Q99. You have been asked to build a database warehouse using Amazon Redshift. You know a little about it, including that it is a SQL data warehouse solution, and uses industry standard ODBC and JDBC connections and PostgreSQL drivers. However you are not sure about what sort of storage it uses for database tables. What sort of storage does Amazon Redshift use for database tables?

A.InnoDB Tables

B.NDB data storage

C.Columnar data storage

D.NDB CLUSTER Storage

正确答案C

**解析:**

Amazon Redshift achieves efficient storage and optimum query performance through a combination of massively parallel processing, columnar data storage, and very efficient, targeted data compression encoding schemes.Columnar storage for database tables is an important factor in optimizing analytic query performance because it drastically reduces the overall disk I/O requirements and reduces the amount of data you need to load from
disk.Reference:http://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmnt.html

Q100. You are checking the workload on some of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes and it seems that the I/O latency is higher than you require. You should probably check the _____ to make sure that your application is not trying to drive more IOPS than you have provisioned.

A.Amount of IOPS that are available

B.Acknowledgement from the storage subsystem

C.Average queue length

D.Time it takes for the I/O operation to complete

正确答案C

**解析:**

In EBS workload demand plays an important role in getting the most out of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes. In order for your volumes to deliver the amount of IOPS that are available, they need to have enough I/O requests sent to them. There is a relationship between the demand on the volumes, the amount of IOPS that are available to them, and the latency of the request (the amount of time it takes for the I/O operation to complete). Latency is the true end-to-end client time of an I/O operation; in other words, when the client sends a IO, how long does it take to get an acknowledgement from the storage subsystem that the IO read or write is complete.If your I/O latency is higher than you require, check your average queue length to make sure that your application is not trying to drive more IOPS than you have provisioned. You can maintain high IOPS while keeping latency down by maintaining a low average queue length (which is achieved by provisioning more IOPS for your volume).Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-workload-demand.html

Q101. Which of the below mentioned options is not available when an instance is launched by Auto Scaling with EC2 Classic?

A.Public IP

B.Elastic IP

C.Private DNS

D.Private IP

正确答案 B

**解析:**

Auto Scaling supports both EC2 classic and EC2-VPC. When an instance is launched as a part of EC2 classic, it will have the public IP and DNS as well as the private IP and DNS.Reference:http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html

Q102. You have been given a scope to deploy some AWS infrastructure for a large organisation. The requirements are that you will have a lot of EC2 instances but may need to add more when the average utilization of your Amazon EC2 fleet is high and conversely remove them when CPU utilization is low. Which AWS services would be best to use to accomplish this?

A.Auto Scaling, Amazon CloudWatch and AWS Elastic Beanstalk

B.Auto Scaling, Amazon CloudWatch and Elastic Load Balancing.

C.Amazon CloudFront, Amazon CloudWatch and Elastic Load Balancing.

D.AWS Elastic Beanstalk , Amazon CloudWatch and Elastic Load Balancing.

正确答案 B

**解析:**

Auto Scaling enables you to follow the demand curve for your applications closely, reducing the need to manually provision Amazon EC2 capacity in advance. For example, you can set a condition to add new Amazon EC2 instances in increments to the Auto Scaling group when the average utilization of your Amazon EC2 fleet is high; and similarly, you can set a condition to remove instances in the same increments when CPU utilization is low. If you have predictable load changes, you can set a schedule through Auto Scaling to plan your scaling activities. You can use Amazon CloudWatch to send alarms to trigger scaling activities and

Elastic Load Balancing to help distribute traffic to your instances within Auto Scaling groups. Auto Scaling enables you to run your Amazon EC2 fleet at optimal utilization.Reference:
http://aws.amazon.com/autoscaling/

Q103. A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption.Due to new compliance requirements, all existing and new data in this database must be encrypted.How should this be accomplished?

A. Create an Amazon S3 bucket with server-side encryption enabled.Move all the data to Amazon S3 Delete the RDS instance.

B. Enable RDS Multi-AZ mode with encryption at rest enabled.Perform a failover to the standby instance to delete the original instance.

C. Take a snapshot of the RDS instance Create an encrypted copy of the snapshot.Restore the RDS instance from the encrypted snapshot.

D. Create an RDS read replica with encryption at rest enabled.Promote the read replica to master and switch the application over to the new master Delete the old RDS instance.

正确答案 C

**解析:**

How do I encrypt Amazon RDS snapshots? The following steps are applicable to Amazon RDS for MySQL, Oracle, SQL Server, PostgreSQL, or MariaDB. Important: If you use Amazon Aurora, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster if you specify an AWS Key Management Service (AWS KMS) encryption key when you restore from the unencrypted DB cluster snapshot. For more information, see Limitations of Amazon RDS Encrypted DB Instances. Open the Amazon RDS console, and then choose Snapshots from the navigation pane. Select the snapshot that you want to encrypt. Under Snapshot Actions, choose Copy Snapshot. Choose your Destination Region, and then

enter your New DB Snapshot Identifier. Change Enable Encryption to Yes. Select your Master Key from the list, and then choose Copy Snapshot. After the snapshot status is available, the Encrypted field will be True to indicate that the snapshot is encrypted. You now have an encrypted snapshot of your DB. You can use this encrypted DB snapshot to restore the DB instance from the DB snapshot. Reference: https://aws.amazon.com/premiumsupport/knowledge-center/encrypt-rds-snapshots/

Q104. A company has a three-tier image-sharing application it uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application.Which solution meets these requirements'?

A.Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer.Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.

B.Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers.Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.

C.Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer.Move the database to a memory optimized instance type to store and serve users' images.

D.Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers.Move the database to an Amazon RDS instance with a Multi-AZ deployment Use Amazon S3 to store and serve users' images.

正确答案 D

**解析:**

ExplanantionKeyword: Highly available + Least amount of changes to the application High Availability = Multi-AZLeast amount of changes to the application = Elastic Beanstalk Automatically handles thedeployment, from Capacity provisioning, Load Balancing, Auto Scaling to application health monitoringOption - D will be the right choice and Option - A; Option - B and Option - C out of race due to Cost & inter-operability.HA with Elastic Beanstalk and RDSAWS Elastic BeanstalkAWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.There is no additional charge for Elastic Beanstalk - you pay only for the AWS resources needed to store and run your applications.AWS RDSAmazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.Amazon RDS is available on several database instance types - optimized for memory, performance or I/O - and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. You can use the AWS Database Migration Service to easily migrate or replicate your existing databases to Amazon RDS.AWS S3Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry- leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet

your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.References:https://aws.amazon.com/elasticbeanstalk/?nc2=h_ql_prod_cp_ebs
https://aws.amazon.com/rds/?nc2=h_ql_prod_db_rdshttps://aws.amazon.com/s3/?nc2=h_ql_prod_st_s3Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws- elastic-beanstalk/https://digitalcloud.training/certification-training/aws-solutions-architect- associate/database/amazon-rds/

Q105. A web application is deployed in the AWS Cloud It consists of a two-tier architecture that includes a web layer and a database layer.The web server is vulnerable to cross-site scripting (XSS) attacks. What should a solutions architect do to remediate the vulnerability?

A.Create a Classic Load Balancer.Put the web layer behind the load balancer and enable AWS WAF.

B.Create a Network Load Balancer.Put the web layer behind the load balancer and enable AWS WAF.

C.Create an Application Load Balancer.Put the web layer behind the load balancer and enable AWS WAF.

D.Create an Application Load Balancer.Put the web layer behind the load balancer and use AWS Shield Standard.

正确答案 C

**解析:**

The AWS Web Application Firewall (WAF) is available on the Application Load Balancer (ALB). You can use AWS WAF directly on Application Load Balancers (both internal and external) in a VPC, to protect your websites and web services.Attackers sometimes insert scripts into web

requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF to inspect for possible malicious scripts.CORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is the correct answer.INCORRECT: "Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a classic load balancer. INCORRECT: "Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a network load balancer. INCORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard" is incorrect as you cannot use AWS Shield to protect against XSS attacks. Shield is used to protect against DDoS attacks.References:https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity- compliance/aws-waf-and-shield/

Q106. A recently acquired company is required to buikl its own infrastructure on AWS and migrate multiple applications to the cloud within a month.Each application has approximately 50 TB of data to be transferred. After the migration is complete this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity.Which solution will meet these requirements''

A.AWS Direct Connect for both the initial transfer and ongoing connectivity

B.AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity

C.AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity

D.AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

正确答案 C

**解析:**

"Each application has approximately 50 TB of data to be transferred" = AWS Snowball; "secure network connectivity with consistent throughput from their data centers to the applications" What are the benefits of using AWS Direct Connect and private network connections? In many circumstances, private network connections can reduce costs, increase bandwidth, and provide a more consistent network experience than Internet-based connections. "more consistent network experience", hence AWS Direct Connect.Direct Connect is better than VPN; reduced cost+increased bandwith+(remain connection or consistent network) = direct connect

Q107. Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world The files are stored in an Amazon S3 bucket.A solutions architect has been asked to design an efficient and effective solution. Which action should the solutions architect take to accomplish this?

A.Generate presigned URLs for the files

B.Use cross-Region replication to all Regions

C.Use the geoproximity feature of Amazon Route 53

D.Use Amazon CloudFront with the S3 bucket as its origin

正确答案 D

**解析:**

Amazon CloudFront can be used to cache the files in edge locations around the world and this will improve the performance of the webpages.To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:Using a REST API endpoint as the origin with access restricted by an origin access identity (OAI) Using a website endpoint as the origin with anonymous (public) access allowed Using a website endpoint as the origin with access restricted by a Referer header CORRECT:"Use Amazon CloudFront with the S3 bucket as its origin" is the correct answer. INCORRECT: "Generate presigned URLs for the files" is incorrect as this is used to restrict access which is not a requirement.INCORRECT: "Use cross-Region replication to all Regions" is incorrect as this does not provide a mechanism for directing users to the closest copy of the static webpages. INCORRECT: "Use the geoproximity feature of Amazon Route 53" is incorrect as this does not include a solution for having multiple copies of the data in different geographic locations.References:https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/ Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-cloudfront/

Q108. A company runs an application on a group of Amazon Linux EC2 instances, The application writes log files using standard API calls For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently.Which storage service should a solutions architect use to provide the MOST cost-effective solution?

A.Amazon EBS

B.Amazon EFS

C.Amazon EC2 instance store

D.Amazon S3

正确答案 D

**解析:**

The application is writing the files using API calls which means it will be compatible with Amazon S3 which uses a REST API. S3 is a massively scalable key-based object store that is well-suited to allowing concurrent access to the files from many instances. Amazon S3 will also be the most cost-effective choice. A rough calculation using the AWS pricing calculator shows the cost differences between 1TB of storage on EBS, EFS, and S3 Standard.CORRECT: "Amazon S3" is the correct answer.INCORRECT: "Amazon EFS" is incorrect as though this does offer concurrent access from many EC2 Linux instances, it is not the most cost-effective solution. INCORRECT: "Amazon EBS" is incorrect. The Elastic Block Store (EBS) is not a good solution for concurrent access from many EC2 instances and is not the most cost-effective option either. EBS volumes are mounted to a single instance except when using multi-attach which is a new feature and has several constraints.INCORRECT: "Amazon EC2 instance store" is incorrect as this is an ephemeral storage solution which means the data is lost when powered down.Therefore, this is not an option for long-term data storage.References:https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/

Q109. A company's application is running on Amazon EC2 instances m a single Region in the event of a disaster a solutions architect needs to ensure that the resources can also be deployed to a second Region.Which combination of actions should the solutions architect take to accomplish this-? (Select TWO)

A. Detach a volume on an EC2 instance and copy it to Amazon S3

B. Launch a new EC2 instance from an Amazon Machine image (AMI) in a new Region

C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance

D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination

E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume

正确答案 B,D

**解析:**

Cross Region EC2 AMI Copy - We know that you want to build applications that span AWS Regions and we're working to provide you with the services and features needed to do so. We started out by launching the EBS Snapshot Copy feature late last year. This feature gave you the ability to copy a snapshot from Region to Region with just a couple of clicks. In addition, last month we made a significant reduction (26% to 83%) in the cost of transferring data between AWS Regions, making it less expensive to operate in more than one AWS region. Today we are introducing a new feature: Amazon Machine Image (AMI) Copy. AMI Copy enables you to easily copy your Amazon Machine Images between AWS Regions. AMI Copy helps enable several key scenarios including: Simple and Consistent Multi-Region Deployment "" You can copy an AMI from one region to another, enabling you to easily launch consistent instances based on the same AMI into different regions. Scalability "" You can more easily design and build world-scale applications that meet the needs of your users, regardless of their location. Performance "" You can increase performance by distributing your application and locating critical components of your application in closer proximity to your users. You can also take advantage of region-specific features such as instance types or other AWS services. Even Higher Availability "" You can design and deploy applications across AWS regions, to increase

availability. Once the new AMI is in an Available state the copy is complete. Reference: https://aws.amazon.com/blogs/aws/ec2-ami-copy-between-regions/

Q110. A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet Security is a high priority for the company.How should security groups be configured in this situation? (Select TWO)

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0

B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0

C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier

D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier

E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier

正确答案 A,C

**解析:**

In this scenario an inbound rule is required to allow traffic from any internet client to the web front end on SSL/TLS port 443. The source should therefore be set to 0.0.0.0/0 to allow any inbound traffic.To secure the connection from the web frontend to the database tier, an outbound rule should be created from the public EC2 security group with a destination of the private EC2 security group. The port should be set to 1433 for MySQL. The private EC2 security group will also need to allow inbound traffic on 1433 from the public EC2 security group.This

configuration can be seen in the diagram:CORRECT: "Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0" is a correct answer.CORRECT: "Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier" is also a correct answer. INCORRECT: "Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0" is incorrect as this is configured backwards. INCORRECT: "Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier" is incorrect as the MySQL database instance does not need to send outbound traffic on either of these ports. INCORRECT: "Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier" is incorrect as the database tier does not need to allow inbound traffic on port 443.References:https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-vpc/

Q111. A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only.What is the MOST cost-effective solution?

A.Amazon S3 Glacier

B.Amazon S3 Standard

C.Amazon S3 intelligent-Tiering

D.Amazon S3 One Zone-Infrequent Access {S3 One Zone-IA)

正确答案 B

**解析:**

S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object.CORRECT: "Amazon S3 Standard" is the correct answer.INCORRECT: "Amazon S3 Intelligent-Tiering" is incorrect as there is an additional fee for using this service and for a short-term requirement it may not be beneficial. INCORRECT: "Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as this storage class has a minimum capacity charge per object (128 KB) and a per GB retrieval fee. INCORRECT: "Amazon S3 Glacier Deep Archive" is incorrect as this storage class is used for archiving data. There are retrieval fees and it take hours to retrieve data from an archive.References:https://aws.amazon.com/s3/storage-classes/Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/

Q112. A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user- uploaded documents in an Amazon EBS volume.For better scalability and availability the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone: placing both behind an Application Load Balancer.After completing this change users reported that each time they refreshed the website they could see one subset of their documents or the other but never all of the documents at the same time. What should a solutions architect propose to ensure users see all of their documents at once''

A. Copy the data so both EBS volumes contain all the documents.

B. Configure the Application Load Balancer to direct a user to the server with the documents.

C. Copy the data from both EBS volumes to Amazon EFS.Modify the application to save new documents to Amazon EFS.

D. Configure the Application Load Balancer to send the request to both servers.Return each document from the correct server.

正确答案C

**解析:**

While both EBS and EFS offer great features, these two storage solutions are actually built for two completely different uses. EBS volumes are limited to a single instance, and, more importantly, then can only be accessed by one instance at a time. With EFS, you can have hundreds or thousands of instances accessing the file system simultaneously. This makes AWS EFS a great fit for any use that requires a decent performing centralized shared storage — uses like media processing or shared code repositories. user will never get all the documents at one place in other solutions .
https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2

Q113. You are building infrastructure for a data warehousing solution and an extra request has come through that there will be a lot of business reporting queries running all the time and you are not sure if your current DB instance will be able to handle it. What would be the best solution for this?

A.DB Parameter Groups

B.Read Replicas

C.Multi-AZ DB Instance deployment

D.Database Snapshots

正确答案B

**解析:**

Read Replicas make it easy to take advantage of MySQL's built-in replication functionality to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. There are a variety of scenarios where deploying one or more Read Replicas for a given source DB Instance may make sense. Common reasons for deploying a Read Replica include:Scaling beyond the compute or I/O capacity of a single DB Instance for read-heavy database workloads. This excess read traffic can be directed to one or more Read Replicas. Serving read traffic while the source DB Instance is unavailable. If your source DB Instance cannot take I/O requests (e.g. due to I/O suspension for backups or scheduled maintenance), you can direct read traffic to your Read Replica(s). For this use case, keep in mind that the data on the Read Replica may be "stale" since the source DB Instance is unavailable. Business reporting or data warehousing scenarios; you may want business reporting queries to run against a Read Replica, rather than your primary, production DB Instance.Reference: https://aws.amazon.com/rds/faqs/

Q114. In DynamoDB, could you use IAM to grant access to Amazon DynamoDB resources and API actions?

A.In DynamoDB there is no need to grant access

B.Depended to the type of access

C.No

D.Yes

正确答案 D

**解析:**

Amazon DynamoDB integrates with AWS Identity and Access Management (IAM). You can use AWS IAM to grant access to Amazon DynamoDB resources and API actions. To do this, you first write an AWS IAM policy, which is a document that explicitly lists the permissions you want to grant. You

then attach that policy to an AWS IAM user or role.Reference:http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/UsingIAMWithDDB.html

Q115. Much of your company's data does not need to be accessed often, and can take several hours for retrieval time, so it's stored on Amazon Glacier. However someone within your organization has expressed concerns that his data is more sensitive than the other data, and is wondering whether the high level of encryption that he knows is on S3 is also used on the much cheaper Glacier service. Which of the following statements would be most applicable in regards to this concern?

A.There is no encryption on Amazon Glacier, that's why it is cheaper.

B.Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method than Amazon S3 but you can change it to AES-256 if you are willing to pay more.

C.Amazon Glacier automatically encrypts the data using AES-256, the same as Amazon S3.

D.Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method than Amazon S3.

正确答案 C

**解析:**

Like Amazon S3, the Amazon Glacier service provides low-cost, secure, and durable storage. But where S3 is designed for rapid retrieval, Glacier is meant to be used as an archival service for data that is not accessed often, and for which retrieval times of several hours are suitable. Amazon Glacier automatically encrypts the data using AES-256 and stores it durably in an immutable form. Amazon Glacier is designed to provide average annual durability of 99.999999999% for an archive. It stores each archive in multiple facilities and multiple devices. Unlike traditional systems which can require laborious data verification and

manual repair, Glacier performs regular, systematic data integrity checks, and is built to be automatically self-healing. Reference: http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

Q116. Your EBS volumes do not seem to be performing as expected and your team leader has requested you look into improving their performance. Which of the following is not a true statement relating to the performance of your EBS volumes?

A.Frequent snapshots provide a higher level of data durability and they will not degrade the performance of your application while the snapshot is in progress.

B.General Purpose (SSD) and Provisioned IOPS (SSD) volumes have a throughput limit of 128 MB/s per volume.

C.There is a relationship between the maximum performance of your EBS volumes, the amount of I/O you are driving to them, and the amount of time it takes for each transaction to complete.

D.There is a 5 to 50 percent reduction in IOPS when you first access each block of data on a newly created or restored EBS volume

正确答案 A

**解析:**

Several factors can affect the performance of Amazon EBS volumes, such as instance configuration, I/O characteristics, workload demand, and storage configuration. Frequent snapshots provide a higher level of data durability, but they may slightly degrade the performance of your application while the snapshot is in progress. This trade off becomes critical when you have data that changes rapidly. Whenever possible, plan for snapshots to occur during off-peak times in order to minimize workload impact.Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html

Q117. You've created your first load balancer and have registered your EC2 instances with the load balancer. Elastic Load Balancing routinely performs health checks on all the registered EC2 instances and automatically distributes all incoming requests to the DNS name of your load balancer across your registered, healthy EC2 instances. By default, the load balancer uses the ___ protocol for checking the health of your instances.

A.HTTPS

B.HTTP

C.ICMP

D.IPv6

正确答案 B

**解析:**

In Elastic Load Balancing a health configuration uses information such as protocol, ping port, ping path (URL), response timeout period, and health check interval to determine the health state of the instances registered with the load balancer.Currently, HTTP on port 80 is the default health
check.Reference:http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyCo ncepts.html

Q118. A major finance organisation has engaged your company to set up a large data mining application. Using AWS you decide the best service for this is Amazon Elastic MapReduce(EMR) which you know uses Hadoop. Which of the following statements best describes Hadoop?

A.Hadoop is 3rd Party software which can be installed using AMI

B.Hadoop is an open source python web framework

C.Hadoop is an open source Java software framework

D.Hadoop is an open source javascript framework

正确答案C

**解析:**

Amazon EMR uses Apache Hadoop as its distributed data processing engine. Hadoop is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware. Hadoop implements a programming model named "MapReduce," where the data is divided into many small fragments of work, each of which may be executed on any node in the cluster.This framework has been widely used by developers, enterprises and startups and has proven to be a reliable software platform for processing up to petabytes of data on clusters of thousands of commodity machines.Reference: http://aws.amazon.com/elasticmapreduce/faqs/

Q119. In Amazon EC2 Container Service, are other container types supported?

A.Yes, EC2 Container Service supports any container service you need.

B.Yes, EC2 Container Service also supports Microsoft container service.

C.No, Docker is the only container platform supported by EC2 Container Service presently.

D.Yes, EC2 Container Service supports Microsoft container service and Openstack.

正确答案C

**解析:**

In Amazon EC2 Container Service, Docker is the only container platform supported by EC2 Container Service presently.Reference: http://aws.amazon.com/ecs/faqs/

Q120. A Solutions Architect is designing the architecture for a web application that will be hosted on AWS. Internet users will access the application using HTTP and HTTPS.How should the Architect design the traffic control requirements?

A. Use a network ACL to allow outbound ports for HTTP and HTTPS. Deny other traffic for inbound and outbound.

B. Use a network ACL to allow inbound ports for HTTP and HTTPS. Deny other traffic for inbound and outbound.

C. Allow inbound ports for HTTP and HTTPS in the security group used by the web servers.

D. Allow outbound ports for HTTP and HTTPS in the security group used by the web servers.

正确答案 C

**解析:**

Unlike a traditional web hosting model, inbound network traffic filtering should not be confined to the edge; it should also be applied at the host level. Amazon EC2 provides a feature named security groups. A security group is analogous to an inbound network firewall, for which you can specify the protocols, ports, and source IP ranges that are allowed to reach your EC2 instances. You can assign one or more security groups to each EC2 instance. Each security group routes the appropriate traffic to each instance. Security groups can be configured so that only specific subnets or IP addresses have access to an EC2 instance. Or they can reference other security groups to limit access to EC2 instances that are in specific groups. because we have to select only 1 option. If we had to select 2 Answer and another option would have been something like NACL allowing inbound and outbound access then that would also have been answer. Reference: https://d1.awsstatic.com/whitepapers/aws-web-hosting-best-practices.pdf

Q121. A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed.The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started.Once completed, the system is expected to run for a minimum of 1 year. Which type of Amazon EC2 instances should be used to reduce the cost of the system?

A.Spot Instances

B.On-Demand Instances

C.Standard Reserved Instances

D.Scheduled Reserved Instances

正确答案 D

**解析:**

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week. CORRECT: "Scheduled Reserved Instances" is the correct answer. INCORRECT: "Standard Reserved Instances" is incorrect as the workload only runs for 4 hours a day this would be more expensive.INCORRECT: "On-Demand Instances" is incorrect as this would be much more expensive as there is no discount applied.INCORRECT: "Spot Instances" is incorrect as the workload cannot be interrupted once started. With Spot instances workloads can be terminated if the Spot price changes or capacity is required.References:https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/

ec2-scheduled-instances.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/compute/amazon-ec2/

Q122. A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost- effective solution. What should a solutions architect do to accomplish this?

A.Copy the website content to an Amazon S3 bucket.Configure the bucket to serve static webpage content.Replicate the S3 bucket to multiple AWS Regions

B.Copy the website content to an Amazon S3 bucket.Configure the bucket to serve static webpage content.Configure Amazon CloudFront with the S3 bucket as the origin

C.Copy the website content to an Amazon EBS-backed.Amazon EC2 instance running Apache HTTP Server.Configure Amazon Route 53 geolocation routing policies to select the closest origin

D.Copy the website content to multiple Amazon EBS-backed.Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions.Configure Amazon CloudFront geolocation routing policies to select the closest origin

正确答案 B

**解析:**

The most cost-effective option is to migrate the website to an Amazon S3 bucket and configure that bucket for static website hosting. To enable good performance for global users the solutions architect should then configure a CloudFront distribution with the S3 bucket as the origin. This will cache the static content around the world closer to users. CORRECT: "Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with

the S3 bucket as the origin" is the correct answer.INCORRECT: "Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions" is incorrect as there is no solution here for directing users to the closest region. This could be a more cost-effective (though less elegant) solution if AWS Route 53 latency records are created. INCORRECT: "Copy the website content to an Amazon EC2 instance. Configure Amazon Route 53 geolocation routing policies to select the closest origin" is incorrect as using Amazon EC2 instances is less cost-effective compared to hosting the website on S3. Also, geolocation routing does not achieve anything with only a single record.INCORRECT: "Copy the website content to multiple Amazon EC2 instances in multiple AWS Regions. Configure AWS Route 53 geolocation routing policies to select the closest region" is incorrect as using Amazon EC2 instances is less cost-effective compared to hosting the website on S3.References:https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/ Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

Q123. A solutions architect is implementing a document review application using an Amazon S3 bucket for storage.The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available.Users must be able to download, modify, and upload documents. Which combination of actions should be taken to meet these requirements'? (Select TWO )

A. Enable a read-only bucket ACL

B. Enable versioning on the bucket

C. Attach an IAM policy to the bucket

D. Enable MFA Delete on the bucket

E. Encrypt the bucket using AWS KMS

正确答案 B,D

**解析:**

None of the options present a good solution for specifying permissions required to write and modify objects so that requirement needs to be taken care of separately. The other requirements are to prevent accidental deletion and the ensure that all versions of the document are available. The two solutions for these requirements are versioning and MFA delete. Versioning will retain a copy of each version of the document and multi-factor authentication delete (MFA delete) will prevent any accidental deletion as you need to supply a second factor when attempting a delete. CORRECT: "Enable versioning on the bucket" is a correct answer. CORRECT: "Enable MFA Delete on the bucket" is also a correct answer. INCORRECT: "Set read-only permissions on the bucket" is incorrect as this will also prevent any writing to the bucket which is not desired.INCORRECT: "Attach an IAM policy to the bucket" is incorrect as users need to modify documents which will also allow delete. Therefore, a method must be implemented to just control deletes.INCORRECT: "Encrypt the bucket using AWS SSE-S3" is incorrect as encryption doesn't stop you from deleting an object.References:https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/

Q124. A company built a food ordering application that captures user data and stores it for future analysis.The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance.The backend application then stores the data in Amazon RDS What

should a solutions architect do to decouple the architecture and make it scalable''

A.Use Amazon S3 to serve the front-end application which sends requests to Amazon EC2 to execute the backend application.The backend application will process and store the data in Amazon RDS

B.Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic.Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS

C.Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue.Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS

D.Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue.Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS

正确答案 D

**解析:**

ExplanationKeyword: Static + Decouple + ScalableStatic=S3Decouple=SQS QueueScalable=ASGOption B will not be there in the race due to Auto-Scaling unavailability. Option A will not be there in the race due to Decouple unavailability. Option C & D will be in the race and Option D will be correct answers due to all 3 combination matches [Static=S3; Decouple=SQS Queue; Scalable=ASG] & Option C will loose due to Static option unavailabilityReference:Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-api-gateway/https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application- integration/amazon-sqs/https://digitalcloud.training/certification-training/aws-solutions-

architect-associate/compute/aws- auto-scaling/https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/https://digitalcloud.training/certification-training/aws-solutions-architect- associate/database/amazon-rds/

Q125. A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access.Which of the following would be the LEAST complicated implementation?

A. Use an Amazon CloudFront distribution with an origin access identity (OAI) Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLsDesign a Lambda function to remove data that is older than 14 days

B. Use an S3 bucket and provide direct access to the tile Design the application to track purchases in a DynamoDH table Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB

C. Use an Amazon CloudFront distribution with an OAIConfigure the distribution with an Amazon S3 origin to provide access to the file through signed URLsDesign the application to sot an expiration of 14 days for the URL

D. Use an Amazon CloudFront distribution with an OAIConfigure the distribution with an Amazon S3 origin to provide access to the file through signed URLsDesign the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary

正确答案 C

**解析:**

Justification: Since no mention of the signature version in the question, I assume using signature v2, you can setup the pre-signed URL to expire in 7-days. This will be the least complicated

Q126. A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.What should a solutions architect do to accomplish this?

A. Use Amazon S3 with Transfer Acceleration to host the application.

B. Use Amazon S3 with CacheControl headers to host the application.

C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.

D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

正确答案 A

**解析:**

这一题是争议题，A 和 C 之间，我们保留 A 作为正确答案。

A is the correct answer as per below s3 faq on official site as requirement is Gigabytes of file size.

Q:How should I choose between S3 Transfer Acceleration and Amazon CloudFront's PUT/POST?

S3 Transfer Acceleration optimizes the TCP protocol and adds additional intelligence between the client and the S3 bucket, making S3 Transfer Acceleration a better choice if a higher throughput is desired. If you have objects that are smaller than 1GB or if the data set is less than 1GB in size, you should consider using Amazon CloudFront's PUT/POST commands for optimal performance.

Option A is correct. Option C is incorrect. Because Amazon Cloudfront's

usage is not for uploading, it's only for downloading. Additional, Amazon Auto Scaling Group is only in a Region, not for multi-regions or across-regions.

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

认为是C答案的分析

Second, your users can now benefit from accelerated content uploads. After you enable the additional HTTP methods for your application's distribution, PUT and POST operations will be sent to the origin (e.g. Amazon S3) via the CloudFront edge location, improving efficiency, reducing latency, and allowing the application to benefit from the monitored, persistent connections that CloudFront maintains from the edge locations to the origin servers.

https://aws.amazon.com/blogs/aws/amazon-cloudfront-content-uploads-post-put-other-methods/



Q127. A company captures clickstream data from multiple websites and analyzes it using batch processing.The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead. Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

A.Amazon EC2

B.AWS Lambda

C.Amazon Kinesis Data Streams

D.Amazon Kinesis Data Firehose

E.Amazon Kinesis Data Analytics

正确答案 D,E

**解析:**

A) Amazon EC2 - ExpensiveB) AWS lambda - Non Minimal EffortC) Kinesis Data Stream - Non Near Real TimeD) Kinesis Data Firehose- By default the manner to ingest Data - CORRECT E) Kinesis Data Analytics- We need perform analytics - CORRECT
https://d0.awsstatic.com/whitepapers/whitepaper-streaming-data-solutions-on-aws-with- amazonkinesis.pdf
(9)https://aws.amazon.com/kinesis/#Evolve_from_batch_to_real-time_analytics

Q128. A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries.These performance issues were caused by users generating different real-time reports from the application duringworking hours.Which solution will improve the performance of the application when it is moved to AWS?

A.Import the data into an Amazon DynamoDB table with provisioned capacity.Refactor the application to use DynamoDB for reports.

B.Create the database on a compute optimized Amazon EC2 instance.Ensure compute resources exceed the on-premises database.

C.Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas.Configure the application reader endpoint for reports.

D.Create an Amazon Aurora MySQL Multi-AZ DB cluster.Configure the application to use the backup instance of the cluster as an endpoint for the reports.

正确答案 C

**解析:**

The MySQL-compatible edition of Aurora delivers up to 5X the throughput of standard MySQL running on the same hardware, and enables existing MySQL applications and tools to run without requiring modification.https://aws.amazon.com/rds/aurora/mysql-features/

Q129. A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.What should a solutions architect do to accomplish this?

A. Provision EC2 instances in us-west-1.Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.

B. Provision EC2 instances and an Application Load Balancer in us-west-1.Make the load balancer distribute the traffic based on the location of the request.

C. Provision EC2 instances and configure an Application Load Balancer in us-west-1.Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.

D. Provision EC2 instances and configure an Application Load Balancer in us-west-1.Configure Amazon Route 53 with a weighted routing policy.Create alias records in Route 53 that point to the Application Load Balancer.

正确答案 C

**解析:**

D is using weight policy which can not be right, at least it should use latency policy. D 如果加个 CloudFront 的话， 可以选 D, 但是 D 又没有说，所以我觉得还是应该选 C, 因为 Accelerator 能够从边缘站点到区域，所以肯定

是 C 的效率高， AWS Global Accelerator provides traffic management across multiple Regions [...] AWS Global Accelerator complements ELB by extending these capabilities beyond a single AWS Region, allowing you to provision a global interface for your applications in any number of Regions. If you have workloads that cater to a global client base, we recommend that you use AWS Global Accelerator. If you have workloads hosted in a single AWS Region and used by clients in and around the same Region, you can use an Application Load Balancer or Network Load Balancer to manage your resources." https://aws.amazon.com/global-accelerator/faqs/

Q130. A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset.The company's disaster recovery policy states that all data multiple AWS Regions. How should a solutions architect design the S3 solution?

A.Create an additional S3 bucket in another Region and configure cross-Region replication.

B.Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).

C.Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.

D.Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

正确答案 C

**解析:**

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region.

Both source and destination buckets must have versioning enabled. CORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-Region replication" is the correct answer.INCORRECT: "Create an additional S3 bucket in another Region and configure cross-Region replication" is incorrect as the destination bucket must also have versioning enabled. INCORRECT: "Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication. INCORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication.References:https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/

Q131. A company has application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications. Which action will fulfill these requirements and maintain security?

A.Configure an S3 interface endpoint.

B.Configure an S3 gateway endpoint.

C.Create an S3 bucket in a private subnet.

D.Create an S3 bucket in the same Region as the EC2 instance.

正确答案 B

**解析:**

Gateway Endpoint for S3 and DynamoDBhttps://medium.com/tensult/aws-vpc-endpoints-introduction-ef2bf85c4422

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html
https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html

Q132. A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data.During the financial closing period at the start of every month. Accountants run large queries that impact the database's performance due to high usage.The company wants to minimize the impact that the reporting activity has on the web application. What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

A.Create a read replica and direct reporting traffic to the replica.

B.Create a Multi-AZ database and direct reporting traffic to the standby.

C.Create a cross-Region read replica and direct reporting traffic to the replica.

D.Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

正确答案 A

**解析:**

Amazon RDS uses the MariaDB, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server DB engines' built-in replication functionality to create a special type of DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica.https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Q133. A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.Which pricing model should the company choose?

A.Reserved Instances

B.Spot Block Instances

C.On-Demand Instances

D.Scheduled Reserved Instances

正确答案 D

**解析:**

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html

Q134. A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.Which configuration should the solutions architect choose to meet these requirements?

A.Configure Amazon CloudFront with AWS WAF.

B.Configure Application Load Balancers with AWS WAF.

C.Configure Amazon Route 53 with a geolocation policy.

D.Configure Amazon Route 53 with a geoproximity routing policy.

正确答案 C

**解析:**

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html (geolocation routing)

Q135. A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage.There are other internal systems that query this DB instance to fetch data for internal batch processing.The RDS DB instance slows down significantly the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times.Which solution will improve the website's performance?

A. Use an RDS PostgreSQL DB instance instead of a MySQL database.

B. Use Amazon ElastiCache to cache the query responses for the website.

C. Add an additional Availability Zone to the current RDS MySQL Multi.AZ DB instance.

D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

正确答案 D

**解析:**

Amazon RDS Read Replicas- Enhanced performance- You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. Read replicas allow you to elastically

scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Because read replicas can be promoted to master status, they are useful as part of a sharding implementation. To further maximize read performance, Amazon RDS for MySQL allows you to add table indexes directly to Read Replicas, without those indexes being present on the master. Reference:
https://aws.amazon.com/rds/features/read-replicas

Q136. A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux.The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.Which storage option would be the optimal solution?

A. Amazon Elastic File System (Amazon EFS)

B. Amazon FSx for Lustre

C. Amazon EC2 instance store

D. Amazon EBS Provisioned IOPS SSD (io1)

正确答案 B

**解析:**

Amazon FSx for Lustre makes it easy and cost effective to launch and run the world ' s most popular high-performance file system. Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.
https://aws.amazon.com/fsx/lustre/
https://d1.awsstatic.com/whitepapers/AWS%20Partner%20Network_HPC%20Storage%200ption s_2019_FINAL.pdf (p.8)

Q137. A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS.The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft

Active Directory domain controller that was install recently to support other AWS services.A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff.What should the solutions architect recommend?

A.Use AWS Directory Service to create a managed Active Directory.Uninstall Active Directory on the current EC2 instance.

B.Create another EC2 instance in the same subnet and reinstall Active Directory on it.Uninstall Active Directory.

C.Use AWS Directory Service to create an Active Directory connector.Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.

D.Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller.Modify the EC2 instance's security group to deny public access to Active Directory.

正确答案 A

**解析:**

Migrate AD to AWS Managed AD and keep the webserver alone.. Reduce risk = remove AD from that EC2. Minimize admin = remove AD from any EC2-> use AWS Directory ServiceActive Directory connector is only for ON-PREM AD. The one they have exists in the cloud already.

Q138. A company runs an application in a branch office within a small data closet with no virtualized compute resources.The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.Which solution meet these requirements?

A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.

B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.

C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.

D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

正确答案 A

**解析:**

https://aws.amazon.com/storagegateway/file/

AWS Storage Gateway Hardware Appliance

Hardware Appliance

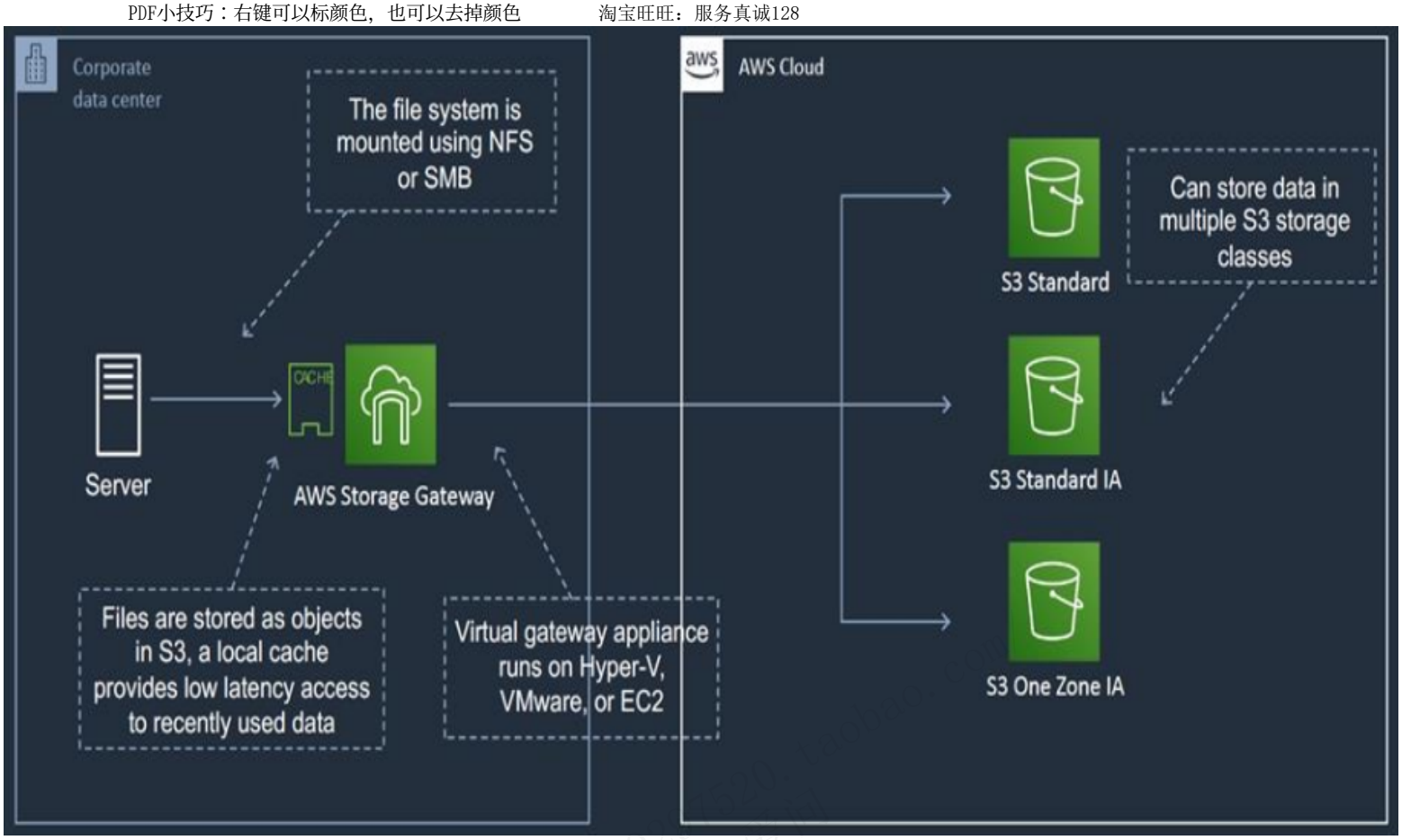
Storage Gateway is available as a hardware appliance, adding to the existing support for VMware ESXi, Microsoft Hyper-V, and Amazon EC2. This means that you can now make use of Storage Gateway in situations where you do not have a virtualized environment, server-class hardware or IT staff with the specialized skills that are needed to manage them. You can order appliances from Amazon.com for delivery to branch offices, warehouses, and “outpost” offices that lack dedicated IT resources. Setup (as you will see in a minute) is quick and easy, and gives you access to three storage solutions:

File Gateway C A file interface to Amazon S3, accessible via NFS or SMB. The files are stored as S3 objects, allowing you to make use of specialized S3 features such as lifecycle management and cross-region replication. You can trigger AWS Lambda functions, run Amazon Athena queries, and use Amazon Macie to discover and classify sensitive data.

https://aws.amazon.com/blogs/aws/new-aws-storage-gateway-hardware-appliance/

原来是B答案的解释 Keyword: NFS + Compliance File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2- resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching. File Gateway AWS Storage Gateway The table below shows the different gateways available and the interfaces and use cases:

Storage Gateway Overview CORRECT: "Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3" is the correct answer. INCORRECT: "Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3" is incorrect. INCORRECT: "Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3" is incorrect as unsupported NFS. INCORRECT: "Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3" is incorrect as unsupported NFS.



| New Name | Old Name | Interface | Use Case |
|---|---|---|---|
| File Gateway | None | NFS, SMB | Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount points |
| Volume Gateway Stored Mode | Gateway-Stored Volumes | iSCSI | Asynchronous replication of on-prem data to S3 |
| Volume Gateway Cached Mode | Gateway-Cached Volumes | iSCSI | Primary data stored in S3 with frequently accessed data cached locally on-prem |
| Tape Gateway | Gateway-Virtual Tape Library | ISCSI | Virtual media changer and tape library for use with existing backup software |

Q139. An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size.The application owner will make the log file available to the vendor for a limited time.What is the MOST secure way to do this?

A. Enable public read on the S3 object and provide the link to the vendor.

B. Upload the file to Amazon WorkDocs and share the public link with the vendor.

C. Generate a presigned URL and have the vendor download the log file before it expires.

D. Create an IAM user for the vendor to provide access to the S3 bucket and the application.Enforce multifactor authentication.

正确答案C

**解析:**

A and B providing public link which security concerns.
option D is not suitable because here in question it is a vendor user accessing a log file, here user use to access the application which is hosted in AWS he is not the one who has access permission to AWS console management so creating IAM is not feasible.
S3 - All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a presigned URL, using their own security credentials, to grant time-limited permission to download the objects.
CloudFront - Uses Signed URL and igned Cookies to allow user access to your files

Q140. A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an

Application Load Balancer in an Auto Scaling group.The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate.The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website. What should a solutions architect do to meet these requirements?

A. Redesign the application to use Amazon CloudFront.

B. Redesign the application to use AWS Elastic Beanstalk.

C. Redesign the application to use a Network Load Balancer.

D. Redesign the application to use Amazon S3 static website hosting.

正确答案 A

**解析:**

CloudFront to cache contents, ALB as Origin What Is Amazon CloudFront?
Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.
CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with
CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.
If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.
If the content is not in that edge location, CloudFront retrieves it from an origin that you've defined "" such as an Amazon S3 bucket, a MediaPackage channel, or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.
As an example, suppose that you're serving an image from a traditional web server, not from CloudFront. For example, you might serve an image,

[1]

Your users can easily navigate to this URL and see the image. But they probably don't know that their request was routed from one network to another "" through the complex collection of interconnected networks that comprise the internet "" until the image was found.

CloudFront speeds up the distribution of your content by routing each user request through the AWS backbone network to the edge location that can best serve your content. Typically, this is a CloudFront edge server that provides the fastest delivery to the viewer. Using the AWS network dramatically reduces the number of networks that your users' requests must pass through, which improves performance. Users get lower latency "" the time it takes to load the first byte of the file "" and higher data transfer rates.

You also get increased reliability and availability because copies of your files (also known as objects) are now held (or cached) in multiple edge locations around the world.

Reference:

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

Q141. A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost- effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete. What should the solutions architect do to meet these requirements?

A. Increase the minimum capacity for the Auto Scaling group.

B. Increase the maximum capacity for the Auto Scaling group.

C. Configure scheduled scaling to scale up to the desired compute level.

D. Change the scaling policy to add more EC2 instances during each scaling operation.

正确答案 C

**解析:**

scheduled autoscaling

Q142. An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2. and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns. Which action should be taken to improve the performance of the backend?

A. Implement Amazon SNS to store the database calls.

B. Implement Amazon ElastiCache to cache the large datasets.

C. Implement an RDS for MySQL read replica to cache database calls.

D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

正确答案 B

**解析:**

ElastiCache for Redis can be used as a primary in-memory key-value data store, providing fast, sub millisecond data performance, high availability and scalability up to 250 nodes and 250 shards, giving you up to 170.6 TB of in-memory data.

Q143. A company's application hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Due to data sensitivity, traffic cannot traverse the internet How should a solutions architect configure access?

A. Create a private hosted zone using Amazon Route 53.

B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.

C. Configure AWS PrivateLink between the EC2 instance and the S3 bucket.

D. Set up a site-to-site VPN connection between the VPC and the S3 bucket.

正确答案 B

**解析:**

Anytime the connection happens inside the same VPC

Q144. An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

A. Use a VPC endpoint for DynamoDB.

B. Use a NAT gateway in a public subnet.

C. Use a NAT instance in a private subnet.

D. Use the internet gateway attached to the VPC.

正确答案 A

**解析:**

Keyword: Private Subnets + Application needs to access DynamoDB.
Condition: Traffic does not leave the AWS Network.
DynamoDB = VPC Enpoint /VPC Gateway Endpoint.
Options - A - Win the battle, which securely access AWS PrivateLink endpoints across AWS Regions using Inter-Region VPC Peering
Options - B - Out of race, which is not meeting the condition Options - C - Out of race, which is not meeting the condition Options - D - Out of race, which is not meeting the condition VPC Enpoint.
An Interface endpoint uses AWS PrivateLink and is an elastic network

interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service.
Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.
AWS PrivateLink access over Inter-Region VPC Peering:
Applications in an AWS VPC can securely access AWS PrivateLink endpoints across AWS Regions using Inter-Region VPC Peering.
AWS PrivateLink allows you to privately access services hosted on AWS in a highly available and scalable manner, without using public IPs, and without requiring the traffic to traverse the Internet.
Customers can privately connect to a service even if the service endpoint resides in a different

AWS Region.
Traffic using Inter-Region VPC Peering stays on the global AWS backbone and never traverses

the public Internet.
A gateway endpoint is a gateway that is a target for a specified route in your route table, used
for traffic destined to a supported AWS service.
An interface VPC endpoint (interface endpoint) enables you to connect to services powered by

AWS PrivateLink.
The table below highlights some key information about both types of endpoint:

References:
https://aws.amazon.com/vpc/?nc2=h_ql_prod_nt_avpc
https://youtu.be/jZAvKgqlrjY

Save time with our exam-specific cheat sheets:
https://digitalcloud.training/certification-training/aws-solutions-

architect-associate/networking-and- content-delivery/amazon-vpc/
https://tutorialsdojo.com/amazon-vpc/

| | Interface Endpoint | Gateway Endpoint |
|---|---|---|
| What | Elastic Network Interface with a Private IP | A gateway that is a target for a specific route |
| How | Uses DNS entries to redirect traffic | Uses prefix lists in the route table to redirect traffic |
| Which services | API Gateway, CloudFormation, CloudWatch etc. | Amazon S3, DynamoDB |
| Security | Security Groups | VPC Endpoint Policies |

Q145. A solutions architect needs to design a low-latency solution for a static single-page application accessed by users utilizing a custom domain name. The solution must be serverless, encrypted in transit, and cost- effective.Which combination of AWS services and features should the solutions architect use? (Select TWO.)

A. Amazon S3

B. Amazon EC2

C. AWS Fargate

D. Amazon CloudFront

E. Elastic Load Balancer

正确答案 A,D

**解析:**

S3, Cloud Front - Serverless
S3- Static website with less cost
Cloud front - Low latency with less cost.

Q146. A company has global users accessing an application deployed in different AWS Regions, exposing public static IP addresses. The users are experiencing poor performance when accessing the application over the internet.What should a solutions architect recommend to reduce internet latency?

A. Set up AWS Global Accelerator and add endpoints.

B. Set up AWS Direct Connect locations in multiple Regions.

C. Set up an Amazon CloudFront distribution to access an application.

D. Set up an Amazon Route 53 geoproximity routing policy to route traffic.

正确答案 A

**解析:**

AWS Global Accelerator is a service in which you create accelerators to improve availability and performance of your applications for local and global users. Global Accelerator directs traffic to optimal endpoints over the AWS global network. This improves the availability and performance of your internet applications that are used by a global audience. Global Accelerator is a global service that supports endpoints in multiple AWS Regions, which are listed in the AWS Region Table.
By default, Global Accelerator provides you with two static IP

addresses that you associate with your accelerator. (Or, instead of using the IP addresses that Global Accelerator provides, you can configure these entry points to be IPv4 addresses from your own IP address ranges that you bring to Global Accelerator.)

The static IP addresses are anycast from the AWS edge network and distribute incoming application traffic across multiple endpoint resources in multiple AWS Regions, which increases the availability of your applications. Endpoints can be Network Load Balancers, Application Load Balancers, EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.

CORRECT: "Set up AWS Global Accelerator and add endpoints" is the correct answer. INCORRECT: "Set up AWS Direct Connect locations in multiple Regions" is incorrect as this is used to connect from an on-premises data center to AWS. It does not improve performance for users who are not connected to the on-premises data center. INCORRECT: "Set up an Amazon CloudFront distribution to access an application" is incorrect as CloudFront cannot expose static public IP addresses.

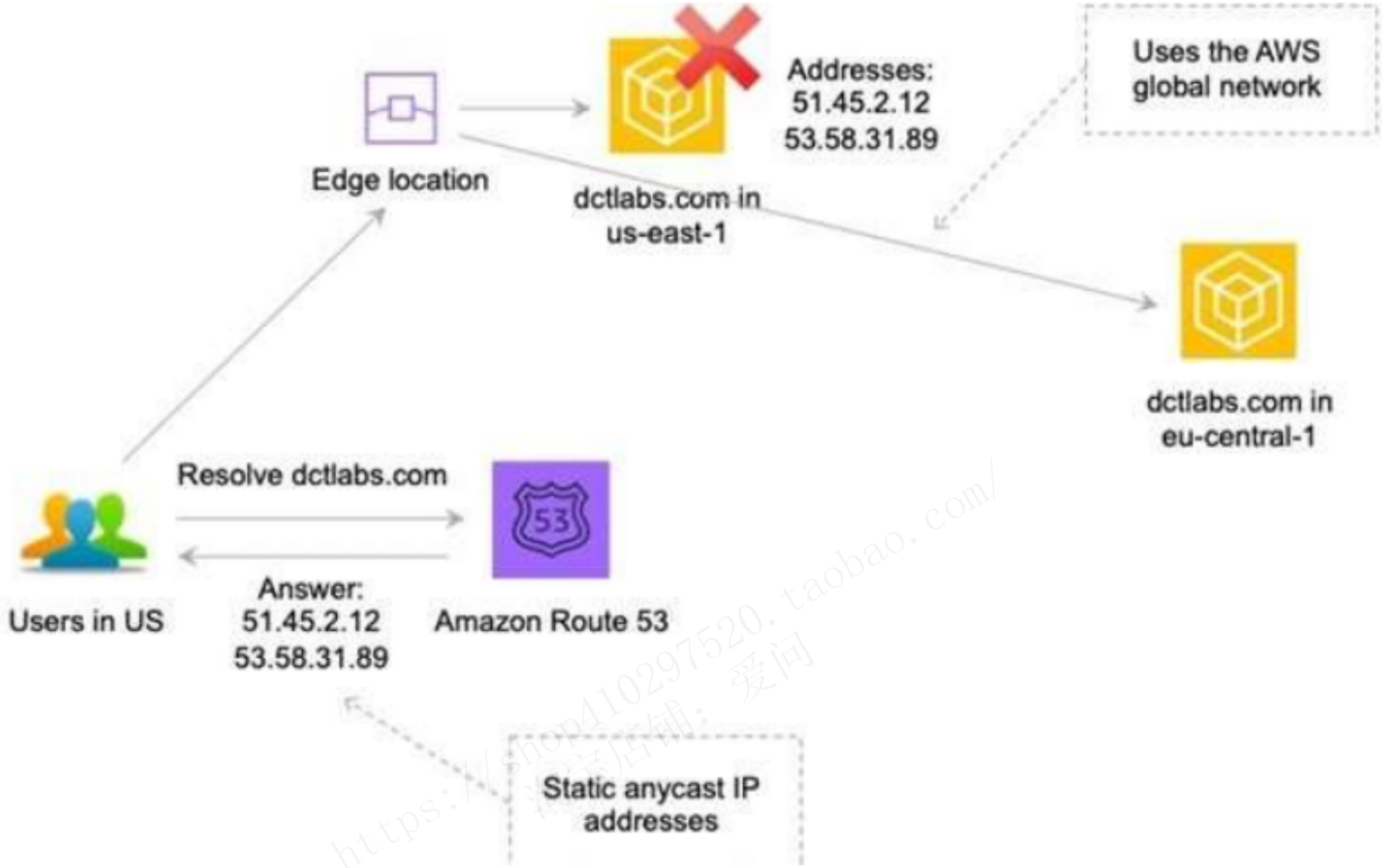
INCORRECT: "Set up an Amazon Route 53 geoproximity routing policy to route traffic" is incorrect as this does not reduce internet latency as well as using Global Accelerator. GA will direct users to the closest edge location and then use the AWS global network.

References:

https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html

Save time with our exam-specific cheat sheets:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/aws-global-accelerator/




Q147. An application requires a development environment (DEV) and production environment (PROD) for several years. The DEV instances will run for 10 hours each day during normal business hours, while the PROD instances will run 24 hours each day. A solutions architect needs to determine a compute instance purchase strategy to minimize costs.Which solution is the MOST cost-effective?

A. DEV with Spot Instances and PROD with On-Demand Instances

B. DEV with On-Demand Instances and PROD with Spot Instances

C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances

D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

正确答案 C

**解析:**

"Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week."

Q148. A solutions architect is designing a customer-facing application. The application is expected to have a variable amount of reads and writes depending on the time of year and clearly defined access patterns throughout the year. Management requires that database auditing and scaling be managed in the AWS Cloud. The Recovery Point Objective (RPO) must be less than 5 hours.Which solutions can accomplish this? (Select TWO.)

A. Use Amazon DynamoDB with auto scaling.Use on-demand backups and AWS CloudTrail.

B. Use Amazon DynamoDB with auto scaling.Use on-demand backups and Amazon DynamoDB Streams.

C. Use Amazon Redshift Configure concurrency scaling.Enable audit logging.Perform database snapshots every 4 hours.

D. Use Amazon RDS with Provisioned IOPS.Enable the database auditing parameter.Perform database snapshots every 5 hours.

E. Use Amazon RDS with auto scaling.Enable the database auditing parameter.Configure the backup retention period to at least 1 day.

正确答案 A,E

**解析:**

A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.
CORRECT - Scalable, with backup and AWS Managed Auditing
B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
INCORRECT - AWS DDB Streams can be used for auditing, but its not AWS managed auditing.
C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.
INCORRECT - Not a database. Datalake
D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5 hours.
INCORRECT - This does not scale
E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.
CORRECT - Scalable, AWS managed auditing and backup. The backup frequency is not stated but have no technical limitation which states it cannot be less 5 hours (1 day is retention period of the backup).
First, the question has 2 demands we need to understand it clearly.
1) Auditing and scaling
2) RPO should be less than 5 hrs.
We are talking about one data source where this is done. There is no point in the question that says we need to audit on a different data source and RPO on different data source.
Hence we must not mix and match the data sources.
There is no Audit for Red Shift hence C is out.
RDS had audit and RPO but the is 5 hrs and as per the question it should be less than 5 so the pair D and E is out.
What remains is A and B, which satisfy both the condition of the

question.
Hence Answer is A and B.

Q149. a website on Amazon S3. The website serves petabytes of outbound traffic monthly, which accounts for most of the company's AWS costs. What should a solutions architect do to reduce costs?

A. Configure Amazon CloudFront with the existing website as the origin.

B. Move the website to Amazon EC2 with Amazon EBS volumes for storage.

C. Use AWS Global Accelerator and specify the existing website as the endpoint.

D. Rearchitect the website to run on a combination of Amazon API Gateway and AWS Lambda.

正确答案 A

**解析:**

A textbook case for CloudFront. The data transfer cost in CloudFront is lower than in S3. With heavy read operations of static content, it's more economical to add CloudFront in front of you S3 bucket.

Q150. A solution architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group. A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

**Policy1**

```
{
    "Version": "2012-10-17", "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:Get*",
                "iam:List*",
                "kms:List*",
                "ec2:*",
                "ds:*",
                "logs:Get*",
                "logs:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

**Policy2**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ds:Delete*",
            "Resource": "*"
        }
    ]
}
```



A. Deleting IAM users

B. Deleting directories

C. Deleting Amazon EC2 instances

D. Deleting logs from Amazon CloudWatch Logs

正确答案 C

**解析:**

policy 2 不允许删除 directory

There is an explicit DENY on deleting directories in the second policy. So the only thing that can be deleted is EC2 instances as per the permission in the first policy.

Q151. A solutions architect is helping a developer design a new ecommerce shopping cart application using AWS services. The developer is unsure of the current database schema and expects to make changes as the

ecommerce site grows. The solution needs to be highly resilient and capable of automatically scaling read and write capacity.Which database solution meets these requirements?

A. Amazon Aurora PostgreSQL

B. Amazon DynamoDB with on-demand enabled

C. Amazon DynamoDB with DynamoDB Streams enabled

D. Amazon SQS and Amazon Aurora PostgreSQL

正确答案 B

Q152. A solutions architect is designing an architecture for a new application that requires low network latency and high network throughput between Amazon EC2 instances. Which component should be included in the architectural design?

A.An Auto Scaling group with Spot Instance types.

B.A placement group using a cluster placement strategy.

C.A placement group using a partition placement strategy.

D.An Auto Scaling group with On-Demand instance types.

正确答案 B

Q153. A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.Which solution will meet these requirements?

A. Amazon DynamoDB

B. Amazon RDS for MySQL

C. MySQL-compatible Amazon Aurora Serverless

D. MySQL deployed on Amazon EC2 in an Auto Scaling group

正确答案 C

**解析:**

as we want cost effective, something that scales and no modifications
A. modifications, so thats out
B. does not specify scaling in the choice
C. scales, no modifications and can migrate MYSQL to Aurora Migrating Data from a MySQL DB Instance to an Amazon Aurora MySQL DB Cluster by Using a DB Snapshot
D. extra cost as there is an EC2 instance associated

From AWS Aurora Serverless: "It enables you to run your database in the cloud without managing any database instances. It's a simple, cost-effective option for infrequent, intermittent, or unpredictable workloads."
https://aws.amazon.com/rds/aurora/serverless/

The question clearly states that it is sporadic. Indeed, it is predictable because we do know when the traffic is low and when it increases. However, I think a serverless solution will better work for this kind of workload as it scales out and in only when it needs --> costs savings.

Q154. A solutions architect is designing a mission-critical web application. It will consist of Amazon EC2 instances behind an Application Load Balancer and a relational database. The database should be highly available and fault tolerant.Which database implementations will meet these requirements? (Select TWO.)

A. Amazon Redshift

B. Amazon DynamoDB

C. Amazon RDS for MySQL

D. MySQL-compatible Amazon Aurora Multi-AZ

E. Amazon RDS for SQL Server Standard Edition Mufti-AZ

正确答案 D,E

**解析:**

Since the Multi-AZ support by Amazon RDS for MS SQL Server
A - Redshift is a cloud data warehouse not a sql database
B - it does not say that global tables is active and it is a NoSQL database
C - It is not multi az

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_SQLServerMultiAZ.html

Q155. A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing. 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore. Which set of services should a solutions architect recommend to meet these requirements?

A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

B. Amazon EBS for maximum performance. Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage

C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage

D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

正确答案 A

**解析:**

As per question this is media company and as per AWS Amazon EC2 instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.
s3 for durable, they need 300TB, as 3 has no limit on objects.
glacier for archiving the 900 TB.
it will be logical for an architect to use S3, then use policy to archive the files instead of using EFS.
EBS has the maximum capacity of 16TB
Certainly S3 is cost effective over EFS considering the use case.
Glacier is for deep archival.

Q156. A company hosts an application on an Amazon EC2 instance that requires a maximum of 200 GB storage space. The application is used infrequently, with peaks during mornings and evenings. Disk I/O varies, but peaks at 3,000 IOPS. The chief financial officer of the company is concerned about costs and has asked a solutions architect to recommend the most cost-effective storage option that does not sacrifice performance.Which solution should the solutions architect recommend?

A.Amazon EBS Cold HDD (sc1)

B.Amazon EBS General Purpose SSD (gp2)

C.Amazon EBS Provisioned IOPS SSD (io1)

D.Amazon EBS Throughput Optimized HDD (st1)

正确答案 B

**解析:**

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time.Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.In this case the volume would have a baseline performance of 3 x 200 = 600 IOPS. The volume could also burst to 3,000 IOPS for extended periods. As the I/O varies, this should be suitable. CORRECT: "Amazon EBS General Purpose SSD (gp2)" is the correct answer. INCORRECT: "Amazon EBS Provisioned IOPS SSD (io1) " is incorrect as this would be a more expensive option and is not required for the performance characteristics of this workload. INCORRECT: "Amazon EBS Cold HDD (sc1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload. INCORRECT: "Amazon EBS Throughput Optimized HDD (st1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.References:https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/compute/amazon-ebs/

Q157. A company delivers files in Amazon S3 to certain users who do not have AWS credentials. These users must be given access for a limited lime. What should a solutions architect do to securely meet these requirements?

A. Enable public access on an Amazon S3 bucket.

B. Generate a presigned URL to share with the users.

C. Encrypt files using AWS KMS and provide keys to the users.

D. Create and assign IAM roles that will grant GetObject permissions to the users.

正确答案 B

**解析:**

Grant time-limited permissions

https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html

Q158. A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements. What is the MOST cost-effective storage solution for this situation?

A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.

B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.

C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.

D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class.Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

正确答案 D

**解析:**

The S3 Standard-IA and S3 One Zone-IA storage classes are suitable for objects larger than 128 KB that you plan to store for at least 30 days. If an object is less than 128 KB, Amazon S3 charges you for 128 KB. If you delete an object before the end of the 30-day minimum storage duration period, you are charged for 30 days.

Q159. A solutions architect is moving the static content from a public website hosted on Amazon EC2 instances to an Amazon S3 bucket. An Amazon CloudFront distribution will be used to deliver the static assets. The security group used by the EC2 instances restricts access to a limited set of IP ranges. Access to the static content should be similarly restricted. Which combination of steps will meet these requirements? (Select TWO.)

A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.

B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.

C. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the CloudFront distribution.

D. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the S3 bucket hosting the static content.

E. Create a new IAM role and associate the role with the distribution. Change the permissions either on the S3 bucket or on the files within

the S3 bucket so that only the newly created IAM role has read and download permissions.

正确答案 A,B

**解析:**

Use signed URLs or cookies
- Restrict access to content in Amazon S3 buckets => A
- Use AWS WAF web ACLs => B
- Use geo restriction

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/data-protection-summary.html#data-protection-summary-restrict-access
https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html

Q160. A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.Which solution will satisfy these requirements?

A.Configure Amazon EFS storage and set the Active Directory domain for authentication.

B.Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.

C.Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.

D.Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

正确答案 D

**解析:**

ExplanationAmazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi- AZ deployment options, fully managed backups, and encryption of data at rest and in transit. You can optimize cost and performance for your workload needs with SSD and HDD storage options; and you can scale storage and change the throughput performance of your file system at any time. Amazon FSx file storage is accessible from Windows, Linux, and MacOS compute instances and devices running on AWS or on premises.Works with Microsoft Active Directory (AD) to easily integrate file systems with Windows environments.CORRECT: "Amazon FSx" is the correct answer.INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems. INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on- premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.References:https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.htmlSave time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-fsx/

Q161. A company runs multiple Amazon EC2 Linux instances in a VPC with applications that use a hierarchical directory structure. The applications need to rapidly and concurrently read and write to shared storage How can this be achieved?

A. Create an Amazon EFS file system and mount it from each EC2 instance.

B. Create an Amazon S3 bucket and permit access from all the EC2 instances in the VPC.

C. Create a file system on an Amazon EBS Provisioned IOPS SSD (io1) volume. Attach the volume to all the EC2 instances.

D. Create file systems on Amazon EBS volumes attached to each EC2 instance. Synchronize the Amazon EBS volumes across the different EC2 instances.

正确答案 A

**解析:**

"Mulitple Amazon EC2 Linux instances" "Concurrently" "Shared Storage" all EFS buzz words/phrases.

Q162. A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3. How can a solutions architect ensure that the application has permission to access Amazon S3?

A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.

B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.

C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.

D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

正确答案 B

**解析:**

taskRoleArn The short name or full Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that grants containers in

the task permission to call AWS APIs on your behalf.

Q163. A solutions architect has configured the following IAM policy. Which action will be allowed by the policy?

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lambda:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction"
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "220.100.16.0/20"
                }
            }
        }
    ]
}
```

A. An AWS Lambda function can be deleted from any network.

B. An AWS Lambda function can be created from any network.

C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.

D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network

正确答案 C

**解析:**

There is an explicit deny for the source IP block in the second statement. So only IPs outside that block can delete or create Lambda functions as per the Allow rule in the first statement.

Q164. A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have been complaining of timeouts. The architecture uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests. How should a solutions architect redesign the architecture to better respond to changing traffic?

A. Configure a Network Load Balancer with a slow start configuration.

B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.

C. Configure an Auto Scaling step scaling policy with an instance warmup condition.

D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

正确答案 C

**解析:**

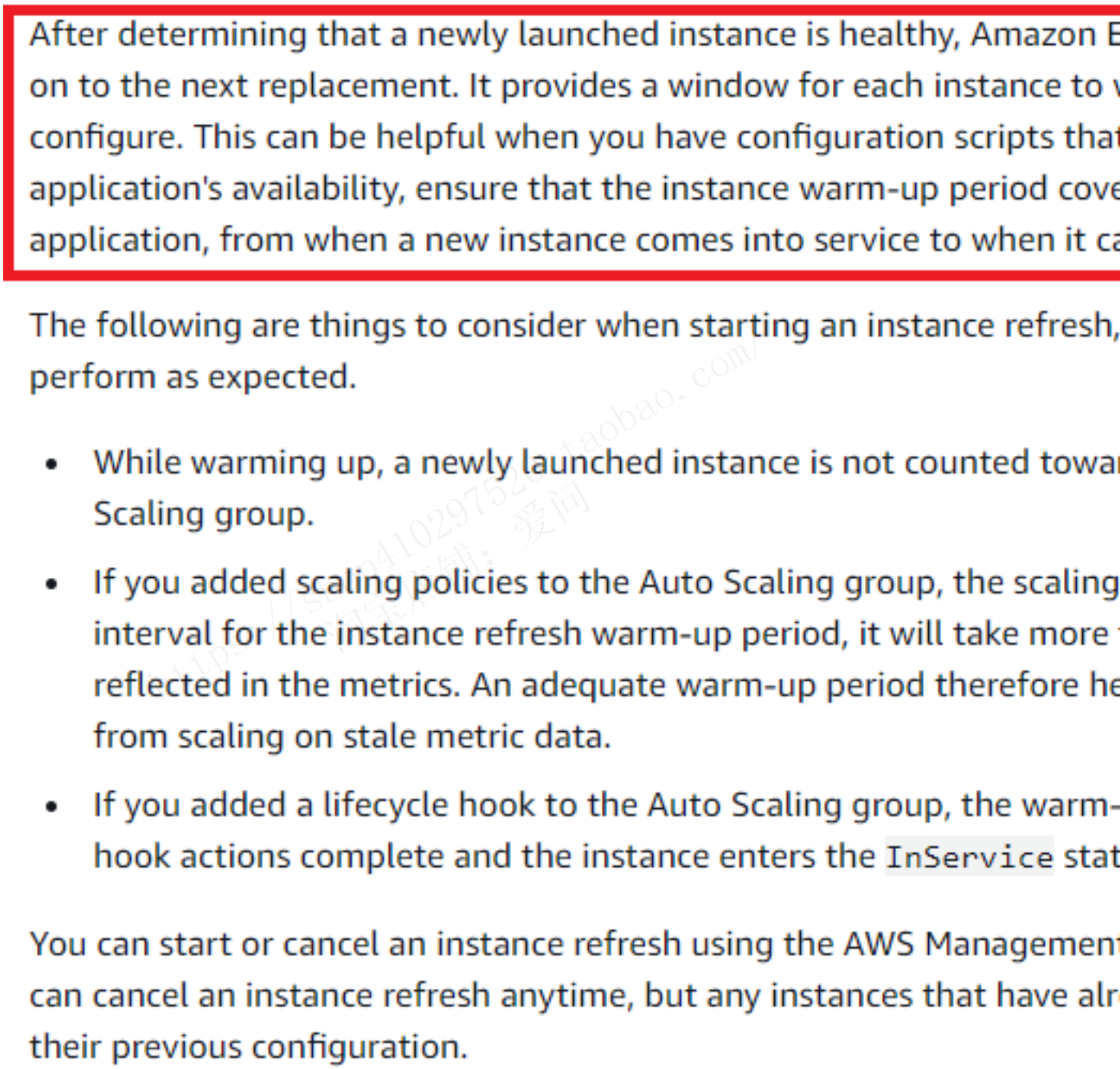
原始答案是 D，更正为 C, ID=94 实例启动后，需要一分钟才能 Ready. C is correct. CloudFront would not help in upload scenario. If you are creating a step policy, you can specify the number of seconds that it takes for a newly launched instance to warm up. Until its specified warm-up time has expired, an instance is not counted toward the aggregated metrics of the Auto Scaling group.

主张 D 答案：

The key word here i sredesign the architecture . So why wouldn't i redesign in cloudfront

The Key here is use of ALB as origin from Cloud Front, once we have ALB in place it won't route traffic to the instances which are unhealthy or

at start up there by taking care of time out, Cloud Front serves shared content if its already cached there by decreasing the traffic to Origin.



After determining that a newly launched instance is healthy, Amazon E
on to the next replacement. It provides a window for each instance to
configure. This can be helpful when you have configuration scripts that
application's availability, ensure that the instance warm-up period cove
application, from when a new instance comes into service to when it ca

The following are things to consider when starting an instance refresh,
perform as expected.

- While warming up, a newly launched instance is not counted towa
Scaling group.
- If you added scaling policies to the Auto Scaling group, the scaling
interval for the instance refresh warm-up period, it will take more
reflected in the metrics. An adequate warm-up period therefore he
from scaling on stale metric data.
- If you added a lifecycle hook to the Auto Scaling group, the warm-
hook actions complete and the instance enters the `InService` stat

You can start or cancel an instance refresh using the AWS Managemen
can cancel an instance refresh anytime, but any instances that have alr
their previous configuration.

Q165. A company has a website running on Amazon EC2 instances across two Availability Zones. The company is expecting spikes in traffic on

specific holidays, and wants to provide a consistent user experience. How can a solutions architect meet this requirement?

A. Use step scaling.

B. Use simple scaling.

C. Use lifecycle hooks.

D. Use scheduled scaling.

正确答案 D

**解析:**

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Q166. A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.Which configuration will meet this requirement?

A. Configure the security group for the EC2 instances.

B. Configure the security group on the Application Load Balancer.

C. Configure AWS WAF on the Application Load Balancer in a VPC.

D. Configure the network ACL for the subnet that contains the EC2 instances.

正确答案 C

**解析:**

"Geographic (Geo) Match Conditions in AWS WAF. This new condition type allows you to use AWS WAF to restrict application access based on the geographic location of your viewers. With geo match conditions you can choose the countries from which AWS WAF should allow access. "

https://aws.amazon.com/es/blogs/security/how-to-use-aws-waf-to-filter-incoming-traffic-from-embargoed-countries/
https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographic-match/

Q167. A company has 150 TB of archived image data stored on-premises that needs to be mowed to the AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only. What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

A. Use AWS Snowmobile to ship the data to AWS.

B. Order multiple AWS Snowball devices to ship the data to AWS.

C. Enable Amazon S3 Transfer Acceleration and securely upload the data.

D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

正确答案 B

**解析:**

Couple of snowball devices (80 TB) should able to move 150 TB easily.

Q168. A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS. and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times. Which action will be MOST effective in accomplishing this?

A. Replace the SQS queue with Amazon Kinesis Data Firehose.

B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.

C. Add an Amazon CloudFront distribution to cache the responses for the web tier.

D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SOS queue depth.

正确答案 D

**解析:**

The easiest to remove is option A.
Replacnig SQS queue with KDF will only mkae it worse as KDF will "flood" and overwhelm
the middle tier with all the requests.

The next one that can be removed is option C.
Cloudfront can't cache responses from the web tier since user will have different orders, thus the responses will contain different item for each user's request.

This leaves us with option B and D.
Now, what most people seem to ignore is this important detail:
"..At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times..."

If the middle tier EC2 instances doesn't scale, messages in SQS queue will not be processed fast enough and users will face delay.
Answer is D as it addresses this issue.

Q169. A company wants to host a web application on AWS that will communicate to a database within a VPC.The application should be highly available.What should a solutions architect recommend?

A. Create two Amazon EC2 instances to host the web servers behind a load balancer, and then deploy the database on a large instance.

B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.

C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.

D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones.

正确答案 B

**解析:**

Anything that says something like "..deploy database to an instance.." is not highly scaleable.
The best way to take advantage of the available AWS services for databases.
From here, you can already rule out A,C, and D

Q170. A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol. Which AWS managed service meets these requirements?

A.Amazon EBS

B.Amazon EC2

C.Amazon FSx

D.Amazon S3

正确答案 C

**解析:**

ExplanationAmazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs).Additionally, Amazon FSX for Windows File Server supports Distributed File System Replication (DFSR) in both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.CORRECT: "Amazon FSx" is the correct answer.INCORRECT: "Amazon Elastic Block Store (EBS)" is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.INCORRECT: "Amazon EC2" is incorrect as no SMB support. INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.References:https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.htmlSave time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-fsx/

Q171. A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.Which method should the solutions architect select?

A.Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.

B.Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.

C.Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.

D.Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

正确答案 A

**解析:**

ExplanationAmazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache that can reduce Amazon DynamoDB response times from milliseconds to microseconds, even at millions of requests per second.Amazon ElastiCache is incorrect because although you may use ElastiCache as your database cache, it will not reduce the DynamoDB response time from milliseconds to microseconds as compared with DynamoDB DAX.AWS Device Farm is incorrect because this is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time.DynamoDB Read Replica is incorrect because this is primarily used to automate capacity management for your tables and global secondary indexes.References:https://aws.amazon.com/dynamodb/daxhttps://aws.amazon.com/device-farmCheck out this Amazon DynamoDB Cheat Sheet:https://tutorialsdojo.com/aws-cheat-sheet-amazon-dynamodb/

Q172. A company wants to use an AWS Region as a disaster recovery location for its on-premises infrastructure. The company has 10 TB of existing data, and the on-premise data center has a 1 Gbps internet connection. A solutions architect must find a solution so the company can have its existing data on AWS in 72 hours without transmitting it using an unencrypted channel. Which solution should the solutions architect select?

A.Send the initial 10 TB of data to AWS using FTP.

B.Send the initial 10 TB of data to AWS using AWS Snowball.

C.Establish a VPN connection between Amazon VPC and the company's data center.

D.Establish an AWS Direct Connect connection between Amazon VPC and the company's data center.

正确答案C

**解析:**

Keyword: AWS Region as DR for On-premises DC (Existing Data=10TB) + 1G Internet ConnectionCondition: 10TB on AWS in 72 Hours + Without Unencrypted ChannelWithout Unencrypted Channel = VPNFTP = Unencrypted ChannelOptions - A - Out of race, since this is unencrypted channel & not matching the condition Options - B - Out of race due to the timebound target & order /delivering AWS Snowball device will take timeOptions - C - Win th race, using the existing 1G Internet Link we can transfer this 10TB data within 24Hrs using encrypted ChannelOptions - D - Out of race due to the timebound target & order /delivering AWS Direct Connect will take timeReferences:https://docs.aws.amazon.com/snowball/latest/ug/mailing-storage.htmlSave time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/aws-direct-connect/https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-vpc/https://tutorialsdojo.com/aws-direct-connect/https://tutorialsdojo.com/amazon-vpc/

Q173. A web application runs on Amazon EC2 instances behind an Application Load Balancer. The application allows users to create custom reports of historical weather data. Generating a report can take up to 5 minutes. These long-running requests use many of the available incoming connections, making the system unresponsive to other users. How can a solutions architect make the system more responsive?

A. Use Amazon SQS with AWS Lambda to generate reports.

B. Increase the idle timeout on the Application Load Balancer to 5 minutes.

C. Update the client-side application code to increase its request timeout to 5 minutes.

D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading to the user.

正确答案 A

**解析:**

Need de-coupling. So go with SQS and Lambda.

Q174. A company decides to migrate its three-tier web application from on premises to the AWS Cloud. The new database must be capable of dynamically scaling storage capacity and performing table joins.Which AWS service meets these requirements?

A. Amazon Aurora

B. Amazon RDS for SqlServer

C. Amazon DynamoDB Streams

D. Amazon DynamoDB on-demand

正确答案 A

**解析:**

As a custom engine for RDS, Amazon Aurora has additional features to make it faster and more modern. Aurora has high throughput, storage auto-scaling, and a self-healing, fault-tolerant storage system. It also provides point-in-time recovery and continuous backup, and it offers replication across three availability zones to keep your data secure.
Arora is relational and supports dynamic storage scaling upto 64 TB.

Q175. A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer. Amazon Route 53 is used for the DNS. The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down.How should the company deploy this solution?

A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.

B. Use Amazon S3 website hosting for the backup website and Route 53 latency routing policy.

C. Deploy the application in another AWS Region and use ELB health checks for failover routing.

D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

正确答案 A

**解析:**

Static content , backup site = s3
Trigger on Website down = Failover routing

Q176. A company needs to implement a relational database with a multi-Region disaster recovery Recovery Point Objective (RPO) of 1 second and an Recovery Time Objective (RTO) of 1 minute.Which AWS solution can achieve this?

A. Amazon Aurora Global Database

B. Amazon DynamoDB global tables.

C. Amazon RDS for MySQL with Multi-AZ enabled.

D. Amazon RDS for MySQL with a cross-Region snapshot copy.

正确答案 A

**解析:**

Cross-Region Disaster Recovery If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

Amazon Aurora Global Database = RPO of less than 5 seconds and an RTO of less than 1 minute.

https://aws.amazon.com/rds/aurora/global-database/

https://aws.amazon.com/blogs/database/building-globally-distributed-mysql-applications-using-write-forwarding-in-amazon-aurora-global-database/

Q177. A company running an on-premises application is migrating the application to AWS to increase its elasticity and availability. The current architecture uses a Microsoft SQL Server database with heavy read activity. The company wants to explore alternate database options and migrate database engines, if needed. Every 4 hours, the development team does a full copy of the production database to populate a test database. During this period, users experience latency. What should a solution architect recommend as replacement database?

A. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore from mysqldump for the test database.

B. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore snapshots from Amazon RDS for the test database.

C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas, and use the standby instance for the test database.

D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

正确答案 B

**解析:**

B -> Willing to change DB & no performance hit for taking backups
D -> I/O activity is suspended briefly during backup for Multi-AZ deployments for SQL servers. So it rules out D.
1. Question itself states " What should a solution architect recommend as replacement database?"
2. " users experience latency" when backup is taken from SQL Server. This means an alternate DB needs to be considered. Migrating to Aurora will eliminate this latency.
For SQL Server, I/O activity is suspended briefly during backup -

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_CreateSnapshot.html
3. Elasticity, availability, replicas - everything is provided by Aurora

Q178. A company currently stores symmetric encryption keys in a hardware security module (HSM). A solution architect must design a solution to migrate key management to AWS. The solution should allow for key rotation and support the use of customer provided keys. Where should the key material be stored to meet these requirements?

A. Amazon S3

B. AWS Secrets Manager

C. AWS Systems Manager Parameter store

D. AWS Key Management Service (AWS KMS)

正确答案 D

**解析:**

AWS Secrets Manager: helps you protect secrets needed to access your applications, services, and IT resources. but it is not for Key management.
KMS is Key management which will provide rotation of the key in CMK, also can import customer managed key into customer key store, KMS = HSM.
You can configure AWS Key Management Service (KMS) to use your AWS CloudHSM cluster as a custom key store rather than the default KMS key store.
https://aws.amazon.com/cloudhsm/

Q179. A company wants to run a hybrid workload for data processing. The data needs to be accessed by on- premises applications for local data processing using an NFS protocol, and must also be accessible from the AWS Cloud for further analytics and batch processing.Which solution will meet these requirements?

A. Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.

B. Use an AWS storage Gateway tape gateway to copy the backup of the local data to AWS, then perform analytics on this data in the AWS cloud.

C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.

D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS cloud, then perform analytics on this data in the cloud.

正确答案 A

**解析:**

Since it mentions NFS protocols its should use a Storage File Gateway. File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2-resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.

因为它提到了 NFS 协议，所以它应该使用存储文件网关。
文件网关提供了一个虚拟的本地文件服务器，它使您能够在 Amazon S3 中存储和检索作为对象的文件。它可以用于本地应用程序，也可以用于 Amazon ec2 驻留应用程序，这些应用程序需要在 S3 中为基于对象的工作负载存储文件。仅用于直接存储在 S3 上的平面文件。文件网关通过本地缓存提供对 Amazon S3 中的数据的基于 SMB 或 nfs 的访问。

Q180. A company must re-evaluate its need for the Amazon EC2 instances it currently has provisioned in an Auto Scaling group. At present, the Auto Scaling group is configured for minimum of two instances and a maximum of four instances across two Availability zones. A Solutions architect reviewed Amazon CloudWatch metrics and found that CPU utilization is consistently low for the EC2 instances. What should the solutions architect recommend to maximize utilization while ensuring the application remains fault tolerant?

A. Remove some EC2 instances to increase the utilization of remaining instances.

B. Increase the Amazon Elastic Block Store (Amazon EBS) capacity of instances with less CPU utilization.

C. Modify the Auto Scaling group scaling policy to scale in and out based on a higher CPU utilization metric.

D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

正确答案 D

**解析:**

Since most of the time CPU is under utilized.
C also looks reasonable, but ASG launch configuration is not able to modify once created, but create new and replace it.
The requirement here is to optimize the existing solution.
Since the CPU utilization were consistently low, then it means they are "over-proviisoning".
The running instances has more capacity that what is actually being consumed or used.
Now you'll have to find a way to maximize the use of the instances.
One way is to have more traffic coming in or more data coming in to be processed which will consume the instance's CPU.
The other way is to change the instance to a much smaller version with capacity enough to handle any load.
Since it's an ASG and ASG uses launch configuration, we can change the instance type in the launch configuration. However, we can only modify the launch configuration DURING CREATION.
So the best way here is have a new launch configuration with a smaller instance.

The question says minimum 2 across 2 availability zones means only 1 EC2 instance in each availability zone so for fault tolerance we cant remove the instances in an availability zone using auto scaling but just decrease the volume size of instance .so answer is D

Q181. A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost effective, limit the? provisioning of Into and provide the fastest

possible response time. Which combination should a solutions architect recommend to meet these requirements?

A.Amazon CloudFront and Amazon S3

B.AWS Lambda and Amazon Dynamo

C.Application Load Balancer with Amazon EC2 Auto Scaling

D.Amazon Route 53 with internal Application Load Balances

正确答案 A

Q182. A company is developing a real-time multiplier game that uses UDP for communications between client and servers in an Auto Scaling group Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention. Which solution should a solution architect recommend?

A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.

B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.

C. Use a Network Load Balancer for traffic distribution and amazon Aura Global for data storage.

D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage

正确答案 B

**解析:**

UDP ==> network load balancer, Non Relational DB ==> DynamoDB
https://aws.amazon.com/blogs/aws/new-udp-load-balancing-for-network-load-balancer/

Q183. A company currently has 250 TB of backup files stored in Amazon S3 in a vendor's proprietary format. Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversation. What should a solution architect do to accomplish this?

A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.

B. Install the conversion software onto an on-premises virtual machines. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.

C. Use AWS Snowball Edge device to expert the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball devices.

D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

正确答案 D

**解析:**

S3 works with EC2 to large files. Mindful of the 250TB. Since the data is in S3, you can have the EC2 in the same region with S3, hence no transfer cost.
Also note that you need to install the vendor provided software on the EC2.. Hence D is the best option.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonS3.html

Q184. A company has an Amazon EC2 instance running on a private subnet that needs to access a public websites to download patches and updates. The company does not want external websites to see the EC2 instance IP address or initiate connection to it.How can a solution architect achieve this objective?

A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed

B. Create a NAT gateway in a public subnet Route outbound traffic from the private subnet through the NAI gateway

C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website

D. Create a security group that only allows connections from the IP address range of the public website.Attach the security group to the EC2 instance.

正确答案 B

**解析:**

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
NAT gateway is like proxy server and connect EC2 instances in a private subnet to internet.

Q185. A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region.What should a solution architect do to automate the failover process?

A. Enable an ALB health check

B. Enable an Amazon Route 53 health check.

C. Crate an CNAME record on Amazon Route 53 pointing to the ALB endpoint.

D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

正确答案 B

**解析:**

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances You can use Route 53 to check the health of your resources and only return healthy resources in response to DNS queries. There are three types of DNS failover configurations:

1. Active-passive: Route 53 actively returns a primary resource. In case of failure, Route 53 returns the backup resource. Configured using a failover policy.
2. Active-active: Route 53 actively returns more than one resource. In case of failure, Route 53 fails back to the healthy resource. Configured using any routing policy besides failover.
3. Combination: Multiple routing policies (such as latency-based, weighted, etc.) are combined into a tree to configure more complex DNS failover.

In this case an alias already exists for the secondary ALB. Therefore, the solutions architect just needs to enable a failover configuration with an Amazon Route 53 health check.

The configuration would look something like this:

CORRECT: "Enable an Amazon Route 53 health check" is the correct answer.

INCORRECT: "Enable an ALB health check" is incorrect. The point of an ALB health check is to identify the health of targets (EC2 instances).

It cannot redirect clients to another Region. INCORRECT: "Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint" is incorrect as an Alias record already exists and is better for mapping to an ALB. INCORRECT: "Create a latency based routing policy on Amazon Route 53" is incorrect as this will only take into account latency, it is not used for failover. References:
https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/ Save time with our exam-specific cheat sheets:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-route-53/


Q186. A company needs to share an Amazon S3 bucket with an external vendor. The bucket owner must be able to access all objects.Which action should be taken to share the S3 bucket?

A. Update the bucket to be a Requester Pays bucket

B. Update the bucket to enable cross-origin resource sharing (CPORS)

C. Create a bucket policy to require users to grant bucket-owner-full when uploading objects

D. Create an IAM policy to require users to grant bucket-owner-full control when uploading objects.

正确答案 C

**解析:**

https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-bucket-owner-access/
By default, an S3 object is owned by the AWS account that uploaded it. This is true even when the bucket is owned by another account. To get access to the object, the object owner must explicitly grant you (the bucket owner) access.

The object owner can grant the bucket owner full control of the object by updating the access control list (ACL) of the object. The object owner can update the ACL either during a put or copy operation, or after the object is added to the bucket.

Similar:
https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-require-object-ownership/
Resolution
Add a bucket policy that grants users access to put objects in your bucket only when they grant you (the bucket owner) full control of the object.

Q187. A company uses Amazon S3 as its object storage solution. The company has thousands of S3 it uses to store data. Some of the S3 bucket have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented

or are implemented partially. resulting in data being stored in high-cost storage. Which solution will lower costs without compromising the availability of objects?

A. Use S3 ACLs

B. Use Amazon Elastic Block Store EBS) automated snapshots

C. Use S3 inteligent-Tiering storage

D. Use S3 One Zone-infrequent Access (S3 One Zone-IA).

正确答案 C

**解析:**

S3 Intelligent tiering due to this line " lifecycle policies are not consistently implemented or are implemented partially" .. Intellingent Tiering will take care of this

Q188. A solution architect is performing a security review of a recently migrated workload. The workload is a web application that consists of amazon EC2 instances in an Auto Scaling group behind an Application Load balancer. The solution architect must improve the security posture and minimize the impact of a DDoS attack on resources.Which solution is MOST effective?

A. Configure an AWS WAF ACL with rate-based rules Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the EAF ACL on the CloudFront distribution

B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. use the identified information to modify a network ACL to block access.

C. Enable VPC Flow Logs and store then in Amazon S3. Create a custom AWS Lambda functions that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.

D. Enable Amazon GuardDuty and , configure findings written 10 Amazon GloudWatch Create an event with Cloud Watch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS) Have Amzon SNS invoke a custom AWS lambda function that parses the logs looking for a DDoS attack Modify a network ACL to block identified source IP addresses

正确答案 A

**解析:**

Following WAF: You can use AWS WAF web access control lists (web ACLs) to help minimize the effects of a distributed denial of service (DDoS) attack.
The question attention: must improve the security posture and minimize the impact of a DDoS attack.
In all the other options NACL is involved to fix the problem. NACL won't see the attackers (source) IP given it sits behind an ALB. so B,C,D are all incorrect.
https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html

Q189. A company has a custom application running on an Amazon EC2 instance that:- Reads a large amount of data from Amazon S3- Performs a multi stage analysis- Writes the results to Amazon DynamoDBThe application writes a significant number of large temporary files during the multi stage analysis The process performance depends on the temporary storage performance. What would be the fastest storage option for holding the temporary files?

A. Multiple Amazon S3 buckets with Transfer Acceleration for storage

B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization

C. Multiple Amazon EFS volumes using the Network I lie System version 4.1 (NFSv4.1) protocol.

D. Multiple instance store volumes with software RAID 0.

正确答案 D

**解析:**

Both Instance Store Volume & RAID 0 can improve performance for temp storage.
RAID 0 increase performance of disk to double I/O. You can use EBS or instance store to created RAID-0. Here temporary storage means you can use instance store which gives enormous IO performance.
An AWS instance store is a temporary storage type located on disks that are physically attached to a host machine. Instance stores are made up of single or multiple instance store volumes exposed as block devices. Block storage on AWS is available with AWS EBS. ... Once an instance is terminated, all of its data is lost.

Q190. A solution architect must migrate a Windows internet information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network- attached storage (NAS). The solution architected has proposed migrating the IIS web servers Which replacement to the on-promises filo share is MOST resilient and durable?

A. Migrate the file Share to Amazon RDS.

B. Migrate the tile Share to AWS Storage Gateway

C. Migrate the file Share to Amazon FSx dor Windows File Server.

D. Migrate the tile share to Amazon Elastic File System (Amazon EFS)

正确答案 C

**解析:**

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas,

end- user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit.

This is the only solution presented that provides resilient storage for Windows instances. CORRECT: "Migrate the file share to Amazon FSx for Windows File Server" is the correct answer. INCORRECT: "Migrate the file share to Amazon Elastic File System (Amazon EFS)" is incorrect as you cannot use Windows instances with Amazon EFS.

INCORRECT: "Migrate the file share to Amazon RDS" is incorrect as this is not a shared storage solution for multi-AZ deployments.

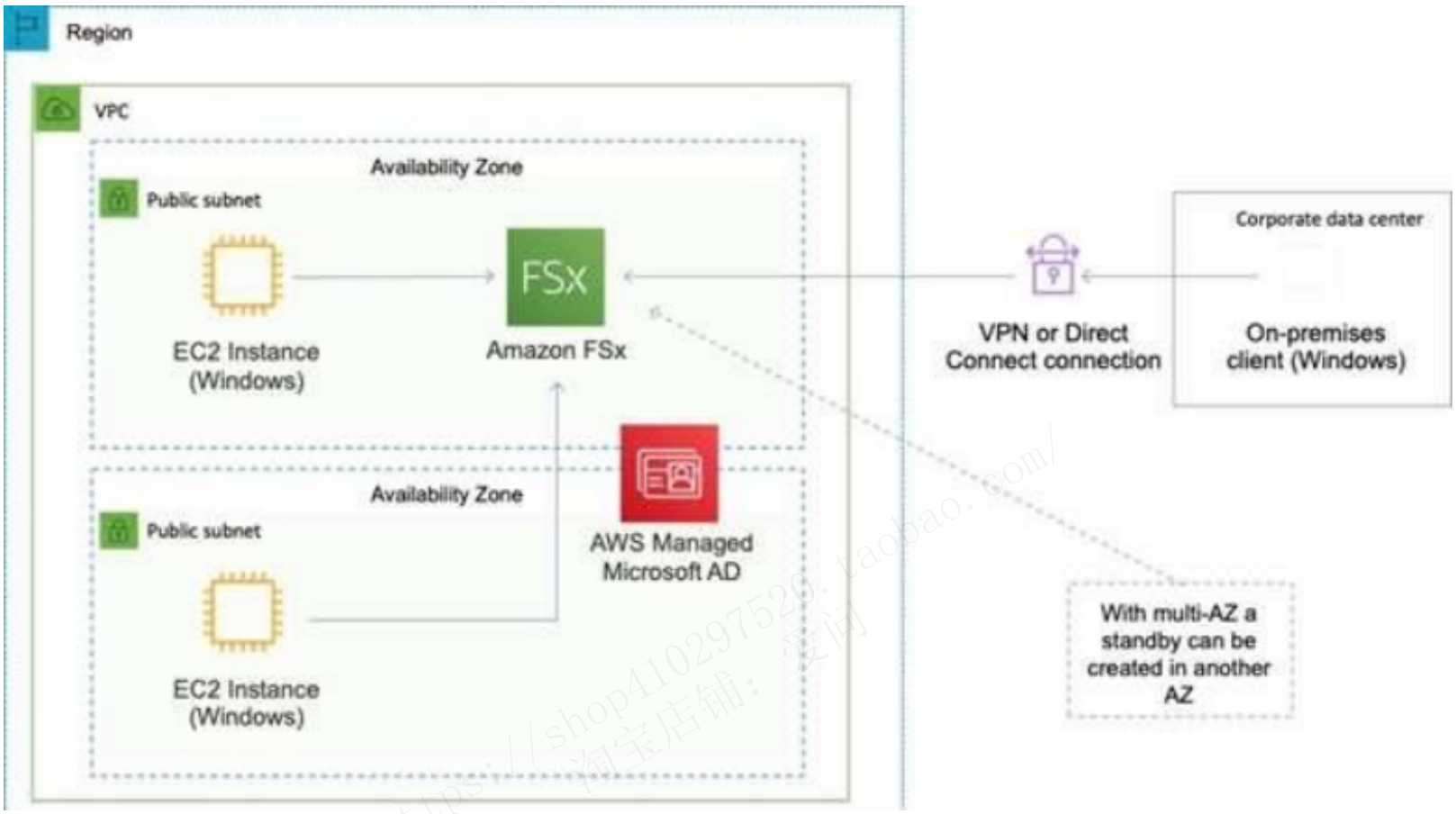
INCORRECT: "Migrate the file share to AWS Storage Gateway" is incorrect as with Storage Gateway replicated files end up on Amazon S3. The replacement storage solution should be a file share, not an object-based storage system.

References:

https://aws.amazon.com/fsx/windows/

Save time with our exam-specific cheat sheets:

https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/




Q191. An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both are in separate. AWS accounts. The network administrator needs to design a solution to enable secure access to EC2 instance in VOC-B from VPC-A,The connectivity should not have a single point of failure or bandwidth concerns.Which solution will meet these requirements?

A. Set up a VPC peering connection between VPC-A and VPC-B.

B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.

C. Attach a virtual private gateway to VPC-B and enable routing from VPC-A.

D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-B.

正确答案 A

**解析:**

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.
The traffic remains in the private IP space. All inter-region traffic is encrypted with no single point of failure, or bandwidth bottleneck.

https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

Q192. A company is seeing access requests by some suspicious IP addresses. The security team discovers the requests are from different IP addresses under the same CIDR range. What should a solutions architect recommend to the team?

A. Add a rule in the inbound table of the security to deny the traffic from that CIDR range.

B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.

C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.

D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

正确答案 C

**解析:**

You can only create deny rules with network ACLs, it is not possible with security groups. Network ACLs process rules in order from the lowest numbered rules to the highest until they reach and allow or deny. The following table describes some of the differences between security groups and network ACLs:

Therefore, the solutions architect should add a deny rule in the inbound table of the network ACL with a lower rule number than other rules.
CORRECT: "Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules" is the correct answer.
INCORRECT: "Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules" is incorrect as this will only block outbound traffic. INCORRECT: "Add a rule in the inbound table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.
INCORRECT: "Add a rule in the outbound table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.
References:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
Save time with our exam-specific cheat sheets:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-vpc/

| Security Group | Network ACL |
| --- | --- |
| Operates at the instance (interface) level | Operates at the subnet level |
| Supports allow rules only | Supports allow and deny rules |
| Stateful | Stateless |
| Evaluates all rules | Processes rules in order |
| Applies to an instance only if associated with a group | Automatically applies to all instances in the subnets its associated with |



Q193. A company is using a VPC peering strategy to connect its VPCs in a single Region to allow for cross- communication. A recent increase in account creations and VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs. There are also new requests to create site-to-site VPNs with some of the VPCs. A solutions architect has been tasked with creating a centrally networking setup for multiple accounts, VPNS, and VPNs.Which networking solution meets these requirements?

A.Configure shared VPCs and VPNs and share to each other

B.Configure a hub-and-spoke and route all traffic through VPC peering.

C.Configure an AWS Direct Connect between all VPCs and VPNs.

D.Configure a transit gateway with AWS Transit Gateway and connected all VPCs and VPNs.

正确答案 D

Q194. A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations, it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails. What would allow for automatic recovery of the EC2 instance as quickly as possible?

A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.

B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.

C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, triggered instance recovery.

D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

正确答案 A

**解析:**

Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.
As mentioned at:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html
You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system

"impairment" occurs.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html

Q195. A company has created a VPC with multiple private subnets in multiple Availability Zones (AZs) and one public subnet in one of the AZs. The public subnet is used to launch a NAT gateway. There are instance in the private subnet that use a NAT gateway to connect to the internet. In case is used of an AZ failure, the company wants to ensure that the instance are not all experiencing internet connectivity issues and that there is a backup plan ready. Which solution should a solutions architect recommend that is MOST highly available?

A.Create a new public subnet with a NAT gateway in the same AZ Distribute the traffic between the two NAT gateways

B.Create an Amazon EC2 NAT instance in a now public subnet Distribute the traffic between the NAT gateway and the NAT instance

C.Create public subnets In each f\Z and launch a NAT gateway in each subnet Configure the traffic from the private subnets In each A2 to the respective NAT gateway

D.Create an Amazon EC2 NAT instance in the same public subnet Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

正确答案C

Q196. A company has multiple AWS accounts, for various departments. One of the departments wants to share an Amazon S3 bucket with all other department. Which solution will require the LEAST amount of effort-?

A. Enable cross-account S3 replication for the bucket

B. Create a pre signed URL tor the bucket and share it with other departments

C. Set the S3 bucket policy to allow cross-account access to other departments

D. Create IAM users for each of the departments and configure a read-only IAM policy

正确答案 C

**解析:**

Set the S3 bucket policy to allow cross-account access to other departments.

Q197. A company collects temperature, humidity, and atmospheric pressure data in cities across multiple continents. The average volume of data collected per site each day is 500 GB. Each site has a high-speed internet connection. The company's weather forecasting applications are based in a single Region and analyze the data daily.What is the FASTEST way to aggregate data for all of these global sites?

A. Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.

B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.

C.Schedule AWS Snowball jobs daily to transfer data to the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.

D. Upload the data to an Amazon EC2 instance in the closes Region. Store the data in an Amazon EBS volume. One a day take an EBS snapshot and copy it to the centralize Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

正确答案 A

**解析:**

Step -1 To transfer to S3 from global sites : Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket.
S3 Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations.
Used to accelerate object uploads to S3 over long distances (latency).
Transfer acceleration is as secure as a direct upload to S3.

Step -2 : When the application analyze/aggregate the data from S3 and then again upload the results - Multipart upload

Q198. A company has implemented one of its microservices on AWS Lambda that accesses an Amazon DynamoDB table named Books. A solutions architect is design an IAM policy to be attached to the Lambda function's IAM role, giving it access to put, update, and delete items in the Books table. the IAM policy must prevent function from performing any other actions on the Books table or any other. Which IAM policy would fulfill these needs and provide the LEAST privileged access?

A.

```
{
  "Version" : "2012-10-17" ,
  "Statement" :[
{
  "Sid" :" PutUpdateDeleteOnBooks" ,
  "Effect" :" Allow" ,
  "Action" :[
  "Dynamodb:PutItem" ,
  "Dynamodb:UpdateItem" ,
  "Dynamodb:DeleteItem"
],
  "Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/Books"
}
]
}
```



B.

```
{
  "Version" : "2012-10-17" ,
  "Statement" :[
{
  "Sid" :" PutUpdateDeleteOnBooks" ,
  "Effect" :" Allow" ,
  "Action" :[
  "Dynamodb:PutItem" ,
  "Dynamodb:UpdateItem" ,
  "Dynamodb:DeleteItem"
],
  "Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/* "
}
]
}
```



C.

```
{
 “Version”：“2012-10-17”，
 “Statement”:[
{
 “Sid”:” PutUpdateDeleteOnBooks”，
 “Effect”:” Allow”，
 “Action”：“Dynamodb:*”，
 “Resource”:” arn:aws:dynamodb:us-west-2:123456789012:table/Books ”
}
]
}
```

D.

```
{
 "Version" : "2012-10-17" ,
 "Statement" :[
{
 "Sid" :" PutUpdateDeleteOnBooks" ,
 "Effect" :" Allow" ,
 "Action" : "Dynamodb:*" ,
 "Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/Books"
},
{
 "Sid" :" PutUpdateDeleteOnBooks" ,
 "Effect" :" Deny" ,
 "Action" : "Dynamodb:*" ,
 "Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/Books"
},
]
}
```

正确答案 A

**解析:**

Minimum Actions permission - Put / Update /Delete
Presise Resource Selection - DynamoDB table /books

Q199. Application developers have noticed that a production application is very slow when business reporting users run large production reports against the Amazon RDS instance backing the application. the CPU and memory utilization metrics for the RDS instance-d not exceed 60% while the reporting queries are running. The business reporting users must be able to generate reports without affecting the applications performance.Which action will accomplish this?

A.Increase the size of the RDS instance

B.Create a read replica and connect the application to it.

C.Enable multiple Availability Zones on the RDS instance

D.Create a read replication and connect the business reports to it.

正确答案 D

Q200. A company's packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution, but wants to future reduce data transfer costs. The company modify the application's source code.What should a solution architect do to reduce costs?

A. Use Lambda adage to compress the files as they are sent to users.

B. Enable Amazon S3 Transfer Acceleration to reduce the response times.

C. Enable caching on the CloudFront distribution to store generated files at the edge.

D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users.

正确答案 A

**解析:**

A - best alternative. Also, lambda is cost-effective in this case. Will work.
B - We are not talking about the speed of the download, its more of cost reduction, S3 with TA will increase the cost. So won't work.
C - No point of caching everything a new file is created although static. So won't work.
D - We are not talking about the speed of the download, will not reduce cost. So won't work.

cause the need to reduce costs. Compressed files -> less outbound traffic. Cache is useless as the file are single-user intended
Also the idea here is to reduce 'data transfer' cost. At Cloudfront, data out to the internet is charged, so option A reduced the size by compressing and sending it to user via internet. Refer : https://aws.amazon.com/cloudfront/pricing/

Use Lambda@Edge. See the question "single-use text file" will be sent in response. Single-use text file means that file will be used only one time so whats the benefit of the caching it on the cloudfront as it will not be abled to be used again. So what other thing can be done is to use Lambda@Edge to compress the file which will reduce the size of the file and hence less data will be transferred and less will be the transfer charges.

Q201. A public-facing web application queries a database hosted on a Amazon EC2 instance in a private subnet. A large number of queries involve multiple table joins, and the application performance has been degrading due to an increase in complex queries. The application team will be performing updates to improve performance.What should a solutions architect recommend to the application team? (Select TWO.)

A. Cache query data in Amazon SQS

B. Create a read replica to offload queries

C. Migrate the database to Amazon Athena

D. Implement Amazon DynamoDB Accelerator to cache data.

E. Migrate the database to Amazon RDS

正确答案 B,E

**解析:**

RDS with read replica should do the the job.

Q202. A company has a Microsoft Windows-based application that must be migrated to AWS. This application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances. What should a solution architect do to accomplish this?

A. Configure a volume using Amazon EFS Mount the EPS volume to each Windows Instance

B. Configure AWS Storage Gateway in Volume Gateway mode Mount the volume to each Windows instance

C. Configure Amazon FSx for Windows File Server Mount the Amazon FSx volume to each Windows Instance

D. Configure an Amazon EBS volume with the required size Attach each EC2 instance to the volume Mount the file system within the volume to each Windows instance

正确答案 C

**解析:**

Configure Amazon FSx for Windows File Server. Mount the Amazon FSx volume to each Windows Instance.
为 Windows 文件服务器配置 Amazon FSx。将 Amazon FSx 卷挂载到每个 Windows 实例。

Q203. A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deploying on Amazon EC2 instances behind an Application Load balancer in an Auto Scaling group. The company needs the ability shift traffic from resources in one region to another.What should a solutions architect recommend?

A. Configure an Amazon Route 53 latency routing policy

B. Configure an Amazon Route 53 geolocation routing policy

C. Configure an Amazon Route 53 geoproximity fouling policy.

D. Configure an Amazon Route 53 multivalue answer routing policy

正确答案 C

**解析:**

Geolocation routing policy - Use when you want to route traffic based on the location of your users.

Geoproximity routing policy - Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

Q204. A company has several business systems that require access to data stored in a file share. the business systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company's legacy on-premises environment and with AWS. Which services mod the business requirements? (Select TWO.)

A. Amazon EBS

B. Amazon EFS

C. Amazon FSx for Windows

D. Amazon S3

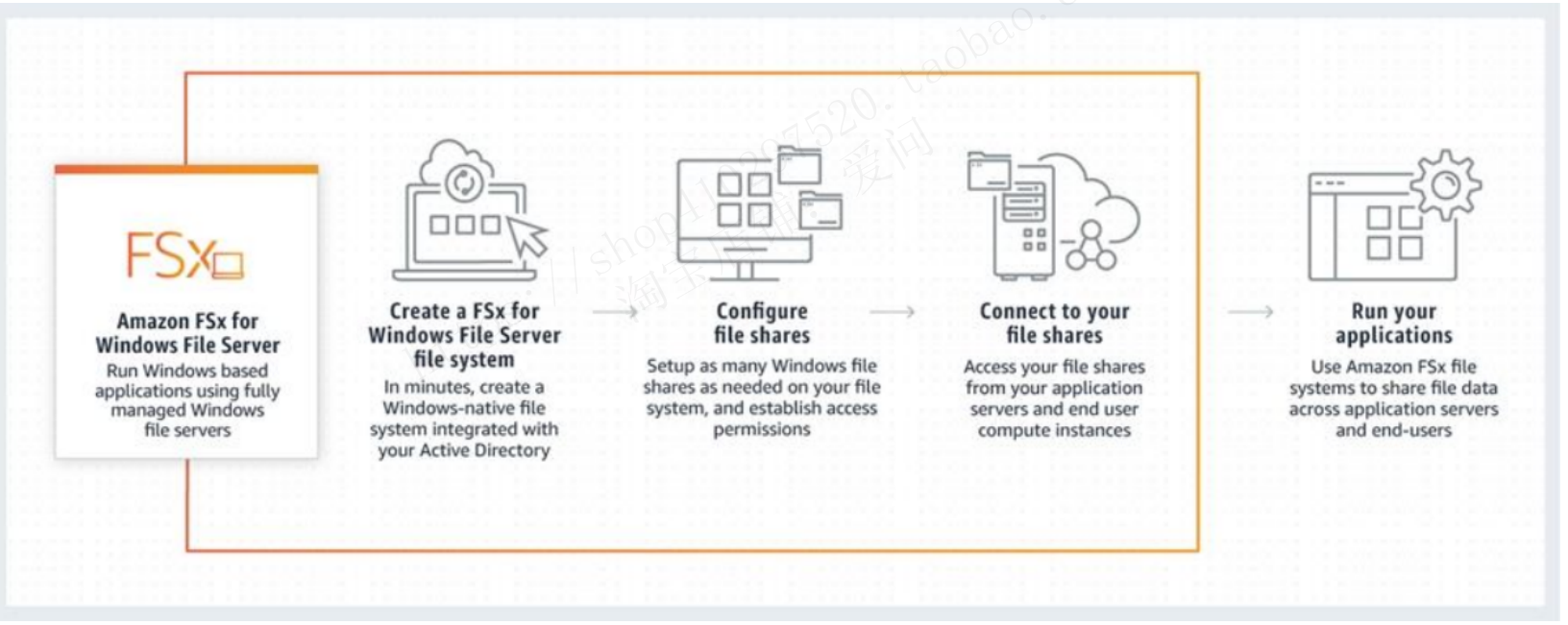
E. AWS Storage Gateway file gateway

正确答案C,E

**解析:**

Keyword: SMB + On-premises Condition: File accessible from both on-premises and AWS Amazon FSx for Windows File Server Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi- AZ deployment options, fully managed backups, and encryption of data at rest and in transit. You can optimize cost and performance for your workload needs with SSD and HDD storage options; and you can scale storage and change the throughput performance of your file system at any time. Amazon FSx file storage is accessible from Windows, Linux, and MacOS compute instances and devices running on AWS or on premises. How FSx for Windows File Server works AWS Storage Gateway AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications. File To support these use cases, Storage Gateway offers three different types of gateways ?that seamlessly connect on-premises Gateway, Tape Gateway, and Volume Gateway applications to cloud storage, caching data locally for low-latency access. Your applications connect to the service through a virtual machine or gateway hardware appliance using standard storage protocols, such as NFS, SMB, and iSCSI. The gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS, and AWS Backup,

providing storage for files, volumes, snapshots, and virtual tapes in AWS. The service includes a highly-optimized and efficient data transfer mechanism, with bandwidth management and automated network resilience. How Storage Gateway works  The table below shows the different gateways available and the interfaces and use cases:  CORRECT: "Amazon FSx for Windows" is the correct answer. CORRECT: "Amazon Storage File Gateway" is the correct answer. INCORRECT: "Amazon EBS" is incorrect as unsupported NFS/SMB. INCORRECT: "Amazon EFS" is incorrect as unsupported NFS/SMB. INCORRECT: "Amazon S3" is incorrect as unsupported NFS/SMB. References: https://aws.amazon.com/fsx/windows/ https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/ https://d0.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid- architectures.pdf https://youtu.be/T5KlnNj7-qg Save time with our exam-specific cheat sheets: https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-fsx/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws- storage-gateway/



| New Name | Old Name | Interface | Use Case |
|---|---|---|---|
| File Gateway | None | NFS, SMB | Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount points |
| Volume Gateway Stored Mode | Gateway-Stored Volumes | iSCSI | Asynchronous replication of on-prem data to S3 |
| Volume Gateway Cached Mode | Gateway-Cached Volumes | iSCSI | Primary data stored in S3 with frequently accessed data cached locally on-prem |
| Tape Gateway | Gateway-Virtual Tape Library | ISCSI | Virtual media changer and tape library for use with existing backup software |

Q205. A company's operations teams has an existing Amazon S3 bucket configured to notify an Amazon SQS queue when new object are created within the bucket. The development team also wants to receive events when new objects are created. The existing operations team workflow must remain intact.Which solution would satisfy these requirements?

A. Create another SQS queue Update the S3 events in bucket to also update the new queue when a new object is created.

B. Create a new SQS queue that only allows Amazon S3 to access the queue, Update Amazon S3 update this queue when a new object is created

C. Create an Amazon SNS topic and SQS queue for the Update. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.

D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic Add subscription for both queue in the topic.

正确答案 D

**解析:**

The existing operations team workflow must remain intact.

Q206. A company wants to deploy a shared file system for its .NET application servers and Microsoft SQL Server database running on Amazon EC2 instance with Windows Server 2016. The solution must be able to be integrated in to the corporate Active Directory domain, be highly durable, be managed by AWS, and provided levels of throuput and IOPS.Which solution meets these requirements?

A. Use Amazon FSx for Windows File Server

B. Use Amazon Elastic File System (Amazon EFS)

C. Use AWS Storage Gateway in file gateway mode.

D. Deploy a Windows file server on two On Demand instances across two Availability Zones.

正确答案 A

**解析:**

FSx for Windows can be integrated with On premise Active Directory.
https://aws.amazon.com/blogs/storage/using-amazon-fsx-for-windows-file-server-with-an-on-premises-active-directory/

Q207. A company is designing a new service that will run on Amazon EC2 instance behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.What should a solution architect recommend to meet the clients' needs? What should a solution architect recommend to meet the clients' needs?

A. A Network Load Balancer with an associated Elastic IP address.

B. An Application Load Balancer with an a associated Elastic IP address

C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address

D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

正确答案 A

**解析:**

Route53 is needed when we are using domain names but here we need to publish the webapp using IP address, so Route53 is out of question.

https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/

Q208. A company is designing a new service that will run on Amazon EC2 instance behind an Elastic Load Balancer.However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.What should a solution architect recommend to meet the clients' needs?

A. A Network Load Balancer with an associated Elastic IP address.

B. An Application Load Balancer with an a associated Elastic IP address

C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address

D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

正确答案 A

**解析:**

Route53 is needed when we are using domain names but here we need to publish the webapp using IP address, so Route53 is out of question.
https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/

Q209. A company is investigating potential solutions that would collect, process, and store users' service usage data.The business objective is to create an analytics capability that will enable the company to gather operational insights quickly using standard SQL queries. The solution should be highly available and ensure Atomicity, Consistency, Isolation, and Durability (ACID) compliance in the data tier.Which solution should a solutions architect recommend?

A. Use Amazon DynamoDB transactions

B. Create an Amazon Neptune database in a Multi AZ design

C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design

D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon EBS Throughput Optimized HDD (st1) storage.

正确答案 C

**解析:**

原始答案 A，现在更正为 C, Amazon DynamoDB is a fully managed proprietary NoSQL database service that supports key-value and document data structures and is offered by Amazon.com as part of the Amazon Web Services portfolio. DynamoDB exposes a similar data model to and derives its name from Dynamo, but has a different underlying implementation.

争议题，主张 A 答案的考生

DynamoDB transactions provide developers atomicity, consistency, isolation, and durability (ACID) across one or more tables within a single AWS account and region. You can use transactions when building applications that require coordinated inserts, deletes, or updates to multiple items as part of a single logical business operation.

Q210. A company runs a web service on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across two Availability Zones. The company needs a minimum of four instances at all times to meet the required service level agreement (SLA) while keeping costs low.

If an Availability Zone fails, how can the company remain compliant with the SLA?

A. Add a target tracking scaling policy with a short cooldown period

B. Change the Auto Scaling group launch configuration to use a larger instance type

C. Change the Auto Scaling group to use six servers across three Availability Zones

D. Change the Auto Scaling group to use eight servers across two Availability Zones

正确答案 D

**解析:**

争议题：

C and D seems to be correct. With the current options given C seems to be cost effective. However if we configure Min:4, Desired:4 and Max 8 then D is achievable. Question didn't mention about max limit and it is unknown and hence C seems to better option.

主张 C 答案

Under the SLA "o For Amazon EC2 (other than Single EC2 Instances),

Amazon ECS, or Amazon Fargate, when all of your running instances or running tasks, as applicable, deployed in two or more AZs in the same AWS region (or, if there is only one AZ in the AWS region, that AZ and an AZ in another AWS region) concurrently have no external connectivity."

https://aws.amazon.com/compute/sla/

主张 D 答案

Come on guys. 6 Instances across 3 AZs = 18 Instances you have to pay for. 8 instances across 2 AZs = 16 Instances you have to pay for.

If one AZ goes down that's 12 Instances in operational state that you are still being billed for, whereas for the other option if one AZ goes down that's only 8 instances you're paying for also meeting the 4 minimum requirement.

This is the perfect explanation for people confused with option C,D. Configuring 8 does not mean run all 8 at a time, it means to set max of 4 EC2 in launch config for each AZ ( AZ1=4,AZ2=4) . You set min:4, desired:4 and max:4 to run at any given time. That way when both AZ are up each will have 2 EC2 instances( balanced) . When one AZ fails the surviving AZ can still host all 4 EC2.

For option C, if 2 AZ fails the surviving AZ can host max of 2 EC2 only. Assuming you divided equally ( AZ1=2,AZ2=2,AZ3=2) . Even if not divided equally, say (AZ1=4, AZ2=1, AZ3=1 ) and if your AZ1 fails, you still cant meet the SLA.

Q211. An ecommerce company has noticed performance degradation of its Amazon RDS based web application.The performance degradation is attribute to an increase in the number of read-only SQL queries triggered by business analysts.A solution architect needs to solve the problem with minimal changes to the existing web application.What should the solution architect recommend?

A. Export the data to Amazon DynamoDB and have the business analysts run their queries.

B. Load the data into Amazon ElasticCache and have the business analysts run their queries.

C. Create a read replica of the primary database and have the business analysts run their queries.

D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

正确答案 C

**解析:**

Read replica is perfect for this.

Q212. A company is building applications in containers.The company wants to migrate its on-premises development and operations services from its on- premises data center to AWS.Management states that production system must be cloud agnostic and use the same configuration and administrator tools across production systems. A solutions architect needs to design a managed solution that will align open-source software.Which solution meets these requirements?

A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.

B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS workers nodes.

C. Launch the containers on Amazon Elastic Containers service (Amazon ECS) with AWS Fargate instances.

D. Launch the containers on Amazon Elastic Container Service (Amazon EC) with Amazon EC2 instance worker nodes.

正确答案 B

**解析:**

When talking about containerized applications, the leading technologies which will always come up during the conversation are Kubernetes and Amazon ECS (Elastic Container Service).
While Kubernetes is an open-sourced container orchestration platform that was originally developed by Google, Amazon ECS is AWS' proprietary, managed container orchestration service.
Management states that production system must be cloud agnostic and use the same configuration and administrator tools across production systems. ECS is AWS Service.

Q213. A company is running a two-tier ecommerce website using services. The current architect uses a publish- facing Elastic Load Balancer that sends traffic to Amazon EC2 instances in a private subnet.The static content is hosted on EC2 instances, and the dynamic content is retrieved from a MYSQL database.The application is running in the United States. The company recently started selling to users in Europe and Australia.A solution architect needs to design solution so their international users have an improved browsing experience.Which solution is MOST cost-effective?

A. Host the entire website on Amazon S3.

B. Use Amazon CloudFront and Amazon S3 to host static images.

C. Increase the number of public load balancers and EC2 instances

D. Deploy the two-tier website in AWS Regions in Europe and Austraila.

正确答案 B

**解析:**

This can be done using CloudFront distribution connected to a custom origin for dynamic content (in this case, an Amazon EC2 web server instance) and an Amazon S3 bucket for static content.
it was stated that static images, however, it is not limited to serving static images but static content.

https://aws.amazon.com/blogs/networking-and-content-delivery/deliver-your-apps-dynamic-content-using-amazon-cloudfront-getting-started-template/

Q214. A database is on an Amazon RDS MYSQL 5.6 Multi-AZ DB instance that experience highly dynamic reads.Application developers notice a significant slowdown when testing read performance from a secondary AWS Region.The developers want a solution that provides less than 1 second of read replication latency.What should the solutions architect recommend?

A. Install MySQL on Amazon EC2 in (he secondary Region.

B. Migrate the database to Amazon Aurora with cross-Region replicas.

C. Create another RDS for MySQL read replica in the secondary.

D. Implement Amazon ElastiCache to improve database query performance.

正确答案 B

**解析:**

ElasticCache is useful when you frequently make the same queries (for example, top 10 users). In this case, it says "highly dynamic reads" 反馈 ID=70 C not correct due to condition not met - less than 1 second of read replication latency

Amazon RDS for MySQL uses asynchronous replication and sometimes the replica isn't able to keep up with the primary DB instance. This can cause replication lag.

https://aws.amazon.com/premiumsupport/knowledge-center/rds-mysql-high-replica-lag/

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Updates.1200.html

Q215. An operations team has a standard that states IAM policies should not be applied directly to users.Some new members have not been following this standard. The operation manager needs a way to easily identify the users with attached policies. What should a solutions architect do to accomplish this?

A. Monitor using AWS CloudTrail

B. Create an AWS Config rule to run daily

C. Publish 1AM user changes lo Amazon SNS

D. Run AWS Lambda when a user is modified

正确答案 B

**解析:**

A new AWS Config rule is deployed in the account after you enable AWS Security Hub. The AWS Config rule reacts to resource configuration and compliance changes and send these change items to AWS CloudWatch. When AWS CloudWatch receives the compliance change, a CloudWatch event rule triggers the AWS Lambda function.
https://aws.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-aws-config/

Q216. A company has established a new AWS account.The account is newly provisioned and no changed have been made to the default settings. The company is concerned about the security of the AWS account root user.What should be done to secure the root user?

A. Create 1AM users for daily administrative tasks.Disable the root user.

B. Create 1AM users for daily administrative tasks.Enable multi-factor authentication on the root user.

C. Generate an access key for the root user.Use the access key for daily administration tasks instead of the AWS Management Console.

D. Provide the root user credentials to the most senior solution architect.Have the solution architect use the root user for daily administration tasks.

正确答案 B

**解析:**

Core understanding of IAM users and security. Basics that everyone can find in start of any AWS course.

Q217. A healthcare company stores highly sensitive patient records. Compliance requires that multiple copies be stored in different locations Each record must be stored for 7 years.The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter.What should a solutions architect recommend?

A. Use Amazon S3 with cross-Region replication enabled.After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy

B. Use Amazon S3 with cross-origin resource sharing (CORS) enabled.After 30 days, transition the data to Amazon S3 Glacier using a lifecycle policy.

C. Use Amazon S3 with cross-Region replication enabled.After 30 days, transition the data to Amazon S3 Glacier Deep Achieve using a lifecycle policy

D. Use Amazon S3 with cross-origin resource sharing (GORS) enabled.After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy

正确答案 A

**解析:**

S3 cross region replication and Standard Glacier. Deep Archive would have been the cheaper option but retrieval time of 4 hours not possible.

Q218. A solutions architect must create a highly available bastion host architecture. The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain.What should the solutions architect do to meet these requirements?

A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.

B. Create a Network Load Balancer backed by a Spot Fleet with instances in a group with instances in a partition placement group.

C. Create a Network Load Balancer backed by the existing serves in different Availability Zones as the target.

D. Create a Network Load Balancer backed by an Auto Scaling with instances in multiple Availability zones as the target

正确答案 D

**解析:**

Those two points are valid. But the question specifically asks for HA and Resiliency (ability to recover).
Resiliency - possible only when you have Auto-Scaling
HA - Multiple AZ
A. Not Valid
B. Not valid - Spot Fleet disruption in service
C. Although this option gives HA, but missing resiliency. when instance (Bastion host) goes down in 1 AZ, it needs manual intervention because there is no Auto Scaling.

Q219. A solution architect is designing a hybrid application using the AWS cloud. The network between the on- premises data center and AWS will

use an AWS Direct Connect (DX) connection.The application connectivity between AWS and the on-premises data center must be highly resilient.Which DX configuration should be implemented to meet these requirements?

A. Configure a DX connection with a VPN on top of it.

B. Configure DX connections at multiple DX locations.

C. Configure a DX connection using the most reliable DX partner.

D. Configure multiple virtual interfaces on top of a DX connection.

正确答案 B

**解析:**

Highly resilient, fault-tolerant network connections are key to a well-architected system. AWS recommends connecting from multiple data centers for physical location redundancy.
高弹性、容错的网络连接是架构良好的系统的关键。AWS 建议从多个数据中心连接以实现物理位置冗余。

Q220. A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandata encryption of data before sending it to Amazon S3.What should a solution architect recommend to satisfy these requirements?

A. Server-side encryption with customer-provided encryption keys

B. Client-side encryption with Amazon S3 managed encryption keys

C. Server-side encryption with keys stored in AWS key Management Service (AWS KMS)

D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

正确答案 D

**解析:**

Client-side encryption is the act of encrypting data before sending it to Amazon S3. To enable client-side encryption, you have the following options:
-Use a customer master key (CMK) stored in AWS Key Management Service (AWS KMS).
-Use a master key that you store within your application.
客户端加密是在将数据发送到 Amazon S3 之前对其进行加密的行为。要启用客户端加密，您有以下选项:
-使用 AWS 密钥管理服务(AWS KMS)中存储的客户主密钥(CMK)。
-使用一个主密钥，你存储在你的应用程序。

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html

Q221. A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day.A solutions architect has been tasked with designing the MOST cost-effective solution.Which solution will accomplish this?

A. Spot Fleet

B. Spot Instances

C. Reserved Instances

D. On-Demand Instances

正确答案 A

**解析:**

This works well for workloads such as big data and analytics, image and media rendering, machine learning, and high performance computing that

may have a higher cost of interruption associated with restarting work and checkpointing. By offering the possibility of fewer interruptions, the capacityOptimized strategy can lower the overall cost of your workload.

Spot fleet uses spot instances AND on-demand instances and let you define target capacity. It will be then less expensive than on-demand only.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-fleet.html

Q222. A company mandates that an Amazon S3 gateway endpoint must allow traffic to trusted buckets only.Which method should a solutions architect implement to meet this requirement?

A. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's trusted VPCs

B. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's S3 gateway endpoint IDs

C. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that blocks access from any VPC other than the company's trusted VPCs

D. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets

正确答案 D

**解析:**

The requirement is to allow traffic in VPC endpoint only. The bucket policy (as proposed in answer B) controls the access in the S3 bucket only. The solution B alone would allow traffic coming from untrusted S3 buckets to the VPC endpoint, which is a scenario to be avoided

VPC endpoints for S3 are secured through VPC endpoint access polices. This allows you to set which S3 buckets the endpoints should and should not have access to. By default, any user or service within the VPC, has access to any S3 resource. Use together with S3 bucket policies to further refine access control over your buckets and objects.

Q223. A company is designing a web application using AWS that processes insurance quotes Users will request quotes from the application.Quotes must be separated by quote type must be responded to within 24 hours, and must not be lost.The solution should be simple to set up and maintain.Which solution meets these requirements?

A. Create multiple Amazon Kinesis data streams based on the quote type.Configure the web application to send messages to the proper data stream.Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL)

B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type.Configure the web application to publish messages to the SNS topic queue.Configure each backend application server to work its own SQS queue

C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic.Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type.Configure each backend application server to work its own SQS queue.

D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster.Configure the web application to send messages to the proper delivery stream.Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly

正确答案 C

**解析:**

https://docs.aws.amazon.com/sns/latest/dg/sns-message-filtering.html It all depends on where you want to do the quote type classification i.e. in the app and send to a different/multiple SNS topics (B) or use SNS filtering to do the type classification (C). The question doesn't really give you enough info to make a clear choice but configuring SNS filtering is probablgt less work and easier to maintain than maintaining app code

"To get the event notifications to the right backend system, you could create a separate topic for each type of quote request, then add message routing logic to your publisher. However, this option can result in overly complicated publishers, topic proliferation, and additional overhead in provisioning and managing your SNS topics. SNS message filtering is much simpler!"

Q224. A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database Compliance regulations mandate that all personally identifiable information (Pll) be encrypted at rest.Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure''

A.Deploy AWS Certificate Manager to generate certificates.Use the certificates to encrypt the database volume

B.Deploy AWS CloudHSM. generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.

C.Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes

D.Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

正确答案 D

Q225. A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group.The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data However the metrics indicate that the EC2 instances do not cross any CPU utilization thresholdsHow can this issue be addressed1?

A. Reduce the threshold for CPU utilization in the Auto Scaling group

B. Replace the Application Load Balancer with a Network Load Balancer.

C. Add read replicas for the RDS instances and direct read traffic to the replica.

D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

正确答案 C

**解析:**

Nice move trying to misdirect you with Ec2 CPU threshold not reached. However the DB instance (RDS instance) may have its CPU at 100% as them EC2 are reading from it and the DB may not be strong enough to sustain. A read replica helps reduce the load. And that should solve the problem

Q226. A company recently released a new type of internet-connected sensor. The company is expecting lo sell thousands of sensors, which are designed to stream high volumes of data each second to a central location.A solutions architect must design a solution that ingests and stores data so that engineering teams can analyze it in near-real time with millisecond responsiveness. Which solution should the solutions architect recommend?

A. Use an Amazon SQS queue to ingest the data.Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.

B. Use an Amazon SOS queue to ingest the data.Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

C. Use Amazon Kinesis Data Streams to ingest the data.Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.

D. Use Amazon Kinesis Data Streams to ingest the data.Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

正确答案 D

**解析:**

争议题,主张 D 答案 keyword "engineering teams can analyze it in near-real time "
AWS database services for real-time applications are Amazon ElastiCache and/or Amazon DynamoDB
Amazon DynamoDB, a key-value database that gives you single-digit millisecond performance at any scale. DynamoDB Accelerator (DAX) delivers up to a 10 x performance improvement - from milliseconds to microseconds.

主张 C 答案
Redshift is meant for analytical processing whereas DynamoDB is meant for Transactional processing. Also, DynamoDB cannot take care of very complex queries (which are especially needed for analysis). I thought it was a very straightforward question but most people are choosing D which is clearly a poor solution for this case though might just do the job!

Q227. A company is migrating a NoSQL database cluster to Amazon EC2. The database automatically replicates data to maintain at least three copies

of the data. I/O throughput of the servers is the highest priority.Which instance type should a solutions architect recommend for the migration?

A.Storage optimized instances with instance store

B.Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume

C.Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

D.Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

正确答案 A

Q228. A company operates a website on Amazon EC2 Linux instances. Some of the instances are faring Troubleshooting points to insufficient swap space on the failed instances.The operations team lead needs a solution to monitor this.What should a solutions architect recommend?

A.Configure an Amazon CloudWatch SwapUsage metric dimension.Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.

B.Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics.Monitor SwapUsage metrics in CloudWatch.

C.Install an Amazon CloudWatch agent on the instances.Run an appropriate script on a set schedule.Monitor SwapUtilizalion metrics in CloudWatch.

D.Enable detailed monitoring in the EC2 console.Create an Amazon CloudWatch SwapUtilizalion custom metric.Monitor SwapUtilization metrics in CloudWatch.

正确答案 C

Q229. A company has two applications it wants to migrate to AWS. Both applications process a large set of files by accessing the same files at the same time. Both applications need to read the files with low

latency. Which architecture should a solutions architect recommend for this situation?

A.Configure two AWS Lambda functions to run the applications.Create an Amazon EC2 instance with an instance store volume to store the data.

B.Configure two AWS Lambda functions to run the applications.Create an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume to store the data.

C.Configure one memory optimized Amazon EC2 instance to run both applications simultaneously.Create an Amazon Elastic Block Store (Amazon EBS) volume with Provisioned IOPS to store the data.

D.Configure two Amazon EC2 instances to run both applications.Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting.Throughput mode to store the data.

正确答案 D

Q230. A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated. Which solution achieves these goals MOST efficiently?

A.Use a scheduled AWS Lambda function and execute a script remotely on all EC2 instances to send data to the audit system.

B.Use EC2 Auto Scaling lifecycle hooks to execute a custom script to send data to the audit system when instances are launched and terminated.

C.Use an EC2 Auto Scaling launch configuration to execute a custom script through user data to send data to the audit system when instances are launched and terminated.

D.Execute a custom script on the instance operating system to send data to the audit system.Configure the script to be executed by the EC2 Auto Scaling group when the instance starts and is terminated.

正确答案 B

Q231. A company requires a durable backup storage solution for its on-premises database servers while ensuring on-premises applications maintain access to these backups for quick recovery. The company will use AWS storage services as the destination for these backups. A solutions architect is designing a solution with minimal operational overhead. Which solution should the solutions architect implement?

A.Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket

B.Back up the databases to an AWS Storage Gateway volume gateway and access it using the Amazon S3 API.

C.Transfer the database backup files to an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance.

D.Back up the database directly to an AWS Snowball device and uss lifecycle rules to move the data to Amazon S3 Glacier Deep Archive.

正确答案 A

Q232. A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address.The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port 443. Which combination of steps will accomplish this task? (Select TWO.)

A.Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.

B.Create a security group with a rule to allow TCP port 443 to destination 0 0 0 0/0.

C.Update the network ACL to allow TCP port 443 from source 0.0 0 0/0.

D.Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.

E.Update the network ACL to allow inbound TCP port 443 from source 0.0.0 0/0 and outbound TCP port 32768-65535 to destination 0 0 0.0/0

正确答案 A,E

Q233. A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling.Management is concerned that the company is over- provisioning its infrastructure, especially at the front end of the three-tier application.A solutions architect needs to ensure costs are optimized without impacting performance. What should the solutions architect do to accomplish this?

A.Use Auto Scaling with Reserved Instances.

B.Use Auto Scaling with a scheduled scaling policy.

C.Use Auto Scaling with the suspend-resume feature

D.Use Auto Scaling with a target tracking scaling policy.

正确答案 D

Q234. A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application.A solutions architect wants to implement a solution that is highly available fault tolerant, and automatically scalable.What should the solutions architect recommend?

A.Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.

B.Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.

C.Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.

D.Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

正确答案 C

Q235. A solutions architect is working on optimizing a legacy document management application running on Microsoft Windows Server in an on-premises data center. The application stores a large number of files on a network file share. The chief information officer wants to reduce the on-premises data center footprint and minimize storage costs by moving on-premises storage to AWS.What should the solutions architect do to meet these requirements?

A.Set up an AWS Storage Gateway file gateway.

B.Set up Amazon Elastic File System (Amazon EFS)

C.Set up AWS Storage Gateway as a volume gateway

D.Set up an Amazon Elastic Block Store (Amazon EBS) volume.

正确答案 A

Q236. A company is processing data on a daily basis.The results of the operations are stored in an Amazon S3 bucket, analyzed daily for one week, and then must remain immediately accessible for occasional analysis What is the MOST cost-effective storage solution alternative to the current configuration?

A.Configure a lifecycle policy to delete the objects after 30 days

B.Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.

C.Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days

D.Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

正确答案C

Q237. A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.What should a solutions architect recommend?

A.Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.

B.Set up an Amazon EFS file system that connects with the backup applications using the NFS interface

C.Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface

D.Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

正确答案D

Q238. A company wants to replicate its data to AWS to recover in the event of a disaster. Today, a system administrator has scripts that copy data to a NFS share Individual backup files need to be accessed with low

latency by application administrators to deal with errors in processing.What should a solutions architect recommend to meet these requirements?

A.Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share

B.Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share

C.Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share.

D.Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

正确答案 D

Q239. A solutions architect is designing the storage architecture for a new web application used for stonng and viewing engineering drawings.All application components will be deployed on the AWS infrastructure. The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load.The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

A.Amazon S3 with Amazon CloudFront

B.Amazon S3 Glacier with Amazon ElastiCache

C.Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront

D.AWS Storage Gateway with Amazon ElastiCache

正确答案 A

Q240. A company that develops web applications has launched hundreds of Application Load Balancers (ALBs) in multiple Regions.The company wants to create an allow list (or the IPs of all the load balancers on its firewall device.A solutions architect is looking for a one-time, highly available solution to address this request, which will also help reduce the number of IPs that need to be allowed by the firewall. What should the solutions architect recommend to meet these requirements?

A.Create a AWS Lambda function to keep track of the IPs for all the ALBs in different Regions Keep refreshing this list.

B.Set up a Network Load Balancer (NLB) with Elastic IPs.Register the private IPs of all the ALBs as targets to this NLB.

C.Launch AWS Global Accelerator and create endpoints for all the Regions.Register all the ALBs in different Regions to the corresponding endpoints

D.Set up an Amazon EC2 instance, assign an Elastic IP to this EC2 instance, and configure the instance as a proxy to forward traffic to all the ALBs.

正确答案C

Q241. A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3.The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services. Which solution should a solutions architect recommend to keep the data private?

A.Deploy an AWS DataSync agent tor the on-premises environment.Configure a sync job to replicate the data and connect it with an AWS service endpoint.

B.Deploy an AWS DataSync agent for the on-premises environment.Schedule a batch job to replicate point-ln-time snapshots to AWS.

C.Deploy an AWS Storage Gateway volume gateway for the on-premises environment.Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

D.Deploy an AWS Storage Gateway file gateway for the on-premises environment.Configure it to store data locally, and asynchronously back up point-in-lime snapshots to AWS.

正确答案 A

Q242. A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs.The solution must allow for immediate retrieval of data at no additional cost.How can these requirements be met?

A.Deploy Amazon S3 Glacier Vault and enable expedited retrieval.Enable provisioned retrieval capacity for the workload

B.Deploy AWS Storage Gateway using cached volumes.Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.

C.Deploy AWS Storage Gateway using stored volumes to store data locally.Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3

D.Deploy AWS Direct Connect to connect with the on-premises data center.Configure AWS Storage Gateway to store data locally.Use Storage Gateway to asynchronously bacK up potnt-tn-time snapshots of the data to Amazon S3.

正确答案 B

Q243. A company Is reviewing Its AWS Cloud deployment to ensure its data is not accessed by anyone without appropriate authorization.A solutions

architect is tasked with identifying all open Amazon S3 buckets and recording any S3 bucket configuration changes.What should the solutions architect do to accomplish this?

A.Enable AWS Config service with the appropriate rules

B.Enable AWS Trusted Advisor with the appropriate checks.

C.Write a script using an AWS SDK to generate a bucket report

D.Enable Amazon S3 server access logging and configure Amazon CloudWatch Events.

正确答案 A

Q244. A company built an application that lets users check in to places they visit, rank the places, and add reviews about their experiences.The application is successful with a rapid increase in the number of users every month. The chief technology officer fears the database supporting the current Infrastructure may not handle the new load the following month because the single Amazon RDS for MySQL instance has triggered alarms related lo resource exhaustion due to read requests. What can a solutions architect recommend to prevent service Interruptions at the database layer with minimal changes to code?

A.Create RDS read replicas and redirect read-only traffic to the read replica endpoints.Enable a Multi-AZ deployment.

B.Create an Amazon EMR cluster and migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.

C.Create an Amazon ElastiCache cluster and redirect all read-only traffic to the cluster.Set up the cluster to be deployed m three Availability Zones.

D.Create an Amazon DynamoDB table to replace the RDS instance and redirect all read-only traffic to the DynamoDB table.Enable DynamoDB Accelerator to offload traffic from the main table.

正确答案 A

Q245. A company runs an application on Amazon EC2 Instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that Is highly available across the Region. Which solution should be implemented to ensure that there are no disruptions to Internet connectivity?

A.Deploy a NAT Instance In a private subnet of each Availability Zone.

B.Deploy a NAT gateway in a public subnet of each Availability Zone.

C.Deploy a transit gateway in a private subnet of each Availability Zone.

D.Deploy an internet gateway in a public subnet of each Availability Zone.

正确答案 B



Q246. A company has migrated an on-premises Oracle database to an Amazon RDS (or Oracle Multi- AZ DB instance In the us-east-l Region.A solutions architect is designing a disaster recovery strategy to have the database provisioned In the us-west-2 Region In case the database becomes unavailable in the us-east-1 Region. The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.How can these requirements be met?

A. Edit the DB instance and create a read replica in us-west-2.Promote the read replica to master In us- west-2 in case the disaster recovery environment needs to be activated.

B. Select the multi-Region option to provision a standby instance in us-west-2.The standby Instance will be automatically promoted to master In us-west-2 in case the disaster recovery environment needs to be created.

C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours.Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.

D. Create a multimaster read/write instances across multiple AWS Regions Select VPCs in us-east- 1 and us-west-2 lo make that deployment.Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

正确答案 A

**解析:**

Implementing disaster recovery. You can promote a read replica to a standalone instance as a disaster recovery solution if the primary DB instance fails.
References: https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/

Q247. A company has an application with a REST-based Interface that allows data to be received in near-real time from a third-party vendor.Once received, the application processes and stores the data for further analysis.The application Is running on Amazon EC2 instances.The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application.When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.Which design should a solutions architect recommend to provide a more scalable solution?

A.Use Amazon Kinesis Data Streams to ingest the data.Process the data using AWS Lambda functions.

B.Use Amazon API Gateway on top of the existing application.Create a usage plan with a quota Iimit for the third-party vendor.

C.Use Amazon Simple Notification Service (Amazon SNS) to ingest the data.Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.

D.Repackage the application as a container.Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

正确答案 A

Q248. A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

A.Use AWS Snowball.

B.Use AWS DataSync.

C.Use a secure VPN connection.

D.Use Amazon S3 Transfer Acceleration.

正确答案 A

Q249. A company recently deployed a two-tier application in two Availability Zones in the us-east-1 Region.The databases are deployed in a private subnet while the web servers are deployed in a public subnet.An internet gateway is attached to the VPC. The application and database run on Amazon EC2 instances.The database servers are unable to access patches on the internet. A solutions architect needs to design a solution that maintains database security with the least operational overhead.Which solution meets these requirements?

A.Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address.Update the routing table of the private subnet to use it as the default route.

B.Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with an Elastic IP address.Update the routing table of the private subnet to use it as the default route.

C.Deploy two NAT instances inside the public subnet for each Availability Zone and associate them with Elastic IP addresses.Update the routing table of the private subnet to use it as the default route.

D.Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses.Update the routing table of the private subnet to use it as the default route.

正确答案 A

Q250. A solutions architect must design a solution for a persistent database that is being migrated from on- premises to AWS.The database requires 64,000 IOPS according to the database administrator. If possible, the database administrator wants to use a single Amazon Elastic Block Store (Amazon EBS) volume to host the database instance.Which solution effectively meets the database administrator's criteria?

A.Use an instance from the 13 I/O optimized family and leverage local ephemeral storage to achieve the IOPS requirement.

B.Create an Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.

C.Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.

D.Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

正确答案 B

Q251. A company recently launched its website to serve content to its global user base. The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin. How should a solutions architect optimize high availability for the application?

A.Use Lambda@Edge for CloudFront.

B.Use Amazon S3 Transfer Acceleration for CloudFront.

C.Configure another EC2 instance in a different Availability Zone as part of the origin group.

D.Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

正确答案 C

Q252. A company is planning to build a new web application on AWS. The company expects predictable traffic most of the year and very high traffic on occasion. The web application needs to be highly available and fault tolerant with minimal latency. What should a solutions architect recommend to meet these requirements?

A.Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions, each with one Amazon EC2 instance.

B.Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones.

C.Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones.

D.Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group.

正确答案 B

Q253. A company wants to migrate a workload to AWS.The chief information security officer requires that all data be encrypted at rest when stored in the cloud.The company wants complete control of encryption key lifecycle management. The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail.The chosen services should integrate with other storage services that will be used on AWS. Which services satisfies these security requirements?

A.AWS CloudHSM with the CloudHSM client

B.AWS Key Management Service (AWS KMS) with AWS CloudHSM

C.AWS Key Management Service (AWS KMS) with an external key material origin

D.AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

正确答案 B

Q254. A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.What is the MOST cost-effective solution?

A.Store the video archives in Amazon S3 Glacier and use Expedited retrievals.

B.Store the video archives in Amazon S3 Glacier and use Standard retrievals.

C.Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).

D.Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

正确答案 A

Q255. A company wants to use Amazon S3 for the secondary copy of its on-premises dataset.The company would rarely need to access this copy.The storage solution's cost should be minimal.Which storage solution meets these requirements?

A.S3 Standard

B.S3 Intelligent-Tiering

C.S3 Standard-Infrequent Access (S3 Standard-IA)

D.S3 One Zone-Infrequent Access (S3 One Zone-IA)

正确答案 D

Q256. A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts.The company has created a central AWS account for streamlining management and audit reviews.An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users.The solution must be secure and optimized. How should a solutions architect meet these requirements?

A.Configure an AWS Lambda function in each developer account to copy the log files to the central account.Create an 1AM role in the central

account for the auditor.Attach an 1AM policy providing read- only permissions to the bucket.

B.Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account.Create an 1AM user in the central account for the auditor.Attach an 1AM policy providing full permissions to the bucket.

C.Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account.Create an 1AM role in the central account for the auditor.Attach an 1AM policy providing read-only permissions to the bucket.

D.Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account.Create an 1AM user in the central account for the auditor.Attach an 1AM policy providing full permissions to the bucket.

正确答案 C



Q257. A company has an application that posts messages to Amazon SQS Another application polls the queue and processes the messages in an l/O-intensive operation. The company has a service level agreement (SLA) that specifies the maximum amount of time that can elapse between receiving the messages and responding to the users. Due to an increase in the number of messages the company has difficulty meeting its SLA consistently.What should a solutions architect do to help improve the application's processing time and ensure it can handle the load at any level?

A.Create an Amazon Machine Image (AMI) from the instance used for processing.Terminate the instance and replace it with a larger size.

B.Create an Amazon Machine Image (AMI) from the instance used for processing.Terminate the instance and replace it with an Amazon EC2 Dedicated Instance

C.Create an Amazon Machine image (AMI) from the instance used for processing.Create an Auto Scaling group using this image in its launch configuration.Configure the group with a target tracking policy to keep us aggregate CPU utilization below 70%.

D.Create an Amazon Machine Image (AMI) from the instance used for processing.Create an Auto Scaling group using this image in its launch configuration.Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

正确答案 D

Q258. A company is planning to deploy an Amazon RDS DB instance running Amazon Aurora. The company has a backup retention policy requirement of 90 days. Which solution should a solutions architect recommend?

A.Set the backup retention period to 90 days when creating the RDS DB instance

B.Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecycle policy set to delete after 90 days.

C.Create an AWS Backup plan to perform a daily snapshot of the RDS database with the retention set to 90 days.Create an AWS Backup job to schedule the execution of the backup plan daily

D.Use a daily scheduled event with Amazon CloudWatch Events to execute a custom AWS Lambda function that makes a copy of the RDS automated snapshot Purge snapshots older than 90 days

正确答案 C

Q259. A company is using a tape backup solution to store its key application data offsite.The daily data volume is around 50 TB.The company needs to retain the backups for 7 years for regulatory purposes. The backups are rarely accessed and a week's notice is typically given

if a backup needs to be restored.The company is now considering a cloud-based option to reduce the storage costs and operational burden of managing tapes.The company also wants to make sure that the transition (rom tape backups to the cloud minimizes disruptions.Which storage solution is MOST cost-effective'?

A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive

B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.

C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier

D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move the backup to Amazon S3 Glacier

正确答案 A

**解析:**

此题为争议题 A 或者 D 之间抉择，题库保留了 A 答案，考生如果在考试中遇到就选择 A 吧，如果自己很有想法就按自己的决定。
选择 D 的理由： 考友 1：For daily move of 50TB data , snowball is not feasible , as it takes ~5 days to receive the Snowball device. Storage gateway cannot write to S3 glacier directly. 考友 2：It has to write to S3 first and then through life cycle policy , data can be archived in S3 Glacier. 考友 3：VTL to S3 then archving tapes to Glacier or deep Clacier. VTL can not directy backup to Glacier or deep Clacier。 snowball is only for migration to AWS once, Storage gateway writes only yo S3 then lifecycle moves the backup to lower cost Glacier. 选择 A 的理由： 考友 1： The data should be go into S3 Glacier direct, no need to set a lifecycle policy, because a week notice was given. "The backups are rarely accessed and a week's notice is typically given"。 The key here is a few things: "Tape backup solution" so Storage gateway is the immediate thought. Then "retain backups for 7 years" and "a week's notice is typically given if a back up needs to be restored" this screams Glacier Deep Archive as it takes at least 12 hours to retrieve

the data and it's the most cost effective solution.

考友 2： The AWS Storage Gateway service now integrates Tape Gateway with Amazon S3 Glacier Deep Archive storage class, allowing you to store virtual tapes in the lowest-cost Amazon S3 storage class, reducing the monthly cost to store your long-term data in the cloud by up to 75%. S3 Glacier Deep Archive is a new S3 storage class that provides secure, durable object storage for long-term data retention and digital preservation. With this feature, Tape Gateway supports archiving your new virtual tapes directly to S3 Glacier and S3 Glacier Deep Archive, helping you meet your backup, archive, and recovery requirements.

考友 3： I'll go with A, because It's the least wrong answer, I'll tell you why:

B. Snowball Edge(up to 80TB) costs about 300$, that means you'd had get about 20 units per month and that's like 6000$ and also it doesn't reduce the "burden of managing tapes" because Snowball doesn't integrate with tape solutions. AND! with Snowball Edge(or the normal) you CAN'T put data directly to Glacier, it has to go to S3 first.

That leave us just option A and D, we don't need much explanation for C. So A and D are almost identical but A is more efficient cause it sends the data directly to Deep Archive which is possible, you don't need a lifecycle to do it. And that's why A is the ANSWER.

But even because that's the answer doesn't mean it's a good solution. You'd have to transfer 50 TB daily... is that possible? Some could say yes, but most no.

Q260. A company relies on an application that needs at least 4 Amazon EC2 instances during regular traffic and must scale up to 12 EC2 instances during peak loads. The application is critical to the business and must be highly available Which solution will meet these requirements?

A. Deploy the EC2 instances in an Auto Scaling group.Set the minimum to 4 and the maximum to M, with 2 in Availability Zone A and 2 in Availability Zone B

B. Deploy the EC2 instances in an Auto Scaling group.Set the minimum to 4 and the maximum to 12, with all 4 in Availability Zone A

C. Deploy the EC2 instances in an Auto Scaling group.Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B

D. Deploy the EC2 instances in an Auto Scaling group.Set the minimum to 8 and the maximum to 12 with all 8 in Availability Zone A

正确答案 A

**解析:**

B and D are not highly available as both in one single Zone C doesn't distribute mentioned instances (4) into two AZ but rather double this A is the correct answer as it dis t ributes 4 min to two AZs for HA .
争议题，主张 C 答案认为 ASG is needed when performance is strained (not neccessarily down), in this case, application is still online. However, in this question, imagine the AZ is done, A is only left with 2 instances. As Mahesh mentioned, it takes ASG 5 mins to bring up to min 4 instances so you will be experience 5 mins of application outage. Cost is not mentioned in this question hence answer C is the best fit for this question. It requires HA and if one AZ is down then at least 4 instances will be active in another AZ which is key for this question.

Q261. A company is planning to migrate its virtual server-based workloads to AWS The company has internet-facing load balancers backed by application servers. The application servers rely on patches from an internet-hosted repository Which services should a solutions architect recommend be hosted on the public subnet? (Select TWO.)

A. NAT gateway

B. Amazon RDS DB instances

C. Application Load Balancers

D. Amazon EC2 application servers

E. Amazon Elastic File System (Amazon EFS) volumes

正确答案 A,C

**解析:**

Both Nat Gateway and ALB needs to be in the Public Subnet.

Q262. An application is running on Amazon EC2 instances Sensitive information required for the application is stored in an Amazon S3 bucket.The bucket needs to be protected from internet access while only allowing services within the VPC access to the bucket.Which combination of actions should a solutions archived take to accomplish this'' (Select TWO.)

A. Create a VPC endpoint for Amazon S3.

B. Enable server access logging on the bucket

C. Apply a bucket policy to restrict access to the S3 endpoint.

D. Add an S3 ACL to the bucket that has sensitive information

E. Restrict users using the 1AM policy to use the specific bucket

正确答案 A,C

**解析:**

ACL is a property at object level not at bucket level .Also by just adding ACL you cant let the services in VPC allow access to the bucket .

Q263. A solution is architect is designing a multi-Region disaster recovery solution for an application that will provide public API access.The application will use Amazon EC2 instances with a userdata script to load application code and an Amazon RDS for MySQL database.The Recovery Time Objective (RTO) is 3 hours and the Recovery Point Objective (RPO) is 24 hours.Which architecture would meet these

requirements at the LOWEST cost?

A. Use an Application Load Balancer for Region failover.Deploy new EC2 instances with the userdata script.Deploy separate RDS instances in each Region

B. Use Amazon Route 53 for Region failover.Deploy new EC2 instances with the userdata script.Create a read replica of the RDS instance in a backup Region

C. Use Amazon API Gateway for the public APIs and Region failover.Deploy new EC2 instances with the userdata script.Create a MySQL read replica of the RDS instance in a backup Region

D. Use Amazon Route 53 for Region failover.Deploy new EC2 instances with the userdata scnpt for APIs, and create a snapshot of the RDS instance daily for a backup.Replicate the snapshot to a backup Region

正确答案 D

**解析:**

A. Application Load Balancer is region based, so this ain't right.https://aws.amazon.com/elasticloadbalancing/ B. We can use Route 53 for a Region failover, but, why create a read replica? we need a snapshot. C. Sounds fishy using a read replica again. D. Right, we create a snapshot of the RDS instance, and replicate the snapshot for a backup Region. This gives cheapest DR solution to meet required RPO and RTO using RDS snapshot which is much cheaper than read-replica or seperate RDS instance.

Q264. A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users.The volume of requests is highly variable, several hours can pass without receiving a single request.The data processing will take place asynchronously but should be completed within a few seconds after a request is madeWhich compute

service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?

A.An AWS Glue job

B.An AWS Lambda function

C.A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)

D.A containerized service hosted in Amazon ECS with Amazon EC2

正确答案B

Q265. A development team needs to host a website that will be accessed by other teams. The website contents.consist of HTML. CSS, client side JavaScript, and images. Which method is the MOST cost-effective for hosting the website?

A. Containerize the website and host it in AWS Fargate

B. Create an Amazon S3 bucket and host the website there.

C. Deploy a web server on an Amazon EC2 instance to host the website.

D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express is framework

正确答案B

**解析:**

Static websites can be delivered to web browsers on desktops, tablets, or mobile devices. They usually consist of a mix of HTML documents, images, videos, CSS style sheets, and JavaScript files. Static doesn ' t have to mean boring - static sites can provide client-side interactivity as well. Using HTML5 and client-side JavaScript technologies such as jQuery, AngularJS, React, and Backbone, you can deliver rich user experiences that are engaging and interactive.

Q266. A company has media and application files that need to be shared internally. Users currently are authenticated using Active Directory and access files from a Microsoft Windows platform.The chief execute officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit.What should a solutions architect recommend?

A. Set up a corporate Amazon S3 bucket and move and media and application files.

B. Configure Amazon FSx for Windows File Server and move all the media and application files.

C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.

D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes and, and move all media and application files.

正确答案 B

**解析:**

It says that the files need to be shared internally, and it's using Active Directory. Amazon FsX for Windows sounds about right.

Q267. A company is moving its legacy workload to the AWS Cloud. The workload files will be shared, appended, and frequently accessed through Amazon EC2 instances when they are first created.The files will be accessed occasionally as they ageWhat should a solutions architect recommend?

A. Store the data using Amazon EC2 instances with attached Amazon Elastic Block Store (Amazon EBS) data volumes

B. Store the data using AWS Storage Gateway volume gateway and export rarely accessed data to Amazon S3 storage

C. Store the data using Amazon Elastic File System (Amazon EFS) with lifecycle management enabled for rarely accessed data

D. Store the data using Amazon S3 with an S3 lifecycle policy enabled to move data to S3 Standard- Infrequent Access (S3 Standard-IA)

正确答案 C

**解析:**

C Unlike S3 lifecycle that moves data to cheaper storage based on number of days that file is there in S3, EFS lifecycle moves based on number of days that file is lying idle

Q268. A company is deploying a multi-instance application within AWS that requires minimal latency between the instances.What should a solutions architect recommend?

A. Use an Auto Scaling group with a cluster placement group.

B. Use an Auto Scaling group with single Availability Zone in the same AWS Region.

C. Use an Auto Scaling group with multiple Availability Zones in the same AWS Region.

D. Use a Network Load Balancer with multiple Amazon EC2 Dedicated Hosts as the targets

正确答案 A

**解析:**

"multi-instance application within AWS that requires minimal latency between the instances" CPG decrease latency between instances

Q269. A company receives structured and semi-structured data from various sources once every day. A solutions architect needs to design a solution that leverages big data processing frameworks. The data should

be accessible using SQL queries and business intelligence tools.
What should the solutions architect recommend to build the MOST high-performing solution?

A. Use AWS Glue to process data and Amazon S3 to store data

B. Use Amazon EMR to process data and Amazon Redshift to store data

C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data

D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data

正确答案 B

**解析:**

Big data EMR, Redshift for analyzing

Q270. Company is designing a website that uses an Amazon S3 bucket to store static images. The company wants ail future requests have taster response times while reducing both latency and cost.Which service configuration should a solutions architect recommend?

A. Deploy a NAT server in front of Amazon S3.

B. Deploy Amazon CloudFront in front of Amazon S3.

C. Deploy a Network Load Balancer in front of Amazon S3.

D. Configure Auto Scaling to automatically adjust the capacity of the website.

正确答案 B

**解析:**

B Keywords are static content on S3 and Faster response

Q271. What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

A.Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set

B.Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set to private

C.Update the bucket policy to deny if the PutObject does not have an aws SecureTransport header set to true

D.Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set

正确答案 D

Q272. A company runs a high performance computing (HPC) workload on AWS. The workload required low- latency network performance and high network throughput with tightly coupled node-to-node communication.The Amazon EC2 instances are properly sized for compute and storage capacity, and are launched using default options. What should a solutions architect propose to improve the performance of the workload'?

A. Choose a cluster placement group while launching Amazon EC2 instances

B. Choose dedicated instance tenancy while launching Amazon EC2 instances

C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances

D. Choose the required capacity reservation while launching Amazon EC2 instances.

正确答案 A

**解析:**

Cluster - packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

Q273. A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe and it wants to optimize site loading times for new European users.The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is neededWhat should the solutions architect recommend?

A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it

B. Move the website to Amazon S3 Use cross-Region replication between Regions.

C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers

D. Use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers

正确答案 C

**解析:**

Amazon CloudFront works with any origin server that holds the original, definitive versions of your content, both static and dynamic. There is no additional charge to use a custom origin. So C is the right option.

Q274. A company is building a media-sharing application and decides to use Amazon S3 for storage. When a media file is uploaded the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation. The amount of traffic is variable

The solution must be able to scale to handle spikes in load without unnecessary expenses.
What should a solutions architect recommend to support this workload?

A. Build the processing into the website or mobile app used to upload the content to Amazon S3.Save the required data to the DynamoDB table when the objects are uploaded

B. Trigger AWS Step Functions when an object is stored in the S3 bucket.Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table

C. Trigger an AWS Lambda function when an object is stored in the S3 bucket.Have the Lambda function start AWS Batch to perform the steps to process the object.Place the object data in the DynamoDB table when complete

D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3.Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocess use the program to perform the processing

正确答案 B

**解析:**

Step Functions is ideal for coordinating session-based applications. You can use Step Functions to coordinate all of the steps of a checkout process on an ecommerce site, for example. Step Functions can read and write from Amazon DynamoDB as needed to manage inventory records. Not C: DynamoDB is used to store MetaData of the picture such as picture name, date taken, place taken, resolution etc.. (DynanoDB is not used to store picture objects) Not D: Same reason as for C, DynamoDB in this case is not to store picture objects (initial data is picture, metadata has not been extracted yet)

Q275. A company has recently updated its internal security standards. The company must now ensure all Amazon S3 buckets and Amazon Elastic

Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists.The company is looking for a native, software-based AWS service to accomplish this goal. What should a solutions architect recommend as a solution?

A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.

B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routing to re-create a new key periodically and replace it in AWS KMS.

C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine a re-create a new key periodically and replace it in the CloudHSM cluster nodes.

D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) keys to store master key material and apply a routine to re-create a new periodically and replace it in the Parameter Store.

正确答案 B

**解析:**

With Secrets Manager AWS automatically rotates your key. With AWS KMS automatic rotation can be enabled/disabled, thus engineers can do it manually.

Q276. A solution architect must design a solution that uses Amazon CloudFront with an Amazon S3 to store a static website.The company security policy requires that all websites traffic be inspected by AWS WAF.
How should the solution architect company with these requirements?

A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only

B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin,

C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only Associate AWS WAF to CloudFront.

D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

正确答案 D

**解析:**

Use OAI to restrict direct access to S3 by exposing the content only at the CloudFront layer. Use WAF in front of CloudFront to intercept requests beforehand

Q277. A company has copied 1 PB of data from a colocation facility to an Amazon S3 bucket in the us- east-1 Region using an AWS Direct Connect link.The company now wants to copy the data to another S3 bucket in the us-west-2 Region. The colocation facility does not allow the use AWS Snowball. What should a solutions architect recommend to accomplish this?

A. Order a Snowball Edge device to copy the data from one Region to another Region.

B. Transfer contents from the source S3 bucket to a target S3 bucket using the S3 console.

C. Use the aws S3 sync command to copy data from the source bucket to the destination bucket.

D. Add a cross-Region replication configuration to copy objects across S3 buckets in different Regions.

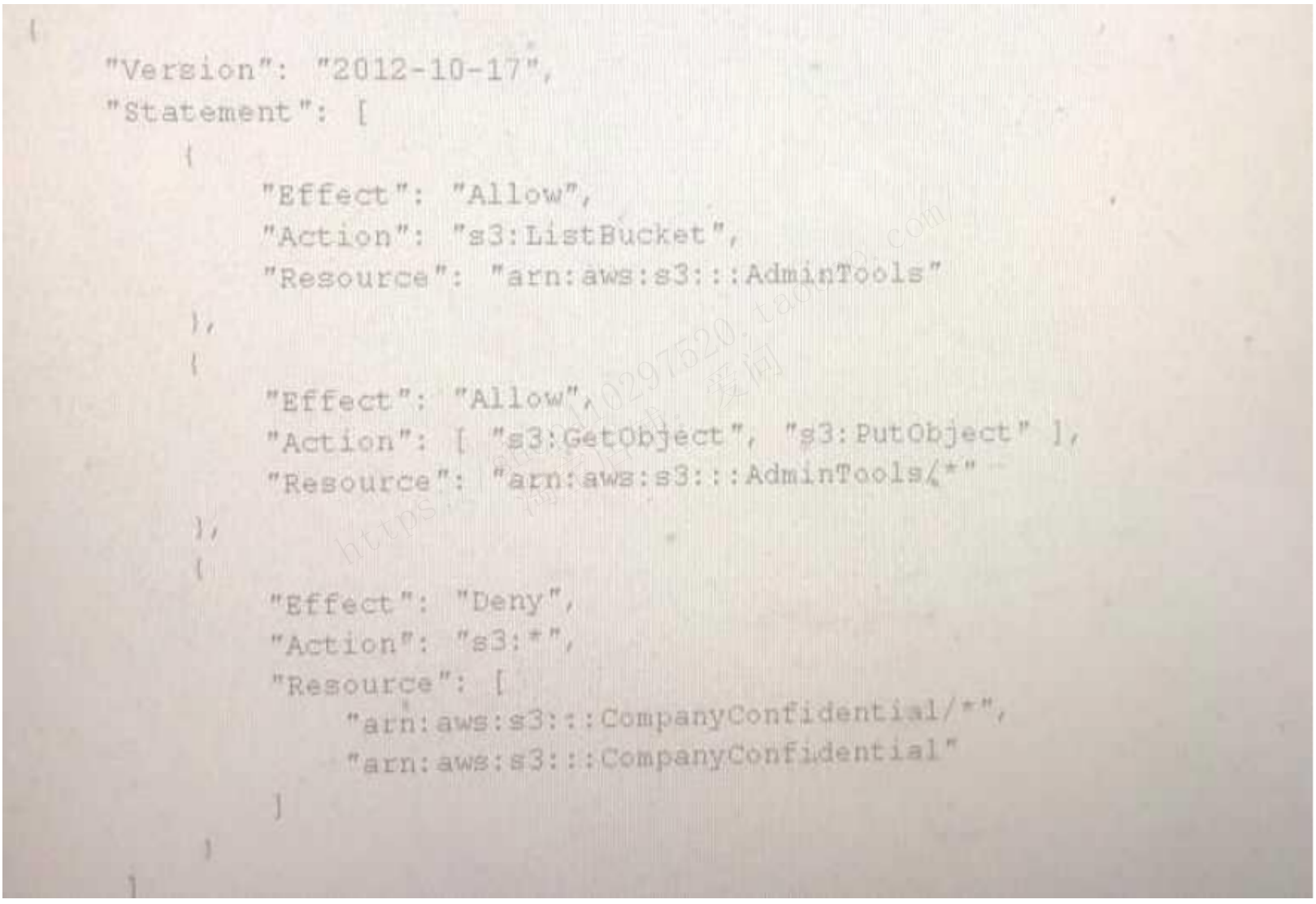
正确答案 D

**解析:**

争议题， C 或者 D, D 作为正确答案 S3 Cross-Region Replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions. Types of object replication You can replicate objects between different AWS Regions or within the same AWS Region. Cross-Region replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions. Same-Region replication (SRR) is used to copy objects across Amazon S3 buckets in the same AWS Region. ---------- Reason : S3 Cross-Region Replication (CRR) is to copy objects across Amazon S3 buckets in different AWS Regions. If your customers are in two geographic locations, you can minimize latency in accessing objects by maintaining object copies in AWS Regions that are geographically closer to your users. Why not D: S3 sync copies missing or outdated files or objects between the source and target so it doesn't copy the entire bucket. If Cross-region replication is enabled on an existing S3 bucket, it will only replicate new objects. The question states that the objects are already in the source S3 bucket so now if you enable CRR, the existing 1PB objects will not be replicated. So CRR cannot be used in this case. The only viable answer is option C.

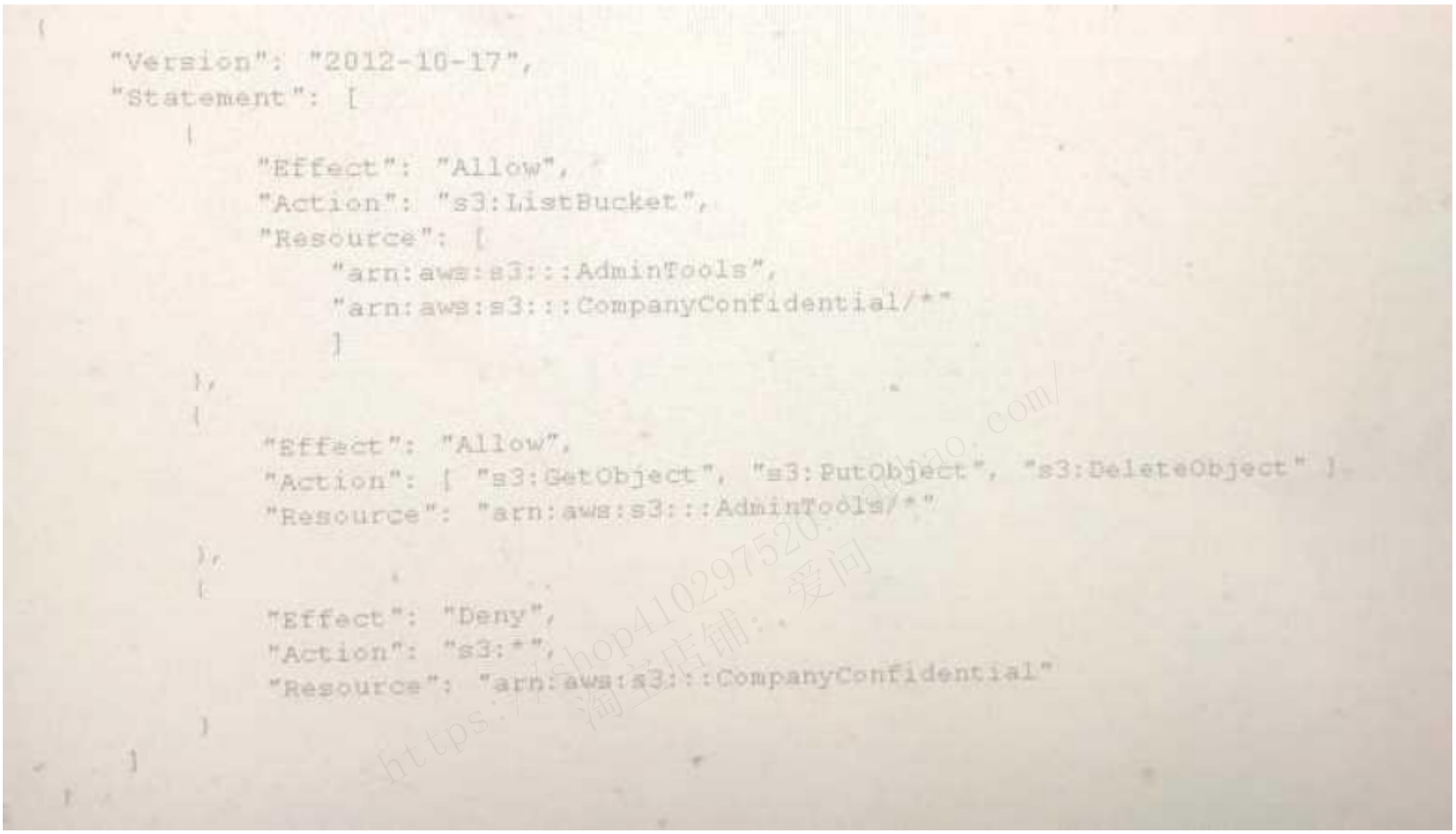
Q278. A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named Company Confidential.The cloud engineer must be able to read from and write to an S3 bucket called AdminTools.Which IAM policy will meet these requirements?

A.



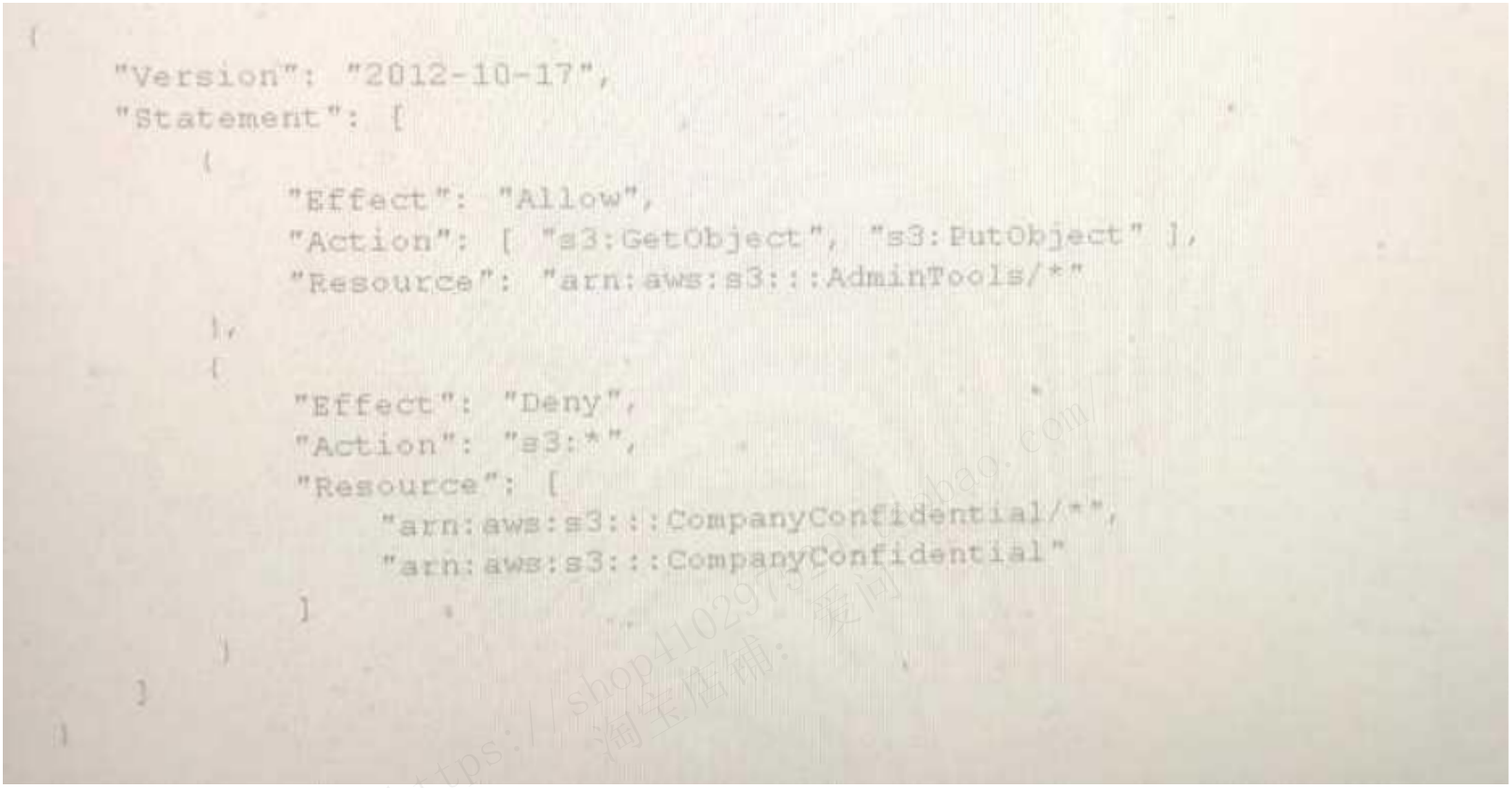
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::AdminTools"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

B.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::AdminTools",
                "arn:aws:s3:::CompanyConfidential/*"
                ]
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::CompanyConfidential"
        }
    ]
}
```

C.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

D.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential",
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::AdminTools/*"
            ]
        }
    ]
}
```

正确答案 A

Q279. An engineering team is developing and deploying AWS Lambda functions. The team needs to create roles and manage policies in AWS IAM to configure the permissions of the Lambda functions.How should the permissions for the team be configured so they also adhere to the concept of least privilege?

A. Create an IAM role with a managed policy attached.Allow the engineering team and the Lambda functions to assume this role

B. Create an IAM group for the engineering team with an lAMFullAccess policy attached.Add all the users from the team to this IAM group

C. Create an execution role for the Lambda functions.Attach a managed policy that has permission boundaries specific to these Lambda functions

D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions.Allow the engineering team to assume this role.

正确答案 D

Q280. A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic.The connection should be set up quickly.What is the MOST cost-effective method to establish this type of connection?

A. Implement a client VPN

B. Implement AWS Direct Connect

C. Implement a bastion host on Amazon EC2 53D.

D. Implement an AWS Site-to-Site VPN connection.

正确答案 D

**解析:**

AWS VPN is comprised of two services: AWS Site-to-Site VPN creates encrypted tunnels between your network and your Amazon Virtual Private Clouds or AWS Transit Gateways. For managing remote access, AWS Client VPN connects your users to AWS or on-premises resources using a VPN software client.
A is incorrect as a client VPN is used to access both your physical data centre and AWS resources via VPN from your workstation. A site to site VPN is used to connect your on premises data centre with your AWS environment.
AWS VPN 由两项服务组成:AWS 站对站 VPN 在您的网络和您的 Amazon 虚拟私有云或 AWS 传输网关之间创建加密隧道。为了管理远程访问，AWS 客户 VPN 使用 VPN 软件客户端将您的用户连接到 AWS 或本地资源。
A 是错误的，因为客户 VPN 是用来通过 VPN 从您的工作站访问您的物理数据中心和 AWS 资源的。站点到站点 VPN 用于将您的现场数据中心与 AWS 环境连接起来。

Q281. A company is building a payment application that must be highly available even during regional service disruptions.A solutions architect must design a data storage solution that can be easily replicated and used in other AWS Regions.The application also requires low-latency atomicity, consistency, isolation, and durability (ACID) transactions that need to be immediately available to generate reports.The development team also needs to use SQL.Which data storage solution meets these requirements'?

A. Amazon Aurora Global Database

B. Amazon DynamoDB global tables

C. Amazon S3 with cross-Region replication and Amazon Athena

D. MySQL on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) snapshot replication

正确答案 A

Q282. A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application.The media files must be resilient to the loss of an Availability Zone Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.Which storage option meets these requirements?

A.S3 Standard

B.S3 Intelligent-Tiering

C.S3 Standard-Infrequent Access (S3 Standard-IA)

D.S3 One Zone-Infrequent Access (S3 One Zone-IA)

正确答案 B

Q283. A company uses a legacy on-premises analytics application that operates on gigabytes of csv files and represents months of data.The legacy application cannot handle the growing size of csv files New csv files are added daily from various data sources to a central on-premises storage location. The company wants to continue to support the legacy application while users learn AWS analytics services.To achieve this, a solutions architect wants to maintain two synchronized copies of all the csv files on-premises and in Amazon S3.Which solution should the solutions architect recommend?

A. Deploy AWS DataSync on-premises.Configure DataSync to continuously replicate the csv files between the company's on-premises storage and the company's S3 bucket

B. Deploy an on-premises file gateway.Configure data sources to write the csv files to the file gateway.Point the legacy analytics application

to the file gateway.The file gateway should replicate the csv files to Amazon S3

C. Deploy an on-premises volume gateway.Configure data sources to write the csv files to the volume gateway.Point the legacy analytics application to the volume gateway.The volume gateway should replicate data to Amazon S3.

D. Deploy AWS DataSync on-premises.Configure DataSync to continuously replicate the csv files between on-premises and Amazon Elastic File System (Amazon EFS).Enable replication from Amazon EFS to the company's S3 bucket.

正确答案 A

**解析:**

"To achieve this, a solutions architect wants to maintain two synchronized copies of all the .csv files on-premises and in Amazon S3." AWS Storage Gateway File Gateway does NOT provide that. Hence the answer is A.

Q284. An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic.A solutions architect needs to optimize the application's performance quickly.What should the solutions architect recommend?

A.Change the existing database to a Multi-AZ deployment.Serve the read requests from the primary Availability Zone.

B.Change the existing database to a Multi-AZ deployment.Serve the read requests from the secondary Availability Zone.

C.Create read replicas for the database.Configure the read replicas with half of the compute and storage resources as the source database.

D.Create read replicas for the database.Configure the read replicas with the same compute and storage resources as the source database.

正确答案 D

Q285. A company wants to optimize the cost of its data storage for data that is accessed quarterly. The company requires high throughput, low latency, and rapid access, when needed. Which Amazon S3 storage class should a solutions architect recommend?

A.Amazon S3 Glacier (S3 Glacier)

B.Amazon S3 Standard (S3 Standard)

C.Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

D.Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

正确答案 D



Q286. A company requires that all versions of objects in its Amazon S3 bucket be retained. Current object versions will be frequently accessed during the first 30 days, after which they will be rarely accessed and must be retrievable within 5 minutes. Previous object versions need to be kept forever, will be rarely accessed, and can be retrieved within 1 week. All storage solutions must be highly available and highly durable. What should a solutions architect recommend to meet these requirements in the MOST cost- effective manner?

A.Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.

B.Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day

C.Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Standard-infrequent Access (S3 Standard-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day

D.Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day

正确答案 B

Q287. A company hosts its core network services, including directory services and DNS. in its on- premises data center.The data center is connected to the AWS Cloud using AWS Direct Connect (DX) Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network servicesWhat should a solutions architect implement to meet these requirements with the LEAST amount of operational overhead?

A. Create a DX connection in each new account.Route the network traffic to the on-premises servers

B. Configure VPC endpoints in the DX VPC for all required services.Route the network traffic to the on- premises servers

C. Create a VPN connection between each new account and the DX VPp Route the network traffic to the on-premises servers

D. Configure AWS Transit Gateway between the accounts.Assign DX to the transit gateway and route network traffic to the on-premises servers

正确答案 D

**解析:**

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex

peering relationships. It acts as a cloud router - each new connection is only made once.

Q288. A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances. Amazon RDS DB instances and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check. What should a solutions architect do to accomplish this''

A.Use AWS Config rules to define and detect resources that are not property tagged

B.Use Cost Explorer to display resources that are not properly tagged Tag those resources manually.

C.Write API calls to check all resources for proper tag allocation.Periodically run the code on an EC2 instance.

D.Write API calls to check all resources for proper tag allocation.Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code

正确答案 A

Q289. An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table.Both the EC2 instance and the DynamoDB table are in the same AWS account. A solutions architect must configure the necessary permissions. Which solution will allow least privilege access to the DynamoDB table from the EC2 instance?

A.Create an IAM role with the appropriate policy to allow access to the DynamoDB table.Create an instance profile to assign this IAM role to the EC2 instance

B.Create an IAM role with the appropriate policy to allow access to the DynamoDB table.Add the EC2 instance to the trust relationship policy document to allow it to assume the role

C.Create an IAM user with the appropriate policy to allow access to the DynamoDB table.Store the credentials in an Amazon S3 bucket and read them from within the application code directly.

D.Create an IAM user with the appropriate policy to allow access to the DynamoDB table.Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls

正确答案 A

Q290. An application uses an Amazon RDS MySQL DB instance.The RDS database is becoming low on disk space.A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

A.Enable storage auto scaling in RDS.

B.Increase the RDS database instance size

C.Change the RDS database instance storage type to Provisioned IOPS.

D.Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance

正确答案 A

Q291. An operations team has a standard that states IAM policies should not be applied directly to users.Some new team members have not been following this standard. The operations manager needs a way to easily identify the users with attached policies. What should a solutions architect do to accomplish this''

A. Monitor using AWS CloudTrail

B. Create an AWS Config rule to run daily.

C. Publish IAM user changes to Amazon SNS

D. Run AWS Lambda when a user is modified

正确答案 B

**解析:**

A new AWS Config rule is deployed in the account after you enable AWS Security Hub. The AWS Config rule reacts to resource configuration and compliance changes and send these change items to AWS CloudWatch. When AWS CloudWatch receives the compliance change, a CloudWatch event rule triggers the AWS Lambda function.
READ215

Q292. A company has an application that runs on Amazon EC2 instances within a private subnet in a VPC.The instances access data in an Amazon S3 bucket in the same AWS Region. The VPC contains a NAT gateway in a public subnet to access the S3 bucket. The company wants to reduce costs by replacing the NAT gateway without compromising security or redundancyWhich solution meets these requirements?

A.Replace the NAT gateway with a NAT instance

B.Replace the NAT gateway with an internet gateway.

C.Replace the NAT gateway with a gateway VPC endpoint

D.Replace the NAT gateway with an AWS Direct Connect connection

正确答案 C

Q293. A company is designing a message-driven order processing application on AWS. The application consists of many services and needs to communicate the results of its processing to multiple consuming

services.Each of the consuming services may take up to 5 days to receive the messages.Which process will meet these requirements?

A. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.Each consuming service subscribes to this SNS topic and consumes the results

B. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.Each consuming service consumes the messages directly from its corresponding SNS topic.

C. The application sends the results of its processing to an Amazon Simple Queue Service (Amazon SQS) queue.Each consuming service runs as an AWS Lambda function that consumes this single SQS queue.

D. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.An Amazon Simple Queue Service (Amazon SQS) queue is created for each service and each queue is configured to be a subscriber of the SNS topic.

正确答案 D

**解析:**

sns 是肯定用的，因为题目里写了 receive the message，所以你需要用 sns 来 push. sqs 只能 poll . 不过为啥不直接从 sns push 到 consumer，要走 sqs 我还没看出来
sns 是”同步”的，无法存储 5 天，所以要到 sqs 蓄积消息

Q294. A company stores call recordings on a monthly basis Statistically, the recorded data may be referenced randomly within a year but accessed rarely after 1 year. Files that are newer than 1 year old must be queried and retrieved as quickly as possible. A delay in retrieving older files is acceptable A solutions architect needs to store the recorded data at a minimal cost.Which solution is MOST cost-effective?

A.Store individual files in Amazon S3 Glacier and store search metadata in object tags created in S3 Glacier.Query S3 Glacier tags and retrieve the files from S3 Glacier

B.Store individual files in Amazon S3 Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year.Query and retrieve the files from Amazon S3 or S3 Glacier.

C.Archive individual files and store search metadata for each archive in Amazon S3.Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year.Query and retrieve the files by searching for metadata from Amazon S3

D.Archive individual files in Amazon S3.Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year.Store search metadata in Amazon DynamoDB Query the files from DynamoDB and retrieve them from Amazon S3 or S3 Glacier

正确答案 B



Q295. A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it.The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.What should the solutions architect recommend?

A. Implement EC2 Spot Instances

B. Purchase EC2 Reserved Instances

C. Implement EC2 On-Demand Instances

D. Implement the processing on AWS Lambda

正确答案 A

**解析:**

Spot instances are cost effective and the question has "stop/start has no negative impact"

Q296. An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service free and paid Photos submitted by paid users are processed before those submitted by free users.Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS. Which configuration should a solutions architect recommend?

A. Use one SQS FIFO queue.Assign a higher priority to the paid photos so they are processed first

B. Use two SQS FIFO queues: one for paid and one for free.Set the free queue to use short polling and the paid queue to use long polling

C. Use two SQS standard queues one for paid and one for free.Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.

D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero.Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first

正确答案 C

**解析:**

FIFO is First In First Out

Q297. A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions.To communicate with each other, the

instances use the internet for connectivity. The security team wants to ensure that no communication between the instances happens over the internet.What should a solutions architect do to accomplish this''

A.Create a NAT gateway and update the route table of the EC2 instances' subnet

B.Create a VPC endpoint and update the route table of the EC2 instances' subnet

C.Create a VPN connection and update the route table of the EC2 instances' subnet

D.Create a VPC peering connection and update the route table of the EC2 instances' subnet

正确答案 D

Q298. A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel.The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime Which solution meets these requirements MOST cost-effectively?

A. Use Spot Instances exclusively to handle the maximum capacity required

B. Use Reserved Instances exclusively to handle the maximum capacity required

C. Use Reserved Instances for the baseline capacity and use Spot InstaKes to handle additional capacity

D. Use Reserved instances for the baseline capacity and use On-Demand Instances to handle additional capacity

正确答案 C

**解析:**

The application is decoup l ed, if the spot instance is terminated, the task(item in the queue) is not lost, hence, the application should still work fine The messages will still be processed by Reserved Instances even there is no available spot instance. It may take longer to process but no message will be lost.

Q299. A company with facilities in North America. Europe, and Asia is designing new distributed application to optimize its global supply chain and manufacturing process. The orders booked on one continent should be visible to all Regions in a second or less. The database should be able to support failover with a short Recovery Time Objective (RTO). The uptime of the application is important to ensure that manufacturing is not impacted.What should a solutions architect recommend?

A.Use Amazon DynamoDB global tables

B.Use Amazon Aurora Global Database

C.Use Amazon RDS for MySQL with a cross-Region read replica

D.Use Amazon RDS for PostgreSQL with a cross-Region read replica

正确答案 A

Q300. A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly.Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to

communicate with Amazon S3 or the outside internet.What should a solutions architect do to optimize costs?

A.Create an additional NAT gateway Update the route table to route to the NAT gateway.Update the network ACL to allow S3 traffic

B.Create an internet gateway Update the route table to route traffic to the internet gateway.Update the network ACL to allow S3 traffic.

C.Create a VPC endpoint for Amazon S3 Attach an endpoint policy to the endpoint.Update the route table to direct traffic to the VPC endpoint

D.Create an AWS Lambda function outside of the VPC to handle S3 requests.Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

正确答案 C

Q301. A company hosts a training site on a fleet of Amazon EC2 instances. The company anticipates that its new course, which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week. What should a solutions architect do to minimize the anticipated server load?

A. Store the videos in Amazon ElastiCache for Redis.Update the web servers to serve the videos using the Elastic ache API

B. Store the videos in Amazon Elastic File System (Amazon EFS).Create a user data script for the web servers to mount the EFS volume.

C. Store the videos in an Amazon S3 bucket.Create an Amazon CloudFlight distribution with an origin access identity (OAI) of that S3 bucket.Restrict Amazon S3 access to the OAI.

D. Store the videos in an Amazon S3 bucket.Create an AWS Storage Gateway file gateway to access the S3 bucket.Create a user data script for the web servers to mount the file gateway

正确答案 C

**解析:**

A. We would have to store the videos on an RDS, not sure if that would be suitable..... B. How does this help minimize the anticipated server load? C. R right, the best option probably. D. We're not running anything on premise.

Q302. A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video file has become popular and a large number of users across the world are accessing this content.This has resulted in a cost increase.Which action will DECREASE cost without compromising user accessibility?

A.Change the EBS volume to Provisioned IOPS (PIOPS).

B.Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.

C.Split the video into multiple, smaller segments so users are routed to the requested video segments only.

D.Clear an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket.

正确答案 B

Q303. A solutions architect is designing the cloud architecture for a new application being deployed to AWS. The application allows users to interactively download and upload files. Files older than 2 years will be accessed less frequently. The solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.Which scalable solutions should the solutions architect recommend? (Choose two.)

A.Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.

B.Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard-Infrequent Access (S3 Standard-IA)

C.Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).

D.Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

E.Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

正确答案 B,C

Q304. A company is hosting multiple websites for several lines of business under its registered parent domain. Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on the subdomain. The websites host static webpages, images, and server-side scripts like PHP and JavaScript.Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.Which combination of AWS services or features will meet these requirements? (Choose two.)

A. AWS Batch

B. Network Load Balancer

C. Application Load Balancer

D. Amazon EC2 Auto Scaling

E. Amazon S3 website hosting

正确答案 C,D

Q305. A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.What should the solutions architect do to reduce the overall data transfer costs?

A.Place all the EC2 instances in an Auto Scaling group.

B.Place all the EC2 instances in the same AWS Region.

C.Place all the EC2 instances in the same Availability Zone.

D.Place all the EC2 instances in private subnets in multiple Availability Zones.

正确答案 C



Q306. A company is hosting an election reporting website on AWS for users around the world. The website uses Amazon EC2 instances for the web and application tiers in an Auto Scaling group with Application Load Balancers. The database tier uses an Amazon RDS for MySQL database. The website is updated with election results once an hour and has historically observed hundreds of users accessing the reports.The company is expecting a significant increase in demand because of upcoming elections in different countries. A solutions architect must improve the website's ability to handle additional demand while minimizing the need for additional EC2 instances.Which solution will meet these requirements?

A.Launch an Amazon ElastiCache cluster to cache common database queries.

B.Launch an Amazon CloudFront web distribution to cache commonly requested website content.

C.Enable disk-based caching on the EC2 instances to cache commonly requested website content.

D.Deploy a reverse proxy into the design using an EC2 instance with caching enabled for commonly requested website content.

正确答案 B

Q307. A company is running a three-tier web application to process credit card payments. The front-end user interface consists of static webpages. The application tier can have long-running processes.The database tier uses MySQL.The application is currently running on a single, general purpose large Amazon EC2 instance. A solutions architect needs to decouple the services to make the web application highly available.Which solution would provide the HIGHEST availability?

A.Move static assets to Amazon CloudFront.Leave the application in EC2 in an Auto Scaling group.Move the database to Amazon RDS to deploy Multi-AZ.

B.Move static assets and the application into a medium EC2 instance.Leave the database on the large instance.Place both instances in an Auto Scaling group.

C.Move static assets to Amazon S3, Move the application to AWS Lambda with the concurrency limit set.Move the database to Amazon DynamoDB with on-demand enabled.

D.Move static assets to Amazon S3.Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled.Move the database to Amazon RDS to deploy Multi-AZ.

正确答案 D