➢ Vendor: Amazon

➢ Exam Code: AWS Certified Solutions Architect - Associate

➢ Exam Name: AWS Certified Solutions Architect - Associate

➢ Question 201 – Question 250

QUESTION 201
Which services allow the customer to retain full administrative privileges of the underlying EC2 instances? Choose 2 answers

A. Amazon Relational Database Service
B. Amazon Elastic Map Reduce
C. Amazon ElastiCache
D. Amazon DynamoDB
E. AWS Elastic Beanstalk

Answer: BE

QUESTION 202
A company is building a two-tier web application to serve dynamic transaction-based content. The data tier is leveraging an Online Transactional Processing (OLTP) database. What services should you leverage to enable an elastic and scalable web tier?

A. Elastic Load Balancing, Amazon EC2, and Auto Scaling
B. Elastic Load Balancing, Amazon RDS with Multi-AZ, and Amazon S3
C. Amazon RDS with Multi-AZ and Auto Scaling
D. Amazon EC2, Amazon DynamoDB, and Amazon S3

Answer: A

QUESTION 203
Your application provides data transformation services. Files containing data to be transformed are first uploaded to Amazon S3 and then transformed by a fleet of spot EC2 instances. Files submitted by your premium customers must be transformed with the highest priority. How should you implement such a system?

A. Use a DynamoDB table with an attribute defining the priority level. Transformation instances will scan the table for tasks, sorting the results by priority level.
B. Use Route 53 latency based-routing to send high priority tasks to the closest transformation instances.
C. Use two SQS queues, one for high priority messages, the other for default priority. Transformation instances first poll the high priority queue; if there is no message, they poll the default priority queue.
D. Use a single SQS queue. Each message contains the priority level. Transformation instances poll high-priority messages first.

Answer: C

QUESTION 204
Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

A. Use an IAM policy that references the LDAP account identifiers and the AWS credentials.
B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
D. Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.
E. Use the LDAP credentials to restrict a group of users from launching specific EC2 instance types.

Answer: B
Explanation:
https://d0.awsstatic.com/whitepapers/aws-whitepaper-single-sign-on-integrating-aws-open-ldap-and-shibboleth.pdf

QUESTION 205
Which of the following are characteristics of Amazon VPC subnets? Choose 2 answers.

A. Each subnet spans at least 2 Availability Zones to provide a high-availability environment.
B. Each subnet maps to a single Availability Zone.
C. CIDR block mask of/25 is the smallest range supported.
D. By default, all subnets can route between each other, whether they are private or public.
E. Instances in a private subnet can communicate with the Internet only if they have an Elastic IP.

Answer: BD
Explanation:
Even though we know the right Answers it is sometimes good to know why the other Answers are wrong.
A. Is wrong because a subnet maps to a single AZ.
C. Is wrong because /28 is the smallest subnet, amazon takes first four and last addresses per subnet.
E. Is wrong because a private subnet needs a NAT appliance.

QUESTION 206
A customer is leveraging Amazon Simple Storage Service in eu-west-1 to store static content for a web-based property. The customer is storing objects using the Standard Storage class. Where are the customers objects replicated?

A. A single facility in eu-west-1 and a single facility in eu-central-1
B. A single facility in eu-west-1 and a single facility in us-east-1
C. Multiple facilities in eu-west-1
D. A single facility in eu-west-1

Answer: C
Explanation:
Objects stored in a region never leave the region unless you explicitly transfer them to another region. For example, objects stored in the EU (Ireland) region never leave it.
http://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html#Regions

QUESTION 207
Your web application front end consists of multiple EC2 instances behind an Elastic Load Balancer. You configured ELB to perform health checks on these EC2 instances, if an instance fails to pass health checks, which statement will be true?

A. The instance gets terminated automatically by the ELB.
B. The instance gets quarantined by the ELB for root cause analysis.
C. The instance is replaced automatically by the ELB.
D. The ELB stops sending traffic to the instance that failed its health check.

Answer: D

QUESTION 208
In AWS, which security aspects are the customer's responsibility? Choose 4 answers.

A. Security Group and ACL (Access Control List) settings
B. Decommissioning storage devices
C. Patch management on the EC2 instance's operating system
D. Life-cycle management of IAM credentials
E. Controlling physical access to compute resources
F. Encryption of EBS (Elastic Block Storage) volumes

Answer: ACDF
Explanation:
http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 209
You have a web application running on six Amazon EC2 instances, consuming about 45% of resources on each instance. You are using auto-scaling to make sure that six instances are running at all times. The number of requests this application processes is consistent and does not experience spikes. The application is critical to your business and you want high availability at all times. You want the load to be distributed evenly between all instances. You also want to use the same Amazon Machine Image (AMI) for all instances. Which of the following architectural choices should you make?

A. Deploy 6 EC2 instances in one availability zone and use Amazon Elastic Load Balancer.
B. Deploy 3 EC2 instances in one region and 3 in another region and use Amazon Elastic Load Balancer.
C. Deploy 3 EC2 instances in one availability zone and 3 in another availability zone and use Amazon Elastic Load Balancer.
D. Deploy 2 EC2 instances in three regions and use Amazon Elastic Load Balancer.

Answer: C
Explanation:
A load balancer accepts incoming traffic from clients and routes requests to its registered EC2 instances in one or more Availability Zones.
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/how-elb-works.html
Updated Security Whitepaper link:
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

QUESTION 210
You have decided to change the instance type for instances running in your application tier that is using Auto Scaling. In which area below would you change the instance type definition?

A. Auto Scaling policy
B. Auto Scaling group
C. Auto Scaling tags
D. Auto Scaling launch configuration

Answer: D

QUESTION 211
When an EC2 EBS-backed (EBS root) instance is stopped, what happens to the data on any ephemeral store volumes?

A. Data is automatically saved in an EBS volume.
B. Data is unavailable until the instance is restarted.
C. Data will be deleted and will no longer be accessible.
D. Data is automatically saved as an EBS snapshot.

Answer: C
Explanation:
An “EBS-backed” instance is an EC2 instance which uses an EBS volume as it’s root device.
An EBS volume behaves like a raw, unformatted, external block device that you can attach to a single instance and are not physically attached to the Instance host computer (more like a network attached storage). The volume persists independently from the running life of an instance. After an EBS volume is attached to an instance, you can use it like any other physical hard drive. You can also detach an EBS volume from one instance and attach it to another instance. EBS volumes can also be created as encrypted volumes using the Amazon EBS encryption feature.

QUESTION 212
Which of the following items are required to allow an application deployed on an EC2 instance to write data to a DynamoDB table? Assume that no security keys are allowed to be stored on the EC2 instance. Choose 2 answers.

A. Create an IAM Role that allows write access to the DynamoDB table.
B. Add an IAM Role to a running EC2 instance.
C. Create an IAM User that allows write access to the DynamoDB table.
D. Add an IAM User to a running EC2 instance.
E. Launch an EC2 Instance with the IAM Role included in the launch configuration.

Answer: AE
Explanation:
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TicTacToe.Phase3.html

QUESTION 213
When you put objects in Amazon S3, what is the indication that an object was successfully stored?

A. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.
B. Amazon S3 is engineered for 99.999999999% durability. Therefore there is no need to confirm that data was inserted.
C. A success code is inserted into the S3 object metadata.
D. Each S3 account has a special bucket named _s3_logs. Success codes are written to this bucket with a timestamp and checksum.

Answer: A
Explanation:
To ensure that data is not corrupted traversing the network, use the Content-MD5 form field. When you use this form field, Amazon S3 checks the object against the provided MD5 value. If they do not match, Amazon S3 returns an error. The status code returned to the client upon successful upload if success_action_redirect is not specified. Accepts the values 200, 201, or 204 (default).
http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html

QUESTION 214
What is one key difference between an Amazon EBS-backed and an instance-store backed instance?

A. Amazon EBS-backed instances can be stopped and restarted.
B. Instance-store backed instances can be stopped and restarted.
C. Auto scaling requires using Amazon EBS-backed instances.
D. Virtual Private Cloud requires EBS backed instances.

Answer: A
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html#storage-for-the-root-device

QUESTION 215
A company wants to implement their website in a virtual private cloud (VPC). The web tier will use an Auto Scaling group across multiple Availability Zones (AZs). The database will use Multi-AZ RDS MySQL and should not be publicly accessible. 'What is the minimum number of subnets that need to be configured in the VPC?

A. 1
B. 2
C. 3
D. 4

Answer: D
Explanation:
Would use VPC with private (DB) and public (WEB) subnets:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html
Multi AZ requirement forces me to multiply subnets by two.
Reasons:
For DB: Your VPC must have at least one subnet in at least two of the Availability Zones in the region where you want to deploy your DB instance. A subnet is a segment of a VPC's IP address range that you can specify and that lets you group instances based on your security and operational needs.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC.html
For Web: After creating a VPC, you can add one or more subnets in each Availability Zone. Each subnet must reside entirely within one Availability Zone and cannot span zones.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION 216
You have launched an Amazon Elastic Compute Cloud (EC2) instance into a public subnet with a primary private IP address assigned, an internet gateway is attached to the VPC, and the public route table is configured to send all Internet-based traffic to the Internet gateway. The instance security group is set to allow all outbound traffic but cannot access the internet. Why is the Internet unreachable from this instance?

A. The instance does not have a public IP address.
B. The internet gateway security group must allow all outbound traffic.
C. The instance security group must allow all inbound traffic.
D. The instance "Source/Destination check" property must be enabled.

Answer: A
Explanation:
Ensure that instances in your subnet have public IP addresses or Elastic IP addresses.
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html

QUESTION 217
You launch an Amazon EC2 instance without an assigned AVVS identity and Access Management (IAM) role. Later, you decide that the instance should be running with an IAM role. Which action must you take in order to have a running Amazon EC2 instance with an IAM role assigned to it?

A. Create an image of the instance, and register the image with an IAM role assigned and an Amazon EBS volume mapping.
B. Create a new IAM role with the same permissions as an existing IAM role, and assign it to the running instance.
C. Create an image of the instance, add a new IAM role with the same permissions as the desired IAM role, and deregister the image with the new role assigned.
D. Create an image of the instance, and use this image to launch a new instance with the desired IAM role assigned.

Answer: D
Explanation:
http://docs.aws.amazon.com/IAM/latest/UserGuide/roles-usingrole-ec2instance.html

QUESTION 218
How can the domain's zone apex, for example, "myzoneapexdomain.com", be pointed towards an Elastic Load Balancer?

A. By using an Amazon Route 53 Alias record
B. By using an AAAA record
C. By using an Amazon Route 53 CNAME record
D. By using an A record

Answer: A
Explanation:
You can create an alias resource record set at the zone apex. You cannot create a CNAME record at the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com.
http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

QUESTION 219
An instance is launched into a VPC subnet with the network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance's security group is configured to allow SSH from any IP address and deny all outbound traffic. What changes need to be made to allow SSH access to the instance?

A. The outbound security group needs to be modified to allow outbound traffic.
B. The outbound network ACL needs to be modified to allow outbound traffic.
C. Nothing, it can be accessed from any IP address using SSH.
D. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.

Answer: B
Explanation:
Need to open TCP Port 1024-65535 at Outbound Rules
“Allows outbound responses to the remote computer. Network ACLs are stateless, therefore this rule is required to allow response traffic for inbound requests.”
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

QUESTION 220
For which of the following use cases are Simple Workflow Service (SWF) and Amazon EC2 an appropriate solution? Choose 2 answers.

A. Using as an endpoint to collect thousands of data points per hour from a distributed fleet of sensors
B. Managing a multi-step and multi-decision checkout process of an e-commerce website
C. Orchestrating the execution of distributed and auditable business processes
D. Using as an SNS (Simple Notification Service) endpoint to trigger execution of video transcoding jobs
E. Using as a distributed session store for your web application

Answer: BC
Explanation:
https://aws.amazon.com/swf/faqs/

QUESTION 221
A customer wants to leverage Amazon Simple Storage Service (S3) and Amazon Glacier as part of their backup and archive infrastructure. The customer plans to use third-party software to support this integration. Which approach will limit the access of the third party software to only the Amazon S3 bucket named "company-backup"?

A. A custom bucket policy limited to the Amazon S3 API in thee Amazon Glacier archive "company-backup"
B. A custom bucket policy limited to the Amazon S3 API in "company-backup"
C. A custom IAM user policy limited to the Amazon S3 API for the Amazon Glacier archive "company-backup"
D. A custom IAM user policy limited to the Amazon S3 API in "company-backup"

Answer: D
Explanation:
http://docs.aws.amazon.com/AmazonS3/latest/dev/example-policies-s3.html

QUESTION 222
A client application requires operating system privileges on a relational database server. What is an appropriate configuration for a highly available database architecture?

A. A standalone Amazon EC2 instance
B. Amazon RDS in a Multi-AZ configuration
C. Amazon EC2 instances in a replication configuration utilizing a single Availability Zone
D. Amazon EC2 instances in a replication configuration utilizing two different Availability Zones

Answer: D
Explanation:
http://docs.aws.amazon.com/dms/latest/userguide/CHAP_Introduction.ReplicationInstance.html

QUESTION 223
What is a placement group?

A. A collection of Auto Scaling groups in the same region
B. A feature that enables EC2 instances to interact with each other via high bandwidth, low latency connections
C. A collection of authorized CloudFront edge locations for a distribution
D. A collection of Elastic Load Balancers in the same Region or Availability Zone

Answer: B
Explanation:
A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gigabits per second (Gbps) network. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION 224
A company has a workflow that sends video files from their on-premise system to AWS for transcoding. They use EC2 worker instances that pull transcoding jobs from SQS. Why is SQS an appropriate service for this scenario?

A. SQS guarantees the order of the messages.
B. SQS synchronously provides transcoding output.
C. SQS checks the health of the worker instances.
D. SQS helps to facilitate horizontal scaling of encoding tasks.

Answer: D
Explanation:
Imho the idea for SQS is to improve scalability.
Elastic Beanstalk is checking the health of EC2 instances, not sure if SQS does.

QUESTION 225
When creation of an EBS snapshot is initiated, but not completed, the EBS volume:

A. Can be used while the snapshot is in progress.
B. Cannot be detached or attached to an EC2 instance until the snapshot completes.
C. Can be used in read-only mode while the snapshot is in progress.
D. Cannot be used until the snapshot completes.

Answer: A
Explanation:
Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html

QUESTION 226
What are characteristics of Amazon S3? Choose 2 answers.

A. S3 allows you to store objects of virtually unlimited size.
B. S3 offers Provisioned IOPS.
C. S3 allows you to store unlimited amounts of data.
D. S3 should be used to host a relational database.
E. Objects are directly accessible via a URL.

Answer: CE
Explanation:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

QUESTION 227
Per the AWS Acceptable Use Policy, penetration testing of EC2 instances:

A. May be performed by AWS, and will be performed by AWS upon customer request.
B. May be performed by AWS, and is periodically performed by AWS.
C. Are expressly prohibited under all circumstances.
D. May be performed by the customer on their own instances with prior authorization from AWS.
E. May be performed by the customer on their own instances, only if performed from EC2 instances.

Answer: D
Explanation:
http://aws.amazon.com/security/penetration-testing/

QUESTION 228
You are working with a customer who has 10 TB of archival data that they want to migrate to Amazon Glacier. The customer has a 1-Mbps connection to the Internet. Which service or feature provides the fastest method of getting the data into Amazon Glacier?

A. Amazon Glacier multipart upload
B. AWS Storage Gateway
C. VM Import/Export
D. AWS Import/Export

Answer: A
Explanation:
You can only perform an Amazon Glacier import from devices of 4 TB in size or smaller.
https://docs.aws.amazon.com/es_es/AWSImportExport/latest/DG/createGlacierimportjobs.html

QUESTION 229

How can you secure data at rest on an EBS volume?

A. Attach the volume to an instance using EC2's SSL interface.
B. Write the data randomly instead of sequentially.
C. Encrypt the volume using the S3 server-side encryption service.
D. Create an IAM policy that restricts read and write access to the volume.
E. Use an encrypted file system on top of the EBS volume.

Answer: E
Explanation:
https://aws.amazon.com/blogs/aws/protect-your-data-with-new-ebs-encryption/

QUESTION 230
A customer needs to capture all client connection information from their load balancer every five minutes. The company wants to use this data for analyzing traffic patterns and troubleshooting their applications. Which of the following options meets the customer requirements?

A. Enable AWS CloudTrail for the load balancer.
B. Enable access logs on the load balancer.
C. Install the Amazon CloudWatch Logs agent on the load balancer.
D. Enable Amazon CloudWatch metrics on the load balancer.

Answer: B
Explanation:
Elastic Load Balancing access logs
The access logs for Elastic Load Balancing capture detailed information for all requests made to your load balancer and stores them as log files in the Amazon S3 bucket that you specify. Each log contains details such as the time a request was received, the client's IP address, latencies, request path, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot your back-end applications. For more information, see Monitor Your Load Balancer Using Elastic Load Balancing Access Logs.

QUESTION 231
If you want to launch Amazon Elastic Compute Cloud (EC2) instances and assign each instance a predetermined private IP address you should:

A. Launch the instance from a private Amazon Machine Image (AMI).
B. Assign a group of sequential Elastic IP address to the instances.
C. Launch the instances in the Amazon Virtual Private Cloud (VPC).
D. Launch the instances in a Placement Group.
E. Use standard EC2 instances since each instance gets a private Domain Name Service (DNS) already.

Answer: C
Explanation:
Each instance in a VPC has a default network interface (eth0) that is assigned the primary private IP address.

QUESTION 232
You need to configure an Amazon S3 bucket to serve static assets for your public-facing web application. Which methods ensure that all objects uploaded to the bucket are set to public read? Choose 2 answers.

A. Set permissions on the object to public read during upload.
B. Configure the bucket ACL to set all objects to public read.
C. Configure the bucket policy to set all objects to public read.
D. Use AWS Identity and Access Management roles to set the bucket to public read.
E. Amazon S3 objects default to public read, so no action is needed.

Answer: AC
Explanation:
https://aws.amazon.com/articles/5050
You can use ACLs to grant permissions to individual AWS accounts; however, it is strongly recommended that you do not grant public access to your bucket using an ACL. So the recommended approach is create bucket policy, but not ACL. Following link give you an example about how to make the bucket content public.

http://docs.aws.amazon.com/AmazonS3/latest/dev/HostingWebsiteOnS3Setup.html#step2-add-bucket-policy-make-content-public

QUESTION 233
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 3 answers.

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

QUESTION 234
Which procedure for backing up a relational database on EC2 that is using a set of RAIDed EBS volumes for storage minimizes the time during which the database cannot be written to and results in a consistent backup?

A. 1. Detach EBS volumes, 2. Start EBS snapshot of volumes, 3. Re-attach EBS volumes
B. 1. Stop the EC2 Instance. 2. Snapshot the EBS volumes
C. 1. Suspend disk I/O, 2. Create an image of the EC2 Instance, 3. Resume disk I/O
D. 1. Suspend disk I/O, 2. Start EBS snapshot of volumes, 3. Resume disk I/O
E. 1. Suspend disk I/O, 2. Start EBS snapshot of volumes, 3. Wait for snapshots to complete, 4. Resume disk I/O

Answer: B
Explanation:
https://aws.amazon.com/cn/premiumsupport/knowledge-center/snapshot-ebs-raid-array/
To create an “application-consistent” snapshot of your RAID array, stop applications from writing to the RAID array, and flush all caches to disk. Then ensure that the associated EC2 instance is no longer writing to the RAID array by taking steps such as freezing the file system, unmounting the RAID array, or *shutting down the associated EC2 instance*. After completing the steps to halt all I/O, take a snapshot of each EBS volume.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-detaching-volume.html
You can detach an Amazon EBS volume from an instance explicitly or by terminating the instance. However, if the instance is running, you must first unmount the volume from the instance.”

QUESTION 235
A company needs to deploy virtual desktops to its customers in a virtual private cloud, leveraging existing security controls. Which set of AWS services and features will meet the company's requirements?

A. Virtual Private Network connection. AWS Directory Services, and ClassicLink
B. Virtual Private Network connection. AWS Directory Services, and Amazon Workspaces
C. AWS Directory Service, Amazon Workspaces, and AWS Identity and Access Management
D. Amazon Elastic Compute Cloud, and AWS Identity and Access Management

Answer: B
Explanation:
To enable integration, you need to ensure that your domain is reachable via an Amazon Virtual Private Cloud VPC (this could mean that Active Directory domain controllers for your domain are running on Amazon EC2 instances, or that they are reachable via a VPN connection and are located in your on-premises network).

QUESTION 236
After creating a new IAM user which of the following must be done before they can successfully make API calls?

A. Add a password to the user.
B. Enable Multi-Factor Authentication for the user.
C. Assign a Password Policy to the user.
D. Create a set of Access Keys for the user.

Answer: D
Explanation:
http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_SettingUpUser.html

QUESTION 237
Which of the following are valid statements about Amazon S3? Choose 2 answers.

A. S3 provides read-after-write consistency for any type of PUT or DELETE.
B. Consistency is not guaranteed for any type of PUT or DELETE.
C. A successful response to a PUT request only occurs when a complete object is saved.
D. Partially saved objects are immediately readable with a GET after an overwrite PUT.
E. S3 provides eventual consistency for overwrite PUTS and DELETES.

Answer: CE
Explanation:
http://api-portal.anypoint.mulesoft.com/amazon/api/amazon-s3-api/docs/concepts#DataConsistencyModel

QUESTION 238
You are configuring your company's application to use Auto Scaling and need to move user state information. Which of the following AWS services provides a shared data store with durability and low latency?

A. AWS ElastiCache Memcached
B. Amazon Simple Storage Service
C. Amazon EC2 instance storage
D. Amazon DynamoDB

Answer: D
Explanation:
https://media.amazonwebservices.com/AWS_Storage_Options.pdf
To speed access to relevant data, many developers pair Amazon S3 with a database, such as Amazon DynamoDB or Amazon RDS. Amazon S3 stores the actual information, and the database serves as the repository for associated metadata (e.g., object name, size, keywords, and so on). Metadata in the database can easily be indexed and queried, making it very efficient to locate an object's reference via a database query. This result can then be used to pinpoint and then retrieve the object itself from Amazon S3.

QUESTION 239
Which features can be used to restrict access to data in S3? Choose 2 answers.

A. Set an S3 ACL on the bucket or the object.
B. Create a CloudFront distribution for the bucket.
C. Set an S3 bucket policy.
D. Enable IAM Identity Federation.
E. Use S3 Virtual Hosting.

Answer: AC
Explanation:
Amazon S3 is secure by default. Only the bucket and object owners originally have access to Amazon S3 resources they create. Amazon S3 supports user authentication to control access to data. You can use access control mechanisms such as bucket policies and Access Control Lists (ACLs) to selectively grant permissions to users and groups of users. You can securely upload/download your data to Amazon S3 via SSL endpoints using the HTTPS protocol. If you need extra security you can use the Server Side Encryption (SSE) option or the Server Side Encryption with Customer-Provide Keys (SSE-C) option to encrypt data stored-at-rest. Amazon S3 provides the encryption technology for both SSE and SSE-C. Alternatively you can use your own encryption libraries to encrypt data before storing it in Amazon S3.
https://aws.amazon.com/s3/faqs/

QUESTION 240
Which of the following are characteristics of a reserved instance? Choose 3 answers.

A. It can be migrated across Availability Zones
B. It is specific to an Amazon Machine Image (AMI)
C. It can be applied to instances launched by Auto Scaling
D. It is specific to an instance Type

E. It can be used to lower Total Cost of Ownership (TCO) of a system

Answer: ACE
Explanation:
You can use Auto Scaling or other AWS services to launch the On-Demand instances that use your Reserved Instance benefits. For information about launching On-Demand instances, see Launch Your Instance. For information about launching instances using Auto Scaling, see the Auto Scaling User Guide.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts-on-demand-reserved-instances.html
https://forums.aws.amazon.com/thread.jspa?threadID=56501

QUESTION 241
Which Amazon Elastic Compute Cloud feature can you query from within the instance to access instance properties?

A. Instance user data
B. Resource tags
C. Instance metadata
D. Amazon Machine Image

Answer: C
Explanation:
Although you can only access instance metadata and user data from within the instance itself, the data is not protected by cryptographic methods.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html#instancedata-data-retrieval

QUESTION 242
Which of the following requires a custom CloudWatch metric to monitor?

A. Memory Utilization of an EC2 instance
B. CPU Utilization of an EC2 instance
C. Disk usage activity of an EC2 instance
D. Data transfer of an EC2 instance

Answer: A
Explanation:
CloudWatch relies on the information provided by this hypervisor, which can only see the most hardware-sided part of the instance's status, including CPU usage (but not load), total memory size (but not memory usage), number of I/O operations on the hard disks (but not it's partition layout and space usage) and network traffic (but not the processes generating it).

QUESTION 243
You are tasked with setting up a Linux bastion host for access to Amazon EC2 instances running in your VPC. Only clients connecting from the corporate external public IP address 72.34.51.100 should have SSH access to the host. Which option will meet the customer requirement?

A. Security Group Inbound Rule: Protocol -TCP. Port Range -22, Source 72.34.51.100/32
B. Security Group Inbound Rule: Protocol -UDP, Port Range -22, Source 72.34.51.100/32
C. Network ACL Inbound Rule: Protocol -UDP, Port Range -22, Source 72.34.51.100/32
D. Network ACL Inbound Rule: Protocol -TCP, Port Range-22, Source 72.34.51.100/0

Answer: A

QUESTION 244
A customer needs corporate IT governance and cost oversight of all AWS resources consumed by its divisions. The divisions want to maintain administrative control of the discrete AWS resources they consume and keep those resources separate from the resources of other divisions. Which of the following options, when used together will support the autonomy/control of divisions while enabling corporate IT to maintain governance and cost oversight? Choose 2 answers.

A. Use AWS Consolidated Billing and disable AWS root account access for the child accounts.
B. Enable IAM cross-account access for all corporate IT administrators in each child account.
C. Create separate VPCs for each division within the corporate IT AWS account.
D. Use AWS Consolidated Billing to link the divisions' accounts to a parent corporate account.
E. Write all child AWS CloudTrail and Amazon CloudWatch logs to each child account's Amazon S3 'Log' bucket.

Answer: BD
Explanation:
http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html
http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html

QUESTION 245
You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site. At some point you find out that other sites have been linking to the photos on your site, causing loss to your business. What is an effective method to mitigate this?

A. Remove public read access and use signed URLs with expiry dates.
B. Use CloudFront distributions for static content.
C. Block the IPs of the offending websites in Security Groups.
D. Store photos on an EBS volume of the web server.

Answer: A
Explanation:
A signed URL includes additional information, for example, an expiration date and time, that gives you more control over access to your content.

QUESTION 246
You are working with a customer who is using Chef configuration management in their data center. Which service is designed to let the customer leverage existing Chef recipes in AWS?

A. Amazon Simple Workflow Service
B. AWS Elastic Beanstalk
C. AWS CloudFormation
D. AWS OpsWorks

Answer: D
Explanation:
http://aws.amazon.com/opsworks/

QUESTION 247
An Auto-Scaling group spans 3 AZs and currently has 4 running EC2 instances. When Auto Scaling needs to terminate an EC2 instance by default, AutoScaling will: ____. Choose 2 answers.

A. Allow at least five minutes for Windows/Linux shutdown scripts to complete, before terminating the instance.
B. Terminate the instance with the least active network connections. If multiple instances meet this criterion, one will be randomly selected.
C. Send an SNS notification, if configured to do so.
D. Terminate an instance in the AZ which currently has 2 running EC2 instances.
E. Randomly select one of the 3 AZs, and then terminate an instance in that AZ.

Answer: CD
Explanation:
Auto Scaling determines whether there are instances in multiple Availability Zones. If so, it selects the Availability Zone with the most instances and at least one instance that is not protected from scale in.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AutoScalingBehavior.InstanceTermination.html

QUESTION 248
When an EC2 instance that is backed by an S3-based AMI is terminated, what happens to the data on the root volume?

A. Data is automatically saved as an EBS snapshot.
B. Data is automatically saved as an EBS volume.
C. Data is unavailable until the instance is restarted.
D. Data is automatically deleted.

Answer: D
Explanation:

Using the legacy S3 based AMIs, either of the above terminates the instance and you lose all local and ephemeral storage (boot disk and /mnt) forever. Hope you remembered to save the important stuff elsewhere.

QUESTION 249
In order to optimize performance for a compute cluster that requires low inter-node latency, which of the following feature should you use?

A. Multiple Availability Zones
B. AWS Direct Connect
C. EC2 Dedicated Instances
D. Placement Groups
E. VPC private subnets

Answer: D
Explanation:
A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gigabits per second (Gbps) network.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION 250
You have an environment that consists of a public subnet using Amazon VPC and 3 instances that are running in this subnet. These three instances can successfully communicate with other hosts on the Internet. You launch a fourth instance in the same subnet, using the same AMI and security group configuration you used for the others, but find that this instance cannot be accessed from the internet. What should you do to enable Internet access?

A. Deploy a NAT instance into the public subnet.
B. Assign an Elastic IP address to the fourth instance.
C. Configure a publically routable IP Address in the host OS of the fourth instance.
D. Modify the routing table for the public subnet.

Answer: B
Explanation:
You launched your instance into a public subnet - a subnet that has a route to an Internet gateway. However, the instance in your subnet also needs a public IP address to be able to communicate with the Internet. By default, an instance in a nondefault VPC is not assigned a public IP address. In this step, you'll allocate an Elastic IP address to your account, and then associate it with your instance.