AWS\_SAA\_Exam\_Questions

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 typecan 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 singleEC2 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 logsto an S3 bucket. A user wants to keep the logs forone 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.

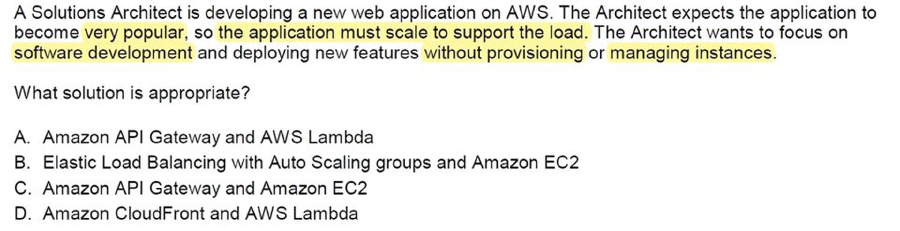
10) A Solutions Architect is designing an online shopping application running in a VPC on EC2 instances behind an ELB Application Load Balancer.The instances run in an Auto Scaling group across multiple Availability Zones. The application tiermust read and write data to a customer managed database cluster. 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.

11) 

12) Your architecture team has recommended the following for the VPC's in your AWS Account

· A shared services VPC which would provide services to other VPC's.

· A hosted VPC that will be accessible to the customer.

· The hosted VPC will also interact with the shared services VPC.

Which of the following should also be considered as part of the design? Choose 3 answers from the options given below. Each answer is an independent design solution.

**A.** Ensure a virtual private link is available for accessing the Shared services VPC.

**B.** Use VPC peering between the shared services VPC and other VPC's

**C.** Put the shared services VPC as public. Ensure the right security measures are in place for accessing the shared services.

**D.** Create a VPN between each VPC. Ensure the Virtual private gateway is in place for the other VPC's

**E.** Create 'transitive peering' where necessary between the VPC's

13) You have a daily job running on top of your RDS database, running at 7 am. It processes shipping orders for the past day, and usually you get around 2000 rows that need to be processed based on a Python script. The processing of each row takes about 3 seconds. What platform do you recommend to run this batch job?

A. Glue

B. Kinesis Streams

C. Lambda

D. RDS

E. EC2

14) You have an application running on an Amazon EC2 instance that uploads 10 GB video objects to amazon S3. Video uploads are taking longer than expected inspite of using multipart upload cause of internet bandwidth, resulting in poor application performance. Which action can help improve the upload performance?

A. Apply an Amazon S3 bucket policy

B. Use Amazon EBS provisioned IOPS

C. Use VPC endpoints for S3

D. Request a service limit increase

15) What are the services supported by VPC endpoints, using Gateway endpoint type? Choose 2 answers

A. Amazon S3

B. Amazon EFS

C. Amazon DynamoDB

D. Amazon GlacierAmazon SQS

16. What are the different types of endpoint types supported by VPC endpoints? Choose 2answers

A. Gateway

B. Classic

C. Interface

D. Virtual

E. Network

17) 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.

18) You need to design a VPC for a three-tier architecture, web-application consisting of an Elastic Load Balancer (ELB), a fleet of web/application servers, and backend consisting of an RDS database. The entire Infrastructure must be distributed over 2 availability zones. Which VPC configuration works while assuring the least components are exposed to Internet?

A. Two public subnets for ELB, two private subnets for the web-servers, two private subnets for RDS and DynamoDB

B. Two public subnets for ELB and web-servers, two private subnets for RDS and DynamoDB

C. Two public subnets for ELB, two private subnets for the web-servers, two private subnets for RDS and VPC Endpoints for DynamoDB

D. Two public subnets for ELB and web-servers, two private subnets for RDS and VPC Endpoints for DynamoDB

1. What does Amazon Route53 provide?
   1. A global Content Delivery Network.
   2. None of these.
   3. **A scalable Domain Name System**
   4. An SSH endpoint for Amazon EC2.
2. Does Amazon Route 53 support NS Records?
   1. Yes, it supports Name Service records.
   2. No
   3. It supports only MX records.
   4. **Yes, it supports Name Server records.**
3. Does Route 53 support MX Records?
   1. **Yes**
   2. It supports CNAME records, but not MX records.
   3. No
   4. Only Primary MX records. Secondary MX records are not supported.
4. Which of the following statements are true about Amazon Route 53 resource records? Choose 2 answers
   1. **An Alias record can map one DNS name to another Amazon Route 53 DNS name.**
   2. A CNAME record can be created for your zone apex.
   3. **An Amazon Route 53 CNAME record can point to any DNS record hosted anywhere.**
   4. TTL can be set for an Alias record in Amazon Route 53.
   5. An Amazon Route 53 Alias record can point to any DNS record hosted anywhere.
5. Which statements are true about Amazon Route 53? (Choose 2 answers)
   1. Amazon Route 53 is a region-level service
   2. **You can register your domain name**
   3. **Amazon Route 53 can perform health checks and failovers to a backup site in the even of the primary site failure**
   4. Amazon Route 53 only supports Latency-based routing
6. A customer is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The customer also uses Amazon Route 53 to manage their public DNS. How should the customer configure the DNS zone apex record to point to the load balancer?
   1. Create an A record pointing to the IP address of the load balancer
   2. Create a CNAME record pointing to the load balancer DNS name.
   3. Create a CNAME record aliased to the load balancer DNS name.
   4. **Create an A record aliased to the load balancer DNS name**
7. A user has configured ELB with three instances. The user wants to achieve High Availability as well as redundancy with ELB. Which of the below mentioned AWS services helps the user achieve this for ELB?
   1. **Route 53**
   2. AWS Mechanical Turk
   3. Auto Scaling
   4. AWS EMR
8. How can the domain’s zone apex for example “myzoneapexdomain com” be pointed towards an Elastic Load Balancer?
   1. By using an AAAA record
   2. By using an A record
   3. By using an Amazon Route 53 CNAME record
   4. **By using an Amazon Route 53 Alias record**
9. You need to create a simple, holistic check for your system’s general availability and uptime. Your system presents itself as an HTTP-speaking API. What is the simplest tool on AWS to achieve this with?
   1. **Route53 Health Checks (**Refer [link](http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html)**)**
   2. CloudWatch Health Checks
   3. AWS ELB Health Checks
   4. EC2 Health Checks
10. Your organization’s corporate website must be available on www.acme.com and acme.com. How should you configure Amazon Route 53 to meet this requirement?
    1. **Configure acme.com with an ALIAS record targeting the ELB. www.acme.com with an ALIAS record targeting the ELB.**
    2. Configure acme.com with an A record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
    3. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
    4. Configure acme.com using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.

**ANS:**

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. **For more information click**[**here.**](https://youtu.be/YCSxln-10aQ)

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. **For more information click**[**here.**](https://youtu.be/_AzblCVy5Z4)

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 - Asingle 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. **For more information Click**[**here**](https://asmed.com/amazon-aws-auto-scaling-with-load-balancing/)

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.  **For more information Click**[**here**](https://asmed.com/amazon-aws-s3-vpc-endpoint/)

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. **For more information Click**[**here**](https://youtu.be/uEzf1TznKEA)

10) C - The online application must be inpublic 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. **For more information Click**[**here**](https://asmed.com/amazon-aws-nat-instance-and-nat-gateway/)

11) A

12) **A, B & C** - D (you don't need VPN between VPC) & E (transitive peering is not supported) are not correct options. ABC are correct.

13) C

14) C

15) A & C

16) A & C

17) D

18) C

1. C
2. D
3. A
4. A,C
5. B,C
6. D
7. A
8. D
9. A
10. A

**Scenario -1**: There are client feed files coming in via SFTP - we need to take this data, apply some basic quality checks and load it into a RDBMS - All of this needs to be in AWS. These files follow a fixed format with separators. Size of daily files could be ~100 MB

Kindly advise what are the AWS PaaS services available to do the job? I am OK to add few custom stuff supplementing the AWS services

**ANS**: You can use AWS STFP transfer service to drop the files to an s3 bucket and use SNS and lambda to trigger the glue job to process and push the data to RDS. you can use lamda to collect metadata about files and persit the metadata in dynamo db.

Q) What is a **VPC Endpoint**?

A VPC endpoint enables you to create a private connection between your VPC and another AWS service without requiring access over the Internet, through a NAT device, a VPN connection, or AWS Direct Connect.

REF: <https://medium.com/nubego/how-to-save-money-with-aws-vpc-endpoints-9bac8ae1319c>

<http://jayendrapatil.com/aws-vpc-endpoints/>