Module - 3 (System Management and Public Cloud)

1.Different type of cloud storage

Open cloud.

Open cloud is a type of cloud storage that is available to the public. This means that anyone with an internet connection can use it and there are no restrictions on what you store or who accesses your files, even if they’re not authorized to do so. An open cloud has many advantages, such as low cost for small businesses and easy accessibility from anywhere. The disadvantages to open clouds are that they can be difficult to back up and there is a risk of data being compromised, which could lead to significant consequences.

Private cloud.

Private cloud is a type of cloud storage that can be accessed by only certain people and organizations. It requires the user to log in with their username, password, or both so that it’s secure from any unauthorized access. Private cloud has many advantages such as high security for sensitive data, and easy administration of policies and rules. The disadvantages of using a private cloud include increased cost for storage because of the need to buy your own hardware, and difficulty accessing data outside of a private cloud.

Hybrid cloud.

A hybrid cloud is a combination or mix between an open cloud and private cloud. The public side allows anyone with access to it to use it while the private side can only be accessed by authorized people/organizations. The key benefits of using a hybrid cloud include:

high security for all your data, easy administration, and increased access to resources with better performance than on just one type of cloud alone. The disadvantages are that a hybrid cloud can be more expensive and it also has more downtime than just a single type of cloud.

2. What is role base access control and identity and access management and MFA

identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations. Systems used for IAM include single sign-on systems, two-factor authentication, multifactor authentication and privileged access management. These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.

IAM systems can be deployed on premises, provided by a third-party vendor through a cloud-based subscription model or deployed in a hybrid model.

On a fundamental level, IAM encompasses the following components:

- how individuals are identified in a system (understand the difference between identity management and authentication);
- how roles are identified in a system and how they are assigned to individuals;
- adding, removing and updating individuals and their roles in a system;
- assigning levels of access to individuals or groups of individuals; and

- protecting the sensitive data within the system and securing the system itself.

When it comes to identity and access, most organizations that are considering using the public cloud are concerned about two things:

1. Ensuring that when people leave the organization, they lose access to resources in the cloud.
2. Striking the right balance between autonomy and central governance – for example, giving project teams the ability to create and manage virtual machines in the cloud while centrally controlling the networks those VMs use to communicate with other resources.

Azure Active Directory (Azure AD) and Role-Based Access Control (RBAC) work together to make it simple to carry out these goals.

3.What is physical and virtual host allocation?

Before we dive into VM resource allocation, let's go over the general definition and purpose of resource allocation in IT administration. Resource allocation describes the process of figuring out the best way to distribute limited resources between multiple applications. Virtual machine resource allocation is this same task: determining how to best divide VM resources between the VMs present in your network. Effective resource allocation will ensure all VMs complete jobs successfully and without draining excessive resources.

Virtual allocation is the act of provisioning virtual machine processors onto physical hosts or cores, such as your CPU, to increase networking facilities and opportunities. Enacting proper virtual machine resource allocation will help you distribute operations fairly among VMs used for virtual allocation. Virtual allocation may seem like a dream come true, but keep in mind virtual machine resource allocation often leads to optimization problems — more VM processors means more connections within your network, which increases the number of simultaneously occurring operations. The more operations going on at once, the higher your chances of latency, bottlenecks, and other performance issues.

Now, the general rule is you shouldn't over-allocate your virtual machine processors. This means you should maintain a 1:1 ratio between your virtual machine processor and its host or core. It's recommended to only have one VM processor per host because if you over-subscribe virtual machine processors to a single core, events could be stalled or delayed to the point of extreme frustration and user dissatisfaction. But it's unrealistic to maintain you should *never* over-allocate your VM resources, or to pretend IT administrators don't over-allocate their virtual machine processors.

The truth is, you can add as many virtual machine processors as you like to a host. However, it's best to start small to prevent overloading your network. A good general rule for bringing virtual allocation into your IT infrastructure is to start at a 2:1 ratio and work your way up in small increments — for example, start at 2:1 then move to 4:1, to 8:1, to 12:1, and so on. If you monitor for the potential consequences of virtual machine resource allocation, such as latency and bottlenecks, you can indefinitely increase your virtual machine resource distribution.

Oftentimes, IT administrators will enlist the help of a hypervisor to run virtual machines and aid with virtual machine resource allocation. Hypervisors manage processes using threads, which are sequences of CPU instructions. While you cannot permanently assign hypervisors to a particular host, you can assign specific threads to specific cores for more customization. Hyper-V is one common hypervisor used to manage virtual machine resource allocation. Like VM resource allocation, Hyper-V virtual processor allocation can still yield delayed or lost operations and other performance issues. But using Hyper-V or any other hypervisor will certainly help you stay on top of your virtual machine resource distribution and individual VM performance.

3.How to access resource of cloud computing?

Resource pooling is an information technology(IT) term used in cloud computing environments to describe a situation in which suppliers deliver temporary and expandable services to numerous clients, customers, or "tenants." These services can be adjusted to meet each client's demands without requiring the client or end-user to notice any changes.

Cloud computing platforms are accessible via internet connection. It can also be shared, maintained, or developed platforms that provide specific services. These are also cutting-edge technologies that provide clients with greater flexibility and scalability. In the cloud computing resource sharing paradigm, the service provider serves numerous clients simultaneously. To handle and deal with such clients, they employ a multi-tenant approach.

As a result, IT resources such as central processing units (CPUs), storage devices, and Random Access Memory(RAM) is included in this model. And to ensure flexibility in service delivery, all of these devices are handled as one. These platforms allow for various paths and have boosted server speed. In a nutshell, it's the IT industry's multi-tenant concept. Here, the service provider delivers the same service to many consumers with no technological difficulties.

Now we will learn about the working of resource pooling in cloud computing, its types, and its advantages and disadvantages.

5. Type of backup in cloud?

There are various **data backup** types, each designed to address different risks, vulnerabilities and storage needs. Effectively backing up the files, networks, servers and other assets begin with addressing a network's capabilities and selecting the proper type of backup for the circumstances.

A **backup** is a copy of the data that store in the cloud. Backing-up is an important process that everyone should do to have a fail-safe for when the inevitable happens. The principle is to make copies of particular data to use those copies for restoring the information if a failure occurs. A data loss event occurs due to deletion, corruption, theft, viruses, etc.

Protecting data against loss, corruption, disasters (human-caused or natural), and other problems is one of the IT organizations' top priorities. To avoid this loss, implementing an efficient and effective set of backup operations can be difficult.

The term backup has become synonymous with data protection over the past several decades and maybe accomplished via several methods. Backup software applications reduce the complexity of performing backup and recovery operations. Backing up data is only one part of a disaster protection plan and may not provide the level of data and disaster recovery capabilities desired without careful design and testing.

location or automatically using a backup program. Each backup program has its approach in executing the backup.

There are four most common backup types implemented and generally used in most of these programs, such as:

1. Full backup
2. Incremental backup
3. Differential backup
4. Mirror backup

A type of backup defines how data is copied from source to destination and lays the data repository model's grounds or how the back-up is stored and structured.

There are some types of backup that are better in certain locations. If we perform cloud backup, then incremental backups are generally a better backup type because they consume fewer resources. We might start with a full backup in the cloud and then shift to incremental backups. Mirror backup, though, is typically more of an on-premises approach and often involves disks.

Full backups

The most basic and complete type of backup operation is a full backup. As the name implies, this backup type makes a copy of all data to a storage device, such as a disk or tape. The primary advantage of performing a full backup during every operation is that a complete copy of all data is available with a single media set.

It takes the shortest time to restore data, a metric known as a recovery time objective. However, the disadvantages are that it takes longer to perform a full backup than other types, requiring more storage space.

Thus, full backups are typically run only periodically. Data centers with a small amount of data may choose to run a full backup daily or even more often in some cases. Typically, backup operations employ a full backup in combination with either incremental or differential backups.

Incremental backups

An incremental backup operation will result in copying only the data that has changed since the last backup operation of any type. An organization typically uses the modified timestamp on files and compares them to the last backup timestamp.

Backup applications track and record the date and time that backup operations occur to track files modified since these operations. Because an incremental backup will only copy data since the last backup of any type, an organization may run it as often as desired, with only the most recent changes stored.

The benefit of an incremental backup is that it copies a smaller amount of data than a full. Thus, these operations will have a faster backup speed and require fewer media to store the backup.

6.What is disaster recovery?

Cloud-based backup and retrieval capabilities help you to back-up and reestablish business-critical directories if they are breached. Thanks to its high adaptability, cloud technologies allow efficient disaster recovery, irrespective of the task's nature or ferocity. Data is kept in a virtual storage environment designed for increased accessibility. The program is accessible on availability, enabling companies of various sizes to customize Disaster Recovery (DR) solutions to their existing requirements.

Cloud disaster recovery (CDR) is simple to configure and maintain, as opposed to conventional alternatives. Companies no longer ought to waste a lot of time transmitting data backups from their in-house databases or hard drive to restore after a tragedy. Cloud optimizes these procedures, decisions correctly, and information retrieval.

Cloud Disaster Recovery (CDR) is based on a sustainable program that provides you recover safety functions fully from a catastrophe and offers remote access to a computer device in a protected virtual world.

When it comes to content DRs, maintaining a supplementary data center can be expensive and time taking. CDR (Cloud disaster recovery) has altered it all in the conventional DR (Disaster recovery) by removing the requirement for a centralized system and drastically reducing leisure time. Information technology (IT) departments can now use the cloud's benefits to twist and refuse instantly. This leads to faster recovery periods at a fraction of the price.

As corporations keep adding system and software apps and services to their day-to-day procedures, the associated privacy concerns significantly raise. Crises can happen at any point and maintain a company decimated by huge information loss. When you recognize what it can charge, it is evident why it makes good sense to establish an information restore and retrieval plan.

Disaster recovery data shows that 98 percent of the surveyed companies signify that a couple of hours of leisure time can charge their corporation more than $100,000. Any quantity of rest time can cost the organization

10 of thousands to hundreds and thousands of person-hour workers expended recovering or redeploying missed productivity.

An 8-hour leisure time screen can pay up to $20k for a small business and tens of millions for large companies in certain instances.

Given the estimates, it is apparent why every second of assistance or structure disruption counts data and the real benefit of containing a crisis management plan.

How is cloud disaster management working?

Cloud disaster recovery is taking a very differentiated perspective from classical DR (Disaster recovery). Rather than stacking data centers with Operating system technology and fixing the final configuration used in manufacturing, cloud disaster recovery captures the whole server, including the OS, apps, fixes, and information, into a separate software package or virtual environment.

The virtual server is then replicated or supported to an off-site server farm or rolled to a remote server in mins. While the virtual server is not hardware-dependent, the OS, apps, flaws, and information can be moved from one to another data center much quicker than conventional DR methodologies.