RGPVNOTES.IN

Program : **B.E**

Subject Name: **Cloud Computing**

Subject Code: **CS-8002**

Semester: **8th**

Subject Notes
CS 8002 - Cloud Computing

Unit-3

Cloud Management

Following tasks are the main components of cloud management:

- **Task Resubmission**

A job may fail now whenever a failed task is detected, In this case at runtime the task is resubmitted either to the same or to a different resource for execution.

- **Timing check**

This is done by watch dog. This is a supervision technique with time of critical function.

- **Rescue workflow**

This technique allows the workflow to persist until it becomes unimaginable to move forward without catering the failed task.

- **Software Rejuvenation**

It is a technique that designs the system for periodic reboots. It restarts the system with clean state and helps to fresh start.

- **Preemptive Migration**

Preemptive Migration count on a feedback-loop control mechanism. The application is constantly monitored and analyzed.

- **Masking**

After employment of error recovery the new state needs to be identified as a transformed state. Now if this process applied systematically even in the absence of effective error provide the user error masking.

- **Reconfiguration**

In this procedure we eliminate the faulty component from the system.

- **Resource Co-allocation**

This is the process of allocating resources for further execution of task.

- **User specific (defined) exception handling**

In this case user defines the particular treatment for a task on its failure.

Several models are implemented based on these types of techniques. Table summarized the Comparison among various models based on protection against the type of fault, and procedure.

“AFTRC” a fault tolerance model for real time cloud computing based on the fact that a real time system can take advantage the computing capacity, and scalable virtualized environment of cloud computing for better implement of real time application. In this proposed model the system tolerates the fault proactively and makes the diction on the basis of reliability of the processing nodes [9].

“LLFT” is a propose model which contains a low latency fault tolerance (LLFT) middleware for providing fault tolerance for distributed applications deployed within the cloud computing environment as a service offered by the owners of the cloud. This model is based on the fact that one of the main challenges of cloud computing is to ensure that the application which are running on the cloud without a hiatus in the service they provided to the user. This middleware replicates application by the using of semi-active replication or semi-passive replication process to protect the application against various types of faults.

“FTWS” is a proposed model which contains a fault tolerant work flow scheduling algorithm for providing fault tolerance by using replication and resubmission of tasks based on the priority of the tasks in a heuristic metric. This model is based on the fact that work flow is a set of tasks processed in some order based on data and control dependency. Scheduling the workflow included with the task failure consideration in a cloud environment is very challenging. FTWS replicates and schedule the tasks to meet the deadline.

“FTM” is a proposed model to overcome the limitation of existing methodologies of the on-demand service. To achieve the reliability and resilience they propose an innovative perspective on creating and managing fault tolerance .By this particular methodology user can specify and apply the desire level of fault tolerance without requiring any knowledge about its implementation. FTM architecture this can primarily be viewed as an assemblage of several web services components, each with a specific functionality.

”Candy” is a component base availability modeling frame work, which constructs a comprehensive availability model semi automatically from system specification describe by systems modeling language. This model is based on the fact that high availability assurance of cloud service is one of the main characteristic of cloud service and also one of the main critical and challenging issues for cloud service provider.

“Vega-warden” is a uniform user management system which supplies a global user space for different virtual infrastructure and application services in cloud computing environment. This model is constructed for virtual cluster base cloud computing environment to overcome the 2 problems: usability and security arise from sharing of infrastructure.

"FT-Cloud" is a component ranking based frame work and its architecture for building cloud application. FT-Cloud employs the component invocation structure and frequency for identify the component. There is an algorithm to automatically determine fault tolerance stately.

"Magi-Cube" a high reliable and low redundancy storage architecture for cloud computing. The build the system on the top of HDFS and use it as a storage system for file read /write and metadata management. They also built a file scripting and repair component to work in the back ground independently. This model based on the fact that high reliability and performance and low cost (space) are the 3 conflicting component of storage system. To provide these facilities to a particular model Magi cube is proposed.

Model no	**Model name**	**Protection against Type of fault**	**Applied procedure for tolerate the fault**
M1	AFTRC	Reliability	1.Delete node depending on their reliability 2.Back word recovery with the help of check pointing
M2	LLFT	Crash-cost, trimming fault	Replication.
M3	FTWS	Dead line of work flow	Replication and resubmission of jobs
M4	FTM	Reliability, availability, on demand service	Replication users application and in the case of replica failure use algorithm like gossip based protocol.
M5	CANDY	Availability	1. It assembles the model components generated from IBD and STM according to allocation notation. 2. Then activity SNR is synchronized to system SRN by identifying the relationship between action in activity SNR and state transition in system SRN.
M6	VEGA-WARDEN	Usability, security, scaling	1. Two layer authentication and standard technical solution for the application.
M7	FT-CLOUD	Reliability, crash and value fault	1. Significant component is determined based on the ranking. 2. Optimal ft technique is determined.
M8	MAGI-CUBE	Performanc e, reliability, low storage cost	1. Source file is encoded in then splits to save as a cluster. 2. File recovery procedure is triggered is the original file is lost.

Table: 3.1 Comparison among various models based on protection against the type of fault, and procedure

Resiliency

Resilient computing is a form of failover that distributes redundant implementations of IT resources across physical locations. IT resources can be pre-configured so that if one becomes deficient, processing is automatically handed over to another redundant implementation. Within cloud computing, the characteristic of resiliency can refer to redundant IT resources within the same cloud (but in different physical locations) or across multiple clouds. Cloud consumers can increase both the reliability and availability of their applications by leveraging the resiliency of cloud-based IT resources.

- Resiliency is the capacity to rapidly adapt and respond to risks, as well as opportunities.
- This maintains continuous business operations that support growth and operate in potential adverse conditions.
- The reach and range step of the assessment process examines business driven, data-driven and event -driven risks.
- The resiliency blueprint includes different layers- facilities, technology, applications and data, processes
- The framework enables people to examine business, understand what areas of vulnerabilities that might exist and quickly pinpoint areas of concern and help them understand what actions they can take to reduce the risk associated with those areas.

The framework combines multiple parts to mitigate risks and improve business resilience

- From a facilities perspective, you may need to implement power protection
- from security perspective- to protect applications and data
- From process perspective- you may implement identification and documentation of most critical business process
- From organizational perspective- geographical diversity, backup of workstation data
- From strategy and vision perspective, you would want to have a crisis management

Provisioning

Cloud provisioning is the allocation of a cloud provider's resources to a customer.

When a cloud provider accepts a request from a customer, it must create the appropriate number of virtual machines (VMs) and allocate resources to support them. The process is conducted in several different ways: advance provisioning, dynamic provisioning and user self-provisioning. In this context, the term provisioning simply means “to provide."

With advance provisioning, the customer contracts with the provider for services and the provider prepares the appropriate resources in advance of start of service. The customer is

charged a flat fee or is billed on a monthly basis.

With dynamic provisioning, the provider allocates more resources as they are needed and removes them when they are not. The customer is billed on a pay-per-use basis. When dynamic provisioning is used to create a hybrid cloud, it is sometimes referred to as cloud bursting.

With user self-provisioning (also known as cloud self-service), the customer purchases resources from the cloud provider through a web form, creating a customer account and paying for resources with a credit card. The provider's resources are available for customer use within hours, if not minutes.

Provisioning process is a service that uses group of compliant processes called “solution Realization”

- Provisioned products are servers built with all the software and infrastructure required to support a business application.
- Standard solutions are defined so that standard workflows can be derived
- Server hardware is assembled, cabled and connected to the network and SAN before work orders are released.

Asset management

Cloud computing offers the potential to transform asset managers’ technology ecosystem. However, CIOs will need to consider a number of criteria to determine whether cloud solutions fit into their future plans and strategies.

Asset managers have traditionally developed custom technology or implemented a vendor solution. This decision was primarily influenced by the importance of the business function, the ability of the internal technology team to support it and the availability of mature products in the space.

Recently, however, the advent of cloud computing has added a completely new dimension to this decision-making process. It has opened up avenues to host custom-developed applications on third-party-managed platforms and created opportunities to use software as a service (SaaS).

According to a recent Confluence survey, over a four-year period, cloud solutions could lower the total cost of ownership by 55 percent. Numbers like these are making CIOs around the world take notice and realize that cloud computing provides an opportunity to shift to an entirely new technology operating model. With this shift, IT can move from managing applications on an internal infrastructure to managing the integration of different cloud services, platforms and cloud-based solutions. And while the potential benefits are clear, firms must conduct proper due diligence and understand the impact before making the move.

Asset management and change management interact regularly. The asset management strategy includes

- Software packaging
- Incident management
- Pool Management
- Release management
- configuration management
- Systems management
- Operational readiness Management
- Backup management

Concept of Map Reduce

The MapReduce framework has two parts:

1. A function called "Map," which allows different points of the distributed cluster to distribute their work
2. A function called "Reduce," which is designed to reduce the final form of the clusters' results into one output

The main advantage of the MapReduce framework is its fault tolerance, where periodic reports from each node in the cluster are expected when work is completed.

A task is transferred from one node to another. If the master node notices that a node has been silent for a longer interval than expected, the main node performs the reassignment process to the frozen/delayed task.

The MapReduce framework is inspired by the "Map" and "Reduce" functions used in functional programming. Computational processing occurs on data stored in a file system or within a database, which takes a set of input key values and produces a set of output key values.

Each day, numerous MapReduce programs and MapReduce jobs are executed on Google's clusters. Programs are automatically parallelized and executed on a large cluster of commodity machines. The runtime system deals with partitioning the input data, scheduling the program's execution across a set of machines, machine failure handling and managing required inter machine communication. Programmers without any experience with parallel and distributed systems can easily use the resources of a large distributed system.

MapReduce is used in distributed grep, distributed sort, Web link-graph reversal, Web access log stats, document clustering, machine learning and statistical machine translation.

Cloud Governance

This is a brief summary of some Cloud Computing governance issues:

Technical Issues

Determine how the Cloud Provider::

- Supports change management
- Provides for high-availability
- Provides for redundancy and failover (if any)
- Provides for security related to the Internet
- Provides for physical security

Legal Issues

It is important to determine what needs to be in a contract with your Cloud provider. Things to consider:

- Service standards to be maintained
- Retention of rights to your data
- Legal jurisdiction where the data center is located
- Privacy laws where the data center is located
- Liability of data breaches
- Policies and procedures related to providing digital forensics data in the event of any legal dispute, cyber attack, or data breach.
- Notification of changes when they occur at the data center
- Disaster recovery
- Remedies for various possible problems
- Details for what occurs at the beginning and end of the contract period

Business Issues

Your business relationship with a Cloud provider should involve:

- The Cloud provider's reputation
- Financial stability of the Cloud provider
- The length of time the Cloud provider has been in business
- Management practices for the data center

Cloud Backup

Get maneuverability by replacing expensive backup equipment and complicated media outsourcing by cheap backup in the cloud. With our **Cloud Backup Service**, we provide cheap and reliable backup storage of AWS in your data center or corporate network. You can continue to use your existing Enterprise Backup Software. We take care of all the technology and

guarantee the performance and security of cloud backups. While your data remains in Germany. The best: We adapt the cloud backup as your needs grow over time.

This complete Cloud Backup Service consists of part services that you can make use of individually:

- **Consultation and Implementation:** Determination of performance and quantity requirement based on Recovery Point Objectives (RPOs), recovery-time objectives (RTOs) and configuring and tuning Enterprise Backup Software of leading manufacturers for the utilization of backup targets in the Cloud.
- **Gateway Realization and Operation:** Installation of backup gateways from leading vendors including NetApp Steel gates, Ctera, Veeam and AWS Storage Gateway with corresponding encryption and redundancy configurations. Operation of the gateways includes maintenance, updates and troubleshooting.
- **Automation of the Backup Lifecycle Management:** Cloud Backup is usually done on backup gateways in the data center. From there the backups are automatically replicated on durable cloud storage by AWS. Prior to transfer data is de-duplicated, compressed and encrypted with user-defined keys. This ensures that, just in case, foreign intelligence services only get to see encrypted data. Lifecycle policies control how long backup data is stored in the data center, for fast recovery. Policies also regulate when backups are moved from durable cloud storage to an even more favorable long-term archive in the cloud and when backups are deleted, for example, at the end of the retention period.

Cloud Disaster Recovery

Get maneuverability by shifting the provision of expensive recovery infrastructure to the cloud. We provide proven recovery scenarios of your applications to secure Virtual Private Clouds (VPCs) with our **Cloud Recovery Service** in all available AWS regions worldwide. Your regular cloud backups guarantee the most current data state. We take care of the adjustments of the complete scenario, guarantee recovery point objectives (RPOs) and recovery time objectives (RTOs), and the safety and ease of use of the Cloud Recovery environment. The best: We adapt the Cloud Recovery if your application environments or your disaster recovery requirements change over time. This complete Cloud Recovery Service consists of part services that you can make use of individually:

- **Cloud Recovery Consultation and Implementation:** Analysis of Cloud Recovery scenarios, determining the resource and performance requirements, design and implementation of recovery scripts.
- **Automated Application Tests:** Regular automated checking the serviceability of the Cloud Recovery scenarios.

The Cloud Recovery Services - whether booked individually or as a whole - can be used for example for:

- 2-stage Cloud Recovery for all application environments of your company: while the restore takes place into the data center, quickly restore to a temporary cloud environment.
- Forks of the production environment for testing, simulations, expert opinions or reproduction of transactions outside the production environment.
- Recovery environments for critical communications infrastructure such as email, important documents (SharePoint, file servers), chat and video / audio conferencing for board and Communications Department, to other regions and continents, if necessary.

Virtualization Technology

Virtualization is the process of converting a physical IT resource into a virtual IT resource. Most types of IT resources can be virtualized, including:

- **Servers** - A physical server can be abstracted into a virtual server.
- **Storage** - A physical storage device can be abstracted into a virtual storage device or a virtual disk.
- **Network** - Physical routers and switches can be abstracted into logical network fabrics, such as VLANs.

- **Power** - A physical UPS and power distribution units can be abstracted into what are commonly referred to as virtual UPSs.

This section focuses on the creation and deployment of virtual servers through server virtualization technology.

The terms virtual server and virtual machine (VM) are used synonymously throughout this book. The first step in creating a new virtual server through virtualization software is the allocation of physical IT resources, followed by the installation of an operating system. Virtual servers use their own guest operating systems, which are independent of the operating system in which they were created.

Both the guest operating system and the application software running on the virtual server are unaware of the virtualization process, meaning these virtualized IT resources are installed and executed as if they were running on a separate physical server. This uniformity of execution that allows programs to run on physical systems as they would on virtual systems is a vital characteristic of virtualization. Guest operating systems typically require seamless usage of software products and applications that do not need to be customized, configured, or patched in order to run in a virtualized environment.

Virtualization software runs on a physical server called a host or physical host, whose underlying

hardware is made accessible by the virtualization software. The virtualization software functionality encompasses system services that are specifically related to virtual machine management and not normally found on standard operating systems. This is why this software is sometimes referred to as a virtual machine manager or a virtual machine monitor (VMM), but most commonly known as a hypervisor.

This section covers the following topics:

- Hardware Independence
- Server Consolidation
- Resource Replication
- Hardware-based and Operating System-based Virtualization
- Virtualization Operation and Management
- Technical and Business Considerations

Hardware Independence

The installation of an operating system's configuration and application software in a unique IT hardware platform results in many software-hardware dependencies. In a non-virtualized environment, the operating system is configured for specific hardware models and requires reconfiguration if these IT resources need to be modified.

Virtualization is a conversion process that translates unique IT hardware into emulated and standardized software-based copies. Through hardware independence, virtual servers can easily be moved to another virtualization host, automatically resolving multiple hardware-software incompatibility issues. As a result, cloning and manipulating virtual IT resources is much easier than duplicating physical hardware. The architectural models explored in Part III of this book provide numerous examples of this.

Server Consolidation

The coordination function that is provided by the virtualization software allows multiple virtual servers to be simultaneously created in the same virtualization host. Virtualization technology enables different virtual servers to share one physical server. This process is called server consolidation and is commonly used to increase hardware utilization, load balancing, and optimization of available IT resources. The resulting flexibility is such that different virtual servers can run different guest operating systems on the same host.

These features directly support common cloud computing features, such as on-demand usage, resource pooling, elasticity, scalability, and resiliency.

Resource Replication

Virtual servers are created as virtual disk images that contain binary ?le copies of hard disk content. These virtual disk images are accessible to the host's operating system, meaning simple file operations, such as copy, move, and paste, can be used to replicate, migrate, and back up the virtual server. This ease of manipulation and replication is one of the most salient features of virtualization technology as it enables:

- The creation of standardized virtual machine images commonly configured to include virtual hardware capabilities, guest operating systems, and additional application software, for pre-packaging in virtual disk images in support of instantaneous deployment.

- Increased agility in the migration and deployment of a virtual machine's new instances by being able to rapidly scale out and up.

- The ability to roll back, which is the instantaneous creation of VM snapshots by saving the state of the virtual server's memory and hard disk image to a host-based file. (Operators can easily revert to these snapshots and restore the virtual machine to its prior state.)

- The support of business continuity with efficient backup and restoration procedures, as well as the creation of multiple instances of critical IT resources and applications.

Operating System-Based Virtualization

Operating system-based virtualization is the installation of virtualization software in a pre-existing operating system, which is called the host operating system. For example, a user whose workstation has a specific version of Windows installed decides it wants to generate virtual machines. It installs the virtualization software into its host operating system like any other program and uses this application to generate and operate one or more virtual machine. This user needs to use its virtualization software to enable direct access to any of the generated virtual machines. Since the host operating system can provide hardware devices with the necessary support, operating system virtualization can rectify hardware compatibility issues even if the hardware driver is unavailable to the virtualization software.

Hardware independence that is enabled by virtualization allows hardware IT resources to be more flexibly used. For example, let's take a scenario in which the host operating system has the software necessary for controlling five network adapters that are available to the physical computer. The virtualization software can make the five network adapters available to the virtual machine, even if the virtualized operating system is usually incapable of physically housing five network adapters.

Virtualization software translates hardware IT resources that require unique software for operation into virtualized IT resources that are compatible with a range of operating systems. Since the host operating system is a complete operating system in itself, many operating system-based services that are available as organizational management and administration tools can be used to manage the virtualization host.

Examples of such services include:

- Backup and Recovery
- Integration to Directory Services
- Security Management

Operating system-based virtualization can introduce demands and issues related to performance overhead, such as:

- The host operating system consumes CPU, memory, and other hardware IT resources.
- Hardware-related calls from guest operating systems need to traverse several layers to and from the hardware, which decreases overall performance.
- Licenses are usually required for host operating systems, in addition to individual licenses for each of their guest operating systems.

A concern with operating system-based virtualization is the processing overhead required to run the virtualization software and host operating systems. Implementing a virtualization layer will negatively affect overall system performance. Estimating, monitoring, and managing the resulting impact can be challenging because it requires expertise in system workloads, software and hardware environments, and sophisticated monitoring tools.

VMware Virtualization

Server Virtualization

The architecture of today's x86 servers allows them to run only one operating system at a time. Server virtualization unlocks the traditional one-to-one architecture of x86 servers by abstracting the operating system and applications from the physical hardware, enabling a more cost-efficient, agile and simplified server environment. Using server virtualization, multiple operating systems can run on a single physical server as virtual machines, each with access to the underlying server's computing resources.

Server virtualization unleashes the potential of today's powerful x86 servers. Most servers operate less than 15 percent of capacity; not only is this highly inefficient, it also introduces server sprawl and complexity.

VMware vSphere offers a complete server virtualization platform that delivers:

- 80 percent greater utilization of server resources
- Up to 50 percent savings in capital and operating costs
- 10:1 or better server consolidation ratio

Network Virtualization

Network virtualization is the complete reproduction of a physical network in software. Virtual

networks offer the same features and guarantees of a physical network, yet they deliver the operational benefits and hardware independence of virtualization—rapid provisioning, no disruptive deployment, automated maintenance and support for both legacy and new applications.

Network virtualization presents logical networking devices and services—logical ports, switches, routers, firewalls, load balancers, VPNs and more—to connected workloads. Applications run on the virtual network exactly the same as if on a physical network.

You can create a highly scalable network fabric that provides greater levels operational efficiency and agility, faster provisioning, troubleshooting and cloning, with monitoring, QoS, and security all backed by VMware network virtualization software.

VMware NSX™ will be the world's leading network and security virtualization platform providing a full-service, programmatic and mobile virtual network for virtual machines, deployed on top of any general purpose IP network hardware.

The VMware NSX platform brings together the best of Nicira NVP and VMware vCloud® Networking and Security™ (vCNS) into one unified platform. VMware NSX exposes a complete suite of simplified logical networking elements and services including logical switches, routers, firewalls, load balancers, VPN, QoS, monitoring and security.

Desktop Virtualization

Deploying desktops as a managed service gives you the opportunity to respond quicker to changing needs and opportunities. You can reduce costs and increase service by quickly and easily delivering virtualized desktops and applications to branch offices, outsourced and offshore employees and mobile workers on iPad and Android tablets.

VMware desktop solutions are scalable, consistent, fully secure and highly available to ensure maximum uptime and productivity.

- Streamline deployment and management by delivering desktops as a service.
- Provide secure remote access to teleworkers and temporary workers without sacrificing performance.

Application Virtualization

Organizations are increasingly virtualizing more of their Tier 1 mission-critical business applications and platforms, such as databases, ERP, CRM, email, collaboration, Java middleware, business intelligence and many others.

In order to maintain the required levels of QoS and SLA for these Tier 1 business applications in virtual environments, IT organizations must focus equally on the virtualization components of the project and on the robust management and monitoring of virtualized business applications, as well as on maintaining corporate guidelines for business continuity and disaster recovery.

These virtualized applications simply run better and provide high availability, disaster recovery, speed and agility as well as cloud-readiness. With the VMware Tier 1 Application Virtualization solution built on VMware vCloud® Suite™, you can enhance the quality of IT services delivered, while simplifying your infrastructure, maximizing efficiency and eliminating costly over-provisioning.

Storage Virtualization

Storage virtualization is part of the software-defined storage layer that must offer improvements in performance and space efficiency without requiring the purchase of additional storage hardware.

It must enable rapid provisioning so that high-performance, space-efficient storage can be spun up as fast as a VM can be spun up today. It must offer a VM-centric storage management model that is intuitive for virtual administrators who are taking on more of the storage management tasks in virtual environments. And it must integrate with the hypervisor platform to leverage familiar, native workflows.

VMware storage virtualization is a combination of capabilities that provide an abstraction layer for physical storage resources to be addressed, managed and optimized in a virtualization deployment.

Storage virtualization technology provides a fundamentally better way to manage storage resources for your virtual infrastructure, giving your organization the ability to:

- Significantly improve storage resource utilization and flexibility
- Simplify OS patching and driver requirements, regardless of storage topology
- Increase application uptime and simplify day-to-day operations
- Leverage and complement your existing storage infrastructure

Block level storage

Anyone who has used a Storage Area Network (SAN) has probably used block level storage before. Block level storage presents itself to servers using industry standard Fibre Channel and iSCSI connectivity mechanisms. In its most basic form, think of block level storage as a hard drive in a server except the hard drive happens to be installed in a remote chassis and is accessible using Fibre Channel or iSCSI.

When it comes to flexibility and versatility, you can't beat block level storage. In a block level storage device, raw storage volumes are created, and then the server-based operating system connects to these volumes and uses them as individual hard drives. This makes block level storage usable for almost any kind of application, including file storage, database storage, virtual machine file system (VMFS) volumes, and more. You can place any kind of file system on block level storage. So, if you're running Windows, your volumes will be formatted with NTFS; VMware servers will use VMFS.

File level storage devices are often used to share files with users. By creating a block-based volume and then installing an operating system and attaching to that volume, you can share files out using that native operating system. Remember, when you use a block-based volume, you're basically using a blank hard drive with which you can do anything.

When it comes to backup, many storage devices include replication-type capabilities, but you still need to think about how to protect your workloads. With this type of storage, it's not unusual for an organization to be able to use operating system native backup tools or third-party backup tools such as Data Protection Manager (DPM) to back up files. Since the storage looks and acts like a normal hard drive, special backup steps don't need to be taken.

With regard to management complexity, block-based storage devices tend to be more complex than their file-based counterparts; this is the tradeoff you get for the added flexibility. Block storage device administrators must:

- Carefully manage and dole out storage on a per server basis.
- Manage storage protection levels (i.e., RAID).
- Track storage device performance to ensure that performance continues to meet server and application needs.
- Manage and monitor the storage communications infrastructure (generally iSCSI or Fibre Channel).

From a use case standpoint, there are a lot of applications that make use of this block-level shared storage, including:

- Databases. This is especially true when you want to cluster databases, since clustered databases need shared storage.
- Exchange. Although Microsoft has made massive improvements to Exchange, the company still does not support file level or network-based (as in, CIFS or NFS) storage. Only block level storage is supported.
- VMware. Although VMware can use file level storage via Network File System (NFS), it's very common to deploy VMware servers that use shared VMFS volumes on block level storage.
- Server boot. With the right kind of storage device, servers can be configured to boot from block level storage.

File level storage

Although block level storage is extremely flexible, nothing beats the simplicity of file level storage when all that's needed is a place to dump raw files. After all, simply having a centralized, highly available, and accessible place to store files and folders remains the most critical need in many organizations. These file level devices -- usually Network Attached Storage (NAS) devices provide a lot of space at what is generally a lower cost than block level storage.

File level storage is usually accessible using common file level protocols such as SMB/CIFS (Windows) and NFS (Linux, VMware). In the block level world, you need to create a volume, deploy an OS, and then attach to the created volume; in the file level world, the storage device handles the files and folders on the device. This also means that, in many cases, the file level storage device or NAS needs to handle user access control and permissions assignment. Some devices will integrate into existing authentication and security systems.

On the backup front, file level storage devices sometimes require special handling since they might run non-standard operating systems, so keep that in mind if you decide to go the file level route.

With the caveat that you may need to take some steps with regard to authentication, permissions, and backup, file level-only devices are usually easier to set up than block level devices. In many cases, the process can be as simple as walking through a short configuration tool and moving forward.

If you're looking for storage that screams -- that is, if you need high levels of storage performance -- be very careful with the file level option. In most cases, if you need high levels of performance, you should look at the block level options. Block level devices are generally configurable for capacity and performance. Although file-level devices do have a performance component, capacity is usually the bigger consideration.

File level use cases are generally:

- Mass file storage. When your users simply need a place to store files, file-level devices can make a lot of sense.

- VMware (think NFS). VMware hosts can connect to storage presented via NFS in addition to using block level storage.

The block and file worlds are converging. Some new storage devices include both block and file level capabilities. So if you are torn about whether to go with block or file, a hybrid/converged device might fit your needs.

Hypervisor Virtualization Software

A hypervisor, also known as a virtual machine manager/monitor (VMM), is computer hardware platform virtualization software that allows several operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and resources to it. Instead, the hypervisor is controlling the host processor and resources, distributing what is needed to each operating system in turn and ensuring that the guest operating systems/virtual machines are unable to disrupt each other.

The term 'hypervisor' originated in IBM's CP-370 reimplementation of CP-67 for the System/370, released in 1972 as VM/370. The term 'hypervisor call' refers to the paravirtualization interface, by which a guest operating system accesses services directly from the higher-level control program. This is the same concept as making a supervisor call to the same level operating system.

Hypervisor Classifications

Hypervisors are classified into two types:

- **Bare Metal/Native Hypervisors**

Software systems that run directly on the host's software as a hardware control and guest operating system monitor. A guest operating system thus runs on another level above the hypervisor. This is the classic implementation of virtual machine architectures.

A variation of this is embedding the hypervisor in the firmware of the platform, as is done in the case of Hitachi's Virtage hypervisor and VMware ESXi. See below definition.

- **Embedded/Host Hypervisors**

Software applications that run within a conventional operating system environment. Considering the hypervisor layer being a distinct software layer, guest operating systems thus run at the third level above the hardware.

Comparison between VLAN and VSAN

S.No.	VLAN(Virtual Local Area Network)	VSAN(Virtual Storage Area Network)
1	VLAN is a network technology used to logically separate large broadcast domains using layer 2 devices.	VSAN is a logical partition in a storage area network.
2	It divides the network into different virtual sub-networks reduces unnecessary traffic and improve performance.	VSANs allow traffic to be isolated within specific portions of a storage area network.
3	VLANs are implemented to achieve scalability, security and ease of network management.	The use of multiple VSAN's can make a system easier to configure and scale out.
4	VLAN's can quickly adapt to change in network requirements and relocation of workstations and server nodes.	In this subscribers can be added or relocated without the need for changing the physical layout.
5	The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security features.	The VSANs minimizes the total system's vulnerability, security is improved. VSANs also offer the possibility of data redundancy, minimizing the risk of catastrophic data loss.

Table: 3.2 Comparison between VLAN & SAN

Web Resources:

https://hortonworks.com/

https://www.itgovernance.co.uk/cloud-governance

http://www.cloudcomputingpatterns.org/map_reduce/

http://searchstorage.techtarget.com/definition/virtual-storage-area-network

http://www.netmagicsolutions.com/disaster-recovery-on-cloud

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in