# Module 4

**Syllabus:** Cloud Computing and Virtualization Cloud Enabling Technologies, Characteristics of Cloud Computing, Benefits of Cloud Computing, Cloud Service Models, Cloud Deployment Models, Cloud Computing Infrastructure, Cloud Challenges and Cloud Adoption Considerations. **Virtualization Appliances**: Black Box Virtualization, In-Band Virtualization Appliances, Outof-Band Virtualization Appliances, High Availability for Virtualization Appliances, Appliances for Mass Consumption. **Storage Automation and Virtualization**: Policy-Based Storage Management, Application-Aware Storage Virtualization, Virtualization-Aware Applications.

Text Book-1 Ch13: 13.1 to 13.8. Text Book-2 Ch9: 9.1 to 9.5 Ch13: 13.1 to 13.3

# Cloud Computing

*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*

## 13.1 Cloud Enabling Technologies

Grid computing, utility computing, virtualization, and service-oriented architecture are enabling technologies of cloud computing.

- *Grid computing* is a form of distributed computing that enables the resources of numerous heterogeneous computers in a network to work together on a single task at the same time. Grid computing enables parallel computing and is best for large workloads.
- *Utility computing* is a service-provisioning model in which a service pro- vider makes computing resources available to customers, as required, and charges them based on usage. This is analogous to other utility services, such as electricity, where charges are based on the consumption.

- *Virtualization* is a technique that abstracts the physical characteristics of IT resources from resource users. It enables the resources to be viewed and managed as a pool and lets users create virtual resources from the pool. Virtualization provides better flexibility for provisioning of IT resources compared to provisioning in a non-virtualized environment. It helps optimize resource utilization and delivering resources more efficiently.
- *Service Oriented Architecture* (SOA) provides a set of services that can com- municate with each other. These services work together to perform some activity or simply pass data among services.

## 13.2 Characteristics of cloud computing

A computing infrastructure used for cloud services must have certain capabili-ties or characteristics. According to NIST, the cloud infrastructure should have five essential characteristics:

**On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction with each service provider. A cloud service provider publishes a service catalogue, which contains information about all cloud services available to consumers. The service catalogue includes information about service attributes, prices, and request processes. Consumers view the service catalogue via a web-based user

interface and use it to request for a service. Consumers can either lever- age the "ready-to-use" services or change a few service parameters to customize the services.

**Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, tablets, laptops, and workstations).

**Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned

and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (for example, country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.

**Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward com- mensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

**Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstrac- tion appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

## 13. 3 Benefits of Cloud Computing

Cloud computing offers the following key benefits:

- **Reduced IT cost:** Cloud services can be purchased based on pay-per-use or subscription pricing. This reduces or eliminates the consumer's IT capital expenditure (CAPEX).
- **Business agility:** Cloud computing provides the capability to allocate and scale computing capacity quickly. Cloud computing can reduce the time required to provision and deploy new applications and services from months to minutes. This enables businesses to respond more quickly to market changes and reduce time-to-market.
- **Flexible scaling:** Cloud computing enables consumers to scale up, scale down, scale out, or scale in the demand for computing resources easily. Consumers can unilaterally and automatically scale computing resources without any interaction with cloud service providers. The flexible service provisioning capability of cloud computing often provides a sense of unlimited scalability to the cloud service consumers.
- **High availability:** Cloud computing has the capability to ensure resource availability at varying levels depending on the consumer's policy and priority. Redundant infrastructure components (servers, network paths, and storage equipment, along with clustered software) enable fault tolerance for cloud deployments. These techniques can encompass multiple data centers located in different geographic regions, which prevents data unavailability due to regional failures.

13.4 Cloud Service Models

According to NIST, cloud service offerings are classifi ed primarily into three models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

### 13.4.1 Infrastructure-as-a-Service

IaaS is the base layer of the cloud services stack (see Figure 13-1 [a]). It serves as the foundation for both the SaaS and PaaS layers.

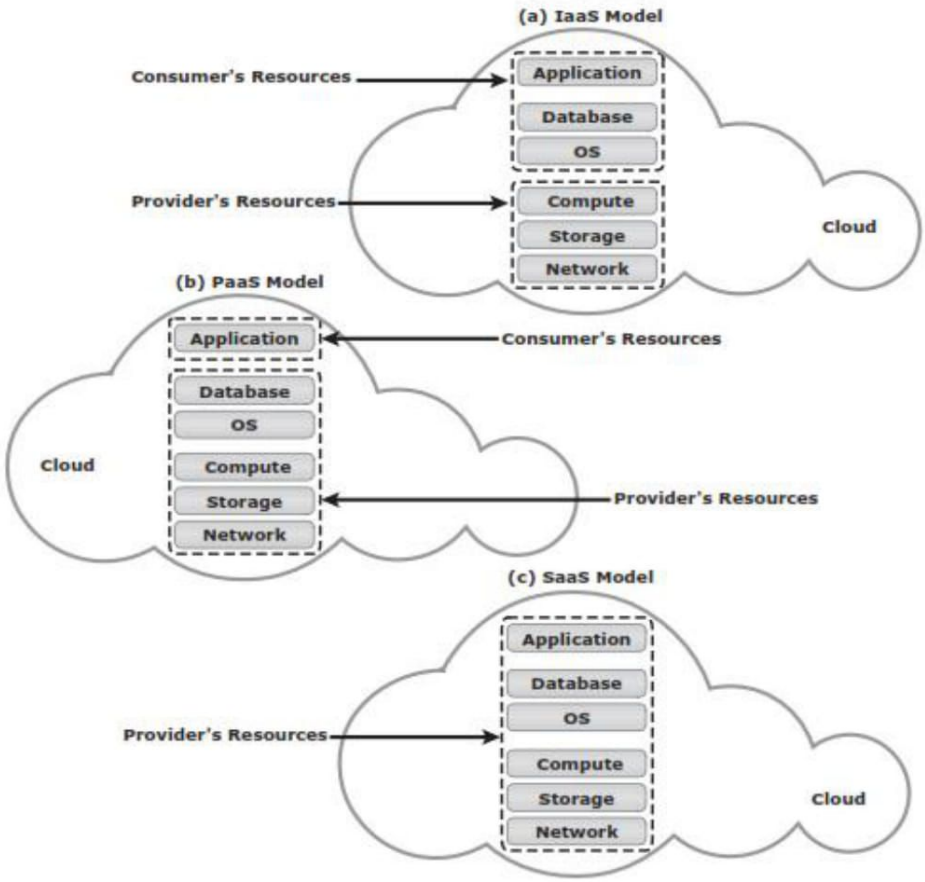



**Figure 13-1:** IaaS, PaaS, and SaaS models

Amazon Elastic Compute Cloud (Amazon EC2) is an example of IaaS that provides scalable compute capacity, on-demand, in the cloud. It enables consumers to leverage Amazon's massive computing infrastructure with no up-front capital investment.

13. 4. 2 Platform-as-a-Ser vice

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, braries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (See Figure 13-1[b]).

PaaS is also used as an application development environment, offered as aservice by the cloud service provider. The consumer may use these platforms to code their applications and then deploy the applications on the cloud.

13. 4. 3 Software-as-a-Ser vice

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based e-mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings(See Figure 13-1[c]).

In a SaaS model, applications, such as customer relationship management (CRM), e-mail, and instant messaging (IM), are offered as a service by the cloud service providers. The cloud service providers exclusively manage the required computing infrastructure and software to support these services.

13.5 Cloud Deployment Models

According to NIST, cloud computing is classified into four deployment models — public, private, community, and hybrid — which provide the basis for how cloud infrastructures are constructed and consumed.

13.5.1 Public Cloud

In a ***public cloud*** model, the cloud infrastructure is provisioned for open usemby the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Consumers use the cloud services offered by the providers via the Internet and pay metered usage charges or subscription fees. An advantage of the public cloud is its low capital cost with enormous scalability. However, for consumers, these benefits come with certain risks: no control over the resources in the cloud, the security of confidentiality data, network performance, and interoperability issues. Popular public cloud service providers are Amazon, Google and

Salesforce.com. Figure 13-2 shows a public cloud that provides cloud services organizations and individuals.

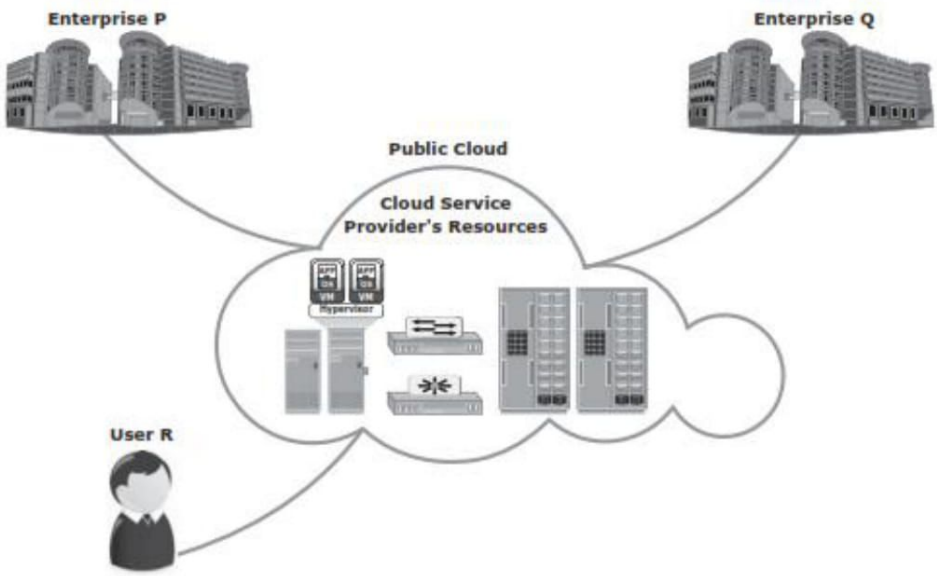



**Figure 13-2:** Public cloud

13.5.2 Private Cloud

In a *private cloud* model, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (for example, business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Following are two variations to the private cloud model:

**On-premise private cloud:** The on-premise private cloud, also known as internal cloud, is hosted by an organization within its own data centers (see Figure 13-3 [a]). This model enables organizations to standardize their cloud service management processes and security, although this model has limitations in terms of size and resource scalability. Organizations would also need to incur the capital and operational costs for the physical resources. This is best suited for organizations that require complete control over their applications, infrastructure configurations, and security mechanisms.

**Externally hosted private cloud:** This type of private cloud is hosted external to an organization (see Figure 13-3 [b]) and is managed by a third- party organization. The third-party

organization facilitates an exclusive cloud environment for a specifi c organization with full guarantee of privacy and confidentiality.

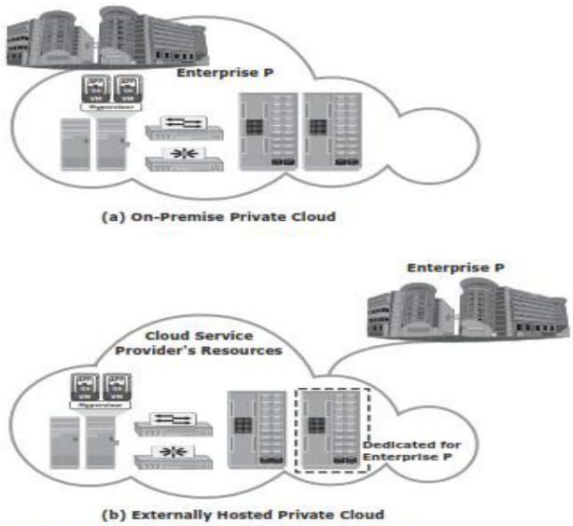



**Figure 13-3:** On-premise and externally hosted private clouds

13.5.3 Community Cloud

In a *community cloud* model, the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (for example, mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. (See Figure 13-4).

In a community cloud, the costs spread over to fewer consumers than a public cloud. Hence, this option is more expensive but might offer a higher level of privacy, security, and compliance. The community cloud also offers organizations access to a vast pool of resources compared to the private cloud.

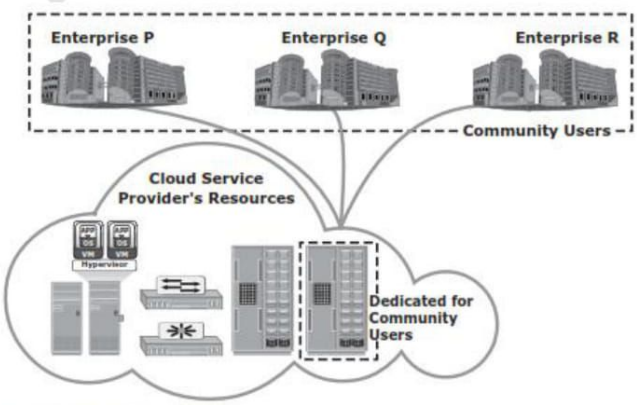



**Figure 13-4:** Community cloud

13.5.4 Hybrid Cloud

In a *hybrid cloud* model, the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (for example, cloud bursting for load balancing between clouds).

The hybrid model allows an organization to deploy less critical applications and data to the public cloud, leveraging the scalability and cost-effectiveness of the public cloud. The organization's mission-critical applications and data remain on the private cloud that provides greater security. Figure 13-5 shows an example of a hybrid cloud.

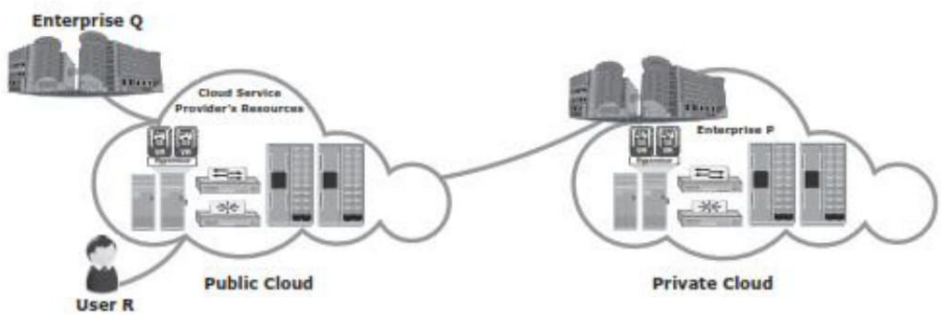



**Figure 13-5:** Hybrid cloud

13.6 Cloud Computing Infrastructure

A cloud computing infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. Cloud computing infrastructure usually consists of the following layers:

- Physical infrastructure
- Virtual infrastructure
- Applications and platform software
- Cloud management and service creation tools

13.6.1 Physical Infrastructure

The physical infrastructure consists of physical computing resources, which include physical servers, storage systems, and networks. Physical servers are connected to each other, to the storage systems, and to the clients via networks, such as IP, FC SAN, IP SAN, or FCoE networks.

Cloud service providers may use physical computing resources from one or more data centers to provide services. If the computing resources are distributed across multiple data centers, connectivity must be established among them. The connectivity enables the data centers in different locations to work as a single large data center. This enables migration of business applications and data across data centers and provisioning cloud services using the resources from multiple data centers.

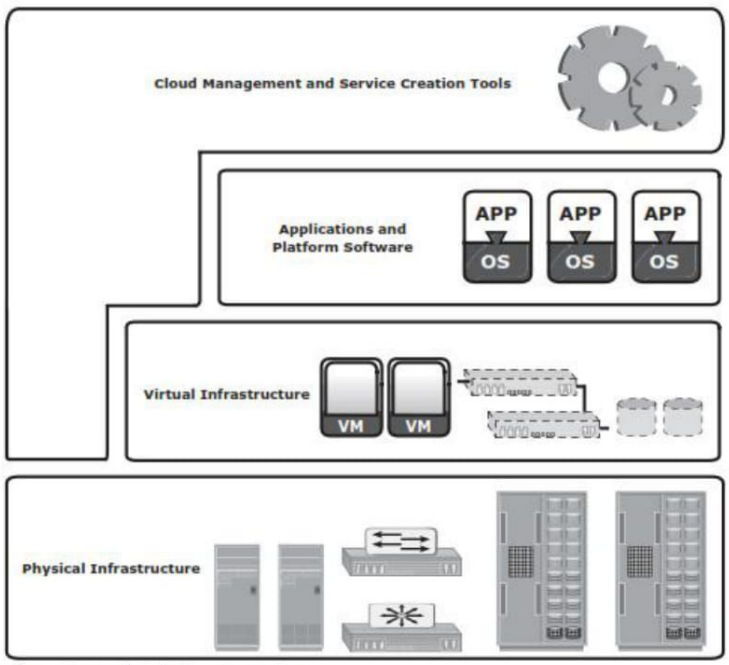



**Figure 13-6:** Cloud infrastructure layers

## 13.6.2 Virtual Infrastructure

- Cloud service providers employ virtualization technologies to build a virtual infrastructure layer on the top of the physical infrastructure.
- Virtualization enables fulfilling some of the cloud characteristics, such as resource pooling
  and rapid elasticity. It also helps reduce the cost of providing the cloud services.

- Virtualization abstracts physical computing resources and provides a consolidated view of the resource capacity.
- The
- Consolidated resources are managed as a single entity called a *resource pool*. For example, a resource pool might group CPUs of physical servers within a cluster.
- The capacity of the resource pool is the sum of the power of all CPUs (for example, 10,000 megahertz) available in the cluster.
- In addition to the CPU pool, the virtual infrastructure includes other types of resource pools, such as memory pool, network pool, and storage pool.
- Apart from resource pools, the virtual infrastructure also includes *identity pools*, such as VLAN ID pools and VSAN ID pools.
- Virtual infrastructure also includes virtual computing resources, such as virtual machines, virtual storage volumes, and virtual networks.
- These resources obtain capacities, such as CPU power, memory, network bandwidth, and storage space from the resource pools.
-

### 13.6.3 Applications and Platform Software

- This layer includes a suite of business applications and platform software, such as the OS and database.
- Platform software provides the environment on which business applications run.
- Applications and platform software are hosted on virtual machines to create SaaS and PaaS.

### 13.6.4 Cloud Management and Service Creation Tools

The cloud management and service creation tools layer includes three types of software:

- Physical and virtual infrastructure management software
- Unified management software
- User-access management software

***The physical and virtual infrastructure management software*** is offered by the vendors of various infrastructure resources and third-party organizations. For example, a storage array has its own management software. Similarly, network and physical servers are managed independently using network and compute management software respectively.

- This software provides interfaces to construct a virtual infrastructure from the underlying physical infrastructure.

- ***Unified management software*** interacts with all standalone physical and virtual infrastructure management software.
- It collects information on the existing physical and virtual infrastructure configurations, connectivity, and utilization.

- Unified management software compiles this information and provides a consolidated view of infrastructure resources scattered across one or more data centers.
- It allows an administrator to monitor performance, capacity, and availability of physical and virtual resources centrally.
- Unified management software also provides a single management interface to configure physical and virtual infrastructure and integrate the compute (both CPU and memory), network, and storage pools.
- The key function of the unified management software is to automate the creation of cloud services.
- It enables administrators to define service attributes such as CPU power, memory, network bandwidth, storage capacity, name and description of applications and platform software, resource location, and backup policy.
- When the unified management software receives consumer requests for cloud services, it creates the service based on predefined service attributes.
- The ***user-access management software*** provides a web-based user interface to consumers.
- Consumers can use the interface to browse the service catalogue and request cloud services.
- The user-access management software authenticates users before forwarding their request to the unified management software.
- It also monitors allocation or usage of resources associated to the cloud service instances.
- Based on the allocation or usage of resources, it generates a chargeback report.
- The chargeback report is visible to consumers and provides transparency between consumers and providers.

## 13.7 Cloud Challenges

### 13.7.1 Challenges for Consumers

- **Security and regulation**
- Consumers are indecisive to transfer control of sensitive data
- Regulation may prevent organizations to use cloud services
- **Network latency**
- Real time applications may suffer due to network latency and limited bandwidth
- **Supportability**
- Service provider might not support proprietary environments
- Incompatible hypervisors could impact VM migration
- **Vendor lock-in**
- Restricts consumers from changing their cloud service providers
- Lack of standardization across cloud-based platforms

Business-critical data requires protection and continuous monitoring of its access. If the data moves to a cloud model other than an on-premise private cloud, consumers could lose absolute control of their sensitive data. Although most of the cloud service providers offer enhanced data security, consumer might not be willing to transfer control of their business-critical data to the cloud.

Cloud service providers might use multiple data centers located in different countries to provide cloud services. They might replicate or move data across these data centers to ensure high availability and load distribution. Consumers may or may not know in which country their data is stored.

Cloud services can be accessed from anywhere via a network. However, network latency increases when the cloud infrastructure is not close to the access point. A high network latency can either increase the application response time or cause the application to timeout. This can be addressed by implementing stringent Service Level Agreements (SLAs) with the cloud service providers.

Another challenge is that cloud platform services may not support consumers' desired applications. For example, a service provider might not be able to support highly specialized or proprietary environments, such as compatible Oss and preferred programming languages, required to develop and run the consumer's application. Also, a mismatch between hypervisors could impact migration of virtual machines into or between clouds.

Another challenge is vendor lock-in: the difficulty for consumers to change their cloud service provider. A lack of interoperability between the APIs of different cloud service providers could also create complexity and high migration costs when moving from one service provider to another.

## 13.7.2 Challenges for Providers

- **Service warranty and service cost**
- Resources must be kept ready to meet unpredictable demand
- Hefty penalty, if SLAs are not fulfilled
- **Complexity in deploying vendor software in the cloud**
- Many vendors do not provide cloud-ready software licenses
- Higher cost of cloud-ready software licenses
- 
- **No standard cloud access interface**
- Cloud consumers want open APIs
- Need agreement among cloud providers for standardization

Cloud service providers usually publish a service-level agreement (SLA) so that their consumers know about the availability of service, quality of service, downtime compensation, and legal and regulatory clauses. Alternatively, customer-specific SLAs may be signed between a cloud service provider and a consumer. SLAs typically mention a penalty amount if cloud service providers fail to provide the service levels. Therefore, cloud service providers must ensure that they have adequate resources to provide the required levels of services. Because the cloud resources are distributed and service demands fluctuate, it is a challenge for cloud service providers to provision physical resources for peak demand of all consumers and estimate the actual cost of providing the services.

Many software vendors do not have a cloud-ready software licensing model. Some of the software vendors offer standardized cloud licenses at a higher price compared to traditional licensing models. The cloud software licensing complexity has been causing challenges in deploying vendor software in the cloud. This is also a challenge to the consumer.

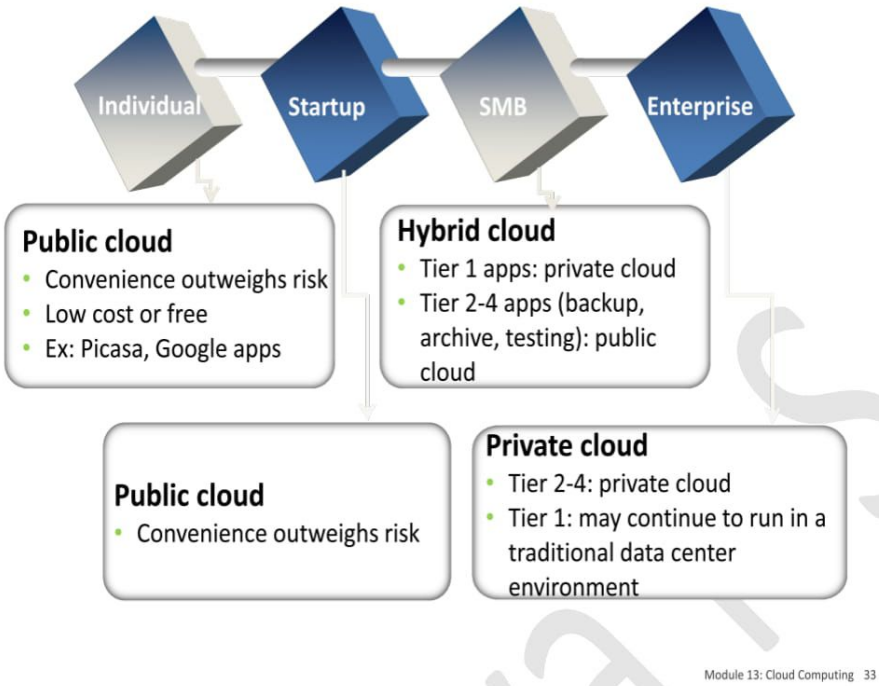
Cloud service providers usually offer proprietary APIs to access their cloud. However, consumers might want open APIs or standard APIs to become the tenant of multiple clouds. This is a challenge for cloud service providers because this requires agreement among cloud service providers.

## 13.8 Cloud Adoption Considerations

**Cloud Adoption Considerations**

- CIOs/IT Managers seeking to move to the cloud face several questions:
  - Which deployment model fits organization's requirements?
    - Private, public, hybrid
  - Which are the applications suitable for cloud?
  - How do I choose the cloud service provider?
  - Is the cloud infrastructure capable of providing the required Quality of Service (QoS)?
    - Performance, availability, and security
  - What is the financial benefit in adopting cloud?

**Selection of a deployment model:**




**Application suitability:**

- Some key questions to ask before migrating a consumer application to the public cloud:
  - Is the application compatible to cloud platform software? Is it a legacy application?
  - Is the application proprietary and mission-critical? Does the application provide competitive advantage?
  - Is the application workload network traffic intensive? Will application performance be impacted by network latency and limited network bandwidth?
  - Does the application communicate with other data center resources or applications?

**Financial advantage:**

- Require analysis of financial benefits in adopting cloud
- Consider CAPEX and OPEX to deploy and maintain own infrastructure versus cloud-adoption cost

**Selection of a cloud service provider:**

- Some key questions to ask before selecting a provider:

- How long and how well has the provider been delivering the services?
- How well does the provider meet the organization's current and future requirements?
- How easy is it to add or remove services?
- How easy is it to move to another provider, when required?
- What happens when the provider upgrades their software? Is it forced on everyone? Can you upgrade on your own schedule?
- Does the provider offer the required security services?
- Does the provider meet your legal and privacy requirements?
- Does the provider have good customer service support?

**Service-level agreement (SLA):**

- Consumers should check whether the QoS attributes meet their requirements
- SLA is a contract between the cloud service provider and consumers that defines QoS attributes
  - Attributes examples: throughput, uptime, and so on

# VIRTUALIZATION APPLIANCES

- A virtual appliance is a software application residing and operating in a preconfigured virtual environment or platform.
- Storage virtualization appliances offer a means to pool storage assets and automate data replication, snapshot and other storage operation.
- Device with plug and play capability.
- Virtual appliances are accessed remotely by users and do not require locally-installed hardware.
- Variety of protocols like fibre channel, ISCSI, IP are supported by the host to access the appliances

## 9.1 Black box virtualization

- Virtualization appliances may exists as hardware processing platform that run an OS and Software and provide a variety of interconnects for attaching to SCSI, Fibre Channel or iSCSI environments.
- The appliance is attached to the network as a peer end device or inserted in-line between storage and servers.
- Appliance architecture vary from vendor to vendor.
- It can accommodate a variety of heterogeneous OS, host platform, storage target from different vendors.
- For enterprise data center the connectivity is done to the **fibre channel SAN's**
- For medium and small business the connectivity is done to **SCSI storage devices or a mix of parallel SCSI and Fibre channel array.**


## 9.2 In-Band Virtualization appliances

- Storage virtualization works on **control information** about where virtualized data storage actually exists and the transport of the actual data itself to and from the virtualized storage.
- **In-band virtualization appliances combine control information and data transport over the same path.**
- In a networked environment the control information in the form of meta data and the data is transmitted along the same path.
- In-line or in-band virtualization may be implemented in an number of ways depending on the type of storage targets and block access protocols used.

- For Fibre channel environments, in-band virtualization may split the storage network into 2 separate fabrics :
  - Host connectivity to the appliance
  - Appliance connectivity to storage targets.
- Server platforms have no direct access to physical storage arrays but communicate through the virtualization appliances.
- The virtualization appliance appear as a storage target to the fabric switch
- Fabric switch connects the server and presents target ID's and virtualized LUN's to the server fabric.
- For physical storage devices on the storage fabric the **appliances appears as an initiator** proxying multiple servers.

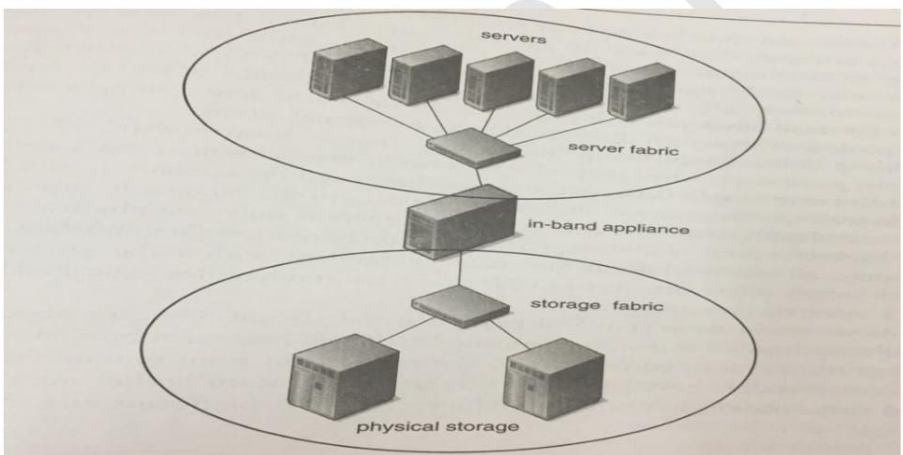



*Figure 9.1 An in-band storage virtualization appliance may sit directly between separate Fibre Channel fabrics to physically segregate servers from the storage targets.*

- **Ethernet attached host in-band virtualization.**
- **Block storage access over ethernet** is accomplished using iSCSI or vendor specific IP block protocols

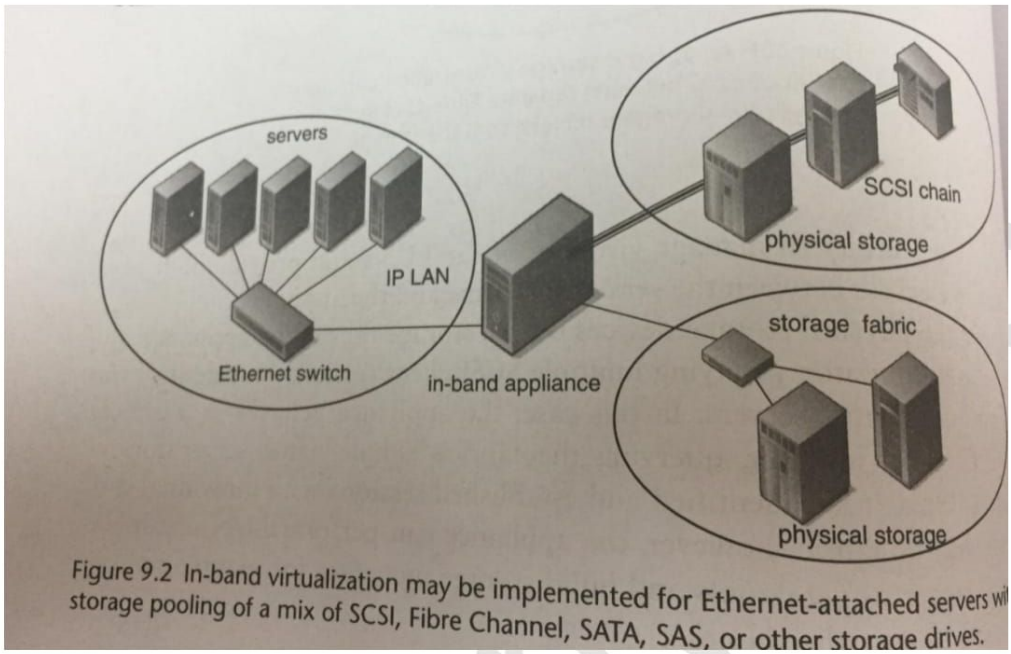



Figure 9.2 In-band virtualization may be implemented for Ethernet-attached servers wi storage pooling of a mix of SCSI, Fibre Channel, SATA, SAS, or other storage drives.

- **Backend storage access** may be through fibre channel, parallel SCSI, SATA or other disk protocols.
- Some in-band appliance solutions may require **host resident software drivers** particularly when proprietary protocols are used.
- Control metadata may be split between the server client and the appliance.
- Alternately all control information may be resident within the appliance.
- Advantage
  - Ability to enforce physical separation between the servers and the storage. The appliance acts as an intermediate between initiator and target.
  - It prevents servers from independently discovering and attaching to SAN based storage assets.
  -
- Dis Advantage

- In in-band virtualization the appliance itself will become a bottleneck for storage transaction *particularly as the traffic load from multiple servers increases.*
- As a solution, in-band virtualization software is hosted on multi process PC platforms and large amount of Cache memory is maintained.

## 9.3 Out-of-band of virtualization appliances

- Out-of band virtualization appliances use **separate path for control information and data** and thus place the appliance outside the primary path between the servers and the storage.
- An out-of band appliance may attach to an existing fibre channel SAN as a peer on the storage network.
- The control path is between the appliance and each SAN attached server switched directly through the fabric.
- Storage data doesn't pass through the appliance but traverses through the fabric directly between the storage and the servers.

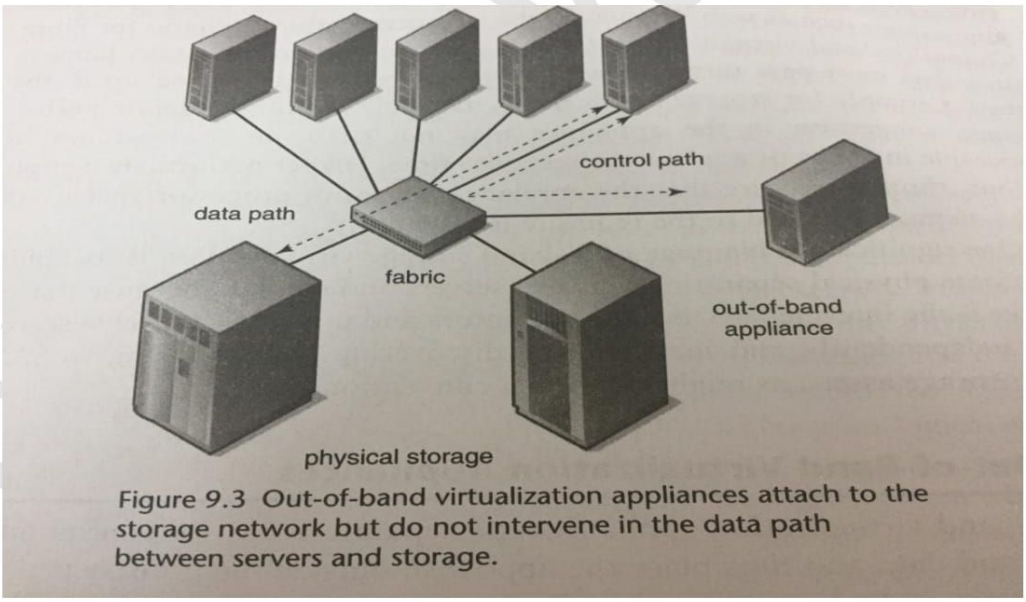



Figure 9.3 Out-of-band virtualization appliances attach to the storage network but do not intervene in the data path between servers and storage.

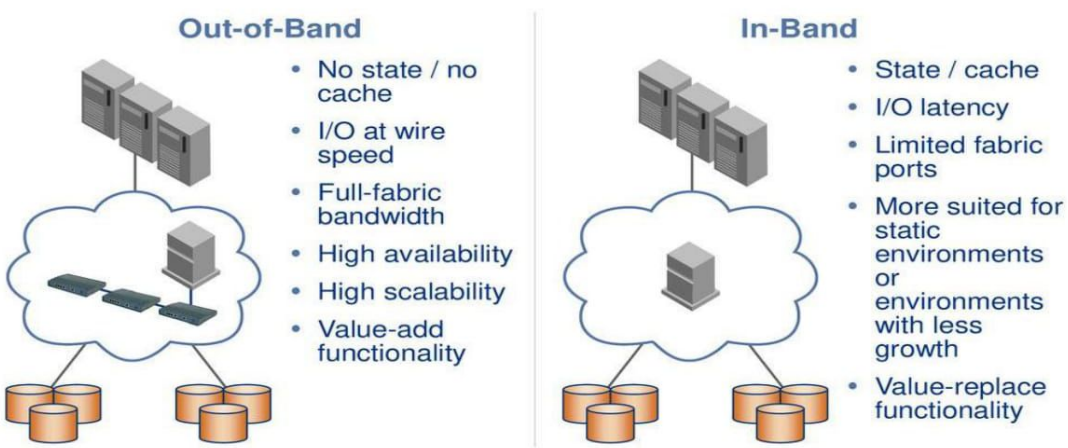
- Out-of band virtualization performance is exclusively dependent on the performance of the SAN switch and the end devices.
- Out-of band virtualization appliances may also require host resident drivers : to maintain the virtualization mapping generated by the appliance and to pass exceptions to the appliance for processing.

- Example: A 256 KB write operation to a striped virtual volume may need to be broken 4 separate 64KB write operations directed to 4 different storage targets.
- **Host-resident software** is required for the server to access the virtualized storage across the network.

Advantage:

- This configuration eliminates the potential bottle neck issue, since only small amount of metadata are exchanged between the appliances and servers.
- Out-of band virtualization appliance require NO significant changes to the SAN infrastructure.
- An out-of band appliance attaches to the SAN discovers the storage assets, configures storage pools and corresponding LUN's and distribute block address mapping metadata to the client servers.

## Comparison of Virtualization Architectures




## 9.4 High availability for virtualization appliances

- Single instance of the virtualization appliance can't meet high availability requirements.
- Therefore implemented distributed appliances solution that enables the task of one appliance to be assumed by another.
- An **active/passive configuration** provides failover in the event that a primary appliance or path is down.

- An **active/active configuration** is preferable, since it utilizes both the appliances and can provide the load balancing in addition to failure.
- A fully redundant in-band solution duplicates all connections, switches and appliances.
- Servers are provided with redundant HBA and thus safeguarded in the event of adapter card failure.
- The server fabric is built with 2 switches each of which has its own links to each server and to the virtualization appliances.
- The storage fabric provide dual pathing between the storage array and redundant switches.
- Both the storage fabric and the server fabric are dual linked with each of the appliances.
- The failure of either appliance or any link to the server or storage will result in failover to the appropriate alternate path or appliance.

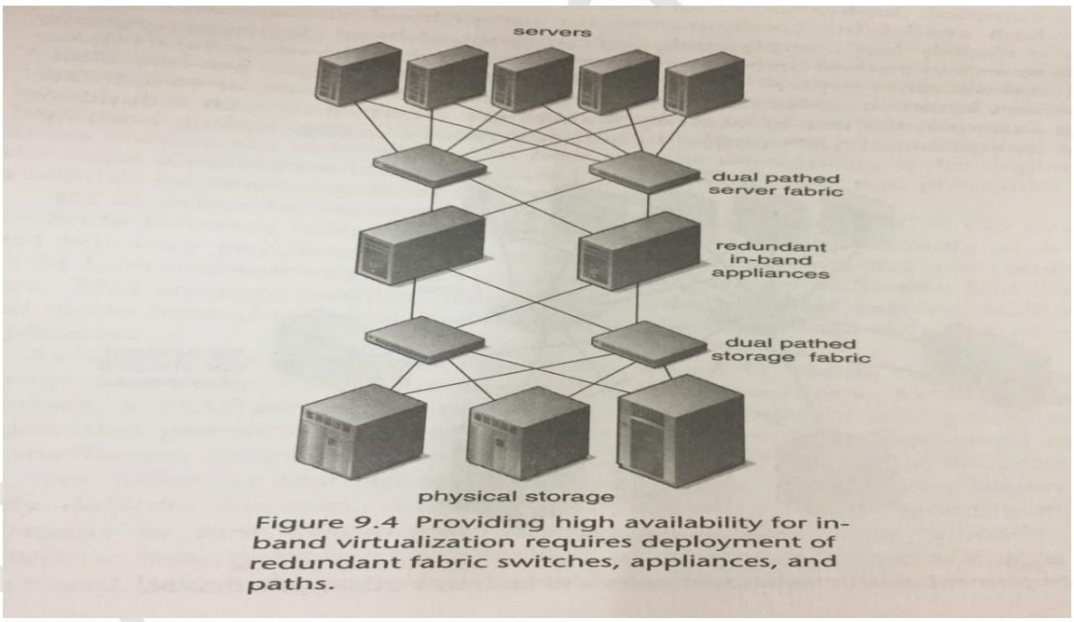



Figure 9.4 Providing high availability for in-band virtualization requires deployment of redundant fabric switches, appliances, and paths.

- It's less complicated compared to in band. The out-of band appliances are attached to each redundant switches.
- Both the in-band and out –of –band high availability configuration could be supplemented with the additional high availability SAN options such as server clustering, virtualization services such as data replications and snapshots.

- Each increment in high availability builds more complexity into the total installation and requires deliberate design and configuration

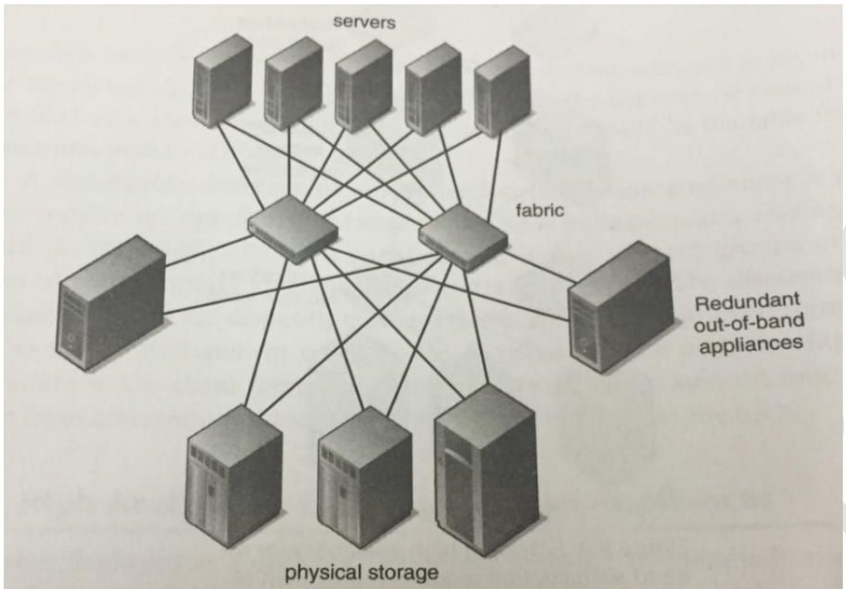



Figure 9.5 High availability for out-of-band appliances can be implemented with redundant units and links to a dual-pathed SAN.

## 9.5 Appliances for mass consumption

- The combination of iSCSI and virtualization technology is enabling low-cost but sophisticated shared storage solutions.

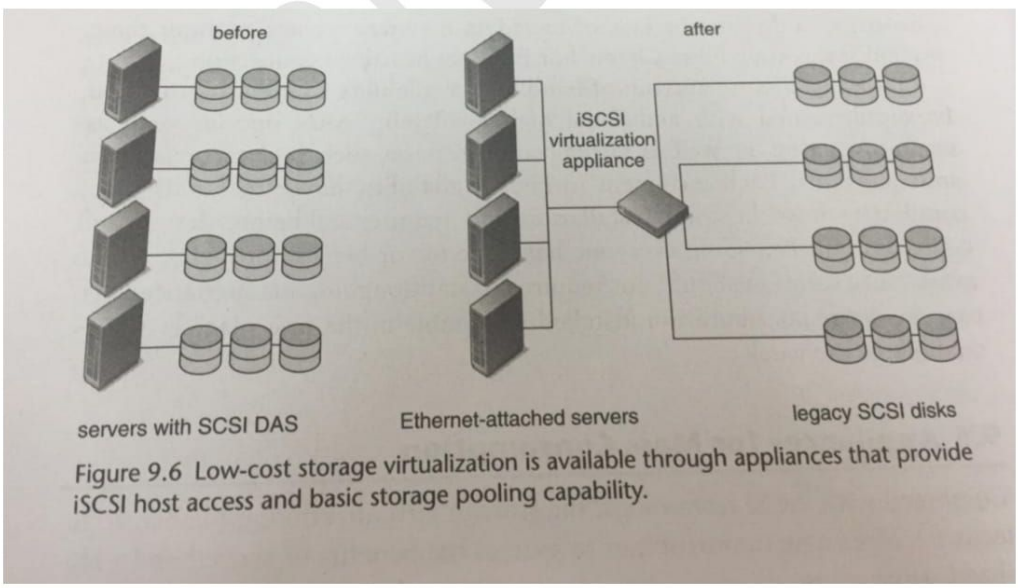



Figure 9.6 Low-cost storage virtualization is available through appliances that provide iSCSI host access and basic storage pooling capability.

- Economical iSCSI virtualization appliances may repurpose legacy direct-attached storage to provide virtualized shared storage.
- Low-cost iSCSI virtualization appliances provide a migration path from small to large shared storage networking.

***Model Questions:***

1. **What is cloud computing? Explain the benefits and characteristics of cloud computing?**
2. **Explain the various cloud service models available**
3. **Explain the cloud computing infrastructure in detail**
4. **Explain In-band and Out-of Band virtualization Appliances**

# MODULE 4
# Chapter 13:
# STORAGE AUTOMATION AND VIRTUALIZATION

# Policy-based management

**Policy-based management is a broad category that includes a diversity of IT resources such as applications, computer platforms, networks, and storage.**

- It is used for aligning underlying technology to business requirements
- **Policy-based management incorporates <u>three basic elements</u>:**

**1. Measurement of actual behavior**

**2. Evaluation of that behavior against predefined *rules* or goals 3. Enforcement through behavior modification.**

- **Goal of policy management initiatives:**
- **Automate IT operations on the basis of specific criteria that align with higher level business requirements**
- **Regulatory compliance example: archived customer information be secured and confidential and retrievable within 24 hours. Identify which transactions are candidates for special treatment, and then to enforce data handling that meets the desired requirements.**

Policy definition may be provided -by an upper layer management platform

- But **policy enforcement** requires a tight integration of management and the complex environment of compute resources such as network, and storage that supports data transactions.
- Ideally, this integration is provided by a common management interface that combines both management frameworks and a wide spectrum of infrastructure equipment.

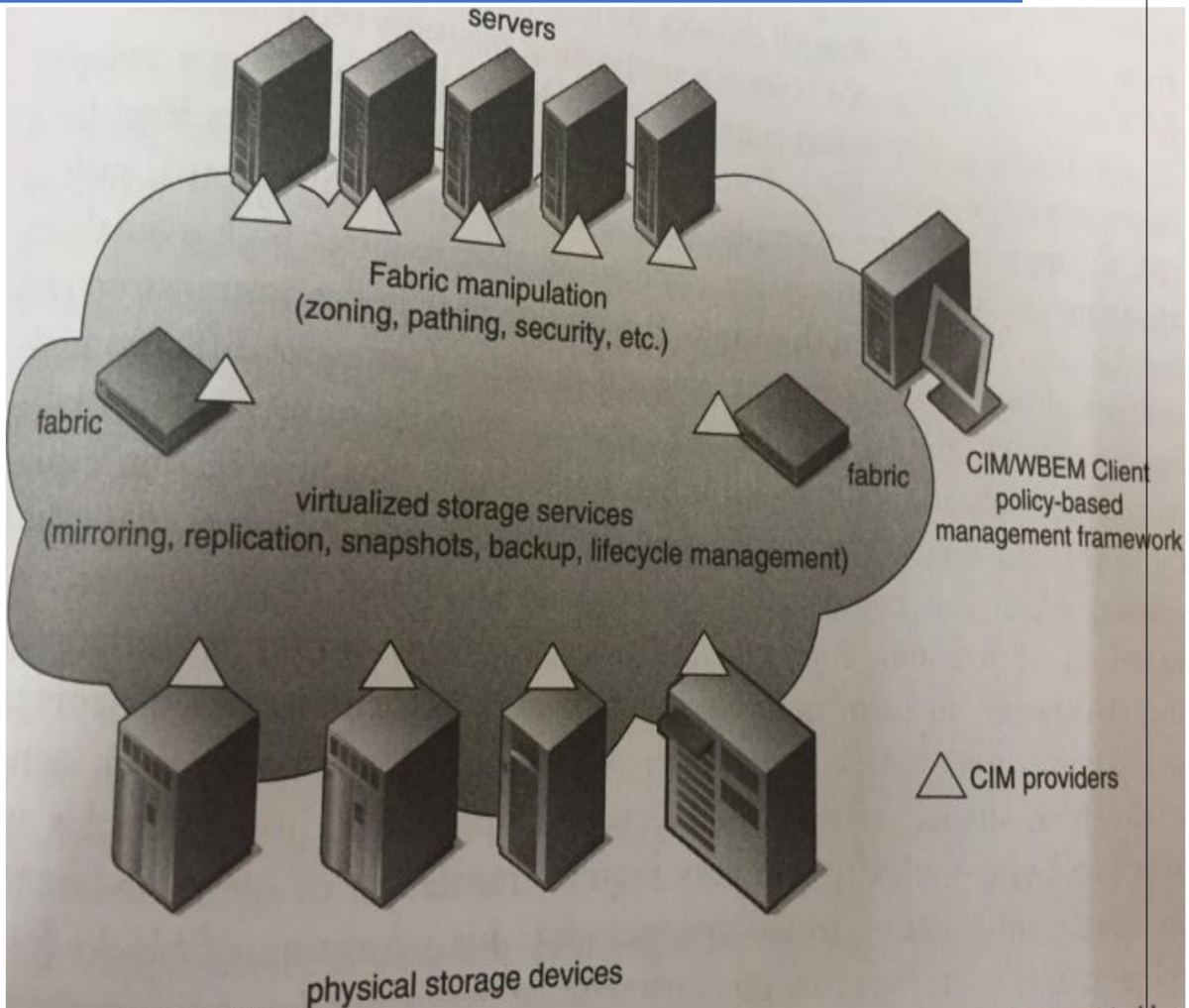
- The effort to define a common management interface for storage is being led by the Storage Networking Industry Association (SNIA).
- The SNIA Storage Management Interface Specification (SMI-S) is based on the common information model (CIM), which was originally developed by another industry group, the Desktop Management Task Force (DMTF).
- The SNIA storage management interface specification (SMI-S) establishes common management structure for heterogeneous SAN's.
- CIM : ***Defines management objects for a wide diversity of network and compute resource. It is managed through web based enterprise management (WBEM) protocol.***

CIM schema includes policy classes for automating IT processes, defining policies and policy execution.

- **Applying CIM/WBEM to storage HBAs, SAN switches, and storage devices requires:**
- **Creation of profiles with classes whose attributes reflect the unique capabilities of each type of product.**
- **A profile for a Fibre Channel switch, for example, may specify parameters for port statistics, device configuration, topology, regardless of manufacturer.**

- **SMI-S Common features**
  - **RAID definition and LUN management,**
  - **Storage virtualization through active management of storage pools**
  - **Mirroring and snapshots between storage systems.**
- The CIM Schema, for example, provides active management method calls such
- CreateOrModify Storage Pool( ) and CreateOrModifyElement From Storage Pool() to generate and resize virtual pools and virtual volumes from them.

- As shown in the diagram CIM/WBEM implementation requires that Physical devices such as HBA's, switches, storage arrays, and tape systems offer standards which are compliant with CIM providers
- Such that CIM can map vendor as specific features generic capabilities
- Example: Techniques for configuring RAID levels, may vary from vendor to vendor, but the CIM provider translates generic- RAID configuration instructions from a CIMWBEM management framework into appropriate commands for a particular vendor.



- Policy-based management must be flexible enough to accommodate changing business requirements as well as changes to the underlying infra-structure.
- Data archiving, for example, may be a phase of a particular policy for data handling.
- If the **archive infrastructure** is changed from disk-to-tape to disk -to-disk-to-tape, that change should be transparent to the upper layer application policy but recognized by lower layer policy objects that interface more directly with physical assets.

- **As shown in the diagram Policy-based management transforms the physical SAN into a collection of services supporting business application requirements.**

- **The physical connectivity of the SAN, pathing, zones, LUNs, and virtual volumes are <u>transparent to policy definition.</u>**

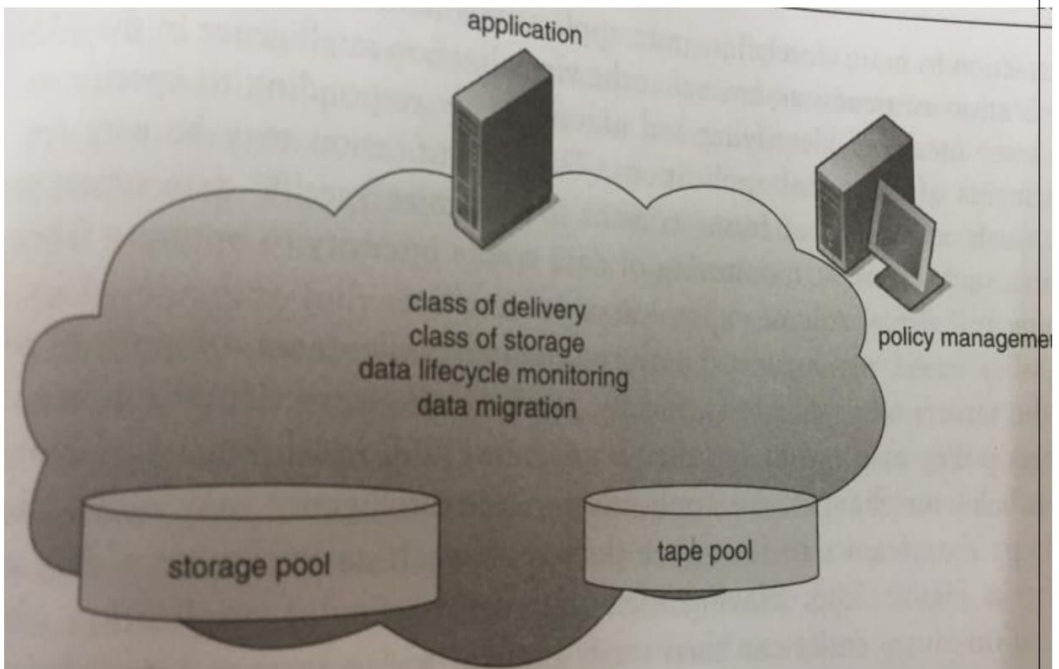



Figure 13.2 Policy-based management is predicated on a hierarchy of policy objec that govern different aspects of a virtualized infrastructure. Services under policy enforcement must be coordinated to accomplish the overall policy goal.

# Application awareness

- **Application awareness** assumes that the virtualization intelligence in the SAN has some means of identifying and automatically responding to specific re-quirements of individual applications.
- That identification may be very spe-cific, such as
  - analysis of frame content to recognize specific data types,
- Or ***generic,*** such as simple monitoring of data traffic intensity to optimize fabric pathing and virtual volume expansion or contraction.
- Policy-based management provides a foundation for tighter integration of applications and storage virtualization.
- An application-aware virtualization entity must identify specific application data types and launch the appropriate policies for data handling.
- Application-aware virtualization must respond to changing application needs, such as capacity requirements and lifecycle management.

- Application aware virtualization automates policy association and then implements additional policies as application behavior changes.
- An application-aware intelligence may index into transport data frames to identify a data type, such as streaming video, as shown in Figure 13.3
  - Once the application is identified application aware entity can then verify that the video stream data is being serviced as per the defined policies.

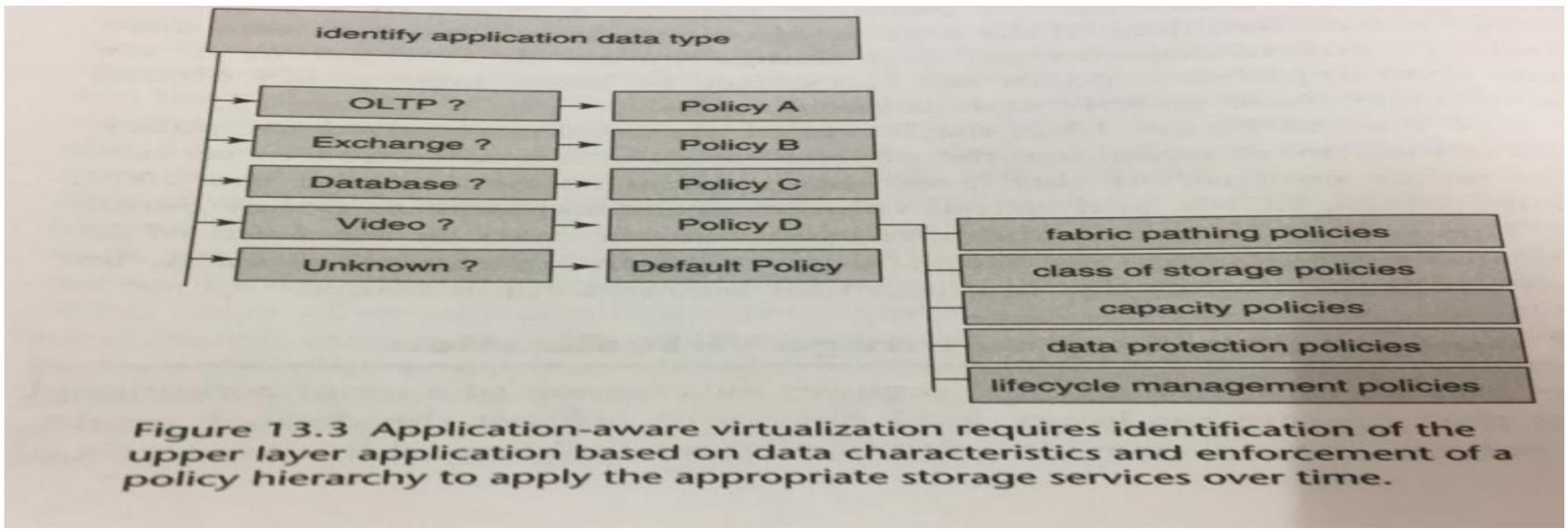



*Figure 13.3 Application-aware virtualization requires identification of the upper layer application based on data characteristics and enforcement of a policy hierarchy to apply the appropriate storage services over time.*

# Virtualization awareness

- **Virtualization awareness within applications simplifies the task of linking applications to storage policy enforcement.**

- Virtualization APIs with an operating system enable upper layer applications to communicate requirements to storage virtualization entities in the SAN.
- Virtualization-awareness facilitates the integration of applications and infrastructure by enabling the application to define its own storage requirements.
- Virtualization-aware applications expand the scope of storage intelligence beyond the SAN .

- As shown in the figure the **storage services requirements such as**
  - **Availability,**
  - **Class of storage,**
  - **Archiving**
- **May be communicated to the SAN via configuration parameters**
- **Configuration parameters are loaded when the application establishes its connection to the SAN.**
- **Those parameters may be processed by the operating system, which in turn leverages the appropriate APIs to communicate with SAN-based virtualization entity.**

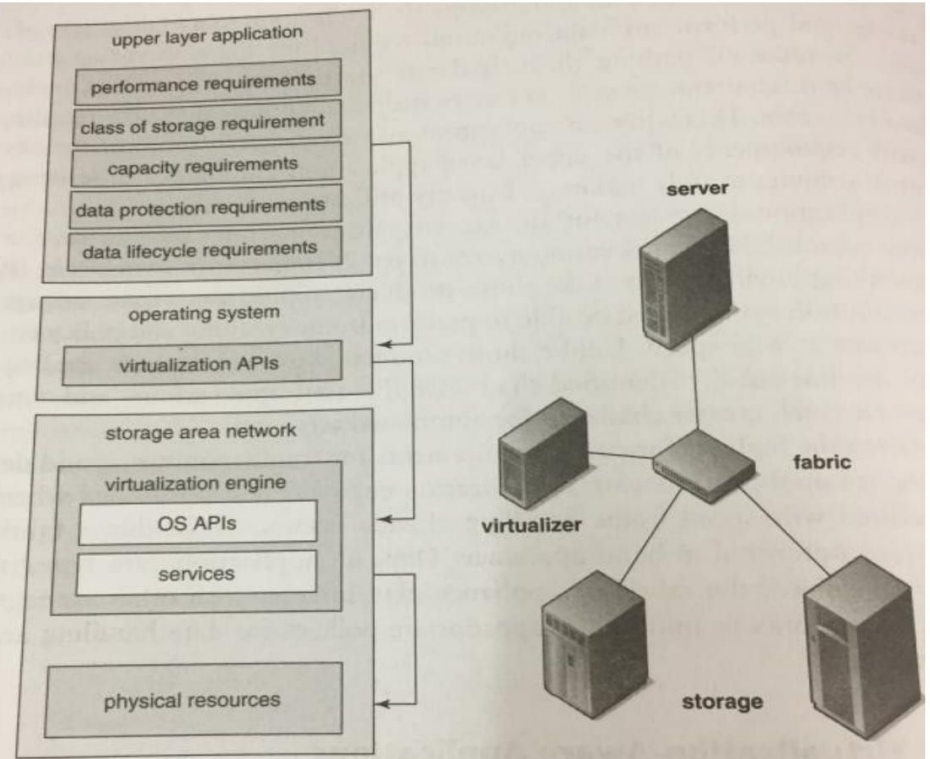



Figure 13.4 A virtualization-aware application may communicate its requirements to the operating system virtualization APIs, which in turn notifies the SAN-based virtualization engine. This configuration puts the application in control of its supporting storage infrastructure.