Amazon-Web-Services

Exam Questions SAA-C01

AWS Certified Solutions Architect - Associate

NEW QUESTION 1
Your customer wishes to deploy an enterprise application to AWS which will consist of several web servers, several application servers and a small (50GB) Oracle database information is stored, both in the database and the file systems of the various servers. The backup system must support database recovery whole server and whole disk restores, and individual file restores with a recovery time of no more than two hours. They have chosen to use RDS Oracle as the database.
Which backup architecture will meet these requirements?

A. Backup RDS using automated daily DB backups Backup the EC2 instances using AMIs and supplement with file-level backup to S3 using traditional enterprise backup software to provide file level restore
B. Backup RDS using a Multi-AZ Deployment Backup the EC2 instances using Amis, and supplement by copying file system data to S3 to provide file level restore.
C. Backup RDS using automated daily DB backups Backup the EC2 instances using EBS snapshots and supplement with file-level backups to Amazon Glacier using traditional enterprise backup software to provide file level restore
D. Backup RDS database to S3 using Oracle RMAN Backup the EC2 instances using Amis, and supplement with EBS snapshots for individual volume restore.

Answer: A

Explanation:
You need to use enterprise backup software to provide file level restore. See
https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf Page 18:
If your existing backup software does not natively support the AWS cloud, you can use AWS storage gateway products. AWS Storage Gateway is a virtual appliance that provides seamless and secure integration between your data center and the AWS storage infrastructure.

NEW QUESTION 2
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 EMR.
C. 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.
D. Utilize EMR to collect the inbound sensor data, analyze the data from EUR with Amazon Kinesis and save me results to DynamoDB.

Answer: B

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

NEW QUESTION 3
Amazon EC2 provides virtual computing environments known as _____ .

A. instances
B. volumes
C. microsystems
D. servers

Answer: A

Explanation:
Amazon EC2 provides virtual computing environments known as instances. When you launch an instance, the instance type that you specify determines the hardware of the host computer used for your instance. Each instance type offers different compute, memory, and storage capabilities and are grouped in instance families based on these capabilities. Select an instance type based on the requirements of the application or software that you plan to run on your instance.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

NEW QUESTION 4
Your application is using an ELB in front of an Auto Scaling group of web/application servers deployed across two AZs and a Multi-AZ RDS Instance for data persistence.
The database CPU is often above 80% usage and 90% of I/O operations on the database are reads. To improve performance you recently added a single-node Memcached ElastiCache Cluster to cache frequent DB query results. In the next weeks the overall workload is expected to grow by 30%.
Do you need to change anything in the architecture to maintain the high availability or the application with the anticipated additional load? Why?

A. Yes, you should deploy two Memcached ElastiCache Clusters in different AZs because the RDS instance will not be able to handle the load if the cache node fails.
B. No, if the cache node fails you can always get the same data from the DB withouthaving any availability impact.
C. No, if the cache node fails the automated ElastiCache node recovery feature will prevent any availability impact.
D. Yes, you should deploy the Memcached ElastiCache Cluster with two nodes in the same AZ as the RDS DB master instance to handle the load if one cache node fails.

Answer: A

Explanation:
A single-node Memcached ElastiCache cluster failure is nothing but a total failure. (Even though AWS will automatically recover the failed node, there are no other nodes in the cluster) http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/BestPractices.html Mitigating Node Failures

To mitigate the impact of a node failure, spread your cached data over more nodes. Because Memcached does not support replication, a node failure will always result in some data loss from your cluster.
When you create your Memcached cluster you can create it with 1 to 20 nodes, or more by special request. Partitioning your data across a greater number of nodes means you'll lose less data if a node fails. For example, if you partition your data across 10 nodes, any single node stores approximately 10% of your cached data. In this case, a node failure loses approximately 10% of your cache which needs to be replaced when a replacement node is created and provisioned.
Mitigating Availability Zone Failures
To mitigate the impact of an availability zone failure, locate your nodes in as many availability zones as possible. In the unlikely event of an AZ failure, you will lose only the data cached in that AZ, not the data cached in the other AZs.

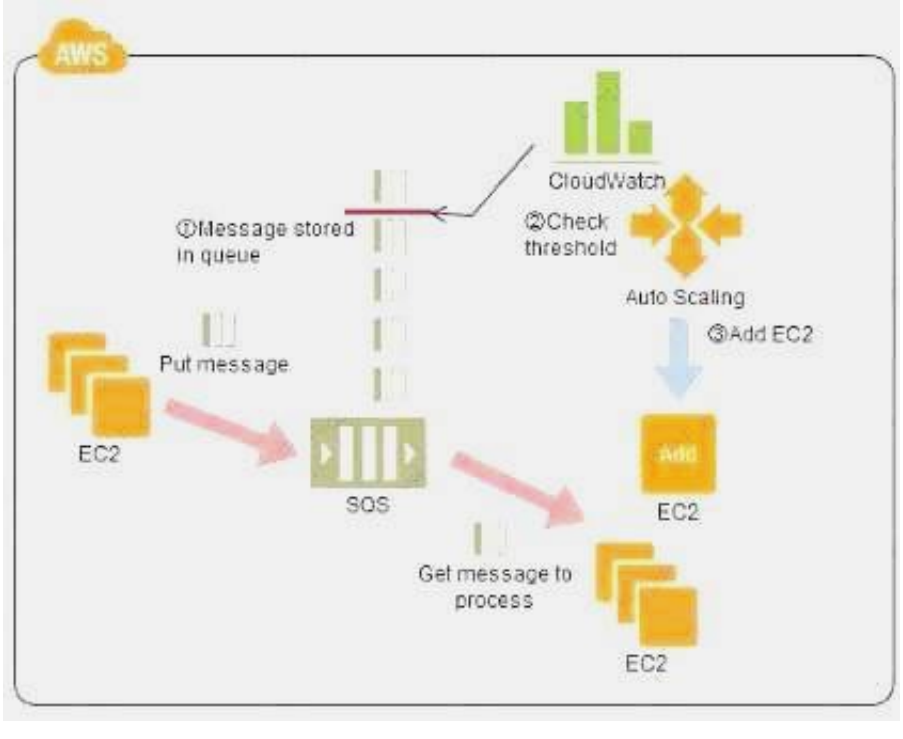
NEW QUESTION 5
You are responsible for a legacy web application whose server environment is approaching end of life You would like to migrate this application to AWS as quickly as possible, since the application environment currently has the following limitations:
The VM's single 10GB VMDK is almost full
Me virtual network interface still uses the 10Mbps driver, which leaves your 100Mbps WAN connection completely underutilized
It is currently running on a highly customized. Windows VM within a VMware environment: You do not have me installation media
This is a mission critical application with an RTO (Recovery Time Objective) of 8 hours. RPO (Recovery Point Objective) of 1 hour. How could you best migrate this application to AWS while meeting your business continuity requirements?

A. Use the EC2 VM Import Connector for vCenter to import the VM into EC2.
B. Use Import/Export to import the VM as an ESS snapshot and attach to EC2.
C. Use S3 to create a backup of the VM and restore the data into EC2.
D. Use me ec2-bundle-instance API to Import an Image of the VM into EC2

Answer: A

Explanation:
https://aws.amazon.com/developertools/2759763385083070

NEW QUESTION 6
Refer to the architecture diagram above of a batch processing solution using Simple Queue Service (SQS) to set up a message queue between EC2 instances which are used as batch processors Cloud Watch monitors the number of Job requests (queued messages) and an Auto Scaling group adds or deletes batch servers automatically based on parameters set in Cloud Watch alarms. You can use this architecture to implement which of the following features in a cost effective and efficient manner?



A. Reduce the overall lime for executing jobs through parallel processing by allowing a busy EC2 instance that receives a message to pass it to the next instance in a daisy-chain setup.
B. Implement fault tolerance against EC2 instance failure since messages would remain in SQS and worn can continue with recovery of EC2 instances implement fault tolerance against SQS failure by backing up messages to S3.
C. Implement message passing between EC2 instances within a batch by exchanging messages through SQS.
D. Coordinate number of EC2 instances with number of job requests automatically thus Improving cost effectiveness.
E. Handle high priority jobs before lower priority jobs by assigning a priority metadata field to SQS messages.

Answer: D

NEW QUESTION 7
Your company currently has a 2-tier web application running in an on-premises data center. You have experienced several infrastructure failures in the past two months resulting in significant financial losses. Your CIO is strongly agreeing to move the application to AWS. While working on achieving buy-in from the other company executives, he asks you to develop a disaster recovery plan to help improve Business continuity in the short term. He specifies a target Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour or less. He also asks you to implement the solution within 2 weeks. Your database is 200GB in size and you have a 20Mbps Internet connection. How would you do this while minimizing costs?

A. Create an EBS backed private AMI which includes a fresh install of your applicatio
B. Develop a CloudFormation template which includes your AMI and the required EC2, AutoScaling, and ELB resources to support deploying the application across Multiple- Availability-Zone
C. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection.
D. Deploy your application on EC2 instances within an Auto Scaling group across multiple availability zone
E. Asynchronously replicate transactions from your on-premises database to a database instancein AWS across a secure VPN connection.
F. Create an EBS backed private AMI which includes a fresh install of your applicatio

G. Setup a script in your data center to backup the local database every 1 hour and to encrypt and copy the resultingfile to an S3 bucket using multi-part upload.
H. Install your application on a compute-optimized EC2 instance capable of supporting the application's average loa
I. Synchronously replicate transactions from your on-premises database to a database instance in AWS across a secure Direct Connect connection.

Answer: A

Explanation:
Overview of Creating Amazon EBS-Backed AMIs
First, launch an instance from an AMI that's similar to the AMI that you'd like to create. You can
connect to your instance and customize it. When the instance is configured correctly, ensure data integrity by stopping the instance before you create an AMI, then create the image. When you create an Amazon EBS-backed AMI, we automatically register it for you.
Amazon EC2 powers down the instance before creating the AMI to ensure that everything on the instance is stopped and in a consistent state during the creation process. If you're confident that your instance is in a consistent state appropriate for AMI creation, you can tell Amazon EC2 not to power down and reboot the instance. Some file systems, such as XFS, can freeze and unfreeze activity, making it safe to create the image without rebooting the instance.
During the AMI-creation process, Amazon EC2 creates snapshots of your instance's root volume and any other EBS volumes attached to your instance. If any volumes attached to the instance are encrypted, the new AMI only launches successfully on instances that support Amazon EBS encryption. For more information, see Amazon EBS Encryption.
Depending on the size of the volumes, it can take several minutes for the AMI-creation process to complete (sometimes up to 24 hours). You may find it more efficient to create snapshots of your volumes prior to creating your AMI. This way, only small, incremental snapshots need to be created when the AMI is created, and the process completes more quickly (the total time for snapshot creation remains the same). For more information, see Creating an Amazon EBS Snapshot.
After the process completes, you have a new AMI and snapshot created from the root volume of the instance. When you launch an instance using the new AMI, we create a new EBS volume for its root volume using the snapshot. Both the AMI and the snapshot incur charges to your account until you delete them. For more information, see Deregistering Your AMI.
If you add instance-store volumes or EBS volumes to your instance in addition to the root device volume, the block device mapping for the new AMI contains information for these volumes, and the block device mappings for instances that you launch from the new AMI automatically contain information for these volumes. The instance-store volumes specified in the block device mapping for the new instance are new and don't contain any data from the instance store volumes of the instance you used to create the AMI. The data on EBS volumes persists. For more information, see Block Device Mapping.

NEW QUESTION 8
An ERP application is deployed across multiple AZs in a single region. In the event of failure, the Recovery Time Objective (RTO) must be less than 3 hours, and the Recovery Point Objective (RPO) must be 15 minutes the customer realizes that data corruption occurred roughly 1.5 hours ago.
What DR strategy could be used to achieve this RTO and RPO in the event of this kind of failure?

A. Take hourly DB backups to S3, with transaction logs stored in S3 every 5 minutes.
B. Use synchronous database master-slave replication between two availability zones.
C. Take hourly DB backups to EC2 Instance store volumes with transaction logs stored In S3 every 5 minutes.
D. Take 15-minute DB backups stored In Glacier with transaction logs stored in S3 every 5 minute

Answer: A

NEW QUESTION 9
Your company hosts a social media site supporting users in multiple countries. You have been asked to provide a highly available design tor the application that leverages multiple regions tor the most recently accessed content and latency sensitive portions of the wet) site The most latency sensitive component of the application involves reading user preferences to support web site personalization and ad selection.
In addition to running your application in multiple regions, which option will support this
application’s requirements?

A. Serve user content from S3. CloudFront and use Route53 latency-based routing between ELBs in each region Retrieve user preferences from a local DynamoDB table in each region and leverage SQS to capture changes to user preferences with SOS workers for propagating updates to each table.
B. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3. CloudFront with dynamic content and an ELB in each region Retrieve user preferences from an ElasticCache cluster in each region and leverage SNS notifications to propagate user preference changes to a worker node in each region.
C. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3 CloudFront and Route53 latency-based routing Between ELBs In each region Retrieve user preferences from a DynamoDB table and leverage SQS to capture changes to user preferences with SOS workers for propagating DynamoDB updates.
D. Serve user content from S3. CloudFront with dynamic content, and an ELB in each region Retrieve user preferences from an ElastiCache cluster in each region and leverage Simple Workflow (SWF) to manage the propagation of user preferences from a centralized OB to each ElastiCache cluster.

Answer: A

Explanation:
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_mediasharing_09.pdf
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_adserving_06.pdf

NEW QUESTION 10
Your system recently experienced down time during the troubleshooting process. You found that a new administrator mistakenly terminated several production EC2 instances.
Which of the following strategies will help prevent a similar situation in the future? The administrator still must be able to:
- launch, start stop, and terminate development resources.
- launch and start production instances.

A. Create an IAM user, which is not allowed to terminate instances by leveraging production EC2 termination protection.
B. Leverage resource based tagging along with an IAM user, which can prevent specific users from terminating production EC2 resources.
C. Leverage EC2 termination protection and multi-factor authentication, which together require users to authenticate before terminating EC2 instances
D. Create an IAM user and apply an IAM role which prevents users from terminating production EC2 instances.

Answer: B

Explanation:
Working with volumes

When an API action requires a caller to specify multiple resources, you must create a policy statement that allows users to access all required resources. If you need to use a Condition element with one or more of these resources, you must create multiple statements as shown in this example. The following policy allows users to attach volumes with the tag "volume_user=iam-user-name" to
instances with the tag "department=dev", and to detach those volumes from those instances. If you attach this policy to an IAM group, the aws:username policy variable gives each IAM user in the group permission to attach or detach volumes from the instances with a tag named volume_user that has his or her IAM user name as a value.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AttachVolume",
      "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/department": "dev"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:AttachVolume",
      "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/volume_user": "${aws:username}"
      }
    }
  }
 ]
}
```

Launching instances (RunInstances)
The RunInstances API action launches one or more instances. RunInstances requires an AMI and creates an instance; and users can specify a key pair and security group in the request. Launching into EC2-VPC requires a subnet, and creates a network interface. Launching from an Amazon EBS-backed AMI creates a volume. Therefore, the user must have permission to use these Amazon EC2
resources. The caller can also configure the instance using optional parameters to RunInstances, such as the instance type and a subnet. You can create a policy statement that requires users to specify an optional parameter, or restricts users to particular values for a parameter. The examples in this section demonstrate some of the many possible ways that you can control the configuration of an instance that a user can launch.
Note that by default, users don't have permission to describe, start, stop, or terminate the resulting instances. One way to grant the users permission to manage the resulting instances is to create a specific tag for each instance, and then create a statement that enables them to manage instances with that tag. For more information, see 2: Working with instances.
/a. AMI
The following policy allows users to launch instances using only the AMIs that have the specified tag, "department=dev", associated with them. The users can't launch instances using other AMIs because the Condition element of the first statement requires that users specify an AMI that has this tag. The users also can't launch into a subnet, as the policy does not grant permissions for the subnet and network interface resources. They can, however, launch into EC2-Classic. The second statement uses a wildcard to enable users to create instance resources, and requires users to specify the key pair project_keypair and the security group sg-1a2b3c4d. Users are still able to launch instances without a key pair.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/department": "dev"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/project_keypair",
      "arn:aws:ec2:region:account:security-group/sg-1a2b3c4d"
    ]
  }
]
}
```

Alternatively, the following policy allows users to launch instances using only the specified AMIs, ami-9e1670f7 and ami-45cf5c3c. The users can't launch an instance using other AMIs (unless another statement grants the users permission to do so), and the users can't launch an instance into a subnet.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-9e1670f7",
      "arn:aws:ec2:region::image/ami-45cf5c3c",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
    ]
  }
]
}
```

Alternatively, the following policy allows users to launch instances from all AMIs owned by Amazon. The Condition element of the first statement tests whether ec2:Owner is amazon. The users can't launch an instance using other AMIs (unless another statement grants the users permission to do so). The users are able to launch an instance into a subnet.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:Owner": "amazon"
        }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

/b. Instance type

The following policy allows users to launch instances using only the t2.micro or t2.small instance type, which you might do to control costs. The users can't launch larger instances because the Condition element of the first statement tests whether ec2:InstanceType is either t2.micro or t2.small.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:InstanceType": ["t2.micro", "t2.small"]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

Alternatively, you can create a policy that denies users permission to launch any instances except t2.micro and t2.small instance types.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
      "StringNotEquals": {
        "ec2:InstanceType": ["t2.micro", "t2.small"]
        }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

/c. Subnet

The following policy allows users to launch instances using only the specified subnet, subnet- 12345678. The group can't launch instances into any another subnet (unless another statement grants the users permission to do so). Users are still able to launch instances into EC2-Classic.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:subnet/subnet-12345678",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
    ]
   }
  ]
}
```

Alternatively, you could create a policy that denies users permission to launch an instance into any other subnet. The statement does this by denying permission to create a network interface, except where subnet subnet-12345678 is specified. This denial overrides any other policies that are created to allow launching instances into other subnets. Users are still able to launch instances into EC2- Classic.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:network-interface/*"
    ],
    "Condition": {
      "ArnNotEquals": {
        "ec2:Subnet": "arn:aws:ec2:region:account:subnet/subnet-12345678
        }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

https://aws.amazon.com/blogs/security/resource-level-permissions-for-ec2-controllingmanagement- access-on-specific-instances/
August 2016 Update One way to work around this is to use a combination of an Amazon CloudWatch Events rule and AWS Lambda to tag newly created instances.

NEW QUESTION 10
Your company previously configured a heavily used, dynamically routed VPN connection between your on-premises data center and AWS. You recently provisioned a DirectConnect connection and would like to start using the new connection. After configuring DirectConnect settings in the AWS Console, which of the following options win provide the most seamless transition for your users?

A. Delete your existing VPN connection to avoid routing loops configure your DirectConnect router with the appropriate settings and verity network traffic is leveraging DirectConnect.
B. Configure your DirectConnect router with a higher 8GP priority man your VPN router, verify network traffic is leveraging Directconnect and then delete your existing VPN connection.
C. Update your VPC route tables to point to the DirectConnect connection configure your DirectConnect router with the appropriate settings verify network traffic is leveraging DirectConnect and then delete the VPN connection.
D. Configure your DirectConnect router, update your VPC route tables to point to the DirectConnect connection, configure your VPN connection with a higher BGP point
E. And verify network traffic is leveraging the DirectConnect connection.

Answer: C

Explanation:
Q. Can I use AWS Direct Connect and a VPN Connection to the same VPC simultaneously?
Yes. However, only in fail-over scenarios. The Direct Connect path will always be preferred, when established, regardless of AS path prepending.
https://aws.amazon.com/directconnect/faqs/

NEW QUESTION 11
A web company is looking to implement an external payment service into their highly available application deployed in a VPC. Their application EC2 instances are behind a public lacing ELB Auto scaling is used to add additional instances as traffic increases under normal load the application runs 2 instances in the Auto Scaling group but at peak it can scale 3x in size. The application instances need to communicate with the payment service over the Internet which requires whitelisting of all public IP addresses used to communicate with it. A maximum of 4 whitelisting IP addresses is allowed at a time and can be added through an API.
How should they architect their solution?

A. Route payment requests through two NAT instances setup for High Availability and whitelist the Elastic IP addresses attached to the MAT instances.
B. Whitelist the VPC Internet Gateway Public IP and route payment requests through the Internet Gateway.
C. Whitelist the ELB IP addresses and route payment requests from the Application servers through the ELB.
D. Automatically assign public IP addresses to the application instances in the Auto Scaling group andrun a script on boot that adds each instances public IP address to the payment validation whitelist API.

Answer: A

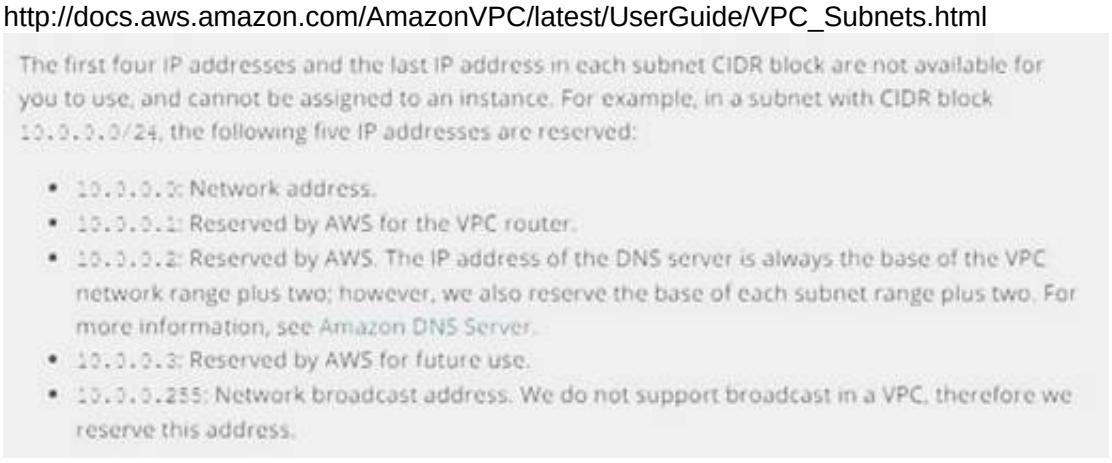
Explanation:
B is incorrect as you do not have insight into the public ip associated with a VPC Internet Gateways. C is incorrect as ELB receives a public DNS name.
D would exceed the maximum of 4 whitelisting IP addresses.

NEW QUESTION 15
You have deployed a three-tier web application in a VPC with a CIOR block of 10 0 0 0/28. You initially deploy two web servers, two application servers, two database servers and one NAT instance tor a
total of seven EC2 instances. The web. Application and database servers are deployed across two availability zones (AZs). You also deploy an ELB in front of the two web servers, and use Route53 for DNS Web (raffile gradually increases in the first few days following the deployment, so you attempt to double the number of instances in each tier of the application to handle the new load unfortunately some of these new instances fail to launch.
Which of the following could De the root caused? (Choose two.)

A. AWS reserves the first and the last private IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances
B. The Internet Gateway (IGW) of your VPC has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
C. The ELB has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
D. AWS reserves one IP address in each subnet's CIDR block for Route53 so you do not have enough addresses left to launch all of the new EC2 instances
E. AWS reserves the first four and the last IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances

Answer: CE

Explanation:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html


The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For more information, see Amazon DNS Server.
- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

NEW QUESTION 19
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 subnet
C. Configure a DNS A record that points to the NAT instance public IP address.
D. Configure a CloudFront distribution and configure the origin to point to the private IP addresses ofyour Web server
E. Configure a Route53 CNAME record to your CloudFront distribution.
F. Place all your web servers behind EL8. Configure a Route53 CNMIE to point to the ELB DNS name.
G. Assign EIPs to all web server
H. Configure a Route53 record set with all EIPs with health checks and DNS failover.
I. Configure ELB with an EI
J. Place all your Web servers behind EL
K. Configure a Route53 A record that points to the EIP.

Answer: CD

NEW QUESTION 21
A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC) and is connected to the corporate data center via an iPsec VPN. The application must authenticate against the on-premises LDAP server. After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user.
Which two approaches can satisfy these objectives? (Choose two.)

A. Develop an identity broker that authenticates against IAM security Token service to assume a IAM role in order to get temporary AWS security credentials The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.
B. The application authenticates against LDAP and retrieves the name of an IAM role associated withthe use
C. The application then calls the IAM Security Token Service to assume that IAM rol
D. The application can use the temporary credentials to access the appropriate S3 bucket.
E. Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credential
F. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.
G. The application authenticates against LDAP the application, then calls the AWS identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials, the application can use the IAM temporary credentials to access the appropriate S3 bucket.
H. The application authenticates against IAM Security Token Service using the LDAP credentials, the application uses those temporary AWS security credentials to access the appropriate S3 bucket.

Answer: BC

Explanation:
Imagine that in your organization, you want to provide a way for users to copy data from their computers to a backup folder. You build an application that users can run on their computers. On the back end, the application reads and writes objects in an S3 bucket. Users don’t have direct access to AWS. Instead, the application communicates with an identity provider (IdP) to authenticate the user. The IdP gets the user information from your organization’s identity store (such as an LDAP directory) and then generates a SAML assertion that includes authentication and authorization information about that user. The application then uses that assertion to make a call to the AssumeRoleWithSAML API to get temporary security credentials. The app can then use those credentials to access a folder in the

S3 bucket that's specific to the user. http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

NEW QUESTION 26
You are designing a multi-platform web application for AWS. The application will run on EC2 instances and will be accessed from PCs. tablets and smart phones Supported accessing platforms are Windows. MACOS. IOS and Android Separate sticky session and SSL certificate setups are required for different platform types which of the following describes the most cost effective and performance efficient architecture setup?

A. Setup a hybrid architecture to handle session state and SSL certificates on-prem and separate EC2 Instance groups running web applications for different platform types running in a VPC
B. Set up one ELB for all platforms to distribute load among multiple instance under it Each EC2 instance implements ail functionality for a particular platform.
C. Set up two ELBs The first ELB handles SSL certificates for all platforms and the second ELB handles session stickiness for all platforms for each ELB run separate EC2 instance groups to handle the web application for each platform.
D. Assign multiple ELBS to an EC2 instance or group of EC2 instances running the common components of the web application, one ELB for each platform type Session stickiness and SSL termination are done at the ELBs.

Answer: D

Explanation:
One ELB cannot handle different SSL certificates but since we are using sticky sessions it must be handled at the ELB level. SSL could be handled on the EC2 instances only with TCP configured ELB,
ELB supports sticky sessions only in HTTP/HTTPS configurations.
The way the Elastic Load Balancer does session stickiness is on a HTTP/HTTPS listener is by utilizing an HTTP cookie. If SSL traffic is not terminated on the Elastic Load Balancer and is
terminated on the back-end instance, the Elastic Load Balancer has no visibility into the HTTP headers and therefore cannot set or read any of the HTTP headers being passed back and forth. http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-sticky-sessions.html

NEW QUESTION 27
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 hostin
B. Migrate your DNS to Route53 using zone file import, and leverage Route53 DNS failover to failover to the S3 hosted website.
C. 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 traffi
D. Leverage Elastic Load Balancing to balance traffic between on-premises web servers and those hosted In AWS.
E. Offload traffic from on-premises environment: Setup a CIoudFront distribution, and configure CloudFront to cache objects from a custom origi
F. Choose to customize your object cache behavior, and select a TTL that objects should exist in cache.
G. Migrate to AWS: Use VM Import/Export to quickly convert an on-premises web server to an AM
H. Create an Auto Scaling group, which uses the imported AMI to scale the web tier based on incoming traffi
I. 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.

NEW QUESTION 28
Your department creates regular analytics reports from your company's log files. All log data is collected in Amazon S3 and processed by daily Amazon Elastic MapReduce (EMR) jobs that generate daily PDF reports and aggregated tables in CSV format for an Amazon Redshift data warehouse. Your CFO requests that you optimize the cost structure for this system.
Which of the following alternatives will lower costs without compromising average performance of the system or data integrity for the raw data?

A. Use reduced redundancy storage (RRS) for all data In S3. Use a combination of Spot Instances and Reserved Instances for Amazon EMR job
B. Use Reserved Instances for Amazon Redshift.
C. Use reduced redundancy storage (RRS) for PDF and .csv data in S3. Add Spot Instances to EMR job
D. Use Spot Instances for Amazon Redshift.
E. Use reduced redundancy storage (RRS) for PDF and .csv data In Amazon S3. Add Spot Instances to Amazon EMR job
F. Use Reserved Instances for Amazon Redshift.
G. Use reduced redundancy storage (RRS) for all data in Amazon S3. Add Spot Instances to Amazon EMR job
H. Use Reserved Instances for Amazon Redshift.

Answer: D

Explanation:
Reserved Instances (a.k.a. Reserved Nodes) are appropriate for steady-state production workloads, and offer significant discounts over On-Demand pricing. https://aws.amazon.com/redshift
Q: What are some EMR best practices?
If you are running EMR in production you should specify an AMI version, Hive version, Pig version, etc. to make sure the version does not change unexpectedly (e.g. when EMR later adds support for a newer version). If your cluster is mission critical, only use Spot instances for task nodes because if the Spot price increases you may lose the instances. In development, use logging and enable debugging
to spot and correct errors faster. If you are using GZIP, keep your file size to 1–2 GB because GZIP files cannot be split. Click here to download the white paper on Amazon EMR best practices. https://aws.amazon.com/elasticmapreduce/faqs

NEW QUESTION 32

Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high resolution MP4 format. Your workforce is distributed globally often on the move and using
company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video. Your company has no video transcoding expertise and it required you may need to pay for a consultant.
How do you implement the most cost-efficient architecture without compromising high availability and quality of video delivery'?

A. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queu
B. EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few day
C. CloudFront to serve HLS transcoded videos from EC2.
D. Elastic Transcoder to transcode original high-resolution MP4 videos to HL
E. EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few day
F. CloudFront to serve HLS transcoded videos from EC2.
G. Elastic Transcoder to transcode original high-resolution MP4 videos to HL
H. S3 to host videos with Lifecycle Management to archive original files to Glacier after a few day
I. CloudFront to serve HLS transcoded videos from S3.
J. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queu
K. S3 to host videos with Lifecycle Management to archive all files to Glacier after a few day
L. CloudFront to serve HLS transcoded videos from Glacier.

Answer: C

NEW QUESTION 34
You currently operate a web application. In the AWS US-East region The application runs on an autoscaled layer of EC2 instances and an RDS Multi-AZ database Your IT security compliance officer has
tasked you to develop a reliable and durable logging solution to track changes made to your EC2.IAM And RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?

A. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selecte
B. Use IAM roles S3 bucket policies and Multi Factor Authentication (MFA). Delete on the S3 bucket that stores your logs.
C. Create a new CloudTrail with one new S3 bucket to store the log
D. Configure SNS to send log file delivery notifications to your management syste
E. Use IAM roles and S3 bucket policies on the S3 bucket mat stores your logs.
F. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selecte
G. Use S3 ACLs and Multi Factor Authentication (MFA). Delete on the S3 bucket that stores your logs.
H. Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tool
I. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.

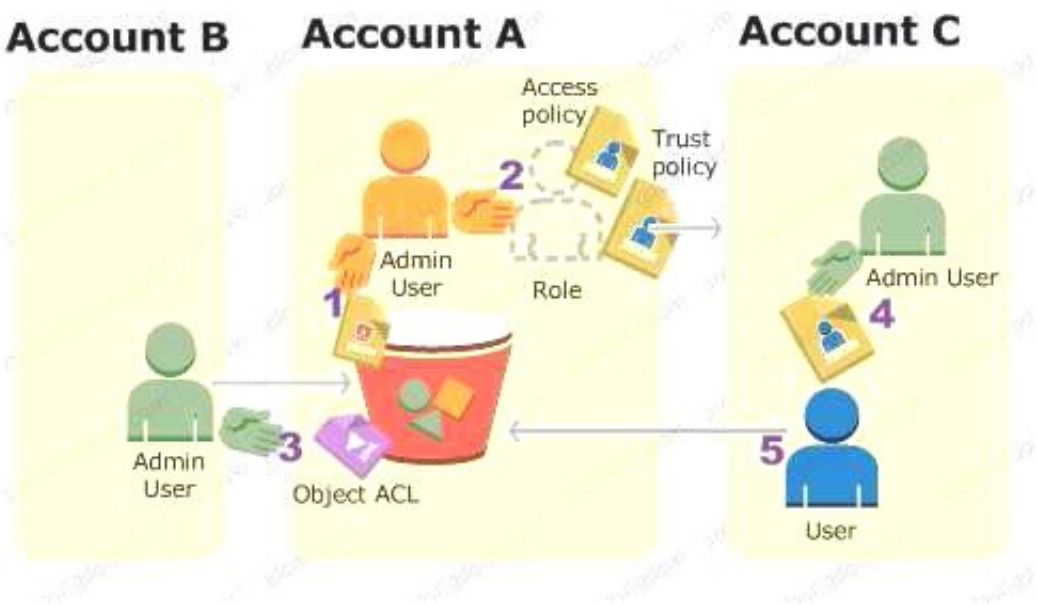
Answer: A

NEW QUESTION 38
An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?

A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
B. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application create a new access and secret key for the user andprovide these credentials to the SaaS provider.
C. Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
D. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required tor the Saas application to work, provide the role ARM to the SaaS provider to use when launching their application instances.

Answer: C

Explanation:
Granting Cross-account Permission to objects It Does Not Own
In this example scenario, you own a bucket and you have enabled other AWS accounts to upload objects. That is, your bucket can have objects that other AWS accounts own.
Now, suppose as a bucket owner, you need to grant cross-account permission on objects, regardless of who the owner is, to a user in another account. For example, that user could be a billing application that needs to access object metadata. There are two core issues:
The bucket owner has no permissions on those objects created by other AWS accounts. So for the bucket owner to grant permissions on objects it does not own, the object owner, the AWS account that created the objects, must first grant permission to the bucket owner. The bucket owner can then delegate those permissions.
Bucket owner account can delegate permissions to users in its own account but it cannot delegate permissions to other AWS accounts, because cross-account delegation is not supported.
In this scenario, the bucket owner can create an AWS Identity and Access Management (IAM) role with permission to access objects, and grant another AWS account permission to assume the role temporarily enabling it to access objects in the bucket.
Background: Cross-Account Permissions and Using IAM Roles
IAM roles enable several scenarios to delegate access to your resources, and cross-account access is one of the key scenarios. In this example, the bucket owner, Account A, uses an IAM role to temporarily delegate object access cross-account to users in another AWS account, Account C. Each IAM role you create has two policies attached to it:
A trust policy identifying another AWS account that can assume the role.
An access policy defining what permissions—for example, s3:GetObject—are allowed when someone assumes the role. For a list of permissions you can specify in a policy, see Specifying Permissions in a Policy.
The AWS account identified in the trust policy then grants its user permission to assume the role. The user can then do the following to access objects:
Assume the role and, in response, get temporary security credentials. Using the temporary security credentials, access the objects in the bucket.
For more information about IAM roles, go to Roles (Delegation and Federation) in IAM User Guide. The following is a summary of the walkthrough steps:



Account A administrator user attaches a bucket policy granting Account B conditional permission to upload objects.
Account A administrator creates an IAM role, establishing trust with Account C, so users in that account can access Account A. The access policy attached to the role limits what user in Account C can do when the user accesses Account A.
Account B administrator uploads an object to the bucket owned by Account A, granting full-control permission to the bucket owner.
Account C administrator creates a user and attaches a user policy that allows the user to assume the role.
User in Account C first assumes the role, which returns the user temporary security credentials. Using those temporary credentials, the user then accesses objects in the bucket.
For this example, you need three accounts. The following table shows how we refer to these accounts and the administrator users in these accounts. Per IAM guidelines (see About Using an Administrator User to Create Resources and Grant Permissions) we do not use the account root credentials in this walkthrough. Instead, you create an administrator user in each account and use those credentials in creating resources and granting them permissions

AWS Account ID	Account Referred To As	Administrator User in the Account
1111-1111-1111	Account A	AccountAadmin
2222-2222-2222	Account B	AccountBadmin
3333-3333-3333	Account C	AccountCadmin

NEW QUESTION 43
You are designing a data leak prevention solution for your VPC environment. You want your VPC Instances to be able to access software depots and distributions on the Internet for product updates. The depots and distributions are accessible via third party CONs by their URLs. You want to explicitly deny any other outbound connections from your VPC instances to hosts on the Internet.
Which of the following options would you consider?

A. Configure a web proxy server in your VPC and enforce URL-based rules for outbound access Remove default routes.
B. Implement security groups and configure outbound rules to only permit traffic to software depots.
C. Move all your instances into private VPC subnets remove default routes from all routing tables and add specific routes to the software depots and distributions only.
D. Implement network access control lists to all specific destinations, with an Implicit deny as a rul

Answer: A

Explanation:
Organizations usually implement proxy solutions to provide URL and web content filtering, IDS/IPS, data loss prevention, monitoring, and advanced threat protection.
https://d0.awsstatic.com/aws-answers/Controlling_VPC_Egress_Traffic.pdf

NEW QUESTION 47
You are designing an SSUTLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication. The solution must be resilient.
Which of the following options would you consider for configuring the web server infrastructure? (Choose two.)

A. Configure ELB with TCP listeners on TCP/4d3. And place the Web servers behind it.
B. Configure your Web servers with EIPS Place the Web servers in a Route53 Record Set and configure health checks against all Web servers.
C. Configure ELB with HTTPS listeners, and place the Web servers behind it.
D. Configure your web servers as the origins for a CloudFront distributio
E. Use custom SSL certificateson your CloudFront distributio

Answer: AB

Explanation:
This question is regarding “two-way” SSL authentication.
Currently, ELBs cannot support authentication for the client side SSL/TLS cert required for two-way SSL authentication to succeed. Therefore, you only have two options:
\A. Configure the ELB with a TCP/443 listener. This is effectively TLS “pass through” mode, where the TLS connection does not terminate on the ELB, it is passed through and decrypted on the back-end servers. This will cause quite a bit of CPU overhead on the back-end instances, due to the lack of TLS offload that cannot happen on the ELB, so an auto-scaling group which monitors the web server CPU metrics would be essential here. (Not that you probably wouldn’t have it anyway, just saying!)
\B. Don’t use an ELB. Just have the web servers act as the endpoint for the traffic, and let Route53 DNS serve in the place of the ELB by load balancing client DNS queries across the web servers. C and D are not options here, since neither are supported by AWS.

NEW QUESTION 48

You have an application running on an EC2 Instance which will allow users to download files from a private S3 bucket using a pre-assigned URL. Before generating the URL the application should verify the existence of the file in S3.
How should the application use AWS credentials to access the S3 bucket securely?

A. Use the AWS account access Keys the application retrieves the credentials from the source code of the application.
B. Create an IAM user for the application with permissions that allow list access to the S3 bucket launch the instance as the IAM user and retrieve the IAM user's credentials from the EC2 instance user data.
C. Create an IAM role for EC2 that allows list access to objects in the S3 bucke
D. Launch the instancewith the role, and retrieve the role's credentials from the EC2 Instance metadata
E. Create an IAM user for the application with permissions that allow list access to the S3 bucke
F. The application retrieves the IAM user credentials from a temporary directory with permissions thatallow read access only to the application use

Answer: C

Explanation:
Reference
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

NEW QUESTION 52
You are designing a social media site and are considering how to mitigate distributed denial-ofservice (DDoS) attacks. Which of the below are viable mitigation techniques? (Choose three.)

A. Add multiple elastic network interfaces (ENIs) to each EC2 instance to increase the network bandwidth.
B. Use dedicated instances to ensure that each instance has the maximum performance possible.
C. Use an Amazon CloudFront distribution for both static and dynamic content.
D. Use an Elastic Load Balancer with auto scaling groups at the we
E. App and Amazon Relational Database Service (RDS) tiers
F. Add alert Amazon CloudWatch to look for high Network in and CPU utilization.
G. Create processes and capabilities to quickly add and remove rules to the instance OS firewal

Answer: CDE

NEW QUESTION 57
A company is building a voting system for a popular TV show, viewers win watch the performances then visit the show's website to vote for their favorite performer. It is expected that in a short period of time after the show has finished the site will receive millions of visitors. The visitors will first login to the site using their Amazon.com credentials and then submit their vote. After the voting is completed the page will display the vote totals. The company needs to build the site such that can handle the rapid influx of traffic while maintaining good performance but also wants to keep costs to a minimum. Which of the design patterns below should they use?

A. Use CloudFront and an Elastic Load balancer in front of an auto-scaled set of web servers, the web servers will first can the Login With Amazon service to authenticate the user then process the users vote and store the result into a multi-AZ Relational Database Service instance.
B. Use CloudFront and the static website hosting feature of S3 with the Javascript SDK to call the Login With Amazon service to authenticate the user, use IAM Roles to gain permissions to a DynamoDB table to store the users vote.
C. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Login with Amazon service to authenticate the user, the web servers will process the users vote and store the result into a DynamoDB table using IAM Roles for EC2 instances to gain permissions to the DynamoDB table.
D. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Logi
E. With Amazon service to authenticate the user, the web servers win process the users vote and store the result into an SQS queue using IAM Roles for EC2 Instances to gain permissions to the SQS queu
F. A set of application servers will then retrieve the items from the queue and store the result into a DynamoDB table.

Answer: D

NEW QUESTION 58
You are looking to migrate your Development (Dev) and Test environments to AWS. You have decided to use separate AWS accounts to host each environment. You plan to link each accounts bill to a Master AWS account using Consolidated Billing. To make sure you Keep within budget you would like to implement a way for administrators in the Master account to have access to stop, delete and/or terminate resources in both the Dev and Test accounts. Identify which option will allow you to
achieve this goal.

A. Create IAM users in the Master account with full Admin permission
B. Create cross-account roles in the Dev and Test accounts that grant the Master account access to the resources in the account by inheriting permissions from the Master account.
C. Create IAM users and a cross-account role in the Master account that grants full Admin permissions to the Dev and Test accounts.
D. Create IAM users in the Master accoun
E. Create cross-account roles in the Dev and Test accounts that have full Admin permissions and grant the Master account access.
F. Link the accounts using Consolidated Billin
G. This will give IAM users in the Master account access to resources in the Dev and Test accounts

Answer: C

NEW QUESTION 63
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 VPC,
B. 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.
C. Configure servers running in the VPC using the host-based 'route' commands to send all traffic through the platform to a scalable virtualized IDS/IPS.
D. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.

Answer: D

Explanation:
\A. Not possible to set an instance's NIC into promiscuous mode.
\B. Incorrect… VPC peering connections are not "transitive", i.e. you cannot pass traffic through a VPC peering connection into another VPC, and then have that other VPC send the traffic to some third VPC, or the Internet, or a VPN, or a direct connect circuit. (I would assume AWS does not allow redistribution of routes from one VPC's back-end VRF into another VPC's back-end VRF, unless it is that first VPC's CIDR block? Someone from AWS would have to chime in here, and they're probably not going to tell us.)
\C. This one is incorrect because adding static routes on an instance won't affect the routing from any point after the packet leaves the instance's NIC. AWS will check the destination IP address in the packet header and forward according to the VPC routing table's routes. You'd need to make routing changes in the VPC route table for that instance's traffic to get sent through another device (e.g. NAT gateway, VPN instance, or security proxy in this case). (You could tunnel/proxy the traffic over through the IPS tier by changing the destination IP address in the IP header of the packet before it left the instance. But choice C did not state anything about doing anything like that. It just said add a static route on the instance, which does not change the destination IP address in the IP header of the packet.)
\D. Correct, this is the standard approach, and is definitely scalable.

NEW QUESTION 68
What does Amazon S3 stand for?

A. Simple Storage Solution.
B. Storage Storage Storage (triple redundancy Storage).
C. Storage Server Solution.
D. Simple Storage Servic

Answer: D

Explanation:
Amazon Simple Storage Service (Amazon S3) is storage for the Internet. It provides a simple interface to manage scalable, reliable, and low latency data storage service over the Internet. http://docs.aws.amazon.com/AmazonS3/latest/gsg/GetStartedWithS3.html

NEW QUESTION 70
You must assign each server to at least _____ security group

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

Answer: D

Explanation:
Your AWS account automatically has a default security group per region for EC2-Classic. When you create a VPC, we automatically create a default security group for the VPC. If you don't specify a different security group when you launch an instance, the instance is automatically associated with the appropriate default security group. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

NEW QUESTION 75
Before I delete an EBS volume, what can I do if I want to recreate the volume later?

A. Create a copy of the EBS volume (not a snapshot)
B. Store a snapshot of the volume
C. Download the content to an EC2 instance
D. Back up the data in to a physical disk

Answer: B

Explanation:
After you no longer need an Amazon EBS volume, you can delete it. After deletion, its data is gone and the volume can't be attached to any instance. However, before deletion, you can store a snapshot of the volume, which you can use to re-create the volume later.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-volume.html

NEW QUESTION 78
What does RRS stand for when talking about S3?

A. Redundancy Removal System
B. Relational Rights Storage
C. Regional Rights Standard
D. Reduced Redundancy Storage

Answer: D

Explanation:
In Amazon S3, RRS stands for Reduced Redundancy Storage. Reduced redundancy storage stores objects on multiple devices across multiple facilities, providing 400 times the durability of a typical disk drive, but it does not replicate objects as many times as Amazon S3 standard storage. In addition, reduced redundancy storage is designed to sustain the loss of data in a single facility. http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingRRS.html

NEW QUESTION 80
All Amazon EC2 instances are assigned two IP addresses at launch, out of which one can only be reached from within the Amazon EC2 network?

A. Multiple IP address
B. Public IP address
C. Private IP address
D. Elastic IP Address

Answer: C

NEW QUESTION 84
What is the Reduced Redundancy option in Amazon S3?

A. Less redundancy for a lower cost.
B. It doesn't exist in Amazon S3, but in Amazon EBS.
C. It allows you to destroy any copy of your files outside a specific jurisdiction.
D. It doesn't exist at all

Answer: A

NEW QUESTION 89
While creating an Amazon RDS DB, your first task is to set up a DB that controls what IP addresses or EC2 instances have access to your DB Instance.

A. Security Pool
B. Secure Zone
C. Security Token Pool
D. Security Group

Answer: D

NEW QUESTION 91
Amazon SWF is designed to help users...

A. Design graphical user interface interactions
B. Manage user identification and authorization
C. Store Web content
D. Coordinate synchronous and asynchronous tasks which are distributed and fault toleran

Answer: D

NEW QUESTION 93
Can I control if and when MySQL based RDS Instance is upgraded to new supported versions?

A. No
B. Only in VPC
C. Yes

Answer: C

NEW QUESTION 97
When you view the block device mapping for your instance, you can see only the EBS volumes, not the instance store volumes.

A. Depends on the instance type
B. FALSE
C. Depends on whether you use API call
D. TRUE

Answer: D

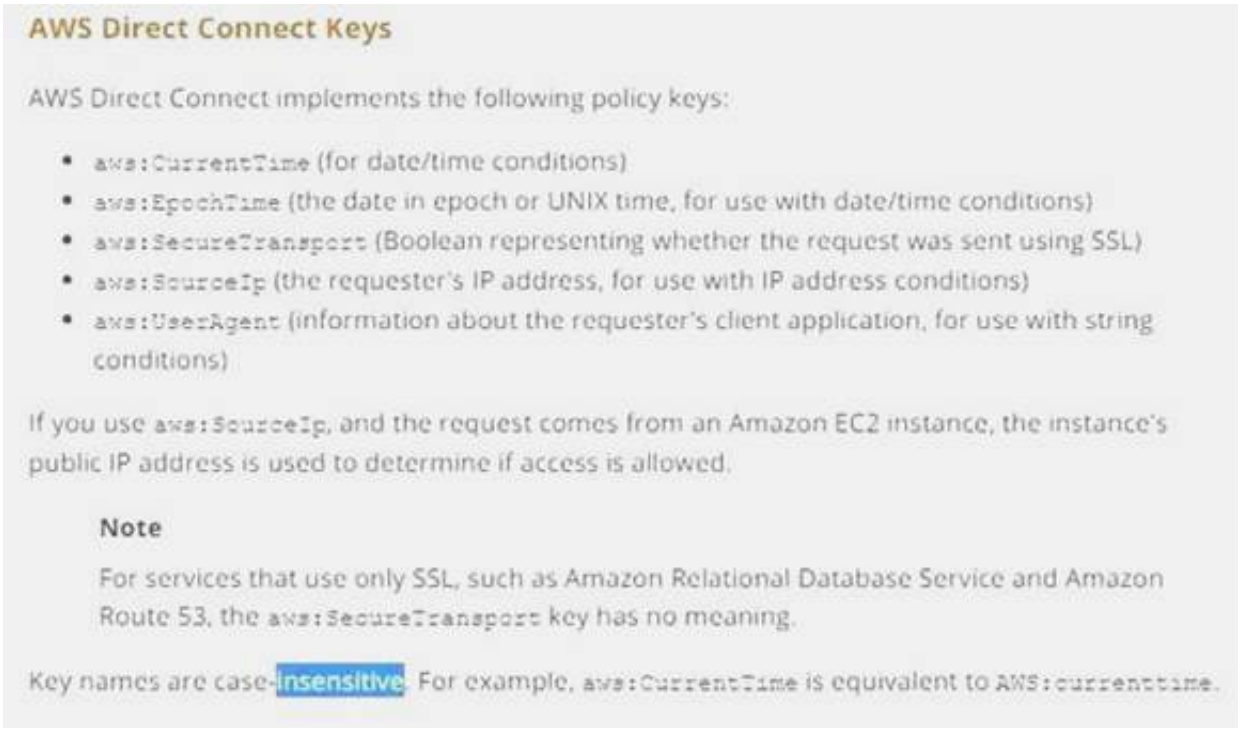
Explanation:
When you view the block device mapping for your instance, you can see only the EBS volumes, not the instance store volumes. You can use instance metadata to query the complete block device mapping. The base URI for all requests for instance metadata is http://169.254.169.254/latest/. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mappingconcepts. html#bdm-instance-metadata

NEW QUESTION 101
True or False: When using IAM to control access to your RDS resources, the key names that can be used are case sensitive. For example, aws:CurrentTime is NOT equivalent to AWS:currenttime.

A. TRUE
B. FALSE

Answer: A

Explanation:



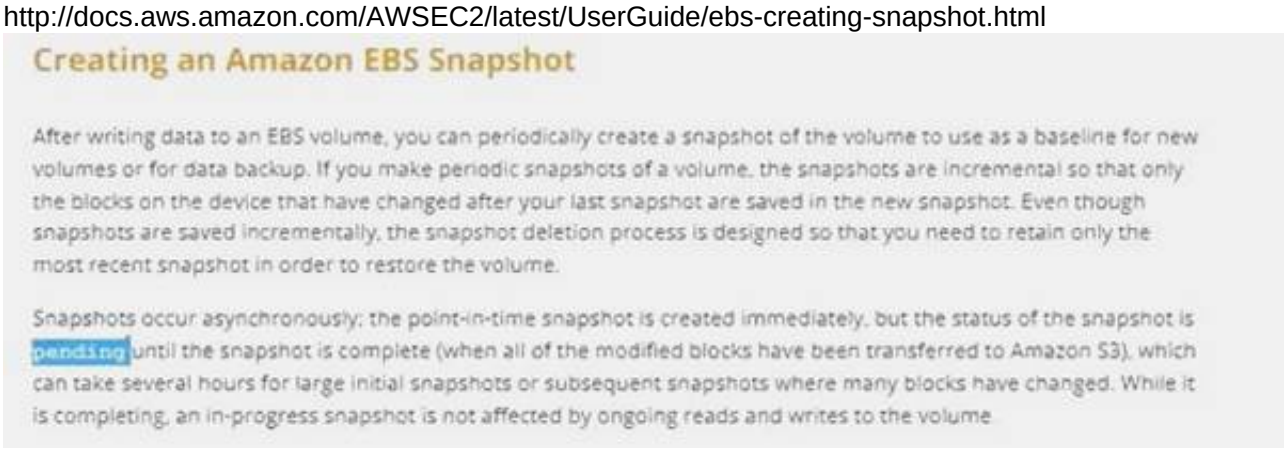
http://docs.aws.amazon.com/directconnect/latest/UserGuide/using_iam.html

NEW QUESTION 102
What will be the status of the snapshot until the snapshot is complete.

A. running
B. working
C. progressing
D. pending

Answer: D

Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html



NEW QUESTION 105
Can we attach an EBS volume to more than one EC2 instance at the same time?

A. No
B. Yes.
C. Only EC2-optimized EBS volumes.
D. Only in read mod

Answer: A

NEW QUESTION 110
Amazon RDS automated backups and DB Snapshots are currently supported for only the _ storage engine

A. InnoDB
B. MyISAM

Answer: A

NEW QUESTION 113
While creating the snapshots using the command line tools, which command should I be using?

A. ec2-deploy-snapshot
B. ec2-fresh-snapshot
C. ec2-create-snapshot
D. ec2-new-snapshot

Answer: C

Explanation:
http://docs.aws.amazon.com/cli/latest/reference/ec2/create-snapshot.html

NEW QUESTION 114
Typically, you want to check your application whether a request generated an error before you spend any time processing results. The easiest way to find out if an error occurred is to look for an ____ node in the response from the Amazon RDS API.

A. Incorrect
B. Error
C. FALSE

Answer: B

Explanation:
Typically, you want your application to check whether a request generated an error before you spend any time processing results. The easiest way to find out if an error occurred is to look for an Error node in the response from the Amazon RDS API.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/APITroubleshooting.html

NEW QUESTION 117
In the Amazon CloudWatch, which metric should I be checking to ensure that your DB Instance has enough free storage space?

A. FreeStorage
B. FreeStorageSpace
C. FreeStorageVolume
D. FreeDBStorageSpace

Answer: B

NEW QUESTION 122
Amazon RDS DB snapshots and automated backups are stored in

A. Amazon S3
B. Amazon ECS Volume
C. Amazon RDS
D. Amazon EMR

Answer: A

NEW QUESTION 124
You must increase storage size in increments of at least _____ %

A. 40
B. 20
C. 50
D. 10

Answer: D

NEW QUESTION 125
Using Amazon CloudWatch's Free Tier, what is the frequency of metric updates which you receive?

A. 5 minutes
B. 500 milliseconds.
C. 30 seconds
D. 1 minute

Answer: A

Explanation:
You can get started with Amazon CloudWatch for free. Many applications should be able to operate within these free tier limits.
New and existing customers also receive 3 dashboards of up to 50 metrics each per month at no
additional charge Basic Monitoring metrics (at five-minute frequency) for Amazon EC2 instances are free of charge, as are all metrics for Amazon EBS volumes, Elastic Load Balancers, and Amazon RDS DB instances.
https://aws.amazon.com/cloudwatch/pricing/

NEW QUESTION 130
What are the Amazon EC2 API tools?

A. They don't exis
B. The Amazon EC2 AMI tools, instead, are used to manage permissions.
C. Command-line tools to the Amazon EC2 web service.
D. They are a set of graphical tools to manage EC2 instances.
E. They don't exis
F. The Amazon API tools are a client interface to Amazon Web Services.

Answer: B

NEW QUESTION 131

What are the two types of licensing options available for using Amazon RDS for Oracle?

A. BYOL and Enterprise License
B. BYOL and License Included
C. Enterprise License and License Included
D. Role based License and License Included

Answer: B

Explanation:
https://aws.amazon.com/rds/oracle/

You can run Amazon RDS for Oracle under two different licensing models – "License Included" and "Bring-Your-Own-License (BYOL)". In the "License Included" service model, you do not need separately purchased Oracle licenses; the Oracle Database software has been licensed by AWS. "License Included" pricing starts at $0.04 per hour, inclusive of software, underlying hardware resources, and Amazon RDS management capabilities. If you already own Oracle Database licenses, you can use the "BYOL" model to run Oracle databases on Amazon RDS, with rates starting at $0.025 per hour. The "BYOL" model is designed for customers who prefer to use existing Oracle database licenses or purchase new licenses directly from Oracle. For more information, see Licensing Amazon RDS for Oracle.

NEW QUESTION 134
Can Amazon S3 uploads resume on failure or do they need to restart?

A. Restart from beginning
B. You can resume them, if you flag the "resume on failure" option before uploading.
C. Resume on failure
D. Depends on the file size

Answer: C

NEW QUESTION 139
Fill in the blanks: _____ let you categorize your EC2 resources in different ways, for example, by purpose, owner, or environment.

A. wildcards
B. pointers
C. Tags
D. special filters

Answer: C

NEW QUESTION 141
How can I change the security group membership for interfaces owned by other AWS, such as Elastic Load Balancing?

A. By using the service specific console or API\CLI commands
B. None of these
C. Using Amazon EC2 API/CLI
D. using all these methods

Answer: A

Explanation:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-security-groups.html

Security Groups for Load Balancers in a VPC

When you use the AWS Management Console to create a load balancer in a VPC, you can choose an existing security group for the VPC or create a new security group for the VPC. If you choose an existing security group, it must allow traffic in both directions to the listener and health check ports for the load balancer. If you choose to create a security group, the console automatically adds rules to allow all traffic on these ports.

[Nondefault VPC] If you use the AWS CLI or API to create a load balancer in a nondefault VPC, but you don't specify a security group, your load balancer is automatically associated with the default security group for the VPC.

[Default VPC] If you use the AWS CLI or API to create a load balancer in your default VPC, you can't choose an existing security group for your load balancer. Instead, Elastic Load Balancing provides a security group with rules to allow all traffic on the ports specified for the load balancer. Elastic Load Balancing creates only one such security group per AWS account, with a name of the form default_elb_*id* (for example, `default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE`). Subsequent load balancers that you create in the default VPC also use this security group. Be sure to review the security group rules to ensure that they allow traffic on the listener and health check ports for the new load balancer. When you delete your load balancer, this security group is not deleted automatically.

If you add a listener to an existing load balancer, you must review your security groups to ensure they allow traffic on the new listener port in both directions.

NEW QUESTION 143
What does the following command do with respect to the Amazon EC2 security groups? ec2-revoke RevokeSecurityGroupIngress

A. Removes one or more security groups from a rule.
B. Removes one or more security groups from an Amazon EC2 instance.

C. Removes one or more rules from a security group.
D. Removes a security group from our accoun

Answer: C

Explanation:
Removes one or more ingress rules from a security group. The values that you specify in the revoke request (for example, ports) must match the existing rule's values for the rule to be removed. http://docs.aws.amazon.com/cli/latest/reference/ec2/revoke-security-group-ingress.html

NEW QUESTION 148
True or False: Manually created DB Snapshots are deleted after the DB Instance is deleted.

A. TRUE
B. FALSE

Answer: B

Explanation:
If you choose not to create a final DB snapshot, you will not be able to later restore the DB instance to its final state. When you delete a DB instance, all automated backups are deleted and cannot be recovered. Manual DB snapshots of the instance are not deleted.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_DeleteInstance.html

NEW QUESTION 152
Can I move a Reserved Instance from one Region to another?

A. No
B. Only if they are moving into GovCloud
C. Yes
D. Only if they are moving to US East from another region

Answer: A

NEW QUESTION 153
Will my standby RDS instance be in the same Availability Zone as my primary?

A. Only for Oracle RDS types
B. Yes
C. Only if configured at launch
D. No

Answer: D

NEW QUESTION 155
What happens to the data on an instance if the instance reboots (intentionally or unintentionally)?

A. Data will be lost
B. Data persists
C. Data may persist however cannot be sure

Answer: B

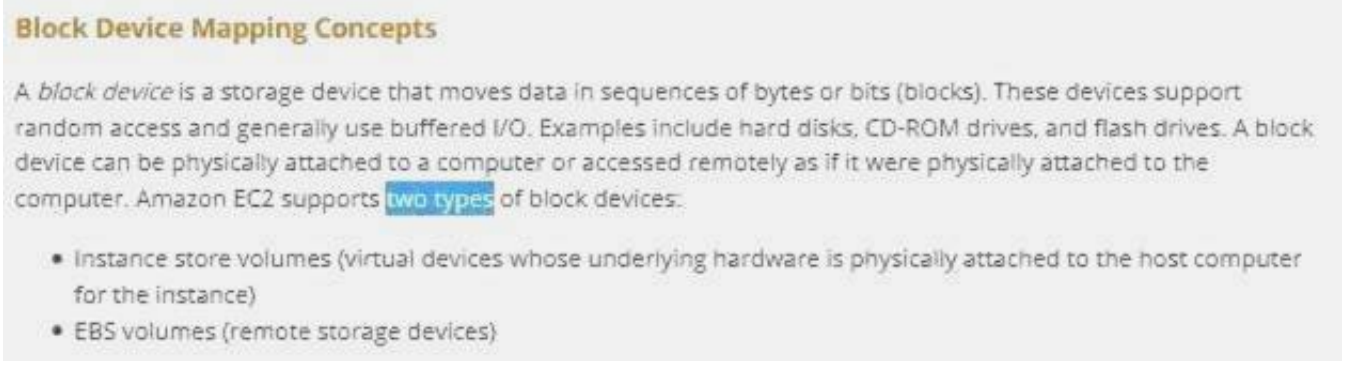
Explanation:
Instance Store Lifetime
You can specify instance store volumes for an instance only when you launch it. The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data in the instance store is lost under the following circumstances:
The underlying disk drive fails The instance stops
The instance terminates http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

NEW QUESTION 159
How many types of block devices does Amazon EC2 support?

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

Answer: A

Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html Amazon EC2 supports two types of block devices:
Instance store volumes (virtual devices whose underlying hardware is physically attached to the host computer for the instance)
EBS volumes (remote storage devices)
A block device mapping defines the block devices (instance store volumes and EBS volumes) to attach to an instance.


Block Device Mapping Concepts

A *block device* is a storage device that moves data in sequences of bytes or bits (blocks). These devices support random access and generally use buffered I/O. Examples include hard disks, CD-ROM drives, and flash drives. A block device can be physically attached to a computer or accessed remotely as if it were physically attached to the computer. Amazon EC2 supports two types of block devices:

- Instance store volumes (virtual devices whose underlying hardware is physically attached to the host computer for the instance)
- EBS volumes (remote storage devices)

NEW QUESTION 162
For each DB Instance class, what is the maximum size of associated storage capacity?

A. 5GB
B. 6TB
C. 2TB
D. 500GB

Answer: B

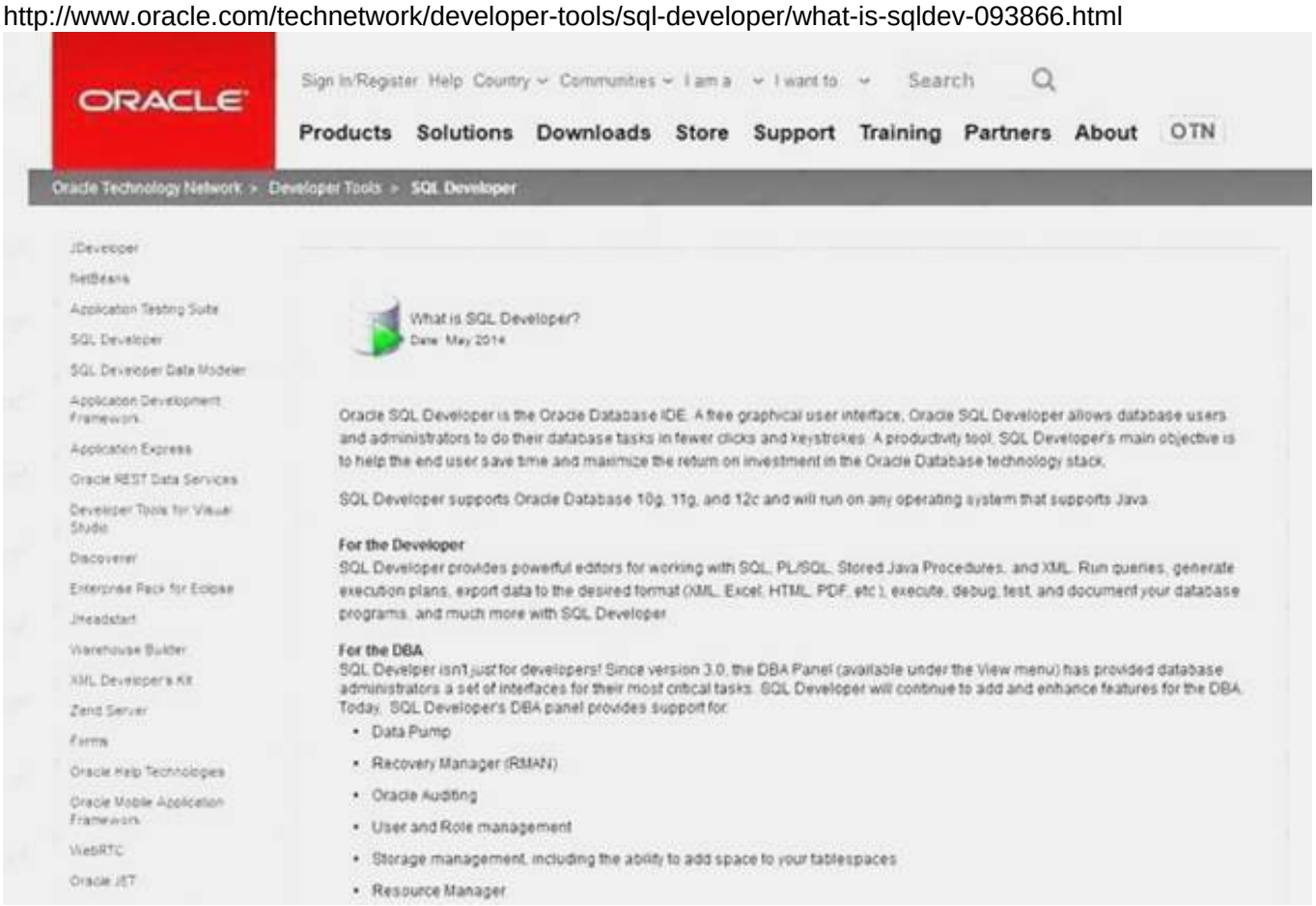
Explanation:
"You can now create MySQL, PostgreSQL, and Oracle RDS database instances with up to 6TB of storage and SQL Server RDS database instances with up to 4TB of storage when using the Provisioned IOPS and General Purpose (SSD) storage types. Existing MySQL, PostgreSQL, and Oracle RDS database instances can be scaled to these new database storage limits without any downtime."

NEW QUESTION 164
What is Oracle SQL Developer?

A. An AWS developer who is an expert in Amazon RDS using both the Oracle and SQL Server DB engines
B. A graphical Java tool distributed without cost by Oracle.
C. It is a variant of the SQL Server Management Studio designed by Microsoft to support Oracle DBMS functionalities
D. A different DBMS released by Microsoft free of cost

Answer: B

Explanation:
http://www.oracle.com/technetwork/developer-tools/sql-developer/what-is-sqldev-093866.html


ORACLE

Sign In/Register Help Country Communities I am a I want to Search

Products Solutions Downloads Store Support Training Partners About OTN

Oracle Technology Network > Developer Tools > SQL Developer

JDeveloper
NetBeans
Application Testing Suite
SQL Developer
SQL Developer Data Modeler
Application Development Framework
Application Express
Oracle REST Data Services
Developer Tools for Visual Studio
Discoverer
Enterprise Pack for Eclipse
JHeadstart
Warehouse Builder
XML Developer's Kit
Zend Server
Forms
Oracle Help Technologies
Oracle Mobile Application Framework
WebRTC
Oracle JET

What is SQL Developer?
Date: May 2014

Oracle SQL Developer is the Oracle Database IDE. A free graphical user interface, Oracle SQL Developer allows database users and administrators to do their database tasks in fewer clicks and keystrokes. A productivity tool, SQL Developer's main objective is to help the end user save time and maximize the return on investment in the Oracle Database technology stack.

SQL Developer supports Oracle Database 10g, 11g, and 12c and will run on any operating system that supports Java.

For the Developer
SQL Developer provides powerful editors for working with SQL, PL/SQL, Stored Java Procedures, and XML. Run queries, generate execution plans, export data to the desired format (XML, Excel, HTML, PDF, etc.), execute, debug, test, and document your database programs, and much more with SQL Developer.

For the DBA
SQL Developer isn't just for developers! Since version 3.0, the DBA Panel (available under the View menu) has provided database administrators a set of interfaces for their most critical tasks. SQL Developer will continue to add and enhance features for the DBA. Today, SQL Developer's DBA panel provides support for:

- Data Pump
- Recovery Manager (RMAN)
- Oracle Auditing
- User and Role management
- Storage management, including the ability to add space to your tablespaces
- Resource Manager

NEW QUESTION 165
Using Amazon IAM, can I give permission based on organizational groups?

A. Yes but only in certain cases
B. No
C. Yes always

Answer: C

Explanation:
An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users. http://docs.aws.amazon.com/IAM/latest/UserGuide/id.html

NEW QUESTION 170
What is an isolated database environment running in the cloud (Amazon RDS) called?

A. DB Instance
B. DB Server
C. DB Unit
D. DB Volume

Answer: A

NEW QUESTION 171
When running my DB Instance as a Multi-AZ deployment, can I use the standby for read or write operations?

A. Yes
B. Only with MSSQL based RDS
C. Only for Oracle RDS instances
D. No

Answer: D

Explanation:
Q: When running my DB instance as a Multi-AZ deployment, can I use the standby for read or write operations?

No, the standby replica cannot serve read requests. Multi-AZ deployments are designed to provide enhanced database availability and durability, rather than read scaling benefits. As such, the feature uses synchronous replication between primary and standby. Our implementation makes sure the primary and the standby are constantly in sync, but precludes using the standby for read or write operations. If you are interested in a read scaling solution, please see the FAQs on Read Replicas.

NEW QUESTION 176
When should I choose Provisioned IOPS over Standard RDS storage?

A. If you have batch-oriented workloads
B. If you use production online transaction processing (OLTP) workloads.
C. If you have workloads that are not sensitive to consistent performance

Answer: B

Explanation:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html
Amazon RDS provisions that IOPS rate and storage for the lifetime of the DB instance or until you change it. Provisioned IOPS storage is optimized for I/O intensive, online transaction processing (OLTP) workloads that have consistent performance requirements. Provisioned IOPS helps performance tuning.

NEW QUESTION 178
In the 'Detailed' monitoring data available for your Amazon EBS volumes, Provisioned IOPS volumes automatically send _____ minute metrics to Amazon CloudWatch.

A. 3
B. 1
C. 5
D. 2

Answer: B

NEW QUESTION 182
What is the command line instruction for running the remote desktop client in Windows?

A. desk.cpl
B. mstsc

Answer: B

NEW QUESTION 187

MySQL installations default to port _____ .

A. 3306
B. 443
C. 80
D. 1158

Answer: A

Explanation:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ConnectToInstance.html

NEW QUESTION 188
If you have chosen Multi-AZ deployment, in the event of a planned or unplanned outage of your primary DB Instance, Amazon RDS automatically switches to the standby replica. The automatic failover mechanism simply changes the _____ record of the main DB Instance to point to the standby DB Instance.

A. DNAME
B. CNAME
C. TXT
D. MX

Answer: B

Explanation:
"When failing over, Amazon RDS simply flips the canonical name record (CNAME) for your DB Instance to point at the standby, which is in turn promoted to become the new primary" https://aws.amazon.com/rds/faqs/

NEW QUESTION 190
If I modify a DB Instance or the DB parameter group associated with the instance, should I reboot the instance for the changes to take effect?

A. No
B. Yes

Answer: B

NEW QUESTION 194
If I want to run a database in an Amazon instance, which is the most recommended Amazon storage option?

A. Amazon Instance Storage
B. Amazon EBS
C. You can't run a database inside an Amazon instance.
D. Amazon S3

Answer: B

Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Storage.html

NEW QUESTION 196
Can I test my DB Instance against a new version before upgrading?

A. No
B. Yes
C. Only in VPC

Answer: B

Explanation:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Upgrading.h tml

NEW QUESTION 200
Making your snapshot public shares all snapshot data with everyone. Can the snapshots with AWS Marketplace product codes be made public?

A. No
B. Yes

Answer: A

Explanation:
"Making your snapshot public shares all snapshot data with everyone; however, snapshots with AWS Marketplace product codes cannot be made public. Encrypted snapshots cannot be shared between
accounts or made public." http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifyingsnapshot- permissions.html
"This is not a valid option for encrypted snapshots or snapshots with AWS Marketplace product codes."

NEW QUESTION 204
Fill in the blanks: "To ensure failover capabilities, consider using a ____ for incoming traffic on a network interface".

A. primary public IP
B. secondary private IP
C. secondary public IP
D. add on secondary IP

Answer: B

Explanation:
To ensure failover capabilities, consider using a secondary private IP for incoming traffic on an elastic network interface. In the event of an instance failure, you can move the interface and/or secondary private IP address to a standby instance

NEW QUESTION 207
What does Amazon CloudFormation provide?

A. The ability to setup Autoscaling for Amazon EC2 instances.
B. None of these.
C. A templated resource creation for Amazon Web Services.
D. A template to map network resources for Amazon Web Service

Answer: C

Explanation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you.

NEW QUESTION 211
Can I encrypt connections between my application and my DB Instance using SSL?

A. No
B. Yes
C. Only in VPC
D. Only in certain regions

Answer: B

NEW QUESTION 213
Can the string value of 'Key' be prefixed with: aws:"?

A. Only in GovCloud
B. Only for S3 not EC2
C. Yes
D. No

Answer: D

Explanation:
"The tag key is the required name of the tag. The string value can be from 1 to 128 Unicode characters in length and cannot be prefixed with "aws:" or "rds:"."
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Tagging.html http://docs.aws.amazon.com/cli/latest/reference/rds/list-tags-for-resource.html

NEW QUESTION 215
Through which of the following interfaces is AWS Identity and Access Management available?
A) AWS Management Console
B) Command line interface (CLI)
C) IAM Query API
D) Existing libraries

A. Only through Command line interface (CLI)
B. A, B and C
C. A and C
D. All of the above

Answer: D

Explanation:
Accessing IAM:
1 - AWS Management Console 2 - AWS Command Line Tools
3 - AWS SDKs (i.e. Existing libraries) 4 - IAM HTTPS API
http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html#intro-accessing

NEW QUESTION 218
How are the EBS snapshots saved on Amazon S3?

A. Exponentially
B. Incrementally
C. EBS snapshots are not stored in the Amazon S3

D. Decrementally

Answer: B

NEW QUESTION 221
Can I delete a snapshot of the root device of an EBS volume used by a registered AMI?

A. Only via API
B. Only via Console
C. Yes
D. No

Answer: D

Explanation:
Note that you can't delete a snapshot of the root device of an EBS volume used by a registered AMI. You must first deregister the AMI before you can delete the snapshot.
Source: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-snapshot.html

NEW QUESTION 225
The ____ service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console.

A. Amazon RDS
B. AWS Integrity Management
C. AWS Identity and Access Management
D. Amazon EMR

Answer: C

Explanation:
https://aws.amazon.com/documentation/iam/?nc1=h_ls

NEW QUESTION 228
When automatic failover occurs, Amazon RDS will emit a DB Instance event to inform you that automatic failover occurred. You can use the ____ to return information about events related to your DB Instance

A. FetchFailure
B. DescriveFailure
C. DescribeEvents
D. FetchEvents

Answer: C

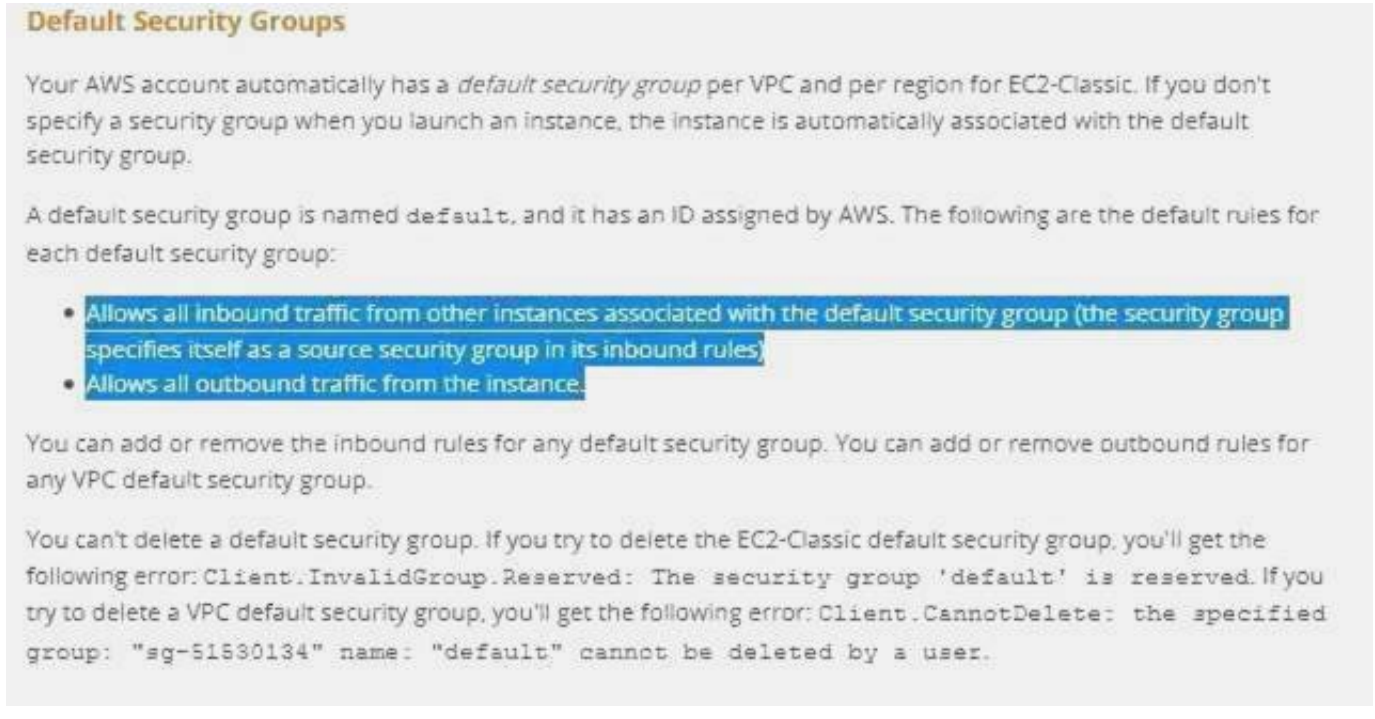
Explanation:
Q: Will I be alerted when automatic failover occurs?
Yes, Amazon RDS will emit a DB Instance event to inform you that automatic failover occurred. You can use the DescribeEvents to return information about events related to your DB Instance, or click the "DB Events" section of the AWS Management Console
https://aws.amazon.com/rds/faqs/

NEW QUESTION 231
Select the correct set of options. These are the initial settings for the default security group:

A. Allow no inbound traffic, Allow all outbound traffic and Allow instances associated with this security group to talk to each other
B. Allow all inbound traffic, Allow no outbound traffic and Allow instances associated with this security group to talk to each other
C. Allow no inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other
D. Allow all inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other

Answer: A

Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#defaultsecurity- group
A default security group is named default, and it has an ID assigned by AWS. The following are the initial settings for each default security group:
Allow inbound traffic only from other instances associated with the default security group Allow all outbound traffic from the instance
The default security group specifies itself as a source security group in its inbound rules. This is what allows instances associated with the default security group to communicate with other instances associated with the default security group.



NEW QUESTION 235
What does Amazon Route53 provide?

A. A global Content Delivery Network.
B. None of these.
C. A scalable Domain Name System.
D. An SSH endpoint for Amazon EC2.

Answer: C

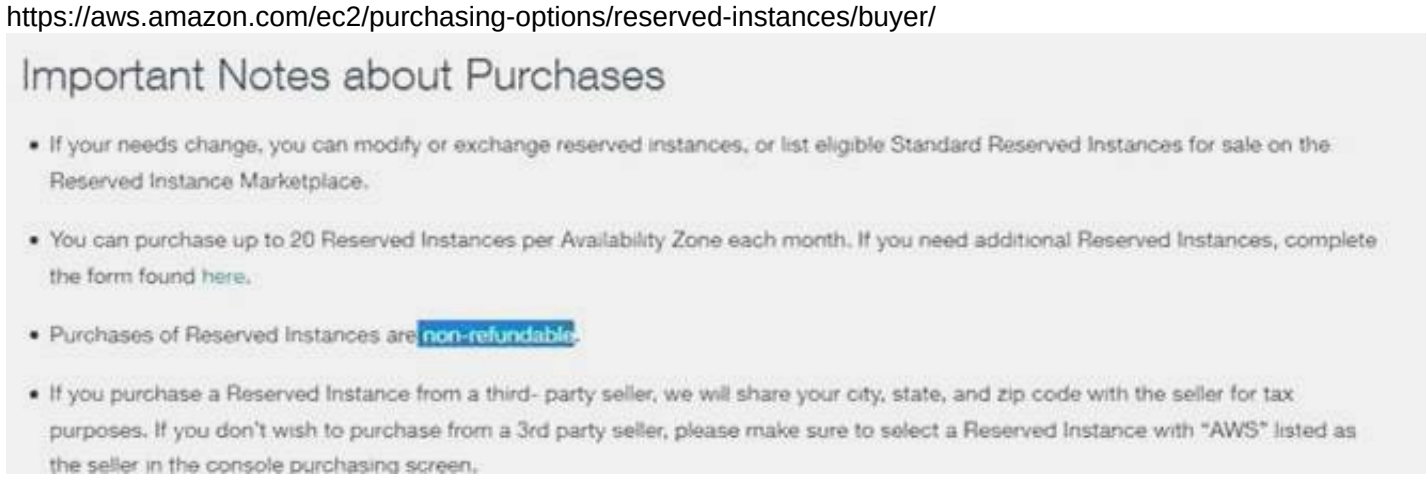
Explanation:
https://aws.amazon.com/route53/

NEW QUESTION 236
The one-time payment for Reserved Instances is ____ refundable if the reservation is cancelled.

A. always
B. in some circumstances
C. never

Answer: C

Explanation:
the one-time fee is non-refundable.
https://aws.amazon.com/ec2/purchasing-options/reserved-instances/buyer/



NEW QUESTION 239
If an Amazon EBS volume is the root device of an instance, can I detach it without stopping the instance?

A. Yes but only if Windows instance
B. No
C. Yes
D. Yes but only if a Linux instance

Answer: B

Explanation:
"If an EBS volume is the root device of an instance, you must stop the instance before you can detach the volume."
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-detaching-volume.html

NEW QUESTION 242
Which of the following statements are true about Amazon Route 53 resource records? (Choose two.)

A. An Alias record can map one DNS name to another Amazon Route 53 DNS name.
B. A CNAME record can be created for your zone apex.
C. An Amazon Route 53 CNAME record can point to any DNS record hosted anywhere.
D. TTL can be set for an Alias record in Amazon Route 53.
E. An Amazon Route 53 Alias record can point to any DNS record hosted anywher

Answer: AC

NEW QUESTION 246
A _____ is an individual, system, or application that interacts with AWS programmatically.

A. user
B. AWS Account
C. Group
D. Role

Answer: A

Explanation:
Q: What is a user?
A user is a unique identity recognized by AWS services and applications. Similar to a login user in an operating system like Windows or UNIX, a user has a unique name and can identify itself
using familiar security credentials such as a password or access key. A user can be an individual, system, or application requiring access to AWS services. IAM supports users (referred to as “IAM users”) managed in AWS’s identity management system, and it also enables you to grant access to AWS resources for users managed outside of AWS in your corporate directory (referred to as “federated users”).

NEW QUESTION 249
Select the correct statement:

A. You don't need not specify the resource identifier while stopping a resource
B. You can terminate, stop, or delete a resource based solely on its tags
C. You can't terminate, stop, or delete a resource based solely on its tags
D. You don't need to specify the resource identifier while terminating a resource

Answer: C

Explanation:
You can’t terminate, stop, or delete a resource based solely on its tags; you must specify the resource identifier.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html#tag-restrictions

NEW QUESTION 253
Amazon EC2 has no Amazon Resource Names (ARNs) because you can't specify a particular Amazon EC2 resource in an IAM policy.

A. TRUE
B. FALSE

Answer: B

Explanation:
http://blogs.aws.amazon.com/security/post/Tx29HCT3ABL7LP3/Resource-level-Permissions-for-EC2- Controlling- Management-Access-on-Specific-Ins

NEW QUESTION 255
Is the encryption of connections between my application and my DB Instance using SSL for the MySQL server engines available?

A. Yes
B. Only in VPC
C. Only in certain regions
D. No

Answer: A

Explanation:
https://aws.amazon.com/rds/faqs/

NEW QUESTION 257
True or False: Common points of failures like generators and cooling equipment are shared across Availability Zones.

A. TRUE
B. FALSE

Answer: B

NEW QUESTION 262
Security groups act like a firewall at the instance level, whereas _____ are an additional layer of security that act at the subnet level.

A. DB Security Groups
B. VPC Security Groups
C. network ACLs

Answer: C

NEW QUESTION 264
While controlling access to Amazon EC2 resources, which of the following acts as a firewall that controls the traffic allowed to reach one or more instances?

A. A security group
B. An instance type
C. A storage cluster
D. An object

Answer: A

Explanation:
A security group acts as a firewall that controls the traffic allowed to reach one or more instances. When you launch an instance, you assign it one or more security groups. http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM.html

NEW QUESTION 269
Which DNS name can only be resolved within Amazon EC2?

A. Internal DNS name
B. External DNS name
C. Global DNS name
D. Private DNS name

Answer: D

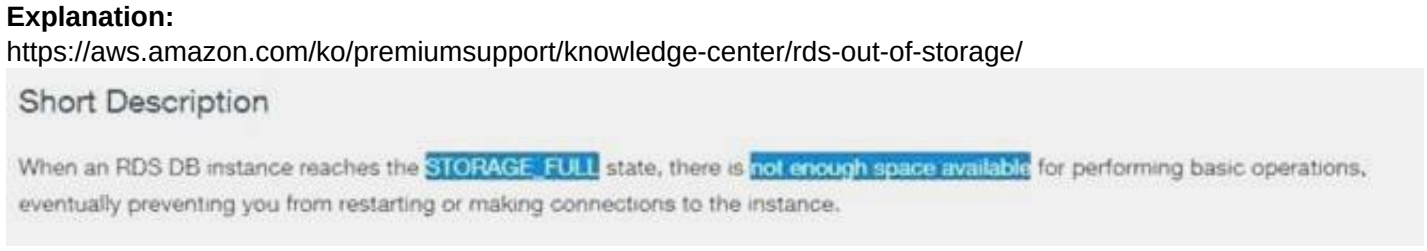
Explanation:
To view DNS hostnames for an instance using the console
1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose Instances.
3. Select your instance from the list.
4. In the details pane, the Public DNS (IPv4) and Private DNS fields display the DNS hostnames, if applicable.

NEW QUESTION 271
If your DB instance runs out of storage space or file system resources, its status will change to _____ and your DB Instance will no longer be available.

A. storage-overflow
B. storage-full
C. storage-exceed
D. storage-overage

Answer: B

Explanation:
https://aws.amazon.com/ko/premiumsupport/knowledge-center/rds-out-of-storage/



NEW QUESTION 274
Select the correct set of steps for exposing the snapshot only to specific AWS accounts

A. Select public for all the accounts and check mark those accounts with whom you want to expose the snapshots and click save.
B. SelectPrivate, enter the IDs of those AWS accounts, and clickSave.
C. SelectPublic, enter the IDs of those AWS accounts, and clickSave.
D. SelectPublic, mark the IDs of those AWS accounts as private, and clickSav

Answer: B

Explanation:
"To expose the snapshot to only specific AWS accounts, choose Private, enter the ID of the AWS account (without hyphens) in the AWS Account Number field, and choose Add Permission. Repeat until you've added all the required AWS accounts" http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshot-permissions.html

NEW QUESTION 277
By default, what are ENIs that are automatically created and attached to instances using the EC2 console set to do when the attached instance terminates?

A. Remain as is
B. Terminate
C. Hibernate
D. Pause

Answer: B

Explanation:
By default, elastic network interfaces that are automatically created and attached to instances using the console are set to terminate when the instance terminates. However, network interfaces created using the command line interface aren't set to terminate when the instance terminates.

NEW QUESTION 278
Fill in the blanks: is a durable, block-level storage volume that you can attach to a single, running Amazon EC2 instance.

A. Amazon S3
B. Amazon EBS
C. None of these
D. All of these

Answer: B

NEW QUESTION 280
Do the Amazon EBS volumes persist independently from the running life of an Amazon EC2 instance?

A. No
B. Only if instructed to when created
C. Yes

Answer: C

NEW QUESTION 285
What is the minimum time Interval for the data that Amazon CloudWatch receives and aggregates?

A. One second
B. Five seconds
C. One minute
D. Three minutes
E. Five minutes

Answer: C

Explanation:
Many metrics are received and aggregated at 1-minute intervals. Some are at 3-minute or 5-minute intervals.

NEW QUESTION 289
Does Dynamic DB support in-place atomic updates?

A. It is not defined
B. No
C. Yes
D. It does support in-place non-atomic updates

Answer: C

Explanation:
Q: Does DynamoDB support in-place atomic updates?
Amazon DynamoDB supports fast in-place updates. You can increment or decrement a numeric attribute in a row using a single API call. Similarly, you can atomically add or remove to sets, lists, or maps.
https://aws.amazon.com/dynamodb/faqs/

NEW QUESTION 292
Can I detach the primary (eth0) network interface when the instance is running or stopped?

A. Yes, You can.
B. N
C. You cannot
D. Depends on the state of the interface at the time

Answer: B

Explanation:
Each instance in a VPC has a default elastic network interface (the primary network interface, eth0) that is assigned a private IP address from the IP address range of your VPC. You cannot
detach a primary network interface from an instance.

NEW QUESTION 294

What's an ECU?

A. Extended Cluster User.
B. None of these.
C. Elastic Computer Usage.
D. Elastic Compute Uni

Answer: B

Explanation:
The EC2 Compute Unit (ECU) provides the relative measure of the integer processing power of an Amazon EC2 instance.
https://aws.amazon.com/ec2/faqs/

NEW QUESTION 299
What does the "Server Side Encryption" option on Amazon S3 provide?

A. It provides an encrypted virtual disk in the Cloud.
B. It doesn't exist for Amazon S3, but only for Amazon EC2.
C. It encrypts the files that you send to Amazon S3, on the server side.
D. It allows to upload files using an SSL endpoint, for a secure transfe

Answer: C

Explanation:
Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3- managed encryption keys (SSE-S3) employs strong multi-factor encryption.
Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
References:

NEW QUESTION 302
Within the IAM service a GROUP is regarded as a:

A. A collection of AWS accounts
B. It's the group of EC2 machines that gain the permissions specified in the GROUP.
C. There's no GROUP in IAM, but only USERS and RESOURCES.
D. A collection of user

Answer: D

Explanation:
Use groups to assign permissions to IAM users
Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (administrators, developers, accounting, etc.), define the relevant permissions for each group, and then assign IAM users to those groups. All the users in an IAM group inherit the permissions assigned to the group. That way, you can make changes for everyone in a group in just one place. As people move around in your company, you can simply change what IAM group their IAM user belongs to.
http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-forpermissions

NEW QUESTION 306
A _____ is the concept of allowing (or disallowing) an entity such as a user, group, or role some type of access to one or more resources.

A. user
B. AWS Account
C. resource
D. permission

Answer: D

Explanation:
A permission is the concept of allowing (or disallowing) an entity such as a user, group, or role some type of access to one or more resources.

NEW QUESTION 307
True or False: When you add a rule to a DB security group, you do not need to specify port number or protocol.

A. Depends on the RDMS used
B. TRUE
C. FALSE

Answer: B

Explanation:


DB Security Groups

Each DB security group rule enables a specific source to access a DB instance that is associated with that DB security group. The source can be a range of addresses (e.g., 203.0.113.0/24), or an EC2 security group. When you specify an EC2 security group as the source, you allow incoming traffic from all EC2 instances that use that EC2 security group. Note that DB security group rules apply to inbound traffic only; outbound traffic is not currently permitted for DB instances.

You do not need to specify a destination port number when you create DB security group rules; the port number defined for the DB instance is used as the destination port number for all rules defined for the DB security group. DB security groups can be created using the Amazon RDS APIs or the Amazon RDS page of the AWS Management Console.

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.RDSSecurityGroups.html

NEW QUESTION 308
Can I initiate a "forced failover" for my Oracle Multi-AZ DB Instance deployment?

A. Yes
B. Only in certain regions
C. Only in VPC
D. No

Answer: A

Explanation:
https://aws.amazon.com/public-data-sets/
If your DB instance is a Multi-AZ deployment, you can force a failover from one availability zone to another when you select the Reboot option. When you force a failover of your DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone and updates the DNS record for the DB instance to point to the standby DB instance. As a result, you will need to clean up and re-establish any existing connections to your DB instance. Reboot with failover is beneficial when you want to simulate a failure of a DB instance for testing, or restore operations to the original AZ after a failover occurs.
Source: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RebootInstance.html

NEW QUESTION 313
Amazon EC2 provides a repository of public data sets that can be seamlessly integrated into AWS cloud-based applications. What is the monthly charge for using the public data sets?

A. A 1 time charge of 10$ for all the datasets.
B. 1$ per dataset per month
C. 10$ per month for all the datasets
D. There is no charge for using the public data sets

Answer: D

NEW QUESTION 316
Amazon RDS supports SOAP only through _____ .

A. HTTP or HTTPS
B. TCP/IP
C. HTTP
D. HTTPS

Answer: D

Explanation:
Amazon RDS supports SOAP only through HTTPS
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/using-soap-api.html


WSDL and Schema Definitions

You can access the Amazon Relational Database Service using the SOAP web services messaging protocol. This interface is described by a Web Services Description Language (WSDL) document, which defines the operations and security model for the particular service. The WSDL references an XML Schema document, which strictly defines the data types that might appear in SOAP requests and responses. For more information on WSDL and SOAP, see Web Services References.

Note

Amazon RDS supports SOAP only through HTTPS.

NEW QUESTION 319
Is creating a Read Replica of another Read Replica supported?

A. Only in VPC
B. Yes

C. Only in certain regions
D. No

Answer: D

NEW QUESTION 320
What is the name of licensing model in which I can use your existing Oracle Database licenses to run Oracle deployments on Amazon RDS?

A. Bring Your Own License
B. Role Bases License
C. Enterprise License
D. License Included

Answer: A

Explanation:
https://aws.amazon.com/oracle/

NEW QUESTION 324
When you resize the Amazon RDS DB instance, Amazon RDS will perform the upgrade during the next maintenance window. If you want the upgrade to be performed now, rather than waiting for the maintenance window, specify the ____ option.

A. ApplyNow
B. ApplySoon
C. ApplyThis
D. ApplyImmediately

Answer: D

Explanation:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.DBInstance.Modifying.html

NEW QUESTION 325
If I scale the storage capacity provisioned to my DB Instance by mid of a billing month, how will I be charged?

A. You will be charged for the highest storage capacity you have used
B. On a proration basis
C. You will be charged for the lowest storage capacity you have used

Answer: B

Explanation:
https://aws.amazon.com/ebs/pricing/

NEW QUESTION 328
Will I be alerted when automatic failover occurs?

A. Only if SNS configured
B. No
C. Yes
D. Only if Cloudwatch configured

Answer: A

Explanation:
See http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.html
Amazon RDS uses the Amazon Simple Notification Service (Amazon SNS) to provide notification when an Amazon RDS event occurs. These notifications can be in any notification form supported by
Amazon SNS for an AWS region, such as an email, a text message, or a call to an HTTP endpoint. Amazon RDS groups these events into categories that you can subscribe to so that you can be notified when an event in that category occurs.
C is not correct because even though event is created by RDS you will not be alerted for it unless you configure your subscription in SNS.

NEW QUESTION 331
If you're unable to connect via SSH to your EC2 instance, which of the following should you check and possibly correct to restore connectivity?

A. Adjust Security Group to permit egress traffic over TCP port 443 from your IP.
B. Configure the IAM role to permit changes to security group settings.
C. Modify the instance security group to allow ingress of ICMP packets from your IP.
D. Adjust the instance's Security Group to permit ingress traffic over port 22 from your IP.
E. Apply the most recently released Operating System security patche

Answer: D

Explanation:
In a VPC everything is allowed out by default. References:

NEW QUESTION 336
You are using an m1.small EC2 Instance with one 300 GB EBS volume to host a relational database. You determined that write throughput to the database needs to be increased. Which of the following approaches can help achieve this? (Choose two.)

A. Use an array of EBS volumes.
B. Enable Multi-AZ mode.
C. Place the instance in an Auto Scaling Groups
D. Add an EBS volume and place into RAID 5.
E. Increase the size of the EC2 Instance.
F. Put the database behind an Elastic Load Balance

Answer: AE

NEW QUESTION 340
You have multiple Amazon EC2 instances running in a cluster across multiple Availability Zones within the same region. What combination of the following should be used to ensure the highest network performance (packets per second), lowest latency, and lowest jitter? (Choose three.)

A. Amazon EC2 placement groups
B. Enhanced networking
C. Amazon PV AMI
D. Amazon HVM AMI
E. Amazon Linux
F. Amazon VPC

Answer: BDF

Explanation:
Enhanced Networking enables you to get significantly higher packet per second (PPS) performance,
lower network jitter and lower latencies. This feature uses a new network virtualization stack that provides higher I/O performance and lower CPU utilization compared to traditional implementations. In order to take advantage of Enhanced Networking, you should launch an HVM AMI in VPC, and install the appropriate driver. For instructions on how to enable Enhanced Networking on EC2 instances, see the Enhanced Networking on Linux and Enhanced Networking on Windows tutorials. For availability of this feature by instance, or to learn more, visit the Enhanced Networking FAQ section.

NEW QUESTION 343
When using the following AWS services, which should be implemented in multiple Availability Zones for high availability solutions? Choose 2 answers

A. Amazon DynamoDB
B. Amazon Elastic Compute Cloud (EC2)
C. Amazon Elastic Load Balancing
D. Amazon Simple Notification Service (SNS)
E. Amazon Simple Storage Service (S3)

Answer: BC

NEW QUESTION 348
You have an EC2 Security Group with several running EC2 instances. You change the Security Group rules to allow inbound traffic on a new port and protocol, and launch several new instances in the same Security Group. The new rules apply:

A. Immediately to all instances in the security group.
B. Immediately to the new instances only.
C. Immediately to the new instances, but old instances must be stopped and restarted before the new rules apply.
D. To all instances, but it may take several minutes for old instances to see the changes.

Answer: A

Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#vpc-securitygroups

NEW QUESTION 349
Which services allow the customer to retain full administrative privileges of the underlying EC2 instances? (Choose two.)

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

Answer: BE

NEW QUESTION 353
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

NEW QUESTION 354
Your application provides data transformation services. Files containing data to be transformed are first uploaded to Amazon S3 and then transformed by a fileet 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 leve
B. Transformation instances will scan the table for tasks, sorting the results by priority level.
C. Use Route 53 latency based-routing to send high priority tasks to the closest transformation instances.
D. Use two SQS queues, one for high priority messages, the other for default priorit
E. Transformation instances first poll the high priority queue; if there is no message, they poll the default priorityqueue.
F. Use a single SQS queu
G. Each message contains the priority leve
H. Transformation instances poll high-priority messages first.

Answer: C

NEW QUESTION 357
Which technique can be used to integrate AWS IAM (Identity and Access Management) with an onpremise 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 type

Answer: B

Explanation:
https://d0.awsstatic.com/whitepapers/aws-whitepaper-single-sign-on-integrating-aws-open-ldapand- shibboleth.pdf

NEW QUESTION 358
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 References:

NEW QUESTION 362
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 two.)

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 configuratio

Answer: AB

NEW QUESTION 364
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% durabilit
C. Therefore there is no need to confirm that data was inserted.
D. A success code is inserted into the S3 object metadata.
E. Each S3 account has a special bucket named _s3_log
F. 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

NEW QUESTION 365
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:
Since multi-AZ RDS needs 2 private subnets to provide high availability and 2 public subnets are needed for ELB(web-tier) application.
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.WorkingWithRDSInstancein aVPC.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

NEW QUESTION 370
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 enable

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

NEW QUESTION 372
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

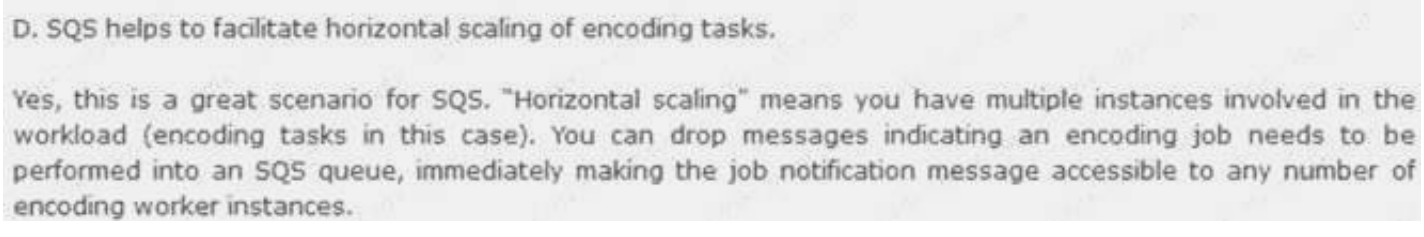
Explanation:
Need to open TCP Port 1024-65535 at Outbound Rules
"Allows outbound responses to the remote computer. Network ACLs are stateless, therefore this rule is required to allow response traffic for inbound requests."
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

NEW QUESTION 373
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 task

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.



NEW QUESTION 377
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 complete

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. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html

NEW QUESTION 380
What are characteristics of Amazon S3? (Choose two.)

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 UR

Answer: CE

NEW QUESTION 385
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 volum

Answer: E

NEW QUESTION 390
Which procedure for backing up a relational database on EC2 that is using a set of RAlDed 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 Instanc
C. 2. Snapshot the EBS volumes
D. 1. Suspend disk I/O, 2. Create an image of the EC2 Instance, 3. Resume disk I/O
E. 1. Suspend disk I/O, 2. Start EBS snapshot of volumes, 3. Resume disk I/O
F. 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/ebsdetaching- 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."

NEW QUESTION 392
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 use

Answer: D

NEW QUESTION 394
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.

NEW QUESTION 398
Which of the following are characteristics of a reserved instance? (Choose three.)

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-reservedinstances. html
https://forums.aws.amazon.com/thread.jspa?threadID=56501

NEW QUESTION 403
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

NEW QUESTION 406
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 delete

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.

NEW QUESTION 410
You have a distributed application that periodically processes large volumes of data across multiple Amazon EC2 Instances. The application is designed to recover gracefully from Amazon EC2 instance failures. You are required to accomplish this task in the most cost-effective way.
Which of the following will meet your requirements?

A. Spot Instances
B. Reserved instances
C. Dedicated instances
D. On-Demand instances

Answer: A

Explanation:
Using reserved instances is not the most cost-effective way. https://aws.amazon.com/blogs/aws/new-scheduled-reserved-instances/
"Scheduled Reserved
Instance model allows you to reserve instances for predefined blocks of time on a recurring basis for a one-year term, with prices that are generally 5 to 10% lower than the equivalent On-Demand rates." You can get spot instances with much lower prices: https://aws.amazon.com/ec2/spot/pricing/
"Spot instances are also available to run for a predefined duration in hourly increments up to six hours in length at a significant discount (30-45%) compared to On-Demand pricing plus an additional 5% during off-peak times for a total of up to 50% savings."

NEW QUESTION 413
Which of the following are true regarding AWS CloudTrail? (Choose three.)

A. CloudTrail is enabled globally
B. CloudTrail is enabled by default
C. CloudTrail is enabled on a per-region basis

D. CloudTrail is enabled on a per-service basis.
E. Logs can be delivered to a single Amazon S3 bucket for aggregation.
F. CloudTrail is enabled for all available services within a region.
G. Logs can only be processed and delivered to the region in which they are generate

Answer: ACE

Explanation:
A: have a trail with the Apply trail to all regions option enabled.
C: have multiple single region trails.
E: Log files from all the regions can be delivered to a single S3 bucket. Global service events are always delivered to trails that have the Apply trail to all regions option enabled. Events are delivered from a single region to the bucket for the trail. This setting cannot be changed. If you have a single region trail, you should enable the Include global services option. If you have multiple single region trails, you should enable the Include global services option in only one of the trails.
D: Incorrect. Once enabled it is applicable for all the supported services, service can't be selected.

NEW QUESTION 418
A company is preparing to give AWS Management Console access to developers Company policy mandates identity federation and role-based access control. Roles are currently assigned using groups in the corporate Active Directory. What combination of the following will give developers access to the AWS console? (Select 2) Choose 2 answers

A. AWS Directory Service AD Connector
B. AWS Directory Service Simple AD
C. AWS Identity and Access Management groups
D. AWS identity and Access Management roles
E. AWS identity and Access Management users

Answer: AD

Explanation:
http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html

NEW QUESTION 423
You are deploying an application to collect votes for a very popular television show. Millions of users will submit votes using mobile devices. The votes must be collected into a durable, scalable, and highly available data store for real-time public tabulation. Which service should you use?

A. Amazon DynamoDB
B. Amazon Redshift
C. Amazon Kinesis
D. Amazon Simple Queue Service

Answer: A

Explanation:
This example looks at using AWS Lambda and Amazon API Gateway to build a dynamic voting application, which receives votes via SMS, aggregates the totals into Amazon DynamoDB, and uses Amazon Simple Storage Service (Amazon S3) to display the results in real time.
http://www.allthingsdistributed.com/2016/06/aws-lambda-serverless-reference-architectures.html

NEW QUESTION 424
A photo-sharing service stores pictures in Amazon Simple Storage Service (S3) and allows application sign-in using an OpenID Connect-compatible identity provider. Which AWS Security Token Service approach to temporary access should you use for the Amazon S3 operations?

A. SAML-based Identity Federation
B. Cross-Account Access
C. AWS Identity and Access Management roles
D. Web Identity Federation

Answer: D

Explanation:
Web identity federation - You can let users sign in using a well-known third party identity provider such as Login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) 2.0 compatible provider. AWS STS web identity federation supports Login with Amazon, Facebook, Google, and any OpenID Connect (OICD)-compatible identity provider.

NEW QUESTION 428
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SAA-C01 Practice Exam Features:

* SAA-C01 Questions and Answers Updated Frequently

* SAA-C01 Practice Questions Verified by Expert Senior Certified Staff

* SAA-C01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SAA-C01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year