WRONG ANSWERS

**Explanations**

1. **An accountant asks you to design a small VPC network for him and due to the nature of his business just needs something where the workload on the network will be low and dynamic data will be accessed infrequently. Being an accountant low cost is also a major factor. Which EBS volume type would best suit his requirements?**

Magnetic

You can choose between three EBS volume types to best meet the needs of their workloads: General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic. General Purpose (SSD) is the new, SSD-backed, general purpose EBS volume type that we recommend as the default choice for customers.

* General Purpose (SSD) volumes are suitable for a broad range of workloads, including small to medium sized databases, development and test environments, and boot volumes.
* Provisioned IOPS (SSD) volumes offer storage with consistent and low-latency performance, and are designed for I/O intensive applications such as large relational or NoSQL databases.
* Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types. **Magnetic volumes are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.**

LEARN MORE: <https://aws.amazon.com/ec2/faqs/>

1. **An organization has three separate AWS accounts, one each for development, testing and production. The organization wants the testing team to have access to certain AWS resources of the production account. How can the organization achieve this?**

Create the IAM roles with cross account access.

Create the IAM user in a test account and allow it access to the production environment with the IAM policy.

An organization has multiple AWS accounts **to isolate a development environment from a testing or production environment**. At times the users from one account need to access resources in the other account, such as promoting an update from the development environment to the production environment. In this case the**IAM role with cross account access will provide a solution**. Cross account access lets one account share access to their resources with users in the other AWS accounts.

LEARN MORE: <http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf>

1. **A user is assigning an elastic IP to an instance when the instance is booted. The user is running AWS CLI inside instance to assign the IP. The AWS CLI requires the AWS credentials to execute the action. Which of the below mentioned options is a possible solution to achieve the above task without compromising on the AWS credentials security?**

Create an IAM user which only has the EC2 assigned IP related permission and use its credentials.

A user can create a specific IAM user which will have access only to the required API. In this case the user can assign IP related permissions to the user. Generate credentials for that user and use it inside the application. The IAM role is the best solution for this. However, the option mentions using the IAM role credentials which is not possible.

LEARN MORE: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

1. **You are setting up your first Amazon Virtual Private Cloud (Amazon VPC) network so you decide you should probably use the AWS Management Console and the VPC Wizard. Which of the following is not an option for network architectures after launching the "Start VPC Wizard" in Amazon VPC page on the AWS Management Console?**

VPC with a Public Subnet Only and Hardware VPN Access

VPC with Public and Private Subnets and Hardware VPN Access

Amazon VPC enables you to build a virtual network in the AWS cloud - no VPNs, hardware, or physical datacenters required.

Your AWS resources are automatically provisioned in a ready-to-use default VPC. You can choose to create additional VPCs by going to Amazon VPC page on the AWS Management Console and click on the "Start VPC Wizard" button.

You’ll be presented with four basic options for network architectures. After selecting an option, you can modify the size and IP address range of the VPC and its subnets. If you select an option with Hardware VPN Access, you will need to specify the IP address of the VPN hardware on your network. You can modify the VPC to add more subnets or add or remove gateways at any time after the VPC has been created.

The four options are:

1. **VPC with a Single Public Subnet Only**
2. **VPC with Public and Private Subnets**
3. **VPC with Public and Private Subnets and Hardware VPN Access**
4. **VPC with a Private Subnet Only and Hardware VPN Access**

LEARN MORE: <https://aws.amazon.com/vpc/faqs/>

1. **You have a lot of data stored in the AWS Storage Gateway and your manager has come to you asking about how the billing is calculated, specifically the Virtual Tape Shelf usage. What would be a correct response to this?**

You are billed for the virtual tape data you store in Amazon Glacier and billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.

The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization’s on-premises IT environment and AWS’s storage infrastructure.

AWS Storage Gateway billing is as follows.

* Volume storage usage (per GB per month):   
  You are billed for the Cached volume data you store in Amazon S3. You are only billed for volume capacity you use, not for the size of the volume you create.
* Snapshot Storage usage (per GB per month): You are billed for the snapshots your gateway stores in Amazon S3. These snapshots are stored and billed as Amazon EBS snapshots. Snapshots are incremental backups, reducing your storage charges. When taking a new snapshot, only the data that has changed since your last snapshot is stored.
* Virtual Tape Library usage (per GB per month):  
  You are billed for the virtual tape data you store in Amazon S3. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
* Virtual Tape Shelf usage (per GB per month):   
  You are billed for the virtual tape data you store in Amazon Glacier. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.

LEARN MORE: <https://aws.amazon.com/storagegateway/faqs/>

1. **An edge location refers to which Amazon Web Service?**

An edge location is the location of the data center used for Amazon CloudFront.

Amazon CloudFront is a content distribution network. A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers across the world. The location of the data center used for CDN is called edge location.

Amazon CloudFront can cache static content at each edge location. This means that your popular static content (e.g., your site’s logo, navigational images, cascading style sheets, JavaScript code, etc.) will be available at a nearby edge location for the browsers to download with low latency and improved performance for viewers. Caching popular static content with Amazon CloudFront also helps you offload requests for such files from your origin sever – CloudFront serves the cached copy when available and only makes a request to your origin server if the edge location receiving the browser’s request does not have a copy of the file.

LEARN MORE: <http://aws.amazon.com/cloudfront/>

1. **You have set up an auto scaling group. The cool down period for the Auto Scaling group is 7 minutes. The first instance is launched after 3 minutes, while the second instance is launched after 4 minutes. How many minutes after the first instance is launched will Auto Scaling accept another scaling activity request?**

11 minutes

7 minutes

Cool down is the wait period between the time a scaling activity ends and another scaling activity can start.

If an Auto Scaling group is launching more than one instance, the cool down period for each instance starts after that instance is launched. The group remains locked until the last instance that was launched has completed its cool down period. In this case the cool down period for the first instance starts after 3 minutes and finishes at the 10th minute (3+7 cool down), while for the second instance it starts at the 4th minute and finishes at the 11th minute (4+7 cool down). Thus, the Auto Scaling group will receive another request only after 11 minutes.

LEARN MORE: <http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html>

1. **You have just finished setting up an advertisement server in which one of the obvious choices for a service was Amazon EMR(Elastic Map Reduce) and are now troubleshooting some weird cluster states that you are seeing. Which of the below is not an Amazon EMR cluster state?**

STOPPED

STARTING

Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data.

Amazon EMR historically referred to an Amazon EMR cluster (and all processing steps assigned to it) as a "cluster". Every cluster or cluster has a unique identifier that starts with "j-".

The different cluster states of an Amazon EMR cluster are listed below.

**STARTING** – The cluster provisions, starts, and configures EC2 instances.  
**BOOTSTRAPPING** – Bootstrap actions are being executed on the cluster.  
**RUNNING** – A step for the cluster is currently being run.  
**WAITING** – The cluster is currently active, but has no steps to run.  
**TERMINATING** - The cluster is in the process of shutting down.  
**TERMINATED** - The cluster was shut down without error.  
**TERMINATED\_WITH\_ERRORS** - The cluster was shut down with errors.

LEARN MORE: <https://aws.amazon.com/elasticmapreduce/faqs/>

1. **You have some very sensitive data stored on AWS S3 and want to try every possible alternative to keeping it secure in regards to access control. What are the mechanisms available for access control on AWS S3?**

(IAM) policies, Access Control Lists (ACLs), bucket policies, and query string authentication.

(IAM) policies, Access Control Lists (ACLs), bucket policies, query string authentication and encryption.

Amazon S3 supports several mechanisms that give you flexibility to control who can access your data as well as how, when, and where they can access it.

Amazon S3 provides four different access control mechanisms:

**AWS Identity and Access Management (IAM) policies, Access Control Lists (ACLs), bucket policies, and query string authentication.**

IAM enables organizations to create and manage multiple users under a single AWS account. With IAM policies, you can grant IAM users fine-grained control to your Amazon S3 bucket or objects. You can use ACLs to selectively add (grant) certain permissions on individual objects.

Amazon S3 bucket policies can be used to add or deny permissions across some or all of the objects within a single bucket.

With Query string authentication, you have the ability to share Amazon S3 objects through URLs that are valid for a specified period of time.

1. **One of your customers is a large multi-national company whose infrastructure on AWS has grown significantly over the past year. The CIO has come to you asking how the huge amount of data that is being generated can be accessed in real-time which would give them a significant edge over all of their competitors. You know that AWS can provide a range of analytics but which of the following would be best to try and accomplish this?**

Amazon Kinesis

Amazon Kinesis is a fully managed service for real-time processing of streaming data at massive scale. Amazon Kinesis can continuously capture and store terabytes of data per hour from hundreds of thousands of sources such as website clickstreams, financial transactions, social media feeds, IT logs, and location-tracking events. With Amazon Kinesis Client Library (KCL), you can build Amazon Kinesis Applications and use streaming data to power real-time dashboards, generate alerts, and implement dynamic pricing and advertising, and more.

LEARN MORE: <http://docs.aws.amazon.com/kinesis/latest/dev/introduction.html>

1. **One of the criteria for a new deployment is that the customer wants to use AWS Storage Gateway. However you are not sure whether you should use gateway-cached volumes or gateway-stored volumes or even what the differences are. Which statement below best describes those differences?**

Gateway-stored lets you store your data locally in storage volumes whilst gateway-cached lets you create storage volumes and mount them iSCSI devices.

AWS Storage Gateway offers two volume-based storage solutions, gateway-cached volumes and gateway-stored volumes.

The gateway-stored solution lets you store all your data locally in storage volumes on your on-premises storage hardware. In this solution, the gateway periodically takes snapshots as incremental backups and stores them in Amazon S3.

The gateway-cached solution lets you create storage volumes and mount them as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers. In this solution, the gateway stores data you write to your gateway-cached volume in Amazon Simple Storage Service (Amazon S3) and stores only a cache of frequently accessed data on your on-premises storage hardware.

LEARN MORE: <http://docs.aws.amazon.com/storagegateway/latest/userguide/volume-gateway.html>

1. **You are building a system to distribute confidential documents to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publically accessible from S3 directly?**

Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.

You restrict access to Amazon S3 content by creating an Origin Access Identity, which is a special CloudFront user. You change Amazon S3 permissions to give the origin access identity permission to access your objects, and to remove permissions from everyone else. When your users access your Amazon S3 objects using CloudFront URLs, the CloudFront origin access identity gets the objects on your users' behalf. If your users try to access objects using Amazon S3 URLs, they're denied access. The origin access identity has permission to access objects in your Amazon S3 bucket, but users don't.

LEARN MORE: <http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

1. **A friend wants you to set up a small BitTorrent storage area for him on Amazon S3. You tell him it is highly unlikely that AWS would allow such a thing in their infrastructure. However you decide to investigate. Which of the following statements best describes using BitTorrent with Amazon S3?**

You can use the BitTorrent protocol but only for objects that are less than 5 GB in size.

Amazon S3 does not support the BitTorrent protocol because it is used for pirated software.

BitTorrent is an open, peer-to-peer protocol for distributing files. You can use the BitTorrent protocol to retrieve any publicly-accessible object in Amazon S3.

Amazon S3 supports the BitTorrent protocol so that developers can save costs when distributing content at high scale. Amazon S3 is useful for simple, reliable storage of any data. The default distribution mechanism for Amazon S3 data is via client/server download. In client/server distribution, the entire object is transferred point-to-point from Amazon S3 to every authorized user who requests that object. While client/server delivery is appropriate for a wide variety of use cases, it is not optimal for everybody. Specifically, the costs of client/server distribution increase linearly as the number of users downloading objects increases. This can make it expensive to distribute popular objects.

BitTorrent addresses this problem by recruiting the very clients that are downloading the object as distributors themselves: Each client downloads some pieces of the object from Amazon S3 and some from other clients, while simultaneously uploading pieces of the same object to other interested "peers." The benefit for publishers is that for large, popular files the amount of data actually supplied by Amazon S3 can be substantially lower than what it would have been serving the same clients via client/server download. Less data transferred means lower costs for the publisher of the object.

LEARN MORE: <http://docs.aws.amazon.com/AmazonS3/latest/dev/S3Torrent.html>

1. **A user is planning to launch a scalable web application. Which of the below mentioned options will not affect the latency of the application?**

Availability Zone.

Instance size.

* In AWS, **the instance size decides the I/O characteristics**. The provisioned IOPS ensures higher throughput, and lower latency.
* The region does affect the latency; latency will always be less when the instance is near to the end user.
* Within a region the user uses any AZ and this does not affect the latency. The AZ is mainly for fault toleration or HA.

LEARN MORE: <http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf>

1. **You are planning and configuring some EBS volumes for an application. In order to get the most performance out of your EBS volumes, you should attach them to an instance with enough \_\_\_\_\_\_\_\_ to support your volumes.**

Bandwidth

Storage

When you plan and configure EBS volumes for your application, it is important to consider the configuration of the instances that you will attach the volumes to. In order to get the most performance out of your EBS volumes, you should attach them to an instance with enough bandwidth to support your volumes, such as an EBS-optimized instance or an instance with 10 Gigabit network connectivity. This is especially important when you use General Purpose (SSD) or Provisioned IOPS (SSD) volumes, or when you stripe multiple volumes together in a RAID configuration.

LEARN MORE: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-ec2-config.html>

1. **Doug has created a VPC with CIDR 10.201.0.0/16 in his AWS account. In this VPC he has created a public subnet with CIDR block 10.201.31.0/24. While launching a new EC2 from the console he is not able to assign the private IP address 10.201.31.6 to this instance. Which might be the more likely reason for this issue?**

Private address IP 10.201.31.6 is currently assigned to another interface

In Amazon VPC, you can assign any Private IP address to your instance as long as it is:

* Part of the associated subnet's IP address range
* Not reserved by Amazon for IP networking purposes
* Not currently assigned to another interface

LEARN MORE: <http://aws.amazon.com/vpc/faqs/>

1. **A user is running a batch process which runs for 1 hour every day. Which of the below mentioned options is the right instance type and costing model in this case if the user performs the same task for the whole year?**

EBS backed instance with on-demand instance pricing.

EBS backed instance with low utilized reserved instance pricing.

For Amazon Web Services, the reserved instance helps the user save money if the user is going to run the same instance for a longer period. Generally if the user uses the instances around 30-40% annually it is recommended to use RI. Here as the instance runs only for 1 hour daily it is not recommended to have RI as it will be costlier. The user should use on-demand with EBS in this case.

LEARN MORE: <http://aws.amazon.com/ec2/purchasing-options/reserved-instances/>

1. **You have been requested to tighten up the password policies in your organization after a serious security breach. So you need to consider every possible security measure. Which of the following is not an account password policy for IAM Users that can be set?**

Force IAM users to contact an account administrator when the user has entered his password incorrectly.

Allow all IAM users to change their own passwords.

IAM users need passwords in order to access the AWS Management Console. (They do not need passwords if they will access AWS resources programmatically by using the CLI, AWS SDKs, or the APIs.)

You can use a password policy to do these things:

* Set a minimum password length.
* Require specific character types, including uppercase letters, lowercase letters, numbers, and non-alphanumeric characters. Be sure to remind your users that passwords are case sensitive.
* Allow all IAM users to change their own passwords.
* Require IAM users to change their password after a specified period of time (enable password expiration).
* Prevent IAM users from reusing previous passwords.
* Force IAM users to contact an account administrator when the user has allowed his or her password to expire.

LEARN MORE: <http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_ManagingPasswordPolicies.html>

1. **You are architecting an auto-scalable batch processing systems using video processing pipelines and Amazon Simple Queue Service (Amazon SQS) for a customer. You are however unsure of the limitations of SQS and need to find out. What do you think is a correct statement about the limitations of Amazon SQS?**

It supports an unlimited number of queues and unlimited number of messages per queue for each user but automatically deletes messages that have been in the queue for more than 4 days.

It supports an unlimited number of queues but a limited number of messages per queue for each user but automatically deletes messages that have been in the queue for more than 4 weeks.

Amazon Simple Queue Service (Amazon SQS) is a messaging queue service that handles message or workflows between other components in a system.

Amazon SQS supports an unlimited number of queues and unlimited number of messages per queue for each user.Please be aware that Amazon SQS automatically deletes messages that have been in the queue for more than 4 days.

LEARN MORE: <http://aws.amazon.com/documentation/sqs/>

1. **You need to import several hundred megabytes of data from a local Oracle database to an Amazon RDS DB instance. What does AWS recommend to use to accomplish this?**

Oracle Data Pump

Oracle Export/Import utilities

How you import data into an Amazon RDS DB instance depends on the amount of data you have and the number and variety of database objects in your database.

For example, you can use Oracle SQL Developer to import a simple, 20 MB database; you want to use **Oracle Data Pump** to import complex databases or databases that are several hundred megabytes or several terabytes in size.

LEARN MORE: <http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Oracle.Procedural.Importing.html>

1. **After a major security breach your manager has requested a report of all users and their credentials in AWS. You discover that in IAM you can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, MFA devices, and signing certificates. Which following statement is incorrect in regards to the use of credential reports?**

Credential reports are downloaded XML files.

To access your AWS account resources, users must have credentials.

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, MFA devices, and signing certificates. You can get a credential report using the AWS Management Console, the AWS CLI, or the IAM API.

You can use credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password rotation. You can provide the report to an external auditor, or grant permissions to an auditor so that he or she can download the report directly.

You can generate a credential report as often as once every four hours. When you request a report, IAM first checks whether a report for the account has been generated within the past four hours. If so, the most recent report is downloaded. If the most recent report for the account is more than four hours old, or if there are no previous reports for the account, IAM generates and downloads a new report.

**Credential reports are downloaded as comma-separated values (CSV) files.**

You can open CSV files with common spreadsheet software to perform analysis, or you can build an application that consumes the CSV files programmatically and performs custom analysis.

LEARN MORE: <http://docs.aws.amazon.com/IAM/latest/UserGuide/credential-reports.html>

1. **A customer enquires about whether all his data is secure on AWS and is especially concerned about Elastic Map Reduce(EMR) so you need to inform him of some of the security features in place for AWS. Which of the below statements would be an incorrect response to your customers enquiry?**

Every packet sent in the AWS network uses Internet Protocol Security (IPsec)

* Amazon S3 provides authentication mechanisms to ensure that stored data is secured against unauthorized access. Unless the customer who is uploading the data specifies otherwise, only that customer can access the data.
* Amazon EMR customers can also choose to send data to Amazon S3 using the HTTPS protocol for secure transmission. In addition, Amazon EMR always uses HTTPS to send data between Amazon S3 and Amazon EC2.
* For added security, customers may encrypt the input data before they upload it to Amazon S3 (using any common data compression tool); they then need to add a decryption step to the beginning of their cluster when Amazon EMR fetches the data from Amazon S3.

LEARN MORE: <https://aws.amazon.com/elasticmapreduce/faqs/>

1. **A user has configured a website and launched it using the Apache web server on port 80. The user is using ELB with the EC2 instances for Load Balancing. What should the user do to ensure that the EC2 instances accept requests only from ELB?**

Configure the security group of EC2, which allows access to the ELB source security group

When a user is configuring ELB and registering the EC2 instances with it, ELB will create a source security group. If the user wants to allow traffic only from ELB, he should remove all the rules set for the other requests and open the port only for the ELB source security group.

LEARN MORE: <http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/using-elb-security-groups.html>

1. **You have just built an Amazon Relational Database Service(RDS) and you now need to set up a high level of security for this database as it is very confidential information so you need to find out all the possible options that are available for security. What security groups does Amazon RDS use?**

DB security groups, VPC security groups, and EC2 security groups

A security group controls the access to a DB instance. It does so by allowing access to IP address ranges or Amazon EC2 instances that you specify.

**Amazon RDS uses DB security groups, VPC security groups, and EC2 security groups.** In simple terms, a DB security group controls access to a DB instance that is not in a VPC, a VPC security group controls access to a DB instance inside a VPC, and an Amazon EC2 security group controls access to an EC2 instance and can be used with a DB instance.

LEARN MORE: <http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

1. **You have sent a portable storage device to AWS to import to Amazon S3. You want the data spread across different buckets and you are unsure of how your files will be mapped to Amazon S3 objects. Which statement below best summarises AWS's policy on Import/Export?**

Data loads are restricted to one bucket per job and each filename on your storage device is mapped to an Amazon S3 key name based on its full path.

Data loads are not restricted to one bucket per job and each filename on your storage device is mapped to an Amazon S3 key name based on its full path.

AWS Import/Export accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS transfers your data directly onto and off of storage devices using Amazon’s high-speed internal network and bypassing the Internet. For significant data sets, AWS Import/Export is often faster than Internet transfer and more cost effective than upgrading your connectivity.

Data loads are restricted to **one bucket per job.**

Each filename on your storage device is mapped to an **Amazon S3 key name based on its full path.**For example if your storage device has a file located at “mydir/myfile”, the key will be name “mydir/myfile”. A forward slash ‘/’ is always used as the directory separator when mapping your filename to a key name. The Create Job request can include instructions for adding a prefix to each key and setting the following object attributes: Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Type, Expires, and x-amz-acl.

LEARN MORE: <https://aws.amazon.com/importexport/faqs/>

1. **You need to create a management network using network interfaces for a virtual private cloud (VPC) network. Which of the following statements is incorrect pertaining to Best Practices for Configuring Network Interfaces.**

Attaching another network interface to an instance is a valid method to increase or double the network bandwidth to or from the dual-homed instance

You can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach).

**Best Practices for Configuring Network Interfaces**

* You can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach).
* You can detach secondary (ethN) network interfaces when the instance is running or stopped. However, you can't detach the primary (eth0) interface.
* You can attach a network interface in one subnet to an instance in another subnet in the same VPC, however, both the network interface and the instance must reside in the same Availability Zone.
* When launching an instance from the CLI or API, you can specify the network interfaces to attach to the instance for both the primary (eth0) and additional network interfaces.
* Launching an instance with multiple network interfaces automatically configures interfaces, private IP addresses, and route tables on the operating system of the instance.
* A warm or hot attach of an additional network interface may require you to manually bring up the second interface, configure the private IP address, and modify the route table accordingly. (Instances running Amazon Linux automatically recognize the warm or hot attach and configure themselves.)
* Attaching another network interface to an instance is not a method to increase or double the network bandwidth to or from the dual-homed instance.

LEARN MORE: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#use-network-and-security-appliances-in-your-vpc>

1. **You have multiple VPN connections and want to provide secure communication between sites using the AWS VPN CloudHub. Which statement is the most accurate in describing what you must do to set this up correctly?**

Create a Virtual Private Gateway with multiple customer gateways, each with unique Border Gateway Protocol (BGP) Autonomous System Numbers (ASNs)

If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who'd like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.

To use the AWS VPN CloudHub, you must **create a virtual private gateway with multiple customer gateways, each with unique Border Gateway Protocol (BGP) Autonomous System Numbers (ASNs). Customer gateways advertise the appropriate routes (BGP prefixes) over their VPN connections**. These routing advertisements are received and re-advertised to each BGP peer, enabling each site to send data to and receive data from the other sites. The routes for each spoke must have unique ASNs and the sites must not have overlapping IP ranges. Each site can also send and receive data from the VPC as if they were using a standard VPN connection.

LEARN MORE: <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html>

1. **A very important Government client needs you to set up secure cryptographic key storage for some of their extremely confidential data. You decide that the AWS CloudHSM is the best service for this however there seems to be a few pre-requisites before this can happen. One of those being a security group that has certain ports open. Which of the following is correct in regards to those security groups?**

A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network.

AWS CloudHSM provides secure cryptographic key storage to customers by making hardware security modules (HSMs) available in the AWS cloud.

AWS CloudHSM requires the following environment (**pre-requisites) before** an HSM appliance can be provisioned.

* A virtual private cloud (VPC) in the region where you want the AWS CloudHSM service.
* One private subnet (a subnet with no Internet gateway) in the VPC. The HSM appliance is provisioned into this subnet.
* One public subnet (a subnet with an Internet gateway attached). The control instances are attached to this subnet.
* An AWS Identity and Access Management (IAM) role that delegates access to your AWS resources to AWS CloudHSM
* An EC2 instance, in the same VPC as the HSM appliance, that has the SafeNet client software installed. This instance is referred to as the control instance and is used to connect to and manage the HSM appliance.
* **A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network.** This security group is attached to your control instances so you can access them remotely.

1. **You have just set up a large site for a client which involved a huge database which you set up with Amazon RDS to run as a Multi-AZ deployment. You now start to worry about what will happen if the database instance fails. Which statement best describes how this database will function if there is a database failure?**

Updates to your DB Instance are **synchronously** replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure.

Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity, while managing time-consuming database administration tasks, freeing you up to focus on your applications and business.

When you create or modify your DB Instance to run as a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous “standby” replica in a different Availability Zone.   
**Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure.**   
During certain types of planned maintenance, or in the unlikely event of DB Instance failure or Availability Zone failure, Amazon RDS will automatically failover to the standby so that you can resume database writes and reads as soon as the standby is promoted. Since the name record for your DB Instance remains the same, you application can resume database operation without the need for manual administrative intervention. With Multi-AZ deployments, replication is transparent: you do not interact directly with the standby, and it cannot be used to serve read traffic. If you are using Amazon RDS for MySQL and are looking to scale read traffic beyond the capacity constraints of a single DB Instance, you can deploy one or more Read Replicas.

LEARN MORE: <http://aws.amazon.com/rds/faqs/>

1. **A user is making a scalable web application with compartmentalization. The user wants to achieve that the log module will be accessed by all the application functionalities in an asynchronous way. Each module of the application sends data to the log module and based on the resource availability it will process the logs. Which AWS service helps this functionality?**

AWS Simple Queue Service.

**Amazon Simple Queue Service (SQS)** is a highly reliable distributed messaging system for storing messages as they travel between computers. By using Amazon SQS, developers can simply move data between distributed application components. It is used to achieve compartmentalization or loose coupling. In this case all the modules will send a message to the logger queue and the data will be processed by queue as per the resource availability.

LEARN MORE: <http://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf>

1. **You have been using T2 instances as your CPU requirements have not been that intensive. However you now start to think about larger instance types and start lookig at M1 and M3 instances. You are a little confused as to the differences between them as they both seem to have the same ratio of CPU and memory. Which statement below is incorrect as to why you would use one over the other?**

M3 instances are configured with more swap memory than M1 instances.

M3 instances also offer SSD-based instance storage that delivers higher I/O performance.

Amazon EC2 allows you to set up and configure everything about your instances from your operating system up to your applications. An Amazon Machine Image (AMI) is simply a packaged-up environment that includes all the necessary bits to set up and boot your instance.

M1 and M3 Standard instances have the same ratio of CPU and memory, some reasons below as to why you would use one over the other.

* M3 instances provide better, more consistent performance that M1 instances for most use-cases.
* M3 instances also offer SSD-based instance storage that delivers higher I/O performance.
* M3 instances are also less expensive than M1 instances. Due to these reasons, we recommend M3 for applications that require general purpose instances with a balance of compute, memory, and network resources.
* However, if you need more disk storage than what is provided in M3 instances, you may still find M1 instances useful for running your applications.

LEARN MORE: <https://aws.amazon.com/ec2/faqs/>

1. **You need to establish a dedicated network connection from your premises to AWS as you think this may save you some money by not needing to go via your internet provider so much. You are sure there must be some other benefits. Which of the following would not be considered a benefit if you were to establish such a connection?**

Everything listed is a benefit.

Compatible with all AWS Services

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS.

Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

You could expect the following benefits if you use AWS Direct Connect.

* Reduces Your Bandwidth Costs
* Consistent Network Performance
* Compatible with all AWS Services
* Private Connectivity to your Amazon VPC
* Elasticity
* Simpler

LEARN MORE: <http://aws.amazon.com/directconnect/>

1. **You are architecting a highly-scalable and reliable web application which will have a huge amount of content .You have decided to use Cloudfront as you know it will speed up distribution of your static and dynamic web content and know that Amazon CloudFront integrates with Amazon CloudWatch metrics so that you can monitor your web application. Because you live in Sydney you have chosen the the Asia Pacific (Sydney) region in the AWS console. However you have set up this up but no CloudFront metrics seem to be appearing in the CloudWatch console. What is the most likely reason from the possible choices below for this?**

Metrics for CloudWatch are available only when you choose the US East (N. Virginia)

Metrics for CloudWatch are available only when you choose the same region as the application you are monitoring.

CloudFront is a global service, and metrics are available only when you choose the US East (N. Virginia) region in the AWS console. If you choose another region, no CloudFront metrics will appear in the CloudWatch console.

LEARN MORE: <http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/monitoring-using-cloudwatch.html>

1. **As AWS grows most of your clients main concerns seem to be about security especially when all of their competitors seem to be using AWS also. Consequently one of your clients asks you if one of your competitors EC2 instances are on the same physical host would that make it easier for them to hack into your data. Which of the following statements would be the best choice to put your clients mind at rest?**

Different instances running on the same physical machine are isolated from each other via the Xen hypervisor.

Different instances running on the same physical machine are isolated from each other via the Xen hypervisor and via a 256-bit Advanced Encryption Standard (AES-256).

Amazon Elastic Compute Cloud (EC2) is a key component in Amazon’s Infrastructure as a Service (IaaS), providing resizable computing capacity using server instances in AWS’s data centers. Amazon EC2 is designed to make web-scale computing easier by enabling you to obtain and configure capacity with minimal friction.

You create and launch instances, which are collections of platform hardware and software.  
**Different instances running on the same physical machine are isolated from each other via the Xen hypervisor.**

Amazon is active in the Xen community, which provides awareness of the latest developments. In addition, the AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance’s neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.

LEARN MORE: <http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf>

1. **You have been given a scope to deploy some AWS infrastructure for a large organization. The requirements are that you will have a lot of EC2 instances but may need to add more when the average utilization of your Amazon EC2 fleet is high and conversely remove them when CPU utilization is low. Which AWS services would be best to use to accomplish this?**

Auto Scaling, Amazon CloudWatch and Elastic Load Balancing.

Auto Scaling, Amazon CloudWatch and AWS Elastic Beanstalk

* Auto Scaling enables you to follow the demand curve for your applications closely, reducing the need to manually provision Amazon EC2 capacity in advance. For example, you can set a condition to add new Amazon EC2 instances in increments to the Auto Scaling group when the average utilization of your Amazon EC2 fleet is high; and similarly, you can set a condition to remove instances in the same increments when CPU utilization is low. If you have predictable load changes, you can set a schedule through Auto Scaling to plan your scaling activities.
* You can use **Amazon CloudWatch** to send alarms to trigger scaling activities and
* **Elastic Load Balancing** to help distribute traffic to your instances within Auto Scaling groups. **Auto Scaling** enables you to run your Amazon EC2 fleet at optimal utilization.

LEARN MORE: <http://aws.amazon.com/autoscaling/>

1. **Your company has multiple IT departments, each with their own VPC. Some VPCs are located within the same AWS account, and others in a different AWS account. You want to peer together all VPCs to enable the IT departments to have full access to each others' resources. There are certain limitation placed on VPC peering. Which of the following statements is incorrect in relation to VPC peering?**

You can have up to 3 VPC peering connections between the same two VPCs at the same time.

To create a VPC peering connection with another VPC, you need to be aware of the following limitations and rules:

* You cannot create a VPC peering connection between VPCs that have matching or overlapping CIDR blocks.
* You cannot create a VPC peering connection between VPCs in different regions.
* You have a limit on the number active and pending VPC peering connections that you can have per VPC.   
  VPC peering does not support transitive peering relationships; in a VPC peering connection, your VPC will not have access to any other VPCs that the peer VPC may be peered with. This includes VPC peering connections that are established entirely within your own AWS account.
* **You cannot have more than one VPC peering connection between the same two VPCs at the same time.**
* The Maximum Transmission Unit (MTU) across a VPC peering connection is 1500 bytes.
* A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs.
* Unicast reverse path forwarding in VPC peering connections is not supported.
* You cannot reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group. Instead, reference CIDR blocks of the peer VPC as the source or destination of your security group's ingress or egress rules.
* Private DNS values cannot be resolved between instances in peered VPCs.

LEARN MORE: <http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-overview.html#vpc-peering-limitations>

1. **You have been asked to set up a database in AWS that will require frequent and granular updates. You know that you will require a reasonable amount of storage space but are not sure of the best option. What is the recommended storage option when you run a database on an instance with the above criteria?**

Amazon EBS

Amazon S3

* Amazon EBS provides durable, block-level storage volumes that you can attach to a running Amazon EC2 instance.
* You can use Amazon EBS as a primary storage device for data that requires frequent and granular updates. For example, Amazon EBS is the recommended storage option when you run a database on an instance.

LEARN MORE: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Storage.html>

1. **Your organization is in the business of architecting complex transactional databases and this for a variety of reasons has been done on EBS. What is AWS's recommendation for customers who have architected databases using EBS for backups?**

Backups to Amazon S3 be performed through the database management system .

If you take regular snapshots no further backups are required.

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge.

However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.

**For customers who have architected complex transactional databases using EBS, it is recommended that backups to Amazon S3 be performed through the database management system so that distributed transactions and logs can be check pointed.**

AWS does not perform backups of data that are maintained on virtual disks attached to running instances on Amazon EC2.

LEARN MORE: <http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf>

1. **You are in the process of building an Online Game site for a client and one of the requirements is that it must be able to process vast amounts of data easily. Which AWS Service would be very helpful in processing all this data?**

Amazon EMR

Amazon S3

Managing and analyzing high data volumes produced by online games platforms can be difficult. Online games back-end infrastructures can be challenging to maintain and operate. Peak usage periods, multiple players, and high volumes of write operations are some of the most common problems that operations teams face.

**Amazon Elastic MapReduce (Amazon EMR)** is a service that processes vast amounts of data easily. Input data can be retrieved from web server logs stored on Amazon S3 or from player data stored in Amazon DynamoDB tables to run analytics on player behavior, usage patterns, etc. Those results can be stored again on Amazon S3, or inserted in a relational database for further analysis with classic business intelligence tools.

LEARN MORE: <http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_games_10.pdf>

1. **Your EBS volumes do not seem to be performing as expected and your team leader has requested you look into improving their performance. Which of the following is not a true statement relating to the performance of your EBS volumes?**

Frequent snapshots provide a higher level of data durability and they will not degrade the performance of your application while the snapshot is in progress.

General Purpose (SSD) and Provisioned IOPS (SSD) volumes have a throughput limit of 128 MB/s per volume.

Several factors can affect the performance of Amazon EBS volumes, such as instance configuration, I/O characteristics, workload demand, and storage configuration.

* **Frequent snapshots provide a higher level of data durability, but they may slightly degrade the performance of your application while the snapshot is in progress.** This trade off becomes critical when you have data that changes rapidly. Whenever possible, plan for snapshots to occur during off-peak times in order to minimize workload impact.

LEARN MORE: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html>

1. **An organization has a statutory requirement to protect the data at rest for the S3 objects. Which of the below mentioned options need not be enabled by the organization to achieve data security?**

Data replication

MFA delete for S3 objects

AWS S3 provides multiple options to achieve the protection of data at REST. The options include **Permission** (Policy), **Encryption** (Client and Server Side), **Bucket Versioning**and**MFA** **based delete**. The user can enable any of these options to achieve data protection. Data replication is an internal facility by AWS where S3 replicates each object across all the Availability Zones and the organization need not enable it in this case.

LEARN MORE: <http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf>

1. **An EC2 instance is connected to an ENI (Elastic Network Interface) in one subnet. What happens when you attach an ENI of a different subnet to this EC2 instance?**

The EC2 instance follows the rules of both the subnets

* AWS allows you create an elastic network interface (ENI), attach an ENI to an EC2 instance, detach an ENI from an EC2 instance and attach this ENI to another EC2 instance.
* The attributes of a network traffic follow the ENI which is attached to an EC2 instance or detached from an EC2 instance.
* When you move an ENI from one EC2 instance to another, network traffic is redirected to the new EC2 instance. You can create and attach additional ENIs to an EC2 instance.

Attaching multiple network interfaces (ENIs) to an EC2 instance is useful to:

* Create a management network.
* Use network and security appliances in your VPC.
* Create dual-homed instances with workloads/roles on distinct subnets
* Create a low-budget, high-availability solution.

LEARN MORE: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>

1. **Having just set up your first Amazon Virtual Private Cloud (Amazon VPC) network which defined a default network interface you decide that you need to create and attach an additional network interface, known as an elastic network interface (ENI) to one of your instances. Which of the following statements is true regarding attaching network interfaces to your instances in your VPC?**

The number of ENIs you can attach varies by instance type.

You can only attach 1 ENI per instance type.

Each instance in your VPC has a default network interface that is assigned a private IP address from the IP address range of your VPC. You can create and attach an additional network interface, known as an elastic network interface (ENI), to any instance in your VPC. **The number of ENIs you can attach varies by instance type.**