1) **A company is storing an access key (access key ID and secret access key) in a text file on a custom AMI. The company uses the access key to access DynamoDB tables from instances created from the AMI. The security team has mandated a more secure solution.**

   Which solution will meet the security team's mandate?

   A. Put the access key in an S3 bucket, and retrieve the access key on boot from the instance.
   B. Pass the access key to the instances through instance user data.
   C. Obtain the access key from a key server launched in a private subnet.
   D. Create an IAM role with permissions to access the table, and launch all instances with the new role.

2) **A company is developing a highly available web application using stateless web servers. Which services are suitable for storing session state data? (Select TWO.)**

   A. CloudWatch
   B. DynamoDB
   C. Elastic Load Balancing
   D. ElastiCache
   E. Storage Gateway

3) **Company salespeople upload their sales figures daily. A Solutions Architect needs a durable storage solution for these documents that also protects against users accidentally deleting important documents.**

   Which action will protect against unintended user actions?

   A. Store data in an EBS volume and create snapshots once a week.
   B. Store data in an S3 bucket and enable versioning.
   C. Store data in two S3 buckets in different AWS regions.
   D. Store data on EC2 instance storage.

4) **An application requires a highly available relational database with an initial storage capacity of 8 TB. The database will grow by 8 GB every day. To support expected traffic, at least eight read replicas will be required to handle database reads.**

   Which option will meet these requirements?

   A. DynamoDB
   B. Amazon S3
   C. Amazon Aurora
   D. Amazon Redshift

5) A Solutions Architect is designing a critical business application with a relational database that runs on an EC2 instance. It requires a single EBS volume that can support up to 16,000 IOPS.

Which Amazon EBS volume type can meet the performance requirements of this application?

A. EBS Provisioned IOPS SSD
B. EBS Throughput Optimized HDD
C. EBS General Purpose SSD
D. EBS Cold HDD

6) A web application allows customers to upload orders to an S3 bucket. The resulting Amazon S3 events trigger a Lambda function that inserts a message to an SQS queue. A single EC2 instance reads messages from the queue, processes them, and stores them in an DynamoDB table partitioned by unique order ID. Next month traffic is expected to increase by a factor of 10 and a Solutions Architect is reviewing the architecture for possible scaling problems.

Which component is MOST likely to need re-architecting to be able to scale to accommodate the new traffic?

A. Lambda function
B. SQS queue
C. EC2 instance
D. DynamoDB table

7) An application saves the logs to an S3 bucket. A user wants to keep the logs for one month for troubleshooting purposes, and then purge the logs.

What feature will enable this?

A. Adding a bucket policy on the S3 bucket.
B. Configuring lifecycle configuration rules on the S3 bucket.
C. Creating an IAM policy for the S3 bucket.
D. Enabling CORS on the S3 bucket.

8) An application running on EC2 instances processes sensitive information stored on Amazon S3. The information is accessed over the Internet. The security team is concerned that the Internet connectivity to Amazon S3 is a security risk.

Which solution will resolve the security concern?

A. Access the data through an Internet Gateway.
B. Access the data through a VPN connection.
C. Access the data through a NAT Gateway.
D. Access the data through a VPC endpoint for Amazon S3.

9) An organization is building an Amazon Redshift cluster in their shared services VPC. The cluster will host sensitive data.

How can the organization control which networks can access the cluster?

A. Run the cluster in a different VPC and connect through VPC peering.
B. Create a database user inside the Amazon Redshift cluster only for users on the network.
C. Define a cluster security group for the cluster that allows access from the allowed networks.
D. Only allow access to networks that connect with the shared services network via VPN.

10) A Solutions Architect is designing an online shopping application running in a VPC on EC2 instances behind an ELB Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The application tier must read and write data to a customer managed database cluster. There should be no access to the database from the Internet, but the cluster must be able to obtain software patches from the Internet.

Which VPC design meets these requirements?

A. Public subnets for both the application tier and the database cluster
B. Public subnets for the application tier, and private subnets for the database cluster
C. Public subnets for the application tier and NAT Gateway, and private subnets for the database cluster
D. Public subnets for the application tier, and private subnets for the database cluster and NAT Gateway

Answers

1) D – IAM roles for EC2 instances allow applications running on the instance to access AWS resources without having to create and store any access keys. Any solution involving the creation of an access key then introduces the complexity of managing that secret.

2) B, D – Both DynamoDB and ElastiCache provide high performance storage of key-value pairs. CloudWatch and ELB are not storage services. Storage Gateway is a storage service, but it is a hybrid storage service that enables on-premises applications to use cloud storage.

3) B – If a versioned object is deleted, then it can still be recovered by retrieving the final version. Response A would lose any changes committed since the previous snapshot. Storing the data in 2 S3 buckets would provide slightly more protection, but a user could still delete the object from both buckets. EC2 instance storage is ephemeral and should never be used for data requiring durability.

4) C – Amazon Aurora is a relational database that will automatically scale to accommodate data growth. Amazon Redshift does not support read replicas and will not automatically scale. DynamoDB is a NoSQL service, not a relational database. Amazon S3 is object storage, not a relational database.

5) A – EBS Provisioned IOPS SSD provides sustained performance for mission-critical low-latency workloads. EBS General Purpose SSD can provide bursts of performance up to 3,000 IOPS and have a maximum baseline performance of 10,000 IOPS for volume sizes greater than 3.3 TB. The 2 HDD options are lower cost, high throughput volumes.

6) C – A single EC2 instance will not scale and is a single point of failure in the architecture. A much better solution would be to have EC2 instances in an Auto Scaling group across 2 availability zones read messages from the queue. The other responses are all managed services that can be configured to scale or will scale automatically.

7) B – Lifecycle configuration allows lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. Bucket policies and IAM define access to objects in an S3 bucket. CORS enables clients in one domain to interact with resources in a different domain.

8) D – VPC endpoints for Amazon S3 provide secure connections to S3 buckets that do not require a gateway or NAT instances. NAT Gateways and Internet Gateways still route traffic over the Internet to the public endpoint for Amazon S3. There is no way to connect to Amazon S3 via VPN.

9) C – A security group can grant access to traffic from the allowed networks via the CIDR range for each network. VPC peering and VPN are connectivity services and cannot control traffic for security. Amazon Redshift user accounts address authentication and authorization at the user level and have no control over network traffic.

10) C – The online application must be in public subnets to allow access from clients' browsers. The database cluster must be in private subnets to meet the requirement that there be no access from the Internet. A

NAT Gateway is required to give the database cluster the ability to download patches from the Internet. NAT Gateways must be deployed in public subnets.

