Service	My Priority	Notes	
ACM	1	ACM certicates **CANNOT** be directly installed on EC2 instance, instead, they need to install on the ACM integrated services such as ELB, CloudFront, Beanstalk, Cloudformation and API gateway. Certificates could either be stored in ACM or IAM certificate store. You can use IAM AWS CLI to retrieve/upload these certificates	
Athena	1	SQL based query on S3	
Auto-Sacling		Could be extended to Dedicated instances, BUT NOT Dedicated Hosts	
Auto-Scaling		Cool-Down: you need to wait an amount of time before another autoscaling event can happen. **Warm-up**, you need to wait before the new instances are considered into the target metric (which implies that another autoscaling event can happen in the meantime). Cooldown is only supported by Simple policy. Target tracking and Step policies instead support warm-up period.	
AutoScaling		Launch configuration cannot be modified Launch configuration is combination of AMI, instance type, user defined steps could be added while launching it	
AWS Active Directory		Used in hybrid cloud strategy. Active Directory on AWS needs to establish trust relationship of type Forest (one or two way) with on-premise Active Directory service.	
AWS Active Directory		Could be used for cloud strategy where in AWS Active directory used could be assigned AWS role	
AWS Active Directory		EC2/RDS could join AWS AD domain while being created through AWS Mgmt Console. This will allow all AWS AD user to gain access to EC2 instance	
AWS Active Directory		On-premised AD to IAM Identify Provider 1. Configure user and group in AD and map them to role in IAM 2. When user get authenticated by AD, it request AWS STS service to generate a token. STS contains role that user has been assigned to. 3. Using STS token, a user/application access to AWS resources	
AWS Cognito		Prefereable used for mobile/gaming use through which user/access/authorization could be maintanined without creating IAM user/role for accessing AWS services	
AWS Firewal Manager		Applicable at Organization level (multiple accounts), NOT a single account	
AWS Nepture		Graph database	
AWS Orgnaizations		Payer/Master account can turn off Reserved Instance sharing with other accounts	
AWS Shield		Mostly for Layer3/4 attacks (DDOS Category Reflect, Amplification, SSL abuse). For Layer 7 HTTP attack, WAF is used In advance edition, you get additional features like detailed monitoring, WAF, AWS DDOS Support, etc Applies to Application/Classic Load Balancer, CDN and Route 53	
AWS STS		Concept: **Identify Provider (IdP)** - A provider that maintains identify and authenticate these identities. Upon authentication, IdP generates authentication token, which then can be exchanged with AWS for temporary security credentials that map to an IAM role with permissions to use the resources in your AWS account. Examples are Amazon, Google, Facebook and your corporate active directory **Service Provider** - a provider that provides services such AWS, Udemy, etc. **Federation** - An association comprising any number of service providers and identity providers. **IAM Identify Provider** - When you want to create a federation between AWS (Service Provider) and any external Identify Provider, then you need to create an IAM Identify Provider to establish a trust relationship between your AWS account and external IdP. IAM IdP supports two types of federation with external IdP Open ID Connect (OIDC) Standards Providers such as Amazon, Google, etc, also know as Web Identify Federation SAML 2.0 Based Model Standard provides such Microsoft AD, OAuth, etc	
AWS STS		Open ID Connect Federations Detailed Steps: 1. Register your app with external IdP, which will issue you a audience ID 2. Create IAM IdP, specify IdP URL and audience ID and establish a trust between them 3. Create a role for this federation and assign policy. There are two policies to be assigned to this role 3.1 Trust policy, which indicate who from external IdP can assume this role i.e. STS service to use AssumeRoleWithWedIdentify 3.2 What AWS resources and access previlieges to be provided to this role	

Service	My Priority	Notes	
AWS STS		**AssumeRoleWithWebIdentify(**Role ARN, TokenFromIdp, Duration, RoleSessionName, Optional SessionPolicy**)** - API to exchange the authentication token issued by OIDC standard IdPs for AWS temporary security credentials Though Amazon recommends to use AWS Cognito for mobile apps for user authentication **AssumeRoleWithSAML** (Role ARN, IAMSAMLProviderARN, SAMLAssetion, Duration, Optional SessionPolicy) - API to exchange the authentication token issued by SAML 2.0 standard IdPs for AWS temporary security credentials **AssumeRole**(Role ARN, Duration, RoleSessionName, Optional SessionPolicy, Option MFARequired and Optional ExternalID) - Cross-Account Delegation and Federation Through a Custom Identity Broker. Caller must be an existing IAM user, which assume role in the delegated aws account. **GetFederationToken**() - normally used by a proxy app. Must be call by an existing IAM user **GetSessionToken**() - Must be call by an existing IAM user Useful link - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_request.html	
AWS VPN CloudHub		If you have multiple AWS Site-to-Site VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. This enables your remote sites to communicate with each other, and not just with the VPC. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC	
AWS WAF		1. For Layer 7 HTTP attacks. Apply filter on incoming traffic based on 1.Condition (Standard or Rate Based like number of HTTP request from same client) --> 2.Rule --> 3.WebACL Could be appplied to Application/Classic Load Balancer, CDN and API Gateway Also included in AWS Shield Advance edition	
VPC		First address (xx.xx.xx.0) for network and then subsequent three IP address (xx.xx.xx.1/2/3 VPC router, DNS server and future address respectively) and last (xx.xx.xx.255) for boradcast are reserved by AWS and can't be used for assignment in a subnet.	
Cloud Formation		**Template** - parameters (including validation such max length, default, etc), resources, output **Mapping** - can define mapping such as AMI per region and at run time stack can determine which AMI to use depending upon on which Stack is being created. **Functions/Psueddo Params** - many pre-defined functions such as findinMap, Join, Select,etc and Params such as AWS::Region, AWS:StackID, etc are available which could be referenced in the template **Stack Policy** - by default, deny everything unless explicit allow statement is mentioned. Once assigned, it cannot be removed, and could only be updated through CLI and API, NOT console **Stack** - References to AWS resources in the region where stack is being created must exist else resource lookup will fail . **Bootstrap** - Option 1 is through user data and 2 is through helper scripts (init, get-meta-data, hup and) **Conditions** - use can use condition along with resource section to determine if that resource to be created or NOT. **DeletionPolicy** - could be set to snapshot, retain or delete	
CloudFront		Pricing is based on 1) Data transfer to edge location, 2) Data transfer to Origin and 3) Number of HTTP requests Caching - Origin server can control caching requirement by adding a Cache-Control header to your objects . This is applicable only if you have selected **"Use Origin Cache Headers"** while creating CDN **Caching header/attributes** - max-age, expire, s-maxage **Encryption** - HTTPS on cloud front will ensure that client and CDN will be over SSL. **Field level encryption** allows you to encrypt field in your client POST method with a client provided public key. Only app that has corresponding private key will be able to decrypt it.	
CloudHSM		Support Qouram based authentication Is Region specific	
Cloudwatch		Can trigger event for ALB, EBS and EC2 only. Also Autoscalling could be triggered	
CloudWatch		CloudWatch Unified Agent - install as agent on EC2 instance/on-prem server, which could collect log and metrics and send it to CloudWatch Log CloudWatch Insight - enables you to interactively search and analyze your log data in Amazon CloudWatch Logs CloudWatch Logs - stores log, which can be monitor and generate alarms for subsequent action	
Code Pipeline		AWS CodePipeline is a continuous delivery service you can use to model, visualize, and automate the steps required to release your software. You can quickly model and configure the different stages of a software release process. AWS CodePipeline automates the steps required to release your software changes continuously.	
Cost		EFS is three times and twenty times expansive than EBS and S3 respectively	

Service	My Priority	Notes	
CRR		Cross region replication is only for RDS using read replicas and S3	
Data Pipeline		automate the movement and transformation of data. With AWS Data Pipeline, you can define data-driven workflows, so that tasks can be dependent on the successful completion of previous tasks	
DDOS		Cloudfront - Layers 3, 4, 6 and 7 Route 53 - 3, 4 and 7 ELB - 3, 4, 7 and 7 if 7 used with WAF API Gateway - 3, 4 and 6 VPC - EC2 -	
Dedicated Instance/Host		Hardware dedicated for you, however, could host dedicated as well non-dedicated instance from your SAME ACCOUNT ONLY. Host is physical hardware dedicated to you and limit it usage to a particular instance family/size	
Direct Connect		Create Virtual Private Interface to connect to your VPC and Virtual Public Interfaces for other AWS services using your Direct Connect network band-width	
DMS		In addition to 6, support SAP, MongoDB and DB2	
Dynamodb		Key-value and document database Single digit-milli second performance at any scale Fully managed, multiregion, multimaster database with built-in security, backup and restore, and in-memory caching for internet-scale applications. Can handle more than 10 trillion requests per day and support peaks of more than 20 million requests per second. good for mobile, web, gaming, ad tech, IoT,	
Dynamodb		DynamoDB global tables replicate your data across multiple AWS Regions to give you fast, local access to data for your globally distributed applications DynamoDB Accelerator (DAX) provides a fully managed in-memory cache for milli second latency DynamoDB Streams capture a time-ordered sequence of item-level modifications in any DynamoDB table and store this information in a log for up to 24 hours.	
DynamoDb		Partition keys - use it with distinct value could provide higher performance	
DynamoDB		Max of 5 global and 5 local secondary indexe. Total of 20 attributes that could be part of all secondary index.	
DynamoDB		Useful link for indexes. https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SecondaryIndexes.html	
DynamoDB		**Read Types:** **Eventual Consistency** - low latency as most recent data is not guaranted. happens within a second. If need in less than a second, then go for **Strong Consistency** **ACID transaction** - possible through DynamoDB Transaction SDK **Partion Key** - key that define where DynamoDB will physically store that data. For each partition key, DynamoDB create a storage capacity of 10GB **Index** - local share same partition key as table partion key, however, global could use different partition key. **Data Size** - max 400K **Partition Calculation:** - By Capacity - RCU/3000 + WCU/3000 By table size - size / 10GB Total Partition = MAX (By Capacity or table size) **Global Tables** - same data available in all region configured. How - Global table achieve it by creating a ONE replica table in each configured region, enable DynamoDB stream in that replica table to nofity table changes, which intern replicate changes from one replica to all other replica in each region	
EBS		IOPS related to number of read/write to a disc. Throughput is number of times, amount data could be written to a disk. In question is around IOPS, then choose from SDD. If it is around throughput, then choose from HDD	

Service	My Priority	Notes	
EBS		Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. Throughput Optimized HDD (st1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing Cold HDD (sc1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. With a lower throughput limit than st1, sc1 is a good fit ideal for large, sequential cold-data workloads. If you require infrequent access to your data and are looking to save costs, sc1 provides inexpensive block storage. Bootable sc1 volumes are not supported.	
EBS		Cheapest is COLD HDD for lower workload Use GP2 SSD for general workload and cost consideration	
EBS		Storage up-to 16 TB For high performace, always use SSD over HDD. For highest performance, create RAID 0 Throughput / IOPS (SSD - 250, 10000: Provisioned SSD - 1000/64000, Through HDD - 500/500, COLD - 250/250)	Verified
EBS		Default replication ensuring durability and availabilty of an EBS is within an AZ, which is not charged to customer A snapshot is constrained to the Region where it was created	
EBS		When price and performance mixed in question, then GP2 SSD. Else, cheapest is COLD HDD	
EBS		RAID 0 for fastest performance, but not replication RAID 1 for replication, but not as fast as RADI 0	
EC2		With enhannced networking configured, could reduce latency	
EC2		Auto Scaling - replaces unhealth instance with a new instance only if either of the below happend 1. EC2 status checks fails 2. Health check on of the associate ELB fails	
EC2 - AMI		When create AMI, it will contain public keys as well. If you have corresponding private key, then whoever create an instance from this AMI, you can login to that EC2 instance using your private keys	
EC2 Key-Pair		PEM Keys name are unique in a region within your account i.e. in your aws account, you canot not have more than one key having same name in a single region You can import your public keys (AWS generated or personel) to a region.	
ECS		Fully manged ECS through Fargate Launch. Manually managed through ECS Launch Type	
ECS		**Retreiving Sensative Information From Secrets Manager or Parameter Store** Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of either the Secrets Manager secret or Systems Manager Parameter Store parameter containing the sensitive data to present to the container. The parameter that you reference can be from a different Region than the container using it, but must be from within the same account. For tasks that use the Fargate launch type, the only supported method is referencing a Systems Manager Parameter Store paramete2. For EC2 launch type, both are supported	
EFS		Based on NFS version 4 and 4.1	
EFS		Use MAX I/O mode for more than 7000 operation / second / efs	
EFS		Burst credit - get accumulated over w.r.t. to baseline rate	
Egress-Only Internet Gateways		Support outgoing only traffic from VPC over ipV6 version. For iPV4 outgoing only, use NAT Gateway	
Elastic Beanstalk			
Elasticbeanstalk		Supported version are: Packer Builder, Single Container Docker, Multicontainer Docker, Preconfigured Docker, Go, Java SE, Java with Tomcat, .NET on Windows Server with IIS, Node.js, PHP, Python, Ruby	

Service	My Priority	Notes	
ElasticBeanstalk vs CloudFormation		Elastic Beanstalk is more to make developer life easy by easily deploying applicaiton. CloudFormation on the other hand is more like configure your entire infrastructure that include EC2, DB, Cache, Cluster, ALB, etc	
ElasticCache		Redis - persitent data store, Memcached is NOT. Memcached - multi-threaded Redis - Advance Data Structure, persistent data store, replication to read replica, atomic transaction Both are highly available and could scale automatically	
ElasticCache		Billed by node size and hours of usage Redis modes - Single Node with read replica and feature of auto failover to read-replica in multi-az and Cluster Memcached - no multi-az auto failover	
ELB		Application does but Network NOT - Support path (/static vs /dynamic) and host () routing. + SNI, Sticky session Network does but Application NOT - preserve source ip address. (client IP in case of target is instance based else ELB IP in case of target is IP address based)	
ELB		**Proxy Protocol** is an Internet protocol used to carry connection information using **Proxy Protocol Header** from the source requesting the connection to the destination for which the connection was requested. **Supported by Network and Classic Load Balancer** **Connection Draining** - time window during a target de-registeration process, which is required by target to complete thier task before ELB close connection and de-registering target from ELB **Sticky sessions** are a mechanism to route requests from the same client to the same target. **Application Load Balancer supports** sticky sessions using load balancer generated cookies. If you enable sticky sessions, the same target receives the request and can use the cookie to recover the session context. Stickiness is defined at a target group level **Request Tracing -** The Application Load Balancer injects a new custom identifier “X-Amzn-Trace-Id” HTTP header on all requests coming into the load balancer. Request tracing allows you to track a request by its unique ID as the request makes its way across various services that make up the your websites and distributed applications. You can use the unique trace identifier to uncover any performance or timing issues in your application stack at the granularity of an individual request. Application Load Balancers and Classic Load Balancers support **X-Forwarded-For, X-Forwarded-Proto, and X-Forwarded-Port headers.**	
General		When report is used, think of S3 as storage instead of using ElastichCache or ReadReplicas unless explicitly mentioned real time reports	
Glacier		Range Retrieval - retrieve a range from an archive glacier	
GuardDuty		IDS (intruder Detection System, not prevention) - Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads	
IAM		Policy (PARC - Principal, Action, Resource and Condition) are JSON and ACL are in XML (no explicit deny)	
IAM		**Most secured cross account use case** - a user named John in DEV account accessing a file from S3 in PROD account in most secured way PROD Account Setup: Setup an cross-account role, enforce DEV account user to provide a unique external ID, assign below to this role. 1. STS Service Assume Role permission in trust relationship. - Make sure that asume role is not provided to all users, but to only John in DEV acccount by using John ARN in Principal section of the policy Also add a conditional access to provide access only if external id provided John is 2. Allow access to S3 file - add permission to access S3 file DEV Account Setup: 1. Create a group, assign STS Service "Assume Role" policy. Assign John to this group 2. Provide PROD account id, role name and external ID to John, which he can use to switch role in PROD acccount. Behind the scene - When John switch role, STS services checks if John has permission to switch role, then accordingly generate a temporary credential to John for logging into PROD account	
IAM		**Resource Based Policy** - using this you can grant access to a resource in your account to other AWS account without having to create a role in your account, which users in other AWS account needs to assume	

Service	My Priority	Notes	
IAM		**Servie Linked Role** - A service-linked role is a unique type of IAM role that is linked directly to an AWS service. Service-linked roles are predefined by the service and include all the permissions that the service requires to call other AWS services on your behalf.	
Identify Federation		Could be used for hybrid could strategy i.e. AD remains at on-premise and get access to AWS using Federation --> IAM Integration using SAML Identify Federation services such as Facebook, Microsoft AD Federation service generate SAML based assertion request with AWS SAML endpoint (i.e. IAM), which interns create new role to access AWS services	
Inspector		Inspect security thread and compliace	
Kinesis			
Kinesis Stream		Data storage limitation is 1 MB Data retention default is 24 hours and max of 7 days Shard - consist of 1. partition key - a unique key that identify a shard. Partition key shall be something that could have higher distinct value to allow evenly distribute data into multiple shards i.e. same concept as it was in DynamoDB table. This has to be specified by producer of the data like session id 2. Sequence number 3. Data	
NAT		NAT Gateway doesn't support iPV6, instead use Egress Only Internet Gateway You **CANNOT** disassociate an Elastic IP address from a NAT gateway after it's created You **CANNOT** associate a security group with a NAT gateway.	
OAuth 2.0		Provides authorization only and issue tokens	
Organization		**Service Policy - ?**	
RDS		Aurora - replication lag under 100ms. Could have 15 replicas as oppose to 5 replica for RDS	
RDS		You can set up replication between an Amazon RDS MySQL or MariaDB DB instance and a MySQL or MariaDB instance that is external to Amazon RDS.	
RDS-Aurora	1	If entire region is down, auto fail over to one of its read-replica in another region. For RDS, it requires manual intervantion i.e. first promote of the read replica in another region to a new instance, reconfigure that instance to support Multi-AZ. Cross region replicas available only for MySQL, no for PostgreSQ:	
RDS-Aurora		**Global Database** - An Aurora global database consists of one primary AWS Region where your data is mastered, and one read-only, secondary AWS Region. Aurora replicates data to the secondary AWS Region with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS Region. Aurora global databases use dedicated infrastructure to replicate your data, leaving database resources available entirely to serve application workloads.	
RedShift		Cross region back-up enable copying backup snapshot automatically to another reason. There is no cross region replication of entire cluster in real time. You have to take snapshopt and enable cross region snalshot replication	
RedShift		Currently, Amazon Redshift only supports Single-AZ deployments. You can run data warehouse clusters in multiple AZ's by loading data into two Amazon Redshift data warehouse clusters in separate AZs from the same set of Amazon S3 input files.	
Redshift		Keywords - Cluster, Block + Sort, Slices, Compute vs Leader Node,	
Redshift Spectrum		Used for queries large amount of date stored in S3 in real time	

Service	My Priority	Notes	
Reserved Instances		Type: Standard, Convertible and Scheduled Could be bought for RDS as well Could change AZ, Instance Size and Networking Type Can change Instance Family, OS, Tenancy (Dedicated/Shared), Payment Option for Convertible, but NOT for standard If AZ specific, capacity guranteed and discount applied to AZ only. For regional, no guranteed capacity and discount applicable to entire region Instance size flexibility - available only for Unit/Linux (NOT for Window, REHL, S). For example, RI on ONE M.2Xlarge instance size could be used to provide discount on TWO M.xlarge instance size Reserved Instances can not be moved between two regions For consolidated billing, discount applied on account, which uses reserve instance of same type/family of the other member account are only if both instances were launched in same AZ	
Route 53		Simple vs Multi-value. Simple will have one A record for all IP addresses, whereas Multi-answer will have A-record for each IP address, due to which it can check health status of the IP address	
Route 53		**Private Hostage Zone** - a container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains within one or more VPCs that you create with the Amazon VPC service. **To use private hosted zones, you must set enableDnsHostnames and enableDnsSupport to true**	
Route 53		**Alias** - existing AWS service **A** - is an IPv4 address in dotted decimal notation. **AAAA** - is an IPv6 address in colon-separated hexadecimal format. **CNAME** - Value element is the same format as a domain name. The DNS protocol does not allow you to create a CNAME record for the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com. You cannot create a CNAME record for example.com, but you can create CNAME records for www.example.com, newproduct.example.com, and so on. In addition, if you create a CNAME record for a subdomain, you cannot create any other records for that subdomain. For example, if you create a CNAME for www.example.com, you cannot create any other records for which the value of the Name field is www.example.com. **NS -** identifies the name servers for the hosted zone **CAA** -lets you specify which certificate authorities (CAs) are allowed to issue certificates for a domain or subdomain	
S3		Lifecycle policy allowing expiring object expiry, which is equivalent to deletion	
S3		Until file gets propogated (replicated, NOT just completed), if you make a HEAD or GET request you will get a 404 Not Found error until the upload is fully replicated.	
S3		**Server Side Encryptions** (SSE-S3, SSE-KMS and SSE-C)	
S3		Pre-Signed URL are referrred for S2, where Signed URL are refferred with CloudFrontDistribution	
S3 Requester Pays		Has to have an AWS account for accessing S3 URL	
SAM		Serverless application management supports API, Lamda and DynamoDB	
Secret Manager		AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.	
Snowball		If data is in TB, then use it. If data is in PB, then Snowball is the only option	
SPOT Instances		Basic attributes: AMI, instance type/size, VPC, etc Three types: Fill and Kill (One-time-request), Maintain(re-provision instance as soon as price come below your bid price even you manually terminate it all by yourself) and Duration Based (specify duration and you have your instance NOT stopped during that time-frame) For Request/Maintain, I can configure to either terminate, stop or hibernate my instance as soon as price go above my bid price so I do not loose any data	

Service	My Priority	Notes	
SQS		FIFO queques are limited to 300 transactions/sec	
Storage Gateway		File Gateway - NFS/SMB protocol based. Backup data onto S3 and keep a local copy of cache for frequently access data. Stored Volume - iSCSI protocol based. Keep entire data set at on-premise and create data snapshot and store them in S3 as EBS snapshot Cache Volume - iSCSI protocol based. Keep frequently access data set at on-premise, create EBS volumes in AWS and then take backups in S3 as EBS snapshots	
System Manager		AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage your infrastructure securely at scale. **could also stoe username/passwords in parameter store**	
System Patch Mgr		For patching operating system	
TIPS		Cost Saving - Don't assume replacing large number of smaller instances with one large instance can reduce cost unless some context is provided, which could validate it	
VMWare vCenter Plugin		it enables you to migrate on-prem VMware VMs to Amazon EC2 and manage AWS resources from within vCenter Serve	
VPC		**enableDnsHostnames** - Indicates whether the instances launched in the VPC get public DNS hostnames. If this attribute is true, instances in the VPC get public DNS hostnames, but only if the enableDnsSupport attribute is also set to true. **enableDnsSupport** - Indicates whether the DNS resolution is supported for the VPC. If this attribute is false, the Amazon-provided DNS server in the VPC that resolves public DNS hostnames to IP addresses is not enabled. If this attribute is true, queries to the Amazon provided DNS server at the 169.254.169.253 IP address, or the reserved IP address at the base of the VPC IPv4 network range plus two will succeed.	
VPC		**Bring Your Own IP Addresses (BYOIP)** - You can bring part or all of your public IPv4 address range from your on-premises network to your AWS account. You continue to own the address range, but AWS advertises it on the Internet. After you bring the address range to AWS, it appears in your account as an address pool. You can create an Elastic IP address from your address pool and use it with your AWS resources, such as EC2 instances, NAT gateways, and Network Load Balancers	
VPC CIDR Block		Within netmask range of /16 to /18	
VPC Endpoint		Gateway for S3 and Dynamo DB, for evething else Interface endpoint	
VPC Limits		VPCs per Region -- 5 -- The limit for internet gateways per Region is directly correlated to this one. Increasing this limit increases the limit on internet gateways per Region by the same amount. Subnets per VPC -- 200 IPv4 CIDR blocks per VPC -- 5 -- This limit is made up of your primary CIDR block plus 4 secondary CIDR blocks. IPv6 CIDR blocks per VPC -- 1 -- This limit cannot be increased. Elastic IP addresses per Region -- 5 This is the limit for the number of Elastic IP addresses for use in EC2-VPC. For Elastic IP addresses for use in EC2-Classic, see Amazon EC2 Limits in the Amazon Web Services General Reference.	
VPN Connection		Requires Virtual Private Gateway to AWS VPC connectd with Customer Gateway at on-premise data center	
AD Connector		AD Connector is a directory gateway with which you can redirect directory requests to your on-premises Microsoft Active Directory without caching any information in the cloud. AD Connector comes in two sizes, small and large. You can spread application loads across multiple AD Connectors to scale to your performance needs. There are no enforced user or connection limits. AD Connector comes in two sizes, small and large. A small AD Connector is designed for smaller organizations of up to 500 users. A large AD Connector can support larger organizations of up to 5,000 users.	
IAM		Revoke Active Session - revoke all active session started by a role except Service-Linked-Role	

Service	My Priority	Notes	
Snowball		Snowball 50 TB (42 TB usable) only available in US regions 80 TB (72 TB usable) Snowball Edge Storage Optimized 100 TB (80 TB usable) Snowball Edge Compute Optimized 42 TB (39.5 usable) plus 7.68 TB of dedicated NVMe SSD for compute instances Snowball Edge Compute Optimized with GPU 42 TB (39.5 usable) plus 7.68 TB of dedicated NVMe SSD for compute instances	
Volume Gateway		Max Storage Size Stored - 512 TB Cached - 1024 TB	
CloudFront		If accessing content over HTTPS using CDN URL, could use default CDN SSL certs. If accessing content over HTTPS using Domain URL (www.example.com), ,must install client certificate on CDN.	
CloudFront		Use signed URLs for the following cases: 1. You want to use an RTMP distribution. Signed cookies aren't supported for RTMP distributions. 2. You want to restrict access to individual files, for example, an installation download for your application. 3. Your users are using a client (for example, a custom HTTP client) that doesn't support cookies. Use signed cookies for the following cases: 1. You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of a website. 2. You don't want to change your current URLs.	
Snowball		Snowball edge benefits over standard Snowball Import data into Amazon S3 Export from Amazon S3 Durable local storage Local compute with AWS Lambda Amazon EC2 compute instances Use in a cluster of devices Use with AWS Greengrass (IoT) Transfer files through NFS with a GUI	
OpsWorks		Best Practice updating a stack: 1. Create and start new instances to replace your current online instances. Then delete the current instances. The new instances will have the latest set of security patches installed during setup. 2. On Linux-based instances in Chef 11.10 or older stacks, run the Update Dependencies stack command, which installs the current set of security patches and other updates on the specified instances.	
ELB		**Session Stickyness:** If your application has its own session cookie, then you can configure Elastic Load Balancing so that the session cookie follows the duration specified by the application's session cookie. If your application does not have its own session cookie, then you can configure Elastic Load Balancing to create a session cookie by specifying your own stickiness duration. Elastic Load Balancing creates a cookie, named AWSELB, that is used to map the session to the instance.	