

<b>Elastic Beanstalk through CLI</b>	AWS EB CLI cannot create the instance profile for your beanstalk environment if your IAM role has no access to creating roles. This error is also thrown when the instance profile has insufficient or outdated policies that beanstalk needs to function.
<b>Glacier Vault Lock</b>	Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual Glacier vaults with a vault lock policy. You can specify controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits. Once locked, the policy can no longer be changed.
<b>Route 53 DNS Routing</b>	<ul style="list-style-type: none"><li>✓ <b>Simple Routing Policy</b> You can only have one record with multiple IP Address. If you specify multiple values in a record, Route 53 returns all values to the user in a random order.</li><li>✓ <b>Weighted Routing Policy</b> Weighted Routing Policies let you split your traffic based on different weights assigned. E.g. You can set 10% of your traffic to go to Server1 and 90% to go to Server2.</li><li>✓ <b>Latency Based Routing Policy</b> It allows you to route your traffic based on the lowest network latency for your end user.</li><li>✓ <b>Failover Routing Policy</b> Failover routing policies are used when you want to create an Active/Passive set up. For example, you may want your primary site to be in EU-WEST-1 and secondary DR site in AP-WEST-2. Route 53 will monitor the health of your primary site using a health check. A health check monitors the health of your end points.</li><li>✓ <b>Geolocation</b> Geolocation routing lets you choose where your traffic will be sent based on the geographic location of your users.</li><li>✓ <b>Multivalue Routing</b> Creating more than one record of the same name and type Routing traffic to multiple resources Associating a Route 53 health check with records</li></ul>
<b>Trusted Advisor</b>	✓ Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. It also provides real time guidance to help you provision your resources in compliance with the AWS best practices.
<b>AWS Inspector</b>	✓ AWS Inspector is used to check for vulnerabilities in resources such as EC2 Instances. It does not provide a report on how you can further improve your architecture, unlike with Trusted Advisor.

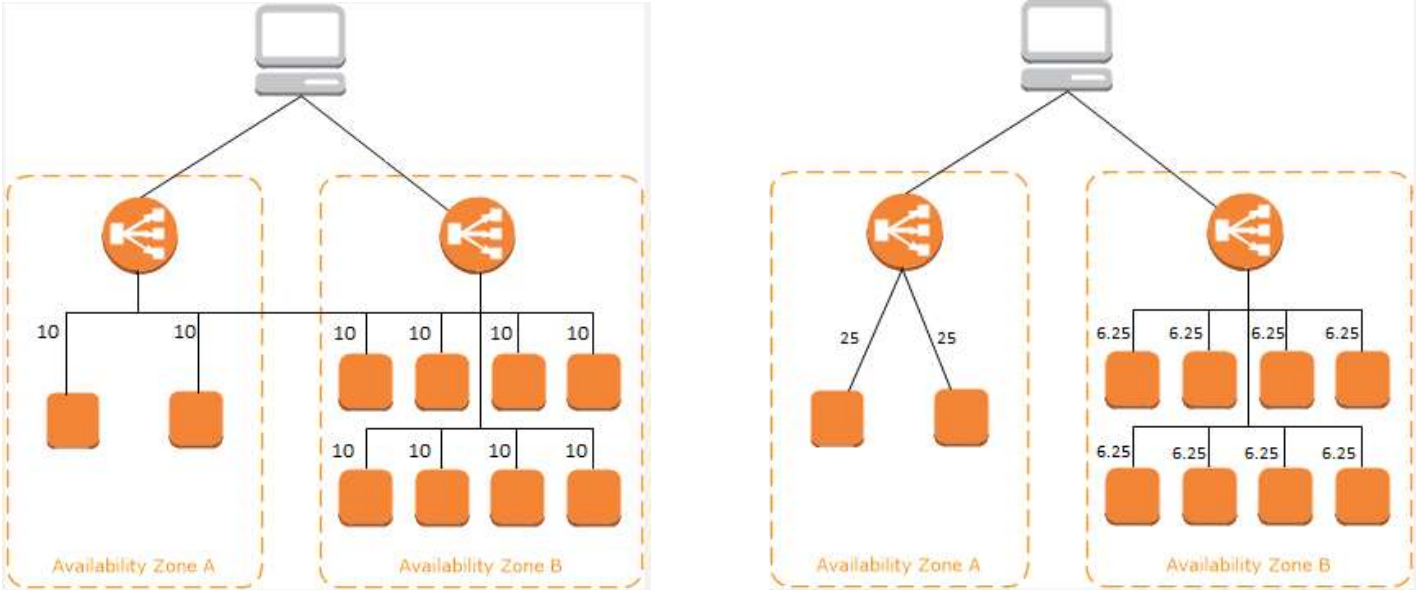
<b>Performance Insights</b>	<ul style="list-style-type: none"> <li>✓ Performance Insights expands on existing Amazon RDS monitoring features to illustrate your database's performance and help you analyze any issues that affect it.</li> </ul>
<b>AWS Config</b>	<p>A fully managed service that provide you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.</p> <ul style="list-style-type: none"> <li>✓ To analyze potential security weaknesses</li> <li>✓ Detailed historical information about your AWS resource configurations, such as the AWS Identity and Access Management (IAM) permissions that are granted to your users, or the Amazon EC2 security group rules that control access to your resources.</li> <li>✓ To view the IAM policy that was assigned to an IAM user, group, or role at any time in which AWS Config was recording. This information can help you determine the permissions that belonged to a user at a specific time</li> </ul>
<b>AWS WAF</b>	<ul style="list-style-type: none"> <li>✓ AWS WAF is used as a Web Application firewall in AWS and only provides security to your VPC.</li> </ul>
<b>CloudFront</b>	<ul style="list-style-type: none"> <li>✓ Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.</li> <li>✓ It is used as a Content Distribution Service.</li> <li>✓ Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with <b>low latency</b>, high transfer speeds, all within a developer-friendly environment.</li> </ul>
<b>Internal Classic Load Balancers</b>	<p><b>Internal load balancer &amp; Internet-facing load balancer</b></p> <p>When you create a load balancer in a VPC, you must choose whether to make it an internal load balancer or an Internet-facing load balancer.</p> <p>The nodes of an Internet-facing load balancer have public IP addresses. The DNS name of an Internet-facing load balancer is publicly resolvable to the public IP addresses of the nodes. Therefore, Internet-facing load balancers can route requests from clients over the Internet.</p> <p>The nodes of an internal load balancer have only private IP addresses. The DNS name of an internal load balancer is publicly resolvable to the private IP addresses of the nodes. Therefore, internal load balancers can only route requests from clients with access to the VPC for the load balancer.</p> <p>If your application has multiple tiers, for example web servers that must be connected to the Internet and database servers that are only connected to the web servers, you can design an architecture that uses both internal and Internet-facing load balancers. Create an Internet-facing load balancer and register the web servers with it. Create an internal load balancer and register the database servers with it. The web servers receive requests from the Internet-facing load balancer and send requests for the database servers to the internal load balancer. The database servers receive requests from the internal load balancer.</p>
<b>AWS Direct Connect</b>	<p>AWS Direct Connect is a cloud service solution that 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.</p>
<b>VPC Peering</b>	<p>VPC Peering is mainly used to connect two or more VPCs.</p>

<b>Accessing a Corporate or Home Network</b>	<ul style="list-style-type: none"> <li>You can optionally connect your VPC to your own corporate data center using an IPsec AWS managed VPN connection, making the AWS Cloud an extension of your data center.</li> <li>To enable instances in your VPC to reach your customer gateway, you must configure your route table to include the routes used by your VPN connection and point them to your virtual private gateway.</li> </ul> <p><b>A VPN connection consists of:</b></p> <ul style="list-style-type: none"> <li>✓ a virtual private gateway (which is the VPN concentrator on the Amazon side of the VPN connection) attached to your VPC.</li> <li>✓ a customer gateway (which is a physical device or software appliance on your side of the VPN connection) located in your data center.</li> </ul>
<b>AWS Storage Gateway</b>	AWS Storage Gateway is primarily used to augment your on-premise storage capacity and not for migration. In addition, it would still take a lot of time to move 80TB of data using your Internet connection.
	✓
<b>Amazon EC2 Systems Manager</b>	<p><b>AWS launched Amazon EC2 Systems Manager, which helps you</b></p> <ul style="list-style-type: none"> <li>✓ Automatically apply OS patches</li> <li>✓ Collect software inventory</li> <li>✓ Configure Windows and Linux operating systems</li> </ul> <p>These capabilities enable automated configuration and ongoing management of systems at scale and help maintain software compliance for instances running in Amazon EC2 or on-premises.</p> <p>One of the capabilities of Systems Manager is <b>Patch Manager</b>, which can automate the process of patching Windows managed instances at scale. With Patch Manager, you can scan instances for missing patches, or scan and install missing patches to individual instances or large groups of instances by using EC2 tags. Patch Manager can also be used with Systems Manager Maintenance Windows, so you can create a schedule to perform patch operations on your instances within a customized maintenance window.</p>
<b>AWS Organizations &amp; Service control policies</b>	<p>AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. AWS Organizations includes consolidated billing and account management capabilities that enable you to better meet the budgetary, security, and compliance needs of your business.</p> <p>Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs enable you to restrict, at the account level of granularity, what services and actions the users, groups, and roles in those accounts can do.</p>
<b>Amazon Kinesis Data Streams (KDS)</b>	It is a massively scalable and durable real-time data streaming service.
<b>SQS</b>	<ul style="list-style-type: none"> <li>✓ Only a messaging service.</li> <li>✓ It enables you to decouple and scale micro services, distributed systems, and server less applications.</li> </ul>
<b>SNS</b>	Mainly used as a notification service.
<b>Amazon Inspector</b>	Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you to identify potential security issues.
<b>AWS Storage Gateway</b>	AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure.

	Note: - S3 is used as a scalable object storage, you still have to go through AWS Storage Gateway to set up an iSCSI target.
<b>NAT Gateways</b>	You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
<b>Amazon EFS</b>	Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system.
<b>ACL</b>	A network access control list ( <b>ACL</b> ) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You may set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.
<b>Elastic Network Interface</b>	Elastic Network Interface is only used to create and attach additional network interfaces for the EC2 instance.
<b>Placement Group</b>	Placement Group simply determines how instances are placed on underlying hardware.
<b>Enhanced Networking</b>	Enhanced Networking feature is mainly used to provide high-performance networking capabilities for EC2 instances on supported instance types.
<b>Types of Amazon Route 53 Health Checks</b>	<ul style="list-style-type: none"> <li>✓ Health checks that monitor an endpoint.</li> <li>✓ Health checks that monitor other health checks (calculated health checks).</li> <li>✓ Health checks that monitor CloudWatch alarms.</li> </ul>

## Networking

<b>Egress-only Internet gateway</b>	<p>An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet, and prevent inbound communication. An egress-only Internet gateway supports <b>IPv6</b> traffic only.</p> <ul style="list-style-type: none"> <li>✓ <b>NAT</b> instance does not support IPv6 address.</li> <li>✓ <b>m3.large</b> instance type does not support IPv6 address.</li> </ul>
<b>Migrating to IPv6</b>	<p>If you have an existing VPC that supports IPv4 only, and resources in your subnet that are configured to use IPv4 only, you can enable IPv6 support for your VPC and resources. Your VPC can operate in dual-stack mode — your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 communication are independent of each other.</p> <p>You cannot disable IPv4 support for your VPC and subnets; this is the default IP addressing system for Amazon VPC and Amazon EC2.</p> <p><b>Steps to enable your VPC and subnets to use IPv6</b></p> <ul style="list-style-type: none"> <li>✓ Step 1: Associate an IPv6 CIDR Block with Your VPC and Subnets</li> <li>✓ Step 2: Update Your Route Tables</li> <li>✓ Step 3: Update Your Security Group Rules</li> <li>✓ Step 4: Change Your Instance Type</li> <li>✓ Step 5: Assign IPv6 Addresses to Your Instances</li> <li>✓ Step 6: (Optional) Configure IPv6 on Your Instances</li> </ul> <p>For an EC2 instance to be able to communicate to the Internet over IPv6, the following configuration should be done in the VPC:</p>

	<p>Associate a /56 IPv6 CIDR block with the VPC. The size of the IPv6 CIDR block is fixed (/56) and the range of IPv6 addresses is automatically allocated from Amazon's pool of IPv6 addresses (you cannot select the range yourself).</p> <p>Create a subnet with a /64 IPv6 CIDR block in your VPC. The size of the IPv6 CIDR block is fixed (/64).</p> <p>Create a custom route table, and associates it with your subnet, so that traffic can flow between the subnet and the Internet gateway.</p>
<b>VPC Peering</b>	<p>A network connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network.</p> <p>Full mesh configuration supports VPC peering.</p> <p>Transitive Peering and Edge to Edge Routing are not supported.</p>
<b>Cross-zone load balancing</b>	<p>Cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled Availability Zone, and improves your application's ability to handle the loss of one or more instances.</p> <p>If cross-zone load balancing is enabled, each of the 10 targets receives <b>10%</b> of the traffic. This is because each load balancer node can route its <b>50%</b> of the client traffic to all <b>10</b> targets.</p> <p>If cross-zone load balancing is disabled, each of the 2 targets in Availability Zone A receives <b>25%</b> of the traffic and each of the <b>8</b> targets in Availability Zone B receives <b>6.25%</b> of the traffic. This is because each load balancer node can route <b>50%</b> of the client traffic only to targets in its Availability Zone.</p>  <p>The diagram consists of two parts, each showing a client (laptop icon) at the top connected to two load balancers (orange circles with a white 'K' icon) in two separate Availability Zones (AZs), labeled 'Availability Zone A' and 'Availability Zone B' at the bottom. In the left part, representing cross-zone load balancing enabled, each load balancer is connected to two targets (orange squares) in its own AZ and four targets in the other AZ. The traffic distribution is labeled as 10% for each of the 10 targets. In the right part, representing cross-zone load balancing disabled, each load balancer is only connected to targets within its own AZ. In AZ A, there are 2 targets, each receiving 25% of the traffic. In AZ B, there are 8 targets, each receiving 6.25% of the traffic.</p>

	Cross-Zone Load Balancing Enabled	Cross-Zone Load Balancing Disabled
<b>Network ACLs</b>	A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. <b>You can't define an Inbound deny rule for Security Groups. You can only add allow rules to your Security Groups.</b>	
<b>AWS X-Ray</b>	You can use AWS X-Ray to trace and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services. API Gateway supports AWS X-Ray tracing for all API Gateway endpoint types: regional, edge-optimized, and private. You can use AWS X-Ray with Amazon API Gateway in all regions where X-Ray is available.  VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your entire VPC. Although it can capture some details about the incoming user requests, it is still better to use AWS X-Ray as it provides a better way to debug and analyze your micro services applications with request tracing so you can find the root cause of your issues and performance.	
<b>VPC Flow Logs</b>	✓ VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3	
<b>CloudTrail</b>	CloudTrail is primarily used for API logging of all of your AWS resources.	
<b>Amazon Redshift Enhanced VPC Routing</b>	✓ By using Enhanced VPC Routing, you can use VPC features to manage the flow of data between your cluster and other resources. ✓ You can also use VPC flow logs to monitor COPY and UNLOAD traffic.	

### High Availability

<b>Elastic Load Balancer (ELB)</b>	<p><b>Elastic Load Balancing supports three types of load balancers.</b></p> <ul style="list-style-type: none"> <li>✓ <b>Application Load Balancer.</b> If you need flexible application management and TLS termination then we recommend that you use Application Load Balancer. Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic.</li> <li>✓ <b>Network Load Balancer.</b> If extreme performance and static IP is needed for your application then we recommend that you use Network Load Balancer. Network Load Balancer can scale to millions of requests per second.</li> <li>✓ <b>Classic Load Balancer.</b> If your application is built within the EC2 Classic network then you should use Classic Load Balancer. Classic ELB cannot scale to handle millions of requests per second.</li> </ul> <p>✓ <b>Elastic Load Balancing supports the Server Order Preference option for negotiating connections between a client and a load balancer.</b></p>
------------------------------------	---

### Storage and Data Management

<b>S3 Glacier</b>	<p>Amazon S3 Glacier is a storage service optimized for infrequently used data, or "cold data."</p> <p>Glacier works together with Amazon S3 lifecycle rules to help you automate archiving of S3 data and reduce your overall storage costs.</p> <ul style="list-style-type: none"> <li>✓ Glacier is an extremely low-cost storage service.</li> <li>✓ It provides durable storage with security features for data archiving and backup.</li> <li>✓ Customers can store their data cost effectively for months, years, or even decades.</li> <li>✓ It enables customers to offload the administrative burdens of operating and scaling storage to AWS, so they don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations.</li> </ul>
<b>Snowball and Snowball Edge</b>	<p>Snowball is designed as a data transport solution for moving high volumes of data into and out of a designated AWS region. Snowball Edge adds the additional capability to run simple computing functions on the device, for use cases that require local processing before returning the data to AWS.</p> <p>Snowball Storage Capacity - 80 TB Usable Capacity - 72 TB</p> <p>Snowball Edge Storage Capacity - 100 TB Usable Capacity - 83 TB</p>
<b>S3 Storage Classes</b>	<ul style="list-style-type: none"> <li>▪ <b>Storage Classes for Frequently Accessed Objects</b> <ul style="list-style-type: none"> <li>✓ S3 STANDARD - The default storage class. If you don't specify the storage class when you upload an object, Amazon S3 assigns the STANDARD storage class.</li> <li>✓ S3 REDUCED_REDUNDANCY - The Reduced Redundancy Storage (RRS) storage class is designed for noncritical, reproducible data that can be stored with less redundancy than the STANDARD storage class.</li> </ul> </li> <li>▪ <b>Storage Classes for Infrequently Accessed Objects</b> <ul style="list-style-type: none"> <li>✓ S3 STANDARD_IA - for long lived, but less frequently accessed data. It stores the object data redundantly across multiple geographically separated AZ's.</li> <li>✓ S3 ONEZONE_IA - stored the object data in only one AZ. Less expensive than STANDARD_IA, but data is not resilient to the physical loss of the AZ.</li> </ul> </li> <li>▪ <b>Glacier</b> <ul style="list-style-type: none"> <li>✓ For long-term archive.</li> <li>✓ Archived objects are not available for real-time access.</li> </ul> </li> </ul>

<b>RDS</b>	<ul style="list-style-type: none"> <li>✓ RDS does not support Oracle RAC (Real Application Cluster).</li> <li>✓ Read Replicas and Multi-AZ deployments are only used for RDS.</li> <li>✓ RDS is used to manage SQL databases.</li> </ul>
<b>RDS Read Replicas</b>	<p>Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.</p> <p><b>Launching a large ElastiCache instance is expensive compared to Read Replicas.</b></p>
<b>DynamoDB</b>	<ul style="list-style-type: none"> <li>✓ It provides high availability and durability since it replicates data across AWS regions. It is also fast, flexible and easily scalable, which is perfect for mobile backend.</li> <li>✓ DynamoDB is a fully managed NoSQL database.</li> </ul>
<b>DynamoDB global tables</b>	<p>Amazon DynamoDB global tables provide a fully managed solution for deploying a multi-region, multi-master database, without having to build and maintain your own replication solution. When you create a global table, you specify the AWS regions where you want the table to be available. DynamoDB performs all of the necessary tasks to create identical tables in these regions, and propagate ongoing data changes to all of them. Multi</p>
<b>Athena</b>	<p>Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.</p>
<b>Redshift</b>	<ul style="list-style-type: none"> <li>✓ It is a petabyte storage service for OLAP applications</li> <li>✓ Redshift is used as a data warehousing solution.</li> </ul>
<b>HTTP 503 Slow Down</b>	<p>If you notice a significant increase in the number of HTTP 503-slow down responses received for Amazon S3 PUT or DELETE object requests to a bucket that has versioning enabled, you might have one or more objects in the bucket for which there are millions of versions.</p>
<b>The instance always terminates after going into the pending state</b>	<p>The following are a few reasons why your EC2 instance goes from the pending state to the terminated state immediately after restarting it:</p> <ul style="list-style-type: none"> <li>✓ You've reached your EBS volume limit.</li> <li>✓ An EBS snapshot is corrupt.</li> <li>✓ The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.</li> <li>✓ The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file).</li> </ul>
<b>Protecting Data Using Server-Side Encryption</b>	<p>Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it.</p> <p><b>You have three mutually exclusive options depending on how you choose to manage the encryption keys:</b></p> <p><b>Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) :-</b> Each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.</p> <p><b>Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) :-</b></p>



	<p>Similar to SSE-S3, but with some additional benefits along with some additional charges for using this service. There are separate permissions for the use of an envelope key (that is, a key that protects your data's encryption key) that provides added protection against unauthorized access of your objects in S3. SSE-KMS also provides you with an audit trail of when your key was used and by whom.</p> <p><b>Use Server-Side Encryption with Customer-Provided Keys (SSE-C) :-</b> You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when you access your objects.</p> <p><b>You can't apply different types of server-side encryption to the same object simultaneously.</b></p>
<b>Multi-AZ DB instances</b>	Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. Creating this DB snapshot on a Single-AZ DB instance results in a brief I/O suspension that can last from a few seconds to a few minutes, depending on the size and class of your DB instance. Multi-AZ DB instances are not affected by this I/O suspension since the backup is taken on the standby.
<b>S3 analytics</b>	<b>S3 analytics</b> is a useful tool for analyzing storage access patterns to help you determine when to transition less frequently accessed Standard storage to the IA storage class. Once you see the access patterns in the data, you can then set a lifecycle policy which will transfer the contents to Glacier.

## Deployment and Provisioning

<b>cfn-signal</b>	The <b>cfn-signal helper script</b> signals AWS CloudFormation to indicate whether Amazon EC2 instances have been successfully created or updated.
<b>cfn-init</b>	The <b>cfn-init helper script</b> is mainly used to read template metadata from the AWS::CloudFormation::Init key. Although this can be used to install software packages in the EC2 instance, you still need to use the cfn-signal helper script to indicate whether the Amazon EC2 instance and the 3rd party package have been successfully created.
<b>cfn-get-metadata</b>	The <b>cfn-get-metadata helper script</b> is mainly used to fetch a metadata block from AWS CloudFormation and print it to standard out.
<b>cfn-hup</b>	The <b>cfn-hup helper script</b> is basically a daemon that detects changes in resource metadata and runs user-specified actions when a change is detected.
<b>Standard Reserved Instance &amp; Convertible Reserved Instance.</b>	<p><b>Standard Reserved Instance</b></p> <ul style="list-style-type: none"> <li>✓ It can upgrade or downgrade the instance size.</li> <li>✓ The instance size can be modified</li> <li>✓ The instance type cannot be modified</li> </ul> <p><b>Convertible Reserved Instance.</b></p> <ul style="list-style-type: none"> <li>✓ It can upgrade or downgrade the instance size.</li> <li>✓ The instance size can be modified</li> <li>✓ It can change the instance type</li> </ul>
<b>OpsWorks</b>	OpsWorks is a configuration management service that provides managed instances of <b>Chef</b> and <b>Puppet</b> . Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.
<b>AWS Step Functions</b>	<ul style="list-style-type: none"> <li>✓ AWS Step Functions provides server less orchestration for modern applications. Orchestration centrally manages a workflow by breaking it into multiple steps, adding flow logic, and tracking the inputs and outputs between the steps.</li> </ul>

	<ul style="list-style-type: none"> <li>✓ It can coordinate multiple AWS services into server less workflows.</li> </ul>
<b>AWS Direct Connect gateway</b>	<p>You can use an AWS Direct Connect gateway to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different regions.</p> <p>You associate a Direct Connect gateway with the virtual private gateway for the VPC, and then create a private virtual interface for your AWS Direct Connect connection to the Direct Connect gateway. You can attach multiple private virtual interfaces to your Direct Connect gateway. A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any public region and access it from all other public regions.</p>
<b>CIDR block</b>	<ul style="list-style-type: none"> <li>✓ Cannot modify the CIDR block of your subnet in AWS.</li> <li>✓ Cannot increase or decrease the size of an existing CIDR block.</li> <li>✓ <b>You can associate secondary IPv4 CIDR blocks with your VPC to increase its size.</b></li> <li>✓ <b>Can only add up to four (4) secondary CIDR blocks after the creation of the VPC.</b></li> </ul>

### Monitoring & Metrics

<b>AWS SNS</b>	AWS SNS to send event notifications as required on this scenario. Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables fan out notifications to end users using mobile push, SMS, and email. Amazon SNS is simple and cost effective to send push notifications to mobile device users, email recipients and email to other distributed services.
<b>AWS SES</b>	AWS SES (Simple Email Service) is used as an AWS hosted emailing service.
<b>CloudTrail</b>	CloudTrail is used for API logging services and activities across your AWS infrastructure.
<b>CloudWatch</b>	<ul style="list-style-type: none"> <li>✓ This service is used for logging metrics and monitoring AWS resources.</li> <li>✓ You can monitor AWS resources in multiple Regions using a single CloudWatch dashboard, but you cannot aggregate the data across Regions.</li> <li>✓ There is no "<b>Memory Utilization</b>" metric available in CloudWatch for EC2. You have to setup a custom metric to set this up.</li> </ul>
<b>ELB access logs</b>	Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.
<b>Amazon API Gateway</b>	Amazon API ( <b><i>Application Program Interface</i></b> ) Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.
<b>CloudFront Reports</b>	<ul style="list-style-type: none"> <li>✓ <b>Popular Objects Report</b> can determine what objects are frequently being accessed, and get statistics on those objects.</li> <li>✓ <b>Usage Reports</b> tells you the number of HTTP and HTTPS requests that CloudFront responds to from edge locations in selected regions.</li> <li>✓ <b>Viewers Reports</b> can determine the locations of the viewers that access your content most frequently.</li> <li>✓ <b>CloudFront Cache Statistics Reports</b></li> </ul> <p>The CloudFront cache statistics report includes the following information:</p> <ol style="list-style-type: none"> <li>1. Total Requests</li> <li>2. Percentage of Viewer Requests by Result Type</li> <li>3. Bytes Transferred to Viewers</li> <li>4. HTTP Status Codes</li> </ol>

	<p>5. Percentage of GET Requests that Didn't Finish Downloading</p> <p>✓ <b>The CloudFront top referrers report</b> includes the top 25 referrers, the number of requests from a referrer, and the number of requests from a referrer as a percentage of the total number of requests during the specified period.</p>
--	--

### Security and Compliance

<b>Load balancer with Security features</b>	<ul style="list-style-type: none"> <li>✓ SSL Server Certificates</li> <li>✓ SSL Negotiation</li> <li>✓ Back-End Server Authentication</li> </ul>
<b>AWS services (To provide log files for all activities carried out on AWS)</b>	<p><b><u>AWS CloudTrail</u></b> is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides an event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.</p> <p><b><u>Amazon CloudWatch</u></b> Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances and other services, this will not provide you with all the activities recorded for each AWS resource.</p> <p><b><u>AWS Trusted Advisor</u></b> will only give you recommendations to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, and follow best practices for your AWS resources.</p> <p><b><u>AWS Config</u></b> is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. This is used mainly for ensuring your AWS resources have the correct configuration according to your specified internal guidelines.</p>
<b>AWS Certificate Manager</b>	<p><b><u>AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks.</u></b></p>