AWS CERTIFIED SOLUTION ARCHITECT PROFESSIONAL SAP-C02

Mock Examination

DILIP BAVISKAR
Baviskar.dilip@gmail.com

AWS SAP-C02 Examination 01 Q & A

1. Which AWS Transit Gateway feature facilitates branch connectivity through native integration of SD-WAN network virtual appliances?

   A. Which AWS Transit Gateway feature facilitates branch connectivity through native integration of SD-WAN network virtual appliances?
   B. AWS Transit Gateway Peering
   C. AWS Transit Gateway VGW attachments
   D. AWS Transit Gateway Connect
   E. AWS Transit Gateway VPN connections

   Answer Key: B

   ### Explanation:

   Transit Gateway Peering allows connecting VPCs in different regions. A Transit Gateway attachment attaches a specific AZ in a VPC to the Transit Gateway. Transit Gateway VPN connections are used to connect your on prem to a Transit Gateway. Transit Gateway Connect is a feature that simplifies branch connectivity via software defined WAN virtual appliances.

   Reference: https://docs.aws.amazon.com/config/latest/developerguide/recording-managed-instance-inventory.html

2. You need to see network traffic from EC2 instances in your VPC for deep packet inspection. You cannot install any new software on the EC2 instances you want to monitor. Which solution would you choose?
   A. Turn on VPC logging for the entire VPC.
   B. Turn on VPC logging only for the ENIs that require deep packet inspection.
   C. Set up VPC traffic mirroring on the EC2 instances that require deep packet inspection and send those packets to a target EC2 instance for inspection.
   D. Turn on VPC logging only for the ENIs that require deep packet inspection and configure VPC logging to log the entire contents of the packet.

   Answer Key: C

   Explanation:

   VPC Flow Logs do not log network packet contents, only the packet meta-data. Traffic Mirroring is an Amazon VPC feature that you can use to copy network traffic from the elastic network interface of an Amazon EC2 instance. You can then send the traffic to out-of-band security and monitoring appliances for content inspection.

3. How can you record Software Configuration for Managed Instances? Select all that apply.
   A. Turn on recording for the managed instance inventory resource type in AWS Config.
   B. Choose the AWS managed Config rule to record software changes.
   C. Config does not record software configuration changes.

D. Configure EC2 and on-premises servers as managed instances in AWS Systems Manager.
E. Initiate collection of software inventory from your managed instances using the Systems Manager Inventory capability.

Select 3 answers

Explanation:

System manager is required to collect software inventory. Config will then be able to record the changes to the EC2 instances or on prem servers. Config can also be used with Config rules to specify if changes are compliant or non-compliant.
Reference:
https://docs.aws.amazon.com/config/latest/developerguide/recording-managed-instance-inventory.html

4. You are preparing to use Control Tower to create a landing zone. What must you do before you can begin? Choose any that apply.
   A. Disable trusted access for AWS Config in your AWS organization.
   B. Move all member AWS accounts out of the organization and delete the organization.
   C. Enable trusted access for AWS Config in your organization.
   D. Disable trusted access for AWS CloudTrail in your AWS organization.

   Explanation:

   Before Control Tower can create a landing zone, if you already have an AWS organization, trusted access must be disabled for both AWS Config and AWS CloudTrail.

   Reference: https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html

5. You are configuring your public DNS to point to your CloudFront distribution. The domain is example.com.
   What type of DNS RR record would you use?
   A. PTR
   B. A
   C. CNAME
   D. Alias

   Explanation:

   Example.com is an apex record. A CNAME (canonical name record) cannot be used for an apex record. You can, however, use an Alias record.

   Reference: https://aws.amazon.com/cloudfront/faqs/?nc=sn&loc=5&dn=2

6. You disable Service Control Policies in the root account. What will be the effect on the organization?

A. All SCP are automatically detached from all entities in that root. If you reenable Service Control policies all the Service Control policies will be in affect again.
B. All SCP are automatically detached from all entities in that root. If you reenable Service Control policies, all Service Control Policy attachments are lost. You may manually reattach them.

C. All SCP are automatically detached from all entities in that root. All Service Control policies are deleted. If you reenable Service Control policies, the default FullAWSAccess policy will be attached to the root. You will then need to create new Service Control Policies and attach them to the appropriate entities.

D. All SCP are automatically detached from all entities in that root. If you reenable Service Control policies, the default FullAWSAccess policy will be attached to the root. All Service Control Policy attachments are lost. You may manually reattach them.

Explanation:

Reference:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_enable-disable.html

7. What are the recommended configuration settings for CloudTrail? Choose all that apply.
   A. Create a trail that monitors all regions.
   B. Create a trail that monitors only the regions that the organization uses.
   C. Configure CloudTrail to send an SNS message whenever there is a root login.
   D. Place all Organization CloudTrail logs in a separate AWS log account and centralized S3 bucket.
   E. Place the organization log files in a centralized bucket for each account.
   F. Turn on log file validation and configure log files to be encrypted.

Select 3 answers

Explanation:

AWS best practices recommend monitoring all regions regardless of whether they are used by the organization. Log files should be aggregated into a centralized S3 bucket in an account created specifically for log files. Log files should also be validated and encrypted. You cannot configure CloudTrail to send notifications when a specific API call is made. Keeping CloudTrail logs in the account that created them is not secure or efficient.

Reference:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html

8. How can an AWS Account be moved out of an AWS Organization?
   A. An AWS account cannot be moved out of an AWS Organization.

B. Only an administrator of the master account can remove an AWS account from an AWS Organization.
C. Only an administrator of the member account can remove an AWS Account from an AWS Organization.
D. Either an administrator from the AWS Organization master account or an administrator of the member account can remove an account out of the AWS Organization.

Explanation:

Either an administrator from the AWS Organization master account or an administrator of the member account can remove an account out of the AWS Organization. An AWS member account can be moved out of an organization by the organization administrators or an administrator of the AWS account. The member account administrator must have permission to remove the AWS account from the organization.

Reference: https://aws.amazon.com/organizations/faqs/

9. Which method below is a best practice detective control, and can send a notification if root user access keys exist?
   A. Use AWS Config iam-root-access-key-check compliance rule configured with remediation to notify via SNS.
   B. Write a script that checks for root use access key and, if found, publishes to an SNS topic that sends notifications.
   C. Send CloudTrail logs to CloudWatch and configure a filter if the root user creates access keys.
   D. Use and SCP that denies API calls to create root user access keys.

   Explanation:

   AWS Config is used for AWS Organization detective controls and AWS has created an AWS managed rule specifically for the purpose if monitoring if root user access keys exist. The rule is triggered every 24 hours. While other answers could work, they would be more complex and unnecessary.

   Reference: https://docs.aws.amazon.com/config/latest/developerguide/iam-root-access-key-check.html

10. Which of the following features are available for AWS Global Accelerator? Choose all that apply.
   A. Associate static IPs to regional AWS resources or endpoints.
   B. Move endpoints between Availability Zones or Regions.
   C. Control traffic to specific regions by using a traffic dial.
   D. Assign weights to different endpoints to control the proportion of traffic to each.
   E. All choices are correct.

   Explanation:

   AWS Global Accelerator is a networking service that helps you improve the availability and performance of the applications that you offer to your global users. AWS Global Accelerator is easy to set up, configure, and manage. It provides static IP addresses that provide a fixed entry point to your applications and eliminate the complexity of managing specific IP addresses for different AWS Regions and Availability Zones. AWS Global Accelerator always routes user traffic to the optimal endpoint based on performance, reacting instantly to changes in application health, your user's location, and policies that you configure. You can test the performance benefits from your location with a speed comparison tool. Like other AWS services, AWS Global Accelerator is a self-service, pay-per-use offering, requiring no long-term commitments or minimum fees.

Reference: https://aws.amazon.com/global-accelerator/faqs/

11. You are the administrator of your company's RedShift Cluster. At times you need to resize the cluster due to increased demand. RedShift needs to respond to these changes in demand quickly. Which is the correct solution?
    A. Use classic resize to change the number of nodes or the node size.
    B. Query the data in S3 using Amazon Redshift Spectrum.
    C. Perform a restore to create a new cluster when demand is high.
    D. Use Amazon Redshift Elastic Resize.

    Explanation:

    Amazon Redshift Elastic Resize can resize the cluster in 15 minutes by adding nodes.

    Reference: https://aws.amazon.com/blogs/big-data/scale-your-amazon-redshift-clusters-up-and-down-in-minutes-to-get-the-performance-you-need-when-you-need-it/

12. Where does AWS backup store backups?
    A. EBS volumes
    B. S3 bucket
    C. EFS volumes
    D. Backup vault

    Explanation: AWS Backup uses a Backup Vault for storage.

13. You have a requirement for a transactional relational DB. The load on the DB changes often and is sometimes non-existent. The solution must auto scale and require little if any management overhead. Which solution would you choose?
    A. Amazon Aurora Serverless
    B. Amazon Red Shift with Autoscaling
    C. Amazon Aurora Auto Scaling with replicas
    D. Amazon MySQL RDS with read replicas

    Explanation:

    Amazon Aurora Serverless scales quickly without you having to manage database capacity. You only pay for when the resource is being used.

    Reference: https://aws.amazon.com/rds/aurora/serverless/

14. You require your AWS application to connect to S3 without traversing the Internet. You do not require access from multiple VPCs on premises or S3 resources in a

different region. You must use the most cost-effective method. Which resource would you choose?

A. An S3 Gateway Endpoint
B. An S3 Interface Endpoint
C. An S3 Access Point
D. AWS Global Accelerator

Explanation:

Gateway Endpoints do not allow access from on premises, other regions, or other VPCs. They are also free.

Reference: https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

15. There are multiple update behaviours that may happen when updating a CloudFormation Stack. Select the update behaviours from the list below.

A. Update with no interruption
B. Update with some interruption
C. Replacement
D. Total stack rebuilds

Select 2 answers
Explanation: There is no update behaviour called total stack rebuild.
Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-update-behaviors.html

A. You are creating a HPC cluster. Inter-node latency needs to be kept to a minimum even if an infrastructure failure brings down multiple nodes. Choose a suitable solution.

A. Use a cluster placement group.
B. Use a partition placement group.
C. Use a spread placement group.
D. Use only nodes with high-speed networking.

Explanation:
A cluster placement group offers the lowest inter-node latency and does not span multiple AZs.

Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

16. You have created an AWS Backup Vault. You want to use the Vault Lock feature. Which of the following should be checked to make sure that previously created backup jobs do not fail?

A. Export all backup jobs created prior to creating the backup vault lock. After the backup vault lock is configured, import the previous backup jobs.

B. Make sure that all the retention periods for previous backup jobs meet the vault locks' retention periods. Any backup jobs that do not meet the vault lock retention period settings will fail.
C. AWS backup note in the backup audit logs any backup jobs that do not meet the vault lock retention periods settings, although all previous backup jobs will succeed.
D. The creation of the vault lock feature will not succeed unless all previous backup jobs meet the acceptable retention period.

Explanation:
Reference: https://aws.amazon.com/backup/faqs/?nc=sn&loc=6&refid=d61c61a5-6875-45ba-ab44-554e174e41b5

17. As a solutions architect for your company, you are asked to deploy a service using microservices. The requirements are that start-up time for the microservices needs to be minimal. The microservices should also be able to run on other operating systems. There may be different versions of the programming languages used across microservices. What deployment option would you select?
    A. EC2 Virtual Machines
    B. Virtual machines running on VMware Cloud on AWS
    C. Docker containers
    D. Bare metal running your hyper-visor of choice
    Explanation:
    The solution that provides the fastest start-up times, platform independence, and isolation between various versions of the OS or run time platform are containers. This is because containers only virtualize the OS kernel. All other resource are contained within the container image.
18. You want to provide end users with predefined automated infrastructure builds as an MSP/MSO. Which resource would best be used to provide the service?
    A. Service Catalog
    B. Stack Sets
    C. CloudFormation Templates
    D. Lambda functions
    Explanation:
    While any service that automates infrastructure builds can be used, the Service Catalog is the best tool as it provides all the features that are required to build a portfolio of products with usage constraints that can easily be published to other AWS accounts.
19. Each month you provision new Windows and Linux custom AMI with the latest patches. You need a centralized location to store the AMI IDs in each region. The solution must not add additional cost. The solution should also make it easy to find or list all Windows or Linux AMIs. Which solution would fulfil the requirements?
    A. Store the current company custom AMIs in S3. Use the CSV format. Use Amazon Athena to search the list for Windows or Linux AMIs.
    B. Store the current company AMIs in Systems Manager Parameter Store. Store all Windows AMIs under company-amis/windows/ and all Linux AMIs under company-amis/Linux.
    C. Store the current company custom AMIs in DynamoDB table with an attribute for OS. Query the table using DynamoDB query command.

D. Use the command such as “aws ssm get-parameters --names /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 --region us-east-1” to find the latest AMI.

Explanation:
All the above answers would work except querying -names/aws/service/ami-amazon-linux etc. That would find the current Amazon Linux AMI not a custom company AMI. The correct answer is to use the AWS Systems Manager Parameter Store because that option is free.

20. You want to update an application on Windows Server using AWS Systems Manager. The update is not issued by Microsoft. What method could you use to update the application?
    A. AWS Systems Manager Patch Manager
    B. AWS Systems Manager Run command
    C. AWS Systems Manager Application Manager
    D. AWS Systems Manager Compliance Manager
    E. AWS Systems Manager State Manager

    Explanation:
    AWS System Manager Patch Manager can only update using Microsoft issued updates. AWS Systems Manager Run command can be used to update applications and is also used by AWS State Manager to install required updates.
    Reference: https://docs.aws.amazon.com/systems-manager/latest/userguide/distributor-working-with-packages-deploy.html

21. Which DR architecture provides a zero or near zero RTO/RPO objective?
    A. Backup and restore
    B. Pilot light
    C. Warm standby
    D. Multi-site active/active

    Explanation:
    All of the other options except multi-site active/active have an RTO with some recovery or down time.

    Reference: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/

22. One of the IT administrators in your company has brought up two EC2 instances that are being used as file servers. Network throughput testing to and from the nodes has shown that network throughput is quite low. The administrator used t2.2xlarge instance types to keep cost down. As your company’s solution architect, you are asked to solve the problem. How can you increase network throughput?
    A. Change to a more powerful instance type. Network throughput is limited by the instance type. t2.2xlarge offers moderate network performance.
    B. Add additional ENIs.
    C. Configure the ENI for advanced networking.
    D. Configure giant frames.

    Explanation:

Network throughput along with other areas of performance are throttled at the hypervisor level on AWS EC2. You must use an instance type and size that supports the network throughput your use case requires. Adding ENIs will not increase network throughput.

23. You need to verify that a target account meets certain requirements before your Stack Sets begin operations on the account. Which feature or services would you use? Choose all that apply.
    A. A target account gate
    B. AWS Lambda Function
    C. CodePipeline
    D. Amazon Simple Workflow Service
    Explanation:
    Reference:
    https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-account-gating.html
24. Which AWS service and TCP protocol provide multi-region HA with two static IP addresses using edge locations to enter the AWS private network?
    A. Transit Gateway and multicast
    B. Transit Gateway and anycast
    C. AWS Global Accelerator and multicast
    D. AWS Global Accelerator and anycast
    Explanation: Reference: https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works.html

25. Your company is using DynamoDB for its gaming platform for scores and leader boards. The company has players for their games worldwide. You require microsecond read latency for local reads to DynamoDB. Which solution would provide the best performance and be the most efficient to setup?
    A. Build a multi-master DynamoDB solution using regions in SA, AP, US, and EU. Use S3 and Lambda to store and write DynamoDB writes to the other regions.
    B. Build a multi-master DynamoDB solution using Global Tables in multiple AWS regions. Use DAX (DynamoDB Accelerator) as in inline cache to reduce read latency.
    C. Build a multi-master DynamoDB solution using Global Tables in multiple AWS regions. Use ElastiCache with Redis to build a caching layer in each region where you have DynamoDB.
    D. Build a multi-master DynamoDB solution using Global Tables in multiple AWS regions. Use DAX (DynamoDB Accelerator) to build a side-line cache to reduce read latency.

    Explanation:
    The simplest solution would be to use DynamoDB with Global Tables as this creates a multi-master model without any coding on your part. DynamoDB latency is usually single-digit milliseconds. DAX reduces latency to microseconds and is an inline cache. It cannot be used as a side-line cache.

26. You have been asked to come up with a solution to store RDS credentials in a secure manner. The credentials must be rotated monthly. What would be the most efficient way to accomplish this?
    A. Use the AWS System Manager parameter store along with the AWS KMS to store encrypted credentials and create an AWS Lambda function to rotate the credentials once per month.
    B. Store the encrypted credentials in S3. Tightly control access to the credentials in S3 and the KMS key used to decrypt the credentials. Create an AWS Lambda function to rotate the key once per month.
    C. Store the credentials on an EBS volume in a secure VPC on a Windows Server with encryption turned on for the folder where the credentials are stored. Tightly control access via NTFS to access the credentials.
    D. Store the credentials in Secrets Manager. Configure the Lambda function for RDS to rotate the keys once per month.

    Explanation:

    Secrets Manager is designed exactly for the required need. AWS has created a Lambda function for rotating the credentials. Secrets Manager also has the ability to create its own passwords.
27. You want to restrict CloudFront origin access so that all requests must go through CloudFront and cannot go directly to a S3 URL. How would you accomplish this? Choose all that apply.
    A. On the permissions tab for the S3 bucket, select “Only allow access from CloudFront.”
    B. Use an ACL to only allow access from CloudFront.
    C. Create and origin access identity and associate it with your CloudFront distribution.
    D. Create a S3 bucket policy that only allows access to the origin access identity.

    Explanation:

    An origin access identity (OAI) is a special type of CloudFront user that is used to restrict access to an S3 origin and force access to the S3 bucket to CloudFront.
28. You want to test for failure pathways using chaos engineering. You need to include high CPU and memory utilization on EC2 instances in your AWS environment. What tool could you use to achieve this? Choose all that apply.
    A. AWS EC2 Auto Recovery
    B. AWS Well Architected Tool
    C. AWS Fault Injection Simulator
    D. AWS SSM agent

    Explanation:

    The AWS Fault injection simulator is designed for Chaos Engineering to inject faults into your service to improve performance and resiliency among other things. The SSM agent is required to simulate high CPU and memory utilization. AWS EC2 Auto Recovery can bring up an EC2 instance on a new house should the original host fail. The Well Architected tool is a question-and-answer tool that will gauge how well you are meeting AWS Well Architected best practices.
    Reference: https://aws.amazon.com/fis/faqs/
29. When creating parameters in a CloudFormation stack, which parameter type is NOT supported?
    A. String
    B. Boolean

C. AWS-Specific Parameter Types
D. SSM Parameter Types
E. CommaDelimitedList

Explanation:
Boolean, true/false datatypes are not supported.
Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html#parameters-section-structure-properties-type

30. You want to protect your MySQL RDS database by having a copy of the DB in another region. Choose the most efficient solutions to achieve this.
A. Create a multi-region MySQL RDS.
B. Write an AWS Lambda function to copy the RDS automated backup each day to another region.
C. Create a RDS Read Replica in another region.
D. Copy manual snapshots of the RDS instance to another region.

Explanation:
AWS does not provide multi-region MySQL RDS. Although you can copy an automated backup to another region, using AWS Lambda to automate the process is much more efficient. Read Replicas can be promoted to a master as a last resort.
Reference: https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/

31. As the Elasticsearch administrator for you company, you need to migrate to the AWS OpenSearch service. What steps would you take? Choose all that apply.
A. Detach the EBS volume holding your Elasticsearch domain data.
B. Snapshot the existing Elastisearch cluster.
C. Attach the EBS volume to the new Opensearch server for a new OpenSearch Domain.
D. Create a new OpenSearch Service domain and perform a restore using the snapshot.

Explanation:
OpenSearch is a managed service. You cannot detach and attach EBS volumes. Snapshot and restore are the recommended method provided by AWS.
Reference: https://aws.amazon.com/opensearch-service/faqs/

32. Your company is migrating to AWS. There is a requirement for a database that offers a centralized and trusted authority to maintain a scalable, immutable, and cryptographically verifiable record of transactions. Which DB type would you choose?
- Time Series
- Relational
- NoSQL
- Ledger

Explanation:
Reference: https://aws.amazon.com/products/databases/

33. You are looking to quickly relocate workloads running on premises to AWS. Which of the following is classified as a relocation?

- Migrating an on-premises MS SQL database to MS SQL running in AWS RDS.
- Migrating an on-premises MS SQL dataset to run on EC2.
- Migrating a monolithic application to AWS using micro services.
- Migrating VMware virtual machines to VMware Cloud on AWS.

Explanation:
Moving a VMware VM to VMware Cloud on AWS is a simple relocation since you are running the same VM only in a different location.

34. You are using AWS DMS for the migration of DB. You need to keep the downtime of your DB migration to a minimum. Your migration does not need to keep both source and target DB running simultaneously for writes. Which cutover strategy meets these requirements?
    - Active/active
    - Flash-cut migration
    - Offline Migration
    - None of provided solutions

    Explanation:
    Reference: https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-migration/cut-over.html

35. Your company uses AWS S3 to store company data and also as storage for your customers data The security team is very concerned over how to track IP, sensitive information such as credit card number. It is also concerned about storage of credentials and private keys. They want a service that monitors S3 data and its use and reports when it finds sensitive information or any access that is unusual. Which AWS service offers these features?
    - AWS Athena
    - AWS Security Hub
    - AWS Config
    - AWS Macie

    Explanation:
    AWS Macie is designed specifically for monitoring S3 data and usage patterns and provides all the required features.
    Reference: https://aws.amazon.com/macie/
36. You are using The AWS Discovery Connector and want to disable auto-upgrades. How would you configure this? Select any correct answers.
    - There is no configuration option to stop auto-upgrades.
    - There is no auto-upgrade option. The connector must be upgraded manually.
    - Go to Error! Hyperlink reference not valid.> for your Discovery Connector appliance.
    - Disable Auto-Upgrade.

      Explanation:
      Reference: https://docs.aws.amazon.com/application-discovery/latest/userguide/configure-connector.html

37. During which stage of an AWS migration does AWS recommend you build a Landing Zone?
    - Mobilize
    - Migrate and modernize
    - Assess
    - Pre-Assessment

    Explanation:
    Reference: https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-migration/mobilize-phase.html

38. You have a large relational database to migrate to AWS. You are using the AWS DMS. What can you do to speed up the migration?
    - Turn off backups and transaction logging.
    - Turn off multi-AZ until the data is transferred.
    - Use multiple tasks.
    - Optimize change processing.
    - All answers are correct.

    Explanation:
    Reference:
    https://docs.aws.amazon.com/dms/latest/userguide/CHAP_BestPractices.html#CHAP_BestPractices.Performance

39. You have a large relational database to migrate to AWS. You are using the AWS DMS. What can you do to speed up the migration?
    - Turn off backups and transaction logging.
    - Turn off Multi-AZ until the data is transferred.
    - Use multiple tasks.
    - Optimize change processing.
    - All answers are correct.

    - Explanation:
    - Reference:
      https://docs.aws.amazon.com/dms/latest/userguide/CHAP_BestPractices.html#CHAP_BestPractices.Performance

40. The company you are migrating to AWS has many databases. Most of the databases are hosted by relational database software such as Oracle, MS SQL, etc. Upon inspection, you find that approximately 50% of the databases are flat tables that require no relational capabilities. The company wants to move these databases to AWS and utilize a NoSQL database engine. For some of the tables, the load varies drastically and therefore it would be hard to specify lower and upper capacity limits. You require a database engine with low latency and no limit on database size or number of items in the table. The database engine must also scale as needed. Select the best option. The option should also be a totally managed solution.
    - AWS Document DB
    - AWS KeySpaces
    - AWS DynamoDB with on-demand scaling
    - AWS DynamoDB with autoscaling

Explanation:
While DocumentDB (Mongo compatible) and KeySpaces (Cassandra) are flat NoSQL databases, they do not offer all the requirements such as no limits in storage size. DynamoDB offers this capability and along with "on-demand" scaling will handle erratic or nonpredictable demand.
Reference: https://aws.amazon.com/blogs/aws/amazon-dynamodb-on-demand-no-capacity-planning-and-pay-per-request-pricing/

41. You are managing a complex migration that includes many workloads. You are looking for a tool that will help manage the migration. The tool should be able to import CMDB information to build an IT portfolio, integrate with other migration tools for migration status information, and allow the grouping of servers of related workloads. Which tool would you choose?

    - AWS Migration Hub
    - Application Migration Service
    - AWS DMS
    - AWS SCT

    Explanation:
    AWS Migration Hub offers all of the required features. It allows import of CMDB (configuration management databases), along with discovery of your IT portfolio using the AWS Discovery Agent of AWS Discovery Connector (for vSphere). It also integrates with other migration services such as DMS for migration status.

42. You are migrating data stored on premises to AWS. You have 2 petabytes of data to transfer. You have a 10 Gb/s WAN link with 30% overhead. You require the transfer to be complete in 14 days. What is the most cost-effective solution?
    - AWS Snowball Edge
    - AWS Snowcone
    - AWS Storage Gateway
    - AWS Snowmobile

    Explanation:
    Transferring the data over the network would take more than 14 days using a 10Gb/s WAN link with 30% overhead. Using multiple Snowball Edge devices will work and the data will be loaded in AWS within 13 days. You can also expedite shipping to shorten the shipping time for Snowball devices. Snowcone cannot handle that much data and Snowmobile is overkill and expensive.

43. You are planning a migration for your company to AWS. Some of the workloads use unsupported operating systems. Which classifications for migration would these workloads belong to? Choose all correct answers.
    - Retain
    - Rehost
    - Relocate
    - Re-purchase
    - Re-platform

Explanation:
You could retain the workload on premises, re-purchase a product that runs in AWS, or re-platform using a different product. You cannot rehost or relocate since the OS is not supported in AWS.
Reference: https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/

44. The company you work for uses Lambda extensively. Some of the developers are just out of college and therefore inexperienced. The company has created a budget for running Lambda functions based on number of function calls, hardware allocated, and function run time. The cost of running the Lambda functions is quite a bit higher than budgeted. Upon closer inspection, you find that at times functions that are supposed to run in a few seconds are running for 15 minutes. Based on your findings how your you remedy the situation?

- Adjust the hardware spec for the functions that are running for 15 minutes.
- Have the developer use a different programming language when writing functions.
- Delete the Lambda functions and run them on EC2 instead.
- Have the developers set TTLs for all functions they create based on expected run time.

Explanation:
The problem is most likely that the functions are hanging due to poor coding by some of the new developers. The easiest way to control cost is to put a TTL on all functions. If a function hangs and runs past its usual run time it will be automatically terminated, therefore abrogating the cost of a hung function running for the max Lambda run time of 15 minutes.

45. Your company provides a service for storing and managing photographs in a Catalog. The service is using m4.xlarge instance type. The servers are auto scaled. Metrics show that the instances are using the underlying hardware efficiently. You are looking for ways to reduce the cost of running these instances. What would be an easy way to accomplish this?

- Change the instance type to m4.large.
- Use less expensive storage.
- Upgrade to the latest generation m instance type.
- Have autoscaling terminate unneeded instances instead of turning them off.
- Make sure the instances are up to date on patches.

Explanation:
The only change that you can make above that would guarantee a cost reduction without affecting performance would be to upgrade to the newest instance type. Each new generation of instances within an instance family increases the performance to price ratio.

46. Which of the below are true for AWS-Generated Cost Allocation Tags? Select all that apply.
    - The tags will show up in Tag Editor.
    - The tags must be activated.
    - The tags are available in the Billing and Cost Management console.
    - The tags count toward your account quota.
    - The tags do not count toward your account quota.

    Explanation:
    Reference: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/aws-tags.html

47. You require the most comprehensive cost and usage data for your AWS account. What would you use?
    AWS Cost Explorer
    AWS bill
    AWS Cost and Usage reports
    Billing Conductor

    Explanation:
    Reference: https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html

48. In the last meeting of the Cloud Center of Excellence, an issue was raised regarding the cost of EC2 instances. You were asked to find a way to save the maximum amount for short-term use of flexible EC2 workloads. How would you achieve this based on AWS best practices?

    - Use Reserved Instances.
    - Use Scheduled Reserved Instances.
    - Use On Demand.
    - Use Spot Instances and select the cheapest Availability Zone.
    - Use spot and be flexible about instance types and Availability Zones.

    Explanation:
    Spot is the least expensive pricing model for short-term flexible workloads. In order to achieve the lowest spot cost and the least disruption due to spot instance termination requests, you should use as many Availability Zones and Instance types as you can.
    Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-best-practices.html

49. Your company uses DynamoDB. The DynamoDB load is predictable and varies gradually over time. The company is looking to cut costs for using DynamoDB. What method would save the maximum amount?
    - DynamoDB On-Demand scaling
    - DynamoDB Auto Scaling
    - DynamoDB reservations
    - Use DynamoDB Transactions

    Explanation:

DynamoDB Transactions is about ACID compliance. It is not a method of cutting costs. Using DynamoDB with Auto Scaling and purchasing a reservation based on your minimum expected use would offer the most savings.
Reference: https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-reservation-models/amazon-dynamodb-reservations.html

50. You are running an AWS EMR cluster every day at the same time. You cannot easily change the time the cluster is needed. You are running Linux on the cluster. You may need to change the AZ or instance size. What EC2 purchasing option would fulfill the requirements and be the least expensive?

    - EC2 Savings Plan
    - EC2 Standard RI
    - EC2 Convertible RI
    - Spot

    Explanation:
    EC2 Savings plan cannot be used for EMR. Although spot may be less expensive, the cluster is needed the same time every day and the requirement states that this cannot be easily changed. RI can be used and since you only need to change AZ or instance size, the largest savings would be from Standard RI.
    Reference: https://aws.amazon.com/ec2/pricing/reserved-instances/

51. Your company is spending a lot on S3 storage. The company is made up of many AWS accounts, each operating separately. What could you do to help lower the cost/GB for S3 storage?

    - Compress the file before storing it in S3.
    - Create and AWS Organization and invite all the accounts to join.
    - Utilize multi-part uploads.
    - Set up a lifecycle management policy for all S3 buckets.
    - Access the S3 data over an endpoint.

    Explanation:
    While many of the answers might reduce overall S3 costs, the goal is to lower cost/GB for storage. If you create an AWS Organization, all S3 use from all accounts in the organization will be totaled and used to apply larger volume discounts than could be achieved by any individual account.

52. Your company is spending much more than expected on storage. You notice that the costs are mostly associated with EBS snapshots. Most of the snapshots are no longer needed because they are old. What would be the most cost-effective way to manage the creation of snapshots and deleting snapshots when they are no longer needed?

    - Use Amazon Data Lifecycle Manager.
    - Use Lambda to write housekeeping scripts.
    - Run python housekeeping scripts on EC2 and run then on a CRON schedule.

- Set up the EBS snapshots to autodelete after the time frame where they are no longer of use.

Explanation:
Amazon Data Lifecycle Manager is free to use and can automate both the creation and deletion of EBS snapshots. Lambda is not free nor is EC2, therefore the other solutions would not be as cost effective.
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html

53. Your company is using AWS Storage Gateway as a file gateway. How can you control access for NFS shares? Select all that apply.
    - NFS permissions
    - Client IP address
    - Username and password
    - POSIX permissions

    Select 2 answers
    Explanation:
    Reference:
    https://docs.aws.amazon.com/filegateway/latest/files3/GettingStartedCreateFileShare.html

54. The company you work for has a service that allows users to upload files for collaboration with other users. Currently the files are stored in EFS. You want to lower the cost of storage and want the files to be available to users worldwide and have extremely high durability. The maximum file size the service supports is 25GB. What solution would you implement to achieve these requirements?

    - Store the files in an Aurora Global DB.
    - Store the files in multiple EFS targets in various regions using DataSync to keep the targets in sync.
    - Store the file in S3.
    - Store the files in S3 and implement multi-part upload

    Explanation:
    Objects in S3 are available worldwide by their very nature. S3 storage costs less than EFS. The maximum put in S3 is 5GB. Since the maximum file size is 25GB, a multipart upload will be required.
    Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/upload-objects.html

55. The company you work for is having issues with the reliability of the services it offers both internally and to the public. The reliability issues are causing harm both with internal stakeholders and the company's customer base. You need to address this issue by building services with better high availability and fault tolerance. What tool would best help you to find and address areas in your architecture to improve reliability in case of failure of a resource or service?

- Autoscaling
- Load balancer
- AWS Fault Injection Simulator
- AWS Trusted Advisor
- AWS Compute Optimizer

Explanation:
A tool that can uncover failure pathways is needed. The tool that AWS provides is AWS Fault Injection Simulator. While all of the other answers may help improve reliability, none will specifically allow you to find out what will happen to a workload when specific resources or services fail.
Reference: https://aws.amazon.com/fis/

56. Your company manufactures sports apparel and stands up hundreds of web sites per year for various sporting events that the company sponsors. The website developers usually develop 2-3 versions of each website with different themes. A marketing manager tests the various versions and then, after deciding which is preferred, asks the IT department to stand the website up. The process is laborious and time consuming because the marketing manager needs help bringing up the websites to test them out and then, after deciding which is to be used, needs to wait for help from the IT team to bring the website on line. You need to find a better solution that allows the marketing manager to not require any help from IT for any of the processes. Is there a way to accomplish this?

- Have the marketing manager use OpsWorks.
- Use CloudFormation templates.
- Use Stack Sets.
- Use Elastic Beanstalk.
- Use Docker containers.

Explanation:
All of the solutions except Elastic Beanstalk require technical expertise to bring the websites online for either testing or production. Elastic Beanstalk is an AWS service that can create front-end or worker-tier environments without any systems knowledge with just a few keystrokes.

57. You are looking for ways to reduce the cost of running DynamoDB for you company. For most DynamoDB tables, you know the minimum monthly usage. What can you do to reduce the cost of running DynamoDB in specific regions without affecting performance?

- Move the DynamoDB tables to a less expensive region.
- Lower the provisioned throughput for read and write access units.
- Set up a DAX (DynamoDB Accelerator) for tables that require low latency access.
- Purchase Reserved Capacity to cover minimum known usage in each region where you are running DynamoDB.
- Purchase Reserved Capacity to cover minimum known usage based on the total throughput for all regions to get the largest bulk discount.

Explanation:
DynamoDB reservations can save money if you know the minimum required read and write commit units. Reservations are limited to a specific region.

58. You would like to increase performance of the companies EFS File Systems. Which options below would increase performance? Choose all that apply.

Asynchronous writes
Synchronous writes
Larger average IO size
NFSv4.1 if supported by client OS
Smaller average IO size

Explanation:
Each file operation has latency. Larger IO size amortized the latency over more data. Synchronous write increase latency since it takes a round trip between client and EFS so it is slower than asynchronous, which does not require the round trip. For clients that support the NFSv4.1 small file read operations provides better performance.
Reference: https://docs.aws.amazon.com/efs/latest/ug/performance-tips.html

59. Your company manually tracks software license usage. As the company grows in size, they are looking for a way to automate managing software licenses. You are looking at using AWS License Manager. Which features below does License Manager support?

- Track licenses based on vCPUs, physical cores, sockets, and number of instances.
- Track license use on premises.
- Only works at the AWS account level.
- Work with AWS Organizations.
- Does not discover existing licenses.

Explanation:
AWS License Manager tracks licenses based on vCPUs, physical cores, sockets, and number of instances. It also works at the AWS Organization level and can discover existing licenses.
Reference: https://aws.amazon.com/license-manager/features/

60. You are setting up containers to run microservices in ECS. You need to run multiple instantiations of the task on a host. What should you do?
- Use port triggering.
- Use NAT.
- Use host mode.
- Use bridge mode.

Explanation:
There are two network modes when using ECS: host mode and bridge mode. Using host mode networking of the container is tied directly to the underlying host. Using bridge mode with dynamic mapping allows for multiple instantiations of a task on the same node.

Reference:
https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/bestpracticesguide.pdf

61. You are troubleshooting an issue concerning EBS IOPs performance. The EBS volume is using gp2. You find that IOPs requirements are increasing in a nonlinear way compared to disk size. You need to find a way to get more IOPs even though disk size it not increasing at the same rate. What would you do?

    - Use gp3 disk type.
    - Use Instance Storage.
    - Use provisioned IOPs.
    - Use an in-memory disk cache.

    Explanation:
    IOPs on gp type disks increase in a linear fashion as disk size increases. Provisioned IOPs would allow you to increase IOPs at a higher rate than disk size is increasing.

62. Your company uses AWS Redshift. They often run the same analytical workloads such as dash-boarding. You want to improve the query performance for these repeated workloads. Which solution would you choose?
    - Materialized views
    - Amazon Redshift Advisor
    - Elastic resize
    - Amazon Redshift data lake integration
    - Temporary tables

    Explanation:
    Reference: https://aws.amazon.com/blogs/big-data/top-10-performance-tuning-techniques-for-amazon-redshift/

63. Which type of mapping of Lambda functions to Kinesis Data Steams increases throughput?
    - Standard Iterator
    - Shard Iterator
    - Partition Iterator
    - Data stream consumer with enhanced fan out
    - Shared Iterator

    Explanation:
    There are two types of consumers that Lambda can use to process data in Kinesis Data Streams. A standard iterator. Standard iterators share read throughput with other consumers of the shard. A data stream consumer with enhanced fan out gets a dedicated connection to each shard that does not impact other applications reading from the same stream.
    Reference: https://docs.aws.amazon.com/lambda/latest/dg/with-kinesis.html

64. Your company is running a service with a web front end. You have noticed that application layer DDOS attacks are getting through to your EC2 front end web servers. What can you do to best mitigate these attacks?

    - Put an ELB NLB in front of your web servers and move your EC2 instances onto a private subnet.
    - Put an ELB ALB in front of your web servers and move your EC2 instances onto a private subnet.
    - Configure AWS Shield to block layer 7 application layer attacks.
    - Use WAF in front of your web servers. Configure a WebACL to control traffic to your web servers based on conditions. Change the WAF WebACL rules in near real time based on WAF metrics in CloudWatch.

      Explanation:
      WAF would provide a layer 7 firewall that can be reconfigured based on near real time log info sent to CloudWatch logs. You configure one or more conditions to create one or more rules in WebACLs. You can use Lambda functions to reconfigure the WebACLs based on the log files.

65. You have created a service catalog that your IT staff can self serve approved AWS environments. The security administrator has found out that the IT staff can create resources outside of using the service catalog. How can you allow the IT admins to launch products in the Service Catalog, while not giving them permissions to create any resources?

    - Create a role that has the permissions needed to launch the product in the Service Catalog and assign it to the product. Create roles that allow the IT admins to launch the needed products.
    - Use stack sets instead of the Service Catalog.
    - Configure the Service Catalog products with IAM groups that have permissions to build the resources in the product.
    - You cannot use the Service Catalog for self-service without giving the IT admins permissions to create all resources required by the product.

      Explanation:
      The solution is to assign a role to the product. It is also an AWS best practice

66. You are part of your company's network team. You would like to find ways to optimize the use of the company's transit gateways. Which design practices will improve your transit gateway implementations? Select all that apply.

    - If you use multiple transit gateways, use unique ASNs for each transit gateway.
    - If you use multiple transit gateways, use the same ASN for all transit gateways.
    - Use multiple transit gateways in each region.
    - Use a single transit gateway in each region.
    - Use security group referencing.

    Select 2 answers

Explanation:
Transit gateways are highly available within their region. A single transit gateway in each region using unique Autonomous System Numbers (ASN) is recommended.
Reference: https://docs.aws.amazon.com/vpc/latest/tgw/tgw-best-design-practices.html

67. Your company has a service that uses DynamoDB. The DynamoDB table is configured to use on-demand autoscaling. Every month the company has a flash sale that lasts 24 hours. The maximum read and write throughputs are configured correctly to handle the flash sale. During the flash sale, the latency of the DynamoDB is very high, causing services slowdowns. What could be the reason for the high latency? How would you troubleshoot the DynamoDB table to find out how to eliminate the latency issue?
    - Contact a member of your company's AWS support team and ask them to look at performance activity on the DynamoDB table to look for hot partitions/hot keys.
    - Switch to On-Demand scaling for the DynamoDB table.
    - Create a DAX (DynamoDB Accelerator) cluster for the DynamoDB table.
    - Create an ElastiCache cluster using Memcached.

    Explanation:
    Performance issues when scaling are usually caused by selecting inefficient partition keys that do not load the partitions equally and therefore do not spread write or read load properly across the partitions. When this happens, it is called "hot keys" or "hot partitions."

68. You are moving data currently stored in a relational database. You want to move this data to DynanoDB since it is a flat table and you would like to increase performance. The database requires ACID compliance. Which feature could you use to enable this requirement?

    - DynamoDB streams
    - Global tables
    - DynamoDB Transactions
    - PartiQL

    Explanation:
    Reference: https://aws.amazon.com/blogs/aws/new-amazon-dynamodb-transactions/

69. You are using Lambda functions that access an AWS VPC for Internet Access. Sometimes your functions lose Internet access or times out after connecting to the VPC. What could be causing these errors?
    - The Lambda function execution role is misconfigured and does not have sufficient permissions.
    - You should configure the Lambda function to have direct Internet access.
    - Lambda does not support packet fragmentation.
    - Make sure the VPC has a NAT gateway in a public subnet for outgoing Internet traffic and a route to the NAT GW in the private subnets.

Explanation:
The Lambda function execution role would not cause intermittent issues with Internet access nor would the NAT GW or routing. The issue is probably IP packet fragmentation with Lambda cannot handle. You would use the MTU and MSS settings to avoid fragmentation.
Reference: https://docs.aws.amazon.com/lambda/latest/dg/troubleshooting-networking.html

70. Your company is currently using Cognito to authenticate users of your service. The company has decided to make some advanced customizations to the user sign-on experience, such as post-authentication SNS messages. Which solution below can be used to meet the requirement?

- Specify the required code in the triggers configuration for the Cognito User Pool.
- Cognito does not offer a way to customize the user authentication experience.
- Use Lambda@edge to intercept the authentication request.
- Create a Lambda function. Attach a Lambda function resource policy that allows Cognito to invoke the function. Specify the Lambda function in the trigger configuration of the user pool.
- Create a Lambda function. Attach a Lambda function resource policy that allows Cognito to invoke the function. Specify the Lambda function in the UI Customization configuration of the user pool.

Explanation:
Reference: https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools-working-with-aws-lambda-triggers.html#cognito-user-pools-lambda-trigger-event-parameter-shared

71. Your company is currently using SSE-S3 to encrypt objects in an S3 bucket. The manager of the IT Security team determines that key use is not being logged. The manager also wants the key automatically rotated yearly. What solution would satisfy the requirements? The solution must work through the console and programmatically.

- Configure CloudTrail auditing of key use. Configure the KMS key to rotate.
- Use SSE-C. Use a new key each year.
- Use S3-CSE.
- Use SSE-KMS.

Explanation:
SSE-S3 is using the AWS managed regional S3 key. You cannot audit or rotate this key. SSE-C only works programmatically and there is no auto key rotation since you are providing the key when reading and writing to S3. CSE-S3 is client-side encryption, which again does not provide automatic encryption since it is client-side encryption. SSE-KMS uses a customer-managed key (CMK). A CMK belongs to your account and can be audited, automatically rotated yearly, and works both through the console and programmatically.

72. You are running a EMR cluster. Which metric could you use to find out if the cluster is running at reduced capacity?
    - RunMapTasks
    - IsIdle
    - MRUnhealthyNodes
    - HDFSUtilization
    - MRLostNodes

    Explanation:
    Reference:
    https://docs.aws.amazon.com/emr/latest/ManagementGuide/UsingEMR_ViewingMetrics.html
73. Your company uses the AWS KMS for encryption. The company needs an encryption key for use outside of AWS by users who cannot call the AWS KMS. What type of key would you create in the KMS?
    - The KMS only works if the requestor can access the AWS KMS.
    - Custom Key Store
    - Symmetrical key
    - Asymmetrical key
        - An external access key

        Explanation:
        If a client cannot access the AWS KMS, the public key from an asymmetrical key pair can be used to encrypt the data. The data can then be encrypted by the AWS KMS that has the private key.
        Reference:
        https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.htmln
74. You want to find a way to simplify IAM permissions to resources without having to specify IAM principles for each resource. What method could you use to accomplish this?
    - Use IAM groups to control access to resources.
    - Use IAM roles to control access to resources.
    - Use Tags and conditions to control access to all resources.
    - Use Tags and conditions to control access to all resources that say "Yes" in "Authorization based on tags."

    Explanation:
    Reference:
    https://docs.aws.amazon.com/IAM/latest/UserGuide/access_tags.html

AWS SAP-C02 Examination 02 Q&A

1. What AWS service will create a landing zone using AWS best practices?
   A. AWS Organizations
   B. AWS Well-Architected Tool
   C. AWS Trusted Advisor
   D. AWS Control Tower

   Answer Key: D

   Explanation:

   AWS Control Tower is an AWS Service that will automate the creation of a landing zone that includes a multi-account organization, core and custom OUs, and mandatory guardrails following AWS best practices.

   Reference: https://aws.amazon.com/controltower/?control-blogs.sort-by=item.additionalFields.createdDate&control-blogs.sort-order=desc

2. How can you control what AWS API calls AWS account root users can make?
   A. Attach an IAM policy to the root user that denies API calls that are not allowed.
   B. Attach an IAM policy to the root user that denies API calls that are not allowed, with the property –Include root=”true”.
   C. Make the AWS account a member account in an AWS organization and use SCPs to control API calls.
   D. Make the AWS account a member account in an AWS organization and use IAM policies to control API calls.

   Answer Key: C

   Explanation:

   Root user AWS API call permissions cannot be controlled via IAM because the root user is not an IAM security principle. Organization SCPs are not IAM permissions, and they control all users in the member accounts that they apply to.

3. You have been asked to set up DNS name resolution between your data center and an AWS VPC. You need the EC2 instances in the VPC to be able to resolve data center DNS names for example.com. You need a solution with low management overhead. Choose the best solution.
   A. Set up a DNS server on EC2. Create a conditional forwarder for example.com and point it to the DNS servers in your data center that is authoritative for example.com.
   B. Set up an AWS RT 53 resolver with an inbound endpoint for example.com that points to your data center DNS servers that are authoritative for example.com.

C. Set up an AWS RT 53 resolver with an outbound endpoint for example.com that points to your data center DNS servers that are authoritative for example.com.

D. Set up a domain in RT 53 for example.com and set up zone replication with a source of the on prem DNS server that is authoritative for example.com.

Answer Key Q3: C

Explanation:

A RT 53 Resolver can have both outbound and inbound endpoints. Inbound endpoints allow on-premises data centres to resolve DNS names for VPC resources. Outbound endpoints allow VPC resources to resolve DNS names for on premises data centre resources. Setting up your own DNS on EC2 and configuring forwarding would work, although it is not low management overhead.

4. You have an AWS Organization. You have a Service Control Policy that denies the use of a specific service. In CloudTrail you find that a Lambda function is making API calls to this service successfully. What is causing this issue?
   A. A Service Control policy higher in the hierarchy is overriding the lower SCP.
   B. The policy has been created to explicitly not control API calls made by Lambda functions.
   C. Service-linked-roles are not affected by Service Control Policies.
   D. The Lamba function is using root user credentials.

Answer Key Q4: C

Explanation: Service Control Policies affect the root user along with all IAM users. Service Control policies do not affect service-linked-roles, which is where Lambda functions get their permissions.
Reference:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html#scp-about-inheritance

5. What types of centralized organization policies does an AWS Organization provide? Choose all that apply.
   A. Centralized billing
   B. Backup policies
   C. IAM policies
   D. Service Control policies
   E. Tag policies

Select 3 answers
Answer Key Q5: B,D,E

Explanation:
IAM is controlled at the account level. AWS Organizations do not provide IAM policies. AI Opt out, Backup, SCP and Tag policies are supported.

6. You have been asked to connect three VPCs with the least effort and lowest cost. Which solution would you choose?
   A. Set up a transit VPC using subnets in two AZs for HA. Create VPN connections to connect all three VPCs.
   B. Set up a transit gateway and use it as a hub to connect the three VPCs.
   C. Create a single VPC peering connection that connects all three VPCs.
   D. Create three VPC peering connections, each with two endpoints to create a full mesh.

   Answer Key Q6: D
   Explanation:
   While a transit VPC and a transit gateway would both work and provide a solution that is able to grow and handle more complex VPC connectivity, they would not be the lowest effort or lowest cost. A VPC peering connection can only have two endpoints, therefore creating a single VPC peering connection would not work.

7. How can you configure which resources Config monitors?
   A. Config monitors all resources. You cannot configure monitored resource types.
   B. You can only control the regions for which Config records resource events.
   C. You can only control the retention period, not which resources are recorded.
   D. Config records all object types by default. You can control the object types that Config records by opening the settings page and clicking edit after which you can configure "Resource Types to record."

   Answer Key Q7: D

   Explanation:
   Config allows the configuration of which resource types events are recorded along with the retention period and whether it records a single regions event in addition to events from global services such as IAM users, groups, and customer-managed policies.   Reference:
   https://docs.aws.amazon.com/config/latest/developerguide/select-resources.html

8. Which resources does the AWS Access Analyzer monitor for cross account or public access? Choose all that apply.
   A. AWS S3 buckets
   B. AWS SQS queues
   C. AWS Secrets Manager secrets
   D. AWS Lambda functions
   E. AWS KMS keys
   F. AWS IAM roles
   G. All of the above

   Answer Key: G
   Explanation: The AWS Access Analyzer monitors the following 6 resource types: AWS Simple Storage(S3) buckets, AWS Identity and Access Management roles, AWS Key Management Service Keys, AWS Lambda functions and layers, AWS Simple Queue Service queues, and AWS Secrets Manager secrets.
   Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-resources.html.

9. You need to redirect the DNS name www.example.com to an on-premises load balancer using RT 53. The load balancer DNS name is loadbalancer.on-prem.com. Choose the simplest solution.
   A. Create a PTR (Pointer) record for www.example.com that points to loadbalancer.on-prem.com.
   B. Create an ALIAS record for www.example.com that points to loadbalancer.on-prem.com.
   C. Create a conditional forwarder in RT 53 that forwards queries for www.example.com to the DNS servers authoritative for loadbalancer.on-prem.com
   D**. Create a CNAME record for www.example.com that points to loadbalancer.on-prem.com.**

   Explanation:
   Creating a CNAME record to redirect www.example.com to loadbalancer.on-prem.com is the simplest solution. You cannot use an ALIAS because an alias record cannot point to a record in a domain in another hosted zone. There is no need to use conditional forwarding since you only want to do a simple redirect.

10. Which feature is NOT supported by AWS OpsWorks Stacks?
    A. Load balancer creation
    B. Auto healing of EC2 instances
    C. Windows and Linux server management
    D. On-premises Windows and Linux servers

    Answer Key Q10: A
    Explanation:

OpsWorks Stacks cannot create an ELB. You create a LB outside of OpsWorks Stacks and then attach it to an existing layer. Reference: https://docs.aws.amazon.com/opsworks/latest/userguide/layers-elb.html

11. As a security administrator you notice that EC2 instances in a VPC are being port scanned from a specific range of IP addresses.
You need to stop the port scanning in the quickest possible way, with the least effort.
What solution would you use?
A. Use WAF to block the malicious range of IP addresses.
B. Modify the EC2 security groups to block the malicious range of addresses.
C. Use a Network Access Control List (NACL) to deny access from the malicious range of IP addresses.
D. Set up a gateway load balancer and a third-party virtual security appliance.

Answer Key Q11: C
Explanation:
WAF is used to control layer 7 HTTP(S) traffic based on specific conditions used to create rules in a WebACL. The scenario does not say that WAF is being used. EC2 security groups only have "allow" rules and do not support "deny" rules, therefore they are not suitable for blocking based on IP addresses. NACLs are the easiest and quickest solution for blocking a specific IP address since they support "deny" rules and apply to the entire subnet. While a Gateway Load Balancer could be used with security appliances this is not a quick and easy solution.

12. You need to recommend an AWS Service to allow employees who don't know how to build infrastructure to bring up websites for test and production.
Which tool would you recommend?
A. OpsWorks Stacks
B. AWS Code Deploy
C. CloudFormation
D. Elastic Beanstalk

Answer Key Q12: D

Explanation:
Elastic Beanstalk is the service in AWS that can be used to deploy code without any knowledge of deploying infrastructure.

13. You need to upgrade your Windows Servers from Server 2016 to Server 2019.
How would you accomplish this?
A. Use AWS Systems Manager Patch Manager.
B. Use AWS Systems Manager Run command.
C. Use WSUS.

D. Create a new AMI using Windows Server 2019. Use this as a base AMI to replace the Microsoft 2016 servers with Microsoft Server 2019.

Answer Key: D
Explanation:
AWS System Manager Patch Manager does not support major upgrades. WSUS does not support major upgrades. A clean install of the operating system is always the best way to perform major OS upgrades. Creating a new golden AMI with the new OS would be the best solution.

14. You want to use a placement group to keep internode latency low for your cluster. You do not want power or network outages in a server rack causing multiple node failures. Which type of placement group should you choose?
    A. Cluster placement group
    B. Partition placement group
    C. Spread placement group
    D. Do not use a placement group because there is no way to distribute nodes across different racks.

Answer Key Q14: C
Explanation:
A spread placement group is a group of instances that are each placed on distinct racks.
Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

15. You have a 3-tier application: web, application, and DB backend. You want to improve reliability and also have the ability to offload data during times of high volume. Which would provide the best solution?
    A. Put an external facing ALB in front of the web tier and an internal load balancer between the web and application tier. Create a multi-AZ back-end DB.
    B. Put an external facing ALB in front of an auto-scaled web tier and an internal load balancer between the web and an auto-scaled application tier. Create a multi-AZ back-end DB.
    C. Put an external facing ALB in front of the web tier. Have the web tier place its data in an AWS SQS queue. Have your application tier poll the SQS queue to receive the data. Auto-scale the application tier. Have the application tier put its output in another SQS queue. Have a tier to service the second SQS queue and place the data in the DB. Create a multi-AZ back-end DB.

D. Put an external facing ALB in front of an auto-scaled web tier and an internal load balancer between the web tier and an auto-scaled application tier. Create an active-active back-end DB.

Answer Key Q15 : C
Explanation:
The best solution would be to use SQS queues between the web and application tier and the application tier and DB tier. The SQS queues provide asynchronous loose coupling between tiers and remove dependencies that would otherwise reduce reliability. In addition, the SQS queues can offload data if the next tier cannot keep up with the volume.

16. You require your AWS application to connect to S3 without traversing the Internet. You require access from multiple VPCs on premises and S3 resources in a various regions. Which resource would you choose?

A. An S3 Gateway EndPoint
B. An S3 Interface EndPoint
C. An S3 Access Point
D. AWS Global Accelerator

Answer Key Q16: B
Explanation:
Interface endpoints allow access from on-premises resources to multiple VPCs and resources in other AWS regions.
Reference: https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

You can use two types of VPC endpoints to access Amazon S3: *gateway endpoints* and *interface endpoints* (using AWS PrivateLink). A *gateway endpoint* is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. *Interface endpoints* extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on premises, or from a VPC in another AWS Region using VPC peering or AWS Transit Gateway.

Interface endpoints are compatible with gateway endpoints. If you have an existing gateway endpoint in the VPC, you can use both types of endpoints in the same VPC.

Gateway endpoints for Amazon S3	**Interface endpoints for Amazon S3**
In both cases, your network traffic remains on the AWS network.	
Use Amazon S3 public IP addresses	Use private IP addresses from your VPC to access Amazon S3
Use the same Amazon S3 DNS names	Require endpoint-specific Amazon S3 DNS names

Gateway endpoints for Amazon S3	Interface endpoints for Amazon S3
Does not allow access from on premises	Allow access from on premises
Does not allow access from another AWS Region	Allow access from a VPC in another AWS Region using VPC peering or AWS Transit Gateway
Not billed	Billed

Gateway endpoints

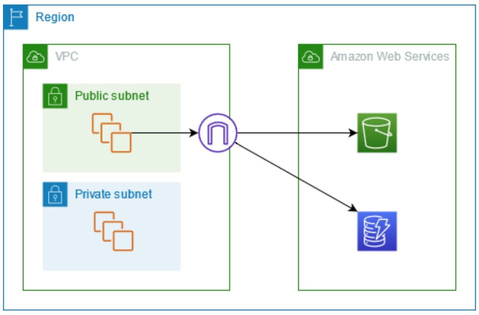
Gateway endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC. Gateway endpoints do not enable AWS PrivateLink.

There is no additional charge for using gateway endpoints.

Amazon S3 supports both gateway endpoints and interface endpoints. For a comparison of the two options, in the *Amazon S3 User Guide*.

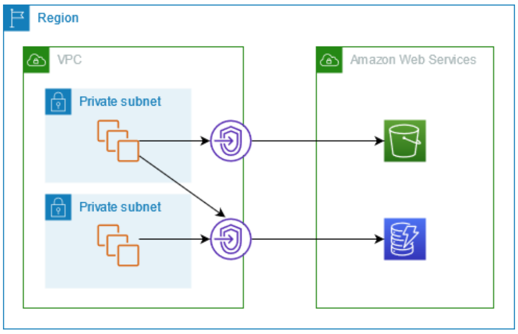
Access through an internet gateway

The following diagram shows how instances access Amazon S3 and DynamoDB through their public service endpoints. Traffic to Amazon S3 or DynamoDB from an instance in a public subnet is routed to the internet gateway for the VPC and then to the service. Instances in a private subnet can't send traffic to Amazon S3 or DynamoDB, because by definition private subnets do not have routes to an internet gateway. To enable instances in the private subnet to send traffic to Amazon S3 or DynamoDB, you would need to add a NAT device to the public subnet and route traffic in the private subnet to the NAT device. While traffic to Amazon S3 or DynamoDB traverses the internet gateway, it does not leave the AWS network.



Access through a gateway endpoint

The following diagram shows how instances access Amazon S3 and DynamoDB through a gateway endpoint. Traffic from your VPC to Amazon S3 or DynamoDB is routed to the gateway endpoint. Each subnet route table must have a route that sends traffic destined for the service to the gateway endpoint using the prefix list for the service.



Routing

When you create a gateway endpoint, you select the VPC route tables for the subnets that you enable. The following route is automatically added to each route table that you select. The destination is a prefix list for the service owned by AWS and the target is the gateway endpoint.

Destination	Target
prefix_list_id	gateway_endpoint_id

17. You are the administrator of an AWS CloudFormation stack. A new template is available to update the stack. You are concerned that the update might cause a service disruption. What would you do to determine what the result of updating the stack will be?

A. Create a new stack using the new template. Test the service to make sure it is operating correctly before updating the current stack.
B. Create deletion policies for resources in the current stack that should not be deleted to make sure no data is lost if stack update causes a resource to be deleted.
C. Use Stack Sets to update the stack.
D. Create a Change Set. View the Change Set. If the results of the Change Set are satisfactory, execute the Change Set.

Answer Key: D

Explanation:
The requirement is for no service disruption. The only method that will let you know the results of using the template to update the stack is to use a Change Set.

Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-changesets.html

18. You are using CloudFront in front of your web servers. You require a layer of protection for specific information such as credit card data to control which applications can access the data. Which feature would you use to accomplish this?
A. HTTPS
B. SSL
C. TLS
D. Field-level encryption
Answer Key: D
Explanation:
While HTTPS, SSL, and TLS all provide encryption of data in transit, they do not control access to the data for specific information types that is stored in AWS. Field-level encryption encrypts data with a public key upon entering the service and the data stays encrypted. Only applications with access to the private key can decrypt it.
Reference:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html

19. You are the DBA for your company. You need to build a multi-AZ Aurora DB. You do not need a Replica node at this time. What should you do?
A. When creating the Aurora DB select the multi-AZ option to create a master and standby.
B. When creating the Aurora DB, select "Do not create an Aurora Replica under Multi-AZ deployment."
C. Create a Global Aurora DB.
D. Create an Aurora DB in a single AZ. Use AWS Backup to schedule snapshots at 15 minutes intervals to another AZ.

Answer Key: B

Explanation:
Aurora automatically creates 6 copies of your DB data in 3 AZs. Unless you require a replica there's no need to do anything further. You can add and remove replicas at any time.

20. Your national company has a public-facing website. The web servers are operating out of us-east-1. Customers on the west coast are complaining that the website is slow to respond. The website also needs to be able to respond quickly to malicious traffic or DDOS attacks. The solution should be cost effective. What architecture below would fulfil all the requirements?

A> Put the web servers in a private subnet behind a public facing ALB (application load balancer). Create a reverse proxy farm to cache often used web pages.

B> Put the web servers in a private subnet behind an ALB (application load balancer). Put a WAF server in front of your web servers.

C> Put the web servers in a private subnet behind an ALB (application load balancer). Auto scale the web servers. Use AWS WAF along with AWS CloudFront in front of the ALB. When setting up CloudFront, choose Price Class 100. Use S3 as the CloudFront origin for static content.

D> Put the web servers in a public subnet behind an ALB (application load balancer). Auto scale the web servers. Use AWS WAF along with AWS CloudFront in front of the ALB. When setting up CloudFront choose Price Class 100. Use S3 as the CloudFront origin for static content.

Answer Key: C

Explanation:
When you load balance the web tier the servers go in a private subnet and only communicate with the load balancer. Using WAF along with CloudFront provides both layer 4 and layer 7 protection against DDOS and other malicious traffic. CloudFront caches the website's static content in all edge locations in the US, which will drastically lower latency when used with latency-based routing.

21. The company you work for has a business requirement to notify its users of transactions made on their account in near real time. You require custom code to handle these transactions. The transaction data is high velocity and considered to be big data. What solution would you recommend?

A> Send the individual transactions to S3. Create an S3 event for puts that triggers an AWS Lambda function that sends an email via SNS.

B> Send the transactions to Kinesis Data Streams. Service the stream using auto scaled EC2 instances running your custom code.

C> Send the transactions to Kinesis Firehose. Service the stream using auto scaled EC2 instances running your custom code.

D> Store the transactions in DynamoDB. Create a DynamoDB stream for the table. Have an AWS Lambda function watching the DynamoDB stream for the table that sends an SNS notification when new transactions occur.

Answer Key: C

Explanation:
Kinesis Data Streams is the service designed to accept high-volume, high-velocity data and work in near real time. You write custom code to consume the data in the stream. Kinesis Firehose does not allow custom code or work in near real time. The other two options, S3 events and DynamoDB streams, are not suitable for near real-time responses.

22. What are the two DR objectives of a business continuity plan?

A> RTO – Recovery Time objective

B> Multi-AZ recovery plan objective

C> Multi-Region recovery plan objective

D> RPO – Recovery Point objective

Select 2 options
Answer Key: A, D

Explanation:
RTO: How long until the service is back up and providing acceptable levels of service. RPO: How much data are you prepared to lose.
Reference: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/

23. You want to copy an automated RDS DB snapshot to another AWS account. What are the required steps? Choose all that apply.

A> Share the manual DB snapshot with another AWS account.

B> Copy the automated snapshot to another AWS account.

C> Copy the automated snapshot to create a manual snapshot.

D> Restore the DB to an existing DB instance.

E> Restore the DB is a new DB instance.

Select 3 answers
Answer Key : A C E
Explanation:
You cannot share an automated RDS backup with another account.
You must first copy it to create a manual snapshot.
You cannot restore a snapshot to an existing DB instance.

You must create a new DB instance.

Reference: https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/

24. What on-premises data can be backed up with AWS Backup?
A> Physical servers
B> Hyper-v servers
C> Hyper-v virtual machines
D> AWS Storage Gateway volumes
E> VMware virtual machines

Select 2 answers
Answer Key : D,E

Explanation:
Only VMware virtual machines and Storage Gateway volumes can be backed up on premises.
Reference:
https://aws.amazon.com/backup/faqs/?nc=sn&loc=6&refid=d61c61a5-6875-45ba-ab44-554e174e41b5

25.You are using AWS MySQL RDS. The database access pattern is read heavy. During times of high read load DB read latency is high or unresponsive. A multithreaded architecture is preferred. What solution would you use to solve the read performance issues in a cost-effective way.
A> Choose a more powerful DB instance type.
B> Use DynamoDB with DAX.
C> Use AWS ElastiCache with Memcached.
D> Use AWS ElastiCache with Redis.

Answer Key: C

Explanation:
An in-memory cache would solve the performance issues. Memcached supports multithreading; Redis does not. A more powerful instance type might solve the issues, although it would not autoscale and would most likely be more expensive. DynamoDB is not a relational DB.
Reference: https://aws.amazon.com/elasticache/redis-vs-memcached/

26.You have been asked to architect an active/active solution with the lowest possible RTO and RPO solution. You have built your web and application servers to be stateless. The DB needs to also be active/active. What would be an appropriate solution?

A> DynamoDB with global tables or Aurora deployed as an Aurora Global Database. Select appropriate read/write patterns (such as read local/write local, read local/write global, read local/write partitioned) based on acceptable latency and failover design.

B> AWS RDS multi-region write copies.

C> Configure the EBS volume that the RDS is using for the database for continuous replication to another region.

D> Configure AWS RDS read replicas to use synchronous replication. Fail over to a read replica if the master/write DB instance fails.

Answer Key : A

Explanation:

RDS read replicas do not support synchronous replication and do not support automatic failover. There are no built in AWS RDS solutions for active/active. EBS volumes do not have a continuous replication feature. You would have to use a third-party CDR solution.

Reference: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iv-multi-site-active-active/

27. Your company has a MySQL RDS. At the end of each quarter, database read and write latency increases and performance suffers. During the period of high latency, quarterly reports are being created. You have been asked to find a solution that is quick, efficient, and cost effective. Choose an appropriate solution that meets all the requirements.

A> Prior to the end of the quarter, create one or more read replicas in the same region. Use the read replicas for the quarterly reports. Remove the replicas once the quarterly reports are complete.

B> Prior to the end of the fiscal quarter, when quarterly reports start, create one or more read replicas in another region. Use the read replicas for the quarterly reports. Remove the replicas once the quarterly reports are complete.

C> Introduce a Memcached caching layer. Direct all reads to the cache. If the date is not cached, write the data to the cache for subsequent reads.

D> Set up RDS DB auto scaling based on read latency.

Answer Key : A

Explanation:

The simplest cost-effective solution is to create RDS MySQL read replicas just prior to the load increasing for quarterly reports. They can easily be added when needed and removed when no longer needed. The read replicas should be in the same region since they are not for DR or compliance. Introducing caching is not necessary and would require rearchitecting the service to use the cache. It would also not be cost effective in this situation. There is no auto scaling AWS RDS feature.

28. Which AWS Services support AWS Backup Advanced features such as “lifecycle tiering”?

A> AWS RDS
B> AWS EFS
C> AWS S3
D> AWS DynamoDB

Select 2 options
Answer Key: B (AWS EFS), D (AWS DynamoDB)

Explanation:
Reference:
https://aws.amazon.com/backup/faqs/?nc=sn&loc=6&refid=d61c61a5-6875-45ba-ab44-554e174e41b5

29. You are advising your Dev team on what type of APIs are supported by the AWS API Gateway. Select the types of APIs that API Gateway supports.

A> HTTP
B> RPC
C> MAPI
D> REST
E> WebSocket

Select 3 answers
Answer Key : A , D , E

Explanation:
Amazon API Gateway offers two options to create RESTful APIs—HTTP APIs and REST APIs—as well as an option to create WebSocket APIs.

30. You require a feature that will allow you to create, update, or delete stacks across multiple accounts and regions. Which AWS feature was created to provide this (MSO/MSP) ability?

A> CodePipeline
B> Elastic Beanstalk
C> CloudFormation
D> CloudFormation StackSets

Answer Key : D CloudFormation StackSets
Explanation:
While any automation that can create AWS infrastructure can be used, AWS created CloudFormation StackSets for exactly this purpose.

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

31. Your company is using OpenSearch. You would like to know if there are performance issues with indexing or searching. What solution would you recommend? Choose all that apply.

A> Set up alerts in CloudWatch on the OpenSearch Domain based on standard OpenSearch metrics.
B> Set up Search slow logs.
C> Turn on slow logs and slow indexing notifications in the OpenSearch domain.
D> Setup Index slow logs.

Select 2 answers
Answer Key : B , D

Explanation:
You must enable both types of slow logs for your OpenSearch domain.
Reference: https://aws.amazon.com/blogs/database/viewing-amazon-elasticsearch-service-slow-logs/
https://aws.amazon.com/opensearch-service/faqs/

32. As the administrator of your company's RedShift cluster, you have just performed a manual elastic resize.
You begin to get complaints that the cluster is unavailable.
What is the issue?

A> The RedShift cluster will not accept reads or writes until the nodes have been added or removed and all data has been transferred from S3.
B> The RedShift cluster will available as soon as the cluster is resized (nodes added or removed). Reads and writes will be accepted while data is being transferred from S3.
C> A new cluster was created with a new DB path. Reads and writes must be directed to the new DB path.
D> The cluster is offline until you bring it back online after a resize.

Answer Key: B

Explanation:
Reference: https://docs.aws.amazon.com/redshift/latest/mgmt/managing-cluster-operations.html

33. You are using a CloudFront distribution as your entry point for public web servers. You have the web servers, application servers, and DB all set up for multi-AZ. You also have duplicated your three tiers in another AWS region to achieve HA if there is a regional failure. Currently the websites static assets are stored in S3 Standard Class with the default replication settings. Is your architecture highly available and fault tolerant in case of a regional failure? Choose the best answer.

A> Yes, S3 is a global service, therefore a regional failure will not affect the availability your data in the S3 bucket.
B> No, S3 objects are stored in a bucket that is in one specific region. You need to set up S3 bucket replication to another region for the S3 bucket static assets.
C> No, S3 is a regional service. The data is stored in a bucket created in a single region. You need to set up replication to another region for the S3 bucket static assets. Configure CloudFront with an alternate origin for the static assets that points to a bucket with the same name in another region.
D>No, S3 is a regional service. The data is stored in a bucket created in a single region. You need to set up replication to another region for the S3 bucket static assets. Configure CloudFront with an alternate origin for the static assets that points to a bucket with a different name in another region.

Answer Key : D

Explanation:
Although you cannot select a region in the S3 console, when you create a bucket, you must select a region that the bucket will be created in. Objects in that bucket are only available from the selected region. You should replicate the contents of the bucket to another region. All S3 bucket names must be unique, so you cannot create another bucket with the same name. You can configure your CloudFront distribution with an alternate origin should the primary fail.

34. You install the AWS Discovery Connector appliance on VMware. After a while, you notice VMware virtual machines showing up as resources. None of the Hyper-v VMs are showing up. What is the cause of this issue?

A> You have not configured the Discovery Connector with credentials to communicate with the Hyper-v Manager.
B> You need to install the connector as an appliance on a Hyper-v host.
C> Restart the Hyper-v hosts after installing the connector.
D> The AWS Discovery Connector only works with VMware.

Answer Key: D

Explanation:
The AWS Discovery Connector only works with VMware vCenter Server
Reference: https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-connector.html

35.During which stage of an AWS migration is a detailed portfolio discovery done?
A> Access
B> Migrate and modernize
C> Mobilize
D> Pre-Assessment

Answer Key : C

Explanation:
Reference: https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-migration/mobilize-phase.html

36. Your company is migrating to AWS. They have created an IT portfolio of the company's current IT footprint. You have been asked to select a workload to start the migration. Which workload would you choose?

A> A complex customer-facing service
B> A development environment
C> A service that utilizes a mainframe computer
D> A service that uses software that does not support running in a public cloud environment
E> A service with servers running IBM AIX OS

Answer Key: B

Explanation:
Early migrations should be easy, quick, and provide success quickly. IBM AIX OS does not run directly in AWS nor do mainframes. If you use software that is not supported in the cloud, workloads that use the software should be moved later on and most likely will be re-architected.

37. Your company has decided there are business benefits for using AWS services. However, the company is not ready to run workloads in a public cloud. Is there a solution that allows your company to use AWS services and not run in a public cloud?
A> AWS Local Zones

B> AWS LightSail
C> AWS On-Premises Zones
D> AWS Outposts

Answer Key: D
Explanation:
AWS Outposts allow you to run certain AWS services in racks in your data center.
Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

38. You are using AWS DMS for the migration of a DB. You need to keep the downtime of your DB migration to a minimum. Your migration requires keeping both source and target DB in sync and running simultaneously for writes. Which cutover strategy meets these requirements?
A> Active/active
B> Flash-cut migration
C> Offline Migration
D> None of provided solutions

Answer Key: A

Explanation:
The only multi-master solution is active/active.
Reference: https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-migration/cut-over.html

39. Your company is migrating to AWS. They need to perform a migration from an Oracle Relational DB to Aurora. Which migration tools would you use? Select all that apply.
A> AWS Server Migration Service
B> CloudEndure Migration Service
C> AWS Application Migration Service
D> AWS DMS
E> AWS Migration Hub
F> AWS SCT

Select 2 answers
Answer Key : D , F

Explanation:
This is a heterogenous migration. Use the SCT to convert the schema and DMS to migrate the data.

40. You migrate an on-premises MySQL DB to run on EC2 in AWS. What type of migration is that classified as?

A> Rehost
B> Relocate
C> Re-architect
D> Re-platform

Answer Key: A

Explanation:
Reference: https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/

41. As part of the company's customer support, third-party software is used to create text or voice interactions that allow certain issues to be handled with automation. During the migration of this service, the company wants to build a conversational voice or text interface using a service that is native to AWS Cloud. Which AWS service is specifically designed for this purpose and what type of migration is it? Select the correct answers.

A> Replatform
B> AWS Mechanical Turk
C> AWS Lex
D> AWS Step Functions
E> Repurchase

Select 2 answers
Answer Key: C , E

42. Your datacenter is in Los Angeles, CA. Your customers are in Los Angeles, CA. Very low latency is required by your customers when accessing your services. Your company is moving to AWS. You are advised that the stakeholder for the services is concerned about any increase in latency since the closet AWS region is us—west-1 in Northern CA. You cannot migrate these services until the stakeholder is convinced the latency will not increase. How will you overcome the latency issues so that you will get the required stakeholder support?

A> Use Wavelength Zones
B> Use AWS Global Accelerator
C> Use CloudFront
D> Use Local Zones

Answer Key: D

Explanation:

Local Zones offer compute, storage, DB, and other services closer to end users. There is a local zone in Los Angeles, CA.

Reference: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

43. Your company is migrating to AWS. Some workloads will continue to run on premises for quite a while. Some of the workloads have large datastores. The company is ready to migrate this workload to AWS; the datastore will need to be migrated. The datastore in AWS must be no more than a few hours behind. Which solution would you choose to meet these requirements?

A> AWS Storage Gateway
B> Snowcone
C> Snowmobile
D> Snowball

Answer Key:A AWS Storage Gateway

Explanation:

AWS Storage Gateway can copy your data to AWS storage. Depending on the type to storage you set up on AWS Storage Gateway, the data can be up to date or nearly up to date. The Snow family requires shipping AWS storage devices to AWS to have the data transferred to storage in AWS. The time delay is multiple days with the default being about 13 days.

44. Your company runs many workloads that are made of up of microservices. For microservices that do not run continually, the company requires a service where you only pay when you are running code. Which service would best support this requirement?

A> AWS Lambda
B> Docker containers
C> AWS Lightsail
D> EC2 instances

Answer Key:A AWS Storage Gateway

Explanation:

AWS Storage Gateway can copy your data to AWS storage. Depending on the type to storage you set up on AWS Storage Gateway, the data can be up to date or nearly up to date. The Snow family requires shipping AWS storage devices to AWS to have the data transferred to storage in AWS. The time delay is multiple days with the default being about 13 days.

45. Your company is running an SQS queue to loosely couple two tiers in one of their services. The queue does not always have messages in it. When there are messages in the queue they must be actioned as soon as possible. The company would like to keep the cost of running this service as low as possible while still meeting the above requirement. What could you do to help meet the requirements? Choose all that apply.

A> Use short polling.
B> Use long polling.
C> Process the message in batches.
D> Autoscale the EC2 tier that is polling the queue and processing the messages with an autoscaling policy with a minimum set to 0.
E> Autoscale the EC2 tier that is polling the queue and processing the messages with an autoscaling policy with a minimum set to 1.

Select 2 answers
Answer Key : B,E

Explanation:
You pay for each time you poll an SQS queue. The queue is often empty. Long polling keeps the connection open when polling the queue and waits for messages to become available. Long polling will keep the cost of polling down. Autoscaling the tier that processes the messages in the queue will keep cost down, although you must set the autoscaling policy to a minimum of 1 so that there is always an EC2 instance ready to action messages to meet the requirement to action messages ASAP.

46. You are using AWS EMR. You want to keep costs at a minimum. You also need to run jobs at specific times. What solution would meet these requirements?

A> Use spot instances.
B> Use spot instances in an autoscaling group.
C> Use reserved instances.
D> Use EMR instance fleet feature.

Answer Key : D

Explanation:
EMR instance fleet allows you to mix spot and on demand instances and up to five instance types in the same autoscaling group.

47. Your company is international and has offices in many countries. You have assets in S3 that are read millions of times per day from all the company's offices. The cost of accessing these assets is high and there have been complaints regarding high latency from some offices. What would you recommend as a solution to lower access cost and reduce latency?

A> Replicate the assets to multiple buckets located in regions that are close to your offices.
B> Set up a CloudFront distribution in front of your S3 bucket and force access to the assets through CloudFront.
C> Set up a CloudFront distribution in front of your S3 bucket.
D> Move the assets to EFS.

Answer Key : B
Explanation:
EFS is much more expensive per GB than S3. EFS is also region based. Keeping the assets in S3 and fronting them with CloudFront would keep access cost down and keep latency down due to edge caching. It is important to force access to the assets through CloudFront so that access can be directly to the S3 bucket.

48. You are looking at your cost expenditure in AWS. You notice that the cost of EBS volumes has been growing steadily for a very long time. After a bit of research, you find that there are many unattached and unused volumes. The number of these unattached and unused volumes increases daily. What is the most likely cause?

A> When EC2 instances are being launched the box that says "delete on termination" is not being selected.
B> When EC2 instances are being launched the box that says "delete on termination" is being selected.
C> EBS storage is being used when S3 storage would be a better solution.
D> EBS Lifecycle Manager is not being used.

Answer Key : A

Explanation:
If the check box for "delete on termination" is not checked when creating an EC2 instance, the EBS volumes will not be deleted each time an EC2 instance is terminated. This will cause an ever-increasing number of EBS volumes over time. EBS volumes should normally be deleted when the EC2 instances that

they are attached to are terminated unless there is a need to attach those volumes to another EC2 instance.

49. Your company spend on EC2 is higher than expected. They have asked you to look at how efficiently EC2 is being used. They also want to do the same for EBS and Lambda. Memory utilization should also be reviewed. What method would you use to accomplish this? Select all that apply.

A> Publish your EC2 memory metrics using CloudWatch Agent to CWAgent namespace.

B> Use the AWS Compute Optimizer.

C> Use Trusted Advisor.

D> Use Cost Explorer EC2 Resource Rightsizing Recommendations.

Select 2 answers

Answer Key : A, B

Explanation:

You must push memory metrics to CWAgent log group for Compute Optimizer to make rightsizing recommendations based on memory consumption. While all of the answers would provide assistance in right sizing, Compute Optimizer would be the most helpful in the above scenario.

Reference: https://aws.amazon.com/compute-optimizer/faqs/

50. You are an unfunded startup and have not used AWS before. You have a functioning website. What is the most cost-effective way to start and build your business in AWS?

A> Use the AWS Free Tier.

B> Contact AWS Sales Team and ask for discounts based on your company being a startup.

C> Apply to join AWS Activate.

D> Build you company based on non-expiring free tier services.

Answer Key: C

Explanation:

Reference:

https://aws.amazon.com/activate/founders/?sc_channel=we&sc_campaign=pmmfreetier1&sc_geo=global&sc_country=global&trkcampaign&awswt=245

51. Your company is trying to lower the cost of running EC2 instances, Lambda and Fargate. The company is willing to make a commitment for multi-year use. The company does not want to commit to any particular instance type and wants maximum flexibility. Which purchasing option would you choose?

A> Standard Reserved instances
B> Convertible Reserviced Instances
C> Compute Savings Plans
D> EC2 Savings Plans

Answer Key : C Compute Savings Plans
Explanation:
Reference: https://aws.amazon.com/savingsplans/faq/

52. You have been asked by your company to provide a low latency, secure front end for your web servers. Your customers only reside in the USA. You must achieve the lowest cost. How would you proceed?

A> Use CloudFront and an ALB in front of your web servers.
B> Use CloudFront and an ALB in front of your web servers and select Price Class 100 for CloudFront.
C> Use CloudFront and an ALB in front of your web servers and select Price Class 100 for CloudFront and the CloudFront Savings Bundle.
D> Use CloudFront and an ALB in front of your web servers. Choose the shortest TTLs possible for your static assets

Answer Key : D

Explanation:
Reference:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/savings-bundle.html

53. You have created tags for cost allocation. When you look in Budgets, Cost Explorer, and Cost and Usage reports you do not see your tags. Why?
A> Only AWS can define Cost Allocation Tags.
B> When you created the tags you did not specify that they were cost allocation tags.
C> You must activate the tags in the Billing and Cost Management console.
D> The Tag Name must be in the format CostAllocTag:<tag_name>.

Answer Key : C

Explanation:
Any tags you create are user defined tags. Tags that you create for cost allocation must be activated in the Billing and Cost Management console.
Reference:
https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html

54. Your company (account A) uploads objects to an S3 bucket in another account (account B). The bucket owner cannot access the uploaded objects. It is required that the bucket owner must have full control of all objects in the bucket. What must you do to remedy this?

A> Give the user in account A S3:PutObjectACL permission in their IAM policy.

B> Give the bucket owner full control permission of all objects in the bucket.

C> Enforce all S3 Put operations to include the bucket-owner-full-control canned ACL.

D> Provide the bucket owner with a script that changes the permissions on all objects in the bucket to give FC to the bucket owner.

Answer Key : C

Explanation:

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-owner-full-control-acl/

55. Your company is currently using the KMS to create and store master encryption keys. The head of security specifies that it is no longer acceptable for AWS to have the master keys or manage the master keys lifecycle. The solution is required to work with AWS services and work like using the AWS KMS. What solution best fulfils the requirements?

A> Use Cloud HSM.

B> Use AWS KMS Customer Managed Keys.

C> Use a third-party on premises KMS.

D> Use CloudHSM with a Custom Key Store.

Answer Key: D

Explanation:

The only solution that works transparently with the AWS KMS is to use CloudHSM with a Custom Key Store.

Reference: https://docs.aws.amazon.com/kms/latest/developerguide/key-store-concepts.html

56. Which sources are supported for CodePipeline push events? Select all that apply.

A> CodeCommit

B> S3

C> GitHub

D> AWS Container Registry Service

E> AWS App Runner

Select 3 answers

Answer Key: A,B,C

Explanation:
Reference:
https://docs.aws.amazon.com/codepipeline/latest/userguide/update-change-detection.html

57. Your company is having trouble controlling how resources are deployed. You have been asked to find a way to take control of how resources are deployed and still allow self service. What feature or service below would fill that requirement?

A> Stack Sets
B> Service Catalog
C> AWS Config
D> Service Control Policies

Answer Key: B

Explanation:
The best tools are those that provide MSP/MSO functionality where a team or department can publish automation that fulfils company standards for security, cost management, etc. and still allow self service. The Service Catalog is self service and fulfils that requirement. You could use Stack Sets if you didn't have the self-service requirement.

58. Your company has set up EKS. You are seeing nodes that have failed to join the cluster. Which reasons below could be the cause of this issue? Choose all that apply.

A> You are using Fargate instead of a self-managed EC2 cluster.
B> The instance profile ARN has been specified in the aws-auth-cm.yaml file.
C> The node IAM role ARN has been specified in the aws-auth-cm.yaml file.
D> The STS endpoint for the region you are deploying in is not enabled for your account.
E> The worker node does not have a private DNS entry.

Select 3 answers
Answer Key: B, D, E

Explanation:
EKS can use both Fargate and EC2 clusters to launch nodes. The STS endpoint for the deployment region must be enabled. The worker nodes must have a private DNS entry or a node not found error will occur. The node IAM role must be present in the aws-auth-cm.yaml file when using self-managed Amazon Linux nodes.

Reference:
https://docs.aws.amazon.com/eks/latest/userguide/troubleshooting.html

59. Your company wants to process customer texts, chat, email, and phone calls for entity, sentiment, and key phrases and analyze them with business intelligence to improve customer outcomes and provide insights when training customer service reps. What service could they use?

A> Amazon Lex
B> Amazon Rekognition
C> Amazon Transcribe
D> Amazon Comprehend
E> Amazon Forecast

Answer Key : D
Explanation:
Reference: https://aws.amazon.com/comprehend/

60. Your company uses CloudFormation to bring up RDS databases. Currently the database credentials are provided at runtime by the person creating the stack by using a CloudFormation parameter. Once the RDS is online and ready for use, the person who created the RDS DB provides the credentials to the administrator of the regional SMS Parameter store who stores the credentials so that they can be access centrally. Every 30 days, the person who created the DB will contact the administrator of the regional SMS parameter store to rotate the credentials. You would like to streamline this process by automating it. What solution would you choose?

A> Store the credentials in AWS Secrets Manager. Have the CloudFormation template call AWS Secrets Manager to get the credentials when creating the RDS DB. Configure Secrets Manager to use a Lambda function to rotate the credentials monthly.

B> Store the credentials in AWS SMS Parameter Store. Have the CloudFormation template call AWS SMS Parameter Store to get the credentials when creating the RDS DB. Configure the AWS SMS Parameter Store to use a Lambda function to rotate the credentials monthly.

C> Store the credentials in an encrypted AWS S3 bucket. Have the CloudFormation template get the credentials from the S3 bucket when creating the RDS DB. Create a Lambda function to rotate the credentials monthly.

D> Store the credentials in an encrypted AWS DynamoDB table. Have the CloudFormation template get the credentials from the DynamoDB table when creating the RDS DB. Create a Lambda function to rotate the credentials monthly.

Explanation:

AWS Secrets Manager has a built-in password generator and has pre-created Lambda functions available to rotate RDS credentials on a schedule you determine. All of the other methods could work, although they would be less efficient and more time consuming to set up.

61. Your company runs various software on EC2. Internal compliance requires that CVE, CIS, and networking best practices testing be done periodically. What would you choose to fulfil the requirements?

A> AWS Trusted Advisor
B> AWS GuardDuty
C> AWS X-ray
D> AWS Detective
E> AWS Inspector

Explanation:

Reference:
https://docs.aws.amazon.com/inspector/v1/userguide/inspector_rule-packages.html

62. You are getting a lot of false positives for a custom identifier in Macie. What can you do to reduce the number of false positives?

A> Use a keyword with a maximum match distance.
B> Lower the occurrences threshold.
C> Raise the occurrences threshold.
D> Tell Macie to only look at structured data.

Answer Key : A

Explanation:

Using a keyword with a maximum match distance helps to lower false positives. When using a keyword, it must be in proximity of the text that matches the regex pattern.

Reference: https://docs.aws.amazon.com/macie/latest/user/custom-data-identifiers.html

63. Your company uses Storage Gateway as a file gateway. You are getting complaints from users that sometimes file access fails. When you look into the issue, you start to find InaccessibleStorageClass. What is the likely cause of the issue?

A> DNS issue accessing AWS S3
B> File/object stored in One Zone IA
C> Storage Gateway network issues
D> File moved to Glacier or Glacier Deep Archive

Explanation:

Reference: https://docs.aws.amazon.com/filegateway/latest/files3/troubleshooting-file-gateway-issues.html

64. Your company needs to redirect your zone apex. You are trying to use a DNS CNAME RR to accomplish this. The configuration is failing. What type of record should you be using?

A> PTR record

B> MX record

C> Service locator RR

D> Alias

Answer Key: D RT53 Alias Record

Explanation:

CNAME records cannot be use for zone apex records. You can use an AWS RT 53 Alias resource record

Reference: https://www.isc.org/blogs/cname-at-the-apex-of-a-zone/

65. You have built a Kubernetes cluster. You want to visualize and manage it in the AWS Kubernetes console. How can you achieve this?

A> Use the Amazon EKS connector to visualize the external EKS cluster.

B> Use the Amazon EKS connector to visualize and manage the external EKS cluster.

C> Provide the DNS name of the master node of your external EKS cluster and import it from the EKS console.

D> Provide the IP address of the master node of your external EKS cluster and import it from the EKS console.

E> Set up a EKS bridge and connect it to the AWS EKS console and the external EKS master node.

Answer Key: A

Explanation:

You can visualize an external EKS cluster in the AWS EKS console. You cannot manage it.

Reference: https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html

66. Your company uses AWS Redshift. You want to improve performance by improving distribution keys, sort keys, and compression recommendations. Which feature below would minimize the administrative work?

A> Materialized views
B> Amazon Redshift Advisor
C> Elastic resize
D> Amazon Redshift data lake integration
E> Temporary tables

Answer Key: D
Explanation:
Reference: https://aws.amazon.com/blogs/big-data/top-10-performance-tuning-techniques-for-amazon-redshift/

67. Example.com is looking to share AWS resources with other AWS accounts within the company. They are going to use AWS Resource Manager. Which of the resource types listed below can be shared in AWS Resource Manager? Choose all that apply.
A> EBS volumes
B> S3 bucket
C> AWS VPC
D> AWS EC2
E> AWS Network Firewall

Select 3 answers
Answer Key: C, D, E

Explanation:
Reference:
https://docs.aws.amazon.com/ram/latest/userguide/shareable.html

68. Your company has some back-end services running in EC2 such as DNS servers, Microsoft Domain Controllers, etc. These EC2 instances are long running and need to be patched on a regular basis. The servers get their updates over the Internet. You notice that every once in a while, the servers cannot get updates. You are troubleshooting the issue. What would be the most likely cause?

A> Internet Gateway failure
B> Network ACLs misconfiguration
C> Security Group misconfiguration
D> Virtual private gateway failure
E> NAT GW failure due to AZ failure

Answer Key: E NAT GW failure due to AZ failure

Explanation:

The most likely cause would be a NAT GW failure due to AZ failure. Internet and Virtual Private gateways are highly available by their very nature. NAT gateways live in an AZ and are vulnerable to AZ failure. It is your responsibility to make your NAT gateway highly available by creating two, each in a different AZ. Security groups and NACLs don't intermittently fail.

69. Your company runs a customer-facing service that has millions of users. Currently users must create an account to use the service. You are looking for a way to allow new customers access to the service with a choice of creating a new account specific to the service or use an existing web identity account (Google, FaceBook, AWS, etc.) that they already have. What would be the most efficient way of implementing such a solution?

A> Set up federated trusts with each web identity provider. Attach a role to each web identity provider that has an associated policy that allows access to the required AWS services.

B> Use AWS Single Sign On (SSO) service.

C> Use IAM Identity Providers.

D> Use Amazon Cognito.

Answer Key: D Amazon Cognito

Explanation:

The easiest way to implement the requirement would be to use AWS Cognito. Cognito allows authentication from any directory including, web identity (incl OpenID), SAML, developer created authentication, and Cognito user pools. This provides the flexibility required to achieve the requirements.

Reference:

https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html

70. Your company runs a service that relies on a RDS DB. The service has a 90/10 read/write load. The number of DB read transactions is quite high requiring an expensive DB instance type and Provisioned IOPS EBS volume. You would like to lower the cost of running the DB. The solution must have persistence and be able to fail over in the event of a failure. Which solution would you choose?

A> Use DynamoDB for the DB.

B> Use RedShift for the DB.

C> Use multi-AZ for the RDS. Set up ElastiCache with Memcached with replica nodes.

D> Use multi-AZ for the RDS. Set up ElastiCache with Redis with replica nodes.

Answer Key: D

Explanation:
The scenario does not state that a NoSQL database can be used so you cannot assume that DynamoDB can be used. Redshift is a data warehouse not an OLTP database. ElastiCache would enable read load to be offloaded from the DB reducing RDS costs. Only Redis offers persistence via replicas and failover.

71. You have a firewall application that is mission critical. The application currently runs in a single AZ. The application needs to be highly available within the region. The application runs on EC2. You decide to set the application up on EC2 instances in two subnets in different AZs in the same region. The two instances will be primary and standby. You want the two instances to use the same volume for storing configuration information. The solution should provide the standby EC2 instance up to date configuration information when it comes online. What kind of storage should you choose?

A> EBS Multi-Attach volumes
B> S3
C> Instance storage
D> EFS
E> EBS

Answer Key: D
Explanation:
The only storage type that allows multiple EC2 instances to connect to the same volume is EFS. EBS can only be attached to a single EC2 instance at a time and EBS is AZ scoped, therefore it cannot be attached to the instance in another AZ. EBS multi-attach volumes have specific requirements for OS and application support and are not available in all regions. S3 does not provide block storage; it is object storage.

72. Your company has many DynamoDB tables. You want to lower the latency of your GetItem on an ongoing basis. What steps can you take to achieve this? Choose all that apply.
A> Always use strongly consistent reads.
B> Increase your read commit units for the DynamoDB table.
C> Use On-Demand scaling for your DynamoDB tables.
D> Use caching.
E> Use eventually consistent reads whenever possible.

Select 2 answers

Answer Key : D,E

Explanation:

Strongly consistent reads take longer than eventually consistent reads. An in memory cache will also reduce latency ongoing.

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/dynamodb-high-latency/

73. Your company uses many EFS file systems. You require the data stored in EFS to be highly available. You also want to keep access costs down. Which configuration option fulfils the requirements?

A> Create an EFS file system using a One Zone storage class. Create a single mount target in the same AZ where the EFS file system exists. Configure EC2 instances in each AZ to access the mount target.

B> Create an EFS file system using the Standard storage class. Create a single mount target. Configure EC2 instances in each AZ to access the mount target.

C> Create an EFS file system using the Standard storage class. Create a mount target in each AZ that has EC2 instances that need access to the file system. Configure EC2 instances in each AZ to access the local mount target.

D> Create an EFS file system using a One Zone storage class. Create a mount target in each AZ that has EC2 instances accessing the file system. Configure EC2 instances in each AZ to access the local mount target.

Answer Key: C

Explanation:

One Zone storage class does not offer HA if the AZ hosting the file system fails. Standard storage class stores the EFS file system regionally which makes it highly available. If you access an EFS file system in another AZ, data transfer costs are higher. Having a mount target in all AZs that are going to have EC2 instances accessing the file system keeps data transfer costs down.

Reference: https://docs.aws.amazon.com/efs/latest/ug/accessing-fs.html

74. You are currently using IAM roles to allow access to DynamoDB tables for both users and applications. All access to the DynamoDB tables happens from within a VPC. How could you increase security for the DynamoDB tables?

A> Use client-side encryption.

B> Use a resource policy on the DynamoDB tables.

C> Use SCPs to deny access to certain API calls.

D> Create an Interface VPC endpoint with policies to access DynamoDB. Only allow access via the endpoint.

Answer Key: D

Explanation:
The scenario states that all access is from within a VPC. The best way to increase security is to use IAM roles for access permissions and have all access going though a VPC endpoint with policies to limit access to only the required VPCs.

75. You wish to find issues that may cause service outages. You want to include issues such as CPU load and insufficient memory. What would you do to achieve the stated requirements?

A> Use AWS Fault Injection Simulator
B> Use AWS Fault Injection Simulator with the FIS agent
C> Use AWS Fault Injection Simulator with the SSM agent
D> Use AWS CloudWatch Events with a scheduled action

Answer Key: C

Explanation:
Reference: https://aws.amazon.com/fis/faqs/