QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

SAP-C01 Dumps
SAP-C01 Braindumps
SAP-C01 Real Questions
SAP-C01 Practice Test
SAP-C01 dumps free

Amazon

SAP-C01

AWS Certified Solutions Architect – Professional

Question: 99

You would like to create a mirror image of your production environment in another region for disaster recovery purposes.

Which of the following AWS resources do not need to be recreated in the second region? (Choose two.)
A . Route 53 Record Sets
B . IAM Roles
C . Elastic IP Addresses (EIP)
D . EC2 Key Pairs
E . Launch configurations
F . Security Groups

Answer: AB

Explanation:

As per the document defined, new IPs should be reserved not the same ones Elastic IP Addresses are static IP addresses designed for dynamic cloud computing. Unlike traditional static IP addresses, however, Elastic IP addresses enable you to mask instance or Availability Zone failures by programmatically remapping your public IP addresses to instances in your account in a particular region. For DR, you can also pre-allocate some IP addresses for the most critical systems so that their IP addresses are already known before disaster strikes. This can simplify the execution of the DR plan.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html

Question: 100

A web company is looking to implement an intrusion detection and prevention system into their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC.

How should they architect their solution to achieve these goals?
A . Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see an traffic across the VP
C . Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides.
D . Configure servers running in the VPC using the host-based ‘route’ commands to send all traffic through the platform to a scalable virtualized IDS/IP
F . Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.

Answer: D

Question: 101

A customer is deploying an SSL enabled web application to AWS and would like to implement a separation of roles

between the EC2 service administrators that are entitled to login to instances as well as making API calls and the security officers who will maintain and have exclusive access to the application's X.509 certificate that contains the private key.
A . Upload the certificate on an S3 bucket owned by the security officers and accessible only by EC2 Role of the web servers.
B . Configure the web servers to retrieve the certificate upon boot from an CloudHSM is managed by the security officers.
C . Configure system permissions on the web servers to restrict access to the certificate only to the authority security officers
D . Configure IAM policies authorizing access to the certificate store only to the security officers and terminate SSL on an EL

Answer: D

Explanation:

You'll terminate the SSL at ELB. and the web request will get unencrypted to the EC2 instance, even if the certs are stored in S3, it has to be configured on the web servers or load balancers somehow, which becomes difficult if the keys are stored in S3.

However, keeping the keys in the cert store and using IAM to restrict access gives a clear separation of concern between security officers and developers. Developer's personnel can still configure SSL on ELB without actually handling the keys.

Question: 102

A web company is looking to implement an intrusion detection and prevention system into their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC.

How should they architect their solution to achieve these goals?
A . Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see an traffic across the VP
C . Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides.
D . Configure servers running in the VPC using the host-based 'route' commands to send all traffic through the platform to a scalable virtualized IDS/IP
F . Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.

Answer: D

Question: 103

You've been hired to enhance the overall security posture for a very large e-commerce site. They have a well architected multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3. They are using a combination of RDS and DynamoDB for their dynamic data and then archiving nightly into S3 for further processing with EMR. They are concerned because they found questionable log entries and suspect someone is attempting to gain unauthorized access.

Which approach provides a cost effective scalable mitigation to this kind of attack?

A . Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to their VPC they would then establish Internet connectivity into their space, filter the traffic in hardware Web Application Firewall (WAF). And then pass the traffic through the DirectConnect connection into their application running in their VP
C . Add previously identified hostile source IPs as an explicit INBOUND DENY NACL to the web tier subnet.
D . Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WA
E . They would redirect Route 53 to resolve to the new WAF tier EL
F . The WAF tier would their pass the traffic to the current web tier The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group
G . Remove all but TLS 1.2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.

Answer: C

Question: 104

Your team has a tomcat-based Java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC.

The optimal setup for persistence and security that meets the above requirements would be the following.
A . Create your RDS instance as part of your Elastic Beanstalk definition and alter its security group to allow access to it from hosts in your application subnets.
B . Create your RDS instance separately and add its IP address to your application's DB connection strings in your code Alter its security group to allow access to it from hosts within your VPC's IP address block.
C . Create your RDS instance separately and pass its DNS name to your app's DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself.
D . Create your RDS instance separately and pass its DNS name to your's DB connection string as an environment variable Alter its security group to allow access to It from hosts in your application subnets.

Answer: A

Explanation:

Elastic Beanstalk provides support for running Amazon RDS instances in your Elastic Beanstalk environment. This works great for development and testing environments, but is not ideal for a production environment because it ties the lifecycle of the database instance to the lifecycle of your application's environment.

Reference: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo.RDS.html

Question: 105

Your company is in the process of developing a next generation pet collar that collects biometric information to assist families with promoting healthy lifestyles for their pets. Each collar will push 30kb of biometric data in JSON format every 2 seconds to a collection platform that will process and analyze the data providing health trending information back to the pet owners and veterinarians via a web portal. Management has tasked you to architect the collection platform ensuring the following requirements are met.

– Provide the ability for real-time analytics of the inbound biometric data

– Ensure processing of the biometric data is highly durable. Elastic and parallel

– The results of the analytic processing should be persisted for data mining

Which architecture outlined below win meet the initial requirements for the collection platform?
A . Utilize S3 to collect the inbound sensor data analyze the data from S3 with a daily scheduled Data Pipeline and save the results to a Redshift Cluster.
B . Utilize Amazon Kinesis to collect the inbound sensor data, analyze the data with Kinesis clients and save the results to a Redshift cluster using EM
D . Utilize SQS to collect the inbound sensor data analyze the data from SQS with Amazon Kinesis and save the results to a Microsoft SQL Server RDS instance.
E . Utilize EMR to collect the inbound sensor data, analyze the data from EUR with Amazon Kinesis and save me results to DynamoD

Answer: B

Question: 106

Your company policies require encryption of sensitive data at rest. You are considering the possible options for protecting data while storing it at rest on an EBS data volume, attached to an EC2 instance.

Which of these options would allow you to encrypt your data at rest? (Choose three.)
A . Implement third party volume encryption tools
B . Implement SSL/TLS for all services running on the server
C . Encrypt data inside your applications before storing it on EBS
D . Encrypt data using native data encryption drivers at the file system level
E . Do nothing as EBS volumes are encrypted by default

Answer: ACD

Question: 107

A company is storing data on Amazon Simple Storage Service (S3). The company’s security policy mandates that data is encrypted at rest.

Which of the following methods can achieve this? (Choose three.)
A . Use Amazon S3 server-side encryption with AWS Key Management Service managed keys.
B . Use Amazon S3 server-side encryption with customer-provided keys.
C . Use Amazon S3 server-side encryption with EC2 key pair.
D . Use Amazon S3 bucket policies to restrict access to the data at rest.
E . Encrypt the data on the client-side before ingesting to Amazon S3 using their own master key.
F . Use SSL to encrypt the data while in transit to Amazon S3.

Answer: ABE

Explanation:

Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

Question: 108

You are designing Internet connectivity for your VPC. The Web servers must be available on the Internet. The application must have a highly available architecture.

Which alternatives should you consider? (Choose two.)
A . Configure a NAT instance in your VP
B . Create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address.
C . Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your CloudFront distribution.
D . Place all your web servers behind EL
E . Configure a Route53 CNMIE to point to the ELB DNS name.
F . Assign EIPs to all web servers. Configure a Route53 record set with all EIPs, with health checks and DNS failover.
G . Configure ELB with an EI
H . Place all your Web servers behind EL
. Configure a Route53 A record that points to the EI

Answer: CD

Question: 109

Your firm has uploaded a large amount of aerial image data to S3. In the past, in your on-premises environment, you used a dedicated group of servers to oaten process this data and used Rabbit MQ – An open source messaging system to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost.

Which is correct?
A . Use SQS for passing job messages use Cloud Watch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
B . Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SOS Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
C . Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS Once data is processed, change the storage class of the S3 objects to Glacier.
D . Use SNS to pass job messages use Cloud Watch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.

Answer: C

Question: 110

You are implementing AWS Direct Connect. You intend to use AWS public service end points such as Amazon S3, across the AWS Direct Connect link. You want other Internet traffic to use your existing link to an Internet Service Provider.

What is the correct way to configure AWS Direct connect for access to services such as Amazon S3?

A . Configure a public Interface on your AWS Direct Connect link. Configure a static route via your AWS Direct Connect link that points to Amazon S3 Advertise a default route to AWS using BG
C . Create a private interface on your AWS Direct Connect link. Configure a static route via your AWS Direct connect link that points to Amazon S3 Configure specific routes to your network in your VP
E . Create a public interface on your AWS Direct Connect link. Redistribute BGP routes into your existing routing infrastructure; advertise specific routes for your network to AW
G . Create a private interface on your AWS Direct connect link. Redistribute BGP routes into your existing routing infrastructure and advertise a default route to AW

Answer: C

Explanation:

https://aws.amazon.com/directconnect/faqs/

Question: 111

You have recently joined a startup company building sensors to measure street noise and air quality in urban areas. The company has been running a pilot deployment of around 100 sensors for 3 months each sensor uploads 1KB of sensor data every minute to a backend hosted on AWS. During the pilot, you measured a peak or 10 IOPS on the database, and you stored an average of 3GB of sensor data per month in the database. The current deployment consists of a load-balanced auto scaled Ingestion layer using EC2 instances and a PostgreSQL RDS database with 500GB standard storage. The pilot is considered a success and your CEO has managed to get the attention or some potential investors. The business plan requires a deployment of at least 100K sensors which needs to be supported by the backend. You also need to store sensor data for at least two years to be able to compare year over year Improvements. To secure funding, you have to make sure that the platform meets these requirements and leaves room for further scaling.

Which setup win meet the requirements?
A . Add an SQS queue to the ingestion layer to buffer writes to the RDS instance
B . Ingest data into a DynamoDB table and move old data to a Redshift cluster
C . Replace the RDS instance with a 6 node Redshift cluster with 96TB of storage
D . Keep the current architecture but upgrade RDS storage to 3TB and 10K provisioned IOPS

Answer: C

Explanation:

The POC solution is being scaled up by 1000, which means it will require 72TB of Storage to retain 24 months' worth of data. This rules out RDS as a possible DB solution which leaves you with Redshift. I believe DynamoDB is a more cost effective and scales better for ingest rather than using EC2 in an auto scaling group. Also, this example solution from AWS is somewhat similar for reference.

http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_timeseriesprocessing_16.pdf

Question: 112

Your company has an on-premises multi-tier PHP web application, which recently experienced downtime due to a large burst in web traffic due to a company announcement Over the coming days, you are expecting similar announcements to drive similar unpredictable bursts, and are looking to find ways to quickly improve your

infrastructures ability to handle unexpected increases in traffic. The application currently consists of 2 tiers a web tier which consists of a load balancer and several Linux Apache web servers as well as a database tier which hosts a Linux server hosting a MySQL database.

Which scenario below will provide full site functionality, while helping to improve the ability of your application in the short timeframe required?
A . Failover environment: Create an S3 bucket and configure it for website hosting. Migrate your DNS to Route53 using zone file import, and leverage Route53 DNS failover to failover to the S3 hosted website.
B . Hybrid environment: Create an AMI, which can be used to launch web servers in EC2. Create an Auto Scaling group, which uses the AMI to scale the web tier based on incoming traffic. Leverage Elastic Load Balancing to balance traffic between on-premises web servers and those hosted in AW
D . Offload traffic from on-premises environment: Setup a CIoudFront distribution, and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behavior, and select a TTL that objects should exist in cache.
E . Migrate to AWS: Use VM Import/Export to quickly convert an on-premises web server to an AM
F . Create an Auto Scaling group, which uses the imported AMI to scale the web tier based on incoming traffic. Create an RDS read replica and setup replication between the RDS instance and on-premises MySQL server to migrate the database.

Answer: C

Explanation:

You can have CloudFront sit in front of your on-prem web environment, via a custom origin (the origin doesn’t have to be in AWS). This would protect against unexpected bursts in traffic by letting CloudFront handle the traffic that it can out of cache, thus hopefully removing some of the load from your on-prem web servers.