* AWS is made up of regions which are a grouping of independently separated data centers in specific geographic regions known as “Availability Zones”.
* Availability zones work together in a region to make up a collection of your AWS resources. Properly designing applications will utilize multiple availability zones for fault tolerance and failover. AZ’s have direct low latency connections between each AZ in a region but each AZ is isolated from other AZ’s to ensure fault tolerance.
* An edge location is an AWS datacenter which does not contain AWS services. It is used to deliver content to parts of the world. An example would be CloudFront which is a CDN. Cached items such as a PDF file can be cached on an edge location which reduces the amount of “space/time/latency” required for a request from that part of the world.
* VPC allows for the isolation of AWS resources in the cloud. Resources fired up in a single VPC will be part of the same network can communicate internally. However, if multiple VPCs are used to provision resources then resources in one VPC are completely isolated from the other VPC by default. Resource sharing between VPCs in the same region can be allowed with VPC peering.
* Simple Storage Service (S3) is an object storage service from AWS. It can not only serve objects through a CDN to CloudFront, manage access to specific objects, enable versioning, and lifecycle policies, but it can also serve static HTML files with Route 53. It is a simple key-value store designed for unlimited object storage. Designed for “11 nines” durability and 99.99% availability. Data transfer from S3 to an EC2 instance within the same region is free. S3 objects can be encrypted using the S3 encryption option as well as data sent to and from end points are encrypted using the HTTPS protocol. Bucket names are unique across the entire S3 design.
* Amazon Storage Gateway: Connects local data center software appliances to cloud based storage such as Amazon S3. We can achieve this by using Gateway-Cached volumes and Gateway-Stored volumes.

Gateway-Cached Volumes: Create storage volumes and mount them as iSCSI devices on the

On-premise servers. The gateway will store the data written to this volume in Amazon S3 and will cache frequently access data On-premise in the storage device.

Gateway-Stored Volumes: Store all the data locally in storage volumes. Gateway will periodically take snapshots of the data as incremental backups and stores them on Amazon S3

* If there is an “explicit deny” in any of the policies associated with the user, then it will deny access regardless of allow associated with other groups/policies
* S3 provides unlimited storage. Objects can be small as 0Bytes and as large as 5TB. Only 100 buckets can be created in an aws account at a time. Bucket ownership cannot be transferred once a bucket is created. All buckets and objects are private by default. ACL’s (Can share accounts across accounts with ACLs).
* We can implement Bucket policies in S3 storage. Bucket policies are used for permissions such as granting access to an anonymous user, restricting access based off of IP address, restricting access based off of HTTP referrer.
* S3 Supports Multipart upload: Allows for uploading part of a file concurrently. Allows for stopping/resuming file uploads. Object stay within an AWS region is synced across all AZ’s.
* All regions now support read-after-write consistency for PUTS of new objects into S3. All regions use eventual consistency for PUTS overwriting existing objects and DELETES of objects.
* EC2 instance sizes will vary in the amount of network capacity and other limitations such as number of Elastic Network Interfaces (ENI) able to be attached to an instance.
* EC2 instances can be created with two “types” of storage: Instance-store volume, EBS backed volume.

Instance store volumes are considered (ephemeral data) the data on the volumes only exists for the duration of the instance life. Once the instance is “stopped” or “shutdown” the data is erased. The instance can be rebooted and still maintain its ephemeral data. Instance-store volumes are virtual devices whose underlying hardware is physically attached to the host computer for the instance.

EBS backed volumes are network attached storage. Provide persistent data across EC2 instances even if they are shutdown. We can attach multiple EBS volumes to single instance. You can attach one EBS volume to one instance at a time. EBS volumes contain IOPS which are input/output operations per second. An IOP is 256 KB or smaller. Operations that are greater than256KB are separated into 256KB units.

* EBS volume types:

General Purpose SSD: Commonly used as the “root” volume on a system. 3 IOPS/GiB (burstable with baseline performance). Volume size of 1GiB to 16 TiB.

Provisioned IOPS: Mission critical applications that require sustained IOPS performance. Volume size of 4GiB to 16TiB. Performs at provisioned level and can provision up to 20,000 IOPS.

Magnetic: Low storage cost. Workloads where performance is not important or data is infrequently accessed. Volume size of Min 1GiB Max 1024 GiB.

* EBS snapshots will be stored in S3. When a snapshot is being taken against the EBS volume, it can degrade performance. So snapshots should occur during non-production or non-peak load hours.
* Security Groups: We can have 500 security groups per VPC. Each security group can have up to 50 rules. You can apply 5 security groups per EC2 network interface. By default all rules are denied unless specifically allowed, you cannot create deny rules. Responses to inbound traffic are allowed REGARDLESS of outbound rules (stateful) same applies to outbound traffic. Instances associated with a security group cannot communicate with each other unless the ports are open to those instances; one exception is the default security group.
* Placement Groups: A placement group is a cluster of instances within the same availability zones. Instances within a placement group have a low-latency, 10 Gbps network connections between them. Used for instances that run applications whose requirements are an extremely low latency network between them. Instances not originally launched/created in the placement group cannot be moved into the placement group. You can create an AMI from your existing instance, and then launch a new instance from the AMI into a placement group. Placement groups cannot be merged together but, they can be connected to have low latency connection between instances within multiple placement groups. A placement group cannot span multiple availability zones. Placement group names must be unique within your own AWS account.
* Bastion Host: A bastion host sits on the “outside” of an internal network and is used as a gateway into the private network and is considered the “critical strong point” of the network. The bastion host will maintain extremely tight security and monitoring as it is available to the public. A bastion host is to “ssh” into the internal network to access private resources without a VPN.
* VPC peering enables the ability to create direct network route between one VPC and another. This allows the sharing of resources between two subnets as if it was on the same network. Basically, at a high level it creates a link between the two. VPC peering can occur between the other AWS accounts and other VPCs within the same region. VPC peering connection cannot occur between two regions. We can have 5 VPCs per region, 5 internet gateways, 200 route tables per region/50 entries per route table, 500 security groups per VPC, 50 rules per security group.
* When you create VPC, it automatically creates route table.
* VPC Networking: Each subnet must be associated with a route table; however each subnet can be associated with only one route table. By default all subnets traffic is allowed to each other available subnet within your VPC which is called the local route. You cannot modify the local rule
* To enable access to or from the internet for instances in a VPC subnet, you must attach an internet gateway to your VPC, ensure that your subnet’s route table points to the internet Gateway, ensure that instance in your subnet have a public IP address or Elastic IP address, and ensure that your network access control and security group rules allow the relevant traffic to and from your instance.
* Kinesis is a real-time data processing service that continuously captures and stores large amount of data to power real time streaming dash boards of incoming data streams. Kinesis dashboards can be creating using the AWS provided SDKs and can create real-time dashboards, integrate dynamic pricing strategies, and also allows you to export data from kinesis to other AWS services for storage. Including EMR, S3, Redshift, and Lambda. Kinesis keeps 24 hours of streaming data stored by default, but can be configured to store up to 7 days.
* CloudFront is a global CDN which delivers content from and “origin” location to an “edge” location. An origin can be an S3 bucket or an Elastic Load Balancer CNAME that distributes requests among origin instances. Signed URLs can allow access to “private content” by creating a temporary one time use URL based off of the number of seconds it is supposed to be available. CloudFront can integrate with Route 53 for “alternate” cnames. This allows you to create a URL such as <http://cdn.mydomain.com> that works with your distribution.
* CloudFront is designed for caching, if caching is enabled then CloudFront will serve the cached file stored on the edge location until cache expires. In order to serve a new version of object either to create a new object with a new name or creates an “invalidation” on the CloudFront distribution based off the object name. Invalidations cost so if you have to invalidate an entire large CloudFront distribution then perhaps you should just create a new distribution and move DNS name.
* Amazon EMR is a service which deploys out EC2 instances based off of the Hadoop big data software. EMR is used to analyze and process vast amounts of data. The data which is mapped to a cluster of Hadoop Master/Slave nodes for processing, allows for computations to be performed by the servers and reduces to a single output set of return information.
* EMR launches EC2 instances for processing the data passed to Hadoop. It gives the admin ability to access the underlying operating system. Integrates in with AWS services such as S3, DynamoDB, RedShift to receive and output data. Bootstrapper enables the ability to pass configuration information before Hadoop starts when a new cluster is created.
* Mappers are essentially the processes that split the large data file for processing. Reducers takes the result and combines it back into a data file on the disk.
* Elastic Beanstalk is designed to make it easy to deploy out less complex applications. This helps reduce the management required for building and deploying applications. Elastic Beanstalk is used to deploy out easy single tier applications that take advantage of core services such as EC2, Auto Scaling, ELB, RDS, SQS, and CloudFront.
* CloudFormation allows you to create and provision resources in a reusable template fashion. CloudFormation allows you to secure control your infrastructure by building templates which allow you to “script” the ability to delete/create resources on demand. CloudFormation templates are built using JSON syntax. CloudFormatoin allows you to launch a single collection of resources together that are defined within the CloudFormation template.
* Monitoring with AWS config: AWS config is a service which provides detailed configuration information about an environment. It takes a point in time “snapshot” of all supported AWS resources to determine the state of your environment. View historical configurations within your environment by viewing snapshots. Receive notifications whenever resources are created, modified, or deleted. View relationships between resources, i.e. what EC2 instances an EBS volume is attached to.
* AWS CloudTrail is great for security and compliance and monitors all actions taken against the AWS account which CloudTrail enabled. Monitors and be notified of changes to IAM accounts with CloudWatch/SNS integration. View what API keys/user performed any given API action against an environment I.E view what user terminated a set of instances or instance. Can be used in order to meet auditing requirements inside of organization.
* Encryption solutions:

S3: S3 has built-in features that allow you to encrypt your data. AES-256 bit encryption that encrypts data at REST. It is decrypted at it is sent to the customer at download.

EBS encrypted volumes: The data is encrypted on the EC2 instance and copied to the EBS for storage. If a snapshot it taken that snapshot automatically encrypted.

RDS Encryption: MySQL, Oracle, PostgreSQL, MS SQL, Aurora all support this feature. Encrypts the underlying storage space for the instance. Automated backups encrypted as well as snapshots. Read Replicas are encrypted. Provides SSL to encrypt a connection to a DB instance.

* Cloud HSM: HSM (Hardware Security Module) is a dedicated physical machine/appliance isolated in order to store security keys and other types of encryption keys used within an application. The key is used within the domain of the HSM appliance instead of being exposed outside the appliance. HSM appliance have special security mechanisms to make them more secure. They are isolated physically from other resources.
* Troubleshooting of EC2 instances:

Connectivity issues to an EC2 instance: Ports on the correct security group are not open. Remember, all ports are closed by default and only the default security group has ports open to all instances in the same security group (can create this on your own by referencing the SG id as a source).

Cannot attach EBS volume to an EC2 instance: EBS volumes must live in the same availability zone as the EC2 instance they are to be attached to. Create a snapshot from the volume and launch the volume in the correct availability zone.

Cannot launch additional instances: Reached EC2 capacity limit and need to contact AWS to increase limit.

AMI unavailable in other regions: AMI’s are only available in the regions that they are created. An AMI can be copied to another region but will receive a new AMI id.

* Troubleshooting VPC issues:

New EC2 instances are not being assigned a pubic IP address automatically: Modify Auto-Assign Public IP setting on the subnet.

Traffic is not making to the instances even though security group rules are correct: Check the Network Access Control lists to ensure the proper ports from the proper sources are open.

Error when attempting to attach multiple internet gateways to a VPC: Only one internet gateway can be attached to a VPC at any given time

Error when attempting to attach multiple Virtual Private Gateways to a VPC: Only one Virtual Private Gateway is needed on a VPC.

VPC security group (for EC2 instances) does not have enough rules for the required application: Assign the EC2 instance to multiple security groups.

* Troubleshooting ELB issues:

Load balancing is not occurring between instances in multiple availability zones: Enable cross-zone load balancing.

The ELB is configured to listen on port 80 but traffic is not making in to the instances that belong to the ELB: Listeners are not the same as the security group rules; port 80 still needs to be open on the SG that the ELB is using.

Unable to add instances from a specific subnet to the ELB: The specific subnet that instances will be launching in needs to be added to the ELB.

* S3 is an object based storage and each object can size from 0 Bytes to 5 TB. By default you can have 100 buckets per account.
* The maximum visibility timeout for an Amazon SQS message is 12 hours. Amazon SQS messages can contain up to 256 KB of size.
* We can configure the Amazon SQS message retention period to a value from 1 minute to 14 days. The default is 4 days. Once the message retention limit is reached, your messages are automatically deleted.
* When you upload a file to S3 you will receive a HTTP 200 code if the upload was successful.
* Data Consistency Model for S3:

Read after write consistency for PUTS of new objects. Eventual consistency for overwrite PUTS and DELETES (can take some time to propagate)

* Amazon S3 Transfer Acceleration enables fast, easy, and secure transfer of files over long distances between your end users and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront’s globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.
* Once S3 versioning is enabled, Versioning cannot be disabled, only suspended. Versioning’s MFA delete capability, which uses multi-factor authentication, can be used to provide an additional layer of security.
* S3 – Cross Region Replication

Versioning must be enabled on both the source and destination buckets. Files in an existing bucket are not replicated automatically. All subsequent updated files will be replicated automatically. You cannot replicate to multiple buckets or use daisy chaining (at this time). Delete markers are replicated. Deleting individual versions or delete markers will not be replicated.

* Amazon CloudFront can be used to deliver your entire website including dynamic, static, streaming and interactive content using a global network of edge locations. Requests for your content are automatically routed to the nearest edge location, so content is delivered with the best possible performance.
* AWS Storage Gateway is a service that connects 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. The service enables you to securely store data to the AWS cloud for scalable and cost-effective storage. AWS storage gateway’s software appliance is available for download as a Virtual Machine (VM) image that install on a host in your datacenter. Storage Gateway supports either VMware ESXi or Microsoft Hyper-V. Once you’ve installed your gateway and associated it with your AWS account through the activation process, you can use the AWS Management Console to create the storage gateway option that is right for you.
* Types of Storage Gateways: There are four types of storage Gateways

File Gateways (NFS): Files are stored as objects in your S3 buckets, accessed through a Network File System (NFS) mount point. Ownership, permissions, and timestamps are durably stored in S3 in the user-metadata of the object associated with the file. Once objects are transferred to S3, they can be managed as native S3 objects, and bucket policies such as versioning, lifecycle management, and cross-region replication apply directly to objects stored in your bucket.

Volume Gateways: The volume interface presents your applications with disk volumes using the iSCSI block protocol. Data written to these volumes can be asynchronously backed up as point-in-time snapshots of your volumes, and stored in the cloud as Amazon EBS snapshots. There are two types of volume gateways

Volume Gateway – Stored Volumes: Stored volumes let you store your primary data locally, while asynchronously backing up that data to AWS. Stored volumes provide your on-premises applications with low-latency access to their entire datasets, while providing durable, off-site backups. You can create storage volumes and mount them as iSCSI devices from your on-premises application servers. Data written to your stored volumes is stored on your on-premises storage hardware. This data is asynchronously backed up to Amazon Simple Storage Service (S3) in the form of Amazon Elastic Block Store (Amazon EBS) snapshots. 1 GB- 16 TB in size for stored volumes.

Volume Gateway – Cached Volumes: Cached volumes let you use Amazon S3 as your primary data storage while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stored data that your write to these volumes in Amazon S3 and retain recently read data in your on-premises storage gateway’s cache and upload buffer storage. 1 GB – 32 TB in size for cached volumes.

Volume Gateway – Tape Gateway: Tape Gateway offers a durable, cost-effective solution to archive your data in the AWS cloud. The VTL interface it provides lets you leverage your existing tape-based backup application infrastructure to store data on virtual tape cartridges that you create on your tape gateway. Each tape gateway is preconfigured with a media changer and tape drives, which are available to your existing client backup applications as iSCSI devices. You add tape cartridges as you need to archive your data. Supported by NetBackup, Backup Exec, Veam etc.

* S3 Transfer Acceleration utilizes the CloudFront Edge Network to accelerate your uploads to S3. Instead of uploading directly to your S3 bucket, you can use a distinct URL to upload directly to an edge location which will then transfer that file to S3. You will get a distinct URL to upload to.
* EBS Volume Types:

General Purpose SSD (GP2): Designed for General Purpose, balances both price and performance. Ratio of 3 IOPS per GB with up to 10,000 IOPS and the ability to burst up to 3000 IOPS for extended period of time for volumes under 1 Gib

Provisioned IOPS SSD (IO1): Designed for I/O intensive applications such as large relational or NoSQL databases. Use if need more than 10,000 IOPS. Can provision up to 20,000 IOPS per volume.

Throughput Optimized HDD (ST1): used for Big data, Data warehousing, Log processing, cannot be a boot volume

Cold HDD (SC1): Lowest cost storage for infrequently accessed workloads. Cannot be a boot volume.

Magnetic (Standard): Lowest cost per gigabyte of all EBS volume types that is bootable. Magnetic volumes are ideal for workloads where data is accessed infrequently, and applications where the lowest storage is important.

* You cannot mount 1 EBS volume to multiple EC2 instances, instead use EFS.
* For EC2 instances termination protection is turned off by default, you must turn it on. On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated.
* EBS Root Volumes of your DEFAULT AMI’s cannot be encrypted. You can also use a third party tool (such as bit locker etc.) to encrypt the root volume, or this can be done when creating AMI’s in the AWS console or using the API. Additional volumes can be encrypted.
* Security Groups: All inbound traffic is blocked by default. All outbound traffic is allowed by default. Changes to security groups take effect immediately. You can have any number of EC2 instances within a security groups. You can have multiple security groups attached to EC2 instances. Security groups are STATEFUL. If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again. You can block specific IP addresses using security groups, instead use Network Access Control Lists. You can specify allow rules, but not deny rules
* An Amazon Machine Image (AMI) provides the information required to launch a virtual server in the cloud. You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need. You can also launch instances from as many different AMIs as you need. AMI contains A template for the root volume for the instance. Launch permissions that control which AWS account can use the AMI to launch instances. A block device mapping that specifies the volumes to attach to the instance when it’s launched.
* AMI’s are regional. You can only launch an AMI from the region in which it is stored. However, you can copy AMI’s to other regions using the console, command line or the Amazon EC2 API.
* Instance store volumes are sometimes called Ephemeral storage. Instance store volumes cannot be stopped. If the underlying host fails, you will lose your data. EBS backed instances can be stopped. You will not lose the data on this instance if it is stopped. By default, both ROOT volumes will be deleted on termination, however with EBS volumes, you can tell AWS to keep the root device volume.
* IAM Roles are universal; you can use them in any region.
* AWS Lambda is a compute service that runs your code in response to events and automatically manages the underlying compute resources for you. AWS Lambda can automatically run code in response to modifications to objects in Amazon S3 buckets, messages arriving in Amazon Kinesis streams, or table updates in Amazon DynamoDB. Lambda runs your code in high-availability compute infrastructure and performs all the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code and security patch deployment, and code monitoring and logging. All you need to do is supply the code.
* Lambda supported programming language is JavaScript. AWS lambda is designed to provide 99.99% availability for both the service itself and for the function it operates. First 1 million requests are free and $0.20 per 1 million requests thereafter. Lambda pricing also counts duration, Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms. The price depends on the amount of memory you allocate to your function. You are charged $0.00001667 for every GB-second used.
* You cannot delete a snapshot of an EBS volume that is used as the root device of a registered AMI
* ELB’s do not have pre-defined IPv4 addresses, you resolve to them using a DNS name.
* There is a limit of 50 domain names you can manage using Route 53, however this limit can be raised by contacting AWS support.
* Relational Database Types: SQL Server, Oracle, MySQL Server, PostgreSQL, Aurora, MariaDB
* ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory caches, instead of relying entirely on slower disk-based databased. ElastiCache supports two open-source in-memory caching engines: MemCached, Redis.
* RDS database backups: Automated backups are enabled by default. The backup data is stored in S3 and you get free storage space equal to the size of your database. So if you have an RDS instance of 10Gb you will get 10Gb worth of storage. Backups are taken within a defined window. During the backup window, storage I/O may be suspended while your data is being backed up and you may experience elevated latency.
* DB snapshots are done manually (i.e. they are user initiated). They are stored even after you delete the original RDS instance, unlike automated backups.
* When you restore either an Automatic Backup or a manual Snapshot, the restored version of the database will be a new RDS instance with a new end point.
* At the present time, encrypting an existing DB instance is not supported. To use Amazon RDS encryption for an existing database, create a new DB instance with encryption enabled and migrate your data into it.
* Read Replica’s allows you to have a read only copy of your production database. This is achieved by using Asynchronous replication from the primary RDS instance to the read replica. You use read replicas primarily for very read-heavy database workloads. Read replica supported databases are MySQL server, PostgreSQL, MariDB.
* You must have automatic backups turned on in order to deploy a read replica. You can have up to 5 read replicas copies of any database. You can have read replicas of read replicas. Each read replica will have its own DNS end point. You cannot have read replicas that have Multi-AZ. You can create read replicas of multi-AZ source databases however. Read replicas can be promoted to their own databases, this breaks the replication. Read replica in second region for MySQL and MariaDB, not for PostgreSQL.
* Amazon Redshift is a fast and powerful, fully managed, petabyte-scale data warehouse service in the cloud. Customers can start small for just $0.25 per hour with no commitments or upfront costs and scale to a petabyte or more for $1000 per terabyte per year, less than a tenth of most other data warehousing solutions.
* Aurora you can start with 10Gb, scales in 10Gb increments to 64Tb. Compute resources can scale up to 32vCPUs and 244Gb of Memory. 2 copies of your data is contained in each availability zone, with minimum of 3 availability zones. 6 copies of your data. Aurora is designed to transparently handle the loss of up to two copies of your data without affecting database write availability and up to three copies without affecting read availability. Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and repaired automatically.
* If you are using Amazon RDS provisioned IOPS storage with MySQL and oracle database engines, the maximum size RDS volume you can have by default is 6TB.
* In RDS when using multiple availability zones, you cannot use the secondary database as an independent read mode.
* VPC peering allows you to connect one VPC with another via a direct network route using private IP addresses.
* You can peer VPC’s with other AWS accounts as well as with other VPCs in the same account. Peering is in a star configuration, i.e. 1 central VPC peers with 4 others. NO TRANSITIVE PEERING
* Network ACL’s: Your VPC automatically comes a default network ACL and by default it allows all outbound and inbound traffic. You can create a custom ACL. By default, each custom network ACL denies all inbound and outbound traffic until you add rules. Each subnet in your VPC must be associated with a network ACL. If you don’t explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL. You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is remove. A network ACL contains a numbered list of rules that is evaluated in order, starting with the lowest numbered rule. A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
* Amazon SQS is a web service that gives you access to a message queue that can be used to store messages while waiting for a computer to process them. A queue is a temporary repository for messages that are waiting processing. Messages can contain up to 256 KB of text in any format.
* SNS allows you to group multiple recipients using topics. A topic is an “access point” for allowing recipients to dynamically subscribe for identical copies of the same notification. One topic can support deliveries to multiple endpoint types—for example, you can group together iOS, Android and SMS recipients. When you publish once to a topic, SNS delivers approximately formatted copies of your message to each subscriber. Users pay $0.50 per 1 million Amazon SNS requests. %0.06 per 100,000 notification deliveries over HTTP. $0.75 per 100 notification deliveries over SMS. $2.00 per 100,000 notifications deliveries over Email.
* SWF Actors: Workflow starters, Deciders, Activity workers
* Amazon RDS does not currently support increasing storage on a SQL Server DB instance.
* The AWS platform consists of 16 regions currently.
* You cannot move reserved instance from one region to another.
* When you create a new security group, all outbound traffic is allowed by default and all inbound traffic is NOT allowed by default.
* In RDS what is the maximum size for a Microsoft SQL server DB with SQL server Express edition?

There are two different limits. That of the DB (10GB) , and that of the DB instance server storage (300GB).

* Four levels of AWS premium support: Basic, Developer, Business, Enterprise
* Maximum response for a Business level premium support case with Amazon is 1 Hour.
* When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process.
* 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.
* Amazon Redshift uses which block size for its columnar storage? Ans: 1024KB/1MB
* It is possible to transfer reserved instances from one Availability Zone to another
* Using SAML (Security Assertion Markup Language 2.0) you can give your federated users single sign-on (SSO) access to the AWS management console.