**Test Prep Summary**

**AWS Service Catalog** allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

**AWS OpsWorks** is a configuration management service that provides managed instances of Chef and Puppet.

**Amazon Cloud Directory** enables you to build flexible cloud-native directories for organizing hierarchies of data along multiple dimensions.

**AWS Organizations** offers policy-based management for multiple AWS accounts.

**Amazon Simple Notification Service (SNS)** is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging. Using Amazon SNS topics, your publisher systems can fan out messages to a large number of subscriber endpoints for parallel processing, including Amazon SQS queues, AWS Lambda functions, and HTTP/S webhooks.

Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

**Amazon Simple Email Service (Amazon SES)** is used for sending email but not SMS text messages.

**Amazon Simple Workflow Service (Amazon SWF)** helps developers build, run, and scale background jobs that have parallel or sequential steps. You can think of Amazon SWF as a fully-managed state tracker and task coordinator in the Cloud.

**Amazon Simple Queue Service (Amazon SQS)** is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications.

**LightSail** provides preconfigured virtual private servers (instances) that include everything required to deploy and application or create a database.

LightSail includes everything you need to launch your project quickly – a virtual machine, SSD-based storage, data transfer, DNS management, and a static IP.

**CloudFormation** is used to deploy resources through code, as a service it does not include preconfigured servers.

**Amazon Elastic Container Service (ECS)** is a highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances.

**Lambda** is a serverless computing technology that allows you to run code without provisioning or managing servers.

To connect an on-premises network to an Amazon VPC using an Amazon Managed VPN connection, Two of the components you need to connect to your VPC with a VPN connection are a **virtual private gateway on the VPC side and a customer gateway on the on-premise network side.**

**NAT instances** are not used for VPN, they are used by EC2 instances in private subnets to access the Internet.

**AWS Direct Connect** can be used to connect an on-premise network to the cloud however it is not part of the configuration of an Amazon Managed VPN connection

**Availability Zones (not regions)** have direct, low-latency, high throughput and redundant network connections between each other. **Each AWS Region** consist of 2 or more Availability Zones. AWS Regions are geographical areas and each AWS Region is designed to be completely isolated from other AWS Regions.

**VPCs** exist within accounts on a per region basis.

**Edge locations** are Content Delivery Network (CDN) endpoints for CloudFront

A manager needs to keep a check on his AWS spend. How can the manager setup alarms that notify him when his bill reaches a certain amount?

The best ways to do this is to use **CloudWatch** to configure alarms that deliver a notification when activated. The alarms can use cost metrics that trigger the alarm when a certain amount of spend has been reached.

**AWS Trusted Advisor** is focused on providing guidance for provisioning resources following AWS best practices.

**AWS CloudTrail** is used for auditing API activity.

You can use the **consolidated billing** feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. Every organization in AWS Organizations has a master (payer) account that pays the charges of all the member (linked) accounts.

Consolidated billing has the following benefits:

• **One bill** – You get one bill for multiple accounts.

• **Easy tracking** – You can track the charges across multiple accounts and download the combined cost and usage data.

• **Combined usage** – You can combine the usage across all accounts in the organization to share the volume pricing discounts, Reserved Instance discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts.

• **No extra fee** – Consolidated billing is offered at no additional cost.

**Cloud Directory** is used for creating cloud-native directories.

**AWS Cost Explorer** has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. It does not centralize billing.

**The AWS Cost & Usage Report** lists AWS usage for each service category used by an account and its IAM users in hourly or daily line items, as well as any tags that you have activated for cost allocation purposes.

**Amazon S3 Standard-Infrequent Access** is the most cost-effective choice. It provides immediate access and is suitable for this use case as it is lower cost than S3 standard. Note that you must pay a fee for retrievals which is why you would only use this tier for infrequent access use cases.

AWS is a cost-effective for dynamic workloads because it is **elastic**, meaning your workload can scale based on demand. And because **you only pay for what you use** (pay-as-you-go pricing).

**Latency** (slow response times) is experienced when resources are far away. Distance is the single biggest factor that causes latency. The easiest option presented to resolve this situation is to **place resources closer to where the users are.**

**Direct Connect** is a private network connection from your network or data center into a nearby AWS Region.

**AWS Transit Gateway** is used to connect Amazon Virtual Private Clouds (VPCs) and on-premises networks to a single gateway for connecting multiple VPCs and on-premises networks.

**The Amazon Elastic Compute Cloud (EC2)** provides elastic web-scale computing in the cloud allowing you to deploy instances running the Windows and Linux operating systems.

**Amazon Elastic Block Store (Amazon EBS)** provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud.

**AWS Lambda** lets you run code without provisioning or managing server operating systems.

**Amazon Relational Database Service (Amazon RDS)** makes it easy to set up, operate, and scale a relational database in the cloud.

Turning of resources that are not used can reduce spend. You can also use reserved capacity to reduce the monthly spend at the expense of having to lock into a 1 or 3-year contract – good for stable workloads.

**AWS WAF** is a web application firewall that protects against common exploits that could compromise application availability, compromise security or consume excessive resources.

**AWS Shield** is a managed Distributed Denial of Service (DDoS) protection service.

**Security groups** are firewalls applied at the instance level.

**Network ACLs** are firewalls applied at the subnet level.

**CloudTrail** is a web service that records activity made on your account and delivers log files to an Amazon S3 bucket. CloudTrail records API activity. CloudTrail is used for auditing whereas CloudWatch is used for performance monitoring.

**CloudFormation** is used for deploying infrastructure through code.

**CloudHSM** is a hardware security module for generating, managing and storing encryption keys.

**AWS Managed Services** manages the daily operations of your AWS infrastructure in **alignment with ITIL processes**. AWS Managed Services provides **a baseline integration with IT Service Management** (ITSM) tools such as the ServiceNow platform.

AWS Managed Services provides ongoing **management of your AWS infrastructure so you can focus on your applications.** By implementing best practices to maintain your infrastructure, AWS Managed Services helps to reduce your operational overhead and risk.

AWS Managed Services **currently supports the 20+ services most critical for Enterprises**, and will continue to expand our list of integrated AWS services.

AWS Managed Services is **designed to meet the needs of Enterprises** that require stringent SLAs, adherence to corporate compliance, and integration with their systems and ITIL®-based processes.

**The TCO calculators** allow you to estimate the cost savings when using AWS, compared to on-premises, and provide a detailed set of reports that can be used in executive presentations. The calculators also give you the option to modify assumptions that best meet your business needs.

**AWS Cost & Usage Report** generates reports that break down AWS Cloud compute costs by duration, resource, or tags.

**AWS Pricing Calculator (or Simple Monthly Calculator)** estimates a monthly bill for the AWS Cloud resources that will be used.

Billing alerts can be enabled using **Amazon CloudWatch**.

**Amazon DynamoDB** is fully managed and can be scaled without incurring downtime. DynamoDB scales horizontally and it does so seamlessly.

**Both RDS and ElastiCache** use EC2 instances and therefore scaling (vertically) requires downtime.

**S3** is not a fully managed database, it is an object store.

With **Amazon S3** you don’t need to specify any capacity at any time, the service scales in both capacity and performance as required.

**AWS Lambda** lets you run code without provisioning or managing servers. You pay only for the compute time you consume – there is no charge when your code is not running.

**With Amazon EC2** you need to select your instance sizes and number of instances.

**With RDS** you need to select the instance size for the DB.

**With DynamoDB** provisioned mode you need to specify the read/write capacity of the DB. On-demand mode does allow elasticity, as does DynamoDB Auto Scaling.

Only the **business and enterprise plans** provide **support via email, chat and phone.**

**Inspector** is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Inspector automatically assesses applications for vulnerabilities or deviations from best practices.

**AWS Artifact** is your go-to, central resource for compliance-related information that matters to you.

**AWS Shield** is a managed Distributed Denial of Service (DDoS) protection service.

**AWS Web application Firewall (WAF)** is a firewall service, it is not used for assessing best practice.

**Amazon S3** is an object storage system. Typical use cases include: Backup and storage, application hosting, media hosting, software delivery and hosting a static website.

The customer is responsible for installing security updates on EC2 instances and enabling MFA. AWS is responsible for security of the physical data center and the infrastructure upon which customer services run.

Collecting syslog messages from physical firewalls is an AWS responsibility.

Issuing data center access keycards is an AWS responsibility.

Installing security updates for server firmware is an AWS responsibility.

**An Availability Zone (AZ)** is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. AZ’s give customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data center.

AZs are located within an AWS Region. Every region is connected via a high bandwidth, fully redundant network. There are 22 regions around the world. Each region is completely independent.

**Edge locations** are used by Amazon CloudFront for caching content.

**Subnets** are created within AZs.

**A company needs a consistent and dedicated connection between AWS resources and an on-premise system.** An **AWS Direct Connect** connection is a private, dedicated link to AWS. As it does not use the internet, performance is consistent.

**AWS Managed VPN** uses the public internet so it is not a dedicated link and performance will not be consistent.

**Amazon Connect** is an easy to use omnichannel cloud contact center that helps companies provide superior customer service at a lower cost.

**AWS DataSync** makes it simple and fast to move large amounts of data online between on-premises storage and Amazon S3, Amazon Elastic File System (Amazon EFS), or Amazon FSx for Windows File Server.

**An architect wants to find a tool for consistently deploying the same resources through a templated configuration. AWS CloudFormation** provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.

**AWS Elastic Beanstalk** is used for running applications in a managed environment. It is not used for deploying templated configurations.

**AWS CodeBuild** is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy.

**AWS CodeDeploy** is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Lambda, and on-premises servers. It does not use a templated configuration for deployment.

**Scaling vertically** takes place through an increase in the specifications of an individual resource (e.g., upgrading a server with a larger hard drive or a faster CPU). On Amazon EC2, this can easily be achieved by stopping an instance and resizing it to an instance type that has more RAM, CPU, IO, or networking capabilities.

**Scaling horizontally** takes place through an increase in the number of resources (e.g., adding more hard drives to a storage array or adding more servers to support an application). Adding additional EC2 instances through Auto Scaling. Adding additional hard drives to a storage array. Distributed processing.

**Amazon EBS** volumes are used by EC2 instances for persistent storage. EBS volumes must be in the same AZ as the instances they are attached to and you can attach multiple EBS volumes to an instance.

You cannot attach an EBS volume to multiple instances (use Elastic File Store instead).

EBS volume data persists independently of the life of the instance.

EBS volumes are block storage devices.

With **IaaS** the IT department have the most flexibility and management control over resources as only the infrastructure layer is provided by the Cloud Provider. Everything else is managed by the end customer. This means more control and more responsibility for management.

With **PaaS and SaaS**, the Cloud Provider manages up to a higher level in the stack. This means that as an organization using the service you have less control (and less responsibility).

On-premises cloud is a cloud deployment model, not a cloud computing model. Other cloud deployment models are Private, Public and Hybrid.

**Which AWS dashboard displays relevant and timely information to help users manage events in progress, and provides proactive notifications to help plan for scheduled activities? AWS Personal Health Dashboard** provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the **Service Health Dashboard** displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.

**AWS Service Health Dashboard** shows the current status of services across regions. However, it does not provide proactive notifications of scheduled activities or guidance of any kind.

**AWS Trusted Advisor** is an online tool that provides you real time guidance to help you provision your resources following AWS best practices.

**Amazon CloudWatch dashboard** is used for monitoring performance related information for your infrastructure and resources, not the underlying AWS resources.

**AWS OpsWorks** is a configuration management service that provides managed instances of Chef and Puppet. 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.

**AWS Config** is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.

**AWS CloudFormation** provides a common language for you to model and provision AWS and third party application resources in your cloud environment.

**AWS Systems Manager** gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources.

**AWS Secrets Manager** enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

**AWS Key Management Service (AWS KMS**) is involved with creating and managing encryption keys but does not use dedicated hardware.

**AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD,** enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

**The AWS Storage Gateway** service enables hybrid storage between on-premises environments and the AWS Cloud. It provides low-latency performance by caching frequently accessed data on premises, while storing data securely and durably in Amazon cloud storage services. **AWS Storage Gateway supports three storage interfaces: file, volume, and tape**

File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3

The volume gateway represents the family of gateways that support block-based volumes, previously referred to as gateway-cached and gateway-stored modes

Tape Gateway (formerly known as Gateway Virtual Tape Library) is used for backup with popular backup software.

The file system is mounted using NFS or SMB

Files are stored as objects in S2, a local cache provides low latency access to recently used data.

Virtual gateway appliance runs on Hyper-V, VMmare, or EC2.

AWS Storage Gateway can store data in multiple S3 storage classes.

**You need to ensure you have the right amount of compute available to service demand. Which AWS service can automatically scale the number of EC2 instances for your application?**

**Amazon EC2 Auto Scaling** automates the process of adding (scaling up) OR removing (scaling down) EC2 instances based on the traffic demand for your application.

**Amazon Elastic Load Balancer (ELB)** automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses.

**Amazon ElastiCache** offers fully managed Redis and Memcached database services.

**Amazon Redshift** is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake.

AWS offer many services without charge. These include the AWS IAM services for creating users, groups, roles and policies and the Amazon VPC service for creating virtual private clouds, subnets, route tables etc.

A couple of the benefits that companies will realize immediately when using the AWS Cloud are increased agility and a change from capital expenditure to variable operational expenditure.

Agility is enabled through the flexibility of cloud services and the ease with which applications can be deployed, scaled, and managed. When using cloud services you pay for what you use and this is a variable, operational expense which can be beneficial to company cashflow.

**A tag** is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment.

Reserved Instances (RI) provide a significant discount (up to 72%) compared to On-Demand pricing and provide a capacity reservation when used in a specific Availability Zone. The following types of RI are available:

Standard RIs: These provide the most significant discount (up to 75% off On-Demand) and are best suited for steady-state usage.

Convertible RIs: These provide a discount (up to 54% off On-Demand) and the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value. Like Standard RIs, Convertible RIs are best suited for steady-state usage.

Scheduled RIs: These are available to launch within the time windows you reserve. This option allows you to match your capacity reservation to a predictable recurring schedule that only requires a fraction of a day, a week, or a month.

**Network Access Control Lists (ACLs)** are a firewall/security layer applied at the subnet level.

**Security Groups** are a firewall/security layer applied at the instance level.

**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.

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.

**LightSail** is a good service to use when you don’t have good knowledge of AWS. However, you cannot deploy a scalable node.js application into a VPC.

**CloudFormation** is used for automating the deployment of infrastructure resources in AWS.

**Amazon EC2** would require more expertise that using Elastic Beanstalk.

For extra security, AWS recommends that you require multi-factor authentication (MFA) for all users in your account. With MFA, users have a device that generates a response to an authentication challenge.

Both the user's credentials (something you know) and the device-generated response (something you have) are required to complete the sign-in process. If a user's password or access keys are compromised, your account resources are still secure because of the additional authentication requirement.

Additionally, strong password policies should be used to enforce measures including minimum password length, complexity, and password reuse restrictions.

**AWS Secrets Manager** enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

**AWS Certiﬁcate Manager** is incorrect. This service is used for creating SSL/TLS certificates for use with HTTPS connections.

**Security group rules** are used to restrict traffic to/from your EC2 instances.

You need to identify the items that have a cost on-premise and that will be rolled into the service in the cloud. Compute hardware costs and data center security costs will be rolled in the service cost in the cloud so you need to include them in the model so you can really understand the true TCO on-premise vs. the cloud.

Firewall management, application licensing and operating system patching need to be paid for on-premise and in the cloud so there is little difference.

**AWS Artifact**, available in the console, is a self-service audit artifact retrieval portal that provides our customers with on-demand access to AWS’ compliance documentation and AWS agreements.

You can use AWS Artifact Reports to download AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and System and Organization Control (SOC) reports.

**AWS Trusted Advisor** is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment.

**Inspector** is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

**AWS Personal Health Dashboard** provides alerts and remediation guidance when AWS is experiencing events that may impact you.

You can connect from your on-premise data center to a VPC via **Direct Connect or VPN CloudHub.** AWS Direct Connect is a network service that provides an alternative to using the Internet to connect a customer’s on premise sites to AWS.If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub.

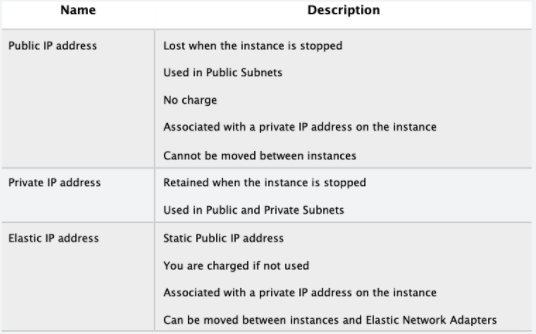
**VPC Peering**" is a way to connect VPCs to each other, not on-premises locations

**Internet Gateway** is used to provide internet connectivity to a VPC.

**VPC Router** is used for routing within a VPC.

Both Amazon EC2 and Amazon S3 are managed at a regional level. Note: Amazon S3 is a global namespace but you still create your buckets within a region. Amazon CloudFront, Amazon Route 52 and AWS IAM are managed at a global level.

**An Elastic IP** address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.



There are three fundamental drivers of cost with AWS: compute, storage, and outbound data transfer. These characteristics vary somewhat, depending on the AWS product and pricing model you choose.

In most cases, there is no charge for inbound data transfer or for data transfer between other AWS services within the same region. However, there are some exceptions.

**AWS Key Management Service (KMS)** gives you centralized control over the encryption keys used to protect your data. **AWS CloudHSM** is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

**AWS Database Migration Service** is used for migration of databases.

**AWS Server Migration Service** is used for migration of virtual machines.

**Amazon Elastic Load Balancing** is used for distributing incoming connections to pools of EC2 instances

Scaling horizontally takes place through an increase in the number of resources (e.g., adding more hard drives to a storage array or adding more servers to support an application)

Scaling vertically takes place through an increase in the specifications of an individual resource (e.g., upgrading a server with a larger hard drive or a faster CPU). On Amazon EC2, this can easily be achieved by stopping an instance and resizing it to an instance type that has more RAM, CPU, IO, or networking capabilities.

**Amazon Elastic Container Service (ECS)** is a highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances.

**AWS Lambda** is a serverless technology that lets you run code in response to events as functions

**Amazon Elastic Container Registry (ECR)** is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images

**Amazon Machine Images (AMI)** store configuration information for Amazon EC2 instances.

You can use Amazon S3 to host a static website. On a static website, individual webpages include static content. They might also contain client-side scripts.

By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting, but AWS has other resources for hosting dynamic websites.

By default new users are created with NO access to any AWS services – they can only login to the AWS console. You must apply permissions to users to allow them to access services.

The recommended way to do this is to organize users into groups and then apply permissions policies to the group.

**AWS Glue** is an Extract, Transform, and Load (ETL) service. You can use AWS Glue with data sources on Amazon S3, RedShift and other databases. With AWS Glue you transform and move the data to various destinations. It is used to prepare and load data for analytics.

**Amazon RedShift** is a data warehouse. With a data warehouse you load data from other databases such as transactional SQL databases and run analysis. You can analyze data using SQL and Business Intelligence tools.

**Amazon EMR** is a managed Hadoop framework running on EC2 and S3. It is used for analyzing data, not for ETL.

**Amazon Kinesis** is used for collecting, processing and analyzing real-time streaming data.

**AWS Key Management Service** gives you centralized control over the encryption keys used to protect your data. You can create, import, rotate, disable, delete, define usage policies for, and audit the use of encryption keys used to encrypt your data.

**The AWS Security Token Service (STS)** is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users.

**Amazon Elastic Block Store (Amazon EBS)** provides persistent block storage volumes for use with Amazon EC2instances in the AWS Cloud.

**Amazon Route 53** services include domain registration, DNS (hosted zone), health checking (availability monitoring) and traffic management.

**Amazon Simple Queue Service (Amazon SQS)** is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers. SQS is used for distributed/decoupled application.

**Amazon Simple Notification Service (SNS)** is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

**Amazon DynamoDB** is a nonrelational database that delivers reliable performance at any scale.

**Amazon SWF** helps developers build, run, and scale background jobs that have parallel or sequential steps.

Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it (DR only). Read replicas are used for read heavy DBs and replication is asynchronous. With a read replica you direct your database queries to the read replica and this offloads pressure from the main database.

**Amazon Inspector** is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

**Security groups** are instance-level firewalls used for controlling network traffic reaching and leaving EC2 instances.

**AWS Config** is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.

**Amazon Macie** is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data in AWS.

AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) to use the secure AWS environment to process, maintain, and store protected health information.

The Amazon Simple Storage Service (S3) is an object store so you create objects (files, images, video etc.) within buckets. Though it is a flat structure (no hierarchy), you can mimic a hierarchical structure by using folders.

If you have multiple EC2 instances that are part of an application, you should deploy them into separate availability zones (AZs). Each AZ has redundant power and is also fed from a different grid. AZs also have low-latency network links which is often advantageous for most applications.

You do not need to deploy into separate regions to prevent a power outage bringing your application down. AZs have redundant power and grids so you are safe deploying your applications into multiple AZs. If you split your applications across regions you introduce latency which may impact your application. You may also run into data sovereignty issues in some cases.

Deploying your EC2 instances into different VPCs is not required and would complicate your application deployment. Also, bear in mind that VPCs within a region use the same underlying infrastructure so deploying into different VPCs may still result in your EC2 instances being deployed into the same AZs. It is a best practice to deploy into separate AZs.

**A resource group** is a collection of resources that share one or more tags or portions of tags. To create a resource group, you simply identify the tags that contain the items that members of the group should have in common.

**AWS Storage Gateway** is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases.

These include moving tape backups to the cloud, reducing on-premises storage with cloud-backed file shares, providing low latency access to data in AWS for on-premises applications, as well as various migration, archiving, processing, and disaster recovery use cases.

**AWS Backup** is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services. It is not used for connecting on-premises storage to cloud storage.

**Amazon Connect** is an easy to use omnichannel cloud contact center that helps companies provide superior customer service at a lower cost. It has nothing to do with storing data.

**AWS Direct Connect** is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. It is not related to storage of data.

AWS recommends that you create individual IAM users rather than sharing IAM user accounts.

For extra security, AWS recommends that you require multi-factor authentication (MFA) for all users in your account. For privileged IAM users who are allowed to access sensitive resources or API operations, AWS recommend using U2F or hardware MFA devices.

You should use groups to assign permissions to IAM users and should avoid embedding access keys in application code.

AWS recommend creating individual IAM users and assigning the least privilege necessary for them to perform their role.

**A virtual private cloud (VPC)** is a virtual network dedicated to your AWS account. A VPC is analogous to having your own DC inside AWS. It is logically isolated from other virtual networks in the AWS Cloud.

**Amazon WorkSpaces** is a managed desktop computing service running on the AWS cloud.

**Amazon Elastic Compute Cloud (Amazon EC2)** is a web service that provides secure, resizable compute capacity in the cloud.

**IAM** is used to securely control individual and group access to AWS resources.