AWS Certified Solutions Architect – Professional Official Practice Exam (SAP-C02)

**Question 01/75**

A company stores many static files on premises. Users add a small number of new files each day. The company is refactoring and migrating some of its existing applications to AWS. The company expects this process to take 6 months. After the company completes the migration, each application will access the files directly from Amazon S3. During the migration, the files must remain accessible to the applications that the company is still running on premises. The on-premises applications run on multiple servers. The company does not want to maintain multiple copies of the static files. How should the company manage the daily migration and the on-premises access to the files?

1. ***Configure an AWS Storage Gateway Amazon S3 File Gateway and connect the S3 File Gateway to the S3 bucket. Create an on-premises NFS file share for the existing on-premises directory to establish access to the files.***
2. Create an AWS Data Sync task to transfer the new files to the S3 bucket at the end of each day. Maintain the files on premises until the company completes the refactoring.
3. Configure an AWS Storage Gateway Volume Gateway and connect the Volume Gateway to the S3 bucket. Create an on-premises iSCSI volume share for the existing on-premises directory to establish access to the files.
4. Create an S3 sync script and configure a recurring job to run the script at the end of each day. Maintain the files on premises until the company completes the refactoring and migration.

**Correct Answer: A**

**Explanation:** Configure an AWS Storage Gateway Amazon S3 File Gateway and connect the S3 File Gateway A to the S3 bucket. Create an on-premises NFS file share for the existing on-premises directory to establish access to the files. S3 File Gateway supports a file interface with Amazon S3 and combines a service and a virtual software appliance. This combination can store and retrieve objects from Amazon S3 by using industry-standard file protocols, including NFS and SMB. NFS is a shared file system that can share data for multiple client connections. This solution will also provide access to the files for the on-premises applications.

For more information <https://docs.aws.amazon.com/filegateway/latest/files3/StorageGatewayConcepts.html#file-gateway-concepts>

**Incorrect Option B)** Data Sync is an online data-transfer service that simplifies, automates, and accelerates the movement of data between on-premises storage systems and AWS storage services. Data Sync would not provide access to the on-premises applications. The company would have to maintain a copy on premises.

**Incorrect Option C)** A Volume Gateway provides cloud-backed storage volumes that you can mount as iSCSI devices from on-premises application servers. However, you cannot connect multiple hosts to a Volume Gateway without additional configuration.

**Incorrect Option D)** The S3 sync command synchronizes the contents of an S3 bucket and a local directory or the contents of two buckets. You could use this command to synchronize the data that is on premises to an S3 bucket. Data Sync would not provide access to the on-premises applications. The company would have to maintain a copy on premises.

For more information about the S3 sync command, see <https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-commands.html#using-s3-commands-managing-objects-sync>

For more information about DataSync, see <https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html>

For more information about how to configure a Volume Gateway, see <https://docs.aws.amazon.com/storagegateway/latest/vgw/create-volume-gateway-volume.html>

**Question 02/75**

A company runs a group of Amazon EC2 instances in a private subnet. The subnet is in a VPC in the us-east-1 Region the EC2 instances store a large amount of sensitive data in an Amazon S3 bucket. Data that transfers between the EC2 instances and the S3 bucket must not travel across the internet. A solutions architect creates a gateway VPC endpoint to allow the EC2 instances to access the S3 bucket. The solutions architect creates a second group of EC2 instances in a private subnet of a VPC in the eu-west-2 Region The second group of EC2 instances requires infrequent access to the same data that is stored in the existing S3 bucket. The amount of data that will travel between the S3 bucket in us-east-1 and the EC2 instances in eu-west-2 will be low. The company needs to grant the second group of EC2instances access to the data in the S3 bucket.

Which solution will meet these requirements MOST cost-effectively?

1. ***Create an interface VPC endpoint for the S3 bucket in the VPC in us-east-1 by using AWS PrivateLink. Peer the VPCs and configure routing between the VPCs. Configure access to the S3 bucket in us-east-1 from the EC2 instances in eu- west-2 by using the endpoint.***
2. Create an Amazon Elastic File System (Amazon EFS) file system in us-east-1. Create mount targets in each subnet where the EC2 instances are running to provide access to the file system. Transfer all the data from the S3 bucket to the file system.
3. Create a second S3 bucket in eu-west-2. Create a gateway VPC endpoint for the second S3 bucket. Allow the EC2 instances in eu-west-2 to communicate with the second S3 bucket. Copy the existing data and configure S3 Cross-Region Replication (CRR) between the two S3 buckets. Create a second S3 bucket in eu-west-2.
4. Create a gateway VPC endpoint for the second S3 bucket. Allow the EC2 instances in eu-west-2 to communicate with the second S3 bucket. Copy the existing data and use an AWS Lambda function to copy new objects between the two S3 buckets.

**Correct Answer: A**

Explanation:

**Correct Option A)** An interface VPC endpoint allows instances that are running in a VPC to connect to other AWS services privately through an elastic network interface. Use of a single S3 bucket along with an interface VPC endpoint is the most cost-effective solution because the volume of data that is stored is large and the volume of data that is transferred is low.

**Incorrect Option B)** Amazon EFS provides a shared NFS for use with multiple AWS services within a Region. However, with standard access patterns, S3 storage has a lower cost per GB than Amazon EFS. In a scenario where the amount of data that is stored is high but the amount of data that is transferred is low, the storage cost is the biggest factor. S3 storage is a more cost-effective solution.

**Incorrect Option C)** Solution that uses CRR between the two S3 buckets would double the cost of the S3 storage and would add the cost of the replication of the complete dataset. The volume of data that is stored is large, but the volume of data that is transferred is low. Therefore, a solution that duplicates all the data would not be as cost-effective as a solution that stores the data once and allows access when the data is needed across the network.

**Incorrect option D)** You can use Lambda to replicate objects to multiple destination S3 buckets in the same Region or different Regions. However, this solution adds costs for data transfer and the use of Lambda. This solution also increases S3 storage costs. The volume of data that is stored is large, but the volume of data that is transferred is low. Therefore, a solution that duplicates all the data would not be as cost-effective as a solution that stores the data once and allows access when the data is needed across the network.

For more information about Amazon EFS, see What Is Amazon Elastic File System.

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

For more information about CRR, see When to Use Cross-Region Replication <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html#crr-scenario>

For more information about gateway VPC endpoints, see Gateway VPC Endpoints.

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway.html>

For more information about Lambda, see What Is AWS Lambda?

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

**Question 03/75**

A company runs a grid computing application on eight Amazon EC2 instances. The instances are fully patched and updated. The application frequently fails because of network timeout errors. A solutions architect creates an AMI that is based on the existing EC2 instances. The solutions architect uses the AMI to add two additional EC2 instances. However, this change does not resolve the timeout errors.

Which solution will resolve the timeout errors with the LEAST operational effort?

1. Configure Elastic Network Adapters (ENAs) for all the instances.
2. Configure Elastic Fabric Adapters (EFAs) for all the instances.
3. Use the existing AMI to create new EC2 instances in an EC2 Fleet. Terminate the old instances.
4. ***Use the existing AMI to create new EC2 instances in a cluster placement group. Terminate the old instances.***

**Correct Answer: D**

Explanation:

**Correct Option D)** because a cluster placement group packs instances close together inside an Availability Zone. This solution will reduce the network latency between the EC2 instances. Reduction of network latency can resolve the timeout errors. Because an AMI already exists, the creation of a cluster placement group requires less operational effort than other network enhancements require.

**Incorrect Option A)** ENAs provide enhanced networking capabilities to EC2 instances. However, ENA configuration would require significant operational effort.

**Incorrect Option B)** An EFA is a network device that attaches to EC2 instances to accelerate high performance computing (HPC) and machine learning applications. However, EFA configuration would require significant operational effort.

**Incorrect Option C)** An EC2 Fleet creates multiple EC2 instances in a single API call. In this scenario, there does not appear to be an issue with the number of EC2 instances. The problem is more likely to be related to network latency. For this reason, the creation of an EC2 Fleet is not likely to address timeout errors.

For more information about cluster placement groups, see Placement Groups <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-fleet.html>

For more information about ENAs see, Enable Enhanced Networking with the Elastic Network Adapter (ENA) on Linux Instances.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena.html>

For more information about EFAs, see Elastic Fabric Adapter.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html>

**Question 04/75**

To be FIPS 140-2 Level 3 compliant, a company needs to store encryption keys The keys need to be available between the hours of 8 00 AM and 6:00 PM US Eastern Time, Monday through Friday the keys must not be available outside of these hours. The company needs a highly available solution to store the encryption keys.

Which solution will meet these requirements MOST cost-effectively?

1. ﻿***Create an AWS CloudHSM cluster with instances in multiple Availability Zones. Store the CloudHSM metadata as standard parameters in AWS Systems Manager Parameter Store. Create and schedule AWS Lambda functions to delete and recreate the CloudHSM cluster from a cluster backup. Configure the Lambda functions to retrieve the necessary metadata from Parameter Store.***
2. Store the encryption keys in AWS Key Management Service (AWS KMS). Create and schedule AWS Lambda functions to disable and enable the stored encryption keys as necessary.
3. Create an AWS CloudHSM cluster with instances in multiple Availability Zones. Create an Amazon DynamoDB table. Store the CloudHSM metadata in the DynamoDB table. Create and schedule AWS Lambda functions to delete and recreate the CloudHSM cluster from a cluster backup. Configure the Lambda functions to retrieve the necessary metadata from the DynamoDB table.
4. Store the encryption keys in AWS Key Management Service (AWS KMS). Create and schedule AWS Lambda functions to remove and add key access policies as necessary.

**Correct Answer: A**

Explanation:

**Correct Option A)** CloudHSM provides dedicated hardware security modules in the AWS Cloud that are FIPS 140-2 Level 3 compliant. Parameter Store provides secure, hierarchical storage for configuration data management and secrets management. Storage of standard parameters in Parameter Store is free. A solution that deletes the CloudHSM cluster when the cluster is not needed and that stores secrets in Parameter Store is the most cost-effective option.

**Incorrect Option B)** because AWS KMS is a managed service that gives you the ability to create and control the cryptographic keys that are used to protect data. However, AWS KMS is FIPS 140-2 Level 2 compliant. The company needs to be FIPS 140-2 Level 3 compliant.

**Incorrect Option C)** because CloudHSM provides dedicated hardware security modules in the AWS Cloud that are FIPS 140-2 Level 3 compliant. DynamoDB is a fully managed NoSQL database service. It is cost-effective to delete the CloudHSM cluster when the cluster is not needed. However, data storage in DynamoDB would incur unnecessary costs.

**Incorrect Option D)** AWS KMS is a managed service that gives you the ability to create and control the cryptographic keys that are used to protect data. However, AWS KMS is FIPS 140-2 Level 2 compliant. The company needs to be FIPS 140-2 Level 3 compliant.

For more information about how to reduce the cost of CloudHSM by limiting operating hours, see How to Lower Costs by Automatically Deleting and Recreating HSMs.

<https://aws.amazon.com/blogs/security/how-to-lower-costs-by-automatically-deleting-and-recreating-hsms>

**Question 05/75**

A company is running a critical application on AWS. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) The instances run in an Amazon EC2 Auto Scaling group The application uses an Amazon RDS for MySQL DB instance as the backend in a multi-AZ deployment All the services that the application supplies are currently in a single AWS Region. A new disaster recovery (OR) regulation requires the company to have a multi-Region configuration. The "failover deployment in the second Region must handle a full-capacity workload as quickly as possible. To prepare a DR configuration, a solutions architect has created an ALB and an EC2 Auto Scaling group in a second Region.

Which solution will meet these requirements with the FASTEST recovery time?

﻿

1. Use AWS Backup to back up the DB instance to a backup vault in the second Region. Use the backup to create a new RDS DB instance in the second Region if needed. Configure Amazon Route 53 with a failover routing policy.
2. ***Create a read replica of the DB instance in the second Region. Promote the read replica to be the primary DB instance if needed. Configure Amazon Route 53 with a failover routing policy.***
3. Use AWS Backup to back up the DB instance to a backup vault in the second Region. Use the backup to create a new RDS DB instance in the second Region if needed. Configure Amazon Route 53 with a weighted routing policy.
4. Create a read replica of the DB instance in the second Region. Promote the read replica to be the primary DB instance if needed. Configure Amazon Route 53 with a weighted routing policy.

**Correct Answer: B**

Explanation:

**Correct Option is B**) because the promotion of a read replica would be a faster option than the creation of a database from backups. The configuration of a failover routing policy for Route 53 would automatically move the incoming workload to the second deployment. This solution would have the fastest recovery time.

**Incorrect Option A)** Creation of a new database from backups is part of a backup and restore DR strategy, which takes a long time. A pilot light strategy would result in faster recovery time. The promotion of a read replica of the primary database would be an example of a pilot light strategy.

**Incorrect Option C)** The creation of a new database from backups is part of a backup and restore DR strategy, which takes a long time. A pilot light strategy would result in faster recovery time. The promotion of a read replica of the primary database would be an example of a pilot light strategy.

**Incorrect Option D)** because the promotion of a read replica would be a faster option than the creation of a database from backups. However, configuration of a weighted routing policy for Route 53 would not automatically route traffic to the second Region. This solution would require a manual intervention. This solution would not have the fastest recovery time.

For more information about how to create a read replica for Amazon RDS in a different Region, see Creating a Read Replica in a Different AWS Region.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.XRgn.html>

For more information about the promotion of read replicas, see Working with Read Replicas.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.XRgn.html>

For more information about routing policies, see Choosing a Routing Policy

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

For more information about restoration from a DB snapshot, see Restoring from a DB Snapshot.

For more information about DR strategies, see Disaster Recovery Options in the Cloud.

For more information about restoration from a DB snapshot, see Restoring from a DB Snapshot.

For more information about DR strategies, see Disaster Recovery Options in the Cloud.

For more information about the promotion of read replicas, see Working with Read Replicas.

For more information about routing policies, see Choosing a Routing Policy.

**Question 06/75**

A company has deployed multiple copies of a reporting application in separate AWS accounts to serve users from different departments The applications run on Amazon EC2 instances that run in Auto Scaling groups. When the EC2 instances in the Auto Scaling groups scale in, they leave behind objects in a central Amazon S3 bucket These objects must be cleaned up within a few minutes. The S3 objects are prefixed with the instance ID. The team that manages these applications wants to minimize cost and must use Amazon Event Bridge as part of the solution.

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

1. Create EventBridge rules in each of the AWS accounts to push events to an Amazon Simple Queue Service (Amazon SQS) queue in a central account. Configure Spot Instances to process the SQS messages and clean up the S3 folder and objects.
2. Create an EventBridge bus in a central account. Create an EventBridge rule in each of the AWS accounts. Configure the rule to push the events to the central account event bus from source "aws.autoscaling". Specify an Amazon Elastic Container Service (Amazon ECS) task as a target in the central account.
3. ***Create an EventBridge bus in a central account. Create an EventBridge rule in each of the AWS accounts. Configure the rule to push the events to the central account event bus from source "aws.autoscaling". Invoke an AWS Lambda function in the central account to clean up the S3 folder and objects.***
4. Create an EventBridge rule in each of the AWS accounts to handle events from source "aws.autoscaling". Configure AWS Lambda functions on each of the accounts to clean up the S3 folder and objects.

**Correct Answer: C**

Explanation:

**Correct Option C**) You can centralize the event logging by using EventBridge. You can also use a single Lambda function to perform cleanup. A solution that updates only one Lambda function is operationally efficient.

**Incorrect Option A)** Although Amazon SQS can manage the message queue, a solution that uses Amazon SQS with EC2 Spot Instances would require more operational overhead than necessary.

**Incorrect Option B)** Although Amazon ECS can be the target in the central account, this is not the solution with least operational overhead.

**Incorrect Option D)** This solution would result in multiple pipeline configurations and duplication of code in Lambda functions. These drawbacks would make operations cumbersome.

**Question 07/75**

A company has offices in several countries. Each office has its own AWS account. The company manages

all accounts centrally by using AWS Organizations While implementing a process to centralize security policies, system operators from multiple accounts simultaneously report an inability to access any Amazon S3 buckets.

What should the system operators do to restore access to the S3 buckets?

1. Sign in to each of the member accounts as the account root user. Open AWS Identity and Access Management (IAM). Correct any IAM policy that is blocking access to Amazon S3.
2. Sign in to the management account as an IAM user with appropriate permissions. Open AWS Identity and Access Management (IAM). Correct any IAM policy that is blocking access to Amazon S3.
3. ***Sign in to the management account as an IAM user with appropriate permissions. Open Organizations. Correct any SCP that is blocking access to Amazon S3.***
4. Sign in to each of the member accounts as the account root user. Open Organizations. Correct any SCP that is blocking access to Amazon S3.

**Correct Answer: C**

Explanation:

**Correct Option C)** because the fact that multiple accounts are affected simultaneously indicates that SCPs are a cause. The management account allows access to manage SCPs because the management account is unaffected by SCPs.

**Incorrect Option A)** because an administrator can define permissions within a single AWS account by using IAM policies. However, the presence of errors in multiple accounts at the same time indicates that an SCP might be the problem.

For more information about IAM, see Overview of Access/Management: Permissions and Policies.

For more information about SCPs, see Service Control Policies (SCPs).

**Incorrect Option B)** because an administrator can define permissions within a single AWS account by using IAM policies. However, the presence of errors in multiple accounts at the same time indicates that an SCP might be the problem.

**Incorrect Option D)** The fact that the outages occurred at the same time indicates that the problem might be related to SCPs at a higher level of the organization. The member accounts of an organization are not able to inspect or change the SCPs that have been applied at any level in the organization's hierarchy.

For more information about SCPs, see Service Control Policies

For more information about Organizations management accounts, see Best Practices for the Management Account.

**Question 08/75**.

A company is developing a new game app for mobile devices. The app has two user tiers one tier for

*free-play users and another tier for premium* users. The company currently uses custom identity authentication across its apps The company wants to continue to use custom authentication if possible, However, the company's custom identity provider (ldP) is *not compatible with either the SAML or OpenlD Connect (OIDC)* standards. A solutions architect needs to design an authentication approach that makes it easy to transition free-play users to premium users.

Which design will meet these requirements with the **LEAST** development effort?

﻿

1. ***Create a single Amazon Cognito identity pool. Develop an authentication provider for the pool that calls the existing custom IdP. Implement two separate authentication flows in the mobile app: one for the free-play users and one for the premium users.***
2. Create an Amazon Cognito user pool for the premium users. Add a user pool sign-in through the custom IdP. Create a second Amazon Cognito user pool to provide guest access for the free-play users.
3. Create two Amazon Cognito identity pools. Develop an authentication provider for the premium user identity pool that calls the existing custom IdP. For the second identity pool, configure an authentication flow for the free-play users.
4. Create a single Amazon Cognito user pool. Add a user pool sign-in through the custom IdP. Set up Amazon Cognito guest access in the same user pool for the free-play users.

**Correct Answer: A**

**Explanation:**

**Correct Option A)** because the code for the authentication provider would be a wrapper that allows the company to use its existing identity authentication functionality. The company should design the mobile app with two authentication flows to support free-play users and premium users. The use of a single identity pool also supports an easy transition between the free-play tier and the premium tier.

**Incorrect Option B**) The company has a custom IdP that is not based on SAML or OIDC. The user pool sign-in features of Amazon Cognito would not support the company's custom IdP. Significant development effort would be necessary to build a new IdP that is compliant with SAML or OIDC.

**Incorrect Option C)** because the creation of two identity pools would potentially require double the development work. This design would also be difficult to implement on the mobile app side. The use of two pools would also make the transition between the free-play tier and the premium tier more difficult. Significant development effort would be necessary to create a new premium user in the respective identity pool and to remove the user from the free-play user identity pool.

**Incorrect Option D)** because the company has a custom IdP that is not based on SAML or OIDC. The user pool sign-in features in Amazon Cognito would not support the company's custom IdP. Significant development effort would be necessary to build a new IdP that is compliant with SAML or OIDC.

**Question 09/75**

A company operates a large mixed fleet of Windows and Linux servers that are deployed on Amazon

EC2. A solutions architect needs to design a unified and ongoing maintenance solution. The solution must deploy any updates and security patches in an automated and secure manner.

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

1. Install and use each operating system's native patching service to manage the update frequency. Release approval for all instances. Configure AWS Config to query the operating system state on each instance and report on any patch compliance issues.
2. Migrate all applications to AWS OpsWorks Stacks. Use OpsWorks automatic patching support to keep the operating systems up to date after the initial installation. Configure AWS Config to query OpsWorks to report on the results of compliance audits.
3. Use AWS OpsWorks for Chef Automate to run a set of Chef recipes that will iterate through all instances that require patching. Issue the appropriate operating system command to get and install updates on each instance during a maintenance window.
4. ***Deploy AWS Systems Manager Agent on all instances. To patch instances, use the preconfigured Systems Manager documents that AWS provides. Apply baselines. Deploy updates and patches to production during a maintenance window.***

**Correct Answer: D**

Explanation:

**Correct Option D)** because with Systems Manager, administrators can automate operational tasks across Windows and Linux operating systems. AWS provides preconfigured Systems Manager documents to help keep managed instances patched with the latest security-related updates.

**Incorrect Option A)** because AWS Config provides a detailed view of the configuration of AWS resources in an AWS account. Use of AWS Config to query the operating system state would not meet the requirements because AWS Config not would have the ability to collect data from the operating system.

**Incorrect Option B)** OpsWorks Stacks provides a flexible way to create and manage stacks and applications on AWS. OpsWorks Stacks can automatically install the latest updates for select Linux operating systems. However, OpsWorks Stacks does not provide a way to apply updates to online Windows instances.

**Incorrect Option C)** With OpsWorks for Chef Automate, administrators can focus on configuration management tasks instead of management of a Chef server. A patching solution that uses OpsWorks for Chef Automate would involve considerable effort to build all the Chef recipes. A solution with less operational overhead would use Systems Manager.

For more information about AWS Config, see What is AWS Config?

<https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>

**Question 10/75**

A company has a serverless application that is backed by an Amazon RDS database. The company's AWS Lambda functions share the same user account to access the database.

A database administrator updates the password in the database to comply with security policies Shortly after the update, several Lambda functions fail. The user receives an error message for credentials that are not valid. After investigating the error, a solutions architect discovers that the affected Lambda functions use hardcoded credentials. The solutions architect needs to address the errors and improve the

security of the credentials.

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

1. Store the user’s name and password in AWS Secrets Manager. Update the Lambda functions to retrieve the user’s name and password from Secrets Manager. Configure an alternating user’s automatic rotation of the credentials as required.
2. Create a Lambda function to update the credentials in the RDS database. Schedule the Lambda function to run as required. Configure an Amazon EventBridge rule that invokes a Lambda function to update the hardcoded passwords whenever the password is changed in the RDS database.
3. ***Store the user’s name and password in AWS Secrets Manager. Update the Lambda functions to retrieve the user’s name and password from Secrets Manager. Configure a single user automatic rotation of the credentials as required.***
4. Store the credentials in AWS Systems Manager Parameter Store. Update the Lambda functions to retrieve the user’s name and password from Parameter Store. Configure an Amazon EventBridge rule that invokes a Lambda function to update Parameter Store whenever the password is changed in the RDS database.

**Correct Answer: C**

Explanation:

**Correct Option C)** because secrets Manager replaces hardcoded credentials with API calls to retrieve secrets programmatically. You can configure Secrets Manager to automatically rotate RDS database passwords. In this scenario, the database has a single application user account. For this reason, the single user rotation strategy would be appropriate. This solution requires no new Lambda functions, so it requires the least development effort.

For more information about Secrets Manager, see What is AWS Secrets Manager?

For more information about rotation strategies, see Rotation Strategies.

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets_strategies.html>

**Incorrect Option A)** Secrets Manager replaces hardcoded credentials with API calls to retrieve secrets programmatically. You can configure Secrets Manager to automatically rotate RDS database passwords. An alternating user’s rotation updates credentials for two users in one secret. However, in this scenario, the database has only a single application user account.

For more information about Secrets Manager, see What is AWS Secrets Manager?

For more information about rotation strategies, see Rotation Strategies.

**Incorrect Option B)** because significant code development would be required to create multiple Lambda functions to rotate the passwords both in the database and the applications.

**Incorrect Option D)** Parameter Store can securely store the credentials. However, the creation of an extra Lambda function to rotate the password involves significant code development. This solution also requires manual updates of the database.

**Question 11/75**

A company needs to migrate two individual applications from on premises to AWS

* The first application is a legacy custom application that is hosted on a physical Windows server. The

application source code is no longer available. This application has little documentation, has hardcoded operating system configuration settings, and is used by an external third party."

* The second application is an IBM Db2 database that is hosted on a single Linux VM that uses

network-attached storage (NAS) to store the database data. The company uses this database internally for employee records.

The applications are hosted in a data center that the company plans to decommission in 90 days. Wherever

possible, the company must use managed AWS services.

Which actions for migration should a solutions architect recommend to meet these requirements?

(Select TWO}

1. ***Migrate the Windows server with the legacy application to Amazon EC2 by using AWS Application Migration Service (CloudEndure Migration).***
2. Migrate the Linux VM with the IBM Db2 database service to an Amazon EC2 instance by using AWS Application Migration Service (CloudEndure Migration).
3. Migrate the Windows server with the legacy application to Amazon EC2 by using AWS Server Migration Service (AWS SMS).
4. ***Migrate the IBM Db2 database data to Amazon RDS for MySQL by using AWS Database Migration Service (AWS DMS) and the AWS Schema Conversion Tool (AWS SCT) replication agent.***
5. Migrate the IBM Db2 database data to Amazon RDS for MySQL by using AWS DataSync and the AWS Schema Conversion Tool data extraction agent.

**Correct Answer: A, D**

Explanation:

Correct Option A) because rehost (lift and shift) method is the only viable option because of the application type and because the application is on a physical server. Because the application uses custom OS configurations, Application Migration Service is the best option. Although Amazon EC2 is not a managed service, it is the only option for this use case.

**Correct Option D)** This solution will replatform the existing database server to Amazon RDS. AWS DMS gives you the ability to convert from IBM Db2 to a supported RDS engine such as MySQL. You need AWS SCT to support the schema conversion to Amazon RDS.

**Incorrect Option B)** Although this solution is a possibility, the company wants to use a managed AWS service. Amazon EC2 is not the best option because it is not a managed service. The company can migrate the IBM Db2 database to a managed database service such as Amazon RDS for MySQL.

**Incorrect Option C)** You cannot use AWS SMS in this scenario because the application is on a physical server.

**Incorrect Option E)** DataSync is an online data transfer service that simplifies, automates, and accelerates the movement of data between storage systems and services. You cannot use DataSync to migrate databases.

For more information about AWS SMS, see What Is [AWS Server Migration Service](https://aws.amazon.com/server-migration-service/)?

For more information about AWS DMS, see [AWS Database Migration Service](https://aws.amazon.com/dms/) Supports IBM Db2 as a Source.

For more information about AWS SCT, see What Is the [AWS Schema Conversion Tool](https://docs.aws.amazon.com/dms/latest/sbs/schema-conversion-oracle-aurora-mysql.html)?

**Question 12/75**

A company migrates its application to AWS with 25 VPCs and 1 transit gateway in a single AWS Region.

The company establishes hybrid connectivity between its on-premises data center and that Region by using AWS Direct Connect The company's client base is growing in a new geographic area, and the company creates two VPCs in a second Region The plan is to move some applications to the second Region for testing purposes. The company needs to have hybrid connectivity to communicate with resources in the second Region from the on-premises data center.

Which combination of steps will meet these requirements with the LEAST operational effort?

(Select TWO) ﻿

1. ***Associate a Direct Connect gateway with virtual private gateways for the two VPCs in the second Region. Create a private VIF for the Direct Connect connection to the Direct Connect gateway.***
2. Order a second connection through Direct Connect to connect to the second Region. Deploy private VIFs on the Direct Connect connections for the VPCs that are attached to the virtual private gateways.
3. Deploy private VIFs for each VPC. Attach the private VIFs to a virtual private gateway.
4. ***Create a Direct Connect gateway in the first Region. Attach the transit gateway in the first Region to the new Direct Connect gateway by using a transit VIF.***
5. Deploy a new transit gateway in the second Region. Peer the transit gateway in the first Region to the new transit gateway in the second Region.

**Correct Answer: A, D**

Explanation:

**Correct Option A)** A Direct Connect gateway can connect a Direct Connect connection to a VPC or transit gateway in any Region. The connection between the VPCs in the second Region and the Direct Connect gateway in the first Region will extend the hybrid connectivity to the new VPCs.

**Correct Option D)** A transit gateway connects VPCs and on-premises networks through a central hub. An attachment between the transit gateway and a new Direct Connect gateway will extend hybrid connectivity to any VPCs that are associated with the Direct Connect gateway.

**Incorrect Option B)** A second Direct Connect connection, along with a private VIF deployed on the Direct Connect connection, would meet the requirements. However, this solution requires additional operational effort to maintain a second Direct Connect connection. A better solution would use the existing connection to avoid this additional operational effort.

**Incorrect Option C)** A private VIF should be used to access a VPC by using private IP addresses. However, deployment of private VIFs for each VPC is a part of the configuration step in the sequence of steps to set up a second Direct Connect connection. In this scenario, the use of a second Direct Connect connection would require more operational effort than using the existing connection.

**Incorrect Option E)** A transit gateway connects VPCs and on-premises networks through a central hub. If you create a second transit gateway and peer the two transit gateways, you establish traffic between only the two Regions. This solution does not establish hybrid connectivity from the on-premises data center to the second Region.

For more information about Direct Connect gateways, see Direct Connect Gateways.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

For more information about transit gateways and Direct Connect, see

<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-dcg-attachments.html>

For more information about Direct Connect VIFs, see Which Type of Virtual Interface Should I Use to Connect Different Resources in AWS?

<https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx>

**Question 13/75**

A company recently migrated a large, re-startable batch computing workload from on-premises servers to

AWS Batch. The batch job runs monthly in an Amazon EC2 compute environment that requires a custom AMI. The company wants to reduce the overhead that is associated with the management of the compute

environment. The company also wants to reduce the cost to run the AWS Batch workload.

Which solution will meet these requirements?

﻿

1. Modify the AWS Batch job to run in a managed EC2 compute environment that uses the AMI. Select On-Demand as the provisioning model.
2. Modify the AWS Batch job to run in a managed EC2 compute environment that uses the AMI. Select Spot as the provisioning model.
3. Modify the AWS Batch job to run in an AWS Fargate compute environment. Select Fargate as the provisioning model.
4. Modify the AWS Batch job to run in an AWS Fargate compute environment. Select Fargate Spot as the provisioning model.

**Correct Answer: B**

Explanation:

**Correct Option B)** With AWS Batch, you need an EC2 compute environment in order to use the custom AMI. A managed compute environment would help reduce the overhead that is associated with the management of the compute environment. Also, the Spot provisioning model would have a lower cost for a restartable, monthly workload. This solution meets the requirements.

For more information about the compute environment options for AWS Batch, see Compute Environment.

<https://docs.aws.amazon.com/batch/latest/userguide/compute_environments.html>

**Incorrect Option A)** With AWS Batch, you need a managed EC2 compute environment in order to use the custom AMI. However, because the AWS Batch job is restartable and runs monthly, Spot provisioning would be a lower-cost option than On-Demand.

**Incorrect Option C)** Fargate would reduce the overhead that is associated with management of the compute environment. However, you need a managed EC2 compute environment in order to use the custom AMI.

For more information about AWS Batch on Fargate, see AWS Batch on AWS Fargate.

<https://docs.aws.amazon.com/batch/latest/userguide/fargate.html>

**Incorrect Option D)** Fargate would reduce the overhead that is associated with management of the compute environment. However, you need an EC2 compute environment in order to use the custom AMI.

**Question 14/75**

A company uses AWS Organizations with OUs in a single organization. The OUs are Finance, HR, IT, and Recruiting. Each OU contains several accounts. All the OUs have different SCPs attached to them. The HR and Recruiting OUs share some common policy requirements. However, the Recruiting OU has some additional required restrictions. When the company needs to create new common SCP restrictions for the HR and Recruiting OUs, the company wants to avoid duplicating effort to update both SCPs.

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

1. Move the accounts that are under the Recruiting OU out of the organization. Remove the Recruiting OU. Recreate the Recruiting OU as a child OU under the HR OU. Add the accounts back into the new Recruiting OU. Remove the duplicate rules from the SCP for the Recruiting OU. Attach the updated SCP to the new Recruiting OU.
2. ***Rename the Recruiting OU to Recruiting\_Old. Create a new OU named Recruiting as a child OU under the HR OU. Move the accounts that are under Recruiting\_Old to the new Recruiting OU. Remove the duplicate rules from the SCP for the Recruiting Old OU. Attach the updated SCP to the new Recruiting OU. Remove the Recruiting Old OU from the organization.***
3. Rename the HR OU to HR\_Old. Create a new OU named HR as a child OU under the Recruiting OU. Move the accounts that are under HR\_Old to the new HR OU. Remove the duplicate rules from the SCP for the HR\_Old OU. Attach the updated SCP to the new HR OU. Remove the HR\_Old OU from the organization.
4. Move the accounts that are under the HR OU out of the organization. Remove the HR OU. Recreate the HR OU as a child OU under the Recruiting OU. Add the accounts back into the new HR OU. Remove the duplicate rules from the SCP for the HR OU. Attach the updated SCP to the new HR OU.

**Correct Answer: B**

Explanation:

**Correct Option B)** Organizations gives you the ability to create new OUs and to move accounts between OUs. Because the SCP for Recruiting has more restrictions than the SCP for HR, Recruiting should be the child OU with the more restrictive SCP attached. This solution requires minimal operational overhead.

**Incorrect Option A)** If you move an account out of an organization, you need to issue new invitations to add the account back to the organization. This solution requires more operational effort than a solution that moves accounts between OUs.

**Incorrect Option C)** Organizations gives you the ability to create new OUs and to move accounts between OUs. However, because the SCP for Recruiting has more restrictions than the SCP for HR, the Recruiting OU should be the child with the more restrictive SCP attached.

**Incorrect Option D)** If you move an account out of an organization, you need to issue new invitations to add the account back to the organization. This solution requires more operational effort than a solution that moves accounts between OUs.

**Question 15/75**

A company is planning to migrate a mix of Windows-based applications and Linux-based applications that

run on on-premises physical servers to Amazon EC2 instances. The company needs to manage and monitor the migration from the AWS Management Console by using Amazon CloudWatch and AWS CloudTrail. The company needs to control the migration process permissions and access by using AWS Identity and Access Management (IAM)

Which solution will meet these requirements?

1. ***Install the AWS Replication Agent on each source server. Initialize AWS Application Migration Service. Configure the launch settings and deploy the target EC2 instances.***
2. Install and register the VMware Hybrid Cloud Extension (HCX) connector. Select servers from the company's server catalog. Configure the replication settings and deploy the target EC2 instances.
3. C)Install and register the VMware Hybrid Cloud Extension (HCX) connector. Select servers from the company's server catalog. Configure the replication settings and deploy the target EC2 instances.
4. D)Install the CloudEndure Agent on each source server. Create a Blueprint for the target environment. Use CloudEndure Migration to migrate to EC2.

**Correct Answer: A**

Explanation:

**Correct Option A)** AWS Application Migration Service is a highly automated lift-and-shift solution that simplifies and accelerates the migration to AWS for applications that are running on physical servers and VMs. This solution can be managed and monitored from the console and can be used with IAM, CloudWatch, and CloudTrail.

**Incorrect Option B)** VMware HCX automates the migration of on-premises VMs to the AWS Cloud. AWS SMS can be used only for VMs, not the physical servers that the company intends to migrate.

**Incorrect Option C)** AWS Application Discovery Service collects usage and configuration data about on-premises servers to help you plan migrations to the AWS Cloud by. Application Discovery Service requires additional services to perform the actual migration.

**Incorrect Option D)** CloudEndure Migration cannot be managed and monitored in the AWS Management Console. Also, permissions and access cannot be controlled by IAM.

For more information about Application Migration Service ([CloudEndure Migration](https://docs.aws.amazon.com/mgn/latest/ug/what-is-application-migration-service.html)), see What Is AWS Application Migration Service?

For more information about [VMware HCX, see Migrate VMware SDDC to VMware Cloud on AWS using VMware HCX](https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-vmware-sddc-to-vmware-cloud-on-aws-using-vmware-hcx.html).

For more information about Application Discovery Service, see What Is [AWS Application Discovery Service?](https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html)

**Question 16/75**

A global company uses multiple accounts. Each account runs resources in three AWS Regions The company needs identical Amazon EC2 instances as test systems in the different accounts. A solutions architect creates a custom AMI and an AWS CloudFormation template to provision the test systems in the company's main development account The solutions architect shares the AMI across accounts and copies the AMI to each Region The solutions architect shares the CloudFormation template to the various accounts and edits the template to refer to the appropriate AMI ID for each Region. The solutions architect needs to reduce the manual work that is necessary to create each new custom AMI.

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

1. ﻿Create AWS Systems Manager Parameter Store parameters that have identical names in each Region for each account. Include the appropriate AMI IDs for that Region in the parameters. Configure the CloudFormation template to retrieve the AMI ID from the parameters. Use the single CloudFormation template in the main development account to provision the test systems in all the accounts. Update the parameters as required when the company creates and shares a new AMI.
2. Create AWS Systems Manager Parameter Store parameters that have identical names in each Region for each account. Include the appropriate AMI IDs for that Region. Configure the CloudFormation template to retrieve the AMI ID from the parameters. Copy the CloudFormation template to each account and Region. Use the template to create the required resources. Update the parameters as required when the company creates and shares a new AMI.
3. Create a mapping section in the CloudFormation template to hold the AMI IDs for each Region. Update the template to retrieve the correct AMI ID from the mapping. Import the CloudFormation template into each account. Use the template to create the required resources. Update the mapping as required when the company creates and shares a new AMI.
4. ***Create a mapping section in the CloudFormation template to hold the AMI IDs for each Region. Update the template to retrieve the correct AMI ID from the mapping. Use CloudFormation StackSets to create a stack set in the main development account. Use the stack set to deploy stack instances in each account as needed. Update the mapping as required when the company creates and shares a new AMI.***

Correct Answer: **D**

Explanation:

**Correct Option D)** StackSets extends the functionality of CloudFormation stacks by giving users tools to manage stacks across multiple accounts and Regions. A solution that uses mappings in a CloudFormation template and creates a single stack set to deploy multiple stack instances to the multiple accounts and Regions would require less operational overhead than a solution that requires maintenance of multiple CloudFormation templates.

**Incorrect option A)** CloudFormation template can create resources only in the account where the template resides. This solution would not give the solutions architect the ability to provision test systems in the other accounts.

**Incorrect option B)** Parameter Store provides storage for configuration data, including passwords, database strings, and AMI IDs. Less operational overhead is required to store the AMI ID in Parameter Store than to hardcode the AMI IDs in the CloudFormation templates. A solution that relies on maintenance of parameters in each account and of multiple CloudFormation templates will require more operational overhead than a solution that uses CloudFormation StackSets and mappings.

**Incorrect Option C)** A solution that uses mappings in a CloudFormation template requires less operational overhead than a solution that hardcodes the AMI IDs. Maintenance of multiple CloudFormation templates would require more operational overhead than usage of CloudFormation StackSets.

For more information about mappings, see Mappings.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/mappings-section-structure.html>

For more information about StackSets, see Working with AWS CloudFormation StackSets.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/what-is-cfnstacksets.html>

**Question 17/75**

A company recently deployed a prototype application on an Amazon EC2 instance that runs Linux. The

EC2 instance uses a Provisioned IOPS SSD Amazon Elastic Block Store (EBS) volume. The prototype application was successful, and the company plans to deploy the application to production.

The application has one step that produces an output file for subsequent steps to read and update. The

company plans to run two copies of the application It is possible to process the individual steps on

different servers. A solutions architect needs to update the architecture to be highly available for both the files and the application

Which solution will meet these requirements?﻿

1. Deploy a second EC2 instance in another Availability Zone with an identical EBS volume. Configure AWS DataSync to synchronize data between the two EBS volumes.
2. Deploy a second EC2 instance in another Availability Zone. Configure EBS Multi-Attach to share access to the files from both EC2 instances.
3. Deploy a second EC2 instance in another AWS Region. Create an Amazon Elastic File System (Amazon EFS) file system that uses EFS Standard storage. Configure both EC2 instances with shared access to the EFS file system.
4. ***Deploy a second EC2 instance in another Availability Zone. Create an Amazon Elastic File System (Amazon EFS) file system that uses EFS Standard storage. Configure both EC2 instances with shared access to the EFS file system.***

**Correct Answer: D**

Explanation:

**Correct Option D)** Deployment of a second EC2 instance in another Availability Zone would improve the availability of the application. Shared access is needed because steps can be processed on different servers. An EFS file system with EFS Standard storage would provide both EC2 instances with shared access to the data. Additionally, the EFS file system would automatically provide high availability for the data.

For more information about Amazon EFS, see What is [Amazon Elastic File System](https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html)?

**Incorrect Option A)** DataSync can move data between some AWS storage services. However, DataSync does not work with EBS volumes.

**Incorrect Option B)** Shared access is needed because steps can be processed on different servers. With EBS Multi-Attach, multiple instances could access the EBS volume. However, the instances must be in the same Availability Zone. Additionally, EBS Multi-Attach would not provide high availability protection for the data.

For more information about EBS Multi-Attach, see Attach a Volume to Multiple Instances with [Amazon EBS Multi-Attach.](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html)

**Incorrect Option C)** Shared access is needed because steps can be processed on different servers. An EFS file system with EFS Standard storage would provide both EC2 instances with shared access to the data. However, EC2 instances can access an EFS shared file system only if the EFS file system is in the same Region as the EC2 instances.

**Question 18/75**

A company is running an application on Amazon EC2 instances in an Amazon EC2 Auto Scaling group

The Auto Scaling group extends across multiple Availability Zones in a single AWS Region. A new requirement states that the architecture must support a multi-Region, active-active disaster recovery strategy.

The company clones the same architecture to the second Region The company needs to provide two

static IP addresses to customers so that customers can connect to the application without a need for the company to change the configuration The new architecture must serve requests with the lowest possible latency.

Which solution meets these requirements with the LOWEST latency?

1. Use Network Load Balancers (NLBs). Create a Route 53 failover routing record that points to the two NLBs.
2. Use Application Load Balancers (ALBs). Create a Route 53 latency routing record that points to the two ALBs.
3. ***Use Network Load Balancers (NLBs). Configure AWS Global Accelerator to point to the two NLBs.***
4. Use Network Load Balancers (NLBs). Create a Route 53 geolocation routing policy that resolves to the two NLBs.

**Correct Answer: C**

Explanation:

**Correct Option C)** Global Accelerator simplifies global traffic management by providing two static anycast IP addresses that you would need to configure only once. With Global Accelerator, traffic will remain within the low-latency AWS global network, and the static IP addresses will allow customer applications to connect without the need for reconfiguration.

For more information about Global Accelerator, see How [AWS Global Accelerator](https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works.html#about-static-ip-addresses) Works.

**Incorrect Option A)** Route 53 failover routing does not dispatch requests with the lowest possible latency. Requests would travel across the regular internet instead of the low-latency AWS global network.

For more information about Route 53 routing options, see Choosing a Routing Policy.

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

**Incorrect Option B)** ALBs do not support static IP addresses. The company needs to provide static IP addresses.

For more information about Elastic Load Balancer types, see Elastic Load Balancing Types.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html#integrations-aws-elastic-load-balancing-types>

**Incorrect Option D)** A Route 53 geolocation routing policy serves traffic based on the geographic location. This solution does not provide the lowest latency because requests would travel across the regular internet instead of the low-latency AWS global network.

**Question 19/75**

A company uses several services to store important data within a single AWS Region. These services include Amazon S3, Amazon Elastic Block Store (Amazon EBS), Amazon Elastic File System (Amazon EFS), Amazon RDS, and on-premises storage servers. The company wants a backup and data protection solution that would offer Regional protection for all the company's existing data. The solution must automate the processes on AWS as much as possible. The company has configured AWS Storage Gateway Volume Gateway for the on-premises data.

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

1. ﻿Configure AWS Data Sync to replicate the data that is in EFS file systems to another Region. Create a cross-Region backup plan in AWS Backup that includes data that is in S3 buckets, EBS volumes, RDS databases, and the Storage Gateway volumes.
2. ***Create an AWS Backup vault in another Region. Create a cross-Region backup plan in AWS Backup by using the vault that includes data that is in S3 buckets, EBS volumes, EFS file systems, RDS databases, and the Storage Gateway volumes.***
3. Create a read replica of the RDS databases in another Region. Create a cross-Region backup plan in AWS Backup that includes the data that is in S3 buckets, EBS volumes, EFS file systems, and the Storage Gateway volumes.
4. Create EBS snapshots and copy the EBS snapshots to a different Region. Create a cross-region backup plan in AWS Backup that includes data that is in S3 buckets, EFS file systems, RDS databases, and the Storage Gateway volumes.

**Correct Answer: B**

Explanation:

**Correct Option B)** AWS Backup can automatically back up data that is in S3 buckets, Storage Gateway volumes, EBS volumes, EFS file systems, and RDS databases. A cross-Region backup plan would offer the required regional protection for the data. This solution would incur the least operational overhead.

**Incorrect Option A)** AWS Backup can automatically back up data that is in S3 buckets, Storage Gateway volumes, EBS volumes, EFS file systems, and RDS databases. Replicas of the EFS file systems are not necessary and would incur unnecessary operational overhead.

**Incorrect Option C)** AWS Backup can automatically back up data that is in S3 buckets, Storage Gateway volumes, EBS volumes, EFS file systems, and RDS databases. RDS read replicas are not a backup solution. Read replicas of the RDS databases would not address the requirements but would add unnecessary operational overhead.

**Incorrect Option D)** AWS Backup can automatically back up data that is in S3 buckets, Storage Gateway volumes, EBS volumes, EFS file systems, and RDS databases. However, it is not necessary to use DataSync to replicate the EBS volumes because AWS Backup can back up EBS volumes. Cross-Region replication would automatically protect the data that is in S3 buckets with less operational overhead.

**Question 20/75**

A company uses AWS Key Management Service (AWS KMS) to manage a small number of AWS KMS

customer-managed keys. Recently, one of the keys was accidentally deleted. The company did not

discover the error within the mandatory waiting period for deleting AWS KMS keys, so the company lost a small amount of infrequently accessed data.

The company has configured AWS CloudTrail to deliver logs to Amazon CloudWatch Logs and Amazon

S3 buckets. The company wants its systems administrator to receive notification about AWS KMS key deletions in a timely manner so that the company can avoid accidental key deletions in the future.

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

1. Create an Amazon Athens query to check the CloudTrail entries in the S3 bucket for AWS KMS key deletion requests. Run the query regularly. Configure the query to deliver the results to the systems administrator. Cancel deletion requests if necessary.
2. Create an Amazon EventBridge rule to produce an alert when an AWS KMS key deletion request is performed. Configure the rule to invoke an AWS Lambda function as the target. Configure the Lambda function to cancel the deletion request.
3. Create and schedule a daily Amazon Athens query to check the Cloud Trail entries in the S3 bucket for AWS KMS key deletion requests. Configure the query to deliver the results to the systems administrator. Cancel deletion requests if necessary.
4. ***Create an Amazon EventBridge rule to produce an alert when an AWS KMS key deletion request is performed. Configure the rule to send an Amazon Simple Notification Service (Amazon SNS) message to the systems administrator. Cancel the deletion request if necessary.***

**Correct Answer: D**

Explanation:

**Correct option D)** EventBridge has prebuilt rules to produce alerts for AWS KMS key deletion requests. Amazon SNS is a managed service that provides message delivery from publishers to subscribers. This solution requires the least operational effort to provide the notification to the systems administrator.

**Incorrect Option A)** Athena is an interactive query service that helps users analyse data directly in Amazon S3 by using standard SQL. This solution requires more operational effort than the correct answer.

**Incorrect Option B)** EventBridge has prebuilt rules to produce alerts for AWS KMS key deletion requests. However, the use of a Lambda function to cancel the delete request is not appropriate if the request is not an accident. The system administrator needs to review the request to determine if the request was made in error.

**Incorrect option C)** Athena is an interactive query service that helps users analyse data directly in Amazon S3 by using standard SQL. This solution requires more operational effort than the correct answer.

**Question 21/75**

A company wants to store thousands of objects in Amazon S3. Object key names can have the following

prefixes

• mk (marketing)

• sa (sales)

• ex (executive)

Access should be based on the following rules

• Marketing managers must have access only to objects with the **mk** prefix

• Sales managers must have access only to objects with the **sa** prefix

• Sales and marketing directors must have access to objects with both the **mk** and **sa** prefixes

• The finance administrator needs access to all objects with any prefix

The company needs an access solution that provides the ability to add more prefixes in the future.

Which solution will meet these requirements with the LEAST ongoing administrative effort?

1. Create four S3 buckets. Separate the mk, sa, and ex objects into three separate S3 buckets. Replicate the mk and sa objects into the fourth $3 A bucket and the ex S3 bucket. Define the appropriate IAM resource-based policy for each $3 bucket to control access. Give the correct URL for each S3 bucket to each employee.
2. Create one S3 bucket. Place all the objects in the S3 bucket. Create multiple appropriate IAM policies based on the three prefixes. Attach the correct IAM policy to each object in the S3 bucket based on the object name. Give the single URL for the S3 bucket to all employees.
3. Create one S3 bucket. Create a folder with subfolders for the mk and sa objects. Attach the appropriate IAM resource-based policies to the folders. Create a separate folder for the ex C objects. Define the appropriate IAM resource- based policy on the S3 bucket for the finance administrator. Give the folder URLs to the managers and directors. Give the S3 bucket URL to the finance administrator.
4. ***Create one S3 bucket. Place all the objects in the S3 bucket. Create three $3 access points that are based on the object prefixes for mk, sa, and both. Attach the appropriate IAM resource-based policies to the S3 access points and the $3 bucket. Give the appropriate S3 access point aliases to the managers and directors. Give the URL for the S3 bucket to the finance administrator.***

**Correct Answer: D**

Explanation:

**Correct Option D)** S3 access points simplify data access for any AWS service or customer application that stores data in Amazon S3. You can attach IAM policies directly to the S3 access points. Employees would have a single URL to access their objects. This solution also gives the company a flexible way to add S3 access points for future prefixes.

For more information about S3 access points, see Managing Data Access with Amazon S3 Access Points.

For more information about IAM resource-based policies, see Resource-Based Policies.

**Incorrect Option A)** This solution would separate access and would provide a single URL for each employee. However, if you add a new prefix later, you would have to create a new S3 bucket and replicate the new bucket to the ex bucket. This solution does not require the least ongoing administrative effort.

**Incorrect Option B)** A policy defines the permissions for the identities or resources with which the policy is associated. You cannot attach IAM policies directly to objects. You must attach IAM resource-based policies to the S3 buckets.

**Incorrect Option C)** A policy defines the permissions for the identities or resources with which the policy is associated. You cannot attach IAM policies directly to folders in an S3 bucket. You must attach IAM resource-based policies to the S3 buckets.

**Question 22/75**

A company runs a web application on Amazon EC2 instances behind an Application Load Balancer (ALB)

The instances run in an Amazon EC2 Auto Scaling group The company's customers use the DNS name of the ALB to reach the application.

The company has gained new customers in a new geographic area and hopes to expand further. The

company has purchased a new domain and wants customers to use the apex domain name to access the application from anywhere. The company has deployed an identical configuration in a second AWS Region in the new area. The company wants to reconfigure its deployment to provide a highly available

solution and a faster experience to its new global customers.

What should the company do to meet these requirements?

1. ***Create an Amazon Route 53 public hosted zone with a record for the apex domain name. Set up a DNS active-active failover configuration that uses latency-based routing. Set "Evaluate Target Health" to "Yes" for the set of alias resource records.***
2. Create an Amazon Route 53 public hosted zone with a record for the apex domain name. Set up a DNS active-active failover configuration that uses latency-based routing. Set "Evaluate Target Health" to "Yes" for the set of CNAME resource records.
3. Create an Amazon Route 53 private hosted zone with a record for the apex domain name. Set up a DNS active-active failover configuration that uses latency-based routing. Set "Evaluate Target Health" to "Yes" for the set of alias resource records.
4. Create an Amazon Route 53 private hosted zone with a record for the apex domain name. Set up a DNS active-active failover configuration that uses latency-based routing. Set "Evaluate Target Health" to "Yes" for the set of CNAME resource records.

**Correct Answer: A**

Explanation:

**Correct Option A)** Route 53 hosted zone is a container for records. Records contain information that is needed to route traffic for a specific domain. You need a public hosted zone to route traffic from the internet. A latency-based routing policy would serve user requests from the Region that provides the lowest latency. You need a set of alias records to map to the apex domain name.

**Incorrect Option B)** Route 53 hosted zone is a container for records. Records contain information that is needed to route traffic for a specific domain. You need a public hosted zone to route traffic from the internet. However, it is not possible to map a CNAME record to an apex domain name. An alias record is required

**Incorrect Option C)** Route 53 hosted zone is a container for records. Records contain information that is needed to route traffic for a specific domain. A private hosted zone would route traffic in a VPC. A public hosted zone is required for internet traffic.

**Incorrect Option D)** Route 53 hosted zone is a container for records. Records contain information that is needed to route traffic for a specific domain. A private hosted zone would route traffic in a VPC. A public hosted zone is required for internet traffic. Additionally, it is not possible to map a CNAME record to an apex domain name. An alias record is required.

For more information about public hosted zones, see [Working with Public Hosted Zones](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHZWorkingWith.html).

For more information about how to route traffic based on latency, see [Latency-Based Routing](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency).

For more information about alias records, see [Choosing between Alias and Non-alias Records](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html).

**Question 23/75**.

A company has released a new line of appliances The appliances use AWS loT Core sensors that write

data to an Amazon S3 bucket several times each day. The company configured the bucket with the S3 Standard storage class. The company accesses data from the most recent 6 months frequently to report usage patterns. The company must store the data indefinitely to meet compliance requirements. A solutions architect needs to reduce costs that are associated with storing the growing dataset in the S3 bucket.

Which storage solution will meet these requirements MOST cost-effectively?

1. Move the data to a new S3 bucket and set the storage class to S3 Standard-Infrequent Access (S3 Standard-IA). Implement S3 Intelligent-Tiering and set automatic data archiving to begin at 180 days.
2. Create a new S3 Intelligent-Tiering configuration for the existing S3 bucket. Set automatic data archiving to begin at 180 days.
3. Move the data to a new S3 bucket and set the storage class to S3 Standard-Infrequent Access (S3 Standard-IA). Create an S3 Lifecycle rule to transfer data older than 180 days into S3 Glacier Flexible Retrieval.
4. ***Create a new S3 Lifecycle rule for the existing S3 bucket. Configure the rule with bucket-wide object-tiering settings that will move data into S3 Glacier Deep Archive after 180 days.***

Correct Answer: **D**

Explanation:

**Correct Option D)** S3 Glacier Deep Archive is suitable when you do not need immediate access to data. S3 Glacier Deep Archive is less expensive than any immediate-access tier, including S3 Standard and S3 Standard-IA. S3 Lifecycle rules are the correct choice to move data for this company because usage patterns do not change.

**Incorrect Option A)** It would cost more to move the data into an S3 Standard-IA bucket than to leave the data in S3 Standard because the company accesses the data frequently during the first 6 months. S3 Standard-IA costs more for each retrieval than S3 Standard costs for each retrieval. After 6 months, when the data is no longer frequently accessed, the data should be moved to a less expensive storage class. You can automate the change of storage class with an S3 Lifecycle rule because the access patterns in this scenario are well known and do not change. S3 Intelligent-Tiering is well suited to situations with unknown usage patterns or when access patterns frequently change. S3 intelligent-Tiering would take time to recognize the change in access patterns and would keep the data in a more expensive storage class longer than necessary.

**Incorrect Option B)** After 6 months, when the data is no longer frequently accessed, the data should be moved to a less expensive storage class. You can automate the change of storage class with an S3 Lifecycle rule because the access patterns in this scenario are well known and do not change. S3 Intelligent-Tiering is well suited to situations with unknown usage patterns or when access patterns frequently change. S3 Intelligent-Tiering would take time to recognize the change in access patterns and would keep the data in a more expensive storage class longer than necessary.

**Incorrect Option C)** It would cost more to move the data into an S3 Standard-IA bucket than to leave the data in a bucket that uses S3 Standard because the company accesses the data frequently during the first 6 months. S3 Standard-IA costs more for each retrieval than S3 Standard costs for each retrieval.

**Question 24/75**

A company has an Amazon S3 bucket that contains millions of unencrypted objects To comply with a

recent security audit, a solutions architect needs to ensure that all objects are encrypted and needs to

compile a list of objects that contain sensitive data. Many applications access objects in the S3 bucket, and the development team has limited resources.

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

1. Run an Amazon Inspector report on the S3 bucket to identify sensitive data. Create a new S3 bucket with default encryption enabled. Transfer the unencrypted objects to the new S3 bucket. Update the applications to access the new S3 bucket.
2. Run an Amazon Macie report on the S3 bucket to identify sensitive data. Create a new S3 bucket with default encryption enabled. Transfer the unencrypted objects to the new S3 bucket. Update the applications to access the new S3 bucket.
3. Run an Amazon Inspector report against the S3 bucket to identify sensitive data. Modify the S3 bucket to enable default encryption. Use an Amazon S3 Inventory report and Amazon S3 Batch Operations to encrypt the existing unencrypted objects in the same S3 bucket.
4. ***Run an Amazon Macie report on the S3 bucket to identify sensitive data. Modify the S3 bucket to enable default encryption. Use an S3 Inventory report and S3 Batch Operations to encrypt the existing unencrypted objects in the same S3 bucket.***

**Correct Answer**: **D**

Explanation:

**Correct Option D)** Macie is a service that can identify sensitive data in Amazon S3. You can use an S3 Inventory report to create a list of objects that need to be encrypted. You can use that list as the manifest for S3 Batch Operations to encrypt existing data. No code changes are necessary for the applications that access the S3 objects.

**Incorrect Option A)** Amazon Inspector is an automated service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. However, Amazon Inspector does not examine S3 buckets for sensitive data.

**Incorrect Option B)** Macie is a service that can identify sensitive data in Amazon S3. However, additional development effort would be required to move the objects to a new S3 bucket and to update all the applications. You would have to inspect the code of each application for usage of the old S3 bucket names, update the code, and test the code.

**Incorrect Option C)** Amazon Inspector is an automated service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. However, Amazon Inspector does not examine S3 buckets for sensitive data.

Question 25/75

A company manages 50 AWS accounts through AWS Organizations. Different workloads in these

accounts require different security groups with appropriate rules. The company's security team wants to allow SSH access only from trusted IP CIDR blocks in all AWS accounts. The security team wants to ensure that this implementation remains compliant and cannot be modified by other accounts.

How can a solutions architect meet these requirements?

1. ***Create a firewall policy for AWS Network Firewall in AWS Firewall Manager. Add a stateless rule group to allow SSH access from trusted IP CIDR blocks with the lowest order priority. Restrict SSH access from 0.0.0.0/0. Select all accounts for this policy.***
2. Create a common security group policy in AWS Firewall Manager. Add a primary security group with an SSH rule that allows access from trusted IP CIDR blocks. Provide the option to identify resources that do not comply with the policy rules. Select all accounts for this policy.
3. Create a firewall policy for AWS Network Firewall in AWS Firewall Manager. Add a stateful rule group with a strict evaluation order to allow SSH access from trusted IP CIDR blocks with the highest order priority. Restrict SSH access from 0.0.0.0/0. Select all accounts for this policy.
4. Create a content audit security group policy in AWS Firewall Manager. Configure custom policy rules to deny SSH traffic from 0.0.0.0/0. Use an audit security group to allow SSH traffic from trusted IP CIDR blocks. Enable automatic remediation for any noncompliant resources. Select all accounts for this policy.

**Correct Answer: A**

Explanation:

**Correct Option A)** Firewall policy with a stateless group will allow or restrict traffic based on the rules within the group. In a stateless group, rules are processed starting from the lowest numbered priority setting. A rule that restricts SSH access from trusted sources will be processed and allowed first. The rest of the SSH traffic (0.0.0.0/0) will be restricted. These network firewalls and rule groups cannot be modified by the member accounts of an organization on AWS Organizations. This solution fulfils all the requirements.

**Incorrect Option B)** Firewall Manager does not restrict SSH access from any other sources. Additionally, Firewall Manager does not automatically remediate such broad SSH access. For these reasons, this solution does not meet the requirements.

**Incorrect Option C)** A stateful rule group with a strict evaluation order will evaluate the rules by order of priority, starting from the lowest number. In this scenario, a rule that restricts SSH access from 0.0.0.0/0 will be evaluated first and will restrict all traffic, including SSH access from the trusted sources. This solution does not meet the requirements.

**Incorrect Option D)** A content audit security group policy in Firewall Manager is used to audit security groups across multiple accounts and to recognize any noncompliant rules. Policy rules can either allow or deny rules defined in the audit security group, but not both. With this setting, other security groups across accounts are evaluated. In this scenario, the policy rule allows SSH traffic from trusted IP CIDR blocks and denies SSH traffic from 0.0.0.0/0. This denial is not possible. Additionally, other security groups across accounts must be within the scope of the audit security group. Any out-of-scope rules will make these security groups noncompliant. Automatic remediation will occur, and Firewall Manager will remove any additional rules. Such actions will disrupt multiple workloads across all accounts.

For more information about stateful rule groups with strict evaluation order, see [Strict Evaluation Order](https://docs.aws.amazon.com/network-firewall/latest/developerguide/suricata-rule-evaluation-order.html#suricata-strict-rule-evaluation-order)

For more information about stateless rule groups, see [Stateless Rule Groups in AWS Network Firewall](https://docs.aws.amazon.com/network-firewall/latest/developerguide/stateless-rule-groups-5-tuple.html)

**Question 26/75**

A company wants to provide desktop as a service (DaaS) to a number of employees using Amazon

WorkSpaces. WorkSpaces will need to access files and services hosted on premises with authorization based on the company's Active Directory Network connectivity will be provided through an existing AWS Direct Connect connection.

The solution has the following requirements

• Credentials from Active Directory should be used to access on-premises files and services.

• Credentials from Active Directory should not be stored outside the company

• End users should have single sign-on (SSO) to on-premises files and services once connected to WorkSpaces

Which strategy should the solutions architect use for end user authentication?

1. Create an AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) directory within the WorkSpaces VPC. Use the Active Directory Migration Tool (ADMT) with the Password Export Server to copy users from the on-premises Active Directory to AWS Managed Microsoft AD. Set up a one-way trust allowing users from AWS Managed Microsoft AD to access resources in the on-premises Active Directory. Use AWS Managed Microsoft AD as the directory for WorkSpaces.
2. Create a service account in the on-premises Active Directory with the required permissions. Create an AD Connector in AWS Directory Service to be deployed on premises using the service account to communicate with the on-premises Active Directory. Ensure the required TCP ports are open from the WorkSpaces VPC to the on-premises AD Connector. Use the AD Connector as the directory for WorkSpaces.
3. ***Create a service account in the on-premises Active Directory with the required permissions. Create an AD Connector in AWS Directory Service within the WorkSpaces VPC using the service account to communicate with the on-premises Active Directory. Use the AD Connector as the directory for WorkSpaces.***
4. Create an AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) directory in the AWS Directory Service within the WorkSpaces VPC. Set up a one-way trust allowing users from the on-premises Active Directory to access resources in the AWS Managed Microsoft AD. Use AWS Managed Microsoft AD as the directory for WorkSpaces. Create an identity provider with AWS Identity and Access Management (IAM) from an on-premises ADFS server. Allow users from this identity provider to assume a role with a policy allowing them to run WorkSpaces.

**Correct Answer: C**

Explanation:

**Correct Option C)** AD Connector is a directory gateway that you can use to redirect directory requests to your on-premises Active Directory without the need to cache any information in the cloud. This solution will authenticate the Active Directory credentials of the end users. The WorkSpaces will be members of the Active Directory that provide SSO to on-premises resources.

[For more information about AD Connector, see Active Directory Connector](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html)

**Incorrect Option A)** This solution copies the users to AWS Managed Microsoft AD. However, the company requires a solution that does not store credentials from Active Directory outside the company.

For more information [about AWS Managed Microsoft AD, see AWS Managed Microsoft AD](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html)

**Incorrect Option B)** You cannot deploy AD Connector on premises.

[For more information about the requirements for AD Connector, see AD Connector Prerequisites](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.html)

**Incorrect Option D)** To set up AWS IAM Identity Center (AWS Single Sign-On) with Amazon WorkSpaces Web, you would also need to set up AWS Organizations.

For more information about how to set up IAM Identity Center for WorkSpaces, see [Set Up IAM Identity Center as Your IdP](https://docs.aws.amazon.com/workspaces-web/latest/adminguide/sso-idp.html)

**Question 27/75**

A company stores customer data in an Amazon S3 bucket An analytics team from another AWS account

accesses the data securely through an S3 Object Lambda access point All access activity from the analytics team must be recorded for compliance reasons. Access activity for the S3 bucket is logged through S3 server access logs.

Auditors from the analytics team currently scan through all available S3 access logs. The auditors need

an easier way to collect all access activity that pertains to their team only.

Which solution will meet these requirements?

1. Use Amazon Athena to query the S3 server access logs automatically by using a schedule-based AWS Lambda function. Filter the analytics team’s access activity. Save the results in a specified S3 bucket.
2. Configure an AWS CloudTrail trail to log data events. Use the basic event selectors option to specify the resource ARN of the S3 Object Lambda access point. Store the trail logs in a specified S3 bucket through the trail configuration.
3. Configure an AWS CloudTrail trail to log data events. Use the advanced event selectors option to specify the resource ARN of the S3 Object Lambda access point. Store the trail logs in a specified S3 bucket through the trail configuration.
4. Use Amazon Athena to query the S3 server access logs by using the AWS CLI as needed. Filter the analytics team’s access activity. Save the results in a specified S3 bucket.

**Correct Answer : C**

Explanation:

**Correct Option C)** You can record API activity of S3 Object Lambda access points by using advanced event selector options. This solution meets the company's requirement that the process will not unnecessarily expose any additional activities to the analytics team. CloudTrail ensures that all activity is captured. For more information about how to log data events by using advanced event selectors, see [Logging Data Events for Trails](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html) . For more information about CloudTrail data events, see [What are CloudTrail Events](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-events)?

**Incorrect Option A)** S3 server access logs are best-effort delivery and are not meant for complete accounting of all requests. A better solution would be one that guarantees tracking accuracy.

**Incorrect Option B)** The basic event selectors option does not record S3 Object Lambda access point activity. This option does not meet the company's requirements.

**Incorrect Option D)** S3 server access logs are best-effort delivery and are not meant for complete accounting of all requests. A better solution would be one that guarantees tracking accuracy.

For more information about how to log data events by using basic event selectors, see [Logging Data Events for Trails](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html). For more information about delivery of S3 server access logs, see [Logging Requests Using Server Access Logging](https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerLogs.html)

**Question 28/75**

A company's chief financial officer (CFO) wants advanced notification if projections show that the costs for Amazon EC2 instances will exceed 75% of the company's monthly AWS budget. To reduce costs, the CFO wants specific EC2 instances to stop when the CFO receives the advanced notification. A solutions architect plans to use an AWS Budgets alert as part of the solution.

Which solution will meet the CFO's requirements with the LOWEST risk of future overspending?

A) Create an alert based on actual costs of 75% of the monthly budget, filtered on instance type. Add an AWS Budgets action to stop the specified EC2 instances.

B) Create an alert based on actual costs of 75% of the monthly budget, filtered on instance type. Send an alert to a systems operator to stop the specified EC2 instances.

C) ***Create an alert based on projected costs of 75% of the monthly budget, filtered on instance type. Add an AWS Budgets action to stop the specified EC2 instances.***

D) Create an alert based on projected costs of 75% of the monthly budget, filtered on instance type. Send an alert to a systems operator to stop the specified EC2 instances.

**Correct Answer: C**

Explanation:

**Correct Option C)** This AWS Budgets alert would activate when the projected expenditure reaches the threshold. An automatic AWS Budgets action is the best way to stop the EC2 instances. This automatic stop would prevent future overspending.

For more information about AWS Budgets, see [Managing Your Costs with AWS Budgets](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html)

**Incorrect Option A)** This AWS Budgets alert would activate when the actual expenditure reaches the threshold. The requirements are based on projected spending. An alert based on actual spending would be too late.

For more information about AWS Budgets, see Managing Your Costs with AWS Budgets

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html

Incorrect Option B) This AWS Budgets alert would activate when the actual expenditure reaches the threshold. The requirements are based on projected spending. An alert based on actual spending would be too late.

For more information about AWS Budgets, see Managing Your Costs with AWS Budgets

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html

Incorrect Option D). This AWS Budgets alert could partially meet the requirements because it would activate an alert based on projected expenditure. However, the manual step that requires the systems operator to stop the specified EC2 instances could result in overspending if the systems operator does not stop the EC2 instances quickly. An automatic AWS Budgets action is the best way to stop the EC2 instances. The automatic stop would prevent future overspending.

For more information about AWS Budgets, see Managing Your Costs with AWS

Budgets https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html

**Question 29/75**

A company uses AWS to host resources for developers to help the developers develop and test applications The developers have created their own resources on AWS,which has led to cost fluctuations and a lack of enforcement of company standards. The company has decided to provide two standard configurations one for development systems and one for test systems The company wants a solution that will give the developers the ability to create the resources they need. However, the company wants to limit developers to the approved configurations only.

Which solution will meet these requirements?

1. ***Create products in AWS Service Catalog for development and testing. Attach an IAM role that has appropriate permissions to the products. Create IAM policies to allow the developers to launch the products.***
2. Create AWS CloudFormation templates for each standard configuration. Store the templates in an Amazon S3 bucket. Create IAM policies to allow the developers to use the templates to create stacks.
3. Create Docker-based containers to use with Amazon Elastic Container Service (Amazon ECS) for each standard configuration. Create IAM policies to allow the developers to launch the containers.
4. Create identity-based IAM policies that allow the creation of only standard resources. Attach the policies to the developers. Allow the developers to create new resources.

Correct Answer: A

Explanation:

**Correct Option A)** AWS Service Catalog provides a self-service option for users to create resources. Attachment of an IAM role to the products will allow developers to create the resources without the need to maintain direct privileges for resource creation on AWS. For more information about AWS Service Catalog, see What Is [AWS Service Catalog](https://docs.aws.amazon.com/servicecatalog/latest/adminguide/introduction.html)

**Incorrect Option B)** CloudFormation helps model and set up AWS resources so that developers can spend less time on the management of those resources and spend more time on the applications that run on AWS. To create resources by using CloudFormation templates, the developers would need direct privileges. This solution would not limit the developers to the approved configurations.

**Incorrect Option C)** Amazon ECS is a highly scalable, fast container-management service that provides tools to run, stop, and manage containers on a cluster. Use of containers would give the developers the ability to deploy only application components instead of the ability to deploy standard resource configurations.

**Incorrect Option D)** IAM policies define permissions for an action regardless of the method that developers use to perform the operation. Identity-based IAM policies can restrict which resources the developers can create. However, developers would have the ability to deploy only partial resources instead of the full, approved resource configurations.

Available resources on AWS change constantly, and the company would need to regularly review and update IAM policies. For more information about IAM policies, see Policies and Permissions in [IAM](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

**Question 30/75**

A company's solutions architect is designing a disaster recovery (DR) solution for an application that runs on AWS. The application uses PostgreSQL 11.7 as its database. The company has an RPO of 30 seconds. The solutions architect must design a DR solution with the primary database in the us-east-1

Region and the failover database in the us-west-2 Region

What should the solutions architect do to meet these requirements with minimum application change?

1. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a read replica in us-west-2. Set the managed RPO for the RDS database to 30 seconds.
2. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a standby replica in an Availability Zone in us-west-2. Set the managed RPO for the RDS database to 30 seconds.
3. ***Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us-west-2. Set the managed RPO for the Aurora database to 30 seconds.***
4. Migrate the database to Amazon DynamoDB in us-east-1. Set up global tables with replica tables that are created in us-west-2.

**Correct Answer: C**

Explanation:

**Correct Option C)** Aurora global databases provide managed RPO. Users can set RPO as low as 20 seconds.

For more information about RPO parameters, see [Managing RPOs for Aurora PostgreSQL–Based Global Databases](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database-disaster-recovery.html#aurora-global-database-manage-recovery)

**Incorrect Option A)** Managed RPO is not a feature of Amazon RDS.

**Incorrect Option B)** Managed RPO is not a feature of Amazon RDS.

**Incorrect Option D)** DynamoDB is not a relational database. This solution would require significant changes to the application.

**Question 31/75**

A company plans to set up multiple AWS accounts by using AWS Organizations. A company-wide policy

requires teams to take a backup of Amazon Elastic Block Store (Amazon EBS) volumes each day. The

company's Cloud Center of Excellence (CCoE) team wants to design a backup solution that it can enforce consistently across all the accounts.

Which solution will meet these requirements MOST reliably?

1. Create an organizations backup policy to back up resources by using Amazon Data Lifecycle Manager (Amazon DLM). Validate and attach the backup policy to the root of the organization.
2. Create an AWS Service Catalog product that creates an Amazon Data Lifecycle Manager (Amazon DLM) snapshot policy. Enable all account administrators to launch the product within each account.
3. ***Create an Organizations backup policy to back up resources by using AWS Backup. Validate and attach the backup policy to the root of the organization.***
4. Create an AWS CloudFormation template to create a backup plan through AWS Backup. Use the template to deploy the backup plan to multiple accounts by using CloudFormation StackSets.

**Correct Answer: C**

Explanation:

**Correct Option C)** AWS Backup centralizes and automates data backups across AWS services, including Amazon EBS. AWS Backup can implement a backup plan with the appropriate backup rule to meet the company's backup policy. Additionally, Organizations backup policies conveniently create these backup plans across multiple accounts. It is not possible to delete or edit these backup plans individually within the account. This solution will enforce the company's backup policy reliably and consistently. For more information about [AWS Backup, see Creating a Backup Plan](https://docs.aws.amazon.com/aws-backup/latest/devguide/creating-a-backup-plan.html) For more information about Organizations backup policies, [see Creating, Updating, and Deleting Backup Policies](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_backup_create.html)

**Incorrect Option A)** Amazon DLM automates the creation, retention, and deletion of EBS snapshots. However, you cannot create an [Amazon DLM snapshot policy by using an organizations backup policy.](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html)

**Incorrect option B)** Amazon DLM automates the creation, retention, and deletion of EBS snapshots. However, you cannot ensure reliability by creating an Amazon DLM snapshot policy as an AWS Service Catalog product. An individual account administrator might not launch the product or might accidentally delete the product. For more information about Amazon DLM, see Amazon Data Lifecycle Manager

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>

<https://docs.aws.amazon.com/servicecatalog/latest/adminguide/what-is_concepts.html>

**Incorrect Option D)** AWS Backup centralizes and automates data backups across AWS services, including Amazon EBS. CloudFormation StackSets can reliably launch the solution as stack instances across the accounts. However, it is possible to delete these stack instances internally within the account. This solution will not meet the requirement to consistently enforce the company's backup policy.

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

**Question 32/75**

A company that designs multiplayer online games wants to expand its user base outside of Europe The company transfers a significant amount of UDP traffic to keep all the live and interactive sessions of the games. The company has plans for rapid expansion and wants to build its architecture to provide an optimized online experience to its users.

Which architecture will meet these requirements with the LOWEST latency for users?

1. Set up a Multi-AZ environment in a single AWS Region. Use Amazon CloudFront to cache user sessions.
2. ***Set up environments in multiple AWS Regions. Create an accelerator in AWS Global Accelerator, and add endpoints from different Regions to it.***
3. Set up environments in multiple AWS Regions. Use Amazon Route 53, and select latency-based routing.
4. Set up a Multi-AZ environment in a single AWS Region. Use AWS Lambda@Edge to update sessions closer to the users.

**Correct Answer: B**

Explanation:

**Correct Option B)** You can reduce latency by setting up the access perimeter in multiple Regions. Global Accelerator is well suited for UDP (and gaming) services, among other use cases. For more information about Global Accelerator, see [AWS Global Accelerator](https://aws.amazon.com/global-accelerator/faqs/) FAQs

**Incorrect Option A)** CloudFront delivers HTML, CSS, JS, and image files, not UDP traffic.

**Incorrect Option C)** Latency-based routing will route over the public internet instead of AWS's global network. Latency-based routing will not provide the same level of performance as Global Accelerator.

**Incorrect Option D)** In this solution, all customers will interact with a single Region. This solution can add to latency or performance issues.

**Question 33/75**

A company has deployed a Python application on an Amazon Elastic Container Service (Amazon ECS)

cluster. The application includes a stateless frontend, an Amazon RDS Multi-AZ database, and a two node Amazon ElastiCache for Memcached cluster to offload the database read requests for frequently"

accessed data. The number of read requests to the database is increasing A solutions architect adds two more nodes to

the ElastiCache cluster. However, performance does not appear to improve after the addition of the nodes, and the new Memcached instances seem idle.

How can the solutions architect resolve this issue with the LEAST code changes?

1. Replace the ElastiCache for Memcached cluster with an ElastiCache for Redis cluster that has cluster mode disabled. Add four read replicas to the Redis cluster.
2. ***Use the AWS CLI to discover the newly added node endpoints. Configure the application for reads and writes to all the endpoints.***
3. Use the AWS CLI to discover the newly added node endpoints. Configure the RDS database for reads and writes to all the endpoints.
4. Replace the ElastiCache for Memcached cluster with an ElastiCache for Redis cluster that has cluster mode enabled. Add four shards to the Redis cluster.

**Correct Answer: B**

Explanation:

**Correct Option B)** ElastiCache for Memcached can support Auto Discovery for certain clients. Auto Discovery is not in use in this scenario because the newly added nodes are not being discovered. You need to add the new endpoints to the application code. Some code change would be necessary, but this process would not require a complete rewrite of the code that interacts with Memcached.

For more information about how to discover connection endpoints for a newly added Memcached node, [see Finding Connection Endpoints](https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/Endpoints.html) For more information about how to connect to cache nodes manually, see Connecting to Cache Nodes Manually <https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/AutoDiscovery.Manual.html>

**Question 34/75**

During migration to the AWS Cloud, a company modernized an application to use a microservices

architecture. The company will deploy the application across multiple AWS Regions to meet latency and disaster recovery requirements. During both full and partial failures, the traffic must be automatically rerouted to the healthy deployments in other Regions The company will route traffic to an Amazon API Gateway API by using a custom domain name that the company manages with Amazon Route 53. The company will monitor the infrastructure, including API Gateway endpoints, by using multiple Amazon CloudWatch metrics.

Which solution will route user requests to fully functional microservices?

1. Configure Route 53 Application Recovery Controller readiness checks for each resource type of the application. Create AWS Lambda functions that will be invoked based on readiness checks. Use the Lambda functions to update the Route 53 record sets to automate routing appropriately.
2. ***Configure Route 53 Application Recovery Controller routing controls and health checks for each deployment. Create AWS Lambda functions that will be invoked based on each resource’s metric alarms. Use the Lambda functions to toggle routing controls to automate routing appropriately.***
3. Select the Route 53 Evaluate Target Health option for each record set to automate routing appropriately.
4. Configure Route 53 health checks for each Regional API Gateway endpoint to automate routing appropriately.

**Correct Answer: B**

Explanation:

**Correct Option B)** Route 53 Application Recovery Controller routing controls provide simple on/off switches that give you the ability to direct traffic from one replica to another. These routing controls are based on Route 53 health checks that you configure. The Route 53 health checks become healthy or unhealthy by toggling routing controls. Based on multiple metrics from various application components, you can automate the toggling of these routing controls with CloudWatch alarms and Lambda functions.

For more information about how to create Route 53 Application Recovery Controller routing controls, see [Create Routing Control Structures in ARC](https://docs.aws.amazon.com/r53recovery/latest/dg/routing-control.create.html)

**Incorrect Option A)** A Route 53 Application Recovery Controller readiness check continuously monitors AWS resource configurations, capacity, and network routing policies. These checks give you the ability to monitor for changes that would affect your ability to enact a recovery operation. These checks ensure that you have scaled and configured the recovery environment appropriately to take over when necessary. However, this is an assessment feature which, by itself, will not route traffic to the healthy Regions. For more information about Route 53 Application Recovery Controller readiness checks, [see Amazon Route 53 Application Recovery Controller Components](https://docs.aws.amazon.com/r53recovery/latest/dg/introduction-components.html)

**Incorrect Option C)** You would not detect any partial failures within the application by monitoring API Gateway endpoints with the Route 53 Evaluate Target Health option. This option will not meet the requirements.

**Incorrect Option D)** You would not detect any partial failures within the application by monitoring API Gateway endpoints with Route 53 health checks. This option will not meet the requirements.

**Question 35/75**

A company wants to migrate its on-premises order entry system to a highly available solution on AWS.

The existing order entry system is a PHP web application that accepts orders and publishes them to

Apache ActiveMQ by using its own proprietary protocol. A processing application polls the queued orders and stores them in JSON format in a document database.

Which migration strategies would require the LEAST migration effort? (Select THREE)

1. Rehost the web application to an Amazon S3 bucket. Rehost the processing application on Amazon EC2 instances that use Amazon EC2 Auto Scaling.
2. ***Replatform the message queue to Amazon MQ. Configure both applications to use this queue.***
3. ***Refactor the database server into Amazon DynamoDB tables. Modify the processing application to write to DynamoDB.***
4. Replatform the message queue to Amazon Simple Queue Service (Amazon SQS). Configure both applications to use this queue.
5. Refactor the database server into a Multi-AZ Amazon RDS DB instance. Modify the processing application to write to Amazon RDS.
6. ***Rehost both applications to Amazon EC2 instances that use Amazon EC2 Auto Scaling. Use an Elastic Load Balancer in front of the web application.***

**Correct Answer: B, C, F**

Explanation:

**Correct Option B)** Amazon MQ is a managed message broker service for ActiveMQ. This solution requires minimal code changes because the existing application uses ActiveMQ.

**Correct Option C)** DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. You can use DynamoDB for document storage. A solution that refactors the application to use DynamoDB would require less work than a solution that refactors the application to use a relational database.

**Correct Option F)** A solution that rehosts the applications on EC2 instances that use EC2 Auto Scaling would be scalable and highly available. An Elastic Load Balancer automatically distributes incoming traffic across multiple targets in one or more Availability Zones.

**Incorrect Option D)** Amazon SQS offers a secure, durable, and available hosted queue that integrates and decouples distributed software systems and components. However, Amazon SQS supports only the HTTP and HTTPS protocols, and the requirement is to use the ActiveMQ protocol.

**Incorrect Option E)** Amazon RDS helps to set up, operate, and scale a relational database in the cloud. Because the application uses JSON documents, a solution that refactors the application to use DynamoDB would require less work than a solution that refactors the application to use a relational database.

**Question 36/75**

A company is migrating its marketing website and content management system from an on-premises data

center to AWS. The company wants the AWS application to be deployed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database. The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers. After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.

How can the application and environment be deployed and automated in AWS with the LEAST operational

overhead, while allowing for future changes?

1. Update the runbook to describe how to create the VPC, the EC2 instances, and the RDS instance for the application by using the AWS Console. Make sure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.
2. Write a Python script that uses the AWS API to create the VPC, the EC2 instances, and the RDS instance for the application. Write shell scripts that implement the rest of the steps in the runbook. Have the Python script copy and run the shell scripts on the newly created instances to complete the installation.
3. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Ensure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.
4. ***Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Include EC2 user data in the AWS CloudFormation template to install and configure the software.***

**Correct Answer: D**

Explanation:

**Correct Option D)** CloudFormation and Amazon EC2 user data scripts are the best option. You can use stack updates to deploy multiple versions of the template to change the environment in the future.

**Incorrect Option A)** This solution does not include significant automation. It would be difficult to change the environment to use other services if necessary.

**Incorrect Option B)** This solution includes some automation, but a Python script is not the best choice. Significant effort would be necessary to build the script. A Python script will require more operational overhead to handle future updates to the environment than a CloudFormation template will.

**Incorrect Option C)** The CloudFormation template will help you build an automated solution. However, the installation and configuration of the software is still manual.

For more information about CloudFormation, see [AWS CloudFormation Stack Updates](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks.html)

**Question 37/75**

A company has two AWS accounts:AccountA and Accounts. An audit requirement exists to allow an IAM

user named Auditor in Accounts to have read-only access to the Amazon EC2 resources in AccountA.A security administrator in AccountA has created an IAM role named EC2Audit with read-only access to EC2 resources.A security administrator in Accounts has created the IAM user named Auditor with an

inline IAM policy that allows a call to sis AssumeRol!e. The callspecifies the resource as

"arn:aws:iam AccountA role/EC2Audit". No other user in AccountB can have the ability to assume the role of "EC2Audit" , when Auditor attempts to assume the EC2Audit role through the AWS Management Console, Auditor is not able to sign in to AccountA.

Which action will give Auditor in Accounts the ability to assume the EC2Audit role in AccountA?

1. The security administrator in AccountB must change the inline IAM policy to be a managed IAM policy and attach the policy to Auditor.
2. The security administrator in AccountB must create an IAM role that includes read-only access to Amazon EC2 for the resource "arn.aws.ec2::AccountA/\*".
3. The security administrator in AccountA must add a trust policy to the EC2Audit role with the resource "arn:aws:iam::AccountB:user/\*"
4. ***The security administrator in AccountA must add a trust policy to the EC2Audit role with the resource "arn:aws:iam::AccountB:user/Auditor"***

**Correct Answer: D**

Explanation:

**Correct Option D)** This trust policy will allow only Auditor in AccountB to assume the EC2Audit role.

For more information about cross-account access, see Providing Access to an IAM User in Another AWS Account That You Own <https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html>

**Incorrect Option A)** An appropriate trust policy is needed to ensure that Auditor in AccountB can access the EC2Audit role in AccountA. If the inline IAM policy is changed to a managed IAM policy, Auditor will not be able to assume the role in AccountA.

**Incorrect Option B)** The addition of a role in AccountB would not have any effect on resources in AccountA. An appropriate trust policy is needed to ensure that Auditor in AccountB can assume the role in AccountA.

For more information about cross-account access, see Providing Access to an IAM User in Another AWS Account That You Own <https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html>

**Incorrect Option C)** This trust policy would allow all users in AccountB to assume the EC2Audit role in AccountA. This policy setting is incorrect because the requirement is that only Auditor should be able to assume the role in AccountA.

**Question 38/75**

A company deploys a new internal application on two Amazon EC2 instances behind an Application Load

Balancer (ALB) The ALB and the EC2 instances operate across two Availability Zones. The company's employees depend on the application to perform their work.

When workloads are high,employees report slow response times and reliability issues with the

application Some incoming requests can generate significant compute activity on the EC2 instances. The workload can increase by 2 to 10 times the typical load in a matter of minutes.A solutions architect needs to change the configuration so that the application willscale in response to multiple workload changes in the least amount of time possible

How should the solutions architect configure Amazon EC2 Auto Scaling to meet these requirements?

1. ***Configure a step scaling policy that scales EC2 instances based on the CPUUtilization metric.***
2. Configure a simple scaling policy that scales EC2 instances based on the CPUUtilization metric.
3. Configure a step scaling policy that scales EC2 instances based on the RequestCountPerTarget metric from the ALB.
4. Configure a simple scaling policy that scales EC2 instances based on the RequestCountPerTarget metric from the ALB.

**Correct Answer: A**

Explanation:

**Correct Option A)** EC2 Auto Scaling helps to ensure that the correct number of instances are available to handle the load for an application. An Auto Scaling group with a step scaling policy would quickly respond to multiple workload changes, even while another scale-out activity is in progress. CPU utilization is the correct policy basis because requests can generate different amounts of activity on the instances.

For more information about Auto Scaling groups, see [What Is Amazon EC2 Auto Scaling?](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html)

**Incorrect Option B)** EC2 Auto Scaling helps to ensure that the correct number of instances are available to handle the load for an application. CPU utilization is the correct policy basis because requests can generate different amounts of activity on the instances. However, an Auto Scaling group with a simple scaling policy must wait for scaling activity to finish running, followed by a cooldown period, before the Auto Scaling group can respond to additional workload changes. The requirement is that the solution must respond to multiple workload changes in the least amount of time possible. A step scaling policy would respond faster to workload changes.

**Incorrect Option C)** EC2 Auto Scaling helps to ensure that the correct number of instances are available to handle the load for an application. An Auto Scaling group with a step scaling policy would quickly respond to multiple workload changes, even while another scale-out activity is in progress. However, different requests can generate different levels of activity on the instances, and a few requests could generate a lot of activity. A policy that is based on the RequestCountPerTarget metric would not be as effective as a policy that is based on CPU utilization.

**Incorrect Option D)** EC2 Auto Scaling helps to ensure that the correct number of instances are available to handle the load for an application. However, an Auto Scaling group with a simple scaling policy must wait for scaling activity to finish running, followed by a cooldown period, before the Auto Scaling group can respond to additional alarms. The requirement is that the solution must respond to multiple workload changes in the least amount of time possible. A step scaling policy would respond faster to workload changes. Additionally, different requests can generate different levels of activity on the instances, so a few requests could generate a lot of activity. A policy that is based on the **RequestCountPerTarget** metric would not be as effective as a policy that is based on CPU utilization.

For more information about step and simple scaling policies, see Step and [Simple Scaling Policies for Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html)

**Question 39/75**

A company runs a three-tier architecture on AWS. The web tier and application tier run in Amazon EC2 Auto Scaling groups with a database as the backend. Scaling is based on CPU utilization of the application tier. The company creates an Amazon Simple Queue Service (Amazon SQS) standard queue to decouple the web tier and the application tier. However, tests reveal that duplicate transactions occur and that the EC2 instances are not scaling. The laclk of scaling sometimes delays application processing. A solutions architect needs to eliminate the duplicate transactions and correct the scaling delay.

Which solution will meet these requirements in the MOST scalable way?

1. ***Create an SQS FIFO queue. Configure content-based deduplication. Update the application to use the new queue. Create an Amazon CloudWatch custom metric to calculate the backlog per instance that is acceptable to the company. Use a target tracking scaling policy based on the custom metric.***
2. ***Create an SQS FIFO queue. Configure content-based deduplication. Update the application to use the new*** queue. Change the application tier scaling to use the *ApproximateNumberOfMessagesVisible* metric.
3. Change the existing SQS standard queue to an SQS FIFO queue. Configure content-based deduplication for the queue. Change the application tier scaling to use the *ApproximateNumberOfMessagesVisible* metric.
4. Change the existing SQS standard queue to an SQS FIFO queue. Configure content-based deduplication for the queue. Create an Amazon CloudWatch custom metric to calculate the backlog per instance that is acceptable to the company. Use a target tracking scaling policy based on the custom metric.

**Correct Answer: A**

Explanation:

**Correct Option A)** FIFO queues can enhance message transmission between applications when the order of operations and events is critical or when duplicates are not acceptable. A custom metric to scale based on an acceptable backlog per instance would base the scaling on the system load in the SQS queue. The custom metric is calculated based on the approximate number of messages, processing latency, and the number of running EC2 instances. This solution provides more accurate scaling.

For more information about scaling in response to activity in SQS queues, see Scaling Based on [Amazon SQS](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html) For more information about FIFO queues, see [Amazon SQS FIFO (First-In-First-Out) Queues](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html) For more information about [high throughput for FIFO queues, see High Throughput for FIFO Queues](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/high-throughput-fifo.html)

**Incorrect Option B)** FIFO queues can enhance message transmission between applications when the order of operations and events is critical or when duplicates are not acceptable. However, the *ApproximateNumberOfMessagesVisible* metric will not change in proportion to the size of the Auto Scaling group that processes messages. A better solution is to use a custom metric based on an acceptable backlog per instance. A custom metric would scale better as the Auto Scaling group grows.

**Incorrect Option C)** FIFO queues can enhance message transmission between applications when the order of operations and events is critical or when duplicates are not acceptable. However, you cannot change an SQS standard queue to a FIFO queue.

**Incorrect Option D)** FIFO queues can enhance message transmission between applications when the order of operations and events is critical or when duplicates are not acceptable. However, you cannot change an SQS standard queue to a FIFO queue.

**Question 40/75**

A company has created an Amazon CloudFront distribution with two Amazon S3 buckets as origins The

company discovers that objects in both S3 buckets are publicly accessible. The desired state for the first S3 bucket is to allow access through CloudFront and otherAWS resources with appropriate permissions. Objects in the second S3 bucket should be accessible only through CloudFront for all users except for the S3 bucket owner.

How should a solutions architect configure access to the buckets to meet these requirements?

1. Create an IAM policy and an IAM role that allow access to the first S3 bucket. Assign the role to the CloudFront distribution and the other resources that need access to the first S3 bucket. Create an origin access identity (OAI) for the CloudFront distribution. Create an S3 bucket policy for the the second S3 bucket that allows access only with the OAI as the principal.
2. Create a separate S3 bucket policy for each S3 bucket. Configure the policy for the first S3 bucket to allow read access to appropriate AWS resources and the CloudFront distribution as principals. Configure the policy for the second S3 bucket to allow only read access for the CloudFront distribution as the principal.
3. Create a separate origin access identity (OAI) for the CloudFront distribution for each S3 bucket. Configure the first OAI to include access for the other AWS resources. Configure the second OAI to include only CloudFront. Update the S3 bucket policies to restrict access to the correct OAIs.
4. ***Create a separate origin access identity (OAI) for the CloudFront distribution for each S3 bucket. Create an S3 bucket policy for the first S3 bucket that allows access to the appropriate AWS resources and the OAI as principals. Create an S3 bucket policy for the second S3 bucket that allows access to the appropriate OAI as the principal.***

**Correct Answer: D**

Explanation:

**Correct Option D)** An OAI is a special CloudFront user that is associated with S3 origins to secure all or some S3 content. You can use an S3 bucket policy to restrict access to the objects. You can list an OAI as a principal in a resource policy. For more information about how to use an OAI to restrict access to S3 content, see Restricting Access to [Amazon S3 Content by Using an Origin Access Identity (OAI)](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html) For more information about resource-based policies, see [Identity-Based Policies and Resource-Based Policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_identity-vs-resource.html)

**Incorrect Option A)** You can assign an IAM role to certain AWS resources. However, you cannot assign an IAM role to a CloudFront distribution.

**Incorrect Option B)** You can use an S3 bucket policy to restrict access to the objects. However, you cannot list a CloudFront distribution as a principal. An OAI must represent the CloudFront distribution for both bucket policies.

**Incorrect Option C)** An OAI is a special CloudFront user that is associated with S3 origins to secure all or some of the S3 content. However, an OAI cannot include principal information from AWS resources other than CloudFront.

For more information about how to use an OAI to restrict access to S3 content, see Restricting Access to Amazon S3 Content by Using an [Origin Access Identity (OAI)](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html) For more information about resource-based policies, see [Identity-Based Policies and Resource-Based Policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_identity-vs-resource.html)

**Question 41/75**

A company has several legacy on-premises C++ applications. The applications are highly integrated and dependent on one another. The servers and operating systems that support the applications are highly customized and fine-tuned. Currently, the company cannot modernize the applications The company wants to move the applications to AWS. The company requires a highly available and scalable solution.

Which solution will meet these requirements with the LEAST migration effort?

1. Containerize the applications. Create Docker-based images and deploy the images by using Amazon Elastic Container Service (Amazon ECS) by using the Fargate launch type.
2. Containerize the applications. Create Docker-based images and deploy the images to Amazon Elastic Container Service (Amazon ECS) by using the EC2 launch type.
3. Package the C++ code and create application source bundles. Deploy the bundles to multiple AWS Elastic Beanstalk environments.
4. ***Use AWS Application Migration Service (CloudEndure Migration) to rehost the applications to run on instances in an Amazon EC2 Auto Scaling group.***

**Correct Answer: D**

Explanation:

**Correct Option D)** A solution that rehosts the existing applications to instances in an Auto Scaling group would provide the high availability and scalability that the company requires. Application Migration Service (CloudEndure Migration) is a highly automated lift-and-shift solution to migrate servers, databases, and applications to the AWS Cloud. This solution would require the least migration effort.

**Incorrect Option A)** Fargate runs containers without the need to manage servers or clusters of Amazon EC2 instances. However, the existing servers have been highly customized to support the applications. Containerization of the applications and their operating systems might require significant migration effort. A better solution would run the applications directly on EC2 instances that the company can manage.

**Incorrect Option B)** Amazon ECS is a scalable and fast container-management service. However, the existing servers have been highly customized to support the applications. Containerization of the applications and their operating systems might require significant migration effort. A better solution would run the applications directly on EC2 instances that the company can manage.

**Incorrect Option C)** You can use Elastic Beanstalk to quickly deploy and manage applications in the AWS Cloud without the need to learn about the infrastructure that runs the applications. However, the applications are written in C++, which would require the creation of a custom runtime. Additionally, it would take considerable effort to modify the servers that are deployed by Elastic Beanstalk to match the high amount of operating system customization that is needed to support the applications.

**Question 42/75**

A company uses AWS Organizations with all features turned on to manage multiple AWS accounts. The tag names and values that are applied to the resources across accounts are inconsistent. The company wants to generate cost allocation reports based on a standardized set of tag names and values. The company needs to identify and correct noncompliant tags. After these corrections, the company will enforce the use of the standardized tags. How can a solutions architect correct the noncompliant tags and enforce the use of only compliant tags in the future?

1. Use AWS Config to create managed rules in each account. Use the required-tags rule to apply specific tags to the AWS resources. Activate AWS Config for the organization. Create a custom AWS Systems Manager Automation runbook to automatically apply the appropriate tag to the AWS resource.
2. Create tag policies in Organizations for the required tags. Select the option to prevent noncompliant operations for this tag to enforce use of the tags. Attach the tag policies to the organization entities as required. Use AWS Resource Groups to find noncompliant tags. Correct the tags by using the AWS service that created the resources.
3. ***Create tag policies in Organizations for the required tags. Attach the tag policies to the organization entities as required. Use AWS Resource Groups to find noncompliant tags. Correct the tags by using the AWS service that created the resources. Use SCPs to enforce the use of the tags across the organization.***
4. Create an Amazon EventBridge rule to monitor the addition of noncompliant tags to an AWS resource. Configure the rule to send a message to Amazon Simple Queue Service (Amazon SQS). Configure the SQS queue to invoke an AWS Lambda function to apply an appropriate tag to the AWS resource.

**Correct Answer: C**

Explanation:

**Correct Option C)** Tag policies help standardize tags across resources in an organization's accounts. You can use Resource Groups to detect noncompliant resources and generate a report so that you can make corrections. You can use SCPs to enforce the use of tags within the organization.

**Incorrect Option A)** AWS Config managed rules can detect and automatically correct noncompliant resources in AWS. However, you cannot use AWS Config to enforce the use of compliant tags in the future.

**Incorrect Option B)** Tag policies help standardize tags across resources in an organization's accounts. You can use Resource Groups to detect noncompliant resources and generate a report so that you can make corrections. However, the option to prevent noncompliant operations for this tag would not have any effect on resources that are created with no tags. An SCP is required to enforce the addition of the tags.

**Incorrect Option D)** EventBridge event-based rules can detect and automatically correct noncompliant resources in AWS. However, EventBridge cannot enforce the use of compliant tags in the future.For more information about AWS Config managed rules, see [AWS Config Managed Rules](https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html)

For more information about the [AWS Config required-tags rule](https://docs.aws.amazon.com/config/latest/developerguide/required-tags.html), see Required-Tags

For more information about [tag policies in Organizations, see Tag Policies](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html)

For more information about [tag policy enforcement, see Understanding Enforcement](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies-enforcement.html)

For more information about how to use Resource Groups to manage compliance[, see What Are Resource Groups](https://docs.aws.amazon.com/ARG/latest/userguide/resource-groups.html)?

**Question 43/75**

A company must migrate some on-premises Linux applications to the AWS Cloud. The applications are independent, complex and backed by MySQL databases. The company wants to eliminate the Linux administration work that is necessary to support these applications Time constraints require a solution with minimal application redesign and coding.

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

1. Containerize the applications. Manage the applications as tasks in Amazon Elastic Container Service (Amazon ECS) with the EC2 launch type. Migrate the databases to run on Amazon RDS for MySQL.
2. Implement the applications by using AWS Lambda. Use AWS Step Functions to coordinate the logical flow of the functions. Migrate the databases to run on Amazon RDS for MySQL.
3. ***Containerize the applications. Manage the applications as tasks in Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Migrate the databases to run on Amazon RDS for MySQL.***
4. Implement the applications by using AWS Lambda. Use AWS Step Functions to coordinate the logical flow of the functions. Migrate the databases to run on Amazon DynamoDB.

**Correct Answer: C**

Explanation:

**Correct Option C)** Containerization of the applications should be straightforward because the applications are independent. You can use Amazon ECS to run, stop, and manage containers on a cluster. The Fargate launch type removes the need to manage the underlying hosts and eliminates the Linux administration work. This solution also eliminates the need to manage the operating system at the backend by migrating the databases to Amazon RDS.

**Incorrect Option A)** ECS clusters that use the EC2 launch type require ongoing operating system management. This solution fails to eliminate the Linux administration that is necessary to support these applications. A better solution would be serverless.

**Incorrect Option B)** A solution that refactors each complex application by using Lambda and Step Functions would require a high level of operational effort. Containerization of the applications should be straightforward because the applications are independent. A solution that containerizes the applications would require less operational effort.

**Incorrect Option D)** A solution that refactors each complex application by using Lambda and Step Functions would require a high level of operational effort. Containerization of the applications should be straightforward because the applications are independent. A solution that containerizes the applications would require less operational effort. Migration of the relational MySQL databases to DynamoDB would also require significant effort.

**Question 44/75**

A company plans to deploy a web application that will serve a global audience. The company will deploy the application by using Amazon EC2 instances across two AWS Regions The company will create an Amazon Aurora global database, with a primary Aurora DB cluster in the first Region and a secondary Aurora DB cluster in the second Region The company needs to minimize latency and ensure read-after­ write consistency for the application's database operations The company also wants to regularly test its disaster recovery (DR) procedures to minimize data loss and maximize recovery speed across the two Regions.

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

1. ***Use the secondary Aurora DB cluster endpoint to perform read and write operations. Configure write forwarding to forward writer operations to the primary Aurora DB cluster endpoint. Test the DR procedure by using managed planned failover.***
2. Use the secondary Aurora DB cluster endpoint to perform read operations. Use the primary Aurora DB cluster endpoint to perform write operations. Test the DR procedure by using managed planned failover.
3. Use the secondary Aurora DB cluster endpoint to perform read operations. Use the primary Aurora DB cluster endpoint to perform write operations. Test the DR procedure by using manual unplanned failover.
4. Use the secondary Aurora DB cluster endpoint to perform read and write operations. Configure write forwarding to forward writer operations to the primary Aurora DB cluster endpoint. Test the DR procedure by using manual unplanned failover.

**Correct Answer: A**

Explanation:

**Correct Option A)** An Aurora global database replicates data with minimal replication lag to a secondary Aurora DB cluster in another Region. This process optimizes read operations for the company's global audience. Write forwarding will allow the secondary DB cluster to accept write operations and will forward write operations to the primary DB cluster. Aurora handles networking across Regions. Aurora also provides multiple consistency modes for the strongest read-after-write consistency, including global consistency. Finally, managed planned failover automatically handles demotion, promotion, and all synchronization across the clusters with no data loss and faster recovery.

**Incorrect Option B)** An Aurora global database replicates data with minimal replication lag to a secondary Aurora DB cluster in another Region. This process optimizes read operations for the company's global audience. However, these read operations could provide stale information. This process will not achieve the required read-after-write consistency.

**Incorrect Option C)** An Aurora global database replicates data with minimal replication lag to a secondary Aurora DB cluster in another Region. This process optimizes read operations for the company's global audience. However, these read operations could provide stale information. This process will not achieve the required read-after-write consistency.

**Incorrect Option D)** A manual unplanned failover process requires the manual performance of a series of tasks. You must detach and promote a secondary DB cluster. These steps are not suitable for the company's plan to test on a regular and frequent basis. A better solution would use managed planned failover, which would eliminate the manual steps and require less operational overhead.

For more information about Aurora global databases, see [Using Amazon Aurora Global Databases](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html)

**Question 45/75**

A company is hosting an ecommerce application on two Amazon EC2 instances behind an application. Load Balancer (ALB) across two Availability Zones. The application is performing well during normal sales activity. However, customers experience slow response times during unexpected peak sales activity. Recently, one of the instances was accidentally stopped, resulting in a significant performance decrease. A solutions architect investigates the slow response t1imes but finds no correlation between the peaks and changes in Amazon CloudWatch metrics for the EC2 instances. The solutions architect is planning to use Amazon EC2 Auto Scaling to help resolve the issues.

How should the solutions architect configure the Auto Scaling group to resolve these issues?

1. Create a predictive scaling policy for the Auto Scaling group to scale based on forecast. Configure the scaling metric to be the request count per target on the ALB target group.
2. Create a dynamic scaling policy for the Auto Scaling group. Configure a target tracking policy to increase the number of EC2 instances based on the average CPU utilization of the Auto Scaling group.
3. Create a scheduled scaling policy for the Auto Scaling group. Configure the scheduled actions to increase the number of EC2 instances during the peak sales periods.
4. ***Create a dynamic scaling policy for the Auto Scaling group. Configure the scaling metric to be the request count per target on the ALB target group.***

**Correct Answer: D**

Explanation:

**Correct Option D)** Dynamic scaling scales the capacity of an Auto Scaling group in response to changes in demand. The only performance differentiator in this scenario is the number of requests sent to each EC2 instance. A target tracking policy based on the number of requests from the ALB will appropriately scale the group.

**Incorrect Option A)** Predictive scaling changes the number of EC2 instances in an Auto Scaling group in advance of daily and weekly patterns in traffic flows. Predictive scaling is not a good option because the peak sales activities happen at unexpected times.

**Incorrect Option B)** Dynamic scaling scales the capacity of an Auto Scaling group in response to changes in demand. Target tracking based on this metric would not scale the group at the appropriate times because the peaks in sales do not correlate with any CloudWatch metrics for EC2 instances, including CPU utilization.

**Incorrect Option C)** Scheduled scaling uses scheduled actions that are performed automatically as a function of date and time. A scheduled time would not address the unexpected peak activity.

**Question 46/75**

A company runs a group of Amazon EC2 instances in private subnets. The EC2 instances store a small amount of infrequently updated data in an Amazon S3 bucket that is in the same AWS Region. A solutions architect creates a gateway VPC endpoint to allow the EC2 instances to access the S3 bucket. The company has a second group of EC2 instances in private subnets in a second Region. The second group of EC2 instances use the S3 bucket's public endpoint for read-only activity. The company is experiencing higher data-transfer costs because of increased repetitive read activity by the second group of EC2 instances. The company needs a lower-cost solution that will give the second group of EC2 instances read access to the data.

Which solution will meet these requirements MOST cost-effectively?

1. Create an interface VPC endpoint for the S3 bucket in the VPC in the first Region by using AWS PrivateLink. Peer the VPCs and establish routing between the VPCs. Configure access to the S3 bucket from the EC2 instances in the second Region.
2. Create an Amazon Elastic File System (Amazon EFS) file system in each Region. Transfer all the data from the S3 bucket to one of the EFS file systems. Use AWS DataSync to synchronize the EFS file systems. Create mount points in each subnet for EC2 access.
3. ***Create a second S3 bucket in the second Region. Create a gateway VPC endpoint for the second S3 bucket. Allow the EC2 instances in the second Region to communicate with the second S3 bucket. Configure S3 Cross-Region Replication (CRR) between the two S3 buckets.***
4. Create a second S3 bucket in the second Region. Create a gateway VPC endpoint for the second S3 bucket. Allow the EC2 instances in the second Region to communicate with the second S3 bucket. Use an AWS Lambda function to copy objects between the two S3 buckets.

**Correct Answer: C**

Explanation:

**Correct Option C)** Gateway VPC endpoints allow resources in AWS to access an S3 bucket without crossing the internet. S3 CRR replicates objects between the two S3 buckets in different Regions. This solution would meet the requirements because the cost of S3 storage is low for a small amount of data. There is no cost for gateway VPC endpoints, and there would be charges only for data transfer between Regions when infrequent changes are made. When the new instances in the second Region repetitively read the data in the S3 bucket, there would be no data-transfer charges.

**Incorrect Option A)** Interface VPC endpoints allow instances that run in a VPC to connect to other AWS services privately through an elastic network interface. However, interface VPC endpoints incur a cost. The additional cost to read the data frequently from a second Region would increase the data-transfer cost. Replication of a small amount of data to an S3 bucket in a different Region would be more cost-effective.

**Incorrect Option B)** Amazon EFS provides simple and scalable file storage for use with EC2 instances. DataSync is an online data-transfer service that simplifies, automates, and accelerates data transfer between AWS storage services. CRR would be a more cost-effective solution.

**Incorrect Option D)** This solution would not meet the requirements because it adds the costs associated with the use of Lambda to replicate the objects. CRR would provide the same functionality with no additional cost beyond the basic data-transfer cost.

For more information about DataSync, see [What Is AWS DataSync](https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html)?

For more information about CRR, see When to [Use Cross-Region Replication](https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html#crr-scenario)

For more information about interface endpoints for Amazon S3, see [AWS PrivateLink for Amazon S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html)

For more information about gateway VPC endpoints, see [Gateway VPC Endpoints](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway.html)

**Question 47/75**

A company wants to replace its call center system with a solution built using AWS managed services. The company call center would like the solution to receive calls, create contact flows, and scale to handle growth projections. The call center would also like the solution to use deep learning capabilities to recognize the intent of the callers and handle basic tasks, reducing the need to speak to an agent. The solution should also be able to query business applications and provide relevant information back to callers as requested.

Which services should the solutions architect use to build this

solution? (Select THREE.)

1. Amazon Rekognition to identify who is calling.
2. ***Amazon Connect to create a cloud-based contact center.***
3. Amazon Alexa for Business to build conversational interfaces.
4. ***AWS Lambda to integrate with internal systems.***
5. ***Amazon Lex to recognize the intent of the caller.***
6. Amazon SQS to add incoming callers to a queue.

**Correct Answer: B, D, E**

Explanation:

**Correct Option B)** You use Amazon Connect to create cloud-based contact centers, to design contact flows (similar to interactive voice response agents),and to onboard agents.

**Correct Option D)** Amazon Lex uses AWS Lambda functions to query business applications, provide information back to callers, and make updates to information as needed.

**Correct Option E)** You can use Amazon Lex to build conversational interfaces that use voice and text into any application. Amazon Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) to convert speech to text. Amazon Lex also provides natural language understanding (NLU) functionality to recognize conversational intent.

**Incorrect Option A)** Amazon Rekognition gives you the ability to add image and video analysis to your applications. This scenario is not an appropriate use case for Amazon Rekognition.

**Incorrect Option C)** Alexa for Business provides features to control Alexa-compatible devices, enroll users, and assign skills at scale within an organization. This scenario is not an appropriate use case for Alexa for Business.

**Incorrect Option F)** Amazon SQS gives users the ability to decouple and scale microservices, distributed systems, and serverless applications. Amazon Connect manages a customer queue flow. You use Amazon SQS to send, store, and receive messages between software components. This scenario is not an appropriate use case for Amazon SQS. For more information about Amazon SQS, see Amazon SQS

For more information about Amazon Rekognition, see [Amazon Rekognition](https://aws.amazon.com/rekognition/)

For more information about [Amazon Connect, see Category: Amazon Connect](https://aws.amazon.com/blogs/aws/category/amazon-connect/)

For more information about contact flows, see Create [Amazon Connect Contact Flows](https://docs.aws.amazon.com/connect/latest/userguide/contactflow.html)

For more information about Alexa, see [Alexa for Business](https://aws.amazon.com/alexaforbusiness/#Benefits)

For more information about Lambda integration with Amazon Lex, see Amazon Lex

<https://aws.amazon.com/lex/#Call_Center_Bots>

For more information about Amazon Lex, see Amazon Lex

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

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

**Question 48/75**

A company plans to migrate 500 workloads to the AWS Cloud. The company creates separate accounts for different workloads by using *AWSOrganizations*. The company has teams that focus solely on security and infrastructure. Most workloads fall into well-defined environments such as production, development, or testing. There are a few unique workloads that require specific security policies. The company is not sure how to organize the workloads and teams. A solutions architect needs to design an account structure.

Which combination of steps should the solutions architect take to set up the correct account structures? (Select THREE.)

1. Set up a centralized security account for logging, tooling, and audit-related activities.
2. ***Set up separate security accounts for logging, tooling, and audit-related activities.***
3. Create one OU for each workload. Add each workload account into each workload OU. Apply appropriate SCPs at the OU level.
4. ***Create OUs for each environment. Add workload accounts to the appropriate environment OUs. Apply appropriate SCPs at the OU level.***
5. Create accounts for unique workloads in the same OUs as the regular workloads. Apply appropriate SCPs at the account level.
6. ***Create accounts for unique workloads in a separate OU that is named "Exceptions." Apply appropriate SCPs at the account level.***

**Correct Answer: B, D, F**

Explanation:

**Correct Option B)** Organizations provides centralized account management in a hierarchical fashion through OUs and policies. You should create separate security accounts for logging, security tooling, read-only access, and emergency access (break-glass access), especially for advanced organizations.

**Correct Option D)** Organizations provides centralized account management in a hierarchical fashion through OUs and policies. A solution that creates OUs based on functional roles would give you the ability to apply common SCPs across the accounts with the same functional role.

**Correct Option F)** Organizations provides centralized account management in a hierarchical fashion through OUs and policies. The creation of a separate OU for any exception accounts would reduce the effort necessary for you to apply SCPs to the relevant accounts as needed.

**Incorrect Option A)** Organizations provides centralized account management in a hierarchical fashion through OUs and policies. You cannot achieve workload isolation, minimal blast radius, and simpler access management by creating a single account for all logging, tooling, and audit activities.

**Incorrect Option C)** Organizations provides centralized account management in a hierarchical fashion through OUs and policies. A solution that creates OUs based on workloads would require you to apply common production and testing SCPs at the account level. This solution would complicate policy management.

**Incorrect Option E)** Organizations provides centralized account management in a hierarchical fashion through OUs and policies. A solution that creates accounts for unique exception workloads in the same OU as the regular workloads would require you to apply common and unique SCPs directly to the accounts. This solution would complicate policy management.

For more information about security account structure, see [Security OU and accounts](https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/security-ou-and-accounts.html)

For more information about the design of [AWS accounts within Organizations, see Design Principles for Organizing](https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/design-principles-for-organizing-your-aws-accounts.html) Your AWS Accounts. For more information about [accounts that have unique requirements, see Exceptions OU](https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/exceptions-ou.html)

**Question 49/75**

A multi-node application runs on Amazon EC2 instances that run in several subnets within the same VPC. Instance A (172.31.16.139) initiates communication to Instance B (10.10.128.14) on port 5001. Communication between the instances is not successful. A solutions architect analyzes VPC flow logs to identify the problem and discovers the following log entries:

2 123456789010 eni‑1235b8ca123456789 172.31.16.139 10.10.128.14 20641 5001 6 20 4249 1418530010 1418530070 ACCEPT OK

2 123456789010 eni‑1235b8ca123456789 10.10.128.14 172.31.16.139 5001 20641 6 20 4249 1418530192 1418530265 REJECT OK

Which solution will resolve this problem?

1. Modify any host-based firewalls on Instance B to allow inbound communications on TCP port 20641.
2. ***Modify the network ACL in the Instance B subnet to allow outbound communications on port 20641.***
3. Modify the inbound rules for the security group on eni-1235b8ca123456789 to allow port 20641.
4. Modify the main route table in the VPC to allow inbound and outbound traffic to both instances.

**Correct Answer: B**

Explanation:

**Correct Option B)** VPC flow logs represent metadata about network packets that flow through the VPC. Network traffic appears to be allowed to exit the network interface. However, the response is not allowed. The problem must be with the network ACL because security groups are stateful and would automatically allow return traffic. Reconfiguration of the network ACL to allow traffic to return on the appropriate ports is the correct solution.

**Incorrect Option A)** VPC flow logs represent metadata about network packets that flow through the VPC. VPC flow logs do not contain information that indicates what the operating system of an instance will accept or reject.

**Incorrect Option C)** VPC flow logs represent metadata about network packets that flow through the VPC. Network traffic appears to be allowed to exit the network interface. However, the response is not allowed. Security groups are stateful and would automatically allow return traffic.

**Incorrect Option D)** VPC flow logs represent metadata about network packets that flow through the VPC. This is not a routing problem because the logs indicate that the traffic has been rejected at the network interface.

For more information about VPC flow logs and what they capture, see [Flow Logs Basics](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#flow-logs-basics)

For more information about security groups and network ACL interpretation within the VPC flow logs, [see Security Group and Network ACL Rules](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#flow-log-example-security-groups)

For more information about [the local route, see Routes](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html#route-table-routes)

**Question 50/75**

A company has multiple AWS accounts with resources in different AWS Regions. The company uses a combination of security services, such as Amazon GuardDuty, Amazon Macie, and AWS Identity and Access Management (IAM) Access Analyzer. A security team needs to provide regular audit reports on security findings and remediation efforts. The security team needs to see consolidated findings for all accounts.

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

1. ***Create an organization in AWS Organizations and activate AWS Security Hub in the management account. Designate a Security Hub administrator account and add the other AWS accounts as member accounts in Security Hub. Use the administrator account to report on the consolidated findings.***
2. Activate AWS Security Hub in each AWS account. Designate an administrator account and add the other AWS accounts as member accounts. Create an aggregation Region in the administrator account. Use the aggregation Region in the administrator account to report on the consolidated findings.
3. Create an organization in AWS Organizations and add all the accounts to the organization. Designate an AWS Audit Manager administrator account in the organization. Activate Audit Manager in the management account. Use the administrator account to run assessments and to view assessment reports.
4. Activate AWS Audit Manager in each Region in each account where AWS resources are running. Create a custom framework that includes the controls and control sets. Share the custom framework with the other accounts. Run assessments and view assessments by using the framework.

**Correct Answer: A**

**Correct Option A)** Organizations gives you the ability to create new AWS accounts programmatically. Security Hub provides a comprehensive view of your security state on AWS and evaluates environments according to security industry standards and best practices. When Organizations is activated, Security Hub can automatically detect new accounts that the company adds to the organization. This is the solution with the least operational overhead.

**Incorrect Option B)** Security Hub provides a comprehensive view of your security state on AWS and evaluates environments according to security industry standards and best practices. However, without Organizations, you would have to manually configure Security Hub in each new account. This solution would require unnecessary operational overhead.

**Incorrect Option C)** Audit Manager continuously audits your AWS usage to assess risks and compliance with regulations and industry standards. However, you need Security Hub to consolidate findings from various AWS security services.

**Incorrect Option D)** Audit Manager continuously audits your AWS usage to assess risks and compliance with regulations and industry standards. However, you need Security Hub to consolidate findings from various AWS security services.

For more information about Security Hub, see What Is [AWS Security Hub](https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html)?

For more information on Audit Manager, see What Is [AWS Audit Manager?](https://docs.aws.amazon.com/audit-manager/latest/userguide/what-is.html)

For more information about Organizations, see [Using AWS Organizations to Manage Accounts](https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-prereq-orgs.html)

**Question 51/75**

A company manages multiple AWS accounts by using AWS Organizations. The company uses AWS Config to continuously audit and evaluate its AWS resources. The company needs to deploy a set of AWS Config rules across almost all accounts, including the management account, while excluding a few accounts. An AWS CloudFormation template already defines the required AWS Config rules. The company wants to ensure consistent application of the rules and wants to prevent any unauthorized modifications.

Which combination of steps will meet these requirements? (Select TWO.)

1. Use a CloudFormation template and AWS Service Catalog to launch a product across all applicable accounts. Use CloudFormation to perform drift detection frequently to ensure consistency.
2. Use AWS CloudFormation StackSets to deploy stacks across all applicable accounts. Perform drift detection frequently to ensure consistency.
3. ***Use AWS Config to deploy an organization conformance pack that uses a CloudFormation template across all the accounts. Include a list of accounts to exclude.***
4. ***Activate trusted access in Organizations for the relevant service. Register a delegated administrator account to implement the relevant solution.***
5. Deactivate trusted access in Organizations for the relevant service. Activate each individual account administrator to implement the relevant solution.

**Correct Answer: C, D**

Explanation:

**Correct Option C)** AWS Config gives you the ability to continuously asses, audit, and evaluate the configurations of your AWS resources. AWS Config can deploy rules in a conformance pack across all AWS accounts within an organization. AWS Config can include the management account of Organizations and exclude other accounts by using the exclusion list. Only the delegated administrator account can modify the rules deployed by AWS Config. This limit ensures consistent compliance and prevents unauthorized modifications.

**Correct Option D)** Organizations is an account-management service in which trusted access allows supported AWS services such as AWS Config to perform tasks across accounts in the organization. AWS Config also supports a delegated administrator that can implement conformance packs across multiple accounts and achieve consistent compliance without any unauthorized modifications.

**Incorrect Option A)** AWS Service Catalog creates and manages catalogs of IT services and solutions. This service helps achieve compliance with organizational business policies. Drift detection does not prevent unauthorized modifications.

**Incorrect Option B)** CloudFormation StackSets gives you the ability to create, update, or delete stacks across multiple accounts and AWS Regions with a single operation. Drift detection does not prevent unauthorized modifications.

**Incorrect Option E)** Organizations is an account-management service in which trusted access allows supported AWS services such as AWS Config and CloudFormation to perform tasks across accounts in the organization. Performance of these tasks requires trusted access. Individual account administrators are not able to perform these tasks.

For more information about CloudFormation drift detection, see [Detecting Unmanaged Configuration Changes to Stacks and Resources](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html) For more information about how to create a stack set, see Create a [Stack Set with Service-Managed Permissions](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-getting-started-create.html#stacksets-orgs-associate-stackset-with-org) For more information about application of AWS Config rules across accounts in an organization, see Enabling [AWS Config Rules Across All Accounts in Your Organization](https://docs.aws.amazon.com/config/latest/developerguide/config-rule-multi-account-deployment.html)

For more information about management of conformance packs within an organization, see [Managing Conformance Packs Across All Accounts in Your Organization](https://docs.aws.amazon.com/config/latest/developerguide/conformance-pack-organization-apis.html) For more information about [trusted access in Organizations, see AWS Services That You Can Use with AWS Organizations](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_integrate_services_list.html) For more information about trusted access in AWS Organizations, see AWS Services That You Can Use with [AWS Organizations](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_integrate_services_list.html)

**Question 52/75**

A company uses AWS Organizations to manage multiple AWS accounts. The accounts share an Amazon Simple Queue Service (Amazon SQS) queue. The SQS queue is also shared with other AWS accounts outside the organization. All internal and external accounts have access to send and receive messages according to a permissions policy that is attached to the SQS queue. The company wants to identify any external principals that have access to the SQS queue.

How should a solutions architect meet this requirement?

1. Set up an AWS CloudTrail trail that logs data events. Use CloudTrail logs to track Amazon SQS API activities by any external principals.
2. ***Use an AWS Identity and Access Management Access Analyzer to create an analyser with the current organization as a zone of trust. Filter by external findings on the SQS queue.***
3. Set up an AWS CloudTrail trail that logs management events. Use CloudTrail logs to track Amazon SQS API activities by any external principals.
4. Use AWS Identity and Access Management Access Analyzer to create an analyzer with the current account as a zone of trust. Filter by external findings on the SQS queue.

**Correct Answer: B**

Explanation:

**Correct Option B)** IAM Access Analyzer helps identify the resources that are shared with an external entity. An analyser with the organization as the zone of trust will generate findings only for external accounts. It will not include the findings of the internal accounts within the organization.

**Incorrect Option A)** CloudTrail records account activity and service events from most AWS services. A trail that logs data events does not capture data events from Amazon SQS such as SendMessage and ReceiveMessage activities.

**Incorrect Option C)** CloudTrail records account activity and service events from most AWS services. A trail that logs management events does not capture data events such as SendMessage and ReceiveMessage activities.

**Incorrect Option D)** IAM Access Analyzer helps identify the resources that are shared with an external entity. An analyzer with a specific account as the zone of trust will generate findings for other internal accounts along with external accounts. This solution does not meet the company's requirements.

For more information about CloudTrail management events, see [CloudTrail Concepts](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-management-events)

For more information about IAM Access Analyzer, see [Using AWS IAM Access Analyzer](https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html)

For more information about CloudTrail data events, see [CloudTrail Concepts](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-data-events)

For more information about IAM Access Analyzer resource types, see [Access Analyzer Resource Types](https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-resources.html)

For more information about filtering [IAM Access Analyzer findings, see Filtering Findings](https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-findings-filter.html)

Question 53/75

A company has multiple AWS accounts. A solutions architect has created an organization in AWS Organizations with two OUs: Dev and Prod. The company enforces the following rules:

\* The root user in all existing and future member accounts must not

have the ability to make any AWS service API calls.

\* Existing and future Dev member accounts must be able to create

resources only in the us-west-2 Region.

\* Existing and future Prod member accounts must be able to create

resources in any Region.

The company creates the following SCPs:

\* SCP1, which denies all actions on all resources with the following condition:

{

"Condition":

{

"StringLike": { "aws:PrincipalArn": "arn:aws:iam::\*:root" }

}

}

\* SCP2, which denies all actions on all resources with the following condition:

{

"Condition":

{

"StringNotEquals": {"aws:RequestedRegion": "us-west-2"}

}

}

How should the company implement the SCPs to meet these requirements with the LEAST operational overhead?

1. Attach SCP1 and SCP2 to the organization's root.
2. Attach SCP1 to the Prod OU. Attach SCP2 to the Dev OU.
3. Attach SCP1 to all accounts. Attach SCP2 to each Dev account.
4. ***Attach SCP1 to the organization's root. Attach SCP2 to the Dev OU.***

**Correct Answer: D**

**Correct Option D)** If you attach SCP1 to the organization's root and attach SCP2 to the Dev OU, you will enforce the rules in the two SCPs correctly with the least operational overhead.

**Incorrect Option A)** If you attach SCP2 to the organization's root, you will enforce all the rules in SCP2 on all member accounts. The requirement is to enforce the rules in SCP2 only on member accounts in the Dev OU.

**Incorrect Option B)** If you attach SCP1 to only the Prod OU, you will enforce the rules in SCP1 only on the accounts under the Prod OU. The requirement is to enforce the rules in SCP1 on all accounts.

**Incorrect Option C)** If you attach SCP1 to all accounts and attach SCP2 to each member account under the Dev OU, you will enforce the rules in both SCPs correctly. However, this solution would incur additional operational overhead that you would avoid by attaching the SCPs at the OU level.

For more information about inheritance for service control policies, see Inheritance for [Service Control Policies](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance_auth.html) For more information about inheritance for service control policies, see [Inheritance for Service Control Policies](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance_auth.html)

For more information [about management of OUs, see Managing Organizational Units (OUs)](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_ous.html)

**Question 54/75**

A company has resources in on-premises networks and in multiple VPCs on AWS. The company needs a networking solution that will give the on-premises resources the ability to communicate with the VPC resources. The VPC resources also must be able to communicate with each other. The company has configured a customer gateway device on premises and has attached virtual private gateways to each VPC. The company wants a scalable solution so that the company can easily add more VPCs in the future.

How should a solutions architect configure the network connectivity to meet these requirements with the LEAST operational overhead?

1. Create an individual AWS Site-to-Site VPN connection between the customer gateway device and each of the virtual private gateways. Configure VPC peering connections between all the VPCs.
2. ***Create a transit gateway. Create an AWS Site-to-Site VPN attachment between the customer gateway device and the transit gateway. Attach the VPCs to the transit gateway. Remove the virtual private gateways.***
3. Set up a connection through AWS Direct Connect. Create VIFs to provide access to the virtual private gateways. Configure VPC peering connections between all the VPCs.
4. Create a transit VPC. Create VPN connections from the transit VPC to each virtual private gateway. Create AWS Site-to-Site VPN connections between the customer gateway device and the transit VPC.

**Correct Answer: B**

Explanation:

**Correct Option B)** A transit gateway is a network transit hub that you can use to interconnect VPCs and on-premises networks. All the necessary connections can occur through a single transit gateway, minimizing operational overhead.

**Incorrect Option A)** Site-to-Site VPN is a fully managed service that creates a secure connection between on-premises resources and AWS resources by using IPsec tunnels. A VPC peering connection is a network connection between two VPCs that gives you the ability to route traffic between the VPCs by using private addresses. A significant amount of operational overhead would result from the creation and management of multiple VPN connections and VPC peering connections.

**Incorrect Option C)** Direct Connect can connect on-premises networks to AWS. This solution would require the configuration and management of a Direct Connect connection and multiple VPC peering connections, significantly increasing operational overhead.

**Incorrect Option D)** A transit VPC is a common way to connect geographically dispersed VPCs and remote networks to create a global network transit center. However, a transit VPC requires additional configuration and operational overhead because you must manage Amazon EC2 instances. With a transit gateway, there are no EC2 instances to manage.

For more information about Site-to-Site VPN, see [What is AWS Site-to-Site VPN](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)?

For more information about how to peer VPCs, see [What is VPC Peering](https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html)?

For more information about transit gateways, see [What is a Transit Gateway](https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html)?

For more information about Direct Connect, see [What is AWS Direct Connect](https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html)?

For more information about transit VPCs, [see Transit VPC Solution](https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/transit-vpc-solution.html)

**Question 55/75**

A company stores a large amount of customer data in an Amazon S3 bucket that uses the S3 Standard storage class. The amount of data will continue to grow. The company needs to reduce the cost of the data storage. The company needs to access some customer data frequently within the first 6 months. However, the company rarely needs to access other customer data during that period. The company rarely needs to access data that is 180 days or older, but the company must have the ability to access this old data within 6 hours.

Which storage strategy will meet these requirements MOST cost-effectively?

1. Implement S3 Intelligent-Tiering on the existing S3 bucket. Activate the Deep Archive Access tier. Set the days until transition to 180.
2. ***Implement S3 Intelligent-Tiering on the existing S3 bucket. Activate the Archive Access tier. Set the days until transition to 180.***
3. Create a new S3 Lifecycle configuration for the existing S3 bucket. Configure the lifecycle rule for all objects to move data to S3 Glacier Flexible Retrieval after 180 days.
4. Create a new S3 Lifecycle configuration for the existing S3 bucket. Configure the lifecycle rule for all objects to move data to S3 Glacier Deep Archive after 180 days.

**Correct Answer: B**

Explanation:

**Correct Option B)** S3 Intelligent-Tiering automatically monitors access patterns and moves objects across multiple access tiers to optimize storage costs. Standard retrieval of objects in the S3 Intelligent-Tiering Archive Access tier occurs within 3–5 hours. This solution addresses both the unknown access patterns and the requirement to access the old data within 6 hours.

**Incorrect Option A)** S3 Intelligent-Tiering automatically monitors access patterns and moves objects across multiple access tiers to optimize storage costs. However, Standard retrieval of objects in the S3 Intelligent-Tiering Deep Access Archive tier occurs within 12 hours. This time frame does not meet the requirement to access the old data within 6 hours.

**Incorrect Option C)** Use of S3 Lifecycle configurations to move data to S3 Glacier Flexible Retrieval would reduce the cost of storage after 180 days. S3 Glacier Flexible Retrieval can retrieve objects quickly. However, this solution leaves all data in S3 Standard for the first 180 days, when many of the infrequently accessed objects could be stored at a much lower cost. This solution does not optimize the storage classes based on unknown or changing access patterns. A better solution would use S3 Intelligent-Tiering.

**Incorrect Option D)** Use of S3 Lifecycle configurations to move data to S3 Glacier Deep Archive would reduce the cost of storage after 180 days. However, S3 Glacier Deep Archive has a retrieval time of 12 hours. This time frame does not meet the requirement to access the old data within 6 hours. Additionally, this solution leaves all data in S3 Standard storage for the first 180 days, when many of the infrequently accessed objects could be stored at a much lower cost.

For more information about S3 Intelligent-Tiering, [see How S3 Intelligent-Tiering](https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering-overview.html) Works

**Question 56/75**

A company has migrated most of its on-premises infrastructure to the AWS Cloud. The company is planning to complete the migration soon. After the migration, the company will retire its on-premises infrastructure. The company currently uses Active Directory to manage and authenticate its users. The company wants an AWS solution to manage users on AWS. The company has hundreds of users and needs only basic LDAP functionality. The company wants to implement multi-factor authentication (MFA) as part of the solution.

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

1. Configure an AWS IAM Identity Center (AWS Single Sign-On) identity store to manage the users in AWS. Provision users, groups, and entitlements in IAM Identity Center.
2. Configure an Active Directory Connector directory in AWS Directory Service. Connect the Active Directory Connector directory to the on-premises Active Directory.
3. Configure a Simple Active Directory directory in AWS Directory Service. Use the Comma Separated Value Directory Exchange (CSVDE) utility to migrate the users from the on-premises Active Directory to AWS.
4. Configure a directory with AWS Directory Service for Microsoft Active Directory. Use the Active Directory Migration Toolkit to migrate the users from the on-premises Active Directory to AWS.

**Correct Answer: C**

Explanation:

**Correct Option C)** AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, runs Active Directory as a managed service. The Active Directory Migration Toolkit can migrate users from an on-premises Active Directory to AWS Managed Microsoft AD. This solution also supports MFA.

**Incorrect Option A)** You configure an identity store when you configure IAM Identity Center. However, migration from Active Directory to the identity store used by IAM Identity Center would require recreation of the users, groups, and assignments (entitlements). This solution requires more operational effort than necessary.

**Incorrect Option B)** Active Directory Connector is a directory gateway that can redirect directory requests to an on-premises Active Directory without the need to cache any information in the cloud. However, the company plans to retire its on-premises infrastructure.

**Incorrect Option D)** Simple Active Directory is a standalone managed directory that is powered by a Samba 4 Active Directory Compatible Server. Simple Active Directory provides a subset of the features that AWS Managed Microsoft AD offers. However, Simple Active Directory does not support MFA, which is one of the requirements.

For more information about how to configure an identity store, see [Manage Identities in IAM Identity Center](https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source-sso.html)

For more information about how to change identity stores from [Active Directory to IAM Identity Center, see Considerations for Changing Your Identity Source](https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source-considerations.html) For more information about Active Directory Connector, see [Active Directory Connector](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html) For more information [about AWS Managed Microsoft AD, see AWS Managed Microsoft AD](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html) For more information about user migration, see [Migrate Users from Active Directory to AWS Managed Microsoft AD](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_migrate_users.html) For more information [about Simple Active Directory, see Simple Active Directory](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_simple_ad.html)

**Question 57/75**

A company has an online event-booking system that consists of a web application that is deployed in a five-instance fleet of Amazon EC2 instances. The EC2 instances run Amazon Linux 2 with identical unencrypted root volumes. A solutions architect has created an Amazon Machine Image (AMI) from the existing configuration. Sometimes there is a gap of up to a month from when one event-booking window ends to when the next booking window begins.

The company wants to shut off resources between event-booking windows. Currently, an administrator stops the instances after each event. However, the boot process is slow, and the long boot time is unacceptable when the company suddenly notifies the administrator that the next event-booking window is open. The company needs to find a solution that will stop and start the system quickly.

Which solution will meet these requirements?

1. ***Create an encrypted snapshot of a root volume. Create a new AMI from the encrypted snapshot. Terminate the existing instances. Launch new instances by using the new AMI with hibernation turned on. Hibernate the instances when they are not in use.***
2. Create an encrypted snapshot of a root volume. Create a new root volume from the snapshot and attach it to the EC2 instances. Modify the EC2 instance options to turn on hibernation. Hibernate the instances when they are not in use.
3. Create a launch template by using the existing AMI. Create an EC2 Auto Scaling group that uses the new launch template. Configure the minimum and desired number of instances to zero. Configure the maximum number of instances to five. Terminate the existing instances.
4. Create a launch template by using the existing AMI. Create an EC2 Auto Scaling group that uses the new launch template. Configure the minimum and desired number of instances to one. Configure the maximum number of instances to five. Terminate the existing instances.

**Correct Answer: A**

Explanation:

**Correct Option A)** A *solution that hibernates instances will have the same cost implications as a solution that stops instances*. It can be faster to restart hibernated instances than to restart stopped instances that take a long time to bootstrap. *To use hibernation for supported EC2 instance types, you must configure hibernation when you first launch the EC2 instance*. You can provide the required root volume encryption by creating an AMI from an encrypted snapshot of the existing volume. This solution would properly configure hibernation.

**Incorrect Option B)** A solution that hibernates instances will have the same cost implications as a solution that stops instances. It can be faster to restart hibernated instances than to restart stopped instances that take a long time to bootstrap. However, to use hibernation for supported EC2 instance types, you must configure hibernation when you first launch the EC2 instance.

**Incorrect Option C)** An EC2 Auto Scaling group with a minimum of zero would terminate all instances that are running if they are not in use. This solution would require the instances to start fresh the for the next event-booking window. This solution would not reduce the boot time for newly launched instances.

**Incorrect Option D)** An EC2 Auto Scaling group with a minimum of one would leave one instance running even if the instance is not in use. The company wants to turn off all instances between booking windows. Additionally, this solution would not reduce the boot time for newly launched instances.

For more information about EC2 instance hibernation, see [Hibernate Your On-Demand or Reserved Linux Instance](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html)

For more information about requirements for hibernation, see [Enable Hibernation for an Instance](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enabling-hibernation.html)

For more information about [how to encrypt root volumes, see Encrypt Unencrypted Resources](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html)

For more information about EC2 hibernation, see Hibernate [Your On-Demand or Reserved Linux Instance](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html)

For more information about [requirements for hibernation, see Enable Hibernation for an Instance](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enabling-hibernation.html)

For more information about [EC2 Auto Scaling, see Auto Scaling Groups](https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html)

**Question 58/75**

A solutions architect needs to create an infrastructure proposal for a web application. The application requires a resilient and highly available design across multiple Availability Zones. The solutions architect proposes the following:

* A VPC with an internet gateway and a NAT gateway
* One public subnet and one private subnet each in two different Availability Zones
* An Amazon EC2 Auto Scaling group spread across multiple Availability Zones behind an internet-facing Application Load Balancer (ALB)
* Amazon DynamoDB tables to store data

What should the solutions architect do to increase the resilience and availability of the proposed architecture?

1. Create a second internet gateway. Attach each internet gateway to a different subnet.
2. Create a second internet-facing ALB. Attach each ALB to a different subnet.
3. Create a second NAT gateway. Update the route tables on each private subnet as needed.
4. Create DynamoDB global tables with two replicated tables that are stored in different AWS Regions.

**Correct Answer: C**

Explanation:

**Correct Option C)** You need to create a second NAT gateway in a separate Availability Zone to achieve a resilient architecture across Availability Zones. A NAT gateway is highly available only within the Availability Zone where it is deployed.

**Incorrect Option A)** You do not need to create a second internet gateway to achieve a resilient architecture across Availability Zones. By default, an internet gateway is a highly available and scalable component that is managed by AWS.

**Incorrect Option B)** You do not need to create a second internet-facing ALB to achieve a resilient architecture across Availability Zones. By default, an ALB is a highly available and scalable resource that is managed by AWS.

**Incorrect Option D)** DynamoDB global tables are not necessary for this solution. Data in DynamoDB tables is automatically replicated across multiple Availability Zones in the Region where the tables are created. You do not need to create a global DynamoDB table to achieve a resilient architecture across Availability Zones.

For more information about internet gateways, see [Connect Subnets to the Internet Using an Internet Gateway](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html)

For more information about [ALBs, see Application Load Balancers](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load-balancers.html)

For more information about [the availability of NAT gateways, see NAT Gateway Basics](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html#nat-gateway-basics)

For more information about [DynamoDB high availability, see What Is Amazon DynamoDB](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html)?

**59/75 Question**

A company runs an HPC cluster in an AWS Region. The cluster consists of a group of Linux instances that run a tightly coupled workload. The company is not satisfied with the current key performance indicators. The company needs to increase network throughput and reduce the network latency between the Amazon EC2 instances that make up the cluster.

Which combination of actions will meet these requirements? (Select THREE.)

1. Deploy the EC2 instances in a partition placement group.
2. Ensure that the EC2 instances run an AMI that supports paravirtual (PV).
3. ***Disable CPU hyperthreading on the EC2 instances.***
4. Use EC2 instances with burstable performance.
5. ***Run the HPC cluster within a single Availability Zone.***
6. ***Select an EC2 instance type that supports the use of an Elastic Fabric Adapter (EFA).***

**Correct Answer: C, E, F**

Explanation:

**Correct Option C)** Intel Hyper-Threading Technology makes a single physical processor appear as multiple logical processors. Most HPC applications will benefit from disabling hyperthreading.

**Correct Option E)** If an HPC cluster runs within a single Availability Zone, workloads can achieve the low-latency network performance that is necessary for the tightly coupled node-to-node communication that is typical for HPC applications.

**Correct Option F)** An EFA is a network device that you can attach to an EC2 instance to accelerate HPC and machine learning applications. With an EFA, HPC applications can scale to thousands of CPUs or GPUs which results in the same application performance as on-premises HPC clusters with the additional benefit of the on-demand elasticity and flexibility of the AWS Cloud.

**Incorrect Option A)** Partition placement groups help reduce the likelihood of correlated hardware failures for an application. Deployment of EC2 instances in a partition placement group spreads EC2 instances across logical partitions and ensures that instances in different partitions do not share the same underlying hardware. A partition placement group would increase network latency, not reduce it.

**Incorrect Option B)** Linux AMIs use one of two types of virtualizations: PV or hardware virtual machine (HVM). Linux PV AMIs would not improve the performance of the cluster because they cannot take advantage of special hardware extensions, such as enhanced networking or GPU processing, to ensure that the EC2 instances are running.

**Incorrect Option D)** The T instance family provides a baseline CPU performance with the ability to burst above the baseline at any time for as long as required. However, burstable performance instances would not typically improve network performance in an HPC cluster.

For more information about EFAs, see [Elastic Fabric Adapter](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html)

For more information about partition placement groups, see [Partition Placement Groups](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-partition)

For more information about burstable performance instances, see [Burstable Performance Instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html)

For more information about Intel Hyper-Threading Technology, see [Compute](https://docs.aws.amazon.com/wellarchitected/latest/high-performance-computing-lens/compute.html)

For more information about Linux AMI virtualization types, see [Linux AMI Virtualization Types](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/virtualization_types.html)

For more information about [network latency, see Architecture Guidelines and Decisions](https://docs.aws.amazon.com/sap/latest/general/arch-guide-architecture-guidelines-and-decisions.html)

**Question 60/75**

A company is manually deploying its application to production and wants to move to a more mature deployment pattern. The company has asked a solutions architect to design a solution that leverages its current Chef tools and knowledge. The application must be deployed to a staging environment for testing and verification before being deployed to production. Any new deployment must be rolled back in 5 minutes if errors are discovered after a deployment.

Which AWS service and deployment pattern should the solutions architect use to meet these requirements?

1. Use AWS Elastic Beanstalk and deploy the application using a rolling update deployment strategy.
2. Use AWS CodePipeline and deploy the application using a rolling update deployment strategy.
3. Use AWS CodeBuild and deploy the application using a canary deployment strategy.
4. ***Use AWS OpsWorks and deploy the application using a blue/green deployment strategy.***

**Correct Answer: D**

Explanation:

**Correct Option D)** OpsWorks can use Chef tools. AWS OpsWorks for Chef Automate gives you the ability to run a Chef Automate server on AWS. This solution meets the requirement to use a staging environment (green). This solution also provides the ability to rollback a deployment quickly by switching user traffic back to the old stack (blue). For more information about Chef and OpsWorks, see AWS OpsWorks for Chef Automate.

**Incorrect Option A)** A solution that uses Elastic Beanstalk with a rolling deployment model would split the application instances into batches and deploy one batch at a time. Because the company must deploy the application to a staging environment before the company will deploy the application to production, rolling updates would not be the appropriate deployment pattern.

**Incorrect Option B)** The company wants to use Chef tools in this scenario. Therefore, CodePipeline is not the appropriate service. Additionally, because the company must deploy the application to a staging environment before the company will deploy the application to production, rolling updates would not be the appropriate deployment pattern.

**Incorrect Option C)** The company wants to use Chef tools in this scenario. Therefore, CodeBuild is not the appropriate service. Additionally, because the company must deploy the application to a staging environment before the company will deploy the application to production, a canary deployment would not be the appropriate deployment pattern.

For more information about CodePipeline, see [What Is AWS CodePipeline](https://docs.aws.amazon.com/codepipeline/latest/userguide/welcome.html)?

For more information about Elastic Beanstalk, see [AWS Elastic Beanstalk](https://aws.amazon.com/elasticbeanstalk/)

For more information about Elastic Beanstalk and rolling updates, see [Elastic Beanstalk Rolling Environment Configuration Updates](https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rollingupdates.html) For more information about CodeBuild, see What Is [AWS CodeBuild](https://docs.aws.amazon.com/codebuild/latest/userguide/welcome.html)?

For more information on [AWS OpsWorks](https://docs.aws.amazon.com/opsworks/latest/userguide/welcome_opscm.html)

For more information about blue/green deployments, see [Using a Blue-Green Deployment Strategy](https://docs.aws.amazon.com/opsworks/latest/userguide/best-deploy.html#best-deploy-environments-blue-green)

**61/75 Question**

A media company has a system that transcodes a set of original video files and stores the newly formatted files in Amazon S3. These video files can be recreated. The company will access the stored files once per day for the first 60 days. After day 60, the company will access the files infrequently for the next 6 months. After that 6-month period, the company will very rarely access the files. However, company policy dictates that the files must be accessible within 5 hours.

Which S3 Lifecycle configuration will meet these requirements MOST cost-effectively?

1. ***Use S3 Standard for the first 60 days. Use S3 One Zone-Infrequent Access (S3 One Zone-IA) for day 60 through the next 6 months. Use S3 Glacier Flexible Retrieval after that 6-month period.***
2. Use S3 Intelligent-Tiering for the first 60 days. Use S3 One Zone-Infrequent Access (S3 One Zone-IA) for day 60 through the next 6 months. Use S3 Glacier Deep Archive after that 6-month period.
3. Use S3 Standard for the first 60 days. Use S3 Standard-Infrequent Access (S3 Standard-IA) for day 60 through the next 6 months. Use S3 Glacier Deep Archive after that 6-month period.
4. Use S3 Intelligent-Tiering for the first 60 days. Continue to use S3 Intelligent-Tiering for the next 6 months. Use S3 Glacier Flexible Retrieval after that 6-month period.

**Correct Answer: A**

Explanation:

**Correct Option A)** For frequently accessed data, S3 Standard provides the lowest cost option for the first 60 days because there are no additional retrieval fees. S3 One Zone-IA is a low-cost option for infrequently accessed data that can be recreated. The company can use S3 One Zone-IA for object access during the next 6 months because the company does not need the higher availability. When the company needs to access the data very rarely, S3 Glacier Flexible Retrieval is the lowest cost object storage that allows retrieval in less than 5 hours.

**Incorrect Option B)** S3 Intelligent-Tiering is ideal when you want to optimize storage costs for data that has unknown or variable access patterns. However, in this scenario, the access patterns are well known. S3 Glacier Deep Archive is a low-cost option for data storage, but retrieval can take up to 12 hours.

**Incorrect Option C)** In a scenario where data can be recreated, you can use S3 One Zone-IA. S3 One Zone-IA has a lower storage cost than S3 Standard-IA. S3 Glacier Deep Archive is a low-cost option for data storage, but retrieval can take up to 12 hours.

**Incorrect Option D)** S3 Intelligent-Tiering is ideal when you want to optimize storage costs for data that has unknown or variable access patterns. However, in this scenario, the access patterns are well known.

For more information about the cost of S3 storage classes, see Using [Amazon S3 Storage Classes](https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html)

For more information about S3 Lifecycle configurations, see [Managing Your Storage Lifecycle](https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html)

**Question 62/75**

A company deploys a serverless application to AWS. A solutions architect needs to develop a reliable and durable solution that logs changes that are made to the application infrastructure. The solution must identify the logs of actions in AWS SDKs and the AWS Management Console. The solution must detect any alterations to log files.

Which solution meets these requirements?

1. Create an AWS CloudTrail trail to record the actions on the application's serverless components. Create a new private S3 bucket to store the logs. Configure S3 server-side file encryption on the S3 bucket that stores the logs.
2. ***Create an AWS CloudTrail trail to record the actions on the application's serverless components. Create a new private S3 bucket to store the logs. Configure validation of log file integrity on the CloudTrail trail.***
3. Create two AWS CloudTrail trails: one trail for the AWS SDK actions and one trail for the AWS Management Console actions. Create two private S3 buckets for the logs. Select the server access logging option for the S3 buckets that store the logs.
4. Create two AWS CloudTrail trails: one trail for the AWS SDK actions and one trail for the AWS Management Console actions. Create two private S3 buckets for the logs. Run an Amazon Macie discovery job on the S3 buckets that store the logs.

**Correct Answer: B**

Explanation:

**Correct Option B)** CloudTrail records API calls to the AWS infrastructure. Events include actions that are taken in the AWS Management Console, AWS CLI, and AWS SDKs and APIs. CloudTrail can deliver events to Amazon S3. Validation of log file integrity could identify alterations to a log file.

**Incorrect Option A)** CloudTrail records API calls to the AWS infrastructure. Events include actions that are taken in the AWS Management Console, AWS CLI, and AWS SDKs and APIs. CloudTrail can deliver events to Amazon S3. Server-side file encryption would not detect alterations to the log files.

**Incorrect Option C)** CloudTrail records API calls to the AWS infrastructure. Events include actions that are taken in the AWS Management Console, AWS CLI, and AWS SDKs and APIs. Two CloudTrail logs would deliver a duplicated stream of logs to Amazon S3. Duplication would make this configuration unnecessary. Use of server access logs would not detect alterations to the log files.

**Incorrect Option D)** CloudTrail records API calls to the AWS infrastructure. Events include actions that are taken in the AWS Management Console, AWS CLI, and AWS SDKs and APIs. Two CloudTrail logs would deliver a duplicated stream of logs to Amazon S3. The duplication makes this configuration unnecessary. Macie automates the discovery of sensitive data in Amazon S3. A Macie discovery job would not detect alterations to the log files.

For more information about CloudTrail, see What Is [AWS CloudTrail](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)?

For more information about integrity validation, see [Validating CloudTrail Log File Integrity](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html)

For more information about server access logs, see Logging Requests [Using Server Access Logging](https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerLogs.html)

**Question 63/75**

A solutions architect is responsible for redesigning a legacy Java application to improve its availability, data durability, and scalability. Currently, the application runs on a single high-memory Amazon EC2 instance. It accepts HTTP requests from upstream clients, adds them to an in-memory queue, and responds with a 200 status. A separate application thread reads items from the queue, processes those items and persists the results to an Amazon RDS MySQL instance. The processing time for each item takes 90 seconds on average, most of which is spent waiting on external service calls, but the application is written to process multiple items in parallel. Traffic to this service is unpredictable. During periods of high load, items may sit in the internal queue for over an hour while the application processes the backlog. In addition, the current system has issues with availability and data loss if the single application node fails. Clients that access this service cannot be modified. They expect to receive a response to each HTTP request they send within 10 seconds before they will time out and retry the request.

Which approach would improve the availability and durability of the system while decreasing the processing latency and minimizing costs?

1. Create an Amazon API Gateway REST API that uses Lambda proxy integration to pass requests to an AWS Lambda function. Migrate the core processing code to a Lambda function and write a wrapper class that provides a handler method that converts the proxy events to the internal application data model and invokes the processing module.
2. ***Create an Amazon API Gateway REST API that uses a service proxy to put items in an Amazon SQS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SQS instead of an in-memory queue. Deploy the new processing application to smaller EC2 instances within an Auto Scaling group that scales dynamically based on the approximate number of messages in the Amazon SQS queue.***
3. Modify the application to use Amazon DynamoDB instead of Amazon RDS. Configure Auto Scaling for the DynamoDB table. Deploy the application within an Auto Scaling group with a scaling policy based on CPU utilization. Back the in-memory queue with a memory-mapped file to an instance store volume and periodically write that file to Amazon S3.
4. Update the application to use a Redis task queue instead of the in-memory queue. Build a Docker container image for the application. Create an Amazon ECS task definition that includes the application container and a separate container to host Redis. Deploy the new task definition as an ECS service using AWS Fargate, and enable Auto Scaling.

**Correct Answer: B**

Explanation:

**Correct Option B)** This solution provides a managed, automatically scaled frontend to receive requests. This solution stores messages durably in Amazon SQS until the messages are successfully processed. The backend will scale horizontally when a surge of requests arrives.

**Incorrect Option A)** API Gateway REST API Lambda proxy integrations are inherently synchronous. The clients would time out before the request finishes. API Gateway has a limit of 29 seconds for backend response times.

**Incorrect Option C)** You would not address the durability concerns by configuring auto scaling for DynamoDB. If an instance fails, you will lose messages.

**Incorrect Option D)** This solution does not improve the durability. This solution is also not cost-effective because the frontend and backend are still coupled and must be scaled together.

For more information about API Gateway with Lambda integration, see Build an [API Gateway REST API with Lambda Integration](https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-with-lambda-integration.html) For more information about API Gateway integrations, see [Setting Up REST API Integrations](https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-integration-settings.html) For more information about auto scaling based on Amazon SQS, see [Scaling Based on Amazon SQS](https://docs.aws.amazon.com/autoscaling/latest/userguide/as-using-sqs-queue.html) For more information about DynamoDB auto scaling, see Managing [Throughput Capacity Automatically with DynamoDB Auto Scaling](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html)

**Question 64/75**

A company is launching a web-based application in multiple Regions around the world. The application consists of both static content that the company stores in a private Amazon S3 bucket and dynamic content that the company hosts in Amazon ECS containers behind an Application Load Balancer (ALB). The company requires that the static and dynamic application content be accessible through Amazon CloudFront only.

Which combination of steps should a solutions architect recommend to restrict direct content access to CloudFront? (Select THREE.)

1. ***Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the ALB.***
2. Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the CloudFront distribution.
3. ***Configure CloudFront to add a custom header to origin requests.***
4. Configure the ALB to add a custom header to HTTP requests.
5. Update the S3 bucket ACL to allow access from the CloudFront distribution only.
6. ***Create a CloudFront Origin Access Identity (OAI) and add it to the CloudFront distribution. Update the S3 bucket policy to allow access to the OAI only.***

**Correct Answer: A, C, F**

Explanation:

**Correct Option A)** You can use AWS WAF to validate custom headers. You can associate an AWS WAF web ACL with the ALB.

**Correct Option C)** CloudFront can add a custom header to a request.

**Correct Option F)** You can use an OAI to restrict access to an S3 bucket to viewers who make requests through CloudFront.

**Incorrect Option B)** CloudFront adds the custom header. A web ACL in front of the CloudFront distribution would block any through traffic.

**Incorrect Option D)** ALBs have HTTP(S) listeners. ALBs do not create new headers.

**Incorrect Option E)** Amazon S3 ACLs define which AWS accounts or groups have access.

For more information about how to add custom headers, see [Adding Custom Headers to Origin Requests](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/add-origin-custom-headers.html)

For more information about web ACLs, see [Web Access Control Lists (Web ACLs)](https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html) For more information about how to add custom headers, see [Adding Custom Headers to Origin Requests](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/add-origin-custom-headers.html)

For more information about web ACLs, see [Web Access Control Lists (Web ACLs)](https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html)

For more information about how to add customer headers, see [Adding Custom Headers to Origin Requests](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/add-origin-custom-headers.html)

For more information about ALBs, see What Is an [Application Load Balancer](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html)?

For more information about Amazon S3 ACLs, see [Access Control List (ACL) Overview](https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html)

For more information about CloudFront OAIs and Amazon S3, see [Granting the OAI Permission to Read Files in Your amazon S3 Bucket](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html#private-content-granting-permissions-to-oai)

**Question 65/75**

A company is designing a new application that stores data in Amazon S3. The company creates an S3 bucket with default settings. According to company regulations, no user can delete objects or write over objects in the S3 bucket for a minimum of 5 years after the initial storage of the objects.

Which solution will meet these requirements?

1. ***Create a new S3 bucket with S3 Versioning and S3 Object Lock turned on. Configure Object Lock with a retention period of 5 years. Set the Object Lock retention to compliance mode. Move the existing objects to the new S3 bucket.***
2. Modify the existing S3 bucket by turning on S3 Versioning and S3 Object Lock. Configure Object Lock with a retention period of 5 years. Set the Object Lock retention to compliance mode.
3. Modify the existing S3 bucket by turning on S3 Versioning and S3 Object Lock. Configure Object Lock with a retention period of 5 years. Set the Object Lock retention to governance mode.
4. Create a new S3 bucket with S3 Versioning and S3 Object Lock turned on. Configure Object Lock with a retention period of 5 years. Set the Object Lock retention to governance mode. Move the existing objects to the new S3 bucket.

**Correct Answer: A**

Explanation:

**Correct Option A)** Object Lock with a 5-year retention period would lock the objects and prevent the objects from being overwritten or deleted. In compliance mode, objects cannot be overwritten or deleted by any user, including the root user of the account, for the duration of the retention period. Because you can configure Object Lock only when you first create a bucket, you would need a new bucket.

**Incorrect Option B)** You can configure S3 Versioning for an existing S3 bucket, but you can configure Object Lock only when you first create a bucket. You cannot configure Object Lock for a bucket that already exists.

**Incorrect Option C)** You can configure S3 Versioning for an existing S3 bucket, but you can configure Object Lock only when you first create a bucket. You cannot configure Object Lock for a bucket that already exists. In governance mode, a user that has appropriate permissions could remove the lock and delete the objects.

**Incorrect Option D)** Object Lock with a 5-year retention period would lock the objects and prevent the objects from being overwritten or deleted. However, in governance mode, a user that has appropriate permissions could remove the lock and delete the objects.

For more information about Object Lock, see [How S3 Object Lock Works](https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html)

For more information about Object Lock retention modes, see [Retention Modes](https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html#object-lock-retention-modes)

**Question 66/75**

A company needs to create a web application on AWS to manage registrations for a conference. A database will store the registration information. Additionally, the web application will use several static files. The company's PHP web developer is familiar with the use of LAMP stack applications but does not have much AWS expertise. The company does not expect large changes in traffic on the web application and wants predictable pricing to facilitate budgeting for the conference.

Which solution will meet these requirements with the LEAST time required to learn new technologies?

1. Create and package the web application as a .zip file. Deploy the web application by using AWS Elastic Beanstalk. Configure Amazon DynamoDB for the database. Configure Amazon S3 for the static files.
2. Create and package the web application as a Docker container. Deploy the container by using AWS Fargate. Configure Amazon DynamoDB for the database. Configure Amazon S3 for the static files.
3. ***Create and package the web application by using Amazon Lightsail. Create a Lightsail instance by using an appropriate preconfigured template. Use Lightsail object storage to store the static files.***
4. Create the web application by using AWS Lambda functions. Deploy the web application by using Amazon API Gateway. Configure Amazon RDS for the database. Configure Amazon S3 for the static files.

**Correct Answer: C**

**Correct Option C)** Lightsail provides developers with compute, storage, and network capacity tools. Lightsail also provides the ability to deploy and manage websites and web applications in the cloud. Lightsail offers affordable and predictable monthly payment plans.

**Incorrect Option A)** You can use Elastic Beanstalk to quickly deploy and manage applications in the AWS Cloud without the need to learn about the underlying infrastructure. However, the price model is based on the resources that the application consumes. This solution would not meet the requirement for predictable pricing. Use of DynamoDB would also require additional time to learn.

**Incorrect Option B)** You can use Fargate to run containers without the need to manage servers or clusters of Amazon EC2 instances. However, you would need to develop some expertise to build and create Docker containers. Use of DynamoDB would also require additional time to learn.

**Incorrect Option D)** API Gateway is an AWS service you can use to create, publish, maintain, monitor, and secure REST, HTTP, and WebSocket APIs at any scale. API developers can create APIs that access AWS services, other web services, and data that is stored in the AWS Cloud. However, you would need to have significant AWS expertise to build the required APIs.

For more information about Elastic Beanstalk, see What is [AWS Elastic Beanstalk](https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html)?

For more information about [DynamoDB, see From SQL to NoSQL](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.html) For more information about Fargate, see [What is AWS Fargate](https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html)? For more information about [DynamoDB, see From SQL to NoSQL](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.html)

For more information about Lightsail, see Amazon Lightsail Documentation

For more information about [Lightsail object storage, see Object Storage in Amazon Lightsail](https://lightsail.aws.amazon.com/ls/docs/en_us/articles/buckets-in-amazon-lightsail)

For more information about API Gateway, see What is [Amazon API Gateway](https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome)?

For more information about the configuration of Lambda functions, see [Configuring AWS Lambda Functions](https://docs.aws.amazon.com/lambda/latest/dg/lambda-functions.html)

**Question 67/75**

A company wants to move many different database engines on physical servers to AWS. Many of the databases use functionality that Amazon RDS does not currently support. The company wants to quickly rehost the database servers in the AWS Cloud.

Which migration solution will meet these requirements with the LEAST migration effort?

1. Use AWS Application Discovery Service to migrate the servers to new Amazon EC2 instances.
2. Create new Amazon EC2 instances to host the databases. Use AWS Database Migration Service (AWS DMS) to migrate the databases to AWS.
3. ***Use AWS Application Migration Service (CloudEndure Migration) to migrate the servers to new Amazon EC2 instances. Use general launch settings.***
4. Use VMware Cloud on AWS to migrate the servers to AWS. Use AWS Database Migration Service (AWS DMS) to migrate the databases to AWS.

**Correct Answer: C**

Explanation:

**Correct Option C)** Application Migration Service (CloudEndure Migration) is a highly automated lift-and-shift (rehost) solution that simplifies and accelerates migration to AWS. Application Migration Service (CloudEndure Migration) can launch appropriate EC2 instances that match the on-premises servers and any software that runs on those servers. This solution will perform the migration quickly, with an agent installation on the servers, and will require the least migration effort.

**Incorrect Option A)** Application Discovery Service collects usage and configuration data about on-premises servers to help you plan migrations to the AWS Cloud. Application Discovery Service does not actually perform migrations.

**Incorrect Option B)** You would need to take multiple steps to create EC2 instances and use AWS DMS for migration. Multiple AWS DMS replication instances would be required, in addition to endpoints and tasks for the various database engines. A better solution would be to perform the lift and shift in a single pass with an agent installation.

**Incorrect Option D)** VMware Cloud on AWS is a preferred service for vSphere-based workloads on AWS. However, the company in this scenario wants to move physical servers to the cloud. The company does not want to move vSphere-based workloads.

For more information about Application Discovery Service, see What Is [AWS Application Discovery Service](https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html)?

For more information about AWS DMS, see What is [AWS Database Migration Service](https://docs.aws.amazon.com/dms/latest/userguide/Welcome.html)?

For more information about Application Migration Service (CloudEndure Migration), see What Is [AWS Application Migration Service](https://docs.aws.amazon.com/mgn/latest/ug/what-is-application-migration-service.html)?

For more information about Application Migration Service (CloudEndure Migration) instances, [see Instance Type Right-Sizing](https://docs.aws.amazon.com/mgn/latest/ug/right-sizing.html) For more information about VMware Cloud on AWS, see [VMware Cloud on AWS](https://aws.amazon.com/vmware)

**Question 68/75**

A company runs multiple Amazon RDS DB instances in the same AWS Region. The company runs a variety of database engines, including Oracle, PostgreSQL, and SQL Server. All the DB instances are encrypted. For disaster-recovery purposes, the company has decided to store the data in a second Region.

Which solution will meet these requirements?

1. Configure Amazon RDS automated backups. Configure Amazon S3 Cross-Region Replication (CRR) on the S3 bucket that stores the backups.
2. Configure an AWS Backup vault in a second Region. Configure Amazon RDS automated backups. Configure a backup plan in AWS Backup to back up the DB instances to the AWS Backup vault.
3. Configure Amazon RDS automated backups. Configure RDS cross-Region backup replication for all DB instances.
4. ***Configure an AWS Backup vault in a second Region. Turn off Amazon RDS automated backups. Configure a backup plan in AWS Backup to back up the DB instances to the AWS Backup vault.***

**Correct Answer: D**

Explanation:

**Correct Option D)** You can use AWS Backup to manage backup RDS DB instances. You can provide the required regional protection by creating a vault in a second Region. You must turn off RDS automated backups to use AWS Backup to manage backups.

**Incorrect Option A)** You can configure automated backups for DB instances. This solution would store the backups in an S3 bucket. However, the S3 bucket is maintained and managed by AWS, so you cannot turn on S3 CRR.

**Incorrect option B)** You can use AWS Backup to manage backup RDS DB instances. You would provide the required regional protection by creating a vault in a second Region. However, you cannot turn on automated backups if you use AWS Backup to back up the DB instances.

**Incorrect Option C)** RDS cross-Region backup replication is supported for some RDS databases. However, encrypted SQL Server databases are not supported for cross-Region backup replication.

For more information about cross-Region backups, see [Enabling Cross-Region Automated Backups](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReplicateBackups.html#AutomatedBackups.Replicating.Enable)

For more information about how to create vaults, see [Creating a Backup Vault](https://docs.aws.amazon.com/aws-backup/latest/devguide/creating-a-vault.html)

For more information about automated backups, see [Enabling Automated Backups](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html#USER_WorkingWithAutomatedBackups.Enabling)

For more information about [S3 CRR, see Replicating Objects](https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html)

**Question 69/75**

A company recently deployed a new application that runs on a group of Amazon EC2 Linux instances in a VPC. In a peered VPC, the company launched an EC2 Linux instance that serves as a bastion host. The security group of the application instances allows access only on TCP port 22 from the private IP of the bastion host. The security group of the bastion host allows access to TCP port 22 from 0.0.0.0/0 so that system administrators can use SSH to remotely log in to the application instances from several branch offices.

While looking through operating system logs on the bastion host, a cloud engineer notices thousands of failed SSH logins to the bastion host from locations around the world. The cloud engineer wants to change how remote access is granted to the application instances and wants to meet the following requirements:

* Eliminate brute-force SSH login attempts.
* Retain a log of commands run during an SSH session.
* Retain the ability to forward ports.

Which solution meets these requirements for remote access to the application instances?

1. ***Configure the application instances to communicate with AWS Systems Manager. Grant access to the system administrators to use Session Manager to establish a session with the application instances. Terminate the bastion host.***
2. Update the security group of the bastion host to allow traffic from only the public IP addresses of the branch offices.
3. Configure an AWS Client VPN endpoint and provision each system administrator with a certificate to establish a VPN connection to the application VPC. Update the security group of the application instances to allow traffic from only the Client VPN IPv4 CIDR. Terminate the bastion host.
4. Configure the application instances to communicate with AWS Systems Manager. Grant access to the system administrators to issue commands to the application instances by using Systems Manager Run Command. Terminate the bastion host.

**Correct Answer: A**

Explanation:

**Correct Option A)** Session Manager helps you improve your security posture by giving you the ability to close inbound SSH ports. With Session Manager, you do not need to manage SSH keys and certificates, bastion hosts, or jump boxes. Session Manager offers the benefit of port forwarding. Session Manager also logs and audits session activity.

**Incorrect Option B)** An update to the security group of the bastion host would not eliminate brute-force SSH attempts because the public IP addresses of the branch offices are open. Additionally, you can configure Session Manager to log session activity. This solution does not address the requirement to log commands.

**Incorrect Option C)** A Client VPN connection can guarantee encryption. However, this connection would not be able to retain a log of commands that a user ran during an SSH session.

**Incorrect Option D)** Run Command gives you the ability to automate common administrative tasks and to perform one-time configuration changes at scale. However, Run Command cannot forward ports.

For more information about Client VPN, see What Is [AWS Client VPN](https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/what-is.html)?

For more information about how to use [Session Manager to log session activity, see Logging Session Activity](https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html)

For more information about Session Manager, see [AWS Systems Manager Session Manager](https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html)

For more information about how to use security groups to control traffic, see [Control Traffic to Resources Using Security Groups](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html) For more information about Run Command, see [AWS Systems Manager Run Command](https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html)

**70/75 Question**

A company deploys a new application on AWS. The application runs on two Amazon EC2 instances in two different Availability Zones behind an internet-facing Elastic Load Balancer (ELB). The application accesses an Amazon RDS Multi-AZ DB instance. Within the first week, customers report that the application is having performance issues. Investigations identify two potential reasons for the performance issues: slow read responses from the RDS database and periodic high CPU utilization on the two EC2 instances. A solutions architect needs to implement changes to improve performance and to improve repetitive read responses for the new infrastructure. The solution must be fault-tolerant and must support native automated failover across Availability Zones.

Which combination of configuration changes will meet these requirements?

(Select TWO.)

1. Increase the instance size of the EC2 instances to meet CPU capacity requirements.
2. ***Add two more EC2 instances to host the application. Register the instances with the ELB***.
3. Create an Amazon EC2 Auto Scaling group across Availability Zones. Configure the EC2 Auto Scaling group to be the target for the ELB.
4. Create an Amazon ElastiCache for Memcached cluster to cache responses from the RDS database.
5. ***Create an Amazon ElastiCache for Redis cluster to cache responses from the RDS database***.

**Correct Answer: C, E**

Explanation:

**Correct Option E)** ElastiCache gives you the ability to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. An ElastiCache cluster to cache the RDS database responses can improve repetitive read response times. ElastiCache for Redis natively supports automatic Multi-AZ failover.

**Correct Option C)** An Auto Scaling group would give the application the ability to scale out when CPU utilization increases. A solution that spreads the EC2 instances across multiple Availability Zones meets the requirement for high availability.

**Incorrect Option A)** A change in the instance size could address the issues with high CPU utilization. However, without an Auto Scaling group to automatically replace failed instances, this solution would only partially meet the requirement for fault tolerance.

**Incorrect Option D)** ElastiCache gives you the ability to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. However, ElastiCache for Memcached does not natively support automatic Multi-AZ failover. ElastiCache for Redis does meet this requirement.

**Incorrect Option B)** The addition of EC2 instances could address the CPU utilization issue. However, more than two additional instances might be necessary. Additionally, this solution would not meet the requirement for high availability because there is no automatic multi-AZ failover response. An Auto Scaling group would be a better solution for scaling and high availability.

For more information about Auto Scaling groups, see [Auto Scaling Groups](https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html)

For more information about how to change an [EC2 instance size, see Change the Instance Type](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html)

For more information about ElastiCache for Memcached, see [What Is Amazon ElastiCache for Memcached](https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/WhatIs.html)?

For more information about the differences between [ElastiCache for Memcached and ElastiCache for Redis, see Comparing Memcached and Redis](https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/SelectEngine.html) For more information about ElastiCache for Redis, see [What Is Amazon ElastiCache for Redis](https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/WhatIs.html)? For more information about how to attach an ELB to an Auto Scaling group, see [Attaching a Load Balancer to Your Auto Scaling Group](https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html)

**71/75 Question**

An ecommerce company wants to migrate its order processing system to AWS. The order processing system is a Java-based application with a backend Oracle database. Most order processing occurs in less than 1 minute. The company will update its frontend website to accommodate a cloud-based solution. The company does not want to manage servers on AWS. The company has extensive Oracle database expertise and wants to use this expertise as part of the solution.

Which solution will meet these requirements?

1. Use Amazon Simple Queue Service (Amazon SQS) to hold the orders. Use AWS Lambda functions to capture and process the orders. Convert the backend database to Amazon Aurora.
2. Use Amazon EC2 instances in an Amazon EC2 Auto Scaling group to host the Java-based order processing application. Use an Amazon RDS for Oracle DB instance with a Multi-AZ deployment as the backend database.
3. Use Amazon Kinesis Data Streams to hold the orders. Use AWS Lambda functions to capture and process the orders. Convert the backend database to Amazon DynamoDB.
4. ***Use Amazon Simple Queue Service (Amazon SQS) to hold the orders. Use AWS Lambda functions to capture and process the orders. Use an Amazon RDS for Oracle DB instance with a Multi-AZ deployment as the backend database***.

**Correct Answer: D**

Explanation:

**Correct Option D)** The use of Amazon SQS, Lambda, and Amazon RDS will eliminate the need to manage servers on AWS. This solution meets all the company's requirements.

**Incorrect Option A)** To use Aurora as the backend database, you would need to convert the Oracle database to Aurora. This solution does not meet the requirements because the company wants to continue to use its current Oracle database expertise.

**Incorrect Option B)** This solution proposes to host the Java-based order processing application on EC2 instances. This solution does not meet the requirements because the company does not want to manage servers on AWS.

**Incorrect Option C)** To use DynamoDB as the database, you would need to convert the Oracle database to DynamoDB. This solution does not meet the requirements because the company wants to continue to use its current Oracle database expertise.

For more information about serverless computing options on [AWS, see Serverless Computing](https://aws.amazon.com/serverless/?nc=sn&loc=0)

For more information about Aurora, see [What Is Amazon Aurora](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_AuroraOverview.html)?

For more information about Oracle on [Amazon RDS, see Oracle on Amazon RDS](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Oracle.html)

For more information about Lambda, see [What Is AWS Lambda](https://docs.aws.amazon.com/lambda/latest/dg/welcome.html)?

**Question 72/75**

A company has multiple on-premises data centers around the world. The company wants to migrate 150 VMs to AWS with minimal downtime. The company also needs to migrate 300 TB of data to a single AWS Region. With the company's current internet connection, the data migration would take 5 days.

Which combination of tools and services will provide the FASTEST migration to AWS?

1. Transfer the data by using AWS Snowball devices. Use VM Import/Export to migrate the VMs.
2. ***Transfer the data by using Amazon S3 Transfer Acceleration. Use AWS Application Migration Service (CloudEndure Migration) to migrate the VMs.***
3. Transfer the data by using AWS Snowball devices. Use AWS Application Migration Service (CloudEndure Migration) to migrate the VMs.
4. Transfer the data by using Amazon S3 Transfer Acceleration. Use VM Import/Export to migrate the VMs.

**Correct Answer: B**

Explanation:

**Correct Option B)** You would need approximately 5 days to transfer the data by using S3 Transfer Acceleration. AWS Application Migration Service (CloudEndure Migration) provides automated, live, incremental server replication and AWS console support. Incremental AWS Application Migration Service (CloudEndure Migration) replication minimizes the business impact that is associated with application downtime during the final cutover.

**Incorrect Option A)** You would need approximately 7 days to transfer the data by using Snowball devices. AWS Application Migration Service (CloudEndure Migration) provides significant improvement over VM Import/Export. AWS Application Migration Service (CloudEndure Migration) provides automated, live, incremental server replication and AWS console support.

**Incorrect Option C)** You would need approximately 7 days to transfer the data by using Snowball devices. AWS Application Migration Service (CloudEndure Migration) provides significant improvement over VM Import/Export. AWS Application Migration Service (CloudEndure Migration) provides automated, live, incremental server replication and AWS console support.  
**Incorrect Option D)** You would need approximately 5 days to transfer the data by using S3 Transfer Acceleration. However, AWS Application Migration Service (CloudEndure Migration) provides significant improvement over VM Import/Export. AWS Application Migration Service (CloudEndure Migration) provides automated, live, incremental server replication and AWS console support.

For more information about Snowball, see [Amazon Snowball](https://aws.amazon.com/snowball/faqs) FAQs

For more information about migration tools and services, see [AWS Application Migration Service](https://aws.amazon.com/application-migration-service/faqs) FAQs

For more information about S3 Transfer Acceleration, [see S3 Transfer Acceleration](https://aws.amazon.com/s3/transfer-acceleration)

73/75 Question

A company has 10 VPCs in the same AWS Region. The VPCs have CIDR ranges that do not overlap. Based on an initial requirement to separate communications between VPCs, a solutions architect creates two transit

gateways. Transit Gateway A (TGW-A) has six VPCs attached: VPC-1 through VPC-6. Transit Gateway B (TGW-B) has four VPCs attached: VPC-7 through VPC-10.

The solutions architect finds out that the networking requirements have changed. The company now requires full communication among all 10 VPCs.

How should the solutions architect change the network configuration to meet this requirement?

1. Create a transit gateway peering attachment with TGW-A as the requester and TGW-B as the accepter. Accept the transit gateway attachment. Create static route table entries between TGW-A and TGW-B.
2. In another Region, create a new transit gateway. Attach VPC-7 through VPC-10 to the new transit gateway. Create and accept a peering attachment with TGW-A. Create a static route table entry to the new transit gateway.
3. ***Delete the attachments for VPC-7 through VPC-10 from TGW-B. Create attachments for VPC-7 through VPC-10 on TGW-A. Create static route table entries for the newly added attachments. Delete TGW-B***.
4. Create an interface VPC endpoint in VPC-7 through VPC-10. Create attachments for the interface VPC endpoints to TGW-A. Create static route table entries for the newly added attachments. Delete TGW-B.

**Correct Answer: C**

Explanation:

**Correct Option C)** The attachment of all the VPCs to one transit gateway will provide full communication among all the VPCs. You must remove the attachments from TGW-B before you delete TGW-B.

**Incorrect Option A)** Two transit gateways in the same Region cannot be peered.

**Incorrect Option B)** For VPCs to be attached to a transit gateway, the VPCs must be in the same Region as the transit gateway.

**Incorrect Option D)** Interface VPC endpoints are used to connect supported services by using private IP addresses. Transit gateway connections are called attachments.

For more information about interface VPC endpoints, see [Interface VPC Endpoints](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html) (AWS PrivateLink)

For more information about transit gateways, see [Transit Gateways](https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html)

For more information about how to delete transit gateways, see [Delete a Transit Gateway](https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html#delete-tgw)

For more information about how to peer transit gateways, see [Transit Gateway Peering Attachments](https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering.html)

**74/75 Question**

A weather forecasting company is migrating an application that stores data on premises in a PostgreSQL database. The company wants to migrate the database to Amazon Aurora PostgreSQL. The database size grows at an average rate of 5 GB daily and is currently 50 TB. The data center has an internet connection with 50 Mbps of available bandwidth. The

migration to AWS must be completed as soon as possible within the next 21 days.

Which data transfer strategy meets these requirements with the LEAST amount of application downtime?

1. Take the application offline. Create a local backup of the database. Transmit the database backup file over the existing connection to an Amazon S3 bucket. Use native database tools to restore the backup onto the new database and to set up replication to capture any changes since the backup. Modify the database connection string, and bring the application online.
2. Install the Server Migration Connector VM in the local data center. Use the AWS Server Migration Service (AWS SMS) console to replicate the on-premises database to the new database. Modify DNS records to point to the new database.
3. Create a local backup of the database, and copy the backup onto an AWS Snowcone device. Activate the AWS DataSync agent on the device, and configure the agent to copy the backup and ongoing changes to an Amazon S3 bucket. Use AWS Backup to restore the backup onto the new database and to apply the changes. Modify DNS records to point to the new database.
4. ***Use AWS Database Migration Service (AWS DMS) to launch a replication instance in a connected VPC. Use the AWS Schema Conversion Tool to extract the data locally and to move the data to an AWS Snowball Edge Storage Optimized device. Ship the device to AWS, and use an AWS DMS task to complete the transfer to the target database. For the migration type, choose the option to migrate existing data and replicate ongoing changes. Modify DNS records to point to the new database.***

**Correct Answer: D**

Explanation:

**Correct Option D)** A Snowball Edge device can contain up to 80 TB of data. Delivery of the device takes about 4 to 6 days. The time to load the data depends on several variables including the speed of the local network. AWS will load the data from the device about 1 day after AWS receives the device. You can use Snowball Edge in conjunction with an AWS DMS task.

**Incorrect Option A)** This solution will cause significant downtime. The application will remain down for several days during the data transfer and replication.

**Incorrect Option B)** You cannot use AWS SMS to migrate a PostgreSQL database to Aurora PostgreSQL. You use AWS SMS to migrate on-premises servers to the AWS Cloud.

**Incorrect Option C)** Snowcone does not have the capacity to transfer 50 TB of data. Instead, Snowcone offers a quick and cost-effective method to transfer up to 8 TB or 14 TB of data to the AWS Cloud by shipping the device back to AWS.

For more information about AWS SMS, see What Is [AWS Server Migration Service](https://docs.aws.amazon.com/server-migration-service/latest/userguide/server-migration.html)? For more information about Snowcone, see What Is [AWS Snowcone](https://docs.aws.amazon.com/snowball/latest/snowcone-guide/snowcone-what-is-snowcone.html)? For more information about Snowball Edge, see What Is [AWS Snowball Edge](https://docs.aws.amazon.com/snowball/latest/developer-guide/whatisedge.html)?

For more information about how to migrate a PostgreSQL database to Aurora PostgreSQL, see [Migrate an On-Premises PostgreSQL Database to Aurora PostgreSQL](https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-postgresql-database-to-aurora-postgresql.html)

**75/75 Question**

A company currently hosts a popular gaming application with an associated on-premises Redis database. The database stores player and leader board data. The company wants to migrate both the application and the Redis database to the AWS Cloud. The company will migrate the application to run on a fleet of Amazon EC2 instances across multiple

Availability Zones. The company requires the new database to be durable and to serve traffic with microsecond read latency. The company does not want to manage the database servers after the migration.

Which solution will meet these requirements and store the data in the MOST durable way?

1. Migrate the on-premises application and the database to separate fleets of EC2 instances by using the AWS Application Migration Service (CloudEndure Migration). Turn on Redis replication with replicas in different Availability Zones.
2. Deploy an Amazon MemoryDB for Redis cluster to host the database. Configure at least one read replica for the MemoryDB cluster with multi-AZ activated. Migrate the on-premises application servers by using the AWS Application Migration Service (CloudEndure Migration). Take a snapshot of the existing Redis cluster and upload it to an Amazon S3 bucket. Seed the MemoryDB cluster with the Redis backup data.
3. Deploy an Amazon ElastiCache for Redis cluster to host the database. Configure a Redis replication group with multi-AZ activated. Migrate the on-premises application servers by using the AWS Application Migration Service (CloudEndure Migration). Take a snapshot of the existing Redis cluster and upload it to an Amazon S3 bucket. Seed the ElastiCache cluster with the Redis backup data.
4. Deploy an Amazon MemoryDB for Redis cluster to host the database. Configure at least one read replica for the MemoryDB cluster with multi-AZ activated. Migrate both the on-premises application and the database by using the AWS Application Migration Service (CloudEndure Migration).

**Correct Answer: B**

Explanation:

**Correct Option B)** Application Migration Service helps make the migration of on-premises servers to EC2 instances seamless. MemoryDB for Redis is a durable, in-memory managed database for workloads that require an ultra-fast, primary database. MemoryDB stores successful write operations durably in a distributed multi-AZ transaction log. You can seed a MemoryDB cluster with a snapshot from an existing Redis cluster. You could access the existing snapshot by uploading the snapshot to an S3 bucket.

**Incorrect Option A)** Significant server management effort would be necessary to run the database on EC2 instances. The company does not want to manage the database servers.

**Incorrect Option C)** Although ElastiCache for Redis does support Multi-AZ deployment and has backup and recovery features, this service is not the most durable option to store Redis data on AWS because of the potential for data loss. Amazon MemoryDB for Redis is better suited for a workload that requires a durable database that provides ultra-fast performance.

**Incorrect Option D)** Application Migration Service (CloudEndure Migration) helps make the migration of on-premises servers to EC2 instances seamless. Although Application Migration Service (CloudEndure Migration) can migrate the application to EC2 instances, this service does not support managed databases such as MemoryDB.

For more information about Application Migration Service (CloudEndure Migration), see [What Is AWS Application Migration Service](https://docs.aws.amazon.com/mgn/latest/ug/what-is-application-migration-service.html)?

For more information about [managed databases on AWS](https://docs.aws.amazon.com/wellarchitected/latest/framework/perf-db.html), see Database

For more information about MemoryDB, see [What Is MemoryDB for Redis](https://docs.aws.amazon.com/memorydb/latest/devguide/what-is-memorydb-for-redis.html)?

For more information about resilience in ElastiCache for Redis, see Resilience in [Amazon ElastiCache](https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/disaster-recovery-resiliency.html)

For more information about how to choose between [MemoryDB and ElastiCache, see Related Services](https://docs.aws.amazon.com/memorydb/latest/devguide/related-services-choose-between-memorydb-and-redis.html)

For more information about durability and [consistency in MemoryDB, see Consistency](https://docs.aws.amazon.com/memorydb/latest/devguide/consistency.html)