

## Monitoring &amp; Reporting

CloudWatch	<p>It is a monitoring service to monitor AWS resources, as well as applications that you run on AWS.</p> <p><b>CloudWatch can monitor things like:</b></p> <table border="1"> <tr> <td data-bbox="456 254 764 352"><b>Compute</b></td><td data-bbox="764 254 1414 352">Autoscaling Groups Elastic Load Balancers Route53 Health Checks</td></tr> <tr> <td data-bbox="456 352 764 457"><b>Storage &amp; Content Delivery</b></td><td data-bbox="764 352 1414 457">EBS Volume Storage Gateways CloudFront</td></tr> <tr> <td data-bbox="456 457 764 636"><b>Databases &amp; Analytics</b></td><td data-bbox="764 457 1414 636">Dynamo DB Elasticache Nodes RDS Instances Elastic MapReduce Job Flows Redshift</td></tr> <tr> <td data-bbox="456 636 764 814"><b>Other</b></td><td data-bbox="764 636 1414 814">SNS Topics SQS Queues Opsworks CloudWatch Logs Estimated Charges on AWS Bill</td></tr> <tr> <td data-bbox="456 814 764 961"><b>EC2 Instance (Host Level Default Metrics)</b></td><td data-bbox="764 814 1414 961">CPU Network Disk Status Check</td></tr> </table>	<b>Compute</b>	Autoscaling Groups Elastic Load Balancers Route53 Health Checks	<b>Storage &amp; Content Delivery</b>	EBS Volume Storage Gateways CloudFront	<b>Databases &amp; Analytics</b>	Dynamo DB Elasticache Nodes RDS Instances Elastic MapReduce Job Flows Redshift	<b>Other</b>	SNS Topics SQS Queues Opsworks CloudWatch Logs Estimated Charges on AWS Bill	<b>EC2 Instance (Host Level Default Metrics)</b>	CPU Network Disk Status Check
<b>Compute</b>	Autoscaling Groups Elastic Load Balancers Route53 Health Checks										
<b>Storage &amp; Content Delivery</b>	EBS Volume Storage Gateways CloudFront										
<b>Databases &amp; Analytics</b>	Dynamo DB Elasticache Nodes RDS Instances Elastic MapReduce Job Flows Redshift										
<b>Other</b>	SNS Topics SQS Queues Opsworks CloudWatch Logs Estimated Charges on AWS Bill										
<b>EC2 Instance (Host Level Default Metrics)</b>	CPU Network Disk Status Check										
CloudWatch Dashboard	Dashboards are multi-region and can display any widget to any region. To add the widget, change to the region that you need and then add the widget to the dashboard.										
Exam Tips	<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> <li>✓ <b>Storage of disks</b> couldn't monitor by using host level metrics.</li> </ul> <p><b>Custom Metrics</b> - Minimum granularity is 1 minute. RAM and Disk utilizations are custom metric.</p> <p><b>Terminated Instances</b> - We can retrieve data from any terminated EC2 or ELB instance after its termination. CloudWatch logs by default are stored indefinitely.</p> <p><b>Metric Granularity</b> - 1 minute for detailed monitoring. 5 minute for standard monitoring.</p> <p><b>CloudWatch can be used on premise</b> - It's not restricted to just AWS resources. Can be on premise too. Just need to download and install the SSM agent and CloudWatch agent.</p>										
CloudWatch Alarms	We can create an alarm to monitor any Amazon CloudWatch metric in our account. This can include EC2 CPU Utilization, Elastic Load Balancer Latency and Charges on AWS bill. We can set the appropriate thresholds in which to trigger the alarms and also set what actions should be taken if an alarm state is reached.										
Monitor Load Balancer	<p><b>4 Different ways to monitor load balancer</b></p> <p><b>1. CloudWatch metrics</b></p> <p>ELB publishes data points to Amazon CloudWatch. CloudWatch enables us to retrieve statistics about those points as an ordered set of time series data, known as metrics. Think of a metric as a variable to monitor, and the data points as the values of that variable over time.</p> <p>For example, we can monitor the total number of healthy targets for a load balancer over a specified time period. Each data point has an associated time stamp and an optional unit of measurement.</p>										

	<p><b>2. Access logs</b></p> <p>ELB provides access logs that capture detailed information about requests sent to 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. We can use this access logs to analyze traffic patterns and troubleshoot issues.</p> <p>It is an optional feature of ELB that is disabled by default. The captured logs are stored in the S3 bucket.</p> <p><b>"Access logs can store data where the EC2 instances has been deleted." For some reason our application has a load of 5xx errors which is only reported by customers a couple of days after the event. If we are not storing the web server logs anywhere persistent, it is still possible to trace these 5xx error using Access logs which would be stored on S3.</b></p> <p><b>3. Request tracing (Available for Application Load Balancers Only)</b></p> <p>We can use request tracing to track HTTP requests from clients to targets or other services. When the load balancer receives a request from a client, it adds or updates the Trace id header before sending the request to the target. Any services or applications between the load balancer and the target can also add or update this header.</p> <p><b>4. CloudTrail logs</b></p> <p>We can use AWS CloudTrail to capture detailed information about the calls made to the Elastic Load Balancing API and store them as log files in S3. We can use these logs to determine which calls were made, the source IP address where the call came from, who made the call, when the call was made, and so on.</p>
<b>ELB Cloud Watch</b>	<ul style="list-style-type: none"> <li>Load Balancer Metrics are published to CloudWatch.</li> <li>You can create a CloudWatch alarm to send you a notification if a certain metric reaches a user defined limit.</li> </ul> <p><b>Types of Metrics</b></p> <ul style="list-style-type: none"> <li>Metrics for general health (Healthy Host Count, HTTP Code etc.).</li> <li>Metrics for performance (Latency, Request Count etc.).</li> </ul>
<b>SurgeQueueLength &amp; SpilloverCount</b>	<p>The amount of request traffic being sent to the ELB is causing the surge queue to fill up relatively quickly.</p> <ul style="list-style-type: none"> <li>✓ The <b>SurgeQueueLength</b> metric tells us the total number of requests (HTTP listener) or connections (TCP listener) that are pending routing to a healthy instance. Additional requests or connections are rejected when the queue is full.</li> <li>✓ The <b>SpilloverCount</b> metric then becomes helpful here because it tells us the total number of requests that were rejected when the surge queue becomes full. From these two metrics, we can therefore estimate how many more instances we need to spin up.</li> </ul>
<b>System Manager</b>	<p>System Manager is used to give visibility and control over your AWS infrastructure. Integrates with CloudWatch dashboards.</p> <p>Allows you to organize your inventory and logically group resources together.</p> <p>Run Command enables to you to perform common operational tasks on groups of instances simultaneously without needing log in to each one.</p>
<b>CloudWatch Vs CloudTrail</b>	<ul style="list-style-type: none"> <li>✓ <b>CloudWatch monitors performance.</b></li> </ul> <p>Monitor EC2 resources like CPU utilizations, Memory utilizations etc.</p> <ul style="list-style-type: none"> <li>✓ <b>CloudTrail monitors API calls in the AWS platform</b></li> </ul> <p>Monitor EC2 instances, RDS instances, Users, S3 buckets etc.</p>
<b>CloudTrail</b>	<p>CloudTrail is used for API logging services and activities across your AWS infrastructure.</p> <p>CloudTrail is a web service that records AWS API calls for your AWS account and delivers log files to an Amazon S3 bucket. The recorded information includes the identity of the user, the start time of the AWS API call, the source IP address, the request parameters, and the response elements returned by the service.</p> <p>Amazon EC2, Amazon EBS, and Amazon VPC are integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon EC2, Amazon EBS, and Amazon VPC. CloudTrail captures all API calls for Amazon EC2, Amazon EBS, and Amazon VPC as events, including calls from the console and from code calls to the APIs.</p>

	<p>If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon EC2, Amazon EBS, and Amazon VPC.</p> <p>If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to Amazon EC2, Amazon EBS, and Amazon VPC, the IP address from which the request was made, who made the request, when it was made, and additional details.</p>
<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>AWS Config</b>	<p><b>AWS Config</b> records the state of AWS environment and can notify you of changes.</p> <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>✓ AWS Config enables continuous monitoring of your AWS resources, making it simple to assess, audit, and record resource configurations and changes.</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 Cost and Usage Report</b>	The AWS Cost and Usage report tracks your AWS usage and provides estimated charges associated with your AWS account. The report contains line items for each unique combination of AWS product, usage type, and operation that your AWS account uses. You can customize the AWS Cost and Usage report to aggregate the information either by the hour or by the day.
<b>The Cost Optimization Monitor</b>	The Cost Optimization Monitor can help you generate reports that provide insight into service usage and costs as you deploy and operate cloud architecture.
<b>AWS Config Rules</b>	<p><b>Permission needed for Config:</b></p> <p><b>AWS Config requires an IAM Role with</b></p> <ol style="list-style-type: none"> <li>1. Read only permission to the recorded resources.</li> <li>2. Write access to S3 logging bucket</li> <li>3. Publish access to SNS</li> </ol> <p><b>Restricted Access:</b></p> <ol style="list-style-type: none"> <li>1. Users need to be authenticated with AWS and have the appropriate permissions set via IAM policies to gain access.</li> <li>2. Only Admins needing to set up and manage Config require full access.</li> <li>3. Provide read only permissions for Config day-to-day use.</li> </ol> <p><b>Monitoring Config:</b></p> <ol style="list-style-type: none"> <li>1. Use CloudTrail with Config to provide deeper insight into resources.</li> <li>2. Use CloudTrail to monitor access to Config, such as someone stopping the Config Recorder.</li> </ol>
<b>Health Dashboards</b>	<p><b>Service Health Dashboard</b> - Shows the health of each AWS Service as a whole per region.</p> <p><b>Personal Health Dashboard</b> - It provides alerts when AWS is experiencing events that may impact you. Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.</p>
<b>Monitoring ElastiCache</b>	<p><b>ElastiCache consists of two engines</b></p> <ol style="list-style-type: none"> <li>1. <b>MemCached</b></li> <li>2. <b>Redis</b></li> </ol> <p>ElastiCache provides metrics that enable us to monitor our clusters. We can access these metrics through CloudWatch.</p> <p>ElastiCache provides both host-level metrics (for example, CPU usage) and metrics that are specific to the cache engine software (for example, cache gets and cache misses). These metrics are measured and published for each Cache node in 60-second intervals.</p> <p>We should consider setting CloudWatch alarms on certain key metrics, so that we will be notified if our cache cluster's performance starts to degrade.</p>

	<p><b>ElastiCache monitor our caching engines there are 4 important things to look at:</b></p> <p><b>1. CPU Utilization</b></p> <table border="1"> <thead> <tr> <th>MemCached</th><th>Redis</th></tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> <li>Multi-threaded.</li> <li>Can handle loads of up to 90%. If it exceeds 90% add more nodes to the cluster</li> </ul> </td><td> <ul style="list-style-type: none"> <li>Not multi-threaded. To determine the point in which to scale, take 90 and divided by the number of cores.</li> </ul> <p>For example, suppose we are using a cache.m1.node, which has four cores. In this case, the threshold for CPU utilization would be <math>(90/4)</math>, or 22.5%</p> </td></tr> </tbody> </table> <p><b>2. Swap Usage</b></p> <p><b>3. Evictions</b></p> <table border="1"> <thead> <tr> <th>MemCached</th><th>Redis</th></tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> <li>There is no recommended settings. Choose a threshold based off our application.</li> <li>Either Scale Up (i.e. increase the memory of existing nodes) or Scale Out (add more nodes).</li> </ul> </td><td> <ul style="list-style-type: none"> <li>There is no recommended settings. Choose a threshold based off our application.</li> <li>Only Scale Out (add read replicas)</li> </ul> </td></tr> </tbody> </table> <p><b>4. Concurrent Connections</b></p> <p>MemCached &amp; Redis</p> <ul style="list-style-type: none"> <li>There is no recommended settings. Choose a threshold based off our application.</li> <li>If there is a large and sustained spike in the number of concurrent connections this can either mean a large traffic spike or our application is not releasing connections as it should be.</li> </ul>	MemCached	Redis	<ul style="list-style-type: none"> <li>Multi-threaded.</li> <li>Can handle loads of up to 90%. If it exceeds 90% add more nodes to the cluster</li> </ul>	<ul style="list-style-type: none"> <li>Not multi-threaded. To determine the point in which to scale, take 90 and divided by the number of cores.</li> </ul> <p>For example, suppose we are using a cache.m1.node, which has four cores. In this case, the threshold for CPU utilization would be <math>(90/4)</math>, or 22.5%</p>	MemCached	Redis	<ul style="list-style-type: none"> <li>There is no recommended settings. Choose a threshold based off our application.</li> <li>Either Scale Up (i.e. increase the memory of existing nodes) or Scale Out (add more nodes).</li> </ul>	<ul style="list-style-type: none"> <li>There is no recommended settings. Choose a threshold based off our application.</li> <li>Only Scale Out (add read replicas)</li> </ul>
MemCached	Redis								
<ul style="list-style-type: none"> <li>Multi-threaded.</li> <li>Can handle loads of up to 90%. If it exceeds 90% add more nodes to the cluster</li> </ul>	<ul style="list-style-type: none"> <li>Not multi-threaded. To determine the point in which to scale, take 90 and divided by the number of cores.</li> </ul> <p>For example, suppose we are using a cache.m1.node, which has four cores. In this case, the threshold for CPU utilization would be <math>(90/4)</math>, or 22.5%</p>								
MemCached	Redis								
<ul style="list-style-type: none"> <li>There is no recommended settings. Choose a threshold based off our application.</li> <li>Either Scale Up (i.e. increase the memory of existing nodes) or Scale Out (add more nodes).</li> </ul>	<ul style="list-style-type: none"> <li>There is no recommended settings. Choose a threshold based off our application.</li> <li>Only Scale Out (add read replicas)</li> </ul>								
<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>								
<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>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>AWS Organizations</b>	<p><b>AWS Organizations</b></p> <ul style="list-style-type: none"> <li>Centrally managed policies across multiple AWS accounts.</li> <li>Control access to AWS services.</li> <li>Automate AWS account creation and management.</li> <li>Consolidate billing across multiple AWS accounts.</li> </ul>								
<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>EC2 Pricing</b>	<p><b>On Demand</b> - Allow you to pay a fixed rate by the hour with no commitment.</p> <p><b>Reserved</b> - Provide you with a capacity reservation, and offer a significant discount on the hourly charge for an instance. 1 - 3 year terms.</p>								

	<p><b>Spot</b> - Enable you to bid whatever price you want for instance capacity, providing for even greater savings if your application have flexible start and end times.</p> <p><b>Dedicated Hosts</b> - Physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software license.</p>
<b>AWS Resource Group &amp; Tagging</b>	<p><b>Tags</b></p> <ul style="list-style-type: none"> <li>• It's a key value pairs attached to AWS resources.</li> <li>• Metadata</li> <li>• Tags can sometimes be inherited             <ul style="list-style-type: none"> <li>- Autoscaling, CloudFormation, and Elastic Beanstalk can create other resources.</li> </ul> </li> </ul> <p><b>Resource Groups</b></p> <p>Resource groups make it easy to group your resources using the tags that are assigned to them. You can group resources that share one or more tags. Resource group contain information such as;</p> <ul style="list-style-type: none"> <li>• Region</li> <li>• Name</li> <li>• Health Checks</li> </ul> <p>Specific information</p> <ul style="list-style-type: none"> <li>• For EC2 - Public &amp; Private IP Address</li> <li>• For ELB - Port Configurations</li> <li>• For RDS – Database Engine etc.</li> </ul> <p><b>Two Types of Resource Groups</b></p> <ol style="list-style-type: none"> <li>1. Classic Resource Groups</li> <li>2. AWS Systems Manager</li> </ol>

## Deployment & Provisioning

<b>EC2 Launch Issues</b>	<p><b>Instance Limit Exceeded error</b></p> <ul style="list-style-type: none"> <li>▪ You have reached the limit on the number of instances you can launch in a Region.</li> <li>▪ AWS sets default limits on the number of instances you can run on a per-region basis – 20 by default.</li> <li>▪ You can request an increase on a per-region basis.</li> </ul> <p><b>Insufficient Instance Capacity error</b></p> <ul style="list-style-type: none"> <li>▪ AWS does not currently have enough available On-Demand capacity to service your request.</li> </ul>
<b>EBS Volumes &amp; IOPS</b>	<ul style="list-style-type: none"> <li>▪ IOPS (Input/output Operations per second) used to benchmark performance for SSD volumes.</li> <li>▪ IOPS is dependent on the size of your volume.</li> <li>▪ If your workload is hitting the IOPS limit for your volume:             <ol style="list-style-type: none"> <li>1. Increase the volume size - (Only works if your gp2 volume is &lt; 5.2TB)</li> <li>2. Change to Provisioned IOPS if your gp2 volume is 5.2TB or greater, or you need more than 16k IOPS.</li> </ol> </li> </ul>
<b>AWS Elastic Beanstalk</b>	<p>AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.</p> <p>You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.</p>
<b>Elastic Beanstalk through CLI</b>	<p>AWS EB CLI cannot create the instance profile for your beanstalk environment if your IAM role has no access to creating roles.</p> <p>This error is also thrown when the instance profile has insufficient or outdated policies that beanstalk needs to function.</p>

<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> <li>✓ It can coordinate multiple AWS services into server less workflows.</li> </ul>
<b>T2 and T3 instances</b>	You can use T2 and T3 instances to prove a baseline level of CPU performance for your fleet of EC2 instances. It can also provides the ability to burst CPU usage to handle the occasional peak loads.
<b>CloudFormation stacks</b>	When you need to make changes to a stack's settings or change its resources, you update the stack instead of deleting it and creating a new stack

## High Availability

<b>Scalability Vs Elasticity</b>	<ul style="list-style-type: none"> <li>▪ <b>Elasticity</b> - Scale with Demand (Short Term).</li> <li>▪ <b>Scalability</b> - Scale out Infrastructure (Long Term).</li> </ul> <p><b>EC2</b></p> <ul style="list-style-type: none"> <li>▪ <b>Scalability</b> - Increase instance size as required, using reserved instances.</li> <li>▪ <b>Elasticity</b> - Increase the number of EC2 instances, based on Autoscaling.</li> </ul> <p><b>DynamoDB</b></p> <ul style="list-style-type: none"> <li>▪ <b>Scalability</b> - Unlimited amount of storage.</li> <li>▪ <b>Elasticity</b> - Increase additional IOPS for additional spikes in traffic. Decrease that IOPS after the spikes.</li> </ul> <p><b>RDS</b></p> <ul style="list-style-type: none"> <li>▪ <b>Scalability</b> - Increase instance size.</li> <li>▪ <b>Elasticity</b> - Not very elastic, cant scale RDS based on demand.</li> </ul> <p><b>Aurora</b></p> <ul style="list-style-type: none"> <li>▪ <b>Scalability</b> - Modify the instance type.</li> <li>▪ <b>Elasticity</b> - Aurora Server less.</li> </ul>
<b>RDS Multi-AZ Failover</b>	<p>Multi AZ (Availability Zone) keeps a copy of your production database in a separate Availability Zone in case of a failure or disaster. AWS manage the failure from one AZ to another automatically.</p> <p><b>Multi-AZ RDS</b></p> <p>Multi-AZ is for Disaster Recovery Only. It is not primarily used for improving performance. For performance improvement, you need Read Replicas.</p>

	<p>Multi-AZ allows you to have an exact copy of your production data base in another AZ. AWS handle the replication for you, so when your production database is written to, this write will automatically be synchronized to the stand by database. In the event of planned database maintenance, DB instance failure, or an AZ failure, Amazon RDS will automatically failover to the standby so that database operations can resume quickly without administrative intervention.</p> <p><b>RDS Multi-AZ Failover Advantages</b></p> <p>High Availability</p> <p>Backups &amp; Restores are taken from the secondary which avoids I/O suspension to the primary.</p> <p><b>Exam Tips</b></p> <ul style="list-style-type: none"> <li>▪ RDS Multi-AZ Failover is not a <b>Scaling Solution</b>.</li> <li>▪ Amazon handles the failover for you. Done by updating the private DNS for the database endpoint.</li> <li>▪ Backups &amp; Restores are taken from the secondary Multi-AZ instances.</li> <li>▪ Read Replicas are used to scale.</li> <li>▪ You can force a failover from one AZ to another by rebooting your instance. This can be done through the AWS management console or by using RebootDBInstance API call.</li> </ul>
<b>Read Replicas</b>	<p>Read Replicas make it easy to take advantage of supported engine's built in replication functionality to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads.</p> <p><b>* Read only copies of your database.</b></p> <p><b>* Replica of your production database is read only</b></p> <p><b>* Once Read Replica is created, database updates on the source DB Instances will be replicated using a support engine's native, asynchronous replication. You can create multiple Read Replicas for a given source DB Instance and distribute your application's read traffic amongst them.</b></p> <p><b>Exam Tips</b></p> <ul style="list-style-type: none"> <li>• You can have up to 5 read replicas for MySQL, PostgreSQL &amp; Maria DB.</li> <li>• You can have read replicas in different REGIONS for all engines.</li> <li>• Replication is Asynchronous only, not synchronous.</li> <li>• Read Replicas can be built off Multi-AZ's databases.</li> <li>• Read Replica's themselves can now be Multi-AZ.</li> <li>• You can have Read Replica's of Read Replica's beware of latency.</li> <li>• DB Snapshots and Automated backups cannot be taken of read replicas.</li> <li>• Key Metric to look for is REPLICA LAG.</li> </ul>
<b>Aurora</b>	<p><b>Amazon Aurora provides up to five times better performance than MySQL (3 times better performance than PostgreSQL).</b></p> <p><b>Aurora comes in 2 flavours</b></p> <ul style="list-style-type: none"> <li>▪ Aurora</li> <li>▪ Aurora Serverless</li> </ul> <p><b>Redundancy</b></p> <p>2 copies of your data is contained in 3 separate availability zones with a total of 6 copies.</p> <p><b>Storage is Self Healing</b></p> <p>Data blocks and disks are continuously scanned for errors and repaired automatically.</p> <p><b>Aurora at 100% CPU utilization?</b></p> <p>Is it writes causing the issue? If so Scale Up (increase instance size)</p> <p>Is it reads causing the issue? If so Scale Out (increase the number of read replicas)</p>
<b>Elastic Load Balancer (ELB)</b>	<p><b>Elastic Load Balancing supports three types of load balancers.</b></p> <p>✓ <b>Application Load Balancer.</b></p> <p>If you need flexible application management and TLS termination then we recommend that you use Application Load Balancer.</p> <p>Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic.</p>



	<p>✓ <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.</p> <p>✓ <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.</p> <p>✓ <b>Elastic Load Balancing supports the Server Order Preference option for negotiating connections between a client and a load balancer.</b></p>
<b>Internal Classic Load Balancers</b>	<p><b>Internal load balancer &amp; Internet-facing load balancer</b> 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>Auto Scaling</b>	Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size.
<b>RESTful</b>	REST is used to build Web services that are lightweight, maintainable, and scalable in nature. A service which is built on the REST architecture is called a RESTful service. The underlying protocol for REST is HTTP, which is the basic web protocol. REST stands for REpresentational State Transfer.
<b>Elastic Container Service (ECS)</b>	Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers and allows you to easily run and scale containerized applications on AWS. Amazon ECS eliminates the need for you to install and operate your own container orchestration software, manage and scale a cluster of virtual machines, or schedule containers on those virtual machines.

## Storage & Data Management

<b>S3</b>	Public access to S3 bucket is disabled by default.
<b>S3 Lifecycle Policies</b>	<p><b>Exam Tips</b> S3 Lifecycle policies are used to ensure you are using the most cost effective option to store your objects in S3. Lifecycle rules are based on object creation date. S3 can transition your objects to <b>Infrequently Accessed Storage</b> or to <b>Glacier</b> based on the rules you configure. You can also set an expiry date for objects you want S3 to delete after a certain time period has elapsed.</p>
<b>S3 Versioning</b>	<ul style="list-style-type: none"> <li>• S3 Versioning enables you to revert to older versions of S3 objects.</li> <li>• Multiple versions of an object are stored in the same bucket.</li> </ul>



	<ul style="list-style-type: none"> <li>Versioning also protects you from accidental / malicious deletes.</li> <li>With versioning enabled, a <b>DELETE</b> action doesn't delete the object version, but applies a delete marker instead.</li> <li>To permanently delete, provide the object Version ID in the delete request.</li> </ul>
<b>MFA Delete</b>	<ul style="list-style-type: none"> <li>It provides an additional layer of protection to S3 Versioning.</li> <li>Use MFA Delete to protect against accidental or malicious deletions of your version-controlled S3 buckets.</li> <li>Two things that MFA Delete enforces:             <ol style="list-style-type: none"> <li>Need a valid code from your MFA device to enable permanent deletion of an S3 object.</li> <li>Need a valid code from your MFA device to suspend or reactivate versioning on the S3 bucket.</li> </ol> </li> </ul>
<b>S3 Encryption</b>	<ul style="list-style-type: none"> <li><b>Encryption In-Transit</b> <ol style="list-style-type: none"> <li>SSL/TLS (HTTPS) Encrypts the data over the network (B/w your PC and S3).</li> </ol> </li> <li><b>Encryption At Rest</b> <ol style="list-style-type: none"> <li>Server Side Encryption                 <ol style="list-style-type: none"> <li>SSE-S3 - Amazon S3 managed keys</li> <li>SSE-KMS - Amazon KMS managed keys</li> <li>SSE-C - Customer managed keys</li> </ol> </li> <li>Client Side Encryption Encrypt your file locally before uploading to S3.</li> </ol> </li> </ul> <p><b>Note:</b> - If you want to enforce the use of encryption for your files stored in S3, use an S3 Bucket Policy to deny all PUT requests that don't include the x-amz-server-side-encryption parameter in the request header.</p>
<b>EC2 Volume Types</b>	<p><b>EBS vs Instance Store</b></p> <ul style="list-style-type: none"> <li>Root device volumes can either be EBS volumes or Instance Store volumes.</li> <li>An instance store root device volume's maximum size is 10GB</li> <li>EBS root device volume can be up to 1 or 2TB depending on the OS.</li> </ul> <p><b>Exam Tips</b></p> <ul style="list-style-type: none"> <li>'Delete on Termination' is the default for all EBS root device volumes. You can set this to false however but only at instance creation time.</li> <li>Additional volumes will persist automatically. You need to delete these manually when you delete an instance.</li> <li>Instance Store is known as ephemeral storage, meaning that data will not persist after an instance is deleted. You cannot set this to false, data will always be deleted when that instance disappears.</li> </ul>
<b>Volume &amp; Snapshots</b>	<ul style="list-style-type: none"> <li>Volumes exist on EBS:             <ul style="list-style-type: none"> <li>Virtual Hard Disk</li> </ul> </li> <li>Snapshots exist on S3.</li> <li>Snapshots are point in time copies of Volumes.</li> <li>Snapshots are incremental – this means that only the blocks that have changed since your last snapshot are moved to S3.</li> <li>If this is your first snapshot, it may take some time to create.</li> </ul>
<b>Snapshots of Root Device Volume</b>	<ul style="list-style-type: none"> <li>To create a snapshot for Amazon EBS volumes that serve as root devices, you should stop the instance before taking the snapshot.</li> <li>However you can take a snap while the instance is running.</li> <li>You can create AMI's from both Images and Snapshots</li> <li>You can change EBS volume sizes on the fly, including changing the size and storage type.</li> <li>Volumes will ALWAYS be in the same availability zone as the EC2 instance.</li> <li>To move an EC2 volume from one AZ/Region to another, take a snap or an image of it, then copy it to the new AZ/Region</li> </ul>

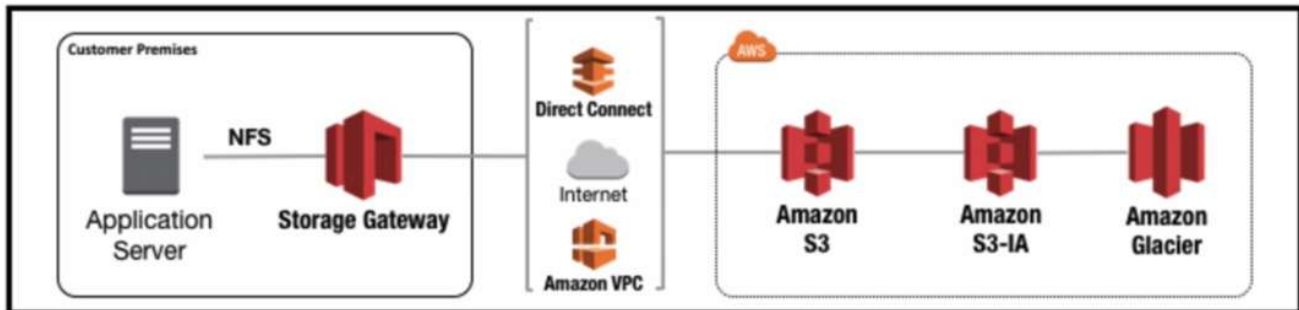
<b>Volumes &amp; Snapshots</b>	<ul style="list-style-type: none"> <li>• Snapshots of encrypted volumes are encrypted automatically.</li> <li>• Volumes restored from encrypted snapshots are encrypted automatically.</li> <li>• You can share snapshots, but only if they are unencrypted. <ul style="list-style-type: none"> <li>• These snapshots can be shared with other AWS accounts or made public.</li> </ul> </li> </ul>
<b>Encryption &amp; Downtime</b>	<p><b>Enabling Encryption</b> For most AWS resources, encryption can only be enabled <b>at creation</b>.</p> <p><b>EFS (Elastic File System)</b> - If you want to encrypt an EFS filesystem that already exists, you will need to create a new encrypted EFS and migrate your data.</p> <p><b>RDS (Relational Database)</b> - If you want to encrypt an existing RDS, you will need to create a new encrypted database and migrate your data.</p> <p><b>EBS Volumes</b> - Encryption must be selected <b>at creation time</b>. You cannot encrypt an unencrypted volume or unencrypt an encrypted volume. So you cannot change the encryption status of EBS volume. You can migrate data between encrypted and unencrypted volumes.</p> <p><b>S3 Buckets</b> - You can enable encryption on your S3 Buckets <b>at any time</b>.</p> <p><b>S3 Objects</b> - You can enable encryption individual S3 objects <b>at any time</b>.</p> <p><b>Exam Tips:</b> Remember that for the majority of services, you will need to enable encryption at creation time.</p> <ul style="list-style-type: none"> <li>• EFS</li> <li>• RDS</li> <li>• EBS Volumes</li> <li>• To add an encryption later will involve migrating your data in some way, you may wish to stop your applications at this time.</li> </ul> <p><b>S3 has greater flexibility, and you can enable for S3 Buckets or Objects at any time and without disrupting your applications.</b></p>
<b>Glacier Vault Lock</b>	<p>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.</p>
<b>KMS &amp; CloudHSM</b>	<ul style="list-style-type: none"> <li>• Both allow you to generate, store and manage cryptographic keys used to protect your data in AWS.</li> <li>• HSMs (Hardware Security Modules) are used to protect the confidentiality of your keys. It is a physical device. It is often used in financial payment systems. It can be used in Credit/Debit Card payment systems.</li> <li>• Both offer a high level of security.</li> </ul> <p><b>KMS Vs CloudHSM</b></p> <p><b>KMS:-</b></p> <ul style="list-style-type: none"> <li>• Shared hardware, multi-tenant managed service.</li> <li>• Allows you to generate, store and manage your encryption keys.</li> <li>• Suitable for applications for which multi-tenancy is not an issue.</li> <li>• Free-tier eligible.</li> <li>• Encrypt data stored in AWS, including EBS Volume, S3, RDS, DynamoDB etc.</li> </ul> <p><b>Cloud HSM:-</b></p> <ul style="list-style-type: none"> <li>• Dedicated HSM instance, hardware is not shared with other tenants no Free-Tier.</li> <li>• Allows you to generate, store and manage your encryption keys.</li> <li>• HSM is under your exclusive control within your own VPC.</li> <li>• FIPS 140-2 Level 3 compliance (US Government standard for HSMs).</li> <li>• Use cases include: Database encryption, Digital Rights Management (DRM), Public Key Infrastructure (PKI), Authentication and Authorization, Document Signing. And Transaction processing.</li> </ul>

	<p><b>Exam Tips:</b></p> <ul style="list-style-type: none"> <li>Both KMS and CloudHSM enable you to generate, store and manage your own encryption keys to encrypt data stored in AWS.</li> <li>KMS is multi-tenancy and good for use cases which do not require dedicated hardware.</li> <li>If your application has a requirement for dedicated hardware for managing keys, use CloudHSM.</li> </ul>
<b>AMIs</b>	<p><b>Exam Tips:</b></p> <ul style="list-style-type: none"> <li>It provide a template for launching EC2 instances</li> <li>You can create your own custom AMI from a customized EC2 instance.</li> <li>AMIs are region-bound, so if you are attempting to launch an instances in a new region using a custom AMI, make sure you have copied your AMI to the new destination region.</li> </ul> <p><b>Sharing AWS AMIs:</b></p> <ul style="list-style-type: none"> <li>AMI can be shared and copied between user accounts.</li> <li>Generally AMI is stored within S3.</li> <li>The owner of the source AMI must grant you read permission for the storage in order to enable you to copy the AMI.</li> <li>Remember the 2 restrictions:</li> </ul> <p><b>1. Encrypted AMIs</b> - Copy the underlying snapshot, re-encrypt using your own key and create a new AMI from the snapshot.</p> <p><b>2. AMI with an associated Billing Products code</b> - You cannot directly copy an AMI with an associated <b>Billing Products</b> code (Applies to Windows, RedHat and Amis from AWS Marketplace)..</p>
<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><b>Snowball</b> is for Data transfer only</p> <p><b>Snowball Edge</b> provides Edge Computing in addition to data transfer.</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>Storage Gateway</b>	<p><b>Storage Gateway</b> consists of an on-premises software appliance which connects with AWS cloud-based storage to give you a seamless and secure integration between your on premises IT environment and AWS.</p> <p><b>Types of Storage Gateway</b></p> <ul style="list-style-type: none"> <li><b>File Gateway - NFS / SMB</b> <ol style="list-style-type: none"> <li>Files stored as objects in your S3 buckets</li> <li>Accessed using NFS or SMB mount point</li> <li>To your on-premises systems this appears like a file system mount backed by S3</li> <li>All the benefits of S3 – bucket policies, S3 versioning, lifecycle management, replication etc.</li> <li>Low-cost alternative to on-premises storage.</li> </ol> </li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Volume Gateway (iSCSI)</b></li> </ul> <p>Volume Gateway provides cloud backed storage which is accessed using iSCSI protocol. Two different Volume Gateway types available.</p> <ol style="list-style-type: none"> <li>1. <b>Stored Volumes</b> - Store your all data locally and only backup to AWS</li> </ol> <ul style="list-style-type: none"> <li>• <b>Stored Volumes</b> - The gateway stores all your data locally, so your applications get low latency access to the entire dataset</li> <li>• You need your own storage infrastructure as all data is stored locally in your data center</li> <li>• Volume Gateway provides durable off-site async backups in the form of EBS snapshots which are stored in S3</li> </ul> <ol style="list-style-type: none"> <li>2. <b>Cached Volumes</b> – Use S3 as your primary storage and cache frequently accessed data in your Storage Gateway.</li> </ol> <ul style="list-style-type: none"> <li>• <b>Cached Volumes</b> - The gateway stores all your data in S3 and caches only frequently accessed data locally</li> <li>• You need only enough local storage capacity to store the frequently accessed data</li> <li>• Applications still get low-latency access to frequently used data without a large investment in on-premises storage</li> </ul> <ul style="list-style-type: none"> <li>• <b>Tape Gateway (VTL)</b></li> </ul> <ul style="list-style-type: none"> <li>• <b>Tape Gateway</b> is a Virtual Tape Library which provides cost effective data archiving in the cloud using Glacier</li> <li>• You don't need to invest in your own tape backup infrastructure</li> <li>• Integrates with existing tape backup infrastructure - NetBackup, Backup Exec, Veeam etc. which connect to the VTL using iSCSI</li> <li>• Data is stored on virtual tapes which are stored in Glacier and accessed using the VTL</li> </ul> <p><b>Exam Tips</b></p> <ul style="list-style-type: none"> <li>• File Gateway - Flat files stored on S3, accessed using NFS or SMB</li> <li>• Volume Gateway – 2 Types:       <ol style="list-style-type: none"> <li>1. Stored Volumes - Entire dataset <b>stored on-site</b>, backed-up to S3 as EBS Snapshots.</li> <li>2. Cached Volumes - Entire dataset stored in S3, only frequently accessed data <b>cached on-site</b></li> </ol> </li> <li>• Tape Gateway - VTL       <ol style="list-style-type: none"> <li>1. Used for archiving your backups to Glacier</li> <li>2. Can be used with or without your own backup application.</li> </ol> </li> </ul>
<b>Athena</b>	<p><b>Exam Tips</b></p> <ul style="list-style-type: none"> <li>• Athena is an interactive query service.</li> <li>• Allows you to query data located in S3 using standard SQL</li> <li>• Serverless</li> </ul>
<b>S3 Exam Tips</b>	<ul style="list-style-type: none"> <li>• Remember that S3 is <b>Object-based</b> (Object-based storage only for files): i.e. allow you to upload files.</li> <li>• Not suitable to install an operating system or running a database on.</li> <li>• Files can be from 0 Bytes to 5 TB.</li> <li>• There is unlimited storage.</li> <li>• Files are stored in Buckets.</li> <li>• S3 is a universal namespaces. That is, names must be unique globally.</li> </ul>

	<ul style="list-style-type: none"> <li>• Read after Write consistency for PUTS of new Objects</li> <li>• Eventual Consistency for overwrite PUTS and DELETES (Can take some time to propagate)</li> <li>• S3 Storage Classes/Tiers: <ul style="list-style-type: none"> <li>- S3 (durable, immediately available, frequently accessed)</li> <li>- S3 - IA (durable, immediately available, infrequently accessed)</li> <li>- S3 - One Zone IA: Same as IA. However, data is stored in a single Availability Zone only.</li> <li>- S3 - Reduced Redundancy Storage (data that is easily reproducible, such as thumbnails, etc.)</li> <li>- Glacier - Archived data, where you can wait 3 - 5 hours before accessing</li> </ul> </li> </ul>
--	--

### Storage Gateway Diagram



<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>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> <li>5. Percentage of GET Requests that Didn't Finish Downloading</li> </ol> <ul style="list-style-type: none"> <li>✓ <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.</li> </ul>
<b>S3 Storage Classes</b>	<ul style="list-style-type: none"> <li>✓ <b>Storage Classes for Frequently Accessed Objects</b></li> <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> <li>✓ <b>Storage Classes for Infrequently Accessed Objects</b></li> <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>

	<ul style="list-style-type: none"> <li>✓ <b>Glacier</b></li> <li>✓ For long-term archive.</li> <li>✓ Archived objects are not available for real-time access.</li> </ul>
<b>RDS</b>	<ul style="list-style-type: none"> <li>✓ Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration task.</li> <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> <li>✓ RDS manages backups, software patching, automatic failure detection, and recovery.</li> <li>✓ You can have automated backups performed when you need them, or manually create your own backup snapshot. You can use these backups to restore a database.</li> </ul>
<b>Limitations of Amazon RDS Encrypted DB Instance</b>	<ul style="list-style-type: none"> <li>✓ You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created.</li> <li>✓ You can encrypt a copy of an unencrypted DB snapshot and effectively add encryption to an unencrypted DB instance.</li> </ul> <p>You can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance.</p> <ul style="list-style-type: none"> <li>✓ DB instances that are encrypted can't be modified to disable encryption.</li> <li>✓ You can't have an encrypted Read Replica of an unencrypted DB instance or an unencrypted Read Replica of an encrypted DB instance.</li> <li>✓ Encrypted Read Replicas must be encrypted with the same key as the source DB instance.</li> <li>✓ You can't restore an unencrypted backup or snapshot to an encrypted DB instance.</li> <li>✓ To copy an encrypted snapshot from one region to another, you must specify the KMS key identifier of the destination region. This is because KMS encryption keys are specific to the region that they are created in.</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>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>Multi-AZ DB instances</b>	<p>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.</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>Redshift</b>	<ul style="list-style-type: none"> <li>✓ It is a petabyte storage service for OLAP applications</li> <li>✓ Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud.</li> <li>✓ Redshift is used as a data warehousing solution.</li> <li>✓ By default, automated backups are enabled for the data warehouse cluster with a 1-day retention period. It provides free storage for snapshots that is equal to the storage capacity of your cluster until you delete the cluster. After you reach the free snapshot storage limit, you are charged for any additional storage at the normal rate.</li> </ul>
<b>Amazon Kinesis Data Streams (KDS)</b>	<p>It is a massively scalable and durable real-time data streaming service.</p>



<b>HTTP 503 Slow Down</b>	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.
<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> 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>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.
<b>Predefined groups in S3</b>	<p>Amazon S3 has a set of predefined groups. When granting account access to a group, you specify one of our URIs instead of a canonical user ID. The following are the available predefined groups in S3:</p> <ul style="list-style-type: none"> <li>✓ Authenticated Users group</li> <li>✓ All Users group</li> <li>✓ Log Delivery group</li> </ul>
<b>Amazon EBS - Provisioned IOPS &amp; Cold HDD</b>	EBS Provisioned IOPS provides high disk read/write performance, which is optimal for large database workloads. Cold HDD, on the other hand, is very cheap and is great for infrequently accessed data.
<b>Amazon Aurora</b>	<b>Amazon Aurora (Aurora)</b> is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. You already know how MySQL and PostgreSQL combine the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. The code, tools, and applications you use today with your existing MySQL and PostgreSQL databases can be used with Aurora. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.
<b>Amazon Data Lifecycle Manager (DLM)</b>	<p>You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes. Automating snapshot management helps you to:</p> <p>Protect valuable data by enforcing a regular backup schedule.</p>



	<p>Retain backups as required by auditors or internal compliance.</p> <p>Reduce storage costs by deleting outdated backups.</p> <p>Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon DLM provides a complete backup solution for EBS volumes at no additional cost.</p>
<b>Amazon EFS</b>	<p>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.</p>
<b>Storage optimized instances</b>	<p>Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications compared with EBS-backed EC2 instances.</p>

## Security

<b>AWS Best Practices for DDoS</b>	<p>Remember the technologies you can use to mitigate a DDoS attack:</p> <ul style="list-style-type: none"> <li>▪ CloudFront</li> <li>▪ Route53</li> <li>▪ ELB's</li> <li>▪ WAFs</li> <li>▪ Autoscaling (Use for both WAFs and Web Servers)</li> <li>▪ CloudWatch</li> </ul>
<b>AWS IAM</b>	<ul style="list-style-type: none"> <li>▪ You can create custom policies using the visual editor or using JSON.</li> <li>▪ You can now attach roles to EC2 instances at any time using the command line or AWS Console.</li> <li>▪ Once attached the role takes effect immediately.</li> <li>▪ Any policy change also takes effect immediately.</li> </ul>
<b>MFA Reporting &amp; IAM</b>	<p>You can enable MFA using the command line and by using the console.</p> <p>MFA can be enabled on both the root account and user accounts.</p> <p>You can report on who's using MFA on a per user basis using credential reports.</p>
<b>AWS Inspector</b>	<ul style="list-style-type: none"> <li>✓ 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.</li> <li>✓ It enables you to analyze the behavior of your AWS resources and helps you to identify potential security issues. You can create an assessment template and launch a security assessment run of this target. During the assessment run, the network, file system, and process activity within the specified target are monitored, and a wide set of activity and configuration data is collected.</li> <li>✓ Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you to identify potential security issues.</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> <li>✓ It helps to protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.</li> <li>✓ AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules.</li> <li>✓ You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.</li> </ul>
<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>

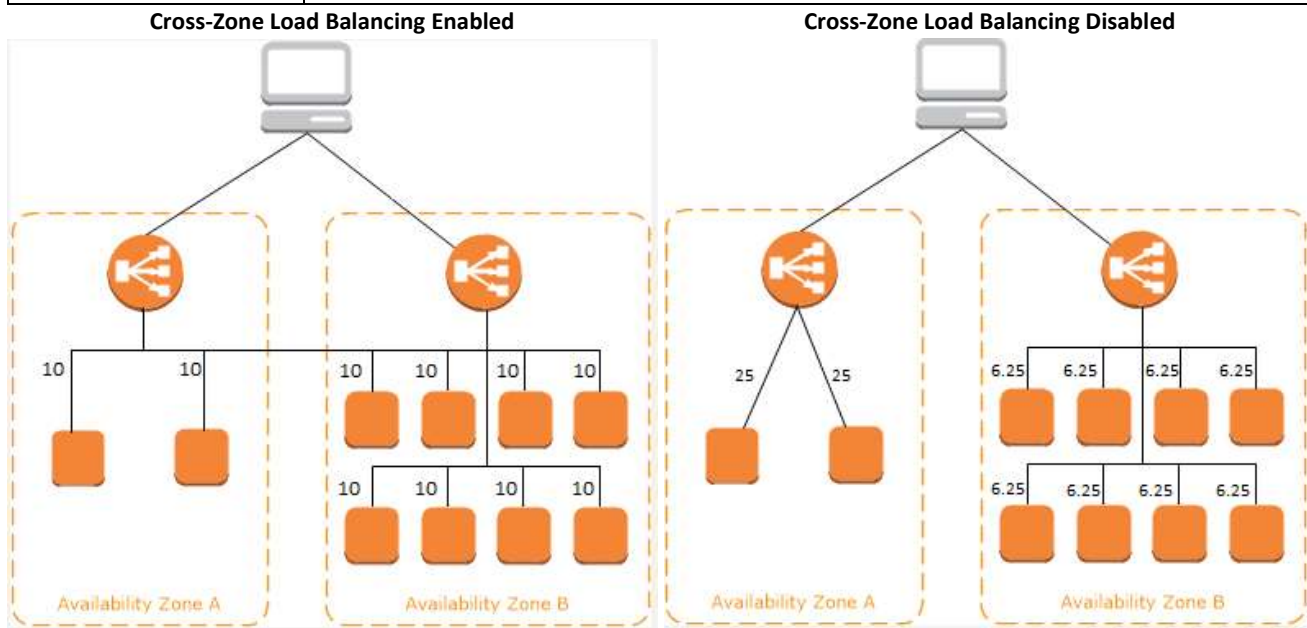
	<p>One of the capabilities of Systems Manager is <b>Patch Manager</b>, which can automate the process of patching Windows managed instances at scale. With Patch Manager, you can scan instances for missing patches, or scan and install missing patches to individual instances or large groups of instances 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> <p><b>Automation capabilities of Systems Manager</b></p> <ul style="list-style-type: none"> <li>✓ Build Automation workflows to configure and manage instances and AWS resources.</li> <li>✓ Create custom workflows or use pre-defined workflows maintained by AWS.</li> <li>✓ Receive notifications about Automation tasks and workflows by using Amazon CloudWatch Events.</li> <li>✓ Monitor Automation progress and execution details by using the Amazon EC2 or the AWS Systems Manager console.</li> </ul>
<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>AWS CloudTrail</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>Amazon CloudWatch</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>AWS Trusted Advisor</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>AWS Config</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>AWS Certificate Manager</b> 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.</p>
<b>Trusted Advisor</b>	<ul style="list-style-type: none"> <li>✓ 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.</li> </ul>
<b>Amazon Cognito</b>	<p>Amazon Cognito identity pools assign your authenticated users a set of temporary, limited privilege credentials to access your AWS resources. The permissions for each user are controlled through IAM roles that you create. You can define rules to choose the role for each user based on claims in the user's ID token. You can define a default role for authenticated users. You can also define a separate IAM role with limited permissions for guest users who are not authenticated.</p>
<b>AWS Shield Advanced</b>	<p>For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall. AWS Shield Advanced also gives you 24x7 access to the AWS DDoS Response Team (DRT) and protection against DDoS related spikes in your Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, and Amazon Route 53 charges.</p>

## Networking &amp; Route53

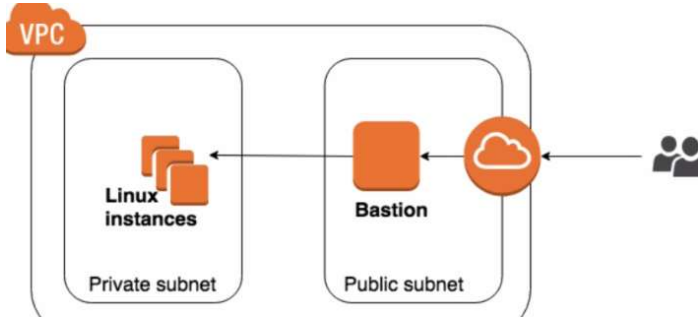
<b>Route 53 DNS Routing</b>	<ul style="list-style-type: none"> <li>✓ <b>Simple Routing Policy</b> You can only have one record with multiple IP Address. If you specify multiple values in a record, Route 53 returns all values to the user in a random order.</li> <li>✓ <b>Weighted Routing Policy</b> Weighted 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>AWS Direct Connect</b>	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.
<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>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>ACL</b>	<p>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.</p> <p><b>You can't define an Inbound deny rule for Security Groups. You can only add allow rules to your Security Groups.</b></p>
<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>	<p>Enhanced Networking feature is mainly used to provide high-performance networking capabilities for EC2 instances on supported instance types.</p> <ul style="list-style-type: none"> <li>✓ m1.small instance type does not support Enhanced Networking</li> </ul>
<b>Egress-only Internet gateway</b>	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.

	<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>VPC Overview</b>	<p>CIDR.xyz</p> <p>VPC as a logical datacenter in AWS.</p> <p>Consists of IGWs (or Virtual Private Gateways), Route Tables, Network Access Control Lists, Subnets, and Security Groups.</p> <p>1 Subnet = 1 Availability Zone</p> <p>Security Groups are <b>Stateful</b> and Network Access Control Lists are <b>Stateless</b>.</p> <p><b>Stateful</b> - If you open port 80 of your security group, automatically you can both send and receive port 80.</p> <p><b>Stateless</b> – You have to both open inbound and outbound ports.</p>
<b>VPC Flow Logs</b>	<ul style="list-style-type: none"> <li>✓ 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</li> </ul> <ul style="list-style-type: none"> <li>• You cannot enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account.</li> <li>• You cannot tag a flow log.</li> <li>• After you've created a flow log, you cannot change its configuration; for example, you can't associate a different IAM role with the flow log.</li> </ul>
<b>VPC Endpoint for S3</b>	<p>These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances.</p> <p>EC2 instances running in private subnets of a VPC can have controlled access to S3 buckets, objects, and API functions that are in the same region as the VPC. You can use an S3 bucket policy to indicate which VPCs and which VPC Endpoints have access to your S3 buckets.</p>

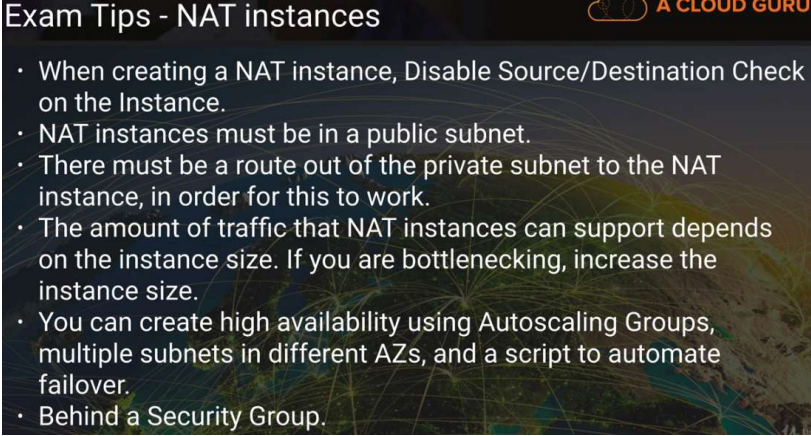
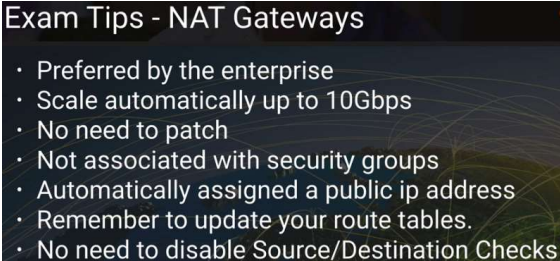
<b>Amazon Redshift Enhanced VPC Routing</b>	<ul style="list-style-type: none"> <li>✓ By using Enhanced VPC Routing, you can use VPC features to manage the flow of data between your cluster and other resources.</li> <li>✓ You can also use VPC flow logs to monitor COPY and UNLOAD traffic.</li> </ul>
<b>Cross-zone 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>



<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>
<b>AWS X-Ray</b>	<p>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.</p> <p>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.</p>

<b>2xx and 3xx response codes</b>	<ul style="list-style-type: none"> <li>✓ Your endpoints should respond with 2xx and 3xx response codes, which will tell Route 53 that your resources are healthy.</li> </ul>
<b>ELB Error Messages</b>	<ul style="list-style-type: none"> <li>▪ 4xx - Client side error</li> <li>▪ 5xx – Server side error</li> </ul>
<b>Failover Types</b>	<p><b>Active-Active Failover</b> Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Route 53 can detect that it's unhealthy and stop including it when responding to queries.</p> <p>In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or latency) are active unless Route 53 considers them unhealthy. Route 53 can respond to a DNS query using any healthy record.</p> <p><b>Active-Passive Failover</b> Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.</p>
<b>SSH Connection</b>	<p><b>For you to be able to SSH into your EC2 instances, you must satisfy the following requirements:</b></p> <ol style="list-style-type: none"> <li>1. You should have a public IP address or attached an Elastic IP address to your instance.</li> <li>2. Your instances should have passed both system status and instance status checks to know they are working correctly.</li> <li>3. You should have an internet gateway attached to your VPC to allow your instances access to the internet.</li> <li>4. You should have a route table that has the appropriate routes entered for all destinations via Internet Gateway. Make sure that there is a default route or a route that specifies your desktop's IP address to allow communication between instances in the VPC to the Internet or your desktop.</li> </ol>
<b>Bastion Host</b>	 <ul style="list-style-type: none"> <li>▪ It is a host connected to a Public subnet.</li> <li>▪ You can connect to it over the internet.</li> <li>▪ Used to securely connect to instances in a Private subnet.</li> <li>▪ Allows you to safely administer your EC2 instances without exposing them to the Internet.</li> <li>▪ For incoming SSH/RDP only.</li> <li>▪ Does not enable outgoing requests, e.g. internet access for your instances.</li> </ul>
<b>NAT vs Bastions</b>	<ul style="list-style-type: none"> <li>▪ A NAT is used to provide internet traffic to EC2 instances in private subnets.</li> <li>▪ A Bastion is used to securely administer EC2 instances (using SSH or RDP) in private subnets.</li> </ul>



<b>NAT Instances &amp; Nat Gateways</b>	<div>  <p><b>Exam Tips - NAT instances</b></p> <ul style="list-style-type: none"> <li>• When creating a NAT instance, Disable Source/Destination Check on the Instance.</li> <li>• NAT instances must be in a public subnet.</li> <li>• There must be a route out of the private subnet to the NAT instance, in order for this to work.</li> <li>• The amount of traffic that NAT instances can support depends on the instance size. If you are bottlenecking, increase the instance size.</li> <li>• You can create high availability using Autoscaling Groups, multiple subnets in different AZs, and a script to automate failover.</li> <li>• Behind a Security Group.</li> </ul> </div> <div>  <p><b>Exam Tips - NAT Gateways</b></p> <ul style="list-style-type: none"> <li>• Preferred by the enterprise</li> <li>• Scale automatically up to 10Gbps</li> <li>• No need to patch</li> <li>• Not associated with security groups</li> <li>• Automatically assigned a public ip address</li> <li>• Remember to update your route tables.</li> <li>• No need to disable Source/Destination Checks</li> </ul> </div>
---	---

## Automation

<b>CloudFormation</b>	<ul style="list-style-type: none"> <li>• CloudFormation allows you to manage, configure and provision AWS infrastructure as code. (YAML /JSON)</li> <li>• Remember the main sections in the CloudFormation Template:             <ol style="list-style-type: none"> <li>1. Parameters - Input custom values.</li> <li>2. Conditions - e.g. Provision resources based on environment.</li> <li>3. Resources - Mandatory, the AWS resources to create.</li> <li>4. Mappings - Create custom mappings like Region : AMI</li> <li>5. Transforms - Reference code located in S3 e.g. Lambda code or reusable snippets of CloudFormation code.</li> </ol> </li> </ul>
<b>Elastic Beanstalk</b>	<ul style="list-style-type: none"> <li>▪ Deploys and scales your web applications including the web application server platform where required.</li> <li>▪ Supports widely used programming technologies - Java, PHP, Python, Ruby, Go, Docker, .Net, Node.js. And application server platforms like Tomcat, Passenger, Puma, and IIS.</li> <li>▪ Provisioning the underlying resources for you.</li> <li>▪ Can fully manage the EC2 instances for you or you can take full administrative control.</li> <li>▪ Also manage the updates, monitoring, metrics and health checks all included.</li> </ul>
<b>OpsWorks</b>	<ul style="list-style-type: none"> <li>▪ It allows you to automate your server configuration using managed instances of Puppet or Chef</li> <li>▪ It's a fully managed services so you do not need to configure and operate your own configuration management environment.</li> <li>▪ So if you have a requirement to manage your EC2 and on-premises systems using Puppet or Chef, <b>OpsWorks</b> is the tools to use.</li> </ul>