by using S3 access points and VPC endpoints for each application. It ensures that the data lake is accessed securely and that access permissions are correctly configured.

S3 – Access Points

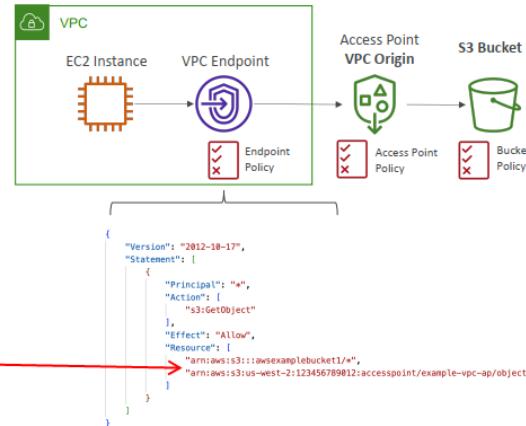


- Access Points đơn giản hóa security management for S3 Buckets
- Each Access Point has:
 - its own DNS name (Internet Origin or VPC Origin)
 - an access point policy (similar to bucket policy) – manage security at scale

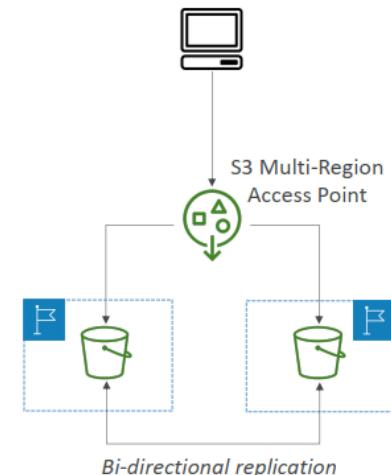
S3 – Multi-Region Access Points

S3 – Access Points – VPC Origin

- We can define the access point to be accessible only from within the VPC
- You must create a VPC Endpoint to access the Access Point (Gateway or Interface Endpoint)
- The VPC Endpoint Policy must allow access to the target bucket and Access Point



- Provide a global endpoint that spans S3 buckets in multiple AWS regions
- Dynamically route requests to the nearest S3 bucket (lowest latency)
- Bi-directional S3 bucket replication rules are created to keep data in sync across regions
- Failover Controls – allows you to shift requests across S3 buckets in different AWS regions within minutes (Active-Active or Active-Passive)



Question 247:

A large company runs workloads in VPCs that are deployed across hundreds of AWS accounts. Each VPC consists of public subnets and private subnets that span across multiple Availability Zones. NAT gateways are deployed in the public subnets and allow outbound connectivity to the internet from the private subnets.

A solutions architect is working on a hub-and-spoke design. All private subnets in the spoke VPCs must route traffic to the internet through an egress VPC. The solutions architect already has deployed a NAT gateway in an egress VPC in a central AWS account.

Which set of additional steps should the solutions architect take to meet these requirements?

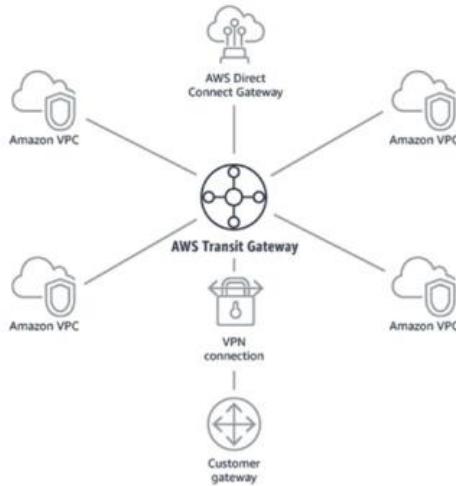
- Create peering connections between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet.
- Create a transit gateway, and share it with the existing AWS accounts. Attach existing VPCs to the transit gateway. Configure the required routing to allow access to the internet.
- Create a transit gateway in every account. Attach the NAT gateway to the transit gateways. Configure the required routing to allow access to the internet.
- Create an AWS PrivateLink connection between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet.

B

Transit Gateway



- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager (RAM)
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with other VPC
- Works with Direct Connect Gateway, VPN connections
- Supports IP Multicast (not supported by any other AWS service)
- Instances in a VPC can access a NAT Gateway, NLB, PrivateLink, and EFS in other VPCs attached to the AWS Transit Gateway.



Question 244:

A company has developed a hybrid solution between its data center and AWS. The company uses Amazon VPC and Amazon EC2 instances that send application logs to Amazon CloudWatch. The EC2 instances read data from multiple relational databases that are hosted on premises.

The company wants to monitor which EC2 instances are connected to the databases in near-real time. The company already has a monitoring solution that uses Splunk on premises. A solutions architect needs to determine how to send networking traffic to Splunk.

How should the solutions architect meet these requirements?

- Enable VPC flows logs, and send them to CloudWatch. Create an AWS Lambda function to periodically export the CloudWatch logs to an Amazon S3 bucket by using the pre-defined export function. Generate ACCESS_KEY and SECRET_KEY AWS credentials. Configure Splunk to pull the logs from the S3 bucket by using those credentials.
- Create an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination. Configure a pre-processing AWS Lambda function with a Kinesis Data Firehose stream processor that extracts individual log events from records sent by CloudWatch Logs subscription filters. Enable VPC flows logs, and send them to CloudWatch. Create a CloudWatch Logs subscription that sends log events to the Kinesis Data Firehose delivery stream.

C. Ask the company to log every request that is made to the databases along with the EC2 instance IP address. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs grouped by database name. Export Athena results to another S3 bucket. Invoke an AWS Lambda function to automatically send any new file that is put in the S3 bucket to Splunk.

D. Send the CloudWatch logs to an Amazon Kinesis data stream with Amazon Kinesis Data Analytics for SQL Applications. Configure a 1-minute sliding window to collect the events. Create a SQL query that uses the anomaly detection template to monitor any networking traffic anomalies in near-real time. Send the result to an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination.

B

VPC Flow Logs → CloudWatch Logs (CloudWatch Logs Subscription Filter) → Kinesis Data Firehose – Lambda pre processing → Splunk



VPC Flow Logs

- Capture information about IP traffic going into your interfaces:
 - VPC Flow Logs
 - Subnet Flow Logs
 - Elastic Network Interface (ENI) Flow Logs
- Helps to monitor & troubleshoot connectivity issues
- Flow logs data can go to S3, CloudWatch Logs, and Kinesis Data Firehose
- Captures network information from AWS managed interfaces too: ELB, RDS, ElastiCache, Redshift, WorkSpaces, NATGW, Transit Gateway...

Kinesis Data Firehose



- Fully Managed Service, no administration, automatic scaling, serverless
 - AWS: Redshift / Amazon S3 / OpenSearch
 - 3rd party partner: Splunk / MongoDB / DataDog / NewRelic / ...
 - Custom: send to any HTTP endpoint
- Pay for data going through Firehose
- Near Real Time
 - 60 seconds latency minimum for non full batches
 - Or minimum 1MB of data at a time
- Supports many data formats, conversions, transformations, compression
- Supports custom data transformations using AWS Lambda
- Can send failed or all data to a backup S3 bucket

Question 245:

A company has five development teams that have each created five AWS accounts to develop and host applications. To track spending, the development teams log in to each account every month, record the current cost from the AWS Billing and Cost Management console, and provide the information to the company's finance team.

The company has strict compliance requirements and needs to ensure that resources are created only in AWS Regions in the United States. However, some resources have been created in other Regions.

A solutions architect needs to implement a solution that gives the finance team the ability to track and consolidate expenditures for all the accounts. The solution also must ensure that the company can create resources only in Regions in the United States.

Which combination of steps will meet these requirements in the MOST operationally efficient way? (Choose three.)

- A. Create a new account to serve as a management account. Create an Amazon S3 bucket for the finance team. Use AWS Cost and Usage Reports to create monthly reports and to store the data in the finance team's S3 bucket.
- B. Create a new account to serve as a management account. Deploy an organization in AWS Organizations with all features enabled. Invite all the existing accounts to the organization. Ensure that each account accepts the invitation.
- C. Create an OU that includes all the development teams. Create an SCP that allows the creation of resources only in Regions that are in the United States. Apply the SCP to the OU.
- D. Create an OU that includes all the development teams. Create an SCP that denies the creation of resources in Regions that are outside the United States. Apply the SCP to the OU.
- E. Create an IAM role in the management account. Attach a policy that includes permissions to view the Billing and Cost Management console. Allow the finance team users to assume the role. Use AWS Cost Explorer and the Billing and Cost Management console to analyze cost.
- F. Create an IAM role in each AWS account. Attach a policy that includes permissions to view the Billing and Cost Management console. Allow the finance team users to assume the role.

B,D,E

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

Service Control Policies (SCP)

- Define allowlist or blocklist IAM actions
- Applied at the OU or Account level
- Does not apply to the Management Account
- SCP is applied to all the Users and Roles in the account, including Root user
- The SCP does not affect Service-linked roles
 - Service-linked roles enable other AWS services to integrate with AWS Organizations and can't be restricted by SCPs.
- SCP must have an explicit Allow (does not allow anything by default)
(adj): rõ ràng, rành mạch
- Use cases:
 - Restrict access to certain services (for example: can't use EMR)
 - Enforce PCI compliance by explicitly disabling services

Cost Explorer



- Visualize, understand, and manage your AWS costs and usage over time
- Create custom reports that analyze cost and usage data.
- Analyze your data at a high level: total costs and usage across all accounts
- Or Monthly, hourly, resource level granularity
- Choose an optimal Savings Plan (to lower prices on your bill)
- Forecast usage up to 12 months based on previous usage

finance team the ability to track and consolidate expenditures for all the accounts ➔ E

Question 246:

A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWS account. The company is using AWS Organizations and created an account for the security team.

How should a solutions architect meet these requirements?

- A. Use the OrganizationAccountAccessRole IAM role to create a new IAM policy with read-only access in each member account. Establish a trust relationship between the IAM policy in each member account and the security account. Ask the security team to use the IAM policy to gain access.
- B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access.
- C. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the management account from the security account. Use the generated temporary credentials to gain access.
- D. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the member account from the security account. Use the generated temporary credentials to gain access.

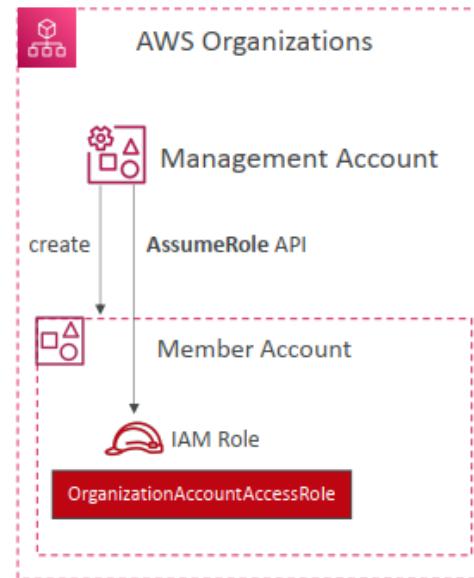
B

B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access. By using the OrganizationAccountAccessRole IAM role, the solutions architect can create a new IAM role with read-only access in each member account. This allows the security team to have read-only access to all accounts from their own AWS account. The trust relationship between the IAM role in each member account and the security account ensures that the security team can assume the IAM role and access the necessary resources.

A is incorrect as you CANNOT establish a trust relationship between the IAM policy and account C and D does NOT talk about readonly access.

AWS Organizations - OrganizationAccountAccessRole

- IAM role which grants full administrator permissions in the Member account to the Management account
- Used to perform admin tasks in the Member accounts (e.g., creating IAM users)
- Could be assumed by IAM users in the Management account
- Automatically added to all new Member accounts created with AWS Organizations
- Must be created manually if you invite an existing Member account



Question 248:

An education company is running a web application used by college students around the world. The application runs in an Amazon Elastic Container Service (Amazon ECS) cluster in an Auto Scaling group behind an Application Load Balancer (ALB). A system administrator detects a weekly spike in the number of failed login attempts, which overwhelm the application's authentication service. All the failed login attempts originate from about 500 different IP addresses that change each week. A solutions architect must prevent the failed login attempts from overwhelming the authentication service.

Which solution meets these requirements with the MOST operational efficiency?

- Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses.
- Create an AWS WAF web ACL with a rate-based rule, and set the rule action to Block. Connect the web ACL to the ALB.
- Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIDR ranges.

D. Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Block. Connect the web ACL to the ALB.

B

AWS WAF (Web Application Firewall) with a rate-based rule allows you to monitor and block traffic based on the rate of requests from different IP addresses. The rate-based rule can help identify and block the excessive login attempts originating from a large number of IP addresses that change weekly. By blocking traffic at the ALB level using AWS WAF, the traffic doesn't reach the application, reducing the load on your authentication service. The rate-based rule can automatically adjust to changing patterns of attack without manual updates, providing an efficient solution. AWS WAF is designed for web application protection and allows you to create flexible rules to mitigate various types of attacks, making it a suitable choice for handling this scenario.

AWS WAF – Web Application Firewall



khai thác

- Protects your web applications from common web exploits (Layer 7)
- Deploy on **Application Load Balancer** (localized rules)
- Deploy on **API Gateway** (rules running at the regional or edge level)
- Deploy on **CloudFront** (rules globally on edge locations)
 - Used to front other solutions: CLB, EC2 instances, custom origins, S3 websites
- Deploy on AppSync (protect your GraphQL APIs)
- **WAF is not for DDoS protection**
- Define Web ACL (Web Access Control List):
 - Rules can include **IP addresses**, HTTP headers, HTTP body, or URI strings
 - Protects from common attack - **SQL injection** and Cross-Site Scripting (XSS)
 - Size constraints, Geo match
 - Rate-based rules (to count occurrences of events)
- Rule Actions: Count | Allow | Block | CAPTCHA

AWS Firewall Manager



- Manage rules in all accounts of an AWS Organization
- Security policy: common set of security rules
 - WAF rules (Application Load Balancer, API Gateways, CloudFront)
 - AWS Shield Advanced (ALB, CLB, NLB, Elastic IP, CloudFront)
 - Security Groups for EC2, Application Load Balancer and ENI resources in VPC
 - AWS Network Firewall (VPC Level)
 - Amazon Route 53 Resolver DNS Firewall
 - Policies are created at the region level
- Rules are applied to new resources as they are created (good for compliance) across all and future accounts in your Organization

dược áp dụng với các resource mới khi chúng được tạo

Question 249:

A company operates an on-premises software-as-a-service (SaaS) solution that ingests several files daily. The company provides multiple public SFTP endpoints to its customers to facilitate the file transfers. The customers add the SFTP endpoint IP addresses to their firewall allow list for outbound traffic. Changes to the SFTP endpoint IP addresses are not permitted.

The company wants to migrate the SaaS solution to AWS and decrease the operational overhead of the file transfer service.

Which solution meets these requirements?

- A. Register the customer-owned block of IP addresses in the company's AWS account. Create Elastic IP addresses from the address pool and assign them to an AWS Transfer for SFTP endpoint. Use AWS Transfer to store the files in Amazon S3.
- B. Add a subnet containing the customer-owned block of IP addresses to a VPC. Create Elastic IP addresses from the address pool and assign them to an Application Load Balancer (ALB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the ALB. Store the files in attached Amazon Elastic Block Store (Amazon EBS) volumes.
- C. Register the customer-owned block of IP addresses with Amazon Route 53. Create alias records in Route 53 that point to a Network Load Balancer (NLB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the NLB. Store the files in Amazon S3.
- D. Register the customer-owned block of IP addresses in the company's AWS account. Create Elastic IP addresses from the address pool and assign them to an Amazon S3 VPC endpoint. Enable SFTP support on the S3 bucket.

A
SFTP ➔ AWS Transfer

AWS Transfer Family



- A fully-managed service for file transfers into and out of Amazon S3 or Amazon EFS using the FTP protocol
- Supported Protocols
 - AWS Transfer for FTP (File Transfer Protocol (FTP))
 - AWS Transfer for FTPS (File Transfer Protocol over SSL (FTPS))
 - AWS Transfer for SFTP (Secure File Transfer Protocol (SFTP))
- Managed infrastructure, Scalable, Reliable, Highly Available (multi-AZ)
- Pay per provisioned endpoint per hour + data transfers in GB
- Store and manage users' credentials within the service
- Integrate with existing authentication systems (Microsoft Active Directory, LDAP, Okta, Amazon Cognito, custom)
- Usage: sharing files, public datasets, CRM, ERP, ...

Question 250:

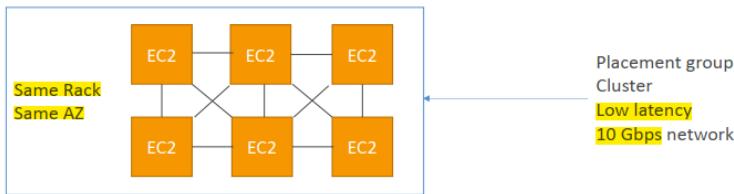
A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region. The application requires high-throughput, low-latency network connections between all of the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant.

Which solution will meet these requirements?

- Launch five new EC2 instances into a cluster placement group. Ensure that the EC2 instance type supports enhanced networking.
- Launch five new EC2 instances into an Auto Scaling group in the same Availability Zone. Attach an extra elastic network interface to each EC2 instance.
- Launch five new EC2 instances into a partition placement group. Ensure that the EC2 instance type supports enhanced networking.
- Launch five new EC2 instances into a spread placement group. Attach an extra elastic network interface to each EC2 instance.

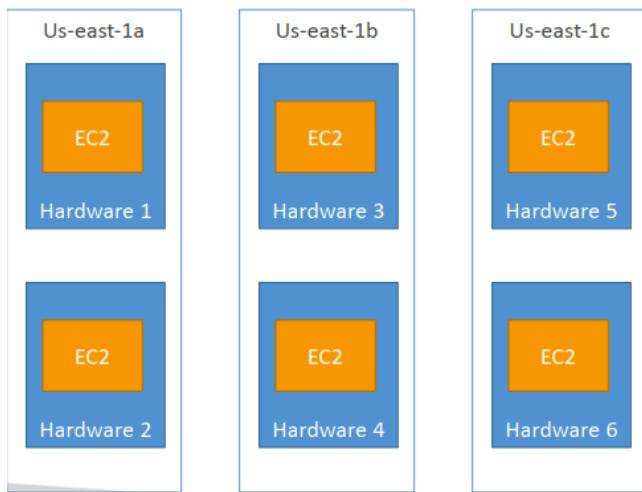
A

Placement Groups Cluster



- Pros: Great network (10 Gbps bandwidth between instances with Enhanced Networking enabled - recommended)
- Cons: If the rack fails, all instances fail at the same time
- Use case:
 - Big Data job that needs to complete fast
 - Application that needs extremely low latency and high network throughput

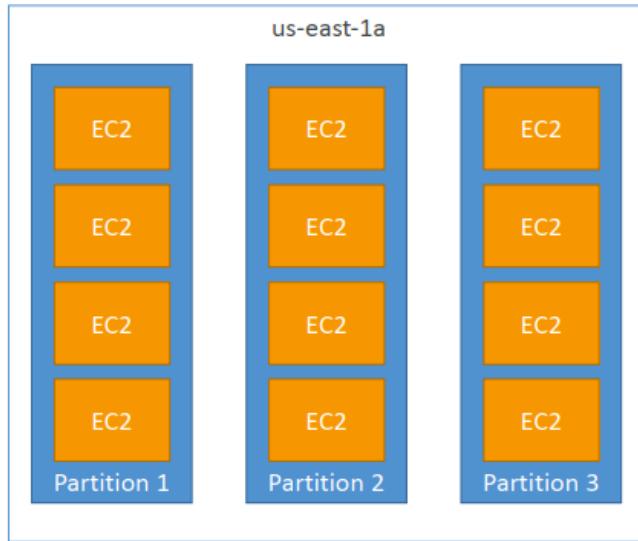
Placement Groups Spread



- Pros:
 - Can span across Availability Zones (AZ)
 - Reduced risk of simultaneous failure
 - EC2 Instances are on different physical hardware
- Cons:
 - Limited to 7 instances per AZ per placement group
- Use case:
 - Application that needs to maximize high availability
 - Critical Applications where each instance must be isolated from failure from each other

Placements Groups

Partition



- Up to 7 partitions per AZ
- Up to 100s of EC2 instances
- The instances in a partition do not share racks with the instances in the other partitions
- A partition failure can affect many EC2 but won't affect other partitions
- EC2 instances get access to the partition information as metadata
- Use cases: HDFS, HBase, Cassandra, Kafka

Question 251:

A company is creating a REST API to share information with six of its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint. Each of the six partners will access the API once per day to post daily sales figures.

After initial deployment, the company observes 1,000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet and wants to secure its API while minimizing cost.

Which approach should the company take to secure its API?

A. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Configure CloudFront with an origin access identity (OAI) and associate it with the distribution. Configure API Gateway to ensure only the OAI can run the POST method.

B. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Add a custom header to the CloudFront distribution populated with an API key. Configure the API to require an API key on the POST method.

C. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API. Create a resource policy with a request limit and associate it with the API. Configure the API to require an API key on the POST method.

D. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API. Create a usage plan with a request limit and associate it with the API. Create an API key and add it to the usage plan.

D

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-aws-waf.html>

Ans is Opt D, A usage plan provides select customers with specific access permissions and request quotas, which helps manage and restrict usage to prevent overuse of resources. API keys are used for tracking and controlling how the API is used. This additional layer of security ensures that only those with the key can access the API. Why not Opt C, Amazon API Gateway doesn't support request limiting through resource policies. You can set permissions on who can access your API using a resource policy, but rate limiting isn't handled by resource policies. API keys alone do not provide throttling or rate limiting. For throttling, you typically would need to use them along with usage plans

API Gateway – Usage Plans & API Keys

- If you want to make an API available as an offering (\$) to your customers
- **Usage Plan:**
 - who can access one or more deployed API stages and methods
 - how much and how fast they can access them
 - uses API keys to identify API clients and meter access
 - configure throttling limits and quota limits that are enforced on individual client
- **API Keys:**
 - alphanumeric string values to distribute to your customers
 - Ex: WBjHxNtoAb4WPKBC7cGm64CBiblb24b4jt8jjHo9
 - Can use with usage plans to control access
 - Throttling limits are applied to the API keys
 - Quotas limits is the overall number of maximum requests
- **429 Too Many Requests:**
 - Account level throttling across all APIs in a region
 - Clients must implement retry mechanisms

Throttling
Limit the rate that users can call your API.

Rate

Burst

Quota
Turn on quotas to limit the number of requests a user can make to your API in a given time period.

Requests
Enter the total number of requests that a user can make in the time period you select in the dropdown list.
 Per month ▾

throttling is limit request rate (unit: request per second). Quota is limit the number of requests per a time period (unit: number of request per month/week/day)

Question 252:

A company uses an Amazon Aurora PostgreSQL DB cluster for applications in a single AWS Region. The company's database team must monitor all data activity on all the databases.

Which solution will achieve this goal?

- A. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon OpenSearch Service cluster for further analysis.
- B. Start a database activity stream on the Aurora DB cluster to capture the activity stream in Amazon EventBridge. Define an AWS Lambda function as a target for EventBridge. Program the Lambda function to decrypt the messages from EventBridge and to publish all database activity to Amazon S3 for further analysis.
- C. Start a database activity stream on the Aurora DB cluster to push the activity stream to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to consume the Kinesis data stream and to deliver the data to Amazon S3 for further analysis.
- D. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon Redshift cluster. Run queries on the Amazon Redshift data to determine database activities on the Aurora database.

C

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

Aurora: activity streams --> Kinesis data stream --> Kinesis Data Firehose --> S3

Aurora



- DB Engines: PostgreSQL-compatible & MySQL-compatible
- Storage: automatically grows up to 128 TB, 6 copies of data, multi-AZ
- Read Replicas: up to 15 RR, reader endpoint to access them all
- Cross Region RR: entire database is copied (not select tables)
- Load / Offload data directly from / to S3: efficient use of resources
- Backup, Snapshots & Restore: same as RDS

Database activity streams monitor and report activities. The stream of activity is collected and transmitted to Amazon Kinesis. From Kinesis, you can monitor the activity stream, or other services and applications can consume the activity stream for further analysis. You can find the underlying Kinesis stream name by using the AWS CLI command `describe-db-clusters` or the RDS API `DescribeDBClusters` operation.

Aurora manages the Kinesis stream for you as follows:

Aurora creates the Kinesis stream automatically with a 24-hour retention period.

Aurora scales the Kinesis stream if necessary.

If you stop the database activity stream or delete the DB cluster, Aurora deletes the Kinesis stream.

The following categories of activity are monitored and put in the activity stream audit log:

SQL commands – All SQL commands are audited, and also prepared statements, built-in functions, and functions in PL/SQL. Calls to stored procedures are audited. Any SQL statements issued inside stored procedures or functions are also audited.

Other database information – Activity monitored includes the full SQL statement, the row count of affected rows from DML commands, accessed objects, and the unique database name. For Aurora PostgreSQL, database activity streams also monitor the bind variables and stored procedure parameters.

Question 253:

An entertainment company recently launched a new game. To ensure a good experience for players during the launch period, the company deployed a static quantity of 12 r6g.16xlarge (memory optimized) Amazon EC2 instances behind a Network Load Balancer. The company's operations team used the Amazon CloudWatch agent and a custom metric to include memory utilization in its monitoring strategy.

Analysis of the CloudWatch metrics from the launch period showed consumption at about one quarter of the CPU and memory that the company expected. Initial demand for the game has subsided and has become more variable. The company decides to use an Auto Scaling group that monitors the CPU and memory consumption to dynamically scale the instance fleet. A solutions architect needs to configure the Auto Scaling group to meet demand in the most cost-effective way.

Which solution will meet these requirements?

- A. Configure the Auto Scaling group to deploy c6g.4xlarge (compute optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- B. Configure the Auto Scaling group to deploy m6g.4xlarge (general purpose) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- C. Configure the Auto Scaling group to deploy r6g.4xlarge (memory optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- D. Configure the Auto Scaling group to deploy r6g.8xlarge (memory optimized) instances. Configure a minimum capacity of 2, a desired capacity of 2, and a maximum capacity of 6.

C

From the question, app is running on memory-optimized instances (r6g.16xlarge) but only utilizing about one quarter of the CPU and memory. So cost-effective to use smaller instances (r6g.4xlarge), which provide a quarter of r6g.16xlarge instances.

Question 254:

A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table. The table uses on-demand capacity mode. Once each day at midnight, a few million new records are loaded into the table. Application read activity against the table happens in bursts throughout the day, and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB.

Which strategy should a solutions architect recommend to meet this requirement?

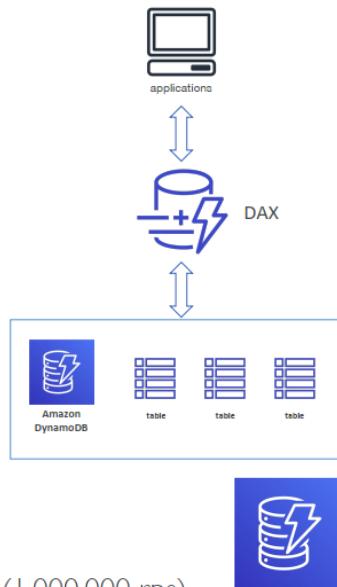
- A. Deploy an Amazon ElastiCache cluster in front of the DynamoDB table
- B. Deploy DynamoDB Accelerator (DAX). Configure DynamoDB auto scaling. Purchase Savings Plans in Cost Explorer.
- C. Use provisioned capacity mode. Purchase Savings Plans in Cost Explorer.
- D. Deploy DynamoDB Accelerator (DAX). Use provisioned capacity mode. Configure DynamoDB auto scaling.

D

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/capacity-mode.html#HowItWorks.ProvisionedThroughput.Manual>

DynamoDB - DAX

- DAX = DynamoDB Accelerator
Lien mạch
- Seamless cache for DynamoDB, no application rewrite
- Writes go through DAX to DynamoDB
- Micro second latency for cached reads & queries
- Solves the Hot Key problem (too many reads)
- 5 minutes TTL for cache by default
- Up to 10 nodes in the cluster
- Multi AZ (3 nodes minimum recommended for production)
- Secure (Encryption at rest with KMS, VPC, IAM, CloudTrail...)



DynamoDB – in short

- NoSQL database, fully managed, quy mô lớn massive scale (1,000,000 rps)
- Similar to Apache Cassandra (can migrate to DynamoDB)
- No disk space to provision, max object size is 400 KB
- Capacity: provisioned (WCU, RCU, & Auto Scaling) or on-demand
- Supports CRUD (Create Read Update Delete)
- Read: eventually or strong consistency
- Supports transactions across multiple tables (ACID support)
- Backups available, point in time recovery
- Table classes: Standard and Infrequent Access (IA)



Amazon DynamoDB cung cấp hai chế độ quản lý công suất: **Provisioned Capacity** và **On-Demand Capacity**. Dưới đây là sự khác biệt chi tiết giữa hai chế độ này:

Provisioned Capacity Mode

Đặc điểm

- **Quản lý công suất:** Bạn cần thiết lập trước số lượng đơn vị đọc (Read Capacity Units - RCUs) và đơn vị ghi (Write Capacity Units - WCUs) cho bảng của mình.

- **Tối ưu chi phí:** Phù hợp với các ứng dụng có lưu lượng ổn định hoặc có thể dự đoán được. Bạn có thể điều chỉnh công suất khi cần thiết nhưng phải quản lý công suất một cách chủ động.
- **Auto Scaling:** Có thể cấu hình để tự động điều chỉnh công suất dựa trên các yêu cầu tải công việc.

Ưu điểm

- **Tiết kiệm chi phí:** Nếu lưu lượng truy cập có thể dự đoán và ổn định, chi phí có thể thấp hơn so với On-Demand.
- **Kiểm soát:** Bạn có thể kiểm soát chính xác công suất đọc và ghi của bảng.

Nhược điểm

- **Phức tạp:** Cần dự đoán và quản lý công suất, có thể gặp khó khăn nếu lưu lượng truy cập biến động mạnh.
- **Thiếu linh hoạt:** Có thể gặp vấn đề về hiệu suất nếu không cấu hình công suất phù hợp với nhu cầu thực tế.

On-Demand Capacity Mode

Đặc điểm

- **Quản lý công suất:** DynamoDB tự động quản lý công suất đọc và ghi cho bạn. Bạn chỉ cần trả phí dựa trên số lượng yêu cầu mà bảng của bạn xử lý.
- **Tối ưu chi phí:** Phù hợp với các ứng dụng có lưu lượng không thể dự đoán được hoặc biến động mạnh. Bạn không cần phải dự đoán và quản lý công suất.
- **Không cần auto scaling:** DynamoDB tự động điều chỉnh công suất để xử lý mọi yêu cầu truy cập.

Ưu điểm

- **Đơn giản:** Không cần phải quản lý hoặc dự đoán công suất. Phù hợp cho các ứng dụng mới hoặc có lưu lượng biến động.
- **Linh hoạt:** Tự động điều chỉnh công suất để đáp ứng mọi yêu cầu truy cập mà không gây ra gián đoạn dịch vụ.

Nhược điểm

- **Chi phí:** Có thể đắt hơn so với chế độ Provisioned nếu lưu lượng truy cập ổn định và cao.

So sánh chi tiết

Đặc điểm	Provisioned Capacity	On-Demand Capacity
Quản lý công suất	Người dùng tự thiết lập và quản lý	Tự động bởi DynamoDB
Chi phí	Dựa trên RCU và WCU	Dựa trên số lượng yêu cầu đọc/ghi
Lưu lượng truy cập	Ôn định hoặc dự đoán được	Biến động hoặc không thể dự đoán
Auto Scaling	Có thể cấu hình	Không cần, tự động điều chỉnh
Kiểm soát công suất	Chính xác theo yêu cầu	Không cần quản lý
Phức tạp trong quản lý	Cao hơn	Thấp hơn

Lựa chọn chế độ nào?

- **Provisioned Capacity:** Nếu bạn có thể dự đoán lưu lượng truy cập và muốn tối ưu chi phí, hoặc nếu bạn có ứng dụng yêu cầu công suất ổn định và không biến động nhiều.
- **On-Demand Capacity:** Nếu lưu lượng truy cập của bạn biến động mạnh, không thể dự đoán được, hoặc bạn muốn sự đơn giản và linh hoạt trong quản lý công suất mà không cần quan tâm đến việc dự đoán và điều chỉnh thủ công.

Question 255:

A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service.

In each AWS account with a client, an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint.

Which combination of steps should a solutions architect take to resolve this issue? (Choose two.)

- Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets. Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances.
- Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets. Check that the NACL is attached to the interface endpoint subnet to allow communications to and from the logging service subnets running on EC2 instances.
- Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets.

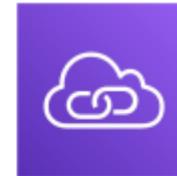
D. Check the security group for the logging service running on EC2 instances to ensure it allows ingress from the clients.

E. Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets.

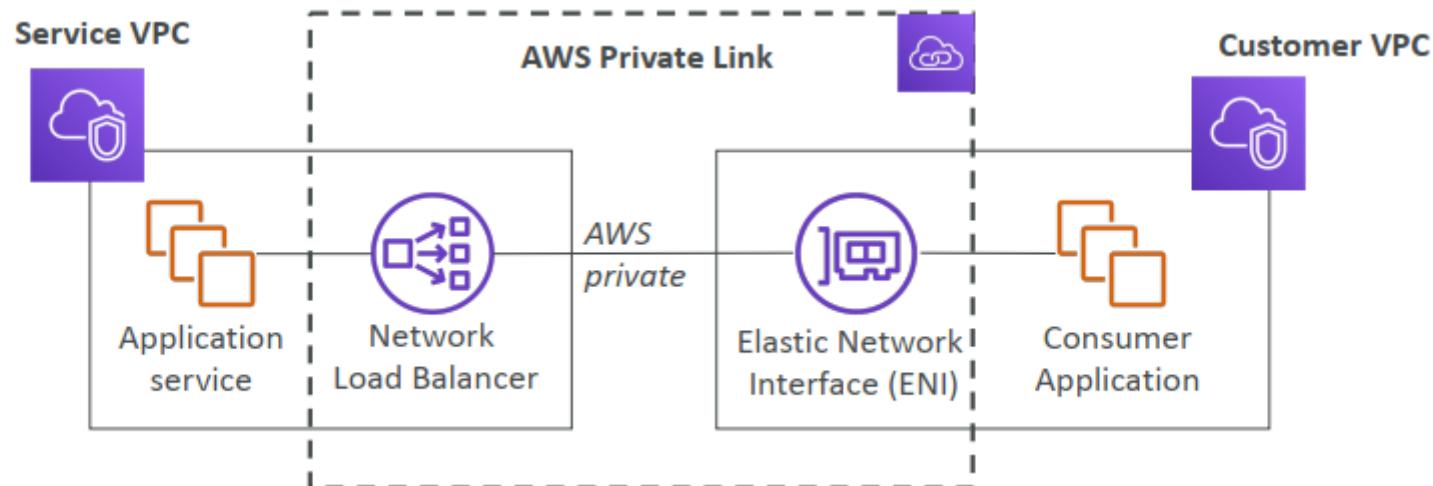
A,C

<https://repost.aws/knowledge-center/security-network-acl-vpc-endpoint>

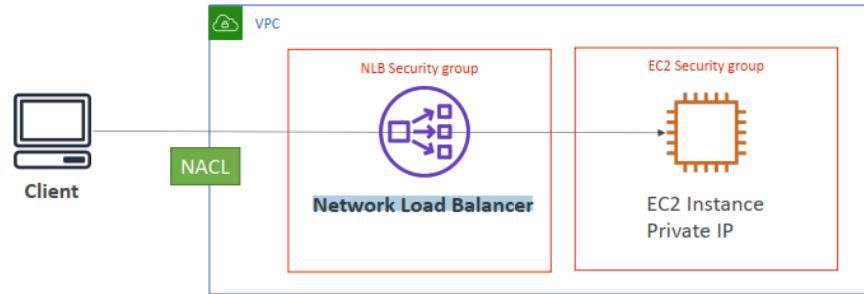
AWS PrivateLink (VPC Endpoint Services)



- Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts)
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)
- If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!



Blocking an IP address – with an NLB



Question 256:

A company has millions of objects in an Amazon S3 bucket. The objects are in the S3 Standard storage class. All the S3 objects are accessed frequently. The number of users and applications that access the objects is increasing rapidly. The objects are encrypted with server-side encryption with AWS KMS keys (SSE-KMS).

A solutions architect reviews the company's monthly AWS invoice and notices that AWS KMS costs are increasing because of the high number of requests from Amazon S3. The solutions architect needs to optimize costs with minimal changes to the application.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new S3 bucket that has server-side encryption with customer-provided keys (SSE-C) as the encryption type. Copy the existing objects to the new S3 bucket. Specify SSE-C.
- B. Create a new S3 bucket that has server-side encryption with Amazon S3 managed keys (SSE-S3) as the encryption type. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Specify SSE-S3.
- C. Use AWS CloudHSM to store the encryption keys. Create a new S3 bucket. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Encrypt the objects by using the keys from CloudHSM.
- D. Use the S3 Intelligent-Tiering storage class for the S3 bucket. Create an S3 Intelligent-Tiering archive configuration to transition objects that are not accessed for 90 days to S3 Glacier Deep Archive.

B

<https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-s3-bucket-keys-reduce-the-costs-of-server-side-encryption-with-aws-key-management-service-sse-kms/>

All the S3 objects are accessed frequently → D is incorrect.

This option switches the encryption method from using AWS Key Management Service (AWS KMS) to using server-side encryption with S3 managed keys (SSE-S3). This change can significantly reduce costs because AWS KMS charges per API request, while SSE-S3 does not have additional charges per API request beyond the S3 usage.

S3 Encryption for Objects

- SSE-S3: encrypts S3 objects using keys handled & managed by AWS
 - SSE-KMS: leverage KMS to manage encryption keys
 - Key usage appears in CloudTrail
 - objects made public can never be read
 - On s3:PutObject, make the permission kms:GenerateDataKey is allowed
 - SSE-C: when you want to manage your own encryption keys
 - Client-Side Encryption
-
- Glacier: all data is AES-256 encrypted, key under AWS control

Amazon S3 > Batch Operations

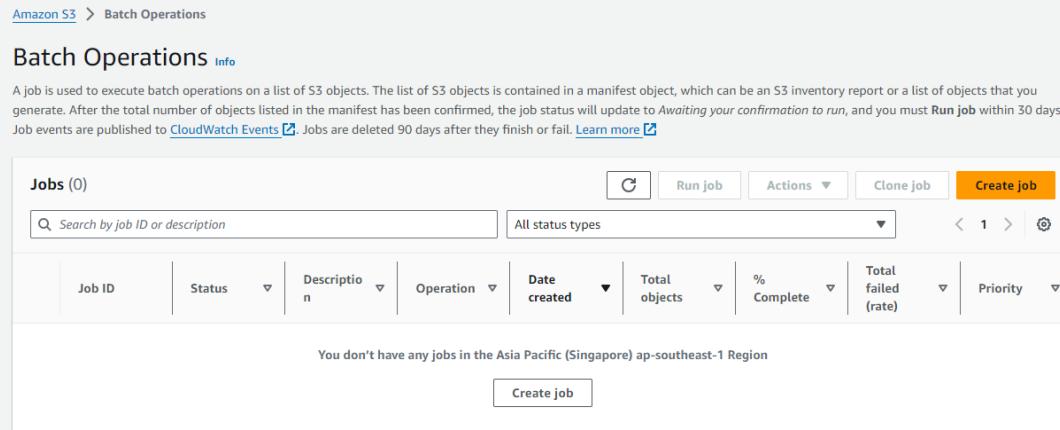
Batch Operations Info

A job is used to execute batch operations on a list of S3 objects. The list of S3 objects is contained in a manifest object, which can be an S3 inventory report or a list of objects that you generate. After the total number of objects listed in the manifest has been confirmed, the job status will update to *Awaiting your confirmation to run*, and you must *Run job* within 30 days. Job events are published to [CloudWatch Events](#). Jobs are deleted 90 days after they finish or fail. [Learn more](#)

Jobs (0)

Job ID	Status	Description	Operation	Date created	Total objects	% Complete	Total failed (rate)	Priority
You don't have any jobs in the Asia Pacific (Singapore) ap-southeast-1 Region								

[Create job](#)



Question 257:

A media storage application uploads user photos to Amazon S3 for processing by AWS Lambda functions. Application state is stored in Amazon DynamoDB tables. Users are reporting that some uploaded photos are not being processed properly. The application developers trace the logs and find that Lambda is experiencing photo processing issues when thousands of users upload photos simultaneously. The issues are the result of Lambda concurrency limits and the performance of DynamoDB when data is saved.

Which combination of actions should a solutions architect take to increase the performance and reliability of the application? (Choose two.)

HANCHE

- A. Evaluate and adjust the RCUs for the DynamoDB tables.
- B. Evaluate and adjust the WCUs for the DynamoDB tables.
- C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions.
- E. Use S3 Transfer Acceleration to provide lower latency to users.

B,D

increase the performance and reliability of the application → SQS
 elastiCache is just increase the performance and not reliability

Adding an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions will help to decouple the Lambda functions from the S3 events and allow the Lambda functions to process photos in batches. This will help to improve the performance of the Lambda functions and reduce the risk of photos not being processed properly. Evaluating and adjusting the WCUs for the DynamoDB tables will help to improve the performance of the DynamoDB tables when data is saved. This will help to reduce the risk of Lambda functions experiencing errors when saving data to DynamoDB.

ElastiCace vs SQS

Question 258:

A company runs an application in an on-premises data center. The application gives users the ability to upload media files. The files persist in a file server. The web application has many users. The application server is overutilized, which causes data uploads to fail occasionally. The company frequently adds new storage to the file server. The company wants to resolve these challenges by migrating the application to AWS.

Users from across the United States and Canada access the application. Only authenticated users should have the ability to access the application to upload files. The company will consider a solution that refactors the application, and the company needs to accelerate application development.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Modify the application to use Amazon S3 to persist the files. Use Amazon Cognito to authenticate users.
- B. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Set up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application. Modify the application to use Amazon S3 to persist the files.
- C. Create a static website for uploads of media files. Store the static assets in Amazon S3. Use AWS AppSync to create an API. Use AWS Lambda resolvers to upload the media files to Amazon S3. Use Amazon Cognito to authenticate users.
- D. Use AWS Amplify to create a static website for uploads of media files. Use Amplify Hosting to serve the website through Amazon CloudFront. Use Amazon S3 to store the uploaded media files. Use Amazon Cognito to authenticate users.

D

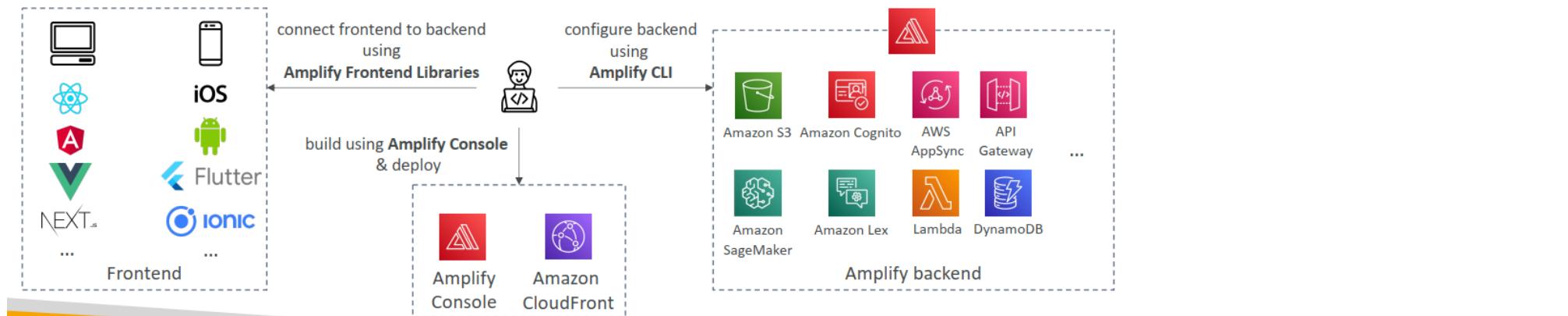
Users from across the United States and Canada access the application → Amazon CloudFront

Only authenticated users should have the ability to access the application to upload files → Amazon Cognito
LEAST operational overhead → AWS Amplify

AWS Amplify - web and mobile applications



- A set of tools and services that helps you develop and deploy scalable full stack web and mobile applications
- Authentication, Storage, API (REST, GraphQL), CI/CD, PubSub, Analytics, AI/ML Predictions, Monitoring, ...
- Connect your source code from GitHub, AWS CodeCommit, Bitbucket, GitLab, or upload directly



Question 259:

A company has an application that is deployed on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are part of an Auto Scaling group. The application has unpredictable workloads and frequently scales out and in. The company's development team wants to analyze application logs to find ways to improve the application's performance. However, the logs are no longer available after instances scale in.

Which solution will give the development team the ability to view the application logs after a scale-in event?

- Enable access logs for the ALB. Store the logs in an Amazon S3 bucket.
- Configure the EC2 instances to publish logs to Amazon CloudWatch Logs by using the unified CloudWatch agent.
- Modify the Auto Scaling group to use a step scaling policy.
- Instrument the application with AWS X-Ray tracing.

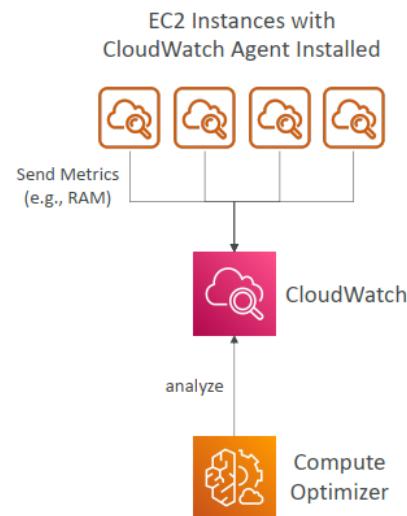
B

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html>

The question states that the development team wants to analyze application logs, and these logs disappear after EC2 instances scale in. To solve this, you can configure the EC2 instances to send their logs to Amazon CloudWatch Logs using the unified CloudWatch agent. This allows you to keep the logs for a longer time period and enables the development team to analyze them at any time, even after the instances have been terminated.

Compute Optimizer – CloudWatch Agent

- Needed to analyze Memory Utilization
- Not needed for CPU, NetworkIn/Out, DiskReadOps, DiskWriteOps, ...



Question 260:

A company runs an unauthenticated static website (<http://www.example.com>) that includes a registration form for users. The website uses Amazon S3 for hosting and uses Amazon CloudFront as the content delivery network with AWS WAF configured. When the registration form is submitted, the website calls an Amazon API Gateway API endpoint that invokes an AWS Lambda function to process the payload and forward the payload to an external API call.

During testing, a solutions architect encounters a cross-origin resource sharing (CORS) error. The solutions architect confirms that the CloudFront distribution origin has the Access-Control-Allow-Origin header set to <http://www.example.com>.

What should the solutions architect do to resolve the error?

- Change the CORS configuration on the S3 bucket. Add rules for CORS to the AllowedOrigin element for www.example.com.
- Enable the CORS setting in AWS WAF. Create a web ACL rule in which the Access-Control-Allow-Origin header is set to www.example.com.
- Enable the CORS setting on the API Gateway API endpoint. Ensure that the API endpoint is configured to return all responses that have the Access-Control-Allow-Origin header set to www.example.com.

D. Enable the CORS setting on the Lambda function. Ensure that the return code of the function has the Access-Control-Allow-Origin header set to www.example.com.

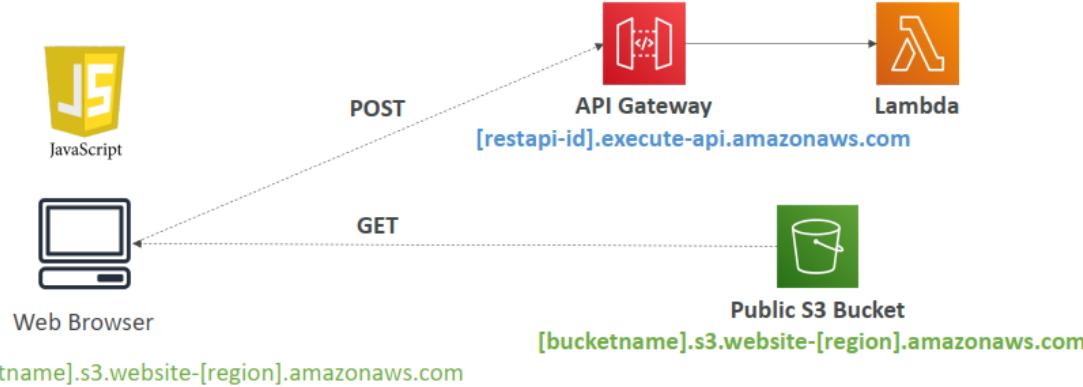
C

<https://repost.aws/knowledge-center/api-gateway-cors-errors>

Question 3 – Final Architecture

CORS is a Browser based security

CORS to allow calls with Origin [bucketname].s3.website-[region].amazonaws.com
Using the header **Access-Control-Allow-Origin**



Question 261:

A company has many separate AWS accounts and uses no central billing or management. Each AWS account hosts services for different departments in the company. The company has a Microsoft Azure Active Directory that is deployed.

A solutions architect needs to centralize billing and management of the company's AWS accounts. The company wants to start using identity federation instead of manual user management. The company also wants to use temporary credentials instead of long-lived access keys.

Which combination of steps will meet these requirements? (Choose three.)

A. Create a new AWS account to serve as a management account. Deploy an organization in AWS Organizations. Invite each existing AWS account to join the organization. Ensure that each account accepts the invitation.

B. Configure each AWS account's email address to be aws+@example.com so that account management email messages and invoices are sent to the same place.

C. Deploy AWS IAM Identity Center (AWS Single Sign-On) in the management account. Connect IAM Identity Center to the Azure Active Directory. Configure IAM Identity Center for automatic synchronization of users and groups.

D. Deploy an AWS Managed Microsoft AD directory in the management account. Share the directory with all other accounts in the organization by using AWS Resource Access Manager (AWS RAM).

E. Create AWS IAM Identity Center (AWS Single Sign-On) permission sets. Attach the permission sets to the appropriate IAM Identity Center groups and AWS accounts.

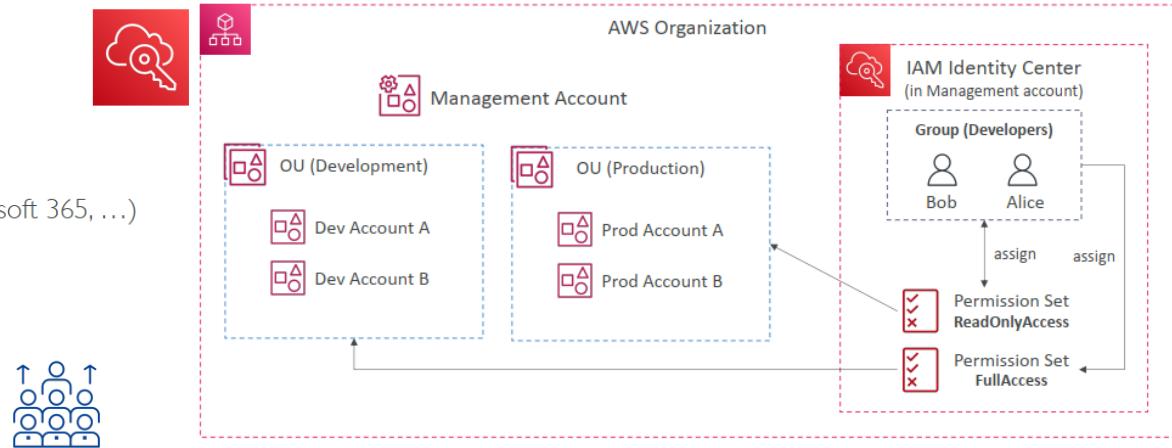
F. Configure AWS Identity and Access Management (IAM) in each AWS account to use AWS Managed Microsoft AD for authentication and authorization.

A,C,E

IAM Identity Center

AWS IAM Identity Center (successor to AWS Single Sign-On)

- One login (single sign-on) for all your
 - AWS accounts in AWS Organizations
 - Business cloud applications (e.g., Salesforce, Box, Microsoft 365, ...)
 - SAML2.0-enabled applications
 - EC2 Windows Instances
- Identity providers
 - Built-in identity store in IAM Identity Center
 - 3rd party: Active Directory (AD), OneLogin, Okta...



Question 262:

A company wants to manage the costs associated with a group of 20 applications that are infrequently used, but are still business-critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology.

Most of the applications are part of month-end processing routines with a small number of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1 GB, though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group is a billing report written in Java that accesses multiple data sources and often runs for several hours.

Which is the MOST cost-effective solution?

A. Deploy a separate AWS Lambda function for each application. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.

B. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon CloudWatch.

C. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources. Monitor each AWS Elastic Beanstalk deployment by using CloudWatch alarms.

D. Deploy a new Amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers. Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved Instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.

B
often runs for several hours → A is incorrect
cost-effective → B is cheaper than C,D

Question 263:

A solutions architect needs to review the design of an Amazon EMR cluster that is using the EMR File System (EMRFS). The cluster performs tasks that are critical to business needs. The cluster is running Amazon EC2 On-Demand Instances at all times for all task, primary, and core nodes. The EMR tasks run each morning, starting at 1:00 AM. and take 6 hours to finish running. The amount of time to complete the processing is not a priority because the data is not referenced until late in the day.

The solutions architect must review the architecture and suggest a solution to minimize the compute costs.

Which solution should the solutions architect recommend to meet these requirements?

- A. Launch all task, primary, and core nodes on Spot Instances in an instance fleet. Terminate the cluster, including all instances, when the processing is completed.
- B. Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate the cluster, including all instances, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- C. Continue to launch all nodes on On-Demand Instances. Terminate the cluster, including all instances, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- D. Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate only the task node instances when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.

B
It provides a balanced approach by using Spot Instances for task nodes to reduce costs and On-Demand Instances for primary and core nodes to ensure cluster stability. Terminating the cluster after processing and purchasing Compute Savings Plans for the On-Demand usage further optimizes costs while maintaining the reliability needed for critical business tasks. The data can also be accessed via S3 if the cluster is not running, so it's ok to terminate it once the processing completes.

Amazon EMR – Node types & purchasing

- Master Node: Manage the cluster, coordinate, manage health – long running
- Core Node: Run tasks and store data – long running
- Task Node (optional): Just to run tasks – usually Spot
- Purchasing options:
 - On-demand: reliable, predictable, won't be terminated
 - Reserved (min 1 year): cost savings (EMR will automatically use if available)
 - Spot Instances: cheaper, can be terminated, less reliable
- Can have long-running cluster, or transient (temporary) cluster

Question 264:

A company has migrated a legacy application to the AWS Cloud. The application runs on three Amazon EC2 instances that are spread across three Availability Zones. One EC2 instance is in each Availability Zone. The EC2 instances are running in three private subnets of the VPC and are set up as targets for an Application Load Balancer (ALB) that is associated with three public subnets.

The application needs to communicate with on-premises systems. Only traffic from IP addresses in the company's IP address range are allowed to access the on-premises systems. The company's security team is bringing only one IP address from its internal IP address range to the cloud. The company has added this IP address to the allow list for the company firewall. The company also has created an Elastic IP address for this IP address.

A solutions architect needs to create a solution that gives the application the ability to communicate with the on-premises systems. The solution also must be able to mitigate failures automatically.

Which solution will meet these requirements?

- A. Deploy three NAT gateways, one in each public subnet. Assign the Elastic IP address to the NAT gateways. Turn on health checks for the NAT gateways. If a NAT gateway fails a health check, recreate the NAT gateway and assign the Elastic IP address to the new NAT gateway.
- B. Replace the ALB with a Network Load Balancer (NLB). Assign the Elastic IP address to the NLB. Turn on health checks for the NLB. In the case of a failed health check, redeploy the NLB in different subnets.

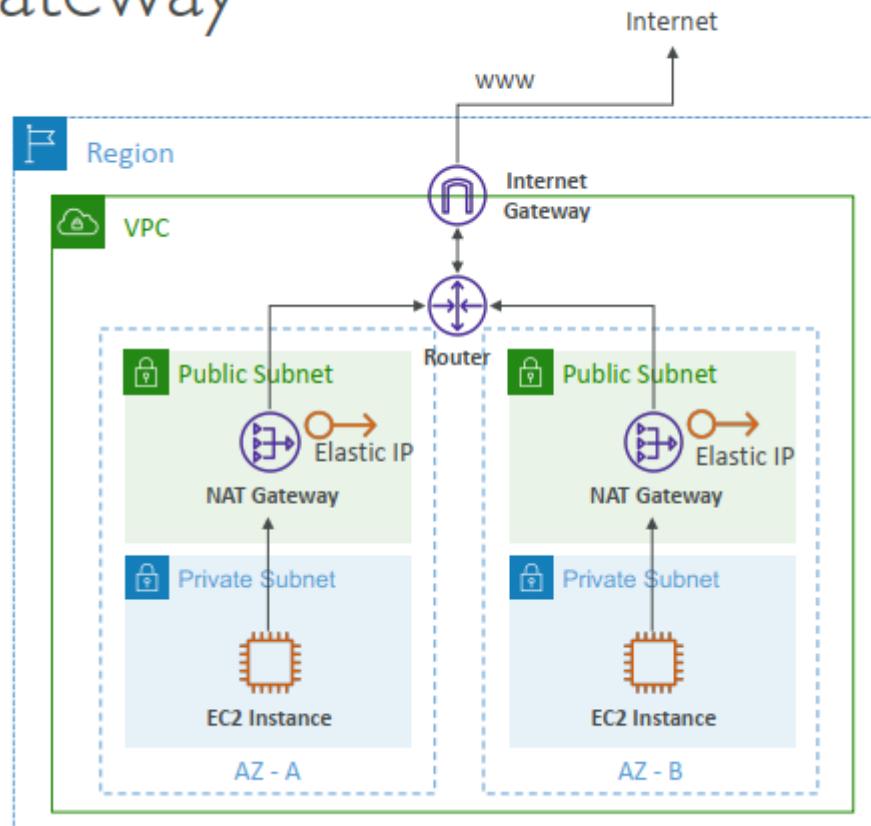
C. Deploy a single NAT gateway in a public subnet. Assign the Elastic IP address to the NAT gateway. Use Amazon CloudWatch with a custom metric to monitor the NAT gateway. If the NAT gateway is unhealthy, invoke an AWS Lambda function to create a new NAT gateway in a different subnet. Assign the Elastic IP address to the new NAT gateway.

D. Assign the Elastic IP address to the ALB. Create an Amazon Route 53 simple record with the Elastic IP address as the value. Create a Route 53 health check. In the case of a failed health check, recreate the ALB in different subnets.

C

VPC Basics – NAT Gateway

- Managed NAT solution, bandwidth scales automatically
- Resilient to failure within a single AZ
- Must deploy multiple NAT Gateways in multiple AZ for HA
- Has an Elastic IP, external services see the IP of the NAT Gateway as the source



Private Subnet → Public Subnet + NAT Gateway + Elastic IP → Firewall allow Elastic IP → Onpremise network

Question 265:

A company uses AWS Organizations to manage more than 1,000 AWS accounts. The company has created a new developer organization. There are 540 developer member accounts that must be moved to the new developer organization. All accounts are set up with all the required information so that each account can be operated as a standalone account.

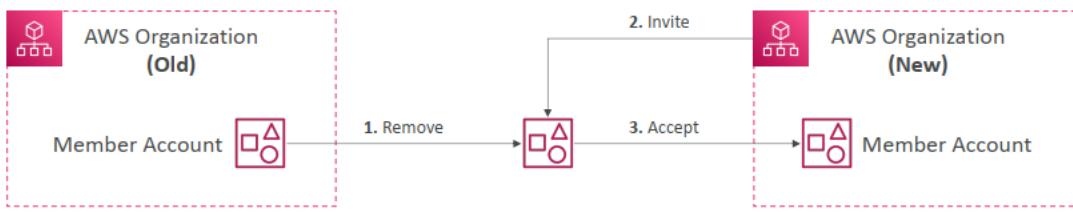
Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? (Choose three.)

- A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization.
- B. From the management account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.
- C. From each developer account, remove the account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.
- D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration.
- E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts.
- F. Have each developer sign in to their account and confirm to join the new developer organization.

B,E,F

AWS Organizations – Moving Accounts

1. Remove the member account from the AWS Organization
2. Send an invite to the member account from the AWS Organization
3. Accept the invite to the new Organization from the member account



Question 266:

A company's interactive web application uses an Amazon CloudFront distribution to serve images from an Amazon S3 bucket. Occasionally, third-party tools ingest corrupted images into the S3 bucket. This image corruption causes a poor user experience in the application later. The company has successfully implemented and tested Python logic to detect corrupt images.

A solutions architect must recommend a solution to integrate the detection logic with minimal latency between the ingestion and serving.

Which solution will meet these requirements?

- A. Use a Lambda@Edge function that is invoked by a viewer-response event.
- B. Use a Lambda@Edge function that is invoked by an origin-response event.
- C. Use an S3 event notification that invokes an AWS Lambda function.
- D. Use an S3 event notification that invokes an AWS Step Functions state machine.

C

<https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html>

tested Python logic to detect corrupt images → using lambda function

The requirement here is to catch and deal with the corruption at the time of ingestion. Hence, the logical place to put the check would be where the ingestion is actually happening, which is when the image is put into the S3 bucket. Amazon S3 can be configured to send an event notification when a new object is created (i.e., put into the bucket). This event can then trigger a Lambda function that uses the Python logic to check the image for corruption. This way, you are catching and dealing with any issues as soon as the image is ingested.

Question 267:

A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events.

When the company deploys new application code versions, the company installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group. The application is set to go live within the next 24 hours.

What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?

- A. Configure Amazon EventBridge to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group. Code the Lambda function to associate the EC2 instances with the CodeDeploy deployment group.
- B. Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches. Resume Amazon EC2 Auto Scaling operations.
- C. Create a new AWS CodeBuild project that creates a new AMI that contains the new code. Configure CodeBuild to update the Auto Scaling group's launch template to the new AMI. Run an Amazon EC2 Auto Scaling instance refresh operation.

D. Create a new AMI that has the CodeDeploy agent installed. Configure the Auto Scaling group's launch template to use the new AMI. Associate the CodeDeploy deployment group with the Auto Scaling group instead of the EC2 instances.

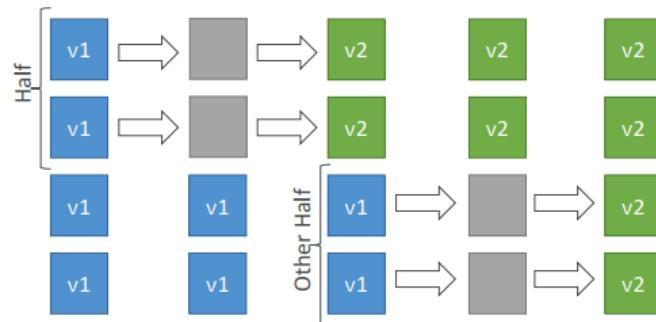
D

The application is set to go live within the next 24 hours and LEAST amount of operational overhead → leverage CodeDeploy

<https://aws.amazon.com/blogs/devops/under-the-hood-aws-codedeploy-and-auto-scaling-integration/>

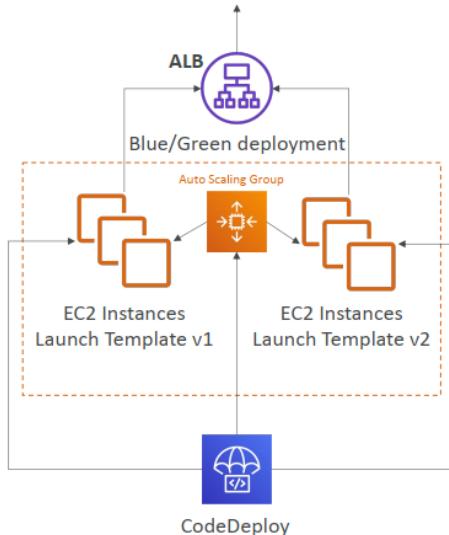
CodeDeploy to EC2

- Define how to deploy the application using `appspec.yml` + deployment strategy
- Will do in-place update to your fleet of EC2 instances
- Can use hooks to verify the deployment after each deployment phase



CodeDeploy to ASG

- In place updates:
 - Updates current existing EC2 instances
 - Instances newly created by an ASG will also get automated deployments
- Blue / green deployment:
 - A new auto-scaling group is created (settings are copied)
 - Choose how long to keep the old instances
 - Must be using an ELB



Question 268:

A company has a website that runs on four Amazon EC2 instances that are behind an Application Load Balancer (ALB). When the ALB detects that an EC2 instance is no longer available, an Amazon CloudWatch alarm enters the ALARM state. A member of the company's operations team then manually adds a new EC2 instance behind the ALB.

A solutions architect needs to design a highly available solution that automatically handles the replacement of EC2 instances. The company needs to minimize downtime during the switch to the new solution.

Which set of steps should the solutions architect take to meet these requirements?

- A. Delete the existing ALB. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Attach the existing EC2 instances to the Auto Scaling group.
- B. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. Attach the existing EC2 instances to the Auto Scaling group.
- C. Delete the existing ALB and the EC2 instances. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Wait for the Auto Scaling group to launch the minimum number of EC2 instances.
- D. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. Wait for the existing ALB to register the existing EC2 instances with the Auto Scaling group.

B

minimize downtime → A,C are incorrect because need to delete the ALB.

Wait for the existing ALB to register the existing EC2 instances with the Auto Scaling group → D is incorrect causing delay

Auto Scaling groups are designed to ensure that you are running your desired number of Amazon EC2 instances. It also can automatically replace any instances that fail or are unhealthy based on health checks. You can specify the minimum, maximum, and desired number of instances in your Auto Scaling group. By attaching a new launch template to the Auto Scaling group, the Auto Scaling group knows what configuration to use for the new instances it launches. There's no need to delete the existing ALB as suggested in options A and C. The ALB is still functional and will work with the newly created Auto Scaling group. You can directly attach the Auto Scaling group to the existing ALB.

Application Load Balancer (v2)

Target Groups

- EC2 instances (can be managed by an Auto Scaling Group) – HTTP
- ECS tasks (managed by ECS itself) – HTTP
- Lambda functions – HTTP request is translated into a JSON event
- IP Addresses – must be private IPs

- ALB can route to multiple target groups
- Health checks are at the target group level

Question 269:

A company wants to optimize AWS data-transfer costs and compute costs across developer accounts within the company's organization in AWS Organizations. Developers can configure VPCs and launch Amazon EC2 instances in a single AWS Region. The EC2 instances retrieve approximately 1 TB of data each day from Amazon S3.

The developer activity leads to excessive monthly data-transfer charges and NAT gateway processing charges between EC2 instances and S3 buckets, along with high compute costs. The company wants to proactively enforce approved architectural patterns for any EC2 instance and VPC infrastructure that developers deploy within the AWS accounts. The company does not want this enforcement to negatively affect the speed at which the developers can perform their tasks.

Which solution will meet these requirements MOST cost-effectively?

A. Create SCPs to prevent developers from launching unapproved EC2 instance types. Provide the developers with an AWS CloudFormation template to deploy an approved VPC configuration with S3 interface endpoints. Scope the developers' IAM permissions so that the developers can launch VPC resources only with CloudFormation.

B. Create a daily forecasted budget with AWS Budgets to monitor EC2 compute costs and S3 data-transfer costs across the developer accounts. When the forecasted cost is 75% of the actual budget cost, send an alert to the developer teams. If the actual budget cost is 100%, create a budget action to terminate the developers' EC2 instances and VPC infrastructure.

C. Create an AWS Service Catalog portfolio that users can use to create an approved VPC configuration with S3 gateway endpoints and approved EC2 instances. Share the portfolio with the developer accounts. Configure an AWS Service Catalog launch constraint to use an approved IAM role. Scope the developers' IAM permissions to allow access only to AWS Service Catalog.

D. Create and deploy AWS Config rules to monitor the compliance of EC2 and VPC resources in the developer AWS accounts. If developers launch unapproved EC2 instances or if developers create VPCs without S3 gateway endpoints, perform a remediation action to terminate the unapproved resources.

C

C is the effective way. A is incorrect because it can allow users to create resources that are defined outside of CloudFormation

AWS Service Catalog



- Users that are new to AWS have too many options, and may create stacks that are not compliant / in line with the rest of the organization
- Some users just want a quick self-service portal to launch a set of authorized products pre-defined by admins
- Includes: virtual machines, databases, storage options, etc...
- Enter AWS Service Catalog!

AWS Service Catalog là một dịch vụ của Amazon Web Services cho phép tổ chức tạo, quản lý và triển khai các danh mục dịch vụ đã được phê duyệt trong AWS. Nó giúp các tổ chức kiểm soát chặt chẽ các tài nguyên AWS mà nhân viên và nhóm của họ có thể triển khai, đảm bảo tuân thủ các chính sách của công ty và tiêu chuẩn bảo mật.

Các đặc điểm chính của AWS Service Catalog:

1. **Tạo và quản lý danh mục dịch vụ:** Bạn có thể tạo và quản lý danh mục các sản phẩm AWS đã được phê duyệt như máy chủ EC2, cơ sở dữ liệu RDS, các ứng dụng phần mềm tùy chỉnh, v.v.

2. **Kiểm soát quyền truy cập:** Cho phép bạn kiểm soát ai có thể truy cập và triển khai các sản phẩm trong danh mục, đảm bảo rằng chỉ những người được phép mới có thể sử dụng các tài nguyên cụ thể.
3. **Đảm bảo tuân thủ:** Đảm bảo rằng các tài nguyên được triển khai tuân thủ các chính sách và quy định của tổ chức bằng cách sử dụng các mẫu CloudFormation đã được kiểm định.
4. **Theo dõi và quản lý tài nguyên:** Cung cấp khả năng theo dõi và quản lý tài nguyên được triển khai từ một nơi duy nhất, giúp dễ dàng theo dõi việc sử dụng và chi phí.

Lợi ích chính:

- **Tính nhất quán:** Đảm bảo rằng tất cả các triển khai đều tuân theo các mẫu và tiêu chuẩn đã được định nghĩa trước.
- **Tiết kiệm thời gian:** Giảm thời gian triển khai bằng cách sử dụng các sản phẩm và cấu hình đã được phê duyệt sẵn.
- **Bảo mật và kiểm soát:** Tăng cường bảo mật và kiểm soát thông qua quản lý quyền truy cập và kiểm định tài nguyên.

AWS Service Catalog giúp các tổ chức quản lý hiệu quả các tài nguyên AWS, đảm bảo tuân thủ và bảo mật, đồng thời tăng cường tính nhất quán và hiệu quả trong việc triển khai các dịch vụ AWS.

Question 270:

A company is expanding. The company plans to separate its resources into hundreds of different AWS accounts in multiple AWS Regions. A solutions architect must recommend a solution that denies access to any operations outside of specifically designated Regions.

Which solution will meet these requirements?

- Create IAM roles for each account. Create IAM policies with conditional allow permissions that include only approved Regions for the accounts.
- Create an organization in AWS Organizations. Create IAM users for each account. Attach a policy to each user to block access to Regions where an account cannot deploy infrastructure.
- Launch an AWS Control Tower landing zone. Create OUs and attach SCPs that deny access to run services outside of the approved Regions.
- Enable AWS Security Hub in each account. Create controls to specify the Regions where an account can deploy infrastructure.

C

B is incorrect as it is too difficult to maintain. C is correct answer.

For this type of question (organization and policy for many accounts), we avoid options that require actions on each account/user. There's always better option to set policies at one place.

AWS Control Tower



- Easy way to set up and govern a secure and compliant multi-account AWS environment based on best practices
- Benefits:
 - Automate the set up of your environment in a few clicks
 - Automate ongoing policy management using guardrails
 - Detect policy violations and remediate them
 - Monitor compliance through an interactive dashboard
- AWS Control Tower runs on top of AWS Organizations:
 - It automatically sets up AWS Organizations to organize accounts and implement SCPs (Service Control Policies)

Automate Ongoing Policy Management Using Guardrails

Guardrails là gì?

Guardrails trong AWS Control Tower là các chính sách bảo mật và tuân thủ được định nghĩa trước để giúp đảm bảo rằng môi trường AWS của bạn luôn tuân thủ các tiêu chuẩn tốt nhất. Guardrails có thể là bắt buộc (mandatory) hoặc tùy chọn (advisory).

Lợi ích của việc sử dụng Guardrails

1. **Tự động hóa quản lý chính sách:**
 - **Thiết lập ban đầu:** Khi bạn thiết lập AWS Control Tower, các guardrails được kích hoạt tự động để thiết lập các chính sách bảo mật và tuân thủ trên các tài khoản AWS của bạn.
 - **Quản lý liên tục:** Guardrails liên tục giám sát và thực thi các chính sách để đảm bảo rằng các tài khoản và tài nguyên luôn tuân thủ các tiêu chuẩn đã được định nghĩa.
2. **Đảm bảo tuân thủ:**
 - Guardrails giúp đảm bảo rằng môi trường AWS của bạn tuân thủ các quy định bảo mật và tuân thủ mà tổ chức của bạn yêu cầu. Điều này bao gồm các tiêu chuẩn bảo mật nội bộ và các quy định bên ngoài như GDPR, HIPAA, v.v.
3. **Giảm thiểu rủi ro:**
 - Bằng cách tự động thực thi các chính sách bảo mật và tuân thủ, guardrails giúp giảm thiểu rủi ro liên quan đến cấu hình sai hoặc các hành động không tuân thủ quy định của người dùng.
4. **Tiết kiệm thời gian và công sức:**
 - Thay vì phải quản lý và giám sát thủ công các chính sách bảo mật và tuân thủ trên mỗi tài khoản AWS, guardrails tự động hóa quá trình này, giúp tiết kiệm thời gian và công sức cho nhóm quản trị.
5. **Giám sát và báo cáo:**

- AWS Control Tower cung cấp các công cụ giám sát và báo cáo để bạn có thể dễ dàng theo dõi việc tuân thủ các guardrails. Bạn có thể xem các vi phạm chính sách và hành động cần thiết để khắc phục.

Ví dụ cụ thể về Guardrails

- **Mandatory Guardrails:**
 - Ví dụ: Bật mã hóa S3 buckets bằng SSE (Server-Side Encryption).
 - Điều này đảm bảo rằng tất cả các dữ liệu trong S3 luôn được mã hóa, giúp bảo vệ dữ liệu khỏi truy cập trái phép.
- **Advisory Guardrails:**
 - Ví dụ: Khuyến nghị bật CloudTrail cho tất cả các tài khoản để theo dõi hoạt động API.
 - Guardrail này không bắt buộc nhưng cung cấp hướng dẫn tốt nhất để tăng cường bảo mật và giám sát.

Kết luận

Tự động hóa quản lý chính sách liên tục bằng cách sử dụng guardrails trong AWS Control Tower mang lại nhiều lợi ích quan trọng như:

- Đảm bảo tuân thủ các tiêu chuẩn bảo mật và quy định.
- Giảm thiểu rủi ro và sai sót do cấu hình thủ công.
- Tiết kiệm thời gian và công sức trong việc quản lý và giám sát.
- Cung cấp giám sát và báo cáo liên tục để theo dõi và khắc phục các vi phạm chính sách.

Guardrails giúp bạn duy trì một môi trường AWS an toàn, tuân thủ và hiệu quả, đồng thời đơn giản hóa việc quản lý chính sách bảo mật và tuân thủ.

Question 271:

A company wants to refactor its retail ordering web application that currently has a load-balanced Amazon EC2 instance fleet for web hosting, database API services, and business logic. The company needs to create a decoupled, scalable architecture with a mechanism for retaining failed orders while also minimizing operational costs.

Which solution will meet these requirements?

- A. Use Amazon S3 for web hosting with Amazon API Gateway for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use Amazon Elastic Container Service (Amazon ECS) for business logic with Amazon SQS long polling for retaining failed orders.
- B. Use AWS Elastic Beanstalk for web hosting with Amazon API Gateway for database API services. Use Amazon MQ for order queuing. Use AWS Step Functions for business logic with Amazon S3 Glacier Deep Archive for retaining failed orders.
- C. Use Amazon S3 for web hosting with AWS AppSync for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use AWS Lambda for business logic with an Amazon SQS dead-letter queue for retaining failed orders.
- D. Use Amazon Lightsail for web hosting with AWS AppSync for database API services. Use Amazon Simple Email Service (Amazon SES) for order queuing. Use Amazon Elastic Kubernetes Service (Amazon EKS) for business logic with Amazon OpenSearch Service for retaining failed orders.

C

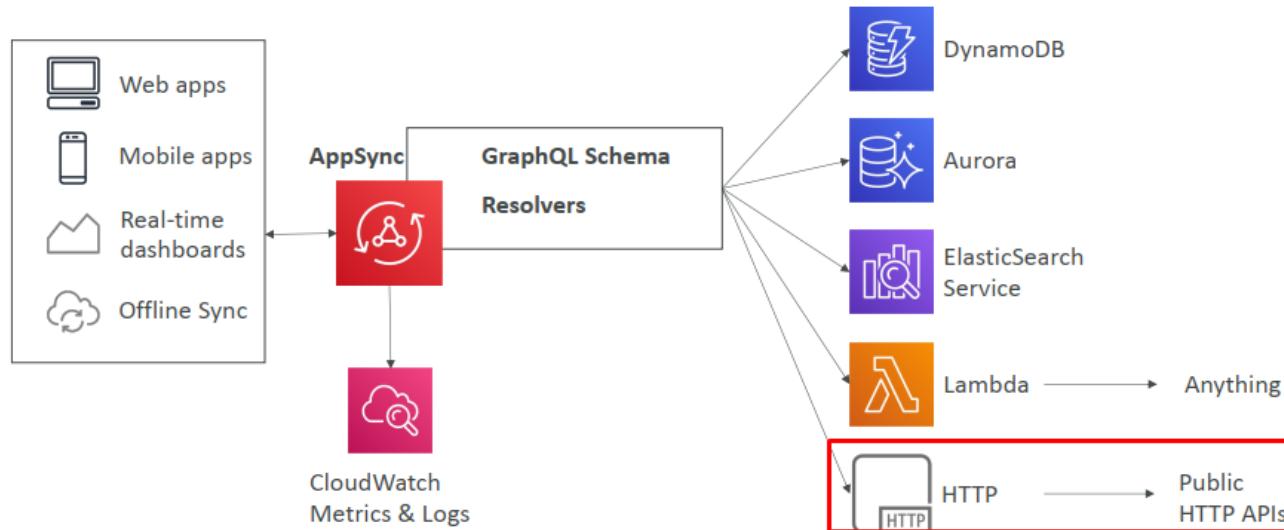
a mechanism for retaining failed orders while also minimizing operational costs → SQS dead-letter queue
database API service → AppSync

AWS AppSync - Overview



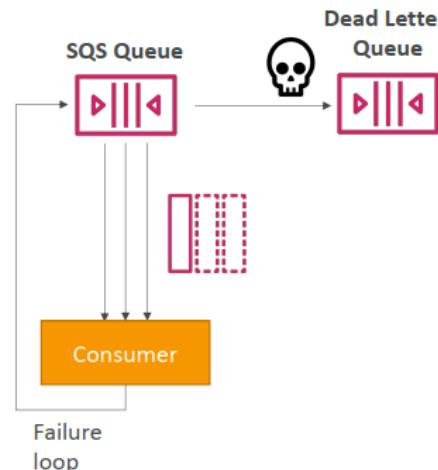
- AppSync is a managed service that uses **GraphQL**
- GraphQL makes it easy for applications to get exactly the data they need.
- This includes combining data from **one or more sources**
 - NoSQL data stores, Relational databases, HTTP APIs...
 - Integrates with DynamoDB, Aurora, Elasticsearch & others
 - Custom sources with AWS Lambda
- **Retrieve data in real-time with WebSocket or MQTT on WebSocket**
- For mobile apps: local data access & data synchronization
- It all starts with uploading one **GraphQL schema**

AppSync Diagram



Amazon SQS – Dead Letter Queue (DLQ)

- If a consumer fails to process a message within the Visibility Timeout...
the message goes back to the queue!
- We can set a threshold of how many times a message can go back to the queue
- After the `MaximumReceives` threshold is exceeded, the message goes into a Dead Letter Queue (DLQ)
- Useful for debugging!
- DLQ of a FIFO queue must also be a FIFO queue
- DLQ of a Standard queue must also be a Standard queue
- Make sure to process the messages in the DLQ before they expire:
 - Good to set a retention of 14 days in the DLQ



Amazon SQS long polling → <https://trello.com/c/HtomJQGo/397-sqs-solution-architecture-idempotency>

Question 272:

A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in a MySQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west-2, and has configured Amazon Route 53 health checks and DNS failover to us-west-2.

Which additional step should the solutions architect take?

- Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us-west-2.
- Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2.
- Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment.
- Create a MySQL standby database on an Amazon EC2 instance in us-west-2.

B

<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>

AWS database service	Replication method to DR Region	Possible standby classification	RTO	RPO
Amazon RDS for MySQL	Cross-Region read replica	1. Pilot light 2. Warm standby with capability for read traffic	Usually minutes. Automation can minimize delays.	Typically under 1 second
Amazon RDS for PostgreSQL	Cross-Region read replica	1. Pilot light 2. Warm standby with capability for read traffic	Usually minutes. Automation can minimize delays.	Typically under 1 second
Amazon RDS for MariaDB	Cross-Region read replica	1. Pilot light 2. Warm standby with capability for read traffic	Usually minutes. Automation can minimize delays.	Typically under 1 second
Amazon RDS for Db2	Multi-AZ or IBM Q Replication (should be set up separately; not part of the managed service)	1. Cold standby 2. Hot standby using IBM Q Replication	Usually minutes.	Usually minutes for Multi-AZ; zero for IBM Q Replication
Amazon Aurora MySQL-Compatible Edition	Global database has secondary cluster(s) in a different Region	1. Hot standby with capability to support read traffic 2. Warm standby with capability to support read traffic	Typically under 1 minute.	Typically under 1 second
Amazon Aurora PostgreSQL-Compatible Edition	Global database has secondary cluster(s) in a different Region	1. Hot standby with capability to support read traffic 2. Warm standby with capability to support read traffic	Typically under 1 minute.	Typically under 1 second
Amazon DocumentDB (with MongoDB compatibility)	Global cluster has secondary cluster(s) in a different Region	1. Hot standby with capability to support read traffic 2. Warm standby with capability to support read traffic	Typically under 1 minute.	In seconds
Amazon ElastiCache for Redis	Global datastore has a secondary cluster in a different Region	1. Hot standby with capability to support read traffic 2. Warm standby with capability to support read traffic	Usually minutes. Automation can minimize delays.	In seconds
Amazon DynamoDB	DynamoDB global tables [Active/active configuration accepts write operations in secondary Region	Zero or near zero.	Sub-second
Amazon RDS for Oracle	Read replica promotion across Regions [(Oracle Enterprise Edition and Active Data Guard)	1. Pilot light 2. Warm standby with capability for read traffic	Usually minutes.	Usually minutes
Amazon RDS for Oracle (alternative)	Mounted read replica promotion across Regions [(Oracle Enterprise Edition)	1. Pilot light 2. Warm standby (doesn't allow read queries)	Usually minutes.	Usually minutes
Amazon RDS for SQL Server	Cross-Region read replica (Microsoft SQL Server Enterprise Edition 2016-2019)	1. Pilot light 2. Warm standby with capability for read traffic	Usually minutes. Automation can minimize delays.	Typically under 1 second

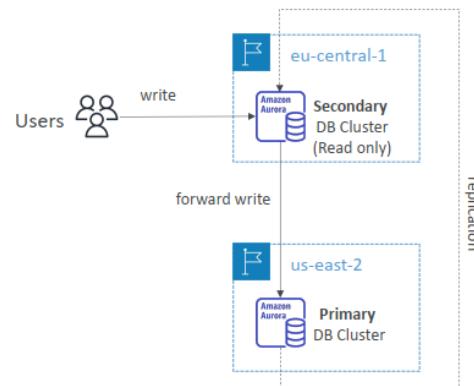
Global Aurora

- Aurora Cross Region Read Replicas
 - Useful for disaster recovery
 - Simple to put in place
- Aurora Global Database (recommended)
 - 1 Primary Region (read / write)
 - Up to 5 secondary (read-only) regions, replication lag is less than 1 second
 - Up to 16 Read Replicas per secondary region
 - Helps for decreasing latency
 - Promoting another region (for disaster recovery) has an RTO of < 1 minute
 - Ability to manage the RPO in Aurora for PostgreSQL



Aurora Global – Write Forwarding

- Enables Secondary DB Clusters to forward SQL statements that perform write operations to the Primary DB Cluster
- Data is always changed first on the Primary DB Cluster; then replicated to the Secondary DB Clusters
- Primary DB Cluster always has an up-to-date copy of all data
- Reduces the number of endpoints to manage



RDS read replica vs Aurora Global: <https://trello.com/c/o7VmUIAX/398-rds-read-replica-vs-aurora-global>

Question 273:

A company is using AWS Organizations to manage multiple accounts. Due to regulatory requirements, the company wants to restrict specific member accounts to certain AWS Regions, where they are permitted to deploy resources. The resources in the accounts must be tagged, enforced based on a group standard, and centrally managed with minimal configuration.

What should a solutions architect do to meet these requirements?

- A. Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy.
- B. From the AWS Billing and Cost Management console, in the management account, disable Regions for the specific member accounts and apply a tag policy on the root.
- C. Associate the specific member accounts with the root. Apply a tag policy and an SCP using conditions to limit Regions.
- D. Associate the specific member accounts with a new OU. Apply a tag policy and an SCP using conditions to limit Regions.

D

Always SCPs for OUs to confine accounts from using services

Service Control Policies (SCP)

- Define allowlist or blocklist IAM actions
- Applied at the OU or Account level
- Does not apply to the Management Account
- SCP is applied to all the Users and Roles in the account, including Root user
- The SCP does not affect Service-linked roles
 - Service-linked roles enable other AWS services to integrate with AWS Organizations and can't be restricted by SCPs.
- SCP must have an explicit Allow (does not allow anything by default)
(adj): rõ ràng, rành mạch
- Use cases:
 - Restrict access to certain services (for example: can't use EMR)
 - Enforce PCI compliance by explicitly disabling services

Question 274:

A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.

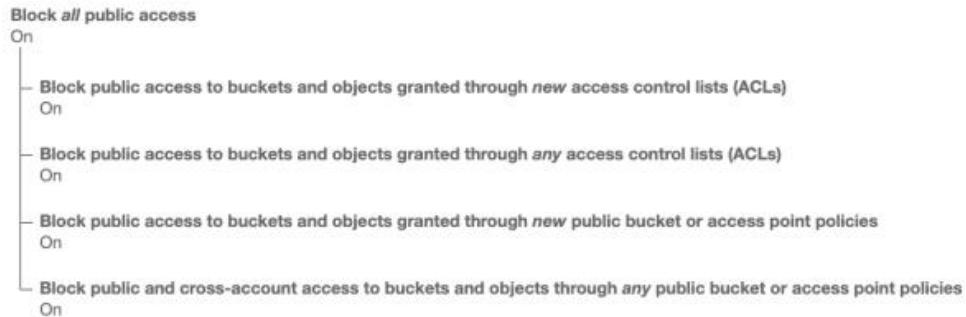
Which set of actions will immediately remediate the security issue without impacting the application's normal workflow?

- A. Create an AWS Lambda function that applies a deny all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function.
- B. Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions.
- C. Run a script that puts a private ACL on all of the objects in the bucket.
- D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket.

D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html>

Bucket settings for Block Public Access



- These settings were created to prevent company data leaks
- If you know your bucket should never be public, leave these on
- Can be set at the account level

Question 275:

A company is planning to migrate an Amazon RDS for Oracle database to an RDS for PostgreSQL DB instance in another AWS account. A solutions architect needs to design a migration strategy that will require no downtime and that will minimize the amount of time necessary to complete the migration. The migration strategy must replicate all existing data and any new data that is created during the migration. The target database must be identical to the source database at completion of the migration process.

All applications currently use an Amazon Route 53 CNAME record as their endpoint for communication with the RDS for Oracle DB instance. The RDS for Oracle DB instance is in a private subnet.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- Create a new RDS for PostgreSQL DB instance in the target account. Use the AWS Schema Conversion Tool (AWS SCT) to migrate the database schema from the source database to the target database.
- Use the AWS Schema Conversion Tool (AWS SCT) to create a new RDS for PostgreSQL DB instance in the target account with the schema and initial data from the source database.

C. Configure VPC peering between the VPCs in the two AWS accounts to provide connectivity to both DB instances from the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.

D. Temporarily allow the source DB instance to be publicly accessible to provide connectivity from the VPC in the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.

E. Use AWS Database Migration Service (AWS DMS) in the target account to perform a full load plus change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint.

F. Use AWS Database Migration Service (AWS DMS) in the target account to perform a change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint.

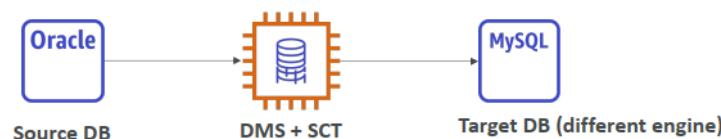
A,C,E

Step 1: migrate schema

Step 2: migrate database

AWS Schema Conversion Tool (SCT)

- Convert your Database's Schema from one engine to another
- Example OLTP: (SQL Server or Oracle) to MySQL, PostgreSQL, Aurora
- Example OLAP: (Teradata or Oracle) to Amazon Redshift

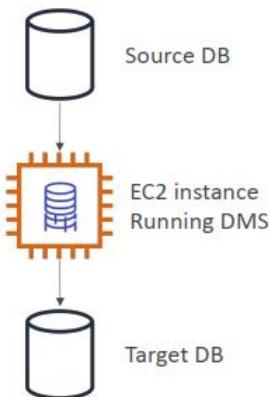


- You do not need to use SCT if you are migrating the same DB engine
 - Ex: on-premises PostgreSQL => RDS PostgreSQL
 - The DB engine is still PostgreSQL (RDS is the platform)

DMS – Database Migration Service



- Quickly and securely migrate databases to AWS, resilient, self healing
- The source database remains available during the migration
- Supports:
 - Homogeneous migrations: ex Oracle to Oracle
 - Heterogeneous migrations: ex Microsoft SQL Server to Aurora
- **Continuous Data Replication using CDC**
- You must create an EC2 instance to perform the replication tasks



DMS – Good things to know

- Works over VPC Peering, VPN (site to site, software), Direct Connect
- Supports Full Load, Full Load + CDC, or CDC only
- **Oracle:**
 - Source: Supports TDE for the source using “BinaryReader”
 - Target: Supports BLOBs in tables that have a primary key, and TDE
- **OpenSearch:**
 - Source: does not exist
 - Target: possible to migrate from a relational database using DMS
 - Therefore, DMS cannot be used to replicate OpenSearch data

Question 276:

A company has implemented an ordering system using an event-driven architecture. During initial testing, the system stopped processing orders. Further log analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SQS) standard queue was causing an error on the backend and blocking all subsequent order messages. The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages.

Which step should the solutions architect take to meet these requirements?

- A. Increase the backend processing timeout to 30 seconds to match the visibility timeout.
- B. Reduce the visibility timeout of the queue to automatically remove the faulty message.
- C. Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages.
- D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages.

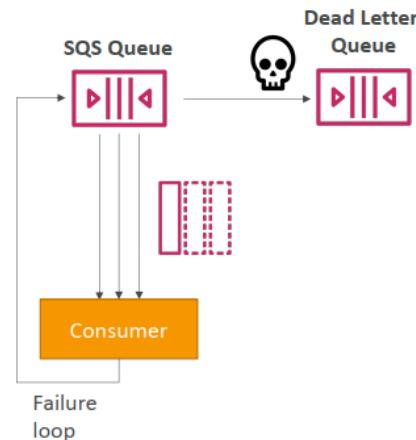
D
ensure that the system continues to process subsequent messages → SQS standard

- **SQS FIFO:**

- receive messages in order they were sent Nhận message theo thứ tự được gửi
- 300 messages/s without batching, 3000 /s with batching

Amazon SQS – Dead Letter Queue (DLQ)

- If a consumer fails to process a message within the Visibility Timeout...
the message goes back to the queue!
- We can set a threshold of how many times a message can go back to the queue
- After the MaximumReceives threshold is exceeded, the message goes into a Dead Letter Queue (DLQ)
- Useful for debugging!
- DLQ of a FIFO queue must also be a FIFO queue
- DLQ of a Standard queue must also be a Standard queue
- Make sure to process the messages in the DLQ before they expire:
 - Good to set a retention of 14 days in the DLQ



Question 277:

A company has automated the nightly retraining of its machine learning models by using AWS Step Functions. The workflow consists of multiple steps that use AWS Lambda. Each step can fail for various reasons, and any failure causes a failure of the overall workflow.

A review reveals that the retraining has failed multiple nights in a row without the company noticing the failure. A solutions architect needs to improve the workflow so that notifications are sent for all types of failures in the retraining process.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic with a subscription of type "Email" that targets the team's mailing list.
- B. Create a task named "Email" that forwards the input arguments to the SNS topic.
- C. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": ["States.ALL"] and "Next": "Email".
- D. Add a new email address to Amazon Simple Email Service (Amazon SES). Verify the email address.
- E. Create a task named "Email" that forwards the input arguments to the SES email address.
- F. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": ["States.Runtime"] and "Next": "Email".

A,B,C

notifications are sent for all types of failures → C "ErrorEquals": ["States.ALL"]

In AWS Step Functions, each state reports heartbeat failure, timeout failure, and all other types of failures. Therefore, to catch all errors, the solutions architect should add a Catch field to all Task, Map, and Parallel states with a statement of "ErrorEquals": ["States.ALL"], and "Next": "Email". Then, a task named "Email" can be created to forward the input arguments to an SNS topic that sends notifications to the team's email.

DE are incorrect because SES cannot be used here. SES can be good for Bulk/Marketing emails

F is incorrect because the error type "States.Runtime" doesn't catch all types of errors

Question 278

A company plans to deploy a new private intranet service on Amazon EC2 instances inside a VPC. An AWS Site-to-Site VPN connects the VPC to the company's on-premises network. The new service must communicate with existing on-premises services. The on-premises services are accessible through the use of hostnames that reside in the company.example DNS zone. This DNS zone is wholly hosted on premises and is available only on the company's private network.

A solutions architect must ensure that the new service can resolve hostnames on the company.example domain to integrate with existing services.

Which solution meets these requirements?

- A. Create an empty private zone in Amazon Route 53 for company.example. Add an additional NS record to the company's on-premises company.example zone that points to the authoritative name servers for the new private zone in Route 53.

- B. Turn on DNS hostnames for the VPC. Configure a new outbound endpoint with Amazon Route 53 Resolver. Create a Resolver rule to forward requests for company.example to the on-premises name servers.
- C. Turn on DNS hostnames for the VPC. Configure a new inbound resolver endpoint with Amazon Route 53 Resolver. Configure the on-premises DNS server to forward requests for company.example to the new resolver.
- D. Use AWS Systems Manager to configure a run document that will install a hosts file that contains any required hostnames. Use an Amazon EventBridge rule to run the document when an instance is entering the running state.

B

A solutions architect must ensure that the new service can resolve hostnames on the company.example domain to integrate with existing services → AWS Cloud → Onprem → outbound Resolver Endpoint

Amazon Route 53 Resolver Endpoints are used to integrate your on-premises networks with Amazon Route 53 Resolver, which is a recursive DNS service provided by AWS. These endpoints allow you to control how DNS queries are routed between your VPCs and your on-premises networks.

****Inbound Endpoint:****

- **Purpose:** Allows DNS queries from your on-premises network to be routed to your VPCs within AWS.
- **Usage:** When you create an inbound endpoint, Route 53 Resolver will listen for DNS queries from your on-premises network. This means that when a DNS query is sent from your on-premises environment, it can be resolved using the DNS rules and records within your VPC.
- **Example Use Case:** If you have a hybrid environment and you need to resolve DNS names for resources hosted in your AWS VPC from your on-premises network, you would use an inbound endpoint.

****Outbound Endpoint:****

- **Purpose:** Allows DNS queries from your VPCs within AWS to be routed to your on-premises network or another DNS service.
- **Usage:** When you create an outbound endpoint, Route 53 Resolver forwards DNS queries from your VPC to your on-premises DNS servers. This means that when a DNS query cannot be resolved within your VPC, it can be forwarded to your on-premises network for resolution.
- **Example Use Case:** If you have internal DNS names or services hosted on your on-premises network that need to be resolved by resources within your VPC, you would use an outbound endpoint.

****How They Work Together:****

- **Hybrid DNS Resolution:** By combining inbound and outbound endpoints, you can achieve seamless DNS resolution across your entire hybrid environment. DNS queries originating from either the on-premises network or the VPC can be resolved using the appropriate DNS servers and rules.

Diagram

...

On-Premises Network <----> Inbound Endpoint <----> Route 53 Resolver <----> Outbound Endpoint <----> On-Premises DNS Server

...

1. **Inbound Endpoint:** Accepts DNS queries from on-premises and forwards them to Route 53 Resolver.

2. **Route 53 Resolver:** Processes the DNS queries based on VPC DNS rules.

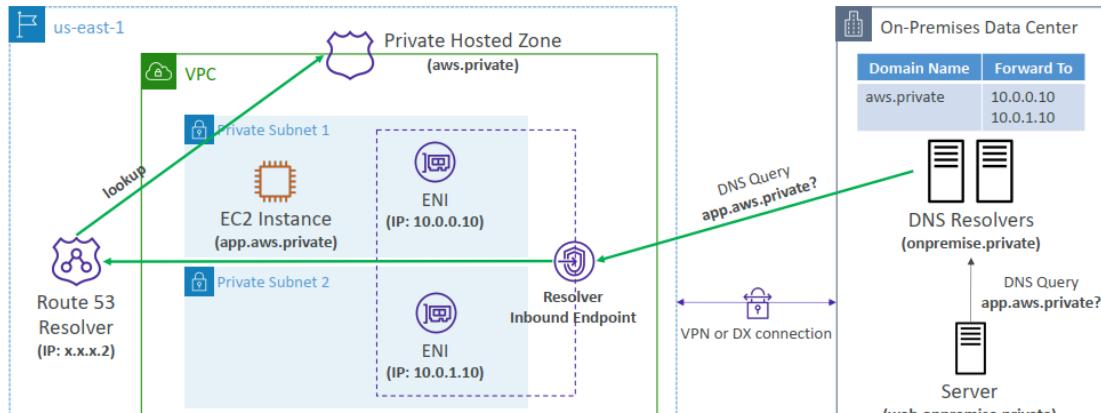
3. **Outbound Endpoint:** Forwards unresolved DNS queries from Route 53 Resolver to the on-premises DNS server.

This setup ensures that both on-premises and AWS VPC environments can resolve DNS queries for each other's resources efficiently.

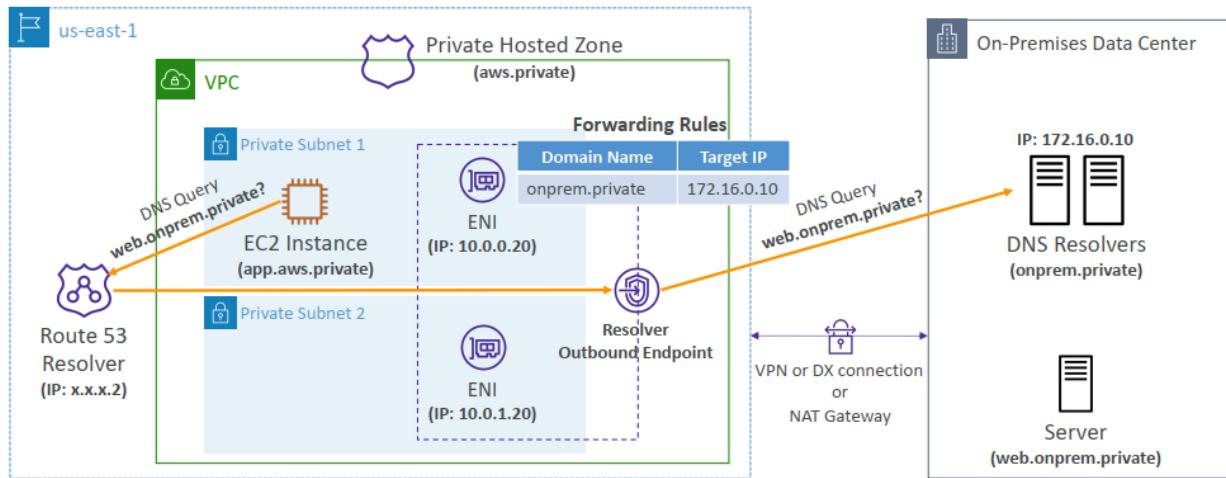
Route 53 – Resolver Endpoints

- Inbound Endpoint
 - DNS Resolvers on your network can forward DNS queries to Route 53 Resolver
 - Allows your DNS Resolvers to resolve domain names for AWS resources (e.g., EC2 instances) and records in Route 53 Private Hosted Zones
- Outbound Endpoint chuyển tiếp có điều kiện
 - Route 53 Resolver conditionally forwards DNS queries to your DNS Resolvers
 - Use Resolver Rules to forward DNS queries to your DNS Resolvers
- Associated with one or more VPCs in the same AWS Region
- Create in two AZs for high availability
- Each Endpoint supports 10,000 queries per second per IP address

Route 53 – Resolver Inbound Endpoints



Route 53 – Resolver Outbound Endpoints



Question 279:

A company uses AWS CloudFormation to deploy applications within multiple VPCs that are all attached to a transit gateway. Each VPC that sends traffic to the public internet must send the traffic through a shared services VPC. Each subnet within a VPC uses the default VPC route table, and the traffic is routed to the transit gateway. The transit gateway uses its default route table for any VPC attachment.

A security audit reveals that an Amazon EC2 instance that is deployed within a VPC can communicate with an EC2 instance that is deployed in any of the company's other VPCs. A solutions architect needs to limit the traffic between the VPCs. Each VPC must be able to communicate only with a predefined, limited set of authorized VPCs.

What should the solutions architect do to meet these requirements?

- A. Update the network ACL of each subnet within a VPC to allow outbound traffic only to the authorized VPCs. Remove all deny rules except the default deny rule.
- B. Update all the security groups that are used within a VPC to deny outbound traffic to security groups that are used within the unauthorized VPCs.
- C. Create a dedicated transit gateway route table for each VPC attachment. Route traffic only to the authorized VPCs.
- D. Update the main route table of each VPC to route traffic only to the authorized VPCs through the transit gateway.

C

Since TGW is responsible for VPCs communicating with each other, there should be default routes for each VPC attachment on the TGW route table limiting access to VPCs

Question 280:

A company has a Windows-based desktop application that is packaged and deployed to the users' Windows machines. The company recently acquired another company that has employees who primarily use machines with a Linux operating system. The acquiring company has decided to migrate and rehost the Windows-based desktop application to AWS.

All employees must be authenticated before they use the application. The acquiring company uses Active Directory on premises but wants a simplified way to manage access to the application on AWS for all the employees.

Which solution will rehost the application on AWS with the LEAST development effort?

A. Set up and provision an Amazon Workspaces virtual desktop for every employee. Implement authentication by using Amazon Cognito identity pools. Instruct employees to run the application from their provisioned Workspaces virtual desktops.

B. Create an Auto Scaling group of Windows-based Amazon EC2 instances. Join each EC2 instance to the company's Active Directory domain. Implement authentication by using the Active Directory that is running on premises. Instruct employees to run the application by using a Windows remote desktop.

C. Use an Amazon AppStream 2.0 image builder to create an image that includes the application and the required configurations. Provision an AppStream 2.0 On-Demand fleet with dynamic Fleet Auto Scaling policies for running the image. Implement authentication by using AppStream 2.0 user pools. Instruct the employees to access the application by starting browser-based AppStream 2.0 streaming sessions.

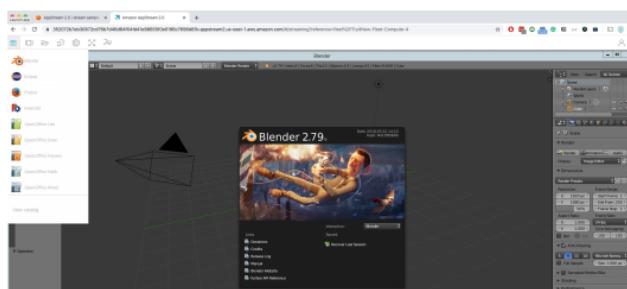
D. Refactor and containerize the application to run as a web-based application. Run the application in Amazon Elastic Container Service (Amazon ECS) on AWS Fargate with step scaling policies. Implement authentication by using Amazon Cognito user pools. Instruct the employees to run the application from their browsers.

C

Amazon AppStream 2.0



- Desktop Application Streaming Service
Cung cấp đến bất kỳ máy tính nào mà không cần mua sắm, cung cấp cơ sở hạ tầng
- Deliver to any computer, without acquiring, provisioning infrastructure
- The application is delivered from within a web browser



Amazon AppStream 2.0 vs WorkSpaces

- Workspaces
 - Fully managed VDI and desktop available
 - The users connect to the VDI and open native or WAM applications
 - Workspaces are on-demand or always on
- AppStream 2.0
 - Stream a desktop application to web browsers (no need to connect to a VDI)
 - Works with any device (that has a web browser)
 - Allow to configure an instance type per application type (CPU, RAM, GPU)

Question 281:

A company is collecting a large amount of data from a fleet of IoT devices. Data is stored as Optimized Row Columnar (ORC) files in the Hadoop Distributed File System (HDFS) on a persistent Amazon EMR cluster. The company's data analytics team queries the data by using SQL in Apache Presto deployed on the same EMR cluster. Queries scan large amounts of data, always run for less than 15 minutes, and run only between 5 PM and 10 PM.

The company is concerned about the high cost associated with the current solution. A solutions architect must propose the most cost-effective solution that will allow SQL data queries.

Which solution will meet these requirements?

- A. Store data in Amazon S3. Use Amazon Redshift Spectrum to query data.
- B. Store data in Amazon S3. Use the AWS Glue Data Catalog and Amazon Athena to query data.
- C. Store data in EMR File System (EMRFS). Use Presto in Amazon EMR to query data.
- D. Store data in Amazon Redshift. Use Amazon Redshift to query data.

B

Storing the data in Amazon S3 is a cost-effective solution compared to running a persistent EMR cluster with HDFS. The AWS Glue Data Catalog provides a centralized metadata repository for organizing and cataloging data in S3. Amazon Athena is a serverless query service that allows you to run SQL queries directly against data in S3 without the need for a dedicated cluster or infrastructure. By using Amazon Athena, you only pay for the queries you run, which aligns with the requirement of cost-effectiveness.

Question 282:

A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into details of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging. Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS instances.

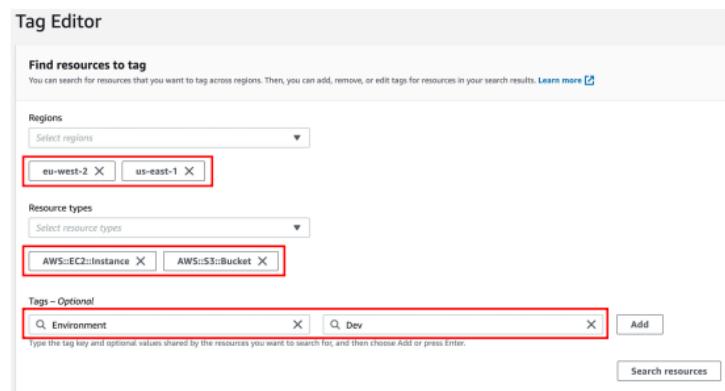
Which strategy should the solutions architect provide to meet these requirements?

- A. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources.
- B. Use an AWS Config rule to alert the finance team of untagged resources. Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role.
- C. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID. Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource.
- D. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources. Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource.

C

AWS Tag Editor

- Allows you to manage tags of multiple resources at once
- You can add/update/delete tags
- Search tagged/untagged resources in all AWS Regions



AWS Cost Allocation Tags

- With Tags we can track resources that relate to each other có thẻ theo dõi các resources có liên quan với nhau
- With Cost Allocation Tags we can enable detailed costing reports báo cáo chi phí chi tiết
- Just like Tags, but they show up as columns in Reports Hiển thị dạng cột
- AWS Generated Cost Allocation Tags
 - Automatically applied to the resource you create tự động áp dụng cho các tài nguyên đã tạo
 - Starts with Prefix aws: (e.g. aws: createdBy)
 - They're not applied to resources created before the activation không được áp dụng cho các tài nguyên tạo trước đó
- User tags
 - Defined by the user
 - Starts with Prefix user:
- Cost Allocation Tags just appear in the Billing Console
- Takes up to 24 hours for the tags to show up in the report Mất 24 giờ để tags hiển thị trong báo cáo

AWS Cost Allocation Tags: Là các nhãn (tags) bạn gán cho tài nguyên AWS để theo dõi và phân loại chi phí. Các nhãn này giúp bạn dễ dàng quản lý và tối ưu hóa chi phí bằng cách gán chi phí cho các dự án, bộ phận hoặc nhóm.

AWS Tag Editor: Là công cụ quản lý cho phép bạn dễ dàng tìm kiếm, xem và chỉnh sửa các nhãn (tags) trên tài nguyên AWS của mình. AWS Tag Editor hỗ trợ việc quản lý các nhãn đồng bộ và hiệu quả trên nhiều dịch vụ và tài nguyên khác nhau.

Question 283:

A company wants to send data from its on-premises systems to Amazon S3 buckets. The company created the S3 buckets in three different accounts. The company must send the data privately without the data traveling across the internet. The company has no existing dedicated connectivity to AWS.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

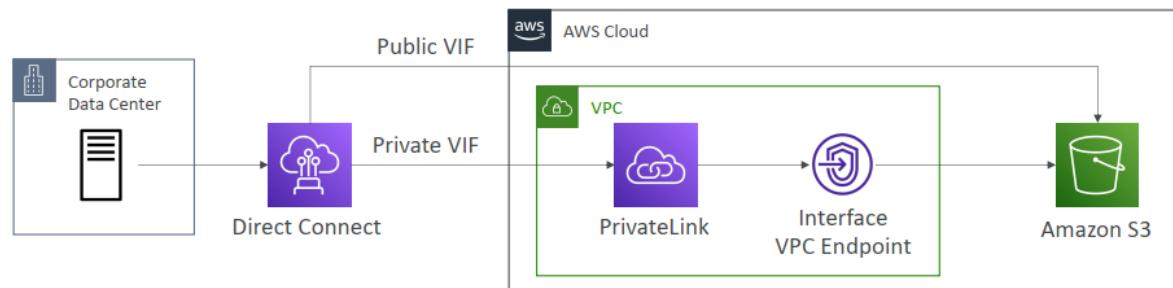
- Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a private VIF between the on-premises environment and the private VPC.
- Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a public VIF between the on-premises environment and the private VPC.
- Create an Amazon S3 interface endpoint in the networking account.

D. Create an Amazon S3 gateway endpoint in the networking account.

E. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Peer VPCs from the accounts that host the S3 buckets with the VPC in the network account.

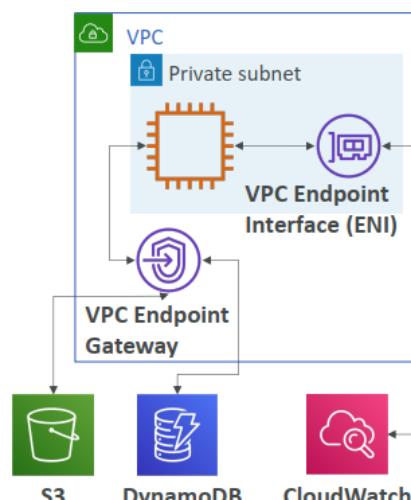
A,C

PrivateLink for Amazon S3 with Direct Connect



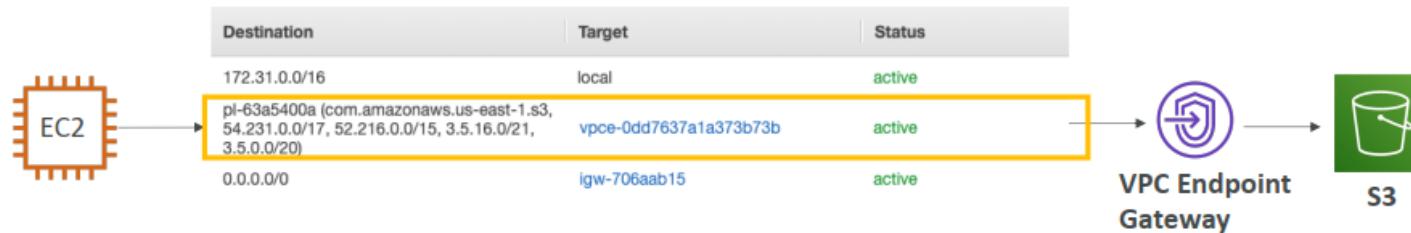
VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)**
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables



VPC Endpoint Gateway

- Only works for S3 and DynamoDB, must create one gateway per VPC
- Must update route tables entries
- Gateway is defined at the VPC level



- DNS resolution must be enabled in the VPC
- The same public hostname for S3 can be used
- Gateway endpoint cannot be extended out of a VPC (VPN, DX, TGW, peering)

Question 284:

A company operates quick-service restaurants. The restaurants follow a predictable model with high sales traffic for 4 hours daily. Sales traffic is lower outside of those peak hours.

The point of sale and management platform is deployed in the AWS Cloud and has a backend that is based on Amazon DynamoDB. The database table uses provisioned throughput mode with 100,000 RCUs and 80,000 WCUs to match known peak resource consumption.

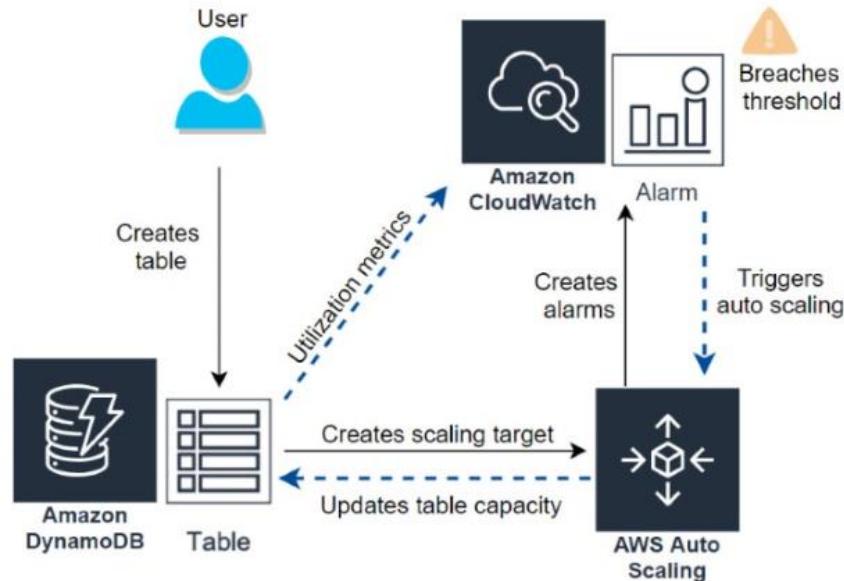
The company wants to reduce its DynamoDB cost and minimize the operational overhead for the IT staff.

Which solution meets these requirements MOST cost-effectively?

- Reduce the provisioned RCUs and WCUs.
- Change the DynamoDB table to use on-demand capacity.
- Enable Dynamo DB auto scaling for the table.

D. Purchase 1-year reserved capacity that is sufficient to cover the peak load for 4 hours each day.

C
<https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/>



Question 285:

A company hosts a blog post application on AWS using Amazon API Gateway, Amazon DynamoDB, and AWS Lambda. The application currently does not use API keys to authorize requests. The API model is as follows:

- GET /posts/{postId}: to get post details
- GET /users/{userId}: to get user details
- GET /comments/{commentId}: to get comments details

The company has noticed users are actively discussing topics in the comments section, and the company wants to increase user engagement by making the comments appear in real time.

Which design should be used to reduce comment latency and improve user experience?

- A. Use edge-optimized API with Amazon CloudFront to cache API responses.
- B. Modify the blog application code to request GET/comments/{commentId} every 10 seconds.
- C. Use AWS AppSync and leverage WebSockets to deliver comments.

D. Change the concurrency limit of the Lambda functions to lower the API response time.

C

AWS AppSync is a managed service that uses GraphQL to make it easy for applications to get exactly the data they need. With AppSync, you can build scalable applications, including those requiring real-time updates, on a range of data sources such as NoSQL data stores, relational databases, HTTP APIs, and your custom data sources with AWS Lambda.

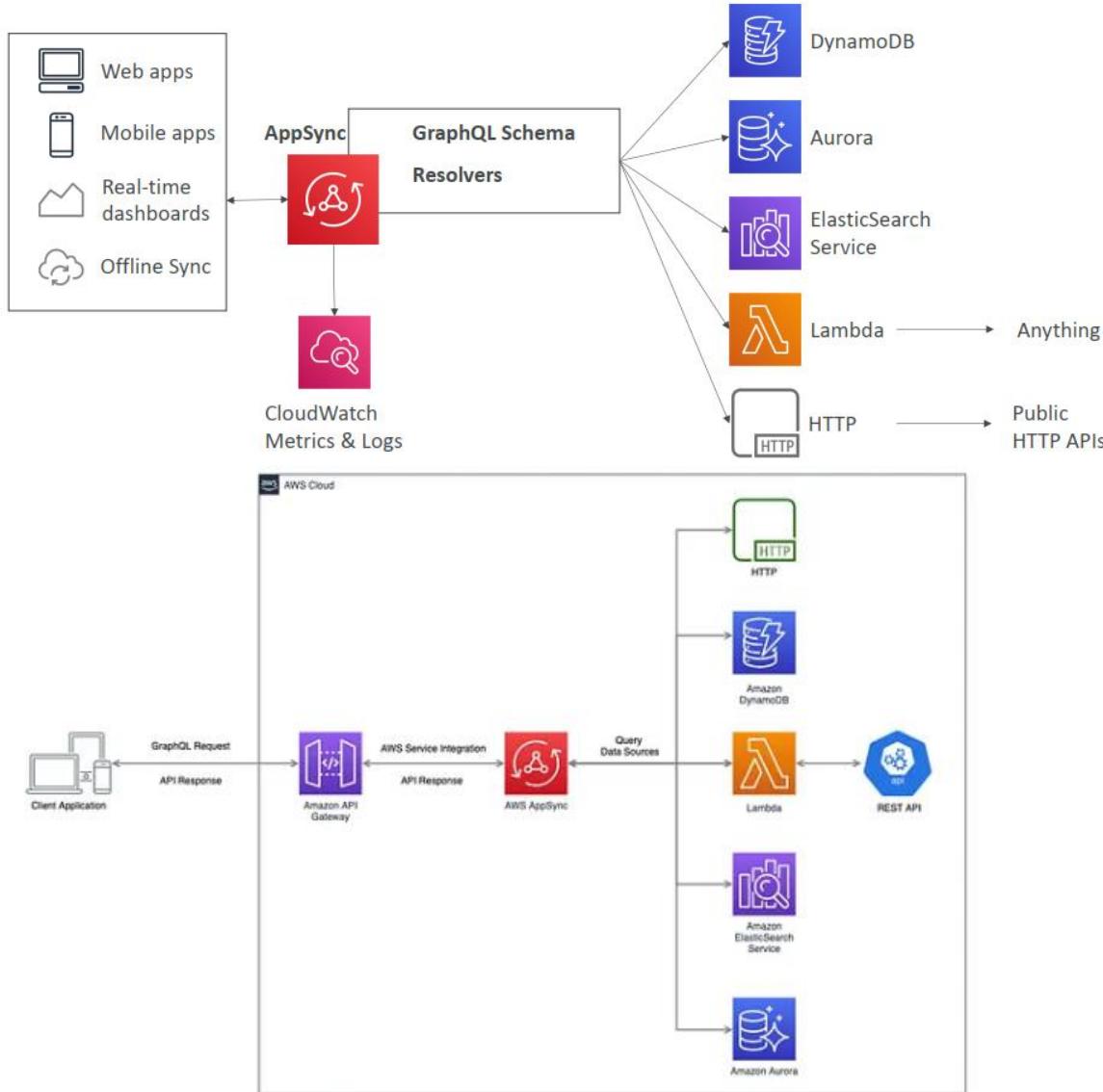
LAB: <https://aswinkumar4018.medium.com/aws-api-gateway-as-a-proxy-to-appsync-5d4dcd609a2c>

AWS AppSync - Overview



- AppSync is a managed service that uses **GraphQL**
- **GraphQL** makes it easy for applications to get exactly the data they need.
- This includes combining data from **one or more sources**
 - NoSQL data stores, Relational databases, HTTP APIs...
 - Integrates with DynamoDB, Aurora, Elasticsearch & others
 - Custom sources with AWS Lambda
- Retrieve data in real-time with WebSocket or MQTT on WebSocket
 - For mobile apps: local data access & data synchronization
 - It all starts with uploading one **GraphQL schema**

AppSync Diagram



Question 286:

A company manages hundreds of AWS accounts centrally in an organization in AWS Organizations. The company recently started to allow product teams to create and manage their own S3 access points in their accounts. The S3 access points can be accessed only within VPCs, not on the internet.

What is the MOST operationally efficient way to enforce this requirement?

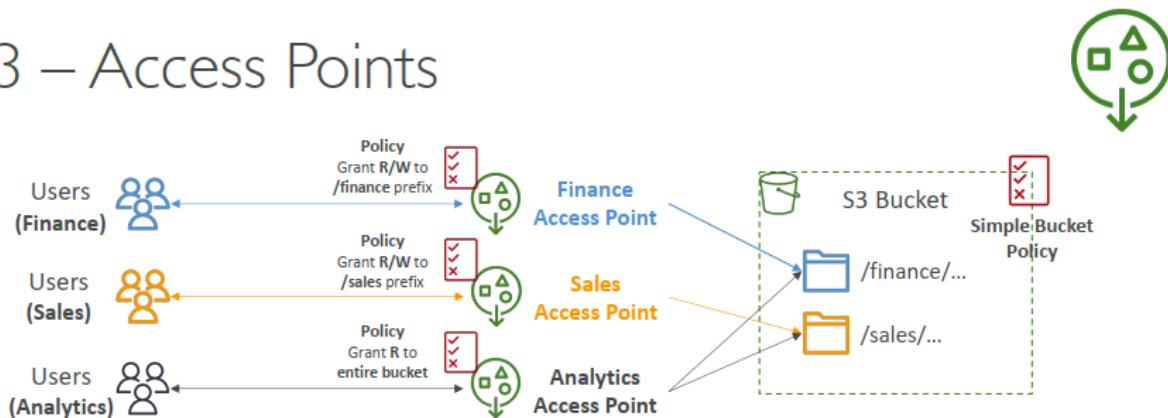
- Set the S3 access point resource policy to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- Create an SCP at the root level in the organization to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- Use AWS CloudFormation StackSets to create a new IAM policy in each AWS account that allows the s3>CreateAccessPoint action only if the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- Set the S3 bucket policy to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

B

LAB: <https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

This approach ensures centralized policy management and consistent enforcement across all AWS accounts within the organization. It avoids the need for configuring bucket policies or access point resource policies in each individual account, making it operationally efficient.

S3 – Access Points



- Access Points simplify security management for S3 Buckets
- Each Access Point has:
 - its own DNS name (Internet Origin or VPC Origin)
 - an access point policy (similar to bucket policy) – manage security at scale

Question 287:

A solutions architect must update an application environment within AWS Elastic Beanstalk using a blue/green deployment methodology. The solutions architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.

What should be done next to complete the update?

- Redirect to the new environment using Amazon Route 53.
- Select the Swap Environment URLs option.
- Replace the Auto Scaling launch configuration.
- Update the DNS records to point to the green environment.

B

The solutions architect creates an environment that is identical to the existing application environment and deploys the application to the new environment. → deploy green environment → when done need swap to URLs

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

Elastic Beanstalk Deployment Blue / Green

- Not a “direct feature” of Elastic Beanstalk
- Zero downtime and release facility
- Create a new “stage” environment and deploy v2 there
- The new environment (green) can be validated independently and roll back if issues
- Route 53 can be setup using weighted policies to redirect a little bit of traffic to the stage environment
- Using Beanstalk, “swap URLs” (DNS swap) when done with the environment test



Question 288:

A company is building an image service on the web that will allow users to upload and search random photos. At peak usage, up to 10,000 users worldwide will upload their images. The will then overlay text on the uploaded images, which will then be published on the company website.

Which design should a solutions architect implement?

- A. Store the uploaded images in Amazon Elastic File System (Amazon EFS). Send application log information about each image to Amazon CloudWatch Logs. Create a fleet of Amazon EC2 instances that use CloudWatch Logs to determine which images need to be processed. Place processed images in another directory in Amazon EFS. Enable Amazon CloudFront and configure the origin to be the one of the EC2 instances in the fleet.
- B. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to Amazon Simple Notification Service (Amazon SNS). Create a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) to pull messages from Amazon SNS to process the images and place them in Amazon Elastic File System (Amazon EFS). Use Amazon CloudWatch metrics for the SNS message volume to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the ALB in front of the EC2 instances.
- C. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to the Amazon Simple Queue Service (Amazon SQS) queue. Create a fleet of Amazon EC2 instances to pull messages from the SQS queue to process the images and place them in another S3 bucket. Use Amazon CloudWatch metrics for queue depth to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the S3 bucket that contains the processed images.
- D. Store the uploaded images on a shared Amazon Elastic Block Store (Amazon EBS) volume mounted to a fleet of Amazon EC2 Spot instances. Create an Amazon DynamoDB table that contains information about each uploaded image and whether it has been processed. Use an Amazon EventBridge rule to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to reference an Elastic Load Balancer in front of the fleet of EC2 instances.

C

up to 10,000 users worldwide will upload their images → CloudFront + S3

Option C (Store the uploaded images in an S3 bucket and use S3 event notification with SQS queue) is the most suitable design. Amazon S3 provides highly scalable and durable storage for the uploaded images. Configuring S3 event notifications to send messages to an SQS queue allows for decoupling the processing of images from the upload process. A fleet of EC2 instances can pull messages from the SQS queue to process the images and store them in another S3 bucket. Scaling out the EC2 instances based on SQS queue depth using CloudWatch metrics ensures efficient utilization of resources. Enabling Amazon CloudFront with the origin set to the S3 bucket containing the processed images improves the global availability and performance of image delivery.

Question 289:

A company has deployed its database on an Amazon RDS for MySQL DB instance in the us-east-1 Region. The company needs to make its data available to customers in Europe. The customers in Europe must have access to the same data as customers in the United States (US) and will not tolerate high application latency or stale data. The customers in Europe and the customers in the US need to write to the database. Both groups of customers need to see updates from the other group in real time.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL replica of the RDS for MySQL DB instance. Pause application writes to the RDS DB instance. Promote the Aurora Replica to a standalone DB cluster. Reconfigure the application to use the Aurora database and resume writes. Add eu-west-1 as a secondary Region to the DB cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.

B. Add a cross-Region replica in eu-west-1 for the RDS for MySQL DB instance. Configure the replica to replicate write queries back to the primary DB instance. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.

C. Copy the most recent snapshot from the RDS for MySQL DB instance to eu-west-1. Create a new RDS for MySQL DB instance in eu-west-1 from the snapshot. Configure MySQL logical replication from us-east-1 to eu-west-1. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.

D. Convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Add eu-west-1 as a secondary Region to the DB cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.

A

You cannot natively convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Instead, you can create an Amazon Aurora MySQL replica of the RDS MySQL RDS DB instance

LAB: <https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/>
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Replica.html>

You can create an Aurora read replica for an RDS for MySQL DB instance by using the console, the AWS CLI, or the RDS API.

After migration completes, you can promote the Aurora read replica to a stand-alone DB cluster using the AWS Management Console or AWS CLI.

Then you can direct your client applications to the endpoint for the Aurora read replica

Question 290:

A company is serving files to its customers through an SFTP server that is accessible over the internet. The SFTP server is running on a single Amazon EC2 instance with an Elastic IP address attached. Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses.

A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure management, and minimize the disruption to customers who access files. The solution must not change the way customers connect.

Which solution will meet these requirements?

A. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.

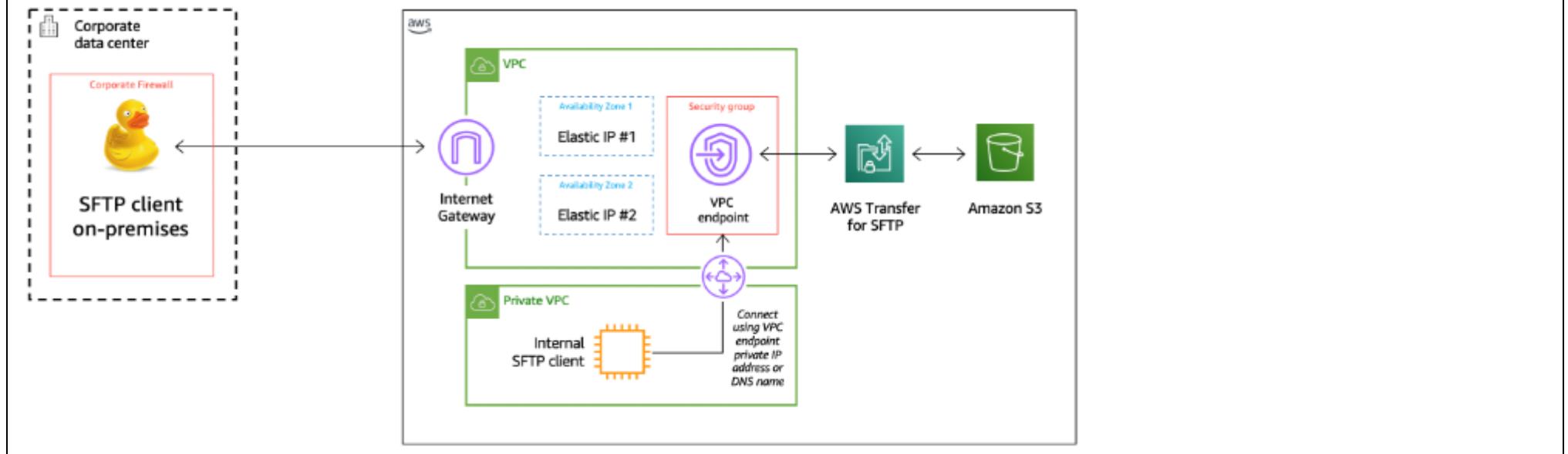
B. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC-hosted, internet-facing endpoint. Associate the SFTP Elastic IP address with the new endpoint. Attach the security group with customer IP addresses to the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.

C. Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition. Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) in front of the service. When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server. Associate the Elastic IP address with the NLB. Sync all files from the SFTP server to the S3 bucket.

D. Disassociate the Elastic IP address from the EC2 instance. Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting. Create a Network Load Balancer (NLB) with the Elastic IP address attached. Create an Auto Scaling group with EC2 instances that run an SFTP server. Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume. Configure the Auto Scaling group to automatically add instances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches. Sync all files from the SFTP server to the new multi-attach EBS volume.

B

LAB: <https://aws.amazon.com/blogs/storage/use-ip-whitelisting-to-secure-your-aws-transfer-for-sftp-servers/>



Question 291:

A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics takes 4 hours to complete. The statistical analysis is not critical to the business, and data points are processed during the next iteration if a particular run fails.

The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year reservations. These EC2 instances run full time to ingest and store the streaming data in attached Amazon Elastic Block Store (Amazon EBS) volumes. A scheduled script launches EC2 On-Demand Instances each night to perform the nightly processing. The instances access the stored data from NFS shares on the ingestion servers. The script terminates the instances when the processing is complete.

The Reserved Instance reservations are expiring. The company needs to determine whether to purchase new reservations or implement a new design.

Which solution will meet these requirements MOST cost-effectively?

- A. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use a scheduled script to launch a fleet of EC2 On-Demand Instances each night to perform the batch processing of the S3 data. Configure the script to terminate the instances when the processing is complete.
- B. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.
- C. Update the ingestion process to use a fleet of EC2 Reserved Instances with 3-year reservations behind a Network LoadBalancer. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.
- D. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon Redshift. Use Amazon EventBridge to schedule an AWS Lambda function to run nightly to query Amazon Redshift to generate the daily statistics.

B

A=> Use a scheduled script to launch a fleet of EC2 On-Demand wrong
 C=> Update the ingestion process to use a fleet of EC2 Reserved Instances wrong
 D=> lambda wrong because “takes 4 hours to complete”

<https://docs.aws.amazon.com/batch/latest/userguide/best-practices.html>

AWS Batch

- Run batch jobs as Docker images
- Two options:
 1. Run on AWS Fargate (fully serverless offering)
 2. Dynamic provisioning of the instances (EC2 & Spot Instances) – in VPC
- Optimal quantity and type based on volume and requirements
- No need to manage clusters, fully **serverless**
- You just pay for the underlying resources used
- Example: batch process of images, running thousands of concurrent jobs
- Schedule Batch Jobs using Amazon EventBridge
- Orchestrate Batch Jobs using AWS Step Functions



AWS Batch – Compute Environments

- Managed Compute Environment:
 - AWS Batch managed the capacity and instance types within the environment
 - You can choose EC2 On-Demand or Spot Instances
 - You can choose Fargate On-Demand or Fargate Spot Instances
 - You can set a maximum price for Spot Instances
 - Launched within your own VPC
 - If you launch within your own private subnet, make sure it has access to the ECS service
 - Either using a NAT gateway / instance or using VPC Endpoints for ECS
- Unmanaged Compute Environment
 - You control and manage EC2 instance configuration, provisioning and scaling

Question 292:

A company needs to migrate an on-premises SFTP site to AWS. The SFTP site currently runs on a Linux VM. Uploaded files are made available to downstream applications through an NFS share.

As part of the migration to AWS, a solutions architect must implement high availability. The solution must provide external vendors with a set of static public IP addresses that the vendors can allow. The company has set up an AWS Direct Connect connection between its on-premises data center and its VPC.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS Transfer Family server. Configure an internet-facing VPC endpoint for the Transfer Family server. Specify an Elastic IP address for each subnet. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.

B. Create an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.

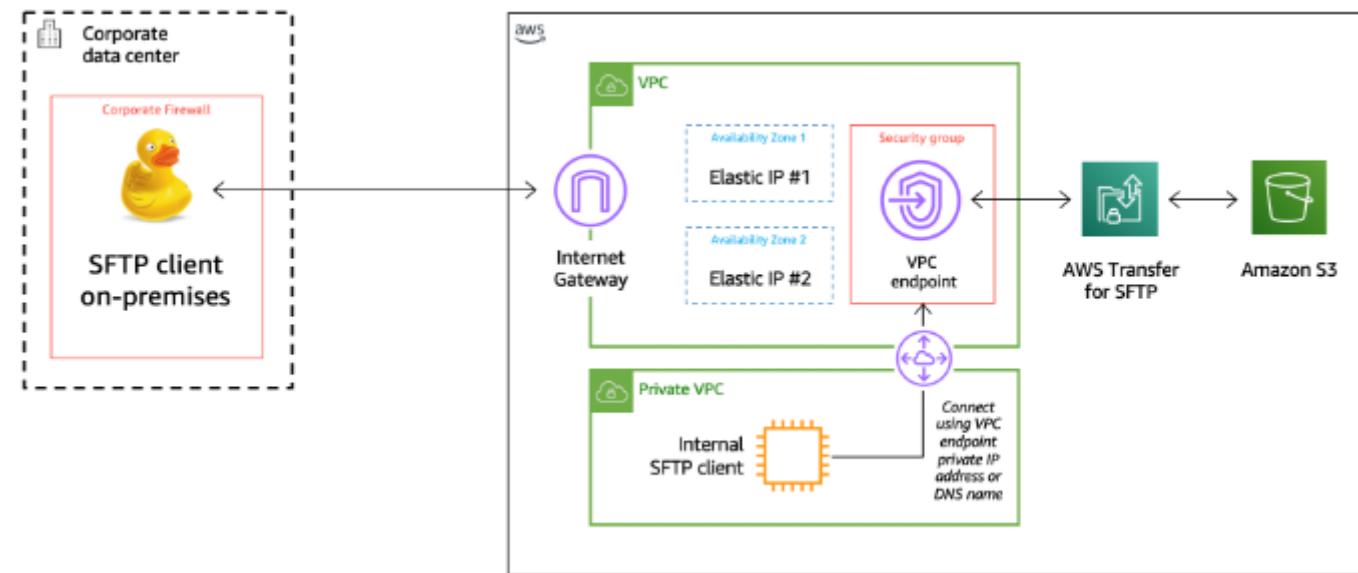
C. Use AWS Application Migration Service to migrate the existing Linux VM to an Amazon EC2 instance. Assign an Elastic IP address to the EC2 instance. Mount an Amazon Elastic File System (Amazon EFS) file system to the EC2 instance. Configure the SFTP server to place files in the EFS file system. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.

D. Use AWS Application Migration Service to migrate the existing Linux VM to an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon FSx for Lustre file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the FSx for Lustre endpoint instead.

A

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-sftp-server-to-aws-using-aws-transfer-for-sftp.html>

Option A suggests creating an AWS Transfer Family server and configuring an internet-facing VPC endpoint for it. By specifying an Elastic IP address for each subnet, the company can provide a set of static public IP addresses to external vendors. The Transfer Family server can be configured to place files into an Amazon Elastic File System (Amazon EFS) file system, which provides a scalable and highly available storage solution across multiple Availability Zones. This allows the company to maintain high availability for the SFTP site and its downstream applications without the need for manual intervention or additional operational overhead.



EFS – Elastic File System

- Use cases: content management, web serving, data sharing, WordPress
- Compatible with Linux based AMI (not Windows), POSIX-compliant
- Uses NFSv4.1 protocol
- Uses security group to control access to EFS
Mã hóa ở phần còn lại
- Encryption at rest using KMS
- Can only attach to one VPC, create one ENI (mount target) per AZ
- POSIX file system (~Linux) that has a standard file API
- File system scales automatically, pay-per-use, no capacity planning!

Question 293:

A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size of the Auto Scaling group is 20 instances in service. The VPC IPv4 addressing is as follows:

- VPC CIDR: 10.0.0.0/23 -
- AZ1 subnet CIDR: 10.0.0.0/24 -
- AZ2 subnet CIDR: 10.0.1.0/24 -

Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime. Which solution will meet these requirements?

A. Update the Auto Scaling group to use the AZ2 subnet only. Delete and re-create the AZ1 subnet using half the previous address space. Adjust the Auto Scaling group to also use the new AZ1 subnet. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Remove the current AZ2 subnet. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.

B. Terminate the EC2 instances in the AZ1 subnet. Delete and re-create the AZ1 subnet using half the address space. Update the Auto Scaling group to use this new subnet. Repeat this for the second AZ. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.

C. Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ. Update the existing Auto Scaling group to target the new subnets in the new VPC.

D. Update the Auto Scaling group to use the AZ2 subnet only. Update the AZ1 subnet to have half the previous address space. Adjust the Auto Scaling group to also use the AZ1 subnet again. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Update the current AZ2 subnet and assign the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.

<https://www.examtopics.com/discussions/amazon/view/112791-exam-aws-certified-solutions-architect-professional-sap-c02/>

A

D is closest, but wrong as you subnets cannot be modified. They have to be deleted and re-created.

without service downtime → B is incorrect because need terminate EC2

without adding additional IPv4 address space → C is incorrect

<https://repost.aws/knowledge-center/vpc-ip-address-range>

Question 294:

A company uses an organization in AWS Organizations to manage the company's AWS accounts. The company uses AWS CloudFormation to deploy all infrastructure. A finance team wants to build a chargeback model. The finance team asked each business unit to tag resources by using a predefined list of project values.

When the finance team used the AWS Cost and Usage Report in AWS Cost Explorer and filtered based on project, the team noticed noncompliant project values. The company wants to enforce the use of project tags for new resources.

Which solution will meet these requirements with the LEAST effort?

A. Create a tag policy that contains the allowed project tag values in the organization's management account. Create an SCP that denies the cloudformation>CreateStack API operation unless a project tag is added. Attach the SCP to each OU.

B. Create a tag policy that contains the allowed project tag values in each OU. Create an SCP that denies the cloudformation>CreateStack API operation unless a project tag is added. Attach the SCP to each OU.

C. Create a tag policy that contains the allowed project tag values in the AWS management account. Create an IAM policy that denies the cloudformation>CreateStack API operation unless a project tag is added. Assign the policy to each user.

D. Use AWS Service Catalog to manage the CloudFormation stacks as products. Use a TagOptions library to control project tag values. Share the portfolio with all OUs that are in the organization.

A

LEAST effort → A because you just only execute in the one account.

Question 295:

An application is deployed on Amazon EC2 instances that run in an Auto Scaling group. The Auto Scaling group configuration uses only one type of instance.

CPU and memory utilization metrics show that the instances are underutilized. A solutions architect needs to implement a solution to permanently reduce the EC2 cost and increase the utilization.

Which solution will meet these requirements with the LEAST number of configuration changes in the future?

- A. List instance types that have properties that are similar to the properties that the current instances have. Modify the Auto Scaling group's launch template configuration to use multiple instance types from the list.
- B. Use the information about the application's CPU and memory utilization to select an instance type that matches the requirements. Modify the Auto Scaling group's configuration by adding the new instance type. Remove the current instance type from the configuration.
- C. Use the information about the application's CPU and memory utilization to specify CPU and memory requirements in a new revision of the Auto Scaling group's launch template. Remove the current instance type from the configuration.
- D. Create a script that selects the appropriate instance types from the AWS Price List Bulk API. Use the selected instance types to create a new revision of the Auto Scaling group's launch template.

C

By using the information about the application's CPU and memory utilization, you can determine the CPU and memory requirements of the application.

In this solution, you create a new revision of the Auto Scaling group's launch template and specify the CPU and memory requirements in the template. This ensures that the new instances launched by the Auto Scaling group meet the application's requirements.

By removing the current instance type from the configuration, you ensure that only instances with the specified CPU and memory requirements are launched, effectively increasing utilization and optimizing costs.

This solution requires minimal configuration changes as you are primarily modifying the launch template with the updated CPU and memory requirements.

B is incorrect → Launch templates are immutable; after you create a launch template, you can't modify it. Instead, you can create a new version of the launch template that includes any changes you require.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/manage-launch-template-versions.html>

Question 296:

A company implements a containerized application by using Amazon Elastic Container Service (Amazon ECS) and Amazon API Gateway. The application data is stored in Amazon Aurora databases and Amazon DynamoDB databases. The company automates infrastructure provisioning by using AWS CloudFormation. The company automates application deployment by using AWS CodePipeline.

A solutions architect needs to implement a disaster recovery (DR) strategy that meets an RPO of 2 hours and an RTO of 4 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon CloudFront with origin failover to route traffic to the secondary Region during a DR scenario.
- B. Use AWS Database Migration Service (AWS DMS), Amazon EventBridge, and AWS Lambda to replicate the Aurora databases to a secondary AWS Region. Use DynamoDB Streams, EventBridge, and Lambda to replicate the DynamoDB databases to the secondary Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.
- C. Use AWS Backup to create backups of the Aurora databases and the DynamoDB databases in a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.
- D. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.

C

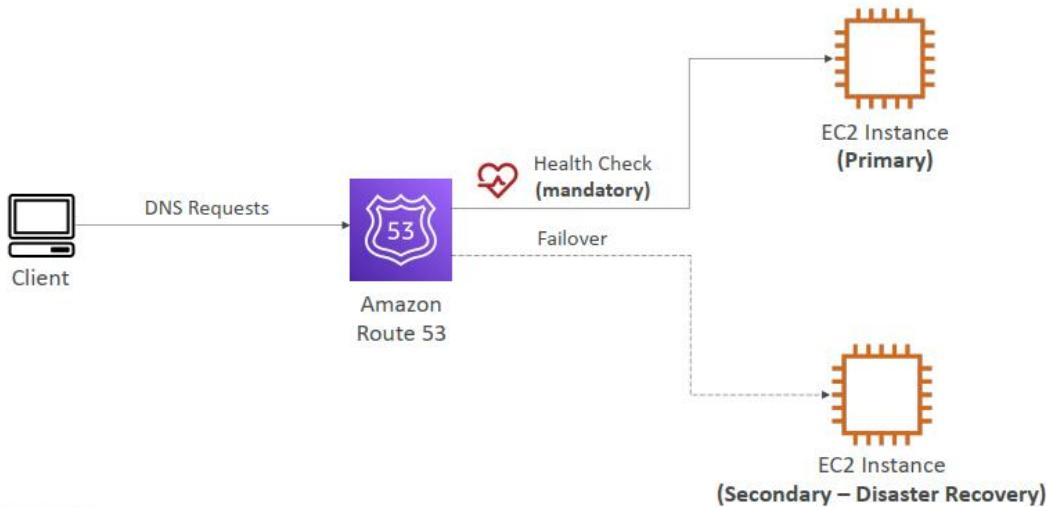
<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

meets an RPO of 2 hours and an RTO of 4 hours → Backup solution or Pilot light or warm standby

MOST cost-effectively → Backup solution



Routing Policies – Failover (Active-Passive)



Question 297:

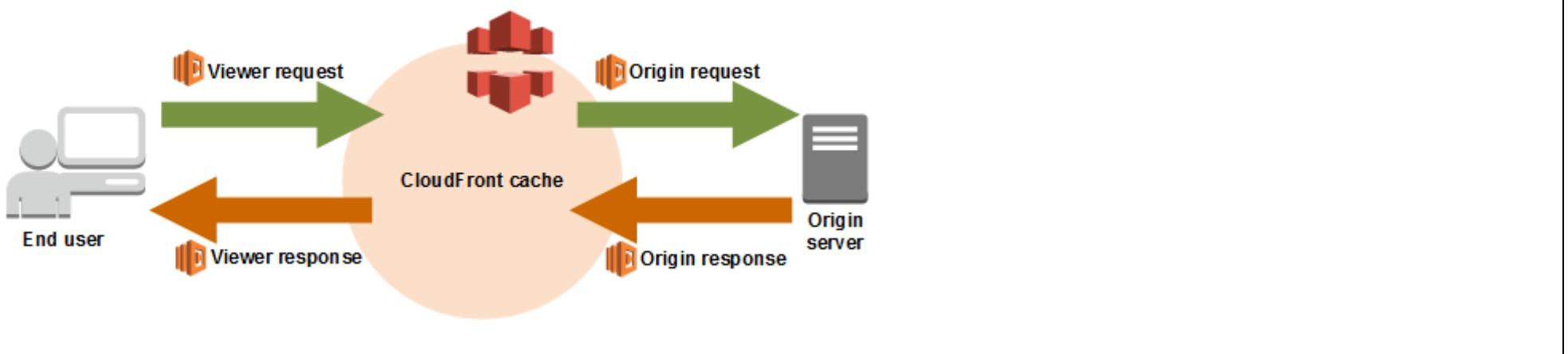
A company has a complex web application that leverages Amazon CloudFront for global scalability and performance. Over time, users report that the web application is slowing down.

The company's operations team reports that the CloudFront cache hit ratio has been dropping steadily. The cache metrics report indicates that query strings on some URLs are inconsistently ordered and are specified sometimes in mixed-case letters and sometimes in lowercase letters.

Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible?

- A. Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase. Select the CloudFront viewer request trigger to invoke the function.
- B. Update the CloudFront distribution to disable caching based on query string parameters.
- C. Deploy a reverse proxy after the load balancer to post-process the emitted URLs in the application to force the URL strings to be lowercase.
- D. Update the CloudFront distribution to specify casing-insensitive query string processing.

A
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-cloudfront-trigger-events.html>
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html>



Question 298:

A company runs an ecommerce application in a single AWS Region. The application uses a five-node Amazon Aurora MySQL DB cluster to store information about customers and their recent orders. The DB cluster experiences a large number of write transactions throughout the day.

The company needs to replicate the data in the Aurora database to another Region to meet disaster recovery requirements. The company has an RPO of 1 hour.

Which solution will meet these requirements with the **LOWEST cost**?

- A. Modify the Aurora database to be an Aurora global database. Create a second Aurora database in another Region.
- B. Enable the Backtrack feature for the Aurora database. Create an AWS Lambda function that runs daily to copy the snapshots of the database to a backup Region.
- C. Use AWS Database Migration Service (AWS DMS). Create a DMS change data capture (CDC) task that replicates the ongoing changes from the Aurora database to an Amazon S3 bucket in another Region.
- D. Turn off automated Aurora backups. Configure Aurora backups with a backup frequency of 1 hour. Specify another Region as the destination Region. Select the Aurora database as the resource assignment.

A

C is incorrect → using S3 as a target is in the same region. Additional, you need create an EC2 instance to perform replication tasks

DMS Sources and Targets

SOURCES:

- On-premises and EC2 instances databases: Oracle, MS SQL Server, MySQL, MariaDB, PostgreSQL, MongoDB, SAP, DB2
- Azure: Azure SQL Database
- Amazon RDS: all including Aurora
- Amazon S3
- DocumentDB

TARGETS:

- On-premises and EC2 instances databases: Oracle, MS SQL Server, MySQL, MariaDB, PostgreSQL, SAP
- Amazon RDS including Aurora
- Amazon Redshift
- Amazon DynamoDB
- Amazon S3
- OpenSearch Service
- Kinesis Data Streams
- DocumentDB

We have an RPO of 1 hour, which means you can tolerate losing up to 1 hour of data in case of a disaster. However, you also need to consider the cost and the recovery time objectives (RTO) of your solution. Using AWS DMS will cost more than using Aurora global database, and it will take longer to recover your data from S3 to a new database. Aurora global database will replicate your data to another Region with low latency, and it will allow you to fail over to the secondary DB cluster in minutes if the primary Region is unavailable. Therefore, Aurora global database is a better solution for your requirements.

Question 299:

A company's solutions architect is evaluating an AWS workload that was deployed several years ago. The application tier is stateless and runs on a single large Amazon EC2 instance that was launched from an AMI. The application stores data in a MySQL database that runs on a single EC2 instance.

The CPU utilization on the application server EC2 instance often reaches 100% and causes the application to stop responding. The company manually installs patches on the instances. Patching has caused downtime in the past. The company needs to make the application highly available.

Which solution will meet these requirements with the LEAST development me?

- A. Move the application tier to AWS Lambda functions in the existing VPC. Create an Application Load Balancer to distribute traffic across the Lambda functions. Use Amazon GuardDuty to scan the Lambda functions. Migrate the database to Amazon DocumentDB (with MongoDB compatibility).
- B. Change the EC2 instance type to a smaller Graviton powered instance type. Use the existing AMI to create a launch template for an Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon DynamoDB.
- C. Move the application tier to containers by using Docker. Run the containers on Amazon Elastic Container Service (Amazon ECS) with EC2 instances. Create an Application Load Balancer to distribute traffic across the ECS cluster. Configure the ECS cluster to scale based on CPU utilization. Migrate the database to Amazon Neptune.
- D. Create a new AMI that is configured with AWS Systems Manager Agent (SSM Agent). Use the new AMI to create a launch template for an Auto Scaling group. Use smaller instances in the Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon Aurora MySQL.

D

D: Classic architecture: ALB + ASG + EC2, scale based on CPU Utilization for cost optimization. The use of SSM to create AMI for launch template of ASG is correct. Aurora MySQL is compatible with current MySQL database.
With least development time, from MySQL to Amazon Aurora MySQL.

Question 300:

A company is planning to migrate several applications to AWS. The company does not have a good understanding of its entire application estate. The estate consists of a mixture of physical machines and VMs.

One application that the company will migrate has many dependencies that are sensitive to latency. The company is unsure what all the dependencies are. However the company knows that the low-latency communications use a custom IP-based protocol that runs on port 1000. The company wants to migrate the application and these dependencies together to move all the low-latency interfaces to AWS at the same time.

The company has installed the AWS Application Discovery Agent and has been collecting data for several months.

What should the company do to identify the dependencies that need to be migrated in the same phase as the application?

- A. Use AWS Migration Hub and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Turn on data exploration in Amazon Athena. Query the data that is transferred between the servers to identify the servers that communicate on port 1000. Return to Migration Hub. Create a move group that is based on the findings from the Athena queries.
- B. Use AWS Application Migration Service and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Configure Application Migration Service to launch test instances for all the servers that interact with the application. Perform acceptance tests on the test instances. If no issues are identified, create a move group that is based on the tested servers.
- C. Use AWS Migration Hub and select the servers that host the application. Turn on data exploration in Network Access Analyzer. Use the Network Access Analyzer console to select the servers that host the application. Select a Network Access Scope of port 1000 and note the matching servers. Return to Migration Hub. Create a move group that is based on the findings from Network Access Analyzer.

D. Use AWS Migration Hub and select the servers that host the application. Push the Amazon CloudWatch agent to the identified servers by using the AWS Application Discovery Agent. Export the CloudWatch logs that the agents collect to Amazon S3. Use Amazon Athena to query the logs to find servers that communicate on port 1000. Return to Migration Hub Create a move group that is based on the findings from the Athena queries.

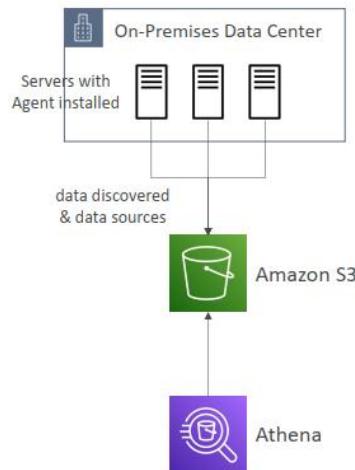
A

<https://aws.amazon.com/blogs/mt/using-aws-migration-hub-network-visualization-to-overcome-application-and-server-dependency-challenges/>

AWS Application Discovery Service – Migration Hub Data Exploration



- Allows you to use Amazon Athena to analyze data collected from on-premises servers during discovery
- Data is automatically stored in S3 bucket at regular intervals
- Use Pre-defined or custom queries in Amazon Athena to analyze data
- Example: type of processes running on each server
- Ability to upload additional data sources such as Configuration Management Database (CMDB) exports
- Integrate Athena with QuickSight to visualize data



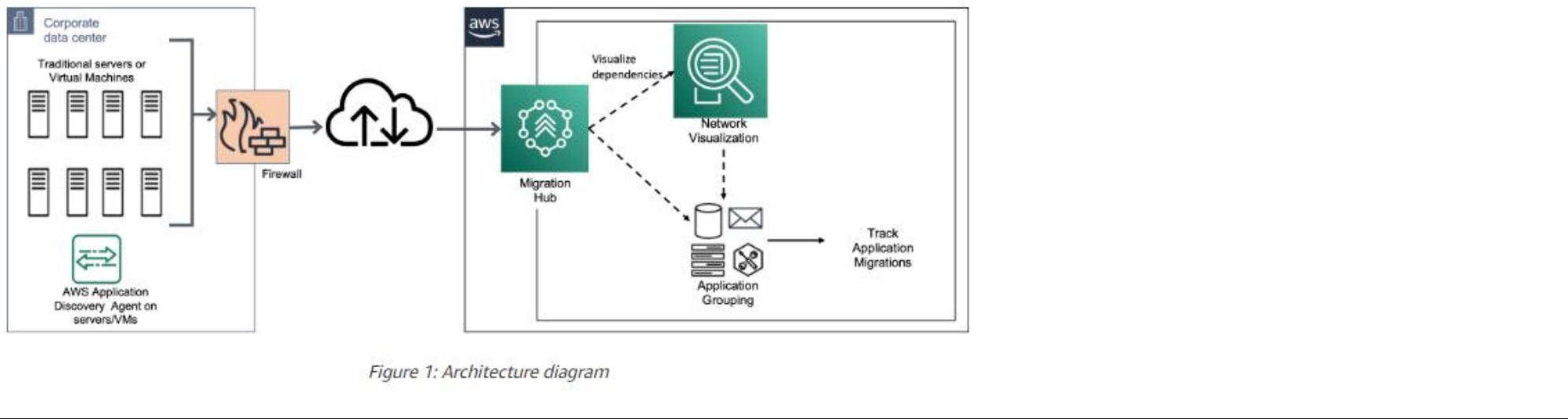


Figure 1: Architecture diagram

Question 301:

A company is building an application that will run on an AWS Lambda function. Hundreds of customers will use the application. The company wants to give each customer a quota of requests for a specific time period. The quotas must match customer usage patterns. Some customers must receive a higher quota for a shorter time period.

Which solution will meet these requirements?

- A. Create an Amazon API Gateway REST API with a proxy integration to invoke the Lambda function. For each customer, configure an API Gateway usage plan that includes an appropriate request quota. Create an API key from the usage plan for each user that the customer needs.
- B. Create an Amazon API Gateway HTTP API with a proxy integration to invoke the Lambda function. For each customer configure an API Gateway usage plan that includes an appropriate request quota Configure route-level throttling for each usage plan. Create an API Key from the usage plan for each user that the customer needs.
- C. Create a Lambda function alias for each customer. Include a concurrency limit with an appropriate request quota. Create a Lambda function URL for each function alias. Share the Lambda function URL for each alias with the relevant customer.
- D. Create an Application Load Balancer (ALB) in a VPC. Configure the Lambda function as a target for the ALB. Configure an AWS WAF web ACL for the ALB. For each customer configure a rate-based rule that includes an appropriate request quota.

A

<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>

LAB: <https://medium.com/geekculture/api-key-and-usage-plan-integration-with-aws-api-gateway-2d07bbb9a2a4>

API Gateway – Usage Plans & API Keys

- If you want to make an API available as an offering (\$) to your customers
- **Usage Plan:**
 - who can access one or more deployed API stages and methods
 - how much and how fast they can access them
 - uses API keys to identify API clients and meter access
 - configure throttling limits and quota limits that are enforced on individual client
- **API Keys:**
 - alphanumeric string values to distribute to your customers
 - Ex: WBjHxNtoAb4WPKBC7cGm64CBibl24b4jt8jjHo9
 - Can use with usage plans to control access
 - Throttling limits are applied to the API keys giới hạn điều chỉnh được áp dụng cho API keys
 - Quotas limits is the overall number of maximum requests
- **429 Too Many Requests:**
 - Account level throttling across all APIs in a region
 - Clients must implement retry mechanisms

Question 302:

A company is planning to migrate its on-premises VMware cluster of 120 VMs to AWS. The VMs have many different operating systems and many custom software packages installed. The company also has an on-premises NFS server that is 10 TB in size. The company has set up a 10 Gbps AWS Direct Connect connection to AWS for the migration.

Which solution will complete the migration to AWS in the LEAST amount of time?

- A. Export the on-premises VMs and copy them to an Amazon S3 bucket. Use VM Import/Export to create AMIs from the VM images that are stored in Amazon S3. Order an AWS Snowball Edge device. Copy the NFS server data to the device. Restore the NFS server data to an Amazon EC2 instance that has NFS configured.
- B. Configure AWS Application Migration Service with a connection to the VMware cluster. Create a replication job for the VMS. Create an Amazon Elastic File System (Amazon EFS) file system. Configure AWS DataSync to copy the NFS server data to the EFS file system over the Direct Connect connection.
- C. Recreate the VMs on AWS as Amazon EC2 instances. Install all the required software packages. Create an Amazon FSx for Lustre file system. Configure AWS DataSync to copy the NFS server data to the FSx for Lustre file system over the Direct Connect connection.
- D. Order two AWS Snowball Edge devices. Copy the VMs and the NFS server data to the devices. Run VM Import/Export after the data from the devices is loaded to an Amazon S3 bucket. Create an Amazon Elastic File System (Amazon EFS) file system. Copy the NFS server data from Amazon S3 to the EFS file system.

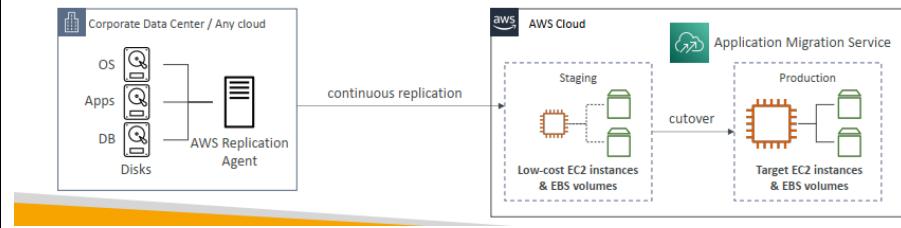
B

LEAST amount of time and 10 Gbps AWS Direct Connect connection → Data Sync

AWS Application Migration Service (MGN)



- The “AWS evolution” of CloudEndure Migration, replacing AWS Server Migration Service (SMS)
- Lift-and-shift (rehost) solution which simplify **migrating** applications to AWS
- Converts your physical, virtual, and cloud-based servers to run natively on AWS
- Supports wide range of platforms, Operating Systems, and databases
- Minimal downtime, reduced costs



• AWS Direct Connect:

- Move GB/s of data to the cloud, over a private secure network

• Snowball & Snowmobile

- Move PB of data to the cloud

• AWS DataSync

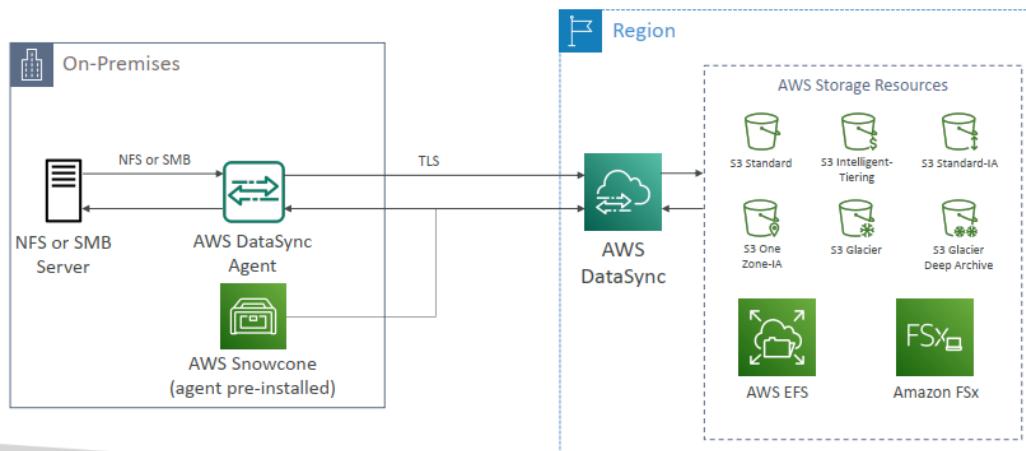
- Move large amount of data between on-premise and S3, EFS, FSx for Windows

AWS DataSync



- Move large amount of data to and from
 - On-premises / other cloud to AWS (NFS, SMB, HDFS, S3 API...) – needs agent
 - AWS to AWS (different storage services) – no agent needed
- Can synchronize to:
 - Amazon S3 (any storage classes – including Glacier)
 - Amazon EFS
 - Amazon FSx (Windows, Lustre, NetApp, OpenZFS...)
- Replication tasks can be scheduled hourly, daily, weekly
- File permissions and metadata are bảo quản (NFS POSIX, SMB...)
- One agent task can use 10 Gbps, can setup a bandwidth limit

AWS DataSync NFS / SMB to AWS (S3, EFS, FSx...)



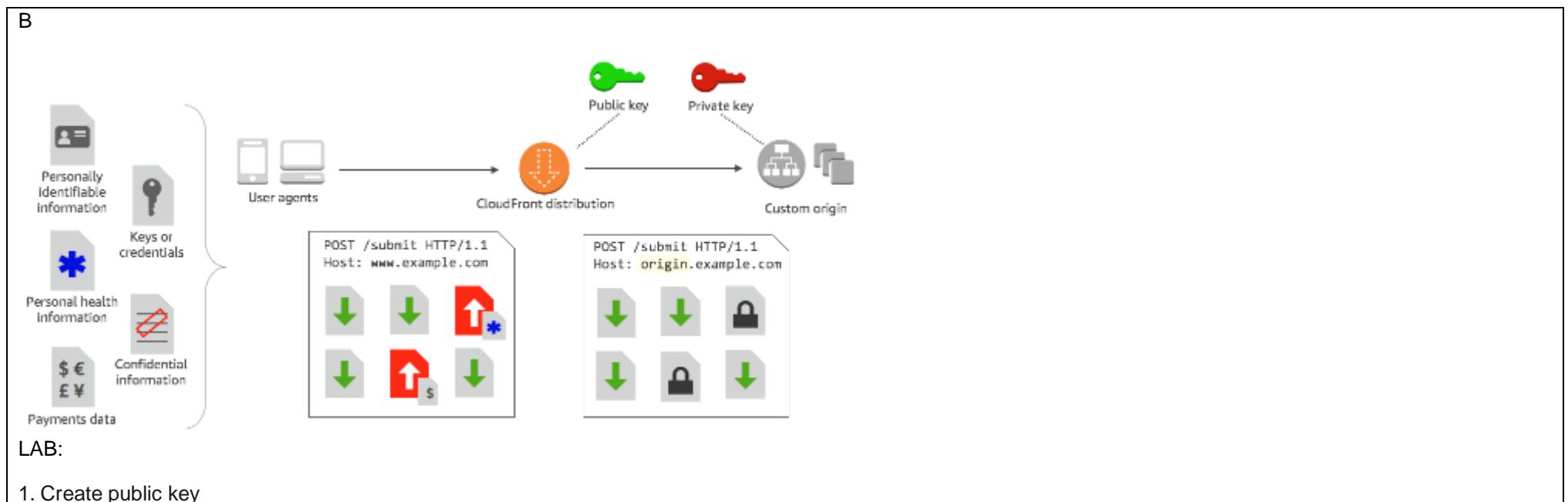
Question 303:

An online survey company runs its application in the AWS Cloud. The application is distributed and consists of microservices that run in an automatically scaled Amazon Elastic Container Service (Amazon ECS) cluster. The ECS cluster is a target for an Application Load Balancer (ALB). The ALB is a custom origin for an Amazon CloudFront distribution.

The company has a survey that contains sensitive data. The sensitive data must be encrypted when it moves through the application. The application's data-handling microservice is the only microservice that should be able to decrypt the data.

Which solution will meet these requirements?

- A. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a field-level encryption profile and a configuration. Associate the KMS key and the configuration with the CloudFront cache behavior.
- B. Create an RSA key pair that is dedicated to the data-handling microservice. Upload the public key to the CloudFront distribution. Create a field-level encryption profile and a configuration. Add the configuration to the CloudFront cache behavior.
- C. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the KMS key to encrypt the sensitive data.
- D. Create an RSA key pair that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the private key of the RSA key pair to encrypt the sensitive data.



Public keys

[Edit](#)[Delete](#)[Create public key](#) Search public keys

ID	Name	Description
No public keys You don't have any public keys.		

[Create public key](#)

2. Create field level encryption

Field-level encryption

[Profiles](#)[Configurations](#)

Profiles

[Edit](#)[Delete](#)[Create encryption profile](#)

Profile ID	Name	Description	Last modified
No profiles You don't have any Profiles.			

[Create encryption profile](#)

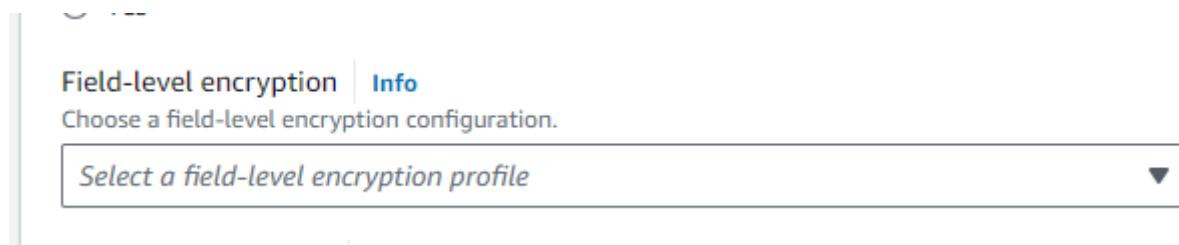
3. Add field-level encryption to CloudFront's cache behavior

To link a field-level encryption configuration to a cache behavior, the distribution must be configured to always use HTTPS, and to accept HTTP POST and PUT requests from viewers. That is, the following must be true:

The cache behavior's **Viewer Protocol Policy** must be set to **Redirect HTTP to HTTPS** or **HTTPS Only**. (In AWS CloudFormation or the CloudFront API, `ViewerProtocolPolicy` must be set to `redirect-to-https` or `https-only`.)

The cache behavior's **Allowed HTTP Methods** must be set to **GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE**. (In AWS CloudFormation or the CloudFront API, `AllowedMethods` must be set to `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`. These can be specified in any order.)

The origin setting's **Origin Protocol Policy** must be set to **Match Viewer** or **HTTPS Only**. (In AWS CloudFormation or the CloudFront API, `OriginProtocolPolicy` must be set to `match-viewer` or `https-only`.)



Question 304:

A solutions architect is determining the DNS strategy for an existing VPC. The VPC is provisioned to use the 10.24.34.0/24 CIDR block. The VPC also uses Amazon Route 53 Resolver for DNS. New requirements mandate that DNS queries must use private hosted zones. Additionally instances that have public IP addresses must receive corresponding public hostnames

Which solution will meet these requirements to ensure that the domain names are correctly resolved within the VPC?

- Create a private hosted zone. Activate the `enableDnsSupport` attribute and the `enableDnsHostnames` attribute for the VPC. Update the VPC DHCP options set to include `domain-name-servers=10.24.34.2`.
- Create a private hosted zone. Associate the private hosted zone with the VPC. Activate the `enableDnsSupport` attribute and the `enableDnsHostnames` attribute for the VPC. Create a new VPC DHCP options set, and configure `domain-name-servers=AmazonProvidedDNS`. Associate the new DHCP options set with the VPC.
- Deactivate the `enableDnsSupport` attribute for the VPC. Activate the `enableDnsHostnames` attribute for the VPC. Create a new VPC DHCP options set, and configure `domain-name-servers=10.24.34.2`. Associate the new DHCP options set with the VPC.
- Create a private hosted zone. Associate the private hosted zone with the VPC. Activate the `enableDnsSupport` attribute for the VPC. Deactivate the `enableDnsHostnames` attribute for the VPC. Update the VPC DHCP options set to include `domain-name-servers=AmazonProvidedDNS`.

B

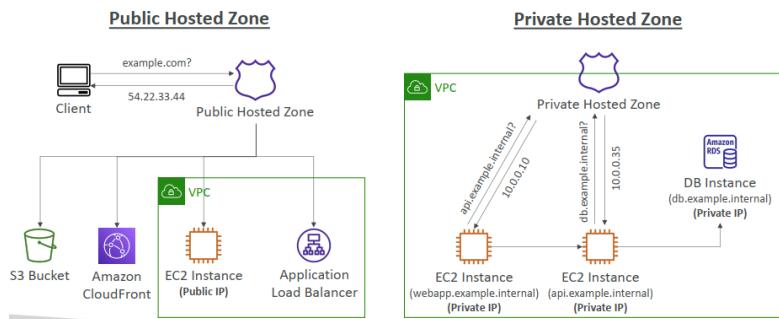
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#AmazonDNS>

Route 53 – Hosted Zones



- A container for records that define how to route traffic to a domain and its subdomains
- **Public Hosted Zones** – contains records that specify how to route traffic on the Internet (public domain names)
`application1.mypublicdomain.com`
- **Private Hosted Zones** – contain records that specify how you route traffic within one or more VPCs (private domain names)
`application1.companyinternal`

Route 53 – Public vs. Private Hosted Zones



Route 53 – Good to Know

- For internal private DNS (Private Hosted Zone), you must enable the VPC settings `enableDnsHostnames` and `enableDnsSupport`
- **DNS Security Extensions (DNSSEC)** xác minh tính toàn vẹn và nguồn gốc dữ liệu DNS
 - A protocol for securing DNS traffic, verifies DNS data integrity and origin
 - Protects against Man in the Middle (MITM) attacks
 - Route 53 supports both DNSSEC for Domain Registration and DNSSEC Signing
 - Works only with Public Hosted Zones
- **Route 53 with 3rd Registrar**
 - You can buy the domain out of AWS and use Route 53 as the DNS provider
 - Update the NS records on the 3rd party Registrar

Question 305:

A data analytics company has an Amazon Redshift cluster that consists of several reserved nodes. The cluster is experiencing unexpected bursts of usage because a team of employees is compiling a deep audit analysis report. The queries to generate the report are complex read queries and are CPU intensive.

Business requirements dictate that the cluster must be able to service read and write queries at all times. A solutions architect must devise a solution that accommodates the bursts of usage.

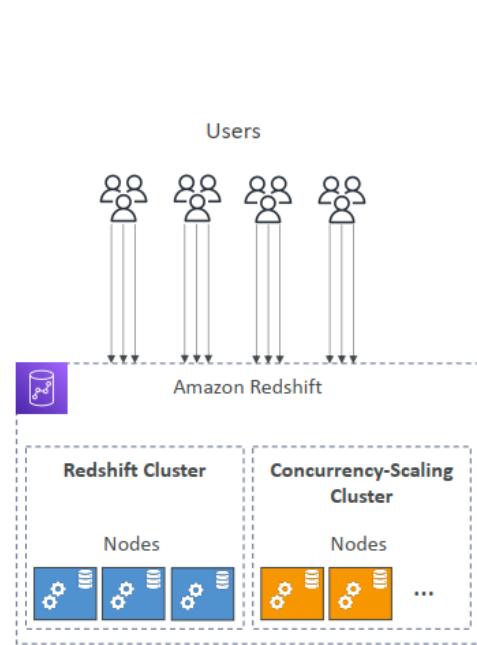
Which solution meets these requirements MOST cost-effectively?

- A. Provision an Amazon EMR cluster Offload the complex data processing tasks.
- B. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using a classic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.
- C. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using an elastic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.
- D. Turn on the Concurrency Scaling feature for the Amazon Redshift cluster.

D

Redshift Concurrency Scaling

- Enables you to provide consistently fast performance with virtually unlimited concurrent users and queries
- Redshift automatically adds additional cluster capacity (**Concurrency-Scaling Cluster**) to process an increase in requests
- Ability to decide which queries sent to the concurrency-Scaling Cluster using WLM
- Charged per second



Question 306:

A research center is migrating to the AWS Cloud and has moved its on-premises 1 PB object storage to an Amazon S3 bucket. One hundred scientists are using this object storage to store their work-related documents. Each scientist has a personal folder on the object store. All the scientists are members of a single IAM user group.

The research center's compliance officer is worried that scientists will be able to access each other's work. The research center has a strict obligation to report on which scientist accesses which documents. The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead.

Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

- A. Create an identity policy that grants the user read and write access. Add a condition that specifies that the S3 paths must be prefixed with `$(aws:username)`. Apply the policy on the scientists' IAM user group.
- B. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket. Store the trail output in another S3 bucket. Use Amazon Athena to query the logs and generate reports.
- C. Enable S3 server access logging. Configure another S3 bucket as the target for log delivery. Use Amazon Athena to query the logs and generate reports.
- D. Create an S3 bucket policy that grants read and write access to users in the scientists' IAM user group.
- E. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket and write the events to Amazon CloudWatch. Use the Amazon Athena CloudWatch connector to query the logs and generate reports.

A,B

LAB: <https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/>

The research center has a strict obligation to report on which scientist accesses which documents → Cloud Trail

Cloud Trail vs S3 access logs: <https://trello.com/c/AZI6xVqo/401-cloud-trail-vs-s3-access-logs>

AWS CloudTrail



- Provides governance, compliance and audit for your AWS Account
- CloudTrail is enabled by default!
- Get an history of events / API calls made within your AWS Account by:
 - Console
 - SDK
 - CLI
 - AWS Services
- Can put logs from CloudTrail into CloudWatch Logs or S3
- A trail can be applied to All Regions (default) or a single Region.
- If a resource is deleted in AWS, investigate CloudTrail first!

AWS Managed Logs

- Load Balancer Access Logs (ALB, NLB, CLB) => to S3
 - Access logs for your Load Balancers
- CloudTrail Logs => to S3 and CloudWatch Logs
 - Logs for API calls made within your account
- VPC Flow Logs => to S3, CloudWatch Logs, Kinesis Data Firehose
 - Information about IP traffic going to and from network interfaces in your VPC
- Route 53 Access Logs => to CloudWatch Logs
 - Log information about the queries that Route 53 receives
- S3 Access Logs => to S3
 - Server access logging provides detailed records for the requests that are made to a bucket
- CloudFront Access Logs => to S3
 - Detailed information about every user request that CloudFront receives
- AWS Config => to S3

Question 307:

A company uses AWS Organizations to manage a multi-account structure. The company has hundreds of AWS accounts and expects the number of accounts to increase. The company is building a new application that uses Docker images. The company will push the Docker images to Amazon Elastic Container Registry (Amazon ECR). Only accounts that are within the company's organization should have access to the images.

The company has a CI/CD process that runs frequently. The company wants to retain all the tagged images. However, the company wants to retain only the five most recent untagged images.

Which solution will meet these requirements with the LEAST operational overhead?

- Create a private repository in Amazon ECR. Create a permissions policy for the repository that allows only required ECR operations. Include a condition to allow the ECR operations if the value of the aws:PrincipalOrgID condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five.
- Create a public repository in Amazon ECR. Create an IAM role in the ECR account. Set permissions so that any account can assume the role if the value of the aws:PrincipalOrgID condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five.
- Create a private repository in Amazon ECR. Create a permissions policy for the repository that includes only required ECR operations. Include a condition to allow the ECR operations for all account IDs in the organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.
- Create a public repository in Amazon ECR. Configure Amazon ECR to use an interface VPC endpoint with an endpoint policy that includes the required permissions for images that the company needs to pull. Include a condition to allow the ECR operations for all account IDs in the company's organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.

A

Only accounts that are within the company's organization should have access to the images. ➔ Private repository in ECR
retain only the five most recent untagged images ➔ Lifecycle policy

Question 308:

A solutions architect is reviewing a company's process for taking snapshots of Amazon RDS DB instances. The company takes automatic snapshots every day and retains the snapshots for 7 days.

The solutions architect needs to recommend a solution that takes snapshots every 6 hours and retains the snapshots for 30 days. The company uses AWS Organizations to manage all of its AWS accounts. The company needs a consolidated view of the health of the RDS snapshots.

Which solution will meet these requirements with the LEAST operational overhead?

- Turn on the cross-account management feature in AWS Backup. Create a backup plan that specifies the frequency and retention requirements. Add a tag to the DB instances. Apply the backup plan by using tags. Use AWS Backup to monitor the status of the backups.
- Turn on the cross-account management feature in Amazon RDS. Create a snapshot global policy that specifies the frequency and retention requirements. Use the RDS console in the management account to monitor the status of the backups.
- Turn on the cross-account management feature in AWS CloudFormation. From the management account, deploy a CloudFormation stack set that contains a backup plan from AWS Backup that specifies the frequency and retention requirements. Create an AWS Lambda function in the management account to monitor the status of the backups. Create an Amazon EventBridge rule in each account to run the Lambda function on a schedule.
- Configure AWS Backup in each account. Create an Amazon Data Lifecycle Manager lifecycle policy that specifies the frequency and retention requirements. Specify the DB instances as the target resource. Use the Amazon Data Lifecycle Manager console in each member account to monitor the status of the backups.

A

<https://docs.aws.amazon.com/aws-backup/latest/devguide/create-cross-account-backup.html>

AWS Backup



- Fully managed service
- Centrally manage and automate backups across AWS services
- No need to create custom scripts and manual processes
- Supported services:
 - Amazon EC2 / Amazon EBS
 - Amazon S3
 - Amazon RDS (all DBs engines) / Amazon Aurora / Amazon DynamoDB
 - Amazon DocumentDB / Amazon Neptune
 - Amazon EFS / Amazon FSx (Lustre & Windows File Server)
 - AWS Storage Gateway (Volume Gateway)
- Supports cross-region backups
- Supports cross-account backups

AWS Backup



- point in time recovery
- Supports PITR for supported services
 - On-Demand and Scheduled backups
 - Tag-based backup policies
 - You create backup policies known as **Backup Plans**
 - Backup frequency (every 12 hours, daily, weekly, monthly, cron expression)
 - Backup window
 - Transition to Cold Storage (Never, Days, Weeks, Months, Years)
 - Retention Period (Always, Days, Weeks, Months, Years)

AWS Backup



Question 309:

A company is using AWS Organizations with a multi-account architecture. The company's current security configuration for the account architecture includes SCPs, resource-based policies, identity-based policies, trust policies, and session policies.

A solutions architect needs to allow an IAM user in Account A to assume a role in Account B.

Which combination of steps must the solutions architect take to meet this requirement? (Choose three.)

- A. Configure the SCP for Account A to allow the action.
- B. Configure the resource-based policies to allow the action.
- C. Configure the identity-based policy on the user in Account A to allow the action.
- D. Configure the identity-based policy on the user in Account B to allow the action.
- E. Configure the trust policy on the target role in Account B to allow the action.
- F. Configure the session policy to allow the action and to be passed programmatically by the GetSessionToken API operation.

C, E, F

https://docs.aws.amazon.com/STS/latest/APIReference/API_GetSessionToken.html

resource-base policy: <https://trello.com/c/NWVczDZg/403-resource-base-policy>

identity-based policy: <https://trello.com/c/KCq7fHKe/404-identity-based-policy>

session policies: <https://trello.com/c/vyWqUuYW/405-sts>

Question 310:

A company wants to use Amazon S3 to back up its on-premises file storage solution. The company's on-premises file storage solution supports NFS, and the company wants its new solution to support NFS. The company wants to archive the backup files after 5 days. If the company needs archived files for disaster recovery, the company is willing to wait a few days for the retrieval of those files.

Which solution meets these requirements MOST cost-effectively?

- A. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- B. Deploy an AWS Storage Gateway volume gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the volume gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.
- C. Deploy an AWS Storage Gateway tape gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the tape gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- D. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.

D
supports NFS → AWS Storage Gateway file gateway
MOST cost-effectively and willing to wait a few days → Glacier Deep Archive is cheaper than Standard-IA

S3 Storage Classes – Infrequent Access

- For data that is less frequently accessed, but requires rapid access when needed
- Lower cost than S3 Standard
- Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
 - 99.9% Availability
 - Use cases: Disaster Recovery, backups
- Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)
 - High durability (99.99999999%) in a single AZ; data lost when AZ is destroyed
 - 99.5% Availability
 - Use Cases: Storing secondary backup copies of on-premise data, or data you can recreate



Amazon S3 Glacier Storage Classes

- Low-cost object storage meant for archiving / backup
- Pricing: price for storage + object retrieval cost

- Amazon S3 Glacier Instant Retrieval

- Millisecond retrieval, great for data accessed once a quarter
truy suất 1 phần nghìn giây, dùng cho truy cập dữ liệu 1 quý 1 lần
- Minimum storage duration of 90 days Lưu trữ tối thiểu 90 ngày

- Amazon S3 Glacier Flexible Retrieval (formerly Amazon S3 Glacier):

- Expedited (1 to 5 minutes), Standard (3 to 5 hours), Bulk (5 to 12 hours) – free
- Minimum storage duration of 90 days

- Amazon S3 Glacier Deep Archive – for long term storage:

- Standard (12 hours), Bulk (48 hours)
- Minimum storage duration of 180 days



Question 311:

A company runs its application on Amazon EC2 instances and AWS Lambda functions. The EC2 instances experience a continuous and stable load. The Lambda functions experience a varied and unpredictable load. The application includes a caching layer that uses an Amazon MemoryDB for Redis cluster.

A solutions architect must recommend a solution to minimize the company's overall monthly costs.

Which solution will meet these requirements?

- Purchase an EC2 instance Savings Plan to cover the EC2 instances. Purchase a Compute Savings Plan for Lambda to cover the minimum expected consumption of the Lambda functions. Purchase reserved nodes to cover the MemoryDB cache nodes.
- Purchase a Compute Savings Plan to cover the EC2 instances. Purchase Lambda reserved concurrency to cover the expected Lambda usage. Purchase reserved nodes to cover the MemoryDB cache nodes.
- Purchase a Compute Savings Plan to cover the entire expected cost of the EC2 instances, Lambda functions, and MemoryDB cache nodes.
- Purchase a Compute Savings Plan to cover the EC2 instances and the MemoryDB cache nodes. Purchase Lambda reserved concurrency to cover the expected Lambda usage.

A

AWS Savings Plan



- New pricing model to get a discount based on long-term usage
Cam kết sử dụng 1 loại
- Commit to a certain type of usage: ex \$10 per hour for 1 to 3 years
- Any usage beyond the savings plan is billed at the on-demand price
- EC2 Instance Savings plan (up to 72% - same discount as Standard RIs)
 - Select instance family (e.g. M5, C5...), and locked to a specific region
 - Flexible across size (m5.large to m5.4xlarge), OS (Windows to Linux), thuê tenancy (dedicated or default)
- Compute Savings plan (up to 66% - same discount as Convertible RIs)
 - Ability to move between instance family (move from C5 to M5), region (Ireland to US), compute type (EC2, Fargate, Lambda), OS & tenancy
- SageMaker Savings plan (up to 64% off)

Question 312:

A company is launching a new online game on Amazon EC2 instances. The game must be available globally. The company plans to run the game in three AWS Regions us-east-1, eu-west-1, and ap-southeast-1. The game's leaderboards, player inventory and event status must be available across Regions.

A solutions architect must design a solution that will give any Region the ability to scale to handle the load of all Regions. Additionally, users must automatically connect to the Region that provides the least latency.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an EC2 Spot Fleet. Attach the Spot Fleet to a Network Load Balancer (NLB) in each Region. Create an AWS Global Accelerator IP address that points to the NLB. Create an Amazon Route 53 latency-based routing entry for the Global Accelerator IP address. Save the game metadata to an Amazon RDS for MySQL DB instance in each Region. Set up a read replica in the other Regions.

B. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses geoproximity routing and points to the NLB in that Region. Save the game metadata to MySQL databases on EC2 instances in each Region. Set up replication between the database EC2 instances in each Region.

C. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses latency-based routing and points to the NLB in that Region. Save the game metadata to an Amazon DynamoDB global table.

D. Use EC2 Global View. Deploy the EC2 instances to each Region. Attach the instances to a Network Load Balancer (NLB). Deploy a DNS server on an EC2 instance in each Region. Set up custom logic on each DNS server to redirect the user to the Region that provides the lowest latency. Save the game metadata to an Amazon Aurora global database.

C

Autoscaling and NLB for Load Distribution, Latency Routing for Least Latency and DynamoDB Global Table for replication across regions

Network Load Balancer (v2)



- Network load balancers (Layer 4) allow to:
 - Forward TCP & UDP traffic to your instances
 - Handle millions of requests per second
 - Less latency ~100 ms (vs 400 ms for ALB)
- NLB has one static IP per AZ, and supports assigning Elastic IP (helpful for whitelisting specific IP)
- NLB are used for extreme performance, TCP or UDP traffic
- Not included in the AWS free tier

Question 313:

A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances.

A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs.

Which steps should the solutions architect recommend to meet these requirements? (Choose three.)

A. Deploy two firewall appliances into the shared services VPC, each in a separate Availability Zone.

B. Create a new Network Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Network Load Balancer. Add each of the firewall appliance instances to the target group.

C. Create a new Gateway Load Balancer in the shared services VPC
Create a new target group, and attach it to the new Gateway Load Balancer Add each of the firewall appliance instances to the target group.

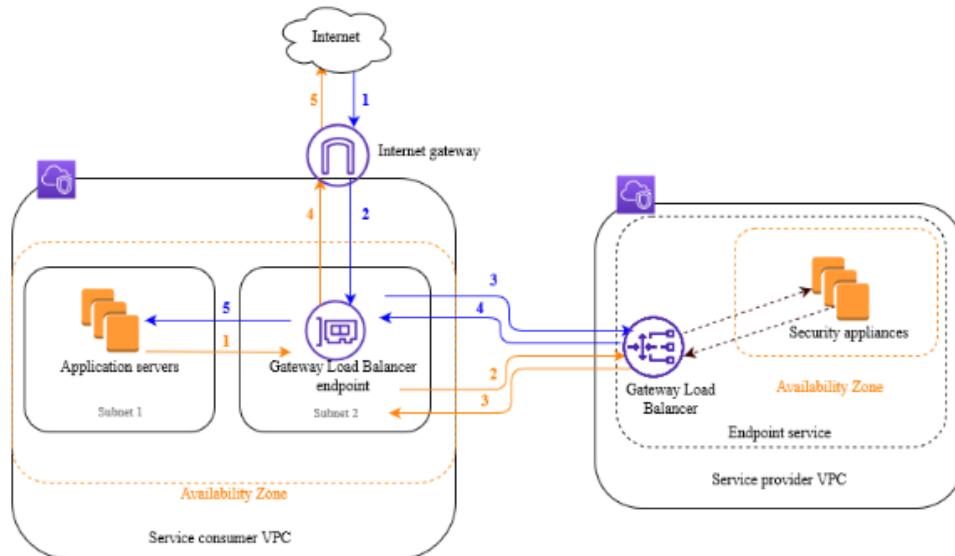
D. Create a VPC interface endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.

E. Deploy two firewall appliances into the shared services VPC, each in the same Availability Zone.

F. Create a VPC Gateway Load Balancer endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.

A,C,F

A two firewalls spread over two availability zones for HA and balanced by an NLB, then (C) a Gateway Load Balancer to interface to the virtual 3rd party network firewalls through the NLB, then (F) a Gateway Load Balancer EndPoint in the Consumer VPC with routes taking the traffic to the shared GLB + Firewalls



<https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html>

Question 314:

A solutions architect needs to migrate an on-premises legacy application to AWS. The application runs on two servers behind a load balancer. The application requires a license file that is associated with the MAC address of the server's network adapter. It takes the software vendor 12 hours to send new license files. The application also uses configuration files with a static IP address to access a database server, host names are not supported.

Given these requirements, which combination of steps should be taken to implement highly available architecture for the application servers in AWS? (Choose two.)

- A. Create a pool of ENIs. Request license files from the vendor for the pool, and store the license files in Amazon S3. Create a bootstrap automation script to download a license file and attach the corresponding ENI to an Amazon EC2 instance.
- B. Create a pool of ENIs. Request license files from the vendor for the pool, store the license files on an Amazon EC2 instance. Create an AMI from the instance and use this AMI for all future EC2 instances.
- C. Create a bootstrap automation script to request a new license file from the vendor. When the response is received, apply the license file to an Amazon EC2 instance.
- D. Edit the bootstrap automation script to read the database server IP address from the AWS Systems Manager Parameter Store, and inject the value into the local configuration files.
- E. Edit an Amazon EC2 instance to include the database server IP address in the configuration files and re-create the AMI to use for all future EC2 instances.

A,D

<https://aws.amazon.com/blogs/aws/new-elastic-network-interfaces-in-the-virtual-private-cloud/>

Question 315:

A company runs its sales reporting application in an AWS Region in the United States. The application uses an Amazon API Gateway Regional API and AWS Lambda functions to generate on-demand reports from data in an Amazon RDS for MySQL database. The frontend of the application is hosted on Amazon S3 and is accessed by users through an Amazon CloudFront distribution. The company is using Amazon Route 53 as the DNS service for the domain. Route 53 is configured with a simple routing policy to route traffic to the API Gateway API.

In the next 6 months, the company plans to expand operations to Europe. More than 90% of the database traffic is read-only traffic. The company has already deployed an API Gateway API and Lambda functions in the new Region.

A solutions architect must design a solution that minimizes latency for users who download reports.

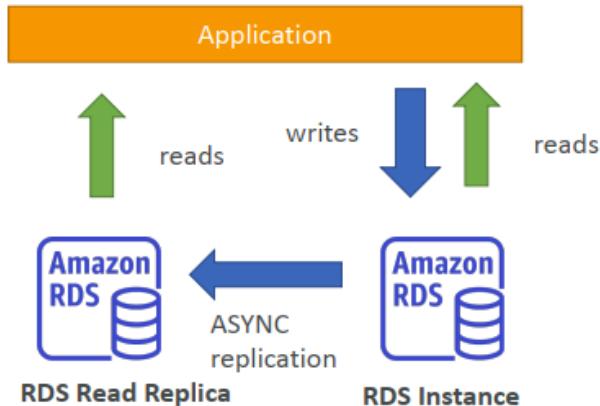
Which solution will meet these requirements?

- A. Use an AWS Database Migration Service (AWS DMS) task with full load to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- B. Use an AWS Database Migration Service (AWS DMS) task with full load plus change data capture (CDC) to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.
- C. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- D. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.

C

More than 90% of the database traffic is read-only traffic → cross region read replica minimizes latency → Route 53 record to latency-based routing

- **Read Replicas:** Increase read throughput. Eventual consistency. Can be cross-region



Routing Policies – Latency-based

- Redirect to the resource that has the least latency close to us
- Super helpful when latency for users is a priority
- Latency is based on traffic between users and AWS Regions
- Germany users may be directed to the US (if that's the lowest latency)
- Can be associated with Health Checks (has a failover capability)



Question 316:

A software company needs to create short-lived test environments to test pull requests as part of its development process. Each test environment consists of a single Amazon EC2 instance that is in an Auto Scaling group.

The test environments must be able to communicate with a central server to report test results. The central server is located in an on-premises data center. A solutions architect must implement a solution so that the company can create and delete test environments without any manual intervention. The company has created a transit gateway with a VPN attachment to the on-premises network.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an AWS CloudFormation template that contains a transit gateway attachment and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets to deploy a new stack for each VPC in the account. Deploy a new VPC for each test environment.
- B. Create a single VPC for the test environments. Include a transit gateway attachment and related routing configurations. Use AWS CloudFormation to deploy all test environments into the VPC.
- C. Create a new OU in AWS Organizations for testing. Create an AWS CloudFormation template that contains a VPC, necessary networking resources, a transit gateway attachment, and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets for deployments into each account under the testing OU. Create a new account for each test environment.
- D. Convert the test environment EC2 instances into Docker images. Use AWS CloudFormation to configure an Amazon Elastic Kubernetes Service (Amazon EKS) cluster in a new VPC, create a transit gateway attachment, and create related routing configurations. Use Kubernetes to manage the deployment and lifecycle of the test environments.

B

LEAST operational overhead ➔ B

Question 317:

A company is deploying a new API to AWS. The API uses Amazon API Gateway with a Regional API endpoint and an AWS Lambda function for hosting. The API retrieves data from an external vendor API, stores data in an Amazon DynamoDB global table, and retrieves data from the DynamoDB global table. The API key for the vendor's API is stored in AWS Secrets Manager and is encrypted with a customer managed key in AWS Key Management Service (AWS KMS). The company has deployed its own API into a single AWS Region.

A solutions architect needs to change the API components of the company's API to ensure that the components can run across multiple Regions in an active-active configuration.

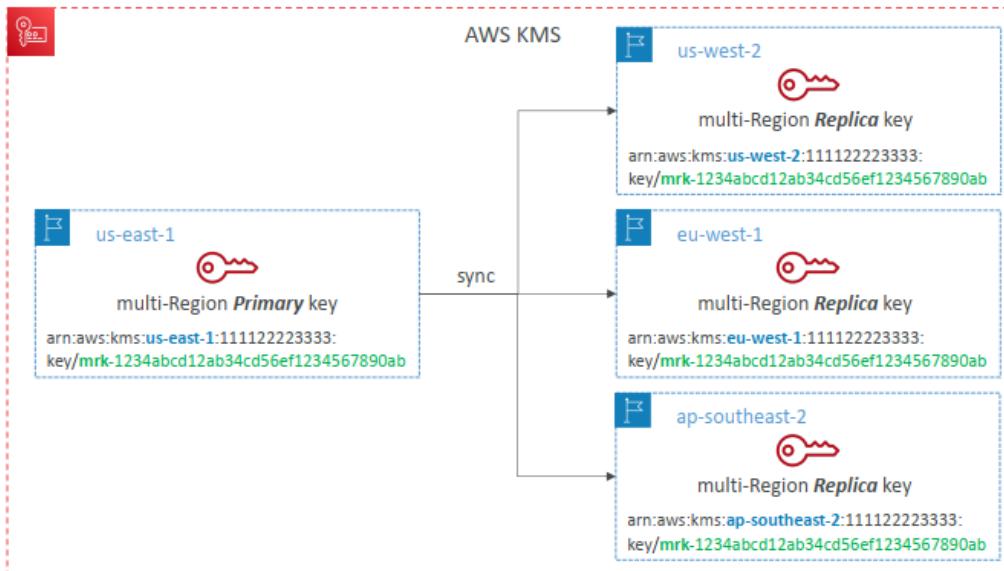
Which combination of changes will meet this requirement with the LEAST operational overhead? (Choose three.)

- A. Deploy the API to multiple Regions. Configure Amazon Route 53 with custom domain names that route traffic to each Regional API endpoint. Implement a Route 53 multivalue answer routing policy.
- B. Create a new KMS multi-Region customer managed key. Create a new KMS customer managed replica key in each in-scope Region.

- C. Replicate the existing Secrets Manager secret to other Regions. For each in-scope Region's replicated secret, select the appropriate KMS key.
- D. Create a new AWS managed KMS key in each in-scope Region. Convert an existing key to a multiRegion key. Use the multi-Region key in other Regions.
- E. Create a new Secrets Manager secret in each in-scope Region. Copy the secret value from the existing Region to the new secret in each in-scope Region.
- F. Modify the deployment process for the Lambda function to repeat the deployment across in-scope Regions. Turn on the multi-Region option for the existing API. Select the Lambda function that is deployed in each Region as the backend for the multi-Region API.

A,B,C

KMS Multi-Region Keys



<https://docs.aws.amazon.com/secretsmanager/latest/userguide/replicate-secrets.html>
<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-create.html>

Question 318:

An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation, the company wants to migrate its application and database to AWS to increase the reliability of its architecture.

Which solution should provide the HIGHEST level of reliability?

- A. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon Neptune
- B. Migrate the database to Amazon Aurora MySQL. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in an Amazon ElastiCache for Redis replication group.
- C. Migrate the database to Amazon DocumentDB (with MongoDB compatibility). Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balancer. Store sessions in Amazon Kinesis Data Firehose.
- D. Migrate the database to an Amazon RDS MariaDB Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon ElastiCache for Memcached.

B

Store sessions → Amazon ElastiCache for redis
MySQL database → RDS or Aurora

Question 319:

A company's solutions architect needs to provide secure Remote Desktop connectivity to users for Amazon EC2 Windows instances that are hosted in a VPC. The solution must integrate centralized user management with the company's on-premises Active Directory. Connectivity to the VPC is through the internet. The company has hardware that can be used to establish an AWS Site-to-Site VPN connection.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy an EC2 instance as a bastion host in the VPC. Ensure that the EC2 instance is joined to the domain. Use the bastion host to access the target instances through RDP.
- B. Configure AWS IAM Identity Center (AWS Single Sign-On) to integrate with the on-premises Active Directory by using the AWS Directory Service for Microsoft Active Directory AD Connector. Configure permission sets against user groups for access to AWS Systems Manager. Use Systems Manager Fleet Manager to access the target instances through RDP.
- C. Implement a VPN between the on-premises environment and the target VPC. Ensure that the target instances are joined to the on-premises Active Directory domain over the VPN connection. Configure RDP access through the VPN. Connect from the company's network to the target instances.
- D. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy a Remote Desktop Gateway on AWS by using an AWS Quick Start. Ensure that the Remote Desktop Gateway is joined to the domain. Use the Remote Desktop Gateway to access the target instances through RDP.

B

<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>
<https://aws.amazon.com/tw/blogs/networking-and-content-delivery/integrating-your-directory-services-dns-resolution-with-amazon-route-53-resolvers/>

Question 320:

A company's compliance audit reveals that some Amazon Elastic Block Store (Amazon EBS) volumes that were created in an AWS account were not encrypted. A solutions architect must implement a solution to encrypt all new EBS volumes at rest.

Which solution will meet this requirement with the LEAST effort?

- A. Create an Amazon EventBridge rule to detect the creation of unencrypted EBS volumes. Invoke an AWS Lambda function to delete noncompliant volumes.
- B. Use AWS Audit Manager with data encryption.
- C. Create an AWS Config rule to detect the creation of a new EBS volume. Encrypt the volume by using AWS Systems Manager Automation.
- D. Turn on EBS encryption by default in all AWS Regions.

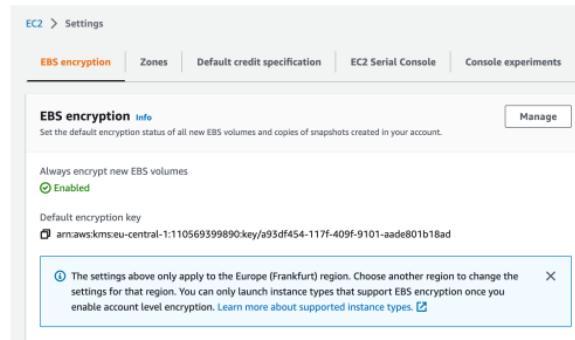
D

must implement a solution to encrypt all new EBS volumes **at rest**, LEAST effort → turn on EBS encryption

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>

EBS Encryption – Account level setting

- New Amazon EBS volumes aren't encrypted by default
- There's an account-level setting to encrypt automatically new EBS volumes and Snapshots
- This setting needs to be enabled on a per-region basis



Encryption of Amazon Elastic Block Store (Amazon EBS) volumes is important to an organization's data protection strategy. It is an important step in establishing a well-architected environment. Although there is no direct way to encrypt existing unencrypted EBS volumes or snapshots, you can encrypt them by creating a new volume or snapshot.

Question 321:

A research company is running daily simulations in the AWS Cloud to meet high demand. The simulations run on several hundred Amazon EC2 instances that are based on Amazon Linux 2. Occasionally, a simulation gets stuck and requires a cloud operations engineer to solve the problem by connecting to an EC2 instance through SSH.

Company policy states that no EC2 instance can use the same SSH key and that all connections must be logged in AWS CloudTrail.

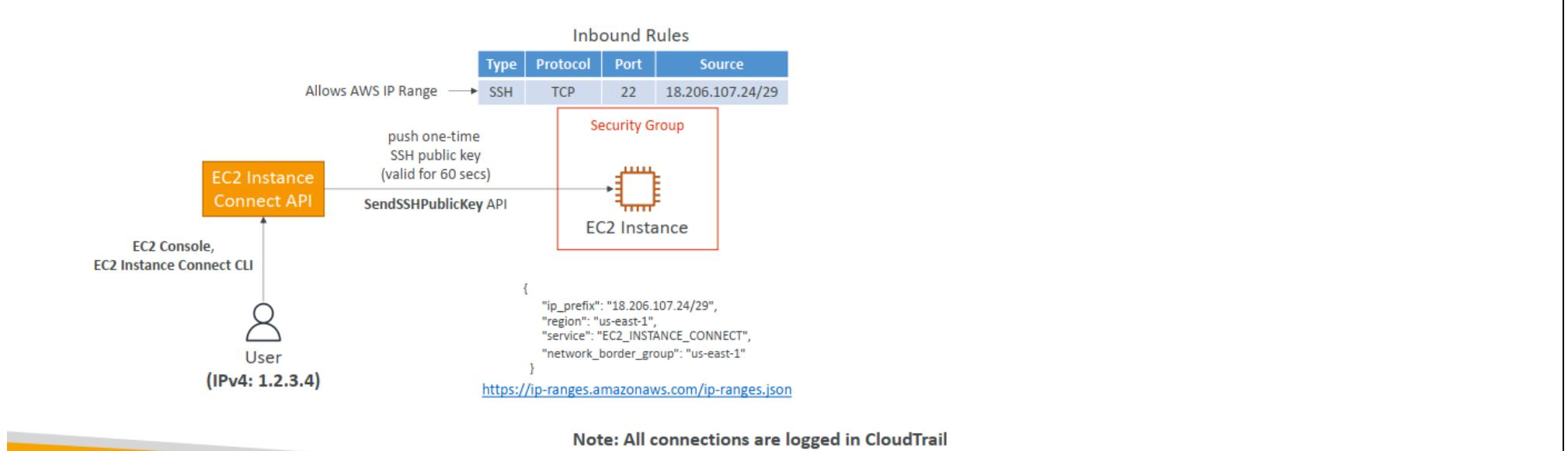
How can a solutions architect meet these requirements?

- A. Launch new EC2 instances, and generate an individual SSH key for each instance. Store the SSH key in AWS Secrets Manager. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the GetSecretValue action. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.
- B. Create an AWS Systems Manager document to run commands on EC2 instances to set a new unique SSH key. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement to run Systems Manager documents. Instruct the engineers to run the document to set an SSH key and to connect through any SSH client.
- C. Launch new EC2 instances without setting up any SSH key for the instances. Set up EC2 Instance Connect on each instance. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the SendSSHPublicKey action. Instruct the engineers to connect to the instance by using a browser-based SSH client from the EC2 console.
- D. Set up AWS Secrets Manager to store the EC2 SSH key. Create a new AWS Lambda function to create a new SSH key and to call AWS Systems Manager Session Manager to set the SSH key on the EC2 instance. Configure Secrets Manager to use the Lambda function for automatic rotation once daily. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.

C

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connect-linux-inst-eic.html>

EC2 Instance Connect (SendSSHPublicKey API)

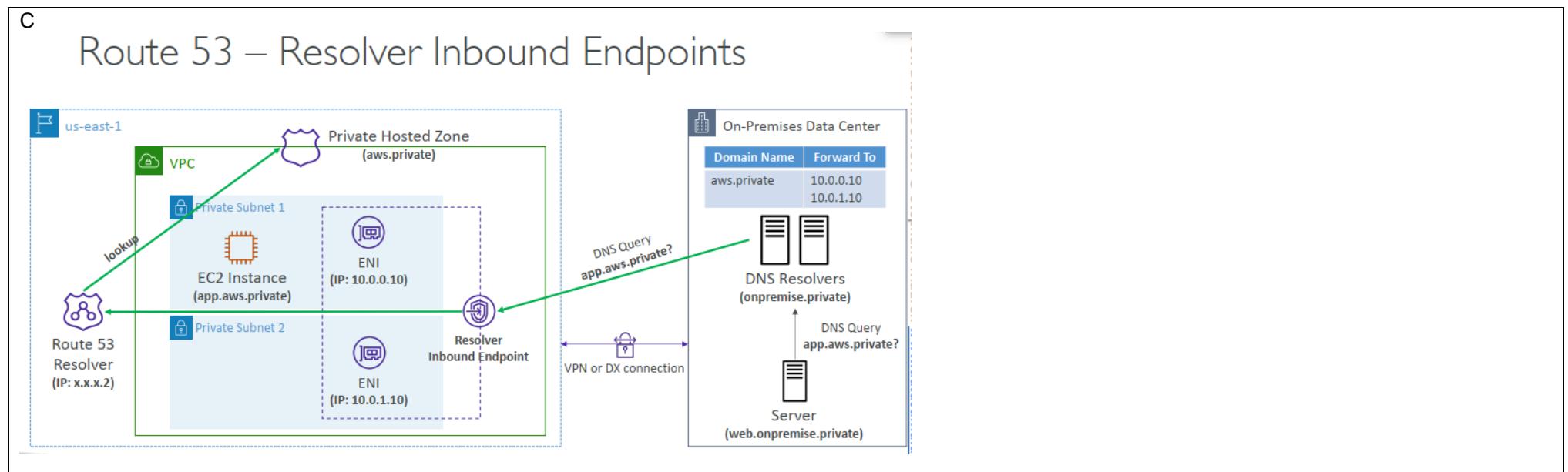


Question 322:

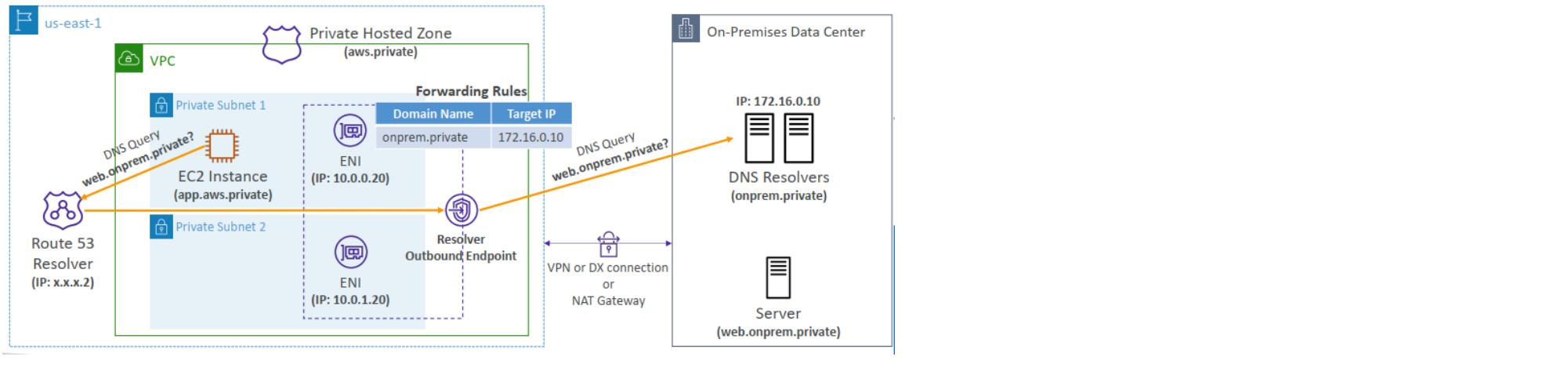
A company is migrating mobile banking applications to run on Amazon EC2 instances in a VPC. Backend service applications run in an on-premises data center. The data center has an AWS Direct Connect connection into AWS. The applications that run in the VPC need to resolve DNS requests to an on-premises Active Directory domain that runs in the data center.

Which solution will meet these requirements with the LEAST administrative overhead?

- Provision a set of EC2 instances across two Availability Zones in the VPC as caching DNS servers to resolve DNS queries from the application servers within the VPC.
- Provision an Amazon Route 53 private hosted zone. Configure NS records that point to on-premises DNS servers.
- Create DNS endpoints by using Amazon Route 53 Resolver. Add conditional forwarding rules to resolve DNS namespaces between the on-premises data center and the VPC.
- Provision a new Active Directory domain controller in the VPC with a bidirectional trust between this new domain and the on-premises Active Directory domain.



Route 53 – Resolver Outbound Endpoints



Question 323:

A company processes environmental data. The company has set up sensors to provide a continuous stream of data from different areas in a city. The data is available in JSON format.

The company wants to use an AWS solution to send the data to a database that does not require fixed schemas for storage. The data must be sent in real time.

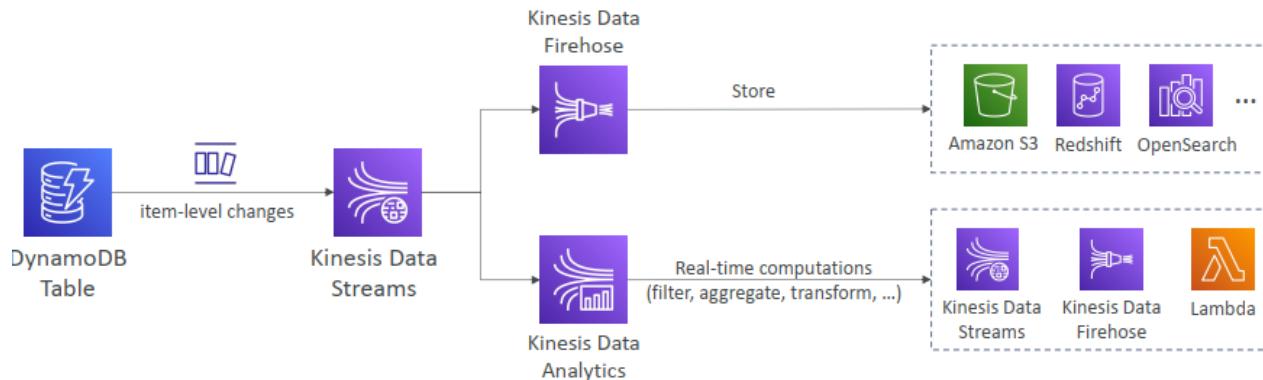
Which solution will meet these requirements?

- A. Use Amazon Kinesis Data Firehose to send the data to Amazon Redshift.
- B. Use Amazon Kinesis Data Streams to send the data to Amazon DynamoDB.
- C. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to send the data to Amazon Aurora.
- D. Use Amazon Kinesis Data Firehose to send the data to Amazon Keyspaces (for Apache Cassandra).

B

Amazon Kinesis Data Streams for DynamoDB

- You can use Kinesis Data Streams to capture item-level changes in DynamoDB
- Custom and longer data retention period (> 24 hours in DynamoDB Streams)



Question 324:

A company is migrating a legacy application from an on-premises data center to AWS. The application uses MongoDB as a key-value database. According to the company's technical guidelines, all Amazon EC2 instances must be hosted in a private subnet without an internet connection. In addition, all connectivity between applications and databases must be encrypted. The database must be able to scale based on demand.

Which solution will meet these requirements?

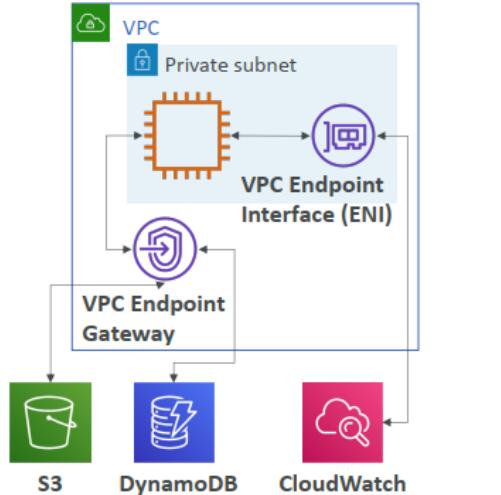
- Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the instance endpoint to connect to Amazon DocumentDB.
- Create new Amazon DynamoDB tables for the application with on-demand capacity. Use a gateway VPC endpoint for DynamoDB to connect to the DynamoDB tables.
- Create new Amazon DynamoDB tables for the application with on-demand capacity. Use an interface VPC endpoint for DynamoDB to connect to the DynamoDB tables.
- Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the cluster endpoint to connect to Amazon DocumentDB.

B

key-value database and The database must be able to scale based on demand ➔ DynamoDB

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in yourVPC
 - Check Route Tables



DynamoDB – in short

- NoSQL database, fully managed, massive scale (1,000,000 rps) quy mô lớn
- Similar to Apache Cassandra (can migrate to DynamoDB)
- No disk space to provision, max object size is 400 KB
- Capacity: provisioned (WCU, RCU, & Auto Scaling) or on-demand
- Supports CRUD (Create Read Update Delete)
- Read: eventually or strong consistency
- Supports transactions across multiple tables (ACID support)
- Backups available, point in time recovery
- Table classes: Standard and Infrequent Access (IA)



Question 325:

A company is running an application on Amazon EC2 instances in the AWS Cloud. The application is using a MongoDB database with a replica set as its data tier. The MongoDB database is installed on systems in the company's on-premises data center and is accessible through an AWS Direct Connect connection to the data center environment.

A solutions architect must migrate the on-premises MongoDB database to Amazon DocumentDB (with MongoDB compatibility).

Which strategy should the solutions architect choose to perform this migration?

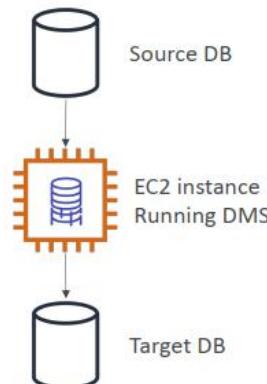
- A. Create a fleet of EC2 instances. Install MongoDB Community Edition on the EC2 instances, and create a database. Configure continuous synchronous replication with the database that is running in the on-premises data center.
- B. Create an AWS Database Migration Service (AWS DMS) replication instance. Create a source endpoint for the on-premises MongoDB database by using change data capture (CDC). Create a target endpoint for the Amazon DocumentDB database. Create and run a DMS migration task.
- C. Create a data migration pipeline by using AWS Data Pipeline. Define data nodes for the on-premises MongoDB database and the Amazon DocumentDB database. Create a scheduled task to run the data pipeline.
- D. Create a source endpoint for the on-premises MongoDB database by using AWS Glue crawlers. Configure continuous asynchronous replication between the MongoDB database and the Amazon DocumentDB database.

B

DMS – Database Migration Service



- Quickly and securely migrate databases to AWS, resilient, self healing
- The source database remains available during the migration
- Supports:
 - Homogeneous migrations: ex Oracle to Oracle
 - Heterogeneous migrations: ex Microsoft SQL Server to Aurora
- Continuous Data Replication using CDC
- You must create an EC2 instance to perform the replication tasks



DMS Sources and Targets

SOURCES:

- On-premises and EC2 instances databases: Oracle, MS SQL Server, MySQL, MariaDB, PostgreSQL, MongoDB, SAP, DB2
- Azure: Azure SQL Database
- Amazon RDS: all including Aurora
- Amazon S3
- DocumentDB

TARGETS:

- On-premises and EC2 instances databases: Oracle, MS SQL Server, MySQL, MariaDB, PostgreSQL, SAP
- Amazon RDS including Aurora
- Amazon Redshift
- Amazon DynamoDB
- Amazon S3
- OpenSearch Service
- Kinesis Data Streams
- DocumentDB

DMS – Good things to know

- Works over VPC Peering, VPN (site to site, software), Direct Connect
- Supports Full Load, Full Load + CDC, or CDC only
- Oracle:
 - Source: Supports TDE for the source using “BinaryReader”
 - Target: Supports BLOBS in tables that have a primary key, and TDE
- OpenSearch:
 - Source: does not exist
 - Target: possible to migrate from a relational database using DMS
 - Therefore, DMS cannot be used to replicate OpenSearch data

Question 326:

A company is rearchitecting its applications to run on AWS. The company's infrastructure includes multiple Amazon EC2 instances. The company's development team needs different levels of access. The company wants to implement a policy that requires all Windows EC2 instances to be joined to an Active Directory domain on AWS. The

company also wants to implement enhanced security processes such as multi-factor authentication (MFA). The company wants to use managed AWS services wherever possible.

Which solution will meet these requirements?

- A. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.
- B. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.
- C. Create an AWS Directory Service Simple AD implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.
- D. Create an AWS Directory Service Simple AD implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.

B

https://docs.aws.amazon.com/workspaces/latest/adminguide/directory_administration.html

You'll perform most administrative tasks for your WorkSpaces directory using directory management tools, such as the Active Directory Administration Tools. However, you'll use the WorkSpaces console to perform some directory-related tasks. For more information, see [Manage directories for WorkSpaces Personal](#).

If you create a directory with AWS Managed Microsoft AD or Simple AD that includes five or more WorkSpaces, we recommend that you centralize administration on an Amazon EC2 instance. Although you can install the directory management tools on a WorkSpace, using an Amazon EC2 instance is a more robust solution.

Question 327:

A company wants to migrate its on-premises application to AWS. The database for the application stores structured product data and temporary user session data. The company needs to decouple the product data from the user session data. The company also needs to implement replication in another AWS Region for disaster recovery.

Which solution will meet these requirements with the HIGHEST performance?

- A. Create an Amazon RDS DB instance with separate schemas to host the product data and the user session data. Configure a read replica for the DB instance in another Region.

B. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create a global datastore in Amazon ElastiCache for Memcached to host the user session data.

C. Create two Amazon DynamoDB global tables. Use one global table to host the product data. Use the other global table to host the user session data. Use DynamoDB Accelerator (DAX) for caching.

D. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create an Amazon DynamoDB global table to host the user session data.

D
structured product data → relational database → RDS

Amazon ElastiCache for Memcached does not support Multi-AZ (Availability Zone) deployments or global datastores → B is incorrect

Question 328:

A company orchestrates a multi-account structure on AWS by using AWS Control Tower. The company is using AWS Organizations, AWS Config, and AWS Trusted Advisor. The company has a specific OU for development accounts that developers use to experiment on AWS. The company has hundreds of developers, and each developer has an individual development account.

The company wants to optimize costs in these development accounts. Amazon EC2 instances and Amazon RDS instances in these accounts must be burstable. The company wants to disallow the use of other services that are not relevant.

What should a solutions architect recommend to meet these requirements?

A. Create a custom SCP in AWS Organizations to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the SCP to the development OU.

B. Create a custom detective control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.

C. Create a custom preventive control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.

D. Create an AWS Config rule in the AWS Control Tower account. Configure the AWS Config rule to allow the deployment of only burstable instances and to disallow services that are not relevant. Deploy the AWS Config rule to the development OU by using AWS CloudFormation StackSets.

C

AWS Control Tower



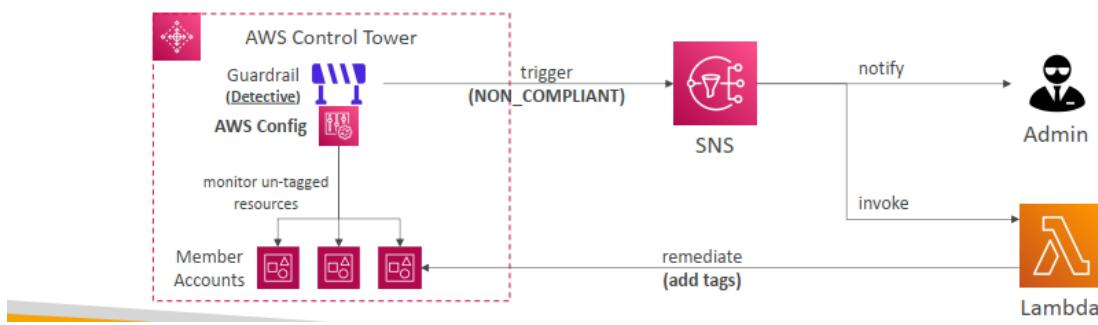
- Easy way to set up and govern a secure and compliant multi-account AWS environment based on best practices
- Benefits:
 - Automate the set up of your environment in a few clicks
 - tự động hóa quản lý chính sách liên tục
 - Automate ongoing policy management using guardrails
 - Detect policy violations and remediate them
 - Monitor compliance through an interactive dashboard
- AWS Control Tower runs on top of AWS Organizations:
 - It automatically sets up AWS Organizations to organize accounts and implement SCPs (Service Control Policies)

AWS Control Tower – Detect and Remediate Policy Violations

• Guardrail

(adj): tiếp tục, tiếp diễn

- Provides ongoing governance for your Control Tower environment (AWS Accounts)
- Preventive – using SCPs (e.g., Disallow Creation of Access Keys for the Root User)
- Detective – using AWS Config (e.g., Detect Whether MFA for the Root User is Enabled)
- Example: identify non-compliant resources (e.g., untagged resources)



Question 329:

A financial services company runs a complex, multi-tier application on Amazon EC2 instances and AWS Lambda functions. The application stores temporary data in Amazon S3. The S3 objects are valid for only 45 minutes and are deleted after 24 hours.

The company deploys each version of the application by launching an AWS CloudFormation stack. The stack creates all resources that are required to run the application. When the company deploys and validates a new application version, the company deletes the CloudFormation stack of the old version.

The company recently tried to delete the CloudFormation stack of an old application version, but the operation failed. An analysis shows that CloudFormation failed to delete an existing S3 bucket. A solutions architect needs to resolve this issue without making major changes to the application's architecture.

Which solution meets these requirements?

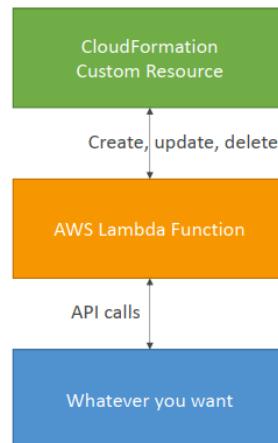
- A. Implement a Lambda function that deletes all files from a given S3 bucket. Integrate this Lambda function as a custom resource into the CloudFormation stack. Ensure that the custom resource has a DependsOn attribute that points to the S3 bucket's resource.
- B. Modify the CloudFormation template to provision an Amazon Elastic File System (Amazon EFS) file system to store the temporary files there instead of in Amazon S3. Configure the Lambda functions to run in the same VPC as the file system. Mount the file system to the EC2 instances and Lambda functions.
- C. Modify the CloudFormation stack to create an S3 Lifecycle rule that expires all objects 45 minutes after creation. Add a DependsOn attribute that points to the S3 bucket's resource.
- D. Modify the CloudFormation stack to attach a DeletionPolicy attribute with a value of Delete to the S3 bucket.

A

C is incorrect because S3 object need delete after 24 hours.

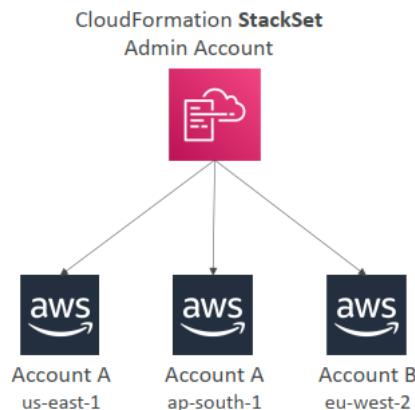
CloudFormation Custom Resources (Lambda)

- You can define a Custom Resource in CloudFormation to address any of these use cases:
- An AWS resource is **not yet supported** (new service for example)
- An **on-premises resource**
- Emptying an S3 bucket before being deleted
- Fetch an AMI id
- Anything you want...!



CloudFormation – StackSets

- Create, update, or delete stacks across multiple accounts and regions with a single operation
- Administrator account to create StackSets
- Trusted accounts to create, update, delete stack instances from StackSets
- When you update a stack set, all associated stack instances are updated throughout all accounts and regions
- Enable Automatic Deployment feature to automatically deploy to accounts in AWS Organization or OUs



Question 330:

A company has developed a mobile game. The backend for the game runs on several virtual machines located in an on-premises data center. The business logic is exposed using a REST API with multiple functions. Player session data is stored in central file storage. Backend services use different API keys for throttling and to distinguish between live and test traffic.

The load on the game backend varies throughout the day. During peak hours, the server capacity is not sufficient. There are also latency issues when fetching player session data. Management has asked a solutions architect to present a cloud architecture that can handle the game's varying load and provide low-latency data access. The API model should not be changed.

Which solution meets these requirements?

- Implement the REST API using a Network Load Balancer (NLB). Run the business logic on an Amazon EC2 instance behind the NLB. Store player session data in Amazon Aurora Serverless.
- Implement the REST API using an Application Load Balancer (ALB). Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- Implement the REST API using Amazon API Gateway. Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- Implement the REST API using AWS AppSync. Run the business logic in AWS Lambda. Store player session data in Amazon Aurora Serverless.

C

REST API with multiple functions and API keys → API Gateway

Question 331:

A company is migrating an application to the AWS Cloud. The application runs in an on-premises data center and writes thousands of images into a mounted NFS file system each night. After the company migrates the application, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system.

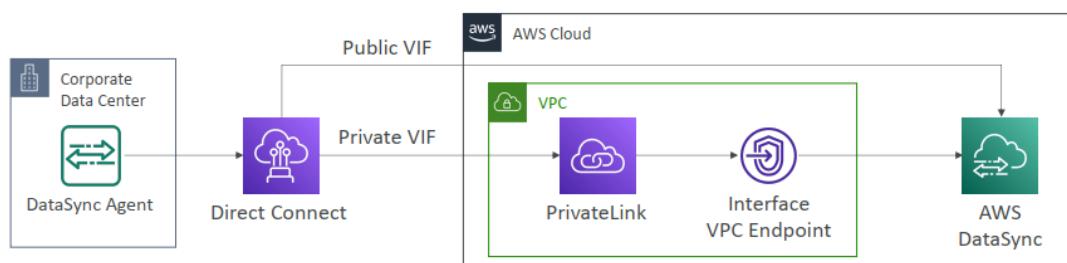
The company has established an AWS Direct Connect connection to AWS. Before the migration cutover, a solutions architect must build a process that will replicate the newly created on-premises images to the EFS file system.

What is the MOST operationally efficient way to replicate the images?

- A. Configure a periodic process to run the aws s3 sync command from the on-premises file system to Amazon S3. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.
- B. Deploy an AWS Storage Gateway file gateway with an NFS mount point. Mount the file gateway file system on the on-premises server. Configure a process to periodically copy the images to the mount point.
- C. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an S3 bucket by using a public VIF. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.
- D. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Configure a DataSync scheduled task to send the images to the EFS file system every 24 hours.

D

AWS DataSync Private VIF through Direct Connect



Question 332:

A company recently migrated a web application from an on-premises data center to the AWS Cloud. The web application infrastructure consists of an Amazon CloudFront distribution that routes to an Application Load Balancer (ALB), with Amazon Elastic Container Service (Amazon ECS) to process requests. A recent security audit revealed that the web application is accessible by using both CloudFront and ALB endpoints. However, the company requires that the web application must be accessible only by using the CloudFront endpoint.

Which solution will meet this requirement with the LEAST amount of effort?

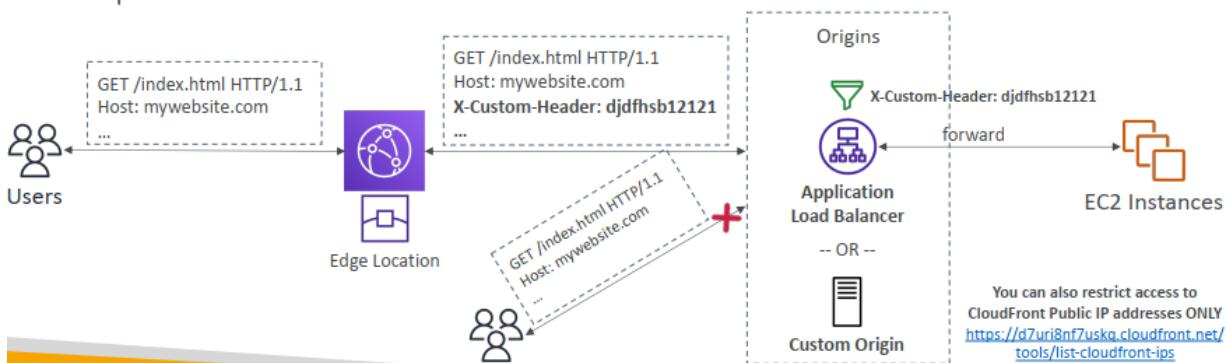
- A. Create a new security group and attach it to the CloudFront distribution. Update the ALB security group ingress to allow access only from the CloudFront security group.
- B. Update ALB security group ingress to allow access only from the com.amazonaws.global.cloudfront.origin-facing CloudFront managed prefix list.
- C. Create a com.amazonaws.region.elasticloadbalancing VPC interface endpoint for Elastic Load Balancing. Update the ALB scheme from internet-facing to internal.
- D. Extract CloudFront IPs from the AWS provided ip-ranges.json document. Update ALB security group ingress to allow access only from CloudFront IPs.

B

https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-cloudfront-managed-prefix-list/?nc1=h_ls

CloudFront – Restrict Access to Application Load Balancers and Custom Origins

- Prevent direct access to your ALB or Custom Origins (only access through CloudFront)
- First, configure CloudFront to add a **Custom HTTP Header** to requests it sends to the ALB
- Second, configure the ALB to only forward requests that contain that Custom HTTP Header
- Keep the custom header name and value secret!



Question 333:

A company hosts a community forum site using an Application Load Balancer (ALB) and a Docker application hosted in an Amazon ECS cluster. The site data is stored in Amazon RDS for MySQL and the container image is stored in ECR. The company needs to provide their customers with a disaster recovery SLA with an RTO of no more than 24 hours and RPO of no more than 8 hours.

Which of the following solutions is the MOST cost-effective way to meet the requirements?

- A. Use AWS CloudFormation to deploy identical ALB, EC2, ECS and RDS resources in two regions. Schedule RDS snapshots every 8 hours. Use RDS multi-region replication to update the secondary region's copy of the database. In the event of a failure, restore from the latest snapshot, and use an Amazon Route 53 DNS failover policy to automatically redirect customers to the ALB in the secondary region.
- B. Store the Docker image in ECR in two regions. Schedule RDS snapshots every 8 hours with snapshots copied to the secondary region. In the event of a failure, use AWS CloudFormation to deploy the ALB, EC2, ECS and RDS resources in the secondary region, restore from the latest snapshot, and update the DNS record to point to the ALB in the secondary region.
- C. Use AWS CloudFormation to deploy identical ALB, EC2, ECS, and RDS resources in a secondary region. Schedule hourly RDS MySQL backups to Amazon S3 and use cross-region replication to replicate data to a bucket in the secondary region. In the event of a failure, import the latest Docker image to Amazon ECR in the secondary region, deploy to the EC2 instance, restore the latest MySQL backup, and update the DNS record to point to the ALB in the secondary region.
- D. Deploy a pilot light environment in a secondary region with an ALB and a minimal resource EC2 deployment for Docker in an AWS Auto Scaling group with a scaling policy to increase instance size and number of nodes. Create a cross-region read replica of the RDS data. In the event of a failure, promote the replica to primary, and update the DNS record to point to the ALB in the secondary region.

B

MOST cost-effective → B is cheaper than A

ECR and RDS Snapshots in Two Regions: Storing Docker images in ECR in two regions and copying RDS snapshots to the secondary region is a good strategy. In case of failure, CloudFormation deploys necessary resources in the secondary region, and the DNS is updated. This option is more cost-effective than A, as it doesn't require maintaining a full duplicate environment or multi-region replication constantly.

Question 334:

A company is migrating its infrastructure to the AWS Cloud. The company must comply with a variety of regulatory standards for different projects. The company needs a multi-account environment.

A solutions architect needs to prepare the baseline infrastructure. The solution must provide a consistent baseline of management and security, but it must allow flexibility for different compliance requirements within various AWS accounts. The solution also needs to integrate with the existing on-premises Active Directory Federation Services (AD FS) server.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Create an organization in AWS Organizations. Create a single SCP for least privilege access across all accounts. Create a single OU for all accounts. Configure an IAM identity provider for federation with the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with conformance packs for all accounts.

B. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Add OUs as necessary. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server.

C. Create an organization in AWS Organizations. Create SCPs for least privilege access. Create an OU structure, and use it to group AWS accounts. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with aggregators and conformance packs.

D. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Configure an IAM identity provider for federation with the on-premises AD FS server.

B

AWS Control Tower



- Easy way to set up and govern a secure and compliant multi-account AWS environment based on best practices
- Benefits:
 - Automate the set up of your environment in a few clicks
 - tự động hóa quản lý chính sách liên tục ongoing policy management using guardrails
 - Detect policy violations and remediate them
 - Monitor compliance through an interactive dashboard
- AWS Control Tower runs on top of AWS Organizations:
 - It automatically sets up AWS Organizations to organize accounts and implement SCPs (Service Control Policies)

AWS IAM Identity Center

(successor to AWS Single Sign-On)



- One login (single sign-on) for all your
 - AWS accounts in AWS Organizations
 - Business cloud applications (e.g., Salesforce, Box, Microsoft 365, ...)
 - SAML2.0-enabled applications
 - EC2 Windows Instances
- Identity providers
 - Built-in identity store in IAM Identity Center
 - 3rd party: Active Directory (AD), OneLogin, Okta...



AWS IAM Identity Center



Question 335:

An online magazine will launch its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balancer in front of the web tier, a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only.

The magazine is expecting a significant spike in internet traffic when the new edition is launched. Optimal performance is a top priority for the week following the launch.

Which combination of steps should a solutions architect take to reduce system response times for a global audience? (Choose two.)

- A. Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region. Replace the web servers with Amazon S3. Deploy S3 buckets in cross-Region replication mode.
- B. Ensure the web and application tiers are each in Auto Scaling groups. Introduce an AWS Direct Connect connection. Deploy the web and application tiers in Regions across the world.
- C. Migrate the database from Amazon Aurora to Amazon RDS for MySQL. Ensure all three of the application tiers – web, application, and database – are in private subnets.
- D. Use an Aurora global database for physical cross-Region replication. Use Amazon S3 with cross-Region replication for static content and resources. Deploy the web and application tiers in Regions across the world.
- E. Introduce Amazon Route 53 with latency-based routing and Amazon CloudFront distributions. Ensure the web and application tiers are each in Auto Scaling groups.

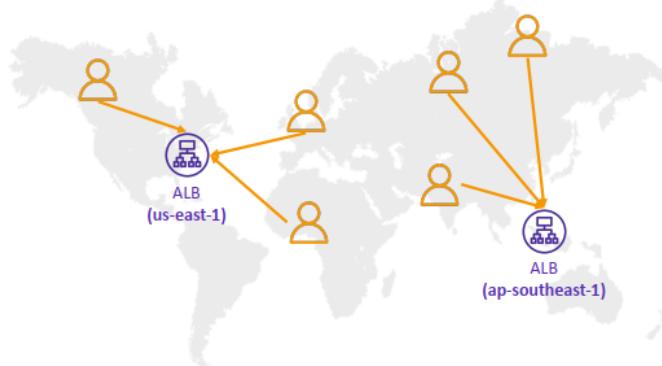
D,E

website include static content → CloudFront and S3.

reduce system response times for a global audience → Route 53 latency-base routing

Routing Policies – Latency-based

- Redirect to the resource that has the least latency close to us
- Super helpful when latency for users is a priority
- Latency is based on traffic between users and AWS Regions
- Germany users may be directed to the US (if that's the lowest latency)
- Can be associated with Health Checks (has a failover capability)



Question 336:

An online gaming company needs to optimize the cost of its workloads on AWS. The company uses a dedicated account to host the production environment for its online gaming application and an analytics application.

Amazon EC2 instances host the gaming application and must always be available. The EC2 instances run all year. The analytics application uses data that is stored in Amazon S3. The analytics application can be interrupted and resumed without issue.

Which solution will meet these requirements MOST cost-effectively?

- Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use On-Demand Instances for the analytics application.
- Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use Spot Instances for the analytics application.
- Use Spot Instances for the online gaming application and the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.
- Use On-Demand Instances for the online gaming application. Use Spot Instances for the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.

B

gaming application and must always be available → Saving Plan
The analytics application can be interrupted and resumed without issue → Spot Instance

EC2 Instance Launch Types

- On Demand Instances: short workload, có thể dự đoán giá, tín cậy
- Spot Instances: short workloads, for cheap, can lose instances (not reliable)
- Reserved: (MINIMUM 1 year)
 - Reserved Instances: long workloads
 - Convertible Reserved Instances: long workloads with flexible instances
- Dedicated Instances: no other customers will share your hardware
- Dedicated Hosts: book an entire physical server; control instance placement
 - Great for software licenses that operate at the core, or socket level
 - Can define host affinity so that instance reboots are kept on the same host

xác định sự liên kết (affinity) giữa instance và host, đảm bảo rằng khi instance khởi động lại, nó sẽ được giữ trên cùng một host. Điều này có ý nghĩa là các instance sẽ được gắn kết với một máy chủ cụ thể và không bị di chuyển sang máy chủ khác trong quá trình khởi động lại.



AWS Savings Plan

- New pricing model to get a discount based on long-term usage
- Cam kết sử dụng Trajai
- Commit to a certain type of usage: ex \$10 per hour for 1 to 3 years
- Any usage beyond the savings plan is billed at the on-demand price
- EC2 Instance Savings plan (up to 72% - same discount as Standard RIs)
 - Select instance family (e.g. M5, C5...), and locked to a specific region
 - Flexible across size (m5.large to m5.4xlarge), OS (Windows to Linux), thuê (tenancy) (dedicated or default)
- Compute Savings plan (up to 66% - same discount as Convertible RIs)
 - Ability to move between instance family (move from C5 to M5), region (Ireland to US), compute type (EC2, Fargate, Lambda), OS & tenancy
- SageMaker Savings plan (up to 64% off)

Question 337:

A company runs applications in hundreds of production AWS accounts. The company uses AWS Organizations with all features enabled and has a centralized backup operation that uses AWS Backup.

The company is concerned about ransomware attacks. To address this concern, the company has created a new policy that all backups must be resilient to breaches of privileged-user credentials in any production account.

Which combination of steps will meet this new requirement? (Choose three.)

- Implement cross-account backup with AWS Backup vaults in designated non-production accounts.
- Add an SCP that restricts the modification of AWS Backup vaults.
- Implement AWS Backup Vault Lock in compliance mode.
- Implement least privilege access for the IAM service role that is assigned to AWS Backup.
- Configure the backup frequency, lifecycle, and retention period to ensure that at least one backup always exists in the cold tier.

F. Configure AWS Backup to write all backups to an Amazon S3 bucket in a designated non-production account. Ensure that the S3 bucket has S3 Object Lock enabled.

A, B, C

A <https://docs.aws.amazon.com/aws-backup/latest/devguide/manage-cross-account.html>

If you set up AWS Organizations, you can configure AWS Backup to monitor activities in all of your accounts in one place. You can also create a backup policy and apply it to selected accounts that are part of your organization and view the aggregate backup job activities directly from the AWS Backup console.

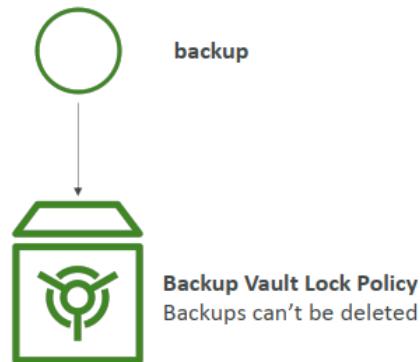
B LAB: <https://aws.amazon.com/blogs/storage/managing-access-to-backups-using-service-control-policies-with-aws-backup/>

C. <https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>

- Vaults locked in governance mode can have the lock removed by users with sufficient IAM permissions.
- Vaults locked in compliance mode cannot be deleted once the cooling-off period ("grace time") expires if any recovery points are in the vault. During grace time, you can still remove the vault lock and change the lock configuration.

AWS Backup Vault Lock

- Enforce a WORM (Write Once Read Many) state for all the backups that you store in your AWS Backup Vault
- Additional layer of defense to protect your backups against:
 - Inadvertent or malicious delete operations
 - Updates that shorten or alter retention periods
- Even the root user cannot delete backups when enabled



Question 338:

A company needs to aggregate Amazon CloudWatch logs from its AWS accounts into one central logging account. The collected logs must remain in the AWS Region of creation. The central logging account will then process the logs, normalize the logs into standard output format, and stream the output logs to a security tool for more processing.

A solutions architect must design a solution that can handle a large volume of logging data that needs to be ingested. Less logging will occur outside normal business hours than during normal business hours. The logging solution must scale with the anticipated load. The solutions architect has decided to use an AWS Control Tower design to handle the multi-account logging process.

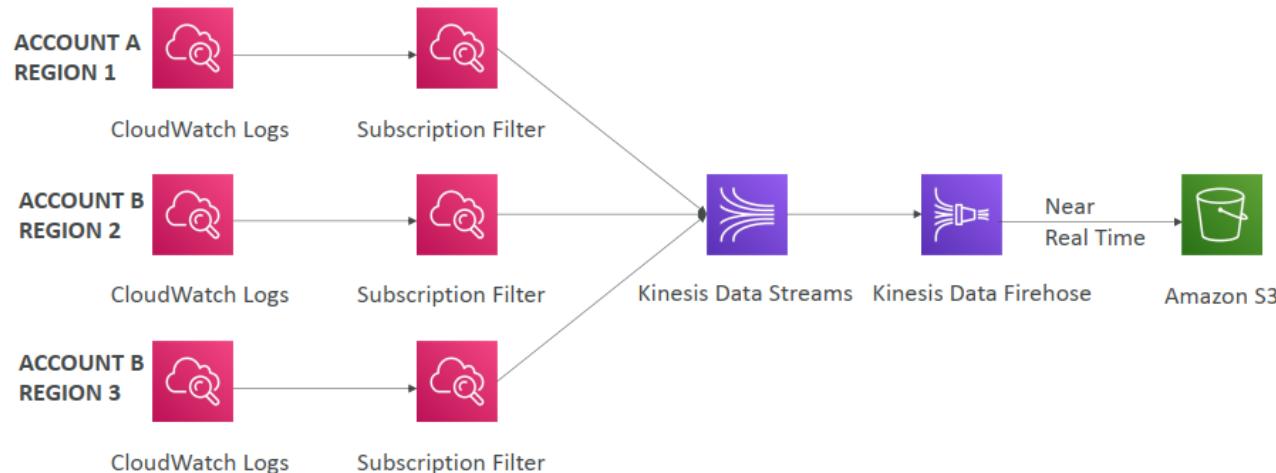
Which combination of steps should the solutions architect take to meet the requirements? (Choose three.)

A. Create a destination Amazon Kinesis data stream in the central logging account.

- B. Create a destination Amazon Simple Queue Service (Amazon SQS) queue in the central logging account.
- C. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Kinesis data stream. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a subscription filter for each log group to send data to the Kinesis data stream.
- D. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Simple Queue Service (Amazon SQS) queue. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a single subscription filter for all log groups to send data to the SQS queue.
- E. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the central logging account and to write the logs to the security tool.
- F. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the member accounts and to write the logs to the security tool.

A,C,E

CloudWatch Logs Aggregation Multi-Account & Multi Region



Question 339:

A company is migrating a legacy application from an on-premises data center to AWS. The application consists of a single application server and a Microsoft SQL Server database server. Each server is deployed on a VMware VM that consumes 500 TB of data across multiple attached volumes.

The company has established a 10 Gbps AWS Direct Connect connection from the closest AWS Region to its on-premises data center. The Direct Connect connection is not currently in use by other services.

Which combination of steps should a solutions architect take to migrate the application with the LEAST amount of downtime? (Choose two.)

HANCHE

- A. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the database server VM to AWS.
- B. Use VM Import/Export to import the application server VM.
- C. Export the VM images to an AWS Snowball Edge Storage Optimized device.
- D. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the application server VM to AWS.
- E. Use an AWS Database Migration Service (AWS DMS) replication instance to migrate the database to an Amazon RDS DB instance.

A,D

RDS SQL maximum storage is 16TB. So we need to move the VM
<https://trello.com/c/RPrz09rg/407-aws-server-migration-service>
<https://trello.com/c/JMswvmaz/408-aws-sms-vs-aws-dms>

Question 340:

A company operates a fleet of servers on premises and operates a fleet of Amazon EC2 instances in its organization in AWS Organizations. The company's AWS accounts contain hundreds of VPCs. The company wants to connect its AWS accounts to its on-premises network. AWS Site-to-Site VPN connections are already established to a single AWS account. The company wants to control which VPCs can communicate with other VPCs.

Which combination of steps will achieve this level of control with the LEAST operational effort? (Choose three.)

- A. Create a transit gateway in an AWS account. Share the transit gateway across accounts by using AWS Resource Access Manager (AWS RAM).
- B. Configure attachments to all VPCs and VPNs.
- C. Setup transit gateway route tables. Associate the VPCs and VPNs with the route tables.
- D. Configure VPC peering between the VPCs.
- E. Configure attachments between the VPCs and VPNs.
- F. Setup route tables on the VPCs and VPNs.

A,B,C

LEAST operational effort → C is incorrect

<https://trello.com/c/V2nfUM9T/409-aws-transit-gateway-vpn-site-to-sit>

Question 341:

A company needs to optimize the cost of its application on AWS. The application uses AWS Lambda functions and Amazon Elastic Container Service (Amazon ECS) containers that run on AWS Fargate. The application is write-heavy and stores data in an Amazon Aurora MySQL database.

The load on the application is not consistent. The application experiences long periods of no usage, followed by sudden and significant increases and decreases in traffic. The database runs on a memory optimized DB instance that cannot handle the load.

A solutions architect must design a solution that can scale to handle the changes in traffic.

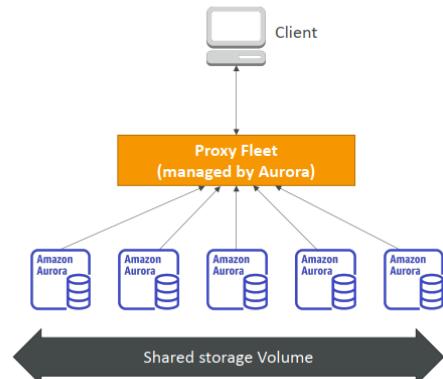
Which solution will meet these requirements MOST cost-effectively?

- A. Add additional read replicas to the database. Purchase Instance Savings Plans and RDS Reserved Instances.
- B. Migrate the database to an Aurora DB cluster that has multiple writer instances. Purchase Instance Savings Plans.
- C. Migrate the database to an Aurora global database. Purchase Compute Savings Plans and RDS Reserved instances.
- D. Migrate the database to Aurora Serverless v1. Purchase Compute Savings Plans.

D
followed by sudden and significant increases and decreases in traffic → Aurora serverless
MOST cost-effectively → Savings Plans

Aurora Serverless

- Automated database instantiation and auto-scaling based on actual usage
- Good for infrequent, intermittent or unpredictable workloads
- No capacity planning needed
- Pay per second, can be more cost-effective



AWS Savings Plan



- New pricing model to get a discount based on long-term usage
Cam kết sử dụng 1 loại
- Commit to a certain type of usage: ex \$10 per hour for 1 to 3 years
- Any usage beyond the savings plan is billed at the on-demand price
- EC2 Instance Savings plan (up to 72% - same discount as Standard RIs)
 - Select instance family (e.g. M5, C5...), and locked to a specific region
 - Flexible across size (m5.large to m5.4xlarge), OS (Windows to Linux), thuê tenancy (dedicated or default)
- Compute Savings plan (up to 66% - same discount as Convertible RIs)
 - Ability to move between instance family (move from C5 to M5), region (Ireland to US), compute type (**EC2, Fargate, Lambda**), OS & tenancy
- SageMaker Savings plan (up to 64% off)

Question 342:

A company migrated an application to the AWS Cloud. The application runs on two Amazon EC2 instances behind an Application Load Balancer (ALB).

Application data is stored in a MySQL database that runs on an additional EC2 instance. The application's use of the database is read-heavy.

The application loads static content from Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. The static content is updated frequently and must be copied to each EBS volume.

The load on the application changes throughout the day. During peak hours, the application cannot handle all the incoming requests. Trace data shows that the database cannot handle the read load during peak hours.

Which solution will improve the reliability of the application?

- Migrate the application to a set of AWS Lambda functions. Set the Lambda functions as targets for the ALB. Create a new single EBS volume for the static content. Configure the Lambda functions to read from the new EBS volume. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.
- Migrate the application to a set of AWS Step Functions state machines. Set the state machines as targets for the ALB. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Configure the state machines to read from the EFS file system. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.
- Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create a new single EBS volume for the static content. Mount the new EBS volume on the ECS cluster. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.

D. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Mount the EFS file system to each container. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.

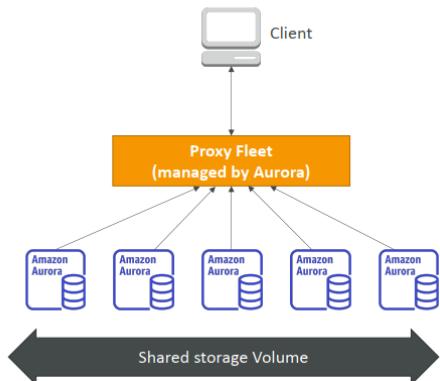
D

During peak hours, the application cannot handle all the incoming requests → ECS + ASG

The application loads static content from Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance → EFS is mounted to each container. the database cannot handle the read load during peak hours → Aurora Serverless

Aurora Serverless

- Automated database instantiation and auto-scaling based on actual usage
- Good for infrequent, intermittent or unpredictable workloads
- No capacity planning needed
- Pay per second, can be more cost-effective



Question 343:

A solutions architect wants to make sure that only AWS users or roles with suitable permissions can access a new Amazon API Gateway endpoint. The solutions architect wants an end-to-end view of each request to analyze the latency of the request and create service maps.

How can the solutions architect design the API Gateway access control and perform request inspections?

- For the API Gateway method, set the authorization to AWS_IAM. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Enable the API caller to sign requests with AWS Signature when accessing the endpoint. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- For the API Gateway resource, set CORS to enabled and only return the company's domain in Access-Control-Allow-Origin headers. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.
- Create an AWS Lambda function as the custom authorizer, ask the API client to pass the key and secret when making the call, and then use Lambda to validate the key/secret pair against the IAM system. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- Create a client certificate for API Gateway. Distribute the certificate to the AWS users and roles that need to access the endpoint. Enable the API caller to pass the client certificate when accessing the endpoint. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

A

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-control-access-using-iam-policies-to-invoke-api.html#api-gateway-who-can-invoke-an-api-method-using-iam-policies>

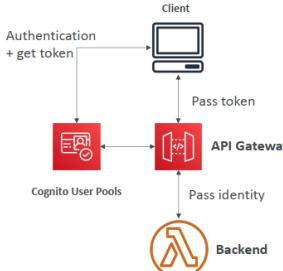
wants an end-to-end view of each request to analyze the latency of the request and create service maps → X-ray

API Gateway – Logging, Monitoring, Tracing

- CloudWatch Logs:
 - Enable CloudWatch logging at the Stage level (with Log Level – ERROR, INFO)
 - Can log full requests / responses data
 - Can send API Gateway Access Logs (customizable)
 - Can send logs directly into Kinesis Data Firehose (as an alternative to CW logs)
- CloudWatch Metrics:
 - Metrics are by stage, possibility to enable detailed metrics
 - *IntegrationLatency, Latency, CacheHitCount, CacheMissCount*
- X-Ray:
 - Enable tracing to get extra information about requests in API Gateway
 - X-Ray API Gateway + AWS Lambda gives you the full picture

API Gateway – Authentication

- IAM based access (AWS_IAM)
 - Good for providing access within your infrastructure
 - Pass IAM credentials in headers through SigV4
- Lambda Authorizer (formerly Custom Authorizer)
 - Use Lambda to verify a custom OAuth / SAML / 3rd party authentication
- Cognito User Pools
 - Client authenticates with Cognito
 - Client passes the token to API Gateway
 - API Gateway knows out-of-the-box how to verify the token



Question 344:

A company is using AWS CodePipeline for the CI/CD of an application to an Amazon EC2 Auto Scaling group. All AWS resources are defined in AWS CloudFormation templates. The application artifacts are stored in an Amazon S3 bucket and deployed to the Auto Scaling group using instance user data scripts. As the application has become more complex, recent resource changes in the CloudFormation templates have caused unplanned downtime.

How should a solutions architect improve the CI/CD pipeline to reduce the likelihood that changes in the templates will cause downtime?

- Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments. Write test plans for a testing team to run in a non-production environment before approving the change for production.
- Implement automated testing using AWS CodeBuild in a test environment. Use CloudFormation change sets to evaluate changes before deployment. Use AWS CodeDeploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes, if needed.

C. Use plugins for the integrated development environment (IDE) to check the templates for errors, and use the AWS CLI to validate that the templates are correct. Adapt the deployment code to check for error conditions and generate notifications on errors. Deploy to a test environment and run a manual test plan before approving the change for production.

D. Use AWS CodeDeploy and a blue/green deployment pattern with CloudFormation to replace the user data deployment scripts. Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected.

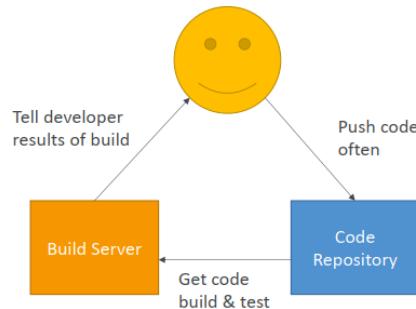
B

improve the CI/CD pipeline to reduce downtime ➔ blue/green

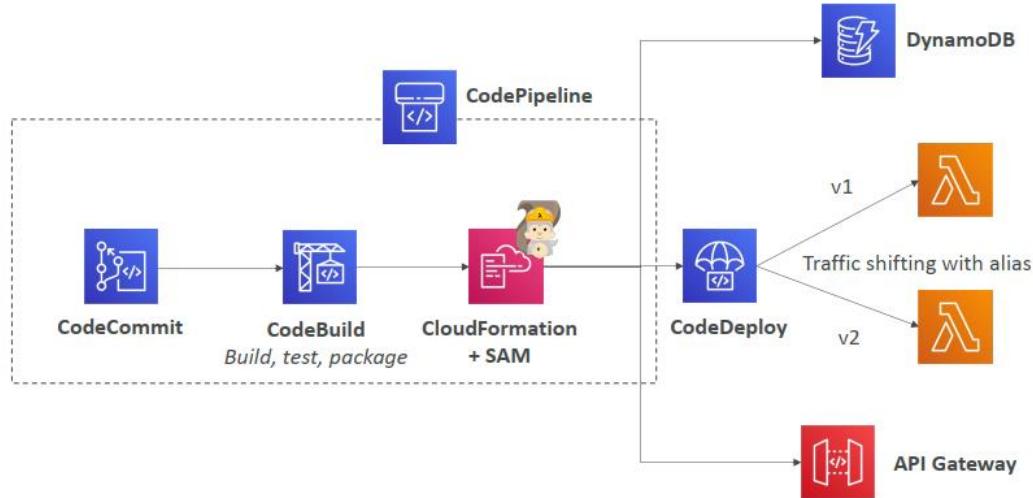
Use Code Build to run unit/automated testing

Continuous Integration

- Developers push the code to a code repository often (GitHub / CodeCommit / Bitbucket / etc...)
- A testing / build server checks the code as soon as it's pushed ([CodeBuild](#) / Jenkins CI / etc...)
- The developer gets feedback about the tests and checks that have passed / failed
- Find bugs early, fix bugs
- Deliver faster as the code is tested
- Deploy often
- Happier developers, as they're unblocked



CICD Architecture for SAM



Question 345:

A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region. The application should dynamically scale to meet user demand and maintain resiliency. Additionally, the application must have disaster recovery capabilities in an active-passive configuration with the us-west-1 Region.

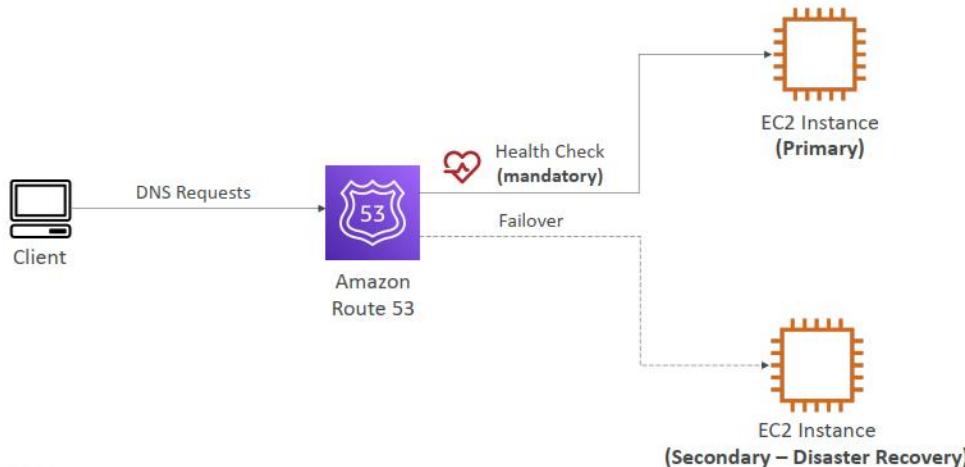
Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

- Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.
- Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions.
- Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) that spans both VPCs. Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB.

D. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.

B
the application must have disaster recovery capabilities in an active-passive configuration → Route 53 failover

Routing Policies – Failover (Active-Passive)



Question 346:

A company has a legacy application that runs on multiple .NET Framework components. The components share the same Microsoft SQL Server database and communicate with each other asynchronously by using Microsoft Message Queueing (MSMQ).

The company is starting a migration to containerized .NET Core components and wants to refactor the application to run on AWS. The .NET Core components require complex orchestration. The company must have full control over networking and host configuration. The application's database model is strongly relational.

Which solution will meet these requirements?

- Host the INET Core components on AWS App Runner. Host the database on Amazon RDS for SQL Server. Use Amazon EventBridge for asynchronous messaging.
- Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the AWS Fargate launch type. Host the database on Amazon DynamoDB. Use Amazon Simple Notification Service (Amazon SNS) for asynchronous messaging.
- Host the .NET Core components on AWS Elastic Beanstalk. Host the database on Amazon Aurora PostgreSQL Serverless v2. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) for asynchronous messaging.

D. Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. Host the database on Amazon Aurora MySQL Serverless v2. Use Amazon Simple Queue Service (Amazon SQS) for asynchronous messaging.

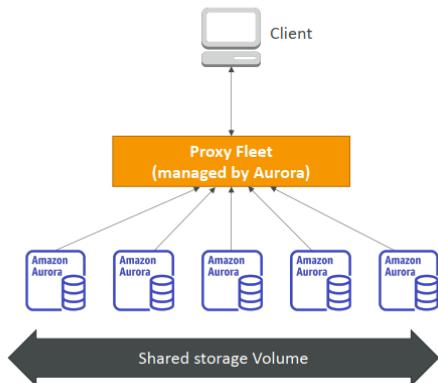
D

The company must have full control over networking and host configuration → ECS

The application's database model is strongly relational → Amazon Aurora MySQL Serverless asynchronously by using Microsoft Message Queueing (MSMQ) → SQS

Aurora Serverless

- Automated database instantiation and auto-scaling based on actual usage
- Good for infrequent, intermittent or unpredictable workloads
- No capacity planning needed
- Pay per second, can be more cost-effective



Question 347:

A solutions architect has launched multiple Amazon EC2 instances in a placement group within a single Availability Zone. Because of additional load on the system, the solutions architect attempts to add new instances to the placement group. However, the solutions architect receives an insufficient capacity error.

What should the solutions architect do to troubleshoot this issue?

- Use a spread placement group. Set a minimum of eight instances for each Availability Zone.
- Stop and start all the instances in the placement group. Try the launch again.
- Create a new placement group. Merge the new placement group with the original placement group.
- Launch the additional instances as Dedicated Hosts in the placement groups.

B

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

EC2 - Placement Groups

- Control the EC2 Instance placement strategy using placement groups
- Group Strategies:
 - *Cluster*—clusters instances into a low-latency group in a single Availability Zone
 - *Spread*—spreads instances across underlying hardware (max 7 instances per group per AZ) – critical applications
 - *Partition*—spreads instances across many different partitions (which rely on different sets of racks) within an AZ. Scales to 100s of EC2 instances per group (Hadoop, Cassandra, Kafka)
- You can move an instance into or out of a placement group
 - You first need to stop it
 - You then need to use the CLI (modify-instance-placement)
 - You can then start your instance

If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error. If you stop an instance in a placement group and then start it again, it still runs in the placement group. However, the start fails if there isn't enough capacity for the instance. If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Starting the instances may migrate them to hardware that has capacity for all of the requested instances.

Question 348:

A company has used infrastructure as code (IaC) to provision a set of two Amazon EC2 instances. The instances have remained the same for several years.

The company's business has grown rapidly in the past few months. In response, the company's operations team has implemented an Auto Scaling group to manage the sudden increases in traffic. Company policy requires a monthly installation of security updates on all operating systems that are running.

The most recent security update required a reboot. As a result, the Auto Scaling group terminated the instances and replaced them with new, unpatched instances.

Which combination of steps should a solutions architect recommend to avoid a recurrence of this issue? (Choose two.)

- A. Modify the Auto Scaling group by setting the Update policy to target the oldest launch configuration for replacement.
- B. Create a new Auto Scaling group before the next patch maintenance. During the maintenance window, patch both groups and reboot the instances.
- C. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure monitoring to ensure that target group health checks return healthy after the Auto Scaling group replaces the terminated instances.
- D. Create automation scripts to patch an AMI, update the launch configuration, and invoke an Auto Scaling instance refresh.
- E. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure termination protection on the instances.

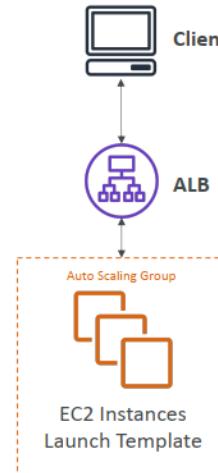
C,D

A incorrect: default oldest launchconfiguration will be terminated first

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-termination-policies.html>

- B. Incorrect: No need to create a new ASG
- C. Correct: Need a loadbalancer to make sure the request route to the healthy instance.
- D. Correct: Script to update OS patch, Lambda to update a launch configuration and trigger Autoscaling Instance refresh
- E. Incorrect: Termination protection is not help.

Auto Scaling – Updating an application



Question 349:

A team of data scientists is using Amazon SageMaker instances and SageMaker APIs to train machine learning (ML) models. The SageMaker instances are deployed in a VPC that does not have access to or from the internet. Datasets for ML model training are stored in an Amazon S3 bucket. Interface VPC endpoints provide access to Amazon S3 and the SageMaker APIs.

Occasionally, the data scientists require access to the Python Package Index (PyPI) repository to update Python packages that they use as part of their workflow. A solutions architect must provide access to the PyPI repository while ensuring that the SageMaker instances remain isolated from the internet.

Which solution will meet these requirements?

- A. Create an AWS CodeCommit repository for each package that the data scientists need to access. Configure code synchronization between the PyPI repository and the CodeCommit repository. Create a VPC endpoint for CodeCommit.
- B. Create a NAT gateway in the VPC. Configure VPC routes to allow access to the internet with a network ACL that allows access to only the PyPI repository endpoint.

C. Create a NAT instance in the VPC and configure VPC routes to allow access to the internet. Configure SageMaker notebook instance firewall rules that allow access to only the PyPI repository endpoint.

D. Create an AWS CodeArtifact domain and repository. Add an external connection for public:pypi to the CodeArtifact repository. Configure the Python client to use the CodeArtifact repository. Create a VPC endpoint for CodeArtifact.

D

LAB: <https://aws.amazon.com/blogs/machine-learning/private-package-installation-in-amazon-sagemaker-running-in-internet-free-mode/>

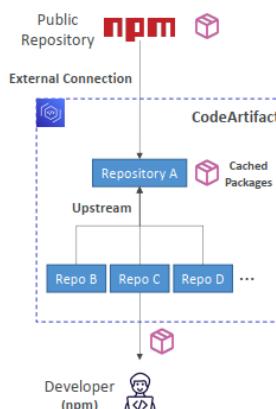
AWS CodeArtifact



- Software packages depend on each other to be built (also called code dependencies), and new ones are created
- Storing and retrieving these dependencies is called **artifact management**
- Traditionally you need to setup your own artifact management system
- CodeArtifact is a secure, scalable, and cost-effective **artifact management** for software development
- Works with common dependency management tools such as Maven, Gradle, npm, yarn, twine, pip, and NuGet
- Developers and CodeBuild can then retrieve dependencies straight from CodeArtifact

CodeArtifact – External Connection

- An External Connection is a connection between a CodeArtifact Repository and an external/public repository (e.g., Maven, npm, PyPI, NuGet...)
- Allows you to fetch packages that are not already present in your CodeArtifact Repository
- A repository has a maximum of 1 external connection
- Create many repositories for many external connections
- Example – Connect to npmj.com
 - Configure one CodeArtifact Repository in your domain with an external connection to npmj.com
 - Configure all the other repositories with an upstream to it
 - Packages fetched from npmj.com are cached in the Upstream Repository, rather than fetching and storing them in each Repository



Question 350:

A solutions architect works for a government agency that has strict disaster recovery requirements. All Amazon Elastic Block Store (Amazon EBS) snapshots are required to be saved in at least two additional AWS Regions. The agency also is required to maintain the lowest possible operational overhead.

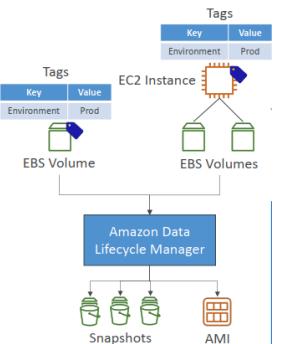
Which solution meets these requirements?

- Configure a policy in Amazon Data Lifecycle Manager (Amazon DLM) to run once daily to copy the EBS snapshots to the additional Regions.
- Use Amazon EventBridge to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.
- Setup AWS Backup to create the EBS snapshots. Configure Amazon S3 Cross-Region Replication to copy the EBS snapshots to the additional Regions.
- Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions.

A

Amazon Data Lifecycle Manager

- Automate the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs
- Schedule backups, cross-account snapshot copies, delete outdated backups, ...
- Uses resource tags to identify the resources (EC2 instances, EBS volumes)
- Can't be used to manage snapshots/AMIs created outside DLM
- Can't be used to manage instance-store backed AMIs



Stephanie Maarek

Amazon Data Lifecycle Manager vs. AWS Backup

- Use Data Lifecycle Manager
 - when you want to automate the creation, retention, and deletion of EBS Snapshots
- Use AWS Backup
 - to manage and monitor backups across the AWS services you use, including EBS volumes, from a single place



Question 351:

A company has a project that is launching Amazon EC2 instances that are larger than required. The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT. The company wants to allow only the launch of t3.small EC2 instances by developers in the project's account. These EC2 instances must be restricted to the us-east-2 Region.

What should a solutions architect do to meet these requirements?

- A. Create a new developer account. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company's organization in AWS Organizations. Enforce a tagging policy that denotes Region affinity.
- B. Create an SCP that denies the launch of all EC2 instances except t3.small EC2 instances in us-east-2. Attach the SCP to the project's account.
- C. Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.
- D. Create an IAM policy that allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the project's account.

D

SCP can be applied only to those users and roles which are managed by accounts that are part of any organization

Service Control Policies (SCP)

- Define allowlist or blocklist IAM actions
- Applied at the OU or Account level
- Does not apply to the Management Account
- SCP is applied to all the Users and Roles in the account, including Root user
- The SCP does not affect Service-linked roles
 - Service-linked roles enable other AWS services to integrate with AWS Organizations and can't be restricted by SCPs.
- SCP must have an explicit Allow (does not allow anything by default)
 - Use cases:
 - Restrict access to certain services (for example: can't use EMR)
 - Enforce PCI compliance by explicitly disabling services

Question 352:

A scientific company needs to process text and image data from an Amazon S3 bucket. The data is collected from several radar stations during a live, time-critical phase of a deep space mission. The radar stations upload the data to the source S3 bucket. The data is prefixed by radar station identification number.

The company created a destination S3 bucket in a second account. Data must be copied from the source S3 bucket to the destination S3 bucket to meet a compliance objective. This replication occurs through the use of an S3 replication rule to cover all objects in the source S3 bucket.

One specific radar station is identified as having the most accurate data. Data replication at this radar station must be monitored for completion within 30 minutes after the radar station uploads the objects to the source S3 bucket.

What should a solutions architect do to meet these requirements?

- A. Setup an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket. Select to use all available bandwidth on the task, and monitor the task to ensure that it is in the TRANSFERRING status. Create an Amazon EventBridge rule to initiate an alert if this status changes.
- B. In the second account, create another S3 bucket to receive data from the radar station with the most accurate data. Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations. Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.
- C. Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint. Monitor the S3 destination bucket's TotalRequestLatency metric. Create an Amazon EventBridge rule to initiate an alert if this status changes.
- D. Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data. Enable S3 Replication Time Control (S3 RTC). Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.

D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-time-control.html>

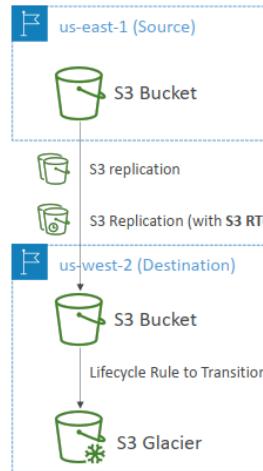
S3 – Replication (Versioning enabled)



- Cross Region Replication (CRR)
- Same Region Replication (SRR)
- Combine with Lifecycle Rules

- Helpful to reduce latency, disaster recovery, security

- S3 Replication Time Control (S3 RTC)
 - Replicates most objects that you upload to Amazon S3 in seconds, and 99.99% of those objects within 15 minutes
 - Helpful for compliance, DR, etc..



Question 353:

A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP applications with MySQL, and Oracle databases. There are many dependent services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration.

Which tools or services should the solutions architect use to plan the cloud migration? (Choose three.)

- A. AWS Application Discovery Service
- B. AWS SMS
- C. AWS X-Ray
- D. AWS Cloud Adoption Readiness Tool (CART)
- E. Amazon Inspector
- F. AWS Migration Hub

A,D,F

AWS Application Discovery Service

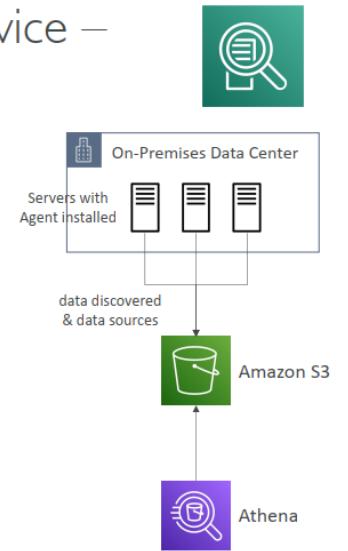


- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping are important for migrations
- **Agentless Discovery (AWS Agentless Discovery Connector)**
 - Open Virtual Appliance (OVA) package that can be deployed to a VMware host
 - VM inventory, configuration, and performance history such as CPU, memory, and disk usage
 - OS agnostic
- **Agent-based Discovery (AWS Application Discovery Agent)**
 - System configuration, system performance, running processes, and details of the network connections between systems
 - Supports Microsoft Server, Amazon Linux, Ubuntu, RedHat, CentOS, SUSE...
- Resulting data can be exported as CSV or viewed within AWS Migration Hub
- Data can be explored using pre-defined queries in Amazon Athena

AWS Application Discovery Service – Migration Hub Data Exploration



- Allows you to use Amazon Athena to analyze data collected from on-premises servers during discovery
- Data is automatically stored in S3 bucket at regular intervals
- Use Pre-defined or custom queries in Amazon Athena to analyze data
- Example: type of processes running on each server
- Ability to upload additional data sources such as Configuration Management Database (CMDB) exports
- Integrate Athena with QuickSight to visualize data



AWS Cloud Adoption Readiness Tool (CART)

- Helps organizations develop efficient and effective plans for cloud adoption and migrations
- Transforms your idea of moving to the cloud into a detailed plan that follows AWS best practices
- Answer a set of questions across six perspectives (business, people, process, platform, operations, security)
- Generates a custom report on your level of migration readiness



<https://trello.com/c/JbEqZl31/411-aws-application-discovery-service-migration-hub-data-exploration>

Question 354:

A solutions architect is reviewing an application's resilience before launch. The application runs on an Amazon EC2 instance that is deployed in a private subnet of a VPC. The EC2 instance is provisioned by an Auto Scaling group that has a minimum capacity of 1 and a maximum capacity of 1. The application stores data on an Amazon RDS for MySQL DB instance. The VPC has subnets configured in three Availability Zones and is configured with a single NAT gateway.

The solutions architect needs to recommend a solution to ensure that the application will operate across multiple Availability Zones.

Which solution will meet this requirement?

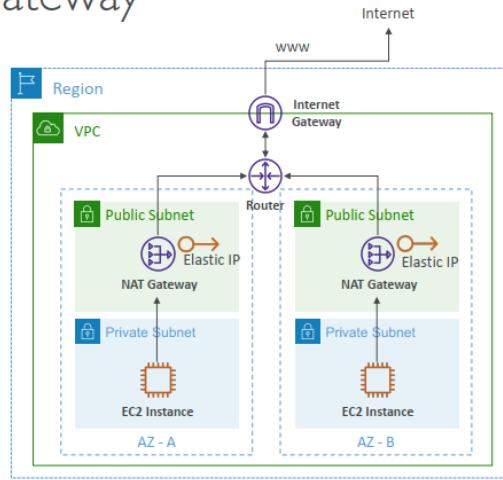
- Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to a Multi-AZ configuration. Configure the Auto Scaling group to launch the instances across Availability Zones. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.
- Replace the NAT gateway with a virtual private gateway. Replace the RDS for MySQL DB instance with an Amazon Aurora MySQL DB cluster. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.
- Replace the NAT gateway with a NAT instance. Migrate the RDS for MySQL DB instance to an RDS for PostgreSQL DB instance. Launch a new EC2 instance in the other Availability Zones.
- Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to turn on automatic backups and retain the backups for 7 days. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Keep the minimum capacity and the maximum capacity of the Auto Scaling group at 1.

A

multiple Availability Zones → NAT Gateway, RDS multi AZ, ASG across AZ

VPC Basics – NAT Gateway

- Managed NAT solution, bandwidth scales automatically
- Resilient to failure within a single AZ
- Must deploy multiple NAT Gateways in multiple AZ for HA
- Has an Elastic IP, external services see the IP of the NAT Gateway as the source



Question 355:

A company is planning to migrate its on-premises transaction-processing application to AWS. The application runs inside Docker containers that are hosted on VMs in the company's data center. The Docker containers have shared storage where the application records transaction data.

The transactions are time sensitive. The volume of transactions inside the application is unpredictable. The company must implement a low-latency storage solution that will automatically scale throughput to meet increased demand. The company cannot develop the application further and cannot continue to administer the Docker hosting environment.

How should the company migrate the application to AWS to meet these requirements?

- Migrate the containers that run the application to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon S3 to store the transaction data that the containers share.
- Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic File System (Amazon EFS) file system. Create a Fargate task definition. Add a volume to the task definition to point to the EFS file system.
- Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic Block Store (Amazon EBS) volume. Create a Fargate task definition. Attach the EBS volume to each running task.
- Launch Amazon EC2 instances. Install Docker on the EC2 instances. Migrate the containers to the EC2 instances. Create an Amazon Elastic File System (Amazon EFS) file system. Add a mount point to the EC2 instances for the EFS file system.

B

The application runs inside Docker containers → ECS or EKS

The Docker containers have shared storage where the application records transaction data → EFS → B is correct

Amazon ECS – Use cases

- Run Microservices
 - Run multiple Docker containers on the same machine
 - Easy Service Discovery features to enhance communication
 - Direct integration with Application Load Balancer and Network Load Balancer
 - Auto Scaling capability
- Run Batch Processing / Scheduled Tasks
 - Schedule ECS tasks to run on On-demand / Reserved / Spot instances
- Migrate Applications to the Cloud
 - Dockerize legacy applications running on-premises
 - Move Docker containers to run on Amazon ECS

Question 356:

A company is planning to migrate to the AWS Cloud. The company hosts many applications on Windows servers and Linux servers. Some of the servers are physical, and some of the servers are virtual. The company uses several types of databases in its on-premises environment. The company does not have an accurate inventory of its on-premises servers and applications.

The company wants to rightsize its resources during migration. A solutions architect needs to obtain information about the network connections and the application relationships. The solutions architect must assess the company's current environment and develop a migration plan.

Which solution will provide the solutions architect with the required information to develop the migration plan?

- A. Use Migration Evaluator to request an evaluation of the environment from AWS. Use the AWS Application Discovery Service Agentless Collector to import the details into a Migration Evaluator Quick Insights report.
- B. Use AWS Migration Hub and install the AWS Application Discovery Agent on the servers. Deploy the Migration Hub Strategy Recommendations application data collector. Generate a report by using Migration Hub Strategy Recommendations.
- C. Use AWS Migration Hub and run the AWS Application Discovery Service Agentless Collector on the servers. Group the servers and databases by using AWS Application Migration Service. Generate a report by using Migration Hub Strategy Recommendations.

D. Use the AWS Migration Hub import tool to load the details of the company's on-premises environment. Generate a report by using Migration Hub Strategy Recommendations.

B

needs to obtain information about the network connections and the application relationships → AWS Application Discovery Agent

AWS Application Discovery Service



- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping are important for migrations
- **Agentless Discovery (AWS Agentless Discovery Connector)**
 - Open Virtual Appliance (OVA) package that can be deployed to a VMware host
 - VM inventory, configuration, and performance history such as CPU, memory, and disk usage
 - OS agnostic
- **Agent-based Discovery (AWS Application Discovery Agent)**
 - System configuration, system performance, running processes, and details of the network connections between systems
 - Supports Microsoft Server, Amazon Linux, Ubuntu, RedHat, CentOS, SUSE...
- Resulting data can be exported as CSV or viewed within AWS Migration Hub
- Data can be explored using pre-defined queries in Amazon Athena

Question 357:

A financial services company sells its software-as-a-service (SaaS) platform for application compliance to large global banks. The SaaS platform runs on AWS and uses multiple AWS accounts that are managed in an organization in AWS Organizations. The SaaS platform uses many AWS resources globally.

For regulatory compliance, all API calls to AWS resources must be audited, tracked for changes, and stored in a durable and secure data store.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new AWS CloudTrail trail. Use an existing Amazon S3 bucket in the organization's management account to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 bucket.
- B. Create a new AWS CloudTrail trail in each member account of the organization. Create new Amazon S3 buckets to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 buckets.
- C. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket with versioning turned on to store the logs. Deploy the trail for all accounts in the organization. Enable MFA delete and encryption on the S3 bucket.

D. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket to store the logs. Configure Amazon Simple Notification Service (Amazon SNS) to send log-file delivery notifications to an external management system that will track the logs. Enable MFA delete and encryption on the S3 bucket.

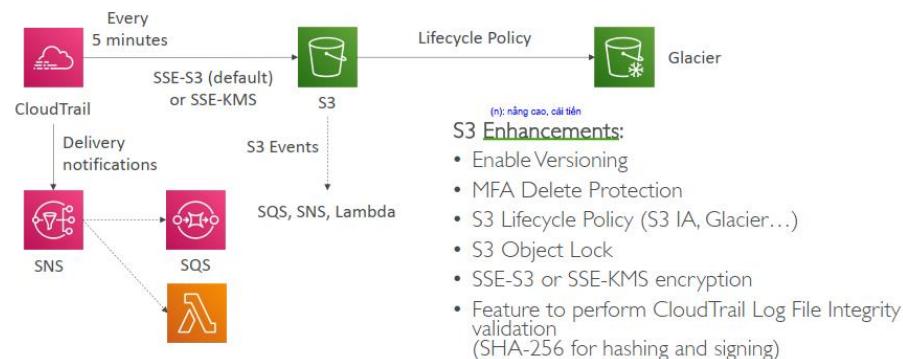
C
tracked for changes → AWS CloudTrail trail, Amazon S3 bucket with versioning turned on to store the logs stored in a durable and secure data store → Enable MFA delete and encryption on the S3 bucket

AWS CloudTrail



- Provides governance, compliance and audit for your AWS Account
- CloudTrail is enabled by default!
- Get an history of events / API calls made within your AWS Account by:
 - Console
 - SDK
 - CLI
 - AWS Services
- Can put logs from CloudTrail into CloudWatch Logs or S3
- A trail can be applied to All Regions (default) or a single Region.
- If a resource is deleted in AWS, investigate CloudTrail first!

CloudTrail – Solution Architecture: Delivery to S3



S3 Enhancements:

- Enable Versioning
- MFA Delete Protection
- S3 Lifecycle Policy (S3 IA, Glacier...)
- S3 Object Lock
- SSE-S3 or SSE-KMS encryption
- Feature to perform CloudTrail Log File Integrity validation (SHA-256 for hashing and signing)

Question 358:

A company is deploying a distributed in-memory database on a fleet of Amazon EC2 instances. The fleet consists of a primary node and eight worker nodes. The primary node is responsible for monitoring cluster health, accepting user requests, distributing user requests to worker nodes, and sending an aggregate response back to a client. Worker nodes communicate with each other to replicate data partitions.

The company requires the lowest possible networking latency to achieve maximum performance.

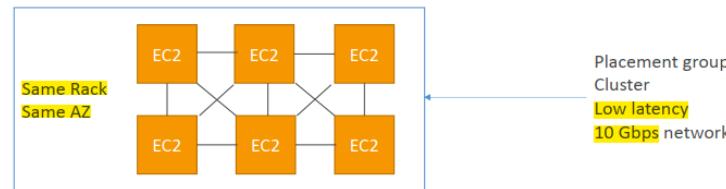
Which solution will meet these requirements?

- A. Launch memory optimized EC2 instances in a partition placement group.
- B. Launch compute optimized EC2 instances in a partition placement group.
- C. Launch memory optimized EC2 instances in a cluster placement group.
- D. Launch compute optimized EC2 instances in a spread placement group.

C
requires the lowest possible networking latency to achieve maximum performance → cluster placement group

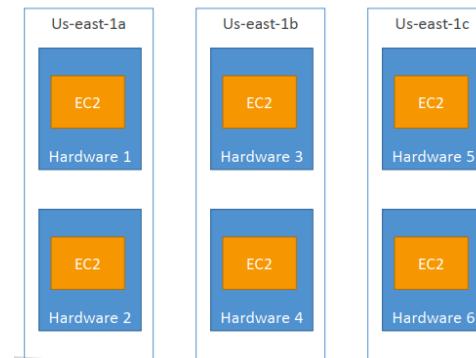
Placement Groups

Cluster



- Pros: Great network (10 Gbps bandwidth between instances with Enhanced Networking enabled - recommended)
- Cons: If the rack fails, all instances fail at the same time
- Use case:
 - Big Data job that needs to complete fast
 - Application that needs extremely low latency and high network throughput

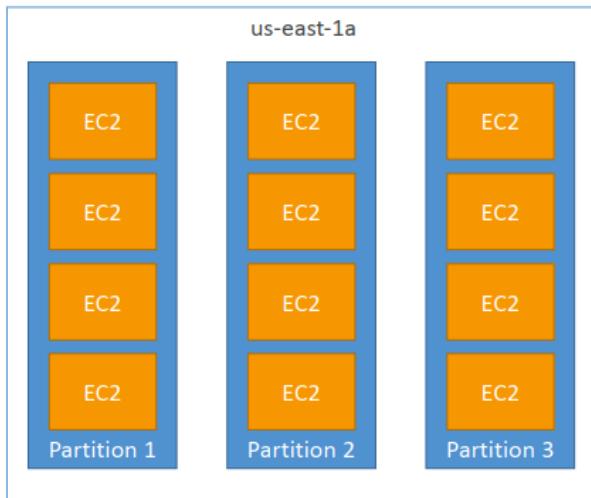
Placement Groups Spread



- Pros:
 - Can span across Availability Zones (AZ)
 - Reduced risk of simultaneous failure
 - EC2 Instances are on different physical hardware
- Cons:
 - Limited to 7 instances per AZ per placement group
- Use case:
 - Application that needs to maximize high availability
 - Critical Applications where each instance must be isolated from failure from each other

Placements Groups

Partition



- Up to 7 partitions per AZ
- Up to 100s of EC2 instances
- The instances in a partition do not share racks with the instances in the other partitions
- A partition failure can affect many EC2 but won't affect other partitions
- EC2 instances get access to the partition information as metadata
- Use cases: HDFS, HBase, Cassandra, Kafka

Question 359:

A company maintains information on premises in approximately 1 million.csv files that are hosted on a VM. The data initially is 10 TB in size and grows at a rate of 1 TB each week. The company needs to automate backups of the data to the AWS Cloud.

Backups of the data must occur daily. The company needs a solution that applies custom filters to back up only a subset of the data that is located in designated source directories. The company has set up an AWS Direct Connect connection.

Which solution will meet the backup requirements with the LEAST operational overhead?

- A. Use the Amazon S3 CopyObject API operation with multipart upload to copy the existing data to Amazon S3. Use the CopyObject API operation to replicate new data to Amazon S3 daily.
- B. Create a backup plan in AWS Backup to back up the data to Amazon S3. Schedule the backup plan to run daily.
- C. Install the AWS DataSync agent as a VM that runs on the on-premises hypervisor. Configure a DataSync task to replicate the data to Amazon S3 daily.
- D. Use an AWS Snowball Edge device for the initial backup. Use AWS DataSync for incremental backups to Amazon S3 daily.

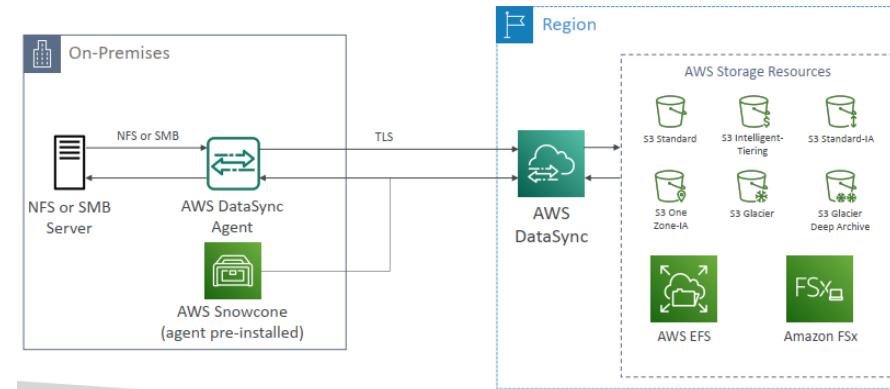
C

LEAST operational overhead, AWS Direct Connect connection ➔ DataSync

AWS DataSync

- Move large amount of data to and from
 - On-premises / other cloud to AWS (NFS, SMB, HDFS, S3 API...) – needs agent
 - AWS to AWS (different storage services) – no agent needed
- Can synchronize to:
 - Amazon S3 (any storage classes – including Glacier)
 - Amazon EFS
 - Amazon FSx (Windows, Lustre, NetApp, OpenZFS...)
- Replication tasks can be scheduled hourly, daily, weekly
- File permissions and metadata are preserved (NFS POSIX, SMB...)
- One agent task can use 10 Gbps, can setup a bandwidth limit

AWS DataSync NFS / SMB to AWS (S3, EFS, FSx...)



Question 360:

A financial services company has an asset management product that thousands of customers use around the world. The customers provide feedback about the product through surveys. The company is building a new analytical solution that runs on Amazon EMR to analyze the data from these surveys. The following user personas need to access the analytical solution to perform different actions:

- Administrator: Provisions the EMR cluster for the analytics team based on the team's requirements
- Data engineer: Runs ETL scripts to process, transform, and enrich the datasets
- Data analyst: Runs SQL and Hive queries on the data

A solutions architect must ensure that all the user personas have least privilege access to only the resources that they need. The user personal must be able to launch only applications that are approved and authorized. The solution also must ensure tagging for all resources that the user personas create.

Which solution will meet these requirements?

- Create IAM roles for each user personal. Attach identity-based policies to define which actions the user who assumes the role can perform. Create an AWS Config rule to check for noncompliant resources. Configure the rule to notify the administrator to remediate the noncompliant resources.
- Setup Kerberos-based authentication for EMR clusters upon launch. Specify a Kerberos security configuration along with cluster-specific Kerberos options.
- Use AWS Service Catalog to control the Amazon EMR versions available for deployment, the cluster configuration, and the permissions for each user personal.
- Launch the EMR cluster by using AWS CloudFormation. Attach resource-based policies to the EMR cluster during cluster creation. Create an AWS Config rule to check for noncompliant clusters and noncompliant Amazon S3 buckets. Configure the rule to notify the administrator to remediate the noncompliant resources.

C

<https://aws.amazon.com/blogs/big-data/build-a-self-service-environment-for-each-line-of-business-using-amazon-emr-and-aws-service-catalog/>

AWS Service Catalog



- Users that are new to AWS have too many options, and may create stacks that are not compliant / in line with the rest of the organization
phần còn lại của tổ chức
- Some users just want a quick **self-service portal** to launch a set of authorized products pre-defined by admins
- Includes: virtual machines, databases, storage options, etc...
- Enter AWS Service Catalog!

Question 361:

A software as a service (SaaS) company uses AWS to host a service that is powered by AWS PrivateLink. The service consists of proprietary software that runs on three Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in private subnets in multiple Availability Zones in the eu-west-2 Region. All the company's customers are in eu-west-2.

However, the company now acquires a new customer in the us-east-1 Region. The company creates a new VPC and new subnets in us-east-1. The company establishes inter-Region VPC peering between the VPCs in the two Regions.

The company wants to give the new customer access to the SaaS service, but the company does not want to immediately deploy new EC2 resources in us-east-1.

Which solution will meet these requirements?

- Configure a PrivateLink endpoint service in us-east-1 to use the existing NLB that is in eu-west-2. Grant specific AWS accounts access to connect to the SaaS service.
- Create an NLB in us-east-1. Create an IP target group that uses the IP addresses of the company's instances in eu-west-2 that host the SaaS service. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

C. Create an Application Load Balancer (ALB) in front of the EC2 instances in eu-west-2. Create an NLB in us-east-1. Associate the NLB that is in us-east-1 with an ALB target group that uses the ALB that is in eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

D. Use AWS Resource Access Manager (AWS RAM) to share the EC2 instances that are in eu-west-2. In us-east-1, create an NLB and an instance target group that includes the shared EC2 instances from eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

<https://www.examtopics.com/discussions/amazon/view/126827-exam-aws-certified-solutions-architect-professional-sap-c02/>

A

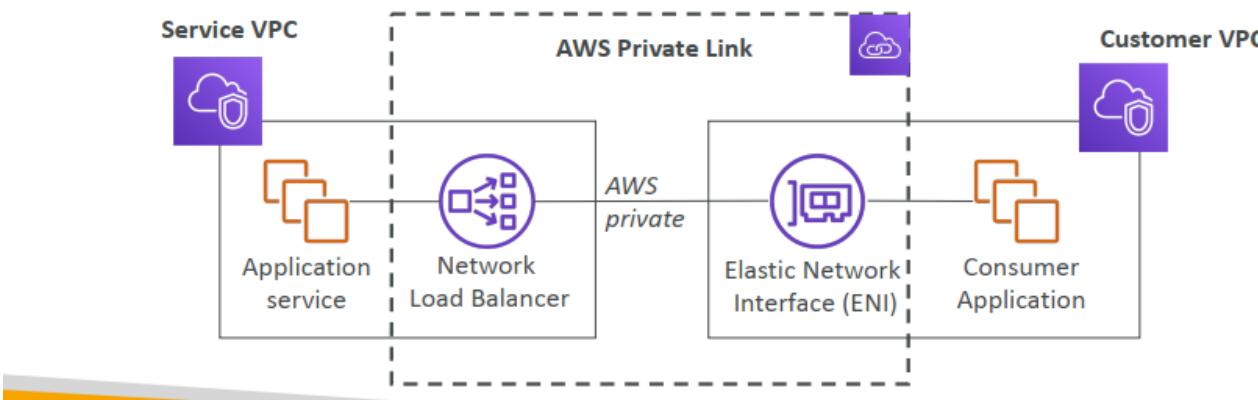
<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-share-your-services.html>

<https://aws.amazon.com/about-aws/whats-new/2018/10/aws-privatelink-now-supports-access-over-inter-region-vpc-peering/>

AWS PrivateLink (VPC Endpoint Services)



- Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts)
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)
- If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!



Question 362:

A company needs to monitor a growing number of Amazon S3 buckets across two AWS Regions. The company also needs to track the percentage of objects that are encrypted in Amazon S3. The company needs a dashboard to display this information for internal compliance teams.

HANCHE

Which solution will meet these requirements with the LEAST operational overhead?

- Create a new 3 Storage Lens dashboard in each Region to track bucket and encryption metrics. Aggregate data from both Region dashboards into a single dashboard in Amazon QuickSight for the compliance teams.
- Deploy an AWS Lambda function in each Region to list the number of buckets and the encryption status of objects. Store this data in Amazon S3. Use Amazon Athena queries to display the data on a custom dashboard in Amazon QuickSight for the compliance teams.
- Use the S3 Storage Lens default dashboard to track bucket and encryption metrics. Give the compliance teams access to the dashboard directly in the S3 console.
- Create an Amazon EventBridge rule to detect AWS CloudTrail events for S3 object creation. Configure the rule to invoke an AWS Lambda function to record encryption metrics in Amazon DynamoDB. Use Amazon QuickSight to display the metrics in a dashboard for the compliance teams.

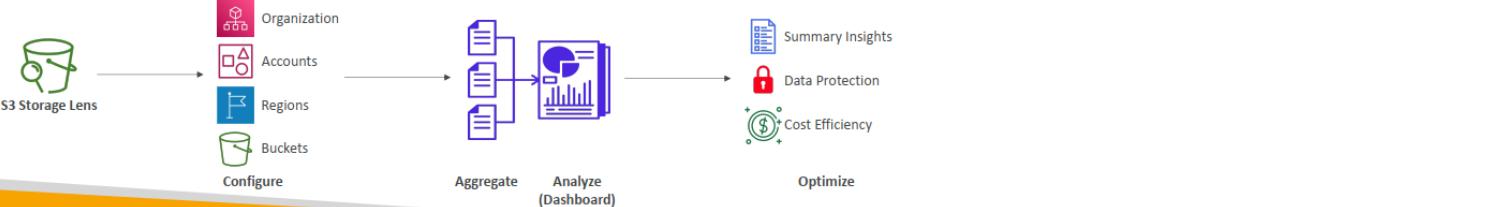
<https://www.examtopics.com/discussions/amazon/view/126828-exam-aws-certified-solutions-architect-professional-sap-c02/>

C
LEAST operational overhead → Use the S3 Storage Lens default dashboard

S3 – Storage Lens



- Understand, analyze, and optimize storage across entire AWS Organization
- Discover anomalies, identify cost efficiencies, and apply data protection best practices across entire AWS Organization (30 days usage & activity metrics)
- Aggregate data for Organization, specific accounts, regions, buckets, or prefixes
- Default dashboard or create your own dashboards
- Can be configured to export metrics daily to an S3 bucket (CSV, Parquet)



Amazon S3 > Storage Lens

Storage Lens Info

Storage Lens provides visibility into storage usage and activity trends at the organization or account level, with drill-downs such as AWS Region, Storage Lens groups, or prefixes.

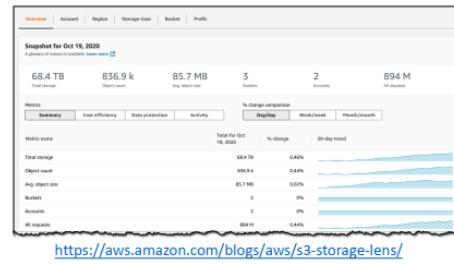
Storage Lens – Default Dashboard



- Visualize summarized insights and trends for both free and advanced metrics
- Default dashboard shows Multi-Region and Multi-Account data
- Preconfigured by Amazon S3
- Can't be deleted, but can be disabled

The screenshot shows the AWS Storage Lens configuration page for a dashboard named "s3-lens-demo". It includes sections for "Regions", "Storage Classes", and "Metrics". Under "Accounts", there are checkboxes for "Select all accounts" and "Exclude accounts". Under "Buckets", there are checkboxes for "Select all buckets" and "Exclude buckets". At the bottom are "Cancel", "Reset", and "Apply" buttons.

<https://aws.amazon.com/blogs/aws/s3-storage-lens/>



Question 363:

A company's CISO has asked a solutions architect to re-engineer the company's current CI/CD practices to make sure patch deployments to its application can happen as quickly as possible with minimal downtime if vulnerabilities are discovered. The company must also be able to quickly roll back a change in case of errors.

The web application is deployed in a fleet of Amazon EC2 instances behind an Application Load Balancer. The company is currently using GitHub to host the application source code, and has configured an AWS CodeBuild project to build the application. The company also intends to use AWS CodePipeline to trigger builds from GitHub commits using the existing CodeBuild project.

What CI/CD configuration meets all of the requirements?

- Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment. Monitor the newly deployed code, and, if there are any issues, push another code update
- Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments. Monitor the newly deployed code, and, if there are any issues, trigger a manual rollback using CodeDeploy
- Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks. Monitor the newly deployed code, and, if there are any issues, push another code update
- Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code, and, if there are any issues, push another code update

B

quickly roll back a change in case of errors ➔ blue/green deployments

Question 364:

A company is managing many AWS accounts by using an organization in AWS Organizations. Different business units in the company run applications on Amazon EC2 instances. All the EC2 instances must have a BusinessUnit tag so that the company can track the cost for each business unit.

A recent audit revealed that some instances were missing this tag. The company manually added the missing tag to the instances.

What should a solutions architect do to enforce the tagging requirement in the future?

A. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned off. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the root of the organization.

B. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned on. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the organization's management account.

C. Create an SCP and attach the SCP to the root of the organization. Include the following statement in the SCP:

```
{  
    "Sid": "DenyEC2Creation",  
    "Effect": "Deny",  
    "Action": [  
        "ec2:RunInstances"  
    ],  
    "Resource": [  
        "arn:aws:ec2:*:*:instance/*"  
    ],  
    "Condition": {  
        "Null": {  
            "aws:RequestTag/BusinessUnit": "true"  
        }  
    }  
}
```

D. Create an SCP and attach the SCP to the organization's management account. Include the following statement in the SCP:

```
{  
    "Sid": "DenyEC2Creation",  
    "Effect": "Deny",  
    "Action": [  
        "ec2:RunInstances"  
    ],  
    "Resource": [  
        "arn:aws:ec2:*:*:instance/*"  
    ],  
    "Condition": {  
        "Null": {  
            "aws:RequestTag/BusinessUnit": "false"  
        }  
    }  
}
```

C

Deny run EC2 instance if tag business unit is null

Question 365:

A company is running a workload that consists of thousands of Amazon EC2 instances. The workload is running in a VPC that contains several public subnets and private subnets. The public subnets have a route for 0.0.0.0/0 to an existing internet gateway. The private subnets have a route for 0.0.0.0/0 to an existing NAT gateway.

A solutions architect needs to migrate the entire fleet of EC2 instances to use IPv6. The EC2 instances that are in private subnets must not be accessible from the public internet.

What should the solutions architect do to meet these requirements?

A. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Update all the VPC route tables, and add a route for ::/0 to the internet gateway.

B. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Update the VPC route tables for all private subnets, and add a route for ::/0 to the NAT gateway.

C. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Create an egress-only internet gateway. Update the VPC route tables for all private subnets, and add a route for ::/0 to the egress-only internet gateway.

D. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Create a new NAT gateway, and enable IPv6 support. Update the VPC route tables for all private subnets, and add a route for ::/0 to the IPv6-enabled NAT gateway.

C

VPC Basics

- IPv6 in short
 - All IPv6 addresses are public, total 3.4×10^{38} addresses (vs 4.3 billion IPv4)
 - Example CIDR: 2600:1f18:80ca:900::/56
 - Addresses are “random” and can’t be scanned online (because too many)
- VPC support for IPv6
 - Create an IPv6 CIDR for VPC & use an IGW (supports IPv6)
 - Public subnet:
 - Create an instance with IPv6 support
 - Create a route table entry to ::/0 (IPv6 “all”) to the IGW
 - Private subnet (instances cannot be reached by IPv6 but can reach IPv6):
 - Create an Egress-Only Internet Gateway in the public subnet
 - Add a route table entry for the private subnet from ::/0 to the Egress-Only IGW

Question 366:

A company is using Amazon API Gateway to deploy a private REST API that will provide access to sensitive data. The API must be accessible only from an application that is deployed in a VPC. The company deploys the API successfully. However, the API is not accessible from an Amazon EC2 instance that is deployed in the VPC.

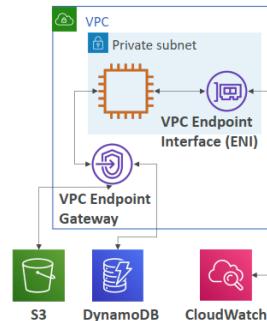
Which solution will provide connectivity between the EC2 instance and the API?

- Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows `apigateway:*` actions. Disable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC. Use the VPC endpoint's DNS name to access the API.
- Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows the `execute-api:Invoke` action. Enable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC endpoint. Use the API endpoint's DNS names to access the API.
- Create a Network Load Balancer (NLB) and a VPC link. Configure private integration between API Gateway and the NLB. Use the API endpoint's DNS names to access the API.
- Create an Application Load Balancer (ALB) and a VPC Link. Configure private integration between API Gateway and the ALB. Use the ALB endpoint's DNS name to access the API.

B

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables



Question 367:

A large payroll company recently merged with a small staffing company. The unified company now has multiple business units, each with its own existing AWS account.

A solutions architect must ensure that the company can centrally manage the billing and access policies for all the AWS accounts. The solutions architect configures AWS Organizations by sending an invitation to all member accounts of the company from a centralized management account.

What should the solutions architect do next to meet these requirements?

- Create the `OrganizationAccountAccess` IAM group in each member account. Include the necessary IAM roles for each administrator.

B. Create the OrganizationAccountAccessPolicy IAM policy in each member account. Connect the member accounts to the management account by using cross-account access.

C. Create the OrganizationAccountAccessRole IAM role in each member account. Grant permission to the management account to assume the IAM role.

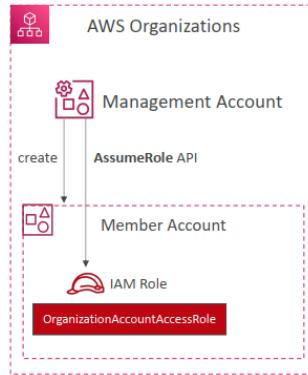
D. Create the OrganizationAccountAccessRole IAM role in the management account. Attach the AdministratorAccess AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account.

C

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html

AWS Organizations - OrganizationAccountAccessRole

- IAM role which grants full administrator permissions in the Member account to the Management account
- Used to perform admin tasks in the Member accounts (e.g., creating IAM users)
- Could be assumed by IAM users in the Management account
- Automatically added to all new Member accounts created with AWS Organizations
- Must be created manually if you invite an existing Member account



This setup enables centralized management of member accounts from the management account. Administrators in the management account can assume the OrganizationAccountAccessRole in member accounts to perform necessary actions, aligning with AWS best practices for Organizations. It simplifies the management and auditing of various accounts and ensures a standardized role exists across all accounts for consistent access control.

Question 368:

A company has application services that have been containerized and deployed on multiple Amazon EC2 instances with public IPs. An Apache Kafka cluster has been deployed to the EC2 instances. A PostgreSQL database has been migrated to Amazon RDS for PostgreSQL. The company expects a significant increase of orders on its platform when a new version of its flagship product is released.

What changes to the current architecture will reduce operational overhead and support the product release?

A. Create an EC2 Auto Scaling group behind an Application Load Balancer. Create additional read replicas for the DB instance. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.

B. Create an EC2 Auto Scaling group behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.

C. Deploy the application on a Kubernetes cluster created on the EC2 instances behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate and enable auto scaling behind an Application Load Balancer. Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

D reduce operational overhead ➔ EKS with Fargate

Question 369:

A company hosts a VPN in an on-premises data center. Employees currently connect to the VPN to access files in their Windows home directories. Recently, there has been a large growth in the number of employees who work remotely. As a result, bandwidth usage for connections into the data center has begun to reach 100% during business hours.

The company must design a solution on AWS that will support the growth of the company's remote workforce, reduce the bandwidth usage for connections into the data center, and reduce operational overhead.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Create an AWS Storage Gateway Volume Gateway. Mount a volume from the Volume Gateway to the on-premises file server.
- B. Migrate the home directories to Amazon FSx for Windows File Server.
- C. Migrate the home directories to Amazon FSx for Lustre.
- D. Migrate remote users to AWS Client VPN.
- E. Create an AWS Direct Connect connection from the on-premises data center to AWS.

B,D LEAST operational overhead ➔ Migrate remote users to AWS Client VPN, setup Direct Connection takes a lot of time Windows home directories ➔ Amazon FSx for Windows File Server
--

Amazon FSx for Windows (File Server)

FSx

- FSx for Windows is a fully managed Windows file system share drive chia sẻ ổ đĩa
- Supports SMB protocol & Windows NTFS
- Microsoft Active Directory integration, ACLs, user quotas
- Can be mounted on Linux EC2 instances
- Supports Microsoft's Distributed File System (DFS) Namespaces (group files across multiple FS)
- Scale up to 10s of GB/s, millions of IOPS, 100s PB of data
- Storage Options:
 - SSD – latency sensitive workloads (databases, media processing, data analytics, ...)
 - HDD – broad spectrum of workloads (home directory, CMS, ...) phạm vi rộng của khối lượng công việc
- Can be accessed from your on-premises infrastructure (VPN or Direct Connect)
- Can be configured to be Multi-AZ (high availability)
- Data is backed-up daily to S3

Question 370:

A company has multiple AWS accounts. The company recently had a security audit that revealed many unencrypted Amazon Elastic Block Store (Amazon EBS) volumes attached to Amazon EC2 instances.

A solutions architect must encrypt the unencrypted volumes and ensure that unencrypted volumes will be detected automatically in the future. Additionally, the company wants a solution that can centrally manage multiple AWS accounts with a focus on compliance and security.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the strongly recommended controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- B. Use the AWS CLI to list all the unencrypted volumes in all the AWS accounts. Run a script to encrypt all the unencrypted volumes in place.
- C. Create a snapshot of each unencrypted volume. Create a new encrypted volume from the unencrypted snapshot. Detach the existing volume, and replace it with the encrypted volume.
- D. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the mandatory controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- E. Turn on AWS CloudTrail. Configure an Amazon EventBridge rule to detect and automatically encrypt unencrypted volumes.

A,C

AWS Control Tower – Guardrails Levels

- Mandatory

- Automatically enabled and enforced by AWS Control Tower
- Example: Disallow public Read access to the Log Archive account

- Strongly Recommended

- Based on AWS best practices (optional)
- Example: Enable encryption for EBS volumes attached to EC2 instances

- Elective Tùy chọn

- Commonly used by enterprises (optional)
- Example: Disallow delete actions without MFA in S3 buckets

Unencrypted EBS detection is part of strongly recommended guardrails, and you cannot encrypt a volume or snapshot in place. You need to create a new encrypted volume from an unencrypted snapshot, and attach it to the instance.

Question 371:

A company hosts an intranet web application on Amazon EC2 instances behind an Application Load Balancer (ALB). Currently, users authenticate to the application against an internal user database.

The company needs to authenticate users to the application by using an existing AWS Directory Service for Microsoft Active Directory directory. All users with accounts in the directory must have access to the application.

Which solution will meet these requirements?

A. Create a new app client in the directory. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule. Configure the listener rule with the appropriate issuer, client ID and secret, and endpoint details for the Active Directory service. Configure the new app client with the callback URL that the ALB provides.

B. Configure an Amazon Cognito user pool. Configure the user pool with a federated identity provider (IdP) that has metadata from the directory. Create an app client. Associate the app client with the user pool. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule. Configure the listener rule to use the user pool and app client.

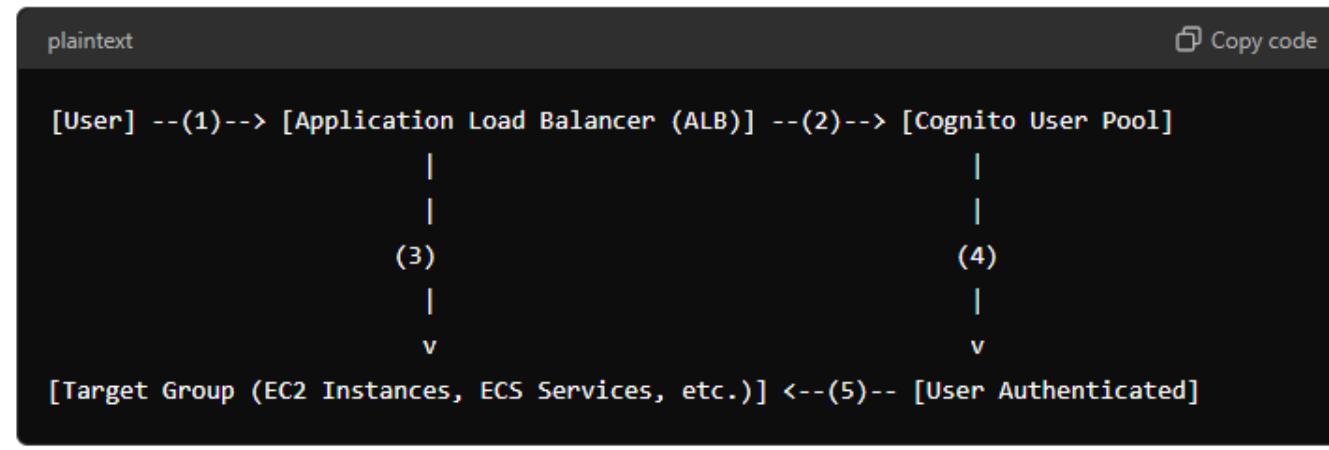
C. Add the directory as a new IAM identity provider (IdP). Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Configure the new role as the default authenticated user role for the IdP. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule.

D. Enable AWS IAM Identity Center (AWS Single Sign-On). Configure the directory as an external identity provider (IdP) that uses SAML. Use the automatic provisioning method. Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Attach the new role to all groups. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule.

B

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>

ALBs can interface directly to Cognito. The correct answer



Question 372:

A company has a website that serves many visitors. The company deploys a backend service for the website in a primary AWS Region and a disaster recovery (DR) Region.

A single Amazon CloudFront distribution is deployed for the website. The company creates an Amazon Route 53 record set with health checks and a failover routing policy for the primary Region's backend service. The company configures the Route 53 record set as an origin for the CloudFront distribution. The company configures another record set that points to the backend service's endpoint in the DR Region as a secondary failover record type. The TTL for both record sets is 60 seconds.

Currently, failover takes more than 1 minute. A solutions architect must design a solution that will provide the fastest failover time.

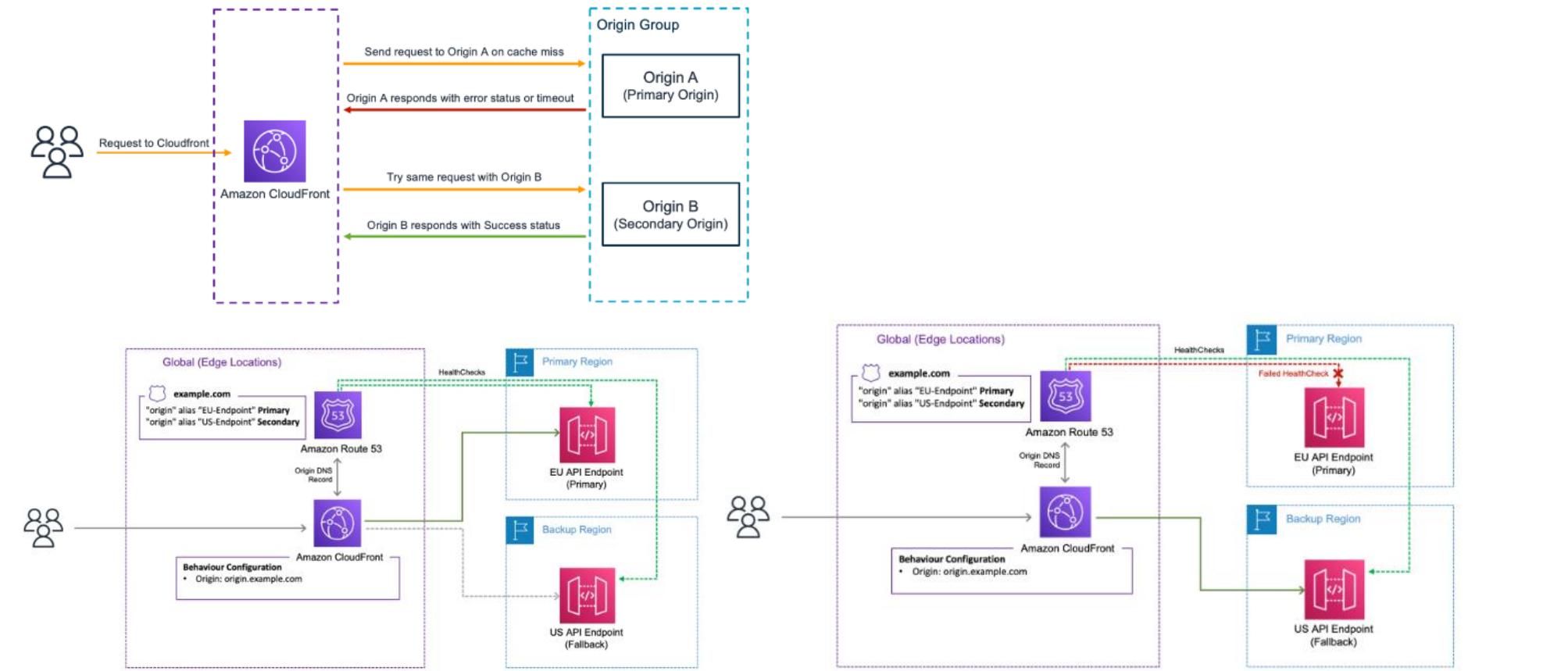
Which solution will achieve this goal?

- A. Deploy an additional CloudFront distribution. Create a new Route 53 failover record set with health checks for both CloudFront distributions.
- B. Set the TTL to 4 second for the existing Route 53 record sets that are used for the backend service in each Region.
- C. Create new record sets for the backend services by using a latency routing policy. Use the record sets as an origin in the CloudFront distribution.
- D. Create a CloudFront origin group that includes two origins, one for each backend service Region. Configure origin failover as a cache behavior for the CloudFront distribution.

D

LAB: <https://aws.amazon.com/blogs/networking-and-content-delivery/improve-web-application-availability-with-cloudfront-and-route53-hybrid-origin-failover/>

CloudFront allows customers to configure primary and secondary origins within an origin group, and specify the HTTP error codes that trigger a failover. When CloudFront receives the configured HTTP error code from the primary origin as a response (e.g., server error or server unreachable), it will attempt the original request with the secondary origin.



Question 373:

A company is using multiple AWS accounts and has multiple DevOps teams running production and non-production workloads in these accounts. The company would like to centrally-restrict access to some of the AWS services that the DevOps teams do not use. The company decided to use AWS Organizations and successfully invited all AWS accounts into the Organization. They would like to allow access to services that are currently in-use and deny a few specific services. Also they would like to administer multiple accounts together as a single unit.

What combination of steps should the solutions architect take to satisfy these requirements? (Choose three.)

HANCHE

- A. Use a Deny list strategy.
- B. Review the Access Advisor in AWS IAM to determine services recently used
- C. Review the AWS Trusted Advisor report to determine services recently used.
- D. Remove the default FullAWSAccess SCP.
- E. Define organizational units (OUs) and place the member accounts in the OUs.
- F. Remove the default DenyAWSAccess SCP.

A,B,E

- A. allow access to services that are currently in-use and deny a few specific services → Deny list
- B. AWS IAM Access Advisor shows the service permissions granted to a user and when those services were last accessed. This information is valuable to understand which AWS services are actively used and which are not, helping to make informed decisions about which services to restrict.
- E. Organizational Units allow for grouping AWS accounts that have similar needs or requirements. This structure enables the solutions architect to apply policies at the OU level, making it easier to manage permissions and restrictions across multiple accounts.

IAM Security Tools

- IAM Credentials Report (account-level)
 - a report that lists all your account's users and the status of their various credentials
- IAM Access Advisor (user-level)
 - Access advisor shows the service permissions granted to a user and when those services were last accessed.
 - You can use this information to revise your policies.

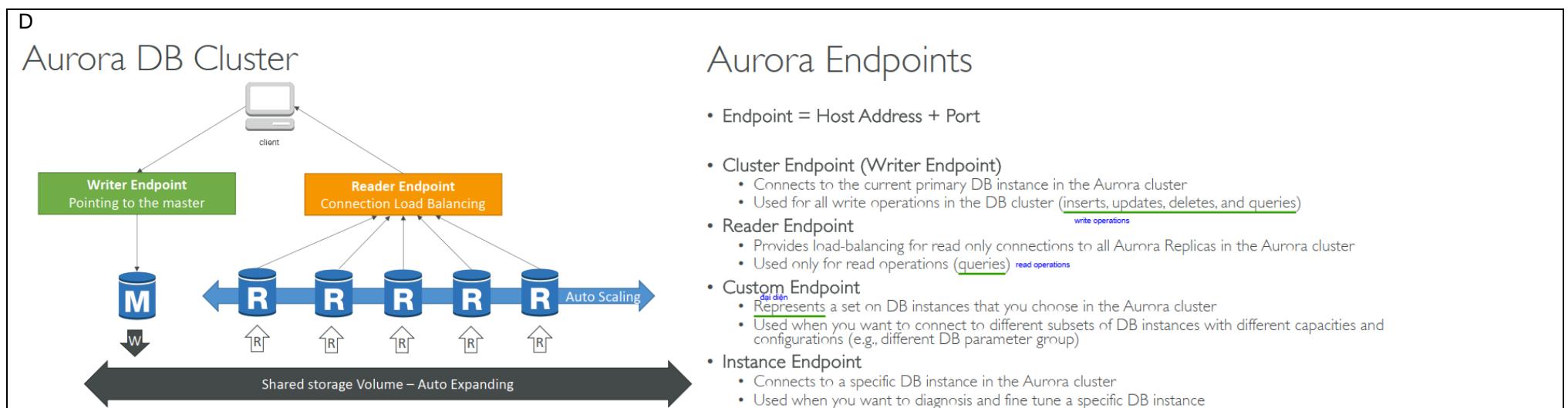
Question 374:

A live-events company is designing a scaling solution for its ticket application on AWS. The application has high peaks of utilization during sale events. Each sale event is a one-time event that is scheduled. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The application uses PostgreSQL for the database layer.

The company needs a scaling solution to maximize availability during the sale events.

Which solution will meet these requirements?

- A. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Serverless v2 Multi-AZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.
- B. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL Multi-AZ DB instance with automatically scaling read replicas. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger read replica before a sale event. Fail over to the larger read replica. Create another EventBridge rule that invokes another Lambda function to scale down the read replica after the sale event.
- C. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL MultiAZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.
- D. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Multi-AZ DB cluster. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger Aurora Replica before a sale event. Fail over to the larger Aurora Replica. Create another EventBridge rule that invokes another Lambda function to scale down the Aurora Replica after the sale event.



Question 375:

A company runs an intranet application on premises. The company wants to configure a cloud backup of the application. The company has selected AWS Elastic Disaster Recovery for this solution.

The company requires that replication traffic does not travel through the public internet. The application also must not be accessible from the internet. The company does not want this solution to consume all available network bandwidth because other applications require bandwidth.

Which combination of steps will meet these requirements? (Choose three.)

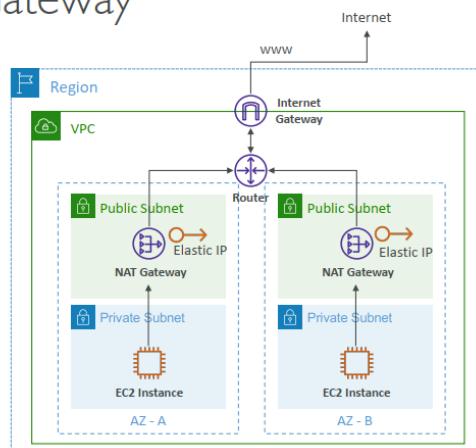
- A. Create a VPC that has at least two private subnets, two NAT gateways, and a virtual private gateway.
- B. Create a VPC that has at least two public subnets, a virtual private gateway, and an internet gateway.
- C. Create an AWS Site-to-Site VPN connection between the on-premises network and the target AWS network.
- D. Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.
- E. During configuration of the replication servers, select the option to use private IP addresses for data replication.
- F. During configuration of the launch settings for the target servers, select the option to ensure that the Recovery instance's private IP address matches the source server's private IP address.

A,D,E

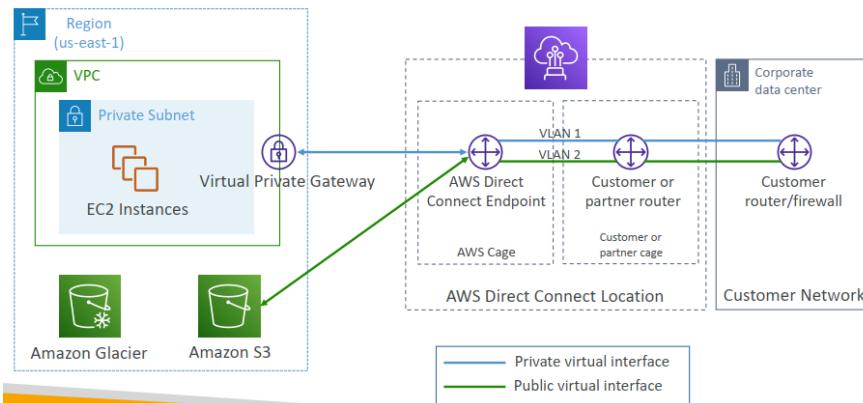
D. Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.

VPC Basics – NAT Gateway

- Managed NAT solution, bandwidth scales automatically
- Resilient to failure within a single AZ
- Must deploy multiple NAT Gateways in multiple AZ for HA
- Has an Elastic IP, external services see the IP of the NAT Gateway as the source

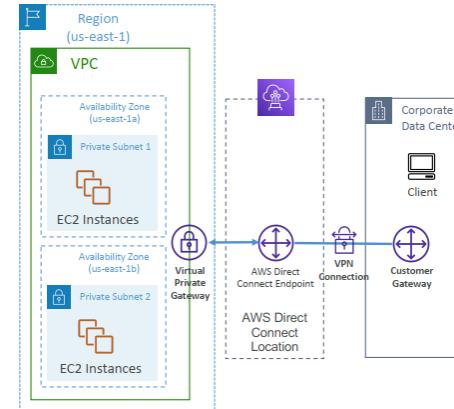


Direct Connect Diagram



Direct Connect – Encryption

- Data in transit is not encrypted but is private
- AWS Direct Connect + VPN provides an IPsec-encrypted private connection
- VPN over Direct Connect connection
Uses Public VIF
- Good for an extra level of security, but slightly more complex to put in place



Question 376:

A company that provides image storage services wants to deploy a customer-facing solution to AWS. Millions of individual customers will use the solution. The solution will receive batches of large image files, resize the files, and store the files in an Amazon S3 bucket for up to 6 months.

The solution must handle significant variance in demand. The solution must also be reliable at enterprise scale and have the ability to rerun processing jobs in the event of failure.

Which solution will meet these requirements MOST cost-effectively?

- Use AWS Step Functions to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.
- Use Amazon EventBridge to process the S3 event that occurs when a user uploads an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.
- Use S3 Event Notifications to invoke an AWS Lambda function when a user stores an image. Use the Lambda function to resize the image in place and to store the original file in the S3 bucket. Create an S3 Lifecycle policy to move all stored images to S3 Standard-Infrequent Access (S3 Standard-IA) after 6 months.
- Use Amazon Simple Queue Service (Amazon SQS) to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image and stores the resized file in an S3 bucket that uses S3 Standard-Infrequent Access (S3 Standard-IA). Create an S3 Lifecycle policy to move all stored images to S3 Glacier Deep Archive after 6 months.

B
 resize the files → Lambda
 store the files in an Amazon S3 bucket for up to 6 months → Lifecycle

B (Amazon EventBridge with AWS Lambda and S3 Lifecycle Expiration Policy) seems to be the most cost-effective and appropriate solution. It combines the scalability and flexibility of AWS Lambda for image processing with the straightforward event handling of Amazon EventBridge, and appropriately manages the image lifecycle with an S3 expiration policy.

C is also a strong contender, the misalignment of the lifecycle policy with the requirement makes Option B a better fit.

A might be more suitable for complex workflows but is likely not needed for this scenario, and Option D includes unnecessary long-term archival steps.

Question 377:

A company has an organization in AWS Organizations that includes a separate AWS account for each of the company's departments. Application teams from different departments develop and deploy solutions independently.

The company wants to reduce compute costs and manage costs appropriately across departments. The company also wants to improve visibility into billing for individual departments. The company does not want to lose operational flexibility when the company selects compute resources.

Which solution will meet these requirements?

- A. Use AWS Budgets for each department. Use Tag Editor to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.
- B. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use SCPs to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.
- C. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use Tag Editor to apply tags to appropriate resources. Purchase Compute Savings Plans.
- D. Use AWS Budgets for each department. Use SCPs to apply tags to appropriate resources. Purchase Compute Savings Plans.

C

manage costs appropriately across departments and visibility into billing for individual departments → AWS Organizations and Tag Editor
reduce compute costs → savings plan
operational flexibility when the company selects compute resources → Compute savings plan

AWS Savings Plan

- New pricing model to get a discount based on long-term usage
Cam kết sử dụng 1 loại
 - Commit to a certain type of usage: ex \$10 per hour for 1 to 3 years
 - Any usage beyond the savings plan is billed at the on-demand price
- EC2 Instance Savings plan** (up to 72% - same discount as Standard RIs)
- Select instance family (e.g. M5, C5...), and locked to a specific region
 - Flexible across size (m5.large to m5.4xlarge), OS (Windows to Linux), tenancy (dedicated or default)
- Compute Savings plan** (up to 66% - same discount as Convertible RIs)
- Ability to move between instance family (move from C5 to M5), region (Ireland to US), compute type (**EC2, Fargate, Lambda**), OS & tenancy
- SageMaker Savings plan** (up to 64% off)



AWS Organization - Feature Modes

- Consolidated billing features:
 - Consolidated Billing across all accounts - single payment method
 - Pricing benefits from aggregated usage (volume discount for EC2, S3...)
- All Features (Default):
 - Includes consolidated billing features, SCP
 - Invited accounts must approve enabling all features
 - Ability to apply an SCP to prevent member accounts from leaving the org
 - Can't switch back to Consolidated Billing Features only

AWS Tag Editor

- Allows you to manage tags of multiple resources at once
- You can add/update/delete tags
- Search tagged/untagged resources in all AWS Regions

Tag Editor

Find resources to tag
You can search for resources that you want to tag across regions. Then, you can add, remove, or edit tags for resources in your search results. [Learn more](#)

Regions

Select regions

eu-west-2 X us-east-1 X

Resource types

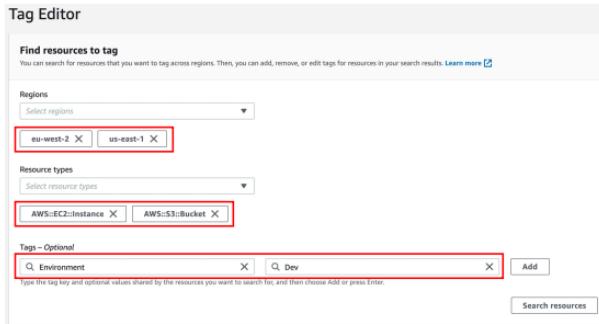
Select resource types

AWS:EC2:Instance X AWS:S3:Bucket X

Tags - Optional

Q: Environment X | Q: Dev X Add

Search resources



AWS Budgets



- Create budget and send alarms when costs exceeds the budget
- 4 types of budgets: Usage, Cost, Reservation, Savings Plans
- For Reserved Instances (RI)
 - Track utilization
 - Supports EC2, ElastiCache, RDS, Redshift
- Up to 5 SNS notifications per budget
- Can filter by: Service, Linked Account, Tag, Purchase Option, Instance Type, Region, Availability Zone, API Operation, etc...
- Same options as AWS Cost Explorer!
- 2 budgets are free, then \$0.02/day/budget

Question 378:

A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket. The company requires that only authenticated users are allowed to post content. The application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB.

What can a solutions architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?

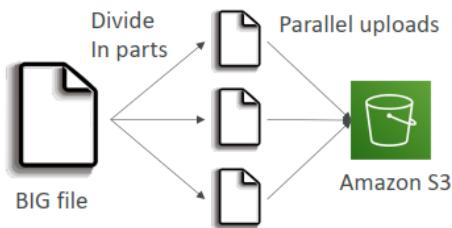
- A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using a COGNITO_USER_POOLS authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using an AWS Lambda authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket. Use the endpoint when generating the presigned URL. Have the browser interface upload the objects to this URL using the S3 multipart upload API.
- D. Configure an Amazon CloudFront distribution for the destination S3 bucket. Enable PUT and POST methods for the CloudFront cache behavior. Update the CloudFront origin to use an origin access identity (OAI). Give the OAI user 3: PutObject permissions in the bucket policy. Have the browser interface upload objects using the CloudFront distribution.

C

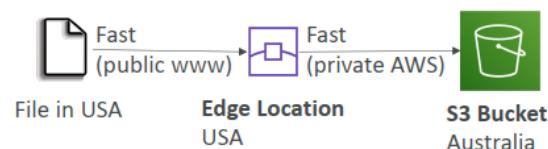
The limit of API Gateway payload is 10MB → A, B are wrong.

S3 Performance

- Multi-Part upload:
 - recommended for files > 100MB, must use for files > 5GB
 - Can help parallelize uploads (speed up transfers)



- S3 Transfer Acceleration
 - Increase transfer speed by transferring file to an AWS edge location which will forward the data to the S3 bucket in the target region
 - Compatible with multi-part upload



Question 379:

A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account that supports both development and test environments. New accounts to support production workloads will be needed soon.

The finance department requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs.

The security team requires a centralized mechanism to control IAM usage in all the company's accounts.

What combination of the following options meets the company's needs with the LEAST effort? (Choose two.)

- A. Use a collection of parameterized AWS CloudFormation templates defining common IAM permissions that are launched into each account. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.
- B. Use AWS Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations.
- C. Require each business unit to use its own AWS accounts. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks.
- D. Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.

E. Consolidate all of the company's AWS accounts into a single AWS account. Use tags for billing purposes and the IAM's Access Advisor feature to enforce the least privilege model.

B, D

requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs → AWS Organizations
control IAM usage in all the company's accounts → SCP → all features of AWS Organizations

AWS Organization - Feature Modes

- Consolidated billing features:
 - Consolidated Billing across all accounts - single payment method
 - Pricing benefits from aggregated usage (volume discount for EC2, S3...)
- All Features (Default):
 - Includes consolidated billing features, SCP
 - Invited accounts must approve enabling all features
 - Ability to apply an SCP to prevent member accounts from leaving the org
 - Can't switch back to Consolidated Billing Features only

Question 380:

A company has a solution that analyzes weather data from thousands of weather stations. The weather stations send the data over an Amazon API Gateway REST API that has an AWS Lambda function integration. The Lambda function calls a third-party service for data pre-processing. The third-party service gets overloaded and fails the pre-processing, causing a loss of data.

A solutions architect must improve the resiliency of the solution. The solutions architect must ensure that no data is lost and that data can be processed later if failures occur.

What should the solutions architect do to meet these requirements?

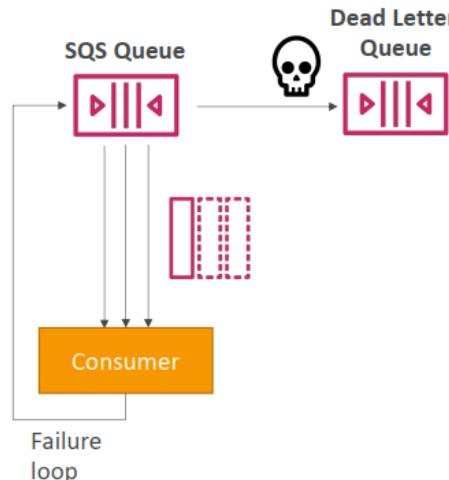
- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue as the dead-letter queue for the API.
- B. Create two Amazon Simple Queue Service (Amazon SQS) queues: a primary queue and a secondary queue. Configure the secondary queue as the dead-letter queue for the primary queue. Update the API to use a new integration to the primary queue. Configure the Lambda function as the invocation target for the primary queue.
- C. Create two Amazon EventBridge event buses: a primary event bus and a secondary event bus. Update the API to use a new integration to the primary event bus. Configure an EventBridge rule to react to all events on the primary event bus. Specify the Lambda function as the target of the rule. Configure the secondary event bus as the failure destination for the Lambda function.
- D. Create a custom Amazon EventBridge event bus. Configure the event bus as the failure destination for the Lambda function.

B

It uses two Amazon SQS queues to ensure that incoming data is not lost and can be processed later in case of failures. The primary queue acts as the initial landing point for data from the API Gateway, and the secondary queue serves as a dead-letter queue, capturing data that could not be processed due to third-party service failures or other issues. This setup maintains data integrity and allows for later processing, effectively improving the solution's resiliency.

Amazon SQS – Dead Letter Queue (DLQ)

- If a consumer fails to process a message within the Visibility Timeout...
the message goes back to the queue!
- We can set a threshold of how many times a message can go back to the queue
- After the **MaximumReceives** threshold is exceeded, the message goes into a Dead Letter Queue (DLQ)
- Useful for debugging!
- DLQ of a FIFO queue must also be a FIFO queue
- DLQ of a Standard queue must also be a Standard queue
- Make sure to process the messages in the DLQ before they expire:
 - Good to set a retention of 14 days in the DLQ



Question 381:

A company built an ecommerce website on AWS using a three-tier web architecture. The application is Java-based and composed of an Amazon CloudFront distribution, an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database.

Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics. Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis.

Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? (Choose three.)

- Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs.
- Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.
- Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis.

D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs.

E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora

F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

A, B, D

LAB: <https://aws.amazon.com/blogs/mt/simplifying-apache-server-logs-with-amazon-cloudwatch-logs-insights/>

<https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-dotnet-messagehandler.html>

Publishing slow query and error logs to CloudWatch Logs will allow for better analysis of database performance issues. It helps in identifying slow-running queries that might be contributing to the application's performance problems. Integrating AWS X-Ray SDK into the application will enable tracing of incoming HTTP requests on the EC2 instances. Tracing SQL queries with the X-Ray SDK for Java will provide insights into how database queries are impacting application performance. X-Ray can give a detailed analysis of both service-level and database-level operations, which is essential for diagnosing performance bottlenecks. Integrating AWS X-Ray SDK into the application will enable tracing of incoming HTTP requests on the EC2 instances. Tracing SQL queries with the X-Ray SDK for Java will provide insights into how database queries are impacting application performance. X-Ray can give a detailed analysis of both service-level and database-level operations, which is essential for diagnosing performance bottlenecks.

AWS X-Ray Visual analysis of our applications



X-Ray



- Tracing requests across your microservices (distributed systems)
- Integrations with:
 - EC2 – install the X-Ray agent
 - ECS – install the X-Ray agent or Docker container
 - Lambda
 - Beanstalk - agent is automatically installed
 - API Gateway – helpful to debug errors (such as 504)
- The X-Ray agent or services need IAM permissions to X-Ray

Question 382:

A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage. The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore. Application read and write traffic is slow during peak seasons.

Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?

A. Migrate the backend services to AWS Lambda. Increase the read and write capacity of DynamoDB.

B. Migrate the backend services to AWS Lambda. Configure DynamoDB to use global tables.

C. Use Auto Scaling groups for the backend services. Use DynamoDB auto scaling.

D. Use Auto Scaling groups for the backend services. Use Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB.

C

LEAST development effort ➔ C is correct, D is complicate because need to use Lambda function.

DynamoDB – in short



- NoSQL database, fully managed, ^{quy mô lớn} massive scale (1,000,000 rps)
- Similar to Apache Cassandra (can migrate to DynamoDB)
- No disk space to provision, max object size is 400 KB
- Capacity: provisioned (WCU, RCU, & Auto Scaling) or on-demand
- Supports CRUD (Create Read Update Delete)
- Read: eventually or strong consistency
- Supports transactions across multiple tables (ACID support)
- Backups available, point in time recovery
- Table classes: Standard and Infrequent Access (IA)

Question 383:

A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory, and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers.

Which would enable the collection of this data MOST cost effectively?

- A. Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center.
- B. Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs.
- C. Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment.
- D. Enable AWS Application Discovery Service in the AWS Management Console and configure the corporate firewall to allow scans over a VPN.

A

evaluate the configurations of virtual machines, wants to collect metrics, such as CPU, memory, and disk utilization → AWS Application Discovery Agent
<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html#compare-tools>

AWS Application Discovery Service



- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping are important for migrations
- **Agentless Discovery (AWS Agentless Discovery Connector)**
 - Open Virtual Appliance (OVA) package that can be deployed to a VMware host
 - VM inventory, configuration, and performance history such as CPU, memory, and disk usage
 - OS agnostic
- **Agent-based Discovery (AWS Application Discovery Agent)**
 - System configuration, system performance, running processes, and details of the network connections between systems
 - Supports Microsoft Server, Amazon Linux, Ubuntu, RedHat, CentOS, SUSE...
- Resulting data can be exported as CSV or viewed within AWS Migration Hub
- Data can be explored using pre-defined queries in Amazon Athena

Agentless discovery can be performed by deploying the Application Discovery Service Agentless Collector (Agentless Collector) (OVA file) through your **VMware vCenter**. After Agentless Collector is configured, it identifies virtual machines (VMs) and hosts associated with vCenter. Agentless Collector collects the following static configuration data: Server hostnames, IP addresses, MAC addresses, disk resource allocations, database engine versions, and database schemas. Additionally, it collects the utilization data for each VM and database providing the average and peak utilization for metrics such as CPU, RAM, and Disk I/O.

Agent-based discovery can be performed by deploying the AWS Application Discovery Agent on each of your VMs and physical servers. The agent installer is available for Windows and Linux operating systems. It collects static configuration data, detailed time-series system-performance information, inbound and outbound network connections, and processes that are running.

Question 384:

A company provides a software as a service (SaaS) application that runs in the AWS Cloud. The application runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in an Auto Scaling group and are distributed across three Availability Zones in a single AWS Region.

The company is deploying the application into additional Regions. The company must provide static IP addresses for the application to customers so that the customers can add the IP addresses to allow lists. The solution must automatically route customers to the Region that is geographically closest to them.

Which solution will meet these requirements?

- A. Create an Amazon CloudFront distribution. Create a CloudFront origin group. Add the NLB for each additional Region to the origin group. Provide customers with the IP address ranges of the distribution's edge locations.
- B. Create an AWS Global Accelerator standard accelerator. Create a standard accelerator endpoint for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.
- C. Create an Amazon CloudFront distribution. Create a custom origin for the NLB in each additional Region. Provide customers with the IP address ranges of the distribution's edge locations.
- D. Create an AWS Global Accelerator custom routing accelerator. Create a listener for the custom routing accelerator. Add the IP address and ports for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.

B

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-accelerator-types.html>

The company must provide static IP addresses for the application → AWS Global Accelerator

There are two types of accelerators that you can use with AWS Global Accelerator: standard accelerators and custom routing accelerators. Both types of accelerators route traffic over the AWS global network to improve performance and stability, but they're each designed for different application needs.

Standard accelerator

By using a standard accelerator, you can improve the availability and performance of your applications running on Application Load Balancers, Network Load Balancers, or Amazon EC2 instances. With a standard accelerator, Global Accelerator routes client traffic across regional endpoints based on geo-proximity and endpoint health. It also allows customers to shift client traffic across endpoints based on controls such as traffic dials and endpoint weights. This works for a wide variety of use cases, including blue/green deployment, A/B testing, and multi-Region deployment. To see more use cases, see AWS Global Accelerator use cases.

To learn more, see Work with standard accelerators in AWS Global Accelerator.

Custom routing accelerator

Custom routing accelerators work well for scenarios where you want to use custom application logic to direct one or more users to a specific destination and port among many, while still gaining the performance benefits of Global Accelerator. One example is VoIP applications that assign multiple callers to a specific media server to start voice, video, and messaging sessions. Another example is online real-time gaming applications where you want to assign multiple players to a single session on a game server based on factors such as geographic location, player skill, and game mode.

Note

Custom routing accelerators support only the IPv4 IP address type.

To learn more, see Work with custom routing accelerators in AWS Global Accelerator.

Based on your specific needs, you create one of these types of accelerators to accelerate your customer traffic.

AWS Global Accelerator vs CloudFront

- They both use the AWS global network and its edge locations around the world
- Both services integrate with AWS Shield for DDoS protection.
- CloudFront
 - Improves performance for both cacheable content (such as images and videos)
 - Dynamic content (such as API ^{su tăng tốc} acceleration and dynamic site delivery)
 - Content is served at the edge
- Global Accelerator
 - Improves performance for a wide range of applications over TCP or UDP
 - Proxying packets at the edge to applications running in one or more AWS Regions.
 - Good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP
 - Good for HTTP use cases that require static IP addresses
 - Good for HTTP use cases that required deterministic, fast regional failover

Question 385:

A company is running multiple workloads in the AWS Cloud. The company has separate units for software development. The company uses AWS Organizations and federation with SAML to give permissions to developers to manage resources in their AWS accounts. The development units each deploy their production workloads into a common production account.

Recently, an incident occurred in the production account in which members of a development unit terminated an EC2 instance that belonged to a different development unit. A solutions architect must create a solution that prevents a similar incident from happening in the future. The solution also must allow developers the possibility to manage the instances used for their workloads.

Which strategy will meet these requirements?

- A. Create separate OUs in AWS Organizations for each development unit. Assign the created OUs to the company AWS accounts. Create separate SCP with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag that matches the development unit name. Assign the SCP to the corresponding OU.
- B. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Update the IAM policy for the developers' assumed IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit.

C. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Create an SCP with an allow action and a StringEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit. Assign the SCP to the root OU.

D. Create separate IAM policies for each development unit. For every IAM policy, add an allow action and a StringEquals condition for the DevelopmentUnit resource tag and the development unit name. During SAML federation, use AWS Security Token Service (AWS STS) to assign the IAM policy and match the development unit name to the assumed IAM role.

B

A - Does not make much sense. An account can only belong to one OU. This is a single production account so it can't be in multiple OUs.

B - Session tag is used to identify which business unit a user is part of. IAM policy prevent them from modifying resources for any business unit but their own.

C. This does not restrict any existing permissions so users can still modify resources from different business units.

D. STS cannot be used to assign a policy to an IAM role. A policy has to be assigned to the role before authentication occurs.

SAML 2.0 Federation

- Security Assertion Markup Language 2.0 (SAML 2.0)
- Open standard used by many identity providers (e.g., ADFS)
 - Supports integration with Microsoft Active Directory Federations Services (ADFS)
 - Or any SAML 2.0-compatible IdPs with AWS
- Access to AWS Console, AWS CLI, or AWS API using temporary credentials
 - No need to create IAM Users for each of your employees
 - Need to setup a trust between AWS IAM and SAML 2.0 Identity Provider (both ways)
- Under-the-hood: Uses the STS API AssumeRoleWithSAML
- SAML 2.0 Federation is the “old way”, Amazon Single Sign-On (AWS SSO) Federation is the new managed and simpler way
 - <https://aws.amazon.com/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/>

Question 386:

An enterprise company is building an infrastructure services platform for its users. The company has the following requirements:

- Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services.
- Use a central account to manage the creation of infrastructure services.
- Provide the ability to distribute infrastructure services to multiple accounts in AWS Organizations.
- Provide the ability to enforce tags on any infrastructure that is started by users.

Which combination of actions using AWS services will meet these requirements? (Choose three.)

- A. Develop infrastructure services using AWS CloudFormation templates. Add the templates to a central Amazon S3 bucket and add the IAM roles or users that require access to the S3 bucket policy.
- B. Develop infrastructure services using AWS CloudFormation templates. Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account. Share these portfolios with the Organizations structure created for the company.
- C. Allow user IAM roles to have AWSCloudFormationFullAccess and AmazonS3ReadOnlyAccess permissions. Add an Organizations SCP at the AWS account root user level to deny all services except AWS CloudFormation and Amazon S3.
- D. Allow user IAM roles to have ServiceCatalogEndUserAccess permissions only. Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption, assign users access, and apply launch constraints.
- E. Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company. Apply the TagOption to AWS Service Catalog products or portfolios.
- F. Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any CloudFormation templates that will be created for users.

B,D,E

Use a central account to manage the creation of infrastructure services → AWS Service Catalog

<https://docs.aws.amazon.com/servicecatalog/latest/adminguide/tagoptions.html>

<https://trello.com/c/BKKfMY0C/423-aws-service-catalog-tagoption>

AWS Service Catalog



- Create and manage catalogs of IT services that are approved on AWS
- The “products” are CloudFormation templates
- Ex: Virtual machine images, Servers, Software, Databases, Regions, IP address ranges
- CloudFormation helps ensure consistency, and standardization by Admins
- They are assigned to Portfolios (teams)
Các nhóm được cung cấp một công thông tin tự phục vụ để họ có thể ra mắt sản phẩm
- Teams are presented a self-service portal where they can launch the products
- All the deployed products are centrally managed deployed services
- Helps with governance, compliance, and consistency
- Can give user access to launching products without requiring deep AWS knowledge
- Integrations with “self-service portals” such as ServiceNow

Question 387:

A company deploys a new web application. As part of the setup, the company configures AWS WAF to log to Amazon S3 through Amazon Kinesis Data Firehose. The company develops an Amazon Athena query that runs once daily to return AWS WAF log data from the previous 24 hours. The volume of daily logs is constant. However, over time, the same query is taking more time to run.

A solutions architect needs to design a solution to prevent the query time from continuing to increase. The solution must minimize operational overhead.

Which solution will meet these requirements?

- Create an AWS Lambda function that consolidates each day's AWS WAF logs into one log file.
- Reduce the amount of data scanned by configuring AWS WAF to send logs to a different S3 bucket each day.
- Update the Kinesis Data Firehose configuration to partition the data in Amazon S3 by date and time. Create external tables for Amazon Redshift. Configure Amazon Redshift Spectrum to query the data source.
- Modify the Kinesis Data Firehose configuration and Athena table definition to partition the data by date and time. Change the Athena query to view the relevant partitions.

D

<https://aws.amazon.com/blogs/big-data/kinesis-data-firehose-now-supports-dynamic-partitioning-to-amazon-s3/>

Partitioning is a powerful technique for optimizing query performance and cost in Athena, especially for large, growing datasets. Firehose and Athena seamlessly support partitioning, making it easy to implement.

Amazon Athena – Performance Improvement

- Use **columnar data** for cost-savings (less scan)
 - Apache Parquet or ORC is recommended
 - Huge performance improvement
 - Use Glue to convert your data to Parquet or ORC
- Compress **data** for smaller retrievals (bzip2, gzip, lz4, snappy, zlip, zstd...)
- Partition datasets in S3 for easy querying on virtual columns
 - s3://yourBucket/pathToTable
 / <PARTITION_COLUMN_NAME>=<VALUE>
 / <PARTITION_COLUMN_NAME>=<VALUE>
 / <PARTITION_COLUMN_NAME>=<VALUE>
 /etc...
 - Example: s3://athena-examples/flight/parquet/year=1991/month=1/day=1/
- Use larger files (> 128 MB) to minimize overhead

Question 388:

A company is developing a web application that runs on Amazon EC2 instances in an Auto Scaling group behind a public-facing Application Load Balancer (ALB). Only users from a specific country are allowed to access the application. The company needs the ability to log the access requests that have been blocked. The solution should require the least possible maintenance.

Which solution meets these requirements?

- Create an IPSet containing a list of IP ranges that belong to the specified country. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from the specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- Configure AWS Shield to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB.
- Create a security group rule that allows ports 80 and 443 from IP ranges that belong to the specified country. Associate the security group with the ALB.

B

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-geo-match.html>

AWS WAF – Web Application Firewall



- Protects your web applications from common web exploits (Layer 7)
- Deploy on **Application Load Balancer** (localized rules)
- Deploy on **API Gateway** (rules running at the regional or edge level)
- Deploy on **CloudFront** (rules globally on edge locations)
 - Used to front other solutions: CLB, EC2 instances, custom origins, S3 websites
- Deploy on AppSync (protect your GraphQL APIs)
- **WAF is not for DDoS protection**
- Define Web ACL (Web Access Control List):
 - Rules can include IP addresses, HTTP headers, HTTP body, or URI strings
 - Protects from common attack - SQL injection and Cross-Site Scripting (XSS)
 - Size constraints, Geo match
 - Rate-based rules (to count occurrences of events)
- Rule Actions: Count | Allow | Block | CAPTCHA

Question 389:

A company is migrating an application from on-premises infrastructure to the AWS Cloud. During migration design meetings, the company expressed concerns about the availability and recovery options for its legacy Windows file server. The file server contains sensitive business-critical data that cannot be recreated in the event of data corruption or data loss. According to compliance requirements, the data must not travel across the public internet. The company wants to move to AWS managed services where possible.

The company decides to store the data in an Amazon FSx for Windows File Server file system. A solutions architect must design a solution that copies the data to another AWS Region for disaster recovery (DR) purposes.

Which solution will meet these requirements?

A. Create a destination Amazon S3 bucket in the DR Region. Establish connectivity between the FSx for Windows File Server file system in the primary Region and the S3 bucket in the DR Region by using Amazon FSx File Gateway. Configure the S3 bucket as a continuous backup source in FSx File Gateway.

B. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Site-to-Site VPN. Configure AWS DataSync to communicate by using VPN endpoints.

C. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using VPC peering. Configure AWS DataSync to communicate by using interface VPC endpoints with AWS PrivateLink.

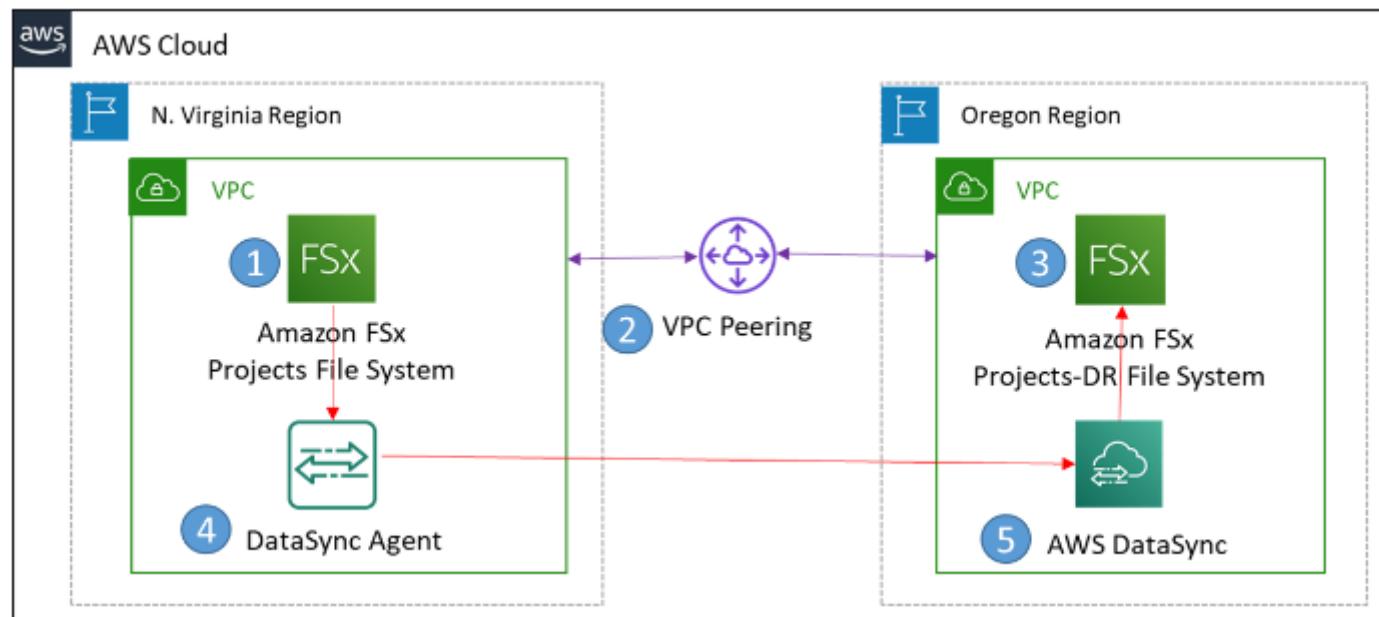
D. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Transit Gateway in each Region. Use AWS Transfer Family to copy files between the FSx for Windows File Server file system in the primary Region and the FSx for Windows File Server file system in the DR Region over the private AWS backbone network.

C

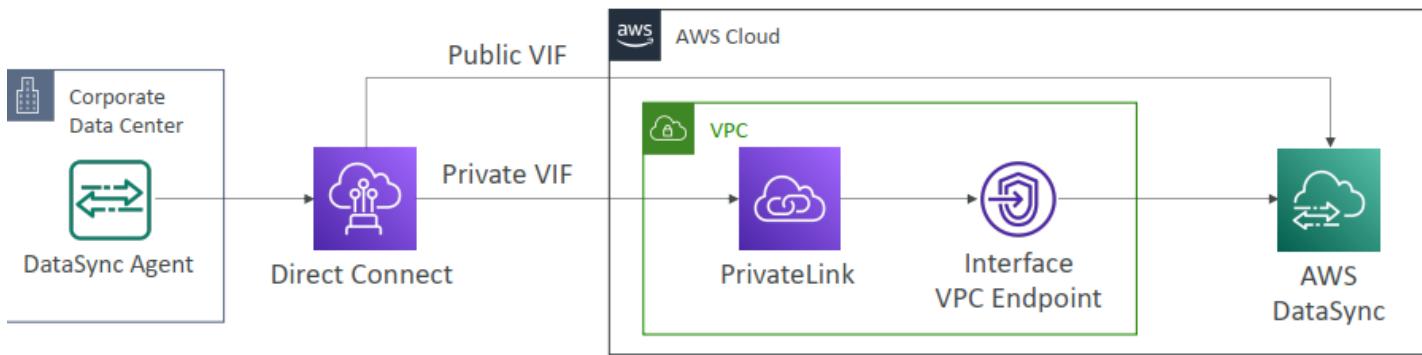
<https://aws.amazon.com/blogs/storage/how-to-replicate-amazon-fsx-file-server-data-across-aws-regions/>

Data Management & Transfer

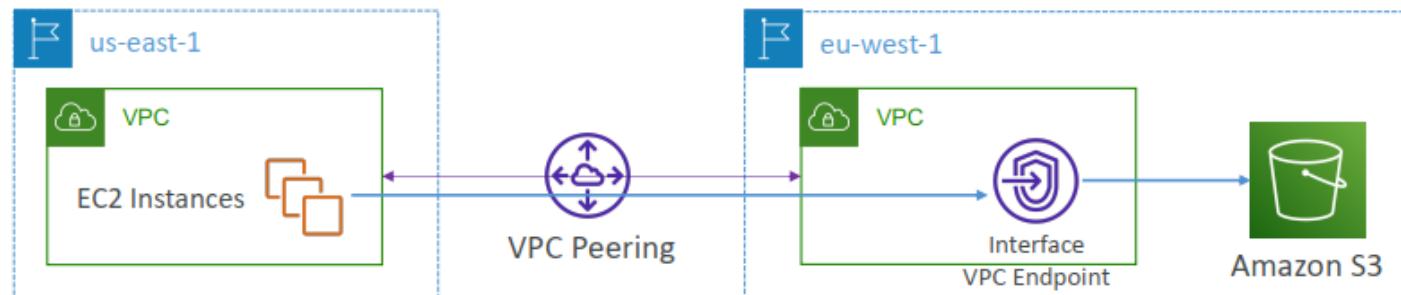
- AWS Direct Connect:
 - Move GB/s of data to the cloud, over a private secure network
- Snowball & Snowmobile
 - Move PB of data to the cloud
- AWS DataSync
 - Move large amount of data between on-premise and S3, EFS, FSx for Windows



AWS DataSync Private VIF through Direct Connect



VPC Endpoints / PrivateLink and VPC Peering



Question 390:

A company is currently in the design phase of an application that will need an RPO of less than 5 minutes and an RTO of less than 10 minutes. The solutions architecture team is forecasting that the database will store approximately 10 TB of data. As part of the design, they are looking for a database solution that will provide the company with the ability to fail over to a secondary Region.

Which solution will meet these business requirements at the LOWEST cost?

- A. Deploy an Amazon Aurora DB cluster and take snapshots of the cluster every 5 minutes. Once a snapshot is complete, copy the snapshot to a secondary Region to serve as a backup in the event of a failure.
- B. Deploy an Amazon RDS instance with a cross-Region read replica in a secondary Region. In the event of a failure, promote the read replica to become the primary.
- C. Deploy an Amazon Aurora DB cluster in the primary Region and another in a secondary Region. Use AWS DMS to keep the secondary Region in sync.
- D. Deploy an Amazon RDS instance with a read replica in the same Region. In the event of a failure, promote the read replica to become the primary.

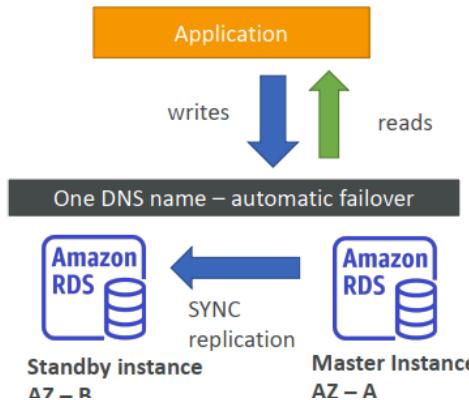
B

LOWEST cost → RDS read replica

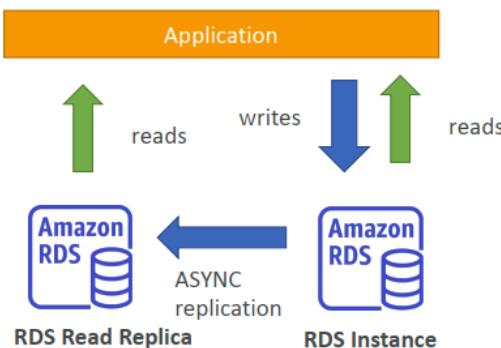
<https://trello.com/c/o7VmUIAX/398-rds-read-replica-vs-aurora-global>

RDS – Multi AZ & Read Replicas

- Multi-AZ: Standby instance for failover in case of outage



- Read Replicas: Increase read throughput. Eventual consistency. Can be cross-region



Question 391:

A financial company needs to create a separate AWS account for a new digital wallet application. The company uses AWS Organizations to manage its accounts. A solutions architect uses the IAM user Support1 from the management account to create a new member account with finance1@example.com as the email address.

What should the solutions architect do to create IAM users in the new member account?

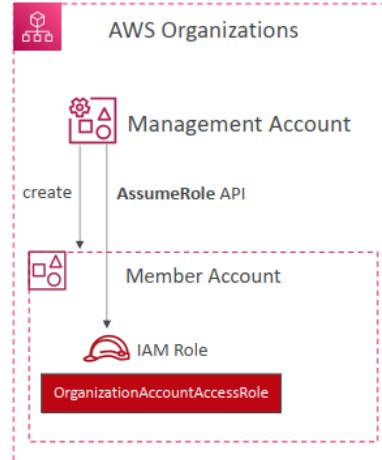
- Sign in to the AWS Management Console with AWS account root user credentials by using the 64-character password from the initial AWS Organizations email sent to finance1@example.com. Set up the IAM users as required.
- From the management account, switch roles to assume the OrganizationAccountAccessRole role with the account ID of the new member account. Set up the IAM users as required.
- Go to the AWS Management Console sign-in page. Choose “Sign in using root account credentials.” Sign in by using the email address finance1@example.com and the management account’s root password. Set up the IAM users as required.
- Go to the AWS Management Console sign-in page. Sign in by using the account ID of the new member account and the Support1 IAM credentials. Set up the IAM users as required.

B

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html
<https://trello.com/c/e8KoAui0/427-organizationaccountaccessrole>

AWS Organizations - OrganizationAccountAccessRole

- IAM role which grants full administrator permissions in the Member account to the Management account
- Used to perform admin tasks in the Member accounts (e.g., creating IAM users)
- Could be assumed by IAM users in the Management account
- Automatically added to all new Member accounts created with AWS Organizations
- Must be created manually if you invite an existing Member account



Question 392:

A car rental company has built a serverless REST API to provide data to its mobile app. The app consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda functions, and an Amazon Aurora MySQL Serverless DB cluster. The company recently opened the API to mobile apps of partners. A significant increase in the number of requests resulted, causing sporadic database memory errors.

Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time. Traffic is concentrated during business hours, with spikes around holidays and other events.

The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution.

Which strategy meets these requirements?

- Convert the API Gateway Regional endpoint to an edge-optimized endpoint. Enable caching in the production stage.
- Implement an Amazon ElastiCache for Redis cache to store the results of the database calls. Modify the Lambda functions to use the cache.
- Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory.
- Enable throttling in the API Gateway production stage. Set the rate and burst values to limit the incoming calls.

A

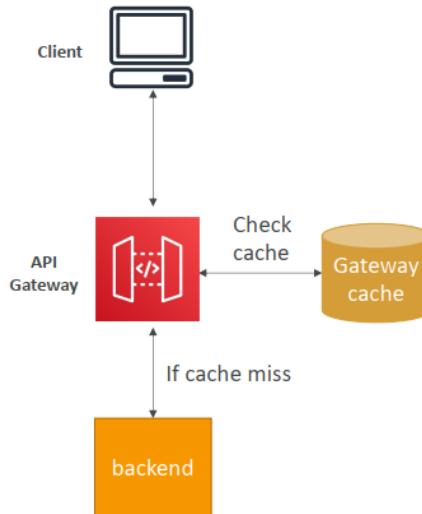
minimizing the increase in costs associated with the solution → A is cheaper than B

<https://trello.com/c/vOt1IpHK/428-api-gateway-cache-vs-elasticache-redis>

LAB: <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html>

Caching API responses

- Caching reduces the number of calls made to the backend
- Default TTL (time to live) is 300 seconds (min: 0s, max: 3600s)
- Caches are defined per stage
có thể ghi đè cấu hình cache cho mỗi method
- Possible to override cache settings per method
- Clients can vô hiệu hóa invalidate the cache with header: Cache-Control: max-age=0 (with proper IAM authorization)
- Able to flush the entire cache (invalidate it) immediately
- Cache encryption option
- Cache capacity between 0.5GB to 237GB



Question 393:

A company is migrating an on-premises application and a MySQL database to AWS. The application processes highly sensitive data, and new data is constantly updated in the database. The data must not be transferred over the internet. The company also must encrypt the data in transit and at rest.

The database is 5 TB in size. The company already has created the database schema in an Amazon RDS for MySQL DB instance. The company has set up a 1 Gbps AWS Direct Connect connection to AWS. The company also has set up a public VIF and a private VIF. A solutions architect needs to design a solution that will migrate the data to AWS with the least possible downtime.

Which solution will meet these requirements?

- Perform a database backup. Copy the backup files to an AWS Snowball Edge Storage Optimized device. Import the backup to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.
- Use AWS Database Migration Service (AWS DMS) to migrate the data to AWS. Create a DMS replication instance in a private subnet. Create VPC endpoints for AWS DMS. Configure a DMS task to copy data from the on-premises database to the DB instance by using full load plus change data capture (CDC). Use the AWS Key Management Service (AWS KMS) default key for encryption at rest. Use TLS for encryption in transit.

C. Perform a database backup. Use AWS DataSync to transfer the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.

D. Use Amazon S3 File Gateway. Set up a private connection to Amazon S3 by using AWS PrivateLink. Perform a database backup. Copy the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.

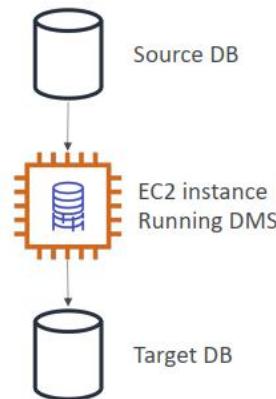
B

A, C, D are incorrect because load data into S3 then copy again to DB → no least possible downtime.

DMS – Database Migration Service



- Quickly and securely migrate databases to AWS, resilient, self healing
- The source database remains available during the migration
- Supports:
 - Homogeneous migrations: ex Oracle to Oracle
 - Heterogeneous migrations: ex Microsoft SQL Server to Aurora
- Continuous Data Replication using CDC
- You must create an EC2 instance to perform the replication tasks



DMS – Good things to know

- Works over VPC Peering, VPN (site to site, software), Direct Connect
- Supports Full Load, Full Load + CDC, or CDC only
- Oracle:
 - Source: Supports TDE for the source using “BinaryReader”
 - Target: Supports BLOBs in tables that have a primary key, and TDE
- OpenSearch:
 - Source: does not exist
 - Target: possible to migrate from a relational database using DMS
 - Therefore, DMS cannot be used to replicate OpenSearch data

Question 394:

Accompany is deploying a new cluster for big data analytics on AWS. The cluster will run across many Linux Amazon EC2 instances that are spread across multiple Availability Zones.

All of the nodes in the cluster must have read and write access to common underlying file storage. The file storage must be highly available, must be resilient, must be compatible with the Portable Operating System Interface (POSIX), and must accommodate high levels of throughput.

Which storage solution will meet these requirements?

- A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucket. Mount the NFS file share on each EC2 instance in the cluster.
- B. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mode. Mount the EFS file system on each EC2 instance in the cluster.
- C. Provision a new Amazon Elastic Block Store (Amazon EBS) volume that uses the io2 volume type. Attach the EBS volume to all of the EC2 instances in the cluster.
- D. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mode. Mount the EFS file system on each EC2 instance in the cluster.

D
big data analytics → Max I/O

EFS – Performance & Storage Classes

- EFS Scale
 - 1000s of concurrent NFS clients, 10 GB+ /s throughput
 - Grow to Petabyte-scale network file system, automatically
- Performance Mode (set at EFS creation time)
 - General Purpose (default) – latency-sensitive use cases (web server, CMS, etc...)
 - Max I/O – higher latency, throughput, highly parallel (big data, media processing)
- Throughput Mode
 - Bursting – 1 TB = 50MiB/s + burst of up to 100MiB/s
 - Provisioned – set your throughput regardless of storage size, ex: 1 GiB/s for 1 TB storage
 - Elastic – automatically scales throughput up or down based on your workloads
 - Up to 3GiB/s for reads and 1GiB/s for writes
 - Used for unpredictable workloads
không thể dự đoán

Question 395:

A company hosts a software as a service (SaaS) solution on AWS. The solution has an Amazon API Gateway API that serves an HTTPS endpoint. The API uses AWS Lambda functions for compute. The Lambda functions store data in an Amazon Aurora Serverless v1 database.

The company used the AWS Serverless Application Model (AWS SAM) to deploy the solution. The solution extends across multiple Availability Zones and has no disaster recovery (DR) plan.

A solutions architect must design a DR strategy that can recover the solution in another AWS Region. The solution has an RTO of 5 minutes and an RPO of 1 minute.

What should the solutions architect do to meet these requirements?

- Create a read replica of the Aurora Serverless v1 database in the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region. Promote the read replica to primary in case of disaster.
- Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region.
- Create an Aurora Serverless v1 DB cluster that has multiple writer instances in the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.

D. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.

D

Aurora Serverless v1 is not support replica. ➔ A is incorrect

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.html#aurora-serverless.limitations>

an RTO of 5 minutes and an RPO of 1 minute ➔ D is correct because using an active-passive configuration

Question 396:

A company owns a chain of travel agencies and is running an application in the AWS Cloud. Company employees use the application to search for information about travel destinations. Destination content is updated four times each year.

Two fixed Amazon EC2 instances serve the application. The company uses an Amazon Route 53 public hosted zone with a multivalue record of travel.example.com that returns the Elastic IP addresses for the EC2 instances. The application uses Amazon DynamoDB as its primary data store. The company uses a self-hosted Redis instance as a caching solution.

During content updates, the load on the EC2 instances and the caching solution increases drastically. This increased load has led to downtime on several occasions. A solutions architect must update the application so that the application is highly available and can handle the load that is generated by the content updates.

Which solution will meet these requirements?

A. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the EC2 instances before the content updates.

B. Set up Amazon ElastiCache for Redis. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.

C. Set up Amazon ElastiCache for Memcached. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the application before the content updates.

D. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.

A

can handle the load that is generated by the content updates. ➔ cached read ➔ DAX (redis is suitable for cached write)

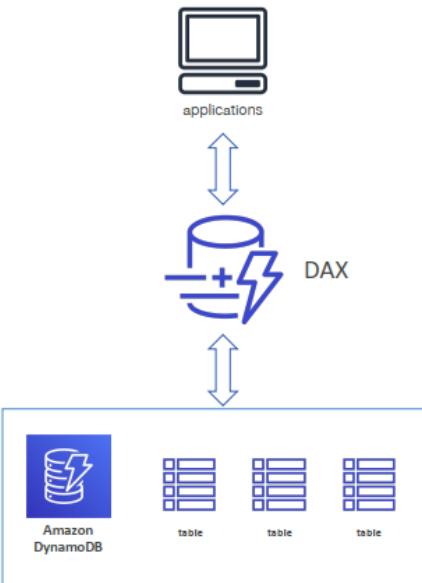
B is incorrect because manually scale up EC2 instances before the content updates.

C is incorrect because of using memcache

D is incorrect because manually scale up EC2 instances before the content updates.

DynamoDB - DAX

- DAX = DynamoDB Accelerator
Liên mạch
- Seamless cache for DynamoDB, no application re-write
- Writes go through DAX to DynamoDB
- Micro second latency for cached reads & queries
- Solves the Hot Key problem (too many reads)
- 5 minutes TTL for cache by default
- Up to 10 nodes in the cluster
- Multi AZ (3 nodes minimum recommended for production)
- Secure (Encryption at rest with KMS, VPC, IAM, CloudTrail...)



Question 397:

A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app. Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app is rarely used at any other time. A user is notified when image processing is complete.

Which combination of actions should a solutions architect take to ensure image processing can scale to handle the load? (Choose three.)

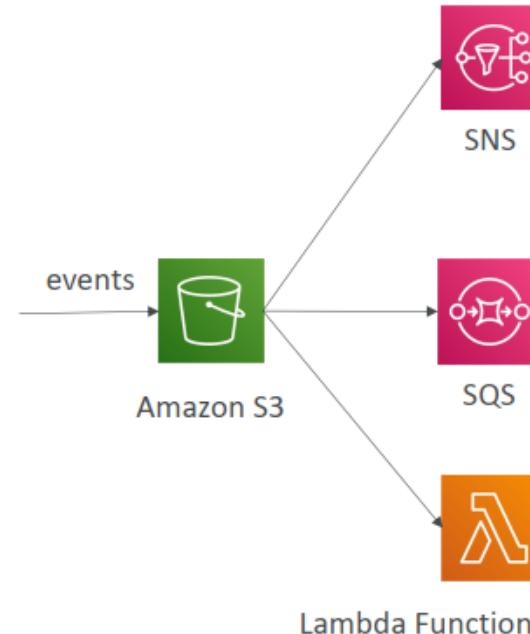
- Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon MQ queue.
- Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon Simple Queue Service (Amazon SQS) standard queue.
- Invoke an AWS Lambda function to perform image processing when a message is available in the queue.
- Invoke an S3 Batch Operations job to perform image processing when a message is available in the queue.
- Send a push notification to the mobile app by using Amazon Simple Notification Service (Amazon SNS) when processing is complete.
- Send a push notification to the mobile app by using Amazon Simple Email Service (Amazon SES) when processing is complete.

B, C, E

A user is notified when image processing is complete → Amazon SNS

S3 Event Notifications

- S3:ObjectCreated, S3:ObjectRemoved, S3:ObjectRestore, S3:Replication...
- Object name filtering possible (*.jpg)
- Use case: generate thumbnails of images uploaded to S3
- Can create as many “S3 events” as desired
Có thể tạo bao nhiêu S3 events tùy thích
- S3 event notifications typically deliver events in seconds but can sometimes take a minute or longer



Question 398:

A company is building an application on AWS. The application sends logs to an Amazon OpenSearch Service cluster for analysis. All data must be stored within a VPC.

Some of the company's developers work from home. Other developers work from three different company office locations. The developers need to access OpenSearch Service to analyze and visualize logs directly from their local development machines.

Which solution will meet these requirements?

- Configure and set up an AWS Client VPN endpoint. Associate the Client VPN endpoint with a subnet in the VPC. Configure a Client VPN self-service portal. Instruct the developers to connect by using the client for Client VPN.
- Create a transit gateway, and connect it to the VPC. Create an AWS Site-to-Site VPN. Create an attachment to the transit gateway. Instruct the developers to connect by using an OpenVPN client.

C. Create a transit gateway, and connect it to the VPC. Order an AWS Direct Connect connection. Set up a public VIF on the Direct Connect connection. Associate the public VIF with the transit gateway. Instruct the developers to connect to the Direct Connect connection.

D. Create and configure a bastion host in a public subnet of the VPC. Configure the bastion host security group to allow SSH access from the company CIDR ranges. Instruct the developers to connect by using SSH.

A

B. Site-to-Site VPN: Designed for connecting entire networks, not individual devices, and requires VPN hardware/software at each office location.

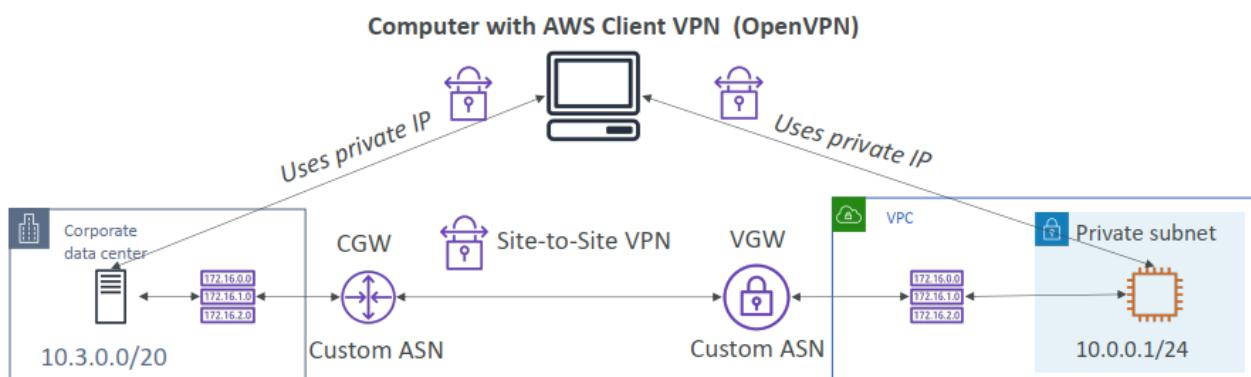
C. Direct Connect: Primarily for high-bandwidth, low-latency connections between on-premises networks and AWS, not individual developer access.

D. Bastion Host: While providing access, it introduces a potential security risk by exposing a public-facing host and requires developers to learn SSH.

AWS Client VPN



- Connect from your computer using OpenVPN to your private network in AWS and on-premises



Question 399:

A company wants to migrate its website from an on-premises data center onto AWS. At the same time, it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege.

A solutions architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster.

What steps are required after the deployment to meet the requirements? (Choose two.)

- A. Create tasks using the bridge network mode.
- B. Create tasks using the awsvpc network mode.
- C. Apply security groups to Amazon EC2 instances, and use IAM roles for EC2 instances to access other resources.
- D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources.
- E. Apply security groups to the tasks, and use IAM roles for tasks to access other resources.

B, E

Amazon ECS – Security & Networking

- You can inject secrets and configurations as Environment Variables into running Docker containers
 - Integration with [SSM Parameter Store](#) and [Secrets Manager](#)
- ECS Tasks Networking
 - **none** – no network connectivity, no port mappings
 - **bridge** – uses Docker's virtual container-based network
 - **host** – bypass Docker's network, uses the underlying host network interface
 - **awsvpc**
 - Every task launched on the instance gets its own ENI and a private IP address
 - Simplified networking, enhanced security, Security Groups, monitoring, VPC Flow Logs
 - Default mode for Fargate tasks

Question 400:

A company is running a serverless application that consists of several AWS Lambda functions and Amazon DynamoDB tables. The company has created new functionality that requires the Lambda functions to access an Amazon Neptune DB cluster. The Neptune DB cluster is located in three subnets in a VPC.

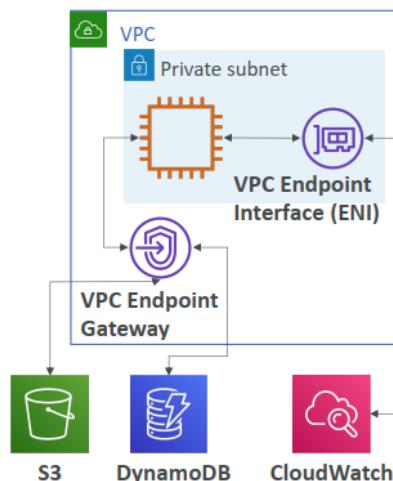
Which of the possible solutions will allow the Lambda functions to access the Neptune DB cluster and DynamoDB tables? (Choose two.)

- A. Create three public subnets in the Neptune VPC, and route traffic through an internet gateway. Host the Lambda functions in the three new public subnets.
- B. Create three private subnets in the Neptune VPC, and route internet traffic through a NAT gateway. Host the Lambda functions in the three new private subnets.
- C. Host the Lambda functions outside the VPC. Update the Neptune security group to allow access from the IP ranges of the Lambda functions.
- D. Host the Lambda functions outside the VPC. Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint.
- E. Create three private subnets in the Neptune VPC. Host the Lambda functions in the three new isolated subnets. Create a VPC endpoint for DynamoDB, and route DynamoDB traffic to the VPC endpoint.

B, E

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in yourVPC
 - Check Route Tables



Question 401:

A company wants to design a disaster recovery (DR) solution for an application that runs in the company's data center. The application writes to an SMB file share and creates a copy on a second file share. Both file shares are in the data center. The application uses two types of files: metadata files and image files.

The company wants to store the copy on AWS. The company needs the ability to use SMB to access the data from either the data center or AWS if a disaster occurs. The copy of the data is rarely accessed but must be available within 5 minutes.

- A. Deploy AWS Outposts with Amazon S3 storage. Configure a Windows Amazon EC2 instance on Outposts as a file server.
- B. Deploy an Amazon FSx File Gateway. Configure an Amazon FSx for Windows File Server Multi-AZ file system that uses SSD storage.

C. Deploy an Amazon S3 File Gateway. Configure the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and to use S3 Glacier Deep Archive for the image files.

D. Deploy an Amazon S3 File Gateway. Configure the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and image files.

D

S3 Storage Classes – Infrequent Access

- For data that is less frequently accessed, but requires rapid access when needed
- Lower cost than S3 Standard

Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

- 99.9% Availability
- Use cases: Disaster Recovery, backups



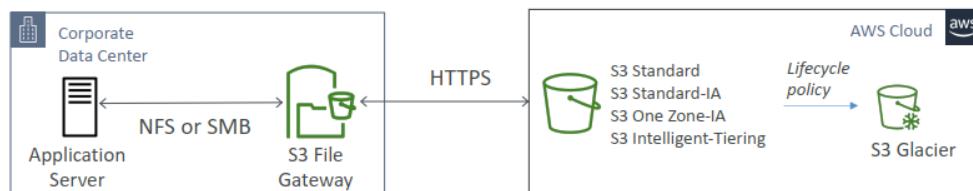
Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

- High durability (99.99999999%) in a single AZ; data lost when AZ is destroyed
- 99.5% Availability
- Use Cases: Storing secondary backup copies of on-premise data, or data you can recreate



Amazon S3 File Gateway

- Configured S3 buckets are accessible using the NFS and SMB protocol
- Most recently used data is cached in the file gateway
- Supports S3 Standard, S3 Standard IA, S3 One Zone A, S3 Intelligent-Tiering
- Transition to S3 Glacier using a Lifecycle Policy
- Bucket access using IAM roles for each File Gateway
- SMB Protocol has integration with Active Directory (AD) for user authentication



Question 402:

A company is creating a solution that can move 400 employees into a remote working environment in the event of an unexpected disaster. The user desktops have a mix of Windows and Linux operating systems. Multiple types of software, such as web browsers and mail clients, are installed on each desktop.

A solutions architect needs to implement a solution that can be integrated with the company's on-premises Active Directory to allow employees to use their existing identity credentials. The solution must provide multifactor authentication (MFA) and must replicate the user experience from the existing desktops.

Which solution will meet these requirements?

- A. Use Amazon WorkSpaces for the cloud desktop service. Set up a VPN connection to the on-premises network. Create an AD Connector, and connect to the on-premises Active Directory. Activate MFA for Amazon WorkSpaces by using the AWS Management Console.
- B. Use Amazon AppStream 2.0 as an application streaming service. Configure Desktop View for the employees. Set up a VPN connection to the on-premises network. Set up Active Directory Federation Services (AD FS) on premises. Connect the VPC network to AD FS through the VPN connection.
- C. Use Amazon WorkSpaces for the cloud desktop service. Set up a VPN connection to the on-premises network. Create an AD Connector, and connect to the on-premises Active Directory. Configure a RADIUS server for MFA.
- D. Use Amazon AppStream 2.0 as an application streaming service. Set up Active Directory Federation Services on premises. Configure MFA to grant users access on AppStream 2.0.

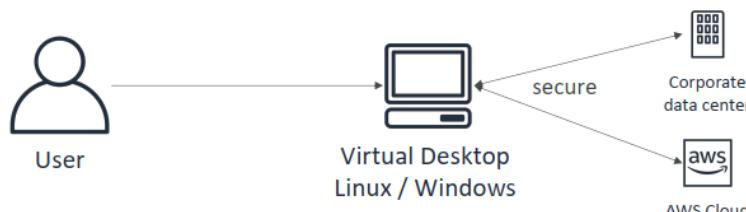
C

LAB: <https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/>

Amazon WorkSpaces



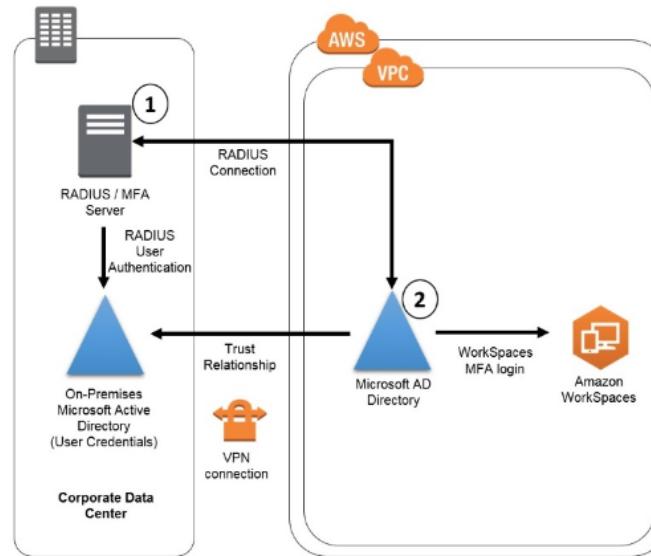
- Managed, Secure Cloud Desktop
- Great to eliminate management of on-premises VDI (Virtual Desktop Infrastructure)
- Pricing is either on-demand (pay per hour) or monthly subscription
- Secure, Encrypted, Network Isolation
- Integrated with Microsoft Active Directory



Amazon WorkSpaces

- WorkSpaces Application Manager (WAM)
 - Deploy and Manage applications as virtualized application containers
 - Provision at scale, and keep the applications updated using WAM
- Windows Updates
 - By default, Amazon Workspaces are configured to install software updates
 - Amazon WorkSpaces with Windows will have Windows Update turned on
 - You have full control over the Windows Update frequency
- Maintenance Windows
 - Updates are installed during maintenance windows (you define them)
 - Always On WorkSpaces: default is from 00h00 to 04h00 on Sunday morning
 - AutoStop WorkSpaces: automatically starts once a month to install updates
 - Manual maintenance: you define your windows and perform maintenance

Amazon WorkSpaces with On-Premises Credentials



Question 403:

A company has deployed an Amazon Connect contact center. Contact center agents are reporting large numbers of computer-generated calls. The company is concerned about the cost and productivity effects of these calls. The company wants a solution that will allow agents to flag the call as spam and automatically block the numbers from going to an agent in the future.

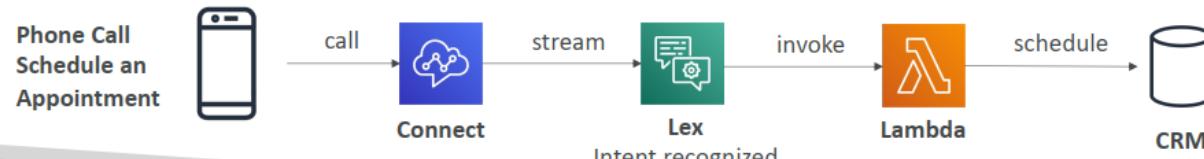
What is the MOST operationally efficient solution to meet these requirements?

- Customize the Contact Control Panel (CCP) by adding a flag call button that will invoke an AWS Lambda function that calls the `UpdateContactAttributes` API. Use an Amazon DynamoDB table to store the spam numbers. Modify the contact flows to look for the updated attribute and to use a Lambda function to read and write to the DynamoDB table.
- Use a Contact Lens for Amazon Connect rule that will look for spam calls. Use an Amazon DynamoDB table to store the spam numbers. Modify the contact flows to look for the rule and to invoke an AWS Lambda function to read and write to the DynamoDB table.
- Use an Amazon DynamoDB table to store the spam numbers. Create a quick connect that the agents can transfer the spam call to from the Contact Control Panel (CCP). Modify the quick connect contact flow to invoke an AWS Lambda function to write to the DynamoDB table.
- Modify the initial contact flow to ask for caller input. If the agent does not receive input, the agent should mark the caller as spam. Use an Amazon DynamoDB table to store the spam numbers. Use an AWS Lambda function to read and write to the DynamoDB table.

A

Amazon Lex & Connect

- Amazon Lex: (same technology that powers Alexa)
 - Automatic Speech Recognition (ASR) to convert speech to text
 - Natural Language Understanding to recognize the intent of text, callers
 - Helps build chatbots, call center bots
- Amazon Connect:
 - Receive calls, create contact flows, cloud-based virtual contact center
 - Can integrate with other CRM systems or AWS
 - No upfront payments, 80% cheaper than traditional contact center solutions



Create a Lambda function to store spam /denied numbers in the DynamDB table. Create a second Lambda function to check the table against any incoming number and take appropriate action.

<https://repost.aws/knowledge-center/connect-deny-list-numbers>

Question 404:

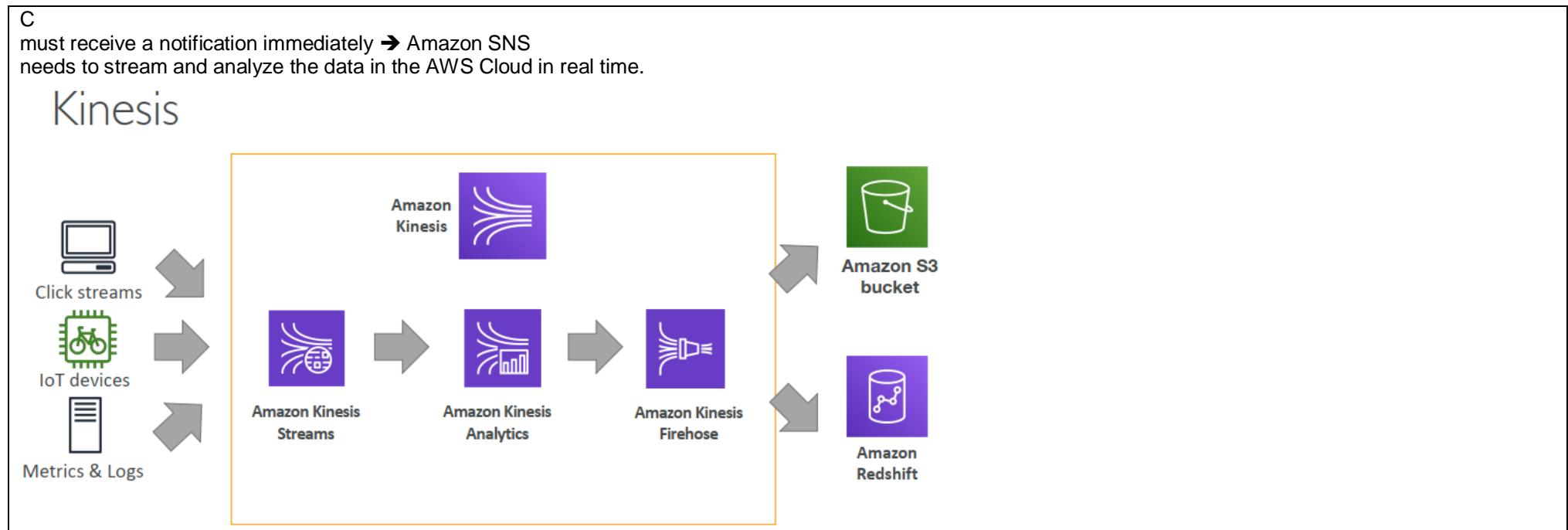
A company has mounted sensors to collect information about environmental parameters such as humidity and light throughout all the company's factories. The company needs to stream and analyze the data in the AWS Cloud in real time. If any of the parameters fall out of acceptable ranges, the factory operations team must receive a notification immediately.

Which solution will meet these requirements?

- Stream the data to an Amazon Kinesis Data Firehose delivery stream. Use AWS Step Functions to consume and analyze the data in the Kinesis Data Firehose delivery stream. Use Amazon Simple Notification Service (Amazon SNS) to notify the operations team.
- Stream the data to an Amazon Managed Streaming for Apache Kafka (Amazon MSK) cluster. Set up a trigger in Amazon MSK to invoke an AWS Fargate task to analyze the data. Use Amazon Simple Email Service (Amazon SES) to notify the operations team.

C. Stream the data to an Amazon Kinesis data stream. Create an AWS Lambda function to consume the Kinesis data stream and to analyze the data. Use Amazon Simple Notification Service (Amazon SNS) to notify the operations team.

D. Stream the data to an Amazon Kinesis Data Analytics application. Use an automatically scaled and containerized service in Amazon Elastic Container Service (Amazon ECS) to consume and analyze the data. Use Amazon Simple Email Service (Amazon SES) to notify the operations team.



Question 405:

A company is preparing to deploy an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for a workload. The company expects the cluster to support an unpredictable number of stateless pods. Many of the pods will be created during a short time period as the workload automatically scales the number of replicas that the workload uses.

Which solution will MAXIMIZE node resilience?

- A. Use a separate launch template to deploy the EKS control plane into a second cluster that is separate from the workload node groups.
- B. Update the workload node groups. Use a smaller number of node groups and larger instances in the node groups.
- C. Configure the Kubernetes Cluster Autoscaler to ensure that the compute capacity of the workload node groups stays underprovisioned.
- D. Configure the workload to use topology spread constraints that are based on Availability Zone.

D
MAXIMIZE node resilience → Multi AZ
LAB: <https://aws.amazon.com/blogs/containers/getting-visibility-into-your-amazon-eks-cross-az-pod-to-pod-network-bytes/>

Question 406:

A company needs to implement a disaster recovery (DR) plan for a web application. The application runs in a single AWS Region.

The application uses microservices that run in containers. The containers are hosted on AWS Fargate in Amazon Elastic Container Service (Amazon ECS). The application has an Amazon RDS for MySQL DB instance as its data layer and uses Amazon Route 53 for DNS resolution. An Amazon CloudWatch alarm invokes an Amazon EventBridge rule if the application experiences a failure.

A solutions architect must design a DR solution to provide application recovery to a separate Region. The solution must minimize the time that is necessary to recover from a failure.

Which solution will meet these requirements?

A. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Create an AWS Lambda function to perform the following actions: take a snapshot of the RDS DB instance, copy the snapshot to the separate Region, create a new RDS DB instance from the snapshot, and update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.

B. Create an AWS Lambda function that creates a second ECS cluster and ECS service in the separate Region. Configure the Lambda function to perform the following actions: take a snapshot of the RDS DB instance, copy the snapshot to the separate Region, create a new RDS DB instance from the snapshot, and update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.

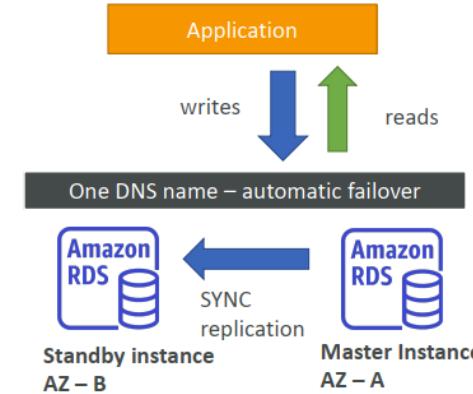
C. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Create a cross-Region read replica of the RDS DB instance in the separate Region. Create an AWS Lambda function to promote the read replica to the primary database. Configure the Lambda function to update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.

D. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Take a snapshot of the RDS DB instance. Convert the snapshot to an Amazon DynamoDB global table. Create an AWS Lambda function to update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.

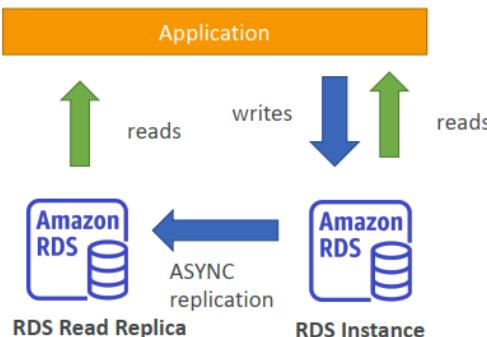
C
Configure RDS read-replica instead of Snapshots. Invoke Lambda function to promote read-replica to primary and update Route53 to point to secondary region incase of DR

RDS – Multi AZ & Read Replicas

- Multi-AZ: Standby instance for failover in case of outage



- Read Replicas: Increase read throughput. Eventual consistency. Can be cross-region



Question 407:

A company has AWS accounts that are in an organization in AWS Organizations. The company wants to track Amazon EC2 usage as a metric. The company's architecture team must receive a daily alert if the EC2 usage is more than 10% higher than the average EC2 usage from the last 30 days.

Which solution will meet these requirements?

- Configure AWS Budgets in the organization's management account. Specify a usage type of EC2 running hours. Specify a daily period. Set the budget amount to be 10% more than the reported average usage for the last 30 days from AWS Cost Explorer. Configure an alert to notify the architecture team if the usage threshold is met.
- Configure AWS Cost Anomaly Detection in the organization's management account. Configure a monitor type of AWS Service. Apply a filter of Amazon EC2. Configure an alert subscription to notify the architecture team if the usage is 10% more than the average usage for the last 30 days.
- Enable AWS Trusted Advisor in the organization's management account. Configure a cost optimization advisory alert to notify the architecture team if the EC2 usage is 10% more than the reported average usage for the last 30 days.
- Configure Amazon Detective in the organization's management account. Configure an EC2 usage anomaly alert to notify the architecture team if Detective identifies a usage anomaly of more than 10%.

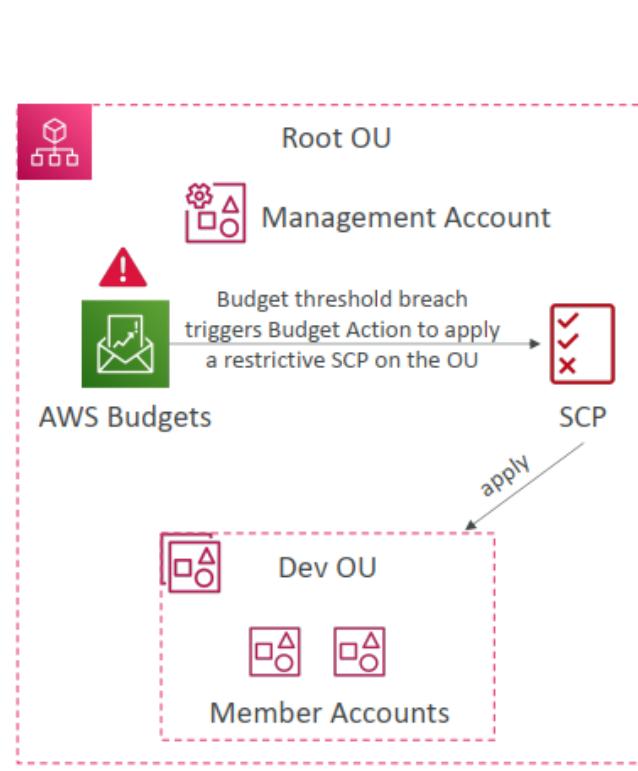
A
LAB: <https://aws.amazon.com/blogs/aws-cloud-financial-management/launch-daily-cost-and-usage-budgets/>

steps to set up an AWS Budget to track EC2 usage and receive an alert if it's more than 10% higher than the average usage from the last 30 days: Go to the AWS Management Console |Open the "Budgets" service |Create a New Budget:|Choose "Cost budget" as the budget type.|Choose the time period for the budget (e.g., Monthly).|Set the start and end dates for the budget. Configure Cost and Usage Details:|Choose the "Cost and usage" option.|Specify the "Service" as "Amazon EC2" to focus on EC2 costs.|Choose the "Usage type" as "Usage Quantity."|Set Budgeted Amount:|Set the budgeted amount to be 110% of the average EC2 usage from the last 30 days. Configure Alerts:|Enable the alert threshold.|Set the alert threshold to be "Actual > Forecasted" and "More than 0%" to be alerted when the actual usage exceeds the forecast.

Budget Actions

Thay đổi bạn thực hiện các hành động khi vượt quá budget hoặc vượt quá nồng độ sử dụng

- Run actions on your behalf when a budget exceeds a certain cost or usage threshold
- Supports 3 action types:
 - Applying an IAM Policy to a user, group, or IAM role
 - Applying Service Control Policy (SCP) to an OU
 - Stop EC2 or RDS Instances
- Actions can be executed automatically or require a workflow approval process
- Reduces unintentional overspending in your account



Question 408:

An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a solutions architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during marketing campaigns to process the orders with minimal delays.

Which of the following is the MOST reliable approach to meet the requirements?

- A. Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.

- B. Receive the orders in an Amazon SQS queue and invoke an AWS Lambda function to process them.
- C. Receive the orders using the AWS Step Functions program and launch an Amazon ECS container to process them.
- D. Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.

B

The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. For now, it just processes one order and send info to Dynamo. Loosely coupled = SQS - Lambda is also the simplest to use

Amazon SQS



- Serverless, managed queue, integrated with IAM
- Can handle extreme scale, no provisioning required
- Used to **decouple** services
- Message size of max 256 KB (use a pointer to S3 for large messages)
- Can be read from EC2 (optional ASG), Lambda
- SQS could be used as a write buffer for DynamoDB
- **SQS FIFO:**
 - receive messages in order they were sent Nhận message theo thứ tự được gửi
 - 300 messages/s without batching, 3000 /s with batching

Question 409:

A company is deploying AWS Lambda functions that access an Amazon RDS for PostgreSQL database. The company needs to launch the Lambda functions in a QA environment and in a production environment.

The company must not expose credentials within application code and must rotate passwords automatically.

Which solution will meet these requirements?

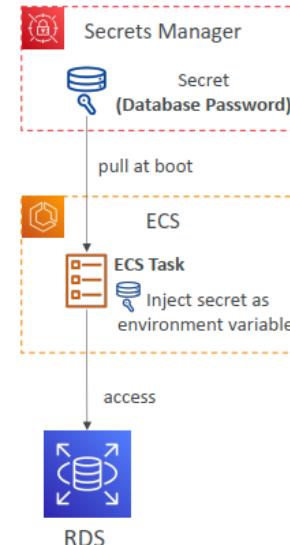
- A. Store the database credentials for both environments in AWS Systems Manager Parameter Store. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Within the application code of the Lambda functions, pull the credentials from the Parameter Store parameter by using the AWS SDK for Python (Boto3). Add a role to the Lambda functions to provide access to the Parameter Store parameter.
- B. Store the database credentials for both environments in AWS Secrets Manager with distinct key entry for the QA environment and the production environment. Turn on rotation. Provide a reference to the Secrets Manager key as an environment variable for the Lambda functions.
- C. Store the database credentials for both environments in AWS Key Management Service (AWS KMS). Turn on rotation. Provide a reference to the credentials that are stored in AWS KMS as an environment variable for the Lambda functions.
- D. Create separate S3 buckets for the QA environment and the production environment. Turn on server-side encryption with AWS KMS keys (SSE-KMS) for the S3 buckets. Use an object naming pattern that gives each Lambda function's application code the ability to pull the correct credentials for the function's corresponding environment. Grant each Lambda function's execution role access to Amazon S3.

B

must rotate passwords automatically → AWS Secrets Manager

AWS Secrets Manager

- Meant for storing secrets (e.g., passwords, API keys, ...)
- Capability to force **rotation of secrets** every X days
 - Automate generation of secrets on rotation (uses Lambda)
 - Natively supports Amazon RDS (all supported DB engines), Redshift, DocumentDB
 - Support other databases and services (custom Lambda function)
- Control access to secrets using Resource-based Policy
- Integration with other AWS services to natively pull secrets from Secrets Manager: CloudFormation, CodeBuild, ECS, EMR, Fargate, EKS, Parameter Store...



Question 410:

A company is using AWS Control Tower to manage AWS accounts in an organization in AWS Organizations. The company has an OU that contains accounts. The company must prevent any new or existing Amazon EC2 instances in the OU's accounts from gaining a public IP address.

Which solution will meet these requirements?

- A. Configure all instances in each account in the OU to use AWS Systems Manager. Use a Systems Manager Automation runbook to prevent public IP addresses from being attached to the instances.
- B. Implement the AWS Control Tower proactive control to check whether instances in the OU's accounts have a public IP address. Set the AssociatePublicIpAddress property to False. Attach the proactive control to the OU.
- C. Create an SCP that prevents the launch of instances that have a public IP address. Additionally, configure the SCP to prevent the attachment of a public IP address to existing instances. Attach the SCP to the OU.
- D. Create an AWS Config custom rule that detects instances that have a public IP address. Configure a remediation action that uses an AWS Lambda function to detach the public IP addresses from the instances.

C

AWS Control Tower



- Easy way to set up and govern a secure and compliant multi-account AWS environment based on best practices
- Benefits:
 - Automate the set up of your environment in a few clicks
tự động hóa quản lý chính sách liên tục
 - Automate ongoing policy management using guardrails
 - Detect policy violations and remediate them
 - Monitor compliance through an interactive dashboard
- AWS Control Tower runs on top of AWS Organizations:
 - It automatically sets up AWS Organizations to organize accounts and implement SCPs (Service Control Policies)

Question 411:

A company is deploying a third-party web application on AWS. The application is packaged as a Docker image. The company has deployed the Docker image as an AWS Fargate service in Amazon Elastic Container Service (Amazon ECS). An Application Load Balancer (ALB) directs traffic to the application.

The company needs to give only a specific list of users the ability to access the application from the internet. The company cannot change the application and cannot integrate the application with an identity provider. All users must be authenticated through multi-factor authentication (MFA).

Which solution will meet these requirements?

- A. Create a user pool in Amazon Cognito. Configure the pool for the application. Populate the pool with the required users. Configure the pool to require MFA. Configure a listener rule on the ALB to require authentication through the Amazon Cognito hosted UI.
- B. Configure the users in AWS Identity and Access Management (IAM). Attach a resource policy to the Fargate service to require users to use MFA. Configure a listener rule on the ALB to require authentication through IAM.
- C. Configure the users in AWS Identity and Access Management (IAM). Enable AWS IAM Identity Center (AWS Single Sign-On). Configure resource protection for the ALB. Create a resource protection rule to require users to use MFA.
- D. Create a user pool in AWS Amplify. Configure the pool for the application. Populate the pool with the required users. Configure the pool to require MFA. Configure a listener rule on the ALB to require authentication through the Amplify hosted UI.

A

ALB authentication only integration with: Cognito AWS_IAM Lambda authorizer

Question 412:

A solutions architect is preparing to deploy a new security tool into several previously unused AWS Regions. The solutions architect will deploy the tool by using an AWS CloudFormation stack set. The stack set's template contains an IAM role that has a custom name. Upon creation of the stack set, no stack instances are created successfully.

What should the solutions architect do to deploy the stacks successfully?

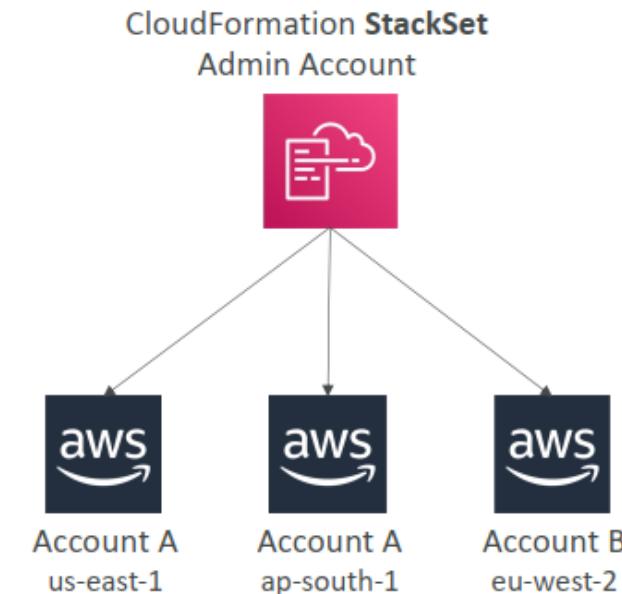
- A. Enable the new Regions in all relevant accounts. Specify the CAPABILITY_NAMED_IAM capability during the creation of the stack set.
- B. Use the Service Quotas console to request a quota increase for the number of CloudFormation stacks in each new Region in all relevant accounts. Specify the CAPABILITY_IAM capability during the creation of the stack set.
- C. Specify the CAPABILITY_NAMED_IAM capability and the SELF_MANAGED permissions model during the creation of the stack set.
- D. Specify an administration role ARN and the CAPABILITY_IAM capability during the creation of the stack set.

A

https://docs.aws.amazon.com/AWSCloudFormation/latest/APIReference/API_CreateStack.html

CloudFormation – StackSets

- Create, update, or delete stacks across multiple accounts and regions with a single operation
- Administrator account to create StackSets
- Trusted accounts to create, update, delete stack instances from StackSets
- When you update a stack set, *all* associated stack instances are updated throughout all accounts and regions
- Enable **Automatic Deployment** feature to automatically deploy to accounts in AWS Organization or OUs



In some cases, you must explicitly acknowledge that your stack template contains certain capabilities in order for AWS CloudFormation to create the stack.

CAPABILITY_IAM and CAPABILITY_NAMED_IAM

Some stack templates might include resources that can affect permissions in your AWS account; for example, by creating new AWS Identity and Access Management (IAM) users. For those stacks, you must explicitly acknowledge this by specifying one of these capabilities.

The following IAM resources require you to specify either the CAPABILITY_IAM or CAPABILITY_NAMED_IAM capability.

- If you have IAM resources, you can specify either capability.
- If you have IAM resources with custom names, you must specify CAPABILITY_NAMED_IAM.
- If you don't specify either of these capabilities, AWS CloudFormation returns an InsufficientCapabilities error.

Question 413:

A company has an application that uses an Amazon Aurora PostgreSQL DB cluster for the application's database. The DB cluster contains one small primary instance and three larger replica instances. The application runs on an AWS Lambda function. The application makes many short-lived connections to the database's replica instances to perform read-only operations.

During periods of high traffic, the application becomes unreliable and the database reports that too many connections are being established. The frequency of high-traffic periods is unpredictable.

Which solution will improve the reliability of the application?

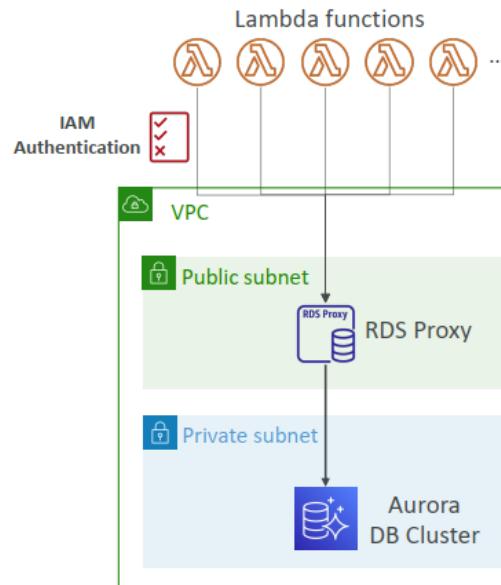
- A. Use Amazon RDS Proxy to create a proxy for the DB cluster. Configure a read-only endpoint for the proxy. Update the Lambda function to connect to the proxy endpoint.
- B. Increase the max_connections setting on the DB cluster's parameter group. Reboot all the instances in the DB cluster. Update the Lambda function to connect to the DB cluster endpoint.
- C. Configure instance scaling for the DB cluster to occur when the DatabaseConnections metric is close to the max connections setting. Update the Lambda function to connect to the Aurora reader endpoint.
- D. Use Amazon RDS Proxy to create a proxy for the DB cluster. Configure a read-only endpoint for the Aurora Data API on the proxy. Update the Lambda function to connect to the proxy endpoint.

A

D is incorrect because RDS Data API is used with Aurora Serverless

RDS Proxy for AWS Lambda

- When using Lambda functions with RDS, it opens and maintains a database connection
- This can result in a “**TooManyConnections**” exception
- With **RDS Proxy**, you no longer need code that handles cleaning up idle connections and managing connection pools
- Supports IAM authentication or DB authentication, auto-scaling
- The Lambda function must have connectivity to the Proxy (public proxy => public Lambda, private proxy => Lambda in VPC)



Question 414:

A retail company is mounting IoT sensors in all of its stores worldwide. During the manufacturing of each sensor, the company's private certificate authority (CA) issues an X.509 certificate that contains a unique serial number. The company then deploys each certificate to its respective sensor.

A solutions architect needs to give the sensors the ability to send data to AWS after they are installed. Sensors must not be able to send data to AWS until they are installed.

Which solution will meet these requirements?

- A. Create an AWS Lambda function that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Add the Lambda function as a pre-provisioning hook. During manufacturing, call the RegisterThing API operation and specify the template and parameters.
- B. Create an AWS Step Functions state machine that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Specify the Step Functions state machine to validate parameters. Call the StartThingRegistrationTask API operation during installation.
- C. Create an AWS Lambda function that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Add the Lambda function as a pre-provisioning hook. Register the CA with AWS IoT Core, specify the provisioning template, and set the allow-auto-registration parameter.
- D. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Include parameter validation in the template. Provision a claim certificate and a private key for each device that uses the CA. Grant AWS IoT Core service permissions to update AWS IoT things during provisioning.

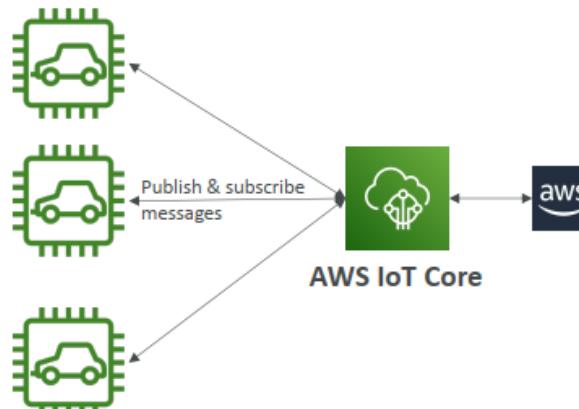
C

<https://docs.aws.amazon.com/iot/latest/developerguide/iot-provision.html>

AWS IoT Core



- IoT stands for “Internet of Things” – the network of internet-connected devices that are able to collect and transfer data
- AWS IoT Core allows you to easily connect IoT devices to the AWS Cloud
- Serverless, secure & scalable to billions of devices and trillions of messages
- Integrates with a lot of AWS services (Lambda, S3, SageMaker, etc.)
- Build IoT applications that gather, process, analyze, and act on data



Question 415:

A startup company recently migrated a large ecommerce website to AWS. The website has experienced a 70% increase in sales. Software engineers are using a private GitHub repository to manage code. The DevOps team is using Jenkins for builds and unit testing. The engineers need to receive notifications for bad builds and zero downtime during deployments. The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue.

The software engineers have decided to use AWS CodePipeline to manage their build and deployment process.

Which solution will meet these requirements?

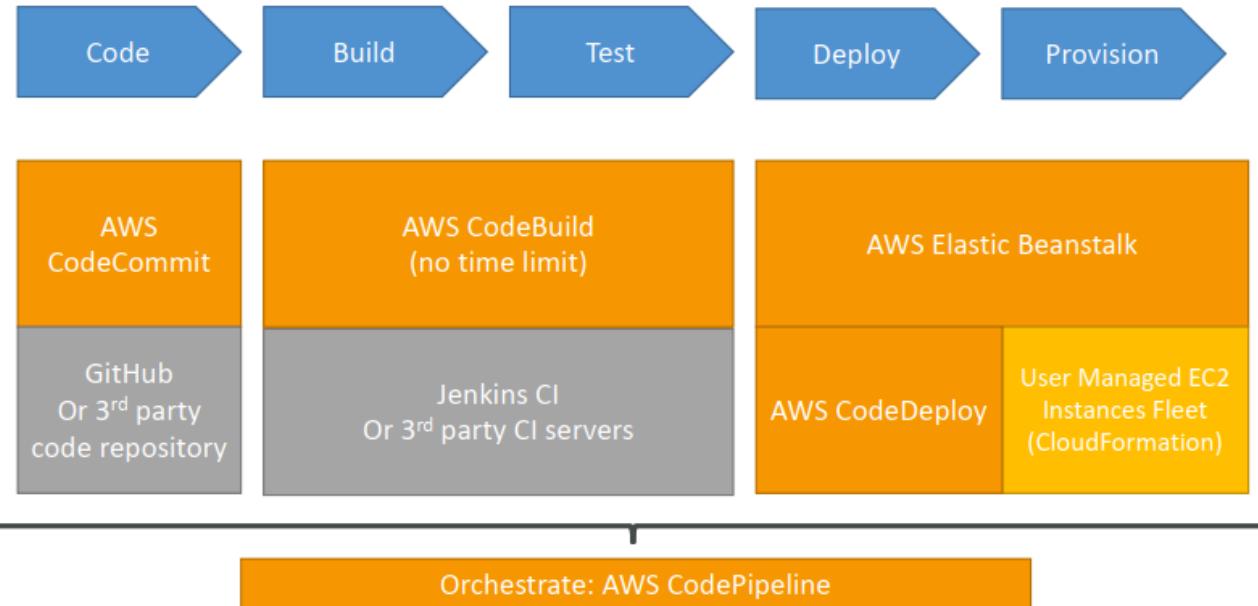
- A. Use GitHub websockets to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.
- B. Use GitHub webhooks to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.
- C. Use GitHub websockets to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.

D. Use GitHub webhooks to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.

B

LAB: <https://aws.amazon.com/blogs/devops/setting-up-a-ci-cd-pipeline-by-integrating-jenkins-with-aws-codebuild-and-aws-codedeploy/>

Technology Stack for CICD



Question 416:

A software as a service (SaaS) company has developed a multi-tenant environment. The company uses Amazon DynamoDB tables that the tenants share for the storage layer. The company uses AWS Lambda functions for the application services.

The company wants to offer a tiered subscription model that is based on resource consumption by each tenant. Each tenant is identified by a unique tenant ID that is sent as part of each request to the Lambda functions. The company has created an AWS Cost and Usage Report (AWS CUR) in an AWS account. The company wants to allocate the DynamoDB costs to each tenant to match that tenant's resource consumption.

Which solution will provide a granular view of the DynamoDB cost for each tenant with the LEAST operational effort?

A. Associate a new tag that is named tenant ID with each table in DynamoDB. Activate the tag as a cost allocation tag in the AWS Billing and Cost Management console. Deploy new Lambda function code to log the tenant ID in Amazon CloudWatch Logs. Use the AWS CUR to separate DynamoDB consumption cost for each tenant ID.

B. Configure the Lambda functions to log the tenant ID and the number of RCU and WCU consumed from DynamoDB for each transaction to Amazon CloudWatch Logs. Deploy another Lambda function to calculate the tenant costs by using the logged capacity units and the overall DynamoDB cost from the AWS Cost Explorer API. Create an Amazon EventBridge rule to invoke the calculation Lambda function on a schedule.

C. Create a new partition key that associates DynamoDB items with individual tenants. Deploy a Lambda function to populate the new column as part of each transaction. Deploy another Lambda function to calculate the tenant costs by using Amazon Athena to calculate the number of tenant items from DynamoDB and the overall DynamoDB cost from the AWS CUR. Create an Amazon EventBridge rule to invoke the calculation Lambda function on a schedule.

D. Deploy a Lambda function to log the tenant ID, the size of each response, and the duration of the transaction call as custom metrics to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the custom metrics for each tenant. Use AWS Pricing Calculator to obtain the overall DynamoDB costs and to calculate the tenant costs.

B

LEAST operational effort → AWS Cost Explorer

<https://aws.amazon.com/blogs/apn/optimizing-cost-per-tenant-visibility-in-saas-solutions/>



Cost Explorer

- Visualize, understand, and manage your AWS costs and usage over time
- Create custom reports that analyze cost and usage data.
- Analyze your data at a high level: total costs and usage across all accounts
- Or Monthly, hourly, resource level granularity
- Choose an optimal Savings Plan (to lower prices on your bill)
- Forecast usage up to 12 months based on previous usage

Question 417:

A company has an application that stores data in a single Amazon S3 bucket. The company must keep all data for 1 year. The company's security team is concerned that an attacker could gain access to the AWS account through leaked long-term credentials.

Which solution will ensure that existing and future objects in the S3 bucket are protected?

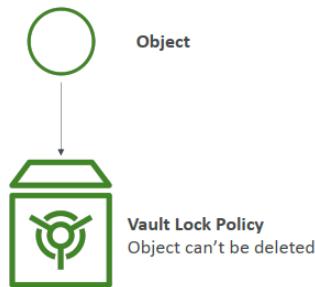
- A. Create a new AWS account that is accessible only to the security team through an assumed role. Create an S3 bucket in the new account. Enable S3 Versioning and S3 Object Lock. Configure a default retention period of 1 year. Set up replication from the existing S3 bucket to the new S3 bucket. Create an S3 Batch Replication job to copy all existing data.
- B. Use the s3-bucket-versioning-enabled AWS Config managed rule. Configure an automatic remediation action that uses an AWS Lambda function to enable S3 Versioning and MFA Delete on noncompliant resources. Add an S3 Lifecycle rule to delete objects after 1 year.
- C. Explicitly deny bucket creation from all users and roles except for an AWS Service Catalog launch constraint role. Define a Service Catalog product for the creation of the S3 bucket to force S3 Versioning and MFA Delete to be enabled. Authorize users to launch the product when they need to create an S3 bucket.
- D. Enable Amazon GuardDuty with the S3 protection feature for the account and the AWS Region. Add an S3 Lifecycle rule to delete objects after 1 year.

A

S3 Object Lock & Glacier Vault Lock

- S3 Object Lock

- Adopt a WORM (Write Once Read Many) model
- Block an object version deletion for a specified amount of time

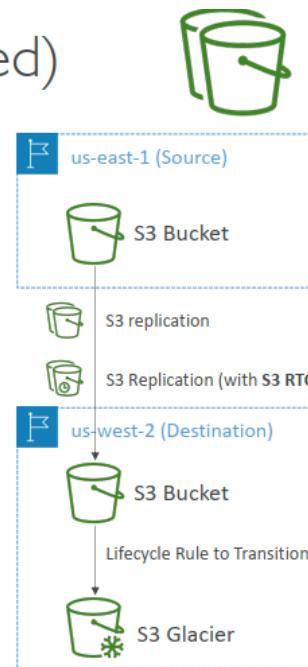


- Glacier Vault Lock

- Adopt a WORM (Write Once Read Many) model
- Lock the policy for future edits (can no longer be changed)
- Helpful for compliance and data retention

S3 – Replication (Versioning enabled)

- Cross Region Replication (CRR)
- Same Region Replication (SRR)
- Combine with Lifecycle Rules
- Helpful to reduce latency, disaster recovery, security
- S3 Replication Time Control (S3 RTC)
 - Replicates most objects that you upload to Amazon S3 in seconds, and 99.99% of those objects within 15 minutes
 - Helpful for compliance, DR, etc..



Question 418:

A company needs to improve the security of its web-based application on AWS. The application uses Amazon CloudFront with two custom origins. The first custom origin routes requests to an Amazon API Gateway HTTP API. The second custom origin routes traffic to an Application Load Balancer (ALB). The application integrates with an OpenID Connect (OIDC) identity provider (IdP) for user management.

A security audit shows that a JSON Web Token (JWT) authorizer provides access to the API. The security audit also shows that the ALB accepts requests from unauthenticated users.

A solutions architect must design a solution to ensure that all backend services respond to only authenticated users.

Which solution will meet this requirement?

- A. Configure the ALB to enforce authentication and authorization by integrating the ALB with the IdP. Allow only authenticated users to access the backend services.
- B. Modify the CloudFront configuration to use signed URLs. Implement a permissive signing policy that allows any request to access the backend services.
- C. Create an AWS WAF web ACL that filters out unauthenticated requests at the ALB level. Allow only authenticated traffic to reach the backend services.
- D. Enable AWS CloudTrail to log all requests that come to the ALB. Create an AWS Lambda function to analyze the logs and block any requests that come from unauthenticated users.

A

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>
<https://trello.com/c/Qr9KTskS/416-authenticate-users-using-an-application-load-balancer>
<https://trello.com/c/n3w8PVXe/435-authenticate-user-using-an-alb-cloudfront>

Question 419:

A company creates an AWS Control Tower landing zone to manage and govern a multi-account AWS environment. The company's security team will deploy preventive controls and detective controls to monitor AWS services across all the accounts. The security team needs a centralized view of the security state of all the accounts.

Which solution will meet these requirements?

- A. From the AWS Control Tower management account, use AWS CloudFormation StackSets to deploy an AWS Config conformance pack to all accounts in the organization.
- B. Enable Amazon Detective for the organization in AWS Organizations. Designate one AWS account as the delegated administrator for Detective.
- C. From the AWS Control Tower management account, deploy an AWS CloudFormation stack set that uses the automatic deployment option to enable Amazon Detective for the organization.
- D. Enable AWS Security Hub for the organization in AWS Organizations. Designate one AWS account as the delegated administrator for Security Hub.

D

<https://aws.amazon.com/blogs/mt/centralized-dashboard-for-aws-config-and-aws-security-hub/>

a centralized view of the security state ➔ AWS Security Hub

AWS Security Hub



- Central security tool to manage security across several AWS accounts and automate security checks
- Integrated dashboards showing current security and compliance status to quickly take actions
- Automatically aggregates alerts in predefined or personal findings formats from various AWS services & AWS partner tools:
Tự động tổng hợp các cảnh báo theo định dạng phát hiện cá nhân hoặc được xác định trước từ nhiều dịch vụ AWS và công cụ của đối tác AWS:
 - Config
 - GuardDuty
 - Inspector
 - Macie
 - IAM Access Analyzer
 - AWS Systems Manager
 - AWS Firewall Manager
 - AWS Health
 - AWS Partner Network Solutions
- Must first enable the AWS Config Service

Amazon Detective



- GuardDuty, Macie, and Security Hub are used to identify potential security issues, or findings
- Sometimes security findings require deeper analysis to isolate the root cause and take action – it's a complex process
- Amazon Detective analyzes, investigates, and quickly identifies the root cause of security issues or suspicious activities (using ML and graphs)
- Automatically collects and processes events from VPC Flow Logs, CloudTrail, GuardDuty and create a unified view
- Produces visualizations with details and context to get to the root cause

Question 420:

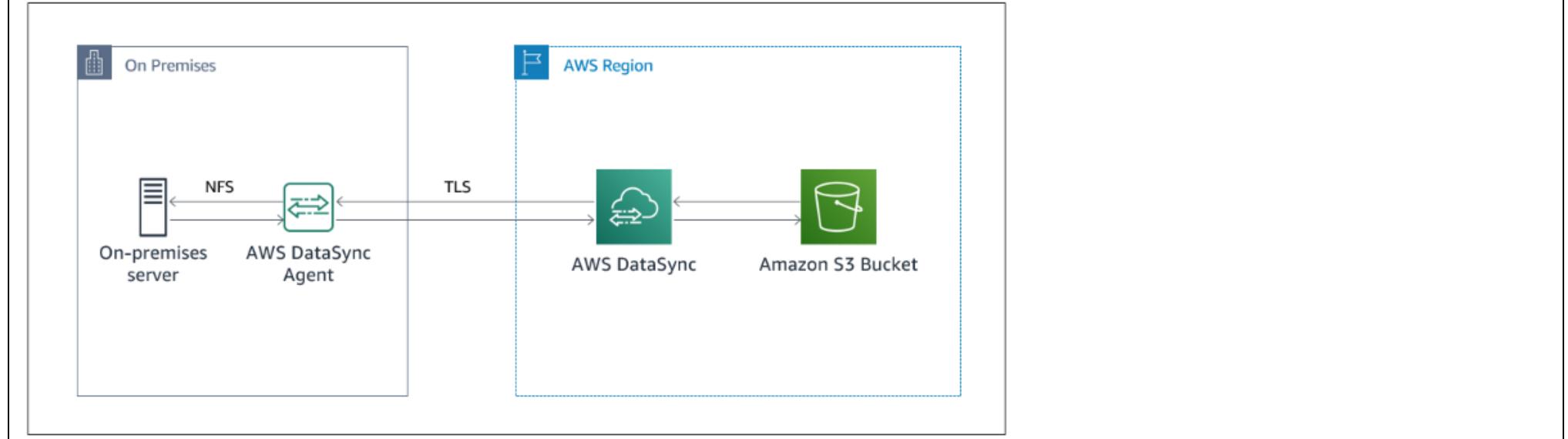
A company that develops consumer electronics with offices in Europe and Asia has 60 TB of software images stored on premises in Europe. The company wants to transfer the images to an Amazon S3 bucket in the ap-northeast-1 Region. New software images are created daily and must be encrypted in transit. The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3.

What is the next step in the transfer process?

- A. Deploy an AWS DataSync agent and configure a task to transfer the images to the S3 bucket.
- B. Configure Amazon Kinesis Data Firehose to transfer the images using S3 Transfer Acceleration.
- C. Use an AWS Snowball device to transfer the images with the S3 bucket as the target.
- D. Transfer the images over a Site-to-Site VPN connection using the S3 API with multipart upload.

A

<https://aws.amazon.com/blogs/storage/synchronizing-your-data-to-amazon-s3-using-aws-datasync/>



Question 421:

A company has a web application that uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. A recent marketing campaign has increased demand. Monitoring software reports that many requests have significantly longer response times than before the marketing campaign.

A solutions architect enabled Amazon CloudWatch Logs for API Gateway and noticed that errors are occurring on 20% of the requests. In CloudWatch, the Lambda function Throttles metric represents 1% of the requests and the Errors metric represents 10% of the requests. Application logs indicate that, when errors occur, there is a call to DynamoDB.

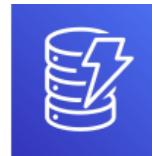
What change should the solutions architect make to improve the current response times as the web application becomes more popular?

- A. Increase the concurrency limit of the Lambda function.
- B. Implement DynamoDB auto scaling on the table.
- C. Increase the API Gateway throttle limit.
- D. Re-create the DynamoDB table with a better-partitioned primary index.

B

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html>

DynamoDB – in short



- NoSQL database, fully managed, massive scale (1,000,000 rps)
- Similar to Apache Cassandra (can migrate to DynamoDB)
- No disk space to provision, max object size is 400 KB
- Capacity: provisioned (WCU, RCU, & Auto Scaling) or on-demand
- Supports CRUD (Create Read Update Delete)
- Read: eventually or strong consistency
- Supports transactions across multiple tables (ACID support)
- Backups available, point in time recovery
- Table classes: Standard and Infrequent Access (IA)

Question 422:

A company has an application that has a web frontend. The application runs in the company's on-premises data center and requires access to file storage for critical data. The application runs on three Linux VMs for redundancy. The architecture includes a load balancer with HTTP request-based routing.

The company needs to migrate the application to AWS as quickly as possible. The architecture on AWS must be highly available.

HANCHE

Which solution will meet these requirements with the FEWEST changes to the architecture?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type in three Availability Zones. Use Amazon S3 to provide file storage for all three containers. Use a Network Load Balancer to direct traffic to the containers.
- B. Migrate the application to Amazon EC2 instances in three Availability Zones. Use Amazon Elastic File System (Amazon EFS) for file storage. Mount the file storage on all three EC2 instances. Use an Application Load Balancer to direct traffic to the EC2 instances.
- C. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) containers that use the Fargate launch type in three Availability Zones. Use Amazon FSx for Lustre to provide file storage for all three containers. Use a Network Load Balancer to direct traffic to the containers.
- D. Migrate the application to Amazon EC2 instances in three AWS Regions. Use Amazon Elastic Block Store (Amazon EBS) for file storage. Enable Cross-Region Replication (CRR) for all three EC2 instances. Use an Application Load Balancer to direct traffic to the EC2 instances.

B
needs to migrate the application to AWS as quickly as possible → A, C are wrong because need containerization code.
AWS must be highly available → multi AZ → B is correct

Question 423:

A company is planning to migrate an on-premises data center to AWS. The company currently hosts the data center on Linux-based VMware VMs. A solutions architect must collect information about network dependencies between the VMs. The information must be in the form of a diagram that details host IP addresses, hostnames, and network connection information.

Which solution will meet these requirements?

- A. Use AWS Application Discovery Service. Select an AWS Migration Hub home AWS Region. Install the AWS Application Discovery Agent on the on-premises servers for data collection. Grant permissions to Application Discovery Service to use the Migration Hub network diagrams.
- B. Use the AWS Application Discovery Service Agentless Collector for server data collection. Export the network diagrams from the AWS Migration Hub in .png format.
- C. Install the AWS Application Migration Service agent on the on-premises servers for data collection. Use AWS Migration Hub data in Workload Discovery on AWS to generate network diagrams.
- D. Install the AWS Application Migration Service agent on the on-premises servers for data collection. Export data from AWS Migration Hub in .csv format into an Amazon CloudWatch dashboard to generate network diagrams.

A
must collect information about network dependencies between the VMs → AWS Application Discovery Service Agent
Agentless can not collect network connection data → B is incorrect

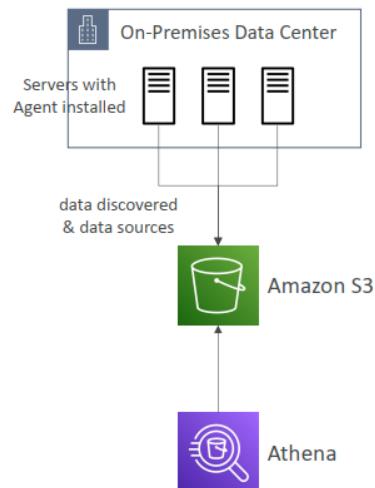
AWS Application Discovery Service



- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping are important for migrations
- **Agentless Discovery (AWS Agentless Discovery Connector)**
 - Open Virtual Appliance (OVA) package that can be deployed to a VMware host
 - VM inventory, configuration, and performance history such as CPU, memory, and disk usage
 - OS agnostic
- **Agent-based Discovery (AWS Application Discovery Agent)**
 - System configuration, system performance, running processes, and details of the network connections between systems
 - Supports Microsoft Server; Amazon Linux, Ubuntu, RedHat, CentOS, SUSE...
- Resulting data can be exported as CSV or viewed within AWS Migration Hub
- Data can be explored using pre-defined queries in Amazon Athena

AWS Application Discovery Service – Migration Hub Data Exploration

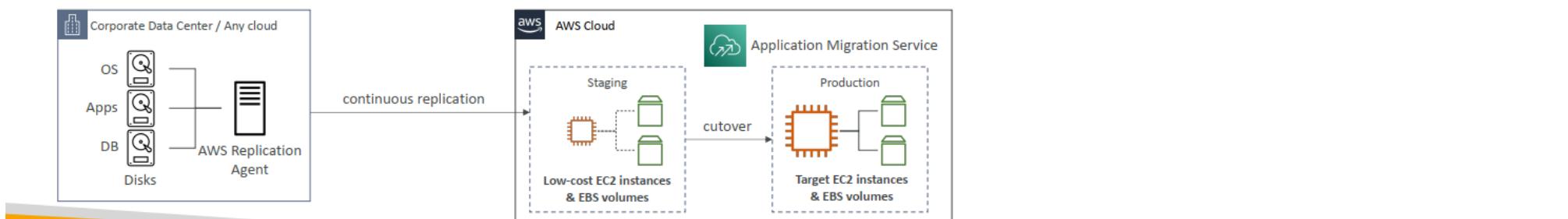
- Allows you to use Amazon Athena to analyze data collected from on-premises servers during discovery
- Data is automatically stored in S3 bucket at regular intervals
- Use Pre-defined or custom queries in Amazon Athena to analyze data
- Example: type of processes running on each server
- Ability to upload additional data sources such as Configuration Management Database (CMDB) exports
- Integrate Athena with QuickSight to visualize data



AWS Application Migration Service (MGN)



- The “AWS evolution” of CloudEndure Migration, replacing AWS Server Migration Service (SMS)
- Lift-and-shift (rehost) solution which simplify **migrating** applications to AWS
- Converts your physical, virtual, and cloud-based servers to run natively on AWS
- Supports wide range of platforms, Operating Systems, and databases
- Minimal downtime, reduced costs



Question 424:

A company runs a software-as-a-service (SaaS) application on AWS. The application consists of AWS Lambda functions and an Amazon RDS for MySQL Multi-AZ database. During market events, the application has a much higher workload than normal. Users notice slow response times during the peak periods because of many database connections. The company needs to improve the scalable performance and availability of the database.

Which solution meets these requirements?

- Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold.
- Migrate the database to Amazon Aurora, and add a read replica. Add a database connection pool outside of the Lambda handler function.
- Migrate the database to Amazon Aurora, and add a read replica. Use Amazon Route 53 weighted records.
- Migrate the database to Amazon Aurora, and add an Aurora Replica. Configure Amazon RDS Proxy to manage database connection pools.

D

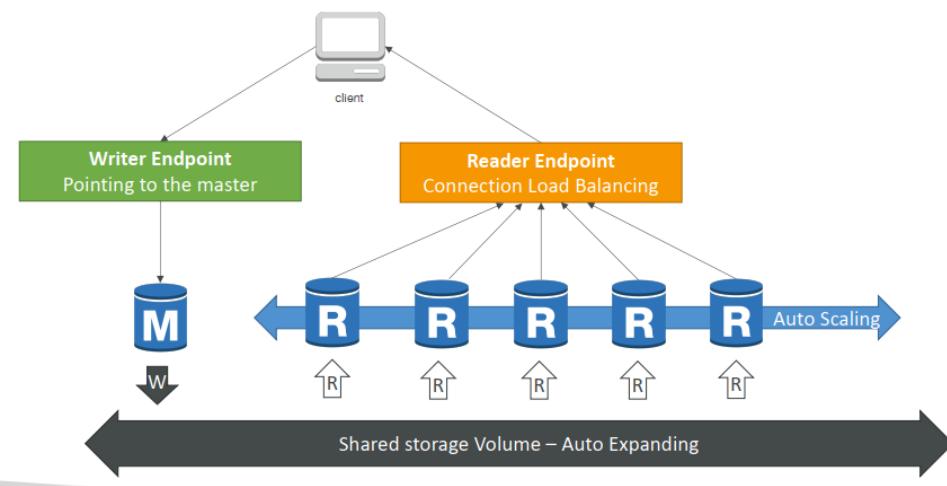
LAB: <https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

Aurora



- DB Engines: PostgreSQL-compatible & MySQL-compatible
- Storage: automatically grows up to 128 TB, 6 copies of data, multi-AZ
- Read Replicas: up to 15 RR, reader endpoint to access them all
- Cross Region RR: entire database is copied (not select tables)
- Load / Offload data directly from / to S3: efficient use of resources
- Backup, Snapshots & Restore: same as RDS

Aurora DB Cluster



Question 425:

A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS. The application data is stored on a shared file system on premises, and the application servers connect to the shared file system through SMB.

A solutions architect must implement a solution that uses an Amazon S3 bucket for shared storage. Until the application is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB. The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data.

Which solution will meet these requirements?

- A. Create a new Amazon FSx for Windows File Server file system. Configure AWS DataSync with one location for the on-premises file share and one location for the new Amazon FSx file system. Create a new DataSync task to copy the data from the on-premises file share location to the Amazon FSx file system.
- B. Create an S3 bucket for the application. Copy the data from the on-premises storage to the S3 bucket.
- C. Deploy an AWS Server Migration Service (AWS SMS) VM to the on-premises environment. Use AWS SMS to migrate the file storage server from on premises to an Amazon EC2 instance.
- D. Create an S3 bucket for the application. Deploy a new AWS Storage Gateway file gateway on an on-premises VM. Create a new file share that stores data in the S3 bucket and is associated with the file gateway. Copy the data from the on-premises storage to the new file gateway endpoint.

D

<https://trello.com/c/mOBOJAJ5/406-aws-storage-gateway-vs-datasync>

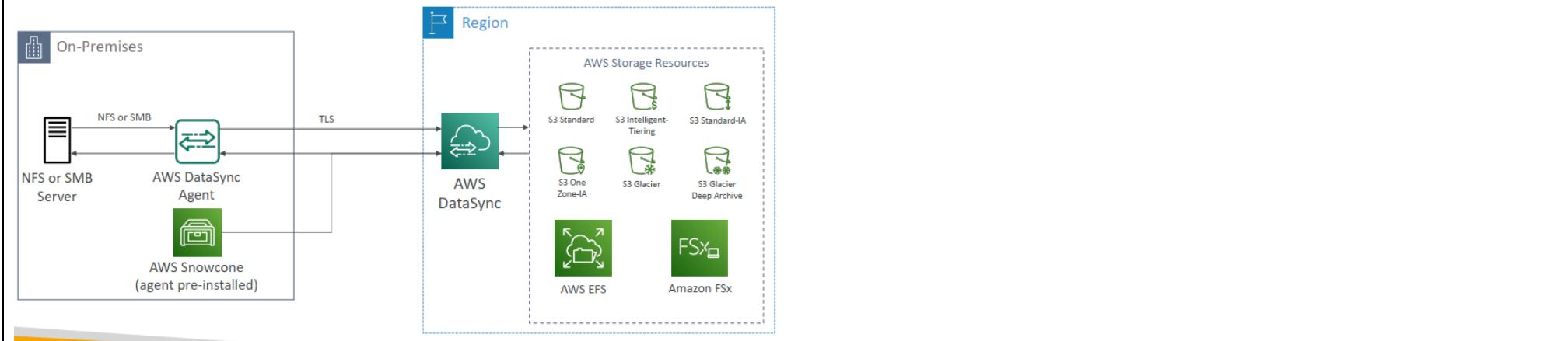
Amazon FSx File Gateway

- Native access to Amazon FSx for Windows File Server
- Local cache for frequently accessed data
- Windows native compatibility (SMB, NTFS, Active Directory...)
- Useful for group file shares and home directories



AWS DataSync

NFS / SMB to AWS (S3, EFS, FSx...)



Question 426:

A global company has a mobile app that displays ticket barcodes. Customers use the tickets on the mobile app to attend live events. Event scanners read the ticket barcodes and call a backend API to validate the barcode data against data in a database. After the barcode is scanned, the backend logic writes to the database's single table to mark the barcode as used.

The company needs to deploy the app on AWS with a DNS name of `api.example.com`. The company will host the database in three AWS Regions around the world.

Which solution will meet these requirements with the **LOWEST** latency?

- Host the database on Amazon Aurora global database clusters. Host the backend on three Amazon Elastic Container Service (Amazon ECS) clusters that are in the same Regions as the database. Create an accelerator in AWS Global Accelerator to route requests to the nearest ECS cluster. Create an Amazon Route 53 record that maps `api.example.com` to the accelerator endpoint
- Host the database on Amazon Aurora global database clusters. Host the backend on three Amazon Elastic Kubernetes Service (Amazon EKS) clusters that are in the same Regions as the database. Create an Amazon CloudFront distribution with the three clusters as origins. Route requests to the nearest EKS cluster. Create an Amazon Route 53 record that maps `api.example.com` to the CloudFront distribution.
- Host the database on Amazon DynamoDB global tables. Create an Amazon CloudFront distribution. Associate the CloudFront distribution with a CloudFront function that contains the backend logic to validate the barcodes. Create an Amazon Route 53 record that maps `api.example.com` to the CloudFront distribution.
- Host the database on Amazon DynamoDB global tables. Create an Amazon CloudFront distribution. Associate the CloudFront distribution with a Lambda@Edge function that contains the backend logic to validate the barcodes. Create an Amazon Route 53 record that maps `api.example.com` to the CloudFront distribution.

D

D is the proper answer CloudFront Functions - can be used only for manipulation with requests data CloudFront Lambda@Edge functions - can be used for anything, because this is a regular lambda function

Question 427:

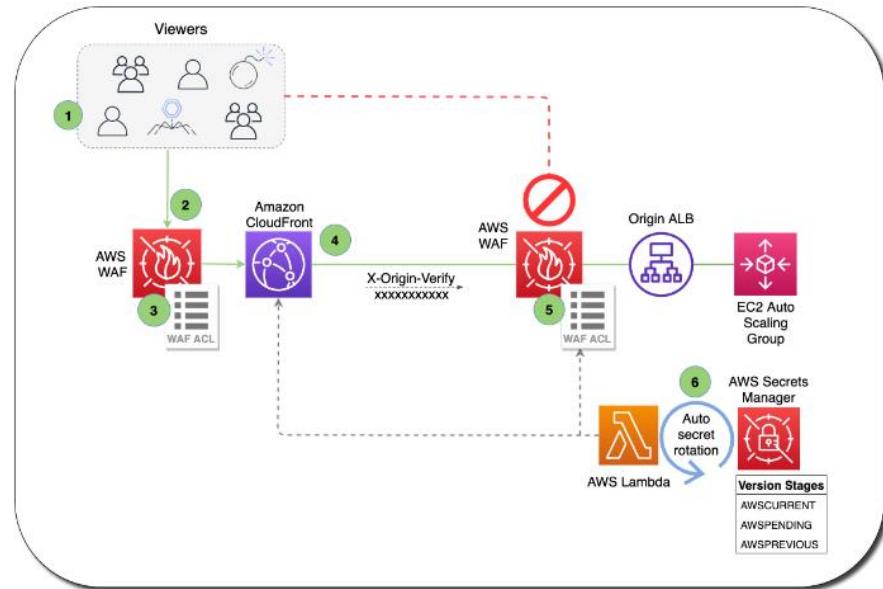
A medical company is running a REST API on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group behind an Application Load Balancer (ALB). The ALB runs in three public subnets, and the EC2 instances run in three private subnets. The company has deployed an Amazon CloudFront distribution that has the ALB as the only origin.

Which solution should a solutions architect recommend to enhance the origin security?

- A. Store a random string in AWS Secrets Manager. Create an AWS Lambda function for automatic secret rotation. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Create an AWS WAF web ACL rule with a string match rule for the custom header. Associate the web ACL with the ALB.
- B. Create an AWS WAF web ACL rule with an IP match condition of the CloudFront service IP address ranges. Associate the web ACL with the ALB. Move the ALB into the three private subnets.
- C. Store a random string in AWS Systems Manager Parameter Store. Configure Parameter Store automatic rotation for the string. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Inspect the value of the custom HTTP header, and block access in the ALB.
- D. Configure AWS Shield Advanced Create a security group policy to allow connections from CloudFront service IP address ranges. Add the policy to AWS Shield Advanced, and attach the policy to the ALB.

A

<https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>

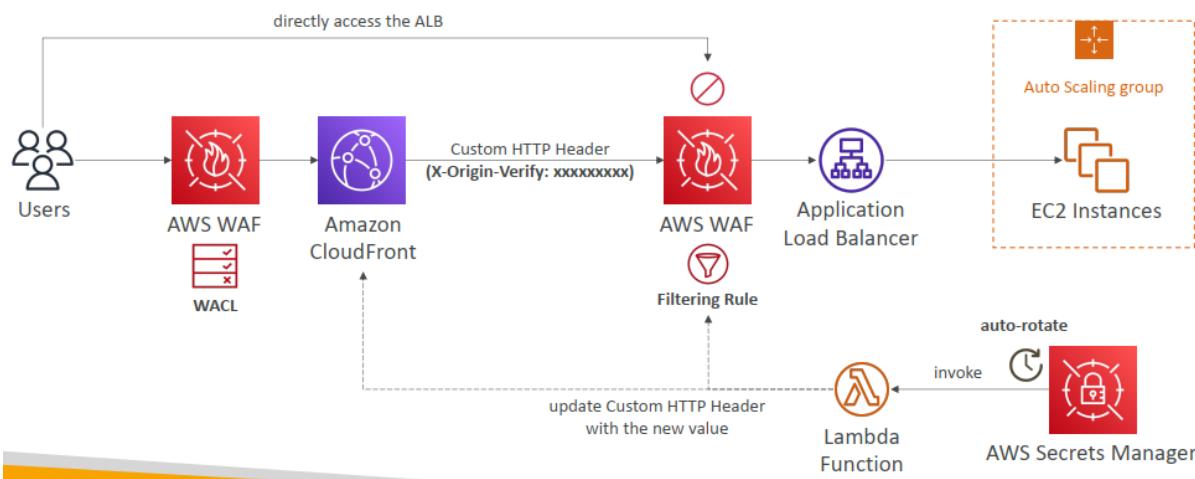


AWS WAF – Web Application Firewall



- Protects your web applications from common web exploits (Layer 7)
- Deploy on Application Load Balancer (localized rules)
- Deploy on API Gateway (rules running at the regional or edge level)
- Deploy on CloudFront (rules globally on edge locations)
 - Used to front other solutions: CLB, EC2 instances, custom origins, S3 websites
- Deploy on AppSync (protect your GraphQL APIs)
- **WAF is not for DDoS protection**
- Define Web ACL (Web Access Control List):
 - Rules can include IP addresses, HTTP headers, HTTP body, or URI strings
 - Protects from common attack - **SQL injection** and Cross-Site Scripting (XSS)
 - Size constraints, Geo match
 - Rate-based rules (to count occurrences of events)
- Rule Actions: Count | Allow | Block | CAPTCHA

Solution Architecture – Enhance CloudFront Origin Security with AWS WAF & AWS Secrets Manager



Question 428:

To abide by industry regulations, a solutions architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located. The solutions architect is required to provide access to the data stored in AWS to the company's global WAN network. The security team mandates that no traffic accessing this data should traverse the public internet.

How should the solutions architect design a highly available solution that meets the requirements and is cost-effective?

- A. Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use. Use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data.
- B. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use inter-region VPC peering to access the data in other AWS Regions.
- C. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use an AWS transit VPC solution to access data in other AWS Regions.
- D. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions.

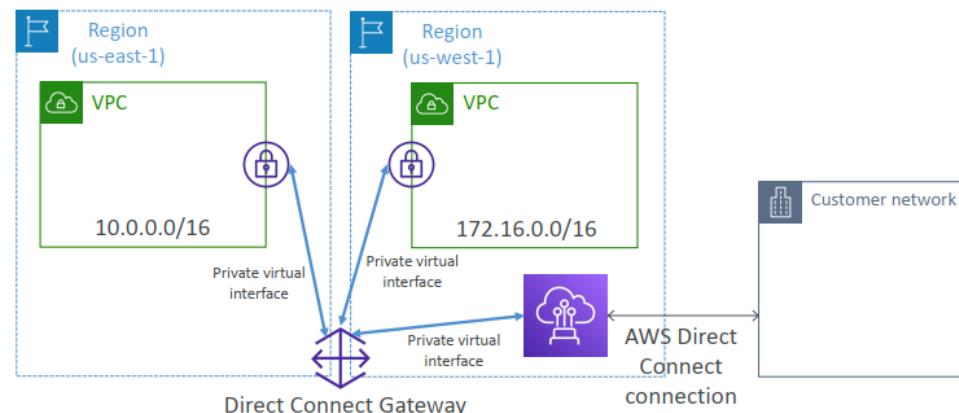
D

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/direct-connect.html>

Direct Connect Gateway



- If you want to setup a Direct Connect to one or more VPC in many different regions (same/cross account), you must use a Direct Connect Gateway



Question 429:

A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts on premises. The application data is stored in a proprietary format that must be read through the application. The company manually provisioned the servers and the application.

As part of its disaster recovery plan, the company wants the ability to host its application on AWS temporarily if the company's on-premises environment becomes unavailable. The company wants the application to return to on-premises hosting after a disaster recovery event is complete. The RPO is 5 minutes.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Configure AWS DataSync. Replicate the data to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and attach the EBS volumes.
- B. Configure AWS Elastic Disaster Recovery. Replicate the data to replication Amazon EC2 instances that are attached to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use Elastic Disaster Recovery to launch EC2 instances that use the replicated volumes.
- C. Provision an AWS Storage Gateway file gateway. Replicate the data to an Amazon S3 bucket. When the on-premises environment is unavailable, use AWS Backup to restore the data to Amazon Elastic Block Store (Amazon EBS) volumes and launch Amazon EC2 instances from these EBS volumes.
- D. Provision an Amazon FSx for Windows File Server file system on AWS. Replicate the data to the file system. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and use AWS::CloudFormation::Init commands to mount the Amazon FSx file shares.

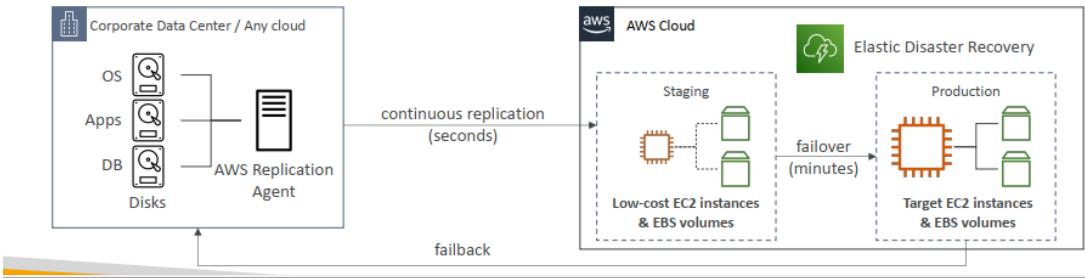
B

A - is out, because DataSync can't replicate data to EBS volumes
C - is out, because AWS Backup can't restore not managed data from S3 to EBS
D - is out, because it is not provide a way HOW we will replicate data from on-premise to FSx. Also, it is require additional amount of operational overhead

AWS Elastic Disaster Recovery (DRS)



- Used to be named "CloudEndure Disaster Recovery"
- Quickly and easily recover your physical, virtual, and cloud-based servers into AWS
- Example: protect your most critical databases (including Oracle, MySQL, and SQL Server), enterprise apps (SAP), protect your data from ransomware attacks, ...
- Continuous block-level replication for your servers



AWS DataSync



- Move large amount of data to and from
 - On-premises / other cloud to AWS (NFS, SMB, HDFS, S3 API...) – **needs agent**
 - AWS to AWS (different storage services) – no agent needed
- Can synchronize to:
 - Amazon S3 (any storage classes – including Glacier)
 - Amazon EFS
 - Amazon FSx (Windows, Lustre, NetApp, OpenZFS...)
- Replication tasks can be scheduled hourly, daily, weekly
- File permissions and metadata are preserved** (NFS POSIX, SMB...)
- One agent task can use 10 Gbps, can setup a bandwidth limit

Question 430:

A company runs a highly available data collection application on Amazon EC2 in the eu-north-1 Region. The application collects data from end-user devices and writes records to an Amazon Kinesis data stream and a set of AWS Lambda functions that process the records. The company persists the output of the record processing to an Amazon S3 bucket in eu-north-1. The company uses the data in the S3 bucket as a data source for Amazon Athena.

The company wants to increase its global presence. A solutions architect must launch the data collection capabilities in the sa-east-1 and ap-northeast-1 Regions. The solutions architect deploys the application, the Kinesis data stream, and the Lambda functions in the two new Regions. The solutions architect keeps the S3 bucket in eu-north-1 to meet a requirement to centralize the data analysis.

During testing of the new setup, the solutions architect notices a significant lag on the arrival of data from the new Regions to the S3 bucket.

Which solution will improve this lag time the MOST?

- A. In each of the two new Regions, set up the Lambda functions to run in a VPC. Set up an S3 gateway endpoint in that VPC.
- B. Turn on S3 Transfer Acceleration on the S3 bucket in eu-north-1. Change the application to use the new S3 accelerated endpoint when the application uploads data to the S3 bucket.
- C. Create an S3 bucket in each of the two new Regions. Set the application in each new Region to upload to its respective S3 bucket. Set up S3 Cross-Region Replication to replicate data to the S3 bucket in eu-north-1.
- D. Increase the memory requirements of the Lambda functions to ensure that they have multiple cores available. Use the multipart upload feature when the application uploads data to Amazon S3 from Lambda.

C

"improve this lag time the MOST" means improve the time for "uploading files" not "uploading the files to the destination." Uploading the files to the bucket in the same region is faster than transferring them to other regions.

s3 transfer acceleration is not supported in eu-north-1 region yet

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>

Question 431:

A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business units. The centralized application front end is configured with a Network Load Balancer (NLB) for scalability.

Up to 10 business unit VPCs will need to be connected to the shared VPC. Some of the business unit VPC CIDR blocks overlap with the shared VPC, and some overlap with each other. Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only.

Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?

- A. Create an AWS Transit Gateway. Attach the shared VPC and the authorized business unit VPCs to the transit gateway. Create a single transit gateway route table and associate it with all of the attached VPCs. Allow automatic propagation of routes from the attachments into the route table. Configure VPC routing tables to send traffic to the transit gateway.

B. Create a VPC endpoint service using the centralized application NLB and enable the option to require endpoint acceptance. Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service. Accept authorized endpoint requests from the endpoint service console.

C. Create a VPC peering connection from each business unit VPC to the shared VPC. Accept the VPC peering connections from the shared VPC console. Configure VPC routing tables to send traffic to the VPC peering connection.

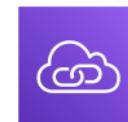
D. Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCs. Establish a Site-to-Site VPN connection from the business unit VPCs to the shared VPC. Configure VPC routing tables to send traffic to the VPN connection.

B

<https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip-ranges/>

some overlap with each other Network connectivity to the centralized application in the shared VPC → VPC endpoint service (Private Link)

AWS PrivateLink (VPC Endpoint Services)

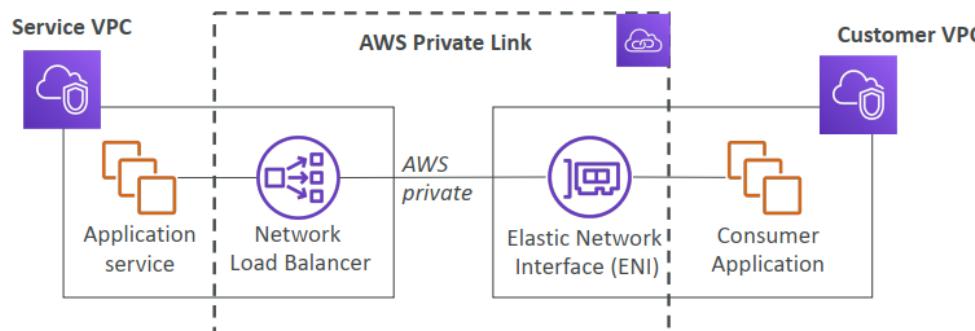


Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts)

Does not require VPC peering, internet gateway, NAT, route tables...

Requires a network load balancer (Service VPC) and ENI (Customer VPC)

If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!





Question 432:

A company wants to migrate its website to AWS. The website uses microservices and runs on containers that are deployed in an on-premises, self-managed Kubernetes cluster. All the manifests that define the deployments for the containers in the Kubernetes deployment are in source control.

All data for the website is stored in a PostgreSQL database. An open source container image repository runs alongside the on-premises environment.

A solutions architect needs to determine the architecture that the company will use for the website on AWS.

Which solution will meet these requirements with the LEAST effort to migrate?

- Create an AWS App Runner service. Connect the App Runner service to the open source container image repository. Deploy the manifests from on premises to the App Runner service. Create an Amazon RDS for PostgreSQL database.
- Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that has managed node groups. Copy the application containers to a new Amazon Elastic Container Registry (Amazon ECR) repository. Deploy the manifests from on premises to the EKS cluster. Create an Amazon Aurora PostgreSQL DB cluster.

C. Create an Amazon Elastic Container Service (Amazon ECS) cluster that has an Amazon EC2 capacity pool. Copy the application containers to a new Amazon Elastic Container Registry (Amazon ECR) repository. Register each container image as a new task definition. Configure ECS services for each task definition to match the original Kubernetes deployments. Create an Amazon Aurora PostgreSQL DB cluster.

D. Rebuild the on-premises Kubernetes cluster by hosting the cluster on Amazon EC2 instances. Migrate the open source container image repository to the EC2 instances. Deploy the manifests from on premises to the new cluster on AWS. Deploy an open source PostgreSQL database on the new cluster.

B
microservices and runs on containers that are deployed in an on-premises, self-managed Kubernetes cluster. ➔ migrate to EKS
All data for the website is stored in a PostgreSQL database ➔ Amazon Aurora PostgreSQL DB
. An open source container image repository ➔ ECR

Question 433:

A company uses a mobile app on AWS to run online contests. The company selects a winner at random at the end of each contest. The contests run for variable lengths of time. The company does not need to retain any data from a contest after the contest is finished.

The company uses custom code that is hosted on Amazon EC2 instances to process the contest data and select a winner. The EC2 instances run behind an Application Load Balancer and store contest entries on Amazon RDS DB instances. The company must design a new architecture to reduce the cost of running the contests.

Which solution will meet these requirements MOST cost-effectively?

A. Migrate storage of the contest entries to Amazon DynamoDB. Create a DynamoDB Accelerator (DAX) cluster. Rewrite the code to run as Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type. At the end of the contest, delete the DynamoDB table.

B. Migrate the storage of the contest entries to Amazon Redshift. Rewrite the code as AWS Lambda functions. At the end of the contest, delete the Redshift cluster.

C. Add an Amazon ElastiCache for Redis cluster in front of the RDS DB instances to cache the contest entries. Rewrite the code to run as Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type. Set the ElastiCache TTL attribute on each entry to expire each entry at the end of the contest.

D. Migrate the storage of the contest entries to Amazon DynamoDB. Rewrite the code as AWS Lambda functions. Set the DynamoDB TTL attribute on each entry to expire each entry at the end of the contest.

D
D is the most cost-effective solution. It leverages DynamoDB for efficient, scalable storage with automatic data expiration via TTL and AWS Lambda for flexible, event-driven processing. This setup minimizes costs by using resources only when needed and automatically scaling to match demand without the need for manual intervention or over-provisioning.
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

Question 434:

A company has implemented a new security requirement. According to the new requirement, the company must scan all traffic from corporate AWS instances in the company's VPC for violations of the company's security policies. As a result of these scans, the company can block access to and from specific IP addresses.

To meet the new requirement, the company deploys a set of Amazon EC2 instances in private subnets to serve as transparent proxies. The company installs approved proxy server software on these EC2 instances. The company modifies the route tables on all subnets to use the corresponding EC2 instances with proxy software as the default route. The company also creates security groups that are compliant with the security policies and assigns these security groups to the EC2 instances.

Despite these configurations, the traffic of the EC2 instances in their private subnets is not being properly forwarded to the internet.

What should a solutions architect do to resolve this issue?

- A. Disable source/destination checks on the EC2 instances that run the proxy software.
- B. Add a rule to the security group that is assigned to the proxy EC2 instances to allow all traffic between instances that have this security group. Assign this security group to all EC2 instances in the VPC.
- C. Change the VPCs DHCP options set. Set the DNS server options to point to the addresses of the proxy EC2 instances.
- D. Assign one additional elastic network interface to each proxy EC2 instance. Ensure that one of these network interfaces has a route to the private subnets. Ensure that the other network interface has a route to the internet.

A

Question 435:

A company is running its solution on AWS in a manually created VPC. The company is using AWS CloudFormation to provision other parts of the infrastructure. According to a new requirement, the company must manage all infrastructure in an automatic way.

What should the company do to meet this new requirement with the LEAST effort?

- A. Create a new AWS Cloud Development Kit (AWS CDK) stack that strictly provisions the existing VPC resources and configuration. Use AWS CDK to import the VPC into the stack and to manage the VPC.
- B. Create a CloudFormation stack set that creates the VPC. Use the stack set to import the VPC into the stack.
- C. Create a new CloudFormation template that strictly provisions the existing VPC resources and configuration. From the CloudFormation console, create a new stack by importing the Existing resources.
- D. Create a new CloudFormation template that creates the VPC. Use the AWS Serverless Application Model (AWS SAM) CLI to import the VPC.

C

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/resource-import.html>

Question 436:

A company has developed a new release of a popular video game and wants to make it available for public download. The new release package is approximately 5 GB in size. The company provides downloads for existing releases from a Linux-based, publicly facing FTP site hosted in an on-premises data center. The company expects the new release will be downloaded by users worldwide. The company wants a solution that provides improved download performance and low transfer costs, regardless of a user's location.

- A. Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- B. Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on each of the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- C. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Use Amazon CloudFront for the website. Publish the game download URL for users to download the package.
- D. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Set Requester Pays for the S3 bucket. Publish the game download URL for users to download the package.

C

The company expects the new release will be downloaded by users worldwide → Route 53 + CloudFront + S3.

Question 437:

A company runs an application in the cloud that consists of a database and a website. Users can post data to the website, have the data processed, and have the data sent back to them in an email. Data is stored in a MySQL database running on an Amazon EC2 instance. The database is running in a VPC with two private subnets. The website is running on Apache Tomcat in a single EC2 instance in a different VPC with one public subnet. There is a single VPC peering connection between the database and website VPC.

The website has suffered several outages during the last month due to high traffic.

Which actions should a solutions architect take to increase the reliability of the application? (Choose three.)

- A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer.
- B. Provision an additional VPC peering connection.
- C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica.
- D. Provision two NAT gateways in the database VPC.
- E. Move the Tomcat server to the database VPC.
- F. Create an additional public subnet in a different Availability Zone in the website VPC.

A,C,F

increase the reliability of the application → HA → Web: Auto Scaling group with multiple EC2 instances behind an Application Load Balancer (A), Multi AZ (F) + Database: replica (C)

Question 438:

A retail company is operating its ecommerce application on AWS. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses an Amazon RDS DB instance as the database backend. Amazon CloudFront is configured with one origin that points to the ALB. Static content is cached. Amazon Route 53 is used to host all public zones.

After an update of the application, the ALB occasionally returns a 502 status code (Bad Gateway) error. The root cause is malformed HTTP headers that are returned to the ALB. The webpage returns successfully when a solutions architect reloads the webpage immediately after the error occurs.

While the company is working on the problem, the solutions architect needs to provide a custom error page instead of the standard ALB error page to visitors.

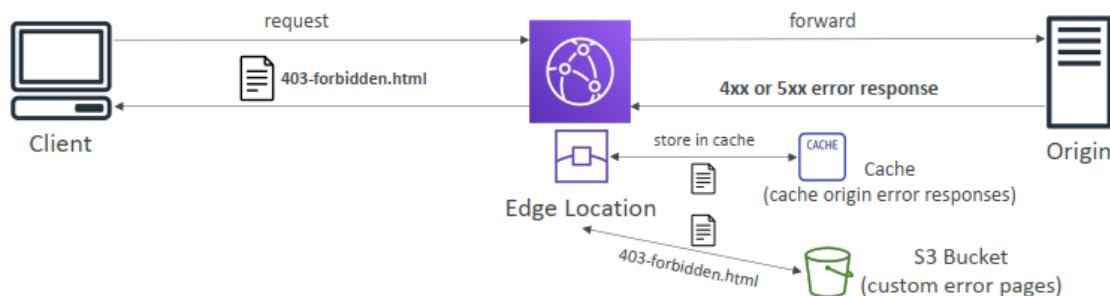
Which combination of steps will meet this requirement with the LEAST amount of operational overhead? (Choose two.)

- A. Create an Amazon S3 bucket. Configure the S3 bucket to host a static webpage. Upload the custom error pages to Amazon S3.
- B. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Target.FailedHealthChecks is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a publicly accessible web server.
- C. Modify the existing Amazon Route 53 records by adding health checks. Configure a fallback target if the health check fails. Modify DNS records to point to a publicly accessible webpage.
- D. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Elb.InternalError is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a public accessible web server.
- E. Add a custom error response by configuring a CloudFront custom error page. Modify DNS records to point to a publicly accessible web page.

A, E
needs to provide a custom error page → custom error pages to Amazon S3 + CloudFront

CloudFront – Custom Error Pages

- Return an object to the viewer (e.g., .html) when your origin returns an HTTP 4xx or 5xx status code to CloudFront
- Use **Error Caching Minimum TTL** to specify how long CloudFront caches the custom error pages



Question 439:

A company wants to migrate an Amazon Aurora MySQL DB cluster from an existing AWS account to a new AWS account in the same AWS Region. Both accounts are members of the same organization in AWS Organizations.

The company must minimize database service interruption before the company performs DNS cutover to the new database.

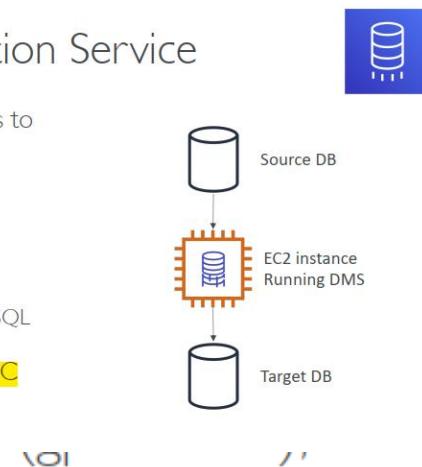
Which migration strategy will meet this requirement? (Choose two.)

- Take a snapshot of the existing Aurora database. Share the snapshot with the new AWS account. Create an Aurora DB cluster in the new account from the snapshot.
- Create an Aurora DB cluster in the new AWS account. Use AWS Database Migration Service (AWS DMS) to migrate data between the two Aurora DB clusters.
- Use AWS Backup to share an Aurora database backup from the existing AWS account to the new AWS account. Create an Aurora DB cluster in the new AWS account from the snapshot.
- Create an Aurora DB cluster in the new AWS account. Use AWS Application Migration Service to migrate data between the two Aurora DB clusters.

A, B

DMS – Database Migration Service

- Quickly and securely migrate databases to AWS, resilient, self healing
- The source database remains available during the migration
- Supports:
 - Homogeneous migrations: ex Oracle to Oracle
 - Heterogeneous migrations: ex Microsoft SQL Server to Aurora
- Continuous Data Replication using CDC
- You must create an EC2 instance to perform the replication tasks



DMS Sources and Targets

SOURCES:

- On-premises and EC2 instances databases: Oracle, MS SQL Server, MySQL, MariaDB, PostgreSQL, MongoDB, SAP, DB2
- Azure: Azure SQL Database
- Amazon RDS: all including Aurora
- Amazon S3
- DocumentDB

TARGETS:

- On-premises and EC2 instances databases: Oracle, MS SQL Server, MySQL, MariaDB, PostgreSQL, SAP
- Amazon RDS including Aurora
- Amazon Redshift
- Amazon DynamoDB
- Amazon S3
- OpenSearch Service
- Kinesis Data Streams
- DocumentDB

- **Backups:** automated with point-in-time recovery. Backups expire
- **Snapshots:** manual, can make copies of snapshots cross region

Question 440:

A software as a service (SaaS) company provides a media software solution to customers. The solution is hosted on 50 VPCs across various AWS Regions and AWS accounts. One of the VPCs is designated as a management VPC. The compute resources in the VPCs work independently.

The company has developed a new feature that requires all 50 VPCs to be able to communicate with each other. The new feature also requires one-way access from each customer's VPC to the company's management VPC. The management VPC hosts a compute resource that validates licenses for the media software solution.

The number of VPCs that the company will use to host the solution will continue to increase as the solution grows.

Which combination of steps will provide the required VPC connectivity with the LEAST operational overhead? (Choose two.)

- Create a transit gateway. Attach all the company's VPCs and relevant subnets to the transit gateway.
- Create VPC peering connections between all the company's VPCs.
- Create a Network Load Balancer (NLB) that points to the compute resource for license validation. Create an AWS PrivateLink endpoint service that is available to each customer's VPC. Associate the endpoint service with the NLB.

D. Create a VPN appliance in each customer's VPC. Connect the company's management VPC to each customer's VPC by using AWS Site-to-Site VPN.

E. Create a VPC peering connection between the company's management VPC and each customer's VPC.

A, C

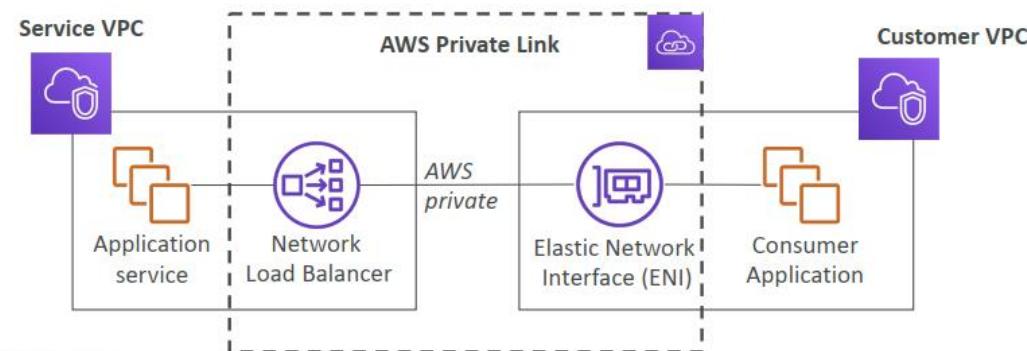
requires all 50 VPCs to be able to communicate with each other ➔ Transit Gateway

The new feature also requires one-way access from each customer's VPC to the company's management VPC ➔ Private Link

AWS PrivateLink (VPC Endpoint Services)



- Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts)
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)
- If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!



Question 441:

A company has multiple lines of business (LOBs) that roll up to the parent company. The company has asked its solutions architect to develop a solution with the following requirements:

- Produce a single AWS invoice for all of the AWS accounts used by its LOBs.
- The costs for each LOB account should be broken out on the invoice.
- Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy.
- Each LOB account should be delegated full administrator permissions, regardless of the governance policy.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Use AWS Organizations to create an organization in the parent account for each LOB. Then invite each LOB account to the appropriate organization.

- B. Use AWS Organizations to create a single organization in the parent account. Then, invite each LOB's AWS account to join the organization.
- C. Implement service quotas to define the services and features that are permitted and apply the quotas to each LOB, as appropriate.
- D. Create an SCP that allows only approved services and features, then apply the policy to the LOB accounts.
- E. Enable consolidated billing in the parent account's billing console and link the LOB accounts.

B,D

Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy → SCP
Consolidated billing is already enabled by default when you create an organization → B, D

Question 442:

A solutions architect has deployed a web application that serves users across two AWS Regions under a custom domain. The application uses Amazon Route 53 latency-based routing. The solutions architect has associated weighted record sets with a pair of web servers in separate Availability Zones for each Region.

The solutions architect runs a disaster recovery scenario. When all the web servers in one Region are stopped, Route 53 does not automatically redirect users to the other Region.

Which of the following are possible root causes of this issue? (Choose two.)

- A. The weight for the Region where the web servers were stopped is higher than the weight for the other Region.
- B. One of the web servers in the secondary Region did not pass its HTTP health check.
- C. Latency resource record sets cannot be used in combination with weighted resource record sets.
- D. The setting to evaluate target health is not turned on for the latency alias resource record set that is associated with the domain in the Region where the web servers were stopped.
- E. An HTTP health check has not been set up for one or more of the weighted resource record sets associated with the stopped web servers.

D, E

Route 53 latency-based routing does not inherently perform health checks. If a web server in one region goes down, Route 53 won't automatically redirect traffic to the other region unless health checks are properly configured and associated with your DNS records.

Question 443:

A flood monitoring agency has deployed more than 10,000 water-level monitoring sensors. Sensors send continuous data updates, and each update is less than 1 MB in size. The agency has a fleet of on-premises application servers. These servers receive updates from the sensors, convert the raw data into a human readable format, and write the results to an on-premises relational database server. Data analysts then use simple SQL queries to monitor the data.

The agency wants to increase overall application availability and reduce the effort that is required to perform maintenance tasks. These maintenance tasks, which include updates and patches to the application servers, cause downtime. While an application server is down, data is lost from sensors because the remaining servers cannot handle the entire workload.

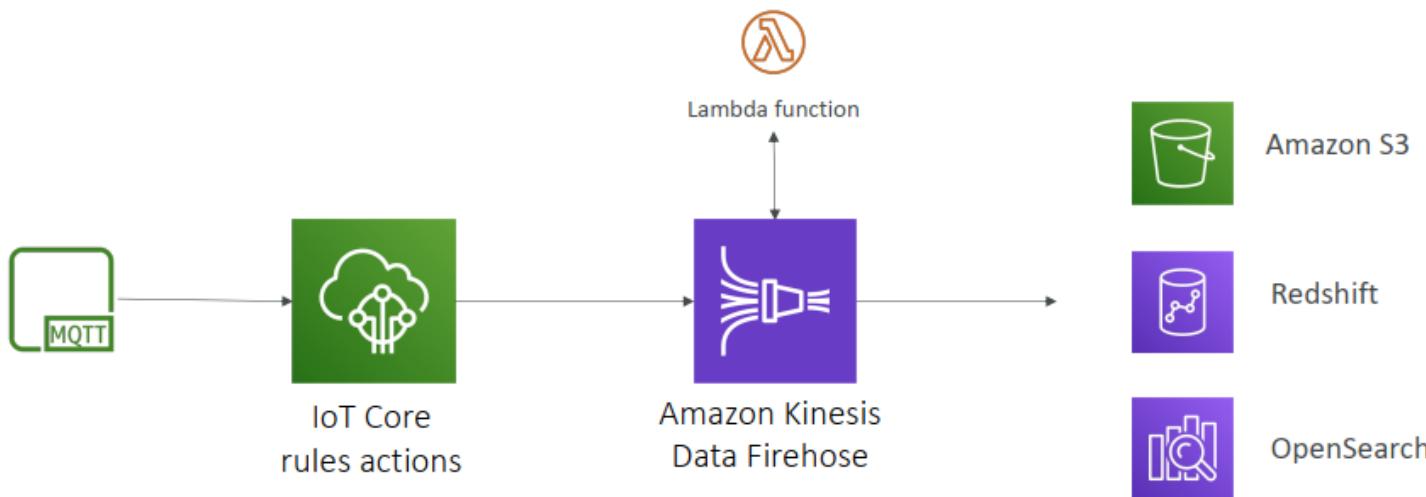
The agency wants a solution that optimizes operational overhead and costs. A solutions architect recommends the use of AWS IoT Core to collect the sensor data.

What else should the solutions architect recommend to meet these requirements?

- A. Send the sensor data to Amazon Kinesis Data Firehose. Use an AWS Lambda function to read the Kinesis Data Firehose data, convert it to .csv format, and insert it into an Amazon Aurora MySQL DB instance. Instruct the data analysts to query the data directly from the DB instance.
- B. Send the sensor data to Amazon Kinesis Data Firehose. Use an AWS Lambda function to read the Kinesis Data Firehose data, convert it to Apache Parquet format, and save it to an Amazon S3 bucket. Instruct the data analysts to query the data by using Amazon Athena.
- C. Send the sensor data to an Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) application to convert the data to .csv format and store it in an Amazon S3 bucket. Import the data into an Amazon Aurora MySQL DB instance. Instruct the data analysts to query the data directly from the DB instance.
- D. Send the sensor data to an Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) application to convert the data to Apache Parquet format and store it in an Amazon S3 bucket. Instruct the data analysts to query the data by using Amazon Athena.

B

IoT Core – Kinesis Data Firehose



Question 444:

A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalog page. Auto Scaling is configured to maintain the web fleet size based on the ALB health check.

Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times.

Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (Choose two.)

- A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.
- B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- C. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- D. Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.
- E. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

B, E

When you talking about a product catalog page, you need to cache information (text, images) to leverage the load on the data tier. ElastiCache is the solution (or a CDN).

Question 445:

A company has an on-premises data center and is using Kubernetes to develop a new solution on AWS. The company uses Amazon Elastic Kubernetes Service (Amazon EKS) clusters for its development and test environments.

The EKS control plane and data plane for production workloads must reside on premises. The company needs an AWS managed solution for Kubernetes management.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using a local cluster configuration on the Outposts server for the production workloads.
- B. Install Amazon EKS Anywhere on the company's hardware in the on-premises data center. Deploy the production workloads on an EKS Anywhere cluster.
- C. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using an extended cluster configuration on the Outposts server for the production workloads.

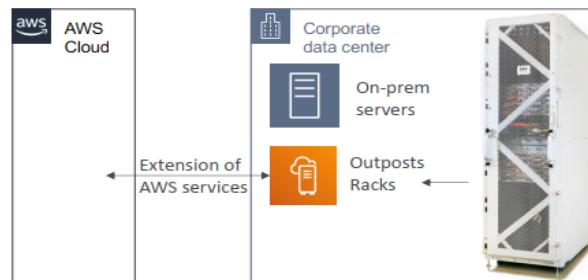
D. Install an AWS Outposts server in the on-premises data center. Install Amazon EKS Anywhere on the Outposts server. Deploy the production workloads on an EKS Anywhere cluster.

A

AWS Outposts



- Hybrid Cloud: businesses that keep an on-premises infrastructure alongside a cloud cùng với infrastructure
- Therefore, two ways of dealing with IT systems:
 - One for the AWS cloud (using the AWS console, CLI, and AWS APIs)
 - One for their on-premises infrastructure
- AWS Outposts are “server racks” that offers the same AWS infrastructure, services, APIs & tools to build your own applications on-premises just as in the cloud
- AWS will setup and manage “Outposts Racks” within your on-premises infrastructure and you can start leveraging AWS services on-premises
- You are responsible for the Outposts Rack physical security



Question 446:

A company uses AWS Organizations to manage its development environment. Each development team at the company has its own AWS account. Each account has a single VPC and CIDR blocks that do not overlap.

The company has an Amazon Aurora DB cluster in a shared services account. All the development teams need to work with live data from the DB cluster.

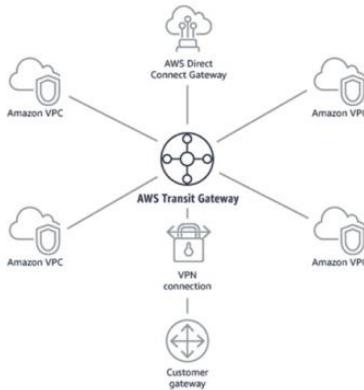
Which solution will provide the required connectivity to the DB cluster with the LEAST operational overhead?

- Create an AWS Resource Access Manager (AWS RAM) resource share for the DB cluster. Share the DB cluster with all the development accounts.
- Create a transit gateway in the shared services account. Create an AWS Resource Access Manager (AWS RAM) resource share for the transit gateway. Share the transit gateway with all the development accounts. Instruct the developers to accept the resource share. Configure networking.
- Create an Application Load Balancer (ALB) that points to the IP address of the DB cluster. Create an AWS PrivateLink endpoint service that uses the ALB. Add permissions to allow each development account to connect to the endpoint service.
- Create an AWS Site-to-Site VPN connection in the shared services account. Configure networking. Use AWS Marketplace VPN software in each development account to connect to the Site-to-Site VPN connection.

B

Transit Gateway

- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager (RAM)
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with other VPC
- Works with Direct Connect Gateway, VPN connections
- Supports IP Multicast (not supported by any other AWS service)
- Instances in a VPC can access a NAT Gateway, NLB, PrivateLink, and EFS in others VPCs attached to the AWS Transit Gateway.



AWS Resource Access Manager (RAM)

- Share AWS resources that you own with other AWS accounts
- Share with any account or within your Organization
- Avoid resource duplication!
- **VPC Subnets**
 - Allow to have all the resources launched in the same subnets
 - Must be from the same AWS Organizations.
 - Cannot share security groups and default VPC
 - Participants can manage their own resources in there
 - Participants can't view, modify, delete resources that belong to other participants or the owner
- **AWS Transit Gateway**
- Route 53 (Resolver Rules, DNS Firewall Rule Groups)
- License Manager Configurations

AWS Resource Access Manager (RAM)

- Aurora DB Clusters
- ACM Private Certificate Authority
- CodeBuild Project
- EC2 (Dedicated Hosts, Capacity Reservation)
- AWS Glue (Catalog, Database, Table)
- AWS Network Firewall Policies
- AWS Resource Groups
- Systems Manager Incident Manager (Contacts, Response Plans)
- AWS Outposts (Outpost, Site)

Question 447:

A company used AWS CloudFormation to create all new infrastructure in its AWS member accounts. The resources rarely change and are properly sized for the expected load. The monthly AWS bill is consistent.

Occasionally, a developer creates a new resource for testing and forgets to remove the resource when the test is complete. Most of these tests last a few days before the resources are no longer needed.

The company wants to automate the process of finding unused resources. A solutions architect needs to design a solution that determines whether the cost in the AWS bill is increasing. The solution must help identify resources that cause an increase in cost and must automatically notify the company's operations team.

Which solution will meet these requirements?

- A. Turn on billing alerts. Use AWS Cost Explorer to determine the costs for the past month. Create an Amazon CloudWatch alarm for total estimated charges. Specify a cost threshold that is higher than the costs that Cost Explorer determined. Add a notification to alert the operations team if the alarm threshold is breached.
- B. Turn on billing alerts. Use AWS Cost Explorer to determine the average monthly costs for the past 3 months. Create an Amazon CloudWatch alarm for total estimated charges. Specify a cost threshold that is higher than the costs that Cost Explorer determined. Add a notification to alert the operations team if the alarm threshold is breached.
- C. Use AWS Cost Anomaly Detection to create a cost monitor that has a monitor type of Linked account. Create a subscription to send daily AWS cost summaries to the operations team. Specify a threshold for cost variance.

D. Use AWS Cost Anomaly Detection to create a cost monitor that has a monitor type of AWS services. Create a subscription to send daily AWS cost summaries to the operations team. Specify a threshold for cost variance.

D

AWS Cost Anomaly Detection is specifically designed to detect unusual spending patterns or anomalies in AWS costs.

<https://docs.aws.amazon.com/cost-management/latest/userguide/getting-started-ad.html#monitor-type-def>

Monitor types

You can choose the monitor type that fits your account structure. Currently, we offer the following monitor types:

- **AWS services** - We recommend this monitor if you don't need to segment your spend by internal organizations or environments. This single monitor evaluates all the AWS services that are used by your individual AWS account for anomalies. When you add new AWS services, the monitor automatically begins to evaluate the new service for anomalies. That way, you don't have to manually configure your settings.
- Linked account - This monitor evaluates the total spend of an individual, or group of, member accounts. If your Organizations need to segment spend by team, product, services, or environment, this monitor is useful. The maximum number of member accounts that you can select for each monitor is 10.
- Cost category - This monitor is recommended if you use cost categories to organize and manage your spend. This monitor type is restricted to one key:value pair.
- Cost allocation tag - This monitor is similar to Linked account. If you need to segment your spend by team, product, services, or environment, this monitor is useful. This monitor type is restricted to one key, but accepts multiple values. The maximum number of values that you can select for each monitor is 10.

Question 448:

A company is deploying a new web-based application and needs a storage solution for the Linux application servers. The company wants to create a single location for updates to application data for all instances. The active dataset will be up to 100 GB in size. A solutions architect has determined that peak operations will occur for 3 hours daily and will require a total of 225 MiBps of read throughput.

The solutions architect must design a Multi-AZ solution that makes a copy of the data available in another AWS Region for disaster recovery (DR). The DR copy has an RPO of less than 1 hour.

Which solution will meet these requirements?

- A. Deploy a new Amazon Elastic File System (Amazon EFS) Multi-AZ file system. Configure the file system for 75 MiBps of provisioned throughput. Implement replication to a file system in the DR Region.
- B. Deploy a new Amazon FSx for Lustre file system. Configure Bursting Throughput mode for the file system. Use AWS Backup to back up the file system to the DR Region.
- C. Deploy a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume with 225 MiBps of throughput. Enable Multi-Attach for the EBS volume. Use AWS Elastic Disaster Recovery to replicate the EBS volume to the DR Region.
- D. Deploy an Amazon FSx for OpenZFS file system in both the production Region and the DR Region. Create an AWS DataSync scheduled task to replicate the data from the production file system to the DR file system every 10 minutes.

A

<https://docs.aws.amazon.com/datasync/latest/userguide/task-scheduling.html>

A. EFS support cross region replication

B is wrong because there is no such thing as bursting mode for Lustre that is an EFS thing, but also Backup will not work for the RPO.

C is wrong obviously because GP3 can't be shared.

D is wrong because DataSync tasks cannot be scheduled for any more frequent than hourly so no D is wrong because you cannot schedule data sync tasks less than hourly so you don't meet the RPO.

So all of those are easily wrong because they have bad information. They fooled everyone on A because all they say is the 'Active working set is 100GB' not the entire filesystem. EFS accumulates bursting credits so for every 100GB of filesystem size you can burst up to 300MiBps for up to 72 minutes. So you provision 75MiBps because that would average out over time so you aren't being overcharged for the provisioned size.

Question 449:

A company needs to gather data from an experiment in a remote location that does not have internet connectivity. During the experiment, sensors that are connected to a local network will generate 6 TB of data in a proprietary format over the course of 1 week. The sensors can be configured to upload their data files to an FTP server periodically, but the sensors do not have their own FTP server. The sensors also do not support other protocols. The company needs to collect the data centrally and move the data to object storage in the AWS Cloud as soon as possible after the experiment.

Which solution will meet these requirements?

- A. Order an AWS Snowball Edge Compute Optimized device. Connect the device to the local network. Configure AWS DataSync with a target bucket name, and unload the data over NFS to the device. After the experiment, return the device to AWS so that the data can be loaded into Amazon S3.
- B. Order an AWS Snowcone device, including an Amazon Linux 2 AMI. Connect the device to the local network. Launch an Amazon EC2 instance on the device. Create a shell script that periodically downloads data from each sensor. After the experiment, return the device to AWS so that the data can be loaded as an Amazon Elastic Block Store (Amazon EBS) volume.
- C. Order an AWS Snowcone device, including an Amazon Linux 2 AMI. Connect the device to the local network. Launch an Amazon EC2 instance on the device. Install and configure an FTP server on the EC2 instance. Configure the sensors to upload data to the EC2 instance. After the experiment, return the device to AWS so that the data can be loaded into Amazon S3.
- D. Order an AWS Snowcone device. Connect the device to the local network. Configure the device to use Amazon FSx. Configure the sensors to upload data to the device. Configure AWS DataSync on the device to synchronize the uploaded data with an Amazon S3 bucket. Return the device to AWS so that the data can be loaded as an Amazon Elastic Block Store (Amazon EBS) volume.

C

Since the sensors only support FTP for data upload, installing and configuring an FTP server on the EC2 instance is essential. This setup allows the sensors to periodically upload their data files to the Snowcone device. Snowcone is specialized for huge data migration.

AWS Snow Family

- Highly-secure, portable devices to collect and process data at the edge, and migrate data into and out of AWS

- Data migration:



Snowcone



Snowball Edge



Snowmobile

- Edge computing:



Snowcone



Snowball Edge

AWS Snowcone & Snowcone SSD



- Small, portable computing, anywhere, rugged & secure, withstands harsh environments
- Light (4.5 pounds, 2.1 kg)
- Device used for edge computing, storage, and data transfer
- Snowcone – 8 TB of HDD Storage
- Snowcone SSD – 14 TB of SSD Storage
- Use Snowcone where Snowball does not fit (space-constrained environment)
- Must provide your own battery / cables
- Can be sent back to AWS offline, or connect it to internet and use [AWS DataSync](#) to send data



Question 450:

A company that has multiple business units is using AWS Organizations with all features enabled. The company has implemented an account structure in which each business unit has its own AWS account. Administrators in each AWS account need to view detailed cost and utilization data for their account by using Amazon Athena.

Each business unit can have access to only its own cost and utilization data. The IAM policies that govern the ability to set up AWS Cost and Usage Reports are in place. A central Cost and Usage Report that contains all data for the organization is already available in an Amazon S3 bucket.

Which solution will meet these requirements with the LEAST operational complexity?

- In the organization's management account, use AWS Resource Access Manager (AWS RAM) to share the Cost and Usage Report data with each member account.
- In the organization's management account, configure an S3 event to invoke an AWS Lambda function each time a new file arrives in the S3 bucket that contains the central Cost and Usage Report. Configure the Lambda function to extract each member account's data and to place the data in Amazon S3 under a separate prefix. Modify the S3 bucket policy to allow each member account to access its own prefix.
- In each member account, access AWS Cost Explorer. Create a new report that contains relevant cost information for the account. Save the report in Cost Explorer. Provide instructions that the account administrators can use to access the saved report.
- In each member account, create a new S3 bucket to store Cost and Usage Report data. Set up a Cost and Usage Report to deliver the data to the new S3 bucket.

B

With the Lambda to extract and separate each member account's cost and utilization data from the central Cost and Usage Report stored in the S3 bucket and S3 events to trigger the Lambda function, the process is automated and requires minimal ongoing management. Each member account can be given access only to its own prefix within the S3 bucket, ensuring that each business unit can only access its own cost data. Other options involve higher operational complexity and overhead.

Question 451:

A company is designing an AWS environment for a manufacturing application. The application has been successful with customers, and the application's user base has increased. The company has connected the AWS environment to the company's on-premises data center through a 1 Gbps AWS Direct Connect connection. The company has configured BGP for the connection.

The company must update the existing network connectivity solution to ensure that the solution is highly available, fault tolerant, and secure.

Which solution will meet these requirements MOST cost-effectively?

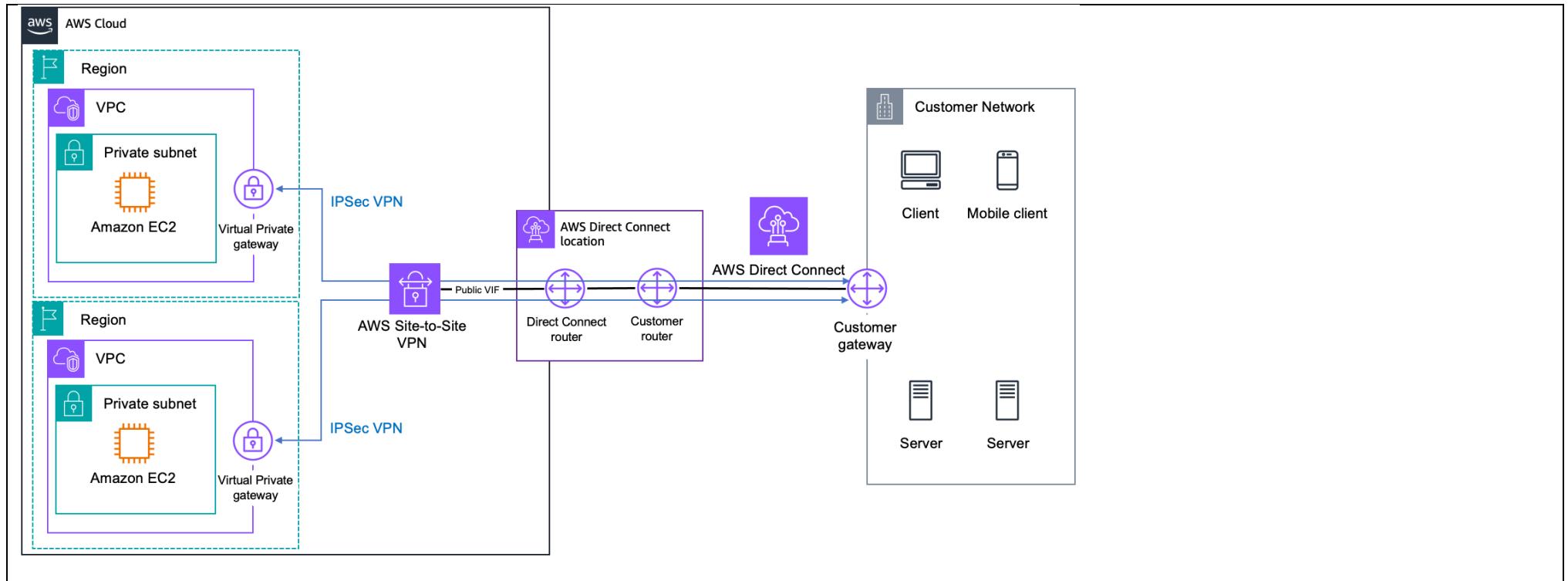
- A. Add a dynamic private IP AWS Site-to-Site VPN as a secondary path to secure data in transit and provide resilience for the Direct Connect connection. Configure MACsec to encrypt traffic inside the Direct Connect connection.
- B. Provision another Direct Connect connection between the company's on-premises data center and AWS to increase the transfer speed and provide resilience. Configure MACsec to encrypt traffic inside the Direct Connect connection.
- C. Configure multiple private VIFs. Load balance data across the VIFs between the on-premises data center and AWS to provide resilience.
- D. Add a static AWS Site-to-Site VPN as a secondary path to secure data in transit and to provide resilience for the Direct Connect connection.

B

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-site-to-site-vpn.html>

<https://repost.aws/knowledge-center/create-vpn-direct-connect>

<https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/>



Question 452:

A company needs to modernize an application and migrate the application to AWS. The application stores user profile data as text in a single table in an on-premises MySQL database.

After the modernization, users will use the application to upload video files that are up to 4 GB in size. Other users must be able to download the video files from the application. The company needs a video storage solution that provides rapid scaling. The solution must not affect application performance.

Which solution will meet these requirements?

- Migrate the database to Amazon Aurora PostgreSQL by using AWS Database Migration Service (AWS DMS). Store the videos as base64-encoded strings in a TEXT column in the database.
- Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as objects in Amazon S3. Store the S3 key in the corresponding DynamoDB item.
- Migrate the database to Amazon Keyspaces (for Apache Cassandra) by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as objects in Amazon S3. Store the S3 object identifier in the corresponding Amazon Keyspaces entry.

D. Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as base64-encoded strings in the corresponding DynamoDB item.

B

must be able to download the video files from the application → S3
user profile data as text in a single table in an on-premises MySQL database. → DynamoDB

Question 453:

A company stores and manages documents in an Amazon Elastic File System (Amazon EFS) file system. The file system is encrypted with an AWS Key Management Service (AWS KMS) key. The file system is mounted to an Amazon EC2 instance that runs proprietary software.

The company has enabled automatic backups for the file system. The automatic backups use the AWS Backup default backup plan.

A solutions architect must ensure that deleted documents can be recovered within an RPO of 100 minutes.

Which solution will meet these requirements?

- A. Create a new IAM role. Create a new backup plan. Use the new IAM role to create backups. Update the KMS key policy to allow the new IAM role to use the key. Implement an hourly backup schedule for the file system.
- B. Create a new backup plan. Update the KMS key policy to allow the AWSServiceRoleForBackup IAM role to use the key. Implement a custom cron expression to run a backup of the file system every 30 minutes.
- C. Create a new IAM role. Use the existing backup plan. Update the KMS key policy to allow the new IAM role to use the key. Enable continuous backups for point-in-time recovery.
- D. Use the existing backup plan. Update the KMS key policy to allow the AWSServiceRoleForBackup IAM role to use the key. Enable Cross-Region Replication for the file system.

A

RPO of 100 minutes. → Implement an hourly backup schedule for the file system.

B is incorrect because B requires a custom cron task to be set up using EventBridge as it is a non-standard one for AWS Backup using the existing default backup plan means backups only once a day, which disqualifies both C and D

Question 454:

A solutions architect must provide a secure way for a team of cloud engineers to use the AWS CLI to upload objects into an Amazon S3 bucket. Each cloud engineer has an IAM user, IAM access keys, and a virtual multi-factor authentication (MFA) device. The IAM users for the cloud engineers are in a group that is named S3-access. The cloud engineers must use MFA to perform any actions in Amazon S3.

Which solution will meet these requirements?

- A. Attach a policy to the S3 bucket to prompt the IAM user for an MFA code when the IAM user performs actions on the S3 bucket. Use IAM access keys with the AWS CLI to call Amazon S3.
- B. Update the trust policy for the S3-access group to require principals to use MFA when principals assume the group. Use IAM access keys with the AWS CLI to call Amazon S3.
- C. Attach a policy to the S3-access group to deny all S3 actions unless MFA is present. Use IAM access keys with the AWS CLI to call Amazon S3.
- D. Attach a policy to the S3-access group to deny all S3 actions unless MFA is present. Request temporary credentials from AWS Security Token Service (AWS STS). Attach the temporary credentials in a profile that Amazon S3 will reference when the user performs actions in Amazon S3.

D

A & C are incorrect - Using IAM access keys with the AWS CLI would bypass the requirement for MFA.
B is incorrect - MFA should be required for specific actions, not just when assuming a role or group.

Question 455:

A company needs to migrate 60 on-premises legacy applications to AWS. The applications are based on the .NET Framework and run on Windows.

The company needs a solution that minimizes migration time and requires no application code changes. The company also does not want to manage the infrastructure.

Which solution will meet these requirements?

- A. Refactor the applications and containerize them by using AWS Toolkit for .NET Refactoring. Use Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to host the containerized applications.
- B. Use the Windows Web Application Migration Assistant to migrate the applications to AWS Elastic Beanstalk. Use Elastic Beanstalk to deploy and manage the applications.
- C. Use the Windows Web Application Migration Assistant to migrate the applications to Amazon EC2 instances. Use the EC2 instances to deploy and manage the applications.
- D. Refactor the applications and containerize them by using AWS Toolkit for .NET Refactoring. Use Amazon Elastic Kubernetes Service (Amazon EKS) with the Fargate launch type to host the containerized applications.

B

<https://github.com/awslabs/windows-web-app-migration-assistant>

AWS Elastic Beanstalk Overview



- Elastic Beanstalk is a developer centric view of deploying an application on AWS
- It uses all the component's we've seen before: EC2, Auto Scaling Group, Elastic Load Balancers, RDS, etc...
- But it's all in one view that's easy to make sense of!
- We still have full control over the configuration of each component
- Beanstalk is free but you pay for the underlying instances

Question 456:

A company needs to run large batch-processing jobs on data that is stored in an Amazon S3 bucket. The jobs perform simulations. The results of the jobs are not time sensitive, and the process can withstand interruptions.

Each job must process 15-20 GB of data when the data is stored in the S3 bucket. The company will store the output from the jobs in a different Amazon S3 bucket for further analysis.

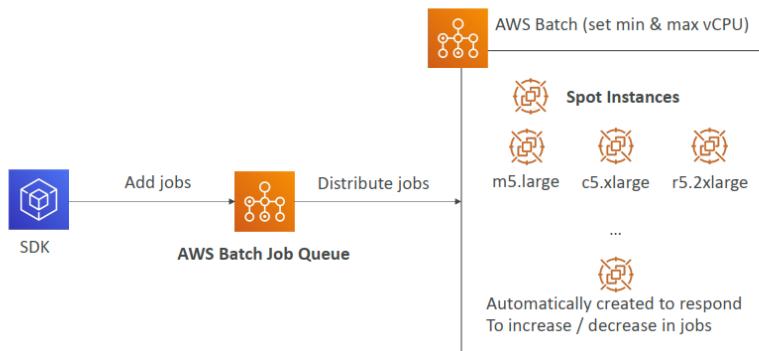
Which solution will meet these requirements MOST cost-effectively?

- A. Create a serverless data pipeline. Use AWS Step Functions for orchestration. Use AWS Lambda functions with provisioned capacity to process the data.
- B. Create an AWS Batch compute environment that includes Amazon EC2 Spot Instances. Specify the SPOT_CAPACITY_OPTIMIZED allocation strategy.
- C. Create an AWS Batch compute environment that includes Amazon EC2 On-Demand Instances and Spot Instances. Specify the SPOT_CAPACITY_OPTIMIZED allocation strategy for the Spot Instances.
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) to run the processing jobs. Use managed node groups that contain a combination of Amazon EC2 On-Demand Instances and Spot Instances.

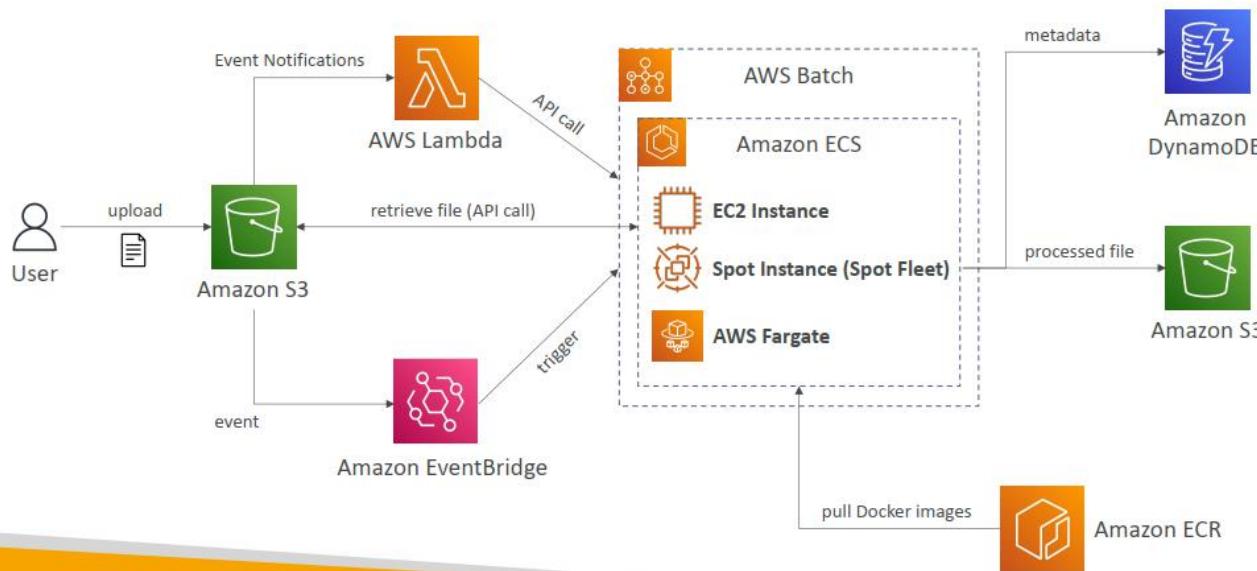
B

<https://aws.amazon.com/blogs/compute/cost-effective-batch-processing-with-amazon-ec2-spot/>

AWS Batch – Managed Compute Environment



AWS Batch – Solution Architecture



Question 457:

A company has an application that analyzes and stores image data on premises. The application receives millions of new image files every day. Files are an average of 1 MB in size. The files are analyzed in batches of 1 GB. When the application analyzes a batch, the application zips the images together. The application then archives the images as a single file in an on-premises NFS server for long-term storage.

The company has a Microsoft Hyper-V environment on premises and has compute capacity available. The company does not have storage capacity and wants to archive the images on AWS. The company needs the ability to retrieve archived data within 1 week of a request.

The company has a 10 Gbps AWS Direct Connect connection between its on-premises data center and AWS. The company needs to set bandwidth limits and schedule archived images to be copied to AWS during non-business hours.

Which solution will meet these requirements MOST cost-effectively?

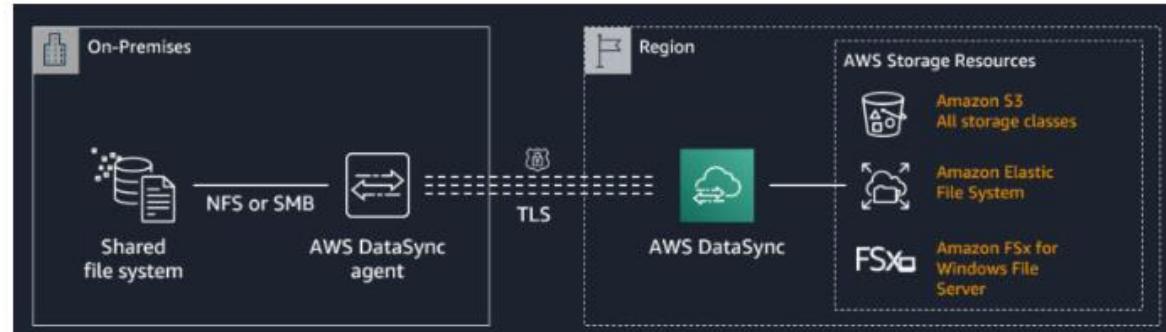
- A. Deploy an AWS DataSync agent on a new GPU-based Amazon EC2 instance. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Glacier Instant Retrieval. After the successful copy, delete the data from the on-premises storage.
- B. Deploy an AWS DataSync agent as a Hyper-V VM on premises. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Glacier Deep Archive. After the successful copy, delete the data from the on-premises storage.
- C. Deploy an AWS DataSync agent on a new general purpose Amazon EC2 instance. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Standard. After the successful copy, delete the data from the on-premises storage. Create an S3 Lifecycle rule to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 day.
- D. Deploy an AWS Storage Gateway Tape Gateway on premises in the Hyper-V environment. Connect the Tape Gateway to AWS. Use automatic tape creation. Specify an Amazon S3 Glacier Deep Archive pool. Eject the tape after the batch of images is copied.

B

<https://aws.amazon.com/blogs/storage/protect-your-file-and-backup-archives-using-aws-datasync-and-amazon-s3-glacier/>

The company does not have storage capacity and wants to archive the images on AWS. → DataSync

The company needs the ability to retrieve archived data within 1 week of a request → Amazon S3 Glacier Deep Archive



Question 458:

A company wants to record key performance indicators (KPIs) from its application as part of a strategy to convert to a user-based licensing schema. The application is a multi-tier application with a web-based UI. The company saves all log files to Amazon CloudWatch by using the CloudWatch agent. All logins to the application are saved in a log file.

As part of the new license schema, the company needs to find out how many unique users each client has on a daily basis, weekly basis, and monthly basis.

Which solution will provide this information with the LEAST change to the application?

- A. Configure an Amazon CloudWatch Logs metric filter that saves each successful login as a metric. Configure the user name and client name as dimensions for the metric.
- B. Change the application logic to make each successful login generate a call to the AWS SDK to increment a custom metric that records user name and client name dimensions in CloudWatch.
- C. Configure the CloudWatch agent to extract successful login metrics from the logs. Additionally, configure the CloudWatch agent to save the successful login metrics as a custom metric that uses the user name and client name as dimensions for the metric.
- D. Configure an AWS Lambda function to consume an Amazon CloudWatch Logs stream of the application logs. Additionally, configure the Lambda function to increment a custom metric in CloudWatch that uses the user name and client name as dimensions for the metric.

A

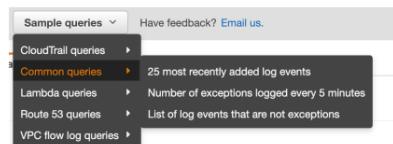
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringLogData.html>

You can search and filter the log data coming into CloudWatch Logs by creating one or more metric filters. Metric filters define the terms and patterns to look for in log data as it is sent to CloudWatch Logs. CloudWatch Logs uses these metric filters to turn log data into numerical CloudWatch metrics that you can graph or set an alarm on.

When you create a metric from a log filter, you can also choose to assign dimensions and a unit to the metric. If you specify a unit, be sure to specify the correct one when you create the filter. Changing the unit for the filter later will have no effect.

CloudWatch Logs Metric Filter & Insights

- CloudWatch Logs can use filter expressions
 - For example, find a specific IP inside of a log
 - Or count occurrences of "ERROR" in your logs
 - Metric filters can be used to trigger alarms
- CloudWatch Logs Insights can be used to query logs and add queries to CloudWatch Dashboards



Question 459:

A company is using GitHub Actions to run a CI/CD pipeline that accesses resources on AWS. The company has an IAM user that uses a secret key in the pipeline to authenticate to AWS. An existing IAM role with an attached policy grants the required permissions to deploy resources.

The company's security team implements a new requirement that pipelines can no longer use long-lived secret keys. A solutions architect must replace the secret key with a short-lived solution.

Which solution will meet these requirements with the LEAST operational overhead?

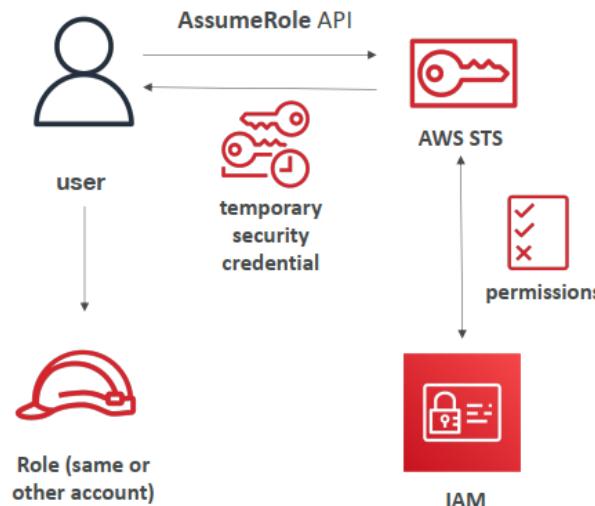
- A. Create an IAM SAML 2.0 identity provider (IdP) in AWS Identity and Access Management (IAM). Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRole API call. Attach the existing IAM policy to the new IAM role. Update GitHub to use SAML authentication for the pipeline.
- B. Create an IAM OpenID Connect (OIDC) identity provider (IdP) in AWS Identity and Access Management (IAM). Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub OIDC IdP. Update GitHub to assume the role for the pipeline.
- C. Create an Amazon Cognito identity pool. Configure the authentication provider to use GitHub. Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub authentication provider. Configure the pipeline to use Cognito as its authentication provider.
- D. Create a trust anchor to AWS Private Certificate Authority. Generate a client certificate to use with AWS IAM Roles Anywhere. Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRole API call. Attach the existing IAM policy to the new IAM role. Configure the pipeline to use the credential helper tool and to reference the client certificate public key to assume the new IAM role.

B

a new requirement that pipelines can no longer use long-lived secret keys ➔ IAM STS

Using STS to Assume a Role

- Define an IAM Role within your account or cross-account
- Define which principals can access this IAM Role
- Use AWS STS (Security Token Service) to retrieve credentials and impersonate the IAM Role you have access to (**AssumeRole API**)
- Temporary credentials can be valid between 15 minutes to 12 hour



Question 460:

A company is running a web-crawling process on a list of target URLs to obtain training documents for machine learning training algorithms. A fleet of Amazon EC2 t2.micro instances pulls the target URLs from an Amazon Simple Queue Service (Amazon SQS) queue. The instances then write the result of the crawling algorithm as a .csv file to an Amazon Elastic File System (Amazon EFS) volume. The EFS volume is mounted on all instances of the fleet.

A separate system adds the URLs to the SQS queue at infrequent rates. The instances crawl each URL in 10 seconds or less.

Metrics indicate that some instances are idle when no URLs are in the SQS queue. A solutions architect needs to redesign the architecture to optimize costs.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Use m5.8xlarge instances instead of t2.micro instances for the web-crawling process. Reduce the number of instances in the fleet by 50%.
- B. Convert the web-crawling process into an AWS Lambda function. Configure the Lambda function to pull URLs from the SQS queue.
- C. Modify the web-crawling process to store results in Amazon Neptune.
- D. Modify the web-crawling process to store results in an Amazon Aurora Serverless MySQL instance.
- E. Modify the web-crawling process to store results in Amazon S3.

B, E

use lambda instead of a fleet of EC2, and store the results into cost-effective S3
crawling algorithm as a .csv file to an Amazon Elastic File System (Amazon EFS) volume → store results in Amazon S3

Question 461:

A company needs to migrate its website from an on-premises data center to AWS. The website consists of a load balancer, a content management system (CMS) that runs on a Linux operating system, and a MySQL database.

The CMS requires persistent NFS-compatible storage for a file system. The new solution on AWS must be able to scale from 2 Amazon EC2 instances to 30 EC2 instances in response to unpredictable traffic increases. The new solution also must require no changes to the website and must prevent data loss.

Which solution will meet these requirements?

- A. Create an Amazon Elastic File System (Amazon EFS) file system. Deploy the CMS to AWS Elastic Beanstalk with an Application Load Balancer and an Auto Scaling group. Use .ebextensions to mount the EFS file system to the EC2 instances. Create an Amazon Aurora MySQL database that is separate from the Elastic Beanstalk environment.
- B. Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume. Deploy the CMS to AWS Elastic Beanstalk with a Network Load Balancer and an Auto Scaling group. Use .ebextensions to mount the EBS volume to the EC2 instances. Create an Amazon RDS for MySQL database in the Elastic Beanstalk environment.
- C. Create an Amazon Elastic File System (Amazon EFS) file system. Create a launch template and an Auto Scaling group to launch EC2 instances to support the CMS. Create a Network Load Balancer to distribute traffic. Create an Amazon Aurora MySQL database. Use an EC2 Auto Scaling scale-in lifecycle hook to mount the EFS file system to the EC2 instances.

D. Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume. Create a launch template and an Auto Scaling group to launch EC2 instances to support the CMS. Create an Application Load Balancer to distribute traffic. Create an Amazon ElastiCache for Redis cluster to support the MySQL database. Use EC2 user data to attach the EBS volume to the EC2 instances.

A

CMS requires persistent NFS-compatible storage for a file system → EFS

AWS Elastic Beanstalk Overview



- Elastic Beanstalk is a developer centric view of deploying an application on AWS
- It uses all the component's we've seen before: EC2, Auto Scaling Group, Elastic Load Balancers, RDS, etc...
- But it's all in one view that's easy to make sense of!
- We still have full control over the configuration of each component
- Beanstalk is free but you pay for the underlying instances

Question 462:

A company needs to implement disaster recovery for a critical application that runs in a single AWS Region. The application's users interact with a web frontend that is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The application writes to an Amazon RDS for MySQL DB instance. The application also outputs processed documents that are stored in an Amazon S3 bucket.

The company's finance team directly queries the database to run reports. During busy periods, these queries consume resources and negatively affect application performance.

A solutions architect must design a solution that will provide resiliency during a disaster. The solution must minimize data loss and must resolve the performance problems that result from the finance team's queries.

Which solution will meet these requirements?

A. Migrate the database to Amazon DynamoDB and use DynamoDB global tables. Instruct the finance team to query a global table in a separate Region. Create an AWS Lambda function to periodically synchronize the contents of the original S3 bucket to a new S3 bucket in the separate Region. Launch EC2 instances and create an ALB in the separate Region. Configure the application to point to the new S3 bucket.

B. Launch additional EC2 instances that host the application in a separate Region. Add the additional instances to the existing ALB in the separate Region, create a read replica of the RDS DB instance. Instruct the finance team to run queries against the read replica. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, promote the read replica to a standalone DB instance. Configure the application to point to the new S3 bucket and to the newly promoted read replica.

C. Create a read replica of the RDS DB instance in a separate Region. Instruct the finance team to run queries against the read replica. Create AMIs of the EC2 instances that host the application frontend. Copy the AMIs to the separate Region. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, promote the read replica to a standalone DB instance. Launch EC2 instances from the AMIs and create an ALB to present the application to end users. Configure the application to point to the new S3 bucket.

D. Create hourly snapshots of the RDS DB instance. Copy the snapshots to a separate Region. Add an Amazon ElastiCache cluster in front of the existing RDS database. Create AMIs of the EC2 instances that host the application frontend. Copy the AMIs to the separate Region. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, restore the database from the latest RDS snapshot. Launch EC2 instances from the AMIs and create an ALB to present the application to end users. Configure the application to point to the new S3 bucket.

C
disaster recovery → read replica of the RDS DB instance in a separate Region, S3 Cross-Region Replication (CRR), create EC2 instances in the separate Region.

Question 463:

A company has many services running in its on-premises data center. The data center is connected to AWS using AWS Direct Connect (DX) and an IPSec VPN. The service data is sensitive and connectivity cannot traverse the internet. The company wants to expand into a new market segment and begin offering its services to other companies that are using AWS.

Which solution will meet these requirements?

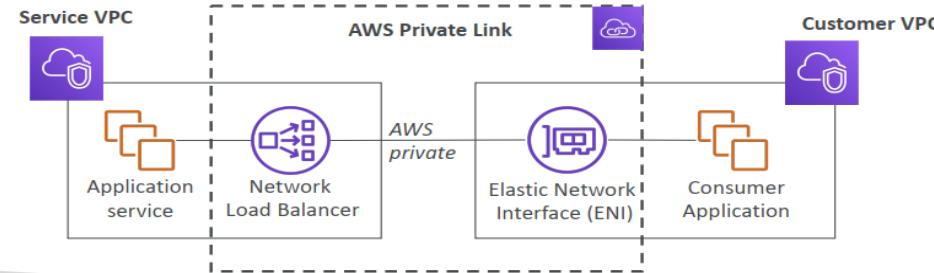
- A. Create a VPC Endpoint Service that accepts TCP traffic, host it behind a Network Load Balancer, and make the service available over DX.
- B. Create a VPC Endpoint Service that accepts HTTP or HTTPS traffic, host it behind an Application Load Balancer, and make the service available over DX.
- C. Attach an internet gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.
- D. Attach a NAT gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.

A
connectivity cannot traverse the internet → VPC Endpoint Service (Private Link)
VPC endpoint used with NLB

AWS PrivateLink (VPC Endpoint Services)



- Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts)
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)
- If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!



Question 464:

A company uses AWS Organizations to manage its AWS accounts. A solutions architect must design a solution in which only administrator roles are allowed to use IAM actions. However, the solutions architect does not have access to all the AWS accounts throughout the company.

Which solution meets these requirements with the LEAST operational overhead?

- Create an SCP that applies to all the AWS accounts to allow IAM actions only for administrator roles. Apply the SCP to the root OU.
- Configure AWS CloudTrail to invoke an AWS Lambda function for each event that is related to IAM actions. Configure the function to deny the action if the user who invoked the action is not an administrator.
- Create an SCP that applies to all the AWS accounts to deny IAM actions for all users except for those with administrator roles. Apply the SCP to the root OU.
- Set an IAM permissions boundary that allows IAM actions. Attach the permissions boundary to every administrator role across all the AWS accounts.

C

A: SCPs don't allow, they deny B: is reactive, not preventive C: is correct D: Boundary Permissions don't allow, they set maximum permissions.

Service Control Policies (SCP)

- Define allowlist or blocklist IAM actions
- Applied at the OU or Account level
- Does not apply to the Management Account
- SCP is applied to all the Users and Roles in the account, including Root user
- The SCP does not affect Service-linked roles
 - Service-linked roles enable other AWS services to integrate with AWS Organizations and can't be restricted by SCPs.
- SCP must have an explicit Allow (does not allow anything by default)
(adj): rõ ràng, rành mạch
- Use cases:
 - Restrict access to certain services (for example: can't use EMR)
 - Enforce PCI compliance by explicitly disabling services

Question 465:

A company uses an organization in AWS Organizations to manage multiple AWS accounts. The company hosts some applications in a VPC in the company's shared services account.

The company has attached a transit gateway to the VPC in the shared services account.

The company is developing a new capability and has created a development environment that requires access to the applications that are in the shared services account. The company intends to delete and recreate resources frequently in the development account. The company also wants to give a development team the ability to recreate the team's connection to the shared services account as required.

Which solution will meet these requirements?

- A. Create a transit gateway in the development account. Create a transit gateway peering request to the shared services account. Configure the shared services transit gateway to automatically accept peering connections.
- B. Turn on automatic acceptance for the transit gateway in the shared services account. Use AWS Resource Access Manager (AWS RAM) to share the transit gateway resource in the shared services account with the development account. Accept the resource in the development account. Create a transit gateway attachment in the development account.
- C. Turn on automatic acceptance for the transit gateway in the shared services account. Create a VPC endpoint. Use the endpoint policy to grant permissions on the VPC endpoint for the development account. Configure the endpoint service to automatically accept connection requests. Provide the endpoint details to the development team.

D. Create an Amazon EventBridge rule to invoke an AWS Lambda function that accepts the transit gateway attachment when the development account makes an attachment request. Use AWS Network Manager to share the transit gateway in the shared services account with the development account. Accept the transit gateway in the development account.

B

A is incorrect: creating and managing another transit gateway in the development account and setting up peering. This adds unnecessary complexity and management overhead.

B is correct: the development account can create transit gateway attachments without needing manual intervention every time an attachment is made.

C is incorrect: Not usecase of VPC endpoints. VPC endpoints are typically used for connecting to AWS services privately without traversing the public internet. This option does not align well with the requirement to access applications in a VPC through a transit gateway.

D is incorrect: too complicated

Question 466:

A company wants to migrate virtual Microsoft workloads from an on-premises data center to AWS. The company has successfully tested a few sample workloads on AWS. The company also has created an AWS Site-to-Site VPN connection to a VPC. A solutions architect needs to generate a total cost of ownership (TCO) report for the migration of all the workloads from the data center.

Simple Network Management Protocol (SNMP) has been enabled on each VM in the data center. The company cannot add more VMs in the data center and cannot install additional software on the VMs. The discovery data must be automatically imported into AWS Migration Hub.

Which solution will meet these requirements?

- A. Use the AWS Application Migration Service agentless service and the AWS Migration Hub Strategy Recommendations to generate the TCO report.
- B. Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Evaluator to generate the TCO report.
- C. Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Hub to generate the TCO report.
- D. Use the AWS Migration Readiness Assessment tool inside the VPC. Configure Migration Evaluator to generate the TCO report.

B

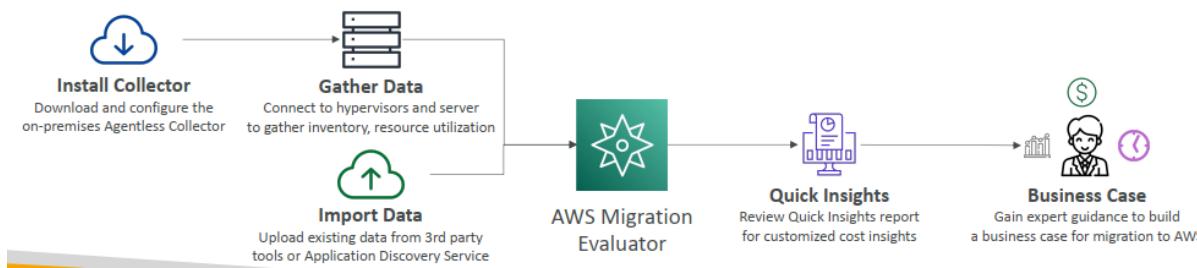
agentless collector to scan the on-premise VMs using SNMP:

AWS Migration Evaluator



dựa trên dữ liệu

- Helps you build a data-driven business case for migration to AWS
- Provides a clear baseline of what your organization is running today
- Install Agentless Collector to conduct broad-based discovery
- Take a snapshot of on-premises foot-print, server dependencies, ...
- Analyze current state, define target state, then develop migration plan



Question 467:

A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets are served from a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The company requires game assets to be fetched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region.

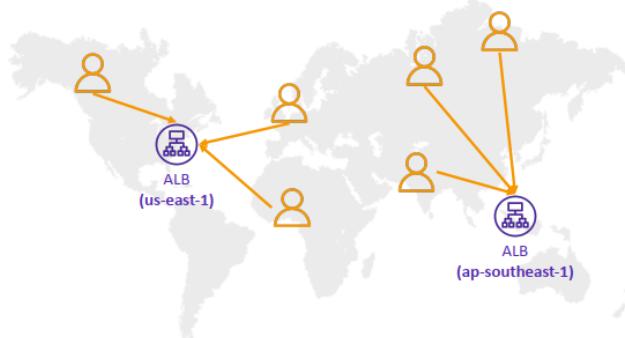
What should a solutions architect do to meet these requirements?

- Create an Amazon CloudFront distribution. Create an origin group with one origin for each ALB. Set one of the origins as primary.
- Create an Amazon Route 53 health check for each ALB. Create a Route 53 failover routing record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.
- Create two Amazon CloudFront distributions, each with one ALB as the origin. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions. Set the Evaluate Target Health value to Yes.
- Create an Amazon Route 53 health check for each ALB. Create a Route 53 latency alias record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.

D

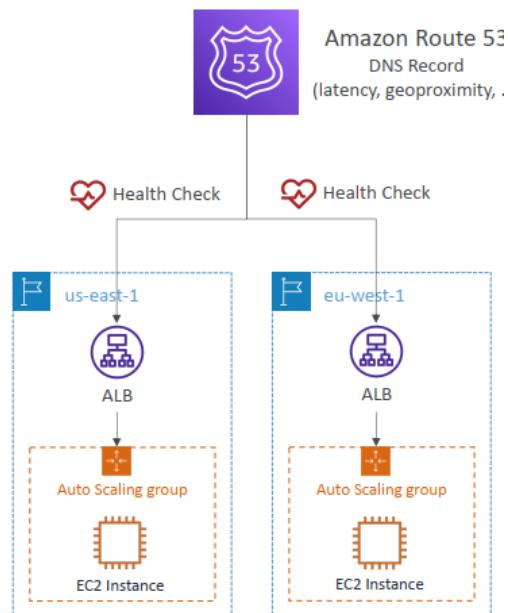
Routing Policies – Latency-based

- Redirect to the resource that has the least latency close to us
- Super helpful when latency for users is a priority
- Latency is based on traffic between users and AWS Regions
- Germany users may be directed to the US (if that's the lowest latency)
- Can be associated with Health Checks (has a failover capability)



Route 53 – Health Checks

- HTTP Health Checks are only for public resources
- Health Check => Automated DNS Failover:
 1. Health checks that monitor an endpoint (application, server, other AWS resource)
 2. Health checks that monitor other health checks (Calculated Health Checks)
 3. Health checks that monitor CloudWatch Alarms (full control !!) – e.g., throttles of DynamoDB, alarms on RDS, custom metrics, ... (helpful for private resources)
- Health Checks are integrated with CW metrics



Question 468:

A company deploys workloads in multiple AWS accounts. Each account has a VPC with VPC flow logs published in text log format to a centralized Amazon S3 bucket. Each log file is compressed with gzip compression. The company must retain the log files indefinitely.

A security engineer occasionally analyzes the logs by using Amazon Athena to query the VPC flow logs. The query performance is degrading over time as the number of ingested logs is growing. A solutions architect must improve the performance of the log analysis and reduce the storage space that the VPC flow logs use.

Which solution will meet these requirements with the LARGEST performance improvement?

- A. Create an AWS Lambda function to decompress the gzip files and to compress the files with bzip2 compression. Subscribe the Lambda function to an s3:ObjectCreated:Put S3 event notification for the S3 bucket.
- B. Enable S3 Transfer Acceleration for the S3 bucket. Create an S3 Lifecycle configuration to move files to the S3 Intelligent-Tiering storage class as soon as the files are uploaded.
- C. Update the VPC flow log configuration to store the files in Apache Parquet format. Specify hourly partitions for the log files.
- D. Create a new Athena workgroup without data usage control limits. Use Athena engine version 2.

C

VPC Flow Logs



- Capture information about IP traffic going into your interfaces:
 - VPC Flow Logs
 - Subnet Flow Logs
 - Elastic Network Interface (ENI) Flow Logs
- Helps to monitor & troubleshoot connectivity issues
- Flow logs data can go to S3, CloudWatch Logs, and Kinesis Data Firehose
- Captures network information from AWS managed interfaces too: ELB, RDS, ElastiCache, Redshift, WorkSpaces, NATGW, Transit Gateway ...

Amazon Athena – Performance Improvement

- Use **columnar data** for cost-savings (less scan)
 - Apache Parquet or ORC is recommended
 - Huge performance improvement
 - Use Glue to convert your data to Parquet or ORC
- Compress data for smaller retrievals (bzip2, gzip, lz4, snappy, zlib, zstd...)
- Partition datasets in S3 for easy querying on virtual columns
 - s3://yourBucket/pathToTable /<PARTITION_COLUMN_NAME>=<VALUE> /<PARTITION_COLUMN_NAME>=<VALUE> /<PARTITION_COLUMN_NAME>=<VALUE> /etc...
 - Example: s3://athena-examples/flight/parquet/year=1991/month=1/day=1/
- Use larger files (> 128 MB) to minimize overhead

<https://aws.amazon.com/about-aws/whats-new/2021/10/amazon-vpc-flow-logs-parquet-hive-prefixes-partitioned-files/>

Question 469:

A company wants to establish a dedicated connection between its on-premises infrastructure and AWS. The company is setting up a 1 Gbps AWS Direct Connect connection to its account VPC. The architecture includes a transit gateway and a Direct Connect gateway to connect multiple VPCs and the on-premises infrastructure.

The company must connect to VPC resources over a transit VIF by using the Direct Connect connection.

Which combination of steps will meet these requirements? (Choose two.)

- Update the 1 Gbps Direct Connect connection to 10 Gbps.
- Advertise the on-premises network prefixes over the transit VIF.
- Advertise the VPC prefixes from the Direct Connect gateway to the on-premises network over the transit VIF.
- Update the Direct Connect connection's MACsec encryption mode attribute to must_encrypt.
- Associate a MACsec Connection Key Name/Connectivity Association Key (CKN/CAK) pair with the Direct Connect connection.

B,C
just need to add routing at both sides.

<https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html>

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-transit-gateways.html>

Question 470:

A company wants to use Amazon WorkSpaces in combination with thin client devices to replace aging desktops. Employees use the desktops to access applications that work with Clinical trial data. Corporate security policy states that access to the applications must be restricted to only company branch office locations. The company is considering adding an additional branch office in the next 6 months.

Which solution meets these requirements with the MOST operational efficiency?

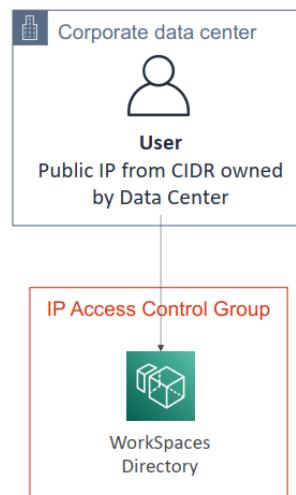
- A. Create an IP access control group rule with the list of public addresses from the branch offices. Associate the IP access control group with the WorkSpaces directory.
- B. Use AWS Firewall Manager to create a web ACL rule with an IPSet with the list of public addresses from the branch office locations. Associate the web ACL with the WorkSpaces directory.
- C. Use AWS Certificate Manager (ACM) to issue trusted device certificates to the machines deployed in the branch office locations. Enable restricted access on the WorkSpaces directory.
- D. Create a custom WorkSpace image with Windows Firewall configured to restrict access to the public addresses of the branch offices. Use the image to deploy the WorkSpaces.

A

<https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-ip-access-control-groups.html>

Amazon WorkSpaces IP Access Control Groups

- Similar to security groups for Amazon WorkSpaces
- List of IP addresses / CIDR address ranges that users are authorized to connect from
- If users access WorkSpaces through VPN or NAT, the IP Access Control Group must authorize the public IP of these



Question 471:

A company uses AWS Organizations. The company runs two firewall appliances in a centralized networking account. Each firewall appliance runs on a manually configured highly available Amazon EC2 instance. A transit gateway connects the VPC from the centralized networking account to VPCs of member accounts. Each firewall appliance uses a static private IP address that is then used to route traffic from the member accounts to the internet.

During a recent incident, a badly configured script initiated the termination of both firewall appliances. During the rebuild of the firewall appliances, the company wrote a new script to configure the firewall appliances at startup.

The company wants to modernize the deployment of the firewall appliances. The firewall appliances need the ability to scale horizontally to handle increased traffic when the network expands. The company must continue to use the firewall appliances to comply with company policy. The provider of the firewall appliances has confirmed that the latest version of the firewall code will work with all AWS services.

Which combination of steps should the solutions architect recommend to meet these requirements MOST cost-effectively? (Choose three.)

- A. Deploy a Gateway Load Balancer in the centralized networking account. Set up an endpoint service that uses AWS PrivateLink.
- B. Deploy a Network Load Balancer in the centralized networking account. Set up an endpoint service that uses AWS PrivateLink.
- C. Create an Auto Scaling group and a launch template that uses the new script as user data to configure the firewall appliances. Create a target group that uses the instance target type.
- D. Create an Auto Scaling group. Configure an AWS Launch Wizard deployment that uses the new script as user data to configure the firewall appliances. Create a target group that uses the IP target type.
- E. Create VPC endpoints in each member account. Update the route tables to point to the VPC endpoints.
- F. Create VPC endpoints in the centralized networking account. Update the route tables in each member account to point to the VPC endpoints.

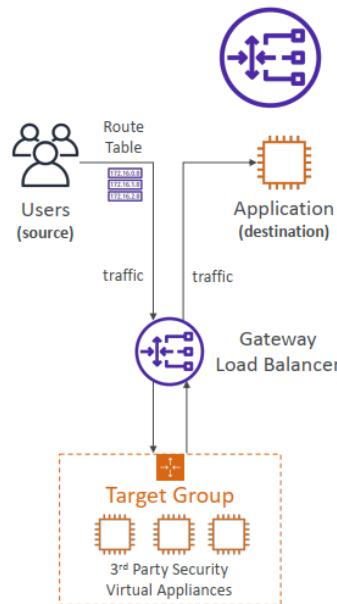
A,C,F

firewall appliances → Gateway load balancer

The firewall appliances need the ability to scale horizontally to handle increased traffic when the network expands → Auto Scaling Group

Gateway Load Balancer

- Deploy, scale, and manage a fleet of 3rd party network virtual appliances in AWS
- Example: Firewalls, Intrusion Detection and Prevention Systems, Deep Packet Inspection Systems, payload manipulation, ...
- Operates at Layer 3 (Network Layer) – IP Packets
- Combines the following functions:
 - Transparent Network Gateway – single entry/exit for all traffic
 - Load Balancer – distributes traffic to your virtual appliances
- Uses the GENEVE protocol on port 6081



Shane Maarek

Question 472:

A solutions architect must implement a multi-Region architecture for an Amazon RDS for PostgreSQL database that supports a web application. The database launches from an AWS CloudFormation template that includes AWS services and features that are present in both the primary and secondary Regions.

The database is configured for automated backups, and it has an RTO of 15 minutes and an RPO of 2 hours. The web application is configured to use an Amazon Route 53 record to route traffic to the database.

Which combination of steps will result in a highly available architecture that meets all the requirements? (Choose two.)

- Create a cross-Region read replica of the database in the secondary Region. Configure an AWS Lambda function in the secondary Region to promote the read replica during a failover event.
- In the primary Region, create a health check on the database that will invoke an AWS Lambda function when a failure is detected. Program the Lambda function to recreate the database from the latest database snapshot in the secondary Region and update the Route 53 host records for the database.
- Create an AWS Lambda function to copy the latest automated backup to the secondary Region every 2 hours.
- Create a failover routing policy in Route 53 for the database DNS record. Set the primary and secondary endpoints to the endpoints in each Region.
- Create a hot standby database in the secondary Region. Use an AWS Lambda function to restore the secondary database to the latest RDS automatic backup in the event that the primary database fails.

A,D

multi-Region architecture ➔ a cross-Region read replica of the database, failover routing policy in Route 53

Question 473:

An ecommerce company runs an application on AWS. The application has an Amazon API Gateway API that invokes an AWS Lambda function. The data is stored in an Amazon RDS for PostgreSQL DB instance.

During the company's most recent flash sale, a sudden increase in API calls negatively affected the application's performance. A solutions architect reviewed the Amazon CloudWatch metrics during that time and noticed a significant increase in Lambda invocations and database connections. The CPU utilization also was high on the DB instance.

What should the solutions architect recommend to optimize the application's performance?

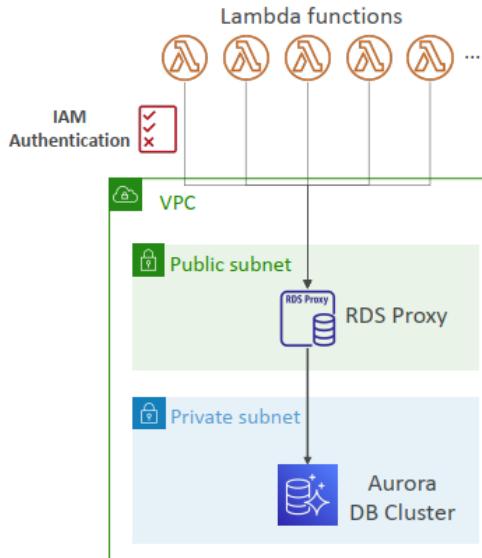
- A. Increase the memory of the Lambda function. Modify the Lambda function to close the database connections when the data is retrieved.
- B. Add an Amazon ElastiCache for Redis cluster to store the frequently accessed data from the RDS database.
- C. Create an RDS proxy by using the Lambda console. Modify the Lambda function to use the proxy endpoint.
- D. Modify the Lambda function to connect to the database outside of the function's handler. Check for an existing database connection before creating a new connection.

C

noticed a significant increase in Lambda invocations and database connections. ➔ RDS proxy

RDS Proxy for AWS Lambda

- When using Lambda functions with RDS, it opens and maintains a database connection
- This can result in a “TooManyConnections” exception
- With [RDS Proxy](#), you no longer need code that handles cleaning up idle connections and managing connection pools
- Supports IAM authentication or DB authentication, auto-scaling
- The Lambda function must have connectivity to the Proxy (public proxy => public Lambda, private proxy => Lambda in VPC)



Question 474:

A retail company wants to improve its application architecture. The company's applications register new orders, handle returns of merchandise, and provide analytics. The applications store retail data in a MySQL database and an Oracle OLAP analytics database. All the applications and databases are hosted on Amazon EC2 instances.

Each application consists of several components that handle different parts of the order process. These components use incoming data from different sources. A separate ETL job runs every week and copies data from each application to the analytics database.

A solutions architect must redesign the architecture into an event-driven solution that uses serverless services. The solution must provide updated analytics in near real time.

Which solution will meet these requirements?

- Migrate the individual applications as microservices to Amazon Elastic Container Service (Amazon ECS) containers that use AWS Fargate. Keep the retail MySQL database on Amazon EC2. Move the analytics database to Amazon Neptune. Use Amazon Simple Queue Service (Amazon SQS) to send all the incoming data to the microservices and the analytics database.
- Create an Auto Scaling group for each application. Specify the necessary number of EC2 instances in each Auto Scaling group. Migrate the retail MySQL database and the analytics database to Amazon Aurora MySQL. Use Amazon Simple Notification Service (Amazon SNS) to send all the incoming data to the correct EC2 instances and the analytics database.

C. Migrate the individual applications as microservices to Amazon Elastic Kubernetes Service (Amazon EKS) containers that use AWS Fargate. Migrate the retail MySQL database to Amazon Aurora Serverless MySQL. Migrate the analytics database to Amazon Redshift Serverless. Use Amazon EventBridge to send all the incoming data to the microservices and the analytics database.

D. Migrate the individual applications as microservices to Amazon AppStream 2.0. Migrate the retail MySQL database to Amazon Aurora MySQL. Migrate the analytics database to Amazon Redshift Serverless. Use AWS IoT Core to send all the incoming data to the microservices and the analytics database.

C

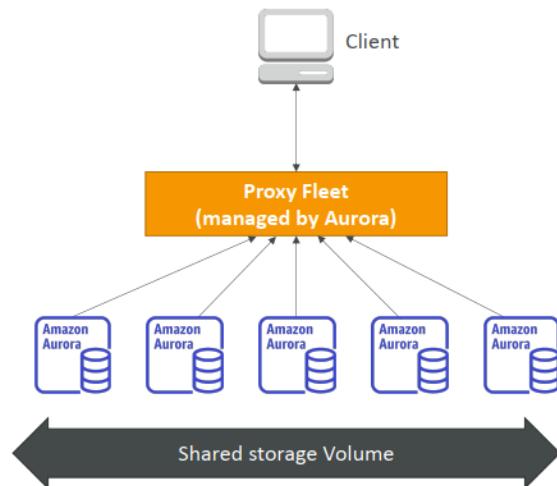
event-driven solution that uses serverless services → EventBridge, Aurora Serverless.

OLAP analytics database → Redshift

A, B are wrong because not serverless

Aurora Serverless

- Automated database instantiation and auto-scaling based on actual usage
- Good for infrequent, intermittent or unpredictable workloads
- No capacity planning needed
- Pay per second, can be more cost-effective



Redshift Overview

- Redshift is based on PostgreSQL, but it's not used for OLTP
- It's OLAP – online analytical processing (analytics and data warehousing)
- 10x better performance than other data warehouses, scale to PBs of data
- Columnar storage of data (instead of row based)
- Massively Parallel Query Execution (MPP)
- Pay as you go based on the instances provisioned
- Has a SQL interface for performing the queries
- BI tools such as AWS Quicksight or Tableau integrate with it



online transaction processing

=> Redshift is
datawarehouse

Question 475:

A company is planning a migration from an on-premises data center to the AWS Cloud. The company plans to use multiple AWS accounts that are managed in an organization in AWS Organizations. The company will create a small number of accounts initially and will add accounts as needed. A solutions architect must design a solution that turns on AWS CloudTrail in all AWS accounts.

What is the MOST operationally efficient solution that meets these requirements?

- Create an AWS Lambda function that creates a new CloudTrail trail in all AWS accounts in the organization. Invoke the Lambda function daily by using a scheduled action in Amazon EventBridge.
- Create a new CloudTrail trail in the organization's management account. Configure the trail to log all events for all AWS accounts in the organization.
- Create a new CloudTrail trail in all AWS accounts in the organization. Create new trails whenever a new account is created. Define an SCP that prevents deletion or modification of trails. Apply the SCP to the root OU.
- Create an AWS Systems Manager Automation runbook that creates a CloudTrail trail in all AWS accounts in the organization. Invoke the automation by using Systems Manager State Manager.

B

turns on AWS CloudTrail in all AWS accounts → Create a new CloudTrail trail in the organization's management account
<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

Question 476:

A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services (AD DS) on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC must be accessible through a VPN. Multi-factor authentication (MFA) must be used for access to a VPN.

What should a solutions architect do to meet these requirements?

- Create an AWS Site-to-Site VPN connection. Configure integration between a VPN and AD DS. Use an Amazon WorkSpaces client with MFA support enabled to establish a VPN connection.
- Create an AWS Client VPN endpoint. Create an AD Connector directory for integration with AD DS. Enable MFA for AD Connector. Use AWS Client VPN to establish a VPN connection.
- Create multiple AWS Site-to-Site VPN connections by using AWS VPN CloudHub. Configure integration between AWS VPN CloudHub and AD DS. Use AWS Copilot to establish a VPN connection.
- Create an Amazon WorkLink endpoint. Configure integration between Amazon WorkLink and AD DS. Enable MFA in Amazon WorkLink. Use AWS Client VPN to establish a VPN connection.

B

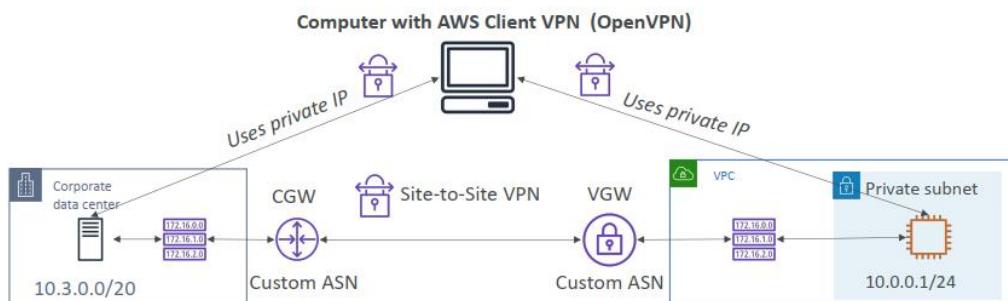
working remotely → AWS Client VPN

Client VPN provides Active Directory support by integrating with AWS Directory Service. Client VPN supports multi-factor authentication (MFA) when it's enabled for AWS Managed Microsoft AD or AD Connector.

AWS Client VPN



- Connect from your computer using OpenVPN to your private network in AWS and on-premises



<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/ad.html>

Question 477:

A company is running a three-tier web application in an on-premises data center. The frontend is served by an Apache web server, the middle tier is a monolithic Java application, and the storage tier is a PostgreSQL database.

During a recent marketing promotion, customers could not place orders through the application because the application crashed. An analysis showed that all three tiers were overloaded. The application became unresponsive, and the database reached its capacity limit because of read operations. The company already has several similar promotions scheduled in the near future.

A solutions architect must develop a plan for migration to AWS to resolve these issues. The solution must maximize scalability and must minimize operational effort

Which combination of steps will meet these requirements? (Choose three.)

A. Refactor the frontend so that static assets can be hosted on Amazon S3. Use Amazon CloudFront to serve the frontend to customers. Connect the frontend to the Java application.

B. Rehost the Apache web server of the frontend on Amazon EC2 instances that are in an Auto Scaling group. Use a load balancer in front of the Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) to host the static assets that the Apache web server needs.

C. Rehost the Java application in an AWS Elastic Beanstalk environment that includes auto scaling.

D. Refactor the Java application, Develop a Docker container to run the Java application. Use AWS Fargate to host the container.

E. Use AWS Database Migration Service (AWS DMS) to replatform the PostgreSQL database to an Amazon Aurora PostgreSQL database. Use Aurora Auto Scaling for read replicas.

F. Rehost the PostgreSQL database on an Amazon EC2 instance that has twice as much memory as the on-premises server.

A,C,E

PostgreSQL database → Amazon Aurora PostgreSQL

Frontend host on S3

Question 478:

A company is deploying a new application on AWS. The application consists of an Amazon Elastic Kubernetes Service (Amazon EKS) cluster and an Amazon Elastic Container Registry (Amazon ECR) repository. The EKS cluster has an AWS managed node group.

The company's security guidelines state that all resources on AWS must be continuously scanned for security vulnerabilities.

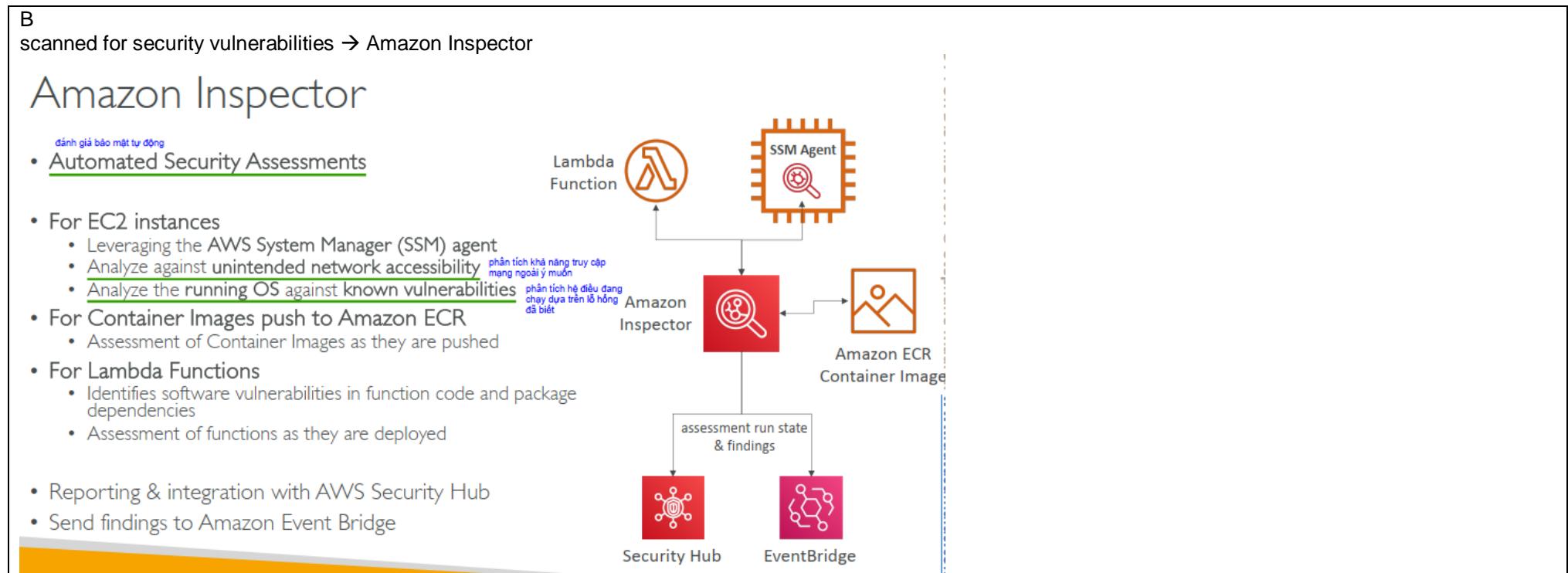
Which solution will meet this requirement with the LEAST operational overhead?

A. Activate AWS Security Hub. Configure Security Hub to scan the EKS nodes and the ECR repository.

B. Activate Amazon Inspector to scan the EKS nodes and the ECR repository.

C. Launch a new Amazon EC2 instance and install a vulnerability scanning tool from AWS Marketplace. Configure the EC2 instance to scan the EKS nodes. Configure Amazon ECR to perform a basic scan on push.

D. Install the Amazon CloudWatch agent on the EKS nodes. Configure the CloudWatch agent to scan continuously. Configure Amazon ECR to perform a basic scan on push.



Question 479:

A company needs to improve the reliability of its ticketing application. The application runs on an Amazon Elastic Container Service (Amazon ECS) cluster. The company uses Amazon CloudFront to serve the application. A single ECS service of the ECS cluster is the CloudFront distribution's origin.

The application allows only a specific number of active users to enter a ticket purchasing flow. These users are identified by an encrypted attribute in their JSON Web Token (JWT). All other users are redirected to a waiting room module until there is available capacity for purchasing.

The application is experiencing high loads. The waiting room module is working as designed, but load on the waiting room is disrupting the applications availability.

This disruption is negatively affecting the application's ticket sale transactions.

Which solution will provide the MOST reliability for ticket sale transactions during periods of high load?

HANCHE

- A. Create a separate service in the ECS cluster for the waiting room. Use a separate scaling configuration. Ensure that the ticketing service uses the JWT information and appropriately forwards requests to the waiting room service.
- B. Move the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Split the waiting room module into a pod that is separate from the ticketing pod. Make the ticketing pod part of a StatefulSet. Ensure that the ticketing pod uses the JWT information and appropriately forwards requests to the waiting room pod.
- C. Create a separate service in the ECS cluster for the waiting room. Use a separate scaling configuration. Create a CloudFront function that inspects the JWT information and appropriately forwards requests to the ticketing service or the waiting room service.
- D. Move the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Split the waiting room module into a pod that is separate from the ticketing pod. Use AWS App Mesh by provisioning the App Mesh controller for Kubernetes. Enable mTLS authentication and service-to-service authentication for communication between the ticketing pod and the waiting room pod. Ensure that the ticketing pod uses the JWT information and appropriately forwards requests to the waiting room pod.

C

- A. No mention of finer control at the CloudFront level
- B. When it comes to migrating to EKS, it may bring additional complexity and cost.
- C. It combines the flexibility of ECS and the edge computing capability of CloudFront.
- D. It involves complex migration, configuration, and authentication mechanisms.

CloudFront Functions: You can validate hashed authorization tokens, such as JSON web tokens (JWT), by inspecting authorization headers or other request metadata.
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cloudfront-functions.html>

CloudFront Functions vs. Lambda@Edge – Use Cases

CloudFront Functions

- Cache key normalization
 - Transform request attributes (headers, cookies, query strings, URL) to create an optimal Cache Key
- Header manipulation thao tác
 - Insert/modify/delete HTTP headers in the request or response
- URL rewrites or redirects
- Request authentication & authorization
 - Create and validate user-generated tokens (e.g., JWT) to allow/deny requests

Lambda@Edge

- Longer execution time (several ms)
- Adjustable CPU or memory
- Your code depends on a 3rd libraries (e.g., AWS SDK to access other AWS services)
- Network access to use external services for processing
- File system access or access to the body of HTTP requests

Question 480:

A solutions architect is creating an AWS CloudFormation template from an existing manually created non-production AWS environment. The CloudFormation template can be destroyed and recreated as needed. The environment contains an Amazon EC2 instance. The EC2 instance has an instance profile that the EC2 instance uses to assume a role in a parent account.

The solutions architect recreates the role in a CloudFormation template and uses the same role name. When the CloudFormation template is launched in the child account, the EC2 instance can no longer assume the role in the parent account because of insufficient permissions

What should the solutions architect do to resolve this issue?

- A. In the parent account, edit the trust policy for the role that the EC2 instance needs to assume. Ensure that the target role ARN in the existing statement that allows the sts:AssumeRole action is correct. Save the trust policy.
- B. In the parent account, edit the trust policy for the role that the EC2 instance needs to assume. Add a statement that allows the sts:AssumeRole action for the root principal of the child account. Save the trust policy.
- C. Update the CloudFormation stack again. Specify only the CAPABILITY_NAMED_IAM capability.
- D. Update the CloudFormation stack again. Specify the CAPABILITY_IAM capability and the CAPABILITY_NAMED_IAM capability.

A

The error occurs because the trust relationship in the parent account that allows the EC2 instance to assume a role may have been broken or misconfigured. This can happen when a role is recreated with a different ARN but the same role name. The trust policy must be updated to reflect the correct ARN.

Option A addresses this by ensuring that the trust policy in the parent account contains the correct ARN for the role in the child account, allowing the sts:AssumeRole action.

Question 481:

A company's web application has reliability issues. The application serves customers globally. The application runs on a single Amazon EC2 instance and performs read-intensive operations on an Amazon RDS for MySQL database.

During high load, the application becomes unresponsive and requires a manual restart of the EC2 instance. A solutions architect must improve the application's reliability.

Which solution will meet this requirement with the LEAST development effort?

- A. Create an Amazon CloudFront distribution. Specify the EC2 instance as the distribution's origin. Configure a Multi-AZ deployment for the RDS for MySQL database. Use the standby DB instance for the read-intensive operations.
- B. Run the application on EC2 instances that are in an Auto Scaling group. Place the EC2 instances behind an Elastic Load Balancing (ELB) load balancer. Replace the database service with Amazon Aurora. Use Aurora Replicas for the read-intensive operations.
- C. Deploy AWS Global Accelerator. Configure a Multi-AZ deployment for the RDS for MySQL database. Use the standby DB instance for the read-intensive operations.
- D. Migrate the application to AWS Lambda functions. Create read replicas for the RDS for MySQL database. Use the read replicas for the read-intensive operations.

B

During high load, the application becomes unresponsive and requires a manual restart of the EC2 instance. A solutions architect must improve the application's reliability
→ Auto Scaling Group + ELB + Aurora replica

Question 482:

A company needs to use an AWS Transfer Family SFTP-enabled server with an Amazon S3 bucket to receive updates from a third-party data supplier. The data is encrypted with Pretty Good Privacy (PGP) encryption. The company needs a solution that will automatically decrypt the data after the company receives the data.

A solutions architect will use a Transfer Family managed workflow. The company has created an IAM service role by using an IAM policy that allows access to AWS Secrets Manager and the S3 bucket. The role's trust relationship allows the transfer.amazonaws.com service to assume the role.

What should the solutions architect do next to complete the solution for automatic decryption?

- A. Store the PGP public key in Secrets Manager. Add a nominal step in the Transfer Family managed workflow to decrypt files. Configure PGP encryption parameters in the nominal step. Associate the workflow with the Transfer Family server.
- B. Store the PGP private key in Secrets Manager. Add an exception-handling step in the Transfer Family managed workflow to decrypt files. Configure PGP encryption parameters in the exception handler. Associate the workflow with the SFTP user.
- C. Store the PGP private key in Secrets Manager. Add a nominal step in the Transfer Family managed workflow to decrypt files. Configure PGP decryption parameters in the nominal step. Associate the workflow with the Transfer Family server.
- D. Store the PGP public key in Secrets Manager. Add an exception-handling step in the Transfer Family managed workflow to decrypt files. Configure PGP decryption parameters in the exception handler. Associate the workflow with the SFTP user.

C

In the context of AWS Transfer Family managed workflows, a ""nominal step"" refers to one of the predefined steps that you can include in a managed workflow to automate file transfer and processing tasks. An ""exception-handling step"" is a specific type of step designed to handle errors or exceptions that occur during the execution of a workflow.

Question 483:

A company is migrating infrastructure for its massive multiplayer game to AWS. The game's application features a leaderboard where players can see rankings in real time. The leaderboard requires microsecond reads and single-digit-millisecond write latencies. The datasets are single-digit terabytes in size and must be available to accept writes in less than a minute if a primary node failure occurs.

The company needs a solution in which data can persist for further analytical processing through a data pipeline.

Which solution will meet these requirements with the LEAST operational overhead?

- B. Create an Amazon RDS database with a read replica. Configure the application to point writes to the writer endpoint. Configure the application to point reads to the reader endpoint.

C. Create an Amazon MemoryDB for Redis cluster in Multi-AZ mode Configure the application to interact with the primary node.

D. Create multiple Redis nodes on Amazon EC2 instances that are spread across multiple Availability Zones. Configure backups to Amazon S3.

C

MEM DB for gaming leaderboard with related latency requirement

ElastiCache – Redis vs Memcached

REDIS

- Multi AZ with Auto-Failover
- Read Replicas to scale reads and have high availability
- Persistent, Data Durability: Append Only File (AOF), backup and restore features



MEMCACHED

- Multi-node for partitioning of data (sharding)
- Non persistent
- No backup and restore
- Multi-threaded architecture



Question 484:

A company is running several applications in the AWS Cloud. The applications are specific to separate business units in the company. The company is running the components of the applications in several AWS accounts that are in an organization in AWS Organizations.

Every cloud resource in the company's organization has a tag that is named BusinessUnit. Every tag already has the appropriate value of the business unit name.

The company needs to allocate its cloud costs to different business units. The company also needs to visualize the cloud costs for each business unit.

Which solution will meet these requirements?

- A. In the organization's management account, create a cost allocation tag that is named BusinessUnit. Also in the management account, create an Amazon S3 bucket and an AWS Cost and Usage Report (AWS CUR). Configure the S3 bucket as the destination for the AWS CUR. From the management account, query the AWS CUR data by using Amazon Athena. Use Amazon QuickSight for visualization.

B. In each member account, create a cost allocation tag that is named BusinessUnit. In the organization's management account, create an Amazon S3 bucket and an AWS Cost and Usage Report (AWS CUR). Configure the S3 bucket as the destination for the AWS CUR. Create an Amazon CloudWatch dashboard for visualization.

C. In the organization's management account, create a cost allocation tag that is named BusinessUnit. In each member account, create an Amazon S3 bucket and an AWS Cost and Usage Report (AWS CUR). Configure each S3 bucket as the destination for its respective AWS CUR. In the management account, create an Amazon CloudWatch dashboard for visualization.

D. In each member account, create a cost allocation tag that is named BusinessUnit. Also in each member account, create an Amazon S3 bucket and an AWS Cost and Usage Report (AWS CUR). Configure each S3 bucket as the destination for its respective AWS CUR. From the management account, query the AWS CUR data by using Amazon Athena. Use Amazon QuickSight for visualization.

A

The company needs to allocate its cloud costs to different business units → AWS Cost and Usage Report (AWS CUR)

The company also needs to visualize the cloud costs for each business unit. → Amazon QuickSight for visualization

Question 485:

A utility company wants to collect usage data every 5 minutes from its smart meters to facilitate time-of-use metering. When a meter sends data to AWS, the data is sent to Amazon API Gateway, processed by an AWS Lambda function, and stored in an Amazon DynamoDB table. During the pilot phase, the Lambda functions took from 3 to 5 seconds to complete.

As more smart meters are deployed, the engineers notice the Lambda functions are taking from 1 to 2 minutes to complete. The functions are also increasing in duration as new types of metrics are collected from the devices. There are many ProvisionedThroughputExceededException errors while performing PUT operations on DynamoDB, and there are also many TooManyRequestsException errors from Lambda.

Which combination of changes will resolve these issues? (Choose two.)

- A. Increase the write capacity units to the DynamoDB table.
- B. Increase the memory available to the Lambda functions.
- C. Increase the payload size from the smart meters to send more data.
- D. Stream the data into an Amazon Kinesis data stream from API Gateway and process the data in batches.
- E. Collect data in an Amazon SQS FIFO queue, which triggers a Lambda function to process each message

A,D

Kinesis allows to process data in batches, which can help reduce the number of requests and the load on your Lambda functions and DynamoDB.

DynamoDB – in short



- NoSQL database, fully managed, massive scale (1,000,000 rps) quy mô lớn
- Similar to Apache Cassandra (can migrate to DynamoDB)
- No disk space to provision, max object size is 400 KB
- Capacity: provisioned (WCU, RCU, & Auto Scaling) or on-demand
- Supports CRUD (Create Read Update Delete)
- Read: eventually or strong consistency
- Supports transactions across multiple tables (ACID support)
- Backups available, point in time recovery
- Table classes: Standard and Infrequent Access (IA)

Question 486:

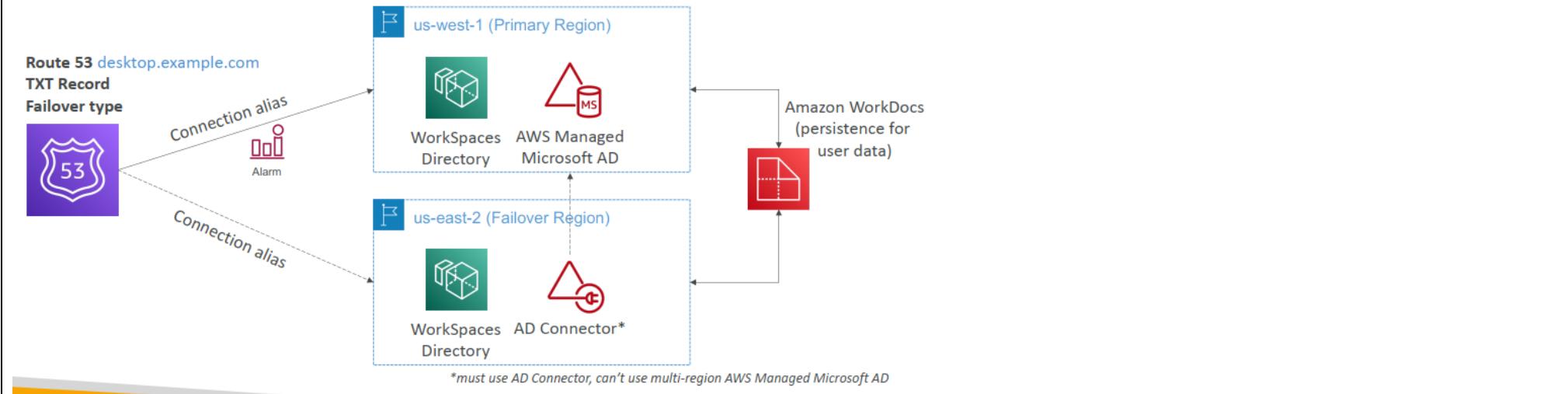
A company recently completed a successful proof of concept of Amazon WorkSpaces. A solutions architect needs to make the solution highly available across two AWS Regions. Amazon WorkSpaces is deployed in a failover Region, and a hosted zone is deployed in Amazon Route 53.

What should the solutions architect do to configure high availability for the solution?

- Create a connection alias in the primary Region and in the failover Region. Associate the connection aliases with a directory in each Region. Create a Route 53 failover routing policy. Set Evaluate Target Health to Yes.
- Create a connection alias in the primary Region and in the failover Region. Associate the connection aliases with a directory in the primary Region. Create a Route 53 multivalue answer routing policy.
- Create a connection alias in the primary Region. Associate the connection alias with a directory in the primary Region. Create a Route 53 weighted routing policy.
- Create a connection alias in the primary Region. Associate the connection alias with a directory in the failover Region. Create a Route 53 failover routing policy. Set Evaluate Target Health to Yes.

A
failover Region → Route 53 failover routing policy

Amazon WorkSpaces - Cross Region Redirection



Question 487:

A company plans to migrate many VMs from an on-premises environment to AWS. The company requires an initial assessment of the on-premises environment before the migration, a visualization of the dependencies between applications that run on the VMs, and a report that provides an assessment of the on-premises environment.

To get this information, the company has initiated a Migration Evaluator assessment request. The company has the ability to install collector software in its on-premises environment without any constraints.

Which solution will provide the company with the required information with the LEAST operational overhead?

- Install the AWS Application Discovery Agent on each on-premises VM. After the data collection period ends, use AWS Migration Hub to view the application dependencies. Download the Quick insights assessment report from Migration Hub.
- Install the Migration Evaluator Collector on each on-premises VM. After the data collection period ends, use Migration Evaluator to view the application dependencies. Download and export the discovered server list from Migration Evaluator. Upload the list to Amazon QuickSight. When the QuickSight report is generated, download the Quick Insights assessment report.
- Setup the AWS Application Discovery Service Agentless Collector in the on-premises environment. After the data collection period ends, use AWS Migration Hub to view the application dependencies. Export the discovered server list from Application Discovery Service. Upload the list to Migration Evaluator. When the Migration Evaluator report is generated, download the Quick Insights assessment.

D. Set up the Migration Evaluator Collector in the on-premises environment. Install the AWS Application Discovery Agent on each VM. After the data collection period ends, use AWS Migration Hub to view the application dependencies. Download the Quick Insights assessment report from Migration Evaluator.

C

Many VMs ➔ Agentless

AWS Application Discovery Service



- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping are important for migrations
- **Agentless Discovery (AWS Agentless Discovery Connector)**
 - Open Virtual Appliance (OVA) package that can be deployed to a VMware host
 - VM inventory, configuration, and performance history such as CPU, memory, and disk usage
 - OS agnostic
- **Agent-based Discovery (AWS Application Discovery Agent)**
 - System configuration, system performance, running processes, and details of the network connections between systems
 - Supports Microsoft Server, Amazon Linux, Ubuntu, RedHat, CentOS, SUSE...
- Resulting data can be exported as CSV or viewed within AWS Migration Hub
- Data can be explored using pre-defined queries in Amazon Athena

Question 488:

A company hosts its primary API on AWS by using an Amazon API Gateway API and AWS Lambda functions that contain the logic for the API methods. The company's internal applications use the API for core functionality and business logic. The company's customers use the API to access data from their accounts. Several customers also have access to a legacy API that is running on a single standalone Amazon EC2 instance.

The company wants to increase the security for these APIs to better prevent denial of service (DoS) attacks, check for vulnerabilities, and guard against common exploits.

What should a solutions architect do to meet these requirements?

- A. Use AWS WAF to protect both APIs. Configure Amazon Inspector to analyze the legacy API. Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.
- B. Use AWS WAF to protect the API Gateway API. Configure Amazon Inspector to analyze both APIs. Configure Amazon GuardDuty to block malicious attempts to access the APIs.
- C. Use AWS WAF to protect the API Gateway API. Configure Amazon Inspector to analyze the legacy API. Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.

D. Use AWS WAF to protect the API Gateway API! Configure Amazon Inspector to protect the legacy API. Configure Amazon GuardDuty to block malicious attempts to access the APIs.

C

Vulnerabilities → Inspector

GuardDuty only monitors but doesn't block malicious attempts. → C is correct, D is incorrect

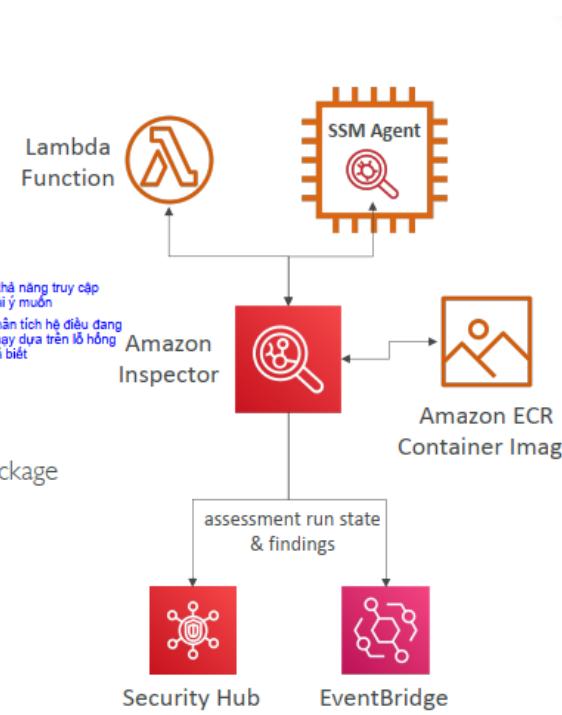
Amazon Inspector

dánh giá bảo mật tự động

- Automated Security Assessments

- For EC2 instances

- Leveraging the AWS System Manager (SSM) agent
- Analyze against unintended network accessibility
- Analyze the running OS against known vulnerabilities



- For Container Images push to Amazon ECR

- Assessment of Container Images as they are pushed

- For Lambda Functions

- Identifies software vulnerabilities in function code and package dependencies
- Assessment of functions as they are deployed

- Reporting & integration with AWS Security Hub

- Send findings to Amazon Event Bridge

Amazon GuardDuty



Phát hiện mối đe dọa để bảo vệ account của bạn

- Intelligent Threat discovery to protect your AWS Account
- Uses Machine Learning algorithms, anomaly detection, 3rd party data
- One click to enable (30 days trial), no need to install software
- Input data includes:
 - CloudTrail Events Logs – unusual API calls, unauthorized deployments
 - CloudTrail Management Events – create VPC subnet, create trail, ...
 - CloudTrail S3 Data Events – get object, list objects, delete object, ...
 - VPC Flow Logs – unusual internal traffic, unusual IP address
 - DNS Logs – compromised EC2 instances sending encoded data within DNS queries
 - compromised EC2 instances sending encoded data within DNS queries
 - Optional Feature – EKS Audit Logs, RDS & Aurora, EBS, Lambda, S3 Data Events...
- Can setup EventBridge rules to be notified in case of findings
- EventBridge rules can target AWS Lambda or SNS
- Can protect against CryptoCurrency attacks (has a dedicated “finding” for it)

Question 489:

A company is running a serverless ecommerce application on AWS. The application uses Amazon API Gateway to invoke AWS Lambda Java functions. The Lambda functions connect to an Amazon RDS for MySQL database to store data.

During a recent sale event, a sudden increase in web traffic resulted in poor API performance and database connection failures. The company needs to implement a solution to minimize the latency for the Lambda functions and to support bursts in traffic.

Which solution will meet these requirements with the LEAST amount of change to the application?

- A. Update the code of the Lambda functions so that the Lambda functions open the database connection outside of the function handler. Increase the provisioned concurrency for the Lambda functions.
- B. Create an RDS Proxy endpoint for the database. Store database secrets in AWS Secrets Manager. Set up the required IAM permissions. Update the Lambda functions to connect to the RDS Proxy endpoint. Increase the provisioned concurrency for the Lambda functions.
- C. Create a custom parameter group. Increase the value of the max_connections parameter. Associate the custom parameter group with the RDS DB instance and schedule a reboot. Increase the reserved concurrency for the Lambda functions.

D. Create an RDS Proxy endpoint for the database. Store database secrets in AWS Secrets Manager. Set up the required IAM permissions. Update the Lambda functions to connect to the RDS Proxy endpoint. Increase the reserved concurrency for the Lambda functions.

B

database connection failures → RDS proxy

Provisioned Concurrency - makes sure Lambda functions could handle traffic bursts RDS proxy endpoint

Question 490:

A company requires that all internal application connectivity use private IP addresses. To facilitate this policy, a solutions architect has created interface endpoints to connect to AWS Public services. Upon testing, the solutions architect notices that the service names are resolving to public IP addresses, and that internal services cannot connect to the interface endpoints.

Which step should the solutions architect take to resolve this issue?

- A. Update the subnet route table with a route to the interface endpoint.
- B. Enable the private DNS option on the VPC attributes.
- C. Configure the security group on the interface endpoint to allow connectivity to the AWS services.
- D. Configure an Amazon Route 53 private hosted zone with a conditional forwarder for the internal application.

B

VPC Endpoints Interface

- Provision an ENI that will have a private endpoint interface hostname
- Leverage Security Groups for security
- Private DNS (setting when you create the endpoint)
 - The public hostname of a service will resolve to the private Endpoint Interface hostname
 - VPC Setting: "Enable DNS hostnames" and "Enable DNS Support" must be 'true'
 - Example for Athena:
 - vpce-0b7d2995e9dfe5418-mwrths3x.athena.us-east-1.vpce.amazonaws.com
 - vpce-0b7d2995e9dfe5418-mwrths3x-us-east-1a.athena.us-east-1.vpce.amazonaws.com
 - vpce-0b7d2995e9dfe5418-mwrths3x-us-east-1b.athena.us-east-1.vpce.amazonaws.com
 - athena.us-east-1.amazonaws.com (private DNS name)
- Interface can be accessed from Direct Connect and Site-to-Site VPN

Question 491:

A company is developing a latency-sensitive application. Part of the application includes several AWS Lambda functions that need to initialize as quickly as possible. The Lambda functions are written in Java and contain initialization code outside the handlers to load libraries, initialize classes, and generate unique IDs.

Which solution will meet the startup performance requirement MOST cost-effectively?

- A. Move all the initialization code to the handlers for each Lambda function. Activate Lambda SnapStart for each Lambda function. Configure SnapStart to reference the \$LATEST version of each Lambda function.
- B. Publish a version of each Lambda function. Create an alias for each Lambda function. Configure each alias to point to its corresponding version. Set up a provisioned concurrency configuration for each Lambda function to point to the corresponding alias.
- C. Publish a version of each Lambda function. Set up a provisioned concurrency configuration for each Lambda function to point to the corresponding version. Activate Lambda SnapStar for the published versions of the Lambda functions.
- D. Update the Lambda functions to add a pre-snapshot hook. Move the code that generates unique IDs into the handlers. Publish a version of each Lambda function. Activate Lambda SnapStart for the published versions of the Lambda functions.

D

<https://aws.amazon.com/blogs/compute/reducing-java-cold-starts-on-aws-lambda-functions-with-snapstart/>
<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html#snapstart-concurrency>

Question 492:

A solutions architect is importing a VM from an on-premises environment by using the Amazon EC2 VM Import feature of AWS Import/Export. The solutions architect has created an AMI and has provisioned an Amazon EC2 instance that is based on that AMI. The EC2 instance runs inside a public subnet in a VPC and has a public IP address assigned.

The EC2 instance does not appear as a managed instance in the AWS Systems Manager console.

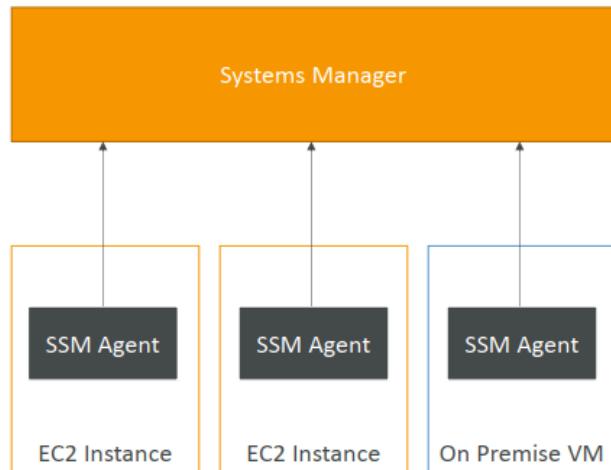
Which combination of steps should the solutions architect take to troubleshoot this issue? (Choose two.)

- A. Verify that Systems Manager Agent is installed on the instance and is running.
- B. Verify that the instance is assigned an appropriate IAM role for Systems Manager.
- C. Verify the existence of a VPC endpoint on the VPC.
- D. Verify that the AWS Application Discovery Agent is configured.
- E. Verify the correct configuration of service-linked roles for Systems Manager.

A,B

How Systems Manager works

- We need to install the SSM agent onto the systems we control
- Installed by default on Amazon Linux AMI & some Ubuntu AMI
- If an instance can't be controlled with Systems Manager, it's probably an issue with the SSM agent!
- Make sure the EC2 instances have a proper IAM role to allow Systems Manager actions



Question 493:

A company is using AWS CloudFormation as its deployment tool for all applications. It stages all application binaries and templates within Amazon S3 buckets with versioning enabled. Developers have access to an Amazon EC2 instance that hosts the integrated development environment (IDE). The developers download the application binaries from Amazon S3 to the EC2 instance, make changes, and upload the binaries to an S3 bucket after running the unit tests locally. The developers want to improve the existing deployment mechanism and implement CI/CD using AWS CodePipeline.

The developers have the following requirements:

- Use AWS CodeCommit for source control.
- Automate unit testing and security scanning.
- Alert the developers when unit tests fail.
- Turn application features on and off, and customize deployment dynamically as part of CI/CD.
- Have the lead developer provide approval before deploying an application.

Which solution will meet these requirements?

A. Use AWS CodeBuild to run unit tests and security scans. Use an Amazon EventBridge rule to send Amazon SNS alerts to the developers when unit tests fail. Write AWS Cloud Development Kit (AWS CDK) constructs for different solution features, and use a manifest file to turn features on and off in the AWS CDK application. Use a manual approval stage in the pipeline to allow the lead developer to approve applications.

B. Use AWS Lambda to run unit tests and security scans. Use Lambda in a subsequent stage in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Write AWS Amplify plugins for different solution features and utilize user prompts to turn features on and off. Use Amazon SES in the pipeline to allow the lead developer to approve applications.

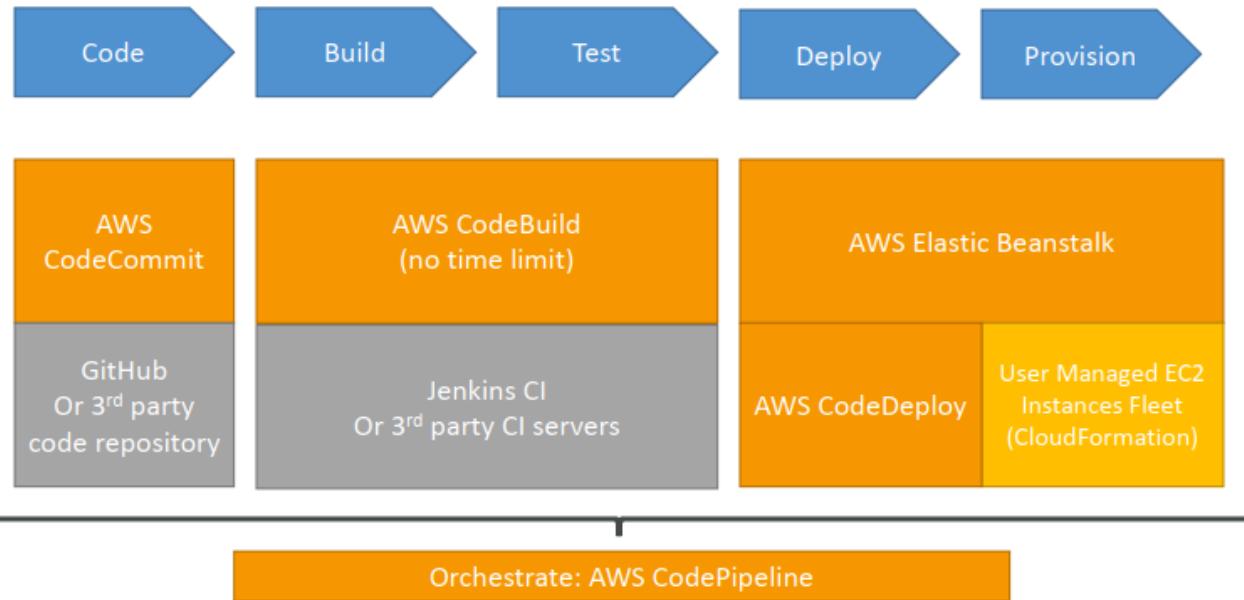
C. Use Jenkins to run unit tests and security scans. Use an Amazon EventBridge rule in the pipeline to send Amazon SES alerts to the developers when unit tests fail. Use AWS CloudFormation nested stacks for different solution features and parameters to turn features on and off. Use AWS Lambda in the pipeline to allow the lead developer to approve applications.

D. Use AWS CodeDeploy to run unit tests and security scans. Use an Amazon CloudWatch alarm in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Use Docker images for different solution features and the AWS CLI to turn features on and off. Use a manual approval stage in the pipeline to allow the lead developer to approve applications.

A

Automate unit testing and security scanning → CodeBuild
Alert the developers when unit tests fail. → SNS

Technology Stack for CICD



Question 494:

A global ecommerce company has many data centers around the world. With the growth of its stored data, the company needs to set up a solution to provide scalable storage for legacy on-premises file applications. The company must be able to take point-in-time copies of volumes by using AWS Backup and must retain low-latency access to frequently accessed data. The company also needs to have storage volumes that can be mounted as Internet Small Computer System Interface (iSCSI) devices from the company's on-premises application servers.

Which solution will meet these requirements?

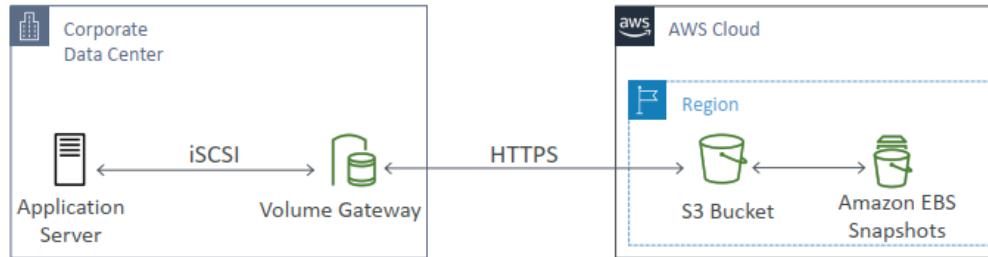
- A. Provision an AWS Storage Gateway tape gateway. Configure the tape gateway to store data in an Amazon S3 bucket. Deploy AWS Backup to take point-in-time copies of the volumes.
- B. Provision an Amazon FSx File Gateway and an Amazon S3 File Gateway. Deploy AWS Backup to take point-in-time copies of the data.
- C. Provision an AWS Storage Gateway volume gateway in cache mode. Back up the on-premises Storage Gateway volumes with AWS Backup.
- D. Provision an AWS Storage Gateway file gateway in cache mode. Deploy AWS Backup to take point-in-time copies of the volumes.

C

iSCSI → AWS Storage Gateway volume gateway

Volume Gateway

- Block storage using iSCSI protocol backed by S3
- Backed by EBS snapshots which can help restore on-premises volumes!
- **Cached volumes:** low latency access to most recent data
- **Stored volumes:** entire dataset is on premise, scheduled backups to S3



Question 495:

A company has an application that uses AWS Key Management Service (AWS KMS) to encrypt and decrypt data. The application stores data in an Amazon S3 bucket in an AWS Region. Company security policies require the data to be encrypted before the data is placed into the S3 bucket. The application must decrypt the data when the application reads files from the S3 bucket.

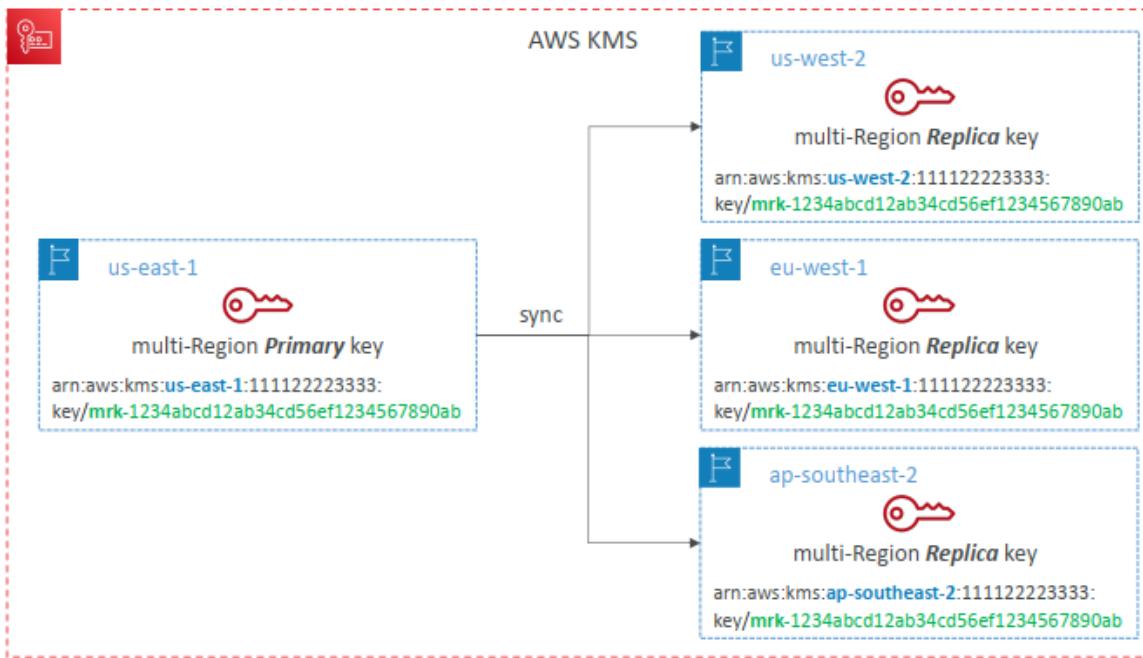
The company replicates the S3 bucket to other Regions. A solutions architect must design a solution so that the application can encrypt and decrypt data across Regions. The application must use the same key to decrypt the data in each Region.

Which solution will meet these requirements?

- A. Create a KMS multi-Region primary key. Use the KMS multi-Region primary key to create a KMS multi-Region replica key in each additional Region where the application is running. Update the application code to use the specific replica key in each Region.
- B. Create a new customer managed KMS key in each additional Region where the application is running. Update the application code to use the specific KMS key in each Region.
- C. Use AWS Private Certificate Authority to create a new certificate authority (CA) in the primary Region. Issue a new private certificate from the CA for the application's website URL. Share the CA with the additional Regions by using AWS Resource Access Manager (AWS RAM). Update the application code to use the shared CA certificates in each Region.
- D. Use AWS Systems Manager Parameter Store to create a parameter in each additional Region where the application is running. Export the key material from the KMS key in the primary Region. Store the key material in the parameter in each Region. Update the application code to use the key data from the parameter in each Region.

A

KMS Multi-Region Keys



Question 496:

A company hosts an application that uses several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). During the initial startup of the EC2 instances, the EC2 instances run user data scripts to download critical content for the application from an Amazon S3 bucket.

The EC2 instances are launching correctly. However, after a period of time, the EC2 instances are terminated with the following error message: "An instance was taken out of service in response to an ELB system health check failure." EC2 instances continue to launch and be terminated because of Auto Scaling events in an endless loop.

The only recent change to the deployment is that the company added a large amount of critical content to the S3 bucket. The company does not want to alter the user data scripts in production.

What should a solutions architect do so that the production environment can deploy successfully?

- A. Increase the size of the EC2 instances.
- B. Increase the health check timeout for the ALB.

C. Change the health check path for the ALB.

D. Increase the health check grace period for the Auto Scaling group.

D

Extending the grace period allows the instances more time to complete their startup tasks, including downloading the additional content from S3, before health checks start. This solution does not require altering the user data scripts in production, which aligns with the company's requirements.

Question 497:

A company needs to move some on-premises Oracle databases to AWS. The company has chosen to keep some of the databases on premises for business compliance reasons.

The on-premises databases contain spatial data and run cron jobs for maintenance. The company needs to connect to the on-premises systems directly from AWS to query data as a foreign table.

Which solution will meet these requirements?

A. Create Amazon DynamoDB global tables with auto scaling enabled. Use the AWS Schema Conversion Tool (AWS SCT) and AWS Database Migration Service (AWS DMS) to move the data from on premises to DynamoDB. Create an AWS Lambda function to move the spatial data to Amazon S3. Query the data by using Amazon Athena. Use Amazon EventBridge to schedule jobs in DynamoDB for maintenance. Use Amazon API Gateway for foreign table support.

B. Create an Amazon RDS for Microsoft SQL Server DB instance. Use native replication to move the data from on premises to the DB instance. Use the AWS Schema Conversion Tool (AWS SCT) to modify the SQL Server schema as needed after replication. Move the spatial data to Amazon Redshift. Use stored procedures for system maintenance. Create AWS Glue crawlers to connect to the on-premises Oracle databases for foreign table support.

C. Launch Amazon EC2 instances to host the Oracle databases. Place the EC2 instances in an Auto Scaling group. Use AWS Application Migration Service to move the data from on premises to the EC2 instances and for real-time bidirectional change data capture (CDC) synchronization. Use Oracle native spatial data support. Create an AWS Lambda function to run maintenance jobs as part of an AWS Step Functions workflow. Create an internet gateway for foreign table support.

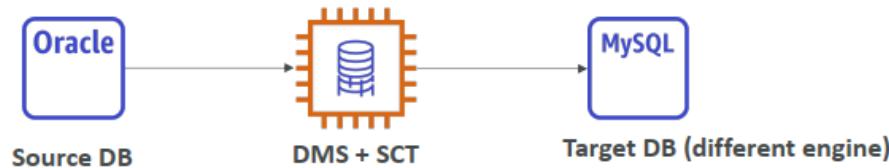
D. Create an Amazon RDS for PostgreSQL DB instance. Use the AWS Schema Conversion Tool (AWS SCT) and AWS Database Migration Service (AWS DMS) to move the data from on premises to the DB instance. Use PostgreSQL native spatial data support. Run cron jobs on the DB instance for maintenance. Use AWS Direct Connect to connect the DB instance to the on-premises environment for foreign table support.

D

AWS Schema Conversion Tool (AWS SCT) and AWS Database Migration Service (AWS DMS) to convert from Oracle to RDS PostgreSQL
company needs to connect to the on-premises systems directly from AWS to query data as a foreign table ➔ DX

AWS Schema Conversion Tool (SCT)

- Convert your Database's Schema from one engine to another
- Example OLTP: (SQL Server or Oracle) to MySQL, PostgreSQL, Aurora
- Example OLAP: (Teradata or Oracle) to Amazon Redshift



- You do not need to use SCT if you are migrating the same DB engine
 - Ex: on-premises PostgreSQL => RDS PostgreSQL
 - The DB engine is still PostgreSQL (RDS is the platform)

Question 498:

Accompany runs an application on Amazon EC2 and AWS Lambda. The application stores temporary data in Amazon S3. The S3 objects are deleted after 24 hours.

The company deploys new versions of the application by launching AWS CloudFormation stacks. The stacks create the required resources. After validating a new version, the company deletes the old stack. The deletion of an old development stack recently failed. A solutions architect needs to resolve this issue without major architecture changes.

Which solution will meet these requirements?

- Create a Lambda function to delete objects from an S3 bucket. Add the Lambda function as a custom resource in the CloudFormation stack with a DependsOn attribute that points to the S3 bucket resource.
- Modify the CloudFormation stack to attach a DeletionPolicy attribute with a value of Delete to the S3 bucket.
- Update the CloudFormation stack to add a DeletionPolicy attribute with a value of Snapshot for the S3 bucket resource
- Update the CloudFormation template to create an Amazon Elastic File System (Amazon EFS) file system to store temporary files instead of Amazon S3. Configure the Lambda functions to run in the same VPC as the EFS file system.

A

DeletionPolicy: Delete: The DeletionPolicy attribute in CloudFormation is used to specify what should happen to a resource when the stack is deleted. The value Delete indicates that CloudFormation should delete the resource (in this case, the S3 bucket) when the stack is deleted. **Non-Empty Buckets:** The problem with this approach is that CloudFormation cannot delete an S3 bucket if it contains any objects. The DeletionPolicy: Delete does not change this behavior; it only specifies that the bucket should be deleted, which will still fail if the bucket is not empty.

Question 499:

A company has an application that stores user-uploaded videos in an Amazon S3 bucket that uses S3 Standard storage. Users access the videos frequently in the first 180 days after the videos are uploaded. Access after 180 days is rare. Named users and anonymous users access the videos.

Most of the videos are more than 100 MB in size. Users often have poor internet connectivity when they upload videos, resulting in failed uploads. The company uses multipart uploads for the videos.

A solutions architect needs to optimize the S3 costs of the application.

Which combination of actions will meet these requirements? (Choose two.)

- A. Configure the S3 bucket to be a Requester Pays bucket.
- B. Use S3 Transfer Acceleration to upload the videos to the S3 bucket.
- C. Create an S3 Lifecycle configuration to expire incomplete multipart uploads 7 days after initiation.
- D. Create an S3 Lifecycle configuration to transition objects to S3 Glacier Instant Retrieval after 1 day.
- E. Create an S3 Lifecycle configuration to transition objects to S3 Standard-infrequent Access (S3 Standard- IA) after 180 days.

C, E

Access after 180 days is rare → S3 Standard- IA

The root cause for failed upload is due to that fact that user has poor internet connectivity. That's not something transfer accelerator can help with, maybe the user need to find a better internet provider.

Question 500:

A company runs an ecommerce web application on AWS. The web application is hosted as a static website on Amazon S3 with Amazon CloudFront for content delivery. An Amazon API Gateway API invokes AWS Lambda functions to handle user requests and order processing for the web application. The Lambda functions store data in an Amazon RDS for MySQL DB cluster that uses On-Demand instances. The DB cluster usage has been consistent in the past 12 months.

Recently, the website has experienced SQL injection and web exploit attempts. Customers also report that order processing time has increased during periods of peak usage. During these periods, the Lambda functions often have cold starts. As the company grows, the company needs to ensure scalability and low-latency access during traffic peaks. The company also must optimize the database costs and add protection against the SQL injection and web exploit attempts.

Which solution will meet these requirements?

- A. Configure the Lambda functions to have an increased timeout value during peak periods. Use RDS Reserved Instances for the database. Use CloudFront and subscribe to AWS Shield Advanced to protect against the SQL injection and web exploit attempts.
- B. Increase the memory of the Lambda functions, Transition to Amazon Redshift for the database. Integrate Amazon Inspector with CloudFront to protect against the SQL injection and web exploit attempts.
- C. Use Lambda functions with provisioned concurrency for compute during peak periods, Transition to Amazon Aurora Serverless for the database. Use CloudFront and subscribe to AWS Shield Advanced to protect against the SQL injection and web exploit attempts.
- D. Use Lambda functions with provisioned concurrency for compute during peak periods. Use RDS Reserved Instances for the database. Integrate AWS WAF with CloudFront to protect against the SQL injection and web exploit attempts.

D
 protection against the SQL injection → WAF
 must optimize the database costs → RDS Reserved Instances
 cold starts → Provisioned concurrency
 In Lambda, concurrency is the number of in-flight requests that your function is currently handling. There are two types of concurrency controls available:

- Reserved concurrency – This represents the maximum number of concurrent instances allocated to your function. When a function has reserved concurrency, no other function can use that concurrency. Reserved concurrency is useful for ensuring that your most critical functions always have enough concurrency to handle incoming requests. Configuring reserved concurrency for a function incurs no additional charges.
- Provisioned concurrency – This is the number of pre-initialized execution environments allocated to your function. These execution environments are ready to respond immediately to incoming function requests. Provisioned concurrency is useful for reducing cold start latencies for functions. Configuring provisioned concurrency incurs additional charges to your AWS account.

<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>

Question 501:

A group of Amazon EC2 instances have been configured as a high performance computing (HPC) cluster. The instances are running in a placement group, and are able to communicate with each other at network speeds of up to 20 Gbps.

The cluster needs to communicate with a control EC2 instance outside of the placement group. The control instance has the same instance type and AMI as the other instances, and is configured with a public IP address.

How can the Solutions Architect improve the network speeds between the control instance and the instances in the placement group?

- Terminate the control instance and relaunch it in the placement group.
- Ensure that the instances are communicating using their private IP addresses.
- Ensure that the control instance is using an Elastic Network Adapter.
- Move the control instance inside the placement group.

D

EC2 - Placement Groups

- Control the EC2 Instance placement strategy using placement groups
- Group Strategies:
 - *Cluster*—clusters instances into a low-latency group in a single Availability Zone
 - *Spread*—spreads instances across underlying hardware (max 7 instances per group per AZ) – critical applications
 - *Partition*—spreads instances across many different partitions (which rely on different sets of racks) within an AZ. Scales to 100s of EC2 instances per group (Hadoop, Cassandra, Kafka)
- You can move an instance into or out of a placement group
 - You first need to **stop** it
 - You then need to **use the CLI** (`modify-instance-placement`)
 - You can then **start** your instance

Question 502:

A company needs to migrate its on-premises database fleet to Amazon RDS. The company is currently using a mixture of Microsoft SQL Server, MySQL, and Oracle databases. Some of the databases have custom schemas and stored procedures.

Which combination of steps should the company take for the migration? (Choose two.)

- A. Use Migration Evaluator Quick Insights to analyze the source databases and to identify the stored procedures that need to be migrated.
- B. Use AWS Application Migration Service to analyze the source databases and to identify the stored procedures that need to be migrated.
- C. Use the AWS Schema Conversion Tool (AWS SCT) to analyze the source databases for changes that are required
- D. Use AWS Database Migration Service (AWS DMS) to migrate the source databases to Amazon RDS.
- E. Use AWS DataSync to migrate the data from the source databases to Amazon RDS.

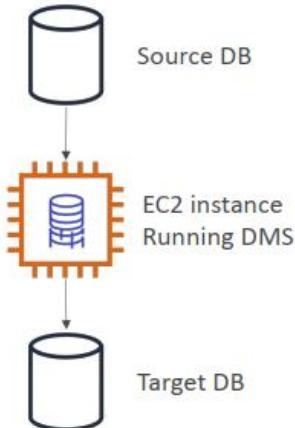
C, D

Some of the databases have custom schemas and stored procedures. ➔ AWS Schema Conversion Tool (AWS SCT)

DMS – Database Migration Service



- Quickly and securely migrate databases to AWS, resilient, self healing
- The source database remains available during the migration
- Supports:
 - dòng nhất homogeneous migrations: ex Oracle to Oracle
 - không đồng nhất heterogeneous migrations: ex Microsoft SQL Server to Aurora
- Continuous Data Replication using CDC
- You must create an EC2 instance to perform the replication tasks



Question 503:

A company is migrating its blog platform to AWS. The company's on-premises servers connect to AWS through an AWS Site-to-Site VPN connection. The blog content is updated several times a day by multiple authors and is served from a file share on a network-attached storage (NAS) server.

The company needs to migrate the blog platform without delaying the content updates. The company has deployed Amazon EC2 instances across multiple Availability Zones to run the blog platform behind an Application Load Balancer. The company also needs to move 200 TB of archival data from its on-premises servers to Amazon S3 as soon as possible.

Which combination of steps will meet these requirements? (Choose two.)

- Create a weekly cron job in Amazon EventBridge. Use the cron job to invoke an AWS Lambda function to update the EC2 instances from the NAS server.
- Configure an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume for the EC2 instances to share for content access. Write code to synchronize the EBS volume with the NAS server weekly.
- Mount an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers to act as the NAS server. Copy the blog data to the EFS file system. Mount the EFS file system to the EC2 instances to serve the content.
- Order an AWS Snowball Edge Storage Optimized device. Copy the static data artifacts to the device. Ship the device to AWS.

E. Order an AWS Snowcone SSD device. Copy the static data artifacts to the device. Ship the device to AWS.

C, D
a file share on a network-attached storage (NAS) server ➔ Amazon EFS
200 TB, as soon as possible ➔ Snowball Edge Storage Optimized device

Question 504:

A company plans to migrate a legacy on-premises application to AWS. The application is a Java web application that runs on Apache Tomcat with a PostgreSQL database.

The company does not have access to the source code but can deploy the application Java Archive (JAR) files. The application has increased traffic at the end of each month.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Launch Amazon EC2 instances in multiple Availability Zones. Deploy Tomcat and PostgreSQL to all the instances by using Amazon Elastic File System (Amazon EFS) mount points. Use AWS Step Functions to deploy additional EC2 instances to scale for increased traffic.
- B. Provision Amazon Elastic Kubernetes Service (Amazon EKS) in an Auto Scaling group across multiple AWS Regions. Deploy Tomcat and PostgreSQL in the container images. Use a Network Load Balancer to scale for increased traffic.
- C. Refactor the Java application into Python-based containers. Use AWS Lambda functions for the application logic. Store application data in Amazon DynamoDB global tables. Use AWS Storage Gateway and Lambda concurrency to scale for increased traffic.
- D. Use AWS Elastic Beanstalk to deploy the Tomcat servers with auto scaling in multiple Availability Zones. Store application data in an Amazon RDS for PostgreSQL database. Deploy Amazon CloudFront and an Application Load Balancer to scale for increased traffic.

D
PostgreSQL database ➔ Amazon RDS for PostgreSQL
is a Java web application that runs on Apache Tomcat and LEAST operational overhead ➔ Elastic Beanstalk

Elastic Beanstalk

- Support for many platforms:
 - Go
 - Java SE
 - Java with Tomcat
 - .NET on Windows Server with IIS
 - Node.js
 - PHP
 - Python
 - Ruby
 - Packer Builder
 - Single Container Docker
- Multicontainer Docker
- Preconfigured Docker
- If not supported, you can write your custom platform (advanced)
- Beanstalk is great to “Replatform” your application from on-premises to the cloud

Question 505:

A company is migrating its on-premises IoT platform to AWS. The platform consists of the following components:

- A MongoDB cluster as a data store for all collected and processed IoT data.
- An application that uses Message Queuing Telemetry Transport (MQTT) to connect to IoT devices every 5 minutes to collect data.
- An application that runs jobs periodically to generate reports from the IoT data. The jobs take 120-600 seconds to finish running.
- A web application that runs on a web server. End users use the web application to generate reports that are accessible to the general public.

The company needs to migrate the platform to AWS to reduce operational overhead while maintaining performance.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

- A. Create AWS Step Functions state machines with AWS Lambda tasks to prepare the reports and to write the reports to Amazon S3. Configure an Amazon CloudFront distribution that has an S3 origin to serve the reports
- B. Create an AWS Lambda function. Program the Lambda function to connect to the IoT devices, process the data, and write the data to the data store. Configure a Lambda layer to temporarily store messages for processing.

C. Configure an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with Amazon EC2 instances to prepare the reports. Create an ingress controller on the EKS cluster to serve the reports.

D. Connect the IoT devices to AWS IoT Core to publish messages. Create an AWS IoT rule that runs when a message is received. Configure the rule to call an AWS Lambda function. Program the Lambda function to parse, transform, and store device message data to the data store.

E. Migrate the MongoDB cluster to Amazon DocumentDB (with MongoDB compatibility).

F. Migrate the MongoDB cluster to Amazon EC2 instances.

A,D,E

A MongoDB cluster → Amazon DocumentDB (with MongoDB compatibility). → E is correct

An application that uses Message Queuing Telemetry Transport (MQTT) → AWS IoT Core → D

The jobs take 120-600 seconds to finish running. → Lambda

generate reports that are accessible to the general public → S3

Question 506:

A company creates an Amazon API Gateway API and shares the API with an external development team. The API uses AWS Lambda functions and is deployed to a stage that is named Production.

The external development team is the sole consumer of the API. The API experiences sudden increases of usage at specific times, leading to concerns about increased costs. The company needs to limit cost and usage without reworking the Lambda functions.

Which solution will meet these requirements MOST cost-effectively?

A. Configure the API to send requests to Amazon Simple Queue Service (Amazon SQS) queues instead of directly to the Lambda functions. Update the Lambda functions to consume messages from the queues and to process the requests. Set up the queues to invoke the Lambda functions when new messages arrive.

B. Configure provisioned concurrency for each Lambda function. Use AWS Application Auto Scaling to register the Lambda functions as targets. Set up scaling schedules to increase and decrease capacity to match changes in API usage.

C. Create an API Gateway API key and an AWS WAF Regional web ACL. Associate the web ACL with the Production stage. Add a rate-based rule to the web ACL. In the rule, specify the rate limit and a custom request aggregation that uses the X-API-Key header. Share the API key with the external development team.

D. Create an API Gateway API Key and usage plan. Define throttling limits and quotas in the usage plan. Associate the usage plan with the Production stage and the API key. Share the API key with the external development team.

D

needs to limit cost and usage without reworking the Lambda functions → API key, usage plan, throttling limits and quotas in the usage plan

API Gateway – Usage Plans & API Keys

- If you want to make an API available as an offering (\$) to your customers
- **Usage Plan:**
 - who can access one or more deployed API stages and methods
 - how much and how fast they can access them
 - uses API keys to identify API clients and meter access
 - configure throttling limits and quota limits that are enforced on individual client
- **API Keys:**
 - alphanumeric string values to distribute to your customers
 - Ex: WBjHxNtoAb4WPKBC7cGm64CBiblb24b4jt8jjHo9
 - Can use with usage plans to control access
 - Throttling limits are applied to the API keys *giới hạn điều chỉnh được áp dụng cho API keys*
 - Quotas limits is the overall number of maximum requests
- **429 Too Many Requests:**
 - Account level throttling across all APIs in a region
 - Clients must implement retry mechanisms

Question 507:

An entertainment company hosts a ticketing service on a fleet of Linux Amazon EC2 instances that are in an Auto Scaling group. The ticketing service uses a pricing file. The pricing file is stored in an Amazon S3 bucket that has S3 Standard storage. A central pricing solution that is hosted by a third party updates the pricing file.

The pricing file is updated every 1-15 minutes and has several thousand line items. The pricing file is downloaded to each EC2 instance when the instance launches.

The EC2 instances occasionally use outdated pricing information that can result in incorrect charges for customers.

Which solution will resolve this problem MOST cost-effectively?

- A. Create an AWS Lambda function to update an Amazon DynamoDB table with new prices each time the pricing file is updated. Update the ticketing service to use DynamoDB to look up pricing
- B. Create an AWS Lambda function to update an Amazon Elastic File System (Amazon EFS) file share with the pricing file each time the file is updated. Update the ticketing service to use Amazon EFS to access the pricing file.
- C. Load Mountpoint for Amazon S3 onto the AMI of the EC2 instances. Configure Mountpoint for Amazon S3 to mount the S3 bucket that contains the pricing file. Update the ticketing service to point to the mount point and path to access the \$3 object,
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume. Use EBS Multi-Attach to attach the volume to every EC2 instance. When a new EC2 instance launches, configure the new instance to update the pricing file on the EBS volume. Update the ticketing service to point to the new local source.

A

- A. DynamoDB provides fast data access and query capabilities, suitable for frequently read but infrequently updated data.
- B. EFS may not be suitable for frequent small file updates, and its cost may be higher than using DynamoDB.
- C. This solution can directly read pricing files from S3, but it does not solve the problem of outdated pricing data being used by old instances even after the pricing files are updated.
- D. EBS is not good at Multi Attach to multiple EC2 instances, and it can increase complexity and cost.

Question 508:

A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The quality assurance (QA) department needs to launch a large number of short-lived environments to test the application. The application environments are currently launched by the manager of the department using an AWS CloudFormation template. To launch the stack, the manager uses a role with permission to use CloudFormation, EC2, and Auto Scaling APIs. The manager wants to allow testers to launch their own environments, but does not want to grant broad permissions to each user.

Which set up would achieve these goals?

- A. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to assume the manager's role and add a policy that restricts the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.
- B. Create an AWS Service Catalog product from the environment template. Add a launch constraint to the product with the existing role. Give users in the QA department permission to use AWS Service Catalog APIs only. Train users to launch the template from the AWS Service Catalog console.
- C. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to use CloudFormation and S3 APIs, with conditions that restrict the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.
- D. Create an AWS Elastic Beanstalk application from the environment template. Give users in the QA department permission to use Elastic Beanstalk permissions only. Train users to launch Elastic Beanstalk environments with the Elastic Beanstalk CLI, passing the existing role to the environment as a service role.

B

The manager wants to allow testers to launch their own environments, but does not want to grant broad permissions to each user. ➔ Service Catalog

AWS CloudFormation



- Infrastructure as code (IaC) in AWS
- Portability of stacks across multiple accounts and regions
- Backbone of the Elastic Beanstalk service
- Backbone of the Service Catalog service
- Backbone of the SAM (Serverless Application Model) framework
- Must-know service as a developer / sysops / devops

AWS Service Catalog



- Users that are new to AWS have too many options, and may create stacks that are not compliant / in line with the rest of the organization
phần còn lại của tổ chức
- Some users just want a quick **self-service portal** to launch a set of **authorized products** pre-defined by **admins**
- Includes: virtual machines, databases, storage options, etc...
- Enter AWS Service Catalog!

Question 509:

A company is using a single AWS Region for its ecommerce website. The website includes a web application that runs on several Amazon EC2 instances behind an Application Load Balancer (ALB). The website also includes an Amazon DynamoDB table. A custom domain name in Amazon Route 53 is linked to the ALB. The company created an SSL/TLS certificate in AWS Certificate Manager (ACM) and attached the certificate to the ALB. The company is not using a content delivery network as part of its design.

The company wants to replicate its entire application stack in a second Region to provide disaster recovery, plan for future growth, and provide improved access time to users. A solutions architect needs to implement a solution that achieves these goals and minimizes administrative overhead.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Create an AWS CloudFormation template for the current infrastructure design. Use parameters for important system values, including Region. Use the CloudFormation template to create the new infrastructure in the second Region.
- B. Use the AWS Management Console to document the existing infrastructure design in the first Region and to create the new infrastructure in the second Region.
- C. Update the Route 53 hosted zone record for the application to use weighted routing. Send 50% of the traffic to the ALB in each Region.
- D. Update the Route 53 hosted zone record for the application to use latency-based routing. Send traffic to the ALB in each Region.
- E. Update the configuration of the existing DynamoDB table by enabling DynamoDB Streams. Add the second Region to create a global table.
- F. Create a new DynamoDB table. Enable DynamoDB Streams for the new table. Add the second Region to create a global table. Copy the data from the existing DynamoDB table to the new table as a one-time operation.

A,D,E

minimizes administrative overhead. ➔ Use AWS CloudFormation to create the new infrastructure in the second Region. ➔ A provide improved access time to users. ➔ Route 53 hosted zone latency-based routing ➔ D disaster recovery ➔ DynamoDB global table ➔ E

Question 510:

A company wants to create a single Amazon S3 bucket for its data scientists to store work-related documents. The company uses AWS IAM Identity Center to authenticate all users. A group for the data scientists was created.

The company wants to give the data scientists access to only their own work. The company also wants to create monthly reports that show which documents each user accessed.

Which combination of steps will meet these requirements? (Choose two.)

- A. Create a custom IAM Identity Center permission set to grant the data scientists access to an S3 bucket prefix that matches their username tag. Use a policy to limit access to paths with the \${aws:PrincipalTag/userName}/* condition.

- B. Create an IAM Identity Center role for the data scientists group that has Amazon S3 read access and write access. Add an S3 bucket policy that allows access to the IAM Identity Center role.
- C. Configure AWS CloudTrail to log S3 data events and deliver the logs to an S3 bucket. Use Amazon Athena to run queries on the CloudTrail logs in Amazon S3 and generate reports.
- D. Configure AWS CloudTrail to log S3 management events to CloudWatch. Use Amazon Athena's CloudWatch connector to query the logs and generate reports.
- E. Enable S3 access logging to EMR File System (EMRFS). Use Amazon S3 Select to query logs and generate reports.

A,C

create monthly reports that show which documents each user accessed. → S3 and Athena → C
 data scientists access to only their own work → \${aws:PrincipalTag/userName}/* → A

Question 511:

A company hosts a data-processing application on Amazon EC2 instances. The application polls an Amazon Elastic File System (Amazon EFS) file system for newly uploaded files. When a new file is detected, the application extracts data from the file and runs logic to select a Docker container image to process the file. The application starts the appropriate container image and passes the file location as a parameter.

The data processing that the container performs can take up to 2 hours. When the processing is complete, the code that runs inside the container writes the file back to Amazon EFS and exits.

The company needs to refactor the application to eliminate the EC2 instances that are running the containers.

Which solution will meet these requirements?

- A. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Extract the container selection logic to run as an Amazon EventBridge rule that starts the appropriate Fargate task. Configure the EventBridge rule to run when files are added to the EFS file system.
- B. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Update and containerize the container selection logic to run as a Fargate service that starts the appropriate Fargate task. Configure an EFS event notification to invoke the Fargate service when files are added to the EFS file system.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Extract the container selection logic to run as an AWS Lambda function that starts the appropriate Fargate task. Migrate the storage of file uploads to an Amazon S3 bucket. Update the processing code to use Amazon S3. Configure an S3 event notification to invoke the Lambda function when objects are created.
- D. Create AWS Lambda container images for the processing. Configure Lambda functions to use the container images. Extract the container selection logic to run as a decision Lambda function that invokes the appropriate Lambda processing function. Migrate the storage of file uploads to an Amazon S3 bucket. Update the processing code to use Amazon S3. Configure an S3 event notification to invoke the decision Lambda function when objects are created.

C

D is incorrect because Lambda can't process up to 2 hours.

B is incorrect because EFS don't have event notification.

A is incorrect because container can't run as an Amazon EventBridge rule

Question 512:

A media company has a 30-TB repository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video, such as objects, scenery items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS.

The company has a high-speed AWS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system.

How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system?

A. Set up an AWS Storage Gateway, file gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata, and push the metadata into the MAM solution.

B. Set up an AWS Storage Gateway, tape gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the tape gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway, retrieve the required metadata, and push the metadata into the MAM solution.

C. Configure a video ingestion stream by using Amazon Kinesis Video Streams. Use the catalog of faces to build a collection in Amazon Rekognition. Stream the videos from the MAM solution into Kinesis Video Streams. Configure Amazon Rekognition to process the streamed videos. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solution. Configure the stream to store the videos in Amazon S3.

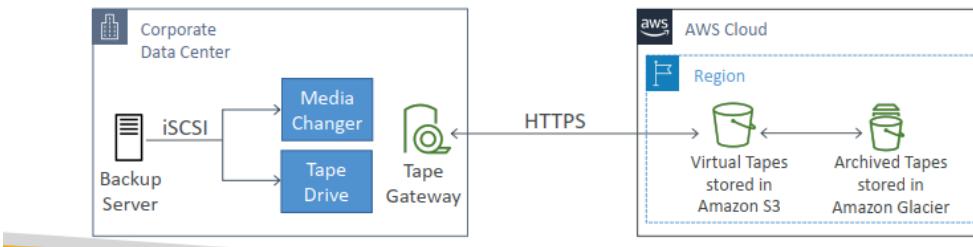
D. Set up an Amazon EC2 instance that runs the OpenCV libraries. Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume mounted on this EC2 instance. Process the videos to retrieve the required metadata, and push the metadata into the MAM solution, while also copying the video files to an Amazon S3 bucket.

B

an on-premises tape library → AWS Storage Gateway tape gateway

Tape Gateway

- Some companies have backup processes using physical tapes (!)
- With Tape Gateway, companies use the same processes but, in the cloud
- Virtual Tape Library (VTL) backed by Amazon S3 and Glacier
- Back up data using existing tape-based processes (and iSCSI interface)
- Works with leading backup software vendors



Question 513:

A company needs to optimize the cost of an AWS environment that contains multiple accounts in an organization in AWS Organizations. The company conducted cost optimization activities 3 years ago and purchased Amazon EC2 Standard Reserved Instances that recently expired.

The company needs EC2 instances for 3 more years. Additionally, the company has deployed a new serverless workload.

Which strategy will provide the company with the MOST cost savings?

- Purchase the same Reserved Instances for an additional 3-year term with All Upfront payment. Purchase a 3-year Compute Savings Plan with All Upfront payment in the management account to cover any additional compute costs
- Purchase a 1-year Compute Savings Plan with No Upfront payment in each member account. Use the Savings Plans recommendations in the AWS Cost Management console to choose the Compute Savings Plan.
- Purchase a 3-year EC2 Instance Savings Plan with No Upfront payment in the management account to cover EC2 costs in each AWS Region. Purchase a 3-year Compute Savings Plan with No Upfront payment in the management account to cover any additional compute costs.
- Purchase a 3-year EC2 Instance Savings Plan with All Upfront payment in each member account. Use the Savings Plans recommendations in the AWS Cost Management console to choose the EC2 Instance Savings Plan.

A

serverless workload → Compute Savings Plan

EC2 instances for 3 more years → Purchase the same Reserved Instances for an additional 3-year term with All Upfront payment

AWS Savings Plan



- New pricing model to get a discount based on long-term usage
Cam kết sử dụng 1 loại
- Commit to a certain type of usage: ex \$10 per hour for 1 to 3 years
- Any usage beyond the savings plan is billed at the on-demand price
- EC2 Instance Savings plan (up to 72% - same discount as Standard RIs)
 - Select instance family (e.g. M5, C5...), and locked to a specific region
 - Flexible across size (m5.large to m5.4xlarge), OS (Windows to Linux), thuê tenancy (dedicated or default)
- Compute Savings plan (up to 66% - same discount as Convertible RIs)
 - Ability to move between instance family (move from C5 to M5), region (Ireland to US), compute type (EC2, Fargate, Lambda), OS & tenancy
- SageMaker Savings plan (up to 64% off)

EC2 Instance Launch Types

- On Demand Instances: short workload, du doan trước chi phí predictable pricing, đáng tin cậy reliable
- Spot Instances: short workloads, for cheap, can lose instances (not reliable)
- Reserved: (MINIMUM 1 year)
 - Reserved Instances: long workloads
 - Convertible Reserved Instances: long workloads with flexible instances
 - Highest to lowest discount: All trả trước Upfront payment, Partial Upfront payment, no Upfront
- Dedicated Instances: no other customers will share your hardware
- Dedicated Hosts: book an entire physical server, control instance placement
 - Great for software licenses that operate at the core, or CPU socket level
 - Can define host affinity so that instance reboots are kept on the same host

Question 514:

A company operates a static content distribution platform that serves customers globally. The customers consume content from their own AWS accounts.

HANCHE

The company serves its content from an Amazon S3 bucket. The company uploads the content from its on-premises environment to the S3 bucket by using an S3 File Gateway.

The company wants to improve the platform's performance and reliability by serving content from the AWS Region that is geographically closest to customers. The company must route the on-premises data to Amazon S3 with minimal latency and without public internet exposure.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

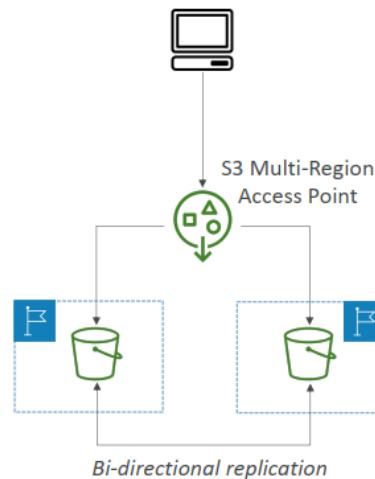
- A. Implement S3 Multi-Region Access Points
- B. Use S3 Cross-Region Replication (CRR) to copy content to different Regions
- C. Create an AWS Lambda function that tracks the routing of clients to Regions
- D. Use an AWS Site-to-Site VPN connection to connect to a Multi-Region Access Point.
- E. Use AWS PrivateLink and AWS Direct Connect to connect to a Multi-Region Access Point.

A, E

serving content from the AWS Region that is geographically closest → Multi region → S3 Multi-Region Access Points
without public internet exposure → AWS PrivateLink

S3 – Multi-Region Access Points

- Provide a global endpoint that spans S3 buckets in multiple AWS regions
- **Dynamically route requests to the nearest S3 bucket (lowest latency)**
- Bi-directional S3 bucket replication rules are created to keep data in sync across regions
- **Failover Controls** – allows you to shift requests across S3 buckets in different AWS regions within minutes (Active-Active or Active-Passive)



Question 515:

A company is migrating its data center to the AWS Cloud and needs to complete the migration as quickly as possible. The company has many applications that are running on hundreds of VMware VMs in the data center. Each VM is configured with a shared Windows folder that contains common shared files. The file share is larger than 100 GB in size.

The company's compliance team requires a change request to be filed and approved for every software installation and modification to each VM. The company has an AWS Direct Connect connection with 10 GB of bandwidth between AWS and the data center.

Which set of steps should the company take to complete the migration in the LEAST amount of time?

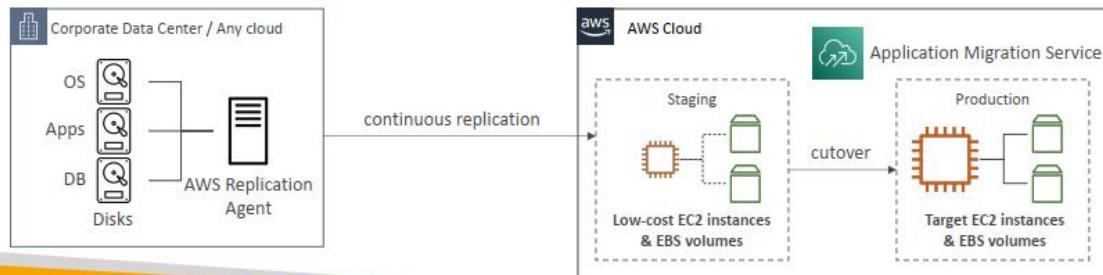
- A. Use VM Import/Export to create images of each VM. Use AWS Application Migration Service to manage and view the images. Copy the Windows file share data to an Amazon Elastic File System (Amazon EFS) file system. After migration, remap the file share to the EFS file system.
- B. Deploy the AWS Application Discovery Service agentless appliance to VMware vCenter. Review the portfolio of discovered VMs in AWS Migration Hub.
- C. Deploy the AWS Application Migration Service agentless appliance to VMware vCenter. Copy the Windows file share data to a new Amazon FSx for Windows File Server file system. After migration, remap the file share on each VM to the FSx for Windows File Server file system.
- C. Create and review a portfolio in AWS Migration Hub. Order an AWS Snowcone device. Deploy AWS Application Migration Service to VMware vCenter and export all the VMs to the Snowcone device. Copy all Windows file share data to the Snowcone device. Ship the Snowcone device to AWS. Use Application Migration Service to deploy all the migrated instances.
- D. Deploy the AWS Application Discovery Service Agent and the AWS Application Migration Service Agent onto each VMware hypervisor directly. Review the portfolio in AWS Migration Hub. Copy each VM's file share data to a new Amazon FSx for Windows File Server file system. After migration, remap the file share on each VM to the FSx for Windows File Server file system.

C C1 - Deploy the AWS Application Migration Service agentless appliance to VMware vCenter. Copy the Windows file share data to a new Amazon FSx for Windows File Server file system. After migration, remap the file share on each VM to the FSx for Windows File Server file system.

AWS Application Migration Service (MGN)



- The “AWS evolution” of CloudEndure Migration, replacing AWS Server Migration Service (SMS)
- Lift-and-shift (rehost) solution which simplify **migrating** applications to AWS
- Converts your physical, virtual, and cloud-based servers to run natively on AWS
- Supports wide range of **platforms**, Operating Systems, and databases
- Minimal downtime, reduced costs



Question 516:

A company has multiple AWS accounts that are in an organization in AWS Organizations. The company needs to store AWS account activity and query the data from a central location by using SQL.

Which solution will meet these requirements?

- Create an AWS CloudTrail trail in each account. Specify CloudTrail management events for the trail. Configure CloudTrail to send the events to Amazon CloudWatch Logs. Configure CloudWatch cross-account observability. Query the data in CloudWatch Logs Insights.
- Use a delegated administrator account to create an AWS CloudTrail Lake data store. Specify CloudTrail management events for the data store. Enable the data store for all accounts in the organization. Query the data in CloudTrail Lake.
- Use a delegated administrator account to create an AWS CloudTrail trail. Specify CloudTrail management events for the trail. Enable the trail for all accounts in the organization. Keep all other settings as default. Query the CloudTrail data from the CloudTrail event history page.
- Use AWS CloudFormation StackSets to deploy AWS CloudTrail Lake data stores in each account. Specify CloudTrail management events for the data stores. Keep all other settings as default. Query the data in CloudTrail Lake.

B

<https://aws.amazon.com/blogs/mt/announcing-aws-cloudtrail-lake-a-managed-audit-and-security-lake/>

CloudTrail Lake enables querying of CloudTrail data using the familiar SQL query language. The platform also includes sample queries that are designed to help users get started with writing queries for common scenarios, such as identifying records of all activities performed by a user to help accelerate security investigations. The immutable nature of storage, coupled with a default retention window of seven years, helps customers meet compliance requirements. CloudTrail Lake supports the collection of events from multiple AWS regions and AWS accounts.

Question 517:

A company is using AWS to develop and manage its production web application. The application includes an Amazon API Gateway HTTP API that invokes an AWS Lambda function. The Lambda function processes and then stores data in a database.

The company wants to implement user authorization for the web application in an integrated way. The company already uses a third-party identity provider that issues OAuth tokens for the company's other applications.

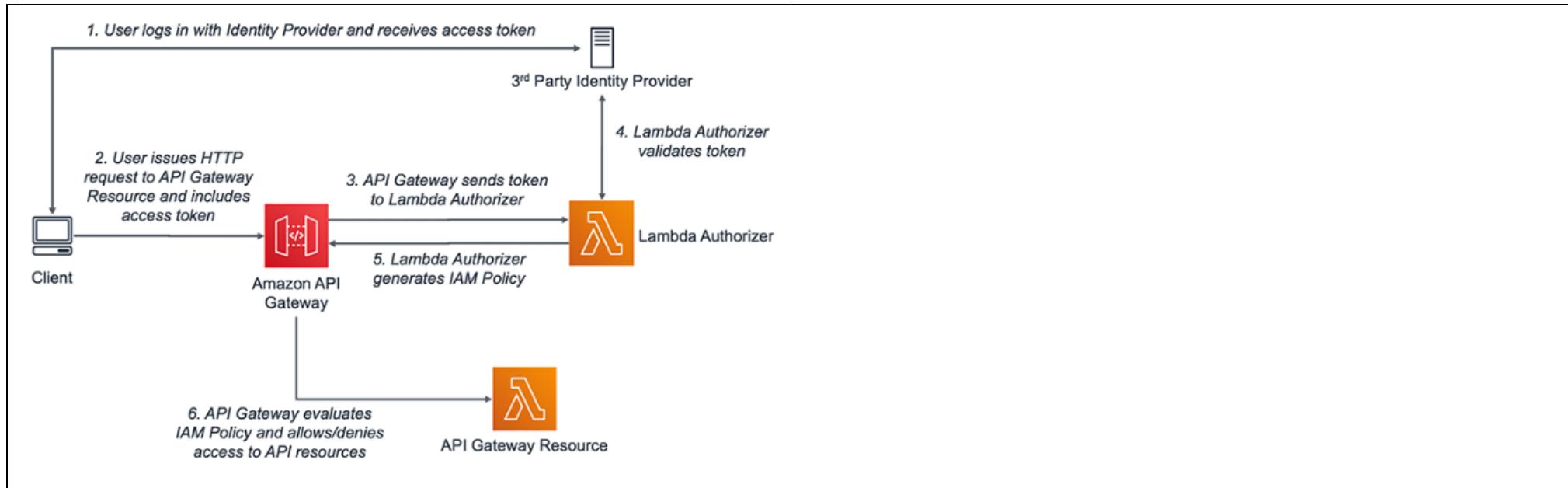
Which solution will meet these requirements?

- A. Integrate the company's third-party identity provider with API Gateway. Configure an API Gateway Lambda authorizer to validate tokens from the identity provider. Require the Lambda authorizer on all API routes. Update the web application to get tokens from the identity provider and include the tokens in the Authorization header when calling the API Gateway HTTP API.
- B. Integrate the company's third-party identity provider with AWS Directory Service. Configure Directory Service as an API Gateway authorizer to validate tokens from the identity provider. Require the Directory Service authorizer on all API routes. Configure AWS IAM Identity Center as a SAML 2.0 identity Provider. Configure the web application as a custom SAML 2.0 application.
- C. Integrate the company's third-party identity provider with AWS IAM Identity Center. Configure API Gateway to use IAM Identity Center for zero-configuration authentication and authorization. Update the web application to retrieve AWS Security Token Service (AWS STS) tokens from IAM Identity Center and include the tokens in the Authorization header when calling the API Gateway HTTP API.
- D. Integrate the company's third-party identity provider with AWS IAM Identity Center. Configure IAM users with permissions to call the API Gateway HTTP API. Update the web application to extract request parameters from the IAM users and include the parameters in the Authorization header when calling the API Gateway HTTP API.

A

Lambda authorizers can integrate with external identity providers, including OAuth2, OpenID Connect, and others, to validate tokens or credentials.

<https://aws.amazon.com/blogs/security/use-aws-lambda-authorizers-with-a-third-party-identity-provider-to-secure-amazon-api-gateway-rest-apis/>



Question 518:

A company has deployed applications to thousands of Amazon EC2 instances in an AWS account. A security audit discovers that several unencrypted Amazon Elastic Block Store (Amazon EBS) volumes are attached to the EC2 instances. The company's security policy requires the EBS volumes to be encrypted.

The company needs to implement an automated solution to encrypt the EBS volumes. The solution also must prevent development teams from creating unencrypted EBS volumes.

Which solution will meet these requirements?

- Configure the AWS Config managed rule that identifies unencrypted EBS volumes. Configure an automatic remediation action. Associate an AWS Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Create an AWS Key Management Service (AWS KMS) customer managed key. In the key policy, include a statement to deny the creation of unencrypted EBS volumes.
- Use AWS Systems Manager Fleet Manager to create a list of unencrypted EBS volumes. Create a Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Create an SCP to deny the creation of unencrypted EBS volumes.
- Use AWS Systems Manager Fleet Manager to create a list of unencrypted EBS volumes. Create a Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.
- Configure the AWS Config managed rule that identifies unencrypted EBS volumes. Configure an automatic remediation action. Associate an AWS Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.

D

must prevent development teams from creating unencrypted EBS volumes → Enabling default encryption for EBSs = Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.

needs to implement an automated solution to encrypt the EBS volumes → AWS Config

AWS Config Rules

- Can use AWS managed config rules (over 75)
- Can make custom config rules (must be defined in AWS Lambda)
 - Evaluate if each EBS disk is of type gp2
 - Evaluate if each EC2 instance is t2.micro
- Rules can be evaluated / triggered:
 - For each config change
 - And / or: at regular time intervals
- Trigger Amazon EventBridge if the rule is non-compliant (chain with Lambda)
- Rules can have auto remediations through **SSM Automations**
 - If a resource is not compliant, you can trigger an auto remediation
 - Ex: remediate security group rules, stop instances with non-approved tags

Question 519:

A company is running a large containerized workload in the AWS Cloud. The workload consists of approximately 100 different services. The company uses Amazon Elastic Container Service (Amazon ECS) to orchestrate the workload.

Recently the company's development team started using AWS Fargate instead of Amazon EC2 instances in the ECS cluster. In the past, the workload has come close to running the maximum number of EC2 instances that are available in the account.

The company is worried that the workload could reach the maximum number of ECS tasks that are allowed. A solutions architect must implement a solution that will notify the development team when Fargate reaches 80% of the maximum number of tasks.

What should the solutions architect do to meet this requirement?

- A. Use Amazon CloudWatch to monitor the Sample Count statistic for each service in the ECS cluster. Set an alarm for when the math expression sample count/SERVICE_QUOTA(service)*100 is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- B. Use Amazon CloudWatch to monitor service quotas that are published under the AWS/Usage metric namespace. Set an alarm for when the math expression metric/SERVICE_QUOTA(metric)*100 is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- C. Create an AWS Lambda function to poll detailed metrics from the ECS cluster. When the number of running Fargate tasks is greater than 80, invoke Amazon Simple Email Service (Amazon SES) to notify the development team.
- D. Create an AWS Config rule to evaluate whether the Fargate SERVICE_QUOTA is greater than 80. Use Amazon Simple Email Service (Amazon SES) to notify the development team when the AWS Config rule is not compliant.

B

a solution that will notify ➔ SNS

The math expression metric/SERVICE_QUOTA(metric)*100 allows you to calculate the percentage of the quota being used, making it easy to set an alarm when usage reaches 80%. CloudWatch Alarm: This is a native and efficient way to monitor service usage, and you can easily configure notifications via Amazon SNS to alert the development team when the threshold is crossed.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Quotas-Visualize-Alarms.html>

Question 520:

A company has several AWS Lambda functions written in Python. The functions are deployed with the .zip package deployment type. The functions use a Lambda layer that contains common libraries and packages in a .zip file. The Lambda .zip packages and Lambda layer .zip file are stored in an Amazon S3 bucket.

The company must implement automatic scanning of the Lambda functions and the Lambda layer to identify CVEs. A subset of the Lambda functions must receive automated code scans to detect potential data leaks and other vulnerabilities. The code scans must occur only for selected Lambda functions, not all the Lambda functions.

Which combination of actions will meet these requirements? (Choose three.)

- A. Activate Amazon Inspector. Start automated CVE scans.
- B. Activate Lambda standard scanning and Lambda code scanning in Amazon Inspector.
- C. Enable Amazon GuardDuty. Enable the Lambda Protection feature in GuardDuty.
- D. Enable scanning in the Monitor settings of the Lambda functions that need code scans.
- E. Tag Lambda functions that do not need code scans. In the tag, include a key of InspectorCodeExclusion and a value of LambdaCodeScanning.
- F. Use Amazon Inspector to scan the S3 bucket that contains the Lambda .zip packages and the Lambda layer .zip file for code scans.

A,B,E

automatic scanning of the Lambda functions and the Lambda layer to identify CVEs → Amazon Inspector

The code scans must occur only for selected Lambda functions, not all the Lambda functions → Tag

<https://docs.aws.amazon.com/inspector/latest/user/scanning-lambda.html>

A: Need to Activate Amazon Inspector first

B: For **CVE**, need to use **Lambda standard scanning**

B: For **data leaks**, need to use Lambda code scanning

E: Tag Lambda functions that do not need code scans

Amazon Inspector

danh giá bảo mật tự động

- Automated Security Assessments

- For EC2 instances

- Leveraging the AWS System Manager (SSM) agent
- Analyze against unintended network accessibility
- Analyze the running OS against known vulnerabilities

phân tích khả năng truy cập
mạng ngoài ý muốn
phân tích hệ điều đang
chạy dựa trên lỗ hổng
đã biết

- For Container Images push to Amazon ECR

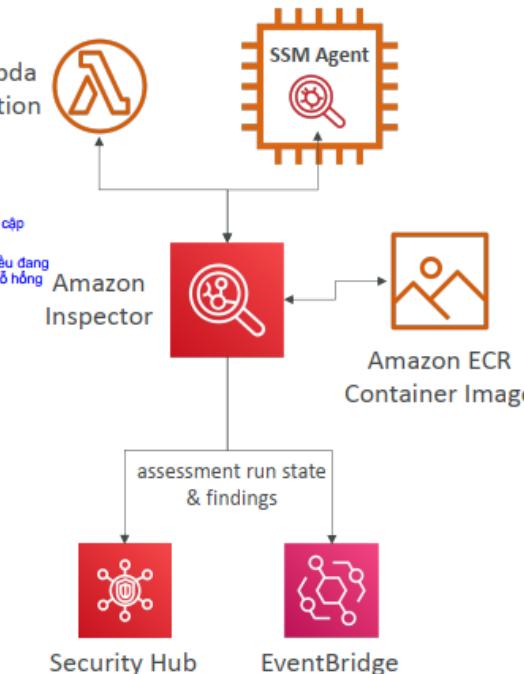
- Assessment of Container Images as they are pushed

- For Lambda Functions

- Identifies software vulnerabilities in function code and package dependencies
- Assessment of functions as they are deployed

- Reporting & integration with AWS Security Hub

- Send findings to Amazon Event Bridge



Question 521:

A company is changing the way that it handles patching of Amazon EC2 instances in its application account. The company currently patches instances over the internet by using a NAT gateway in a VPC in the application account.

The company has EC2 instances set up as a patch source repository in a dedicated private VPC in a core account. The company wants to use AWS Systems Manager Patch Manager and the patch source repository in the core account to patch the EC2 instances in the application account. The company must prevent all EC2 instances in the application account from accessing the internet.

The EC2 instances in the application account need to access Amazon S3, where the application data is stored. These EC2 instances need connectivity to Systems Manager and to the patch source repository in the private VPC in the core account.

Which solution will meet these requirements?

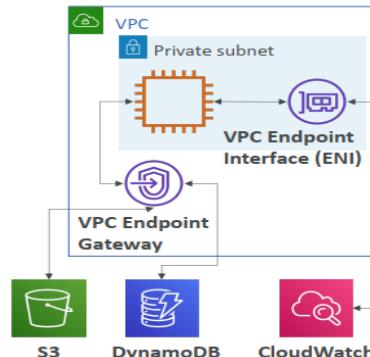
- Create a network ACL that blocks outbound traffic on port 80. Associate the network ACL with all subnets in the application account. In the application account and the core account, deploy one EC2 instance that runs a custom VPN server. Create a VPN tunnel to access the private VPC. Update the route table in the application account.
- Create private VIFs for Systems Manager and Amazon S3. Delete the NAT gateway from the VPC in the application account. Create a transit gateway to access the patch source repository EC2 instances in the core account. Update the route table in the core account.
- Create VPC endpoints for Systems Manager and Amazon S3. Delete the NAT gateway from the VPC in the application account. Create a VPC peering connection to access the patch source repository EC2 instances in the core account. Update the route tables in both accounts.
- Create a network ACL that blocks inbound traffic on port 80. Associate the network ACL with all subnets in the application account. Create a transit gateway to access the patch source repository EC2 instances in the core account. Update the route tables in both accounts.

C

The company must prevent all EC2 instances in the application account from accessing the internet → can't use NAT gateway → Delete NAT Gateway
EC2 instances in the application account need to access Amazon S3 (private network) → VPC endpoints

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in yourVPC
 - Check Route Tables



Question 522:

A company in the United States (US) has acquired a company in Europe. Both companies use the AWS Cloud. The US company has built a new application with a microservices architecture. The US company is hosting the application across five VPCs in the us-east-2 Region. The application must be able to access resources in one VPC in the eu-west-1 Region.

However, the application must not be able to access any other VPCs.

The VPCs in both Regions have no overlapping CIDR ranges. All accounts are already consolidated in one organization in AWS Organizations.

Which solution will meet these requirements MOST cost-effectively?

- A. Create one transit gateway in eu-west-1. Attach the VPCs in us-east-2 and the VPC in eu-west-1 to the transit gateway. Create the necessary route entries in each VPC so that the traffic is routed through the transit gateway.
- B. Create one transit gateway in each Region. Attach the involved subnets to the regional transit gateway. Create the necessary route entries in the associated route tables for each subnet so that the traffic is routed through the regional transit gateway. Peer the two transit gateways.
- C. Create a full mesh VPC peering connection configuration between all the VPCs. Create the necessary route entries in each VPC so that the traffic is routed through the VPC peering connection.
- D. Create one VPC peering connection for each VPC in us-east-2 to the VPC in eu-west-1. Create the necessary route entries in each VPC so that the traffic is routed through the VPC peering connection.

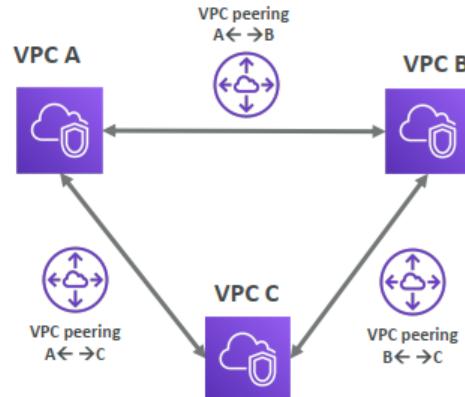
D

no overlapping → VPC peering

C is incorrect because create a full mesh peering is not necessary.

VPC Peering

- Connect two VPC, privately using AWS' network
- Make them behave as if they were in the same network
- Must not have overlapping CIDR
- VPC Peering connection is not transitive (must be established for each VPC that need to communicate with one another)
- You can do VPC peering with another AWS account
- You must update route tables in each VPC's subnets to ensure instances can communicate



Question 523:

A travel company built a web application that uses Amazon Simple Email Service (Amazon SES) to send email notifications to users. The company needs to enable logging to help troubleshoot email delivery issues. The company also needs the ability to do searches that are based on recipient, subject, and time sent.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

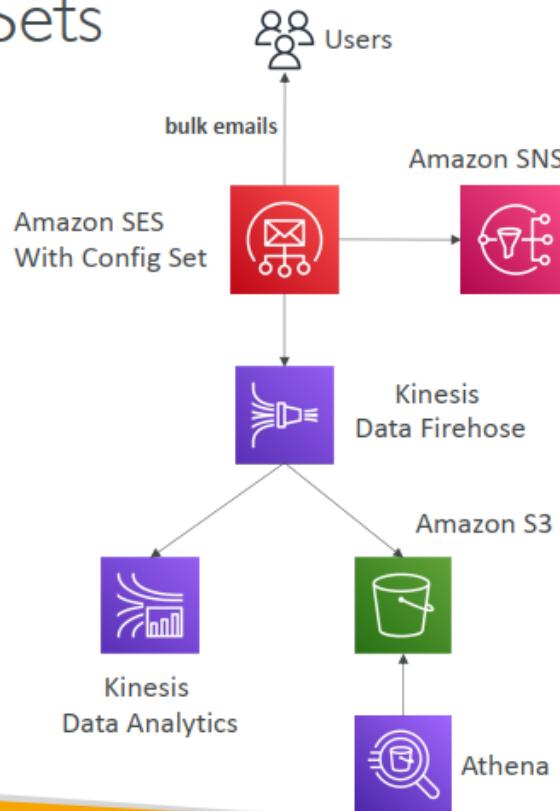
- A. Create an Amazon SES configuration set with Amazon Data Firehose as the destination. Choose to send logs to an Amazon S3 bucket.
- B. Enable AWS CloudTrail logging. Specify an Amazon S3 bucket as the destination for the logs.
- C. Use Amazon Athena to query the logs in the Amazon S3 bucket for recipient, subject, and time sent.
- D. Create an Amazon CloudWatch log group. Configure Amazon SES to send logs to the log group.
- E. Use Amazon Athena to query the logs in Amazon CloudWatch for recipient, subject, and time sent.

A, C

A. Amazon Data Firehose is configured as the target of SES configuration set, which can capture and transfer SES log data in real-time to Amazon S3 storage buckets
C. Amazon Athena allows you to directly analyze data stored in Amazon S3 using SQL queries.

Amazon SES – Configuration Sets

- Configuration sets help you customize and analyze your email send events
- Event destinations:
 - Kinesis Data Firehose: receives metrics (numbers of sends, deliveries, opens, clicks, bounces, and complaints) for each email
 - SNS: for immediate feedback on bounce and complaint information
- IP pool management: use IP pools to send particular types of emails



e Maarek

Question 524:

A company migrated to AWS and uses AWS Business Support. The company wants to monitor the cost-effectiveness of Amazon EC2 instances across AWS accounts. The EC2 instances have tags for department, business unit, and environment. Development EC2 instances have high cost but low utilization.

The company needs to detect and stop any underutilized development EC2 instances. Instances are underutilized if they had 10% or less average daily CPU utilization and 5 MB or less network I/O for at least 4 of the past 14 days.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Configure Amazon CloudWatch dashboards to monitor EC2 instance utilization based on tags for department, business unit, and environment. Create an Amazon EventBridge rule that invokes an AWS Lambda function to stop underutilized development EC2 instances.

B. Configure AWS Systems Manager to track EC2 instance utilization and report underutilized instances to Amazon CloudWatch. Filter the CloudWatch data by tags for department, business unit, and environment. Create an Amazon EventBridge rule that invokes an AWS Lambda function to stop underutilized development EC2 instances.

C. Create an Amazon EventBridge rule to detect low utilization of EC2 instances reported by AWS Trusted Advisor. Configure the rule to invoke an AWS Lambda function that filters the data by tags for department, business unit, and environment and stops underutilized development EC2 instances.

D. Create an AWS Lambda function to run daily to retrieve utilization data for all EC2 instances. Save the data to an Amazon DynamoDB table. Create an Amazon QuickSight dashboard that uses the DynamoDB table as a data source to identify and stop underutilized development EC2 instances.

C

LEAST operational overhead, detect underutilized development EC2 instances → Trusted Advisor
stop any underutilized development EC2 instances → EventBridge



Trusted Advisor

- No need to install anything – high level AWS account assessment
- Analyze your AWS accounts and provides recommendation:
 - Cost Optimization & Recommendations
 - Performance
 - Security
 - Fault Tolerance
 - Service Limits
- Core Checks and recommendations – all customers
- Can enable weekly email notification from the console
- Full Trusted Advisor – Available for Business & Enterprise support plans
 - Ability to set CloudWatch alarms when reaching limits
 - Programmatic Access using AWS Support API

Question 525:

A company is hosting an application on AWS for a project that will run for the next 3 years. The application consists of 20 Amazon EC2 On-Demand Instances that are registered in a target group for a Network Load Balancer (NLB). The instances are spread across two Availability Zones. The application is stateless and runs 24 hours a day, 7 days a week.

The company receives reports from users who are experiencing slow responses from the application. Performance metrics show that the instances are at 10% CPU utilization during normal application use. However, the CPU utilization increases to 100% at busy times, which typically last for a few hours.

The company needs a new architecture to resolve the problem of slow responses from the application.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an Auto Scaling group. Attach the Auto Scaling group to the target group of the NLB. Set the minimum capacity to 20 and the desired capacity to 28. Purchase Reserved Instances for 20 instances.
- B. Create a Spot Fleet that has a request type of request. Set the TotalTargetCapacity parameter to 20. Set the DefaultTargetCapacityType parameter to On-Demand. Specify the NLB when creating the Spot Fleet.
- C. Create a Spot Fleet that has a request type of maintain. Set the TotalTargetCapacity parameter to 20. Set the DefaultTargetCapacityType parameter to Spot. Replace the NLB with an Application Load Balancer.
- D. Create an Auto Scaling group. Attach the Auto Scaling group to the target group of the NLB. Set the minimum capacity to 4 and the maximum capacity to 28. Purchase Reserved Instances for four instances.

D

Need Auto Scaling group.

10% CPU utilization during normal application use ➔ a minimum capacity of 4 is required to meet cost-effective

Question 526:

Accompany is building an application to collect and transmit sensor data from a factory. The application will use AWS IoT Core to send data from hundreds of devices to an Amazon S3 data lake. The company must enrich the data before loading the data into Amazon S3.

The application will transmit the sensor data every 5 seconds. New sensor data must be available in Amazon S3 less than 30 minutes after the application collects the data. No other applications are processing the sensor data from AWS IoT Core.

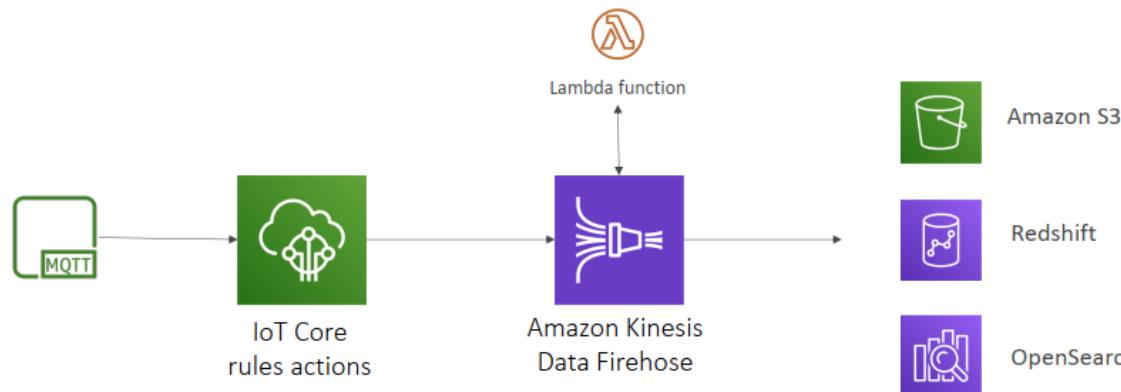
Which solution will meet these requirements MOST cost-effectively?

- A. Create a topic in AWS IoT Core to ingest the sensor data. Create an AWS Lambda function to enrich the data and to write the data to Amazon S3. Configure an AWS IoT rule action to invoke the Lambda function.
- B. Use AWS IoT Core Basic Ingest to ingest the sensor data. Configure an AWS IoT rule action to write the data to Amazon Kinesis Data Firehose. Set the Kinesis Data Firehose buffering interval to 900 seconds. Use Kinesis Data Firehose to invoke an AWS Lambda function to enrich the data. Configure Kinesis Data Firehose to deliver the data to Amazon S3.
- C. Create a topic in AWS IoT Core to ingest the sensor data. Configure an AWS IoT rule action to send the data to an Amazon Timestream table. Create an AWS Lambda function to read the data from Timestream. Configure the Lambda function to enrich the data and to write the data to Amazon S3.
- D. Use AWS IoT Core Basic Ingest to ingest the sensor data. Configure an AWS IoT rule action to write the data to Amazon Kinesis Data Streams. Create a consumer AWS Lambda function to process the data from Kinesis Data Streams and to enrich the data. Call the S3 PutObject API operation from the Lambda function to write the data to Amazon S3.

B

New sensor data must be available in Amazon S3 less than 30 minutes after the application collects the data. → near real time, stream data to s3, no need storage or replay, we shd use autoscaling and fully managed Kinesis Data Firehose.

IoT Core – Kinesis Data Firehose



Question 527:

A company is collecting data from a large set of IoT devices. The data is stored in an Amazon S3 data lake. Data scientists perform analytics on Amazon EC2 instances that run in two public subnets in a VPC in a separate AWS account.

The data scientists need access to the data lake from the EC2 instances. The EC2 instances already have an assigned role with permissions to access Amazon S3.

According to company policies, only authorized networks are allowed to have access to the IoT data.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Create a gateway VPC endpoint for Amazon S3 in the data scientists' VPC.
- B. Create an S3 access point in the data scientists' AWS account for the data lake.
- C. Update the EC2 instance role. Add a policy with a condition that allows the s3:GetObject action when the value for the s3:DataAccessPointArn condition key is a valid access point ARN.
- D. Update the VPC route table to route S3 traffic to an S3 access point.
- E. Add an S3 bucket policy with a condition that allows the s3:GetObject action when the value for the s3:DataAccessPointArn condition key is a valid access point ARN.

B,E

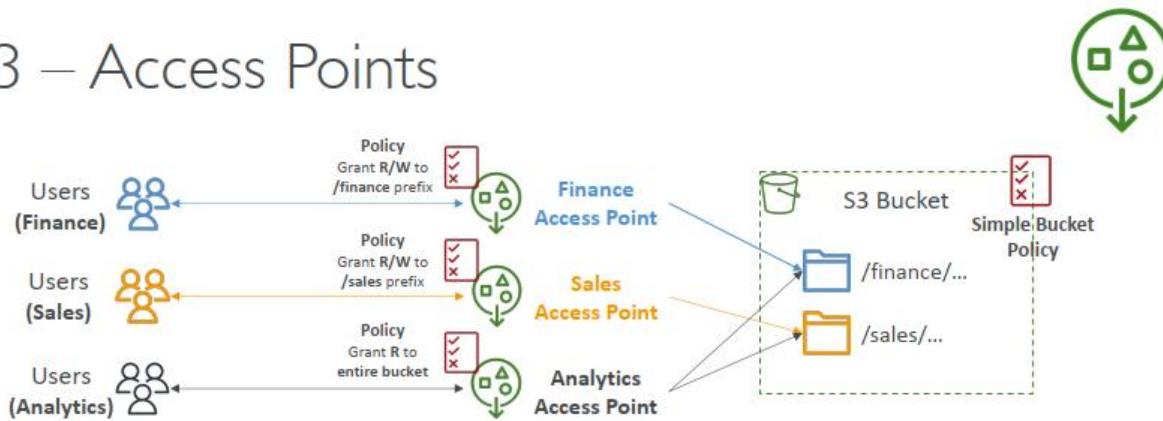
A isn't correct because gateway VPC endpoint doesn't work outside of VPC

B is correct because S3 access point is used If you want to share your bucket with other accounts

HANCHE

E is correct because s3:DataAccessPointArn must be used to set permissions on the S3 bucket side for going through the access point.

S3 – Access Points



- Access Points ^{đơn giản hóa} simplify security management for S3 Buckets
- Each Access Point has:
 - its own DNS name (Internet Origin or VPC Origin)
 - an access point policy (similar to bucket policy) – manage security at scale

Question 528:

A company wants to migrate its website to AWS. The website uses containers that are deployed in an on-premises, self-managed Kubernetes cluster. All data for the website is stored in an on-premises PostgreSQL database.

The company has decided to migrate the on-premises Kubernetes cluster to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster will use EKS managed node groups with a static number of nodes. The company will also migrate the on-premises database to an Amazon RDS for PostgreSQL database.

A solutions architect needs to estimate the total cost of ownership (TCO) for this workload before the migration.

Which solution will provide the required TCO information?

- A. Request access to Migration Evaluator. Run the Migration Evaluator Collector and import the data. Configure a scenario. Export a Quick Insights report from Migration Evaluator.
- B. Launch AWS Database Migration Service (AWS DMS) for the on-premises database. Generate an assessment report. Create an estimate in AWS Pricing Calculator for the costs of the EKS migration.

C. Initialize AWS Application Migration Service. Add the on-premises servers as source servers. Launch a test instance. Output a TCO report from Application Migration Service.

D. Access the AWS Cloud Economics Center webpage to assess the AWS Cloud Value Framework. Create an AWS Cost and Usage report from the Cloud Value Framework.

A

estimate the total cost of ownership (TCO) → Migration Evaluator

Request access to Migration Evaluator. Run the Migration Evaluator Collector and import the data. Configure a scenario. Export a Quick Insights report from Migration Evaluator. Reasoning: Comprehensive TCO Analysis: Migration Evaluator is specifically designed to assess migration projects and provides detailed cost estimates.

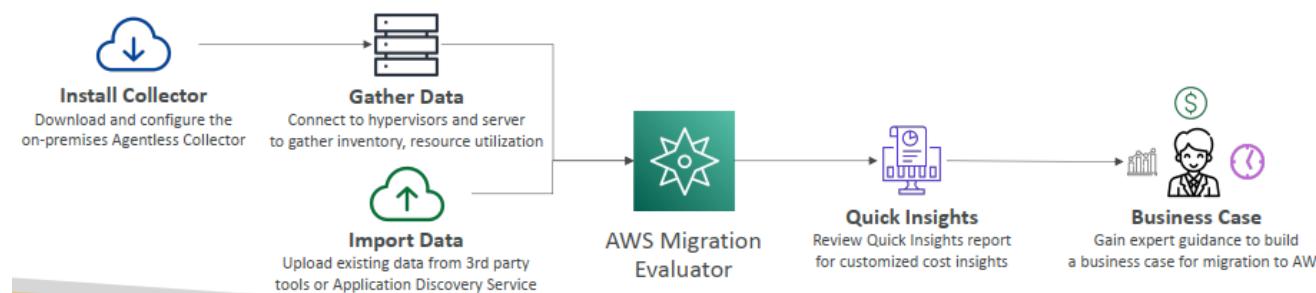
Accurate Data: By collecting data from the on-premises environment, Migration Evaluator can generate more accurate cost estimates. Scenario Modeling: The ability to configure scenarios allows for testing different migration options and their associated costs. Quick Insights Report: This provides a summarized overview of the potential TCO.

AWS Migration Evaluator



dựa trên dữ liệu

- Helps you build a data-driven business case for migration to AWS
- Provides a clear baseline of what your organization is running today
- Install Agentless Collector to conduct broad-based discovery
- Take a snapshot of on-premises foot-print, server dependencies, ...
- Analyze current state, define target state, then develop migration plan



Question 529:

An events company runs a ticketing platform on AWS. The company's customers configure and schedule their events on the platform. The events result in large increases of traffic to the platform. The company knows the date and time of each customer's events.

The company runs the platform on an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS cluster consists of Amazon EC2 On-Demand Instances that are in an Auto Scaling group. The Auto Scaling group uses a predictive scaling policy.

The ECS cluster makes frequent requests to an Amazon S3 bucket to download ticket assets. The ECS cluster and the S3 bucket are in the same AWS Region and the same AWS account. Traffic between the ECS cluster and the S3 bucket flows across a NAT gateway.

The company needs to optimize the cost of the platform without decreasing the platform's availability.

Which combination of steps will meet these requirements? (Choose two.)

- A. Create a gateway VPC endpoint for the S3 bucket.
- B. Add another ECS capacity provider that uses an Auto Scaling group of Spot Instances. Configure the new capacity provider strategy to have the same weight as the existing capacity provider strategy.
- C. Create On-Demand Capacity Reservations for the applicable instance type for the time period of the scheduled scaling policies.
- D. Enable S3 Transfer Acceleration on the S3 bucket.
- E. Replace the predictive scaling policy with scheduled scaling policies for the scheduled events.

A, E

The company knows the date and time of each customer's events → scheduled scaling policies → E

Traffic between the ECS cluster and the S3 bucket flows across a NAT gateway. → need private network → A

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They scale horizontally and are redundant
- No more IGW, NAT, etc... to access AWS Services
- VPC Endpoint Gateway (S3 & DynamoDB)
- VPC Endpoint Interface (all except DynamoDB)
- In case of issues:
 - Check DNS Setting Resolution in your VPC
 - Check Route Tables

