FINAL AZURE QUESTIONS

Unit 1

1.Explain the components of cloud computing.

A) The components of cloud computing are the different parts that work together to deliver cloud services. These components can be divided into two main categories: the front-end and the back-end.

Front-end components are the parts of cloud computing that are visible to users. They include:

- Client infrastructure: This is the hardware and software that users use to access cloud services, such as computers, laptops, smartphones, and tablets.
- Applications: Cloud applications are software programs that are hosted in the cloud and can be accessed over the internet.
- Services: Cloud services are specific features or functionality that are provided by cloud providers. For example, cloud providers offer services such as storage, computing, networking, and databases.

Back-end components are the parts of cloud computing that are hidden from users. They include:

- Runtime cloud: This is the software that provides the execution environment for cloud applications. It includes components such as hypervisors, operating systems, and middleware.
- Storage: Cloud storage is used to store data and applications in the cloud. It is typically provided as a service by cloud providers.
- Infrastructure: Cloud infrastructure is the hardware that powers cloud services. It includes components such as servers, storage devices, and networking equipment.
- Management: Cloud management software is used to manage and monitor cloud resources. It includes features such as provisioning, scaling, and security.
- Security: Cloud security is the process of protecting cloud resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

All of these components work together to deliver cloud services to users. For example, when a user accesses a cloud application, the client infrastructure sends a request to the cloud provider. The cloud provider then uses the runtime cloud to execute the application and

return the results to the client infrastructure. The cloud provider also uses storage to store the application and data, and it uses infrastructure to power the cloud services.

2. What are the types of Cloud Computing Services?

A) There are three main types of cloud computing services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Infrastructure as a Service (IaaS): IaaS provides the basic building blocks of cloud computing, such as computing power, storage, and networking. IaaS customers can use IaaS to deploy and manage their own applications and services.

Platform as a Service (PaaS): PaaS provides a platform for developers to build and deploy applications. PaaS includes everything that IaaS does, plus additional features such as development tools, middleware, and databases.

Software as a Service (SaaS): SaaS is a software delivery model where the software is hosted in the cloud and accessed over the internet. SaaS customers do not need to install or manage the software; they simply log in to the cloud application and start using it.

3. Explain about Cloud Computing Architecture and its Components.

A) Cloud computing architecture is the design and structure of cloud computing systems. It includes the different components that work together to deliver cloud services to users.

The main components of cloud computing architecture are:

- Client infrastructure: This is the hardware and software that users use to access cloud services. It includes computers, laptops, smartphones, and tablets.
- Applications: Cloud applications are software programs that are hosted in the cloud and can be accessed over the internet.
- Services: Cloud services are specific features or functionality that are provided by cloud providers. For example, cloud providers offer services such as storage, computing, networking, and databases.

- Runtime cloud: This is the software that provides the execution environment for cloud applications. It includes components such as hypervisors, operating systems, and middleware.
- Storage: Cloud storage is used to store data and applications in the cloud. It is typically provided as a service by cloud providers.
- Infrastructure: Cloud infrastructure is the hardware that powers cloud services. It includes components such as servers, storage devices, and networking equipment.
- Management: Cloud management software is used to manage and monitor cloud resources. It includes features such as provisioning, scaling, and security.
- Security: Cloud security is the process of protecting cloud resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

4. List out benefits of Cloud computing and describe each of them

A) The benefits of cloud computing are numerous and vary depending on the specific needs of the organization. However, some of the most common benefits include:

- Agility: Cloud computing makes it easy to deploy and scale applications and services quickly. This is because cloud providers offer a wide range of resources that can be provisioned and deprovisioned on demand. This agility can be a major advantage for businesses that need to be able to quickly respond to changing market conditions or customer demands.
- Cost savings: Cloud computing can help businesses save money on IT costs in a number of ways. First, cloud providers offer a variety of pricing options, including pay-as-you-go and subscription models. This allows businesses to only pay for the resources they need, when they need them. Second, cloud providers can help businesses save money on hardware and software costs. This is because cloud providers offer a wide range of services that can be accessed over the internet, eliminating the need for businesses to purchase and maintain their own hardware and software.
- Reliability: Cloud providers offer highly reliable services, with uptime guarantees and disaster recovery plans. This is because cloud providers have invested heavily in infrastructure and security measures to ensure that their services are always available and secure.
- Security: Cloud providers offer a variety of security features to protect customer data. This includes features such as encryption, access control, and auditing. Cloud providers

also have teams of security experts who are constantly monitoring their systems for threats.

5. What are the main advantages of cloud computing?

A) The main advantages of cloud computing are:

- Cost savings: Cloud computing can help businesses save money on IT costs in a number of ways. First, cloud providers offer a variety of pricing options, including pay-as-you-go and subscription models. This allows businesses to only pay for the resources they need, when they need them. Second, cloud providers can help businesses save money on hardware and software costs. This is because cloud providers offer a wide range of services that can be accessed over the internet, eliminating the need for businesses to purchase and maintain their own hardware and software.
- Agility: Cloud computing makes it easy to deploy and scale applications and services quickly. This is because cloud providers offer a wide range of resources that can be provisioned and deprovisioned on demand. This agility can be a major advantage for businesses that need to be able to quickly respond to changing market conditions or customer demands.
- Reliability: Cloud providers offer highly reliable services, with uptime guarantees and disaster recovery plans. This is because cloud providers have invested heavily in infrastructure and security measures to ensure that their services are always available and secure.
- Security: Cloud providers offer a variety of security features to protect customer data. This includes features such as encryption, access control, and auditing. Cloud providers also have teams of security experts who are constantly monitoring their systems for threats.
- Scalability: Cloud computing is highly scalable, meaning that businesses can easily add or remove resources as needed. This can be helpful for businesses that experience seasonal fluctuations in demand or that are rapidly growing.
- Global reach: Cloud computing can help businesses reach a global audience by providing them with the ability to deploy applications and services in multiple data centers around the world. This can be helpful for businesses that have customers or employees in multiple countries.

Overall, cloud computing offers a number of significant advantages for businesses of all sizes. By adopting cloud computing, businesses can improve their agility, cost savings, reliability, security, scalability, and global reach.

6. Describe consumption-based model.

A) A consumption-based model is a pricing model in which customers pay for the resources they use, rather than paying a fixed fee for a set amount of resources. This model is often used in cloud computing, where customers can provision and deprovision resources on demand.

Consumption-based models can offer a number of benefits for businesses, including:

- Cost savings: Businesses only pay for the resources they use, which can save them money, especially if their usage fluctuates over time.
- Flexibility: Businesses can easily add or remove resources as needed, without having to commit to a long-term contract.
- Scalability: Consumption-based models are highly scalable, meaning that businesses can easily scale their resources up or down as needed.

7. What are the types of cloud model?

A) Types of cloud models

There are four main types of cloud models: public cloud, private cloud, community cloud, and hybrid cloud.

Public cloud: Public clouds are owned and operated by third-party cloud providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Public clouds offer a wide range of services, including computing, storage, networking, and databases. Public clouds are typically the most affordable and scalable type of cloud model.

Private cloud: Private clouds are owned and operated by a single organization. Private clouds offer more control and security than public clouds, but they can be more expensive to set up and maintain.

Community cloud: Community clouds are shared by multiple organizations with common interests, such as government agencies or industry associations. Community clouds offer a balance of cost, security, and control.

Hybrid cloud: Hybrid clouds combine elements of public and private clouds. For example, a hybrid cloud might use a public cloud for public-facing applications and a private cloud for sensitive data. Hybrid clouds offer the flexibility to choose the best cloud environment for each application or workload.

8. Define the differences between Infrastructure as a Service (IaaS),

Platform as a Service (PaaS), and Software as a Service (SaaS).

A)

Basis Of	IAAS	PAAS	SAAS
Stands for	Infrastructure as a service.	Platform as a service.	Software as a service.
Uses	IAAS is used by network architects.	PAAS is used by developers.	SAAS is used by the end user.
Access	IAAS gives access to the resources like virtual machines and virtual storage.	PAAS gives access to run time environment to deployment and development tools for application.	SAAS gives access to the end user.
Model	It is a service model that provides virtualized computing resources over the internet.	It is a cloud computing model that delivers tools that are used for the development of applications.	It is a service model in cloud computing that hosts software to make it available to clients.
Technical understanding.	It requires technical knowledge.	Some knowledge is required for the basic setup.	There is no requirement about

Basis Of	IAAS	PAAS	SAAS
			technicalities company handles everything.
Popularity	It is popular among developers and researchers.	It is popular among developers who focus on the development of apps and scripts.	It is popular among consumers and companies, such as file sharing, email, and networking.
Percentage rise	It has around a 12% increment.	It has around 32% increment.	It has about a 27 % rise in the cloud computing model.
Usage	Used by the skilled developer to develop unique applications.	Used by mid-level developers to build applications.	Used among the users of entertainment.
Cloud services.	Amazon Web Services, sun, vCloud Express.	Facebook, and Google search engine.	MS Office web, Facebook and Google Apps.
Enterprise services.	AWS virtual private cloud.	Microsoft Azure.	IBM cloud analysis.
Outsourced cloud services.	Salesforce	Force.com, Gigaspaces.	AWS, Terremark
User Controls	Operating System, Runtime, Middleware, and Application data	Data of the application	Nothing
Others	It is highly scalable and flexible.	It is highly scalable to suit the different	It is highly scalable to suit the small, mid and

Basis Of	IAAS	PAAS	SAAS
		businesses according to resources.	enterprise level business

9.Describe public, private, community and hybrid clouds with its

advantages and disadvantages?

A) Public clouds

Advantages:

- Affordable
- Scalable
- Wide range of services
- Easy to set up and use

Disadvantages:

- Less control and security
- Data privacy concerns

Private clouds

Advantages:

- More control and security
- Data privacy
- Customized to meet specific needs

Disadvantages:

- More expensive to set up and maintain
- Less scalable

- Fewer services

Community clouds

Advantages:

- Balance of cost, security, and control
- Shared by organizations with common interests

Disadvantages:

- May not meet the needs of all organizations
- More complex to manage than public or private clouds

Hybrid clouds

Advantages:

- Flexibility to choose the best cloud environment for each application or workload
- Balance of cost, security, and control

Disadvantages:

- More complex to manage than public or private clouds
- May be more expensive than public clouds

10 .Explain shared responsibility model.

A) The shared responsibility model is a cloud computing model in which the cloud provider and the customer share responsibility for the security and compliance of the customer's data and applications.

The cloud provider is responsible for the security of the underlying infrastructure, such as the hardware and software that power the cloud services. The customer is responsible for the security of their own data and applications, which are deployed on the cloud infrastructure.

11. Describe in short High Availability

A) High availability (HA) is the ability of a system to remain up and running even if one or more of its components fail. HA is achieved by using redundancy and failover mechanisms. Redundancy means that there are multiple copies of each component, so that if one fails, the others can continue to operate. Failover mechanisms are used to automatically switch to a backup component if a primary component fails.

12.Describe scalability and types of Scalability.

A) Scalability is the ability of a system to handle increased or decreased demand. There are two main types of scalability: vertical scalability and horizontal scalability.

Vertical scalability involves adding more resources to a single server or system. For example, you can add more CPU cores, memory, or storage to a server to make it more scalable.

Horizontal scalability involves adding more servers or systems to a distributed system. For example, you can add more web servers to a load balancer to handle more traffic.

13. Differentiate between regions and Availability Zones.

A) Regions are geographically separate areas where cloud resources are located. Regions are typically hundreds or thousands of miles apart.

Availability Zones are isolated locations within a region. Availability Zones are designed to be fault-tolerant, so that if one Availability Zone experiences an outage, the other Availability Zones in the region will remain operational.

Benefits of using regions and Availability Zones:

- Improved availability and reliability: If one Availability Zone experiences an outage, the other Availability Zones in the region will remain operational. This helps to ensure that your applications and data are always available.
- Reduced latency: By deploying your applications and data in regions and Availability Zones that are close to your users, you can reduce latency and improve performance.

- Compliance: Some industries have regulations that require data to be stored in specific locations. By using regions and Availability Zones, you can ensure that your data is stored in compliance with these regulations.

Unit 2

1. **What is Serverless Computing? List an example of serverless**

computing service in Azure.

A) Serverless computing is a cloud computing execution model where the cloud provider manages the server infrastructure and dynamically allocates resources to applications based on demand. This allows developers to focus on writing and deploying code without having to worry about managing servers.

Example of serverless computing service in Azure:

Azure Functions is a serverless computing service that allows developers to run code without provisioning or managing servers. Azure Functions can be used to build a wide variety of applications, such as web APIs, mobile backends, and event-driven processing systems.

2. What is an Azure Subscription? Mention types of Subscriptions,

Management Groups, Resource Groups and Resources in Azure.

A) An Azure subscription is a billing account that gives you access to Azure services. There are three main types of Azure subscriptions:

- Pay-as-you-go: This type of subscription allows you to pay for Azure services on a per-use basis.
- Enterprise Agreement (EA): This type of subscription is for large organizations that commit to a certain level of Azure spending over a period of time.
- Government: This type of subscription is for government organizations that need to comply with specific security and compliance requirements.

Management groups are used to organize and manage Azure resources at scale. Management groups can be used to apply policies, permissions, and compliance settings to multiple resources at once.

Resource groups are containers that hold related Azure resources. Resource groups can be used to organize and manage resources by project, application, or environment.

Resources are the actual Azure services that you use, such as virtual machines, storage accounts, and databases.

3. What is Azure Blob Storage used for?

A) Azure Blob Storage is a cloud storage service that provides highly scalable, secure, and durable storage for your data. Blob Storage can be used to store a wide variety of data, including text and binary data, images, videos, and audio files.

Some common uses for Azure Blob Storage include:

- Web hosting: Blob Storage can be used to store the static and dynamic content for your website.
- Data backup and recovery: Blob Storage can be used to back up your data on-premises and in the cloud.
- Archiving: Blob Storage can be used to archive your data for long-term storage.
- Big data analytics: Blob Storage can be used to store and process large amounts of data for big data analytics.

Blob Storage is a highly scalable service that can grow to meet your needs. You can also choose from a variety of redundancy options to protect your data from loss.

4. What is the difference between Azure Blob Storage and Azure File

Storage?

A) Azure Blob Storage and Azure File Storage are both cloud storage services, but they have different features and use cases.

Azure Blob Storage is a highly scalable object storage service that is designed to store large amounts of unstructured data. Blob Storage is ideal for storing data that is accessed infrequently, such as static website content, media files, and backups.

Azure File Storage is a managed file share service that provides highly available and durable storage for files. File Storage is ideal for storing data that needs to be accessed frequently, such as application data, user profiles, and shared files.

Feature	Azure Blob Storage	Azure File Storage
Type of storage	Object storage	File storage
Ideal for	Storing large amounts of unstructured data	Storing data that needs to be accessed frequently
Common use cases	Static website content, media files, backups	Application data, user profiles, shared files
Scalability	Highly scalable	Highly scalable
Durability	Highly durable	Highly durable
Access	Accessed over the internet	Accessed over the SMB protocol
Security	Secure by default	Secure by default

5. What are azure containers?

A) Azure containers are a way to organize and manage Azure resources. Containers can be used to group resources by project, application, or environment. Containers can also be used to apply policies and permissions to resources.

Azure containers are similar to resource groups, but they offer some additional features, such as:

- Nested containers: Containers can be nested within other containers. This allows you to create a hierarchy of containers to organize your resources.
- Tags: Containers can be tagged with metadata. This allows you to search for and filter resources by tag.
- Deployment slots: Containers can be used to deploy applications to different environments, such as staging and production. This allows you to test and deploy changes to your applications without impacting your production environment.

6..What is Azure App Service?

A) Azure App Service is a fully managed platform for building, deploying, and scaling web applications and mobile backends. App Service supports a variety of programming languages and frameworks, including ASP.NET, Node.js, Python, and Java.

Azure App Service includes a number of features that make it easy to develop, deploy, and manage web applications, such as:

- Automatic scaling: App Service can automatically scale your web application up or down based on demand. This helps to ensure that your web application is always available and performs well.
- Integrated development environment (IDE) support: App Service can be integrated with popular IDEs, such as Visual Studio and Eclipse. This makes it easy to develop and deploy web applications from your IDE.
- Deployment slots: App Service supports deployment slots, which allow you to test and deploy changes to your web application without impacting your production environment.

Azure App Service is a popular choice for developing and deploying web applications because it is easy to use and offers a variety of features that make it easy to build, scale, and manage web applications.

7.Explain about LRS, GRS, ZRS and RA-GRS with appropriate Figure.

A) Azure Storage offers four replication options: locally redundant storage (LRS), geo-redundant storage (GRS), zone-redundant storage (ZRS), and read-access geo-redundant storage (RA-GRS).

Locally redundant storage (LRS) replicates your data three times within the same data center. This means that your data is protected from hardware failures within the data center, but it is not protected from regional outages or disasters.

Geo-redundant storage (GRS) replicates your data to a secondary region that is hundreds of miles away from the primary region. This protects your data from regional outages and disasters. However, GRS can introduce slightly higher latency than LRS because the data needs to be replicated across a long distance.

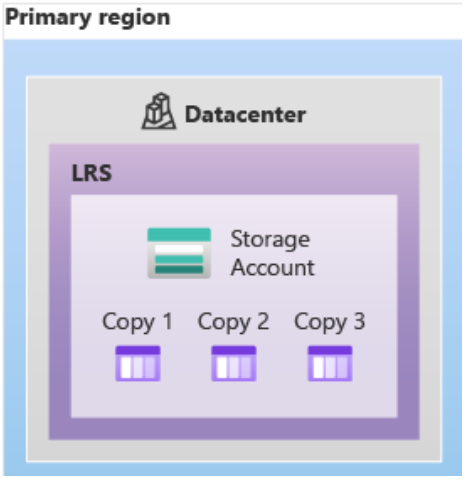
Zone-redundant storage (ZRS) replicates your data three times within three zones in the same region. This protects your data from hardware failures within a zone, but it is not protected from regional outages or disasters. ZRS also offers lower latency than GRS because the data is replicated within the same region.

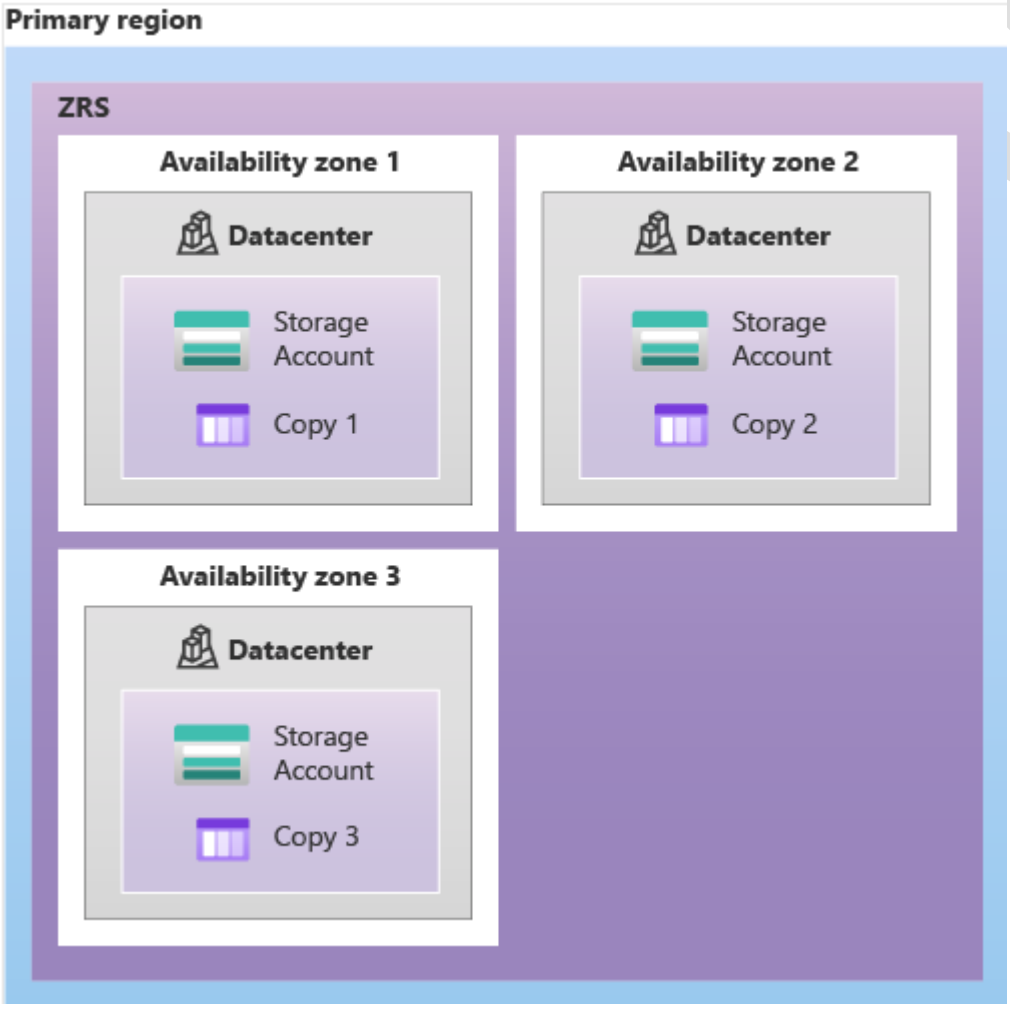
Read-access geo-redundant storage (RA-GRS) is a combination of GRS and ZRS. It replicates your data to a secondary region and within three zones in the primary region. This provides the highest level of redundancy and availability, but it can also be the most expensive option.

The following table summarizes the four Azure Storage replication options:

Replication option	Description
Locally redundant storage (LRS)	**Replicates data three times within the same**

	data center.
Geo-redundant storage (GRS)	**Replicates data to a secondary region that is hundreds of miles away from the primary region.**
Zone-redundant storage (ZRS)	**Replicates data three times within three zones in the same region.**
Read-access geo-redundant storage (RA-GRS)	**Replicates data to a secondary region and within three zones in the primary region.**


Primary region
Datacenter
LRS
Storage Account
Copy 1
Copy 2
Copy 3


Primary region
ZRS
Availability zone 1
Datacenter
Storage Account
Copy 1
Availability zone 2
Datacenter
Storage Account
Copy 2
Availability zone 3
Datacenter
Storage Account
Copy 3

8.What is Azure Virtual Networking

A) Azure Virtual Networking (VNet) is a networking service that allows you to create a private network for your Azure resources. VNet gives you more control over your network environment, including the IP address range, routing, and security policies.

You can use VNet to connect your Azure resources to each other and to on-premises resources. VNet also supports a variety of networking features, such as subnets, network security groups, and load balancers.

9. What is Azure SQL Database?

A) Azure SQL Database is a fully managed relational database service that supports a variety of workloads, including transactional, analytical, and mixed workloads. Azure SQL Database is based on the Microsoft SQL Server database engine.

Azure SQL Database offers a number of features that make it a popular choice for developing and deploying database applications, such as:

- High availability and scalability: Azure SQL Database offers high availability and scalability, with a 99.99% uptime SLA.
- Security: Azure SQL Database includes a number of security features, such as encryption, role-based access control, and auditing.
- Performance: Azure SQL Database offers high performance for a variety of workloads.
- Compatibility: Azure SQL Database is compatible with the Microsoft SQL Server database engine, so you can easily migrate your existing database applications to Azure SQL Database.

10.Explain about SQL Database elastic pool and SQL Managed Instance

Pool.

A) SQL Database elastic pool is a feature that allows you to manage a group of SQL Databases as a single unit. Elastic pools can be used to improve the performance and cost-effectiveness of your SQL Databases.

SQL Managed Instance Pool is a feature that allows you to manage a group of SQL Managed Instances as a single unit. Managed Instance Pools can be used to improve the performance and cost-effectiveness of your SQL Managed Instances.

Benefits of using SQL Database elastic pool and SQL Managed Instance Pool:

- Improved performance: Elastic pools and Managed Instance Pools can improve the performance of your SQL Databases and SQL Managed Instances by distributing the workload across multiple instances.
- Reduced costs: Elastic pools and Managed Instance Pools can reduce the cost of your SQL Databases and SQL Managed Instances by allowing you to share resources across multiple instances.
- Simplified management: Elastic pools and Managed Instance Pools simplify the management of your SQL Databases and SQL Managed Instances by allowing you to manage them as a single

11. List and Explain various Redundancy/Replication options available in

Azure Storage Service.

A) Azure Storage offers four replication options:

- Locally redundant storage (LRS): LRS replicates your data three times within the same data center. This means that your data is protected from hardware failures within the data center, but it is not protected from regional outages or disasters.
- Geo-redundant storage (GRS): GRS replicates your data to a secondary region that is hundreds of miles away from the primary region. This protects your data from regional outages and disasters. However, GRS can introduce slightly higher latency than LRS because the data needs to be replicated across a long distance.
- Zone-redundant storage (ZRS): ZRS replicates your data three times within three zones in the same region. This protects your data from hardware failures within a zone, but it is not protected from regional outages or disasters. ZRS also offers lower latency than GRS because the data is replicated within the same region.
- Read-access geo-redundant storage (RA-GRS): RA-GRS is a combination of GRS and ZRS. It replicates your data to a secondary region and within three zones in the primary region. This provides the highest level of redundancy and availability, but it can also be the most expensive option.

12. List out most common use cases of Azure Functions.

A) Azure Functions is a serverless computing service that allows you to run code without provisioning or managing servers. Azure Functions can be used to build a wide variety of applications, such as web APIs, mobile backends, and event-driven processing systems.

Here are some of the most common use cases of Azure Functions:

- Web APIs: Azure Functions can be used to build RESTful APIs that can be consumed by web applications, mobile apps, and other services.
- Mobile backends: Azure Functions can be used to build mobile backends that provide authentication, authorization, data storage, and other services to mobile apps.
- Event-driven processing: Azure Functions can be used to build event-driven processing systems that respond to events in real time. For example, you could use Azure Functions to build a system that sends notifications to users when new data is added to a database.
- Serverless batch processing: Azure Functions can be used to build serverless batch processing systems that process large amounts of data in batches. For example, you could use Azure Functions to build a system that processes financial data at the end of each day.
- Integration: Azure Functions can be used to integrate different systems and services together. For example, you could use Azure Functions to integrate your on-premises systems with Azure cloud services.

Unit 3

1. Describe Azure Active Directory and its various features including RBAC,

MFA and SSO.

A) Azure Active Directory (Azure AD) is a cloud-based identity and access management (IAM) service. Azure AD provides a single place to manage identities for all of your applications and services, both on-premises and in the cloud.

Azure AD offers a number of features, including:

- Role-based access control (RBAC): RBAC allows you to define roles and assign them to users. Roles define the permissions that users have to access resources.
- Multi-factor authentication (MFA): MFA adds an extra layer of security to your accounts by requiring users to provide two or more factors of authentication, such as a password and a one-time code.
- Single sign-on (SSO): SSO allows users to sign in to multiple applications and services with a single set of credentials.

2. Write a brief note on Authentication and Authorization

A) Authentication is the process of verifying the identity of a user. Authorization is the process of determining whether an authenticated user has permission to access a resource.

Azure AD supports a variety of authentication and authorization protocols, including:

- OpenID Connect: OpenID Connect is an open standard that allows you to authenticate users to applications and services.
- OAuth 2.0: OAuth 2.0 is an open standard that allows you to authorize applications to access data on behalf of users.
- SAML: SAML is an open standard that allows you to exchange authentication and authorization data between different systems.

Benefits of using Azure AD

- Simplify identity management: Azure AD provides a single place to manage identities for all of your applications and services, both on-premises and in the cloud. This can help you to simplify your identity management and reduce costs.
- Improve security: Azure AD offers a number of security features, such as MFA and SSO, which can help you to improve the security of your accounts and applications.
- Increase productivity: Azure AD can help to increase the productivity of your users by making it easier for them to access the applications and services they need.

3.Explain briefly about SSO and Multifactor Authentication

A) Single sign-on (SSO) is a technology that allows users to sign in to multiple applications and services with a single set of credentials. This can help to improve the user experience and reduce the risk of password fatigue.

Multi-factor authentication (MFA) is a security measure that requires users to provide two or more factors of authentication to verify their identity. This can help to protect accounts from unauthorized access, even if an attacker has the user's password.

Azure AD supports both SSO and MFA. Azure AD SSO makes it easy for users to sign in to applications and services that support Azure AD authentication. Azure AD MFA adds an extra layer of security to Azure AD accounts by requiring users to provide a one-time code in addition to their password when signing in.

4. Describe Azure Authentication methods.

A) Azure AD supports a variety of authentication methods, including:

- Password: This is the most common authentication method. Users enter their username and password to verify their identity.
- MFA: Azure AD supports a variety of MFA methods, such as one-time codes generated by a mobile app, phone calls, and text messages.
- FIDO2: FIDO2 is a new authentication standard that allows users to log in to websites and apps using a variety of devices, such as fingerprint scanners, facial recognition, and security keys.

5. What is Single Sign –On?

A) Single sign-on (SSO) is a technology that allows users to sign in to multiple applications and services with a single set of credentials. This can help to improve the user experience and reduce the risk of password fatigue.

For example, with SSO, a user could sign in to their Microsoft 365 account once and then access all of their Microsoft 365 applications, such as Outlook, OneDrive, and Teams, without having to sign in to each application individually.

SSO can be implemented in a variety of ways, but the most common approach is to use a third-party identity provider (IdP), such as Azure AD. The IdP provides a central location for users to manage their credentials and authenticate to applications and services.

6. What is Multi-Factor Authentication?

A) Multi-factor authentication (MFA) is a security measure that requires users to provide two or more factors of authentication to verify their identity. This can help to protect accounts from unauthorized access, even if an attacker has the user's password.

Common MFA factors include:

- Something you know: This could be a password, PIN, or passphrase.
- Something you have: This could be a physical object, such as a smartphone or security key.
- Something you are: This could be a biometric factor, such as a fingerprint scan or facial recognition.

MFA can be implemented in a variety of ways, but the most common approach is to use a one-time code generated by a mobile app. When a user signs in, they are prompted to enter the code in addition to their password.

7. What is RBAC?

A) RBAC stands for Role-Based Access Control. It is a method of restricting access to resources based on the roles of individual users within an enterprise. RBAC allows organizations to assign different levels of access to different users, depending on their job duties and responsibilities.

8. How does RBAC works?

A) RBAC works by defining roles and assigning them to users. Roles define the permissions that users have to access resources. For example, a role might define permissions to read, write, or delete files in a certain directory.

Once a user is assigned to a role, they will have the permissions that are defined for that role. Users cannot access resources that they do not have permission to access.

RBAC can be implemented in a variety of ways, but the most common approach is to use a third-party identity and access management (IAM) solution, such as Azure AD. IAM solutions provide a central location to manage roles and users, and to assign roles to users.

9. How does Azure AD provide single sign-on (SSO) capabilities?

A) Azure AD provides SSO capabilities by acting as a trusted identity provider (IdP) for applications and services. When a user signs in to Azure AD, they are authenticated once and then can access all of their applications and services without having to sign in to each one individually.

Azure AD supports a variety of SSO protocols, including SAML, OpenID Connect, and OAuth 2.0. This allows Azure AD to integrate with a wide variety of applications and services.

10. What is multi-factor authentication (MFA) and its importance in Azure?

A) Multi-factor authentication (MFA) is a security measure that requires users to provide two or more factors of authentication to verify their identity. This can help to protect accounts from unauthorized access, even if an attacker has the user's password.

Azure AD supports a variety of MFA methods, including one-time codes generated by a mobile app, phone calls, and text messages. Azure AD also supports FIDO2, which is a new authentication standard that allows users to log in to websites and apps using a variety of devices, such as fingerprint scanners, facial recognition, and security keys.

MFA is important in Azure because it can help to protect your accounts and data from unauthorized access. Even if an attacker has a user's password, they will not be able to access their account without also providing a one-time code or other factor of authentication.

Benefits of using Azure AD RBAC, SSO, and MFA

Azure AD RBAC, SSO, and MFA can provide a number of benefits, including:

- Improved security: RBAC, SSO, and MFA can help to protect your accounts and data from unauthorized access.

- Simplified access management: RBAC and SSO can simplify the process of managing access to your applications and services.
- Reduced risk of password breaches: MFA can help to reduce the risk of password breaches by requiring users to provide two or more factors of authentication to log in.
- Improved user experience: SSO can simplify the sign-in process for users and make it easier for them to access the applications and services they need.

11. What is Azure AD? Explain different edition of Azure AD?

A) Azure AD is a cloud-based identity and access management (IAM) service. Azure AD provides a single place to manage identities for all of your applications and services, both on-premises and in the cloud.

Azure AD offers a variety of features, including:

- Role-based access control (RBAC): RBAC allows you to define roles and assign them to users. Roles define the permissions that users have to access resources.
- Multi-factor authentication (MFA): MFA adds an extra layer of security to your accounts by requiring users to provide two or more factors of authentication, such as a password and a one-time code.
- Single sign-on (SSO): SSO allows users to sign in to multiple applications and services with a single set of credentials.

Azure AD is available in two editions:

- Free edition: The free edition of Azure AD includes basic features, such as user management, group management, and password management.
- Premium edition: The premium edition of Azure AD includes all of the features of the free edition, plus additional features, such as MFA, SSO, and advanced security features.

12. Explain the concept of Azure B2B and B2C.

A) Azure B2B and B2C are two different ways to use Azure AD to manage identities for external users.

Azure B2B allows you to collaborate with external users, such as partners and customers, without having to share your Azure AD directory with them. Azure B2B provides a way to invite external users to your Azure AD tenant and grant them access to specific resources.

Azure B2C allows you to create a custom identity experience for your customers. Azure B2C provides a way to manage user accounts, sign-in processes, and user profiles for your customers.

13. Define Azure Zero trust model.

A) Azure Zero trust is a security model that assumes that no user or device can be trusted by default. Azure Zero trust requires all users and devices to be authenticated and authorized before being granted access to resources.

Azure Zero trust is based on the following principles:

- Verify explicitly: Azure Zero trust requires all users and devices to be authenticated and authorized before being granted access to resources.
- Use least privilege: Azure Zero trust grants users and devices only the minimum permissions they need to perform their tasks.
- Assume breach: Azure Zero assumes that a breach has already occurred and takes steps to mitigate the damage.

14. Explain defense in depth.

A) Defense in depth is a security strategy that layers multiple security controls to protect resources. Defense in depth makes it more difficult for attackers to succeed because they must overcome multiple security controls in order to reach a resource.

Azure provides a variety of security controls that can be used to implement defense in depth, including:

- Network security: Azure provides network security controls, such as firewalls and network security groups, to protect resources from unauthorized access.
- Application security: Azure provides application security controls, such as web application firewalls and DDoS protection, to protect applications from attacks.
- Data security: Azure provides data security controls, such as encryption and access control, to protect data from unauthorized access.

15. What is difference between Azure Firewall and NSG?

A) Azure Firewall and NSG are both network security controls that can be used to protect resources in Azure. However, there are some key differences between the two services.

Azure Firewall is a cloud-native firewall that provides a comprehensive set of security features, including:

- Intrusion detection and prevention (IDS/IPS): Azure Firewall can detect and block common attacks, such as SQL injection and cross-site scripting.
- Web application firewall (WAF): Azure Firewall can protect web applications from common attacks, such as denial-of-service attacks and SQL injection.
- Application rules: Azure Firewall allows you to define custom rules to control traffic to and from your resources.

NSG is a basic firewall that can be used to filter traffic to and from subnets in Azure. NSG provides a simple way to control traffic to and from your resources, but it does not offer the same level of protection as Azure Firewall.

When to use Azure Firewall:

Azure Firewall is a good choice for organizations that need a comprehensive set of security features to protect their resources. Azure Firewall is also a good choice for organizations that need to protect web applications from attacks.

When to use NSG:

NSG is a good choice for organizations that need a simple way to control traffic to and from their resources.

Unit 4.

1. What is the Azure Pricing Calculator, and how can it assist in estimating costs?

A) The Azure Pricing Calculator is a tool that allows you to estimate the cost of using Azure services. The calculator takes into account the type of service you are using, the region where you are using the service, and the amount of resources you are using.

To use the Azure Pricing Calculator, simply select the service you are using, the region where you are using the service, and the amount of resources you are using. The calculator will then estimate the cost of using that service.

The Azure Pricing Calculator can be helpful for estimating the cost of using Azure services before you start using them. It can also be helpful for budgeting for Azure costs.

2. what is azure cost management?Explain its features and functionalities.

A) Azure cost management is a process of monitoring and managing your Azure costs. Azure cost management can help you to optimize your Azure costs and avoid overspending.

Azure cost management provides a number of features and functionalities, including:

- Cost analysis: Azure cost management provides cost analysis tools that allow you to analyze your Azure costs in detail. This can help you to identify areas where you can reduce your costs.
- Cost budgeting: Azure cost management allows you to create budgets for your Azure costs. This can help you to stay within your budget.
- Cost alerts: Azure cost management allows you to create alerts that will notify you when your Azure costs exceed a certain threshold. This can help you to avoid overspending.

3. Describe Azure's deprecation policies and their impact on services and users.

A) Azure's deprecation policies are designed to ensure that Azure services are reliable and secure. Azure's deprecation policies also ensure that Azure customers are aware of changes to Azure services that may impact them.

Azure's deprecation policies state that Azure services will be deprecated at least 12 months in advance of being retired. This gives Azure customers time to migrate their workloads to other Azure services or to on-premises infrastructure.

The impact of Azure's deprecation policies on services and users is that Azure customers need to be aware of changes to Azure services that may impact them and need to plan accordingly.

4.Describe the different Azure subscription options available

A) There are three main types of Azure subscriptions available:

- Pay-as-you-go: Pay-as-you-go subscriptions are the most flexible type of Azure subscription. Pay-as-you-go subscriptions allow you to pay for Azure services on a per-use basis.
- Enterprise Agreement (EA): EA subscriptions are designed for large organizations that commit to a certain level of Azure spending over a period of time. EA subscriptions can provide discounts on Azure services.
- Government: Government subscriptions are designed for government organizations that need to comply with specific security and compliance requirements.

5. Describe About Pricing calculator and TCO Calculator.

A) Pricing calculator:

The Azure Pricing Calculator is a tool that allows you to estimate the cost of using Azure services. The calculator takes into account the type of service you are using, the region where you are using the service, and the amount of resources you are using.

TCO Calculator:

The Azure Total Cost of Ownership (TCO) Calculator is a tool that allows you to estimate the total cost of ownership of migrating your workloads to Azure. The TCO Calculator takes into account the cost of your current on-premises infrastructure, the cost of migrating your workloads to Azure, and the cost of using Azure services.

The Azure Pricing Calculator and the Azure TCO Calculator can be helpful for estimating the cost of using Azure services and for making decisions about whether to migrate your workloads to Azure.

6. What are cost management factors are their in azure.

A) There are a number of factors that can affect your Azure costs, including:

- The type of services you are using: Some Azure services are more expensive than others. For example, virtual machines are more expensive than storage.
- The region where you are using the services: Some Azure regions are more expensive than others. For example, the West US 2 region is more expensive than the East US 2 region.
- The amount of resources you are using: The more resources you are using, the higher your costs will be. For example, if you are using a large virtual machine, your costs will be higher than if you are using a small virtual machine.
- Your Azure subscription type: Your Azure subscription type can also affect your costs. For example, Enterprise Agreement (EA) subscriptions can provide discounts on Azure services.

7. Explain azure support options.

A) Azure offers a number of support options, including:

- Self-support: Azure provides a variety of self-support resources, such as documentation, tutorials, and forums.

- Basic support: Basic support is included with all Azure subscriptions. Basic support provides access to Azure documentation and to Azure support engineers who can answer your questions.
- Developer support: Developer support is designed for developers who need help with Azure development. Developer support provides access to Azure support engineers who can help you with Azure development tasks.
- Professional direct support: Professional direct support is designed for organizations that need help with Azure deployment and management. Professional direct support provides access to Azure support engineers who can help you with Azure deployment and management tasks.

8. What isCost Management CapabilitiesinAzure and Describe about Budget Alerts, CreditAlerts andDepartment SpendingQuotaAlerts..

A) Azure Cost Management Capabilities is a set of tools and features that help you to monitor and manage your Azure costs. Azure Cost Management Capabilities includes the following features:

- Cost analysis: Cost analysis provides you with insights into your Azure costs. You can use cost analysis to identify areas where you can reduce your costs.
- Cost budgeting: Cost budgeting allows you to create budgets for your Azure costs. You can use cost budgeting to stay within your budget.
- Cost alerts: Cost alerts notify you when your Azure costs exceed a certain threshold. You can use cost alerts to avoid overspending.

Budget alerts: Budget alerts notify you when your Azure costs exceed a certain threshold. You can set up budget alerts for your total Azure costs or for specific Azure services.

Credit alerts: Credit alerts notify you when your Azure credits are about to expire. You can set up credit alerts to remind yourself to use your Azure credits before they expire.

Department spending quota alerts: Department spending quota alerts notify you when a department exceeds its Azure spending quota. You can set up department spending quota alerts to ensure that each department stays within its budget.

9. What aretheFactorsthat affect costin Azure?

A) The following factors can affect your Azure costs:

- The type of services you are using: Some Azure services are more expensive than others. For example, virtual machines are more expensive than storage.
- The region where you are using the services: Some Azure regions are more expensive than others. For example, the West US 2 region is more expensive than the East US 2 region.
- The amount of resources you are using: The more resources you are using, the higher your costs will be. For example, if you are using a large virtual machine, your costs will be higher than if you are using a small virtual machine.
- Your Azure subscription type: Your Azure subscription type can also affect your costs. For example, Enterprise Agreement (EA) subscriptions can provide discounts on Azure services.
- Your usage patterns: Your usage patterns can also affect your costs. For example, if you are using Azure services on a burst basis, your costs will be higher than if you are using Azure services on a consistent basis.
-

Unit 5.

1. **What is the Purpose of Azure Advisor.**

A) Azure Advisor is a service that provides recommendations to help you improve the performance, reliability, security, and cost-effectiveness of your Azure deployments. Azure Advisor analyzes your resource configuration and usage telemetry and then recommends solutions that can help you to optimize your deployments.

Azure Advisor recommendations are categorized into five areas:

- Reliability: Azure Advisor recommends actions that can help you to improve the reliability of your Azure deployments.
- Performance: Azure Advisor recommends actions that can help you to improve the performance of your Azure deployments.

- Security: Azure Advisor recommends actions that can help you to improve the security of your Azure deployments.
- Operational excellence: Azure Advisor recommends actions that can help you to improve the operational excellence of your Azure deployments.
- Cost: Azure Advisor recommends actions that can help you to reduce the cost of your Azure deployments.

2. Describe Service Lifecycles in Cloud Computing.

A) Cloud computing services have a lifecycle that is similar to the lifecycle of on-premises software and hardware. The cloud computing service lifecycle consists of the following phases:

- Planning: In the planning phase, you identify your business needs and requirements and select the cloud computing services that will meet your needs.
- Deployment: In the deployment phase, you deploy your applications and data to the cloud computing services.
- Management: In the management phase, you manage your cloud computing services, including monitoring performance, scaling resources, and applying security updates.
- Retirement: In the retirement phase, you retire your cloud computing services, such as when you no longer need them or when they are no longer supported by the cloud computing provider.

3. Define Azure Service Level Agreements (SLAs) and explain their

significance for businesses.

A) Azure Service Level Agreements (SLAs) are commitments by Microsoft to deliver a certain level of availability and performance for Azure services. Azure SLAs are backed by a financial guarantee.

Azure SLAs are important for businesses because they provide a level of assurance that Azure services will be available and performant. This assurance can help businesses to reduce their risk and to improve their customer satisfaction.

4. What is composite SLA?

A) A composite SLA is an SLA that covers multiple Azure services. Composite SLAs are typically used for complex applications that rely on multiple Azure services.

Composite SLAs can be more complex to manage than SLAs for individual Azure services. However, composite SLAs can provide a simplified view of the SLAs for all of the Azure services that are used by an application.

5.Descibe azure service health.

A) Azure Service Health is a service that provides information about the status of Azure services. Azure Service Health provides information about upcoming maintenance events, service incidents, and service health advisories.

Azure Service Health is important for businesses because it can help them to stay informed about the status of Azure services and to plan for any potential disruptions.

Here are some of the benefits of using Azure Service Health:

- Improved visibility: Azure Service Health provides a centralized view of the status of all Azure services. This can help you to quickly identify any issues with Azure services.
- Reduced downtime: Azure Service Health can help you to avoid downtime by providing information about upcoming maintenance events and service incidents.
- Improved customer satisfaction: Azure Service Health can help you to improve customer satisfaction by providing information about the status of Azure services.