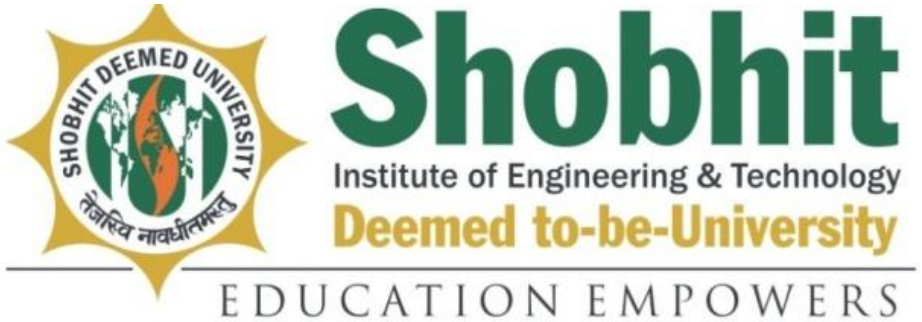
CLOUD COMPUTING

Unit-5

Cloud Issues and Challenges



AVINAV PATHAK
Assistant Professor
Shobhit Institute of Engineering & Technology
(Deemed-to-be-University), Meerut, India

Cloud Provider Lockin

What does 'vendor lock-in' mean?

- ***Vendor lock-in refers to a situation where the cost of switching to a different vendor is so high that the customer is essentially stuck with the original vendor. Because of financial pressures, an insufficient workforce, or the need to avoid interruptions to business operations, the customer is "locked in" to what may be an inferior product or service.***
- ***Imagine an office has coffee brought in by a coffee vendor, and this vendor requires specific coffee machines in the office that only the vendor sells. Now imagine there's a steep decline in the quality of the coffee that this vendor delivers. Switching to a new coffee vendor would mean the old machines they purchased become useless, as the switch likely requires the purchase of new coffee-making equipment. Given the hassle and added expense of replacing every coffee machine, the workers in the office would be effectively locked into their agreement with their old vendor and forced to drink inferior coffee.***
- ***A real-world example of vendor lock-in is the way Apple locked consumers into using iTunes in the early days of the service, because music purchased via iTunes could only be played within the iTunes application or on an iPod.***
- ***What is vendor lock-in in cloud computing?***

Cloud Provider Lockin

In cloud computing, some amount of software or computing infrastructure is outsourced to a cloud vendor, who offers it as a service and delivers it over the Internet. For instance, cloud-hosted servers are Infrastructure-as-a-Service (IaaS), and cloud-hosted applications are Software-as-a-Service (SaaS).

Sometimes, a company may find themselves locked into a certain cloud provider. Vendor lock-in can become an issue in cloud computing because it is very difficult to move databases once they're set up, especially in a cloud migration, which involves moving data to a totally different type of environment and may involve reformatting the data. Also, once a third party's software is incorporated into a business's processes, the business may become dependent upon that software.

Why is vendor lock-in a concern?
A number of circumstances can negatively impact a business if they're locked in with a certain cloud vendor:

If a vendor's quality of service declines, or never meets a desired threshold to begin with, the client will be stuck with it
The vendor may also drastically change their product offerings in such a way that they no longer meet a business's needs
A vendor may go out of business altogether
Finally, a vendor may impose massive price increases for the service, knowing that their clients are locked in
Overall, handing off foundational, business-critical technology to an external vendor is not easy for any company, and it requires a large degree of trust in the vendor.

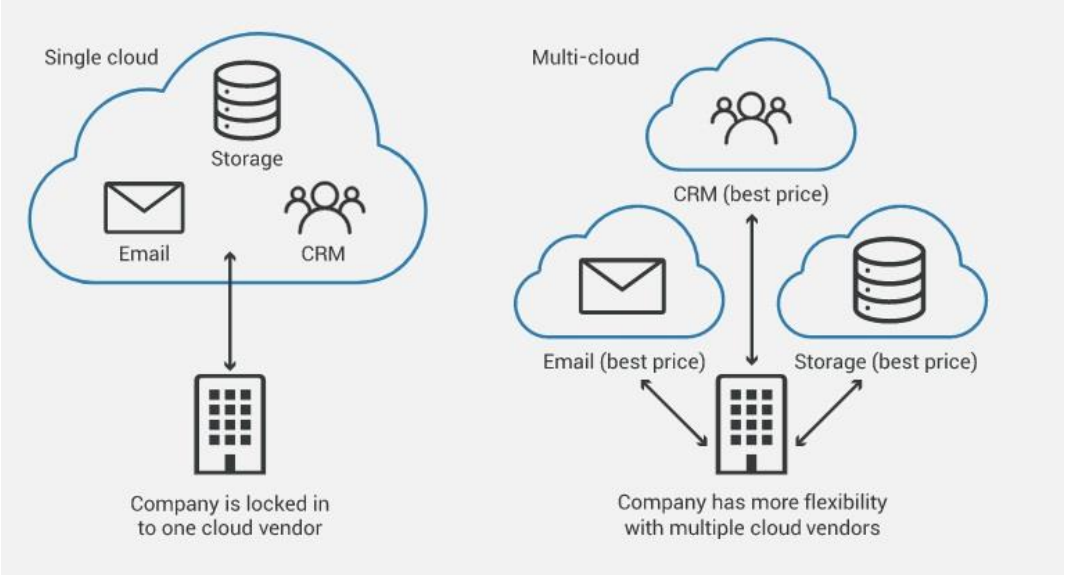
Cloud Provider Lockin

How does Cloudflare help mitigate vendor lock-in?

Operating in the cloud is a must for most modern businesses. Cloudflare helps prevent businesses from becoming too dependent on any one cloud provider.

Cloudflare is infrastructure-agnostic – the Cloudflare product stack can be deployed in front of any type of infrastructure, with any cloud provider or combination of providers (including multicloud and hybrid cloud deployments).

With Cloudflare deployed, a company is not dependent upon cloud infrastructure providers for performance, reliability, and security services, and they can move easily between cloud providers while still offering fast, reliable service to customers.



Security and Privacy Issues in Cloud Computing

The nature of the risks of course, varies in different scenarios, depending among other things, on what type of cloud is being employed. These concerns are serious enough, for example, that public clouds are generally not used at all for sensitive information.

Privacy issues in cloud computing includes:

- ***Data protection: Data security plays an important role in cloud computing environment where encryption technology is the best option whether data at rest or transmitted over the internet. Hard drive producers are supplying self-encrypting drives that provide automated encryption, even if you can use encryption software to protect your data. If we talk about security of transmitted data, then SSL encryption is the best option to secure your online communications as well provides authentication to your website and/or business that assures the data integrity and the users' information is not altered during transmissions.***

- ***User control: This can be both a legal issue and one raised by consumers themselves. SaaS environment offers the control of consumers' data to the service provider so; data visibility and control will be limited. In that case, there is a threat of data stolen, misused or theft, as consumers have no control over cloud. Even data transparency is missing for example, where the data is, who owns it, and how it is being used. However, data exposure can also be possible during data transferring as many countries have implemented the law of accessing data if they found it distrusting.***

Security and Privacy Issues in Cloud Computing

- ***Employee training and knowledge: A full understanding of when cloud services should and be used needs to be a part of basic employee training in many jobs that involve managing information. Due to lack of training people may not understand the impact of decisions related privacy they generally made.***

- ***Unauthorized usage: This can includes usage of data ranging from targeted advertising, to the re-sale of data on the cloud. The service provider may gain income from secondary usage of data. Agreements between clients and providers must be specific about unauthorized usage as it will enhance the trust and lessen the security worries.***

- ***Loss of legal protection: Putting data on the cloud can involve a loss of legal protection of privacy. It can be impossible to follow all the legislation for a cloud computing for example, with Canada's privacy act or health laws. Other policies such as the U.S Patriot Act as mentioned above, can actually force exposure of data to third parties. Different locations have many different laws to protect (or in some cases infringe on) the privacy of these users. Data in the cloud is, at best, extremely unclear in terms of locality. At worst, the nature of this ambiguous and instantaneous data flow across borders can make privacy laws impossible to enforce.***

VMWARE, ESX
Memory Management

VMWare

VMware is a virtualization and cloud computing software provider based in Palo Alto, Calif. Founded in 1998, VMware is a subsidiary of Dell Technologies. EMC Corporation originally acquired VMware in 2004; EMC was later acquired by Dell Technologies in 2016. VMware bases its virtualization technologies on its bare-metal hypervisor ESX/ESXi in x86 architecture.

With VMware server virtualization, a hypervisor is installed on the physical server to allow for multiple virtual machines (VMs) to run on the same physical server. Each VM can run its own operating system (OS), which means multiple OSs can run on one physical server. All the VMs on the same physical server share resources, such as networking and RAM. In 2019, VMware added support to its hypervisor to run containerized workloads in a Kubernetes cluster in a similar way. These types of workloads can be managed by the infrastructure team in the same way as virtual machines and the DevOps teams can deploy containers as they were used to.

Diane Greene, Scott Devine, Mendel Rosenblum, Edward Wang and Edouard Bugnion founded VMware, which launched its first product -- VMware Workstation -- in 1999. The company released its second product, VMware ESX in 2001.

VMware's current CEO is Patrick Gelsinger, appointed in 2012.

Vmware Products

VMware products

VMware products include virtualization, networking and security management tools, software-defined data center software and storage software.

Data center and cloud infrastructure

VMware vSphere is VMware's suite of virtualization products. VMware vSphere, known as VMware Infrastructure prior to 2009, includes the following:

ESXi

vCenter Server

vSphere Client

vMotion

As of April 2018, the most current version is vSphere 6.7, which is available in three editions: Standard, Enterprise Plus and Platinum. There are also two three-server kits targeted toward small and medium-sized businesses named vSphere Essentials and Essentials Plus.

Vmware Features

Networking and security

VMware NSX is a virtual networking and security software offering created when VMware acquired Nicera in 2012. NSX allows an admin to virtualize network components, enabling them to develop, deploy and configure virtual networks and switches through software rather than hardware. A software layer sits on top of the hypervisor to allow an administrator to divide a physical network into multiple virtual networks.

With the latest release of the product, NSX-T Data Center, network virtualization can be added to both ESXi and KVM as hypervisors, as well as to bare-metal servers. Also containerized workloads in a Kubernetes cluster can be virtualized and protected. NSX-T Data Center also offers Network Function Virtualization, with which functions such as a firewall, load balancer and VPN, can be run in the virtualization software stack.

Vmware Features

VMware vRealize Network Insight is a network operations management tool that enables an admin to plan microsegmentation and check on the health of VMware NSX. VRealize Network Insight relies on technology from VMware's acquisition of Arkin in 2016. VRealize Network Insight collects information from the NSX Manager. It also displays errors in its user interface, which helps troubleshoot an NSX environment.

SDDC platform

VMware Cloud Foundation is an integrated software stack that bundles vSphere, VMware vSAN and VMware NSX into a single platform through the SDDC Manager. An admin can deploy the bundle on premises as a private cloud or run it as a service within a public cloud. An administrator can provision an application immediately without having to wait for network or storage.

Storage and availability

VMware vSAN is a software-based storage feature that is built into the ESXi hypervisor and integrated with vSphere; it pools disk space from multiple ESXi hosts and provisions it via smart policies, such as protection limits, thin provisioning and erasure coding. It integrates with vSphere High Availability to offer increased compute and storage availability.

Vmware Features

VMware Site Recovery Manager (SRM) is a disaster recovery management product that allows an administrator to create recovery plans that are automatically executed in case of a failure. Site Recovery Manager allows admins to automatically orchestrate the failover and failback of VMs. SRM also integrates with NSX to preserve network and security policies on migrated VMs.

VMware vCloud NFV is a network functions virtualization platform that enables a service provider to run network functions as virtualized applications from different vendors. NFV provides the same benefits of virtualization and cloud to a communications service provider that previously relied on hardware.

Cloud management platform
The vRealize Suite is a group of software that allows a user to create and manage hybrid clouds. The vRealize Suite includes vRealize Operations for monitoring, vRealize Log Insight for centralized logging, vRealize Automation for data center automation and vRealize Business for Cloud for cost management.

Vmware Features

With this bundle, an administrator can deploy and manage VMs on multiple hypervisors or cloud platforms from a single management console. Released in 2019, VMware Tanzu allows customers to build containerized apps, run enterprise Kubernetes and manage Kubernetes for developers and IT.

Virtual desktop infrastructure
VMware Horizon allows organizations to run Windows desktops in the data center or in VMware Cloud on AWS. This removes the need to place and manage full desktops on the workplace and centralizes management and security for the user's environment.

Memory Management

Cloud Storage is a service that allows to save data on offsite storage system managed by third-party and is made accessible by a web services API.

Storage Devices

Storage devices can be broadly classified into two categories:

1. ***Block Storage Devices***
2. ***File Storage Devices***

Block Storage Devices

The block storage devices offer raw storage to the clients. These raw storage are partitioned to create volumes.

File Storage Devices

The file Storage Devices offer storage to clients in the form of files, maintaining its own file system. This storage is in the form of Network Attached Storage (NAS).

Cloud Storage Classes

Cloud storage can be broadly classified into two categories:

- ***Unmanaged Cloud Storage***
- ***Managed Cloud Storage***

Memory Management

Unmanaged Cloud Storage

Unmanaged cloud storage means the storage is preconfigured for the customer. The customer can neither format, nor install his own file system or change drive properties.

Managed Cloud Storage

Managed cloud storage offers online storage space on-demand. The managed cloud storage system appears to the user to be a raw disk that the user can partition and format.

Creating Cloud Storage System

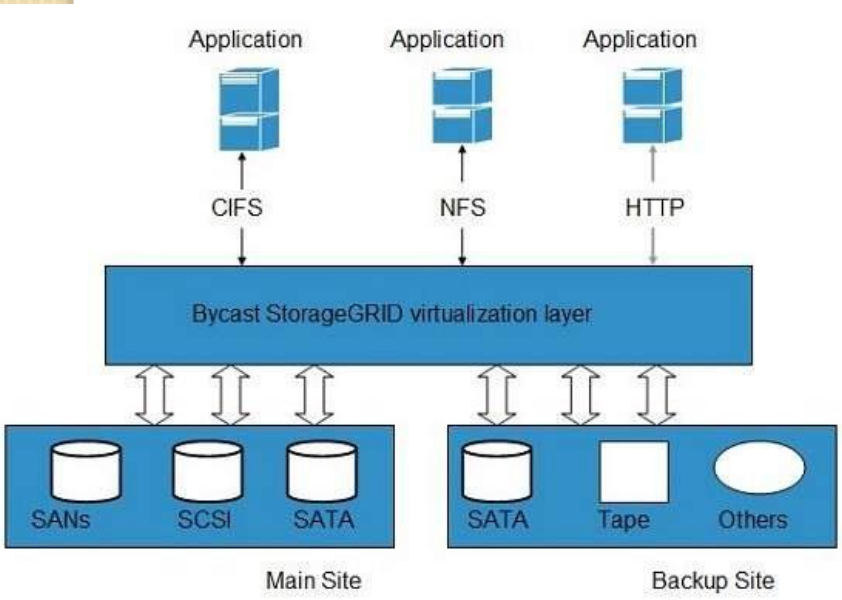
The cloud storage system stores multiple copies of data on multiple servers, at multiple locations. If one system fails, then it is required only to change the pointer to the location, where the object is stored.

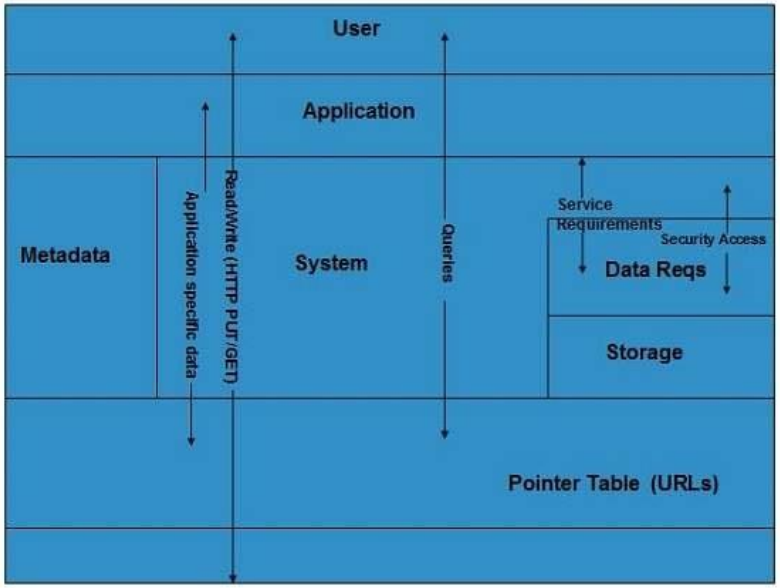
To aggregate the storage assets into cloud storage systems, the cloud provider can use storage virtualization software known as StorageGRID. It creates a virtualization layer that fetches storage from different storage devices into a single management system. It can also manage data from CIFS and NFS file systems over the Internet. The following diagram shows how StorageGRID virtualizes the storage into storage clouds:

Memory Management

Virtual Storage Containers

The virtual storage containers offer high performance cloud storage systems. Logical Unit Number (LUN) of device, files and other objects are created in virtual storage containers. Following diagram shows a virtual storage container, defining a cloud storage domain:





Disaster Recovery

Cloud disaster recovery (cloud DR) is a backup and restore strategy that involves storing and maintaining copies.

Data is the most valuable asset of modern-day organizations. Its loss can result in irreversible damage to your business, including the loss of productivity, revenue, reputation, and even customers. It is hard to predict when a disaster will occur and how serious its impact will be. However, what you can control is the way you respond to a disaster and how successfully your organization will recover from it. Get to discover post how you can use disaster recovery in cloud computing for your benefit.

How does disaster recovery in cloud computing differ from traditional disaster recovery? –
Traditional disaster recovery involves building a remote disaster recovery (DR) site, which requires constant maintenance and support on your part. In this case, data protection and disaster recovery are performed manually, which can be a time-consuming and resource-intensive process. Disaster recovery in cloud computing entails storing critical data and applications in cloud storage and failing over to a secondary site in case of a disaster. Cloud computing services are provided on a pay-as-you-go basis and can be accessed from anywhere and at any time. Backup and disaster recovery in cloud computing can be automated, requiring minimum input on your part.

Disaster Recovery

How does disaster recovery planning work in cloud computing? – Creating, testing, and updating a DR plan can prepare your organization for an unexpected disaster and ensure safety and continuity for your business. A comprehensive DR plan should take into account your infrastructure, potential threats and vulnerabilities, most critical assets and the order of their recovery, and workable DR strategies. Integration of cloud computing services in disaster recovery allows you to design a DR plan and automate each step of the recovery process.

How can NAKIVO Backup & Replication protect your IT infrastructure? – NAKIVO Backup & Replication is a reliable, effective, and affordable data protection solution which can protect VMware, Hyper-V, AWS EC2 and Nutanix environments using backup, backup to cloud, replication, failover, failback, and site recovery.

Read further to discover what makes cloud computing the safest and most versatile approach to disaster recovery.

Disaster Recovery

Backup and Disaster Recovery in Cloud Computing

- Cloud computing is the on-demand delivery of computing services over the internet (more often referred to as 'the cloud') which operates on a pay-as-you-go basis. Cloud computing vendors generally provide access to the following services:

- Infrastructure as a service (IaaS) allows you to rent IT infrastructure, including servers, storages and network component, from the cloud vendor.

- Platform as a service (PaaS) allows you to rent a computing platform from the cloud provider for developing, testing, and configuring software applications.

- Software as a service (SaaS) allows you to access software applications which are hosted on the cloud.

As you can see, each cloud computing service is designed to help you achieve different business needs. More so, cloud computing can considerably improve data the security and high availability of your virtualized workloads. Let's discuss how you can approach disaster recovery in the cloud computing environment.

Capacity Planning

Capacity Planning

Capacity planning seeks to match demand to available resources. Capacity planning examines what systems are in place, measures their performance, and determines patterns in usage that enables the planner to predict demand. Resources are provisioned and allocated to meet demand.

Although capacity planning measures performance and in some cases adds to the expertise needed to improve or optimize performance, the goal of capacity planning is to accommodate the workload and not to improve efficiency. Performance tuning and optimization is not a primary goal of capacity planners.

To successfully adjust a system's capacity, you need to first understand the workload that is being satisfied and characterize that workload. A system uses resources to satisfy cloud computing demands that include processor, memory, storage, and network capacity. Each of these resources has a utilization rate, and one or more of these resources reaches a ceiling that limits performance when demand increases.

It is the goal of a capacity planner to identify the critical resource that has this resource ceiling and add more resources to move the bottleneck to higher levels of demand.

Scaling a system can be done by scaling up vertically to more powerful systems or by scaling out horizontally to more but less powerful systems.

Capacity Planning Steps

1. *Determine the distinctiveness of the present system.*
2. *Determine the working load for different resources in the system such as CPU, RAM, network, etc.*
3. *Load the system until it gets overloaded; & state what's requiring to uphold acceptable performance.*
4. *Predict the future based on older statistical reports & other factors.*
5. *Deploy resources to meet the predictions & calculations.*
6. *Repeat step (i) through (v) as a loop.*

Goal of Capacity Planners

The goal of capacity planners is to identify significant & vital resources that have resource ceiling & add more resources to move the restricted access to higher levels of demand.

Network capacity is one of the hardest factors to resolve & the performance of the network is affected by I/O of the network at the server & network traffic from cloud to ISPs (Internet Service Providers).

Capacity planners try to find the solution to meet future demands on a system by providing additional capacity to fulfill those demands. Capacity planning & system optimization are two both different concepts, and you mustn't mix them as one. Performance & capacity are two different attributes of a system. Cloud 'capacity' measures & concerns about how much workload a system can hold whereas 'performance' deals with the rate at which a task get performed.